

WebSphere Edge Server pour multiplateforme



Network Dispatcher - Guide d'administration

Version 2.0

WebSphere Edge Server pour multiplateforme



Network Dispatcher - Guide d'administration

Version 2.0

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à l'«Annexe I. Remarques» à la page 407.

Première édition - octobre 2001

Réf. US : GC31-8496-06

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT". IBM DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE QUALITE MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- <http://www.fr.ibm.com> (serveur IBM en France)
- <http://www.can.ibm.com> (serveur IBM au Canada)
- <http://www.ibm.com> (serveur IBM aux Etats-Unis)

*Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50*

© Copyright IBM France 2001. Tous droits réservés.

© Copyright International Business Machines Corporation 2001. All rights reserved.

Table des matières

Avis aux lecteurs canadiens	xi
--	-----------

Tableaux	xiii
---------------------------	-------------

Figures	xv
--------------------------	-----------

Bienvenue !	xvii
------------------------------	-------------

Envoi des commentaires	xvii
----------------------------------	------

Chapitre 1. Initiation rapide.	1
---	----------

Matériel requis	2
---------------------------	---

Préparation	2
-----------------------	---

Configuration du composant Dispatcher	3
---	---

Configuration à partir de la ligne de commande	4
--	---

Configuration à l'aide de l'assistant de configuration	4
--	---

Configuration à l'aide de l'interface graphique	5
---	---

Test de vérification de la configuration	7
--	---

Types de configurations de grappe, de port et de serveur	8
--	---

Chapitre 2. Installation de Network Dispatcher	11
---	-----------

Configuration requise pour AIX	12
--	----

Installation pour AIX	13
---------------------------------	----

Avant de commencer l'installation	14
---	----

Étapes de la procédure d'installation	14
---	----

Configuration requise pour Red Hat Linux ou SuSE Linux	17
--	----

Installation sous Linux	18
-----------------------------------	----

Avant de commencer l'installation	18
---	----

Étapes de la procédure d'installation	18
---	----

Configuration requise pour Solaris	20
--	----

Installation pour Solaris	21
-------------------------------------	----

Avant de commencer l'installation	21
---	----

Étapes de la procédure d'installation	21
---	----

Configuration requise pour Windows 2000	22
---	----

Installation pour Windows 2000	23
--	----

Modules d'installation	23
----------------------------------	----

Avant de commencer l'installation	24
---	----

Étapes de la procédure d'installation	24
---	----

Chapitre 3. Présentation de Network Dispatcher	27
---	-----------

Principe de Network Dispatcher	27
--	----

Intérêt et avantages de Network Dispatcher	28
--	----

Nouveautés	30
----------------------	----

Composants de Network Dispatcher	35
--	----

Présentation générale du composant Dispatcher	35
---	----

Présentation générale du composant CBR (Content Based Routing)	39
--	----

Présentation générale du composant Mailbox Locator	41
--	----

Présentation générale du composant Site Selector	42
--	----

Présentation générale du composant Consultant for Cisco CSS Switches	44
--	----

Haute disponibilité	46
-------------------------------	----

Dispatcher	46
----------------------	----

CBR, Mailbox Locator, Site Selector	46
---	----

Chapitre 4. Planification du composant Dispatcher	47
--	-----------

Matériel et logiciels requis	47
--	----

Remarques relatives à la planification	48
--	----

Haute disponibilité	50
-------------------------------	----

Haute disponibilité simple	50
--------------------------------------	----

Haute disponibilité réciproque	51
--	----

Réacheminement MAC de Dispatcher (méthode d'acheminement mac)	52
---	----

Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)	52
--	----

Fonction CBR de Dispatcher (méthode d'acheminement cbr)	54
---	----

Chapitre 5. Configuration du composant Dispatcher	57
--	-----------

Présentation générale des tâches de configuration	57
---	----

Méthodes de configuration	57
-------------------------------------	----

Ligne de commande	58
-----------------------------	----

Scripts	58
-------------------	----

Interface graphique	59
-------------------------------	----

Assistant de configuration	60
--------------------------------------	----

Configuration de la machine Dispatcher	60
--	----

Étape 1. Démarrage de la fonction serveur	62
---	----

Etape 2. Démarrage de la fonction exécuteur	63
Etape 3. Définition de l'adresse de non-réacheminement (si différente du nom d'hôte).	63
Etape 4. Définition et configuration des options de la grappe	63
Etape 5. Affectation d'un alias à la carte d'interface réseau	63
Etape 6. Définition des ports et de leurs options.	65
Etape 7. Définition de serveurs avec équilibrage de charge	66
Etape 8. Lancement de la fonction gestionnaire (facultatif)	66
Etape 9. Lancement de la fonction conseiller (facultatif)	67
Etape 10. Définition du niveau d'importance des informations requis pour la grappe	67
Configuration des serveurs pour l'équilibrage de la charge	67
Etape 1. Affectation d'un alias pour l'unité de bouclage	67
Etape 2. Vérification de l'existence d'une route supplémentaire	70
Etape 3. Suppression d'une route supplémentaire	71
Etape 4. Vérification de la configuration du serveur	71
Installation du correctif du noyau Linux (pour supprimer les réponses ARP sur l'interface de bouclage)	72

Chapitre 6. Planification du composant CBR (Content Based Routing)	77
Matériel et logiciels requis	77
Remarques relatives à la planification	77
Equilibrage de charge sur les connexions sécurisées (SSL).	80
Equilibrage de charge client-proxy dans SSL et proxy-serveur dans HTTP	80

Chapitre 7. Configuration du composant CBR	83
Présentation générale des tâches de configuration.	83
Méthodes de configuration	83
Ligne de commande	84
Scripts	85

Interface graphique	86
Assistant de configuration	87
Configuration du poste CBR	88
Etape 1. Configuration de Caching Proxy pour utiliser CBR	88
Etape 2. Démarrage de la fonction serveur	90
Etape 3. Démarrage de la fonction exécuteur	91
Etape 4. Définition et configuration des options de la grappe	91
Etape 5. Affectation d'un alias à la carte d'interface réseau (facultatif)	91
Etape 6. Définition des ports et de leurs options.	92
Etape 7. Définition des serveurs avec équilibrage de charge	93
Etape 8. Ajout de règles à la configuration	93
Etape 9. Ajout de serveurs à vos règles	93
Etape 10. Démarrage de la fonction gestionnaire (facultatif)	93
Etape 11. Démarrage de la fonction conseiller (facultatif)	93
Etape 12. Définition du niveau d'importance des informations requis pour la grappe	94
Etape 13. Démarrage de Caching Proxy	94
Exemple de configuration CBR.	94

Chapitre 8. Planification du composant Mailbox Locator	97
Matériel et logiciels requis	97
Remarques relatives à la planification	98
Utilisation de la fonction d'affinité	99
Remplacement du délai d'inactivité de POP3/IMAP	100

Chapitre 9. Configuration du composant Mailbox Locator	101
Présentation générale des tâches de configuration	101
Méthodes de configuration.	102
Ligne de commande	102
Scripts	103
Interface graphique	103
Assistant de configuration	104
Installation de la machine Mailbox Locator	105
Etape 1. Démarrage de la fonction serveur	105
Etape 2. Définition d'une grappe et configuration des options de la grappe.	105

Etape 3. Définition des ports et configuration des options de port	106
Etape 4. Définition des serveurs avec équilibrage de charge	106
Etape 5. Lancement de la fonction gestionnaire (facultatif)	106
Etape 6. Lancement de la fonction conseiller (facultatif)	106
Etape 7. Définition du niveau d'importance des informations de la grappe	107

Chapitre 10. Planification du composant

Site Selector	109
Matériel et logiciels requis	109
Remarques relatives à la planification	109
Considérations relatives à la durée de vie (TTL)	112
Utilisation de la fonction de proximité réseau (Network Proximity)	112

Chapitre 11. Configuration du composant

Site Selector	115
Présentation générale des tâches de configuration	115
Méthodes de configuration.	115
Ligne de commande	116
Scripts	117
Interface graphique	117
Assistant de configuration	118
Installation de la machine Site Selector.	119
Etape 1. Démarrage de la fonction serveur	119
Etape 2. Démarrage du serveur de noms	119
Etape 3. Définition d'un nom de site et définition des options du nom de site	119
Etape 4. Définition de serveurs avec équilibrage de charge	120
Etape 5. Lancement de la fonction gestionnaire (facultatif)	120
Etape 6. Lancement de la fonction conseiller (facultatif)	120
Etape 7. Définition des mesures du système (facultatif)	120
Etape 8. Définition du niveau d'importance des informations pour le nom de site	121
Configuration des serveurs pour l'équilibrage de la charge	121

Chapitre 12. Planification du composant

Consultant for Cisco CSS Switches	123
Matériel et logiciels requis	123
Remarques relatives à la planification	123

Chapitre 13. Configuration du composant

Consultant for Cisco CSS Switches	129
Présentation générale des tâches de configuration	129
Méthodes de configuration.	130
Ligne de commande	130
Scripts	131
Interface graphique	131
Installation de la machine Consultant for Cisco CSS Switches	132
Etape 1. Lancement de la fonction serveur	133
Etape 2. Configuration de la fonction exécuteur	133
Etape 3. Définition d'une grappe et des options de grappe	133
Etape 4. Définition de ports et des options de port	133
Etape 5. Définition des serveurs avec équilibrage de charge	133
Etape 6. Lancement de la fonction gestionnaire.	134
Etape 7. Lancement de la fonction conseiller (facultatif)	134
Etape 8. Définition du niveau d'importance des informations de la grappe	134
Etape 9. Lancement du système Metric Server (facultatif)	134
Test de vérification de la configuration.	135

Chapitre 14. Fonctions Network

Dispatcher avancées	137
Optimisation de la fonction d'équilibrage de charge fournie par Network Dispatcher	140
Proportion de l'importance accordée aux données d'état	141
Pondérations	142
Intervalles gestionnaire	144
Seuil de sensibilité	144
Index de filtrage	145
Utilisation de scripts pour la génération d'une alerte ou d'une erreur du serveur d'enregistrement	145
Conseillers	146
Fonctionnement des conseillers	146

Lancement et arrêt d'un conseiller	147	Configuration de l'équilibrage basé sur des règles	180
Intervalles conseiller	148	Evaluation des règles	182
Délai de rapport du conseiller	148	Utilisation de règles basées sur l'adresse IP des clients	182
Délai de connexion du conseiller et délai de réception pour les serveurs	148	Utilisation de règles basées sur l'heure	183
Liste des conseillers	149	Utilisation de règles basées sur le nombre de connexions par seconde d'un port	183
Création de conseillers personnalisés	151	Utilisation de règles basées sur le nombre total de connexions actives d'un port	183
Conseiller WebSphere Application Server	152	Utilisation de règles basées sur le port du client	184
Convention d'attribution de nom	153	Utilisation de règles basées sur le type de services (TOS)	184
Compilation	153	Utilisation de règles basées sur la largeur de bande réservée et sur la largeur de bande partagée	185
Exécution	154	Règle Mesure de tous les serveurs	187
Sous-programmes requis	154	Règle Moyenne des mesures	188
Ordre de recherche	155	Utilisation de règles toujours vraies	188
Affectation du nom et du chemin	155	Utilisation de règles basées sur le contenu des demandes	189
Conseiller type.	155	Ajout de règles à la configuration	189
Conseiller Workload Manager.	155	Option d'évaluation de serveur	190
Restrictions relatives à Metric Server	156	Utilisation de liens explicites	191
Metric Server	157	Utilisation d'une configuration réseau privée	191
Restrictions relatives à WLM	157	Utilisation d'une grappe générique pour combiner les configurations serveurs	193
Conditions préalables	157	Utilisation de la grappe générique pour équilibrer la charge des pare-feux	193
Conditions d'utilisation de Metric Server	157	Utilisation de grappe générique avec Caching Proxy pour le proxy transparent	194
Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)	159	Utilisation du port générique pour acheminer le trafic destiné à un port non configuré	195
Option de demande/réponse (URL) de conseiller HTTP	161	Fonctionnement de la fonction d'affinité pour Network Dispatcher	195
Utilisation de serveurs implantés au même endroit	162	Comportement lors de la désactivation de l'affinité	195
Pour le composant Dispatcher	162	Comportement lors de l'activation de l'affinité	195
Composant CBR	163	API SDA pour le contrôle de l'affinité client/serveur	196
Pour le composant Mailbox Locator.	163	Affinité trans ports	197
Pour le composant Site Selector	164	Masque d'adresse de l'affinité.	198
Pour le composant Cisco Consultant	164	Substitution d'affinité de règle	199
Configuration du support de réseau étendu pour Dispatcher	164	Mise au repos de la gestion des connexions avec maintien de routage	199
Syntaxe des commandes	165	Option d'affinité de la commande rule.	200
Utilisation de conseillers éloignés avec le support de réseau étendu	166	Affinité de cookie actif	200
Exemple de configuration	168		
Remarques	170		
Support GRE (Generic Routing Encapsulation).	171		
Utilisation d'un conseiller Self dans une configuration WAND à deux niveaux	172		
Haute disponibilité	173		
Configuration de la haute disponibilité	173		
Détections des incidents en utilisant signal de présence et cible à atteindre	176		
Stratégie de reprise	177		
Utilisation de scripts	178		

Affinité de cookie passif	202
Affinité d'URI	203
Détection d'attaque de refus de service	204
Utilisation de la journalisation binaire pour analyser les statistiques des serveurs	205
Informations supplémentaires sur les fonctions Cisco Consultant avancées	208
Pondérations de Cisco Consultant	209

Chapitre 15. Exploitation et gestion de Network Dispatcher 213

Administration authentifiée à distance	213
Utilisation des journaux Network Dispatcher	215
Modification des chemins des fichiers journaux	216
Utilisation du composant Dispatcher	217
Lancement et arrêt de Dispatcher	217
Utilisation de la valeur du délai d'attente	217
Utilisation du décompte FIN pour contrôler la collecte des données obsolètes	218
Interface graphique — option de menu Contrôler	218
Utilisation du protocole SNMP (Simple Network Management Protocol) avec le composant Dispatcher	219
Rejet de l'ensemble du trafic vers Network Dispatcher avec la fonction ipchains ou iptables (Linux)	224
Utilisation du composant CBR (Content Based Routing).	225
Lancement et arrêt de CBR.	225
Contrôle de CBR	225
Utilisation des journaux de CBR	225
Utilisation du composant Mailbox Locator	226
Lancement et arrêt de Mailbox Locator	226
Contrôle de Mailbox Locator	226
Utilisation des journaux Mailbox Locator	226
Utilisation du composant Site Selector	226
Lancement et arrêt de Site Selector	226
Contrôle d'Site Selector	226
Utilisation des journaux Site Selector	227
Utilisation du composant Cisco Consultant	227
Lancement et arrêt de Cisco Consultant	227
Contrôle de Cisco Consultant	227
Utilisation des journaux Cisco Consultant	227
Utilisation du composant Metric Server	227
Lancement et arrêt de Metric Server	227
Utilisation des journaux Metric Server	228

Chapitre 16. Résolution des incidents 229

Tableaux de résolution des incidents	229
Vérification des numéros de port de Dispatcher	235
Vérification des numéros de port de CBR	236
Vérification des numéros de port de Mailbox Locator	237
Vérification des numéros de port Site Selector	237
Vérification des numéros de port Cisco Consultant	238
Résolution des incidents courants—Dispatcher	239
Incident : Dispatcher ne fonctionne pas	239
Incident : Le répartiteur et le serveur ne répondent pas	239
Incident : les requêtes Dispatcher ne sont pas équilibrées.	239
Incident : la fonction haute disponibilité de Dispatcher est inopérante	240
Incident : Impossible d'ajouter un signal de présence (Windows 2000)	240
Incident : Routes supplémentaires (Windows 2000)	240
Incident : les conseillers ne fonctionnent pas correctement	240
Incident : SNMPD ne semble pas fonctionner correctement (Windows 2000).	240
Incident : Dispatcher, Microsoft IIS et SSL ne fonctionnent pas (Windows 2000)	241
Incident : Connexion du répartiteur à une machine éloignée	241
Incident : échec de la commande ndcontrol ou ndadmin	241
Incident : le message d'erreur "Impossible trouver fichier ..." s'affiche lorsque vous tentez d'afficher l'aide en ligne (Windows 2000)	242
Incident : Message d'erreur incorrect lors du lancement de ndserver sous Solaris 2.7	242
Incident : l'interface graphique ne démarre pas correctement	242
Incident : Erreur lors de l'exécution de Dispatcher lorsque Caching Proxy est installé	243
Incident : l'interface graphique ne s'affiche pas correctement	243
Incident : sous Windows 2000, les fenêtre d'aide disparaissent parfois sous d'autres fenêtres ouvertes	243

Incident: Network Dispatcher ne peut pas traiter et transmettre un cadre	243	Incident : Site Selector ayant des chemins en double pour lequel l'équilibrage de charge ne s'effectue pas correctement	251
Incident : un écran bleu s'affiche lors du lancement de l'exécuteur Network Dispatcher	244	Résolution des incidents courants—Consultant for Cisco CSS Switches	251
Incident : la fonction Path MTU Discovery permet d'éviter le trafic retour avec Network Dispatcher	244	Incident : lbserver ne démarre pas.	251
Incident : les conseillers indiquent que tous les serveurs sont en panne	245	Incident : la commande lbcontrol ou ndadmin n'a pas abouti.	251
Incident : la fonction haute disponibilité de Network Dispatcher en mode réseau étendu est inopérante	245	Incident : impossible de créer un registre sur le port 14099	251
Incident : Arrêt (ou comportement imprévu) de l'interface graphique lors de la tentative de chargement d'un fichier de configuration volumineux	246	Résolution des incidents courants—Metric Server.	252
Résolution des incidents courants—CBR	247	Incident : IOException Metric Server sous Windows 2000 lors de l'exécution de fichiers de mesures utilisateur de format BAT ou CMD	252
Incident : CBR ne fonctionne pas.	247	Incident : Metric Server n'indique pas la charge à la machine Network Dispatcher	252
Incident : les commandes cbrcontrol ou ndadmin n'ont pas abouti	247	Incident : Le journal de la machine Metric Server indique qu'une signature est nécessaire pour accéder à l'agent	252
Incident : les requêtes ne sont pas équilibrées	247		
Incident : sous Solaris, la commande cbrcontrol n'aboutit pas.	247	Annexe A. Lecture d'un schéma de syntaxe	253
Incident : erreur de syntaxe ou de configuration	248	Symboles et ponctuation	253
Résolution des incidents courants—Mailbox Locator	248	Paramètres	253
Incident : Mailbox Locator ne s'exécute pas.	248	Exemples de syntaxe.	254
Incident : la commande mlserver est arrêtée	248		
Incident : la commande mlcontrol ou ndadmin n'a pas abouti.	249	Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator.	257
Incident : impossible d'ajouter un port	249	Différences de configuration entre CBR, Mailbox Locator et Dispatcher	258
Incident : réception d'une erreur proxy lors d'une tentative d'ajout de port	249	ndcontrol advisor — Contrôle du conseiller	260
Résolution des incidents courants—Site Selector	250	ndcontrol cluster — Configuration des grappes	266
Incident : Site Selector ne s'exécute pas	250	ndcontrol executor — Contrôle de l'exécuteur	271
Incident : Site Selector ne permet pas le trafic à permutation circulaire à partir des clients Solaris	250	ndcontrol file — gestion des fichiers de configuration	276
Incident : la commande sscontrol ou ndadmin n'a pas abouti.	250	ndcontrol help — Affichage ou impression de l'aide sur cette commande.	278
Incident : Echec du démarrage de ssserver sous Windows 2000	250	ndcontrol highavailability — Contrôle de la haute disponibilité	280
		ndcontrol host — configuration d'une machine éloignée	285
		ndcontrol log — Contrôle du fichier journal	286
		ndcontrol manager — Contrôle du gestionnaire.	287
		ndcontrol metric — configuration des mesures du système	294

ndcontrol port — Configuration des ports	296
ndcontrol rule — configuration des règles	303
ndcontrol server — Configuration des serveurs	311
ndcontrol set — Configuration du journal du serveur	318
ndcontrol status — Affichage de l'exécution ou non du gestionnaire et des conseillers	319
ndcontrol subagent — Configuration du sous-agent SNMP	320

Annexe C. Syntaxe des règles de contenu (modèle)	323
Syntaxe de règle de contenu (modèle) :	323
Mots clés réservés.	323

Annexe D. Guide des commandes Site Selector	327
sscontrol advisor — Contrôle du conseiller	328
sscontrol file — Gestion des fichiers de configuration	334
sscontrol help — Affichage ou impression de l'aide sur cette commande	336
sscontrol manager — Contrôle du gestionnaire.	337
sscontrol metric — Configuration des mesures du système	342
sscontrol nameserver — Contrôle de NameServer	343
sscontrol rule — Configuration des règles	344
sscontrol server — Configuration des serveurs	348
sscontrol set — Configuration du journal du serveur	350
sscontrol sitename — Configuration d'un nom de site	351
sscontrol status — Affiche si le gestionnaire et les conseillers sont en cours d'exécution	355

Annexe E. Guide des commandes Consultant for Cisco CSS Switches	357
lbcontrol advisor — Contrôle du conseiller	358
lbcontrol cluster — Configuration des grappes	363
lbcontrol executor — Contrôle de l'exécuteur	365
lbcontrol file — Gestion des fichiers de configuration	367

lbcontrol help — Affichage ou impression de l'aide relative à cette commande	369
lbcontrol host — Configuration d'une machine éloignée	370
lbcontrol log — Contrôle du fichier journal binaire	371
lbcontrol manager — Contrôle du gestionnaire.	372
lbcontrol metric — Configuration des mesures du système	378
lbcontrol port — Configuration des ports	380
lbcontrol server — Configuration des serveurs	382
lbcontrol set — Configuration du journal du serveur	384
lbcontrol status — Indique par affichage si le gestionnaire et les conseillers sont en cours d'exécution	385

Annexe F. Exemples de fichiers de configuration	387
Exemples de fichiers de configuration	
Network Dispatcher	387
Dispatcher Fichier de configuration—AIX, Red Hat Linux, et Solaris	387
Dispatcher Fichier de configuration — Windows	391
Conseiller type.	395

Annexe G. Exemple de configuration de haute disponibilité à deux niveaux utilisant Dispatcher, CBR et Caching Proxy	401
Configuration de la machine serveur	401

Annexe H. Ressources supplémentaires	405
Accès à la ligne de commande	405
Obtention de l'aide en ligne	405
Informations de référence	405

Annexe I. Remarques	407
Marques	409

Glossaire	411
------------------	------------

Index	423
--------------	------------

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.








OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
 (Pos1)		Home
Fin	Fin	End
 (PgAr)		PgUp
 (PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
 (Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Tableaux

1. Images installp AIX.	13	11. Exemple de configuration Cisco CSS	
2. Commande AIX relatives à l'installation	16	Switch en correspondance avec la	
3. Tâches de configuration pour la fonction		configuration Consultant	127
Dispatcher.	57	12. Tâches de configuration du composant	
4. Commandes pour l'affectation d'un alias		Consultant for Cisco CSS Switches . . .	129
à l'unité de bouclage (lo0) pour		13. Tâches de configuration avancées pour	
Dispatcher.	68	Network Dispatcher	137
5. Commandes de suppression d'une route		14. Tableau de résolution des incidents de	
supplémentaire pour Dispatcher	71	Dispatcher	229
6. Tâches de configuration pour le		15. Tableau de résolution des incidents de	
composant CBR	83	CBR	232
7. Commandes pour l'affectation d'un alias		16. Tableau de résolution des incidents	
à la carte d'interface réseau	92	Mailbox Locator	233
8. Tâches de configuration du composant		17. Tableau de résolution des incidents de	
Mailbox Locator	101	Site Selector	233
9. Tâches de configuration pour le		18. Tableau de résolution des incidents de	
composant Site Selector	115	Consultant for Cisco CSS Switches . . .	234
10. Configuration de Consultant et de		19. Tableau de dépannage du système	
Cisco CSS Switch	125	Metric Server	234

Figures

1. Configuration Dispatcher locale simple	1	16. Fichier de configuration CBR pour AIX	89
2. Interface graphique	5	17. Fichier de configuration CBR pour Linux	89
3. Exemple de composant Dispatcher configuré avec une grappe et 2 ports	8	18. Fichier de configuration CBR pour Solaris	90
4. Exemple de composant Dispatcher configuré avec deux grappes, chacune associée à un port	9	19. Fichier de configuration CBR pour Windows 2000	90
5. Exemple de composant Dispatcher configuré avec 2 grappes, chacune associée à 2 ports	10	20. Exemple d'environnement DNS	110
6. Exemple de représentation physique d'un site utilisant Dispatcher pour gérer les serveurs locaux	37	21. Exemple de composant Consultant configuré avec deux grappes, chacune étant associée à 3 ports	126
7. Exemple de site utilisant Dispatcher et Metric Server pour gérer les serveurs	38	22. Exemple de configuration consistant en un seul segment de réseau local	164
8. Exemple de site utilisant Dispatcher pour gérer des serveurs locaux et éloignés	39	23. Exemple de configuration utilisant des serveurs locaux et éloignés	165
9. Exemple de site utilisant CBR pour gérer les serveurs locaux	40	24. Exemple de configuration en réseau étendu avec des composants Network Dispatcher éloignés	168
10. Exemple de site utilisant Mailbox Locator pour gérer les serveurs locaux	41	25. Exemple de configuration en réseau étendu avec une plate-forme serveur prenant en charge GRE	171
11. Exemple de site utilisant Site Selector et Metric Server pour gérer les serveurs locaux et éloignés	43	26. Exemple de configuration WAND à deux niveaux utilisant le conseiller self	172
12. Exemple de site utilisant Cisco Consultant et Metric Server pour gérer les serveurs locaux	45	27. Exemple de réseau privé utilisant Dispatcher	192
13. Exemple de Dispatcher utilisant la haute disponibilité	50	28. Commandes SNMP pour AIX et Solaris	220
14. Exemple de Dispatcher utilisant la haute disponibilité réciproque	51	29. Commandes SNMP pour Windows 2000	221
15. Exemple d'adresses IP nécessaires pour la machine Dispatcher	62	30. Exemple de configuration de haute disponibilité à deux niveaux utilisant Dispatcher, CBR et Caching Proxy	401

Bienvenue !

Le présent manuel explique comment installer, configurer, utiliser et dépanner IBM WebSphere Edge Server Network Dispatcher pour AIX, Linux, Solaris et Windows 2000. Ce produit était connu sous le nom SecureWay Network Dispatcher, eNetwork Dispatcher et Interactive Network Dispatcher.

Une version actualisée du présent manuel est disponible aux formats HTML et PDF, sur le site WEB WebSphere Edge Server. Pour consulter la documentation en ligne, accédez à l'URL suivante :

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

Le site WebSphere Edge Server fournit des informations récentes sur l'utilisation de Network Dispatcher dans le cadre de l'optimisation des performances des serveurs. Ce site présente également des exemples et des scénarios de configuration. Pour y accéder, entrez l'URL suivante :

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

Pour obtenir les dernières mises à jour ainsi que des conseils sur Network Dispatcher, visitez la page Web d'assistance WebSphere Edge Server et cliquez sur *Search for Network Dispatcher hints and tips*. Pour accéder à ce site Web, entrez l'URL suivante :

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

Envoi des commentaires

Vos commentaires sont importants dans la mesure où ils nous aident à offrir des informations précises et de qualité. Pour tout commentaire sur ce manuel ou sur toute autre documentation WebSphere Edge Server :

- Envoyez un courrier électronique à fsdoc@us.ibm.com. N'oubliez pas d'inclure le nom du manuel, son numéro de référence, la version de WebSphere Edge et éventuellement l'emplacement du texte sur lequel porte votre commentaire (par exemple, un numéro de page ou de tableau.

Chapitre 1. Initiation rapide

En combien de temps pouvez-vous faire fonctionner Network Dispatcher ?
Considérons l'exemple ci-après.

Supposons que vous soyez responsable du site Web de la société Intersplash. Vous gérez un site Web local avec deux serveurs HTTP. Vous avez utilisé la permutation circulaire pour gérer la charge de ces deux serveurs, mais l'activité de votre entreprise vient de s'accroître récemment et vous commencez à recevoir des plaintes de certains clients qui ne parviennent pas à accéder à votre site. Que faire ?

Accédez à <http://www.ibm.com/software/webservers/edgeserver> et téléchargez la dernière version de Network Dispatcher. Ce produit se compose de cinq composants : Dispatcher, Content Based Routing (CBR), Mailbox Locator, Site Selector et Consultant for Cisco CSS Switches (Cisco Consultant). Pour l'instant, nous nous contenterons d'aborder le composant **Dispatcher**.

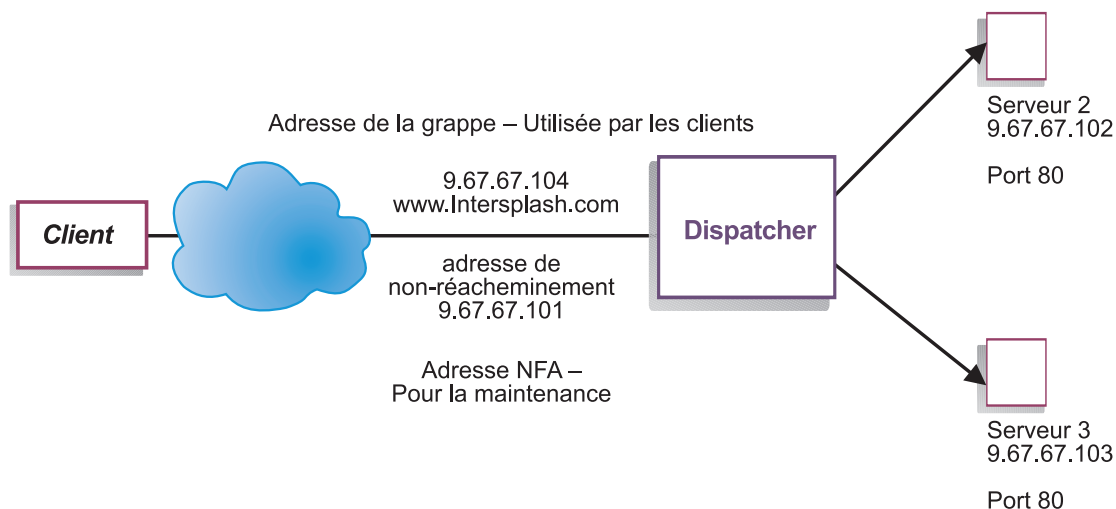


Figure 1. Configuration Dispatcher locale simple

Cet exemple de démarrage rapide indique comment configurer trois postes de travail connectés en local avec la méthode d'acheminement MAC de Dispatcher pour équilibrer la charge de trafic Web entre deux serveurs Web.

Cette configuration est également valable pour l'équilibrage de tout autre trafic d'applications TCP ou UDP sans état.

Remarque : Avec la version AIX, Linux, ou Solaris de Dispatcher, la configuration peut être effectuée avec seulement deux postes de travail, Dispatcher étant installé sur l'un des serveurs Web. Il s'agit d'une configuration co-implantée. Les procédures permettant de paramétrer des configurations plus complexes sont présentées à la section «Configuration de la machine Dispatcher» à la page 60.

Matériel requis

Pour l'exemple à démarrage rapide, vous devez disposer de trois postes de travail et de quatre adresses IP. L'un des postes de travail sera utilisé comme répartiteur (Dispatcher) et les deux autres comme serveurs Web. Chaque serveur Web requiert une adresse IP. Le poste Dispatcher requiert une adresse réelle et une adresse pour l'équilibrage de charge.

Préparation

1. Reportez-vous au «Chapitre 2. Installation de Network Dispatcher» à la page 11 pour vérifier que vous disposez bien des ressources requises.
2. Configurez les postes de travail de sorte qu'ils se trouvent sur le même segment de réseau local. Vérifiez que le trafic réseau entre les trois machines n'a pas à traverser de routeurs ou de ponts.
3. Configurez les cartes réseau de ces trois postes de travail. Dans cet exemple, nous supposons que vous disposez de la configuration réseau suivante :

Poste de travail	Nom	Adresse IP
1	server1.intersplash.com	9.67.67.101
2	server2.intersplash.com	9.67.67.102
3	server3.intersplash.com	9.67.67.103
Masque réseau = 255.255.255.0		

Chaque poste de travail ne contient qu'une carte d'interface réseau Ethernet standard.

4. Vérifiez que server1.intersplash.com peut contacter server2.intersplash.com et server3.intersplash.com (avec la commande ping).
5. Vérifiez que server2.intersplash.com et server3.intersplash.com peuvent contacter server1.intersplash.com (avec la commande ping).

6. Vérifiez que le contenu est identique sur les deux serveurs Web (Serveur 2 et Serveur 3). Pour cela, répliquez les données des deux postes de travail à l'aide d'un système de fichiers partagé tel que NFS, AFS ou DFS, ou à l'aide de tout autre moyen approprié pour votre site.
7. Vérifiez que les serveurs Web de `server2.intersplash.com` et `server3.intersplash.com` sont opérationnels. Utilisez un navigateur Web pour accéder directement aux pages à partir de **`http://server2.intersplash.com`** et **`http://server3.intersplash.com`** .
8. Cherchez une autre adresse IP valide pour ce segment de réseau local. Il s'agit de l'adresse que vous fournirez aux clients qui désirent accéder à votre site. Dans cet exemple, nous utiliserons :
Nom= `www.intersplash.com`
IP=`9.67.67.104`
9. Configurez les deux serveurs Web pour qu'ils acceptent le trafic de `www.intersplash.com`.
Ajoutez un alias pour `www.intersplash.com` à l'interface de **bouclage** de `server2.intersplash.com` et `server3.intersplash.com`.
 - Sous AIX :
`ifconfig lo0 alias www.intersplash.com netmask 255.255.255.0`
 - Sous Solaris 7 :
`ifconfig lo0:1 www.intersplash.com 127.0.0.1 up`
 - Pour les autres systèmes d'exploitation, reportez-vous au tableau 4 à la page 68 .
10. Supprimez toute autre route créée à la suite de l'attribution d'un alias à l'interface de bouclage. Reportez-vous à la section «Etape 2. Vérification de l'existence d'une route supplémentaire» à la page 70.
Vous venez de terminer les étapes de configuration requises pour les deux serveurs Web.

Configuration du composant Dispatcher

A l'aide de Dispatcher, vous pouvez créer une configuration à l'aide de la ligne de commande, de l'assistant de configuration ou de l'interface graphique.

Remarque : Les valeurs des paramètres doivent être saisies à l'aide de caractères anglais. Les seules exceptions sont les valeurs des paramètres des noms d'hôte et des noms de fichiers.

Configuration à partir de la ligne de commande

Si vous utilisez la ligne de commande, suivez la procédure ci-dessous.

1. Lancez ndserver sur Dispatcher :
 - Sous AIX, Linux ou Solaris, exécutez la commande suivante en tant qu'utilisateur root : **ndserver**
 - Sous Windows 2000, ndserver s'exécute en tant que service qui démarre automatiquement.
2. Lancez la fonction exécuteur (executor) de Dispatcher :
ndcontrol executor start
3. Ajoutez l'adresse de la grappe à la configuration de Dispatcher :
ndcontrol cluster add www.intersplash.com
4. Ajoutez le port du protocole http à la configuration de Dispatcher :
ndcontrol port add www.intersplash.com:80
5. Ajoutez chaque serveur Web à la configuration Dispatcher :
ndcontrol server add www.intersplash.com:80:server2.intersplash.com
ndcontrol server add www.intersplash.com:80:server3.intersplash.com
6. Configurez la machine pour accepter le trafic des autres adresses IP :
ndcontrol cluster configure www.intersplash.com
7. Lancez la fonction gestionnaire (manager) de Dispatcher :
ndcontrol manager start
Dispatcher procède maintenant à l'équilibrage de charge en fonction des performances des serveurs.
8. Démarrez la fonction conseiller (advisor) de Dispatcher :
ndcontrol advisor start http 80
Dispatcher vérifie désormais que les demandes des clients ne sont pas envoyées vers un serveur Web arrêté.

La configuration de base comportant des serveurs liés en local est maintenant terminée.

Configuration à l'aide de l'assistant de configuration

Si vous utilisez l'assistant de configuration, suivez la procédure ci-dessous.

1. Lancez ndserver sur Dispatcher :
 - Sous AIX, Linux ou Solaris, exécutez la commande suivante en tant qu'utilisateur root :
ndserver
 - Sous Windows 2000, ndserver s'exécute en tant que service qui démarre automatiquement.

2. Lancez la fonction Assistant de Dispatcher, **ndwizard**.

Cet assistant vous guide dans les étapes requises pour la création d'une configuration de base pour le composant Dispatcher. Vous devez répondre à quelques questions concernant votre réseau. Vous serez guidé dans la configuration d'une grappe pour permettre à Dispatcher d'équilibrer le trafic dans un groupe de serveurs.

Avec l'assistant de configuration, vous découvrirez les panneaux suivants :

- Présentation de l'assistant
- Qu'attendre de l'assistant
- Avant de commencer
- Choix de l'hôte à configurer (si nécessaire)
- Définition d'une grappe
- Ajout d'un port
- Ajout d'un serveur
- Lancement d'un conseiller
- Configuration de la machine serveur

Configuration à l'aide de l'interface graphique

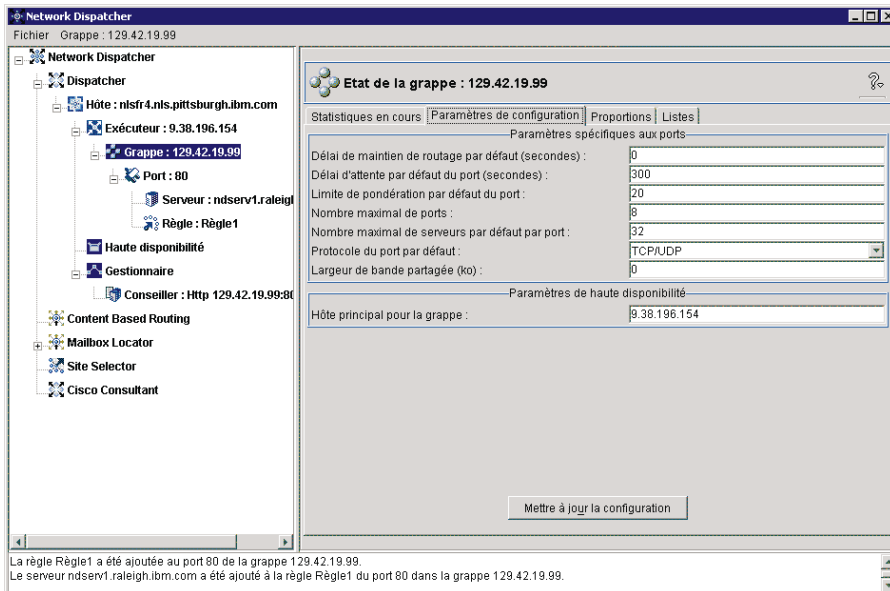


Figure 2. Interface graphique

Pour lancer l'interface graphique, procédez de la manière suivante :

1. Vérifiez que ndserver fonctionne :
 - Sous AIX, Linux ou Solaris, exécutez la commande suivante en tant que root :
ndserver
 - Sous Windows 2000, ndserver s'exécute en tant que service qui démarre automatiquement.
2. Ensuite, effectuez l'une des opérations suivantes :
 - Sous AIX, Linux ou Solaris, entrez **ndadmin**.
 - Sous Windows 2000, sélectionnez **Démarrer, Programmes, IBM WebSphere, Edge Server, IBM Network Dispatcher et Network Dispatcher**.

Instructions générales d'utilisation de l'interface graphique

La partie gauche du panneau affiche une arborescence comportant Network Dispatcher au niveau supérieur et Dispatcher, Content Based Routing, Mailbox Locator, Site Selector et Cisco Consultant en tant que composants. Reportez-vous à la figure 2 à la page 5.

Tous les composants peuvent être configurés à partir de l'interface graphique. Pour sélectionner des éléments dans l'arborescence, cliquez à l'aide du bouton un de la souris (normalement le bouton gauche) et pour afficher les menus en incrustation, cliquez à l'aide du bouton deux (normalement le bouton droit). Les menus en incrustation des éléments de l'arborescence sont également disponibles à partir de la barre de menus située dans la partie supérieure de la fenêtre.

Cliquez sur les signes plus ou moins pour développer ou réduire les éléments de l'arborescence.

La partie droite de la fenêtre contient deux listes d'indicateurs d'état relatifs à l'élément sélectionné.

- L'onglet **Statistiques actuelles** donne des informations statistiques sur l'élément.
- Le bouton **Régénération des statistiques** permet d'afficher les dernières données statistiques. Si aucun bouton Régénération des statistiques n'apparaît, les statistiques sont rafraîchies dynamiquement et sont toujours actuelles.
- L'onglet **Paramétrages configuration** présente les paramètres de configuration qui peuvent être définis en utilisant les procédures décrites dans les chapitres de configuration pour chacun des composants. Cet onglet n'apparaît pas pour tous les éléments de l'arborescence.

- Le bouton **MAJ configuration** applique les dernières modifications à la configuration en cours.
- L'onglet **Proportions** présente les paramètres de proportion (ou de pondération) pouvant être définis à l'aide des informations du «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137. Cet onglet n'apparaît pas pour tous les éléments de l'arborescence.
- L'onglet **Liste** présente des détails supplémentaires sur l'arborescence sélectionnée. Cet onglet n'apparaît pas pour tous les éléments de l'arborescence.
- Le bouton **Retrait** supprime les éléments mis en évidence.

Pour accéder à l'**aide**, cliquez sur le point d'interrogation dans le coin supérieur droit de la fenêtre Network Dispatcher.

- **Aide sur les zones** — décrit les valeurs par défaut de chaque zone.
- **Procédures** — affiche la liste des tâches pouvant être effectuées dans cet écran.
- **Table des matières** — contient toutes les informations d'aide.
- **Index** — est un index alphabétique des rubriques d'aide.

Test de vérification de la configuration

Vérifiez que la configuration fonctionne.

1. A l'aide d'un navigateur Web, accédez à **<http://www.intersplash.com>**. La configuration est correcte si une page apparaît.
2. Rechargez la page dans le navigateur Web.
3. Vérifiez les résultats de la commande suivante : **ndcontrol server report www.intersplash.com:80:**. La colonne du nombre total de connexions des deux serveurs doit contenir la valeur "2."

Types de configurations de grappe, de port et de serveur

Il y a plusieurs manières de configurer Network Dispatcher pour assurer le support de votre site. Si votre site ne comprend qu'un seul nom de système hôte auquel tous vos clients se connectent, vous pouvez ne définir qu'une seule grappe de serveurs. Pour chaque serveur, configurez un port par l'intermédiaire duquel Network Dispatcher communique. Reportez-vous à la figure 3.

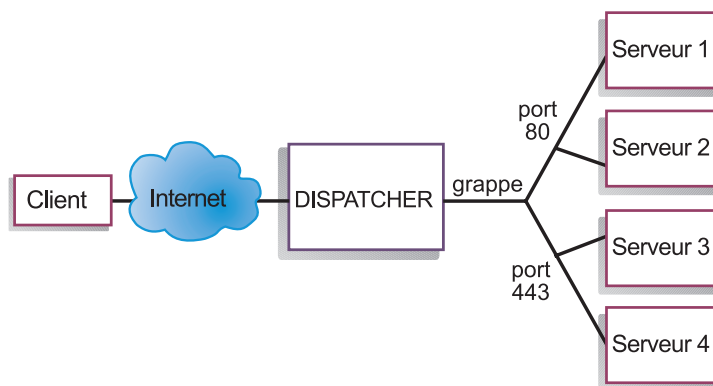


Figure 3. Exemple de composant Dispatcher configuré avec une grappe et 2 ports

Dans cet exemple de composant Dispatcher, une grappe est définie sur www.productworks.com. Elle dispose de deux ports : le port 80 pour HTTP et le port 443 pour SSL. Un client adressant une requête à l'adresse <http://www.productworks.com> (port 80) accédera à un autre serveur qu'un client s'adressant à <https://www.productworks.com> (port 443).

Si le site est très étendu et qu'il comporte un grand nombre de serveurs, chacun étant dédié à un protocole en particulier, Network Dispatcher doit être configuré selon une autre méthode. Dans ce dernier cas, il est souhaitable de définir une grappe pour chaque protocole, avec un seul port mais plusieurs serveurs, comme illustré à la figure 4 à la page 9.

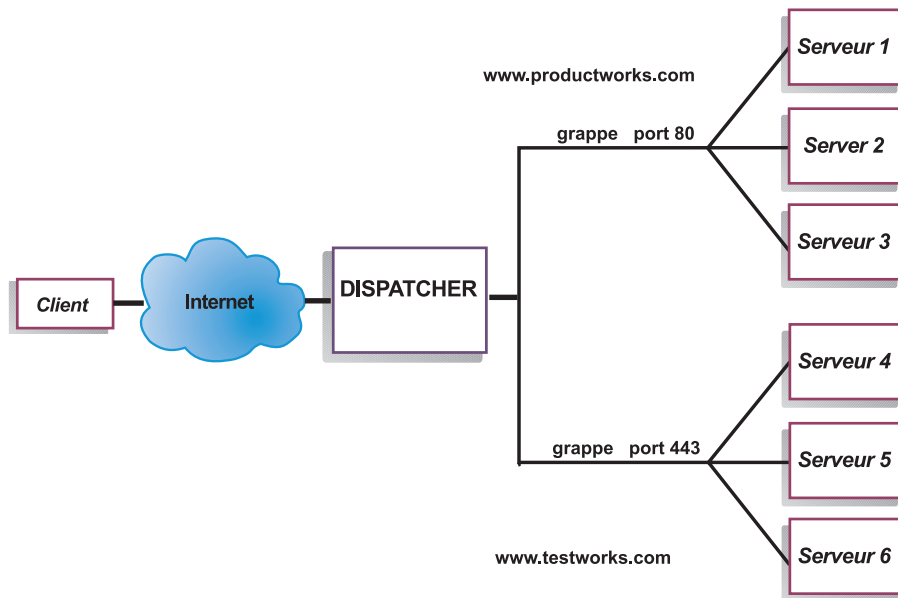


Figure 4. Exemple de composant Dispatcher configuré avec deux grappes, chacune associée à un port

Dans cet exemple de composant Dispatcher, deux grappes sont définies : `www.productworks.com` pour le port 80 (HTTP) et `www.testworks.com` pour le port 443 (SSL).

Une troisième configuration de Network Dispatcher est nécessaire si votre site abrite plusieurs sociétés ou services, chacun accédant à votre site par une adresse URL distincte. Dans ce cas, vous pouvez définir une grappe pour chaque société ou service ainsi qu'un nombre de ports variable pour réceptionner les connexions de cette URL, comme illustré par la figure 5 à la page 10.

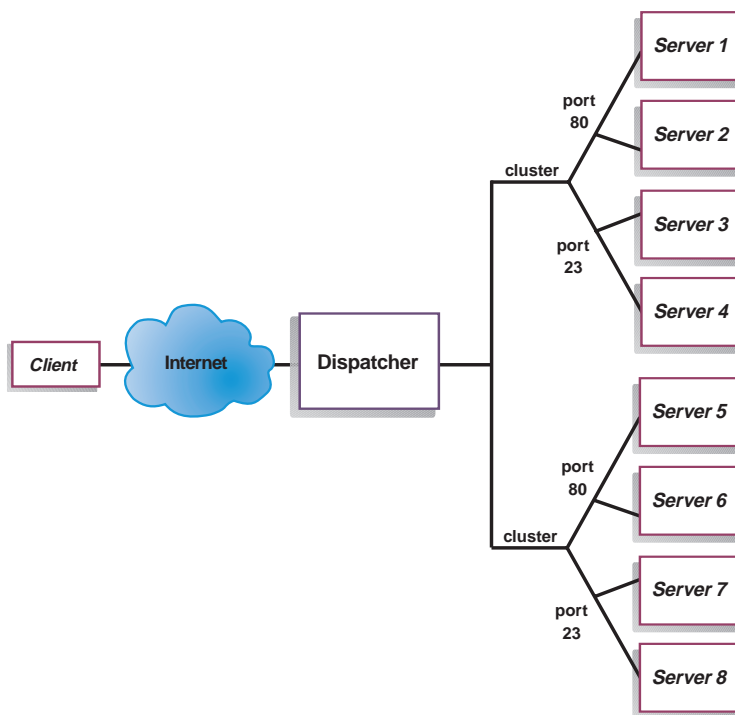


Figure 5. Exemple de composant Dispatcher configuré avec 2 grappes, chacune associée à 2 ports

Dans cet exemple de composant Dispatcher, deux grappes sont définies avec le port 80 pour HTTP et le port 23 pour Telnet pour chacun des sites www.productworks.com et www.testworks.com.

Chapitre 2. Installation de Network Dispatcher

Le présent chapitre décrit les conditions matérielles requises ainsi que la procédure d'installation de Network Dispatcher sous AIX, Linux, Solaris et Windows 2000. Suivez les instructions ci-dessous en vous reportant aux sections suivantes :

- «Configuration requise pour AIX» à la page 12
- «Configuration requise pour Red Hat Linux ou SuSE Linux» à la page 17
- «Configuration requise pour Solaris» à la page 20
- «Configuration requise pour Windows 2000» à la page 22

Remarques :

1. Si vous effectuez une migration à partir d'une version précédente, prenez en compte le fait que la structure du répertoire d'installation de Network Dispatcher a changé. Vous devez déplacer vos fichiers de configuration dans le répertoire `...nd/servers/configurations/composant` (où *composant* correspond à dispatcher, cbr, ml, ss ou lbc). Vous devez également déplacer vos scripts (tels que goldle et goStandby) dans le répertoire `...nd/servers/bin` afin de pouvoir les exécuter.
2. Si vous effectuez une déconnexion après l'installation de Network Dispatcher, vous devez relancer tous les services de Network Dispatcher lors de la reconnexion.
3. Network Dispatcher version 2.0 requiert le niveau Java 1.3.0 ou suivant. Certaines applications du dispositif Network Dispatcher pouvant requérir d'autres versions de Java, il est nécessaire de disposer des versions correctes de ce produit sur le dispositif Dispatcher lors des mises à jour. Pour vérifier que les composants Network Dispatcher utilisent la version correcte de Java lorsque plusieurs versions sont installées, procédez comme suit :
 - a. Installez la version Java 1.3 adaptée au système d'exploitation utilisé, conformément aux indications fournies dans les sections "Configuration requise" du présent chapitre.
 - b. Modifiez les fichiers script de Network Dispatcher pour l'utilisation de Java 1.3. Par défaut, les fichiers script se trouvent dans les répertoires suivants :

Unix `/usr/bin/<fichierscript>`

Windows

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

Modifiez les fichiers script pour chaque composant de Network Dispatcher à mettre à jour. Les fichiers script sont les suivants pour chaque composant :

Administration

ndadmin

Dispatcher

ndserver, ndcontrol, ndwizard, ndkeys

Content Based Routing (CBR)

cbrserver, cbrcontrol, cbrwizard, cbrkeys

Site Selector

ssserver, sscontrol

Cisco Consultant

lbserver, lbcontrol

Remarque : Par défaut, ces fichiers ne sont accessibles qu'en lecture.

Par conséquent, vous devez d'abord modifier les droits d'accès à ces fichiers pour sauvegarder vos modifications.

- c. Lorsqu'une commande java ou javaw se trouve dans les fichiers script, ajoutez son chemin d'accès sous la forme d'un préfixe désignant l'emplacement de cette commande dans le répertoire d'installation de Java 1.3.

Par exemple, sous Windows 2000, si Java 1.3 est installé dans C:\Program Files\IBM\Java13\jre\bin, remplacez la ligne correspondante comme suit dans ndserver.cmd :

Ancienne ligne :

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

Nouvelle ligne :

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

Configuration requise pour AIX

- Toute machine de type IBM RS/6000
- IBM AIX 5.1 avec APAR IY19177. La prise en charge concerne Power PC 32-bit (*non* le noyau 64-bit).

IBM AIX 4.3.3.10 plus les correctifs apar (afin de prendre en charge Java 1.3). Pour obtenir une liste des correctifs apar AIX requis, reportez-vous au fichier README.

- 50 Mo d'espace disque disponible pour l'installation

Remarque : Un espace disque supplémentaire sera nécessaire pour les fichiers journaux.

- Les cartes d'interface réseau (NIC) sont prises en charge :
 - Token ring 16 Mo
 - Ethernet 10 Mo
 - Ethernet 100 Mo
 - Ethernet 1 Go
 - Interface optique FDDI
 - Cartes d'interface réseau Ethernet multi-port

Remarque : L'implémentation des cartes NIC multi-port varient d'un fournisseur à l'autre. La prise en charge de certaines cartes NIC multi-port peut donc être limitée.

- IBM AIX Developer Kit, Java 2 Technology Edition, version 1.3.0 pour l'environnement JRE (Java Runtime Environment). (Pour consulter les informations relatives à l'exécution de plusieurs versions Java, reportez-vous à la remarque 3 à la page 11.)
- Edge Server Caching Proxy V2.0, si vous utilisez le composant CBR pour l'équilibrage de charge de HTTP ou du trafic SSL.
- Netscape Navigator 4.07 (ou supérieur) ou Netscape Communicator 4.61 (ou supérieur) pour afficher l'aide en ligne.
- Pour Consultant for Cisco CSS Switches, le relais Cisco CSS 11000 Series doit être installé et configuré.

Installation pour AIX

Le tableau 1 répertorie les images installp de Network Dispatcher pour AIX.

Tableau 1. Images installp AIX

Dispatcher (composant, administration, licence et messages)	intnd.nd.driver intnd.nd.rte intnd.msg.nd.<langue>.nd intnd.admin.rte intnd.msg.<langue>.admin
Administration (uniquement)	intnd.admin.rte intnd.msg.<langue>.admin
Documentation	intnd.doc.rte
Licence	intnd.nd.license
Système Metric Server	intnd.ms.rte

où <langue> est l'une des suivantes :

- en_US
- de
- es_ES

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

Si vous téléchargez une copie d'évaluation du produit à partir du site Web, suivez les instructions d'installation sur le site (<http://www.ibm.com/software/webserver/edgeserver/download.html>).

Avant de commencer l'installation

Lorsque vous installez le produit, le choix vous est offert d'installer tout ou partie des composants suivants :

- Administration Network Dispatcher
- Pilote du périphérique Network Dispatcher (requis par le composant Dispatcher de Network Dispatcher)
- Licence Network Dispatcher (requis par le composant Dispatcher de Network Dispatcher)
- Documentation Network Dispatcher
- Metric Server Network Dispatcher
- Licence

Etapes de la procédure d'installation

Remarque : Si une version antérieure est déjà installée sur votre système, supprimez-la avant d'installer la version actuelle. Assurez-vous, tout d'abord, que tous les exécuteurs et serveurs sont arrêtés. Puis, pour désinstaller l'intégralité du produit, entrez **installp -u intnd**. Pour désinstaller certains jeux de fichiers, spécifiez-les au lieu d'entrer le nom du package.

Effectuez les opérations ci-dessous pour installer Network Dispatcher pour AIX.

1. Connectez-vous sous l'ID racine (root).
2. Insérez le support fourni dans son lecteur ou, si vous l'installez à partir du Web, copiez les images des disquettes d'installation dans un répertoire.

3. Installez l'image d'installation. Il est conseillé d'utiliser SMIT pour installer Network Dispatcher pour AIX. Ainsi, tous les messages seront installés automatiquement.

A l'aide de **SMIT** :

Sélectionnez

Installation et maintenance de logiciels

Sélectionnez

Installation et mise à jour de logiciels

Sélectionnez

Installation et mise à jour de tous les logiciels disponibles

Entrez l'unité ou le répertoire contenant les images installp

Entrez sur la ligne *PROGICIEL à installer, les données correspondant aux options choisies (ou sélectionnez Liste)

Cliquez sur

OK

Après l'exécution de la commande, appuyez sur **Fin**, puis sélectionnez l'option permettant de **quitter Smit** à partir du menu de sortie ou appuyez sur **F12**. Si vous utilisez SMITTY, appuyez sur **F10** pour quitter le programme.

A partir de la ligne de commande :

Si vous effectuez l'installation à partir d'un CD-ROM, entrez les commandes suivantes pour le monter :

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

Reportez-vous au tableau suivant pour déterminer la ou les commandes à entrer pour installer les composants Network Dispatcher pour AIX :

Tableau 2. Commande AIX relatives à l'installation

Network Dispatcher (avec messages). Inclut : Dispatcher, CBR, Mailbox Locator, Site Selector et Cisco Consultant	installp -acXgd <i>unité</i> intnd.nd.rte intnd.admin.rte intnd.nd.driver intnd.msg.<langue>.nd intnd.msg.<langue>.admin
Documents	installp -acXgd <i>unité</i> intnd.doc.rte intnd.msg.<langue>.doc
Administration (uniquement)	installp -acXgd <i>unité</i> intnd.admin.rte intnd.msg.<langue>.admin
Licence	installp -acXgd <i>unité</i> intnd.nd.license
Système Metric Server	installp -acXgd <i>unité</i> intnd.ms.rte intnd.msg.<langue>.admin

La variable *unité* prend les valeurs suivantes :

- *"/cdrom"* si l'on installe à partir d'un lecteur de CD-ROM.
- *"/dir"* (le répertoire contenant les images d'installation) si l'on installe à partir d'un système de fichiers.

Assurez-vous que la colonne de résultat du résumé d'opération contient la mention "SUCCESS" (réussite) pour chaque composant de Network Dispatcher installé (état APPLY). Ne poursuivez pas avant d'avoir réussi à installer tous les composants choisis.

Remarque : Pour générer la liste des jeux de fichiers d'une image installp avec l'ensemble des catalogues de messages disponibles, entrez

```
installp -ld unité
```

La variable *unité* prend les valeurs suivantes :

- *"/cdrom"* si l'on installe à partir d'un lecteur de CD-ROM.
- *"/dir"* (le répertoire contenant les images d'installation) si l'on installe à partir d'un système de fichiers.

Pour démonter le CD-ROM, tapez la commande suivante :

```
umount /cdrom
```

4. Vérifiez que le produit est installé correctement. Entrez la commande suivante :

```
ls1pp -h | grep intnd
```

Si vous avez installé l'intégralité du produit, cette commande génère le résultat suivant :

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

Les chemins d'installation de Network Dispatcher incluent les éléments suivants :

- Administration - **/usr/lpp/nd/admin**
- Composants Network Dispatcher- **/usr/lpp/nd/servers**
- Système Metric Server - **/usr/lpp/nd/ms**
- Documentation (*Guide d'administration*) - **/usr/lpp/nd/documentation**

Configuration requise pour Red Hat Linux ou SuSE Linux

- Red Hat Linux version 7.1 (noyau Linux version 2.4.2-2) ou SuSE Linux version 7.1 (noyau Linux version 2.4.0-4Go). Les deux types de noyau, monoprocesseur et multiprocesseur, sont pris en charge.

Remarque : Si vous utilisez la méthode d'acheminement MAC de Dispatcher avec un haut niveau de disponibilité et une co-implantation, vous devez installer un correctif de noyau Linux. Pour obtenir plus d'informations sur le mode de téléchargement et d'installation du correctif, reportez-vous à la section «Installation du correctif du noyau Linux (pour supprimer les réponses ARP sur l'interface de bouclage)» à la page 72.

- 50 Mo d'espace disque disponible pour l'installation

Remarque : Un espace disque supplémentaire sera nécessaire pour les fichiers journaux.

- Les cartes d'interface réseau (NIC) sont prises en charge :
 - Ethernet 10 Mo
 - Ethernet 100 Mo
 - Ethernet 1 Go
 - Prise en charge des cartes NIC Ethernet multi-port (mode 1 uniquement). La tolérance des pannes (mode 2) et le regroupement des ports (mode 3) ne sont pas pris en charge.

Remarque : L'implémentation des cartes NIC multi-port varie d'un fournisseur à l'autre. La prise en charge de certaines cartes NIC multi-port peut donc être limitée.

- Une version de Korn Shell (ksh) doit être installée
- IBM Runtime Environment for Linux, Java 2 Technology Edition, version 1.3.0. (Pour consulter les informations relatives à l'exécution de plusieurs versions Java, reportez-vous à la remarque 3 à la page 11.)
- Les variables d'environnement JAVA_HOME et PATH doivent être définies à l'aide de la commande **export**. Le contenu de la variable JAVA_HOME dépend de l'emplacement d'installation de Java. Voici un exemple :
 - JAVA_HOME=/opt/IBMJava2-13/jre
 - PATH=\$JAVA_HOME/bin:\$PATH
- Edge Server Caching Proxy V2.0, si vous utilisez le composant CBR pour l'équilibrage de charge de HTTP ou du trafic SSL
- Netscape Navigator 4.07 (ou supérieur) ou Netscape Communicator 4.61 (ou supérieur) pour afficher l'aide en ligne.
- Pour Consultant for Cisco CSS Switches, le relais Cisco CSS 11000 Series doit être installé et configuré.

Installation sous Linux

La présente section explique comment installer Network Dispatcher sous Red Hat Linux ou SuSE Linux à l'aide du CD du produit ou de sa version d'évaluation téléchargée à partir du site Web. Les instructions d'installation sont disponibles sur le site Web (<http://www.ibm.com/software/webserver/edgeserver/download.html>).

Avant de commencer l'installation

Avant de commencer la procédure d'installation, soyez certain de disposer de droits d'accès root pour installer le logiciel.

Etapes de la procédure d'installation

Remarque : Si une version antérieure est déjà installée sur votre système, supprimez-la avant d'installer la version actuelle. Assurez-vous, tout d'abord, que tous les exécuteurs et serveurs sont arrêtés. Puis, pour procéder à la désinstallation de l'ensemble du produit, entrez **rpm -e pkgname**. Procédez à la désinstallation dans l'ordre inverse des procédures du module d'installation, en vous assurant que les modules d'administration sont les derniers à être désinstallés.

Pour installer Network Dispatcher :

1. Préparez l'installation.
 - Connectez-vous sous l'ID racine (root).

- Insérez le support du produit, ou téléchargez-le à partir de notre site Web, et installez l'image d'installation à l'aide de RPM (Gestionnaire de paquets Red Hat).

Remarque : Le module installable de Red Hat Linux et celui de SuSE Linux ne peuvent pas être exécutés sous une autre version de Linux.

L'image d'installation est un fichier de format **ndlinux-version.tar**.

- Décompactez le fichier compacté dans un répertoire temporaire en entrant la commande suivante : **tar -xf ndlinux-version.tar**. Vous obtiendrez comme résultat un ensemble de fichiers dont l'extension est **.rpm**.

Voici la liste des modules RPM qui peuvent être installés.

- **ibmnd-adm-édition-version.i386.rpm** (Administration ND)
- **ibmnd-doc-édition-version.i386.rpm** (Documentation)
- **ibmnd-ms-édition-version.i386.rpm** (Metric Server)
- **ibmnd-srv-édition-version.i386.rpm** (Network Dispatcher Runtime)
- **ibmnd-lic-édition-version.i386.rpm** (Licence)
- L'ordre d'installation des modules est important. Voici la liste des modules nécessaires à chaque composant et leur ordre d'installation :
 - Administration (adm)
 - Licence (lic)
 - Composants Network Dispatcher (srv)
 - Metric Server (ms)
 - Documentation (doc)

La commande d'installation des modules doit être émise à partir du répertoire où sont situés les fichiers RPM. Tapez la commande suivante pour installer tous les modules : **rpm -i package.rpm**.

Remarque : Il est nécessaire, pour au moins l'un des fichiers RPM, que Java soit installé et enregistré dans la base de données RPM. Si Java est installé mais non enregistré dans la base de données, utilisez la commande d'installation suivante, avec l'option 'no dependencies' :

rpm -i --nodeps package.rpm

- Les chemins d'installation de Network Dispatcher incluent les éléments suivants :
 - Administration - **/opt/nd/admin**
 - Composants Network Dispatcher - **/opt/nd/servers**

- Metric Server - **/opt/nd/ms**
 - Documentation (*Guide d'administration*) - **/opt/nd/documentation**
 - Procédez à la désinstallation des modules dans l'ordre inverse de l'installation, en vous assurant que les modules d'administration sont les derniers à être désinstallés.
2. Vérifiez que le produit est installé correctement. Entrez la commande suivante :
- rpm -qa | grep ibmnd**
- L'installation du produit complet génère une liste comme celle-ci :
- *ibmnd-adm-release-version*
 - *ibmnd-doc-release-version*
 - *ibmnd-ms-release-version*
 - *ibmnd-srv-release-version*
 - *ibmnd-lic-release-version*

Configuration requise pour Solaris

- Tout poste de travail SPARC ou serveur Ultra 60 pris en charge par Solaris Version 7 ou Solaris Version 8. Network Dispatcher prend en charge uniquement le mode 32-bit pour les plate-formes Solaris.
- 50 Mo d'espace disque disponible pour l'installation

Remarque : Un espace disque supplémentaire sera nécessaire pour les fichiers journaux.

- Les cartes d'interface réseau (NIC) sont prises en charge :
 - Ethernet 10 Mo
 - Ethernet 100 Mo
 - Ethernet 1 Go (pris en charge uniquement sur le serveur Ultra 60)
 - Prise en charge des cartes NIC Ethernet multi-port (mode 1 uniquement). La tolérance des pannes (mode 2) et le regroupement des ports (mode 3) ne sont pas pris en charge.

Remarque : L'implémentation des cartes NIC multi-port varie d'un fournisseur à l'autre. La prise en charge de certaines cartes NIC multi-port peut donc être limitée.

- Java 2 JRE, Standard Edition, version 1.3.0. (Pour consulter les informations relatives à l'exécution de plusieurs versions Java, reportez-vous à la remarque 3 à la page 11.)
- Edge Server Caching Proxy V2.0, si vous utilisez le composant CBR pour l'équilibrage de charge de HTTP ou du trafic SSL

- For Solaris 7, Sun Microsystems HotJava Browser 1.0.1 (ou version ultérieure) pour l'affichage de l'aide en ligne
For Solaris 8, Netscape Navigator 4.07 (ou version ultérieure) ou Netscape Communicator 4.61 (ou version ultérieure) pour l'affichage de l'aide en ligne
- Pour Consultant for Cisco CSS Switches, le relais Cisco CSS 11000 Series doit être installé et configuré.

Installation pour Solaris

La présente section explique comment installer Network Dispatcher sur Solaris à partir du CD-ROM du produit. Si vous téléchargez une copie d'évaluation du produit à partir d'Internet, suivez les instructions d'installation sur le site Web (<http://www.ibm.com/software/webserver/edgeserver/download.html>).

Avant de commencer l'installation

Avant de commencer la procédure d'installation, soyez certain de disposer de droits d'accès root pour installer le logiciel.

Etapes de la procédure d'installation

Remarque : Si une version antérieure est déjà installée sur votre système, supprimez-la avant d'installer la nouvelle. Vérifiez d'abord que l'exécuteur et le serveur sont arrêtés. Puis, pour désinstaller Network Dispatcher, entrez **pkgrm pkgname**.

Pour installer Network Dispatcher :

1. Préparez l'installation.

- Connectez-vous en tant que root.
- Insérez le CD-ROM contenant le logiciel Network Dispatcher dans le lecteur approprié.

A l'invite, entrez **pkgadd -d chemin d'accès** où **-d chemin d'accès** est le nom d'unité du lecteur de CD-ROM ou le répertoire du disque dur contenant le module ; par exemple, **pkgadd -d /cdrom/cdrom0/**.

Vous obtenez une liste de modules à installer.

- **ibmdsp** IBM ND pour Solaris (composants Network Dispatcher)
- **ibmndadm** Administration de base IBM ND pour Solaris
- **ibmnddoc** Documentation d'IBM ND pour Solaris
- **ibmndms** IBM ND Metric Server pour Solaris
- **ibmdsplic** Licence pour Solaris

Pour installer tous les modules, entrez "all" et appuyez sur la touche Entrée. Pour installer uniquement certains composants, entrez le ou les noms correspondants aux modules à installer séparés par un espace ou par une virgule et appuyez sur la touche Entrée. Vous serez peut-être invité à changer vos droits d'accès à certains répertoires ou fichiers. Il suffit d'appuyer sur le bouton Entrée ou de répondre "yes". Vous devez installer les modules prérequis (car l'installation s'effectue suivant l'ordre alphabétique et non en fonction des éléments prérequis). Si vous indiquez "all" et que vous répondez "yes" à toutes les questions, l'installation se déroule sans incident.

Tous les modules dépendent du module commun, ibmndadm. Ce module commun doit être installé avec chacun des autres modules.

Si vous voulez installer le produit Network Dispatcher dans son intégralité, vous devez installer cinq éléments : ibmdsp, ibmdsplic, ibmndadm, ibmnddoc et ibmndms. Si vous souhaitez installer l'administration à distance, seule l'installation d'ibmndadm est nécessaire.

Les composants Network Dispatcher se trouvent dans le répertoire d'installation **/opt/nd/servers**.

2. Le composant d'administration se trouve dans le répertoire **/opt/nd/admin**
3. Metric Server se trouve dans le répertoire **/opt/nd/ms**
4. La documentation (*Guide d'administration*) se trouve dans le répertoire **/opt/nd/documentation**
5. Vérifiez que le produit est installé correctement. Entrez la commande suivante : **pkginfo | grep ibm**.

L'installation du produit complet génère une liste comme celle-ci :

- ibmdsp
- ibmndadm
- ibmnddoc
- ibmndms
- ibmdsplic

Configuration requise pour Windows 2000

- Tout PC équipé d'un processeur Intel x86 pris en charge par Microsoft Windows 2000
- Windows 2000 Professional, Server ou Advanced Server
- 50 Mo d'espace disque disponible pour l'installation

Remarque : Un espace disque supplémentaire sera nécessaire pour les fichiers journaux.

- Les cartes d'interface réseau (NIC) sont prises en charge :
 - Token ring 16 Mo
 - Ethernet 10 Mo
 - Ethernet 100 Mo
 - Ethernet 1 Go
 - Cartes d'interface réseau Ethernet multi-port

Remarque : L'implémentation des cartes NIC multi-port varient d'un fournisseur à l'autre. La prise en charge de certaines cartes NIC multi-port peut donc être limitée.

- IBM Cross Platform Technologies pour Windows v2.0 (SDK 1.3.0)
Vous devez télécharger à la fois le module installable Developer Kit et le module installable Runtime Environment avant d'exécuter le programme InstallShield. (Pour consulter les informations relatives à l'exécution de plusieurs versions Java, reportez-vous à la remarque 3 à la page 11.)
- Edge Server Caching Proxy V2.0, si vous utilisez le composant CBR pour l'équilibrage de charge de HTTP ou du trafic SSL
- Vérifiez que le navigateur par défaut est Netscape Navigator 4.07 (ou supérieur), Netscape Communicator 4.61 (ou supérieur) ou Internet Explorer 4.0 (ou supérieur). Le navigateur par défaut est utilisé pour consulter l'aide en ligne.
- Pour Consultant for Cisco CSS Switches, le relais Cisco CSS 11000 Series doit être installé et configuré.

Installation pour Windows 2000

La présente section explique comment installer Network Dispatcher sous Windows 2000 à partir du CD-ROM du produit. Si vous téléchargez une copie d'évaluation du produit à partir du site Web, suivez les instructions d'installation sur le site Web

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

Modules d'installation

Une liste de modules à installer vous est proposée :

- Runtime
- Administration
- Licence
- Documentation
- Système Metric Server

Avant de commencer l'installation

La version Windows 2000 de Network Dispatcher est prise en charge par les produits suivants :

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

Remarque : La version Windows 2000 de Network Dispatcher ne s'exécute *pas* sous d'autres versions de Windows.

Restrictions : La version Windows 2000 de Network Dispatcher ne peut pas être installée sur la même machine qu'IBM Firewall.

Avant de commencer la procédure d'installation, assurez-vous que vous vous êtes connectés en qualité d'administrateur ou d'utilisateur doté de privilèges administratifs.

Etapes de la procédure d'installation

Si une version antérieure est déjà installée sur votre système, supprimez-la avant d'installer la version actuelle. Pour procéder à la désinstallation en utilisant la fonction **Ajouter/Supprimer un programme**, suivez la procédure suivante :

1. Cliquez sur **Démarrer**→**Paramètres**→**Panneau de configuration**
2. Cliquez deux fois sur **Ajout/Suppression de programmes**
3. Sélectionnez *Network Dispatcher*
4. Cliquez sur le bouton **Modifier/Supprimer**

Pour installer Network Dispatcher :

1. Insérez le CD-ROM de Network Dispatcher dans le lecteur de CD-ROM. La fenêtre d'installation doit s'afficher automatiquement.
2. Effectuez l'opération qui suit uniquement si le CD n'est pas lancé automatiquement sur votre machine. Cliquez avec le bouton gauche de la souris pour exécuter les tâches suivantes :
 - Cliquez sur **Démarrer**.
 - Sélectionnez **Exécuter**.
 - Indiquez l'unité de CD-ROM, suivie de "setup.exe". Par exemple :
E:\setup
3. Sélectionnez la **langue** à utiliser pour l'installation.
4. Cliquez sur **OK**.
5. Suivez les instructions du programme d'installation.
6. Si vous désirez changer d'unité ou de répertoire de destination, cliquez sur **Parcourir**.

7. Vous pouvez choisir entre “Produit ND complet” ou “Les composants de votre choix.”
8. Une fois l’installation terminée, un message vous demande de réamorcer le système avant d’utiliser Network Dispatcher. Cette opération est nécessaire pour vous assurer que tous les fichiers sont installés et que la variable d’environnement IBMNDPATH a bien été ajoutée au registre.

Les chemins d’installation de Network Dispatcher incluent les éléments suivants :

- Administration – **c:\Program~1\IBM\edge\nd\admin**
- Composants Network Dispatcher – **c:\Program~1\IBM\edge\nd\servers**
- Système Metric Server –**c:\Program~1\IBM\edge\nd\ms**
- Documentation (Guide d’administration)
–**c:\Program~1\IBM\edge\nd\documentation**

Chapitre 3. Présentation de Network Dispatcher

Ce chapitre contient une présentation générale de Network Dispatcher et comporte les sections suivantes :

- «Principe de Network Dispatcher»
- «Intérêt et avantages de Network Dispatcher» à la page 28
- «Nouveautés» à la page 30
- «Composants de Network Dispatcher» à la page 35
- «Haute disponibilité» à la page 46

Principe de Network Dispatcher

Network Dispatcher constitue une solution logicielle permettant l'équilibrage de charge des serveurs. Il permet d'optimiser les performances en orientant les demandes de session TCP/IP vers différents serveurs au sein d'un groupe, assurant ainsi une répartition équilibrée des demandes entre tous les serveurs. Cette procédure d'équilibrage de charge est parfaitement transparente, tant pour l'utilisateur que pour les applications. Network Dispatcher s'avère particulièrement utile pour les applications telles que les serveurs de messagerie électronique, les serveurs Internet (WWW), les demandes de bases de données parallèles distribuées et autres applications TCP/IP.

Appliqué à des serveurs Web, Network Dispatcher peut contribuer à accroître les capacités d'un site en apportant une solution puissante, souple et modulable aux incidents liés à la surcharge des réseaux. Si les visiteurs ne peuvent pas accéder à votre site pendant les périodes d'affluence, Network Dispatcher peut déterminer automatiquement le serveur le mieux placé pour traiter les demandes en instance. De cette manière, la rentabilité de votre site augmente en même temps que la satisfaction de vos clients.

Network Dispatcher comprend cinq composants pouvant être employés conjointement ou séparément pour vous permettre d'obtenir les meilleurs résultats en matière d'équilibrage de charge :

- Le composant **Dispatcher** peut être utilisé seul pour équilibrer la charge des serveurs, dans le cadre d'un réseau local ou étendu, sur la base de mesures et d'évaluations définies de façon dynamique par Dispatcher. Ce composant assure l'équilibre des charges au niveau des services spécifiques tels que HTTP, FTP, SSL, NNTP, IMAP, POP3, SMTP et Telnet. Il n'utilise pas de serveur de noms de domaine pour associer noms de domaine et adresses IP.

En ce qui concerne le protocole HTTP, le composant fonction CBR de Dispatcher peut être utilisé pour équilibrer la charge à partir du contenu de la demande du client. Le choix du serveur est fonction du résultat de la comparaison de l'URL à une règle donnée.

- En ce qui concerne les protocoles HTTP et HTTPS (SSL), le composant **Content Based Routing (CBR)** peut être utilisé pour équilibrer la charge à partir du contenu de la demande du client. Un client envoie une demande à Caching Proxy, qui la transmet au serveur approprié. Le choix du serveur est fonction du résultat de la comparaison de l'URL à une règle donnée.
- Dans le cas des protocoles IMAP ou POP3, vous pouvez utiliser le composant **Mailbox Locator** qui fonctionne comme proxy et choisit un serveur approprié sur la base de l'ID utilisateur et du mot de passe fournis par le client.
- Le composant **Site Selector** peut être utilisé pour équilibrer la charge des serveurs, dans le cadre d'un réseau local ou étendu, par permutation circulaire des serveurs de noms de domaines ou par une méthode plus évoluée définie par l'utilisateur. Un serveur de noms de domaine est associé à Site Selector. Il met les noms DNS en correspondance avec les adresses IP.
- Le composant **Consultant for Cisco CSS Switches** permet de générer des mesures de pondération de serveur, qui sont envoyées au composant Cisco CSS Switch pour une sélection optimale des serveurs, l'optimisation des charges et la tolérance aux pannes.

Pour plus d'informations sur les composants Dispatcher, CBR, Mailbox Locator, Site Selector et Consultant for Cisco CSS Switches, reportez-vous à la section «Composants de Network Dispatcher» à la page 35.

Intérêt et avantages de Network Dispatcher

Le nombre d'utilisateurs et de réseaux qui se connectent au réseau mondial Internet connaît une croissance exponentielle. Cette croissance entraîne des problèmes d'échelle pouvant limiter l'accès des utilisateurs aux sites les plus fréquentés.

Actuellement, les administrateurs de réseau utilisent diverses méthodes pour optimiser l'accessibilité. Certaines de ces méthodes permettent, par exemple, de sélectionner un autre serveur de manière aléatoire lorsque le premier choisi répond trop lentement ou ne répond pas. Cette approche est peu pratique, peu conviviale et inefficace. Autre méthode utilisée, l'approche circulaire standard, dans laquelle le serveur de noms de domaine sélectionne tour à tour des serveurs pour traiter les demandes. Cette approche est sans doute meilleure que la première, mais reste inefficace dans la mesure où l'acheminement des demandes s'effectue à l'aveuglette, sans tenir compte de la charge des serveurs. En outre, même si un serveur est défaillant, les demandes continuent de lui être adressées.

Né de ce besoin d'une solution plus puissante, Network Dispatcher apporte nombre d'améliorations par rapport aux solutions antérieures comparables :

Modularité

Pour répondre à l'augmentation du nombre de demandes client, IND permet d'ajouter des serveurs de manière dynamique, ouvrant ainsi l'accès à des dizaines de millions de demandes chaque jour sur des dizaines, voire des centaines, de serveurs.

Utilisation optimale des équipements

L'équilibrage de charge permet à chaque groupe de serveurs d'utiliser ses ressources matérielles de manière optimale en réduisant les surcharges qui se produisent fréquemment avec une méthode de permutation de serveurs circulaire classique.

Facilité d'intégration

Network Dispatcher utilise les protocoles TCP/IP standard. Il peut être ajouté à n'importe quel réseau sans qu'aucune modification matérielle soit nécessaire. C'est un produit simple à installer et à configurer.

Faible charge induite

Avec la méthode d'acheminement de niveau MAC simple qu'il utilise, Dispatcher se contente de surveiller les transmissions entrantes du client vers le serveur. Il n'effectue aucun contrôle des transmissions en sortie, du serveur vers le client. Si l'on compare à d'autres méthodes, cet aspect réduit sensiblement son impact sur les performances des applications et permet même d'accroître celles du réseau.

Haute disponibilité

Dispatcher dispose d'une fonction intégrée assurant une haute disponibilité ; à tout moment, une machine de secours peut assurer l'équilibrage de charge si la machine Dispatcher principale vient à défaillir. Dispatcher offre également la fonction de haute disponibilité réciproque qui permet à deux machines d'être simultanément en mode actif et attende l'une pour l'autre. Pour plus de détails, reportez-vous à la section «Haute disponibilité» à la page 46.

Acheminement sur la base du contenu (avec le composant CBR ou Dispatcher)

Associé à Caching Proxy, le composant CBR peut relayer les demandes HTTP et HTTPS (SSL) vers des serveurs spécifiques en fonction du contenu demandé. Par exemple, si une demande contient la chaîne `"/cgi-bin/"` dans la partie répertoire de l'URL et que le

serveur est un serveur local, CBR peut acheminer la demande vers un ensemble de serveurs spécialisés dans les demandes cgi et choisir parmi ceux-ci le serveur optimal.

Le composant Dispatcher assure aussi l'acheminement sur la base du contenu, mais ne nécessite pas que Caching Proxy soit installé. Etant donné que la fonction CBR du composant Dispatcher est exécutée dans le noyau à la réception des paquets, l'acheminement est plus rapide que celui réalisé par le composant CBR. Le composant Dispatcher exécute la fonction fonction CBR (content-based routing) pour HTTP (avec la règle de type de contenu) et HTTPS (avec l'affinité des ID de session).

Remarque : Seul le composant CBR peut utiliser la règle de contenu pour HTTPS (SSL) pour un équilibrage de charge effectué sur la base du contenu de la demande HTTP, ce qui nécessite un déchiffrement et nouveau chiffrement des messages.

Nouveautés

Network Dispatcher pour IBM WebSphere Edge Server Version 2.0 contient un certain nombre de fonctions nouvelles. Les plus importantes sont présentées ci-après.

- **Prise en charge de AIX version 5.1**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Network Dispatcher prend désormais en charge une nouvelle version de AIX : AIX Version 5.1. Pour plus d'informations, reportez-vous à la section «Configuration requise pour AIX» à la page 12.

- **Prise en charge de SuSE Linux Version 7.1**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Network Dispatcher prend désormais en charge SuSE Linux Version 7.1 (version de noyau 2.4.0-4 Go). Auparavant, Network Dispatcher ne prenait en charge que Red Hat Linux. Pour plus d'informations, reportez-vous à la section «Configuration requise pour Red Hat Linux ou SuSE Linux» à la page 17.

- **Prise en charge de Red Hat Linux Version 7.1**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Network Dispatcher prend désormais en charge une nouvelle version de Red Hat Linux : Red Hat Linux Version 7.1 (version de noyau 2.4.2-2).

Pour plus d'informations, reportez-vous à la section «Configuration requise pour Red Hat Linux ou SuSE Linux» à la page 17.

- **Support multilingue sous Linux et Solaris**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Sous les systèmes d'exploitation Linux et Solaris, Network Dispatcher comporte un support multilingue pour les pays du groupe 1.

- **Prise en charge de la nouvelle norme NLS chinoise**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Network Dispatcher comporte un support multilingue conforme à la nouvelle norme NLS chinoise GB 18030.

- **Composant Consultant for Cisco CSS Switches (Cisco Consultant)**

Cette fonction est un nouveau composant de Network Dispatcher.

La collaboration avec Cisco et son CDN (Content Distribution Network (CDN) a conduit au développement d'un nouveau composant de Network Dispatcher : Cisco Consultant. Ce composant (qui a d'abord été proposé en version autonome) permet à Network Dispatcher de générer des pondérations et de prendre des décisions en matière d'équilibrage de charge pour le composant CSS de Cisco.

Pour plus d'informations, reportez-vous aux sections «Chapitre 12.

Planification du composant Consultant for Cisco CSS Switches» à la

page 123 et «Chapitre 13. Configuration du composant Consultant for Cisco CSS Switches» à la page 129.

- **Composant Site Selector**

Cette fonction est un nouveau composant de Network Dispatcher.

Le composant Site Selector équilibre la charge dans un groupe de serveurs en choisissant l'adresse IP de serveur correcte qui correspond à la demande du service annuaire. Le client peut ainsi se connecter directement au serveur pour sa communication. Site Selector remplace Interactive Session Support (ISS), composant de Network Dispatcher figurant dans les versions précédentes. Site Selector offre la même fonctionnalité que ISS mais minimise le nombre d'opérations nécessaires à la configuration de l'équilibrage de charge DNS traditionnel.

Pour plus d'informations, reportez-vous aux sections «Chapitre 10.

Planification du composant Site Selector» à la page 109 et «Chapitre 11.

Configuration du composant Site Selector» à la page 115.

- **Système Metric Server**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Metric Server fournit à Network Dispatcher des informations relatives à la

charge des serveurs sous la forme de mesures système. L'agent Metric

Server est un composant de Network Dispatcher qui peut être installé et

exécuté sur les serveurs dont la charge est équilibrée par Network

Dispatcher. Metric Server remplace l'agent SMA (System Monitoring Agent)

qui était pris en charge sous Linux dans les versions précédentes. Metric

Server est accepté sur toutes les plate-formes. Nous recommandons

d'utiliser Metric Server avec le composant Site Selector.

Pour de plus amples informations, reportez-vous à «Metric Server» à la page 157 .

- **Composant Mailbox Locator**

Cette fonction est un nouveau composant de Network Dispatcher.

Le composant Mailbox Locator était une fonction appartenant au composant CBR, qui assurait l'équilibrage de charge entre les serveurs IMAP et POP3 sur la base des ID utilisateur et des mots de passe. La séparation de CBR en deux composants permet d'exécuter Mailbox Locator (anciennement "CBR for IMAP/POP3") et CBR avec Caching Proxy sur le même poste.

Pour plus d'informations, reportez-vous aux sections «Chapitre 8. Planification du composant Mailbox Locator» à la page 97 et «Chapitre 9. Configuration du composant Mailbox Locator» à la page 101.

- **Améliorations apportées à l'utilisation du composant Content Based Routing (CBR)**

La définition du fichier de configuration du proxy (ibmproxy.conf) pour utiliser CBR a été rationalisée et CBR permet désormais d'exécuter plusieurs instances de Caching Proxy simultanément sur le même poste, qui servent d'interface à CBR. Pour plus d'informations sur la configuration de CBR avec Caching Proxy, reportez-vous à la section «Configuration du poste CBR» à la page 88.

- **Prise en charge de Network Address Translation (NAT) et Network Address Port Translation (NAPT)**

Cette fonction s'applique au composant Dispatcher.

NAT/NAPT élimine la nécessité d'implanter les serveurs principaux sur un réseau local. Il permet aussi à Dispatcher de répartir la charge des demandes TCP du client sur différents démons de serveur exécutés sur le même poste physique. Vous pouvez configurer des serveurs à plusieurs démons de deux façons différentes. Avec NAT, vous pouvez configurer plusieurs démons de serveur pour qu'ils répondent aux demandes selon les adresses IP. En d'autres termes, il s'agit de lier un démon de serveur à une adresse IP. Avec NAPT, vous pouvez configurer plusieurs démons de serveur pour qu'ils écoutent sur différents numéros de port.

La méthode d'acheminement NAT de Dispatcher présente l'avantage d'être configurée au niveau du port et donc d'offrir une meilleure granularité.

Remarque : Pour Network Dispatcher, NAT/NAPT ne fonctionnera pas avec les protocoles d'application, par exemple FTP, qui intègrent les adresses ou les numéros de port dans la partie données des messages. C'est là une restriction déjà identifiée pour les fonctions NAT/NAPT, basées sur les en-têtes.

Pour plus d'informations, reportez-vous à la section «Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)» à la page 52.

- **Composant fonction CBR de Dispatcher (avec règle de contenu et affinité des ID de session SSL)**

Cette fonction s'applique au composant Dispatcher.

Dans les versions précédentes de Network Dispatcher, fonction CBR (content-based routing) était disponible uniquement lorsque le composant CBR était utilisé conjointement à Caching Proxy. Le composant Dispatcher permet désormais d'exécuter la fonction fonction CBR (content-based routing) pour HTTP (avec la règle de type de contenu) et HTTPS (avec l'affinité des ID de session SSL) sans Caching Proxy. Pour le trafic HTTP et HTTPS, le composant Dispatcher peut fournir une fonction fonction CBR (content-based routing) plus rapide que le composant CBR.

Pour plus d'informations sur l'utilisation de la règle de contenu et de l'affinité des ID de session SSL, reportez-vous à la section «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54.

- **Affinité de type cookie passif**

Cette fonction s'applique à la méthode d'acheminement CBR (Content-Based Routing) de Dispatcher et au composant CBR.

Affinité de type cookie passif permet d'équilibrer la charge du trafic Web ayant une affinité avec le même serveur, en se basant sur des cookies générés par les serveurs et s'auto-identifiant. Pour plus d'informations, reportez-vous à la section «Affinité de cookie passif» à la page 202.

- **Affinité d'URI (répartition de la charge sur des proxy avec mémoire cache)**

Cette fonction s'applique à la méthode d'acheminement CBR (Content-Based Routing) de Dispatcher et au composant CBR.

Elle permet d'équilibrer la charge du trafic Web sur les serveurs proxy avec mémoire cache de telle façon que la taille de la mémoire cache augmente effectivement. Pour plus d'informations, reportez-vous à la section «Affinité d'URI» à la page 203.

- **Proportions spécifiques pour les grappes ou les sites**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Dans les versions précédentes, l'importance (attribuée aux connexions actives, aux nouvelles connexions, au port et aux mesures système) pour déterminer les décisions d'équilibrage de charge était définie à partir de la fonction gestionnaire. Ces proportions (niveaux d'importance) étaient appliqués à chaque grappe présente dans la configuration du composant. Toutes les grappes étaient mesurées avec les mêmes proportions quel que soit le site dont la charge était équilibrée.

Avec cette nouvelle fonction, vous pouvez définir le niveau d'importance en prenant la grappe (ou le site) pour base. Pour plus d'informations, reportez-vous à la section «Proportion de l'importance accordée aux données d'état» à la page 141.

- **Partitionnement du serveur**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Network Dispatcher permet désormais de partitionner un serveur physique en plusieurs serveurs logiques. Par exemple, vous pouvez ainsi interroger un service spécifique sur le poste pour détecter si un moteur de servlet ou une demande à la base de données est exécutée plus rapidement ou n'est pas exécutée du tout. Cette fonction permet de répartir la charge en se basant sur une charge plus granulaire, spécifique au service. Pour plus d'informations, reportez-vous à la section «Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)» à la page 159.

- **Option de demande/réponse (URL) de conseiller HTTP**

Cette fonction s'applique aux composants Dispatcher et CBR.

Avec cette fonction pour conseiller HTTP, vous pouvez évaluer l'état des différents services présents sur un serveur. Pour chaque serveur logique sur port HTTP, vous pouvez indiquer une chaîne unique d'URL HTTP de client, spécifique au service à interroger sur le serveur. Pour plus d'informations, reportez-vous à la section «Option de demande/réponse (URL) de conseiller HTTP» à la page 161.

- **Conseillers propres aux grappes ou aux sites**

Cette fonction s'applique à tous les composants de Network Dispatcher.

Network Dispatcher permet de démarrer différents conseillers fonctionnant sur le même port mais configurés sur différentes grappes (sites). Par exemple, cette fonction vous permettra d'utiliser un conseiller HTTP sur le port 80 pour une grappe (site) et un conseiller personnalisé sur le port 80 pour une autre grappe (site). Pour plus d'informations, reportez-vous à la section «Lancement et arrêt d'un conseiller» à la page 147.

- **Détection des refus de service**

Cette fonction s'applique au composant Dispatcher.

Cette fonction permet à Dispatcher de détecter les attaques de "refus de service" possibles et d'en alerter l'administrateur. Pour cela, Dispatcher analyse les demandes entrantes d'un certain nombre de connexions partielles, point commun des attaques de refus de service.

Pour plus d'informations, reportez-vous à la section «Détection d'attaque de refus de service» à la page 204.

- **Programmes d'exit utilisateur améliorés**

Cette fonction s'applique à tous les composants, sauf Consultant for Cisco CSS Switches et Site Selector.

Network Dispatcher fournit des exits utilisateur qui déclenchent des scripts que vous pouvez personnaliser. Vous pouvez créer des scripts afin d'effectuer des actions automatisées. Il est, par exemple, possible de consigner le changement d'un état de haute disponibilité ou de prévenir l'administrateur lorsque les serveurs sont marqués comme inactifs. Network Dispatcher fournit les nouveaux exemples de fichier script suivants :

- serverDown, serverUp, managerAlert et managerClear (pour plus d'informations, reportez-vous à la section «Utilisation de scripts pour la génération d'une alerte ou d'une erreur du serveur d'enregistrement» à la page 145)
- highavailChange (pour plus d'informations, reportez-vous à la section «Utilisation de scripts» à la page 178).
- halfOpenAlert : Une attaque de refus de Service (DoS) probable a été détectée (pour plus d'informations, reportez-vous à la section «Détection d'attaque de refus de service» à la page 204).
- halfOpenAlertDone : L'attaque DoS est terminée (pour plus d'informations, reportez-vous à la section «Détection d'attaque de refus de service» à la page 204)

- **Conseiller DB2**

Cette fonction s'applique au composant Dispatcher.

Dispatcher fournit un conseiller DB2 qui communique avec les serveurs DB2. Pour plus d'informations sur le conseiller DB2, reportez-vous à la section «Liste des conseillers» à la page 149.

Composants de Network Dispatcher

Les cinq composants de Network Dispatcher sont Dispatcher, Content Based Routing (CBR), Mailbox Locator, Site Selector et Consultant for Cisco CSS Switches. Network Dispatcher permet d'utiliser ces composants séparément ou ensemble, selon la configuration de votre site. La section qui suit présente ces composants.

Présentation générale du composant Dispatcher

Le composant Dispatcher assure l'équilibrage de charge du trafic entre les serveurs via une combinaison unique de logiciels d'équilibrage de charge et de gestion. Dispatcher peut aussi détecter l'échec d'un serveur et canaliser le trafic sur les serveurs qui l'entourent. Dispatcher prend en charge les protocoles HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3, Telnet et toute application de type TCP ou UDP sans état.

Toutes les demandes de client adressées à la machine Dispatcher sont acheminées vers le serveur le mieux adapté, compte tenu de mesures définies de façon dynamique. Vous pouvez utiliser les valeurs par défaut associées à ces mesures ou les modifier au cours du processus de configuration.

Dispatcher offre trois méthodes d'acheminement (indiquées sur le port) :

- Méthode d'acheminement MAC (**mac**). Cette méthode d'acheminement permet à Dispatcher d'équilibrer la charge de la demande entrante adressée au serveur. Le serveur renvoie la réponse directement au client sans l'intervention de Dispatcher.
- Méthode d'acheminement NAT/NAPT (**nat**). L'utilisation de la fonction NAT (network address translation)/ NAPT (conversion des ports d'adresse réseau) élimine la nécessité pour les serveurs principaux de se trouver sur un réseau local. Si vous préférez disposer de serveurs éloignés, utilisez la méthode d'acheminement nat plutôt que la technique d'encapsulation GRE/WAND. Cette méthode d'acheminement permet à Dispatcher d'équilibrer la charge de la demande entrante adressée au serveur. Le serveur renvoie la réponse à Dispatcher. La machine Dispatcher renvoie ensuite la réponse au client.
- Méthode d'acheminement Content-Based Routing (**CBR**). Sans Caching Proxy, le composant Dispatcher permet d'exécuter la fonction CBR (content-based routing) pour HTTP (avec la règle de type de contenu) et HTTPS (avec l'affinité des ID de session SSL). Pour le trafic HTTP et HTTPS, le composant Dispatcher peut fournir une fonction CBR (content-based routing) plus rapide que le composant CBR. Cette méthode d'acheminement permet à Dispatcher d'équilibrer la charge de la demande entrante adressée au serveur. Le serveur renvoie la réponse à Dispatcher. La machine Dispatcher renvoie ensuite la réponse au client.

Le composant Dispatcher constitue la clé de voûte d'une gestion efficace et durable d'un réseau de serveurs étendu et modulable. Avec Dispatcher, vous pouvez lier différents serveurs en un seul serveur virtuel. De cette manière, le site est associé à une adresse IP unique. Dispatcher fonctionne indépendamment de tout serveur de noms de domaine ; toutes les demandes sont dirigées sur l'adresse IP de la machine Dispatcher.

Dispatcher présente des avantages spécifiques indéniables en matière d'équilibrage de charge sur des serveurs en grappes. Ces atouts permettent de mettre en oeuvre une gestion de site aussi efficace que stable.

Gestion de serveurs locaux avec Dispatcher

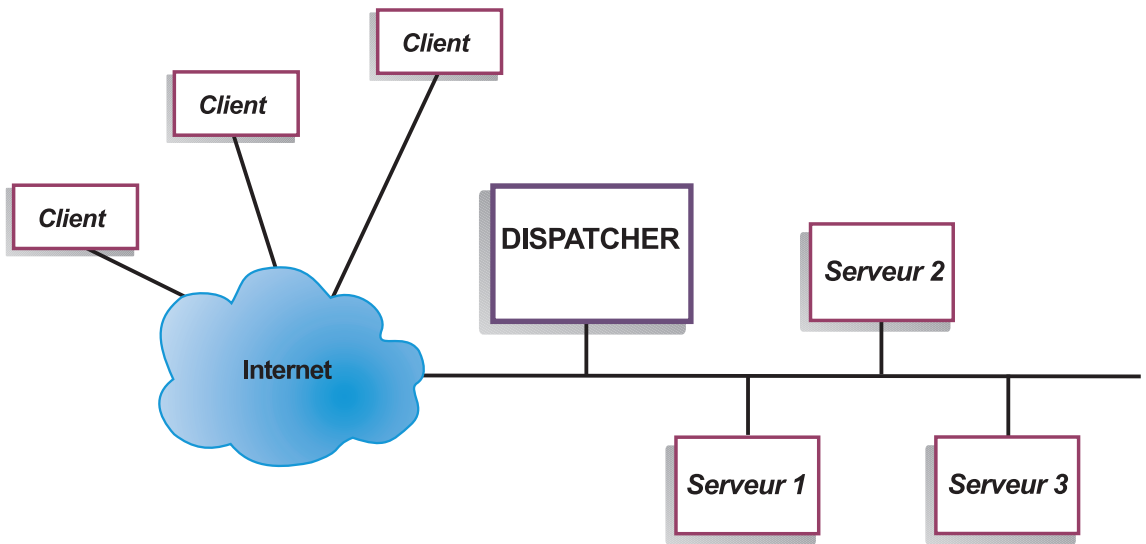


Figure 6. Exemple de représentation physique d'un site utilisant Dispatcher pour gérer les serveurs locaux

La figure 6 est la représentation physique d'un site utilisant une configuration de réseau Ethernet. La machine Dispatcher peut être installée sans apporter de changement physique à la physionomie du réseau. Après acheminement d'une demande de client au serveur optimal par Dispatcher, la réponse correspondante est transmise directement du serveur au client sans intervention de Dispatcher lorsque la méthode d'acheminement MAC est utilisée.

Gestion des serveurs avec Metric Server

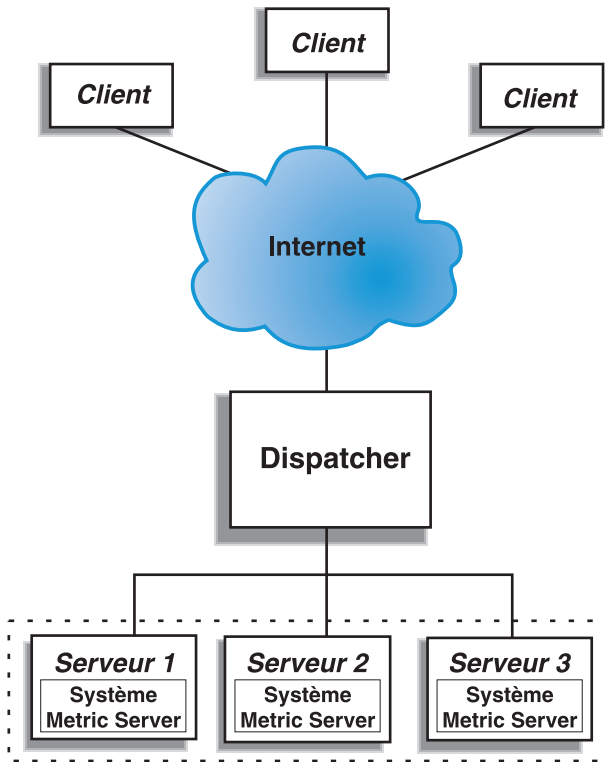


Figure 7. Exemple de site utilisant Dispatcher et Metric Server pour gérer les serveurs

La figure 7 représente un site dans lequel tous les serveurs se trouvent sur un réseau local. Le composant Dispatcher permet d'acheminer les demandes et le composant Metric Server permet de fournir les informations de charge du système au poste Dispatcher.

Dans cet exemple, le démon Metric Server est installé sur chaque serveur principal. Vous pouvez utiliser Metric Server avec le composant Dispatcher ou tout autre composant Network Dispatcher.

Gestion de serveurs locaux et éloignés avec Dispatcher

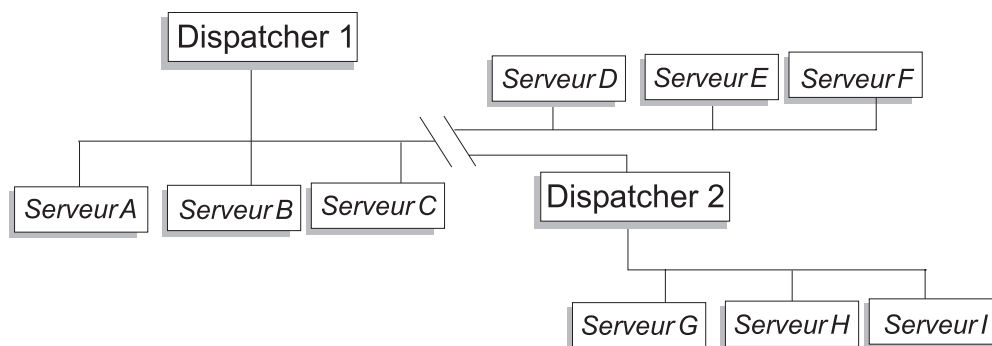


Figure 8. Exemple de site utilisant Dispatcher pour gérer des serveurs locaux et éloignés

La prise en charge de réseau étendu de Dispatcher permet d'utiliser à la fois des serveurs locaux et éloignés (c'est-à-dire des serveurs résidant sur différents sous-réseaux). La figure 8 présente une configuration dans laquelle un Dispatcher "local" (Dispatcher 1) sert de point d'entrée pour l'ensemble des demandes. Il distribue ces demandes entre ses propres serveurs locaux (Serveur A, Serveur B, Serveur C) et au serveur Dispatcher éloigné (Dispatcher 2), qui équilibre la charge sur ses serveurs locaux (Serveur G, Serveur H, Serveur I).

Lors de l'utilisation de la méthode d'acheminement NAT de Dispatcher ou du support GRE, le support de réseau étendu avec Dispatcher peut aussi être assuré sans utiliser de serveur Dispatcher sur le site éloigné (où se trouvent les serveurs D, E et F). Pour plus d'informations, reportez-vous aux sections «Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)» à la page 52 et «Support GRE (Generic Routing Encapsulation)» à la page 171.

Présentation générale du composant CBR (Content Based Routing)

CBR coopère avec Caching Proxy pour relayer les demandes des clients aux serveurs HTTP ou HTTPS (SSL) indiqués. Il permet de manipuler les détails de la mémoire cache pour accélérer le rappel des documents Web avec une petite largeur de bande. CBR et Caching Proxy examinent les requêtes HTTP à l'aide des types de règle indiqués.

CBR permet de spécifier un groupe de serveurs qui doit prendre en charge une demande en fonction de son contenu. CBR permet également d'indiquer plusieurs serveurs pour chaque type de demande. Par conséquent, la charge des demandes peut être répartie pour obtenir une réponse optimale du client. CBR peut aussi détecter les incidents qui se produisent sur un serveur et arrêter d'acheminer des demandes vers ce dernier. L'algorithme d'équilibrage de charge utilisé par le composant CBR est identique à l'algorithme éprouvé utilisé par le composant Dispatcher.

Lorsqu'une demande est reçue par Caching Proxy, elle est comparée aux règles qui ont été définies dans le composant CBR. En cas de correspondance, l'un des serveurs associés à cette règle est désigné pour prendre en charge la demande. Caching Proxy continue alors son traitement normal pour acheminer la demande vers le serveur sélectionné.

CBR offre les mêmes fonctions que Dispatcher à l'exception des fonctions de haute disponibilité, de sous-agent, de réseau étendu et de quelques commandes de configuration.

Caching Proxy doit être en fonction pour permettre à CBR d'équilibrer la charge des demandes des clients.

Gestion des serveurs locaux avec CBR

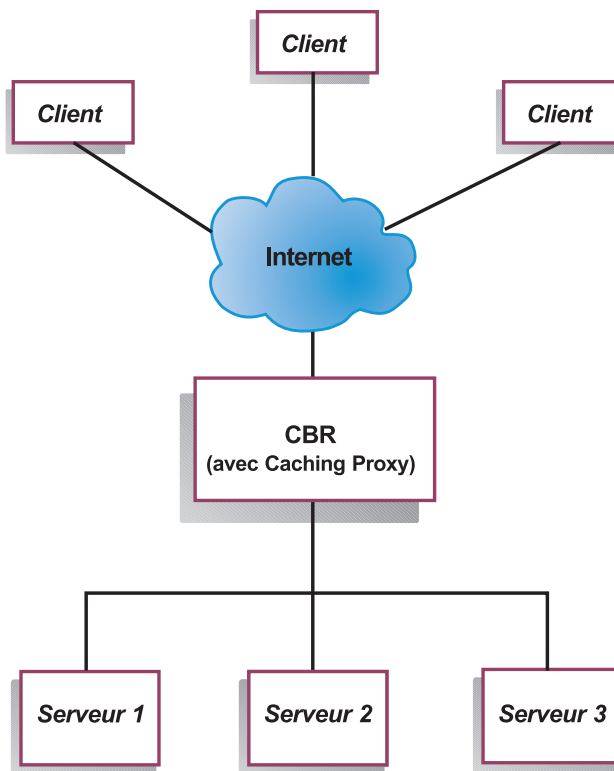


Figure 9. Exemple de site utilisant CBR pour gérer les serveurs locaux

La figure 9 montre la représentation logique d'un site utilisant CBR pour acheminer des demandes issues des serveurs locaux. Le composant CBR utilise Caching Proxy pour acheminer les demandes des clients (HTTP ou HTTPS) aux serveurs en fonction du contenu de l'URL.

Présentation générale du composant Mailbox Locator

Mailbox Locator peut fournir un point de présence unique à plusieurs serveurs IMAP ou POP3. Chacun des serveurs peut disposer d'un sous-réseau de toutes les boîtes aux lettres des utilisateurs desservis par le point de présence. Dans le cas des protocoles IMAP et POP3, Mailbox Locator est un proxy qui choisit un serveur approprié en se fondant sur l'ID utilisateur et le mot de passe donnés par le client. Mailbox Locator ne prend pas en charge l'équilibrage de charge à base de règles.

Remarque : Le composant Mailbox Locator était auparavant une fonction appartenant au composant CBR qui assurait l'équilibrage de charge sur les serveurs de messagerie IMAP et POP3. La répartition de CBR en deux composants permet d'exécuter "CBR for IMAP/POP3" (Mailbox Locator) et "CBR for HTTP/HTTPS" (CBR avec Caching Proxy) sur le même poste.

Gestion de serveurs locaux avec Mailbox Locator

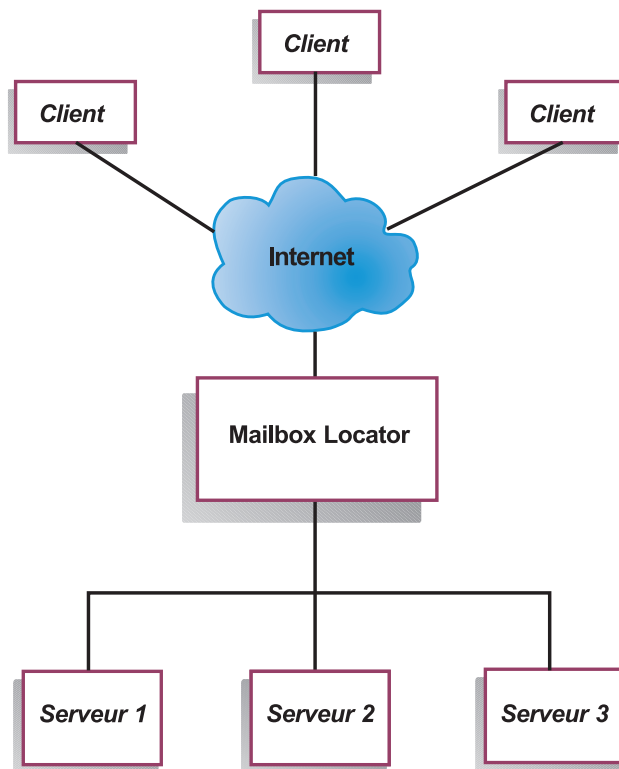


Figure 10. Exemple de site utilisant Mailbox Locator pour gérer les serveurs locaux

La figure 10 à la page 41 montre la représentation logique d'un site utilisant Mailbox Locator pour relayer les demandes des clients (protocole IMAP ou POP3) vers le serveur approprié, en fonction de l'ID utilisateur et du mot de passe.

Présentation générale du composant Site Selector

Site Selector fonctionne avec d'autres serveurs de noms pour équilibrer la charge sur un groupe de serveurs à l'aide des mesures et des pondérations recueillies. Vous pouvez créer une configuration de site pour assurer l'équilibrage de charge sur un groupe de serveurs sur la base du nom de domaine utilisé pour la demande d'un client.

Un client envoie une demande de résolution de nom de domaine à un serveur de noms appartenant au réseau. Le serveur de noms achemine la demande au poste Site Selector. Site Selector résout le nom de domaine en adresse IP de l'un des serveurs qui a été configuré sous le nom du site. Site Selector renvoie l'adresse IP du serveur sélectionné au serveur de noms. Le serveur de noms renvoie l'adresse IP au client.

Metric Server est un composant de Network Dispatcher qui surveille le système et doit être installé sur chaque serveur dont la charge doit être équilibrée dans votre configuration. Metric Server permet à Site Selector de surveiller le niveau d'activité d'un serveur, de détecter le moment où un serveur est le moins chargé et de détecter un serveur défaillant. Par charge, on entend le travail effectivement fourni par le serveur. En personnalisant les fichiers script de mesure du système, vous pouvez choisir le type de mesure utilisé pour évaluer la charge. Site Selector peut être configuré en fonction de chaque environnement, en tenant compte de facteurs tels que la fréquence des accès, le nombre total d'utilisateurs et les différents types d'accès (requêtes courtes, longues, à forte ou faible consommation de ressources CPU).

Gestion des serveurs locaux et éloignés avec Site Selector et Metric Server

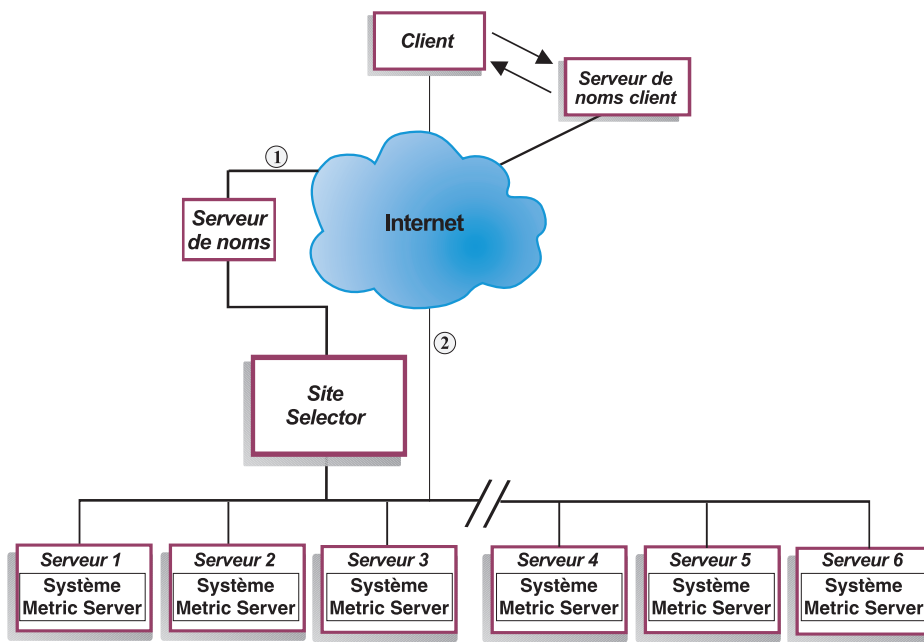


Figure 11. Exemple de site utilisant Site Selector et Metric Server pour gérer les serveurs locaux et éloignés

La figure 11 illustre un site utilisant le composant Site Selector pour répondre aux demandes. Serveur 1, Serveur 2 et Serveur 3 sont des serveurs locaux. Serveur 4, Serveur 5 et Serveur 6 sont des serveurs éloignés.

Un client envoie une demande de résolution de nom de domaine à un serveur de noms client. Le serveur de noms client achemine la demande au poste Site Selector (chemin d'accès 1) via DNS. Site Selector résout ensuite le nom de domaine en adresse IP de l'un des serveurs. Site Selector renvoie l'adresse IP du serveur sélectionné au serveur de noms client. Le serveur de noms renvoie l'adresse IP au client.

Lorsque le client reçoit l'adresse IP du serveur, il achemine les demandes suivantes directement au serveur sélectionné (chemin d'accès 2).

Remarque : Dans cet exemple, le serveur Metric Server fournit les informations de charge du système au poste Site Selector. L'agent Metric Server est installé sur chaque serveur principal. Vous devez utiliser Metric Server conjointement à Site Selector, sinon Site Selector peut seulement utiliser une méthode de sélection par permutation circulaire pour l'équilibrage de charge.

Présentation générale du composant Consultant for Cisco CSS Switches

Consultant for Cisco CSS Switches constitue une solution complémentaire avec le relais Cisco CSS 11000 series. La solution combinée réunit de robustes fonctions d'acheminement de paquets et de routage de contenu à des algorithmes de reconnaissance sophistiqués pour déterminer la disponibilité des serveurs principaux, des applications et des bases de données ainsi que les informations de charge. La fonction Cisco Consultant fait appel au gestionnaire de Network Dispatcher, aux conseillers standard et personnalisés et à Metric Server pour déterminer les mesures, la santé et la charge des serveurs principaux, des applications et des bases de données. Cisco Consultant utilise ces informations pour générer les mesures de pondération, qu'il envoie au serveur Cisco CSS Switch pour la sélection du serveur optimal, l'optimisation de la charge et la tolérance aux pannes.

Le serveur Cisco CSS Switch prend les décisions d'équilibrage de charge en fonction des critères définis par l'utilisateur.

Cisco Consultant suit de nombreux critères, dont :

- les connexions actives et nouvelles,
- la disponibilité des applications et des bases de données, qui est facilitée par l'utilisation de conseillers standard et personnalisés et les agents résidant sur le serveur, adaptés à l'application spécifique,
- l'utilisation de la CPU,
- l'utilisation de la mémoire,
- les mesures du serveur personnalisables par l'utilisateur.

Lorsqu'un serveur Cisco CSS Switch, sans Cisco Consultant, détermine la santé d'un serveur de contenu, il utilise les temps de réponse aux demandes de contenu ou d'autres mesures de réseau. Avec Cisco Consultant, le serveur Cisco CSS Switch se décharge de ces activités sur le serveur Cisco Consultant. Cisco Consultant influence la pondération du serveur ou sa faculté à servir le contenu, et active ou suspend un serveur, selon le cas, lorsque le serveur devient disponible ou indisponible.

Cisco Consultant:

- Utilise une interface SNMP publiée pour obtenir des informations de connexion à partir du serveur Cisco CSS Switch
- Utilise les données d'entrée du conseiller pour analyser les informations de connexion
- Utilise les informations Metric Server pour analyser la santé relative du serveur
- Génère des pondérations pour chaque serveur de la configuration

Les pondérations définies s'appliquent à tous les serveurs connectés sur un même port. Pour chaque port, les demandes sont réparties entre les serveurs selon la pondération relative de chacun. Par exemple, si un serveur a une pondération (paramètre Weight) de 10 et un autre de 5, le premier recevra deux fois plus de demandes que le second. Ces pondérations sont fournies au serveur Cisco CSS Switch avec SNMP. Lorsque la valeur de pondération d'un serveur est augmentée, le serveur Cisco CSS Switch dirige davantage de demandes vers ce serveur.

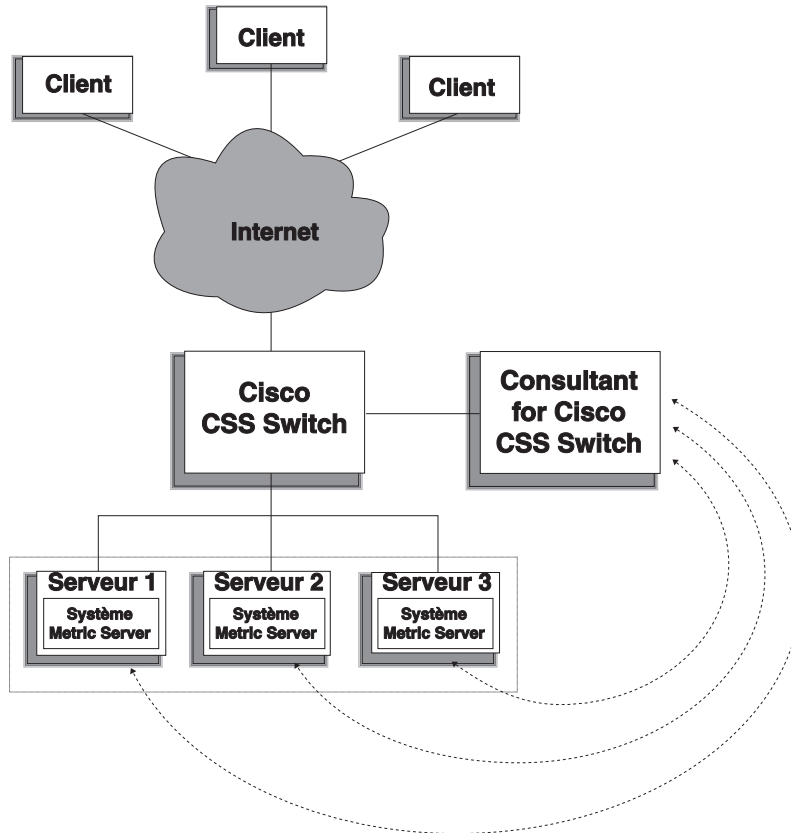


Figure 12. Exemple de site utilisant Cisco Consultant et Metric Server pour gérer les serveurs locaux

Cisco Consultant, conjointement au serveur Cisco CSS Switch, constitue une solution idéale qui combine la commutation de contenu à haute vitesse avec la reconnaissance d'applications sophistiquées, la tolérance aux pannes et l'optimisation de la charge des serveurs. Cisco Consultant appartient à une solution globale complémentaire située entre le serveur Cisco CSS Switch et IBM WebSphere Edge Server.

Pour la liste des éléments requis pour Cisco Consultant, reportez-vous à la section «Chapitre 2. Installation de Network Dispatcher» à la page 11.

Haute disponibilité

Dispatcher

Dispatcher offre une fonctionnalité de haute disponibilité intégrée. Cette dernière implique l'utilisation d'une deuxième machine Dispatcher, chargée de contrôler la machine principale (également appelée machine primaire), et qui reste en attente, prête à assurer l'équilibrage de charge en cas d'incident sur la machine principale. Le composant Dispatcher offre également la fonction de haute disponibilité réciproque qui permet à deux machines de travailler simultanément en mode primaire et secondaire l'une avec l'autre. Reportez-vous à la section «Configuration de la haute disponibilité» à la page 173.

CBR, Mailbox Locator, Site Selector

Lorsque vous utilisez une configuration à deux niveaux avec un poste Dispatcher répartissant la charge sur deux postes serveur ou plus dotés de CBR, Mailbox Locator ou Site Selector, vous pouvez atteindre un niveau de haute disponibilité pour ces composants de Network Dispatcher.

Chapitre 4. Planification du composant Dispatcher

Le présent chapitre décrit les aspects que l'administrateur de réseau doit prendre en compte avant d'installer et de configurer le composant Dispatcher.

- Reportez-vous au «Chapitre 5. Configuration du composant Dispatcher» à la page 57 pour obtenir des informations sur la configuration des paramètres d'équilibrage de charge de Dispatcher.
- Pour obtenir des informations sur la configuration de Network Dispatcher pour les fonctions avancées, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Il contient les sections suivantes :

- «Matériel et logiciels requis»
- «Remarques relatives à la planification» à la page 48
- «Haute disponibilité» à la page 50
- «Réacheminement MAC de Dispatcher (méthode d'acheminement mac)» à la page 52
- «Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)» à la page 52
- «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54

Matériel et logiciels requis

Conditions requises par la plate-forme :

- Pour AIX, reportez-vous à la section «Configuration requise pour AIX» à la page 12
- Pour Linux, reportez-vous à la section «Configuration requise pour Red Hat Linux ou SuSE Linux» à la page 17
- Pour Solaris, reportez-vous à la section «Configuration requise pour Solaris» à la page 20
- Pour Windows 2000, reportez-vous à la section «Configuration requise pour Windows 2000» à la page 22

Remarques relatives à la planification

Dispatcher se compose des fonctions suivantes :

- La commande **ndserver** gère les requêtes adressées à l'exécuteur, au gestionnaire et aux conseillers depuis la ligne de commande.
- L'**exécuteur** assure l'équilibrage de la charge des connexions TCP et UDP sur la base des ports. Il peut transmettre des connexions à des serveurs en fonction du type de demande reçu (par exemple, HTTP, FTP, SSL, etc.)
L'exécuteur s'exécute toujours lorsque le composant Dispatcher est utilisé pour l'équilibrage de charge.
- Le **gestionnaire** définit les mesures utilisées par l'exécuteur en fonction de plusieurs facteurs :
 - Décomptes internes de l'exécuteur
 - Retour d'informations sur les serveurs fourni par les conseillers
 - Retour d'informations émanant d'un programme de contrôle système, tel que Metric Server ou WLM.

L'utilisation du gestionnaire n'est que facultative. Toutefois, s'il n'est pas utilisé, l'équilibrage de charge se fera sur la base d'une planification circulaire pondérée, elle-même basée sur les mesures de charge des serveurs et les conseillers ne seront pas disponibles.

- Les **conseillers** interrogent les serveurs puis analysent les résultats par protocole avant de demander au gestionnaire de régler les capacités comme il convient. Actuellement, il existe des conseillers pour les protocoles suivants : HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3 et Telnet.

Dispatcher fournit également des conseillers qui n'échangent pas d'informations relatives aux protocoles, tels que : le conseiller DB2 qui indique l'état des serveurs DB2 et le conseiller Ping qui indique si le serveur répond à une commande ping. Pour connaître la liste complète des conseillers, reportez-vous à la section «Liste des conseillers» à la page 149.

Vous avez également la possibilité de développer vos propres conseillers (reportez-vous à la section «Création de conseillers personnalisés» à la page 151).

L'utilisation des conseillers est facultative mais recommandée.

- Pour configurer et gérer l'exécuteur, les conseillers et le gestionnaire, utilisez la ligne de commande (**ndcontrol**) ou l'interface utilisateur graphique (**ndadmin**).
- Un **fichier de configuration exemple** est fourni et peut être utilisé pour la configuration et l'administration de la machine Dispatcher. Reportez-vous à l'«Annexe F. Exemples de fichiers de configuration» à la page 387. Une fois le produit installé, ce fichier se trouve dans le sous-répertoire **nd/servers/samples** où réside Network Dispatcher.
- Le **sous-agent SNMP** permet à une application de gestion de type SNMP de contrôler l'état de Dispatcher.

Les trois fonctions clés de Dispatcher (l'exécuteur, le gestionnaire et les conseillers) agissent en collaboration pour équilibrer et répartir entre les serveurs les requêtes réceptionnées. Outre la gestion des requêtes d'équilibrage de charge, l'exécuteur contrôle le nombre de nouvelles connexions, de connexions actives et de connexions terminées. Il assure également le retrait des connexions terminées ou réinitialisées et transmet ces informations au gestionnaire.

Le gestionnaire recueille les informations transmises par l'exécuteur, les conseillers et par tout programme de contrôle tel que Metric Server. Sur la base de ces informations, le gestionnaire ajuste les capacités des machines serveurs, pour chaque port, et transmet ces données à l'exécuteur qui en tient compte pour l'équilibrage de charge des nouvelles connexions.

Les conseillers contrôlent chaque serveur relié au port dont ils ont la charge afin de déterminer leur temps de réponse et leur disponibilité, puis retournent ces informations au gestionnaire. Les conseillers détectent également si un serveur est opérationnel ou non. Sans la contribution du gestionnaire et des conseillers, l'exécuteur assure une planification circulaire basée sur les capacités courantes des serveurs.

Haute disponibilité

Haute disponibilité simple

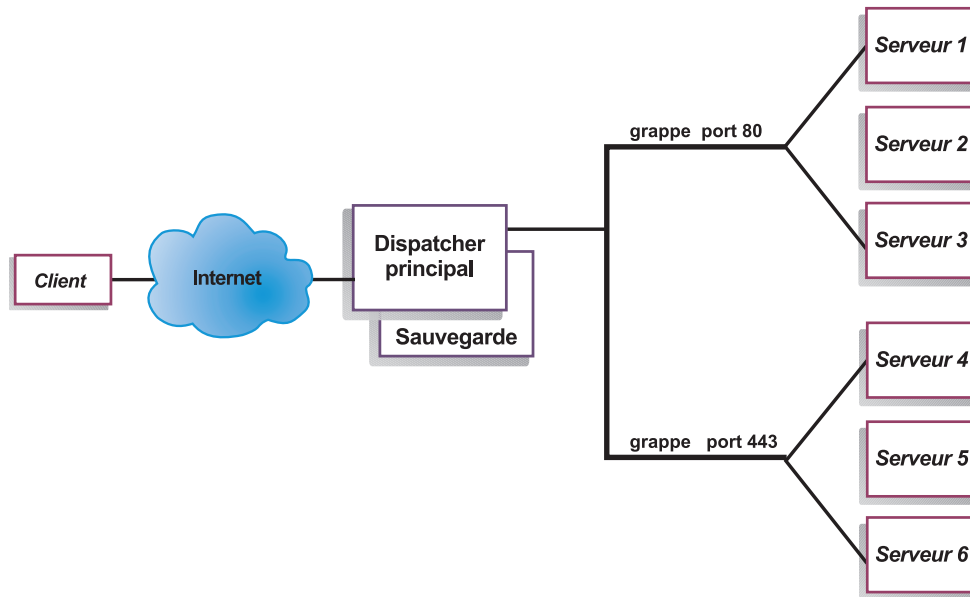


Figure 13. Exemple de Dispatcher utilisant la haute disponibilité

La fonctionnalité de haute disponibilité requiert une deuxième machine. La première se charge de l'équilibrage de charge pour la totalité du trafic client, comme ce serait le cas dans une configuration à une seule machine. La seconde machine surveille le bon fonctionnement de la première et reprend l'équilibrage de charge si elle détecte un échec de la première machine.

Chacune des deux machines se voit affecter un rôle spécifique, *principal* ou de *sauvegarde*. La machine principale envoie régulièrement les données de connexion à la machine de secours. Pendant que la machine principale est *active* (équilibrage de charge), la machine de sauvegarde est en état d'*attente* et ses données s'actualisent en permanence, ce qui lui permet de prendre le relais des opérations en cas de besoin.

Les sessions de communication entre les deux machines sont désignées par le terme *signal de présence*. Ces signaux permettent à chaque machine de contrôler l'état de l'autre.

Si la machine de sauvegarde détecte que la machine principale est défaillante, elle prend en charge l'équilibrage de charge. A cette étape, les *états* respectifs des deux machines s'inversent : la machine de secours devient *active* et la machine principale passe en *attente*.

Dans la configuration à haute disponibilité, les deux machines doivent être sur le même sous-réseau.

Pour plus d'informations sur la fonction de haute disponibilité, reportez-vous à la section «Haute disponibilité» à la page 173.

Haute disponibilité réciproque

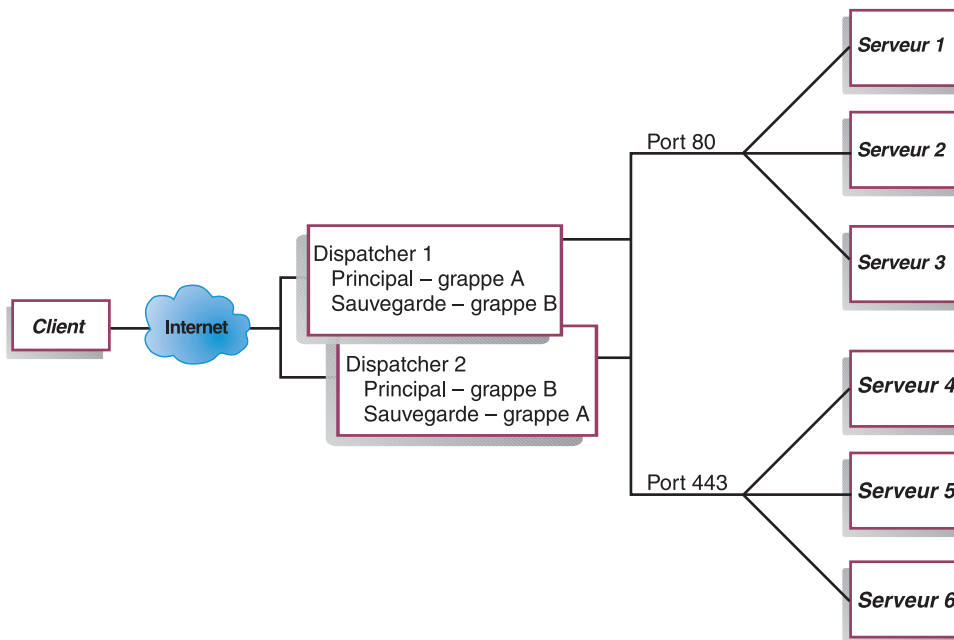


Figure 14. Exemple de Dispatcher utilisant la haute disponibilité réciproque

La fonctionnalité à haute disponibilité réciproque implique l'utilisation de deux machines. Les deux machines effectuent l'équilibrage de charge du trafic client de manière active et assurent réciproquement la sauvegarde l'une de l'autre. Dans une configuration à haute disponibilité, une seule machine effectue l'équilibrage de charge. Dans une configuration à haute disponibilité réciproque, les deux machines assument l'équilibrage de charge d'une partie du trafic du client.

Pour la haute disponibilité réciproque, le trafic client est affecté à chaque machine sur la base d'une adresse de grappe. Chaque grappe peut être configurée avec l'adresse de non-acheminement (NFA) de sa machine primaire. La machine du Dispatcher principal effectue normalement l'équilibrage de charge pour cette grappe. En cas de panne, l'autre machine assume l'équilibrage de charge pour sa propre grappe et pour la grappe du dispatcher qui est en panne.

La figure 14 à la page 51 illustre une configuration de haute disponibilité réciproque avec "grappe partagée A" et "grappe partagée B". Chaque répartiteur peut acheminer activement des paquets pour sa grappe *principale*. Si l'un des répartiteurs venait à échouer et ne pouvait plus activement acheminer les paquets pour sa grappe principale, l'autre répartiteur pourrait le remplacer et acheminerait les paquets pour sa grappe de *sauvegarde*.

Remarque : Les deux machines doivent configurer de la même façon leur ensembles de grappe partagés.

Pour plus d'informations sur la fonction de haute disponibilité, reportez-vous à la section «Haute disponibilité» à la page 173.

Réacheminement MAC de Dispatcher (méthode d'acheminement mac)

La méthode d'acheminement MAC de Dispatcher (qui est la méthode d'acheminement par défaut) permet d'équilibrer la charge de la demande entrante sur le serveur sélectionné et de faire en sorte que le serveur renvoie une réponse *directement* au client sans impliquer le composant Dispatcher. Ainsi, Dispatcher se contente de surveiller les flux entrants du client vers le serveur. Il n'effectue aucun contrôle des transmissions en sortie, du serveur vers le client. Cet aspect réduit sensiblement son impact sur les performances des applications et permet même d'accroître celles du réseau.

La méthode d'acheminement peut être sélectionnée lors de l'ajout d'un port à l'aide de la commande **ndcontrol port add grappe:port method valeur**. La valeur de la méthode d'acheminement par défaut est **mac**. Vous ne pouvez spécifier le paramètre **method** que lorsque le port est ajouté. Une fois le port ajouté, vous ne pouvez pas modifier les paramètres de la méthode d'acheminement. Pour de plus amples informations, reportez-vous à «ndcontrol port — Configuration des ports» à la page 296.

Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)

Si vous utilisez NAT ou NAPT, il n'est pas nécessaire que les serveurs d'équilibrage de charge se trouvent sur un réseau local. Si vous préférez disposer de serveurs à distance, utilisez la méthode d'acheminement NAT plutôt que la technique d'encapsulation GRE/WAN.

Vous pouvez également utiliser la fonction NAPT pour accéder à plusieurs démons de serveur situés sur chaque machine serveur faisant l'objet d'un équilibrage de charge, où chaque démon écoute sur un port unique.

Vous pouvez configurer un serveur à plusieurs démons de deux façons différentes.

- Avec NAT, vous pouvez configurer plusieurs démons de serveur pour qu'ils répondent aux demandes selon les adresses IP. En d'autres termes, il s'agit de lier un démon de serveur à une adresse IP.
- Avec NAPT, vous pouvez configurer plusieurs démons (qui s'exécutent sur le même serveur physique) pour qu'ils écoutent sur différents numéros de port.

L'application fonctionne bien avec des protocoles de niveau supérieur tels que HTTP, SSL, IMAP, POP3, NNTP, SMTP, Telnet, etc.

Restrictions :

- L'implémentation de NAT/NAPT de Dispatcher est une implémentation *simple* de cette fonction. Il ne procède à l'analyse et ne traite que le contenu des en-têtes de paquets TCP/IP. Il n'analyse pas le contenu de la partie données des paquets. Pour Dispatcher, NAT/NAPT ne fonctionnera pas avec les protocoles d'application, tels que FTP, qui intègrent les adresses ou les numéros de port dans la partie données des messages. Il s'agit d'une restriction déjà identifiée des fonctions NAT/NAPT basées sur les en-têtes.
- La fonction NAT/NAPT de Dispatcher ne peut pas fonctionner si vous utilisez la fonction de grappe générique ou de port générique.

Pour implémenter NAT/NAPT, procédez aux opérations ci-dessous.

- Définissez le paramètre **clientgateway** à l'aide de la commande **ndcontrol executor set**. Clientgateway est une adresse IP correspondant à l'adresse du routeur par lequel le trafic de retour est acheminé de Network Dispatcher vers les clients. Sa valeur doit correspondre à une adresse IP non nulle pour que vous puissiez utiliser NAT/NAPT. Pour de plus amples informations, reportez-vous à «ndcontrol executor — Contrôle de l'exécuteur» à la page 271.
- Ajoutez un port à l'aide de la commande **ndcontrol port add grappe:port method valeur**. La valeur de la méthode d'acheminement doit être associée à **nat**. Vous ne pouvez spécifier le paramètre **method** que lorsque le port est ajouté. Une fois le port ajouté, vous ne pouvez pas modifier les paramètres de la méthode d'acheminement. Pour de plus amples informations, reportez-vous à «ndcontrol port — Configuration des ports» à la page 296.

Remarque : Si vous n'associez pas une valeur non nulle à l'adresse de passerelle, la méthode d'acheminement ne peut être que **mac** (méthode d'acheminement basée sur MAC).

- Ajoutez un serveur avec les paramètres **mapport**, **returnaddress** et **router** à l'aide de la commande **ndcontrol**. Par exemple :

```
ndcontrol server add grappe:port:serveur mapport valeur returnaddress  
adresseretour router adresserouteur
```

– **mapport**

Cette commande permet de mapper le numéro de port de destination de la demande client (pour Dispatcher) au numéro de port du serveur que Dispatcher utilise pour équilibrer la charge de la demande du client. Mapport permet à Network Dispatcher de recevoir une demande de client sur un port et de la transmettre à un autre port sur la machine serveur. Le paramètre **mapport** permet d'équilibrer la charge des demandes d'un client sur une machine serveur sur laquelle peuvent s'exécuter plusieurs démons serveur. La valeur par défaut du paramètre **mapport** est le numéro de port de destination de la demande du client.

– **returnaddress**

L'adresse retour correspond à une adresse ou à un nom d'hôte unique que vous configurez sur la machine Dispatcher. Dispatcher utilise l'adresse de retour comme adresse source lors de l'équilibrage de charge de la demande du client sur le serveur. Elle permet de garantir que le serveur renverra le paquet à la machine Dispatcher au lieu d'envoyer le paquet directement au client. (Dispatcher transmettra ensuite le paquet IP au client.) Vous devez indiquer la valeur d'adresse de retour lors de l'ajout du serveur. Vous ne pouvez pas modifier l'adresse de retour sauf si vous supprimez le serveur et que vous l'ajoutez à nouveau. L'adresse de retour ne peut pas être identique à l'adresse de grappe, de serveur ou NFA.

– **router**

Adresse du routeur vers le serveur éloigné.

Pour plus d'informations sur la commande **ndcontrol server** et les paramètres **mapport**, **returnaddress** et **router**, reportez-vous à la section «**ndcontrol server** — Configuration des serveurs» à la page 311.

Fonction CBR de Dispatcher (méthode d'acheminement **cbr**)

Dans les versions précédentes de Network Dispatcher, la fonction CBR (content-based routing) était disponible uniquement lorsque le composant CBR était utilisé avec Caching Proxy. Le composant Dispatcher permet désormais d'exécuter la fonction CBR (content-based routing) pour HTTP (avec la règle de type de contenu) et HTTPS (avec l'affinité des ID de session

SSL) sans Caching Proxy. Pour le trafic HTTP et HTTPS, le composant Dispatcher peut fournir une fonction CBR (content-based routing) plus rapide que le composant CBR.

Pour HTTP : La sélection du serveur, pour fonction CBR de Dispatcher, est effectuée sur la base du contenu d'une adresse URL ou d'un en-tête HTTP. Cette option est configurée à l'aide du type de règle "Contenu". Lors de la configuration de la règle de contenu, spécifiez la chaîne de recherche "pattern" et un ensemble de serveurs pour la règle. Lors du traitement d'une nouvelle demande entrante, cette règle compare la chaîne indiquée à l'URL du client ou à l'en-tête HTTP spécifié dans la demande du client.

Si Dispatcher trouve la chaîne dans la demande du client, il transmet la demande à l'un des serveurs de la règle. Dispatcher achemine ensuite les données de la réponse du serveur vers le client (méthode d'acheminement cbr).

Si Dispatcher ne trouve pas la chaîne dans la demande du client, il ne sélectionne *pas* de serveur dans l'ensemble de serveurs de la règle.

Remarque : La règle de contenu est configuré dans le composant Dispatcher de la même façon que dans le composant CBR. Dispatcher peut utiliser la règle de contenu pour le trafic HTTP. Toutefois, le composant CBR peut utiliser la règle de contenu *à la fois* pour le trafic HTTP et HTTPS (SSL).

Pour HTTPS (SSL) : l'acheminement CBR (content-based routing) de Dispatcher basée sur la zone de session SSL ID de la demande client. Avec SSL, une demande client contient l'ID session SSL d'une session antérieure, et les serveurs gèrent une cache de leurs connexions SSL précédentes. L'affinité de l'ID de session SSL de Dispatcher permet au client et au serveur d'établir une nouvelle connexion à l'aide des paramètres de sécurité de la connexion précédente au serveur. En éliminant la renégociation des paramètres de sécurité SSL, comme les clés partagées et les algorithmes de chiffrement, les serveurs sauvegardent des cycles CPU et le client obtient une réponse plus rapidement. Pour activer l'affinité de l'ID de session SSL, le port **stickytime** doit être associé à une valeur autre que zéro. Si le délai de maintien de routage est dépassé, le client peut être envoyé à un autre serveur.

Pour implémenter la fonction CBR de Dispatcher (méthode d'acheminement cbr), procédez aux opérations ci-dessous.

- Définissez le paramètre **clientgateway** à l'aide de la commande **ndcontrol executor set**. Clientgateway est une adresse IP correspondant à l'adresse du routeur par lequel le trafic de retour est acheminé de Dispatcher vers les clients. La valeur par défaut de clientgateway est zéro. Vous devez associer cette valeur à une adresse IP différente de zéro pour pouvoir ajouter une

méthode d'acheminement CBR (fonction CBR (content-based routing)). Pour de plus amples informations, reportez-vous à «ndcontrol executor — Contrôle de l'exécuteur» à la page 271.

- Ajoutez un port avec le paramètre **method** dans la commande **ndcontrol port add**. La valeur de la méthode d'acheminement doit correspondre à **cbr**. Pour de plus amples informations, reportez-vous à «ndcontrol port — Configuration des ports» à la page 296.

Remarque : Si vous n'associez pas une valeur différente de zéro à l'adresse de passerelle client, la méthode d'acheminement ne peut être que de type **MAC**.

- Ajoutez un serveur avec les paramètres **mapport**, **returnaddress** et **router**
ndcontrol server add *grappe:port:serveur* **mapport** *valeur* **returnaddress** *adresseretur* **router** *adresserouteur*

Remarque : Pour plus d'informations sur la configuration du serveur avec les paramètres **mapport**, **returnaddress** et **router**, reportez-vous à la page 54.

- **Pour HTTP :** procédez à la configuration à l'aide de règles basées sur le contenu de la demande client (type de règle **contenu**). Par exemple,
ndcontrol rule 125.22.22.03:80:contentRule1 **type** content **pattern** *motif*
où *masque* indique le masque à utiliser pour une règle de type de contenu. Pour plus d'informations sur le type de règle de contenu, reportez-vous à la section «Utilisation de règles basées sur le contenu des demandes» à la page 189. Pour plus d'informations sur les expressions valides de *masque*, reportez-vous à la section «Annexe C. Syntaxe des règles de contenu (modèle)» à la page 323.

Pour HTTPS (SSL) : pour configurer l'affinité de l'ID de session SSL, attribuez une valeur différente de zéro au paramètre **stickytime** du port. Pour plus d'informations sur le paramètre **stickytime** de la commande **port**, reportez-vous à la section «ndcontrol rule — configuration des règles» à la page 303.

Remarque : La fonction de réplication des enregistrements de connexions de haute-disponibilité (qui garantit que la connexion d'un client ne sera pas annulée lorsqu'une machine Dispatcher de sauvegarde remplace la machine principale) n'est *pas* pris en charge avec la fonction **cbr** de Dispatcher.

Chapitre 5. Configuration du composant Dispatcher

Avant d'effectuer les opérations décrites dans le présent chapitre, reportez-vous à la section «Chapitre 4. Planification du composant Dispatcher» à la page 47. Ce chapitre décrit comment créer une configuration de base pour le composant Dispatcher de Network Dispatcher.

- Pour de plus amples informations sur Network Dispatcher, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Présentation générale des tâches de configuration

Remarque : Avant de suivre les étapes de configuration détaillées dans ce tableau, assurez-vous que la machine Dispatcher et toutes les machines serveurs sont connectées au réseau, ont des adresses IP valides et peuvent communiquer entre elles par la triangulation ping.

Tableau 3. Tâches de configuration pour la fonction Dispatcher

Tâche	Description	Informations connexes
Configuration de la machine Dispatcher.	Définition de la configuration pour l'équilibrage de charge	«Configuration de la machine Dispatcher» à la page 60
Configuration des machines pour l'équilibrage de charge	Affectation d'un alias à l'unité de bouclage, recherche et suppression de la route supplémentaire	«Configuration des serveurs pour l'équilibrage de la charge» à la page 67

Méthodes de configuration

Il existe quatre méthodes de base pour la configuration de Dispatcher :

- Ligne de commande
- Scripts
- Interface graphique
- Assistant de configuration

Ligne de commande

C'est la méthode la plus directe pour la configuration de Dispatcher. Les valeurs des paramètres de commande doivent être saisies en anglais. Les seules exceptions s'appliquent aux noms d'hôte (utilisés dans les commandes cluster, server et highavailability) et aux noms de fichiers (utilisés dans les commandes file).

Pour lancer Dispatcher à partir de la ligne de commande :

- Lancez la commande **ndserver** à partir de l'invite. Sous Windows 2000, ndserver s'exécute en tant que service NT et démarre automatiquement.

Remarque : Pour arrêter le service, lancez la commande suivante :
ndserver stop.

- Lancez ensuite les commandes de contrôle voulues en vue de définir votre configuration. Les procédures décrites dans ce manuel reposent sur l'utilisation de la ligne de commande. La commande est **ndcontrol**. Pour plus de détails sur les commandes, reportez-vous à la section «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Vous pouvez entrer une version abrégée des paramètres de commandes ndcontrol. Il suffit d'entrer les lettres uniques des paramètres. Par exemple, pour obtenir l'aide correspondant à la commande file save, entrez **ndcontrol he f** à la place de **ndcontrol help file**.

Pour démarrer l'interface de ligne de commande, entrez **ndcontrol** pour ouvrir une invite ndcontrol.

Pour fermer l'interface de ligne de commande, entrez **exit** ou **quit**.

Scripts

Les commandes permettant de configurer Dispatcher peuvent être entrées dans un fichier script de configuration, puis exécutées ensemble. Reportez-vous à la section «Exemples de fichiers de configuration Network Dispatcher» à la page 387.

Remarque : Pour exécuter rapidement le contenu d'un fichier script (par exemple, mon_script), utilisez l'une des commandes suivantes :

- Pour mettre à jour la configuration actuelle, soumettez les commandes exécutables à partir du fichier script, en entrant —
**ndcontrol file
appendload mon_script**
- Pour remplacer la configuration actuelle, soumettez les commandes exécutables à partir du fichier script en entrant —
ndcontrol file newload mon_script

Interface graphique

Pour avoir un exemple de l'interface graphique, reportez-vous à la figure 2 à la page 5.

Pour démarrer l'interface graphique, procédez de la manière suivante :

1. Vérifiez que ndserver est en cours d'exécution.
 - Sous AIX, Linux ou Solaris, exécutez la commande suivante (en tant que superutilisateur) :
ndserver
 - Sous Windows 2000, ndserver s'exécute en tant que service et démarre automatiquement.
2. Ensuite, effectuez l'une des opérations suivantes :
 - Sous AIX, Linux ou Solaris : entrez **ndadmin**.
 - Sous Windows 2000 : cliquez sur **Démarrer, Programmes, IBM WebSphere, Edge Server, IBM Network Dispatcher**, puis sur **Network Dispatcher**.

Pour pouvoir configurer le composant Dispatcher à partir de l'interface graphique, vous devez d'abord sélectionner **Dispatcher** dans l'arborescence. Vous pouvez lancer l'exécuteur et le gestionnaire une fois que vous vous êtes connecté à un hôte. Vous pouvez également créer des grappes contenant des ports et des serveurs, puis lancer des conseillers pour le gestionnaire.

Vous pouvez utiliser l'interface graphique pour toute opération normalement exécutée par la commande **ndcontrol**. Par exemple, pour définir une grappe à l'aide de la ligne de commande, vous devez entrer la commande **ndcontrol cluster add cluster**. Pour définir une grappe à partir de l'interface graphique, cliquez sur Exécuteur à l'aide du bouton droit de la souris, puis dans le menu en incrustation qui apparaît, cliquez sur le bouton **Ajout d'une grappe** à l'aide du bouton gauche de la souris. Entrez l'adresse de la grappe dans la fenêtre en incrustation, puis cliquez sur **OK**.

Les fichiers de configuration Dispatcher existants peuvent être chargés à l'aide des options **Chargement de la nouvelle configuration** (pour remplacer intégralement la configuration en cours) et **Ajout à la configuration en cours** (pour mettre à jour la configuration en cours) du menu en incrustation **Hôte**. Vous devez sauvegarder régulièrement votre configuration Dispatcher dans un fichier en utilisant l'option **Sauvegarder le fichier de configuration sous...** du menu en incrustation **Hôte**. Le menu **Fichier** situé en haut de l'interface graphique permet de sauvegarder les connexions à l'hôte en cours dans un fichier ou de restaurer les connexions dans des fichiers existants sur tous les composants Network Dispatcher.

Les commandes de configuration peuvent également être exécutées à distance. Pour plus de détails, reportez-vous à la section «Administration authentifiée à distance» à la page 213.

Vous pouvez accéder à l'**aide** en cliquant sur le point d'interrogation situé dans le coin supérieur droit de la fenêtre Network Dispatcher.

- **Aide sur les zones** — décrit les valeurs par défaut de chaque zone.
- **Procédures** — affiche la liste des tâches pouvant être effectuées dans cet écran.
- **Table des matières** — contient toutes les informations d'aide.
- **Index** — index alphabétique des rubriques d'aide.

Pour plus de détails sur l'utilisation de l'interface graphique, reportez-vous à la section «Instructions générales d'utilisation de l'interface graphique» à la page 6.

Assistant de configuration

Pour plus d'informations sur l'utilisation de l'assistant de configuration, reportez-vous à la section «Configuration à l'aide de l'assistant de configuration» à la page 4.

Configuration de la machine Dispatcher

L'installation de la machine Dispatcher ne peut être effectuée que par le superutilisateur (pour AIX, Linux ou Solaris) ou l'administrateur pour Windows 2000.

AIX, Linux et Solaris uniquement : Network Dispatcher peut avoir un serveur **co-implanté**. Ceci signifie simplement que Network Dispatcher peut être implanté physiquement sur le serveur dont il assure l'équilibrage de charge.

La machine Dispatcher requiert au moins deux adresses IP valides :

- Une adresse IP spécifiquement associée à la machine Dispatcher.

Cette adresse constitue l'adresse IP principale de la machine Dispatcher et est appelée l'adresse de non-réacheminement (NFA). Il s'agit par défaut de l'adresse renvoyée par la commande **hostname**. Utilisez cette adresse pour vous connecter à la machine en vue de tâches administratives, telles que la configuration à distance via Telnet ou l'accès au sous-agent SNMP. Si la machine Dispatcher peut déjà renvoyer des demandes vers d'autres machines du réseau (par la technique de la triangulation ping), il n'y rien de plus à faire pour définir l'adresse de non-réacheminement.

- Une adresse IP par grappe.

Une adresse de grappe est une adresse associée à un nom de système hôte (par exemple `www.société_X.com`). Cette adresse IP est utilisée par un client pour se connecter aux serveurs de la grappe en question. Dispatcher assure l'équilibrage de charge pour cette adresse.

Solaris uniquement :

1. Par défaut, Dispatcher est configuré pour assurer l'équilibrage de charge avec des cartes d'interface réseau Ethernet 100 Mo/s. Pour modifier le paramètre par défaut, vous devez éditer le fichier **/opt/nd/servers/ibmnd.conf** comme suit :

- La carte Ethernet 100 Mo/s par défaut est désignée dans le fichier `ibmnd.conf` par `hme`.
- Pour utiliser une carte Ethernet 10 Mo/s, remplacez `hme` par `le`.
- Pour utiliser une carte Ethernet 1 Go/s, remplacez `hme` par `ge`.
- Pour utiliser une carte multi-port, remplacez `hme` par `qfe`.
- Pour prendre en charge plusieurs types de cartes, dupliquez le fichier `ibmnd.conf`, puis modifiez chaque ligne en fonction du type de carte dont vous disposez.

Par exemple, pour utiliser deux cartes Ethernet 100 Mo/s, le fichier `ibmnd.conf` doit comporter une seule ligne indiquant l'unité `hme`. Pour utiliser une carte Ethernet 10 Mo/s, le fichier `ibmnd.conf` doit comporter deux lignes, l'une indiquant la carte `le` et l'autre la carte `hme`.

Le fichier **ibmnd.conf** fournit des données à la commande Solaris **autopush** et doit être compatible avec cette dernière.

2. Le démarrage ou l'arrêt de Dispatcher Executor déconfigure tous les alias sur les cartes répertoriées dans le fichier `ibmnd.conf`. Pour reconfigurer automatiquement les alias sur ces cartes (à l'exception de ceux devant être employés par le composant Dispatcher de Network Dispatcher), utilisez le fichier script **goAliases**. Un exemple de script se trouve dans le répertoire **...nd/servers/samples** et doit être déplacé dans le répertoire **...nd/servers/bin** pour son exécution. Le script `goAliases` s'exécute automatiquement lors du démarrage ou de l'arrêt de Dispatcher Executor. Par exemple, si les grappes X et Y sont configurées pour être utilisées par le composant Mailbox Locator sur les cartes répertoriées dans le fichier `ibmnd.conf`, elles sont déconfigurées lors du lancement des commandes **ndcontrol executor start** ou **ndcontrol executor stop**. Ce résultat n'est peut-être pas souhaité. Lorsque les grappes X et Y sont configurées dans le script `goAliases`, elles sont automatiquement reconfigurées une fois Dispatcher Executor lancé ou arrêté.

Windows 2000 uniquement : Assurez-vous que la transmission Internet n'est pas activée pour le protocole TCP/IP. (Voir la configuration TCP/IP sous Windows 2000.)

La figure 15 montre un exemple de Dispatcher configuré avec une seule grappe, deux ports et trois serveurs.

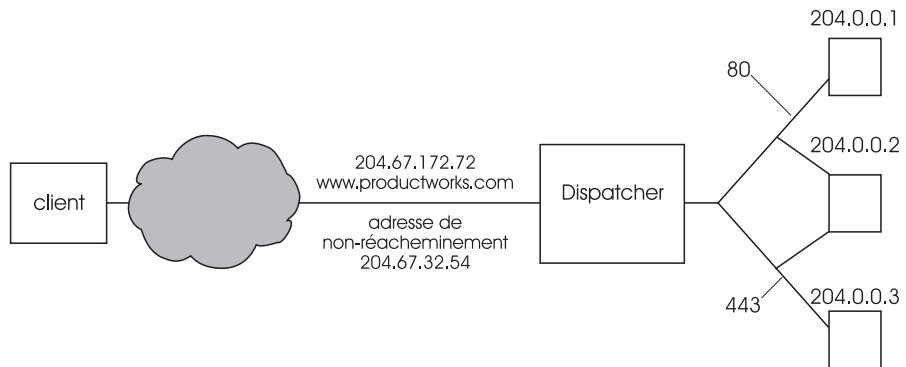


Figure 15. Exemple d'adresses IP nécessaires pour la machine Dispatcher

Pour obtenir une aide sur les commandes utilisées lors de cette procédure, reportez-vous à l'«Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Pour plus d'informations sur le fichier de configuration type, reportez-vous à la section «Exemples de fichiers de configuration Network Dispatcher» à la page 387.

Etape 1. Démarrage de la fonction serveur

AIX, Linux et Solaris : Pour lancer la fonction serveur, entrez **ndserver**.

Windows 2000 : La fonction serveur démarre automatiquement en tant que service.

Remarque : Un fichier de configuration par défaut (default.cfg) est chargé automatiquement pendant le démarrage de ndserver. Si l'utilisateur décide de sauvegarder la configuration Dispatcher dans default.cfg, toutes les données sauvegardées dans ce fichier seront chargées automatiquement au prochain démarrage de ndserver.

Etape 2. Démarrage de la fonction exécuteur

Pour lancer la fonction exécuteur, tapez la commande **ndcontrol executor start**. Notez que vous pouvez également modifier divers paramètres de l'exécuteur à cette occasion. Reportez-vous à l'«Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Etape 3. Définition de l'adresse de non-réacheminement (si différente du nom d'hôte)

Utilisez cette adresse pour vous connecter à la machine en vue de tâches administratives, comme l'utilisation de Telnet ou SMTP, par exemple. Par défaut, cette adresse correspond au nom d'hôte.

Pour définir l'adresse de non-réacheminement, entrez la commande **ndcontrol executor set nfa adresse_IP** ou éditez le fichier de configuration type. *adresse_IP* peut être le nom symbolique ou l'adresse en notation décimale à point.

Etape 4. Définition et configuration des options de la grappe

Dispatcher équilibrera les demandes envoyées à l'adresse de la grappe entre les serveurs configurés sur les ports associés à cette grappe.

La grappe est soit un nom symbolique, soit l'adresse en notation décimale à point, soit l'adresse spéciale 0.0.0.0 qui définit une grappe générique. Pour définir une grappe, tapez la commande **ndcontrol cluster add**. Pour définir les options de grappe, tapez la commande **ndcontrol cluster set** ou utilisez l'interface graphique pour lancer des commandes. Les grappes génériques peuvent être utilisées pour remplacer plusieurs adresses IP afin de permettre l'équilibrage de charge pour les paquets entrants. Pour plus de détails, reportez-vous aux sections «Utilisation d'une grappe générique pour combiner les configurations serveurs» à la page 193, «Utilisation de la grappe générique pour équilibrer la charge des pare-feux» à la page 193 et «Utilisation de grappe générique avec Caching Proxy pour le proxy transparent» à la page 194.

Etape 5. Affectation d'un alias à la carte d'interface réseau

Une fois que la grappe est définie, vous devez normalement configurer son adresse sur l'une des cartes d'interface réseau de la machine Dispatcher. Pour ce faire, lancez la commande **ndcontrol cluster configure adresse_grappe**. Cette commande recherche une carte avec une adresse existante et appartenant au même sous-réseau que l'adresse de la grappe. La commande de configuration de la carte système est ensuite lancée pour l'adresse de la grappe en utilisant la carte trouvée et le masque de réseau de l'adresse existante figurant sur cette carte. Par exemple :

```
ndcontrol cluster configure 204.67.172.72
```

Vous pouvez configurer des adresses de grappes ajoutées à un serveur en attente en mode haute disponibilité ou des adresses de grappes ajoutées à un répartiteur de réseau étendu jouant le rôle de serveur éloigné. Il est également inutile d'exécuter la commande de configuration de la grappe si vous utilisez le modèle de script **goldle**, en mode autonome script. Pour plus d'informations sur le script goldle, reportez-vous à la section «Utilisation de scripts» à la page 178.

Dans de rares cas, vous pouvez avoir une adresse qui ne correspond pas à une adresse de sous-réseau existante. Vous devez alors utiliser l'autre forme de la commande de configuration de grappe et fournir de manière explicite le nom et le masque de réseau de l'interface. Entrez la commande **ndcontrol cluster configure** *adresse_grappe nom_interface sous-masque*.

Exemple :

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

Windows 2000

Pour vous servir de l'autre forme de la commande de configuration de grappe sous Windows 2000, vous devez déterminer le nom de l'interface à utiliser.

Si votre machine comporte une seule carte Ethernet, l'interface portera le nom en0. De même, si vous ne disposez que d'une seule carte en anneau à jeton, l'interface portera le nom tr0. Si la machine comporte plusieurs cartes de l'un ou l'autre type, il est nécessaire de déterminer le mappage des cartes.

Procédez comme suit :

1. Lancez **regedit** à partir de l'invite.
2. Cliquez sur **HKEY_LOCAL_MACHINE\Logiciel, Microsoft, Windows NT**, puis sur **Version actuelle**.
3. Cliquez ensuite sur **Cartes réseau**

Les cartes d'interface réseau supportées apparaissent à l'écran. Cliquez sur chaque entrée de la liste pour déterminer s'il s'agit d'une interface Ethernet ou Token Ring (anneau à jeton). Le type d'interface est répertorié dans la colonne *Description*. Les noms attribués par **ndconfig** correspondent aux types d'interface. Par exemple, la commande ndconfig affecte la première interface Ethernet de la liste à en0, la deuxième à en1, et ainsi de suite ; la première interface Token Ring est affectée à tr0, la deuxième à tr1, et ainsi de suite.

Remarque : Le registre Windows 2000 commence la numérotation des cartes à partir de **1**, et non de **0**.

Après avoir accédé à ces informations de mappage, vous pouvez créer un alias reliant l'interface réseau à l'adresse de la grappe.

Utilisation de ifconfig/ndconfig pour configurer des alias de grappe

La commande de configuration de grappe exécute principalement ifconfig (ou ndconfig sous Windows 2000). Vous pouvez donc continuer d'utiliser les commandes ifconfig (ndconfig) si vous le souhaitez.

Windows 2000 : La commande ndconfig est fournie avec le composant Dispatcher et permet de configurer les alias de grappes à partir de la ligne de commande. Cette commande a la même syntaxe que la commande UNIX ifconfig.

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

Remarque : Le paramètre netmask est obligatoire. Il doit être spécifié en notation décimale à point (255.255.0.0) ou en notation hexadécimale (0xffff0000).

Pour déterminer le nom de l'interface, utilisez la même technique que pour la seconde forme de la commande de configuration de grappe.

Solaris : Lorsque vous utilisez des applications serveur de liaison, qui opèrent une liaison à une liste d'adresses IP ne contenant pas celle du serveur, faites appel à la commande **arp publish** plutôt qu'à ifconfig pour définir dynamiquement une adresse IP sur la machine Network Dispatcher. Par exemple :

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

Etape 6. Définition des ports et de leurs options

Pour définir un port, entrez la commande **ndcontrol port add grappe:port**, éditez le fichier de configuration type ou utilisez l'interface graphique. La valeur de *grappe* peut être le nom symbolique ou l'adresse en notation décimale à point. *Port* représente le numéro du port utilisé pour ce protocole. A ce stade, vous avez également la possibilité de modifier divers paramètres de ports. Vous devez définir et configurer tous les serveurs pour un port. Reportez-vous à l'«Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Le numéro de port 0 (zéro) est utilisé pour spécifier un port générique. Ce port acceptera le trafic vers un port non défini sur la grappe. Le port générique sera utilisé pour configurer des règles et des serveurs pour n'importe quel port. Vous pouvez également utiliser cette fonction en cas de

configuration serveur/règle identique pour plusieurs ports. Le trafic sur un port peut influencer les décisions d'équilibrage de charge pour le trafic sur les autres ports. Pour plus de détails sur les cas d'utilisation d'un port générique, reportez-vous à la section «Utilisation du port générique pour acheminer le trafic destiné à un port non configuré» à la page 195.

Remarque : Le port générique ne peut pas être utilisé pour le traitement du trafic FTP.

Etape 7. Définition de serveurs avec équilibrage de charge

Pour définir un serveur avec équilibrage de charge, tapez la commande **ndcontrol server add** *grappe:port:serveur*, éditez le fichier de configuration type ou utilisez l'interface graphique. *grappe* et *serveur* peuvent correspondre à des noms symboliques ou à des adresses en notation décimale à point. *Port* représente le numéro du port utilisé pour ce protocole. Pour effectuer l'équilibrage de charge, vous devez définir plusieurs serveurs sur le port d'une grappe.

Serveurs de liaison : Si le composant Dispatcher équilibre la charge entre des serveurs de liaison, les serveurs *doivent* être configurés pour effectuer la liaison avec l'adresse de la grappe. Etant donné que Dispatcher réachemine les paquets sans modifier l'adresse IP de destination, lorsque ceux-ci arrivent, l'adresse de grappe qu'ils contiennent indique la destination. Si un serveur a été configuré pour être lié à une adresse IP autre que l'adresse de grappe, il ne pourra pas accepter les paquets/demandes destinés à la grappe.

Remarque : Solaris et Linux : les serveurs de liaison ne doivent pas être co-implantés.

Co-implantation d'adresses multiples : Dans une configuration de co-implantation, l'adresse du serveur co-implanté ne doit *pas* être la même que celle de non-réacheminement (NFA). Vous avez la possibilité d'utiliser une autre adresse si votre machine a été définie avec des adresses IP multiples. En ce qui concerne le composant Dispatcher, le serveur co-implanté doit être défini comme **co-implanté** via la commande **ndcontrol server**. Pour plus d'informations sur les serveurs co-implantés, reportez-vous à la section «Utilisation de serveurs implantés au même endroit» à la page 162.

Pour plus d'informations sur la syntaxe de la commande **ndcontrol server**, reportez-vous à la section «**ndcontrol server** — Configuration des serveurs» à la page 311.

Etape 8. Lancement de la fonction gestionnaire (facultatif)

La fonction gestionnaire permet d'améliorer l'équilibrage de charge. Pour lancer le gestionnaire, entrez la commande **ndcontrol manager start**, éditez le fichier de configuration type ou utilisez l'interface graphique.

Etape 9. Lancement de la fonction conseiller (facultatif)

Les conseillers transmettent au gestionnaire des informations complémentaires sur la capacité des serveur bénéficiant de l'équilibrage de charge à répondre aux demandes. Chaque conseiller est spécifique à un protocole. Par exemple, tapez la commande suivante pour lancer le conseiller HTTP :

```
cbrcontrol advisor start http port
```

Pour consulter la liste des conseillers et des ports par défaut correspondants, reportez-vous à l'«Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257. Pour lire la description de chaque conseiller, reportez-vous à la section «Liste des conseillers» à la page 149.

Etape 10. Définition du niveau d'importance des informations requis pour la grappe

Si vous lancez des conseillers, vous pouvez modifier le niveau d'importance donné aux informations des conseillers entrant dans les décisions d'équilibrage de la charge. Pour définir le niveau d'importance des informations pour la grappe, lancez la commande **ndcontrol cluster set grappe niveau_importance_informations**. Pour plus d'informations, voir «Proportion de l'importance accordée aux données d'état» à la page 141.

Configuration des serveurs pour l'équilibrage de la charge

Si le serveur est co-implanté (Dispatcher est installé sur la machine dont il assure l'équilibrage de charge) ou si vous utilisez les méthodes de réacheminement nat ou cbr, *n'appliquez pas* les procédures suivantes.

Si vous utilisez la méthode de réacheminement mac, Dispatcher travaillera uniquement avec des serveurs périphériques permettant de configurer l'adaptateur de bouclage avec une adresse IP supplémentaire. C'est pourquoi le serveur périphérique ne répondra jamais aux demandes ARP (protocole de résolution d'adresses). Suivez les étapes indiquées dans cette section pour configurer les serveurs avec équilibrage de charge.

Etape 1. Affectation d'un alias pour l'unité de bouclage

Pour que les serveurs bénéficiant d'un équilibrage de charge fonctionnent, vous devez définir (ou de préférence affecter un alias à) l'unité de bouclage (souvent appelé lo0) en fonction de l'adresse de grappe. Si vous utilisez la méthode d'acheminement MAC, le composant Dispatcher ne modifie pas l'adresse IP de destination dans le paquet TCP/IP avant de retransmettre ce paquet au serveur TCP. Si l'unité de bouclage est définie, ou se voit affecter l'adresse de grappe comme alias, les serveurs avec équilibrage de charge accepteront les paquets envoyés à cette adresse de grappe.

Si votre système d'exploitation supporte l'attribution d'alias aux interfaces réseau (telles que AIX, Linux, Solaris, ou Windows 2000), vous devez affecter l'adresse de grappe comme alias à l'unité de bouclage. L'utilisation d'un système d'exploitation supportant les alias à pour avantage de permettre la configuration de serveurs avec équilibrage de charge desservant plusieurs adresses de grappe .

Remarque : Certaines versions de noyau **Linux** requièrent un correctif pour l'affectation d'un alias au dispositif de bouclage. Pour déterminer si un correctif de noyau Linux est nécessaire, reportez-vous à la section «Installation du correctif du noyau Linux (pour supprimer les réponses ARP sur l'interface de bouclage)» à la page 72.

Pour les noyaux **Linux** version 2.2.14 ou suivante, lancez les commandes ci-après avant la commande **ifconfig** :

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

Si le système d'exploitation de votre serveur, tel que HP-UX et OS/2, ne supporte pas les alias, vous devez définir l'adresse de grappe comme alias pour l'unité de bouclage.

Pour définir l'unité de bouclage ou lui affecter un alias, utilisez la commande requise par votre système d'exploitation comme indiqué dans le tableau 4.

Tableau 4. Commandes pour l'affectation d'un alias à l'unité de bouclage (lo0) pour Dispatcher

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

Tableau 4. Commandes pour l'affectation d'un alias à l'unité de bouclage (lo0) pour Dispatcher (suite)

Windows 2000	<ol style="list-style-type: none"> 1. Sélectionnez Démarrer, Paramètres, puis Panneau de configuration. 2. Si vous ne l'avez pas encore fait, ajoutez le pilote de la carte de bouclage MS. <ol style="list-style-type: none"> a. Cliquez deux fois sur Ajout/Suppression de matériel. Cela lance l'assistant correspondant à cette fonction. b. Cliquez sur Suivant, sélectionnez Ajouter/Dépanner un périphérique, puis sur Suivant. c. Le panneau Sélection d'un périphérique matériel s'affiche. d. Si la carte de bouclage MS figure dans la liste, c'est qu'elle est déjà installée. Cliquez sur Annuler pour fermer le panneau. e. Si la carte de bouclage MS <i>ne figure pas</i> dans la liste, sélectionnez Ajouter un nouveau périphérique et cliquez sur Suivant. f. Pour sélectionner le composant matériel dans une liste, dans le panneau Trouver le nouveau matériel, cliquez sur Non, puis sur Suivant. g. Sélectionnez Cartes réseau et cliquez sur suivant. h. Dans le panneau de sélection des cartes réseau, sélectionnez Microsoft dans la liste des fabricants, puis Microsoft Loopback Adapter. i. Cliquez sur Suivant une première fois, puis une deuxième pour installer les paramètres par défaut (ou sélectionnez l'option de support fourni (Have Disk), puis insérez le CD-ROM et effectuez l'installation à partir de ce point). j. Cliquez sur Terminer pour achever l'installation. 3. Dans le Panneau de configuration, cliquez deux fois sur Connexions réseau et accès à distance. 4. Cliquez avec le bouton droit de la souris sur la connexion portant le nom d'unité "Microsoft Loopback Adapter" pour la sélectionner. 5. Sélectionnez Propriétés dans le menu déroulant. 6. Sélectionnez Internet Protocol (TCP/IP), puis cliquez sur Propriétés. 7. Cliquez sur Utiliser l'adresse IP suivante. Pour <i>Adresse IP</i> indiquez l'adresse de la grappe et pour <i>Masque de sous-réseau</i> le masque de sous réseau par défaut (255.0.0.0). Remarque : N'indiquez pas d'adresse de routeur. Utilisez le système hôte local comme serveur DNS par défaut.
--------------	--

Tableau 4. Commandes pour l'affectation d'un alias à l'unité de bouclage (lo0) pour Dispatcher (suite)

OS/390	<p>Configuration d'un alias de bouclage sur le système OS/390</p> <ul style="list-style-type: none"> L'administrateur doit créer une entrée dans la liste d'adresses d'origine du membre (fichier) de paramètres IP. Par exemple <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"> Plusieurs adresses peuvent être définies pour le bouclage. L'adresse 127.0.0.1 est configurée par défaut.
--------	---

Etape 2. Vérification de l'existence d'une route supplémentaire

Sur certains systèmes d'exploitation, il se peut qu'une route par défaut ait été créée. Dans ce cas, elle doit être supprimée.

- Pour vérifier l'existence d'une route supplémentaire sur Windows 2000, utilisez la commande suivante :

```
route print
```

- Pour vérifier l'existence d'une route supplémentaire sur tous les systèmes UNIX, utilisez la commande suivante :

```
netstat -nr
```

Exemple pour Windows 2000 :

- Une fois la commande **route print** soumise, un tableau semblable à celui-ci s'affiche. (Cet exemple illustre la recherche et la suppression d'une route supplémentaire vers la grappe 9.67.133.158, avec le masque de sous-réseau par défaut 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

- L'adresse de la grappe figure dans la colonne de l'adresse de passerelle. Si une route supplémentaire existe, l'adresse de la grappe apparaîtra deux fois. Dans l'exemple, l'adresse de la grappe (9.67.133.158) apparaît sur les lignes 2 et 8.

3. L'adresse du réseau figure sur toutes les lignes où apparaît l'adresse de la grappe. Vous avez uniquement besoin de l'une de ces routes. La route en trop doit être supprimée. La route supplémentaire à supprimer est celle dont l'adresse de réseau commence par le premier chiffre de l'adresse de la grappe, suivi de trois zéros. Dans l'exemple, la route supplémentaire à supprimer est celle qui se trouve sur la ligne 2, avec l'adresse de réseau **9.0.0.0** :

```
9.0.0.0      255.0.0.0    9.67.133.158  9.67.133.158    1
```

Etape 3. Suppression d'une route supplémentaire

Vous devez supprimer la route supplémentaire. Pour cela, utilisez la commande correspondant à votre système d'exploitation fournie dans le tableau 5.

Exemple : Pour supprimer la route supplémentaire comme indiqué pour l'exemple "Routes actives" de l'étape 2, entrez :

```
route delete 9.0.0.0 9.67.133.158
```

Tableau 5. Commandes de suppression d'une route supplémentaire pour Dispatcher

HP-UX	route delete <i>adresse_grappe</i> <i>adresse_grappe</i>
Windows 2000	route delete <i>adresse_reseau</i> (dans une invite MS-DOS) Remarque : Vous devez supprimer la route supplémentaire chaque fois que vous réamorcez le serveur.

Suivant l'exemple fourni dans la figure 15 à la page 62, pour configurer un serveur exécutant AIX, la commande serait :

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

Etape 4. Vérification de la configuration du serveur

Pour vérifier la configuration d'un serveur périphérique, effectuez les étapes suivantes à partir d'une autre machine du même sous-réseau lorsque Network Dispatcher n'est pas être en cours d'exécution et la *grappe* non configurée.

1. Lancez la commande :

```
arp -d grappe
```

2. Lancez la commande :

```
ping grappe
```

La commande ping doit rester sans réponse. Si une réponse est renvoyée, assurez-vous que vous n'avez pas attribué l'adresse de la grappe à l'interface à l'aide de la commande ifconfig. Vérifiez qu'aucune machine n'a une entrée ARP publiée pour l'adresse de la grappe.

Remarque : Pour les versions 2.2.12 et 2.2.13 du noyau **Linux**, vérifiez que "1" est contenu dans
`/proc/sys/net/ipv4/conf/lo/arp_invisible`.

Pour les versions 2.2.14 et suivantes du noyau **Linux**, vérifiez que "1" est contenu dans
`/proc/sys/net/ipv4/conf/lo/hidden` et
`/proc/sys/net/ipv4/conf/all/hidden`.

3. Soumettez une commande ping pour le serveur périphérique, puis lancez immédiatement la commande suivante :

```
arp -a
```

La sortie de la commande doit contenir l'adresse MAC de votre serveur. Lancez la commande :

```
arp -s grappe adresse_mac_serveur
```

4. Soumettez une commande ping pour la grappe. Cette commande doit renvoyer une réponse. Soumettez une demande http, telnet ou d'un autre type, adressée à la grappe que vous voulez voir gérée par votre serveur périphérique. Vérifiez qu'elle fonctionne correctement.
5. Lancez la commande :

```
arp -d grappe
```
6. Soumettez une commande ping pour la grappe. Cette commande doit rester sans réponse.

Remarque : Si une réponse est renvoyée, lancez une instruction **arp grappe** pour obtenir l'adresse MAC de la machine incorrectement configurée. Répétez les étapes 1 à 6.

Installation du correctif du noyau Linux (pour supprimer les réponses ARP sur l'interface de bouclage)

Pour les serveurs Linux exclusivement, un correctif spécifique (dépendant de la version du noyau Linux concernée) est requis pour permettre l'affectation d'un alias à l'unité de bouclage.

Le correctif permet de s'assurer que les réponses ARP (Address Resolution Protocol) ne sont envoyées qu'à partir d'un port de carte réseau dont l'adresse IP est demandée dans la requête ARP. Sans ce correctif, Linux émet les réponses ARP sur le réseau pour les alias du dispositif de bouclage. Le correctif corrige également les conditions d'indétermination ARP qui se produisent lorsque plusieurs ports de carte réseau associés à des adresses IP différentes se trouvent sur le même réseau physique.

Les conditions d'installation du correctif sont décrites ci-après.

- **Versions 2.4.x du noyau Linux**

- Si vous utilisez la méthode d'acheminement MAC de Dispatcher avec un haut niveau de disponibilité et une co-implantation, vous devez installer le correctif sur le dispositif Dispatcher.

Remarque : Dispatcher peut être considéré comme étant co-implanté même s'il ne sert qu'à équilibrer la charge d'un autre composant Edge Server (par exemple, Caching Proxy, Mailbox Locator, CBR) sur l'ordinateur sur lequel il réside.

- Vous devez installer le correctif sur un serveur dorsal qui utilise le noyau 2.4 et dont l'équilibrage de charge est assuré par Dispatcher configuré pour la méthode d'acheminement MAC.
- Vous devez installer le correctif sur un ordinateur qui comporte plusieurs ports de carte réseau sur le même réseau physique.

- **Versions 2.2.12 et 2.2.13 du noyau Linux**

Si vous utilisez le noyau 2.2.12 ou 2.2.13 sur un serveur périphérique.

Remarques :

1. Network Dispatcher ne s'exécute pas sur la version 2.2 du noyau.
2. Le correctif est incorporé au noyau 2.2.14.
3. Le correctif de noyau Linux a été utilisé pour tester le produit IBM et s'est révélé tout à fait satisfaisant dans l'environnement de test IBM. Nous vous conseillons d'évaluer l'adéquation de ce code dans votre propre environnement afin de voir s'il correspond à vos besoins. Il ne sera pas systématiquement inclus dans les versions futures du code source Linux de base.

Versions 2.4.x du noyau Linux

Le correctif du noyau n'est pas requis pour toutes les configurations. Vous devez installer un correctif pour les versions 2.4.x du noyau Linux dans les cas suivants :

- Si vous utilisez la méthode d'acheminement MAC de Dispatcher avec un haut niveau de disponibilité et une co-implantation, vous devez installer le correctif sur le dispositif Dispatcher.

Remarque : Dispatcher peut être considéré comme étant co-implanté même s'il ne sert qu'à équilibrer la charge d'un autre composant Edge Server (par exemple, Caching Proxy, Mailbox Locator, CBR) sur l'ordinateur sur lequel il réside.

- Vous devez installer le correctif sur un serveur dorsal qui utilise le noyau 2.4 et dont l'équilibrage de charge est assuré par Dispatcher configuré pour la méthode d'acheminement MAC.

- Vous devez installer le correctif sur un ordinateur qui comporte plusieurs ports de carte réseau sur le même réseau physique.

Vous pouvez télécharger ce correctif à partir du site :

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

Sélectionnez CVS Tree dans la liste Download.

Pour appliquer le correctif :

1. Procurez-vous le correctif de bouclage à partir du site suivant :
<http://oss.software.ibm.com/developerworks/opensource/cvs/naslib>
2. Installez les RPM du noyau
 - a. Copiez le fichier du correctif **arp.c.2.4.0.patch** dans le répertoire `/usr/src/linux-2.4/net/ipv4/`.
 - b. Lancez les commandes suivantes :


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

Remarque : Cette installation a été testée avec les versions 2.4.0 et 2.4.2 du noyau Linux.
3. Placez-vous dans le répertoire `/usr/src/linux-2.4`.
4. Editez le fichier Makefile et ajoutez **-arppatch** à la valeur EXTRAVERSION.
5. Lancez la commande : `make mrproper`
6. Lancez la commande : `make config`. Ensuite, sélectionnez les valeurs appropriées pour votre système. Assurez-vous que vous configurez le module de support.
7. Lancez les commandes suivantes :


```
make dep;make clean;make bzImage;make modules;make modules_install
cd arch/i386/boot
cat bzImage > /boot/vmlinuz-2.4.2-2-arppatch
cd /usr/src/linux-2.4
cp System.map /boot/System.map-2.4.2-2-arppatch
cd /etc
```
8. Editez le fichier `lilo.conf` et copiez le paragraphe **image=**. Dans la nouvelle copie, remplacez :
 - `/boot/vmlinuz-2.4.2-2` par `/boot/vmlinuz-2.4.2-2-arppatch`
 - `label=linux` par `label=linux-arppatch`
 - `default=linux` par `default=linux-arppatch`
9. Exécutez la commande `/sbin/lilo`.
10. Réamorcer à partir du nouveau noyau.

Versions 2.2.12 et 2.2.13 du noyau Linux

Un correctif des versions 2.2.12 et 2.2.13 du noyau Linux doit être installé sur tout serveur utilisant la méthode d'acheminement MAC. Vous pouvez télécharger ce correctif à partir du site suivant : <http://www.ibm.com/developer/linux>.

Pour appliquer le correctif :

1. Procurez-vous le correctif de bouclage à partir du site <http://www.ibm.com/developer/linux>.
2. Installez le code source du noyau. Pour les instructions d'installation, reportez-vous au fichier **README.kernel-sources** dans le répertoire `/usr/src/linux`.
3. Appliquez le correctif en lançant la commande `patch` à partir du répertoire `/usr/src`. Par exemple :

```
patch -p0 < fichier_correctif
```
4. Compilez le noyau. Pour les instructions de compilation, reportez-vous au fichier **README** dans le répertoire `/usr/src/linux-2.4/`.
5. Installez le nouveau noyau et exécutez la commande **lilo**. Pour connaître les instructions, reportez-vous au fichier **README** dans le répertoire `/usr/src/linux`.
6. Réamorcez à partir du nouveau noyau.
7. Vérifiez le fichier suivant : `/proc/sys/net/ipv4/conf/lo/arp_invisible`. Si ce fichier est présent, l'application du correctif du noyau a réussi. Si le fichier *n'est pas* présent, cela signifie que l'application du correctif a échoué ou que l'amorçage a été effectué à partir d'un noyau auquel le correctif n'a pas été appliqué. Consultez le fichier `/usr/src/linux/README` pour vous assurer que toutes les étapes d'installation ont été respectées.
8. Lancez la commande :

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

Cette commande restera active jusqu'au réamorçage de la machine. Une fois la machine réamorcée, vous devrez répéter ces étapes et les étapes ultérieures.
9. Affectez le masque de réseau 255.255.255.255 comme alias pour le bouclage, par exemple :

```
ifconfig lo:1 cluster netmask 255.255.255.255 up
```
10. Ajoutez le serveur à la grappe.

Chapitre 6. Planification du composant CBR (Content Based Routing)

Le présent chapitre décrit les aspects que l'administrateur réseau doit prendre en compte avant d'installer et de configurer le composant CBR avec Caching Proxy.

- Reportez-vous à la section «Chapitre 7. Configuration du composant CBR» à la page 83 pour obtenir des informations sur la configuration des paramètres d'équilibrage de charge du composant CBR.
- Pour obtenir des informations sur la configuration de Network Dispatcher pour les fonctions avancées, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Le présent chapitre se compose des sections suivantes :

- «Matériel et logiciels requis»
- «Remarques relatives à la planification»

Matériel et logiciels requis

Conditions requises par la plate-forme :

- Pour AIX, reportez-vous à la section «Configuration requise pour AIX» à la page 12
- Pour Linux, reportez-vous à la section «Configuration requise pour Red Hat Linux ou SuSE Linux» à la page 17
- Pour Solaris, reportez-vous à la section «Configuration requise pour Solaris» à la page 20
- Pour Windows 2000, reportez-vous à la section «Configuration requise pour Windows 2000» à la page 22

Remarques relatives à la planification

Le composant CBR permet d'équilibrer la charge du trafic HTTP et SSL à l'aide de Caching Proxy qui permet de transmettre la requête par un serveur proxy.

Remarque : Pour exécuter CBR en tant que module d'extension, installez le mode proxy inverse de Caching Proxy.

La structure de CBR ressemble beaucoup à celle de Dispatcher. CBR comprend les fonctions suivantes :

- **cbrserver** traite les demandes à partir de la ligne de commande adressées à l'exécuteur, au gestionnaire et aux conseillers.
- L'**exécuteur** prend en charge l'équilibrage de charge des demandes client. Vous devez démarrer l'exécuteur pour pouvoir utiliser le composant CBR.
- Le **gestionnaire** définit les mesures utilisées par l'exécuteur en fonction de plusieurs facteurs :
 - décomptes internes de l'exécuteur,
 - retour d'informations sur les serveurs fourni par les conseillers,
 - retour d'informations émanant d'un programme de contrôle système, tel que Metric Server.

L'utilisation du gestionnaire n'est que facultative. Toutefois, s'il n'est pas utilisé, l'équilibrage de charge se fera sur la base d'une planification circulaire pondérée, elle-même basée sur les mesures de charge des serveurs et les conseillers ne seront pas disponibles.

- Les **conseillers** interrogent les serveurs puis analysent les résultats par protocole avant de demander au gestionnaire de régler les capacités comme il convient. L'utilisation de certains de ces conseillers n'est peut-être pas utile dans une configuration typique. Vous avez également la possibilité de développer vos propres conseillers. L'utilisation des conseillers est facultative mais recommandée. Network Dispatcher fournit un conseiller Caching Proxy (ibmproxy). Pour de plus amples informations, reportez-vous à «Conseillers» à la page 146.
- Pour configurer et gérer l'exécuteur, les conseillers et le gestionnaire, utilisez la ligne de commande (**cbrcontrol**) ou l'interface utilisateur graphique (**ndadmin**).

Les trois fonctions clés de CBR (l'exécuteur, le gestionnaire et les conseillers) agissent en collaboration pour équilibrer et répartir entre les serveurs les requêtes réceptionnées. Outre la gestion des requêtes d'équilibrage de charge, l'exécuteur contrôle le nombre de nouvelles connexions et de connexions actives, et transmet ces informations au gestionnaire.

CBR vous permet de spécifier un groupe de serveurs devant prendre en charge une requête en fonction de son contenu. Le composant CBR vous permet de compartimenter votre site en plusieurs parties afin que chaque partie puisse être traitée par des groupes de serveurs différents. Cette répartition sera transparente pour les clients qui accéderont au site. CBR vous permet d'indiquer plusieurs serveurs pour chaque type de requête.

Par conséquent, les requêtes peuvent être équilibrées pour obtenir une réponse optimale du client. L'affectation de plusieurs serveurs à chaque partie de votre site vous permet de vous protéger en cas de défaillance d'un poste de travail ou d'un serveur. CBR reconnaîtra la défaillance et continuera d'équilibrer la charge des requêtes client aux autres serveurs du groupe.

Vous pouvez répartir votre site en affectant à certains serveurs le traitement de requêtes cgi uniquement, et en affectant à un autre groupe de serveurs le traitement de toutes les autres requêtes. Ceci mettrait fin au ralentissement de l'activité des serveurs dû au calcul d'énormes scripts cgi au cours d'un trafic html normal, et permettrait ainsi aux clients d'obtenir de meilleurs temps de réponse. Avec cette méthode, vous pouvez également utiliser des postes de travail plus puissants pour des requêtes normales. Ainsi, les clients obtiendraient un meilleur temps de réponse sans pour autant occasionner des frais de mise à niveau de tous vos serveurs. Vous pouvez également affecter des postes de travail plus puissants pour des requêtes cgi.

Vous pouvez également partitionner votre site en dirigeant vers un groupe de serveurs les clients qui accèdent à des pages nécessitant une opération d'enregistrement, et en acheminant toutes les autres requêtes vers un deuxième groupe de serveurs. Ainsi, les navigateurs occasionnels qui accèdent à votre site n'accapareront plus les ressources qui pourraient être utilisées par des clients devant effectuer des opérations d'enregistrement sur votre site. Cela vous permettrait également d'utiliser des postes de travail plus puissants pour traiter les clients qui se sont enregistrés.

Il est possible de combiner les deux pour plus de souplesse et pour un meilleur service.

Caching Proxy communique avec CBR via son interface de plug-in. Caching Proxy, doit être installé sur la même machine. Désormais, plusieurs instances de Caching Proxy exécutée sur la même machine peuvent communiquer avec CBR simultanément. Dans les versions précédentes, seule une instance de Caching Proxy pouvait communiquer avec CBR.

CBR et Caching Proxy examinent les requêtes HTTP à l'aide destypes de règle indiqués. Pendant l'exécution, Caching Proxy accepte les demandes client et interroge le composant CBR pour savoir quel est le meilleur serveur. Lorsqu'il reçoit cette demande, CBR la compare à un ensemble de règles prioritaires. Dès qu'il en trouve une qui correspond, un serveur approprié est sélectionné dans un groupe de serveurs préconfigurés. Enfin, CBR indique à Caching Proxy le serveur sélectionné, et les demandes sont transmises à ce dernier.

Une fois que vous avez défini une grappe pour la répartition de charge, assurez-vous que toutes les requêtes envoyées à cette grappe ont une règle qui choisira un serveur. Si aucune règle correspondant à une requête spécifique n'est trouvée, Caching Proxy enverra une page d'erreur au client. Le moyen le plus aisé de s'assurer que toutes les demandes correspondront à une règle est de créer une règle toujours vraie avec un niveau de priorité élevé. Assurez-vous que les serveurs auxquels se réfère cette règle peuvent traiter toutes les demandes non gérées explicitement par les règles ayant des niveaux de priorité moins élevés. (Remarque : Les règles de priorité inférieure sont évaluées en premier.)

Équilibrage de charge sur les connexions sécurisées (SSL)

CBR et Caching Proxy peuvent recevoir une transmission SSL d'un client vers le proxy (côté client-serveur) ainsi que prendre en charge une transmission d'un proxy vers un serveur SSL (côté proxy-serveur). Si vous définissez un port SSL sur un serveur dans la configuration CBR pour qu'il reçoive la demande SSL provenant d'un client, vous pouvez gérer un site complètement sécurisé, en utilisant CBR pour équilibrer la charge entre les serveurs sécurisés SSL.

Vous devez insérer une instruction de configuration dans le fichier `ibmproxy.conf` pour que IBM Caching Proxy active le chiffrement SSL du proxy vers le serveur. Le format est le suivant :

```
proxy uri_structure  
url_structure adresse
```

où *uri_structure* correspond à la structure à respecter (par exemple : `/secure/`), *url_structure* à un URL de remplacement (par exemple : `https://clusterA/secure/`) et *adresse* à l'adresse de la grappe (par exemple : `clusterA`).

Équilibrage de charge client-proxy dans SSL et proxy-serveur dans HTTP

CBR et Caching Proxy peuvent également recevoir une transmission SSL d'un client et déchiffrer la demande SSL avant d'acheminer la demande par proxy à un serveur HTTP. Pour que CBR prenne en charge la transmission client-proxy pour SSL et proxy-client pour HTTP, utilisez le mot clé facultatif **mapport** dans la commande `cbrcontrol server`. Il permet d'indiquer si le port du serveur est différent du port d'entrée du client. Voici un exemple d'ajout de port avec le mot clé `mapport`, dans lequel le port du client est 443 (SSL) et le port du serveur est 80 (HTTP) :

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

Le numéro de port de `mapport` peut correspondre à n'importe quel entier positif. La valeur par défaut correspond au numéro de port entrant du client.

Etant donné que CBR doit être capable de traiter une demande HTTP pour un serveur configuré sur le port 443 (SSL), un conseil spécial *ssl2http* est fourni. Il démarre sur le port 443 (le port entrant du client) et opère sur le ou les serveurs configurés pour ce port. Si deux grappes sont configurées et que pour chacune d'entre elles, le port 443 et les serveurs sont configurés avec un paramètre mapport différent, une seule instance du conseiller peut ouvrir le port approprié. Voici un exemple de cette configuration :

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

Chapitre 7. Configuration du composant CBR

Avant d'effectuer les opérations décrites dans le présent chapitre, reportez-vous à la section «Chapitre 6. Planification du composant CBR (Content Based Routing)» à la page 77. Ce chapitre décrit comment créer une configuration de base pour le composant CBR de Network Dispatcher.

- Pour de plus amples informations sur Network Dispatcher, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Présentation générale des tâches de configuration

Remarque : Avant de suivre les étapes de configuration détaillées dans ce tableau, assurez-vous que le poste CBR et tous les postes serveurs sont connectés au réseau, que leurs adresses IP sont valides et qu'ils peuvent communiquer entre eux par ping.

Tableau 6. Tâches de configuration pour le composant CBR

Tâche	Description	Informations connexes
Configurer le poste CBR	Conditions requises	«Configuration du poste CBR» à la page 88
Configurer des machines en vue de l'équilibrage de charge	Définition de la configuration de l'équilibrage de charge.	«Etape 7. Définition des serveurs avec équilibrage de charge» à la page 93

Méthodes de configuration

Il existe quatre méthodes pour créer une configuration de base du composant CBR de Network Dispatcher :

- Ligne de commande
- Scripts
- Interface graphique
- Assistant de configuration

Pour utiliser le composant CBR, Caching Proxy doit être installé.

Remarque : Caching Proxy est un service qui, par défaut, démarre automatiquement après l'installation. Vous devez l'arrêter avant de lancer la fonction serveur CBR (cbrserver). Nous vous recommandons de modifier le service Caching Proxy pour le démarrer manuellement et non automatiquement.

- AIX, Linux et Solaris : pour arrêter Caching Proxy, recherchez l'identificateur de processus correspondant à l'aide de la commande `ps -ef|grep ibmproxy`, puis mettez fin à ce processus à l'aide de la commande `kill ID_processus`.
- Windows : arrêtez Caching Proxy à partir du panneau Services.

Ligne de commande

C'est la méthode de configuration de CBR la plus directe. Les valeurs des paramètres de commandes doivent être saisies à l'aide de caractères anglais. Les seules exceptions s'appliquent aux noms d'hôte (utilisés dans les commandes cluster et server) et aux noms de fichiers.

Pour lancer CBR à partir de la ligne de commande, procédez aux opérations ci-dessous.

- En tant qu'utilisateur root, exécutez la commande **cbrserver** à partir de l'invite.

Remarque : Pour arrêter le service, entrez la commande **cbrserver stop**.

- Ensuite, émettez les commandes de contrôles CBR souhaitées pour définir votre configuration. Les procédures décrites dans ce manuel reposent sur l'utilisation de la ligne de commande. La commande est **cbrcontrol**. Pour plus de détails sur les commandes, reportez-vous à la section «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.
- Démarrez Caching Proxy. Entrez la commande **ibmproxy** à partir de l'invite. (Vous devez lancer l'exécuteur avant Caching Proxy.)

Remarque : Windows 2000 : lancez Caching Proxy à partir du panneau Services en procédant comme suit : **Démarrer-> Paramètres-> Panneau de configuration -> Outils d'administration -> Services**.

Vous pouvez entrer une version abrégée des paramètres de contrôle cbrcontrol. Il suffit d'entrer les lettres uniques des paramètres. Par exemple, pour obtenir l'aide correspondant à la commande file save, vous pouvez entrer **cbrcontrol he f** au lieu de **cbrcontrol help file**.

Pour démarrer l'interface de ligne de commande, entrez **cbrcontrol** pour ouvrir une invite cbrcontrol.

Pour fermer l'interface de ligne de commande, entrez **exit** ou **quit**.

Remarques :

1. Sous Windows 2000, le service ndserver du composant Dispatcher démarre automatiquement. Si vous utilisez uniquement CBR et non le composant Dispatcher, vous pouvez empêcher ndserver de démarrer automatiquement de la manière suivante :
 - a. Dans la fenêtre Services de Windows 2000, cliquez avec le bouton droit de la souris sur IBM Dispatcher.
 - b. Sélectionnez Propriétés.
 - c. Dans la zone **Type de démarrage**, sélectionnez Manuel.
 - d. Cliquez sur OK et fermez la fenêtre Services.
2. Lorsque vous configurez CBR (Content Based Routing) à partir de l'invite du système d'exploitation, et non à partir de l'invite cbrcontrol>>, prenez soin d'utiliser les caractères suivants :
 - () parenthèses ouvrante et fermante
 - & perluète
 - | barre
 - ! point d'exclamation
 - * astérisque

Le shell du système d'exploitation peut interpréter ces caractères comme des caractères spéciaux et les convertir en texte de remplacement avant leur évaluation par cbrcontrol.

Les caractères spéciaux de la liste précédente sont facultatifs dans la commande **cbrcontrol rule add**. Ils sont employés lors de l'indication d'un motif pour une règle de contenu. Par exemple, la commande suivante ne peut être valide qu'avec l'invite cbrcontrol>>.

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

Pour que cette commande fonctionne à partir de l'invite du système d'exploitation, placez le motif entre guillemets (" ") comme suit :

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

Si vous omettez les guillemets, le motif sera peut-être tronqué lors de la sauvegarde de la règle dans CBR. Les guillemets ne sont pas pris en charge avec l'invite cbrcontrol>>.

Scripts

Les commandes de configuration CBR peuvent être entrées dans un fichier script de configuration et exécutées simultanément.

Remarque : Pour exécuter rapidement le contenu d'un fichier script (comme `myscript`), utilisez l'une des commandes ci-dessous.

- Pour mettre à jour la configuration actuelle, soumettez les commandes exécutables à partir du fichier script, en entrant —
`cbrcontrol file appendload myscript`
- Pour remplacer la configuration actuelle, soumettez les commandes exécutables à partir du fichier script en entrant —
`cbrcontrol file newload myscript`

Interface graphique

Pour avoir un exemple de l'interface graphique, reportez-vous à la section figure 2 à la page 5.

Pour démarrer l'interface graphique, procédez aux opérations décrites ci-dessous.

1. Vérifiez que `cbrserver` fonctionne. En tant que superutilisateur ou qu'administrateur, entrez la commande **`cbrserver`** à partir d'une invite.
2. Ensuite, effectuez l'une des opérations ci-dessous.
 - Pour AIX, Linux ou Solaris, entrez **`ndadmin`**
 - Pour Windows 2000, sélectionnez **Démarrer, Programmes, IBM WebSphere, Edge Server, IBM Network Dispatcher** et **Network Dispatcher**
3. Démarrez Caching Proxy. (A partir de l'interface graphique, vous devez d'abord vous connecter à l'hôte et lancer l'exécuteur pour le composant CBR avant de démarrer Caching Proxy.) Effectuez l'une des opérations suivantes :
 - AIX, Linux ou Solaris : pour lancer Caching Proxy, entrez **`ibmproxy`**.
 - Windows 2000 : pour lancer Caching Proxy, accédez au panneau Services en procédant comme suit : **Démarrer-> Paramètres-> Panneau de configuration -> Outils administratifs -> Services**.

Pour pouvoir configurer le composant CBR à partir de l'interface graphique, vous devez d'abord sélectionner **Content Based Routing** dans l'arborescence. Vous pouvez lancer le gestionnaire une fois que vous vous êtes connecté à un hôte. Vous pouvez également créer des grappes contenant des ports et des serveurs, puis lancer des conseillers pour le gestionnaire.

Vous pouvez utiliser l'interface graphique pour toute opération exécutée habituellement par la commande **`cbrcontrol`**. Par exemple, pour définir une grappe à l'aide de la ligne de commande, entrez la commande **`cbrcontrol cluster add cluster`**. Pour définir une grappe à partir de l'interface utilisateur graphique, cliquez à l'aide du bouton droit de la souris sur Exécuteur puis dans le menu en incrustation, sélectionnez **Ajout d'une grappe**. Entrez l'adresse de la grappe dans la fenêtre en incrustation, puis cliquez sur **OK**.

Les fichiers de configuration CBR existants peuvent être chargés à l'aide des options **Chargement de la nouvelle configuration** (pour remplacer intégralement la configuration en cours) et **Ajout à la configuration en cours** (pour mettre à jour la configuration en cours) du menu en incrustation **Hôte**. Vous devez sauvegarder régulièrement votre configuration CBR dans un fichier, en utilisant l'option **Sauvegarder le fichier de configuration en...** du menu en incrustation **Hôte**. Le menu **Fichier** situé dans la partie supérieure de l'interface graphique permet de sauvegarder les connexions à l'hôte en cours dans un fichier ou de restaurer des connexions dans des fichiers existants sur tous les composants Network Dispatcher.

Vous pouvez accéder à l'**Aide** en cliquant sur le point d'interrogation situé dans le coin supérieur droit de la fenêtre Network Dispatcher.

- **Aide sur les zones** — décrit les valeurs par défaut de chaque zone.
- **Procédures** — affiche la liste des tâches pouvant être effectuées dans cet écran.
- **Table des matières** — contient toutes les informations d'aide
- **Index** — index alphabétique des rubriques d'aide

Pour plus de détails sur l'utilisation de l'interface graphique, reportez-vous à la section «Instructions générales d'utilisation de l'interface graphique» à la page 6.

Assistant de configuration

Si vous utilisez l'Assistant de configuration, suivez la procédure ci-dessous :

1. Lancez cbrserver : entrez la commande **cbrserver** à partir de l'invite en tant que superutilisateur ou qu'administrateur root.
2. Lancez la fonction Assistant de CBR.

Pour ce faire, lancez l'assistant à partir de l'invite en entrant **cbrwizard**. Ou alors, sélectionnez l'assistant de configuration dans le menu des composants CBR proposé par l'interface graphique.

3. Démarrez Caching Proxy pour équilibrer la charge du trafic HTTP ou HTTPS (SSL).

AIX, Linux ou Solaris : pour lancer Caching Proxy, entrez **ibmproxy**.

Windows 2000 : pour lancer Caching Proxy, accédez au panneau Services en procédant comme suit : **Démarrer-> Paramètres-> Panneau de configuration -> Outils administratifs -> Services**.

Cet assistant vous guide, pas à pas, pendant la création d'une configuration de base du composant CBR. Il vous demande des renseignements sur votre réseau et vous guide pendant l'installation d'une grappe permettant à CBR d'équilibrer la charge du trafic dans un groupe de serveurs.

L'Assistant de configuration CBR vous proposera les panneaux suivants :

- Présentation de l'assistant
- Possibilités offertes par l'assistant
- Avant de commencer l'installation
- Choix de l'hôte à configurer (si nécessaire)
- Définition d'une grappe
- Ajout d'un port
- Ajout d'un serveur
- Ajout d'une règle
- Lancement d'un conseiller

Configuration du poste CBR

L'installation de la machine CBR ne peut être effectuée que par l'utilisateur root (pour AIX, Linux ou Solaris) ou l'administrateur sous Windows 2000.

Vous aurez besoin d'une adresse IP pour chaque grappe de serveurs configurée. Une adresse de grappe est une adresse associée à un nom de système hôte (par exemple `www.société_X.com`). Cette adresse IP est utilisée par un client pour se connecter aux serveurs de la grappe en question. Cette adresse se trouve dans la requête URL du client. Toutes les requêtes envoyées à la même adresse de grappe font l'objet d'un équilibrage de charge par CBR.

Sous Solaris uniquement : Pour pouvoir utiliser le composant CBR, vous devez modifier les valeurs système par défaut attribuées aux communications IPC (Inter-process Communication). Vous devez augmenter la taille maximale du segment de mémoire partagée et le nombre d'identificateurs de sémaphores. Pour configurer la prise en charge de CBR, ajoutez les instructions suivantes dans le fichier `/etc/system`, puis réamorçez le système :

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

Si vous n'attribuez pas au segment de mémoire partagée les valeurs ci-dessus, la commande `cbrcontrol executor start` échouera.

Etape 1. Configuration de Caching Proxy pour utiliser CBR

Pour utiliser le composant CBR, Caching Proxy doit être installé.

Remarque : Caching Proxy est un service qui, par défaut, démarre automatiquement après l'installation. Vous devez l'arrêter avant de lancer la fonction serveur CBR. Nous vous recommandons de

modifier le service Caching Proxy pour le démarrer manuellement et non automatiquement.

- AIX, Linux et Solaris : pour arrêter Caching Proxy, recherchez l'identificateur de processus correspondant à l'aide de la commande `ps -ef | grep ibmproxy`, puis mettez fin à ce processus à l'aide de la commande `kill ID_processus`.
- Windows : arrêtez Caching Proxy à partir du panneau Services.

Apportez les modifications ci-dessous au fichier de configuration Caching Proxy (`ibmproxy.conf`) :

Modifiez l'instruction URL entrante **CacheByIncomingUrl** de telle sorte qu'elle indique "on".

Quatre entrées doivent être modifiées pour le module d'extension CBR :

- ServerInit
- PreExit
- PostExit
- ServerTerm

Chaque entrée doit figurer sur une ligne. Le fichier `ibmproxy.conf` comporte plusieurs instances de "ServerInit" (une par module d'extension). Les entrées relatives au module d'extension CBR doivent être modifiées et ne doivent comporter aucun commentaire.

Les ajouts spécifiques au fichier de configuration d'AIX, Linux, Solaris et Windows 2000 sont répertoriés ci-dessous.

Figure 16. Fichier de configuration CBR pour AIX

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

Figure 17. Fichier de configuration CBR pour Linux

```
ServerInit  /opt/nd/servers/lib/libndcbr.so:ndServerInit
PreExit    /opt/nd/servers/lib/libndcbr.so:ndPreExit
```

```
PostExit /opt/nd/servers/lib/libndcbr.so:ndPostExit
ServerTerm /opt/nd/servers/lib/libndcbr.so:ndServerTerm
```

Figure 18. Fichier de configuration CBR pour Solaris

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

Figure 19. Fichier de configuration CBR pour Windows 2000

Chemin d'accès courant au répertoire d'installation :

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

Chemin d'accès au répertoire d'installation natif :

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

Etape 2. Démarrage de la fonction serveur

Remarque : Caching Proxy est un service qui, par défaut, démarre automatiquement après l'installation. Vous devez l'arrêter avant de lancer la fonction serveur CBR. Nous vous recommandons de modifier le service Caching Proxy pour le démarrer manuellement et non automatiquement.

- AIX, Linux et Solaris : pour arrêter Caching Proxy, recherchez l'identificateur de processus correspondant à l'aide de la commande `ps -ef|grep ibmproxy`, puis mettez fin à ce processus à l'aide de la commande `kill ID_processus`.
- Windows : arrêtez Caching Proxy à partir du panneau Services.

Pour démarrer la fonction serveur CBR, entrez **cbrserver** sur la ligne de commande.

Un fichier de configuration par défaut (default.cfg) est chargé automatiquement lors du démarrage de cbrserver. Si vous sauvegardez la configuration CBR dans default.cfg, toutes les données enregistrées dans ce fichier seront automatiquement chargées au prochain démarrage de cbrserver.

Etape 3. Démarrage de la fonction exécuteur

Pour démarrer la fonction exécuteur, entrez la commande **cbrcontrol executor start**. Notez que vous pouvez également modifier divers paramètres de l'exécuteur à cette occasion. Voir «ndcontrol executor — Contrôle de l'exécuteur» à la page 271.

Etape 4. Définition et configuration des options de la grappe

CBR équilibrera les requêtes envoyées à l'adresse de la grappe entre les serveurs correspondants configurés sur les ports de cette grappe.

L'adresse de grappe correspond à un nom symbolique ou à une notation décimale. Elle se trouve dans la partie hôte de l'URL.

Pour définir une grappe, tapez la commande suivante :

```
cbrcontrol cluster add grappe
```

Pour définir les options de grappe, tapez la commande suivante :

```
cbrcontrol cluster set valeur d'option de grappe
```

Pour plus d'informations, voir «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Etape 5. Affectation d'un alias à la carte d'interface réseau (facultatif)

Si vous exécutez Caching Proxy dans une configuration de proxy inverse, lors de l'équilibrage de charge pour plusieurs sites Web, vous devez ajouter l'adresse de grappe de chaque site Web à l'une au moins des cartes d'interface réseau du dispositif Network Dispatcher. Sinon, vous pouvez ignorer cette étape.

AIX, Linux ou Solaris : pour ajouter l'adresse de grappe à l'interface réseau, servez-vous de la commande ifconfig. Utilisez la commande adaptée au système d'exploitation (voir tableau 7 à la page 92).

Tableau 7. Commandes pour l'affectation d'un alias à la carte d'interface réseau

AIX	ifconfig <i>nom_interface</i> alias <i>adresse_groupe</i> netmask <i>masque_réseau</i>
Linux	ifconfig <i>nom_interface</i> <i>adresse_groupe</i> netmask <i>masque_réseau</i> up
Solaris 7	ifconfig <i>nom_interface</i> <i>adresse_groupe</i> netmask <i>masque_réseau</i> up
Solaris 8	ifconfig addif <i>nom_interface</i> <i>adresse_groupe</i> netmask <i>masque_réseau</i> up

Remarque : Sous Linux et Solaris, *nom_interface* doit comporter un numéro unique à chaque adresse de grappe ajoutée. Par exemple : eth0:1, eth0:2, etc.

Windows : pour ajouter l'adresse de grappe à l'interface réseau, procédez comme suit :

1. Sélectionnez **Démarrer, Paramètres**, puis **Panneau de configuration**.
2. Cliquez deux fois sur **Connexions réseau et accès à distance**.
3. Cliquez avec le bouton droit de la souris sur **Connexion au réseau local**.
4. Sélectionnez **Propriétés**.
5. Sélectionnez **Protocole Internet (TCP/IP)**, puis cliquez sur **Propriétés**.
6. Sélectionnez **Utiliser l'adresse IP suivante**, puis cliquez sur **Avancé**.
7. Cliquez sur **Ajouter**, puis entrez l'adresse IP et le **masque de sous-réseau** de la grappe.

Etape 6. Définition des ports et de leurs options

Le numéro de port est le port à partir duquel les applications serveur sont à l'écoute. Pour le composant CBR avec Caching Proxy exécutant le trafic HTTP, il s'agit en général du port 80.

Pour définir le port de la grappe définie à l'étape précédente, entrez la commande

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

Pour définir les options de port, tapez la commande suivante :

```
cbrcontrol port set cluster:port option value
```

Pour plus d'informations, reportez-vous à la section «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Etape 7. Définition des serveurs avec équilibrage de charge

Les serveurs sont les postes qui exécutent les applications dont vous souhaitez équilibrer les charges. Le *serveur* est l'adresse à nom symbolique ou notation décimale de la machine serveur. Pour définir un serveur dans la grappe et le port, tapez la commande suivante :

```
cbrcontrol server add grappe:port:serveur
```

Vous devez définir un ou plusieurs serveurs par port sur une grappe pour pouvoir procéder à l'équilibrage des charges.

Etape 8. Ajout de règles à la configuration

Il s'agit de l'étape clé de la configuration CBR avec Caching Proxy. Une règle définit la manière dont une requête URL sera reconnue et envoyée à l'un des ensembles de serveurs appropriés. Le type de règle spéciale utilisé par CBR est appelé règle de contenu. Pour définir une règle de contenu, tapez la commande suivante :

```
cbrcontrol rule add cluster:port:rule type content pattern=pattern
```

La valeur *pattern* est l'expression régulière qui sera comparée à l'URL de chaque requête client. Pour plus d'informations sur la configuration de la structure, voir «Annexe C. Syntaxe des règles de contenu (modèle)» à la page 323.

Certains autres types de règles définis dans Dispatcher peuvent également être utilisés dans CBR. Pour plus d'informations, voir «Configuration de l'équilibrage basé sur des règles» à la page 180.

Etape 9. Ajout de serveurs à vos règles

Lorsqu'une règle correspond à une requête client, l'ensemble de serveurs de la règle est interrogé pour déterminer le meilleur serveur. L'ensemble de serveurs de la règle est un sous-ensemble de serveurs définis dans le port. Pour ajouter des serveurs à un ensemble de serveurs de la règle, lancez la commande suivante :

```
cbrcontrol rule useserver cluster:port:rule server
```

Etape 10. Démarrage de la fonction gestionnaire (facultatif)

La fonction gestionnaire permet d'améliorer l'équilibrage de charge. Pour lancer le gestionnaire, tapez la commande suivante :

```
cbrcontrol manager start
```

Etape 11. Démarrage de la fonction conseiller (facultatif)

Les conseillers transmettent au gestionnaire des informations complémentaires sur la capacité des serveurs ayant fait l'objet d'un équilibrage de charge à répondre aux requêtes. Chaque conseiller est spécifique à un protocole. Par exemple, tapez la commande suivante pour lancer le conseiller HTTP :

```
cbrcontrol advisor start http port
```

Etape 12. Définition du niveau d'importance des informations requis pour la grappe

Si vous lancez des conseillers, vous pouvez modifier le niveau d'importance donné aux informations des conseillers entrant dans les décisions d'équilibrage de la charge. Pour définir le niveau d'importance des informations pour la grappe, entrez la commande **cbrcontrol cluster set *cluster proportions***. Pour plus d'informations, voir «Proportion de l'importance accordée aux données d'état» à la page 141.

Etape 13. Démarrage de Caching Proxy

- Plate-forme AIX : Ajoutez la ligne suivante à votre variable d'environnement LIBPATH :
`/usr/lpp/nd/servers/lib`
- Plate-forme Linux ou Solaris : Ajoutez la ligne suivante à votre variable d'environnement LD_LIBRARY_PATH :
`/opt/nd/servers/lib`
- Plate-forme Windows 2000 : Ajoutez la ligne suivante à votre variable d'environnement PATH :
Chemin d'accès courant au répertoire d'installation :
`c:\Program Files\IBM\edge\nd\servers\lib`

Chemin d'accès au répertoire d'installation natif :
`c:\Program Files\IBM\nd\servers\lib`

Dans le nouvel environnement, démarrez Caching Proxy, en entrant **ibmproxy** à partir de l'invite.

Remarque : Sous Windows 2000 : lancez Caching Proxy à partir du panneau Services en procédant comme suit : **Démarrer-> Paramètres-> Panneau de configuration -> Outils d'administration -> Services.**

Exemple de configuration CBR

Pour configurer CBR, procédez aux opérations ci-dessous.

1. Démarrez CBR : entrez la commande **cbrserver**.
2. Démarrez l'interface de ligne de commande : lancez la commande **cbrcontrol**.
3. L'invite **cbrcontrol** s'affiche. Lancez les commandes suivantes :
(*cluster(c),port(p),rule(r),server(s)*)
 - `executor start`
 - `cluster add c`
 - `port add c:p`

- `server add c:p:s`
 - `rule add c:p:r type content pattern uri=*`
 - `rule use server c:p:r s`
4. Démarrez Caching Proxy : entrez la commande **ibmproxy**. Sous Windows 2000, lancez Caching Proxy à partir du panneau Services.
 5. Supprimez toutes les configurations de proxy du à partir du navigateur.
 6. Chargez `http://c/` dans votre navigateur, où "`c`" est la grappe que vous avez configurée.
 - Le serveur "`s`" est appelé.
 - La page Web suivante s'affiche : `http://s/`

Chapitre 8. Planification du composant Mailbox Locator

Le présent chapitre décrit les aspects que l'administrateur de réseau doit prendre en compte avant d'installer et de configurer le composant Mailbox Locator.

Remarque : Le composant Mailbox Locator était auparavant une fonction appartenant au composant CBR qui assurait l'équilibrage de charge sur les serveurs de messagerie IMAP et POP3, en fonction d'ID utilisateur et de mots de passe. La séparation de CBR en deux composants permet d'exécuter "CBR for IMAP/POP3" (Mailbox Locator) et "CBR for HTTP/HTTPS" (CBR avec Caching Proxy) sur le même poste.

- Reportez-vous au «Chapitre 9. Configuration du composant Mailbox Locator» à la page 101 pour obtenir des informations sur la configuration des paramètres d'équilibrage de charge de Mailbox Locator.
- Pour obtenir des informations sur la configuration de Network Dispatcher pour les fonctions avancées, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Le présent chapitre se compose des sections suivantes :

- «Matériel et logiciels requis»
- «Remarques relatives à la planification» à la page 98

Matériel et logiciels requis

- Pour AIX, reportez-vous à la section «Configuration requise pour AIX» à la page 12
- Pour Linux, reportez-vous à la section «Configuration requise pour Red Hat Linux ou SuSE Linux» à la page 17
- Pour Solaris, reportez-vous à la section «Configuration requise pour Solaris» à la page 20
- Pour Windows 2000, reportez-vous à la section «Configuration requise pour Windows 2000» à la page 22

Remarques relatives à la planification

Le composant Mailbox Locator permet d'acheminer le trafic IMAP et POP3 par proxy en fonction de l'ID utilisateur et du mot de passe de la demande client.

La structure de Mailbox Locator ressemble beaucoup à celle de Dispatcher. Mailbox Locator se compose des fonctions suivantes :

- **mlserver** traite les demandes à partir de la ligne de commande adressées à l'exécuteur, au gestionnaire et aux conseillers.
- L'**exécuteur** prend en charge l'équilibrage de charge des requêtes client. L'exécuteur s'exécute toujours lorsque le composant Mailbox Locator est en cours d'utilisation.
- Le **gestionnaire** définit les mesures utilisées par l'exécuteur en fonction de plusieurs facteurs :
 - décomptes internes de l'exécuteur,
 - retour d'informations sur les serveurs fourni par les conseillers,
 - retour d'informations émanant d'un programme de contrôle système, tel que Metric Server.

L'utilisation du gestionnaire n'est que facultative. Toutefois, s'il n'est pas utilisé, l'équilibrage de charge se fera sur la base d'une planification circulaire pondérée, elle-même basée sur les mesures de charge des serveurs et les conseillers ne seront pas disponibles.

- Les **conseillers** interrogent les serveurs puis analysent les résultats par protocole avant de demander au gestionnaire de régler les capacités comme il convient. L'utilisation de certains de ces conseillers n'est peut-être pas utile dans une configuration typique. Vous avez également la possibilité de développer vos propres conseillers. L'utilisation des conseillers est facultative mais recommandée. Pour de plus amples informations, reportez-vous à «Conseillers» à la page 146.
- Pour configurer et gérer l'exécuteur, les conseillers et le gestionnaire, utilisez la ligne de commande (**mlcontrol**) ou l'interface utilisateur graphique (**ndadmin**).

Les trois fonctions clés de Mailbox Locator(l'exécuteur, le gestionnaire et les conseillers) agissent en collaboration pour équilibrer et répartir entre les serveurs les requêtes réceptionnées. Outre la gestion des requêtes d'équilibrage de charge, l'exécuteur contrôle le nombre de nouvelles connexions et de connexions actives, et transmet ces informations au gestionnaire.

Pour démarrer Mailbox Locator, lancez la commande **mlserver** à partir de l'invite.

Mailbox Locator peut fournir un point de présence unique à plusieurs serveurs IMAP ou POP3. Chaque serveur peut avoir un sous-ensemble de toutes les boîtes aux lettres dont la maintenance est assurée par le point de présence. Dans le cas des protocoles IMAP et POP3, Mailbox Locator est un proxy qui choisit un serveur approprié en se fondant sur l’ID utilisateur et le mot de passe donnés par le client.

Remarque : Mailbox Locator ne prend *pas* en charge l’équilibrage de charge fondé sur des **règles**.

Vous trouverez ci-dessous un exemple d’une méthode de distribution des demandes en fonction de l’ID utilisateur. Si vous avez deux serveurs POP3 (ou plus), vous pouvez choisir de diviser les boîtes aux lettres alphabétiquement par ID utilisateur. Les demandes client dont les ID commencent par les lettres A à I peuvent être distribuées au serveur 1. Les demandes client dont les ID commencent par les lettres J à R peuvent être distribuées sur le serveur 2, etc.

Vous pouvez également choisir que chaque boîte aux lettres soit représentée sur plusieurs serveurs. Dans ce cas, le contenu de chaque boîte aux lettres doit être disponible à tous les serveurs de cette boîte aux lettres. En cas de panne d’un serveur, un autre serveur peut toujours accéder à la boîte aux lettres.

Afin qu’une seule adresse représente plusieurs serveurs de courrier POP3, Mailbox Locator peut être configuré avec une seule adresse de grappe qui devient l’adresse du serveur de courrier POP3 pour tous les clients. Les commandes de configuration sont les suivantes :

```
mlcontrol cluster add pop3MailServer
mlcontrol port add pop3MailServer:110 protocol pop3
mlcontrol server add pop3MailServer:110:pop3Server1+pop3Server2+pop3Server3
```

Dans cet exemple, *pop3MailServer* représente l’adresse de la grappe. Le port 110 avec POP3 comme protocole de commande proxy est ajouté au *pop3MailServer*. *Pop3Server1*, *pop3Server2* et *pop3Server3* représentent les serveurs de courrier POP3 qui sont ajoutés au port. Avec cette configuration, vous pouvez configurer vos requêtes POP3 entrantes du courrier client avec l’adresse de grappe *pop3MailServer*.

Utilisation de la fonction d’affinité

Lorsqu’une requête POP3 ou IMAP arrive sur le proxy, ce dernier tente de contacter tous les serveurs configurés pour le port qui utilise l’ID utilisateur et le mot de passe du client. La requête du client est dirigée vers le premier serveur qui répond. Vous devez utiliser la fonction temps de maintien/affinité en conjonction avec le composant Mailbox Locator pour les serveurs IMAP ou POP3. La fonction d’affinité permet de diriger les requêtes ultérieures provenant de l’ID utilisateur du même client vers le même serveur.

Attribuez au paramètre **stickytime** associé au port une valeur supérieure à zéro pour activer la fonction d'affinité. Pour plus d'informations sur la fonction d'affinité, reportez-vous à la section «Fonctionnement de la fonction d'affinité pour Network Dispatcher» à la page 195

Remplacement du délai d'inactivité de POP3/IMAP

L'horloge d'autologout en cas d'inactivité est, respectivement pour les protocoles POP3 et IMAP, de 10 minutes et 30 minutes. Cette temporisation correspond au nombre de secondes durant lesquelles il peut n'y avoir aucune activité sur une connexion avant que cette dernière ne soit retirée. Pour optimiser les performances, Mailbox Locator remplace la valeur du délai d'inactivité par 60 secondes. Pour modifier le délai d'inactivité, remplacez la valeur **staletimeout** à l'aide de la commande **mlcontrol port**. Pour plus d'informations sur cette commande, reportez-vous à la section «ndcontrol port — Configuration des ports» à la page 296.

Chapitre 9. Configuration du composant Mailbox Locator

Avant d'effectuer les opérations décrites dans le présent chapitre, reportez-vous à la section «Chapitre 8. Planification du composant Mailbox Locator» à la page 97. Ce chapitre décrit comment créer une configuration de base pour le composant Mailbox Locator de Network Dispatcher.

Remarque : Le composant Mailbox Locator était auparavant une fonction appartenant au composant CBR qui assurait l'équilibrage de charge sur les serveurs de messagerie IMAP et POP3, en fonction d'ID utilisateur et de mots de passe. La répartition de CBR en deux composants permet d'exécuter "CBR for IMAP/POP3" (Mailbox Locator) et "CBR for HTTP/HTTPS" (CBR avec Caching Proxy) sur le même poste.

- Pour de plus amples informations sur Network Dispatcher, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Présentation générale des tâches de configuration

Remarque : Avant de suivre les étapes de configuration détaillées dans ce tableau, assurez-vous que la machine Mailbox Locator et toutes les machines serveurs sont connectées au réseau, qu'elles ont des adresses IP valides et qu'elles peuvent communiquer entre elles.

Tableau 8. Tâches de configuration du composant Mailbox Locator

Tâche	Description	Informations connexes
Configurer la machine Mailbox Locator.	Conditions requises	«Installation de la machine Mailbox Locator» à la page 105
Configurer des machines en vue de l'équilibrage de charge	Définition de la configuration de l'équilibrage de charge.	«Etape 4. Définition des serveurs avec équilibrage de charge» à la page 106

Méthodes de configuration

Pour créer une configuration de base pour le composant Mailbox Locator de Network Dispatcher, il existe quatre méthodes :

- Ligne de commande
- Scripts
- Interface graphique
- Assistant de configuration

Ligne de commande

Il s'agit de la méthode la plus directe pour la configuration de Mailbox Locator. Les valeurs des paramètres de commande doivent être saisies en anglais. Les seules exceptions s'appliquent aux noms d'hôte (utilisés dans les commandes cluster et server) et aux noms de fichiers.

Pour lancer Mailbox Locator à partir de la ligne de commande :

- Lancez la commande **mlserver** à partir de l'invite.

Remarque : Pour arrêter le service, entrez la commande : **mlserver stop**.

- Ensuite, émettez les commandes de contrôles Mailbox souhaitées pour définir votre configuration. Les procédures décrites dans ce manuel reposent sur l'utilisation de la ligne de commande. La commande est **mlcontrol**. Pour plus de détails sur les commandes, reportez-vous à la section «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Vous pouvez entrer une version abrégée des paramètres de commande **mlcontrol**. Il suffit d'entrer les lettres uniques des paramètres. Par exemple, pour obtenir l'aide correspondant à la commande **file save**, vous pouvez entrer **mlcontrol he f** au lieu de **mlcontrol help file**.

Pour démarrer l'interface de ligne de commande, entrez **mlcontrol** pour obtenir une invite **mlcontrol**.

Pour fermer l'interface de ligne de commande, entrez **exit** ou **quit**.

Remarque : Sous Windows 2000, le service **ndserver** du composant Dispatcher démarre automatiquement. Si vous utilisez uniquement Mailbox Locator et non le composant Dispatcher, vous pouvez empêcher **ndserver** de démarrer automatiquement de la manière suivante :

1. Dans la fenêtre Services de Windows 2000, cliquez avec le bouton droit de la souris sur IBM Dispatcher.
2. Sélectionnez Propriétés.

3. Dans la zone **Type de démarrage**, sélectionnez Manuel.
4. Cliquez sur OK et fermez la fenêtre Services.

Scripts

Les commandes permettant de configurer Mailbox Locator peuvent être entrées dans un fichier script de configuration, puis exécutées ensemble.

Remarque : Pour exécuter rapidement le contenu d'un fichier script (comme `myscript`), utilisez l'une des commandes ci-dessous.

- Pour mettre à jour la configuration actuelle, soumettez les commandes exécutables à partir du fichier script, en entrant —
`mlcontrol file appendload monscript`
- Pour remplacer la configuration actuelle, soumettez les commandes exécutables à partir du fichier script en entrant —
`mlcontrol file newload monscript`

Interface graphique

Reportez-vous à la section figure 2 à la page 5 pour consulter un exemple de l'interface graphique.

Pour démarrer l'interface graphique, procédez de la manière suivante :

1. Vérifiez que `mlserver` fonctionne. En tant qu'utilisateur root ou administrateur, entrez la commande `mlserver` à partir de l'invite.
2. Ensuite, effectuez l'une des opérations suivantes :
 - Pour AIX, Linux ou Solaris : Entrez `ndadmin`
 - Pour Windows 2000, sélectionnez **Démarrer, Programmes, IBM WebSphere, Edge Server, IBM Network Dispatcher** et **Network Dispatcher**

Pour pouvoir configurer le composant Mailbox Locator à partir de l'interface graphique, vous devez d'abord sélectionner **Mailbox Locator** dans l'arborescence. Vous pouvez lancer le gestionnaire une fois que vous êtes connecté à un hôte. Vous pouvez également créer des grappes contenant des ports et des serveurs, puis lancer des conseillers pour le gestionnaire.

Vous pouvez utiliser l'interface graphique pour toute opération normalement exécutée par la commande `mlcontrol`. Par exemple, pour définir une grappe à l'aide de la ligne de commande, vous devez entrer la commande `mlcontrol cluster add grappe`. Pour définir une grappe à partir de l'interface graphique, cliquez avec le bouton droit de la souris sur Exécuteur, puis dans le menu en incrustation qui apparaît, cliquez sur le bouton **Ajouter une grappe** à l'aide du bouton gauche de la souris. Entrez l'adresse de la grappe dans la fenêtre en incrustation, puis cliquez sur **OK**.

Les fichiers de configuration Mailbox Locator existants peuvent être chargés à l'aide des options **Charger la nouvelle configuration** (pour remplacer intégralement la configuration en cours) et **Ajouter à la configuration en cours** (pour la mise à jour de la configuration en cours) du menu en incrustation **Hôte**. Vous devez sauvegarder votre configuration Mailbox Locator dans un fichier régulièrement en utilisant l'option **Sauvegarder le fichier de configuration en** dans le menu en incrustation **Hôte**. Le menu **Fichier** situé dans la partie supérieure de l'interface graphique permet de sauvegarder les connexions à l'hôte en cours dans un fichier ou de restaurer des connexions dans des fichiers existants sur tous les composants Network Dispatcher.

Vous pouvez accéder à l'**Aide** en cliquant sur le point d'interrogation situé dans le coin supérieur droit de la fenêtre Network Dispatcher.

- **Aide sur les zones** — décrit les valeurs par défaut de chaque zone.
- **Procédures** — affiche la liste des tâches pouvant être effectuées dans cet écran.
- **Table des matières** — contient toutes les informations d'aide
- **Index** — index alphabétique des rubriques d'aide

Pour plus de détails sur l'utilisation de l'interface graphique, reportez-vous à la section «Instructions générales d'utilisation de l'interface graphique» à la page 6.

Assistant de configuration

Si vous utilisez l'Assistant de configuration, suivez la procédure ci-dessous :

1. Exécutez la commande **mlserver** à partir d'une invite en tant qu'utilisateur root ou administrateur.
2. Lancez la fonction d'assistant de Mailbox Locator, **mlwizard**.

Vous pouvez lancer cet assistant à partir de l'invite en entrant la commande **mlwizard** ou sélectionnez l'assistant de configuration à partir du menu du composant Mailbox Locator présenté dans l'interface graphique.

L'assistant Mailbox Locator vous guide pas à pas dans le processus de création d'une configuration de base pour le composant Mailbox Locator. Il vous demande des renseignements sur votre réseau et vous guide pour la configuration d'une grappe permettant à Mailbox Locator d'équilibrer le trafic entre un groupe de serveurs.

L'assistant de configuration Mailbox Locator propose les panneaux suivants :

- Présentation de l'assistant
- Possibilités offertes par l'assistant
- Avant de commencer l'installation

- Choix de l'hôte à configurer (si nécessaire)
- Définition d'une grappe
- Ajout d'un port
- Ajout d'un serveur
- Lancement d'un conseiller

Installation de la machine Mailbox Locator

L'installation de la machine Mailbox Locator ne peut être effectuée que par l'utilisateur root (pour AIX, Linux ou Solaris) ou l'administrateur sous Windows 2000.

Vous aurez besoin d'une adresse IP pour chaque grappe de serveurs configurée. Une adresse de grappe est une adresse associée à un nom de système hôte (par exemple `www.société_X.com`). Cette adresse IP est utilisée par un client pour se connecter aux serveurs de la grappe en question. Toutes les demandes envoyées à la même adresse de grappe font l'objet d'un équilibrage de charge par Mailbox Locator.

Etape 1. Démarrage de la fonction serveur

Pour démarrer la fonction serveur, entrez **mlserver** à partir de la ligne de commande.

Remarque : Un fichier de configuration par défaut (`default.cfg`) est chargé automatiquement pendant le démarrage de **mlserver**. Si l'utilisateur décide de sauvegarder la configuration dans `default.cfg`, toutes les données enregistrées dans ce fichier seront chargée automatiquement au prochain démarrage de **mlserver**.

Etape 2. Définition d'une grappe et configuration des options de la grappe

Mailbox Locator équilibrera les demandes envoyées à l'adresse de la grappe entre les serveurs correspondants configuré sur les ports de la grappe.

L'adresse de grappe correspond à un nom symbolique ou à une notation décimale.

Pour définir une grappe, tapez la commande suivante :

```
mlcontrol cluster add grappe
```

Pour définir les options de grappe, tapez la commande suivante :

```
mlcontrol cluster set cluster option value
```

Pour plus d'informations, reportez-vous à la section «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Etape 3. Définition des ports et configuration des options de port

Le numéro de port est le port à partir duquel les applications serveur sont à l'écoute. Pour le trafic IMAP, il s'agit généralement du port 143 et pour le trafic POP3 du port 110.

Pour définir le port de la grappe définie à l'étape précédente, entrez la commande

```
mlcontrol port add  
grappe:port protocol [pop3|imap]
```

Pour définir les options de port, tapez la commande suivante :

```
mlcontrol port set grappe:port option valeur
```

Remarque : Lorsque vous ajoutez un port, indiquez le protocole proxy (pop3 ou imap). Une fois le port ajouté, vous ne pouvez pas modifier la valeur du protocole de ce port.

Pour plus d'informations, reportez-vous à la section «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Etape 4. Définition des serveurs avec équilibrage de charge

Les serveurs de messagerie sont les postes qui exécutent les applications dont vous souhaitez équilibrer la charge. Le *serveur* est l'adresse à nom symbolique ou notation décimale de la machine serveur. Pour définir un serveur dans la grappe et le port de l'étape 3, tapez la commande suivante :

```
mlcontrol server add cluster:port:server
```

Vous devez définir un ou plusieurs serveurs par port sur une grappe pour pouvoir procéder à l'équilibrage des charges.

Etape 5. Lancement de la fonction gestionnaire (facultatif)

La fonction gestionnaire permet d'améliorer l'équilibrage de charge. Pour lancer le gestionnaire, tapez la commande suivante :

```
mlcontrol manager start
```

Etape 6. Lancement de la fonction conseiller (facultatif)

Les conseillers transmettent au gestionnaire des informations complémentaires sur la capacité des serveurs ayant fait l'objet d'un équilibrage de charge à répondre aux requêtes. Chaque conseiller est spécifique à un protocole. Le système Network Dispatcher fournit les conseillers IMAP et POP3. Par exemple, pour lancer le conseiller IMAP, entrez la commande suivante :

```
mlcontrol advisor start imap port
```

Pour consulter la liste des conseillers et des ports par défaut correspondants, reportez-vous à l'«Annexe B. Guide des commandes Dispatcher, CBR et

Mailbox Locator» à la page 257. Pour lire la description de chaque conseiller, reportez-vous à la section «Liste des conseillers» à la page 149.

Etape 7. Définition du niveau d'importance des informations de la grappe

Si vous lancez des conseillers, vous pouvez modifier le niveau d'importance donné aux informations des conseillers entrant dans les décisions d'équilibrage de la charge. Pour définir le niveau d'importance des informations pour la grappe, entrez la commande **mlcontrol cluster set *grappe* proportions**. Pour plus d'informations, reportez-vous à la section «Proportion de l'importance accordée aux données d'état» à la page 141.

Chapitre 10. Planification du composant Site Selector

Le présent chapitre décrit les aspects que l'administrateur de réseau doit prendre en compte avant d'installer et de configurer le composant Site Selector.

- Reportez-vous au «Chapitre 11. Configuration du composant Site Selector» à la page 115 pour obtenir des informations sur la configuration des paramètres d'équilibrage de charge de Site Selector.
- Pour obtenir des informations sur la configuration de Network Dispatcher pour les fonctions avancées, reportez-vous au «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Le présent chapitre se compose des sections suivantes :

- «Matériel et logiciels requis»
- «Remarques relatives à la planification»

Matériel et logiciels requis

- Pour AIX, reportez-vous à la section «Configuration requise pour AIX» à la page 12
- Pour Linux, reportez-vous à la section «Configuration requise pour Red Hat Linux ou SuSE Linux» à la page 17
- Pour Solaris, reportez-vous à la section «Configuration requise pour Solaris» à la page 20
- Pour Windows 2000, reportez-vous à la section «Configuration requise pour Windows 2000» à la page 22

Remarques relatives à la planification

Site Selector fonctionne avec un serveur de noms de domaine pour équilibrer la charge sur un groupe de serveurs à l'aide des mesures et des pondérations recueillies. Vous pouvez créer une configuration de site pour assurer l'équilibrage de charge sur un groupe de serveurs sur la base du nom de domaine utilisé pour la demande d'un client.

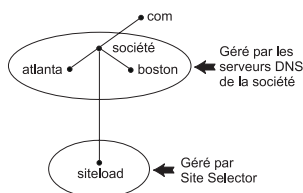


Figure 20. Exemple d'environnement DNS

Lors de la définition d'un sous-domaine de Site Selector dans l'environnement DNS, Site Selector doit disposer de droits d'accès à ce sous-domaine. Par exemple (voir la figure 20), votre entreprise dispose de droits d'accès au domaine **entreprise.com**. Elle dispose de plusieurs sous-domaines. Site Selector doit disposer de droits d'accès à **siteload.entreprise.com** et les serveurs DNS gardent leurs droits d'accès à **atlanta.entreprise.com** et à **boston.entreprise.com**.

Pour permettre au serveur de noms de l'entreprise de reconnaître les droits d'accès de Site Selector au sous-domaine siteload, il est nécessaire d'ajouter une entrée dans le fichier de données du serveur de noms. Par exemple, sous AIX, une entrée de serveur de noms a l'apparence suivante :
siteload.entreprise.com. IN NS siteselector.entreprise.com.

Où **siteselector.entreprise.com** correspond au nom d'hôte de la machine Site Selector. Des entrées équivalentes doivent être insérées dans les autres fichiers de base de données utilisés par les serveurs DNS.

Un client envoie une demande de résolution de nom de domaine à un serveur de noms du réseau. Le serveur de noms achemine la demande au poste Site Selector. Ce dernier résout le nom de domaine en adresse IP de l'un des serveurs qui a été configuré sous le nom du site. Site Selector renvoie l'adresse IP du serveur sélectionné au serveur de noms. Le serveur de noms renvoie l'adresse IP au client. (Site Selector joue le rôle de serveur de noms non récurrents (noeud feuille) et renvoie une erreur s'il ne résout pas la demande de nom de domaine.

Reportez-vous à la figure 11 à la page 43 qui montre un site dans lequel Site Selector est utilisé avec un système DNS pour équilibrer la charge entre des serveurs locaux et éloignés.

Site Selector se compose des fonctions suivantes :

- **ssserver** traite les demandes à partir de la ligne de commande adressées au serveur de noms, au gestionnaire et aux conseillers.
- La fonction de **serveur de noms** prend en charge l'équilibrage de charge des demandes de serveur de noms entrantes. Vous devez démarrer la

fonction de serveur de noms pour que Site Selector puisse commencer la résolution DNS. Site Selector écoute sur le port 53 les requêtes DNS entrantes. Si le nom du site qui émet la demande est configuré, Site Selector renvoie une adresse de serveur unique (à partir d'un ensemble d'adresses de serveurs) associée au nom de site.

- Le **gestionnaire** définit les pondérations utilisées par le serveur de noms en fonction de plusieurs facteurs :
 - le retour d'informations sur les serveurs fourni par les conseillers,
 - le retour d'informations émanant d'un programme de contrôle système, tel que Metric Server.

L'utilisation du gestionnaire n'est que facultative. Toutefois, s'il n'est pas utilisé, l'équilibrage de charge se fera sur la base d'une planification circulaire pondérée, elle-même basée sur les mesures de charge des serveurs et les conseillers ne seront pas disponibles.

- **Metric Server** est un composant de surveillance système de Network Dispatcher installé sur la machine serveur d'arrière-plan. (Si vous co-implantez Network Dispatcher sur une machine serveur dont la charge est en cours d'équilibrage, installez Metric Server sur la machine Network Dispatcher.)

Metric Server permet à Site Selector de surveiller le niveau d'activité d'un serveur, de détecter le moment où un serveur est le moins chargé et de détecter un serveur défaillant. Par charge, on entend le travail effectivement fourni par le serveur. L'administrateur système Site Selector contrôle le type de mesure employé pour évaluer la charge. Site Selector peut être configuré en fonction de chaque environnement, en tenant compte de facteurs tels que la fréquence des accès, le nombre total d'utilisateurs et les différents types d'accès (requêtes courtes, longues, à forte ou faible consommation de ressources CPU).

L'équilibrage de charge est basée sur les pondérations de serveur. Pour Site Selector, il existe quatre niveaux d'importance des informations que le gestionnaire utilise pour déterminer les pondérations :

- CPU
- mémoire
- port
- système

Les valeurs CPU et mémoire sont fournies par Metric Server. Par conséquent, l'utilisation de Metric Server est *recommandée* avec le composant Site Selector.

Pour de plus amples informations, reportez-vous à «Metric Server» à la page 157.

- Les **conseillers** interrogent les serveurs et analysent les résultats par protocole avant d'appeler le gestionnaire pour définir les pondérations comme il convient. L'utilisation de certains de ces conseillers n'est peut-être pas utile dans une configuration typique. Vous avez également la possibilité de développer vos propres conseillers. L'utilisation des conseillers est facultative mais recommandée. Pour de plus amples informations, reportez-vous à «Conseillers» à la page 146.
- Pour configurer et gérer le serveur de noms, les conseillers, Metric Server et le gestionnaire, utilisez la ligne de commande (**sscontrol**) ou l'interface utilisateur graphique (**ndadmin**).

Les quatre fonctions clés de Site Selector (serveur de noms, gestionnaire, Metric Server et conseillers) interagissent afin d'équilibrer les demandes entrantes entre les serveurs et de les résoudre.

Considérations relatives à la durée de vie (TTL)

L'équilibrage de charge utilisant le système DNS nécessite la désactivation de l'enregistrement en mémoire cache de la résolution des noms. La valeur TTL (time to live) détermine l'efficacité de ce type d'équilibrage de charge. Elle détermine la période pendant laquelle la réponse résolue reste en mémoire cache sur un autre serveur de noms. Les valeurs TTL peu élevées permettent d'effectuer plus rapidement les modifications subtiles de la charge du serveur ou du réseau. La désactivation de l'enregistrement en mémoire cache oblige toutefois les clients à contacter le serveur de noms autorisé pour chaque demande de résolution de nom, augmentant potentiellement le temps d'attente des clients. Tenez compte de l'impact sur l'environnement de la désactivation de l'enregistrement en mémoire cache lorsque vous choisissez une valeur TTL. Vous devez en outre savoir que l'équilibrage de charge DNS peut être limité par l'enregistrement en mémoire cache côté client de la résolution des noms.

Vous pouvez configurer la durée de vie (TTL) à l'aide de la commande **sscontrol sitename [add | set]** . Pour plus d'informations, reportez-vous à la section «sscontrol sitename — Configuration d'un nom de site» à la page 351.

Utilisation de la fonction de proximité réseau (Network Proximity)

Network proximity correspond au calcul de la position de chaque serveur par rapport au client émettant la demande. Pour déterminer la proximité réseau, l'agent Metric Server (qui doit se trouver sur chaque serveur dont la charge est équilibrée) envoie une commande ping à l'adresse IP client et renvoie le temps de réponse à Site Selector. Site Selector utilise la réponse de proximité dans la décision relative à l'équilibrage de charge. Il combine la valeur de la réponse de proximité réseau avec la pondération provenant du gestionnaire pour créer une valeur de pondération finale pour le serveur.

L'utilisation de la fonction de proximité réseau (Network Proximity) avec Site Selector est facultative.

Site Selector fournit les options de proximité réseau suivantes pouvant être définies par nom de site :

- Durée de stockage en cache : Période pendant laquelle une réponse de proximité restera valide et sera enregistrée dans la mémoire cache.
- Pourcentage de proximité : Importance de la réponse de proximité par rapport à l'état du serveur (en tant qu'entrée de la pondération du gestionnaire).
- Attente de toutes les réponses : Détermine s'il est nécessaire d'attendre toutes les réponses de proximité (ping) des serveurs avant de répondre à la demande du client.

Si cette option est associée à la valeur **oui**, Metric Server envoie une commande ping au client pour obtenir le temps de réponse de proximité. Le serveur de noms attend que tous les serveurs Metric répondent ou que le délai d'expiration se termine. Ensuite, pour chaque serveur, le serveur de noms combine le temps de réponse de proximité avec la pondération que le gestionnaire a calculée pour créer une valeur de "pondération combinée". Site Selector fournira au client l'adresse IP du serveur associée à la meilleure pondération combinée. (Normalement, la plupart des serveurs de noms client observent un dépassement de délai de 5 secondes. Site Selector tente de répondre avant la fin de ce délai.)

Si la valeur est **non**, une résolution de nom sera fournie au client en fonction des pondérations de gestionnaire actuelles. Ensuite, Metric Server envoie une commande ping au client pour obtenir le temps de réponse de proximité. Le serveur de noms met en cache le temps de réponse qu'il reçoit de Metric Server. Lorsque le client renvoie une deuxième requête, le serveur de noms combine la pondération du gestionnaire actuelle avec la valeur de réponse ping mise en cache pour chaque serveur afin d'obtenir le serveur associé à la meilleure "pondération combinée". Site Selector renvoie l'adresse IP de ce serveur au client pour la deuxième requête.

Les options de proximité réseau peuvent être définies dans la commande **sscontrol sitename [add | set]** . Pour de plus amples informations, reportez-vous à «Annexe D. Guide des commandes Site Selector» à la page 327.

Chapitre 11. Configuration du composant Site Selector

Avant d'effectuer les opérations décrites dans le présent chapitre, reportez-vous à la section «Chapitre 10. Planification du composant Site Selector» à la page 109. Ce chapitre décrit comment créer une configuration de base pour le composant Site Selector de Network Dispatcher.

- Pour de plus amples informations sur Network Dispatcher, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Présentation générale des tâches de configuration

Remarque : Avant de suivre les étapes de configuration détaillées dans ce tableau, assurez-vous que la machine Site Selector et toutes les machines serveurs sont connectées au réseau, ont des adresses IP valides et peuvent communiquer entre elles par la triangulation ping.

Tableau 9. Tâches de configuration pour le composant Site Selector

Tâche	Description	Informations connexes
Configuration de la machine Site Selector.	Conditions requises	«Installation de la machine Site Selector» à la page 119
Configuration des machines en vue de l'équilibrage de charge	Installation de la configuration de l'équilibrage de charge.	«Etape 4. Définition de serveurs avec équilibrage de charge» à la page 120

Méthodes de configuration

Il existe quatre méthodes pour créer une configuration de base du composant Site Selector de Network Dispatcher :

- Ligne de commande
- Scripts
- Interface graphique
- Assistant de configuration

Ligne de commande

C'est la méthode la plus directe pour la configuration de Site Selector. Les valeurs des paramètres de commande doivent être saisies en anglais. Les seules exceptions s'appliquent aux noms d'hôte (utilisés dans les commandes site name et server) et aux noms de fichiers.

Pour lancer Site Selector à partir de la ligne de commande :

- Lancez la commande **ssserver** à partir de l'invite.

Remarque : Pour arrêter le service, lancez la commande **ssserver**.

- Ensuite, lancez les commandes de contrôle Site Selector voulues pour installer votre configuration. Les procédures décrites dans ce manuel reposent sur l'utilisation de la ligne de commande. La commande est **sscontrol**. Pour plus de détails sur les commandes, reportez-vous à la section «Annexe D. Guide des commandes Site Selector» à la page 327.

Vous pouvez entrer une version abrégée des paramètres de commandes **sscontrol**. Il suffit d'entrer les lettres spécifiques des paramètres. Par exemple, pour obtenir l'aide correspondant à la commande file save, entrez **sscontrol he f** à la place de **sscontrol help file**.

Pour démarrer l'interface de ligne de commande, entrez **sscontrol** pour ouvrir une invite **sscontrol**.

Pour fermer l'interface de ligne de commande, entrez **exit** ou **quit**.

Remarque : Sous Windows 2000, le service ndserver du composant Dispatcher démarre automatiquement. Si vous utilisez uniquement Site Selector et non le composant Dispatcher, vous pouvez empêcher ndserver de démarrer automatiquement de la manière suivante :

1. Dans la fenêtre Services de Windows 2000, cliquez avec le bouton droit de la souris sur IBM Dispatcher.
2. Sélectionnez Propriétés.
3. Dans la zone **Type de démarrage**, sélectionnez Manuel.
4. Cliquez sur OK et fermez la fenêtre Services.

Scripts

Les commandes permettant de configurer Site Selector peuvent être entrées dans un fichier script de configuration, puis exécutées ensemble.

Remarque : Pour exécuter rapidement le contenu d'un fichier script (par exemple, `mon_script`), utilisez l'une des commandes suivantes :

- Pour mettre à jour la configuration actuelle, soumettez les commandes exécutables à partir du fichier script, en entrant —
sscontrol file appendload *mon_script*
- Pour remplacer la configuration actuelle, soumettez les commandes exécutables à partir du fichier script en entrant —
sscontrol file newload *mon_script*

Interface graphique

Reportez-vous à la section figure 2 à la page 5 pour consulter un exemple de l'interface graphique.

Pour démarrer l'interface graphique, procédez de la manière suivante :

1. Vérifiez que `ssserver` fonctionne. En tant que superutilisateur ou qu'administrateur root, lancez la commande suivante à partir de l'invite **ssserver**.
2. Ensuite, effectuez l'une des opérations suivantes :
 - Sous AIX, Linux ou Solaris : entrez **ndadmin**.
 - Sous Windows 2000 Cliquez sur **Démarrer, Programmes, IBM WebSphere, Edge Server, IBM Network Dispatcher**, puis sur **Network Dispatcher**.

Pour pouvoir configurer le composant Site Selector à partir de l'interface graphique, vous devez d'abord sélectionner **Site Selector** dans l'arborescence. Vous pouvez lancer le gestionnaire une fois que vous vous êtes connecté à un hôte. Vous pouvez également créer des noms de site contenant des ports et des serveurs, puis lancer des conseillers pour le gestionnaire.

Vous pouvez utiliser l'interface graphique pour toute opération normalement exécutée par la commande **sscontrol**. Par exemple, pour définir un nom de site à partir de la ligne de commande, vous devez entrer la commande **sscontrol sitename add** *nom_site*. Pour définir un nom de site à partir de l'interface graphique, cliquez avec le bouton droit de la souris sur Serveur de noms puis, dans le menu en incrustation qui apparaît, cliquez avec le bouton gauche de la souris sur **Ajouter un nom de site**. Entrez le nom du site dans le menu en incrustation, puis cliquez sur **OK**.

Les fichiers de configuration Site Selector existants peuvent être chargés à l'aide des options **Chargement de la nouvelle configuration** (pour remplacer intégralement la configuration en cours) et **Ajout à la configuration en cours** (pour mettre à jour la configuration en cours) du menu en incrustation **Hôte**. Vous devez sauvegarder votre configuration Site Selector dans un fichier en utilisant l'option **Sauvegarder le fichier de configuration en** du menu en incrustation **Hôte**. Le menu **Fichier** situé dans la partie supérieure de l'interface graphique permet de sauvegarder les connexions à l'hôte en cours dans un fichier ou de restaurer des connexions dans des fichiers existants sur tous les composants Network Dispatcher.

Vous pouvez accéder à l'**Aide** en cliquant sur le point d'interrogation situé dans le coin supérieur droit de la fenêtre Network Dispatcher.

- **Aide sur les zones** — décrit les valeurs par défaut de chaque zone.
- **Procédures** — affiche la liste des tâches pouvant être effectuées dans cet écran.
- **Table des matières** — contient toutes les informations d'aide
- **Index** — index alphabétique des rubriques d'aide

Pour plus de détails sur l'utilisation de l'interface graphique, reportez-vous à la section «Instructions générales d'utilisation de l'interface graphique» à la page 6.

Assistant de configuration

Si vous utilisez l'Assistant de configuration, suivez la procédure ci-dessous :

1. Lancez sserver sur Site Selector en entrant **sserver** à partir de l'invite, en tant que superutilisateur ou qu'administrateur root.
2. Lancez la fonction d'assistant de Site Selector, **sswizard**.

Vous pouvez lancer cet assistant à partir de l'invite en entrant la commande **sswizard**, ou sélectionner l'assistant de configuration à partir du menu du composant Site Selector présenté dans l'interface graphique.

L'assistant Site Selector vous guide pas à pas dans le processus de création d'une configuration de base pour le composant Site Selector. Il vous demande des renseignements sur votre réseau et vous guide pour la configuration d'un nom de site permettant à Site Selector d'équilibrer le trafic entre un groupe de serveurs.

L'assistant de configuration Site Selector vous proposera les panneaux suivants :

- Présentation de l'assistant
- Possibilités offertes par l'assistant
- Avant de commencer l'installation

- Choix de l'hôte à configurer (si nécessaire)
- Définition d'un nom de site
- Ajout d'un serveur
- Lancement d'un conseiller
- Définition du voisinage réseau

Installation de la machine Site Selector

L'installation de la machine Site Selector ne peut être effectuée que par le superutilisateur (pour AIX, Linux ou Solaris) ou l'administrateur pour Windows 2000.

Vous aurez besoin d'utiliser un nom d'hôte DNS ne pouvant être résolu comme nom de site pour le groupe de serveurs que vous configurez. Le nom de site est celui utilisé pour les clients pour accéder à votre site (par exemple, www.yourcompany.com). Site Selector équilibrera la charge du trafic pour ce nom de site entre les serveurs du groupe auquel le nom DNS a été attribué.

Etape 1. Démarrage de la fonction serveur

AIX, Linux et Solaris : Pour lancer la fonction serveur, entrez **ssserver**.

Remarque : Un fichier de configuration par défaut (**default.cfg**) est chargé automatiquement pendant le démarrage de **ssserver**. Si vous décidez de sauvegarder la configuration dans **default.cfg**, toutes les données sauvegardées dans ce fichier seront chargées automatiquement au prochain démarrage de **ssserver**.

Etape 2. Démarrage du serveur de noms

Pour démarrer le serveur de noms, entrez la commande **sscontrol nameserver start**.

Vous pouvez également lancer le serveur de noms à l'aide du mot clé **bindaddress** pour établir un lien uniquement avec l'adresse indiquée.

Etape 3. Définition d'un nom de site et définition des options du nom de site

Site Selector équilibrera les demandes envoyées pour le nom de site aux serveurs correspondants configurés pour cela.

Le nom de site est un nom d'hôte ne pouvant être résolu qui sera demandé par le client. Le nom de site doit être un nom de domaine complet (par exemple, www.dnsdownload.com). Lorsqu'un client demande ce nom de site, l'une des adresses IP de serveur associées au nom de site sera renvoyée.

Pour définir un nom de site, lancez la commande suivante :

```
sscontrol sitename add nom_site
```

Pour définir les options du nom de site, lancez la commande suivante :

```
sscontrol sitename set valeur_option_nom_site
```

Pour plus d'informations, reportez-vous à l'«Annexe D. Guide des commandes Site Selector» à la page 327.

Etape 4. Définition de serveurs avec équilibrage de charge

Les serveurs sont les postes qui exécutent les applications dont vous souhaitez équilibrer la charge. Le *serveur* est l'adresse à nom symbolique ou notation décimale de la machine serveur. Pour définir un serveur sur le nom de site défini à l'étape 3, lancez la commande suivante :

```
sscontrol server add  
nom_site:serveur
```

Vous devez définir plusieurs serveurs sous un nom de site afin de permettre l'équilibrage de charge.

Etape 5. Lancement de la fonction gestionnaire (facultatif)

La fonction gestionnaire permet d'améliorer l'équilibrage de charge. Avant de lancer la fonction gestionnaire, vérifiez que le système Metric Server est installé sur toutes les machines dont la charge est équilibrée.

Pour lancer le gestionnaire, tapez la commande suivante :

```
sscontrol manager start
```

Etape 6. Lancement de la fonction conseiller (facultatif)

Les conseillers transmettent au gestionnaire des informations complémentaires sur la capacité à répondre aux demandes des serveurs ayant fait l'objet d'un équilibrage de charge. Chaque conseiller est spécifique à un protocole. La fonction Network Dispatcher fournit de nombreux conseillers. Par exemple, pour lancer le conseiller HTTP pour un nom de site particulier, entrez la commande suivante :

```
sscontrol advisor start http nom_site:port
```

Etape 7. Définition des mesures du système (facultatif)

Pour plus d'informations sur l'utilisation des mesures du système et de Metric Server, reportez-vous à la section «Metric Server» à la page 157.

Etape 8. Définition du niveau d'importance des informations pour le nom de site

Si vous lancez des conseillers, vous pouvez modifier le niveau d'importance donné aux informations fournies par ces derniers (port) et entrant dans les décisions d'équilibrage de la charge. Pour définir le niveau d'importance pour le nom de site, lancez la commande **sscontrol sitename set *nom_site* proportions**. Pour plus d'informations, reportez-vous à la section «Proportion de l'importance accordée aux données d'état» à la page 141.

Configuration des serveurs pour l'équilibrage de la charge

Il est recommandé d'utiliser Metric Server avec le composant Site Selector. Pour plus d'informations sur la configuration de Metric Server sur tous les serveurs dont Site Selecteur assure l'équilibrage de charge, reportez-vous à la section «Metric Server» à la page 157.

Chapitre 12. Planification du composant Consultant for Cisco CSS Switches

Le présent chapitre décrit les aspects que l'administrateur de réseau doit prendre en compte avant d'installer et de configurer le composant Consultant for Cisco CSS Switches.

- Reportez-vous au «Chapitre 13. Configuration du composant Consultant for Cisco CSS Switches» à la page 129, pour obtenir des informations sur la configuration des paramètres d'équilibrage de charge des composants Consultant for Cisco CSS Switches.
- Pour obtenir des informations sur la configuration de Network Dispatcher pour les fonctions avancées, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Le présent chapitre se compose des sections suivantes :

- «Matériel et logiciels requis»
- «Remarques relatives à la planification»

Matériel et logiciels requis

- Pour AIX, reportez-vous à la section «Configuration requise pour AIX» à la page 12
- Pour Linux, reportez-vous à la section «Configuration requise pour Red Hat Linux ou SuSE Linux» à la page 17
- Pour Solaris, reportez-vous à la section «Configuration requise pour Solaris» à la page 20
- Pour Windows 2000, reportez-vous à la section «Configuration requise pour Windows 2000» à la page 22

Remarques relatives à la planification

La configuration de Cisco Consultant dépend de la configuration de Cisco CSS Switch (voir tableau 10 à la page 125). Une fois la planification et la configuration de Cisco CSS Switch terminée, vous pouvez configurer et utiliser Cisco Consultant. Consultez la documentation Cisco CSS Switch pour des instructions relatives à la planification et à la configuration.

Consultant se compose des fonctions suivantes :

- **lbcserver** contient les informations de configuration et interagit avec Cisco CSS Switch. Le préfixe "lbc" signifie load-balancing consultant (consultant d'équilibrage de la charge). lbcserver se compose des éléments suivants :

- l'**exécuteur**, qui détient les informations de configuration ainsi que les informations nécessaires à la connexion à Cisco CSS Switch.
- le **gestionnaire**, qui utilise les informations recueillies pour générer des pondérations et les envoyer à Cisco CSS Switch. Il regroupe des informations à partir
 - de Cisco CSS Switch
 - des serveurs (avec des conseillers).

Les conseillers interrogent les serveurs puis analysent les résultats par protocole avant de demander au gestionnaire de régler les capacités comme il convient. Actuellement, Cisco Consultant fournit entre autres les conseillers suivants : HTTP, FTP, SSL, SMTP, NNTP, IMAP, POP3. Vous avez également la possibilité de développer vos propres conseillers (reportez-vous à la section «Création de conseillers personnalisés» à la page 151). L'utilisation des conseillers est recommandée, mais reste facultative.

- des serveurs (avec Metric Server)

Metric Server fournit à Consultant les informations de téléchargement sous la forme de mesures spécifiques du système, relatives à l'état du serveur. Le gestionnaire interroge les instances Metric Server qui résident sur chaque serveur, et utilise les mesures recueillies à partir des agents pour contribuer à l'attribution de pondérations au processus d'équilibrage de charge. Les résultats sont regroupés dans le rapport du gestionnaire.

- La configuration et la gestion de l'exécuteur, des conseillers et du gestionnaire peuvent être effectuées à partir de l'interface de ligne de commande ou de l'interface graphique.
 - **lbccontrol** est l'interface de ligne de commande de Consultant.
 - **ndadmin** est l'interface utilisateur graphique utilisée pour configurer Consultant et contrôler son statut.

Le gestionnaire recueille des informations provenant de Cisco CSS Switch, des conseillers et de Metric Server. Selon les informations qu'il reçoit, il ajuste la pondération des machines serveur sur chaque port et transmet ces nouvelles données à Cisco CSS Switch qui en tient compte pour l'équilibrage des nouvelles connexions. Lorsque le gestionnaire découvre qu'un serveur est arrêté, il lui associe la pondération zéro et le serveur est interrompu. Par conséquent, Cisco CSS Switch arrête d'acheminer le trafic vers ce serveur.

Les conseillers contrôlent chaque serveur relié au port dont ils ont la charge afin de déterminer leur temps de réponse et leur disponibilité, puis retournent ces informations au gestionnaire. Les conseillers détectent également si un serveur est opérationnel ou non.

Pour que la configuration de Consultant soit correcte, elle doit refléter celle de Cisco CSS Switch. Tout d'abord, reportez-vous au manuel *Cisco Services Switch Getting Started Guide* pour configurer Cisco CSS Switch. Vérifiez que Switch fonctionne correctement et configurez Consultant.

La configuration Cisco CSS Switch se compose de propriétaires, de règles de contenu et de services qui correspondent à une configuration Consultant, comme expliqué dans le tableau ci-dessous.

Tableau 10. Configuration de Consultant et de Cisco CSS Switch

Cisco CSS Switch	Consultant
Adresse IP virtuelle (VIP) d'une ou plusieurs règles de contenu du propriétaire	grappe
port contenu dans la règle de contenu	port
service	serveur

L'arborescence de configuration de Consultant se compose des éléments suivants :

- une *grappe*, qui correspond à un nom pouvant être résolu ou à une adresse à notation décimale à point,
- un *port*, qui correspond au numéro de port que vous utilisez pour ce protocole,
- des *serveurs*.

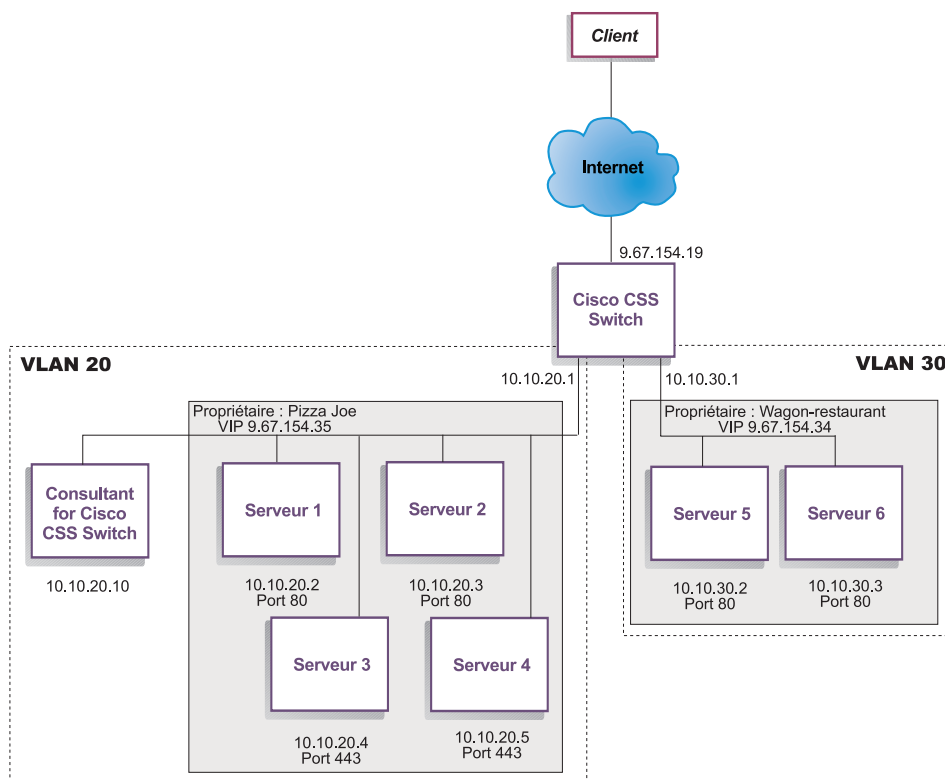


Figure 21. Exemple de composant Consultant configuré avec deux grappes, chacune étant associée à 3 ports

Dans la figure 21 :

- 9.67.154.19 est la connexion réseau vers Internet,
- deux VLANS (20 et 30) sont configurés.

Lors de la configuration de l'exécuteur, vous devez définir une adresse et un nom de communauté SNMP, qui doivent correspondre aux attributs de Cisco CSS Switch. Reportez-vous à la section «lbcontrol executor — Contrôle de l'exécuteur» à la page 365 pour des informations sur la configuration de l'exécuteur.

Tableau 11. Exemple de configuration Cisco CSS Switch en correspondance avec la configuration Consultant

Configuration Cisco CSS Switch	Configuration Consultant
username admin superuser snmp community <i>community</i> private read-write	lbcccontrol executor set address 10.10.20.1 lbcccontrol executor set communityname <i>community</i>
content rule1 port <i>80</i> balance weightedrr add service <i>server1</i> add service <i>server2</i> vip address <i>9.67.154.35</i> activ.	lbcccontrol cluster add <i>9.67.154.35</i> lbcccontrol port add 9.67.154.35: <i>80</i>
content rule 2 protocol tcp port <i>443</i> balance weightedrr add service server3 add service server4 vip address 9.67.154.35 activ.	lbcccontrol port add 9.67.154.35: <i>443</i>
service server1 ip address <i>10.10.20.2</i> port <i>80</i> weight 4 activ.	lbcccontrol server add 9.67.154.35: <i>80</i> :server1 address <i>10.10.20.2</i>
service server3 ip address <i>10.10.20.4</i> port <i>443</i> weight 4 activ.	lbcccontrol server add 9.67.154.35: <i>443</i> :server3 address <i>10.10.20.4</i>

Chapitre 13. Configuration du composant Consultant for Cisco CSS Switches

Avant d'effectuer les opérations décrites dans le présent chapitre, reportez-vous à la section «Chapitre 12. Planification du composant Consultant for Cisco CSS Switches» à la page 123. Ce chapitre décrit comment créer une configuration de base pour le composant Consultant for Cisco CSS Switches d'Network Dispatcher.

- Pour de plus amples informations sur Network Dispatcher, reportez-vous à la section «Chapitre 14. Fonctions Network Dispatcher avancées» à la page 137.
- Reportez-vous au «Chapitre 15. Exploitation et gestion de Network Dispatcher» à la page 213, pour obtenir des informations sur l'administration authentifiée à distance, les fichiers journaux Network Dispatcher et sur l'utilisation des composants Network Dispatcher.

Présentation générale des tâches de configuration

Avant de suivre une des méthodes de configuration décrites dans ce chapitre :

1. Assurez-vous que Cisco CSS Switch et que tous les serveurs sont correctement configurés.
2. Configurez Cisco Consultant, en vérifiant que l'adresse de l'exécuteur et le nom de la communauté correspondent aux attributs équivalents de Cisco CSS Switch. Pour obtenir plus d'informations sur la configuration de l'exécuteur, reportez-vous à la section «lbcontrol executor — Contrôle de l'exécuteur» à la page 365.

Tableau 12. Tâches de configuration du composant Consultant for Cisco CSS Switches

Tâche	Description	Informations connexes
Configuration de la machine Consultant for Cisco CSS Switches	Conditions requises	«Installation de la machine Consultant for Cisco CSS Switches» à la page 132
Test de la configuration	Confirmation du bon fonctionnement de la configuration	«Test de vérification de la configuration» à la page 135

Méthodes de configuration

Pour créer une configuration de base pour le composant Consultant for Cisco CSS Switches de Network Dispatcher, il existe trois méthodes :

- Ligne de commande
- Scripts
- Interface graphique

Ligne de commande

C'est la méthode la plus directe pour la configuration de Cisco Consultant. Les procédures décrites dans ce manuel reposent sur l'utilisation de la ligne de commande. Les valeurs des paramètres de commande doivent être saisies en anglais. Les seules exceptions s'appliquent aux noms d'hôte (utilisés dans les commandes cluster et server) et aux noms de fichiers.

Pour lancer Cisco Consultant à partir de la ligne de commande :

- Lancez la commande **lbserver** à partir de l'invite.

Remarque : Pour arrêter le service, lancez la commande suivante :
lbserver stop.

- Lancez ensuite les commandes de contrôle Cisco Consultant voulues pour définir votre configuration. La commande est **lbcontrol**. Pour plus de détails sur les commandes, reportez-vous à la section «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257.

Vous pouvez entrer une version abrégée des paramètres de contrôle lbcontrol. Il suffit d'entrer les lettres spécifiques des paramètres. Par exemple, pour l'aide correspondant à la commande file save, entrez **lbcontrol he f** à la place de **lbcontrol help file**.

Pour démarrer l'interface de ligne de commande, entrez **lbcontrol** pour obtenir une invite lbcontrol.

Pour fermer l'interface de ligne de commande, entrez **exit** ou **quit**.

Remarque : Sous Windows 2000, le service ndserver du composant Dispatcher démarre automatiquement. Si vous utilisez uniquement Cisco Consultant et non le composant Dispatcher, vous pouvez empêcher ndserver de démarrer automatiquement de la manière suivante :

1. Dans la fenêtre Services de Windows 2000, cliquez avec le bouton droit de la souris sur IBM Dispatcher.
2. Sélectionnez Propriétés.

3. Dans la zone **Type de démarrage**, sélectionnez Manuel.
4. Cliquez sur OK et fermez la fenêtre Services.

Scripts

Les commandes permettant de configurer Consultant for Cisco CSS Switches peuvent être entrées dans un fichier script de configuration puis exécutées ensemble.

Remarque : Pour exécuter rapidement le contenu d'un fichier script (par exemple, *monscript*), utilisez une des commandes suivantes :

- Pour mettre à jour la configuration actuelle, soumettez les commandes exécutables à partir du fichier script, en entrant —
lbcontrol file appendload monscript
- Pour remplacer la configuration actuelle, soumettez les commandes exécutables à partir du fichier script en entrant —
lbcontrol file newload monscript

Interface graphique

Pour avoir un exemple de l'interface graphique, reportez-vous à la section figure 2 à la page 5.

Pour démarrer l'interface graphique, procédez de la manière suivante :

1. Si lbcsrvr n'est pas déjà en cours d'exécution, lancez-le maintenant à l'aide de la commande indiquée ci-après. Pour effectuer cette opération, vous devez disposer des droits root.

lbcsrvr.

2. Ensuite, effectuez l'une des opérations suivantes :
 - Sous AIX, Linux ou Solaris : entrez **ndadmin**.
 - Pour Windows 2000 : cliquez sur **Démarrer, Programmes, IBM WebSphere, Edge Server, IBM Network Dispatcher, Network Dispatcher**

Pour configurer le composant Cisco Consultant à partir de l'interface graphique :

1. Cliquez avec le bouton droit de la souris sur Cisco Consultant dans l'arborescence
2. Connectez-vous à un hôte
3. Créez des grappes contenant des ports et des serveurs
4. Lancez le gestionnaire
5. Lancez les conseillers du gestionnaire

Vous pouvez utiliser l'interface graphique pour toute opération effectuée via la commande **lbcontrol**. Par exemple, pour définir une grappe à l'aide de la ligne de commande, vous devez entrer la commande **lbcontrol cluster add cluster**. Pour définir une grappe à partir de l'interface graphique, cliquez avec le bouton droit de la souris sur Exécuteur, puis cliquez sur **Ajouter une grappe**. Entrez l'adresse de la grappe dans la fenêtre en incrustation, puis cliquez sur **OK**.

Vous pouvez utiliser les options **Charger la nouvelle configuration** (pour le remplacement total de la configuration en cours) et **Ajouter à la configuration en cours** (pour la mise à jour de la configuration en cours) se trouvant dans le menu en incrustation **Hôte** afin de charger les fichiers de configuration Cisco Consultant pré-existants. Sélectionnez l'option **Sauvegarder le fichier de configuration en** pour sauvegarder de façon régulière la configuration Cisco Consultant dans un fichier. Cliquez sur **Fichier** dans la barre de menus afin de sauvegarder les connexions à l'hôte en cours dans un fichier ou de restaurer les connexions dans des fichiers existants sur tous les composants Network Dispatcher.

Pour accéder à l'**aide**, cliquez sur l'icône en forme de point d'interrogation située dans le coin supérieur droit de la fenêtre Network Dispatcher.

- **Aide sur les zones** — décrit les valeurs par défaut de chaque zone.
- **Procédures** — affiche la liste des tâches pouvant être effectuées dans cet écran.
- **Table des matières** — contient toutes les informations d'aide
- **Index** — index alphabétique des rubriques d'aide

Pour plus de détails sur l'utilisation de l'interface graphique, reportez-vous à la section «Instructions générales d'utilisation de l'interface graphique» à la page 6.

Installation de la machine Consultant for Cisco CSS Switches

L'installation de la machine Consultant for Cisco CSS Switches ne peut être effectuée que par l'utilisateur root (pour AIX, Linux ou Solaris) ou l'administrateur sous Windows 2000.

Consultant doit pouvoir se connecter à Cisco CSS Switch en tant qu'administrateur Cisco CSS Switch.

Lors de la configuration de l'exécuteur, vous devez configurer une adresse et un nom de communauté SNMP, qui doivent correspondre aux attributs sur Cisco CSS Switch.

Pour obtenir une aide sur les commandes utilisées lors de cette procédure, reportez-vous à l'«Annexe E. Guide des commandes Consultant for Cisco CSS Switches» à la page 357.

Etape 1. Lancement de la fonction serveur

Si `lbcsrvr` n'est pas déjà en cours d'exécution, lancez-le maintenant à l'aide de la commande indiquée ci-après. Pour effectuer cette opération, vous devez disposer des droits root.

`lbcsrvr`

Etape 2. Configuration de la fonction exécuteur

Vous devez configurer une adresse et un nom de communauté SNMP. Ces valeurs doivent correspondre aux attributs équivalents sur Cisco CSS Switch.

Etape 3. Définition d'une grappe et des options de grappe

Une *grappe* est un nom pouvant être résolu ou une adresse à notation décimale à point. La grappe correspond à l'adresse IP virtuelle de Cisco CSS Switch d'une règle de contenu de propriétaire.

Pour définir une grappe, entrez `lbccntrol cluster add grappe`. Pour définir les options de grappe, entrez `lbccntrol cluster set`.

Etape 4. Définition de ports et des options de port

Pour définir un port, entrez `lbccntrol port add grappe:port`. Le port correspond au port configuré dans la règle de contenu Cisco CSS Switch pour le propriétaire.

Port est le numéro du port que vous utilisez pour ce protocole comme il est indiqué dans la règle de contenu du propriétaire pour Cisco CSS Switch. Pour de plus amples informations, reportez-vous à la section «`lbccntrol port` — Configuration des ports» à la page 380.

Etape 5. Définition des serveurs avec équilibrage de charge

Vous pouvez configurer plusieurs instances du même serveur dans une grappe et un port. (N'oubliez pas que l'adresse et le nom de la communauté SNMP doivent correspondre aux attributs équivalents de Cisco CSS Switch.) Lorsque vous configurez plusieurs instances sur le même serveur, vous pouvez faire la différence entre plusieurs serveurs d'applications qui se trouvent sur la même machine physique et répondent à la même adresse IP sur le même port.

Pour définir un serveur avec équilibrage de charge, entrez :

`lbccntrol server add grappe:port:serveur address x.x.x.x | nomhôte`

Le *serveur* correspond au nom du service Cisco CSS Switch.

Pour effectuer l'équilibrage de charge, vous devez définir plusieurs serveurs sur un port d'une grappe ou le trafic ne sera dirigé que vers un seul serveur. Reportez-vous à la rubrique «Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)» à la page 159.

Pour plus d'informations sur la syntaxe de la commande `lbcontrol`, reportez-vous à la rubrique «`lbcontrol server` — Configuration des serveurs» à la page 382.

Etape 6. Lancement de la fonction gestionnaire

Pour lancer le gestionnaire, entrez la commande `lbcontrol manager start`. Pour de plus amples informations, reportez-vous à la section «`lbcontrol manager` — Contrôle du gestionnaire» à la page 372.

Etape 7. Lancement de la fonction conseiller (facultatif)

Les conseillers transmettent au gestionnaire des informations complémentaires sur la capacité des serveur bénéficiant de l'équilibrage de charge à répondre aux demandes. Chaque conseiller est spécifique à un protocole. Par exemple, tapez la commande suivante pour lancer le conseiller HTTP :

```
lbcontrol advisor start http port
```

Pour consulter la liste des conseillers et des ports par défaut correspondants, reportez-vous à la section «`lbcontrol advisor` — Contrôle du conseiller» à la page 358. Pour lire la description de chaque conseiller, reportez-vous à la section «Liste des conseillers» à la page 149.

Etape 8. Définition du niveau d'importance des informations de la grappe

Si vous lancez un conseiller, vous devez modifier le niveau d'importances des informations de la grappe afin que ces dernières soient incluses dans les décisions d'équilibrage de charge. Utilisez la commande `lbcontrol cluster proportions`. Reportez-vous à la section «Proportion de l'importance accordée aux données d'état» à la page 141.

Remarque : Si vous lancez un conseiller et que le **niveau d'importance attribué aux mesures système** est 0, la valeur 1 doit être soustraite. Etant donné que la somme totale doit être égale à 100, la valeur 1 est soustraite du niveau d'importance ayant la valeur la plus élevée.

Etape 9. Lancement du système Metric Server (facultatif)

Pour obtenir plus d'informations sur Metric Server, reportez-vous à la section «Metric Server» à la page 157.

Test de vérification de la configuration

Vérifiez que la configuration fonctionne.

1. Attribuez la valeur 4 au niveau de journalisation du gestionnaire.
2. Déconnectez un serveur de Cisco CSS Switch pendant une minute *ou* arrêtez le serveur d'applications pendant une minute.
3. Reconnectez le serveur ou lancez à nouveau le serveur d'applications.
4. Attribuez à nouveau le niveau désiré (1) au niveau de journalisation du gestionnaire.
5. Affichez le fichier manager.log se trouvant dans le répertoire .../nd/servers/logs/lbc et cherchez le **service de définition setServerWeights**.

Chapitre 14. Fonctions Network Dispatcher avancées

Le présent chapitre explique comment configurer les paramètres d'équilibrage de charge de Network Dispatcher et comment configurer les fonctions avancées de Network Dispatcher.

Remarque : Lors de la lecture de ce chapitre, si vous n'utilisez *pas* le composant Dispatcher, remplacez "ndcontrol" par l'élément suivant :

- Pour CBR, utilisez **cbrcontrol**
- Pour Mailbox Locator, utilisez **mlcontrol**
- Pour Site Selector, utilisez **sscontrol** (Reportez-vous à l'«Annexe D. Guide des commandes Site Selector» à la page 327)
- Pour Cisco Consultant, utilisez **lbcontrol** (Reportez-vous à l'«Annexe E. Guide des commandes Consultant for Cisco CSS Switches» à la page 357)

Tableau 13. Tâches de configuration avancées pour Network Dispatcher

Tâche	Description	Informations connexes
Modification des paramètres de l'équilibrage de charge	<p>Les paramètres d'équilibrage de charge suivants peuvent être modifiés :</p> <ul style="list-style-type: none">• Proportion de l'importance accordée aux données d'état. Le rapport par défaut est 50-50-0-0. Si vous utilisez la valeur par défaut, les informations fournies par les conseillers et par le système Metric Server ne sont pas exploitées.• Pondérations• Pondérations fixées par l'administrateur• Intervalles gestionnaire• Seuil de sensibilité• Index de filtrage	«Optimisation de la fonction d'équilibrage de charge fournie par Network Dispatcher» à la page 140

Tableau 13. Tâches de configuration avancées pour Network Dispatcher (suite)

Tâche	Description	Informations connexes
Utilisation des scripts pour la génération d'une alerte ou d'une erreur du serveur d'enregistrement lorsque le gestionnaire indique si le serveur est actif ou non	Network Dispatcher fournit des exits utilisateur qui déclenchent des scripts que vous pouvez personnaliser lorsque le gestionnaire indique si le serveur est actif ou non	«Utilisation de scripts pour la génération d'une alerte ou d'une erreur du serveur d'enregistrement» à la page 145
Utilisation des conseillers et création de conseillers personnalisés	Décrit les conseillers ainsi que le mode de développement de vos propres conseillers pour reporter les états spécifiques des serveurs	«Conseillers» à la page 146 «Création de conseillers personnalisés» à la page 151
Utilisation du conseiller WLM (Workload Manager)	Le conseiller WLM fournit des informations de chargement à Network Dispatcher	«Conseiller Workload Manager» à la page 155
Utilisation de l'agent Metric Server	Le système Metric Server fournit des informations de chargement à Network Dispatcher	«Metric Server» à la page 157
Utilisation du partitionnement du serveur	Définit les serveurs logique devant distribuer la charge en fonction de services fournis	«Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)» à la page 159
Utilisation de l'option demande/réponse (URL)	Définit une chaîne HTTP URL client unique propre à un service que vous voulez demander sur la machine	«Option de demande/réponse (URL) de conseiller HTTP» à la page 161
Placement de Network Dispatcher sur une machine d'équilibrage de charge	Configure une machine Network Dispatcher co-implanté.	«Utilisation de serveurs implantés au même endroit» à la page 162
Configuration du support de réseau étendu pour Dispatcher	Installe une machine Dispatcher éloignée pour l'équilibrage de charge sur un réseau étendu. Ou effectue l'équilibrage de charge dans un réseau étendu (sans Dispatcher éloigné) à l'aide d'une plate-forme de serveur prenant en charge GRE.	«Configuration du support de réseau étendu pour Dispatcher» à la page 164
Configuration de la haute disponibilité ou de la haute disponibilité réciproque	Installe une deuxième machine Dispatcher comme répartiteur de secours.	«Haute disponibilité» à la page 173
Configuration d'un équilibrage de charge basé sur des règles	Définition des conditions sous lesquelles un sous-ensemble donné de serveurs est utilisé.	«Configuration de l'équilibrage basé sur des règles» à la page 180
Utilisation de liens explicites	Évitez d'ignorer Dispatcher dans vos liens.	«Utilisation de liens explicites» à la page 191

Tableau 13. Tâches de configuration avancées pour Network Dispatcher (suite)

Tâche	Description	Informations connexes
Utilisation d'un réseau privé	Configurez le répartiteur (Dispatcher) pour qu'il assure l'équilibrage de charge des serveurs sur un réseau privé.	«Utilisation d'une configuration réseau privée» à la page 191
Utilisation d'une grappe générique pour combiner des configurations serveur communes	Les adresses non explicitement configurées utiliseront la grappe générique pour équilibrer le trafic.	«Utilisation d'une grappe générique pour combiner les configurations serveurs» à la page 193
Utilisation d'une grappe générique pour équilibrer la charge des pare-feux.	La totalité du trafic sera équilibré sur les pare-feux.	«Utilisation de la grappe générique pour équilibrer la charge des pare-feux» à la page 193
Utilisation d'une grappe générique avec Caching Proxy pour le proxy transparent	Permet d'utiliser Dispatcher pour activer un proxy transparent.	«Utilisation de grappe générique avec Caching Proxy pour le proxy transparent» à la page 194
Utilisation du port générique pour acheminer le trafic destiné à un port non configuré	Prend en charge le trafic qui n'est configuré pour aucun port particulier.	«Utilisation du port générique pour acheminer le trafic destiné à un port non configuré» à la page 195
Utilisation de la fonction de maintien de routage pour fidéliser un port de grappe.	Permet aux demandes clients d'être acheminées vers le même serveur.	«Fonctionnement de la fonction d'affinité pour Network Dispatcher» à la page 195
Utilisation de l'API SDA (Server Directed Affinity)	Fournit un API qui permet à un agent externe d'influencer le comportement de l'affinité Dispatcher.	«API SDA pour le contrôle de l'affinité client/serveur» à la page 196
Utilisation de l'affinité trans ports pour étendre la fonction de maintien de routage (affinité) aux autres ports.	Permet aux demandes clients reçues par des ports différents d'être dirigées vers le même serveur.	«Affinité trans ports» à la page 197
Utilisation du masque d'adresse d'affinité pour désigner une adresse de sous-réseau IP commune.	Permet aux demandes clients reçues par le même sous-réseau d'être dirigées vers un même serveur.	«Masque d'adresse de l'affinité» à la page 198
Utilisation de la substitution d'affinité de règle pour fournir au serveur un dispositif de remplacement de la fonction de maintien de routage de port.	Permet à un serveur de remplacer sur son port les paramètres de maintien de routage.	«Substitution d'affinité de règle» à la page 199

Tableau 13. Tâches de configuration avancées pour Network Dispatcher (suite)

Tâche	Description	Informations connexes
Utilisation de l'affinité de cookie actif pour l'équilibrage de charge des serveurs pour le composant CBR	Option de règle permettant de conserver l'affinité pour un serveur particulier.	«Affinité de cookie actif» à la page 200
Utilisation de l'affinité de cookie pour le routage en fonction du contenu de Dispatcher et le composant CBR	Option de règle permettant de conserver l'affinité pour un serveur particulier en fonction de la valeur nom du cookie/cookie.	«Affinité de cookie passif» à la page 202
Utilisation de l'affinité d'URI pour effectuer l'équilibrage de charge au sein des serveurs Caching avec un contenu unique à placer en mémoire cache sur chaque serveur	Option de règle permettant de conserver l'affinité pour un serveur particulier en fonction de l'URI.	«Affinité d'URI» à la page 203
Utilisation de la détection de "refus de service" pour indiquer aux administrateurs (via une alerte) des attaques éventuelles	Dispatcher analyse les demandes entrantes d'un certain nombre de connexions partielles sur les serveurs.	«Détection d'attaque de refus de service» à la page 204
Utilisation de la journalisation binaire pour analyser les statistiques des serveurs.	Permet d'enregistrer les informations sur les serveurs dans des fichiers binaires et d'extraire ces informations.	«Utilisation de la journalisation binaire pour analyser les statistiques des serveurs» à la page 205
Utilisation de Cisco Consultant (informations supplémentaires)	Interaction de Cisco Consultant avec Cisco CSS Switch et informations supplémentaires sur la configuration des pondérations.	«Informations supplémentaires sur les fonctions Cisco Consultant avancées» à la page 208

Optimisation de la fonction d'équilibrage de charge fournie par Network Dispatcher

La fonction gestionnaire de Network Dispatcher effectue l'équilibrage de charge en fonction des paramètres suivants :

- «Proportion de l'importance accordée aux données d'état» à la page 141
- «Pondérations» à la page 142
- «Intervalles gestionnaire» à la page 144
- «Intervalles conseiller» à la page 148
- «Délai de rapport du conseiller» à la page 148
- «Seuil de sensibilité» à la page 144
- «Index de filtrage» à la page 145

Tous ces paramètres peuvent être modifiés en vue d'optimiser l'équilibrage de la charge du réseau.

Proportion de l'importance accordée aux données d'état

Le gestionnaire peut utiliser certains ou l'ensembles de facteurs externes suivants pour les décisions de pondération :

- *Connexions actives* : Nombre de connexions actives sur chaque serveur d'équilibrage de charge (indiqué par l'exécuteur). Cette proportion ne s'applique pas à Site Selector.

ou —

Unité centrale : Pourcentage de l'unité centrale utilisé sur chaque serveur d'équilibrage de charge (entrée à partir de l'agent Metric Server). Pour Site Selector uniquement, cette proportion apparaît à la place de la colonne de la proportion des connexions actives.

- *Nouvelles connexions* : Nombre de nouvelles connexion sur chaque serveur d'équilibrage de charge (indiqué par l'exécuteur). Cette proportion ne s'applique pas à Site Selector.

ou —

Mémoire : Pourcentage de mémoire utilisé (entrée à partir de l'agent Metric Server) sur chaque serveur d'équilibrage de charge. Pour Site Selector uniquement, cette proportion apparaît à la place de la colonne de la proportion des nouvelles connexions.

- *Spécifique au port* : Entrée effectuée par les conseillers écoutant au niveau de ce port.
- *Mesure système* : Entrées provenant des outils de contrôle système, tels que Metric Server ou WLM.

Outre la charge courante de chaque serveur et d'autres données nécessaires à ses calculs, le gestionnaire obtient les deux premières valeurs (nouvelles connexions et connexions actives) de la part de l'exécuteur. Ces valeurs dépendent de données générées et stockées en interne par l'exécuteur.

Remarque : Pour Site Selector, le gestionnaire extrait les deux premières valeurs (unité centrale et mémoire) de Metric Server. Pour Cisco Consultant, le gestionnaire extrait les deux premières valeurs (connexions actives et nouvelles connexions) de Cisco CSS Switch.

Vous pouvez modifier la proportion d'importance relative des quatre valeurs sur la base d'une grappe (ou nom de site). Les proportions correspondent à des pourcentages ; la somme des proportions relatives est égale à 100%. Le ratio par défaut est 50/50/0/0, ce qui revient à ignorer les informations système et celles transmises par les conseillers. Dans votre environnement,

vous serez amené à essayer différentes combinaisons de proportions pour déterminer celle qui offre les meilleures performances.

Remarque : Lorsque vous ajoutez un conseiller (autre que WLM), si la **proportion du port** est égal à zéro, le gestionnaire ajoute 1 à cette valeur. Etant donné que la somme des proportions relatives doit être égale à 100, la valeur 1 est soustraite de la valeur la plus élevée.

Lorsque vous ajoutez le conseiller WLM, si la **proportion de la mesure système** est égale à zéro, le gestionnaire ajoute alors 1 à cette valeur. Etant donné que la somme des proportions relatives doit être égale à 1, la valeur 1 est soustraite de la valeur la plus élevée.

Le nombre de connexions actives dépend du nombre de clients ainsi que du délai nécessaire pour accéder aux services offerts par les machines serveurs d'équilibrage de charge. Si les connexions client sont rapides (comme dans le cas de courtes pages Web obtenues par HTTP GET), le nombre de connexions actives sera faible. Si les connexions client sont lentes (comme dans le cas de requêtes de base de données), le nombre de connexions actives sera plus élevé.

Il est recommandé de ne pas attribuer des valeurs trop basses aux nouvelles connexions et aux connexions actives. Si la valeur 20 (au moins) n'est pas attribuée aux deux première valeurs, vous désactivez l'équilibrage de charge et le lissage du Dispatcher.

Pour définir la proportion des valeurs d'importance, utilisez la commande **ndcontrol cluster set grappe proportions**. Pour de plus amples informations, reportez-vous à la section «ndcontrol cluster — Configuration des grappes» à la page 266.

Pondérations

Remarque : Si vous utilisez le composant Cisco Consultant, reportez-vous à la section «Pondérations de Cisco Consultant» à la page 209 pour obtenir plus d'informations.

Les pondérations sont définies par le gestionnaire en fonction des décomptes internes de l'exécuteur, du retour d'informations des conseillers et du retour d'informations procuré par un programme de contrôle système, tel que Metric Server. Si vous voulez définir des pondérations manuellement lors de l'exécution du gestionnaire, indiquez l'option `fixedweight` lors de l'exécution

de la commande `ndcontrol server`. Pour obtenir une description de l'option `fixedweight`, reportez-vous à la section «Pondérations fixées par le gestionnaire».

Les pondérations définies s'appliquent à tous les serveurs connectés sur un même port. Pour chaque port, les demandes seront réparties entre les serveurs selon la pondération relative de chacun. Par exemple, si un serveur a une pondération (paramètre `Weight`) de 10 et un autre de 5, le premier recevra deux fois plus de demandes que le second.

Pour définir pondération maximale d'un serveur, entrez la commande **`ndcontrol port set weightbound`**. Cette commande intervient sur l'écart existant entre les serveurs au niveau du nombre de demandes reçues par chacun. Si la pondération maximale est de 1, tous les serveurs peuvent avoir une pondération égale à 1, 0 en veille, ou -1 si désactivé. A mesure que cette valeur augmente, l'écart entre les pondérations des serveurs augmente également. Avec une pondération maximale de 2, un serveur donné pourra recevoir deux fois plus de demandes qu'un autre. Avec une pondération maximale de 10, un serveur donné pourra recevoir dix fois plus de demandes qu'un autre. La pondération maximale par défaut est de 20.

Si un conseiller détecte la défaillance d'un serveur, il en informe le gestionnaire qui attribue au serveur une pondération de zéro. Ainsi, l'exécuteur n'enverra pas de nouvelles connexions à ce serveur tant que cette pondération restera égale à zéro. Si ce serveur disposait d'une ou plusieurs connexions avant la modification de sa pondération, les connexions pourront toutefois s'achever normalement.

Pondérations fixées par le gestionnaire

Sans le gestionnaire, les conseillers ne peuvent pas être lancés ni détecter les pannes de serveur. Si vous choisissez de lancer les conseillers mais ne voulez *pas* que le gestionnaire mette à jour la pondération que vous fixée pour un serveur particulier, utilisez l'option **`fixedweight`** de la commande de serveur `ndcontrol`. Par exemple :

```
ndcontrol server set  
grappe:port:serveur fixedweight yes
```

Une fois la valeur `yes` attribuée à l'option `fixedweight`, utilisez la commande **`ndcontrol server set weight`** pour attribuer la valeur souhaitée à la pondération. La valeur de pondération du serveur reste fixe tant que le gestionnaire est en activité à moins que vous n'émettiez une commande `ndcontrol` en attribuant la valeur `no` à l'option `fixedweight`. Pour obtenir plus d'informations, reportez-vous à la section «`ndcontrol server` — Configuration des serveurs» à la page 311.

Intervalles gestionnaire

Pour optimiser les performances générales du réseau, la fréquence des interactions entre le gestionnaire et l'exécuteur est limitée. Pour modifier cet intervalle d'interaction, entrez les commandes **ndcontrol manager interval** et **ndcontrol manager refresh**.

L'intervalle gestionnaire indique la fréquence selon laquelle le gestionnaire réactualise les pondérations des serveurs utilisés par l'exécuteur pour acheminer les connexions. Si l'intervalle gestionnaire est trop court, le gestionnaire interrompra l'exécuteur constamment et les performances déclineront. Dans le cas contraire, le routage des demandes assuré par l'exécuteur reposera sur des informations anciennes et incertaines.

Par exemple, pour définir un intervalle gestionnaire d'une seconde, entrez la commande suivante :

```
ndcontrol manager interval 1
```

Le seuil de régénération du gestionnaire détermine la fréquence selon laquelle le gestionnaire demande des données d'état à l'exécuteur. Le seuil de régénération dépend de la durée de l'intervalle.

Par exemple, pour fixer à 3 intervalles le seuil de régénération du gestionnaire, entrez la commande suivante :

```
ndcontrol  
manager refresh 3
```

Après cette commande, le gestionnaire devra patienter 3 intervalles avant de demander des données d'état à l'exécuteur.

Seuil de sensibilité

Network Dispatcher offre d'autres méthodes d'optimisation de l'équilibrage de charge des serveurs. Pour fonctionner en vitesse maximale, les pondérations des serveurs ne sont actualisées que si les pondérations ont évolué de manière significative. La mise à jour constante des pondérations pour un écart mineur de l'état des serveurs induirait un surcroît d'activité injustifié. Lorsque, pour tous les serveurs d'un port donné, l'écart en pourcentage de la pondération totale dépasse le seuil de sensibilité, le gestionnaire réactualise les pondérations des serveurs utilisés par l'exécuteur pour répartir les connexions. Supposons par exemple que la pondération totale passe de 100 à 105. L'écart est de 5%. Avec un seuil de sensibilité par défaut de 5, le gestionnaire ne met pas à jour les pondérations utilisées par l'exécuteur, car l'écart en pourcentage n'est pas **supérieur** au seuil. Si, en revanche la pondération totale passe de 100 à 106, le gestionnaire met à jour les pondérations.

Pour attribuer au seuil de sensibilité du gestionnaire une valeur autre que la valeur par défaut (par exemple, 6), entrez la commande suivante :

```
ndcontrol manager sensitivity 6
```

Dans la plupart des cas, vous n'aurez pas besoin de modifier cette valeur.

Index de filtrage

Le gestionnaire calcule dynamiquement les pondérations des serveurs. Il en découle qu'une fois mise à jour, une nouvelle pondération peut être très différente de l'ancienne. Dans la plupart des cas, cela ne porte pas à conséquence. Cependant, cela peut parfois induire de fortes variations dans la manière dont l'équilibrage de charge est effectué pour les demandes. Par exemple, l'un des serveurs peut finir par réceptionner la plupart des demandes du fait d'une pondération élevée. Le gestionnaire s'apercevra alors que le serveur en question traite un nombre élevé de connexions et répond lentement. Il transposera alors la pondération sur des serveurs moins encombrés et le même phénomène se reproduira, induisant une exploitation improductive des ressources.

Pour corriger ce dysfonctionnement, le gestionnaire utilise un index de filtrage. L'index de filtrage limite l'écart de pondération d'un serveur, filtrant et uniformisant effectivement la variation dans la répartition des demandes. Plus l'index de filtrage sera élevé, moins les pondérations des serveurs varieront. Plus l'index de filtrage sera faible, plus les pondérations des serveurs changeront. La valeur par défaut de l'index de filtrage est de 1,5. Avec un index de 1,5, les pondérations des serveurs seront plutôt fluctuantes. Pour un index de 4 ou 5, ces pondérations seront plus constantes. Par exemple, pour fixer l'index de filtrage à 4, entrez la commande suivante :

```
ndcontrol  
manager smoothing 4
```

Dans la plupart des cas, vous n'aurez pas besoin de modifier cette valeur.

Utilisation de scripts pour la génération d'une alerte ou d'une erreur du serveur d'enregistrement

Network Dispatcher fournit des exits utilisateur qui déclenchent des scripts que vous pouvez personnaliser. Vous pouvez créer des scripts afin d'effectuer des actions automatisées. Il est, par exemple, possible de prévenir un administrateur lorsque le gestionnaire indique qu'un serveur est inactif ou simplement d'enregistrer l'erreur. Des scripts exemples, qu'il est possible de personnaliser, se trouvent dans le répertoire d'installation **...nd/servers/samples**. Afin d'exécuter les fichiers, vous devez les déplacer dans le répertoire **...nd/servers/bin** et supprimer l'extension de fichier ".sample". Les scripts exemples suivants sont fournis :

- **serverDown** — le gestionnaire indique qu'un serveur est inactif.
- **serverUp** — le gestionnaire indique qu'un serveur est à nouveau actif.

- **managerAlert** — il est indiqué que tous les serveurs d'un port particulier sont inactifs.
- **managerClear** — au moins un serveur est à nouveau disponible actif après qu'il a été indiqué que tous les serveurs étaient inactifs pour un port particulier.

Conseillers

Les conseillers sont des agents de Network Dispatcher. Ils ont pour rôle d'évaluer l'état et la charge des serveurs. Ils effectuent cette tâche via un échange proactif de type client/serveur. Les conseillers peuvent être considérés comme des clients des serveurs d'application.

Le produit fournit plusieurs conseillers pour les protocoles les plus couramment utilisés. Cependant, l'utilisation de tous les conseillers fournis avec chaque composant de Network Dispatcher ne présente aucun intérêt. (Par exemple, vous ne pouvez pas utiliser le conseiller Telnet avec le composant CBR.) Network Dispatcher prend également en charge le concept de «conseiller personnalisé» permettant aux utilisateurs d'écrire leurs propres conseillers.

Restriction affectant les applications serveur de liaison sous Linux : Sous Linux, Network Dispatcher ne permet pas l'utilisation de conseillers lors de l'équilibrage de la charge des serveurs de liaison (autres composants Network Dispatcher tels que Mailbox Locator ou Site Selector compris) lorsqu'ils sont reliés à l'adresse IP de la grappe.

Fonctionnement des conseillers

Les conseillers ouvrent régulièrement une connexion TCP avec chaque serveur et envoient un message de demande au serveur. Le contenu du message dépend du protocole exécuté sur le serveur. Par exemple, le conseiller HTTP envoie une demande HTTP «HEAD» au serveur.

Les conseillers attendent ensuite une réponse du serveur. Une fois la réponse obtenue, le conseiller évalue l'état du serveur. Pour calculer la valeur de la «charge», la plupart des conseillers mesurent le délai de réponse du serveur, puis ils utilisent cette valeur (en millisecondes) comme valeur de charge.

Le conseiller reporte cette valeur au gestionnaire. Elle apparaît dans le rapport du gestionnaire, dans la colonne «Port». Le gestionnaire calcule ensuite un ensemble de valeurs de pondération à partir de toutes ses sources, selon les proportions, et définit ces valeurs de pondération dans la fonction exécuteur. L'exécuteur utilise ces pondérations pour équilibrer la charge des nouvelles connexions client entrantes.

Si le conseiller détermine que le serveur est actif et que son état est correct, il renvoie au gestionnaire une valeur de charge positive non nulle. Si le conseiller détermine que le serveur n'est pas actif, il renvoie une valeur de charge spéciale négative (-1). Le gestionnaire et l'exécuteur n'enverront plus aucune connexion en direction de ce serveur.

Lancement et arrêt d'un conseiller

Vous pouvez lancer un conseiller pour un port particulier de toutes les grappes (conseiller de groupe). Vous pouvez également choisir d'exécuter différents conseillers sur le même port mais sur des grappes différentes (conseiller spécifique grappe/site). Par exemple, si Network Dispatcher est défini avec trois grappes (*grappe A*, *grappe B*, *grappe C*), pour chaque grappe le port 80 a une fonction différente.

- Conseiller spécifique grappe/site : Pour lancer un conseiller sur le port 80 pour *grappe A*, indiquez à la fois la grappe et le port :
`ndcontrol advisor start http grappeA:80`

Cette commande lance le conseiller `http` sur le port 80 pour la *grappe A*. Le conseiller `http` fonctionne sur tous les serveurs connectés au port 80 pour la *grappe A*.

- Conseiller de groupe : Pour lancer un conseiller personnalisé sur le port 80 pour toutes les autres grappes, indiquez simplement le port :
`ndcontrol advisor start ADV_personnalisé 80`

Cette commande lance le conseiller *ADV_personnalisé* sur le port 80 pour la *grappe B* et la *grappe C*. Le conseiller personnalisé fonctionne sur tous les serveurs connectés au port 80 pour la *grappe B* et la *grappe C*. (Pour obtenir plus d'informations sur les conseillers personnalisés, reportez-vous à la section «Création de conseillers personnalisés» à la page 151.)

Remarque : Le conseiller de groupes fonctionne sur toutes les grappes/sites ne disposant pas d'un conseiller spécifique.

Lorsque vous utilisez la configuration exemple ci-dessus, vous pouvez choisir d'arrêter le conseiller personnalisé *ADV_custom* pour le port 80 sur une grappe uniquement ou pour les deux grappes (*grappe B* et *grappe C*).

- Pour arrêter le conseiller personnalisé pour le port 80 uniquement pour la *grappe B*, indiquez la grappe et le port :
`ndcontrol advisor stop ADV_personnalisé grappeB:80`
- Pour arrêter le conseiller personnalisé pour le port 80 sur la *grappe B* et la *grappe C*, indiquez uniquement le port :
`ndcontrol advisor stop ADV_personnalisé 80`

Intervalles conseiller

Remarque : Les valeurs par défaut du conseiller doivent être correctes pour la plupart des scénarios possibles. Soyez prudent lorsque vous entrez des valeurs autres que celles fournies par défaut.

L'intervalle conseiller détermine la fréquence selon laquelle un conseiller demande des données d'état aux serveurs associés au port dont il a la charge, puis transmet ces données au gestionnaire. Si l'intervalle conseiller est trop court, le conseiller interrompra les serveurs constamment et les performances déclineront. Dans le cas contraire, les décisions d'allocation de pondérations prises par le gestionnaire reposeront sur des informations anciennes et incertaines.

Par exemple, pour fixer à 3 secondes l'intervalle du conseiller HTTP sur le port 80, entrez la commande suivante :

```
ndcontrol  
advisor interval http 80 3
```

Notez qu'il n'est pas logique de spécifier un intervalle conseiller inférieur à l'intervalle gestionnaire. L'intervalle conseiller par défaut est sept secondes.

Délai de rapport du conseiller

Pour s'assurer que le gestionnaire n'utilise pas d'informations périmées pour ses décisions d'équilibrage de charge, le gestionnaire n'utilisera pas les informations d'un conseiller dont l'horodatage sera antérieur à celui défini dans le délai de rapport du conseiller. Le délai de rapport du conseiller doit être supérieur à l'intervalle de sondage du conseiller. Si le délai est inférieur, le gestionnaire ignore les états qu'il est censé exploiter. Par défaut, les rapports des conseillers n'ont pas de délai d'expiration — la valeur par défaut est illimitée.

Par exemple, pour fixer à 30 secondes l'intervalle du conseiller HTTP sur le port 80, entrez la commande suivante :

```
ndcontrol advisor timeout http 80 30
```

Pour obtenir plus d'informations sur la définition du délai de rapport du conseiller, reportez-vous à la section «ndcontrol advisor — Contrôle du conseiller» à la page 260.

Délai de connexion du conseiller et délai de réception pour les serveurs

Pour Network Dispatcher, vous pouvez définir les valeurs de délai du conseiller lorsqu'une erreur serveur est détectée. Les valeurs de délai d'erreur serveur (connecttimeout et receivetimeout) déterminent la durée attendue par un conseiller avant de signaler qu'une connexion ou une réception n'a pas abouti.

Pour obtenir une détection d'erreur serveur très rapide, attribuez la valeur la plus basse (une seconde) aux délais de connexion et de réception du conseiller et attribuez la valeur la plus basse (une seconde) à l'intervalle du gestionnaire et du conseiller.

Remarque : Si le trafic de votre environnement atteint un volume modéré voire élevé et que le temps de réponse du serveur augmente, assurez-vous de ne pas avoir attribué de valeurs trop faibles à `connecttimeout` et à `receivetimeout`. Sinon, le conseiller peut indiquer de manière prématuré une erreur réseau lorsqu'un serveur est occupé.

Par exemple, pour attribuer la valeur 9 secondes à `connecttimeout` et à `receivetimeout` pour le conseiller HTTP sur le port 80, entrez la commande suivante :

```
ndcontrol advisor connecttimeout http 80 9
ndcontrol advisor receivetimeout http 80 9
```

La valeur par défaut de connexion et de réception est trois fois supérieure à la valeur indiquée pour l'intervalle du conseiller.

Liste des conseillers

- Le conseiller **HTTP** ouvre une connexion, envoie une demande HEAD par défaut attend la connexion et renvoie le temps écoulé comme chargement. Pour obtenir plus d'informations sur le mode de modification du type de demande envoyée par le conseiller HTTP, reportez-vous à la section «Option de demande/réponse (URL) de conseiller HTTP» à la page 161.
- Le conseiller **FTP** ouvre une connexion, envoie une demande SYST, attend une réponse, ferme la connexion et renvoie le temps écoulé en tant que chargement.
- Le conseiller **Telnet** ouvre une connexion, attend le premier message du serveur, ferme la connexion et renvoie le temps écoulé en tant que chargement.
- Le conseiller **NNTP** ouvre une connexion, attend le premier message du serveur, envoie une commande quit, ferme la connexion et renvoie le temps écoulé comme chargement.
- Le conseiller **IMAP** ouvre une connexion, attend la première réponse du serveur, envoie une commande quit, ferme la connexion et renvoie le temps écoulé comme chargement.
- Le conseiller **POP3** ouvre une connexion, attend la première réponse du serveur, envoie une commande quit, ferme la connexion et renvoie le temps écoulé comme chargement.
- Le conseiller **SMTP** ouvre une connexion, attend la première réponse du serveur, envoie une commande quit, ferme la connexion et renvoie le temps écoulé comme chargement.

- Le conseiller **SSL** ouvre une connexion, envoie une demande CLIENT HELLO, attend une réponse, ferme la connexion et renvoie le temps écoulé comme chargement.

Remarque : Le conseiller SSL n'a aucun rapport avec la gestion des clés ou des certificats.

- Le conseiller **ssl2http** est lancé et fonctionne sur les serveurs répertoriés sous le port 443 mais le conseiller ouvre une connexion au "portdemappage" pour les demandes HTTP. Utilisez uniquement le conseiller ssl2http pour CBR si le protocole client vers proxy est de type SSL et si le protocole proxy vers serveur est de type HTTP. Pour obtenir plus d'informations, reportez-vous à la section «Équilibrage de charge client-proxy dans SSL et proxy-serveur dans HTTP» à la page 80.
- Le conseiller Caching Proxy (**ibmproxy**) ouvre une connexion, envoie une demande HTTP GET spécifique de Caching Proxy et interprète la réponse en tant que chargement Caching Proxy.

Remarque : Lors de l'utilisation d'un conseiller ibmproxy, il est nécessaire d'exécuter Caching Proxy sur tous les serveurs faisant l'objet d'un équilibrage de charge. Il n'est pas nécessaire d'installer Caching Proxy sur la machine qui héberge Network Dispatcher à moins qu'il ne s'agisse de la machine dont il assure l'équilibrage de charge.

- Le conseiller **DNS** ouvre une connexion, envoie une demande de pointeur pour DNS, attend une réponse, ferme la connexion et renvoie le temps écoulé comme chargement.
- Le conseiller **Connect** n'échange aucune donnée spécifique du protocole avec le serveur. Il mesure simplement le temps que durent l'ouverture et la fermeture d'une connexion TCP avec le serveur. Ce conseiller est utile pour les applications de serveur qui utilisent TCP, mais ces applications doivent disposer d'un protocole de haut niveau pour lequel aucun conseiller IBM ou personnalisé n'est disponible.
- Le conseiller **ping** n'ouvre pas de connexion TCP avec les serveurs, mais indique si le serveur répond ou non à une commande ping. Bien que le conseiller ping soit utilisable avec tout type de port, il a été conçu pour les configurations utilisant le port générique, capable d'acheminer un trafic multiprotocole. Il est également utile pour les configurations utilisant des protocoles non TCP avec leurs serveurs, tels que UDP.
- Le conseiller **reach** émet des commandes ping vers les machines cibles. Il a été conçu pour permettre aux composants haute disponibilité de Dispatcher de déterminer l'accessibilité des «cibles à atteindre». Ses résultats sont transmis au composant de haute disponibilité et ne figurent pas dans le

rapport du gestionnaire. Contrairement aux autres conseillers, le conseiller reach démarrer *automatiquement* par la fonction gestionnaire du composant Dispatcher.

- Le conseiller **DB2** fonctionne en association avec les serveurs DB2. Dispatcher comporte une fonction intégrée permettant de vérifier l'état des serveurs DB2 sans que les clients aient besoin d'écrire leurs propres conseillers personnalisés. Le conseiller DB2 communique avec le port de connexion DB2 uniquement et non avec le port de connexion Java.
- Le conseiller **WLM** (Workload Manager) est conçu pour fonctionner avec les serveurs sur les gros systèmes OS/390 exécutant le composant WLM (Workload Manager). Pour plus de détails, reportez-vous à la section «Conseiller Workload Manager» à la page 155.
- Le conseiller **self** rassemble des informations sur le statut du chargement des serveurs périphériques. Vous pouvez utiliser le conseiller lors de l'utilisation de Dispatcher dans une configuration à deux niveaux, dans laquelle Dispatcher fournit les informations provenant du conseiller self au composant Network Dispatcher de niveau supérieure. Le conseiller self mesure de manière spécifique les connexions par seconde sur les serveurs périphériques du système Dispatcher se trouvant au niveau de l'exécutant. Pour obtenir plus d'informations, reportez-vous à la section «Utilisation d'un conseiller Self dans une configuration WAND à deux niveaux» à la page 172.
- Dispatcher permet à un utilisateur d'écrire un conseiller *personnalisé*. Cette opération permet la prise en charge de protocoles propriétaires (en plus de TCP) pour lesquels IBM n'a pas développé de conseiller spécifique. Pour plus d'informations, reportez-vous à la section «Création de conseillers personnalisés».
- Le conseiller **WAS** (WebSphere Application Server) fonctionne en coopération avec les serveurs WebSphere. Des fichiers modèle pour ce conseiller sont fournis dans le répertoire install. Pour plus d'informations, voir «Conseiller WebSphere Application Server» à la page 152.

Création de conseillers personnalisés

Le conseiller personnalisé est un petit programme Java, que vous fournissez sous forme de fichier classe, appelé par le code de base. Le code de base fournit tous les services administratifs, tels que le lancement et l'arrêt d'une instance du conseiller personnalisé, la génération d'états et de rapports et l'enregistrement des informations de l'historique dans un fichier journal. Il renvoie également les résultats au composant gestionnaire. Régulièrement, le code de base lance un cycle de conseiller au cours duquel il évalue individuellement tous les serveurs de sa configuration. Il commence par ouvrir une connexion avec la machine serveur. Si la connexion s'ouvre, le code de base appelle la méthode « *getLoad* » (fonction) dans le conseiller personnalisé. Ce dernier effectue la procédure nécessaire à l'évaluation du

serveur. Généralement, il envoie au serveur un message défini par l'utilisateur et attend la réponse. L'accès à la connexion ouverte est fourni au conseiller personnalisé. Le code de base ferme ensuite la connexion au serveur et envoie au gestionnaire les informations relatives à la charge.

Le code de base et le conseiller personnalisé peuvent opérer en mode normal ou en mode replace. Le choix du mode de fonctionnement est indiqué dans le fichier du conseiller personnalisé en tant que paramètre dans la méthode du constructeur.

En mode normal, le conseiller personnalisé échange des données avec le serveur et le code du conseiller de base évalue la durée de l'échange et calcule la valeur de la charge. Le code de base renvoie cette valeur au gestionnaire. Le conseiller personnalisé doit simplement retourner un zéro (succès) ou une valeur négative (échec). Lorsque dans le fichier du constructeur, la valeur false est attribuée à l'indicateur replace, le mode normal est défini.

En mode replace, le code de base n'effectue aucune mesure de temps. Le code du conseiller personnalisé effectue toutes les opérations nécessaires, puis renvoie une valeur de charge. Le code de base accepte la valeur et la retourne au gestionnaire. Pour obtenir de meilleurs résultats, situez votre valeur de charge entre 10 et 1000, 10 représentant un serveur rapide et 1000 un serveur plus lent. Lorsque dans le fichier du constructeur, la valeur true est attribuée à l'indicateur replace, le mode replace est défini.

Avec cette fonctionnalité, vous pouvez développer vos propres conseillers qui fourniront les informations sur les serveurs dont vous avez besoin. Un exemple de conseiller personnalisé, **ADV_exemple.java**, est fourni avec le produit Network Dispatcher. Une fois l'installation de Network Dispatcher effectuée, le code exemple se trouve dans le répertoire d'installation **...nd/servers/samples/CustomAdvisors**.

Les répertoires d'installation par défaut sont :

- AIX : /usr/lpp/nd
- Linux : /opt/nd
- Sun : /opt/nd
- Windows 2000 : c:\Program Files\IBM\nd

Conseiller WebSphere Application Server

Des fichiers exemple de conseiller personnalisé spécifiques au conseiller WebSphere Application Server sont fournis dans le répertoire d'installation de Network Dispatcher.

- Le fichier à compiler et à exécuter sur la machine Network Dispatcher se nomme **ADV_was.java**.

- `NDAdvisor.java.servlet` (à renommer `NDAdvisor.java`) est le fichier à compiler et à exécuter sur la machine WebSphere Application Server.

Les fichiers exemple de conseiller WebSphere Application Server se trouvent dans le même répertoire que le fichier `ADV_exemple.java`.

Convention d'attribution de nom

Le nom de fichier de votre conseiller personnalisé doit avoir le format «`ADV_monconseiller.java`». Il doit être précédé du préfixe «`ADV_`» en majuscules. Tous les caractères suivants doivent être en minuscules.

Conformément aux conventions Java, le nom de la classe définie dans le fichier doit correspondre au nom du fichier. Si vous copiez le code exemple, assurez-vous de remplacer toutes les occurrences de «`ADV_exemple`» dans le fichier par le nom de votre nouvelle classe.

Compilation

Les conseillers personnalisés sont écrits en langage Java. Vous devez obtenir et installer un compilateur Java 1.3 pour votre machine. Les fichiers suivants sont référencés pendant la compilation :

- le fichier du conseiller personnalisé,
- le fichier de classes de base, se trouvant dans le répertoire `...nd/servers/lib` dans lequel Network Dispatcher est installé.

Le chemin d'accès aux classes doit désigner à la fois le fichier du conseiller personnalisé et le fichier de classes de base lors de la compilation.

Pour Windows 2000, une commande de compilation peut avoir l'aspect suivant :

```
javac -classpath <rep_install>\nd\servers\lib\ibmnd.jar
ADV_fred.java
```

où :

- Votre fichier conseiller s'appelle `ADV_fred.java`.
- Votre fichier conseiller se trouve dans le répertoire courant.

Le résultat de la compilation est un fichier `.class`, par exemple :

```
ADV_fred.class
```

Avant de lancer le conseiller, copiez le fichier `.class` dans le répertoire `...nd/servers/lib/CustomAdvisors` dans lequel Network Dispatcher est installé.

Remarque : Si vous le souhaitez, vous pouvez compiler les conseillers personnalisés sur un système d'exploitation et l'exécuter sur un autre. Par exemple, vous pouvez compiler le conseiller sous

Windows 2000, copier le fichier .class (en binaire) sur une machine AIX à partir de laquelle vous exécutez le conseiller personnalisé.

La syntaxe est similaire pour AIX, Linux et Sun.

Exécution

Pour exécuter le conseiller personnalisé, vous devez tout d'abord copier le fichier .class dans le sous-répertoire Network Dispatcher approprié :

```
.../nd/servers/lib/CustomAdvisors/ADV_fred.class
```

Configurez le composant, lancez la fonction gestionnaire, puis exécutez la commande permettant de lancer le conseiller personnalisé.

```
ndcontrol advisor start fred 123
```

où :

- fred est le nom de votre conseiller, comme dans ADV_fred.java,
- 123 est le port sur lequel votre conseiller opérera.

Sous-programmes requis

Comme tous les conseillers, un conseiller personnalisé étend la fonction de la base du conseiller, intitulée ADV_Base. En fait, c'est la base du conseiller qui effectue la plupart des fonctions du conseiller, telles que la communication des charges au gestionnaire afin que ces dernières soient utilisées dans l'algorithme de pondération du gestionnaire. La base du conseiller effectue également les opérations de connexion et de fermeture de la connexion et fournit des méthodes d'envoi et de réception qui seront utilisées par le conseiller. Le conseiller n'est lui-même utilisé que pour l'envoi de données vers le port du serveur conseillé et pour la réception de données sur ce dernier. Les méthodes TCP de la base du conseiller sont programmées pour calculer la charge. Un indicateur du constructeur de ADV_base remplace, si vous le souhaitez, la charge existante par la nouvelle charge renvoyée par le conseiller.

Remarque : En fonction d'une valeur définie dans le constructeur, la base du conseiller fournit la charge à l'algorithme de pondération à un intervalle donné. Si le véritable conseiller n'a pas terminé ses opérations afin de renvoyer une charge valide, la base du conseiller utilise la charge précédente.

Ci-dessous, sont énumérées les méthodes de classe de base.

- Sous-programme **constructeur**. Le constructeur appelle le constructeur de la classe de base (reportez-vous au fichier type de conseiller).

- Méthode **ADV_AdvisorInitialize**. Cette méthode fournit un point d’ancrage au cas où des procédures supplémentaires doivent être suivies une fois l’initialisation de la classe de base terminée.
- Sous-programme **getload** . La classe de base du conseiller se charge de l’ouverture de la connexion ; getload ne doit qu’émettre les demandes d’envoi et de réception appropriées pour terminer le cycle de conseil.

Ordre de recherche

Network Dispatcher consulte tout d’abord la liste des conseillers en langage naturel. S’il ne trouve pas listeacheteurun conseiller donné, Network Dispatcher consulte la liste des conseillers personnalisés du client.

Affectation du nom et du chemin

- La classe de conseiller personnalisé doit se trouver dans le sous-répertoire de **...nd/servers/lib/CustomAdvisors/** dans le répertoire de base de Network Dispatcher. Le répertoire par défaut dépend du système d’exploitation :
 - AIX
/usr/lpp/nd/servers/lib/CustomAdvisors/
 - Linux
/opt/nd/servers/lib/CustomAdvisors/
 - Solaris
/opt/nd/servers/lib/CustomAdvisors/
 - Windows 2000
Chemin d’accès au répertoire d’installation commun :
C:\Program Files\IBM\edge\nd\servers\lib\CustomAdvisors

Chemin d’accès au répertoire d’installation natif :
C:\Program Files\IBM\nd\servers\lib\CustomAdvisors
- Seuls les caractères alphabétiques minuscules sont autorisés. Cela permet d’éliminer la distinction entre majuscules et minuscules lorsqu’un opérateur entre des commandes sur la ligne de commande. Le nom du conseiller doit être précédé de **ADV_**.

Conseiller type

Un programme permettant de créer un conseiller type est présenté à la section «Conseiller type» à la page 395. Après installation, ce conseiller exemple se trouve dans le répertoire **...nd/servers/samples/CustomAdvisors**.

Conseiller Workload Manager

Le code de WLM ne s’exécute que sur des grands systèmes MVS. Il peut être utilisé pour demander la charge sur la machine MVS.

Si MVS Workload Management a été configuré sur votre système OS/390, Dispatcher peut accepter de WLM des informations relatives à la charge et les utiliser dans le processus d'équilibrage de charge. Grâce au conseiller WLM, Dispatcher ouvre régulièrement des connexions via le port WLM sur chaque serveur de la table d'hôte Dispatcher et accepte les chiffres relatifs à la capacité renvoyés. Ces chiffres représentent la capacité encore disponible et Dispatcher attend des valeurs représentant la charge sur chaque machine, le conseiller inverse et normalise les chiffres relatifs à la capacité pour obtenir des valeurs de charge (des chiffres de capacité élevés correspondent à des valeurs de charge faibles et représentent un serveur en bon état). Les valeurs de charge obtenues sont placées dans la colonne relative au système du rapport du gestionnaire.

Il existe plusieurs différences importantes entre le conseiller WLM et les autres conseillers Dispatcher :

1. Les autres conseillers ouvrent des connexions aux serveurs en utilisant le même port que pour le trafic client normal. Le conseiller WLM ouvre des connexions aux serveurs en utilisant un port différent de celui utilisé pour le trafic normal. Sur chaque machine serveur, l'agent WLM doit être configuré pour effectuer l'écoute sur le port sur lequel le conseiller Dispatcher WLM a été lancé. Le port WLM par défaut est 10007.
2. Les autres conseillers évaluent uniquement les serveurs définis dans la configuration grappe:port:serveur de Dispatcher pour laquelle le port serveur correspond au port conseiller. Le conseiller WLM conseille sur chaque serveur de la configuration grappe:port:serveur Dispatcher. Vous ne devez donc pas définir de serveurs non WLM lorsque vous utilisez le conseiller WLM.
3. Les autres conseillers placent les informations relatives à la charge dans la colonne «Port» du rapport du gestionnaire. Le conseiller WLM place les informations sur la charge dans la colonne System du rapport du gestionnaire.
4. Il est possible d'utiliser les conseillers de protocole avec le conseiller WLM. Les conseillers de protocole évaluent la charge des serveurs sur le port utilisé pour le trafic normal et le conseiller WLM évalue la charge du système sur le port WLM.

Restrictions relatives à Metric Server

Comme l'agent Metric Server, le rapport de l'agent WLM concerne les systèmes de serveur dans leur ensemble et non chacun des démons de serveur associés à un protocole. Metric Server et WLM placent leurs résultats dans la colonne relative au système du rapport du gestionnaire. Par conséquent, il n'est pas possible d'exécuter simultanément le conseiller WLM et Metric Server.

Metric Server

Cette fonction est disponible pour tous les composants Network Dispatcher.

Metric Server fournit à Network Dispatcher les informations de téléchargement sous la forme de données numériques-système, relatives à l'état du serveur. Le gestionnaire Network Dispatcher adresse des demandes aux agents du système Metric Server situés sur chacun des serveurs, leur attribuant des pondérations destinées au processus d'équilibrage de charge à l'aide des données rassemblées par les agents. Les résultats sont regroupés dans le rapport du gestionnaire.

Remarque : Des erreurs d'arrondi peuvent se produire lorsque plusieurs données numériques sont rassemblées et normalisées pour chaque serveur en une seule valeur de charge.

Pour obtenir un exemple de configuration, reportez-vous à la figure 11 à la page 43.

Restrictions relatives à WLM

Comme le conseiller WLM, le rapport du Metric Server concerne l'ensemble des systèmes de serveurs et non chaque démon de serveur associé à un protocole. WLM et Metric Server placent leurs résultats dans la colonne relative au système du rapport du gestionnaire. Par conséquent, il n'est pas possible d'exécuter simultanément le conseiller WLM et Metric Server.

Conditions préalables

L'agent de Metric Server doit être installé et en cours d'exécution sur les serveurs pour lesquels Network Dispatcher effectue l'équilibrage de charge.

Conditions d'utilisation de Metric Server

La procédure ci-après permet de configurer Metric Server pour Network Dispatcher. Vous pouvez configurer Metric Server pour les autres composants de Network Dispatcher à l'aide d'une procédure similaire.

- Gestionnaire Network Dispatcher (côté Network Dispatcher)
 1. Lancez **ndserver**.
 2. Emettez la commande : **ndcontrol manager start** *manager.log port*
port correspond au port RMI sur lequel fonctionnent tous les agents du système Metric Server. La valeur par défaut du port RMI est 10004, cette valeur est définie dans le fichier *metricserver.cmd*.
 3. Emettez la commande : **ndcontrol metric add** *grappe:systemMetric systemMetric*
systemMetric correspond au nom du script (se trouvant sur le serveur périphérique) qui doit s'exécuter sur chacun des serveurs de la configuration sous la grappe indiquée (ou nom de site). Deux scripts sont fournis au client - **cpupload** et **memload**. Vous pouvez également créer des scripts de mesure système personnalisés. Le script contient une

commande qui renvoie une valeur numérique comprise entre 0-100. Cette valeur numérique doit représenter une mesure de charge, et non un indicateur de disponibilité.

Remarque : Pour Site Selector, cpuload et memload sont exécutés automatiquement.

Restriction : Pour Windows 2000, si le nom du script System Metric comporte une extension autre que ".exe", vous devez indiquer le nom complet du fichier (par exemple, "monscriptsys.bat"). Cette restriction est due à une limitation Java.

4. Ajoutez à la configuration uniquement les serveurs contenant un agent du système Metric Server s'exécutant sur le port indiqué dans le fichier metricserver.cmd. Le port doit correspondre à la valeur de port indiquée dans la commande **manager start**.

Remarque : Garantie de la sécurité —

- Sur la machine Network Dispatcher, créez un fichier de clés pour le composant en cours d'exécution(en utilisant la commande **ndkeys create**). Pour obtenir plus d'informations sur ndkeys, reportez-vous à la section «Administration authentifiée à distance» à la page 213.
 - Sur le serveur, copiez le fichier de clés obtenu dans le répertoire **.../nd/admin/key**. Vérifiez que l'utilisateur root dispose de droits lui permettant de lire le fichier de clés.
- Agent Metric Server (côté serveur)
 1. Lors de l'installation de Network Dispatcher, installez l'ensemble Metric Server.
 2. Vérifiez le script **metricserver** dans le répertoire **/usr/bin** afin de contrôler que le port RMI souhaité est utilisé. (Pour Windows 2000, le répertoire est C:\WINNT\SYSTEM32.) Le port RMI par défaut est 10004.

Remarque : La valeur du port RMI indiquée doit être identique à la valeur du port RMI du système Metric Server sur la machine Network Dispatcher.

3. Les deux scripts suivants sont déjà fournis au client : **cpuload** (renvoie le pourcentage de cpu utilisé, compris entre 0-100) et **memload** (donne le pourcentage de mémoire utilisée compris entre 0-100). Ces scripts se trouvent dans le répertoire **...nd/ms/script**.

Les clients peuvent éventuellement écrire leurs propres fichiers scripts personnalisés qui définiront la commande passée par Metric Server sur les serveurs. Vérifiez que tous les scripts personnalisés sont exécutables

et qu'ils se trouvent dans le répertoire **...nd/ms/script**. Les scripts personnalisés **doivent** renvoyer une valeur de charge comprise entre 0-100.

Remarque : Un script de mesure personnalisé doit être un programme valide ou un script ayant l'extension ".bat" ou ".cmd". De manière plus spécifique, pour les plate-formes UNIX, les scripts doivent commencer par la déclaration de shell. Dans le cas contraire, il est possible qu'ils ne s'exécutent pas correctement.

4. Lancez l'agent en émettant la commande **metricserver**.
5. Pour arrêter l'agent Metric Server, émettez la commande **metricserver stop**.

Pour exécuter le système Metric Server ailleurs que sur l'hôte local, vous devez modifier le fichier `metricserver` sur le serveur ayant fait l'objet d'un équilibrage de charge. Insérez la ligne suivante après "java" dans le fichier `metricserver` :

```
-Djava.rmi.server.hostname=AUTRE_ADRESSE
```

Ajoutez en outre la ligne suivante avant les instructions "if" dans le fichier `metricserver` : `hostname AUTRE_ADRESSE`.

Windows 2000 : Vous devez également affecter un alias à `AUTRE_ADRESSE` dans la pile Microsoft. Pour ce faire, reportez-vous à la page 180.

Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)

Lors de la définition d'un serveur dans la configuration Network Dispatcher, vous pouvez distribuer la charge en fonction de l'état du serveur dans son ensemble (à l'aide de l'agent du système Metric Server) et/ou de l'état de toute application spécifique du port (à l'aide de la fonction conseiller).

Avec le partitionnement du serveur, vous pouvez effectuer une distinction plus avancée entre des URL particulières et leurs applications spécifiques. Par exemple, un serveur Web permet de gérer plusieurs pages JSP, pages HTML, requêtes de base de données, etc. Network Dispatcher permet maintenant de partitionner une grappe et un serveur spécifiques d'un port en plusieurs serveurs logiques. Ainsi, vous pouvez appliquer le conseiller sur un service particulier de la machine afin de détecter si un moteur de servlet ou une demande de base de données s'exécute très rapidement ou s'il ne s'exécute pas du tout.

Le partitionnement de serveur permet à Network Dispatcher de détecter, par exemple, que le service HTML traite les pages rapidement mais que la connexion à la base de données a été interrompue. Ainsi vous pouvez distribuer la charge en fonction de la charge de travail de chaque service plus granulaire et non en fonction uniquement de la pondération serveur.

Dans la configuration de Network Dispatcher, vous pouvez représenter un serveur physique ou un serveur logique à l'aide de la hiérarchie *grappe:port:serveur*. Le serveur peut être une adresse IP unique de la machine (serveur physique) sous la forme d'un nom symbolique ou au format décimal à point. Ou, si vous configurez le serveur afin qu'il représente un serveur partitionné, vous devez alors fournir une adresse de serveur pouvant être résolue pour le serveur physique dans le paramètre **address** de la commande **ndcontrol server add**. Pour de plus amples informations, reportez-vous à la section «ndcontrol server — Configuration des serveurs» à la page 311.

Ci-dessous se trouve un exemple de partitionnement de serveurs physiques en serveurs logiques afin de gérer différents types de demandes.

```
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
```

Dans cet exemple, le serveur 1.1.1.2 est divisé en deux serveurs logiques — A (gérant les demandes html) et B (gérant les demandes gif). Le serveur 1.1.1.3 est divisé en deux serveurs logiques — C (gérant les demandes html) et D (gérant les demandes jsp). Le serveur 1.1.1.4 est partitionné en deux serveurs logiques — E (gérant les demandes gif) et F (gérant les demandes jsp).

Remarque : Server Directed Affinity peut ne pas fonctionner avec le partitionnement de serveur car pour les fonctions de recherche de SDA, il est nécessaire que les adresses de serveur soient uniques dans la configuration. Pour de plus amples informations, reportez-vous à la section «API SDA pour le contrôle de l’affinité client/serveur» à la page 196.

Option de demande/réponse (URL) de conseiller HTTP

L’option d’URL du conseiller HTTP est disponible pour les composants Dispatcher et CBR.

Après avoir lancé un conseiller HTTP, vous pouvez définir une chaîne HTTP URL client unique, propre au service que vous voulez demander sur le serveur. Ainsi, le conseiller HTTP peut contrôler l’état des services d’un serveur. Vous pouvez effectuer cette opération en définissant des serveurs logiques avec des noms de serveurs uniques ayant la même adresse IP physique. Pour de plus amples informations, reportez-vous à «Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)» à la page 159.

Pour chaque serveur logique défini sous le port HTTP, vous pouvez indiquer une chaîne HTTP URL client unique, spécifique du service pour lequel vous voulez interroger le serveur. Le conseiller HTTP utilise la chaîne **advisorrequest** pour vérifier l’état des serveurs. La valeur par défaut est `HEAD / HTTP/1.0`. La chaîne **advisorresponse** correspond à la réponse du conseiller HTTP recherche dans la réponse HTTP. Le conseiller HTTP utilise la chaîne **advisorresponse** pour comparer la véritable réponse reçue du serveur. La valeur par défaut est null.

Important : Si l’URL HTTP contient un espace :

- Lorsque vous lancez la commande à partir de l’invite du shell **ndcontrol**>>, vous devez mettre la chaîne contenant un espace entre guillemets. Par exemple :

```
server
set grappe:port:serveur advisorrequest "head / http/2.0"
server set grappe:port:serveur
advisorresponse "HTTP 200 OK"
```

- Lorsque vous lancez la commande **ndcontrol** à partir de l’invite du système d’exploitation, vous devez placer les caractères `"\"` et `\""` respectivement avant et après le texte. Par exemple :

```
ndcontrol server set grappe:port:serveur
advisorrequest "\"head / http/2.0\""
ndcontrol server set grappe:port:serveur
advisorresponse "\"HTTP 200 OK\""
```

Remarque : Après le lancement d'un conseiller HTTP pour un numéro de port HTTP indiqué, la valeur demande/réponse du conseiller est activée pour les serveurs sous le port HTTP.

Pour de plus amples informations, reportez-vous à la section «ndcontrol server — Configuration des serveurs» à la page 311.

Utilisation de serveurs implantés au même endroit

Network Dispatcher peut se trouver sur la même machine qu'un serveur pour lequel il effectue des demandes d'équilibrage de charge. On parle alors de *co-implantation* d'un serveur. La co-implantation s'applique aux composants Dispatcher, Site Selector, Mailbox Locator et Cisco Consultant. Elle est également prise en charge pour le composant CBR, mais uniquement avec des serveurs Web et un serveur Caching Proxy de type serveur de liaison.

Remarque : Un serveur co-implanté est en concurrence avec le Network Dispatcher pour les ressources aux moments de trafic élevé. Toutefois, en l'absence de machines surchargées, l'utilisation d'un serveur co-implanté permet de réduire le nombre total de machines nécessaires pour configurer un site avec -équilibrage de charge.

Pour le composant Dispatcher

Red Hat Linux v7.1 (Linux kernel version 2.4.2-2) ou SuSE Linux v7.1 (Linux kernel version 2.4.0-4Go) : pour configurer simultanément la co-implantation et la haute disponibilité lors de l'exécution du composant Dispatcher avec la méthode d'acheminement MAC, vous devez installer un correctif de noyau Linux. Pour obtenir plus d'informations sur l'installation du correctif, reportez-vous à la section «Installation du correctif du noyau Linux (pour supprimer les réponses ARP sur l'interface de bouclage)» à la page 72. Cependant, lorsque vous suivez ces instructions, ignorez l'étape d'attribution d'un adaptateur de bouclage. Vous devez ajouter l'instruction `ifconfig` afin d'attribuer un alias à l'adaptateur de bouclage dans le fichier de script `goStandby high-availability` qui s'exécute lorsqu'un composant Dispatcher passe à l'état Attente.

Solaris : Il existe une restriction. Il n'est pas possible de configurer de conseillers WAND lorsqu'un composant Dispatcher de point d'entrée est co-implanté. Reportez-vous à la section «Utilisation de conseillers éloignés avec le support de réseau étendu» à la page 166.

Dans les versions précédentes, il était nécessaire de préciser que l'adresse du serveur co-implanté devait être la même que l'adresse de non-acheminement (NFA) dans la configuration. Cette restriction a maintenant été éliminée.

Pour configurer un serveur afin qu'il soit co-implanté, la commande **ndcontrol server** propose l'option **collocated** qui peut être *oui* ou *non*. La valeur par défaut est non. L'adresse du serveur doit être une adresse IP valide d'une carte d'interface réseau sur la machine.

Remarque : Pour **Windows 2000** : Vous pouvez co-implanter Dispatcher, mais n'utilisez *pas* le mot clé **collocated**. La co-implantation est prise en charge avec les méthodes d'acheminement NAT et CBR de Dispatcher, mais elle n'est pas prise en charge avec la méthode d'acheminement MAC de Dispatcher. Pour plus d'informations sur les méthodes d'acheminement de Dispatcher, reportez-vous aux sections «Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)» à la page 52, «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54 et «Réacheminement MAC de Dispatcher (méthode d'acheminement mac)» à la page 52.

Vous pouvez configurer un serveur co-implanté de l'une des manières suivantes :

- Si vous utilisez une adresse de non-réacheminement (NFA) en tant qu'adresse de serveur co-implanté, définissez l'adresse NFA à l'aide de la commande **ndcontrol executor set nfa adresse_IP**. Ajoutez ensuite le serveur en utilisant l'adresse NFA avec la commande **ndcontrol server add grappe:port:serveur**.
- Si vous utilisez une adresse autre que l'adresse NFA, ajoutez le serveur avec l'adresse IP voulue tout en attribuant la valeur oui au paramètre **collocated** de la manière suivante : **ndcontrol server add grappe:port:serveur collocated oui**.

Pour obtenir des informations plus détaillées sur la syntaxe de la commande **ndcontrol server**, reportez-vous à la section «**ndcontrol server** — Configuration des serveurs» à la page 311.

Composant CBR

Le composant CBR prend en charge la co-implantation sur toutes les plate-formes sans qu'il soit nécessaire de procéder à des configurations supplémentaires. Vous devez toutefois utiliser des serveurs Web et Caching Proxy de liaison.

Pour le composant Mailbox Locator

Mailbox Locator prend en charge la co-implantation sur toutes les plate-formes. Cependant, le serveur doit être associé à une adresse différente que celle de Network Dispatcher. Afin de co-implanter un serveur POP3 ou IMAP sur la même machine, il doit être lié à une adresse IP différente de l'adresse de la grappe. Cela peut être effectué en utilisant une adresse de bouclage.

Pour le composant Site Selector

Site Selector prend en charge la co-implantation sur toutes les plate-formes sans qu'aucune configuration supplémentaire ne soit requise.

Pour le composant Cisco Consultant

Cisco Consultant prend en charge la co-implantation sur toutes les plate-formes sans qu'aucune configuration supplémentaire ne soit requise.

Configuration du support de réseau étendu pour Dispatcher

Cette fonction est disponible uniquement pour le composant Dispatcher.

Si vous n'utilisez ni le support de réseau étendu de Dispatcher ni la méthode d'acheminement CBR de Dispatcher, la configuration de Dispatcher requiert que la machine Dispatcher et ses serveurs soient tous connectés au même segment de réseau local (reportez-vous à la section figure 22). Un paquet émis par un client est transmis au répartiteur, envoyé au serveur, puis renvoyé au client.

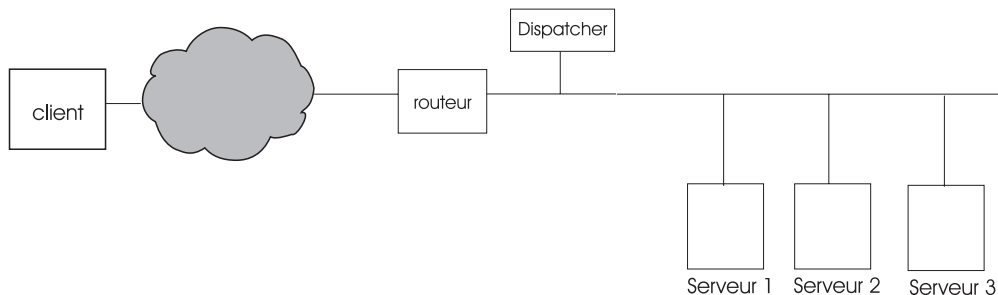


Figure 22. Exemple de configuration consistant en un seul segment de réseau local

L'extension de répartiteur étendu permet la prise en charge des serveurs hors site, appelés *serveurs éloignés* (voir la figure 23 à la page 165). Si GRE n'est pas pris en charge sur le site distant et que vous n'utilisez pas la méthode d'acheminement NAT de Dispatcher, le site distant doit correspondre à une machine Dispatcher éloignée (Dispatcher 2) et aux serveurs associés localement (Serveur G, Serveur H et Serveur I). Toutes les machines Dispatcher doivent exécuter le même système d'exploitation. Un paquet émanant d'un client peut alors être transmis d'Internet à une machine Dispatcher, puis à une machine Dispatcher éloignée géographiquement et enfin à l'un de ses serveurs locaux.

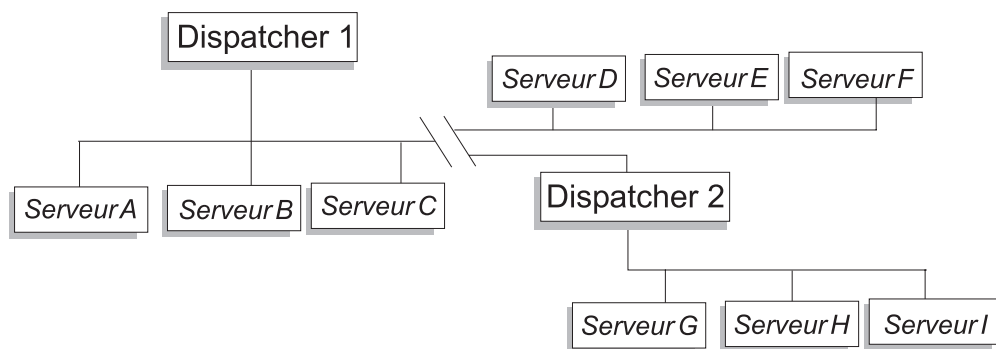


Figure 23. Exemple de configuration utilisant des serveurs locaux et éloignés

Cela permet à une adresse de grappe de supporter l'ensemble des demandes client du monde entier, tout en répartissant la charge entre l'ensemble des serveurs.

La machine Dispatcher qui reçoit le paquet en premier peut tout de même être connectée à des serveurs locaux et répartir la charge entre ses serveurs locaux et les serveurs éloignés.

Syntaxe des commandes

Les commandes de réseau étendu ne sont pas complexes. Pour configurer un support de réseau étendu :

1. Ajoutez les serveurs. Lorsque vous ajoutez un serveur à un répartiteur (Dispatcher), vous devez définir si ce serveur est local ou éloigné (voir plus haut). Pour ajouter un serveur et le définir comme serveur local, entrez la commande **ndcontrol server add** sans spécifier de routeur. Il s'agit de la valeur par défaut. Pour définir ce serveur comme serveur éloigné, vous devez spécifier le routeur par l'intermédiaire duquel le répartiteur doit envoyer le paquet afin d'atteindre le serveur éloigné. Le serveur doit être un autre répartiteur et son adresse doit être l'adresse de non-réacheminement du répartiteur. Par exemple, dans figure 24 à la page 168, si vous ajoutez *ND 2* en tant que serveur éloigné dans *ND 1*, vous devez définir *router 1* comme l'adresse de routage. Syntaxe générale :
`ndcontrol server add grappe:port:serveur router adresse`

Pour obtenir plus d'informations sur le mot clé `router`, reportez-vous à la section «`ndcontrol server` — Configuration des serveurs» à la page 311.

2. Configurez les alias. Sur la première machine Dispatcher (à laquelle la demande client est transmise depuis Internet), un alias doit être affecté à l'adresse de la grappe à l'aide de la commande **cluster configure**, **ifconfig** ou **ndconfig** comme auparavant. Toutefois, sur les machines Dispatcher éloignées, l'adresse de la grappe **n'a pas** d'alias défini sur la carte d'interface réseau.

Utilisation de conseillers éloignés avec le support de réseau étendu

Sur les répartiteurs de base, les conseillers fonctionnent correctement sans configuration particulière pour la plupart des plate-formes.

Linux : Des restrictions affectent l'utilisation des conseillers éloignés avec des configurations de support de réseau étendu. Les conseillers de protocole, tels que le conseiller HTTP, qui s'exécutent sur la machine Dispatcher de point d'entrée ne peuvent évaluer correctement l'état des serveurs du site distant. Pour remédier à ce problème, effectuez l'une des opérations suivantes :

- Exécutez le conseiller Ping (indépendant de tout protocole) sur la machine Dispatcher de point d'entrée.
- Exécutez un conseiller de protocole sur la machine Dispatcher de point d'entrée avec le démon de serveur de protocole correspondant (tel qu'un serveur Web) sur la machine Dispatcher éloignée.

Ces deux options fournissent au conseiller qui s'exécute sur la machine Dispatcher de point d'entrée une évaluation de l'état de la machine Dispatcher éloignée.

Solaris : Dans les composants Network Dispatcher de point d'entrée, vous devez utiliser la méthode de configuration arp (au lieu des méthodes de configuration ifconfig ou cluster). Par exemple :

```
arp -s <mon_adresse_grappe> <mon_adresse_mac> pub
```

Remarque : Sous Solaris, il existe plusieurs restrictions :

- Les conseillers WAND fonctionnent uniquement avec la méthode arp de la configuration de grappe.
- Les conseillers des serveurs de liaison fonctionnent uniquement avec la méthode arp de la configuration de grappe.
- La co-implantation fonctionne uniquement avec la méthode ifconfig de la configuration de grappe.

Sur les répartiteurs éloignés, vous devez exécuter les étapes de configuration suivantes pour chaque adresse de grappe éloignée. Pour une configuration de haute disponibilité à l'emplacement Network Dispatcher éloigné, vous devez effectuer cette configuration sur les deux machines.

AIX

- Ajoutez l'alias d'adresse de grappe à l'adaptateur de bouclage. La valeur de sous-masque doit être définie à 255.255.255.255. Par exemple :

```
ifconfig lo0 alias 9.67.34.123 netmask 255.255.255.255
```

Remarque : Il est nécessaire de disposer de conseillers qui fonctionnent à la fois sur des machines Dispatcher locales et éloignées.

Linux

- Ajoutez l'alias d'adresse de grappe à l'adaptateur de bouclage. Par exemple :

ifconfig lo:1 9.67.34.123 netmask 255.255.255.255 up

Remarque : Il est nécessaire de disposer de conseillers qui fonctionnent à la fois sur des machines Dispatcher locales et éloignées.

Solaris

- Aucune configuration supplémentaire n'est requise.

Windows 2000

1. Deux adresses IP sont requises pour Dispatcher. Une pour la pile Microsoft TCP/IP et l'autre pour la pile Network Dispatcher. Configurez l'adresse NFA en utilisant l'adresse IP de la pile Network Dispatcher. Par exemple :

ndconfig en0 alias 9.55.30.45 netmask 255.255.240.0

2. Configurez la carte de bouclage en utilisant l'adresse de grappe éloignée comme alias. La valeur de sous-masque doit être définie à 255.255.255.255. Par exemple :

ndconfig lo0 alias 9.67.34.123 netmask 255.255.255.255

3. Dans la table arp, supprimez les entrées de l'adresse de grappe éloignée.
 - a. Pour visualiser le contenu de la table arp, tapez :
arp -a
 - b. Pour supprimer une entrée existante, tapez :
arp -d 9.67.34.123

Remarque : Pour déterminer l'adresse MAC de votre interface, tapez :

1) **ping** *votre_nomhôte*

2) **arp -a**

et recherchez l'adresse de votre machine.

4. Ajoutez une route à la grappe éloignée (9.67.34.123) en utilisant l'adresse NFA (adresse IP de la pile Network Dispatcher). La valeur de masque doit être définie à 255.255.255.255. Par exemple :

route add 9.67.34.123 mask 255.255.255.255 9.55.30.45

Exemple de configuration

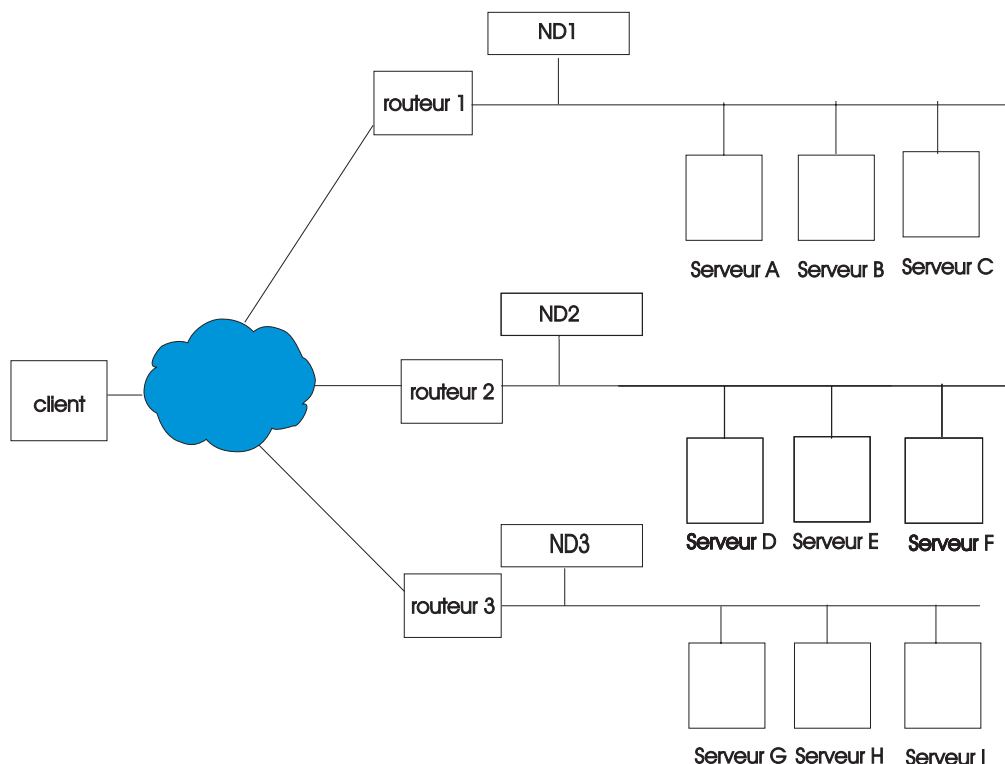


Figure 24. Exemple de configuration en réseau étendu avec des composants Network Dispatcher éloignés

Cet exemple s'applique à la configuration illustrée à la figure 24.

Vous trouverez ci-après la méthode à utiliser pour configurer les machines Dispatcher afin qu'elles supportent l'adresse de grappe xebec sur le port 80. ND1 est défini comme «point d'entrée». Il est supposé qu'une connexion Ethernet est utilisée. ND1 comporte cinq serveurs définis : trois serveurs locaux (ServeurA, ServeurB, ServeurC) et deux serveurs éloignés (ND2 et ND3). Par ailleurs, trois serveurs locaux ont été définis pour chacun des serveurs éloignés ND2 et ND3.

Sur la console de la première machine Dispatcher (ND1), procédez comme suit :

1. Lance l'exécuteur.
ndcontrol executor start

2. Définissez l'adresse de non-réacheminement de la machine Dispatcher.
ndcontrol executor set nfa ND1
3. Définissez la grappe.
ndcontrol cluster add xebec
4. Définissez le port.
ndcontrol port add xebec:80
5. Définissez les serveurs.
 - a. **ndcontrol server add xebec:80:ServeurA**
 - b. **ndcontrol server add xebec:80:ServeurB**
 - c. **ndcontrol server add xebec:80:ServeurC**
 - d. **ndcontrol server add xebec:80:ND2 router Router1**
 - e. **ndcontrol server add xebec:80:ND3 router Router1**
6. Si vous utilisez Windows 2000, configurez l'adresse NFA de la carte de réseau local de Dispatcher.
ndcontrol cluster configure ND1 Configurez également xebec en tant que clusteraddr.
7. Configurez l'adresse de grappe.
ndcontrol cluster configure xebec

Sur la console de la deuxième machine Dispatcher (ND2) :

1. Lance l'exécuteur.
ndcontrol executor start
2. Définissez l'adresse de non-réacheminement de la machine Dispatcher.
ndcontrol executor set nfa ND2
3. Définissez la grappe.
ndcontrol cluster add xebec
4. Définissez le port.
ndcontrol port add xebec:80
5. Définissez les serveurs.
 - a. **ndcontrol server add xebec:80:ServeurD**
 - b. **ndcontrol server add xebec:80:ServeurE**
 - c. **ndcontrol server add xebec:80:ServeurF**
6. Si vous utilisez Windows 2000, configurez l'adresse NFA de la carte de réseau local de Dispatcher.
ndcontrol cluster configure ND2

Sur la console de la troisième machine Dispatcher (ND3) :

1. Lance l'exécuteur.
ndcontrol executor start
2. Définissez l'adresse de non-réacheminement de la machine Dispatcher.
ndcontrol executor set nfa ND3
3. Définissez la grappe.
ndcontrol cluster add xebec
4. Définissez le port.
ndcontrol port add xebec:80
5. Définissez les serveurs.
 - a. **ndcontrol server add xebec:80:ServeurG**
 - b. **ndcontrol server add xebec:80:ServeurH**
 - c. **ndcontrol server add xebec:80:ServeurI**
6. Si vous utilisez Windows 2000, configurez l'adresse nfa de la carte de réseau local de Dispatcher.
ndcontrol cluster configure ND3

Remarques

1. Sur tous les serveurs (A-I) reliez l'adresse de grappe par un alias à une unité de bouclage.
2. Les grappes et les ports sont ajoutés avec la commande `ndcontrol` sur toutes les machines Dispatcher concernées : la machine définie comme point d'entrée et tous les serveurs éloignés.
3. Reportez-vous à la section «Utilisation de conseillers éloignés avec le support de réseau étendu» à la page 166 pour plus d'informations sur l'utilisation des conseillers éloignés avec le support de réseau étendu.
4. Le support de réseau étendu ne permet pas les boucles de routage infinies. (Si une machine Dispatcher reçoit un paquet d'une autre machine Dispatcher, elle ne le transmet pas à une troisième machine Dispatcher.) Un réseau étendu n'accepte qu'un niveau de serveurs éloignés.
5. Un réseau étendu accepte les protocoles UDP et TCP.
6. Un réseau étendu fonctionne avec la haute disponibilité : chaque machine Dispatcher peut être assistée d'une machine de secours adjacente (sur le même segment de réseau local).
7. Le gestionnaire et les conseillers fonctionnent en réseau étendu et, s'ils sont utilisés, doivent être lancés sur l'ensemble des machines Dispatcher concernées.
8. Network Dispatcher ne prend en charge la fonction WAND que sous des systèmes d'exploitation analogues.

Support GRE (Generic Routing Encapsulation)

GRE (Generic Routing Encapsulation) est un protocole Internet défini dans RFC 1701 et RFC 1702. Lorsque vous utilisez GRE, Network Dispatcher peut encapsuler les paquets IP de clients dans des paquets IP/GRE et les transmettre aux plate-formes de serveur telles qu'OS/390 qui prend en charge GRE. Le support GRE permet au composant Dispatcher d'équilibrer la charge des paquets sur plusieurs adresses de serveurs associées à une adresse MAC.

Network Dispatcher implémente GRE comme faisant partie de la fonction WAND (wide area Network Dispatcher). Ainsi, Network Dispatcher peut fournir l'équilibrage de charge de réseau étendu directement aux systèmes de serveur pouvant désencapsuler les paquets GRE. Il n'est pas nécessaire que Network Dispatcher soit installé sur le site éloigné si les serveurs éloignés prennent en charge les paquets GRE encapsulés. Network Dispatcher encapsule les paquets WAND, la valeur décimale 3735928559 étant attribuée à l'ensemble de zones de clés GRE.

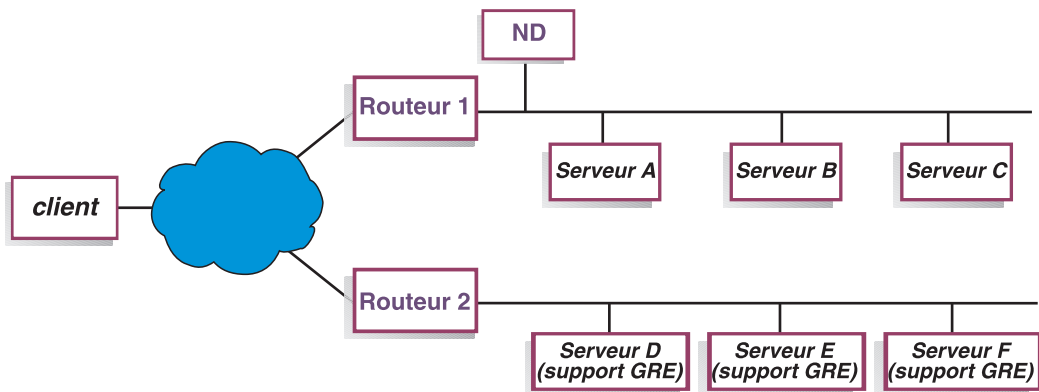


Figure 25. Exemple de configuration en réseau étendu avec une plate-forme serveur prenant en charge GRE

Dans cet exemple, afin d'ajouter le serveur D éloigné, qui prend en charge GRE, définissez-le dans la configuration Network Dispatcher comme si vous définissiez un serveur WAND dans la hiérarchie grappe:port:serveur :

```
ndcontrol server add grappe:port:ServeurD routeur Routeur1
```

Utilisation d'un conseiller Self dans une configuration WAND à deux niveaux

Le conseiller self est disponible dans le composant Dispatcher.

Lorsque Network Dispatcher se trouve dans une configuration WAND (wide area Network Dispatcher) à deux niveaux, un conseiller *self* est fourni qui rassemble des informations de statut de chargement sur les serveurs périphériques.

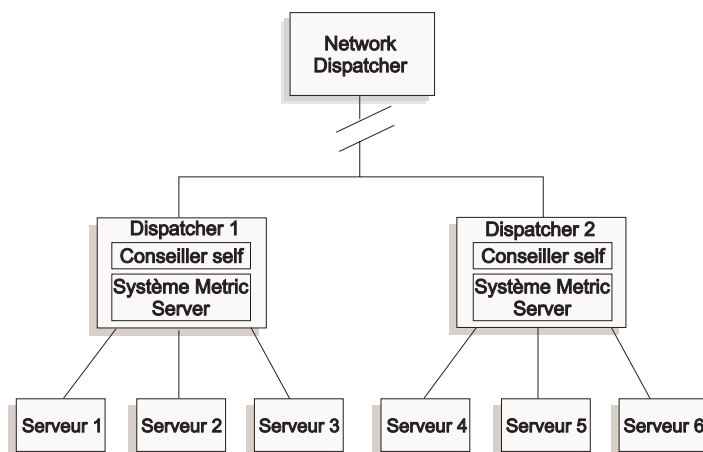


Figure 26. Exemple de configuration WAND à deux niveaux utilisant le conseiller self

Dans cet exemple, le conseiller self ainsi que le système Metric Server se trouvent sur deux machines Dispatcher dont l'équilibrage de charge est assuré par le système Network Dispatcher se trouvant au niveau supérieur. Le conseiller self mesure de manière spécifique les connexions par seconde sur les serveurs périphériques du système Dispatcher se trouvant au niveau de l'exécutant.

Le fichier self inscrit les résultats dans le fichier `ndloadstat`. Network Dispatcher fournit également une mesure externe appelée `ndload`. L'agent du système Metric Server de chaque machine Dispatcher exécute son fichier de configuration qui appelle le script `ndload` de mesure externe. Le script `ndload` extrait une chaîne du fichier `ndloadstat` et le renvoie à l'agent du système Metric Server. Ensuite, chaque agent du système Metric Server (de chaque élément Dispatcher) renvoie la valeur de statut de chargement à l'élément Network Dispatcher se trouvant au niveau supérieure. Cette valeur sera utilisée pour déterminer le système Dispatcher qui transmettra les demandes client.

L'exécutable `ndload` se trouve dans le répertoire `.../nd/ms/script` pour Network Dispatcher.

Haute disponibilité

La fonction haute disponibilité est disponible uniquement pour le composant Dispatcher.

Pour améliorer la disponibilité de Dispatcher, la fonction de haute disponibilité de Dispatcher utilise les mécanismes suivants :

- Deux répartiteurs connectés aux mêmes clients et à la même grappe de serveurs, ainsi qu'une connectivité entre les répartiteurs. Les deux répartiteurs doivent utiliser le même système d'exploitation.
- Un mécanisme de «signal de présence» entre les deux répartiteurs, afin de détecter les incidents au niveau de Dispatcher. Au moins, une des paires de signaux de présence doit disposer des NFA de la paire en tant qu'adresse source et de destination.

Au moins une des paires de signaux de présence doit utiliser si possible un sous-réseau différent du trafic classique de la grappe. Un trafic distinct de signaux de présence permet d'éviter les faux relais lors des fortes charges réseau et d'améliorer les temps de reprise totale.

- Une liste de cibles à atteindre, adresses que les deux machines Dispatcher doivent pouvoir contacter pour équilibrer leur trafic correctement. Pour plus de détails, reportez-vous à la section «Détections des incidents en utilisant signal de présence et cible à atteindre» à la page 176.
- La synchronisation des informations de Dispatcher (c'est-à-dire les tables de connexion, les tables d'accessibilité et d'autres informations).
- Une logique de sélection du répartiteur actif responsable d'une grappe de serveurs déterminée, et du répartiteur de secours qui est synchronisé en continu pour cette grappe de serveurs.
- Un mécanisme permettant une prise de contrôle IP plus rapide lorsque la logique ou un opérateur choisit l'état actif ou l'état de secours.

Remarque : Pour obtenir une description de la configuration *haute disponibilité réciproque* dans laquelle deux machines Dispatcher, qui partagent deux ensembles de grappe, se fournissent une sauvegarde mutuelle, reportez-vous à «Haute disponibilité réciproque» à la page 51. La haute disponibilité réciproque est semblable à la haute disponibilité mais se base sur l'adresse de grappe en particulier et non sur l'ensemble de la machine Dispatcher. Les deux machines doivent configurer de la même façon leur ensembles de grappe partagés.

Configuration de la haute disponibilité

La syntaxe complète de la **haute disponibilité ndcontrol** se trouve dans «ndcontrol highavailability — Contrôle de la haute disponibilité» à la page 280.

Pour plus d'informations sur les tâches détaillées ci-dessous, reportez-vous à la section «Configuration de la machine Dispatcher» à la page 60.

1. Lancez le serveur sur les deux machines serveurs Dispatcher.
2. Lancez l'exécuteur sur les deux machines.
3. Assurez-vous que l'adresse de non-réacheminement (NFA) de chaque machine Dispatcher est configurée et qu'il s'agit d'une adresse IP valide pour le sous-réseau des machines Dispatcher.

Windows 2000 uniquement : Configurez également chaque adresse NFA par la commande **ndconfig**. Par exemple :

```
ndconfig  
en0 adr_nfa netmask masqueréseau
```

4. Définissez les paramètres des grappes, des ports et des serveurs pour les deux machines.

Remarque : Pour la configuration de haute disponibilité réciproque (figure 14 à la page 51), Par exemple, configurez les ensembles de grappe partagés entre les deux machines Dispatcher de la manière suivante :

- Pour le Dispatcher 1, utilisez la commande :

```
ndcontrol cluster set clusterA primaryhost NFAdispatcher1  
ndcontrol cluster set clusterB primaryhost NFAdispatcher2
```

- Pour le Dispatcher 2, utilisez la commande :

```
ndcontrol cluster set clusterB primaryhost NFAdispatcher2  
ndcontrol cluster set clusterA primaryhost NFAdispatcher1
```

5. Lancez le gestionnaire et les conseillers sur les deux machines. Le conseiller reach démarre automatiquement par la fonction gestionnaire.
6. Créez des fichiers de scripts d'alias dans chacune des 2 machines Dispatcher. Reportez-vous à «Utilisation de scripts» à la page 178.
7. Configurez le système de "signal de présence" (heartbeat) sur les deux machines.

```
ndcontrol highavailability heartbeat add adresse_source adresse_destination
```

Remarque : Les variables *adresse_source* et *adresse_destination* ont pour valeur les adresses IP (noms DNS ou adresses en notation décimale à point) des machines Dispatcher. Ces valeurs seront inversées pour chaque machine. Exemple :

```
Machine principale (primary) -  
highavailability heartbeat add 9.67.111.3 9.67.186.8  
machine de secours (backup) - highavailability heartbeat  
add 9.67.186.8 9.67.111.3
```

Au moins, une des paires de signaux de présence doit disposer des NFA de la paire en tant d'adresse source et de destination.

Au moins une des paires de signaux de présence doit utiliser si possible un sous-réseau différent du trafic classique de la grappe. Un trafic distinct de signaux de présence permet d'éviter les faux relais lors des fortes charges réseau et d'améliorer les temps de reprise totale.

8. Sur les deux machines, utilisez la commande **reach add** pour configurer la liste des adresses IP auxquelles Dispatcher doit pouvoir accéder pour assurer un service complet. Exemple :

```
ndcontrol highavailability reach add 9.67.125.18
```

Les cibles à atteindre sont recommandées mais pas obligatoires.

Reportez-vous à «Détections des incidents en utilisant signal de présence et cible à atteindre» à la page 176, pour de plus amples informations.

9. Ajoute les données de sauvegarde à chaque machine :

- Pour la machine **primaire** :

```
ndcontrol highavailability backup add primary [auto |  
manual] port
```

- Pour la machine de **sauvegarde** :

```
ndcontrol highavailability backup add backup [auto |  
manual] port
```

- En cas de haute disponibilité réciproque, chaque machine Dispatcher joue **les deux** rôles de machine primaire et de secours :

```
ndcontrol highavailability backup add both [auto | manual] port
```

Remarque : Sélectionnez un port non utilisé sur les machines en tant que *port*. Vos deux machines vont communiquer par ce port.

10. Contrôlez l'état de la fonction de haute disponibilité pour chaque machine.

```
ndcontrol highavailability status
```

Chacune des machines doit avoir le rôle (primaire, secondaire ou les deux), les états et sous-états qui conviennent. La machine principale doit être active et synchronisée ; la machine de secours doit être en mode veille et se synchroniser rapidement avec l'autre. Les deux stratégies doivent être identiques.

Remarques :

1. Pour configurer une machine Dispatcher unique pour acheminer les paquets sans machine de secours, n'émettez aucune commande de haute disponibilité au moment de l'initialisation.
2. Pour passer de deux machines Dispatcher configurées pour la haute disponibilité à une seule machine autonome, arrêtez l'exécuteur sur l'une des machines, puis supprimez les fonctions de haute disponibilité (les signaux de présence, les seuils et la sauvegarde) sur l'autre machine.

3. Dans les deux cas ci-dessus, la carte d'interface réseau doit être reliée aux adresses de grappe par un alias, selon la procédure adaptée.
4. Lorsque deux machines Dispatcher sont exécutées en mode haute disponibilité et sont synchronisées, il est recommandé d'entrer toutes les commandes `ndcontrol` (afin de mettre à jour la configuration) sur la machine de secours puis sur la machine active.
5. Lorsque deux machines Dispatcher fonctionnent en mode haute disponibilité, des résultats imprévus peuvent se produire si l'on affecte des valeurs différentes à l'un ou l'autre des paramètres de l'exécuteur, des grappes, des ports ou des serveurs (par exemple, port délai de maintien de routage).
6. Dans le cas de la haute disponibilité réciproque, tenez compte du cas où l'une des machine Dispatcher doit acheminer des paquets de données à sa grappe principale tout en prenant en charge des paquets destinés à la grappe de sauvegarde. Assurez-vous que le débit n'excède pas les capacités de la machine.
7. Pour Linux, lors de la configuration simultanée de la haute disponibilité et de la co-implantation à l'aide de la méthode d'acheminement de port MAC du composant Dispatcher, vous devez installer un correctif de noyau Linux. Pour plus d'informations sur l'installation du correctif, reportez-vous à la section «Installation du correctif du noyau Linux (pour supprimer les réponses ARP sur l'interface de bouclage)» à la page 72.

Détections des incidents en utilisant signal de présence et cible à atteindre

Outre les critères de détection d'incidents de base (perte de connectivité entre le système Dispatcher de secours et le système Dispatcher actif, détectée via les messages de signal de présence), un autre mécanisme de détection d'incidents appelé *critères d'accessibilité* est disponible. Lorsque vous configurez Dispatcher, vous pouvez indiquer une liste d'hôtes auxquels chaque système Dispatcher doit pouvoir accéder pour fonctionner correctement.

Vous devez choisir au moins un hôte pour chaque sous-réseau que la machine Dispatcher utilise. Il peut s'agir de systèmes hôtes tels que les routeurs, les serveurs IP ou d'autres types d'hôtes. L'accessibilité de l'hôte est obtenue grâce au conseiller de contact qui lance un ping à l'hôte. Le basculement a lieu si les messages de signal de présence ne peuvent pas être transmis ou si les critères d'accessibilité sont mieux respectés par la machine Dispatcher de secours que par la machine Dispatcher principale. Pour prendre la décision sur la base de toutes les informations disponibles, le répartiteur actif envoie régulièrement au répartiteur de secours ses données d'accessibilité. La machine Dispatcher de secours compare ensuite ces données aux siennes, puis décide de procéder ou non au basculement.

Remarque : Lorsque vous configurez la cible d'accessibilité, vous devez également lancer le *conseiller reach*. Le conseiller reach démarre automatiquement par la fonction gestionnaire. Pour plus d'informations sur le conseiller de contact, reportez-vous à la section 150.

Stratégie de reprise

Deux machines Dispatcher sont configurées : la machine principale et une deuxième machine appelée machine de *sauvegarde* (ou de secours). Au lancement, la machine principale transmet toutes les données de connexion à la machine de secours afin d'obtenir une parfaite synchronisation. La machine principale devient *active*, c'est-à-dire qu'elle commence l'équilibrage de charge. Parallèlement, la machine de secours contrôle l'état de la machine principale et conserve l'état de *veille*.

Si, à tout instant, la machine de secours détecte une défaillance de la machine principale, elle prend le *relais* des fonctions d'équilibrage de charge de la machine principale et devient, à son tour, la machine active. Une fois la machine principale redevenue opérationnelle, les machines se comportent selon la *stratégie* de reprise après incident définie par l'utilisateur. Il existe deux types de stratégie :

Automatique

La machine principale reprend le routage des paquets de données dès qu'elle redevient opérationnelle.

Manuelle

La machine de secours continue le routage des paquets de données, même après que la machine principale soit redevenue opérationnelle. Une intervention manuelle est nécessaire pour rendre de nouveau active la machine principale et replacer la machine de secours en état de veille.

La stratégie définie doit être identique pour les deux machines.

La stratégie de reprise manuelle oblige l'utilisateur à forcer le routage des paquets vers une machine spécifique, à l'aide de la commande "takeover". La reprise manuelle s'avère utile lorsque l'autre machine doit subir des opérations de maintenance. La stratégie de reprise automatique est conçue pour un fonctionnement normal sans surveillance.

Pour une configuration de haute disponibilité réciproque, il n'existe pas de défaillance par grappe. Si l'une des machines est victime d'une défaillance, même si celle-ci ne concerne qu'une des grappes, l'autre machine prendra le relais pour chacune des deux grappes.

Remarque : Des informations de connexion peuvent se perdre pendant le relais. Il peut en résulter une interruption des connexions longues existantes (telnet, par exemple) utilisées au moment du relais.

Utilisation de scripts

Pour que Dispatcher puisse acheminer les paquets de données, chaque adresse de grappe doit posséder un alias la reliant à une interface réseau.

- Dans le cadre d'une configuration Dispatcher autonome, chaque adresse de grappe doit posséder un alias la reliant à une carte d'interface réseau (par exemple, en0, tr0).
- Dans une configuration de haute disponibilité :
 - Sur la machine active, chaque adresse de grappe doit posséder un alias la reliant à une carte d'interface réseau (par exemple, en0, tr0).
 - Sur la machine de secours, chaque adresse de grappe doit être reliée par un alias à une unité de bouclage (par exemple, lo0).
- Sur toute machine où l'exécuteur aura été arrêté, tous les alias doivent être supprimés pour éviter les conflits avec une machine venant d'être initialisée.

Dans la mesure où les machines Dispatcher changent d'état lorsqu'une défaillance est détectée, les commandes citées plus haut doivent être lancées automatiquement. Dispatcher exécutera des scripts créés par l'utilisateur pour le faire. Des scripts exemple sont disponibles dans le répertoire **...nd/servers/samples** et *doivent* être déplacés dans le répertoire **...nd/servers/bin** afin de s'exécuter.

Remarque : Pour une configuration de haute disponibilité réciproque chacun des scripts "go" est appelé par le Dispatcher à l'aide d'un paramètre d'identification de l'adresse primaire du Dispatcher. Le script doit rechercher ce paramètre et exécuter les commandes **ifconfig** (ou **ndconfig** sous Windows 2000) des adresses de grappe associées à ce Dispatcher primaire.

Les scripts exemples suivants peuvent être utilisés :

goActive

Le script goActive s'exécute lorsque l'un des systèmes Dispatcher devient actif et commence à acheminer les paquets de données.

- Si vous exécutez Dispatcher dans le cadre d'une configuration de haute disponibilité, vous devez créer ce script. Ce script doit supprimer les alias des unités de bouclage et en ajouter pour les autres périphériques.
- Si vous utilisez Dispatcher dans le cadre d'une configuration autonome, ce script n'est pas nécessaire.

goStandby

Le script goStandby s'exécute lorsqu'un système Dispatcher passe en mode veille. Il contrôle alors l'état de la machine active mais n'achemine pas de paquets.

- Si vous exécutez Dispatcher dans le cadre d'une configuration de haute disponibilité, vous devez créer ce script. Ce script doit supprimer les alias des périphériques et en ajouter pour les unités de bouclage.
- Si vous utilisez Dispatcher dans le cadre d'une configuration autonome, ce script n'est pas nécessaire.

goInOp

Le script goInOp s'exécute lorsqu'un exécuteur Dispatcher est arrêté et avant son premier lancement.

- Si vous exécutez Dispatcher généralement dans le cadre d'une configuration de haute disponibilité, il peut être nécessaire de créer ce script. Ce script supprime tous les alias de périphériques et de bouclage.
- Si vous utilisez généralement Dispatcher dans une configuration autonome, ce script est facultatif. Vous pouvez le créer afin qu'il supprime les alias de périphériques, ou les supprimer manuellement.

goIdle Le script goIdle s'exécute lorsqu'un des systèmes Dispatcher devient inactif et commence à acheminer les paquets de données. Cela se produit lorsque les fonctions de haute disponibilité n'ont pas été définies, comme dans le cas d'une configuration autonome. Cela peut également arriver dans une configuration de haute disponibilité, avant que ces fonctions n'aient été définies ou après qu'elles aient été supprimées.

- Si vous utilisez Dispatcher généralement dans une configuration de haute disponibilité, **ne créez pas** ce script.
- Si vous utilisez généralement Dispatcher dans une configuration autonome, ce script est facultatif. Vous pouvez le créer de sorte qu'il ajoute les alias de périphériques, ou les ajouter manuellement. Si vous ne créez pas ce script dans une configuration autonome, vous devez utiliser la commande **ndcontrol cluster configure** ou vous devez configurer manuellement les alias à chaque lancement de l'exécuteur.

highavailChange

Le script highavailChange s'exécute lorsque l'état de haute disponibilité est modifié dans le système Dispatcher, de telle sorte qu'un des scripts "go" est appelé. Le paramètre transmis à ce script correspond au nom du script "go" exécuté par Dispatcher.

Vous pouvez créer ce script pour utiliser les informations de changement d'état, par exemple, pour alerter un administrateur ou simplement pour enregistrer l'événement.

Remarque : Windows 2000 : si le composant Site Selector de la configuration équilibre la charge de deux machines Dispatcher fonctionnant en environnement à haute disponibilité, vous devrez définir un alias pour les systèmes Metric Server dans la pile Microsoft. Insérez cet alias dans le script goActive. Par exemple :

```
call netsh interface ip add  
address "Local Area Connection"  
addr=9.37.51.28 mask=255.255.240.0
```

Supprimez les alias des scripts goStandby et GoInOp. Par exemple :

```
call netsh  
interface ip delete address "Local Area Connection"  
addr=9.37.51.28
```

Si la machine est équipée de plusieurs cartes d'interface réseau, vérifiez dans un premier temps l'interface à utiliser en entrant la commande suivante au niveau de l'invite : netsh interface ip show address. Elle renvoie la liste des interfaces configurées et le numéro de la connexion au réseau local (par exemple, "Local Area Connection 2") permettant de déterminer celle à utiliser.

Configuration de l'équilibrage basé sur des règles

Vous pouvez utiliser un équilibrage basé sur des règles pour déterminer de manière précise quand et pourquoi des paquets sont envoyés à des serveurs et quels sont ces serveurs. Network Dispatcher parcourt toute les règles que vous ajoutez, de la première à la dernière priorité et s'arrête sur la première règle vérifiée avant d'équilibrer la charge en fonction du contenu entre les serveurs associés à cette règle. Ils équilibrent déjà la charge en fonction de la destination et du port, mais l'utilisation de règles permet d'étendre votre capacité à répartir les connexions.

Dans la plupart des cas lors de la configuration de règles, vous devez configurer une règle par défaut **toujours vraie** afin d'intercepter les demandes provenant des autres règles de priorité élevée. Il peut s'agir d'une réponse du type "Désolé, ce site est actuellement inaccessible. Faites une nouvelle tentative ultérieurement" lorsque tous les autres serveurs ne peuvent pas traiter la demande client.

Vous devez utiliser l'équilibrage de charge dépendant des règles avec Dispatcher et Site Selector lorsque vous voulez utiliser un sous-ensemble de serveurs pour une raison quelconque. Vous *devez* toujours utiliser des règles pour le composant CBR.

Remarque : La configuration utilisant des règles ne s'applique *pas* à Mailbox Locator (qui transmet par proxy des demandes IMAP ou POP3 à des serveurs spécifiques en fonction de l'ID utilisateur et du mot de passe) ou à Cisco Consultant (qui utilise les fonctions de gestionnaire et de conseillers pour fournir des informations d'équilibrage de charge à Cisco CSS Switch).

Vous pouvez sélectionner les types de règles suivants :

- Pour Dispatcher :
 - Adresse IP du client
 - Heure
 - Nombre de connexions par seconde d'un port
 - Nombre total de connexions actives d'un port
 - Port du client
 - Type de service (TOS)
 - Largeur de bande réservée
 - Largeur de bande partagée
 - Toujours vraie
 - Contenu d'une demande
- Pour CBR :
 - Adresse IP du client
 - Heure
 - Nombre de connexions par seconde d'un port
 - Nombre total de connexions actives d'un port
 - Toujours vraie
 - Contenu d'une demande
- Pour Site Selector :
 - Adresse IP du client
 - Heure
 - Mesure de tous les serveurs
 - Moyenne des mesures
 - Toujours vraie

Il est recommandé de planifier la logique à suivre par les règles avant de commencer à ajouter des règles à votre configuration.

Evaluation des règles

Toutes les règles possèdent un nom, un type, une priorité et peuvent avoir une valeur de début et une valeur de fin ainsi qu'un ensemble de serveurs. En outre, à la règle de type contenu du composant CBR est associée une structure d'expression standard. (Pour obtenir des exemples et des scénarios sur le mode d'utilisation de la règle de contenu et la syntaxe de motif valide pour la règle de contenu, reportez-vous à la section «Annexe C. Syntaxe des règles de contenu (modèle)» à la page 323.)

Les règles sont évaluées en fonction de leur priorité. En d'autres termes, une règle de priorité 1 (nombre le moins élevé) avant une règle de priorité 2 (nombre plus élevé). La première règle vérifiée est utilisée. Une fois la règle vérifiée, aucune autre règle n'est évaluée.

Pour qu'une règle soit vérifiée, elle doit remplir deux conditions :

1. Le prédicat de cette règle doit être vrai. C'est-à-dire que la valeur évaluée doit être comprise entre la valeur de début et la valeur de fin, ou que le contenu doit correspondre à l'expression standard spécifiée dans la structure de la règle de type contenu. Pour les règles de type "vraie", le prédicat est toujours respecté, quelles que soient les valeurs de début et de fin.
2. Si des serveurs sont associés à cette règle, l'un d'eux au moins doit être disponible pour recevoir des paquets.

Si aucun serveur n'est associé à une règle, cette dernière ne doit remplir que la première condition pour être vérifiée. Dans ce cas, Dispatcher abandonne la demande de connexion, Site Selector renvoie la demande de serveur de nom avec une erreur et CBR provoque une page d'erreur Caching Proxy.

Si aucune règle n'est vérifiée, Dispatcher sélectionne un serveur parmi l'ensemble des serveurs disponibles du port, Site Selector sélectionne un serveur parmi l'ensemble des serveurs disponibles sur le nom du site et CBR provoque l'affichage d'une page d'erreur par Caching Proxy.

Utilisation de règles basées sur l'adresse IP des clients

Ce type de règle est disponible dans le composant Dispatcher, CBR ou Site Selector.

Vous pouvez souhaiter utiliser des règles basées sur l'adresse IP des clients pour trier les clients et leur affecter des ressources en fonction de leur provenance.

Par exemple, vous constatez la présence sur le réseau d'un nombre important de transmissions impayées et donc indésirables en provenance de clients

appartenant à un ensemble spécifique d'adresses IP. Vous créez donc une règle à l'aide de la commande **ndcontrol rule**. Par exemple :

```
ndcontrol rule add 9.67.131.153:80:ni type ip beginrange 9.0.0.0 endrange 9.255.255.255
```

Cette règle "ni" permet de trier les connexions de clients IBM. Dans le cas contraire, les demandes provenant des adresses 9.x.x.x ne seront pas transmises par l'un de vos serveurs.

Utilisation de règles basées sur l'heure

Ce type de règle est disponible dans le composant Dispatcher, CBR ou Site Selector.

Vous pouvez souhaiter utiliser des règles basées sur l'heure en vue de la planification des pondérations. Si par exemple votre site Web est surchargé chaque jour pendant les mêmes créneaux horaires, il est préférable de dédier à HTTP cinq serveurs à plein temps, puis d'en ajouter cinq autres aux heures de pointe.

Ce type de règle est également intéressant lorsque vous voulez arrêter certains serveurs chaque jour à minuit, pour des raisons de maintenance. Dans ce cas, vous devez définir une règle qui exclut ces serveurs pendant la période de maintenance nécessaire.

Utilisation de règles basées sur le nombre de connexions par seconde d'un port

Ce type de règle est disponible dans le composant Dispatcher et CBR.

Remarque : Le gestionnaire doit être lancé pour exécuter les opérations suivantes.

Vous pouvez souhaiter utiliser des règles basées sur le nombre de connexions par seconde d'un port lorsque vous devez partager certains serveurs avec d'autres applications. Vous pouvez, par exemple, définir deux règles :

1. Si le nombre de connexions par seconde du port 80 > 100, utiliser ces 2 serveurs
2. Si le nombre de connexions par seconde du port 80 > 2000, utiliser ces 10 serveurs

Vous pouvez aussi utiliser Telnet et vouloir lui réserver deux des cinq serveurs, sauf lorsque le nombre de connexions par seconde dépasse un certain niveau. Ainsi, Dispatcher équilibre la charge entre les cinq serveurs, pendant les heures de pointe.

Utilisation de règles basées sur le nombre total de connexions actives d'un port

Ce type de règle est disponible dans le composant Dispatcher ou CBR.

Remarque : Le gestionnaire doit être lancé pour exécuter les opérations suivantes.

Vous pouvez souhaiter utiliser des règles basées sur le nombre total de connexions actives d'un port lorsque les serveurs sont surchargés et commencent à ignorer certains paquets. Dans ce cas, certains serveurs Web continuent d'accepter les connexions même s'ils ne disposent pas d'un nombre suffisant d'unités d'exécution pour répondre à la demande. Il en résulte que le poste client réclame un certain délai de temporisation et que le client accédant à votre site Web n'est pas servi. Vous pouvez utiliser des règles basées sur le nombre de connexions actives pour équilibrer les pondérations d'un pool de serveurs.

Par exemple, vous savez par expérience que les serveurs arrêteront leur service après avoir accepté 250 connexions. Vous pouvez créer une règle à l'aide de la commande **ndcontrol rule** ou **cbrcontrol rule**. Par exemple :

```
ndcontrol rule add 130.40.52.153:80:pool2 type active beginrange 250  
beginrange 250 endrange 500
```

ou

```
cbrcontrol rule add 130.40.52.153:80:pool2 type active  
beginrange 250 endrange 500
```

Vous pouvez ensuite ajouter à la règle vos serveurs en cours plus d'autres serveurs qui, autrement seraient utilisés pour d'autres processus.

Utilisation de règles basées sur le port du client

Ce type de règle est disponible uniquement avec le composant Dispatcher.

Vous pouvez souhaiter utiliser des règles basées sur le port client lorsque vos clients utilisent un type de logiciel nécessitant un port spécifique de TCP/IP lors des demandes.

Vous pouvez, par exemple, créer une règle spécifiant que toute demande dont le port client est 10002, doit utiliser un ensemble de serveurs rapides spéciaux car vous savez que les demandes client associées à ce port proviennent d'un groupe de clients privilégiés.

Utilisation de règles basées sur le type de services (TOS)

Ce type de règle est disponible uniquement avec le composant Dispatcher.

Vous pouvez souhaiter utiliser des règles fondées sur le contenu du champ "type de service" (TOS) de l'en-tête IP. Par exemple, si la valeur TOS d'une demande client entrante indique un service normal, cette demande peut être routée vers un ensemble de serveurs. Si une autre demande arrive, munie

cette fois d'une valeur TOS différente indiquant une priorité de service élevée, elle peut être dirigée vers un autre ensemble de serveurs.

La règle TOS permet de configurer entièrement chacun des bits de l'octet TOS en utilisant la commande **ndcontrol rule**. Utilisez 0 ou 1 pour les bits importants que vous souhaitez apparier dans l'octet TOS. La valeur x est utilisée par défaut. Voici un exemple d'ajout d'une règle TOST :

```
ndcontrol rule add 9.67.131.153:80:tsr type service tos 0xx1010x
```

Utilisation de règles basées sur la largeur de bande réservée et sur la largeur de bande partagée

L'utilisation de la capacité et les règles de largeur de bande sont disponibles uniquement dans le composant Dispatcher.

Via la fonction d'utilisation de la capacité, Dispatcher mesure le montant des données transmises à chaque serveur. Dispatcher effectue le suivi de la capacité aux niveaux du serveur, de la règle, du port, de la grappe et de l'exécuteur. Pour chacun de ces niveaux, il existe une nouvelle contre-valeur d'octet : les kilo-octets transmis par seconde. La valeur (kilo-octets transférés par seconde) est calculée sur un intervalle de 60 secondes. Vous pouvez consulter ces valeurs de capacité dans l'interface ou dans la sortie d'un rapport de ligne de commande.

Dispatcher permet d'attribuer une largeur de bande indiquée à des ensembles de serveurs dans votre configuration à l'aide de la règle *largeur de bande réservée*. Lorsque le trafic dépasse le seuil de largeur de bande réservée, vous pouvez effectuer une des actions suivantes :

- Envoyer le trafic à un autre serveur, en utilisant une règle toujours vraie, qui répond avec une réponse de type "site occupé"
- ou partagez un montant défini de largeur de bande au niveau de la grappe ou de l'exécuteur à l'aide de la règle *largeur de bande partagée*. Et, lorsque vous vous approchez de la limite générale de largeur de bande partagée, vous pouvez diriger le trafic vers un autre serveur, via la règle toujours vraie, qui répond avec une réponse de type "site occupé".

En utilisant la règle de largeur de bande partagée avec la règle de largeur de bande réservée, comme il est décrit ci-dessus, vous pouvez fournir aux clients préférés un accès au serveur plus rapide et ainsi améliorer les performances liées aux transactions. Par exemple, en utilisant la règle de largeur de bande partagée afin d'exploiter la largeur de bande non utilisée, vous pouvez permettre aux clients d'effectuer des affaires sur des grappes de serveurs. Ainsi l'accès est plus important que lorsque les clients utilisent d'autres grappes de serveurs pour la recherche d'investissements.

Prenez en compte les éléments suivants afin de déterminer si les règles de largeur de bande peuvent vous aider à gérer le volume du trafic de réponses des serveurs vers les clients :

- Les règles de largeur de bande peuvent vous aider à gérer le volume du trafic de réponses provenant d'un ensemble de serveurs, basé sur les demandes client, et passant via Network Dispatcher. Si une partie du trafic client passe directement aux serveurs sans être vue par Network Dispatcher, les résultats peuvent être imprévisibles.
- Les règles de largeur de bande peuvent vous aider à gérer le volume du trafic des réponses transitant via un lien d'un ensemble de serveurs du réseau lorsque tous les serveurs utilisent le même lien réseau. Si les serveurs utilisent des liens différents ou plusieurs liens pour accéder au réseau, les résultats générés pour chaque lien peuvent être imprévisibles.
- Les règles de largeur de bande sont utiles uniquement lorsque tous les serveurs se trouvent sur le même réseau local que la machine Network Dispatcher. Si certains serveurs sont éloignés, ayant différents chemins d'accès au réseau, les résultats peuvent alors être imprévisibles.

Règle de largeur de bande réservée

Ce type de règle est disponible uniquement avec le composant Dispatcher.

La règle de largeur de bande réservée permet d'effectuer l'équilibrage de charge en fonction du nombre de kilo-octets délivrés par seconde à un ensemble de serveurs. En définissant un seuil (définition d'une plage de largeur de bande précise) pour chaque ensemble de serveurs dans la configuration, vous pouvez contrôler et garantir le montant de la largeur de bande utilisé par chaque combinaison grappe-port. Ci-dessous, se trouve un exemple permettant d'ajouter une règle de largeur de bande réservée :

```
ndcontrol rule add 9.67.131.153:80:rbw type reservedbandwidth  
beginrange 0 endrange 300
```

Les valeurs de début et de fin sont indiquées en kilo-octets par seconde.

Règle de largeur de bande partagée

Ce type de règle est disponible uniquement avec le composant Dispatcher.

Si le montant de données transférées dépasse la limite de la règle de la largeur de bande réservée, la règle de largeur de bande partagée vous permet d'exploiter la largeur de bande non utilisée disponible sur le site. Vous pouvez configurer cette règle afin de partager la largeur de bande au niveau de la grappe ou au niveau de l'exécuteur. Le partage de la largeur de bande au niveau de la grappe permet à un port (ou à des ports) de partager une quantité maximale de largeur de bande entre plusieurs ports (applications/protocoles) d'une même grappe. Le partage de la largeur de

bande au niveau de l'exécuteur permet à une grappe (ou à des grappes) de la configuration Dispatcher de partager une quantité maximale de largeur de bande.

Avant de configurer la règle de largeur de bande partagée, vous devez indiquer la quantité maximale de largeur de bande (kilo-octets par seconde) pouvant être partagée au niveau de l'exécuteur ou de la grappe à l'aide de la commande **ndcontrol executor** ou **ndcontrol cluster** avec l'option **sharedbandwidth**. Ci-dessous, se trouvent des exemples de la syntaxe de la commande.

```
ndcontrol executor set sharedbandwidth taille  
ndcontrol cluster [add | set] 9.12.32.9 sharedbandwidth taille
```

La *taille* de l'option **sharedbandwidth** correspond à une valeur entière (kilo-octets par seconde). La valeur par défaut est zéro. Si la valeur est zéro, la bande passante ne peut pas être partagée. Vous devez indiquer une valeur **sharedbandwidth** maximale qui ne dépasse pas la largeur de bande totale (capacité de serveur totale) disponible.

Ci-dessous, se trouvent des exemples d'ajout ou de définition d'une règle **sharedbandwidth**.

```
ndcontrol rule add 9.20.30.4:80:shbw type sharedbandwidth sharelevel valeur  
ndcontrol rule set 9.20.34.11:80:shrul sharelevel valeur
```

La *valeur* de l'option **sharelevel** est soit exécuteur, soit grappe. **Sharelevel** est un paramètre requis dans la règle **sharebandwidth**

Règle Mesure de tous les serveurs

Ce type de règle est disponible uniquement dans le composant Site Selector.

Pour la règle Mesure de tous les serveurs, vous choisissez une mesure système (cpuload, memload ou votre propre script de mesure système personnalisé) et Site Selector compare la valeur de mesure système (renvoyée par l'agent du système Metric Server se trouvant dans chaque serveur d'équilibrage de charge) avec les valeurs de début et de fin indiquées dans la règle. La valeur de mesure de tous les serveurs de l'ensemble de serveurs doit être définie dans la plage afin que la règle puisse être mise en application.

Remarque : Le script de mesure système choisi doit se trouver sur chaque serveur d'équilibrage de charge.

Ci-dessous, se trouve un exemple d'ajout de mesure à toutes les règles de la configuration.

```
sscontrol rule add dnsload.com:allrule1 type metricall  
metricname cpuload beginrange 0 endrange 100
```

Règle Moyenne des mesures

Ce type de règle est disponible uniquement dans le composant Site Selector.

Pour la règle Moyenne des mesures, vous choisissez une mesure système (cpuload, memload ou votre propre script de mesure système personnalisé) et Site Selector compare la valeur de mesure système (renvoyée par l'agent du système Metric Server se trouvant dans chaque serveur d'équilibrage de charge) avec les valeurs de début et de fin indiquées dans la règle. La *moyenne* des valeurs des mesures système de tous les serveurs de l'ensemble de serveurs doit être définie dans la plage pour que la règle puisse être mise en application.

Remarque : Le script de mesure système choisi doit se trouver sur chaque serveur d'équilibrage de charge.

Ci-dessous, se trouve un exemple d'ajout de règle de moyenne des mesures à votre configuration.

```
sscontrol rule add dnsload.com:avgrule1 type metricavg  
metricname cpuload beginrange 0 endrange 100
```

Utilisation de règles toujours vraies

Ce type de règle est disponible dans le composant Dispatcher, CBR ou Site Selector.

Une règle peut être créée comme règle "toujours vraie." Ces règles seront toujours sélectionnées, sauf si tous les serveurs associés sont arrêtés. Pour cette raison, leur niveau de priorité est généralement inférieur à celui de autres règles.

Vous pouvez même avoir plusieurs règles "toujours vraies", chacune d'elles associée à un ensemble de serveurs. La première règle vérifiée pour laquelle un serveur est disponible est choisie. Supposons par exemple que vous disposiez de six serveurs. Vous voulez que deux d'entre eux traitent le trafic quelles que soient les circonstances, à moins qu'ils soient tous les deux arrêtés. Si les deux premiers serveurs sont arrêtés, vous voulez qu'un deuxième jeu de serveurs traite le trafic. Enfin, si les quatre serveurs sont arrêtés, vous utiliserez les deux derniers pour traiter le trafic. Vous pouvez définir trois règles "toujours vraie". Le premier jeu de serveurs est toujours choisi, tant que l'un d'eux est actif. Si les deux serveurs sont arrêtés, l'un des serveurs du deuxième jeu est choisi, etc.

Autre exemple : il se peut que vous vouliez une règle "toujours vraie" pour garantir que les clients entrants qui ne remplissent aucune des règles définies ne sont pas pris en charge. Il vous faut donc créer, à l'aide de la commande **ndcontrol rule**, la règle suivante :

```
ndcontrol rule add 130.40.52.153:80:jamais type true priority 100
```


Vous n'ajoutez alors pas de serveur à cette règle, ce qui provoque l'abandon sans réponse des paquets des clients.

Remarque : Il n'est pas nécessaire de définir de valeur de début et de fin lors de la création d'un règle Toujours vraie.

Vous pouvez définir plusieurs règles "toujours vraies", puis choisir ensuite celle qui doit être exécutée en modifiant les niveaux de priorité.

Utilisation de règles basées sur le contenu des demandes

Ce type de règle est disponible dans le composant Dispatcher ou CBR.

Vous pouvez utiliser des règles basées sur le contenu pour envoyer des demandes à des ensembles de serveurs spécialement configurés pour prendre en charge une partie du trafic de votre site. Par exemple, vous pouvez utiliser un ensemble de serveurs pour la prise en charge de toutes les demandes *cgi-bin*, un autre pour les demandes audio, et un troisième pour toutes les autres demandes. Vous pouvez ajouter une règle dont la structure correspond au chemin d'accès du répertoire *cgi-bin*, une autre correspondant au type de vos fichiers audio, et une troisième règle "toujours vraie" pour prendre en charge le reste du trafic. Vous ajouterez ensuite les serveurs appropriés à chaque type de règle.

Important : Pour obtenir des exemples et des scénarios sur le mode d'utilisation de la règle de contenu et la syntaxe de modèle valide pour la règle de contenu, reportez-vous à la section «Annexe C. Syntaxe des règles de contenu (modèle)» à la page 323.

Ajout de règles à la configuration

Vous pouvez ajouter des règles à l'aide de la commande **ndcontrol rule add**, en modifiant le fichier de configuration exemple ou en utilisant l'interface graphique. Vous pouvez ajouter une ou plusieurs règles à chaque port que vous avez défini.

Il s'agit d'une procédure en deux étapes : vous devez ajouter la règle, puis définir les serveurs sur lesquels les services doivent être effectués si la règle est vraie. Supposons par exemple que l'administrateur système veuille déterminer le taux d'utilisation des serveurs proxy pour chaque division du site. Il connaît les adresses IP de chacune de ces divisions. Il doit créer le premier jeu de règles en fonction des adresses IP des clients pour séparer les charges individuelles de chaque division :

```
ndcontrol rule add 130.40.52.153:80:div1 type ip b 9.1.0.0 e 9.1.255.255
ndcontrol rule add 130.40.52.153:80:div2 type ip b 9.2.0.0 e 9.2.255.255
ndcontrol rule add 130.40.52.153:80:div3 type ip b 9.3.0.0 e 9.3.255.255
```

Il doit ensuite ajouter un serveur distinct à chaque règle, puis mesurer la charge de chaque serveur pour facturer correctement les divisions en fonction des services qu'elles utilisent. Par exemple :

```
ndcontrol rule useserver 130.40.52.153:80:div1 207.72.33.45
ndcontrol rule useserver 130.40.52.153:80:div2 207.72.33.63
ndcontrol rule use server 130.40.52.153:80:div3 207.72.33.47
```

Option d'évaluation de serveur

L'option d'évaluation de serveur est disponible uniquement dans le composant Dispatcher.

Dans la commande **ndcontrol rule**, il existe une option d'évaluation de serveur pour les règles. L'option *evaluate* permet de choisir d'évaluer les conditions de la règle parmi tous les serveurs du port ou d'évaluer les conditions de la règle des serveurs faisant partie de la règle. (Dans les versions précédentes de Network Dispatcher, il n'était possible de mesurer que la condition de chaque règle parmi tous les serveurs du port.)

Remarque : L'option d'évaluation de serveur est valide uniquement pour les règles prenant leurs propres décisions en fonction des caractéristiques des serveurs : règle du nombre total de connexions (par seconde), règle des connexions actives et règle de largeur de bande réservée.

Ci-dessous, se trouvent des exemples d'ajout ou de définition de l'option d'évaluation au niveau d'une règle de largeur de bande réservée.

```
ndcontrol rule add 9.22.21.3:80:rbweval type reservedbandwidth evaluate niveau
ndcontrol rule set 9.22.21.3:80:rbweval evaluate niveau
```

Vous pouvez attribuer la valeur port ou règle au *niveau* d'évaluation. La valeur par défaut est port.

Evaluation des serveurs dans la règle

L'option permettant de mesurer les conditions de la règle dans les serveurs de la règle permet de configurer deux règles ayant les caractéristiques suivantes :

- La première règle évaluée contient tous les serveurs gérant le contenu du site Web et la valeur *règle* est attribuée à l'option d'évaluation (évaluation des conditions de la règle dans les serveurs de la règle).
- La deuxième règle est une règle Toujours vraie qui contient un seul serveur qui répond par une réponse de type "site occupé".

Par conséquent, lorsque le trafic dépasse le seuil des serveurs dans la première règle, le trafic sera envoyé au serveur "site occupé" dans la deuxième règle. Lorsque le trafic est inférieur au seuil des serveurs de la première règle, le trafic reprend pour les serveurs de la première règle.

Evaluation des serveurs sur le port

Lors de l'utilisation des deux règles décrites dans l'exemple précédent, si vous attribuez l'option *port* à l'option d'évaluation pour la première règle (évaluation des conditions de la règle dans tous les serveurs du port), lorsque le trafic dépasse la limite de cette règle, le trafic est envoyé au serveur "site occupé" associé à la deuxième règle.

La première règle mesure l'ensemble du trafic du serveur (incluant le serveur "site occupé") sur le port afin de déterminer si le trafic a dépassé la limite. Alors que la surcharge diminue pour les serveurs associés à la première règle, le trafic se poursuit sur le serveur "site occupé" étant donné que le trafic sur ce port dépasse toujours la limite de la première règle.

Utilisation de liens explicites

En règle générale, les fonctions d'équilibrage de charge de Dispatcher fonctionnent indépendamment de la physionomie des sites sur lesquels le produit est installé. Il existe une zone, cependant, dans laquelle le contenu du site peut s'avérer important, et dans laquelle les décisions prises au sujet de ce contenu peuvent avoir une influence non négligeable sur l'efficacité de Dispatcher. Il s'agit de la zone d'adressage de liens.

Lorsque vos pages indiquent des liens pointant sur des serveurs individuels de votre site, un client est en réalité forcé à s'adresser à une machine déterminée, détournant de ce fait toute fonction d'équilibrage de charge éventuellement mise en oeuvre. Pour cette raison, il est conseillé d'utiliser systématiquement l'adresse de Dispatcher dans tous les liens figurant sur vos pages. Il est à noter que le type d'adressage utilisé n'est pas toujours apparent, notamment si votre site applique une procédure de programmation automatique permettant la création dynamique de HTML. Pour optimiser l'équilibrage de charge, identifiez les éventuelles occurrences d'adressage explicite et évitez-les autant que possible.

Utilisation d'une configuration réseau privée

Vous pouvez configurer Dispatcher et les machines serveurs TCP de sorte qu'ils utilisent un réseau privé. Cette configuration peut réduire l'encombrement des accès utilisateurs ou du réseau externe, susceptible d'affecter les performances.

Pour AIX, cette configuration peut également tirer parti des vitesses élevées du commutateur SP High Performance Switch, si vous utilisez Dispatcher et les machines serveurs TCP comme noeuds sur une Frame SP.

Pour créer un réseau privé, chaque machine doit être équipée d'au moins deux cartes de réseau local, l'une d'elles étant reliée au réseau privé.

La deuxième carte de réseau local doit être également configurée sur un sous-réseau différent. La machine Dispatcher transmettra alors les demandes aux machines serveurs TCP par l’intermédiaire du réseau privé.

Windows 2000 : Exécutez la commande suivante :

```
ndconfig en1 10.0.0.x netmask 255.255.255.0
```

en1 est le nom de la deuxième carte installée sur la machine Dispatcher, 10.0.0.x est l’adresse de réseau de la deuxième carte, et 255.255.255.0 est le masque de réseau du réseau privé.

Les serveurs ajoutés à l’aide de la commande **ndcontrol server add** doivent être ajoutés avec les adresses de réseau privé. Par exemple, reprenant le cas du serveur A de la figure 27, la syntaxe de la commande sera la suivante :

```
ndcontrol server add adresse_grappe:80:10.0.0.1
```

et non

```
ndcontrol server add adresse_grappe:80:9.67.131.18
```

Si vous utilisez Site Selector pour fournir des données de charge à Dispatcher, Site Selector doit être configuré pour acheminer ces états vers les adresses privées.

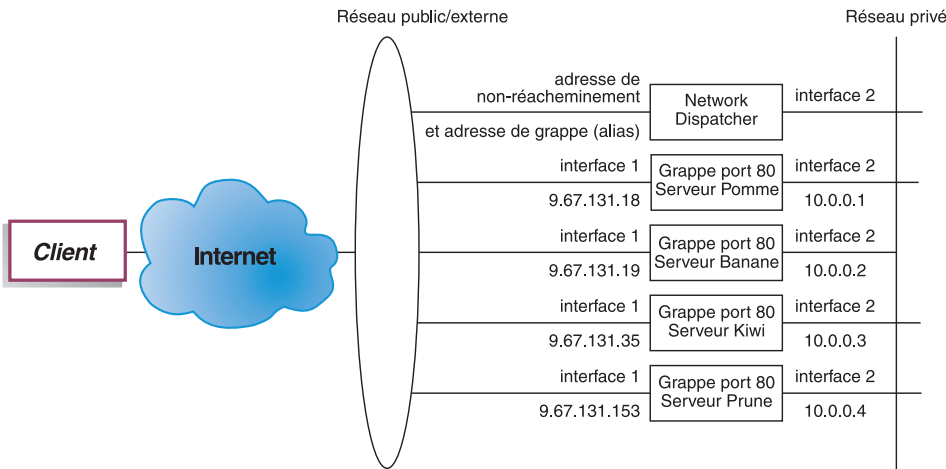


Figure 27. Exemple de réseau privé utilisant Dispatcher

L’utilisation d’une configuration de réseau privé s’applique uniquement au composant Dispatcher.

Utilisation d'une grappe générique pour combiner les configurations serveurs

Le terme "générique" fait référence à l'aptitude de la grappe à s'adapter à plusieurs adresses IP (c'est-à-dire à fonctionner comme un "joker"). L'adresse de grappe 0.0.0.0 est utilisé pour spécifier une grappe générique.

Si vous devez assurer l'équilibrage de plusieurs adresses de grappe ayant des configurations port/serveur identiques, vous pouvez combiner toutes les grappes dans une seule configuration "**".

Vous devez toujours configurer de manière explicite chaque adresse de grappe sur les cartes réseau de votre poste Dispatcher. Toutefois, vous ne devez ajouter aucune des adresses de grappe à la configuration de Dispatcher à l'aide de la commande `ndcontrol cluster add`.

Ajoutez simplement la grappe générique (adresse 0.0.0.0), et configurez les ports et les serveurs correctement pour l'équilibrage de charge. Tout trafic à destination des adresses configurées sur les cartes sera équilibré en utilisant la configuration de la grappe générique.

L'avantage de cette approche réside dans le fait que le trafic vers toutes les adresses de grappes est pris en compte lors du choix du meilleur serveur. Si une grappe est particulièrement chargée et qu'elle a créé de nombreuses connexions sur l'un des serveurs, le trafic vers les autres adresses de grappes sera équilibré en tenant compte de cette information.

Vous pouvez combiner la grappe générique avec des grappes réelles si certaines adresses de grappes ont une configuration port/serveur unique alors que d'autres partagent la même configuration. Les configurations uniques doivent être attribuées à une adresse de grappe réelle. Toutes les configurations communes peuvent être attribuée à la grappe générique.

L'utilisation d'une grappe générique pour combiner les configurations serveurs s'applique uniquement au composant Dispatcher.

Utilisation de la grappe générique pour équilibrer la charge des pare-feux

L'utilisation de la grappe générique pour équilibrer la charge des pare-feux s'applique uniquement au composant Dispatcher. L'adresse 0.0.0.0 permet d'indiquer une grappe générique.

Vous pouvez utiliser la grappe générique pour équilibrer le trafic vers des adresses qui ne sont pas explicitement configurées sur une carte réseau du poste Dispatcher. Pour que cela fonctionne, le répartiteur doit au moins être en mesure de voir la totalité du trafic qu'il est supposé équilibrer. Le poste répartiteur ne verra pas le trafic vers des adresses non explicitement

configurées sur l'une de ses cartes réseau, excepté s'il est configuré en tant que route par défaut pour certains trafic.

Une fois le répartiteur configuré comme route par défaut, le trafic TCP ou UDP passant par le poste répartiteur est équilibré en utilisant la configuration de la grappe générique.

C'est ce principe qui est utilisé pour équilibrer les pare-feux. Les pare-feux peuvent traiter des paquets à destination de n'importe quelle adresse et de n'importe quel port. Pour cette raison, vous devez être en mesure d'équilibrer le trafic indépendamment de l'adresse ou du port cible.

Les pare-feux permettent de gérer le trafic de clients non sécurisés vers des serveurs sécurisés et les réponses de ces serveurs, ainsi que le trafic de clients sécurisés vers des serveurs non sécurisés et les réponses de ces derniers.

Vous devez configurer deux machines Dispatcher : l'une pour envoyer le trafic non-sécurisé vers les adresses de pare-feux non sécurisés et l'autre le trafic sécurisé vers les adresses de pare-feux sécurisés. Comme ces deux postes répartiteurs doivent utiliser la grappe générique et le port générique avec des adresses de serveur différentes, les deux répartiteurs doivent se trouver sur deux machines distinctes.

Utilisation de grappe générique avec Caching Proxy pour le proxy transparent

L'utilisation de la grappe générique avec Caching Proxy pour le proxy transparent s'applique uniquement au composant Dispatcher. L'adresse 0.0.0.0 permet d'indiquer une grappe générique.

La fonction de grappe générique permet également d'utiliser Dispatcher pour activer une fonction de proxy transparent pour un serveur Caching Proxy se trouvant sur le même poste que Dispatcher. Cette fonction est disponible sous AIX uniquement car il doit y avoir communication entre le composant dispatcher et le composant TCP du système d'exploitation.

Pour activer cette fonction, vous devez lancer Caching Proxy écoutant les demandes client sur le port 80. Vous configurez ensuite une grappe générique. Dans la grappe générique, vous configurez le port 80. Dans le port 80, vous configurez l'adresse NFA de la machine Dispatcher en tant que serveur unique. Désormais, tout trafic client vers une adresse du port 80 sera acheminé vers le serveur Caching Proxy exécuté sur le poste de travail Dispatcher. La demande client est ensuite traitée par un proxy et la réponse est envoyée de Caching Proxy au client. Dans ce mode, le composant Dispatcher n'effectue pas l'équilibrage de charge.

Utilisation du port générique pour acheminer le trafic destiné à un port non configuré

Le port générique permet de gérer le trafic destiné à un port non explicitement configuré. Ce principe est utilisé pour équilibrer la charge des pare-feux. Il est également utilisé pour assurer la bonne gestion du trafic destiné à un port non configuré. En définissant un port générique, vous garantisiez que toutes les demandes en direction de ce port non configuré seront supprimées et non renvoyées au système d'exploitation. Le numéro de port 0 (zéro) permet d'indiquer un port générique, par exemple :

```
ndcontrol port add cluster:0
```

Remarque : Le port générique ne peut pas être utilisé pour le traitement du trafic FTP.

Fonctionnement de la fonction d'affinité pour Network Dispatcher

Vous activez la fonction d'affinité lorsque vous faites en sorte que le maintien de routage d'un port de grappes soit conservé. Lorsque vous configurez un port de grappe de telle sorte que le routage soit conservé, les demandes clients peuvent être dirigées vers le même serveur. Cette opération peut être effectuée en attribuant un nombre de secondes à l'option "port délai de maintien de routage". Lorsque vous attribuez la valeur zéro au délai de maintien de routage, cette fonction est désactivée.

Interaction avec l'affinité trans port : Lors de l'activation de l'affinité trans port, les valeurs de délai de maintien de routage des ports partagés doit avoir la même valeur (différente de zéro). Pour obtenir plus d'informations, reportez-vous à la section «Affinité trans ports» à la page 197.

Comportement lors de la désactivation de l'affinité

Lorsque cette fonction est désactivé, dès qu'une connexion TCP est reçue d'un client, Dispatcher utilise le serveur correct et lui transmet les paquets. Si une autre connexion arrive du même client, Dispatcher la traite comme si les deux connexions n'étaient pas liées et utilise à nouveau le serveur correct.

Comportement lors de l'activation de l'affinité

Lorsque cette fonction est activée, si une autre demande est reçue du même client, la demande est acheminée vers le même serveur.

Progressivement, le client arrête d'envoyer des transactions et l'enregistrement d'affinité disparaît. D'où la notion de "délai de maintien de routage." La durée de vie de chaque enregistrement d'affinité est déterminée en secondes par le "délai de maintien de routage". Lorsque des demandes suivantes sont reçues lors du délai de maintien de routage, l'enregistrement d'affinité est toujours valide et la demande est toujours acheminée vers le même serveur.

Si aucune connexion supplémentaire n'est reçue lors du délai de maintien de routage, l'enregistrement est vidé. Un nouveau serveur sera sélectionné pour toute connexion reçue une fois ce délai écoulé.

API SDA pour le contrôle de l'affinité client/serveur

L'API Affinité dirigée vers le serveur s'applique uniquement au composant Dispatcher.

La fonctionnalité SDA fournit une API qui permet à un agent externe d'influencer le comportement de l'affinité Dispatcher.

Remarque : Il existe une restriction indiquant que SDA (Server Direct Affinity) ne fonctionne pas avec le partitionnement de serveur car pour les fonctions de recherche de SDA, il est nécessaire que les adresses de serveur soient uniques dans la configuration. SDA ne fonctionne pas non plus avec la fonction SSL ID car avec SDA, les serveurs contrôlent la table des affinités.

Fonctions SDA

Votre application a peut-être indiqué que ses systèmes de serveurs sont en mesure de diriger les demandes client vers des serveurs particuliers plus efficacement que Dispatcher. Vous pouvez souhaiter que le client soit "redirigé" vers le serveur de votre choix et non vers le serveur sélectionné par la fonction d'équilibrage de charge de Dispatcher. La fonction SDA offre cet API. Vous pouvez créer votre programme pour mettre en oeuvre un agent SDA qui communique avec un module d'écoute dans Dispatcher. Celui-ci est en mesure de manipuler les tables d'affinité de Dispatcher afin :

- de rechercher le contenu,
- d'insérer de nouveaux enregistrements,
- de supprimer des enregistrements.

Les enregistrements insérés dans une table d'affinité par un agent SDA demeurent indéfiniment dans la table. Ils n'expirent jamais. Ils ne peuvent être supprimés que par l'agent SDA ou si un conseiller Dispatcher détecte que le serveur est arrêté.

Composant SDA de Dispatcher

Dispatcher met en oeuvre un nouveau module d'écoute de socket pouvant accepter et traiter des demandes provenant d'un agent SDA. Lorsqu'un agent SDA ouvre une connexion avec Dispatcher, le module d'écoute l'accepte et conserve la connexion. Plusieurs demandes et réponses peuvent utiliser cette connexion permanente. La socket ne sera fermée que par l'agent SDA ou si Dispatcher détecte une erreur irrémédiable. Dans Dispatcher, le module

d'écoute prend chaque demande de l'agent SDA, communique avec la table d'affinité appropriée dans le noyau de l'exécuteur de Dispatcher et prépare une réponse destinée à l'agent SDA.

Pour obtenir plus d'informations, reportez-vous aux fichiers se trouvant dans le répertoire d'installation de Network Dispatcher :

- L'API : `...nd/servers/samples/SDA/SDA_API.htm`
- Le code exemple pour un agent SDA :
`...nd/servers/samples/SDA/SDA_SampleAgent.java`.

Affinité trans ports

L'affinité trans ports s'applique uniquement au composant Dispatcher.

L'affinité trans ports se définit comme l'extension à plusieurs ports de la fonction maintien de routage. Par exemple, si la demande d'un client est d'abord reçue par un port puis une deuxième demande de ce client par un autre port, l'affinité trans ports permet au répartiteur d'envoyer cette demande au même serveur. Pour utiliser cette fonction, les ports doivent :

- partager la même adresse de grappe
- partager les mêmes serveurs
- avoir le même (non nul) **délai de maintien de routage** valeur
- avoir le même **masque de maintien de routage** valeur

Il est possible de relier plusieurs ports au même **trans ports**. Quand un même client se connectera, à l'avenir, sur le même port ou sur un port partagé, ses connexions seront traitées par le même serveur. Voici un exemple de configuration de ports multiples munis d'une affinité trans ports au port 10 :

```
définition de port ndcontrol grappe : 20 trans
ports 10
définition de port ndcontrol
grappe : 30 trans ports 10
définition de port ndcontrol
grappe : 40 trans ports 10
```

Après l'établissement de l'affinité trans ports, vous disposez de la possibilité de modifier le délai de maintien de routage du port. Il est cependant recommandé de choisir la même valeur pour tous les délais de maintien de routage des ports partagés. Dans le cas contraire, des résultats inattendus peuvent se produire.

Pour supprimer l'affinité trans ports, remplacez la valeur trans ports sur son propre numéro de port. Reportez-vous à «ndcontrol port — Configuration des ports» à la page 296, pour de plus amples informations sur la syntaxe de commande de l'option **trans ports**.

Masque d'adresse de l'affinité

Le masque d'adresse de l'affinité s'applique uniquement au composant Dispatcher.

Le masque d'adresse de l'affinité est une amélioration de la fonction de maintien de routage, destinée aux clients de groupe situés à des adresses de sous-réseau communes. La sélection du **masque de maintien de routage** de la commande **port ndcontrol** permet de masquer les bits communs à poids fort de l'adresse IP 32-bits. Si cette fonction est activée lors de la première connexion d'un client à un port, alors toutes les connexions suivantes des clients ayant la même adresse de sous-réseau (indiqué par la partie masquée de l'adresse) seront dirigées vers le même serveur.

Par exemple, si vous souhaitez que toutes les demandes client disposant d'une adresse de réseau classe A identique soient envoyées au même serveur, fixez à 8 (bits) la valeur du port du masque de maintien de routage. En ce qui concerne les demandes de clients de groupe possédant la même adresse de réseau classe B, fixez la valeur du masque de maintien de routage à 16 (bits). Pour les demandes de clients de groupe disposant de la même adresse de réseau classe C, fixez la valeur du masque de maintien de routage à 24 (bits).

Pour obtenir de meilleurs résultats, fixez la valeur du masque de maintien de routage dès le lancement de Network Dispatcher. Si vous modifiez cette valeur, les résultats seront imprévisibles.

Interaction avec l'affinité trans ports : Lors de l'activation de l'affinité trans ports, les valeurs du masque de maintien de routage des ports partagés doivent être identiques. Reportez-vous à «Affinité trans ports» à la page 197, pour de plus amples informations.

Pour activer le masque d'adresse d'affinité, utilisez une commande de port **ndcontrol** du type suivant :

```
définition de  
port ndcontrol grappe : port masque de maintien de  
routage 8
```

Les valeurs possibles des masques de maintien de routage sont 8, 16, 24 et 32. Une valeur de 8 indique que les 8 premiers bits à poids fort de l'adresse IP (adresse de réseau classe A) seront masqués. Une valeur de 16 indique que les 16 premiers bits à poids fort de l'adresse IP (adresse de réseau classe B) seront masqués. Une valeur de 24 indique que les 24 premiers bits à poids fort de l'adresse IP (adresse de réseau classe C) seront masqués. Si vous spécifiez une valeur de 32, l'adresse IP toute entière sera masquée, ce qui entraînera la désactivation de la fonction de masque d'adresse d'affinité. La valeur par défaut du masque de maintien de routage est 32.

Reportez-vous à «`ndcontrol port` — Configuration des ports» à la page 296, pour de plus amples informations sur la syntaxe de commande du masque de maintien de routage(fonction de masque d'adresse d'affinité).

Substitution d'affinité de règle

La substitution d'affinité de règle permet le remplacement du maintien de routage du port d'un serveur spécifique. Par exemple, dans le cas où vous utilisez une règle pour limiter le nombre de connexions alloué à chaque serveur d'application et disposez d'un serveur de débordement à règle fixe qui annonce "please try again later" à propos de cette application. Le délai du maintien de routage du porte est de 25 minutes et vous ne souhaitez pas que le client soit maintenu sur ce serveur. La substitution d'affinité de règle vous permet alors de changer de serveur de débordement afin de remplacer l'affinité qui est habituellement associée à ce port. Ainsi, la prochaine fois que le client adresse une demande à la grappe, la charge de celle-ci est envoyée au serveur d'application le plus disponible, et non au serveur de débordement.

Reportez-vous à «`ndcontrol server` — Configuration des serveurs» à la page 311, pour de plus amples informations sur la syntaxe de commande de la substitution d'affinité de règle, utilisant l'option de serveur **maintien de routage** .

Mise au repos de la gestion des connexions avec maintien de routage

La mise au repos de la gestion des connexions avec maintien de routage s'applique aux composants Dispatcher et CBR.

Pour retirer un serveur de la configuration Network Dispatcher quelle qu'en soit la raison (mises à jour, mises à niveau, service, etc.), vous pouvez utiliser la commande **`ndcontrol manager quiesce`**. La sous-commande `quiesce` permet aux connexions de s'achever (sans avoir été traitées) et transmet les connexions ultérieures du client vers le serveur mis au repos si la connexion est associée à un délai de maintien de routage et que ce dernier n'est pas arrivé à expiration. La sous-commande `quiesce` désactive toute nouvelle connexion au serveur.

N'utilisez l'option `quiesce "now"` que si le délai de maintien de routage est défini et que vous voulez que les nouvelles connexions soient envoyées à un autre serveur (et non au serveur mis au repos) avant que le délai de maintien de routage n'expire. Ci-dessous, se trouve un exemple de l'utilisation de l'option `now` pour mettre le serveur 9.40.25.67 au repos :

```
ndcontrol manager quiesce 9.40.25.67 now
```

L'option `now` détermine comment les options avec maintien de routage seront gérées.

- Si vous n'indiquez *pas* "now," les connexions existantes sont terminées et les connexions ultérieures sont transmises au serveur mis au repos à partir

des clients ayant des connexions associées à un délai de routage tant que le serveur mis au repos reçoit la nouvelle demande avant expiration du délai de routage. Cependant, si vous n'avez pas activé la fonction de maintien de routage (affinité), le serveur mis au repos ne peut pas recevoir de nouvelles connexions.

Il s'agit de la manière la moins brusque de placer des serveurs au repos. Par exemple, vous pouvez mettre au repos un serveur puis attendre le moment où le trafic est faible (peut-être le matin) pour retirer complètement le serveur de la configuration.

- En indiquant l'option "now," vous mettez le serveur au repos. Il permet dorénavant aux connexions existantes de se terminer mais il ne permet pas les nouvelles connexions, incluant les connexions provenant de clients ayant des connexions existantes avec délai de maintien de routage. Il s'agit de la manière la plus brusque de mettre des serveurs au repos, qui était seule disponible dans les versions précédentes de Network Dispatcher.

Option d'affinité de la commande rule

Vous pouvez définir les types d'affinité suivants dans la commande **ndcontrol rule** :

- Active cookie — Permet l'équilibrage de charge du trafic Web et une affinité avec le même serveur en fonction des cookies générés par Network Dispatcher.
- Passive cookie — Permet l'équilibrage de charge du trafic Web et une affinité avec le même serveur en fonction des cookies d'auto-identification générés par les serveurs. Vous devez définir le paramètre cookienam conjointement à l'affinité de cookie passif dans la commande rule.
- URI — Permet l'équilibrage de charge du trafic Web vers des serveurs Caching Proxy dans le but d'augmenter la mémoire cache.

L'option d'affinité par défaut est "none". La valeur zéro (inactif) doit être associée à l'option **stickytime** de la commande port pour affecter la valeur de cookie actif ou URI à l'option d'**affinité** de la commande rule. Lorsque l'affinité de cette dernière est définie, il devient impossible d'activer l'option stickytime de la commande port.

L'affinité de cookie actif ne s'applique qu'au composant CBR. L'affinité de cookie passif et l'affinité URI s'appliquent au composant CBR et à la méthode d'acheminement CBR du composant Dispatcher.

Affinité de cookie actif

L'affinité de cookie actif ne s'applique qu'au composant CBR. Elle permet de "fidéliser" les clients à un serveur donné. Pour l'activer, attribuez un nombre positif au paramètre **stickytime** (délai de maintien de routage) d'une règle et optez pour l'affinité de cookie actif ("activecookie"), lors de l'ajout de la règle

ou à l'aide de la commande `rule set`. Pour obtenir des informations sur la syntaxe de cette commande, reportez-vous à la section «`ndcontrol rule` — configuration des règles» à la page 303.

Une fois la règle configurée pour l'affinité de cookie actif, l'équilibrage de charge des nouvelles demandes client est effectué à l'aide d'algorithmes CBR standard, tandis que les demandes suivantes du même client sont envoyées au serveur initialement choisi. Le serveur choisi est stocké en tant que cookie dans la réponse au client. Tant que les demandes suivantes du client contiennent ce cookie et qu'elles arrivent dans le délai de maintien de routage, le client conserve l'affinité pour le serveur initial.

L'affinité de cookie actif permet d'assurer qu'un client fait l'objet d'un équilibrage de charge vers le même serveur pendant une période déterminée. A cet effet, un cookie est envoyé pour être stocké par le navigateur des clients. Ce cookie indique la règle adoptée pour la prise de décision, le serveur cible de l'équilibrage de charge et la date d'expiration de l'affinité. Lorsqu'une règle est déclenchée et que l'affinité de cookie actif est activée, le cookie envoyé par le client est examiné. En cas de détection d'un cookie contenant l'identificateur de la règle déclenchée, le serveur cible de l'équilibrage de charge et la date d'expiration sont extraits du cookie. Si le serveur figure toujours dans l'ensemble utilisé par la règle, que son poids est supérieur à zéro et que la date d'expiration est ultérieure à la date du jour, le serveur indiqué dans le cookie est choisi comme serveur cible pour l'équilibrage de charge. Si l'une de ces trois conditions n'est pas remplie, le choix d'un serveur s'effectue avec un algorithme normal. Une fois le serveur choisi (à l'aide de l'une des deux méthodes), un nouveau cookie est constitué avec `IBMCBR`, `grappe:port:serveur_choisi` et un horodatage. Ce dernier est la date d'expiration de l'affinité. La valeur "`grappe:port:serveur_choisi`" est codée pour ne révéler aucune information sur la configuration CBR. Un paramètre d'"expiration" est également inclus dans le cookie. Ce paramètre est dans un format lisible par le navigateur et entraîne la non-validité du cookie deux heures après la date d'expiration. Ainsi, la base de cookies du client n'est pas encombrée.

Le nouveau cookie est ensuite inséré dans les en-têtes qui reviennent au client. Le navigateur du client renvoie les demandes suivantes lorsqu'il est configuré pour accepter les cookies.

Pour la commande `rule`, vous ne pouvez attribuer que la valeur `activecookie` (cookie actif) à l'option d'affinité de cookie actif lorsque le délai de maintien de routage est zéro (non activé). Lorsque l'affinité de cookie actif est active au niveau d'une règle, vous ne pouvez pas activer le maintien de routage sur le port.

Activation de l'affinité du cookie actif

Pour activer l'affinité de cookie actif pour une règle donnée, utilisez la commande `rule set` :

```
rule set grappe:port:règle stickytime 60
rule set grappe:port:règle affinity activecookie
```

Objectifs de l'affinité de cookie actif

Le maintien de routage d'une règle est normalement utilisé pour les interfaces CGI ou les servlets qui enregistrent l'état du client sur le serveur. Cet état est identifié par un ID cookie (cookie serveur). L'état du client figure uniquement sur le serveur sélectionné. Pour maintenir cet état d'une demande à l'autre, le client a besoin du cookie du serveur.

Affinité de cookie passif

L'affinité de cookie passif s'applique à la méthode d'acheminement CBR (content-based routing) du composant Dispatcher et au composant CBR. Pour obtenir la procédure de configuration de la méthode d'acheminement CBR de Dispatcher, reportez-vous à la section «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54.

L'affinité de cookie passif offre une façon de fidéliser les clients à un serveur donné. Une fois que vous attribuez la valeur "cookiepassif" à l'affinité d'une règle, l'affinité de cookie passif vous permet d'équilibrer la charge du trafic Web destiné au même serveur, en fonction des cookies d'auto-identification générés par les serveurs. Vous configurez l'affinité de cookie passif au niveau de la règle. Une fois la règle déclenchée, si l'affinité de cookie passif est activée, Network Dispatcher choisit le serveur en fonction du nom du cookie se trouvant dans l'en-tête HTTP de la demande client. Network Dispatcher envoie les nouvelles demandes entrantes aux serveurs en fonction des cookies qui ont été générés par les serveurs lors de connexions précédentes. S'il n'est possible de trouver la valeur du cookie dans la demande client ou si elle ne correspond à aucune des valeurs de cookie du serveur, le serveur sera choisi à l'aide de la technique de permutation circulaire pondérée.

Pour configurer l'affinité de cookie passif :

- Pour Dispatcher, configurez d'abord la méthode d'acheminement CBR de Dispatcher. (Reportez-vous à la section «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54.) Cette étape est ignorée pour le composant CBR.
- Attribuez la valeur "passivecookie" au paramètre **affinity** (affinité) dans la commande **ndcontrol rule [add|set]**. De plus, le nom du cookie devant être recherché par Network Dispatcher dans la demande d'en-tête HTTP doit être attribué au paramètre **cookieName** (nom du cookie).
- Dans la commande **ndcontrol server [add|set]**, définissez le paramètre **cookievalue** (valeur de cookie) pour chaque serveur de l'ensemble de serveurs associé à la règle.

Pour la commande `rule`, vous ne pouvez attribuer que la valeur `"passivecookie"` (cookie passif) à l'option d'affinité de cookie passif lorsque le délai de maintien de routage est zéro (non activé). Une fois que l'affinité de cookie passif est active au niveau d'une règle, il n'est pas possible d'activer le maintien de routage sur le port.

Affinité d'URI

L'affinité d'URI s'applique à la méthode d'acheminement CBR de Dispatcher et au composant CBR. Pour obtenir la procédure de configuration de la méthode d'acheminement CBR de Dispatcher, reportez-vous à la section «Fonction CBR de Dispatcher (méthode d'acheminement `cbr`)» à la page 54.

L'affinité URI permet d'équilibrer le trafic Web sur des serveurs Caching Proxy, ce qui permet de mettre en mémoire cache un contenu unique sur un serveur spécifique. Ainsi, vous augmentez la taille de la mémoire cache du site en éliminant les éléments superflus placés en mémoire cache sur plusieurs machines. Configurez l'affinité d'URI au niveau de la règle. Une fois que la règle est déclenchée, si l'affinité d'URI est activée et que le même ensemble de serveurs est actif et répond, Network Dispatcher transmet les nouvelles demandes client entrantes ayant le même URI au même serveur.

Généralement, Network Dispatcher peut distribuer des demandes à plusieurs serveurs gérant un contenu identique. Lorsque vous utilisez Network Dispatcher avec un groupe de serveurs de mise en mémoire cache, le contenu dont l'accès est souvent demandé peut être placé dans la mémoire cache de tous les serveurs. En répliquant le contenu placé en mémoire cache identique, vous pouvez prendre en charge un grand nombre de clients. Cela est particulièrement utile pour les sites Web dont le volume est important.

Cependant, si le site Web prend en charge un trafic client modéré vers un contenu très divers et que vous préférez une mémoire cache répartie sur plusieurs serveur, votre site sera plus performant si chaque serveur de mise en cache comporte un contenu unique et que Network Dispatcher distribue la demande uniquement au serveur de mise en cache avec ce contenu.

Avec l'affinité d'URI, Network Dispatcher vous permet de distribuer le contenu mis en cache vers des serveurs individuels, éliminant la mise en cache superflue de contenu sur plusieurs machines. Grâce à cette fonction, les performances des sites ayant un contenu divers utilisant les serveurs Caching Proxy sont améliorées. Les demandes identiques sont envoyées au même serveur, plaçant ainsi en mémoire cache le contenu uniquement sur les serveurs individuels. La taille de la mémoire cache s'accroît avec chaque nouveau serveur ajouté au pool.

Pour configurer l'**affinité d'URI** :

- Pour Dispatcher, configurez d'abord la méthode d'acheminement CBR de Dispatcher. (Reportez-vous à la section «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54.) Cette étape est ignorée pour le composant CBR.
- Attribuez la valeur "uri" au paramètre **affinité** dans la commande **ndcontrol rule [add | set]** ou **cbrcontrol rule [add | set]**.

Pour la commande rule, vous ne pouvez attribuer que la valeur "URI" à l'option d'affinité d'URI lorsque le délai de maintien de routage est zéro (non activé). Une fois que l'affinité d'URI est active au niveau d'une règle, il n'est pas possible d'activer le maintien de routage sur le port.

Détection d'attaque de refus de service

Cette fonction est disponible uniquement pour le composant Dispatcher.

Dispatcher permet de détecter les attaques de "refus de service" possible et d'en alerter l'administrateur. Pour cela, Dispatcher analyse les demandes entrantes d'un certain nombre de connexions partielles TCP sur les serveurs, point commun des attaques de refus de service. Dans une attaque de refus de service, un site reçoit un grand nombre de paquets SYN d'un grand nombre d'adresses IP source et de numéros de port source, mais le site ne reçoit pas les paquets suivants de ces connexions TCP. De cette manière, vous avez un grand nombre de connexion partielles TCP sur les serveurs. Les serveurs peuvent devenir très lents et peuvent ne plus accepter de nouvelles connexions entrantes.

Network Dispatcher fournit des exit utilisateur qui déclenchent des scripts que vous pouvez personnaliser. Ces scripts avertissent l'administrateur d'une attaque de refus de service possible. Dispatcher met à votre disposition les fichiers script exemple ci-après dans le répertoire **...nd/servers/samples**.

- **halfOpenAlert** — une attaque de refus de service (DoS) probable a été détectée
- **halfOpenAlertDone** — l'attaque DoS est terminée

Afin d'exécuter les fichiers, vous devez les déplacer dans le répertoire **...nd/servers/bin** et supprimer l'extension de fichier ".sample".

Pour implémenter la détection d'attaque DoS, définissez le paramètre **maxhalfopen** dans la commande **ndcontrol port** de la manière suivante :

```
ndcontrol port set 127.40.56.1:80 maxhalfopen 1000
```

Dans l'exemple ci-dessus, Dispatcher compare le nombre total de connexions partielles (pour tous les serveurs se trouvant sur la grappe 127.40.56.1 du port 80) avec la valeur maximale de 100 (indiqué par le paramètre maxhalfopen).

Si le nombre de connexions partielles dépasse la limite, un appel d'un script d'alerte (`halfOpenAlert`) est effectué. Lorsque le nombre de connexions partielles est inférieur à la limite, un autre script d'alerte (`halfOpenAlertDone`) est effectué pour indiquer que l'attaque est terminée.

Pour déterminer comment définir la valeur `maxhalfopen` : Régulièrement (toutes les 10 minutes, par exemple), effectuez un rapport de connexion partielle (`ndcontrol port halfopenaddressreport grappe:port`) lorsque le trafic de votre site est normal ou élevé. Le rapport de connexion partielle renvoie un message "Nombre total de connexions partielles reçues". Vous devez attribuer au paramètre `maxhalfopen` une valeur supérieure de 50% à 200% au nombre le plus élevée de connexions partielles rencontrées par votre site.

Le paramètre `halfopenaddressport` permet d'effectuer un rapport de données statistiques ainsi que de générer des entrées dans le journal (`./nd/servers/logs/dispatcher/halfOpen.log`) pour toutes les adresses client (jusqu'à environ 8000 paires d'adresses) qui ont accédé à des serveurs disposant de connexions partielles.

Remarque : Il existe une alarme SNMP correspondant aux scripts `halfOpenAlert` et `halfOpenAlertDone`. Si le sous-agent SNMP est configuré et en cours d'exécution, les alarmes correspondantes sont envoyées dans les conditions de déclenchement de scripts. Pour plus d'informations sur le sous-agent SNMP, reportez-vous à la section «Utilisation du protocole SNMP (Simple Network Management Protocol) avec le composant Dispatcher» à la page 219.

Pour renforcer la protection des serveurs dorsaux contre les attaques de refus de service, vous pouvez configurer des grappes et des ports génériques. En particulier, ajoutez sous chaque grappe configurée un port générique sans serveur. Ajoutez également une grappe générique dotée d'un port générique, mais sans serveur. Ces actions ont pour résultat le rejet des paquets qui ne sont pas adressés à une grappe ni à un port non génériques. Pour obtenir des informations sur les grappes et les ports génériques, reportez-vous aux sections «Utilisation d'une grappe générique pour combiner les configurations serveurs» à la page 193 et «Utilisation du port générique pour acheminer le trafic destiné à un port non configuré» à la page 195.

Utilisation de la journalisation binaire pour analyser les statistiques des serveurs

Remarque : La fonction de journalisation binaire ne s'applique pas au composant Site Selector.

La fonction de journalisation binaire permet de stocker les informations du serveur dans des fichiers binaires. Ces fichiers peuvent ensuite être traités pour analyser les informations relatives aux serveurs qui ont été rassemblées.

Les informations suivantes sont stockées dans le journal binaire pour chaque serveur défini dans la configuration.

- Adresse de grappe
- Numéro de port
- ID serveur
- Adresse du serveur
- Pondération du serveur
- Nombre total de connexions sur le serveur
- Connexions actives sur le serveur
- Charge du port du serveur
- Charge système du serveur

Certaines de ces informations sont extraites de l'exécuteur comme faisant partie du cycle du gestionnaire. C'est pourquoi, le gestionnaire doit être en cours d'exécution afin que les informations puissent être consignées dans les journaux binaires.

Utilisez l'ensemble de commandes **ndcontrol log** pour configurer la journalisation binaire.

- log start
- log stop
- log set interval <seconde>
- log set retention <heures>
- log status

L'option start commencer à consigner les informations relatives au serveur dans les journaux binaires du répertoire logs. Un journal est créé au début de chaque heure, la date et l'heure constituant le nom du fichier.

L'option stop arrête la journalisation des informations relatives au serveur dans les journaux binaires. Le service de journalisation est arrêté par défaut.

L'option set interval contrôle la fréquence d'inscription des informations dans les journaux. Le gestionnaire enverra les informations du serveur au serveur de journalisation à chaque intervalle défini pour le gestionnaire. Les informations seront écrites dans les journaux uniquement si l'intervalle de journalisation indiqué a expiré depuis l'écriture du dernier enregistrement dans le journal. Par défaut, la valeur de l'intervalle de journalisation est 60

secondes. Il y a interaction entre les paramètres relatifs à l'intervalle défini pour le gestionnaire et l'intervalle de journalisation. Comme les informations ne seront pas fournies au serveur de journalisation plus fréquemment que l'intervalle défini pour le gestionnaire, l'indication d'un intervalle de journalisation inférieur à l'intervalle du gestionnaire, entraîne en réalité la définition d'un intervalle de journalisation identique à l'intervalle du gestionnaire. Cette technique de journalisation permet d'accéder aux informations du serveur quel que soit le niveau de granularité. Vous pouvez connaître toutes les modifications apportées au serveur qui sont vues par le gestionnaire pour le calcul des pondérations du serveur. Cependant, ces informations peuvent ne pas être requises pour analyser l'utilisation et les tendances du serveur. La journalisation des informations du serveur toutes les 60 secondes permet d'obtenir un aperçu de la progression des informations du serveur. La définition d'un intervalle de journalisation très faible peut générer un nombre de données très important.

L'option `set retention` permet de contrôler la durée de conservation des fichiers journaux. Les journaux dont la durée de vie a dépassé la durée définie seront supprimés par le serveur de journalisation. Cela se produit uniquement si le serveur de journalisation est appelé par le gestionnaire. Par conséquent, si le gestionnaire est arrêté, les fichiers journaux plus anciens ne sont pas supprimés.

L'option `status` renvoie les paramètres courants de la fonction de journalisation, c'est-à-dire l'état actif ou inactif du service, l'intervalle de consignment et la durée de conservation.

Un exemple de programme Java et un fichier de commandes sont fournis dans le répertoire `...nd/servers/samples/BinaryLog`. Ce modèle indique comment rappeler toutes les informations contenues dans les fichiers journaux pour les afficher à l'écran. Il peut être personnalisé pour effectuer n'importe quel type d'analyse. Par exemple (à l'aide du script et du programme fournis) :

```
ndlogreport 2001/05/01 8:00 2001/05/01 17:00
```

Cet exemple permet d'obtenir un rapport sur les informations du serveur Dispatcher de 8 à 17 heures le premier mai 2001. (Pour CBR, utilisez **cblogreport**. Pour Mailbox Locator, utilisez **mllogreport**. Pour Cisco Consultant, utilisez **lbclogreport**.)

Informations supplémentaires sur les fonctions Cisco Consultant avancées

Dans Cisco Consultant, Cisco CSS Switch effectue les mêmes tâches que l'exécuteur dans Dispatcher. Outre la charge en cours de chaque serveur et d'autres données nécessaires à ses calculs, le gestionnaire obtient les valeurs des nouvelles connexions et des connexions actives de Cisco CSS Switch. Ces valeurs dépendent des informations générées et stockées en interne dans Cisco CSS Switch.

Cisco Consultant interroge la base d'informations de gestion (MIB) de Cisco CSS Switch pour obtenir les informations relatives aux connexions actives et aux nouvelles connexion et il reçoit la réponse suivantes :

- **Pour les connexions actives**, Cisco Consultant extrait apSvcConnections de svcExtMIB. La variable est indexée en fonction du nom de service et mappe directement vers les connexions actives comme il est enregistré par le gestionnaire. Ci-dessous, se trouve l'entrée MIB apSvcConnections.

```
apSvcConnections OBJECT-TYPE
SYNTAX Integer32
MAX-ACCESS read-only
STATUS current
DESCRIPTION
    "The current number of TCP connections to this service"
DEFVAL { 0 }
--DEFAULT ap-display-name Service Connections
::= {apSvcEntry 20}
```

L'identificateur d'objet apSvcConnections est :

1.3.6.1.4.1.2467.1.15.2.1.20

Le nombre de connexions actives dépend du nombre de clients de même que du délai nécessaire pour accéder aux services offerts par les machines serveurs d'équilibrage de charge. Si les connexions client sont rapides (comme dans le cas de pages Web de petite taille obtenues par HTTP GET), le nombre de connexions actives est assez bas. Si les connexions client sont lentes (comme dans le cas de requêtes de base de données), le nombre de connexions actives est plus élevé.

- **Pour les nouvelles connexions**, Cisco Consultant définit la variable MIB apCntsvcHits dans cntSvcExtMib de Cisco CSS Switch. Pour chaque service, Cisco Consultant :
 - calcule la somme de tous les éléments apCntsvcHits ayant ce service dans l'index,
 - conserve un enregistrement de l'ensemble des éléments apCntsvcHits reçus,
 - calcule le delta.

L'index de cette variable est :

```
INDEX { apCntsvcOwnName, apCntsvcCntName, apCntsvcSvcName }
```

Ci-dessous, se trouve l'entrée MIB.

```
apCntsvcHits OBJECT-TYPE
```

```
SYNTAX Integer32
```

```
MAX-ACCESS read-only
```

```
STATUS current
```

```
DESCRIPTION
```

```
"Total number of flows placed onto this service for this content rule."
```

```
DEFVAL { 0 }
```

```
--DEFAULT ap-display-name Hits
```

```
--DEFAULT apjam-popup-ref apCntSvcInst, Statistics
```

```
--DEFAULT apjam-chart-def cntSvcHitsChart, pie, apCntInst, "Hit Information Per Servi
```

```
--DEFAULT apjam-chart-item cntSvcHitsChart, getnext, apCntsvcSvcName
```

```
::= {apSvcEntry 20}
```

L'identificateur d'objet apCntsvcHits est :

```
1.3.6.1.4.1.2467.1.18.2.1.4
```

Pondérations de Cisco Consultant

Cisco CSS Switch doit être configuré de manière à pouvoir utiliser l'équilibrage de charge de technique de permutation circulaire pondérée. Pour obtenir plus d'informations sur cette opération, reportez-vous au chapitre "Configuring Weight" du manuel *Content Services Switch Basic Configuration Guide*.

Les pondérations sont définies par la fonction du gestionnaire en fonction des décomptes internes de Cisco CSS Switch et du retour des informations des conseillers et du Metric Server. Si vous voulez définir des pondérations manuellement lors de l'exécution du gestionnaire, indiquez l'option **fixedweight** dans la commande **lbcontrol server**.

Si tous les serveurs sont inactifs, toutes les pondérations sont égales à zéro. Dans ce cas, lorsqu'aucun serveur ne traite les demandes car toutes les charges sont égales à zéro, les charges sont définies à la moitié de la pondération afin que le traitement des demandes soit effectué par n'importe quel serveur. Le contrôleur affiche les valeurs de charge égales à zéro alors que Cisco Consultant affiche une charge d'une demi-pondération à tous les autres emplacements.

Les pondérations sont envoyées à Cisco CSS Switch à l'aide de SNMP. Cisco Consultant définit apSvcWeight dans l'élément svcExt.mib. Ci-dessous, se trouve l'entrée apSvcWeight.

```
apSvcWeight OBJECT-TYPE
```

```
SYNTAX Integer 32(1..10)
```

```
MAX-ACCESS read-create
```

```
STATUS current
```

DESCRIPTION

"The service weight which is used in conjunction with load metrics when making load allocation decisions. The weight may be used to bias flows towards the specified service."

DEFVAL { 1 }

--DEFAULT ap-display-name Service Weight

--DEFAULT apjam-popup-ref apServicesGroupInst, Properties, Advanced

--DEFAULT apjam-wizard-field 2, normal

::= {apSvcEntry 16}

L'identificateur d'objet apSvcWeight est :

1.3.6.1.4.1.2467.1.15.2.1.12

Les pondérations définies s'appliquent à tous les serveurs connectés sur un même port. Pour chaque port, les demandes sont réparties entre les serveurs selon la pondération relative de chacun. Par exemple, si un serveur a une pondération (paramètre Weight) de 10 et un autre de 5, le premier recevra deux fois plus de demandes que le second.

Pour définir la limite de pondération maximale d'un serveur, entrez la commande **lbcontrol port set weightbound**. Cette commande indique les différences entre le nombre de demandes obtenues par chaque serveur. Si la pondération maximale est de 1, tous les serveurs peuvent avoir une pondération égale à 1, 0 en attente ou -1 si désactivé. A mesure que cette valeur augmente, l'écart entre les pondérations des serveurs augmente également. Avec une pondération maximale de 2, un serveur donné peut recevoir deux fois plus de demandes qu'un autre.

Lorsque le serveur est hors ligne...

Si un conseiller détecte qu'un serveur est hors ligne, il en informe le gestionnaire qui affecte au serveur une pondération de zéro. Lorsque la pondération d'un serveur est supérieure à zéro, elle est envoyée à Cisco CSS Switch et le serveur devient actif. Cependant, si la pondération du serveur est inférieure ou égale à zéro, le serveur est interrompu. La définition de la variable MIB apSvcEnable dans svcExt.mib de Cisco CSS Switch permet d'activer ou d'interrompre un service. Ci-dessous, se trouve l'entrée MIB apSvcEnable.

apSvcEnable OBJECT-TYPE

SYNTAX Integer

disable(0)

enable(1)

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"The state of the service, either enabled or disabled."

DEFVAL { disable }

```
--DEFAULT ap-display-name Status
--DEFAULT apjam-popup-ref apServicesGroupInst, Properties
--DEFAULT apjam-wizard-field 2, normal
::= {apSvcEntry 12}
```

L'identificateur d'objet apSvcEnable est :

1.3.6.1.4.1.2467.1.15.2.1.16

Chapitre 15. Exploitation et gestion de Network Dispatcher

Remarque : Lors de la lecture de ce chapitre, dans les sections générales qui ne concernent pas particulièrement un composant, si vous n'utilisez *pas* le composant Dispatcher, remplacez "ndcontrol" et "ndserver" par les éléments suivants :

- Pour CBR, utilisez **cbrcontrol** et **cbrserver**
- Pour Mailbox Locator, utilisez **mlcontrol** et **mlserver**
- Pour Site Selector, utilisez **cbrcontrol** et **ssserver**
- Pour Cisco Consultant, utilisez **lbccontrol** et **lbserver**

Le présent chapitre explique comment exploiter et gérer Network Dispatcher et inclut les sections suivantes :

- «Administration authentifiée à distance»
- «Utilisation des journaux Network Dispatcher» à la page 215
- «Utilisation du composant Dispatcher» à la page 217
 - «Utilisation du protocole SNMP (Simple Network Management Protocol) avec le composant Dispatcher» à la page 219
- «Utilisation du composant CBR (Content Based Routing)» à la page 225
- «Utilisation du composant Mailbox Locator» à la page 226
- «Utilisation du composant Site Selector» à la page 226
- «Utilisation du composant Cisco Consultant» à la page 227

Administration authentifiée à distance

Network Dispatcher offre une option permettant d'exécuter ses programmes de configuration sur une machine autre que celles sur lesquelles s'exécutent les serveurs Network Dispatcher.

Les communications entre les programmes de configuration ((ndcontrol, cbrcontrol, mlcontrol, sscontrol, lbccontrol, ndwizard, cbrwizard, mlwizard, sswizard, ndadmin) sont effectuée à l'aide de l'appel RMI (Remote Method Invocation) Java . La commande permettant de connecter un Network Dispatcher pour l'administration à distance est **ndcontrol host:hôte_éloigné**. Si l'appel RMI vient d'une machine autre que la machine locale, une séquence d'authentification clé publique/clé privée se produit avant l'acceptation de la commande de configuration. la séquence d'authentification se produit avant l'acceptation de la commande de configuration.

Les communications entre les programmes de contrôle exécutés sur la même machine que les serveurs du composant ne sont pas authentifiées.

La commande suivante permet de générer des clés publiques et privées à utiliser pour l'authentification éloignée :

ndkeys [create | delete]

Cette commande s'exécute uniquement sur la même machine que Network Dispatcher.

L'option **create** permet de créer une clé publique dans le répertoire key des serveurs (...**nd/servers/key/**) et de créer des clés privées dans le répertoire keys d'administration (...**nd/admin/keys/**) pour chacun des composants Network Dispatcher. Le nom de fichier de la clé privée est : *composant-AdresseServeur-PortRMI*. Ces clés privées doivent ensuite être transmises aux clients éloignés et placés dans la répertoire keys d'administration.

Pour une machine Network Dispatcher avec une adresse de nom d'hôte 10.0.0.25 utilisant le port RMI par défaut pour chaque composant, la commande **ndkeys create** génère les fichiers suivants :

- La clé publique : .../nd/servers/key/**authorization.key**
- Les clés privées :
 - .../nd/admin/keys/**dispatcher-10.0.0.25-10099.key**
 - .../nd/admin/keys/**cbr-10.0.0.25-11099.key**
 - .../nd/admin/keys/**m1-10.0.0.25-13099.key**
 - .../nd/admin/keys/**ss-10.0.0.25-12099.key**
 - .../nd/admin/keys/**lbc-10.0.0.25-14099.key**

Le jeu de fichiers d'administration a été installé sur une autre machine. Les fichiers de clés privées doivent être placés dans le répertoire **.../nd/admin/keys** sur la machine client éloignée.

Le client éloigné sera désormais autorisé à configurer Network Dispatcher sur 10.0.0.25.

Ces mêmes clés doivent être utilisées sur tous les clients éloignés que vous souhaitez autoriser à configurer Network Dispatcher sur 10.0.0.25.

Si vous devez de nouveau exécuter la commande **ndkeys create**, un nouveau jeu de clés publiques/privées sera généré. Ceci signifie que tous les clients éloignés qui ont tenté de se connecter à l'aide des clés précédentes ne seront plus autorisés. La nouvelle clé doit être placée dans le répertoire adéquat sur les clients auxquels vous voulez attribuer des autorisations.

La commande **ndkeys delete** permet de supprimer les clés publiques et privées sur la machine serveur. Si ces clés sont supprimées, aucun client éloigné ne sera autorisé à se connecter aux serveurs.

L'option **force** peut être associée à la commande **ndkeys** et à la commande **ndkeys delete**. Elle permet de supprimer les invites demandant si vous voulez remplacer ou supprimer les clés existantes.

Utilisation des journaux Network Dispatcher

Network Dispatcher enregistre les entrées dans un journal du serveur, un journal du gestionnaire, un journal du contrôleur de mesures (journalisation des communications avec les agents Metric Server) et dans un journal pour chaque conseiller utilisé.

Remarque : De plus, pour le composant Dispatcher uniquement, les entrées peuvent être ajoutées dans un journal de sous-agent (SNMP).

Vous pouvez définir le niveau de journalisation pour déterminer le détail des messages consignés dans les journaux. Au niveau 0, les erreurs sont enregistrées dans un fichier journal et Network Dispatcher journalise également les en-têtes et les enregistrements des événements survenus une seule fois (par exemple, un message indiquant que le lancement d'un conseiller sera enregistré dans le journal du gestionnaire). Le niveau 1 inclut les données en circulation, et ainsi de suite jusqu'au niveau 5, qui inclut tous les messages émis susceptibles d'aider à résoudre un incident lorsque cela s'avère nécessaire. La valeur par défaut du journal du serveur est 0. La valeur par défaut pour les journaux du gestionnaire, du conseiller et du sous-agent est 1.

Vous pouvez également fixer la taille maximale d'un fichier journal. Dans ce cas, le fichier se bouclera ; une fois sa taille maximale atteinte, les nouvelles entrées seront consignées au début du fichier, écrasant les entrées les plus anciennes. Lorsque vous spécifiez une nouvelle taille pour un fichier journal, elle ne doit pas être inférieure à sa taille courante. Les entrées de fichier journal sont horodatées, ce qui permet de déterminer l'ordre dans lequel elles ont été créées.

Plus le niveau de journalisation choisi est élevé, plus la taille du fichier journal doit être définie judicieusement. Au niveau 0, il sera probablement sage de laisser la taille du fichier journal à sa valeur par défaut (1 Mo). Par contre, à partir du niveau 3, limitez la taille du fichier journal sans trop d'excès pour lui garder son utilité.

- Pour configurer le niveau de journalisation ou la taille maximale du journal, utilisez la commande **ndcontrol set**.

- Pour configurer le niveau de journalisation ou la taille maximale du journal pour un journal de gestionnaire, utilisez la commande **ndcontrol manager**. Cette commande permet également de contrôler le niveau de journalisation du journal du contrôleur de mesures dans lequel les communications avec les agents Metric Server sont enregistrées.
- Pour configurer le niveau de journalisation ou la taille maximale du journal pour un journal de conseiller, utilisez la commande **ndcontrol advisor**.
- Pour configurer le niveau de journalisation ou la taille maximale du journal pour un journal de sous-agent, utilisez la commande **ndcontrol subagent**. (Seul le composant Dispatcher utilise le sous-agent SNMP.)

Modification des chemins des fichiers journaux

Par défaut, les journaux générés par Network Dispatcher seront stockés dans le répertoire logs de l'installation de Network Dispatcher. Pour modifier ce chemin, définissez la variable *nd_logdir* dans le script ndserver.

AIX, Linux et Solaris : Le script ndserver se trouve dans le répertoire /usr/bin. Dans ce script, la variable *nd_logdir* indique le répertoire par défaut. Vous pouvez modifier cette variable pour indiquer le répertoire de fichiers journaux de votre choix. Exemple :

ND_LOGDIR=/chemin/de/mes/fichiers/journaux/

Windows 2000 : Le fichier ndserver se trouve dans le répertoire système de Windows 2000, généralement C:\WINNT\SYSTEM32. Dans le fichier ndserver, la variable *nd_logdir* indique le répertoire par défaut. Vous pouvez modifier cette variable pour indiquer le répertoire de fichiers journaux de votre choix. Exemple :

set ND_LOGDIR=c:\chemin\de\mes\fichiers\journaux

Quel que soit le système d'exploitation utilisé, assurez-vous qu'il n'y a pas d'espace avant ou après le signe égal et que le chemin se termine par une barre oblique ("/" ou "\") selon le cas).

Journalisation binaire

Remarque : La fonction de journalisation binaire ne s'applique pas au composant Site Selector.

La fonction de journalisation binaire de Network Dispatcher utilise le répertoire contenant les autres fichiers journaux. Reportez-vous à la section «Utilisation de la journalisation binaire pour analyser les statistiques des serveurs» à la page 205.

Utilisation du composant Dispatcher

La présente section explique comment utiliser et gérer le composant Dispatcher.

Lancement et arrêt de Dispatcher

- A partir d'une ligne de commande, entrez **ndserver** pour lancer Dispatcher.
- A partir d'une ligne de commande, entrez **ndserver stop** pour arrêter Dispatcher.

Utilisation de la valeur du délai d'attente

Pour Network Dispatcher, les connexions sont considérées comme périmées lorsqu'aucune activité ne s'est produite sur cette connexion pendant le nombre de secondes indiquées dans le délai d'attente. Lorsque ce nombre de secondes est dépassé et qu'aucune activité n'a eu lieu, Network Dispatcher supprime cet enregistrement de connexion de ces tables et le trafic à venir pour cette connexion sera ignoré.

Au niveau du port, par exemple, vous pouvez indiquer la valeur du délai d'attente à partir de la commande **ndcontrol port set staletimeout**.

Le délai d'attente peut être défini au niveau de l'exécuteur, de la grappe et du port. Au niveau de l'exécuteur et de la grappe, la valeur par défaut est 300 secondes et le filtrage est effectué jusqu'au port. Au niveau du port, la valeur par défaut dépend du port. Certains ports bien définis ont des valeurs de délai d'attente différentes. Par exemple, le port telnet 23 a une valeur par défaut de 32,000,000 secondes.

Certains services ont également leurs propres valeurs de délai d'attente. Par exemple, LDAP (Lightweight Directory Access Protocol) dispose d'un paramètre de configuration appelé `idletimeout`. Lorsque le nombre de secondes indiqué à l'aide de ce paramètre est dépassé, la fermeture d'une connexion de client inactif est provoquée. Vous pouvez attribuer la valeur 0 à ce paramètre, ce qui signifie que la fermeture de la connexion ne sera jamais provoquée.

Des problèmes de connectivité peuvent se produire lorsque la valeur du délai d'attente de Network Dispatcher est inférieure à la valeur du délai du service. Dans le cas de LDAP, la valeur par défaut du paramètre de Network est 300 secondes. Si aucune activité ne se produit sur la connexion pendant 300 secondes, Network Dispatcher supprime l'enregistrement de connexion de ses tables. Si la valeur `idletimeout` est supérieure à 300 secondes (ou si elle est égale à 0), le client peut encore croire qu'une connexion au serveur est établie. Lorsque le client transmet des paquets, ces derniers seront ignorés par Network Dispatcher. De cette façon, LDAP n'est pas bloqué lorsqu'une demande au serveur est effectuée. Pour éviter ce problème, attribuez une

valeur différente de zéro au paramètre, identique ou inférieure à la valeur du paramètre `staletimeout` de Network Dispatcher.

Utilisation du décompte FIN pour contrôler la collecte des données obsolètes

Une fois tous les paquets de données transmis, un client envoie un paquet FIN pour informer le serveur que la transaction est terminée. Lorsque Dispatcher réceptionne le paquet FIN, il remplace l'état de la transaction, active, par FIN. Lorsqu'une transaction est à l'état FIN, la mémoire réservée à la connexion est libérée par le collecteur de données obsolètes intégré à l'exécuteur.

Vous pouvez utiliser le délai d'expiration et le décompte FIN pour définir la fréquence à laquelle l'exécuteur collectera les données obsolètes et l'étendue de cette opération. L'exécuteur contrôle périodiquement la liste des connexions accordées. Lorsque le nombre de connexions à l'état FIN devient supérieur ou égal au décompte FIN, l'exécuteur tente de libérer la mémoire ayant servi au stockage des informations de connexion. Vous pouvez modifier la valeur du décompte FIN en entrant la commande **`ndcontrol executor set fincount`**.

Le collecteur de données obsolètes libère la mémoire utilisée par toute connexion affichant l'état FIN et dont la durée excède le nombre de secondes spécifié par le délai d'expiration FIN. Vous pouvez modifier la valeur du délai d'expiration FIN en entrant la commande **`ndcontrol executor set fintimeout`**.

La valeur du délai d'attente correspond au nombre de secondes durant lesquelles il peut n'y avoir aucune activité sur une connexion avant que cette dernière ne soit retirée. Pour plus d'informations, reportez-vous à la section «Utilisation de la valeur du délai d'attente» à la page 217. La valeur du décompte FIN détermine également la fréquence selon laquelle les connexions "bloquées" sont supprimées. Si votre machine Dispatcher dispose de peu de mémoire, spécifiez un décompte FIN raisonnable. Si votre site WEB connaît un trafic important, spécifiez une valeur plus élevée.

Interface graphique — option de menu Contrôler

Divers diagrammes peuvent être affichés en fonction des informations visualisées par l'exécuteur et transmises au gestionnaire. (Le gestionnaire doit s'exécuter pour pouvoir utiliser l'option de menu Contrôler de l'interface graphique).

- Nombre de connexions par seconde pour chaque serveur (plusieurs serveurs peuvent être affichés sur un même graphique)
- Pondérations relatives pour chaque serveur d'un port donné
- Durée moyenne de connexion pour chaque serveur d'un port donné

Utilisation du protocole SNMP (Simple Network Management Protocol) avec le composant Dispatcher

Remarque : Pour Linux, SNMP n'est pas pris en charge sur Network Dispatcher.

Un système de gestion de réseau est un programme qui s'exécute en continu et qui sert à surveiller et à refléter l'état d'un réseau et à contrôler ce dernier. SNMP (Simple Network Management Protocol), protocole courant permettant de communiquer avec des périphériques d'un réseau, est la norme de gestion de réseau en cours. Les périphériques de réseau sont généralement dotés d'un *agent* SNMP et d'un ou de plusieurs sous-agents. L'agent SNMP communique avec le *poste de gestion de réseau* ou répond aux requêtes SNMP de la ligne de commande. Le *sous-agent* SNMP extrait et met à jour des données et transmet ces dernières à l'agent SNMP de sorte que celui-ci communique en retour avec le demandeur.

Dispatcher donne une *Bibliothèque d'informations de gestion* SNMP (ibmNetDispatcherMIB) et un sous-agent SNMP. Ceci vous permet d'utiliser un système de gestion de réseau tel que — Tivoli NetView, Tivoli Distributed Monitoring ou HP OpenView — afin de surveiller l'état, le débit et l'activité de Dispatcher. Les données MIB décrivent la gestion de Dispatcher et reflètent l'état en cours de ce dernier. Elles sont installées dans le sous-répertoire `..nd/admin/MIB`.

Remarque : Les données MIB, ibmNetDispatcherMIB.02, ne seront pas chargées à l'aide du programme `xnmloadmib2` de Tivoli NetView. Pour résoudre ce problème, mettez en commentaire la section NOTIFICATION-GROUP des données MIB. En d'autres termes, insérez `"- "` au début de la ligne `"indMibNotifications Group NOTIFICATION-GROUP"` et au début des 6 lignes suivantes.

Le système de gestion de réseau utilise des commandes SNMP GET pour consulter les valeurs MIB des autres machines. Il peut ensuite vous envoyer une notification en cas de dépassement des valeurs seuil indiquées. Vous pouvez ensuite changer les performances de Dispatcher en modifiant les données de configuration de Dispatcher, afin d'effectuer une mise au point proactive ou de résoudre les incidents liés à Dispatcher avant qu'ils se transforment en pannes de serveur Web ou Dispatcher.

Commandes et protocole SNMP

Le système fournit généralement un agent SNMP pour chaque poste de gestion de réseau. L'utilisateur adresse une commande GET à l'agent SNMP. En retour, ce dernier émet une commande GET pour extraire les valeurs de variables MIB indiquées à partir d'un sous-agent responsable de ces dernières.

Dispatcher fournit un sous-agent qui permet la mise à jour et l'extraction de données MIB. Le sous-agent répond aux données MIB appropriées lorsque l'agent SNMP émet une commande GET. L'agent SNMP communique les données au poste de gestion de réseau. Celui-ci peut vous envoyer une notification en cas de dépassement des valeurs seuil indiquées.

Le support SNMP de Dispatcher comporte un sous-agent SNMP qui utilise la fonction DPI (Distributed Protocol Interface). Il s'agit d'une interface entre un agent SNMP et les sous-agents de ce dernier.

Activation de SNMP sous AIX et Solaris

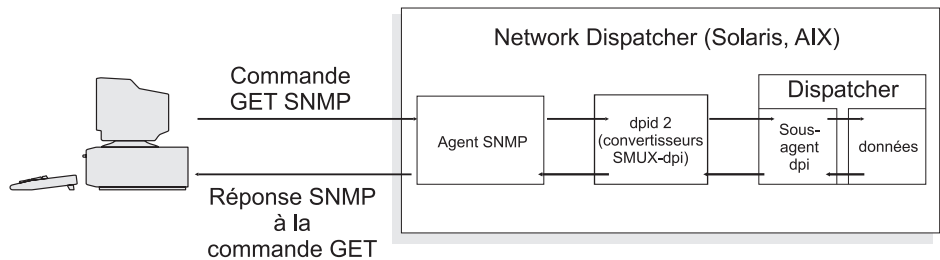


Figure 28. Commandes SNMP pour AIX et Solaris

AIX fournit un agent SNMP qui utilise le protocole SNMP Multiplexer (SMUX) et fournit DPID2, qui est un exécutable supplémentaire fonctionnant comme traducteur entre DPI et SMUX.

Pour Solaris, vous devez obtenir un agent SNMP fonctionnant avec SMUX car Solaris n'en fournit pas. Network Dispatcher fournit DPID2 pour Solaris dans le répertoire `/opt/nd/servers/samples/SNMP`.

L'agent DPI doit fonctionner comme un utilisateur root. Avant d'exécuter le démon DPID2, mettez à jour les fichiers `/etc/snmpd.peers` et `/etc/snmpd.conf` comme suit :

- Dans le fichier `/etc/snmpd.peers`, ajoutez l'entrée suivante pour dpid :

```
"dpid2"      1.3.6.1.4.1.2.3.1.2.2.1.1.2      "mot_de_passe_dpid"
```
- Dans `/etc/snmpd.conf`, ajoutez l'entrée suivante pour dpid :

```
smux      1.3.6.1.4.1.2.3.1.2.2.1.1.2 mot_de_passe_dpid      #dpid
```

Régénérez snmpd de sorte qu'il relise le fichier `/etc/snmpd.conf` :
`refresh -s snmpd`

Lancez l'homologue DPID SMUX :
`dpid2`

Les démons doivent être lancés dans l'ordre suivant :

1. Agent SNMP
2. Programme de traduction DPI
3. Sous-agent Dispatcher

Activation de SNMP sous Windows 2000

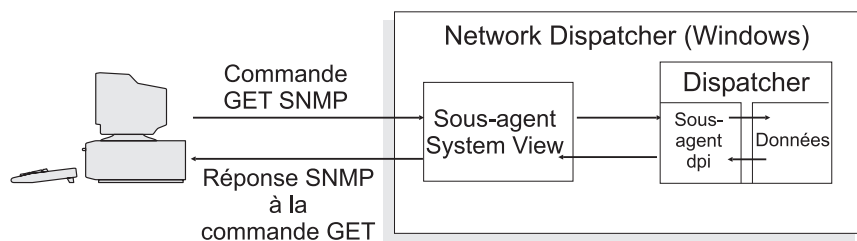


Figure 29. Commandes SNMP pour Windows 2000

Pour accéder à un agent SNMP DPI pour Windows 2000, installez la version Windows NT du kit d'outils IBM SystemView Agent à partir de <http://www.tivoli.com/support/sva>.

Avant de lancer le processus SNMPD de SystemView SNMPD, désactivez le support SNMP de Microsoft Windows. Ce support prend en charge les sous-agents DPI et les agents compatibles Microsoft.

Pour désactiver le support SNMP de Windows, procédez aux opérations ci-dessous.

1. Sélectionnez sur Démarrer->Programmes->Outils administratifs->Services.
2. Cliquez avec le bouton droit de la souris sur **SNMP**, puis sélectionnez **Propriétés**.
3. Remplacez la valeur de **Type de lancement** : par "Désactivé"

Remarque : Si le support SNMP de Microsoft Windows n'est pas désactivé, le sous-agent SNMP de Dispatcher ne parvient pas à se connecter à l'agent snmpd.

Pour configurer l'agent SystemView SNMP, suivez les instructions de la section «Définition d'un nom de communauté pour SNMP».

Définition d'un nom de communauté pour SNMP

Vous devez configurer le nom de communauté SNMP. Le mot de passe SNMP par défaut est public. Sous UNIX, il est défini dans un fichier appelé `/etc/snmpd.conf`.

Sur tous les systèmes, le nom de communauté doit être configuré et utilisé de manière cohérente. En d'autres termes, si le nom de communauté de Network Dispatcher est "OurCommunity" dans la configuration de l'agent SNMP, il doit aussi être défini par "OurCommunity" dans la configuration du sous-agent.

Sous Windows 2000, configurer l'agent SNMP IBM SystemView avant de créer le nom de communauté.

1. Sur le bureau, cliquez sur l'icône **Agent IBM SystemView**.
2. Cliquez sur **snmpcfg**.
3. Dans la boîte de dialogue de configuration SNMP, ajoutez le nom de communauté. Pour des raisons de test, entrez le mot de passe **public**.
Cette opération permet à n'importe quel hôte d'un réseau d'accéder aux variables MIB SNMP. Après avoir vérifié que ces valeurs fonctionnent, vous pouvez les modifier en fonction de vos besoins.
4. Vérifiez le fichier `\sva\dmi\bin\svastart.bat` et assurez-vous que l'option **-dpi** est spécifiée.
5. Démarrez le démon SNMP à l'aide du fichier `svastart.bat` du sous-répertoire `\sva\dmi\bin`.

L'exécuteur étant en cours de fonctionnement, lancez la commande **ndcontrol subagent start** [*nom_communauté*] pour définir le nom de communauté utilisé entre le sous-agent DPI de Dispatcher et l'agent SNMP. Le nom de communauté par défaut est `public`. Si vous modifiez cette valeur, vous devez aussi ajouter le nouveau nom de communauté à l'agent SystemView à l'aide de `snmpcfg` comme décrit plus haut.

Interruptions

SNMP communique en envoyant et en recevant des *interruptions*, messages envoyés par des périphériques gérés afin de signaler des conditions d'erreur ou la survenue d'événements importants, par exemple, le dépassement d'un seuil.

Le sous-agent utilise les interruptions suivantes :

- `indHighAvailStatus`
- `indSrvrGoneDown`
- `indDOSAttack`
- `indDOSAttackDone`

L'interruption **indHighAvailStatus** annonce que la valeur de la variable (hasState) correspondant à l'état de la haute disponibilité a changé. Les valeurs possibles de hasState sont :

- idle** cette machine effectue un équilibrage de charge et n'essaie pas d'établir un contact avec son répartiteur associé.
- listen** La haute disponibilité vient de démarrer et Dispatcher est à l'écoute de son partenaire.
- active** cette machine effectue l'équilibrage de charge.
- standby**
cette machine contrôle la machine active.
- preempt**
cette machine est dans un état transitoire pendant le passage de la machine principale à la machine de secours.
- elect** Le répartiteur choisit, avec son partenaire, la machine principale et la machine de secours.
- no_exec**
L'exécuteur n'est pas lancé.

L'interruption **indSrvrGoneDown** annonce que la pondération du serveur spécifié par les segments csAddr, psNum, ssAddr de l'identificateur d'objet est passée à zéro. Le dernier nombre total de connexions actives du serveur est envoyé avec l'interruption. Cette interruption indique que, pour le répartiteur, le serveur spécifié a été arrêté."

L'interruption **indDOSAttack** indique que numhalfopen (nombre de connexions partielles constituées uniquement de paquets SYN) a dépassé le seuil maxhalfopen pour le port précisé par les segments csAddr, psNum de l'identificateur d'objet. Le nombre de serveurs configurés sur le port est transmis dans l'interruption. Cette interruption indique que Network Dispatcher peut faire l'objet d'une attaque de refus de service.

L'interruption **indDOSAttackDone** indique que numhalfopen (nombre de connexions partielles constituées uniquement de paquets SYN) est en deçà du seuil maxhalfopen pour le port précisé par les segments csAddr, psNum de l'identificateur d'objet. Le nombre de serveurs configurés sur le port est transmis dans l'interruption. Lorsque Network Dispatcher détermine que l'attaque de refus de service est terminée, cette interruption est envoyée après l'interruption indDOSAttack.

En raison d'une restriction au niveau de l'interface API SMUX, il se peut que l'ID entreprise signalé dans des interruptions provenant du sous-agent ibmNetDispatcher corresponde à l'ID entreprise de dpid2 et non à celui

d'ibmNetDispatcher, 1.3.6.1.4.1.2.6.144. Cependant, les utilitaires de gestion SNMP peuvent déterminer la source de l'interruption car les données contiennent un ID objet provenant du MIB ibmNetDispatcher.

Activation et désactivation du support SNMP à partir de la commande `ndcontrol`

Le support SNMP est activé à l'aide de la commande `ndcontrol subagent start`. Il est désactivé à l'aide de la commande `ndcontrol subagent stop`.

Pour plus de détails sur la commande `ndcontrol`, reportez-vous à la section «`ndcontrol subagent` — Configuration du sous-agent SNMP» à la page 320.

Rejet de l'ensemble du trafic vers Network Dispatcher avec la fonction `ipchains` ou `iptables` (Linux)

Le pare-feu `ipchains` est intégré au noyau de Linux. Lors de l'exécution simultanée de Network Dispatcher et de `ipchains`, Network Dispatcher voit le paquets avant `ipchains`. Vous pouvez ainsi utiliser `ipchains` pour renforcer un dispositif Network Dispatcher Linux tel qu'un dispositif Network Dispatcher servant à charger des pare-feux d'équilibrage de charge.

Lorsque `ipchains` ou `iptables` est configuré pour une utilisation restreinte (aucun trafic entrant ou sortant autorisé), la partie dédiée à l'acheminement des paquets de Network Dispatcher continue de fonctionner normalement.

Notez que `ipchains` et `iptables` *ne permettent pas* le filtrage du trafic entrant avant l'équilibrage de la charge.

Le fonctionnement correct de l'ensemble de Network Dispatcher nécessite l'autorisation de trafic supplémentaire. Voici quelques exemples de communication :

- Les conseillers communiquent entre le dispositif Network Dispatcher et les serveurs périphériques.
- Network Dispatcher envoie une commande ping aux serveurs périphériques, aux cibles à atteindre et aux dispositifs Network Dispatcher de haute disponibilité partenaires.
- Les interfaces utilisateur (interface graphique, ligne de commande et assistants) utilisent les appels RMI.
- Les serveurs périphériques doivent répondre aux commandes ping provenant du dispositif Network Dispatcher.

En règle générale, la stratégie `ipchains` adaptée aux dispositifs Network Dispatcher consiste à refuser tout type de trafic, sauf celui à destination et provenant des serveurs périphériques, du Network Dispatcher haute disponibilité partenaire, des cibles à atteindre ou des hôtes de configuration.

Utilisation du composant CBR (Content Based Routing)

La présente section explique comment utiliser le composant CBR de Network Dispatcher.

Lancement et arrêt de CBR

- A partir d'une ligne de commande, entrez **cbrserver** pour lancer CBR.
- A partir d'une ligne de commande, entrez **cbrserver stop** pour arrêter CBR.

CBR et Caching Proxy gèrent conjointement les demandes HTTP et HTTPS (SSL) via l'interface API du module d'extension de Caching Proxy. Caching Proxy doit être en cours d'exécution sur la même machine pour que CBR puisse commencer à effectuer l'équilibrage de charge des serveurs. Configurez CBR et Caching Proxy en respectant les instructions de la section «Exemple de configuration CBR» à la page 94.

Contrôle de CBR

Après avoir lancé CBR, vous pouvez le contrôler en utilisant une des méthodes suivantes :

- Configurez CBR à l'aide de la commande **cbrcontrol**. La syntaxe complète de cette commande est décrite dans «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257. Voici quelques exemples d'utilisation de cette commande.
- Configurez CBR à l'aide de l'interface utilisateur graphique. A partir de la ligne de commande, entrez **ndadmin** pour ouvrir l'interface graphique. Pour obtenir plus d'informations sur le mode de configuration de CBR à l'aide de l'interface graphique, reportez-vous à la section «Interface graphique» à la page 86.

Utilisation des journaux de CBR

Les journaux utilisés par CBR sont similaire à ceux de Dispatcher. Pour plus d'informations, reportez-vous à la section «Utilisation des journaux Network Dispatcher» à la page 215.

Remarque :

Dans les versions précédentes, pour CBR, il était possible de modifier le chemin d'accès au répertoire log dans le fichier de configuration Caching Proxy. Vous pouvez maintenant changer le chemin du répertoire dans lequel le journal est stocké dans le fichier `cbrserver`. Pour plus de détails, reportez-vous à la section «Modification des chemins des fichiers journaux» à la page 216.

Utilisation du composant Mailbox Locator

Lancement et arrêt de Mailbox Locator

- A partir d'une ligne de commande, entrez **mlserver** pour lancer Mailbox.
- A partir d'une ligne de commande, entrez **mlserver stop** pour arrêter Mailbox Locator.

Contrôle de Mailbox Locator

Après avoir lancé Mailbox Locator, vous pouvez le contrôler en utilisant une des méthodes suivantes :

- Configurez Mailbox Locator à l'aide de la commande **mlcontrol**. La syntaxe complète de cette commande est décrite dans «Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator» à la page 257. Voici quelques exemples d'utilisation de cette commande.
- Configurez Mailbox Locator à l'aide de l'interface utilisateur graphique. A partir de la ligne de commande, entrez **ndadmin** pour ouvrir l'interface graphique. Pour obtenir plus d'informations sur le mode de configuration de Mailbox Locator à l'aide de l'interface graphique, reportez-vous à la section «Interface graphique» à la page 103.

Utilisation des journaux Mailbox Locator

Les journaux utilisés par Mailbox Locator sont similaires à ceux utilisés dans Dispatcher. Pour plus d'information, reportez-vous à la section «Utilisation des journaux Network Dispatcher» à la page 215.

Utilisation du composant Site Selector

Lancement et arrêt de Site Selector

- A partir d'une ligne de commande, entrez **sssserver** pour lancer Site Selector.
- A partir d'une ligne de commande, entrez **sssserver stop** pour arrêter Site Selector.

Contrôle d'Site Selector

Après avoir lancé Site Selector, vous pouvez le contrôler en utilisant une des méthodes suivantes :

- Configurez Site Selector à l'aide de la commande **sscontrol**. La syntaxe complète de cette commande est décrite dans «Annexe D. Guide des commandes Site Selector» à la page 327. Voici quelques exemples d'utilisation de cette commande.
- Configurez Site Selector à l'aide de l'interface utilisateur graphique. A partir de la ligne de commande, entrez **ndadmin** pour ouvrir l'interface graphique. Pour obtenir plus d'informations sur le mode de configuration de Site Selector à l'aide de l'interface graphique, reportez-vous à la section «Interface graphique» à la page 117.

Utilisation des journaux Site Selector

Les journaux employés par Site Selector sont similaires à ceux utilisés dans Dispatcher. Pour plus d'information, reportez-vous à la section «Utilisation des journaux Network Dispatcher» à la page 215.

Utilisation du composant Cisco Consultant

Lancement et arrêt de Cisco Consultant

1. A partir d'une ligne de commande, entrez **lbcserver** pour lancer Cisco Consultant.
2. A partir d'une ligne de commande, entrez **lbcserver stop** pour arrêter Cisco Consultant.

Contrôle de Cisco Consultant

Après avoir lancé Cisco Consultant, vous pouvez le contrôler en utilisant une des méthodes suivantes :

- Configurez Cisco Consultant à l'aide de la commande **lbcontrol**. La syntaxe complète de cette commande est décrite dans «Annexe E. Guide des commandes Consultant for Cisco CSS Switches» à la page 357. Voici quelques exemples d'utilisation de cette commande.
- Configurez Cisco Consultant à l'aide de l'interface utilisateur graphique. A partir de la ligne de commande, entrez **ndadmin** pour ouvrir l'interface graphique. Pour obtenir plus d'informations sur le mode de configuration de Cisco Consultant à l'aide de l'interface utilisateur, reportez-vous à la section «Interface graphique» à la page 117.

Utilisation des journaux Cisco Consultant

Les journaux employés par Cisco Consultant sont similaires à ceux utilisés dans Dispatcher. Pour plus d'information, reportez-vous à la section «Utilisation des journaux Network Dispatcher» à la page 215.

Utilisation du composant Metric Server

Lancement et arrêt de Metric Server

Metric Server fournit à Network Dispatcher des informations relatives à la charge des serveurs. Il réside sur chaque serveur soumis à l'équilibrage de charge.

- A partir de la ligne de commande de chaque serveur hébergeant Metric Server, entrez **metricserver start** pour lancer Metric Server.
- A partir de la ligne de commande de chaque serveur hébergeant Metric Server, entrez **metricserver stop** pour arrêter Metric Server.

Utilisation des journaux Metric Server

Modifiez le niveau de journalisation dans le script de démarrage de Metric Server. Vous pouvez indiquer un niveau de journalisation compris entre 0 et 5, à l'instar de la plage admise pour les journaux de Network Dispatcher. Cette action génère un journal des agents dans le répertoire **...ms/logs**.

Chapitre 16. Résolution des incidents

Ce chapitre permet la détection et la résolution des incidents associés à Network Dispatcher. Recherchez le symptôme rencontré dans le «Tableaux de résolution des incidents».

Tableaux de résolution des incidents

Ces tableaux de résolution des incidents concernent Dispatcher, CBR, Mailbox Locator, Site Selector et Consultant for Cisco CSS Switches.

Tableau 14. Tableau de résolution des incidents de Dispatcher

Symptôme	Cause possible	Voir...
Dispatcher ne fonctionne pas correctement	Conflit de numéros de port	«Vérification des numéros de port de Dispatcher» à la page 235
Le serveur configuré ne répond pas aux requêtes d'équilibrage de charge	Conflit d'adresses ou adresse erronée	«Incident : Le répartiteur et le serveur ne répondent pas» à la page 239
Absence de prise en charge des connexions des machines client ou dépassement de délai des connexions	<ul style="list-style-type: none">• Mauvaise configuration de réacheminement• NIC sans alias avec l'adresse de grappe• Le serveur n'a pas de dispositif de bouclage ayant un alias pour l'adresse de grappe• Le chemin supplémentaire n'est pas supprimé• Le port n'est pas défini pour chaque grappe• Les serveurs sont désactivés ou mis à une pondération de zéro	«Incident : les requêtes Dispatcher ne sont pas équilibrées» à la page 239
Les machines client ne sont pas prises en charge ou le délai imparti à ces connexions est dépassé	La fonction haute disponibilité est inopérante	«Incident : la fonction haute disponibilité de Dispatcher est inopérante» à la page 240

Tableau 14. Tableau de résolution des incidents de Dispatcher (suite)

Symptôme	Cause possible	Voir...
Impossible d'ajouter un signal de présence (Windows 2000)	L'adresse source n'est pas configurée sur un adaptateur	«Incident : Impossible d'ajouter un signal de présence (Windows 2000)» à la page 240
Le serveur ne livre pas les requêtes (Window)	Une route supplémentaire a été créée dans la table de routage	«Incident : Routes supplémentaires (Windows 2000)» à la page 240
Les conseillers ne fonctionnent pas correctement en réseau étendu	Les conseillers ne fonctionnent pas sur les machines éloignées	«Incident : les conseillers ne fonctionnent pas correctement» à la page 240
SNMPD ne peut plus être lancé ou exécuté (Windows 2000)	Le nom de communauté entré dans les commandes SNMP n'est pas cohérent avec celui qui a servi à lancer le sous-agent	«Incident : SNMPD ne semble pas fonctionner correctement (Windows 2000)» à la page 240
Dispatcher, Microsoft IIS et SSL ne fonctionnent pas ou risquent de s'arrêter.	Impossible d'envoyer des données codées via les protocoles	«Incident : Dispatcher, Microsoft IIS et SSL ne fonctionnent pas (Windows 2000)» à la page 241
Connexion à une machine distante refusée	Une ancienne version des clés est encore utilisée	«Incident : Connexion du répartiteur à une machine éloignée» à la page 241
La commande ndcontrol ou ndadmin n'a pas abouti, le message 'Le serveur ne répond pas' ou 'Impossible d'accéder au serveur RMI' s'affiche.	<ol style="list-style-type: none"> 1. Echec des commandes en raison d'une pile mise sur "sock". Ou les commandes n'ont pas abouti car ndserver n'a pas été lancé 2. La définition des ports RMI est incorrecte. 	«Incident : échec de la commande ndcontrol ou ndadmin» à la page 241
Message d'erreur "Impossible trouver fichier...", lors de l'exécution de Netscape en tant que navigateur par défaut pour visualiser l'aide en ligne (Windows 2000)	Paramétrage incorrect pour l'association de fichier HTML	«Incident : le message d'erreur "Impossible trouver fichier ..." s'affiche lorsque vous tentez d'afficher l'aide en ligne (Windows 2000)» à la page 242

Tableau 14. Tableau de résolution des incidents de Dispatcher (suite)

Symptôme	Cause possible	Voir...
“stty: : No such device or address” (aucun périphérique ou adresse de ce type) lors du lancement de ndserver sous Solaris 2.7.	Ignorez ce message d’erreur. Il ne s’agit pas d’un problème. Ndserver s’exécute correctement	«Incident : Message d’erreur incorrect lors du lancement de ndserver sous Solaris 2.7» à la page 242
L’interface graphique ne démarre pas correctement	Espace de pagination insuffisant	«Incident : l’interface graphique ne démarre pas correctement» à la page 242
Erreur lors de l’exécution de Dispatcher lorsque Caching Proxy est installé	Dépendance de fichiers Caching Proxy	«Incident : Erreur lors de l’exécution de Dispatcher lorsque Caching Proxy est installé» à la page 243
L’interface utilisateur graphique ne s’affiche pas correctement.	La résolution est incorrecte.	«Incident : l’interface graphique ne s’affiche pas correctement» à la page 243
Les panneaux d’aide apparaissent parfois sous d’autres fenêtres	Limite Java	«Incident : sous Windows 2000, les fenêtre d’aide disparaissent parfois sous d’autres fenêtres ouvertes» à la page 243
Network Dispatcher ne peut pas traiter et transmettre de cadre	Une adresse MAC unique est nécessaire pour chaque carte NIC	«Incident: Network Dispatcher ne peut pas traiter et transmettre un cadre» à la page 243
Un écran bleu apparaît	Aucune carte réseau n’est installée et configurée	«Incident : un écran bleu s’affiche lors du lancement de l’exécuteur Network Dispatcher» à la page 244
La fonction Path MTU Discovery permet d’éviter le trafic retour	La grappe est associée à un alias sur le dispositif de bouclage	«Incident : la fonction Path MTU Discovery permet d’éviter le trafic retour avec Network Dispatcher» à la page 244
Les conseillers indiquent que tous les serveurs sont en panne	Calcul incorrect du total de contrôle TCP	«Incident : les conseillers indiquent que tous les serveurs sont en panne» à la page 245
La fonction haute disponibilité de Network Dispatcher en mode réseau étendu est inopérante	La machine Dispatcher éloignée doit être définie en tant que serveur d’une grappe sur la machine Dispatcher locale	«Incident : la fonction haute disponibilité de Network Dispatcher en mode réseau étendu est inopérante» à la page 245

Tableau 14. Tableau de résolution des incidents de Dispatcher (suite)

Symptôme	Cause possible	Voir...
Arrêt (ou comportement imprévu) de l'interface graphique lors de la tentative de chargement d'un fichier de configuration volumineux.	La mémoire est insuffisante pour permettre à Java de traiter une modification de l'interface graphique de cette ampleur.	«Incident : Arrêt (ou comportement imprévu) de l'interface graphique lors de la tentative de chargement d'un fichier de configuration volumineux» à la page 246

Tableau 15. Tableau de résolution des incidents de CBR

Symptôme	Cause possible	Reportez-vous à la section.
CBR ne fonctionne pas correctement	Conflit de numéros de port	«Vérification des numéros de port de CBR» à la page 236
La commande cbrcontrol ou ndadmin n'a pas abouti, le message 'Le serveur ne répond pas' ou 'Impossible d'accéder au serveur RMI' s'affiche	Echec des commandes en raison d'une pile mise sur "sock". Ou les commandes n'ont pas abouti car cbrserver n'a pas été lancé	«Incident : les commandes cbrcontrol ou ndadmin n'ont pas abouti» à la page 247
La charge des demandes n'est pas équilibrée	Caching Proxy a été lancé avant l'exécuteur	«Incident : les requêtes ne sont pas équilibrées» à la page 247
Sous Solaris, la commande cbrcontrol de démarrage de l'exécuteur affiche le message 'Erreur: l'exécuteur n'a pas été lancé' lorsqu'elle échoue.	La commande peut échouer lorsqu'une modification des valeurs IPC système par défaut est nécessaire	«Incident : sous Solaris, la commande cbrcontrol n'aboutit pas» à la page 247
La règle d'URL ne fonctionne pas	Erreur de syntaxe ou de configuration	«Incident : erreur de syntaxe ou de configuration» à la page 248

Tableau 16. Tableau de résolution des incidents Mailbox Locator

Symptôme	Cause possible	Reportez-vous à la section.
Mailbox Locator ne s'exécute pas correctement	Conflit de numéros de port	«Vérification des numéros de port de Mailbox Locator» à la page 237
La commande mlserver renvoie une exception "java.rmi.RMI Security Exception: security.fd.read"	La limite système imposée pour les descripteurs de fichiers est trop petite pour le nombre de demandes que mlserver tente de traiter	«Incident : la commande mlserver est arrêtée» à la page 248
La commande mlcontrol ou ndadmin n'a pas abouti, le message 'Le serveur ne répond pas' ou 'Impossible d'accéder au serveur RMI' s'affiche	Echec des commandes en raison d'une pile mise sur "sock". Ou les commandes n'aboutissent pas car mlserver n'a pas été lancé.	«Incident : la commande mlcontrol ou ndadmin n'a pas abouti» à la page 249
Impossible d'ajouter un port	Une autre application est déjà en mode écoute sur ce port	«Incident : impossible d'ajouter un port» à la page 249
Réception d'une erreur proxy lors d'une tentative d'ajout d'un port	L'adresse de grappe n'a pas été configurée sur un NIC avant le lancement de la commande sous proxy. Ou une autre application est en cours d'exécution sur ce port.	«Incident : réception d'une erreur proxy lors d'une tentative d'ajout de port» à la page 249

Tableau 17. Tableau de résolution des incidents de Site Selector

Symptôme	Cause possible	Voir...
Site Selector ne s'exécute pas correctement	Conflit de numéros de port	«Vérification des numéros de port Site Selector» à la page 237
Site Selector n'effectue pas de demandes entrantes permutees de façon circulaire à partir des clients Solaris	Les système Solaris exécutent un "démon de mémoire cache de service annuaire"	«Incident : Site Selector ne permet pas le trafic à permutation circulaire à partir des clients Solaris» à la page 250
La commande sscontrol ou ndadmin n'a pas abouti, le message 'Le serveur ne répond pas' ou 'Impossible d'accéder au serveur RMI' s'affiche	Echec des commandes en raison d'une pile mise sur "sock". Ou les commandes n'ont pas abouti car sserver n'a pas été lancé.	«Incident : la commande sscontrol ou ndadmin n'a pas abouti» à la page 250

Tableau 17. Tableau de résolution des incidents de Site Selector (suite)

Symptôme	Cause possible	Voir...
Echec du démarrage de sserver sous Windows 2000	Windows ne nécessite pas la présence du nom d'hôte dans le système DNS.	«Incident : Echec du démarrage de sserver sous Windows 2000» à la page 250
Machine ayant des chemins en double pour lequel l'équilibrage de charge ne s'effectue pas correctement — la résolution de noms semble ne pas aboutir	Machine Site Selector ayant plusieurs cartes associées au même sous-réseau	«Incident : Site Selector ayant des chemins en double pour lequel l'équilibrage de charge ne s'effectue pas correctement» à la page 251

Tableau 18. Tableau de résolution des incidents de Consultant for Cisco CSS Switches

Symptôme	Cause possible	Voir...
Echec du lancement de lbcsrvr	Conflit de numéros de port	«Vérification des numéros de port Cisco Consultant» à la page 238
La commande lbcontrol ou ndadmin n'a pas abouti, le message 'Le serveur ne répond pas' or 'Impossible d'accéder au serveur RMI' s'affiche.	Echec des commandes en raison d'une pile mise sur "sock". Ou les commandes n'ont pas abouti car lbcsrvr n'a pas été lancé.	«Incident : la commande lbcontrol ou ndadmin n'a pas abouti» à la page 251
Erreur de réception : Impossible de créer un registre sur le port 14099	Licence du produit expirée	«Incident : impossible de créer un registre sur le port 14099» à la page 251

Tableau 19. Tableau de dépannage du système Metric Server

Symptôme	Cause possible	Voir...
IOException Metric Server sous Windows 2000 lors de l'exécution de fichiers de mesures utilisateur de format BAT ou CMD	Le nom complet des mesures est obligatoire	«Incident : IOException Metric Server sous Windows 2000 lors de l'exécution de fichiers de mesures utilisateur de format BAT ou CMD» à la page 252

Tableau 19. Tableau de dépannage du système Metric Server (suite)

Symptôme	Cause possible	Voir...
Le système Metric Server ne fournit pas à la machine Network Dispatcher les informations relatives à la charge.	Causes possibles : <ul style="list-style-type: none"> • absence de fichier de clés sur la machine Metric Server • non d'hôte de la machine Metric Server non enregistré sur le serveur de noms local 	«Incident : Metric Server n'indique pas la charge à la machine Network Dispatcher» à la page 252
L'entrée "Signature is necessary for access to agent" (signature nécessaire pour accéder à l'agent) apparaît dans le journal de la machine Metric Server lors du transfert des fichiers de clés vers le serveur	Echec de l'autorisation du fichier de clés en raison d'une altération.	«Incident : Le journal de la machine Metric Server indique qu'une signature est nécessaire pour accéder à l'agent» à la page 252

Vérification des numéros de port de Dispatcher

En cas d'incidents lors de l'exécution de Dispatcher, il se peut que l'une des applications utilise un numéro de port généralement utilisé par Dispatcher. Notez que le serveur Dispatcher utilise les numéros de port suivants :

- 10099 pour recevoir des commandes de ndcontrol
- 10004 pour envoyer des demandes de mesure au système Metric Server
- 10005 pour recevoir des informations de l'agent SDA

Si une autre application utilise l'un des numéros de port Dispatcher, vous pouvez modifier le numéro de port de Dispatcher en procédant comme suit :

- Pour modifier le port permettant de recevoir des commandes
 - Remplacez la variable ND_RMIPORT figurant au début du script du fichier ndserver par le port que Dispatcher doit utiliser pour recevoir les commandes.
- Pour modifier le port permettant de recevoir les rapports de mesure du système Metric Server
 - Remplacez la variable RMI_PORT dans le fichier metricserver par le port devant être utilisé pour les communications avec le système Metric Server.

- Fournissez l'argument `port_mesure` lors du lancement du gestionnaire. Reportez-vous à la description de la syntaxe de commande **ndcontrol manager start** «ndcontrol manager — Contrôle du gestionnaire» à la page 287
- Pour modifier le port utilisé pour la réception des informations SDA, remplacez la variable `ND_AFFINITY_PORT` dans le fichier par le port que Dispatcher doit utiliser pour recevoir des informations SDA.

Remarque : Pour Windows 2000, les fichiers `ndserver` et `metricserver` se trouvent dans le répertoire `c:\winnt\system32`. Pour les autres plate-formes, ces fichiers se trouvent dans le répertoire `/usr/bin/`.

Vérification des numéros de port de CBR

En cas d'incidents lors de l'exécution de CBR, il se peut que l'une des applications utilise un numéro de port généralement utilisé par CBR. Prenez en compte que CBR utilise le numéro de port suivant :

- 11099 pour recevoir des commandes de `cbrcontrol`
- 10004 pour envoyer des demandes de mesure au système Metric Server

Si une autre application utilise l'un des numéros de port de CBR, vous pouvez modifier le numéro de port de CBR en procédant comme suit :

- Pour modifier le port permettant de recevoir des commandes
 - Remplacez la variable `ND_RMIPORT` variable figurant au début du fichier `cbrserver` par le port que CBR doit utiliser pour recevoir des commandes.
- Pour modifier le port permettant de recevoir les rapports de mesure du système Metric Server
 - Remplacez la variable `RMI_PORT` dans le fichier `metricserver` par le port devant être utilisé par CBR pour communiquer avec le système Metric Server.
 - Fournissez l'argument `port_mesure` lors du lancement du gestionnaire. Reportez-vous à la syntaxe de la commande **manager start** «ndcontrol manager — Contrôle du gestionnaire» à la page 287

Remarque : Pour Windows 2000, les fichiers `cbrserver` et `metricserver` se trouvent dans le répertoire `c:\winnt\system32`. Pour les autres plate-formes, ces fichiers se trouvent dans le répertoire `/usr/bin/`.

Vérification des numéros de port de Mailbox Locator

En cas d'incidents lors de l'exécution de Mailbox Locator, il se peut que l'une des applications utilise un numéro de port généralement utilisé par Mailbox Locator. Prenez en compte le fait que Mailbox Locator utilise les numéros de port suivants :

- 13099 pour recevoir des commandes de mlcontrol
- 10004 pour envoyer des demandes de mesure au système Metric Server

Si une autre application utilise l'un des numéros de port Mailbox Locator, vous pouvez modifier le numéro de port de Mailbox Locator' en procédant comme suit :

- Pour modifier le port permettant de recevoir des commandes
 - Remplacez la variable ND_RMIPORT figurant au début du fichier mlserver par le port Mailbox Locator que Mailbox Locator doit utiliser pour recevoir des commandes.
- Pour modifier le port permettant de recevoir les rapports de mesure du système Metric Server
 - Remplacez la variable RMI_PORT dans le fichier metricserver par le port que Mailbox Locator doit utiliser pour communiquer avec le système Metric Server.
 - Fournissez l'argument port_mesure lors du lancement du gestionnaire. Reportez-vous à la syntaxe de la commande **manager start** «ndcontrol manager — Contrôle du gestionnaire» à la page 287

Remarque : Pour Windows 2000, les fichiers mlserver et metricserver se trouvent dans le répertoire c:\winnt\system32. Pour les autres plate-formes, ces fichiers se trouvent dans le répertoire /usr/bin.

Vérification des numéros de port Site Selector

En cas d'incidents lors de l'exécution du composant Site Selector, il se peut que l'une des applications utilise un numéro de port généralement utilisé par Site Selector. Prenez en compte le fait que Site Selector utilise les numéros de port suivants :

- 12099 pour recevoir des commandes de sscontrol
- 10004 pour envoyer des demandes de mesure au système Metric Server

Si une autre application utilise l'un des numéros de port Site Selector, vous pouvez modifier le numéro de port de Site Selector' en procédant comme suit :

- Pour modifier le numéro de port permettant de recevoir des commandes,
 - Remplacez la variable ND_RMIPORT figurant au début du fichier ssserver par le port devant être utilisé par Site Selector pour recevoir les commandes.
- Pour modifier le port permettant de recevoir les rapports de mesure du système Metric Server
 - Remplacez la variable RMI_PORT dans le fichier metricserver par le port que Site Selector doit utiliser pour communiquer avec le système Metric Server.
 - Fournissez l'argument port_mesure lors du lancement du gestionnaire. Reportez-vous à la syntaxe de commande **manager start** «sscontrol manager — Contrôle du gestionnaire» à la page 337

Remarque : Pour Windows 2000, les fichiers ssserver et metricserver se trouvent dans le répertoire c:\winnt\system32. Pour les autres plate-formes, ces fichiers se trouvent dans le répertoire /usr/bin/.

Vérification des numéros de port Cisco Consultant

En cas d'incidents lors de l'exécution du composant Cisco Consultant, il se peut qu'une autre application utilise l'un des numéros de port utilisés par le serveur lbcsrvr de Cisco Consultant. Prenez en compte le fait que Cisco Consultant utilise les numéros de port suivants :

14099 pour recevoir les commandes de lbcscontrol

10004 pour envoyer des demandes de mesure au système Metric Server

Si une autre application utilise l'un des numéros de port Consultant, vous pouvez modifier le numéro de port de Consultant en procédant comme suit :

- Pour modifier le port permettant de recevoir des commandes de lbcscontrol, modifiez la variable dans le fichier ND_RMIPORT dans le fichier lbcsrvr. Remplacez 14099 par le port sur lequel vous voulez que Consultant reçoive les commandes lbcscontrol.
- Pour modifier le port permettant de recevoir les rapports de mesure du système Metric Server :
 1. Modifiez la variable RMI_PORT dans le fichier metricserver. Remplacez 10004 sur lequel Consultant doit communiquer avec le système Metric Server.

2. Fournissez l'argument `port_mesure` lors du lancement du gestionnaire. Pour obtenir une description de la syntaxe de la commande `lbcontrol manager start`, reportez-vous à la section «`lbcontrol manager` — Contrôle du gestionnaire» à la page 372.

Remarque : Pour Windows 2000, les fichiers `lbserver` et `metricserver` se trouvent dans le répertoire `c:\winnt\system32`. Pour les autres plate-formes, ces fichiers se trouvent dans le répertoire `/usr/bin`.

Résolution des incidents courants—Dispatcher

Incident : Dispatcher ne fonctionne pas

Cet incident peut se produire lorsqu'une autre application utilise l'un des ports utilisés par Dispatcher. Pour plus de détails, reportez-vous à la section «Vérification des numéros de port de Dispatcher» à la page 235.

Incident : Le répartiteur et le serveur ne répondent pas

Cet incident se produit lorsque qu'une adresse autre que l'adresse spécifiée est utilisée. Lorsque vous placez le Dispatcher et le serveur sur le même poste, assurez-vous que l'adresse NFA est utilisée ou est configurée comme utilisant le même poste.

Incident : les requêtes Dispatcher ne sont pas équilibrées

Les symptômes de cet incident sont l'absence de prise en charge des connexions des machines client ou le dépassement du délai des connexions. Effectuez les contrôles suivants pour diagnostiquer cet incident :

1. Avez-vous configuré l'adresse de non-réacheminement, les grappes, les ports et les serveurs pour l'acheminement ? Vérifiez le fichier de configuration.
2. L'alias de la carte d'interface de réseau est-il associé à l'adresse de grappe ? Utilisez `netstat -ni` pour vérifier.
3. L'alias de l'unité de bouclage de chaque serveur est-il associé à l'adresse de grappe ? Utilisez `netstat -ni` pour vérifier.
4. La voie d'acheminement supplémentaire est-elle supprimée ? Utilisez `netstat -nr` pour vérifier.
5. Utilisez la commande `ndcontrol cluster status` pour vérifier les informations relatives à chacune des grappes que vous avez définies. Assurez-vous qu'un port est défini pour chaque grappe.
6. Utilisez la commande `ndcontrol server report::` pour vérifier que vos serveurs ne sont pas hors service ou qu'ils n'ont pas pour valeur une pondération égale à zéro.

Incident : la fonction haute disponibilité de Dispatcher est inopérante

Cet incident se produit lorsqu'un environnement de haute disponibilité de Dispatcher est configuré et que les connexions des machines client ne sont pas prises en charge ou que le délai imparti à ces connexions est dépassé.

Effectuez les contrôles suivants pour corriger ou diagnostiquer l'incident :

- Assurez-vous que les scripts `goActive`, `goStandby` et `goInOp` ont été créés et qu'ils se trouvent dans le répertoire `bin` dans lequel Dispatcher est installé. Pour obtenir plus d'informations sur ces scripts, reportez-vous à la rubrique «Utilisation de scripts» à la page 178
- Pour **AIX**, **Linux** et **Solaris**, assurez-vous que droit d'exécution est défini pour les scripts `goActive`, `goStandby` et `goInOp`.
- Sous **Windows 2000**, pensez à configurer l'adresse de non-réacheminement.

Incident : Impossible d'ajouter un signal de présence (Windows 2000)

Cette erreur Windows 2000 se produit lorsque l'adresse source n'est pas configuré sur un adaptateur. Effectuez les contrôles suivants pour corriger ou diagnostiquer l'incident :

- Pour **Windows 2000**, assurez-vous de configurer l'adresse de non-réacheminement en utilisant l'interface en anneau à jeton ou Ethernet et en exécutant l'une des commandes suivantes :

```
ndconfig tr0 <adresse ip> netmask <masque_réseau>
ou
ndcontrol cluster configure
```

Incident : Routes supplémentaires (Windows 2000)

Après la configuration des serveurs, il se peut qu'une ou plusieurs routes supplémentaires aient été créées par inadvertance. Si elles ne sont pas supprimées, ces routes empêchent le fonctionnement de Dispatcher. Reportez-vous à la section «Configuration des serveurs pour l'équilibrage de la charge» à la page 67 pour les contrôler et les supprimer.

Incident : les conseillers ne fonctionnent pas correctement

Si vous utilisez un support de réseau étendu et que les conseillers ne semblent pas fonctionner correctement, vérifiez qu'ils sont bien lancés sur les répartiteurs locaux et éloignés. Reportez-vous à la section «Utilisation de conseillers éloignés avec le support de réseau étendu» à la page 166.

Incident : SNMPD ne semble pas fonctionner correctement (Windows 2000)

Lors de l'utilisation de sous-agents SNMP, si le démon `SystemViewAgent` SNMP ne peut pas être lancé et rester actif, vérifiez que vous avez bien configuré votre communauté SNMP à l'aide du programme `snmpcfg`. Pour que vous puissiez accéder aux données SNMP à partir du sous-agent Dispatcher, le nom de communauté entré dans les commandes SNMP doit être cohérent avec celui avec lequel le sous-agent a été lancé.

Incident : Dispatcher, Microsoft IIS et SSL ne fonctionnent pas (Windows 2000)

Lorsque vous utilisez Dispatcher, Microsoft IIS et SSL, s'ils ne fonctionnent pas ensemble, il se peut qu'un incident lié à la sécurité SSL se soit produit. Pour obtenir plus d'informations sur la génération d'une paire de clés, l'acquisition d'un certificat, l'installation d'un certificat avec une paire de clés et sur la configuration d'un répertoire pour SSL, reportez-vous au manuel *Microsoft Information and Peer Web Services Information and Planning Guide* fourni avec Windows 2000. L'URL locale du document que vous pouvez consulter à l'aide d'un navigateur Web est la suivante :

file:///C:/WINNT/system32/inetsrv/iisadmin/htmldocs/inetdocs.htm.

Incident : Connexion du répartiteur à une machine éloignée

Dispatcher utilise des clés pour vous permettre de vous connecter à une machine éloignée et la configurer. Les clés indiquent un port RMI pour la connexion. Il est possible de changer de port RMI pour des raisons de sécurité ou de conflits. Lorsque vous changez les ports RMI, le nom de fichier ou la clé est différent(e). Si votre répertoire contient plusieurs clés pour la même machine éloignée et qu'elles indiquent des ports RMI différents, la ligne de commande essaie la première qu'elle trouve. Si elle n'est pas appropriée, la connexion est refusée. La connexion ne sera établie que si vous supprimez la clé incorrecte.

Incident : échec de la commande ndcontrol ou ndadmin

1. La commande ndcontrol renvoie : **Erreur : Pas de réponse du serveur**. Ou la commande ndadmin renvoie : **Erreur : impossible accéder au serveur RMI**. Ces erreurs peuvent se manifester lorsque votre machine a une pile sur "sock". Pour corriger ce problème, éditez le fichier socks.cnf pour qu'il contienne les lignes suivantes :

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

2. Les consoles d'administration des interfaces Network Dispatcher (ligne de commande, interface graphique et assistants) communiquent avec ndserver par appels RMI (Remote Method Invocation). Par défaut, la communication utilise deux ports : l'un est défini dans le script de démarrage de ndserver et l'autre est aléatoire.

Le port aléatoire peut être source de problèmes lorsqu'une des consoles d'administration s'exécute sur la même machine qu'un pare-feu ou passe par un pare-feu. Par exemple, lorsque vous émettez la commande ndcontrol alors que Network Dispatcher s'exécute sur la même machine qu'un pare-feu, des erreurs de type **Erreur : Pas de réponse du serveur** peuvent apparaître.

Pour éviter ce type d'incident, modifiez le fichier script ndserver (situé dans PATH) afin de définir le port aléatoire utilisé par RMI. Insérez -DND_RMI_SERVER_PORT=*votrePort* dans la chaîne END_ACCESS, où *votrePort* correspond au port spécifié.

Par exemple :

```
END_ACCESS='-DND_CLIENT_KEYS_DIRECTORY=/usr/lpp/nd/admin/keys/dispatcher
-DND_SERVER_KEYS_DIRECTORY=/usr/lpp/nd/dispatcher/key
-DND_RMI_SERVER_PORT=10100'
ND_RMIPORT=10099
```

Lorsque vous avez terminé, relancez la commande ndserver et ouvrez le trafic des ports 10099 et 10100 ou du port d'adresse hôte choisi pour l'exécution de la console d'administration.

3. Ces erreurs peuvent également se produire si vous n'avez pas encore lancé ndserver.

Incident : le message d'erreur "Impossible trouver fichier ..." s'affiche lorsque vous tentez d'afficher l'aide en ligne (Windows 2000)

Sous Windows 2000, lorsque vous utilisez Netscape comme navigateur par défaut, le message d'erreur s'affiche si cet incident se produit : "Impossible trouver fichier '<nomfichier>.html' (ou un de ses composants). Vérifiez que le chemin et le nom de fichier sont corrects et que toutes les bibliothèques nécessaires sont disponibles.

Le problème est dû à un réglage incorrect pour l'association de fichier HTML. La solution est la suivante :

1. Cliquez sur **My Computer**, cliquez sur **Outils**, sélectionnez **Options dossier** et cliquez sur l'onglet **Types fichiers** tab
2. Sélectionnez "Document hypertexte Netscape"
3. Cliquez sur le bouton **Avancé**, sélectionnez **ouvrir**, cliquez sur le bouton **Editer**
4. Entrez *NSShell* dans la zone **Application :** (et non dans la zone Application utilisée pour réaliser action :), puis cliquez sur **OK**

Incident : Message d'erreur incorrect lors du lancement de ndserver sous Solaris 2.7

Lors du lancement de ndserver sous Solaris 2.7, le message d'erreur incorrect suivant s'affiche : "stty: : No such device or address." (aucun périphérique ou adresse de ce type). Ignorez ce message d'erreur. Ndserver s'exécute correctement.

Incident : l'interface graphique ne démarre pas correctement

Pour que l'interface graphique, ndadmin, fonctionne correctement, vous devez disposer d'une quantité d'espace de pagination suffisante. Dans le cas

contraire, l'interface graphique peut ne pas démarrer complètement. Si cela se produit, vérifiez l'espace de pagination et augmentez-la si nécessaire.

Incident : Erreur lors de l'exécution de Dispatcher lorsque Caching Proxy est installé

Si vous désinstallez Network Dispatcher afin de réinstaller une autre version et que vous obtenez une erreur lorsque vous tentez de lancer le composant Dispatcher, vérifiez si Caching Proxy est installé. Caching Proxy est lié à un des fichiers Dispatcher. Ce fichier sera désinstallé lors de la désinstallation de Caching Proxy.

Pour résoudre ce problème :

1. Désinstallez Caching Proxy.
2. Désinstallez Network Dispatcher.
3. Réinstallez Network Dispatcher et Caching Proxy.

Incident : l'interface graphique ne s'affiche pas correctement

Si des incidents se produisent relatifs à l'apparence de l'interface graphique de Network Dispatcher, vérifiez la configuration de la résolution du bureau du système d'exploitation. Pour un affichage de l'interface graphique optimal, nous vous recommandons d'utiliser une résolution de 1024x768 pixels.

Incident : sous Windows 2000, les fenêtre d'aide disparaissent parfois sous d'autres fenêtres ouvertes

Lorsque vous ouvrez des fenêtres d'aide sous Windows 2000, elles peuvent disparaître en arrière-plan sous les fenêtres existantes. Si cela se produit, cliquez sur la fenêtre pour qu'elle s'affiche à nouveau en premier plan.

Incident: Network Dispatcher ne peut pas traiter et transmettre un cadre

Sous Solaris, chaque carte réseau possède la même adresse MAC par défaut. Cela fonctionne correctement lorsque chaque carte se trouve sur un sous-réseau IP différent. Cependant, dans un environnement commuté, lorsque plusieurs cartes NIC ayant la même adresse MAC et la même adresse de sous-réseau IP communiquent avec le même commutateur, ce dernier envoie l'ensemble du trafic associé à l'adresse MAC (et aux adresses IP) via le même câble. Seule la carte ayant la dernière placé un cadre sur ce réseau voit les paquets IP associés aux deux cartes. Solaris peut ignorer les paquets d'une adresse IP valide arrivant à l'interface "incorrecte".

Si toutes les interfaces réseau ne sont désignées pour Network Dispatcher, comme il est configuré dans le fichier `ibmnd.conf` et si la carte NIC qui n'est pas définie dans `ibmnd.conf` reçoit un cadre, Network Dispatcher ne peut pas traiter et transmettre le cadre.

Pour éviter ce problème, vous devez remplacer la valeur par défaut et définir une adresse unique pour chaque interface. Utilisez la commande ci-après.

```
ifconfig interface ether adrMac
```

Par exemple :

```
ifconfig hme0 ether 01:02:03:04:05:06
```

Incident : un écran bleu s'affiche lors du lancement de l'exécuteur Network Dispatcher

Sous Windows 2000, vous devez avoir une carte réseau installée et configurée avant le lancement de l'exécuteur.

Incident : la fonction Path MTU Discovery permet d'éviter le trafic retour avec Network Dispatcher

Le système d'exploitation AIX contient une fonction de mise en réseau appelée "Path MTU Discovery". Lors d'une transaction avec un client, si le système d'exploitation détermine qu'une unité de transmission maximale (MTU) inférieure doit être utilisée pour les paquets sortants, la fonction Path MTU Discovery entraîne la création par AIX d'une route de rappel de cette unité. La nouvelle route est réservée à cette adresse IP client et enregistre l'unité MTU qui permet d'atteindre celle-ci.

Lors de la création de la route, un incident peut survenir sur les serveurs en raison de l'association de la grappe à un alias sur le dispositif de bouclage. Si l'adresse de la passerelle pour la route entre dans le sous-réseau de la grappe ou du masque réseau, AIX crée la route sur le dispositif de bouclage. Cet événement s'est produit car il s'agissait de l'alias de la dernière interface associé à ce sous-réseau.

Par exemple, soient la grappe 9.37.54.69, le masque réseau 255.255.255.0 et la passerelle prévue 9.37.54.1. Dans ce cas, AIX utilise le dispositif de bouclage pour la route. En raison de cette action, les réponses du serveur ne sortent jamais et le client dépasse le délai d'attente. Habituellement, le client voit une réponse de la grappe, puis il ne reçoit plus rien lorsque la route est créée.

Il existe deux solutions pour pallier cet incident :

1. Désactivez la fonction Path MTU Discovery pour que le système d'exploitation AIX n'ajoute pas de route en mode dynamique. Utilisez les commandes suivantes :

no -a liste les paramètres de mise en réseau AIX

no -o option=valeur
définit les paramètres TCP sous AIX
2. Associez l'adresse IP de grappe sur le dispositif de bouclage au masque réseau 255.255.255.255. Cela signifie que le sous-réseau associé à un alias est uniquement l'adresse IP de grappe. Lorsque le système d'exploitation AIX crée les routes dynamiques, l'adresse IP de la passerelle cible ne correspond pas à ce sous-réseau. En conséquence, la route est amenée à

utiliser l'interface réseau incorrecte. Supprimez ensuite la nouvelle route lo0 créée lors de la définition d'alias. Pour la supprimer, recherchez-la d'abord sur le dispositif de bouclage avec une destination réseau pour l'adresse IP de grappe. Cette action doit être effectuée à chaque utilisation d'alias pour la grappe.

Remarques :

1. La fonction Path MTU Discovery est désactivée par défaut dans les versions d'AIX antérieures à la version 4.3.2 et activée par défaut à partir de la version 4.3.3.
2. Les commandes ci-après permettent de désactiver la fonction Path MTU Discovery et doivent être exécutées à chaque amorçage du système. Ajoutez-les dans le fichier /etc/rc.net.
 - -o udp_pmtu_discover=0
 - -o tcp_pmtu_discover=0

Incident : les conseillers indiquent que tous les serveurs sont en panne

Windows 2000 comporte une nouvelle fonction, Task Offload, qui permet le calcul du total de contrôle TCP par la carte adaptateur, plutôt que par le système d'exploitation. Cette fonction améliore les performances dans le système. Lorsque Task Offload est activé, les conseillers Network Dispatcher signalent que les serveurs sont en panne, alors qu'ils ne le sont pas.

La cause de l'incident est la suivante : le total de contrôle TCP n'est pas calculé correctement pour les paquets provenant de l'adresse de grappe. C'est le cas avec le trafic des conseillers.

Pour éviter cet incident, atteignez les paramètres de la carte et désactivez la fonction Task Offload.

Cet incident a été observé pour la première fois avec la carte Adaptec QuadPort ANA62044. Cette carte désigne la fonction comme option de déchargement Transmit Checksum. Désactivez cette option pour éviter l'incident.

Incident : la fonction haute disponibilité de Network Dispatcher en mode réseau étendu est inopérante

Lorsque vous configurez un mode WAND (Wide Area Network Dispatcher), vous devez définir la machine Dispatcher locale en tant que serveur d'une grappe sur la machine Dispatcher locale. Habituellement, vous utilisez l'adresse de non-réacheminement (NFA) de la machine Dispatcher éloignée pour l'adresse de destination du serveur éloigné. Dans ce cas, si vous configurez ensuite sur la machine Dispatcher éloignée la fonction haute disponibilité, celle-ci reste inopérante. La cause en est la suivante : la machine Dispatcher locale désigne toujours la machine principale côté éloigné lorsque vous utilisez l'adresse NFA.

Pour éviter cet incident :

1. Définissez une autre grappe sur la machine Dispatcher éloignée. Il n'est pas nécessaire de définir des ports ou des serveurs pour cette grappe.
2. Ajoutez l'adresse de cette grappe dans les scripts goActive et goStandby.
3. Sur la machine Dispatcher locale, définissez l'adresse de grappe en tant que serveur, et non en tant qu'adresse NFA de la machine Dispatcher principale éloignée.

Lorsque la machine Dispatcher principale éloignée entre en service, elle associe cette adresse à un alias sur la carte, permettant ainsi l'acceptation du trafic. En cas de défaillance, l'adresse se déplace sur la machine de secours qui continue à accepter le trafic destiné à cette adresse.

Incident : Arrêt (ou comportement imprévu) de l'interface graphique lors de la tentative de chargement d'un fichier de configuration volumineux

Lorsque vous tentez de charger un fichier de configuration volumineux (200 commandes **add** ou plus), l'interface graphique peut s'arrêter ou avoir un comportement imprévu, comme présenter un temps de réponse excessif lorsque vous apportez des modifications à l'écran.

Cela vient du fait que la mémoire est insuffisante pour permettre à Java de traiter une modification de l'interface graphique de cette ampleur.

L'environnement d'exécution dispose d'une option permettant d'augmenter la mémoire disponible dont peut disposer Java.

Il s'agit de l'option `-Xmxn`, où `n` correspond à la taille maximale en octets de la mémoire. `n` doit être un multiple de 1024 et supérieur à 2 Mo. La valeur `n` peut être suivie du caractère `k` ou `K` pour indiquer qu'il s'agit de kilo-octets ou du caractère `m` ou `M` pour indiquer qu'il s'agit de méga-octets. Par exemple, `-Xmx128M` et `-Xmx81920k` sont valides. La valeur par défaut est de 64 Mo. La valeur maximale pouvant être associée aux plate-formes SPARC Solaris 7 et 8 est de 4000 Mo; celle pouvant être associée aux plate-formes Solaris 2.6 et x86 est de 2000 Mo.

Pour ajouter cette option, modifiez le fichier script `ndadmin` comme suit :

- **Windows NT ou 2000**

```
START jrew -mx64m %END_ACCESS% %CONFIG_DIR%  
-DEND_INSTALL_PATH=%IBMNDPATH% -cp %NDCLASSPATH%  
com.ibm.internet.nd.framework.FWK_Framework  
com.ibm.internet.nd.gui.GUI_eNDRootNode1
```

- **Solaris**

```
$JREDIR/$JRE -mx64m $END_ACCESS $CONFIG_DIR  
-DEND_INSTALL_PATH=/opt/&BASEDIR -cp $NDCLASSPATH  
com.ibm.internet.nd.framework.FWK_Framework  
com.ibm.internet.nd.gui.GUI_eNDRootNode &1
```

- **Linux**

```
re -mx64m $END_ACCESS $CONFIG_DIR $NDLOCALE  
-DEND_INSTALL_PATH=/opt/nd -classpath $NDCLASSPATH  
com.ibm.internet.nd.framework.FWK_Framework  
com.ibm.internet.nd.gui.GUI_eNDRootNode 1>/dev/null 2>&1 &1
```

- **AIX**

```
ava -mx64m $END_ACCESS $CONFIG_DIR $NDLOCALE  
-DEND_INSTALL_PATH=/usr/lpp/&BASEDIR -classpath $NDCLASSPATH  
com.ibm.internet.nd.framework.FWK_Framework  
com.ibm.internet.nd.gui.GUI_eNDRootNode 1>/dev/null 2>&1 &
```

Aucune valeur particulière n'est recommandée, mais elle doit être supérieure à l'option par défaut. Pour commencer, vous pouvez doubler cette dernière.

Résolution des incidents courants—CBR

Incident : CBR ne fonctionne pas

Cet incident peut se produire lorsqu'une autre application utilise l'un des ports utilisés par CBR. Pour plus de détails, reportez-vous à la section «Vérification des numéros de port de CBR» à la page 236.

Incident : les commandes **cbrcontrol** ou **ndadmin** n'ont pas abouti

La commande **cbrcontrol** renvoie : "Erreur : Pas de réponse du serveur." Ou la commande **ndadmin** renvoie : "Erreur : impossible accéder au serveur RMI." Ces erreurs peuvent se manifester lorsque votre machine a une pile sur "sock". Pour corriger ce problème, éditez le fichier **socks.cnf** pour qu'il contienne les lignes suivantes :

```
EXCLUDE-MODULE java  
EXCLUDE-MODULE jre  
EXCLUDE-MODULE jrew  
EXCLUDE-MODULE javaw
```

Ces erreurs peuvent également se produire si vous n'avez pas encore lancé **cbrserver**.

Incident : les requêtes ne sont pas équilibrées

Caching Proxy et CBR ont été lancés, mais les requêtes ne sont pas équilibrées. Cette erreur peut se produire lorsque vous lancez Caching Proxy avant l'exécuteur. Si c'est le cas, le journal **stderr** de Caching Proxy contient le message d'erreur indiquant l'échec de la connexion à l'exécuteur (**ndServerInit**). Pour éviter cet incident, lancez l'exécuteur avant Caching Proxy.

Incident : sous Solaris, la commande **cbrcontrol** n'aboutit pas

Sous Solaris, la commande **cbrcontrol** **executor** **start** renvoie le message suivant : "Erreur : l'exécuteur n'a pas été lancé". Cette erreur se produit si

vous ne configurez pas les communications IPC (Inter-process Communication) pour le système de telle sorte que la taille maximale d'un segment de mémoire partagée et des ID sémaphore soit supérieure à la valeur par défaut du système d'exploitation. Pour augmenter la taille du segment de mémoire partagée et des ID sémaphore, vous devez modifier le fichier **/etc/system**. Pour obtenir plus d'informations sur le mode de configuration de ce fichier, reportez-vous à la section 88.

Incident : erreur de syntaxe ou de configuration

Si la règle d'URL ne fonctionne pas, cela peut être dû à une erreur de syntaxe ou de configuration. Pour ce problème, vérifiez :

- que la règle est correctement configurée. Pour obtenir plus de détails, reportez-vous à la section «Annexe C. Syntaxe des règles de contenu (modèle)» à la page 323.
- Lancer un **rapport de règle cbrcontrol** pour cette règle et vérifier la colonne 'Exécutions, s'assurer qu'elle est incrémentée en fonction du nombre de requêtes effectuées. Si tel est le cas, vérifiez à nouveau la configuration du serveur
- Si la règle n'est pas émise, ajouter une règle 'toujours vrai'. Emettre un **rapport de règle cbrcontrol** sur la règle 'toujours vrais' pour vérifier qu'elle est émise.

Résolution des incidents courants—Mailbox Locator

Incident : Mailbox Locator ne s'exécute pas

Cet incident peut se produire lorsqu'une autre application utilise un des ports utilisés par Mailbox Locator. Pour plus de détails, reportez-vous à la section «Vérification des numéros de port de Mailbox Locator» à la page 237.

Incident : la commande mlserver est arrêtée

Sur une plate-forme UNIX, cet incident survient lorsque **mlserver** est utilisé pour équilibrer la charge avec un nombre important de demandes client IMAP/POP3 et que la limite système imposée pour les descripteurs de fichiers est trop petites pour le nombre de demandes que mlserver tente de traiter. mlserver génère l'exception suivante puis est arrêté :

```
java.rmi.RMIException: security.fd.read
```

Le fichier journal de commande sous proxy spécifique au protocole indique :

```
SocketException=java.net.SocketException:  
Socket fermée.
```

La solution consiste à modifier la limite **nfiles** (AIX, Linux) ou **open files** (Solaris) dans le shell où mlserver est lancé. Portez la limite nfiles à un

nombre raisonnable supérieur à la limite nofiles actuelle. Utilisez `ulimit -a` pour afficher la limite nofiles et utilisez `ulimit -n valeur` pour augmenter la valeur.

Incident : la commande `mlcontrol` ou `ndadmin` n'a pas abouti

La commande `mlcontrol` renvoie : "Erreur : Pas de réponse du serveur." Ou la commande `ndadmin` renvoie : "Erreur : impossible accéder au serveur RMI." Ces erreurs peuvent se manifester lorsque votre machine a une pile sur "sock". Pour corriger ce problème, éditez le fichier `socks.cnf` pour qu'il contienne les lignes suivantes :

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Ces erreurs peuvent également se produire si vous n'avez pas encore lancé `mlserver`.

Incident : impossible d'ajouter un port

Lors d'une tentative d'ajout d'un port à une configuration, vous pouvez recevoir le message d'erreur suivant : **Erreur : impossible d'ajouter le port.** Une autre application est peut-être déjà en mode écoute sur ce port. Mailbox Locator tente de lancer un proxy reliant à l'adresse IP de grappe sur le port indiqué dans la commande. Si une autre application relie à cette adresse IP ou est à l'écoute de toutes les adresses IP sur ce port, le démarrage du proxy échoue. Pour utiliser Mailbox Locator sur ce port, vous devez arrêter l'application en conflit.

Sur plate-forme Linux, le démon `xinetd` peut démarrer un programme d'écoute sans exécuter, par exemple, un programme POP3. Par conséquent, il est important de vérifier par la commande `netstat -a` si une application est en mode écoute sur le port voulu.

Incident : réception d'une erreur proxy lors d'une tentative d'ajout de port

Pour Mailbox Locator, la commande `mlcontrol port add` génère le message d'erreur suivant : "Le proxy de la grappe <grappe>, port <port> n'a pas démarré." La solution est de configurer l'adresse de la grappe sur un NIC avant de pouvoir lancer le proxy. Vérifiez également qu'aucune autre application n'est en cours d'exécution sur le port à l'écoute de l'adresse de grappes (incluant une application générale d'écoute globale).

Résolution des incidents courants—Site Selector

Incident : Site Selector ne s'exécute pas

Cet incident peut se produire lorsqu'une autre application utilise un des ports utilisés par Site Selector. Pour plus de détails, reportez-vous à la section «Vérification des numéros de port Site Selector» à la page 237.

Incident : Site Selector ne permet pas le trafic à permutation circulaire à partir des clients Solaris

Symptôme : Le composant Site Selector n'effectue pas de demandes entrantes permutees de façon circulaire à partir des clients Solaris.

Cause possible : Les systèmes Solaris exécutent un démon de mémoire cache de service annuaire. Si ce démon est en cours d'exécution, la demande du programme de résolution suivante sera traitée à partir de cette mémoire cache et non à partir du composant Site Selector ayant effectuée la demande.

Solution : Désactivez le démon de mémoire cache du service annuaire sur la machine Solaris.

Incident : la commande sscontrol ou ndadmin n'a pas abouti

La commande sscontrol renvoie : "Erreur : Pas de réponse du serveur." Ou la commande ndadmin renvoie : "Erreur : impossible accéder au serveur RMI." Ces erreurs peuvent se manifester lorsque votre machine a une pile sur "sock". Pour corriger ce problème, éditez le fichier socks.cnf pour qu'il contienne les lignes suivantes :

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Ces erreurs peuvent également se produire si vous n'avez pas encore lancé ssserver.

Incident : Echec du démarrage de ssserver sous Windows 2000

Site Selector doit pouvoir participer à un système DNS. Toutes les machines concernées par la configuration doivent également participer à ce système. Windows ne nécessite pas toujours la présence du nom d'hôte configuré dans le système DNS. Avec Site Selector, un nom d'hôte doit être défini dans le système DNS pour que le démarrage s'effectue correctement.

Vérifiez que cet hôte est défini dans le système DNS. Modifiez le fichier ssserver.cmd et supprimez le "w" de "javaw". Il devrait en résulter des erreurs supplémentaires.

Incident : Site Selector ayant des chemins en double pour lequel l'équilibrage de charge ne s'effectue pas correctement

Le serveur annuaire de Site Selector n'est associé à aucune adresse sur la machine. Il répond aux demandes destinées aux adresses IP valides de la machine. Site Selector fait confiance au système d'exploitation pour l'acheminement de la réponse au client. Si la machine Site Selector comporte plusieurs cartes et que certaines d'entre elles sont connectées au même sous-réseau, il est possible que le système d'exploitation envoie la réponse au client à partir d'une adresse différente de celle de réception. Certaines applications client n'acceptent pas de réponse provenant d'une adresse différente de celle de l'envoi. Par conséquent, la résolution de nom semble ne pas aboutir.

Résolution des incidents courants—Consultant for Cisco CSS Switches

Incident : lbcsrvr ne démarre pas

Cet incident peut se produire lorsqu'une autre application utilise un des ports employés par le serveur lbcsrvr de Consultant. Pour obtenir plus d'informations, reportez-vous à la section «Vérification des numéros de port Cisco Consultant» à la page 238.

Incident : la commande lbcccontrol ou ndadmin n'a pas abouti

La commande lbcccontrol renvoie : "Erreur : Pas de réponse du serveur." Ou la commande ndadmin renvoie : "Erreur : impossible accéder au serveur RMI." Ces erreurs peuvent se manifester lorsque votre machine a une pile sur "sock". Pour corriger ce problème, éditez le fichier socks.cnf pour qu'il contienne les lignes suivantes :

```
EXCLUDE-MODULE java
EXCLUDE-MODULE jre
EXCLUDE-MODULE jrew
EXCLUDE-MODULE javaw
```

Ces erreurs peuvent également se produire si vous n'avez pas encore lancé **lbcsrvr**.

Incident : impossible de créer un registre sur le port 14099

Cet incident peut se produire lorsqu'il manque une licence de produit valide. Lorsque vous tentez de lancer lbcsrvr, vous recevez le message suivant :

Votre licence a expiré !
Adressez-vous à votre ingénieur commercial ou à votre représentant IBM.

Pour corriger ce problème :

1. Si vous avez déjà tenté de lancer lbcsrvr, entrez **lbcsrvr stop**.
2. Copiez votre licence valide dans le répertoire **...nd/servers/conf**.

3. Entrez **lbcserver** pour lancer le serveur.

Résolution des incidents courants—Metric Server

Incident : IOException Metric Server sous Windows 2000 lors de l'exécution de fichiers de mesures utilisateur de format BAT ou CMD

Vous devez utiliser le nom complet des mesures enregistrées par l'utilisateur sur les postes Metric Server Windows 2000. Par exemple, vous devez indiquer **usermetric.bat**, et non **usermetric**. Le nom **usermetric** est valide sur la ligne de commande, mais est inopérant lorsqu'il est employé à partir de l'environnement d'exécution. Si vous n'utilisez pas de nom complet pour les mesures, vous recevez une exception d'entrée-sortie Metric Server. Attribuez la valeur 3 à la variable LOG_LEVEL dans le fichier de commandes metricserver, puis consultez la sortie de journal. Dans cet exemple, l'exception se présente comme suit :

```
... java.io.IOException: CreateProcess: usermetric error=2
```

Incident : Metric Server n'indique pas la charge à la machine Network Dispatcher

Différentes raisons peuvent expliquer pourquoi le système Metric Server ne transmet pas les informations relatives à la charge à Network Dispatcher. Procédez aux vérifications suivantes pour en déterminer la cause :

- Vérifiez que les fichiers de clés ont bien été transférés sur Metric Server.
- Vérifiez que le nom d'hôte de la machine Metric Server est enregistré sur le serveur de noms local.
- Redémarrez avec un niveau de journalisation supérieur et recherchez les erreurs.
- Augmentez le niveau de journalisation de la machine Network Dispatcher. Recherchez les erreurs dans le journal du contrôleur de mesures.

Incident : Le journal de la machine Metric Server indique qu'une signature est nécessaire pour accéder à l'agent

Le journal de la machine Metric Server présente ce message d'erreur suite au transfert de fichiers de clés sur le serveur.

Cette erreur est consignée lorsque le fichier de clés ne donne pas d'autorisation avec la clé de la paire en raison d'une altération dans cette dernière. Pour remédier à ce problème, procédez comme suit :

- Téléchargez de nouveau le fichier de clés via le protocole FTP selon la méthode de transfert binaire.
- Créez une nouvelle clé et redistribuez-la.

Annexe A. Lecture d'un schéma de syntaxe

Le schéma de syntaxe explique comment indiquer une commande de sorte que le système d'exploitation puisse interpréter correctement les données que vous entrez. Lisez le schéma de syntaxe de gauche à droite et de haut en bas, suivant la ligne horizontale (chemin principal).

Symboles et ponctuation

Les symboles suivants sont utilisés dans les schémas de syntaxe :

Symbole

Description

- » Marque le début de la syntaxe de la commande.
- « Marque la fin de la syntaxe de la commande.

Vous devez inclure tous les signes de ponctuation tels que le deux-points, le point d'interrogation et le signe moins, qui sont indiqués dans le schéma de syntaxe.

Paramètres

Les types de paramètres suivants sont utilisés dans les schémas de syntaxe :

Paramètre

Description

Obligatoire

Les paramètres obligatoires s'affichent dans le chemin principal.

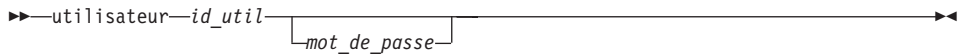
Facultatif

Les paramètres facultatifs s'affichent sous le chemin principal.

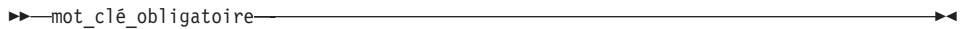
Les paramètres sont classés par mots clés ou par variables. Les mots clés s'affichent en minuscules et peuvent être entrés en minuscules. Par exemple, un nom de commande est un mot clé. Les variables apparaissent en italique et représentent des noms ou des valeurs que vous indiquez.

Exemples de syntaxe

Dans l'exemple suivant, la commande de l'utilisateur correspond à un mot clé. La variable obligatoire est *id_util* et la variable facultative *mot_de_passe*. Remplacez les variables par vos propres valeurs.

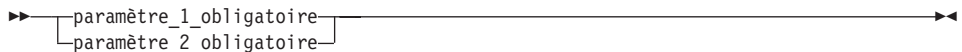


Mots clés obligatoires : Les mots clés et les variables obligatoires apparaissent sur la ligne du chemin principal.

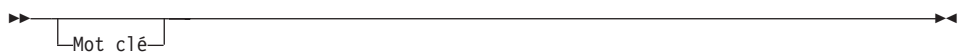


Vous devez codifier les mots clés et les valeurs obligatoires.

Choisissez un élément obligatoire dans une pile : Si vous devez effectuer votre choix parmi plusieurs mots clés ou variables obligatoires qui s'excluent, ceux-ci sont empilés verticalement dans l'ordre alphanumérique.



Valeurs facultatives : Les mots clés et les variables facultatifs apparaissent sous la ligne du chemin principal.



Vous pouvez choisir de ne pas codifier les mots clés et les variables facultatifs.

Choisissez un mot clé facultatif dans une pile : Si vous devez effectuer votre choix parmi plusieurs mots clés ou variables facultatifs qui s'excluent, ceux-ci sont empilés verticalement dans l'ordre alphanumérique sous la ligne du chemin principal.



Variables : Un mot apparaissant intégralement en italique correspond à une *variable*. Lorsque la syntaxe comporte une variable, celle-ci doit être remplacée par un nom ou une valeur admise, comme cela est défini dans le texte.

►►—*variable*—◄◄

Caractères non alphanumériques : Si un schéma indique un caractère non alphanumérique (par exemple, deux-point, des guillemets ou le signe moins), ce dernier doit être codifié dans le cadre de la syntaxe. Dans cet exemple, vous devez codifier *grappe:port*.

►►—*grappe:port*—◄◄

Annexe B. Guide des commandes Dispatcher, CBR et Mailbox Locator

La présente annexe décrit l'utilisation des commandes **ndcontrol** de Dispatcher. Elle traite également les commandes pour CBR et Mailbox Locator. CBR et Mailbox Locator utilisent un sous-ensemble de commandes Dispatcher. Pour de plus amples informations, reportez-vous à «Différences de configuration entre CBR, Mailbox Locator et Dispatcher» à la page 258.

Remarque : Lorsque vous utilisez ce diagramme de syntaxe —

- Pour CBR, substituez **ndcontrol** par **cbrcontrol**
- Pour Mailbox Locator, substituez **ndcontrol** par **mlcontrol**

Vous trouverez ci-dessous la liste des commandes décrites dans la présente annexe.

- «**ndcontrol advisor** — Contrôle du conseiller» à la page 260
- «**ndcontrol cluster** — Configuration des grappes» à la page 266
- «**ndcontrol executor** — Contrôle de l'exécuteur» à la page 271
- «**ndcontrol file** — gestion des fichiers de configuration» à la page 276
- «**ndcontrol help** — Affichage ou impression de l'aide sur cette commande» à la page 278
- «**ndcontrol highavailability** — Contrôle de la haute disponibilité» à la page 280
- «**ndcontrol host** — configuration d'une machine éloignée» à la page 285
- «**ndcontrol log** — Contrôle du fichier journal» à la page 286
- «**ndcontrol manager** — Contrôle du gestionnaire» à la page 287
- «**ndcontrol metric** — configuration des mesures du système» à la page 294
- «**ndcontrol port** — Configuration des ports» à la page 296
- «**ndcontrol rule** — configuration des règles» à la page 303
- «**ndcontrol server** — Configuration des serveurs» à la page 311
- «**ndcontrol set** — Configuration du journal du serveur» à la page 318
- «**ndcontrol status** — Affichage de l'exécution ou non du gestionnaire et des conseillers» à la page 319
- «**ndcontrol subagent** — Configuration du sous-agent SNMP» à la page 320

Vous pouvez entrer une version abrégée des paramètres de commandes **ndcontrol**. Il suffit d'entrer les lettres uniques des paramètres. Par exemple, pour obtenir l'aide correspondant à la commande `file save`, entrez **ndcontrol** **he f** à la place de **ndcontrol help file**.

Pour démarrer l'interface de ligne de commande, entrez **ndcontrol** pour ouvrir une invite `ndcontrol`.

Pour fermer l'interface de ligne de commande, entrez **exit** ou **quit**.

Remarque : Les valeurs des paramètres de commandes doivent être saisies à l'aide de caractères anglais. Les seules exceptions s'appliquent aux noms d'hôte (utilisés dans les commandes `cluster`, `server` et `highavailability`) et aux noms de fichiers (utilisés dans les commandes `file`).

Différences de configuration entre CBR, Mailbox Locator et Dispatcher

L'interface de ligne de commande de CBR et de Mailbox Locator est en grande partie un sous-ensemble de l'interface de ligne de commande de Dispatcher. Utilisez la commande **cbrcontrol** (pour le composant CBR) ou la commande **mlcontrol** (pour le composant Mailbox Locator) à la place de `ndcontrol` pour configurer le composant.

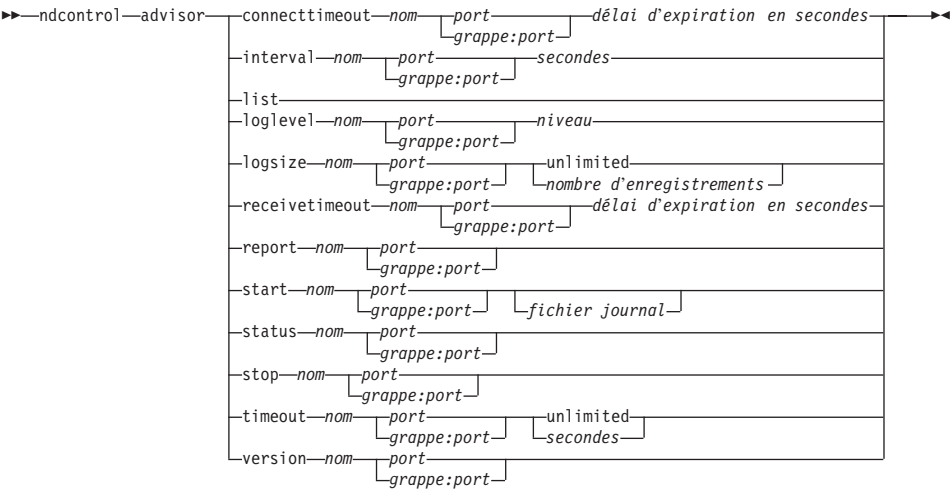
Certaines commandes *inutilisées* dans CBR figurent ci-dessous.

1. `highavailability`
2. `subagent`
3. `executor`
 - `report`
 - `set nfa <valeur>`
 - `set fincount <valeur>`
 - `set fintimeout <valeur>`
 - `set porttype <valeur>`
4. `cluster`
 - `report {c}`
 - `set {c} porttype`
5. `port add {c:p} porttype`
6. `port set {c:p} porttype`
7. `rule add {c:p:r} type port`
8. `server add {c:p:s} router`
9. `server set {c:p:s} router`

Certaines commandes *inutilisées* dans Mailbox Locator sont répertoriées ci-dessous.

1. highavailability
2. rule
3. subagent
4. executor
 - start
 - stop
 - report
 - set nfa <valeur>
 - set fincount <valeur>
 - set fintimeout <valeur>
 - set porttype <valeur>
5. cluster
 - report {c}
 - set {c} porttype
6. port [add | set] {c:p} porttype
7. server [add | set] {c:p:s} router

ndcontrol advisor — Contrôle du conseiller



connecttimeout

Permet de définir la période pendant laquelle un conseiller attend avant de signaler qu’une connexion à un serveur a échoué. Pour plus d’informations, reportez-vous à la section «Délai de connexion du conseiller et délai de réception pour les serveurs» à la page 148.

nom

Nom du conseiller. Les valeurs possibles sont **connect**, **db2**, **dns**, **ftp**, **http**, **ibmproxy (Caching Proxy)**, **imap**, **nnntp**, **ping**, **pop3**, **self**, **smtp**, **ssl**, **ssl2http**, **telnet**, et **wlm**.

Les noms des conseillers personnalisés sont au format **xxxx**, **ADV_xxxx** étant le nom de la classe mettant en oeuvre le conseiller personnalisé. Pour de plus amples informations, reportez-vous à «Création de conseillers personnalisés» à la page 151.

port

Numéro du port contrôlé par le conseiller.

grappe:port

La valeur de grappe (cluster) est facultative dans les commandes du conseiller, mais la valeur de port est requise. Si la valeur de grappe n’est pas indiquée, le conseiller s’exécutera sur le port de toutes les grappes. Si vous indiquez une grappe, le conseiller s’exécutera sur le port uniquement pour la grappe spécifiée. Pour de plus amples informations, reportez-vous à «Lancement et arrêt d’un conseiller» à la page 147.

La grappe correspond à l'adresse au format décimal à point ou au nom symbolique. Le port correspond au numéro du port que le conseiller surveille.

délai d'expiration en secondes

Il s'agit d'un entier positif représentant la période en secondes pendant laquelle le conseiller attend avant de signaler qu'une connexion à un serveur a échoué. La valeur par défaut est trois fois la valeur spécifiée pour l'intervalle du conseiller.

interval

Définit la fréquence à laquelle le conseiller demande des informations aux serveurs.

secondes

Il s'agit d'un entier positif qui représente le nombre de secondes entre les demandes envoyées aux serveurs pour connaître leurs états en cours. Valeur par défaut : 7.

list

Affiche la liste des conseillers qui fournissent des informations au gestionnaire.

loglevel

Définit le niveau de consignment relatif à un journal de conseiller.

niveau

Numéro du niveau (0 à 5). La valeur par défaut est 1. Plus le numéro est élevé, plus la quantité d'informations consignée dans le journal du conseiller est importante. Les valeurs possibles sont les suivantes : 0 (Aucun), 1 (Minimal), 2 (De base), 3 (Modéré), 4 (Avancé), 5 (Prolixe).

logsize

Définit la taille maximale d'un journal de conseiller. Lorsque vous affectez une taille maximale au fichier journal, celui-ci se boucle ; lorsque le fichier atteint la taille indiquée, les entrées suivantes sont écrites à partir du haut du fichier pour écraser les entrées de journal précédentes. La taille du journal ne peut pas être moins élevée que la taille actuelle du journal. Les entrées du journal sont horodatées, ce qui permet de déterminer l'ordre dans lequel elles ont été enregistrées. Plus le niveau de journalisation est élevé, plus la taille du journal doit être choisie attentivement car l'espace peut être saturé rapidement lors d'une consignment à des niveaux plus élevés.

nombre d'enregistrements

Taille maximale (en octets) du fichier journal du conseiller. Vous pouvez indiquer un nombre positif supérieur à zéro, ou le mot **unlimited**. Il se peut que le fichier journal n'atteigne pas la taille maximale exacte avant l'écrasement, car la taille des entrées de journal elles-mêmes varie. La valeur par défaut est 1 Mo.

receivetimeout

Permet de définir la période pendant laquelle un conseiller attend avant de signaler qu'une réception d'un envoi provenant d'un serveur a échoué. Pour plus d'informations, reportez-vous à la section «Délai de connexion du conseiller et délai de réception pour les serveurs» à la page 148.

délai d'expiration en secondes

Il s'agit d'un entier positif qui représente la période en secondes pendant laquelle le conseiller attend avant de signaler qu'une réception d'un envoi provenant d'un serveur a échoué. La valeur par défaut est trois fois la valeur spécifiée pour l'intervalle du conseiller.

report

Affiche un rapport sur l'état du conseiller.

start

Lance le conseiller. Il existe des conseillers pour chaque protocole. Les ports par défaut sont les suivants :

Nom du conseiller	Protocole	Port
connect	ICMP	12345
db2	privé	50000
dns	DNS	53
ftp	FTP	21
http	HTTP	80
ibmproxy	HTTP (via Caching Proxy)	80
imap	IMAP	143
nntp	NNTP	119
ping	PING	0
pop3	POP3	110
self	privé	12345
smtp	SMTP	25
ssl	HTTP	443
ssl2http	SSL	443
telnet	Telnet	23
WLM	privé	10,007

Remarque : Le conseiller FTP doit être activé uniquement pour le port de contrôle FTP (21). Ne lancez pas un conseiller FTP sur le port de données FTP (20).

fichier journal

Nom du fichier dans lequel les données de gestion sont consignées. Chaque enregistrement du journal est horodaté.

Le fichier par défaut se présente sous la forme *nomconseiller_port.log*, par exemple, **http_80.log**. Pour changer le répertoire dans lequel les fichiers journaux vont être stockés, reportez-vous à la section «Modification des chemins des fichiers journaux» à la page 216. Les fichiers journaux par défaut des conseillers spécifiques de grappes (ou de sites) sont créés avec l'adresse de la grappe, comme **http_127.40.50.1_80.log**.

status

Affiche l'état en cours de toutes les valeurs d'un conseiller qui peuvent être affectées globalement, ainsi que les valeurs par défaut associées.

stop

Arrête le conseiller.

timeout

Définit le nombre de secondes pour lequel le gestionnaire considère que les informations provenant du conseiller sont valides. Si le gestionnaire considère que les informations du conseiller sont antérieures à ce délai, il n'utilise pas ces informations pour déterminer les pondérations relatives aux serveurs sur le port contrôlé par le conseiller. Il est fait exception à ce délai lorsque le conseiller a informé le gestionnaire qu'un serveur spécifique est hors service. Le gestionnaire utilise ces informations relatives au serveur même après le dépassement du délai imparti aux informations du conseiller.

secondes

Nombre positif représentant le nombre de secondes, ou le mot **unlimited**. La valeur par défaut est unlimited.

version

Affiche la version en cours du conseiller.

Exemples

- Pour démarrer le conseiller http sur le port 80 pour la grappe 127.40.50.1, entrez :
`ndcontrol advisor start http 127.40.50.1:80`
- Pour démarrer le conseiller http sur le port 88 pour toutes les grappes, entrez :
`ndcontrol advisor start http 88`
- Pour arrêter le conseiller http sur le port 80 pour la grappe 127.40.50.1, entrez :
`ndcontrol advisor stop http 127.40.50.1:80`

- Pour définir la durée (30 secondes) pendant laquelle un conseiller HTTP du port 80 attend avant de signaler qu'une connexion à un serveur a échoué, entrez :
ndcontrol advisor connecttimeout http 80 30
- Pour définir la durée (20 secondes) pendant laquelle un conseiller HTTP du port 80 sur la grappe 127.40.50.1 attend avant de signaler qu'une connexion à un serveur a échoué, entrez :
ndcontrol advisor connecttimeout http 127.40.50.1:80 20
- Pour associer à l'intervalle du conseiller FTP (pour le port 21) la valeur de 6 secondes, entrez :
ndcontrol advisor interval ftp 21 6
- Pour afficher la liste des conseillers qui fournissent des informations au gestionnaire, entrez :
ndcontrol advisor list

Cette commande génère des résultats similaires à l'exemple suivant :

CONSEILLER	GRAPPE:PORT	DELAI
http	127.40.50.1:80	illimité
ftp	21	illimité

- Pour remplacer le niveau de consignation du journal du conseiller par 0, afin d'optimiser les performances, entrez :
ndcontrol advisor loglevel http 80 0
- Pour attribuer à la taille du journal du conseiller ftp pour le port 21 la valeur de 5000 octets, entrez :
ndcontrol advisor logsize ftp 21 5000
- Pour définir la durée (60 secondes) pendant laquelle un conseiller HTTP (pour le port 80) attend avant de signaler qu'une réception d'un envoi provenant d'un serveur a échoué, entrez :
ndcontrol advisor receivetimeout http 80 60
- Pour afficher un rapport sur l'état du conseiller ftp (pour le port 21), entrez :
ndcontrol advisor report ftp 21

Cette commande génère des résultats similaires à l'exemple suivant :

```
Rapport
du conseiller :
-----
Nom du conseiller ..... Ftp
Numéro du port ..... 21

Adresse de grappe ..... 9.67.131.18
Adresse du serveur ..... 9.67.129.230
```

```
Charge ..... 8
Adresse de grappe ..... 9.67.131.18
Adresse du serveur ..... 9.67.131.215
Charge ..... -1
```

- Pour afficher l'état actuel des valeurs associées au conseiller http pour le port 80, entrez :

```
ndcontrol advisor status http 80
```

Cette commande génère des résultats similaires à l'exemple suivant :

Etat du conseiller (advisor) :

```
-----
Intervalle (secondes)..... 7
Délai d'expiration (secondes) ..... Illimité
Délai d'expiration de connexion (secondes)... 21
Délai d'expiration de réception (secondes)... 21
Nom du fichier journal du conseiller ..... Http_80.log
Niveau de consignation ..... 1
Taille maximale du journal (octets) ..... Illimité
```

- Pour associer la valeur de 5 secondes au délai d'attente des informations du conseiller ftp sur le port 21, entrez :

```
ndcontrol advisor timeout ftp 21 5
```

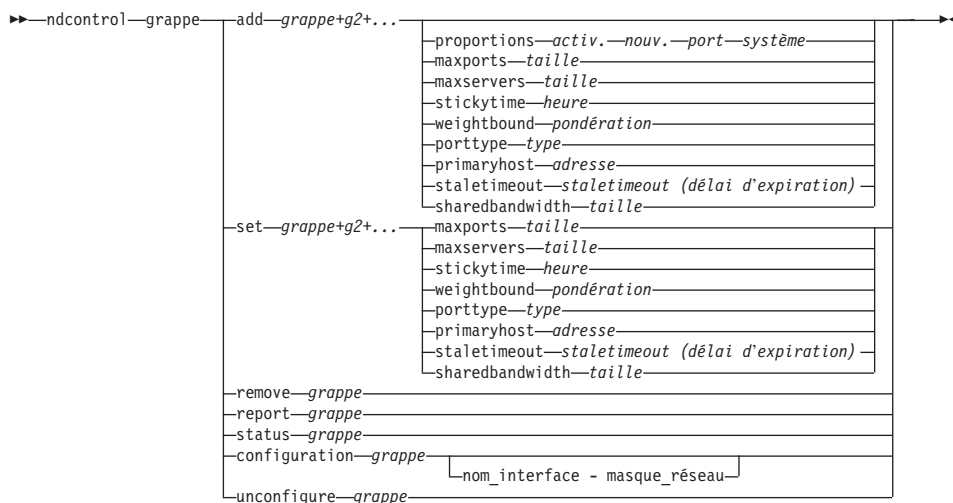
- Pour afficher le numéro de la version actuelle du conseiller ssl pour le port 443, entrez :

```
ndcontrol advisor version ssl 443
```

Cette commande génère des résultats similaires à l'exemple suivant :

```
Version : 04.00.00.00 - 07/12/2001-10:09:56-EDT
```

ndcontrol cluster — Configuration des grappes



add

Ajoute cette grappe. Vous devez définir au moins une grappe.

grappe

Adresse de la grappe sous forme de nom symbolique ou en notation décimale à point. Il est possible d'utiliser une adresse de grappe de valeur 0.0.0.0 pour spécifier une grappe générique. Pour de plus amples informations, reportez-vous à «Utilisation d'une grappe générique pour combiner les configurations serveurs» à la page 193.

Vous pouvez utiliser le signe deux-points (:) comme caractère générique sauf pour la commande `ndcontrol cluster add`. Par exemple, la commande `ndcontrol cluster set : weightbound 80` permet de définir une pondération de 80 pour toutes les grappes.

Remarque : Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

proportions

Au niveau de la grappe, définit le niveau d'importance (la proportion) des connexions actives (*actives*), des nouvelles connexions (*nouvelles*), des informations en provenance des conseillers (*port*) et des informations provenant d'un programme de contrôle système tel que Metric Server (*système*) utilisées par le gestionnaire pour définir les pondérations des serveurs. Chacune des valeurs décrites ci-après est exprimée en pourcentage de la valeur totale, et par conséquent, leur somme est toujours égale à 100. Pour plus d'informations, reportez-vous à la section «Proportion de l'importance accordée aux données d'état» à la page 141.

activ.

Nombre compris entre 0 et 100 représentant la proportion de pondération à affecter aux connexions actives. Valeur par défaut : 50.

nouv.

Nombre compris entre 0 et 100 représentant la proportion de pondération à affecter aux nouvelles connexions. Valeur par défaut : 50.

port

Nombre compris entre 0 et 100 représentant la proportion de pondération à affecter aux informations provenant des conseillers. Valeur par défaut : 0.

Remarque : Lorsqu'un conseiller est démarré et que la proportion du port est 0, Network Dispatcher définit automatiquement la valeur 1 pour que le gestionnaire puisse utiliser les informations du conseiller en tant qu'entrée pour calculer la pondération du serveur.

système

Nombre compris entre 0 et 100 représentant la proportion de pondération à affecter aux informations provenant d'une mesure système, par exemple, Metric Server. Valeur par défaut : 0.

maxports

Nombre maximal de ports. La valeur par défaut du paramètre maxports est 8.

taille

Nombre de ports autorisés

maxservers

Nombre maximal par défaut de serveurs par port. Ce paramètre peut être remplacé pour des ports spécifiques, à l'aide de la commande **port maxservers**. La valeur par défaut du paramètre maxservers est 32. La valeur par défaut de maxservers est 32.

taille

Nombre de serveurs autorisés par port

stickytime

Délai de maintien de routage par défaut pour les ports à créer. Ce paramètre peut être remplacé pour des ports individuels, à l'aide de la commande **port stickytime**. La valeur par défaut du délai de maintien de routage est 0. La valeur par défaut du délai de maintien de routage est 0.

Remarque : Avec la méthode d'acheminement CBR de Dispatcher, l'affinité SSL ID est activée pour tout port ajouté alors que le délai de maintien de routage des ports à créer est différent de

zéro. Pour la désactiver, vous devez associer de façon explicite un délai de maintien de routage de 0 au port.

heure

Valeur du paramètre stickytime en secondes.

weightbound

Limite de pondération par défaut du port. Ce paramètre peut être remplacé pour des ports individuels, à l'aide de la commande **port weightbound**. La valeur par défaut de la pondération est de 20.

pondération

Valeur de la limite de pondération.

porttype

Type de port par défaut. Ce paramètre peut être remplacé pour des ports individuels, à l'aide de la commande **port porttype**.

Remarque : Porttype s'applique à Dispatcher.

type

La valeurs possibles sont **tcp**, **udp** et **both**.

primaryhost

Adresse NFA des machines Dispatcher, principale et de secours. Dans une configuration de haute disponibilité réciproque , la grappe est associée soit à la machine principale, soit à celle de secours.

Si vous modifiez l'hôte principal d'une grappe alors que les machines principale et de secours sont lancés et exécutés en haute disponibilité réciproque, vous devrez contraindre le nouvel hôte primaire à prendre le relais. Vous devrez ensuite mettre à jour les scripts puis déconfigurer et reconfigurer la grappe correctement. Pour de plus amples informations, reportez-vous à «Haute disponibilité réciproque» à la page 51.

adresse

Valeur de l'adresse du primaryhost. Elle correspond par défaut à l'adresse NFA de cette machine.

staletimeout

Nombre de secondes d'inactivité possible sur une connexion avant que cette dernière soit supprimée. La valeur par défaut pour FTP est de 900 et celle pour Telnet de 32 000 000. La valeur par défaut pour tous les autres protocoles est 300. Ce paramètre peut être remplacé pour des ports individuels, à l'aide de la commande **port staletimeout**. Reportez-vous à «Utilisation de la valeur du délai d'attente» à la page 217, pour de plus amples informations.

Remarque : Pour Mailbox Locator, le paramètre staletimeout correspond au délai de déconnexion automatique après une période

d'inactivité de ces protocoles. Pour Mailbox Locator, ce paramètre a pour valeur par défaut 60 secondes, valeur supérieure aux délais d'inactivité de POP3 et IMAP. Pour plus d'informations sur le paramètre `staletimeout` pour Mailbox Locator, reportez-vous à la section «Remplacement du délai d'inactivité de POP3/IMAP» à la page 100.

délai d'expiration

Valeur du paramètre `staletimeout`.

sharedbandwidth

Quantité maximale de bande passante (en kilo-octets par seconde) pouvant être partagée au niveau de la grappe. Pour plus d'informations sur la bande passante partagée, reportez-vous aux sections «Utilisation de règles basées sur la largeur de bande réservée et sur la largeur de bande partagée» à la page 185 et «Règle de largeur de bande partagée» à la page 186.

Remarque : Le concept de bande passante partagée ne concerne pas CBR ni Mailbox Locator.

taille

La taille de la **bande passante partagée** correspond à un entier. La valeur par défaut est zéro. Si la valeur est zéro, la bande passante ne peut pas être partagée au niveau de la grappe.

set

Définit les caractéristiques de la grappe.

remove

Supprime cette grappe.

report

Affiche les zones internes de la grappe.

Remarque : Le paramètre `report` ne s'applique pas à CBR ni à Mailbox Locator.

status

Affiche l'état en cours d'une grappe spécifique.

configure

Configure l'alias d'une grappe pour la carte d'interface réseau.

Remarque : Le paramètre `configure` ne s'applique pas à CBR ni à Mailbox Locator.

nom_interface masque_réseau

Valeur obligatoire s'il s'agit d'un alias différent de celui que le répartiteur trouve en premier.

unconfigure

Supprime l'alias de la grappe de la carte d'interface réseau.

Remarque : Le paramètre `unconfigure` ne s'applique pas à CBR ni à Mailbox Locator.

Exemples

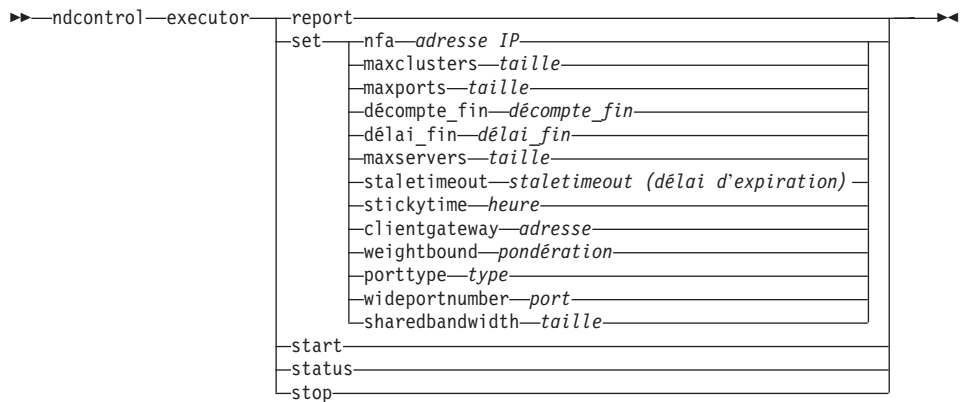
- Pour ajouter l'adresse de grappe 130.40.52.153, entrez :
`ndcontrol cluster add 130.40.52.153`
- Pour supprimer l'adresse de grappe 130.40.52.153, entrez :
`ndcontrol cluster remove 130.40.52.153`
- Pour définir l'importance relative associée aux données (actives, nouvelles, de port, système) reçues par les serveurs se trouvant sur la grappe 9.6.54.12, entrez :
`ndcontrol cluster set 9.6.54.12 proportions 60 35 5 0`
- Ajout d'une grappe générique
`ndcontrol cluster add 0.0.0.0`
- Dans le cas d'une configuration de haute disponibilité réciproque, placez le NFA de la machine de secours (9.65.70.19) en position d'hôte primaire dans l'adresse de grappe 9.6.54.12 :
`ndcontrol cluster set 9.6.54.12 primaryhost 9.65.70.19`
- Pour visualiser l'état de l'adresse de grappe 9.67.131.167, entrez :
`ndcontrol cluster status 9.67.131.167`

Cette commande génère des résultats similaires à l'exemple suivant :

Etat de la grappe (cluster) :

```
-----
Adresse ..... 9.67.131.167
Nombre de ports cibles ..... 3
Délai de maintien de routage par défaut ..... 0
Délai d'expiration par défaut ..... 30
Limite de pondération par défaut du port ..... 20
Nombre maximal de ports ..... 8
Protocole du port par défaut ..... tcp/udp
Nombre maximal de serveurs par défaut ..... 32
Proportion accordée aux connexions actives ..... 0.5
Proportion accordée aux nouvelles connexions ..... 0.5
Proportion accordée aux connexions spécifiques du port 0
Proportion accordée aux mesures du système ..... 0
Largeur de bande partagée (Ko) ..... 0
Adresse de l'hôte primaire ..... 9.67.131.167
```

ndcontrol executor — Contrôle de l'exécuteur



report

Affiche un rapport d'analyse sur les statistiques. Exemple : nombre total de paquets, paquets annulés, paquets transmis avec des erreurs, etc.

Remarque : Le paramètre `report` ne s'applique pas à CBR ni à Mailbox Locator.

set

Définit les zones de l'exécuteur.

nfa

Définit l'adresse de non-réacheminement. Tout paquet envoyé à cette adresse n'est pas réacheminé par la machine Dispatcher.

Remarque : NFA ne s'applique pas à CBR ni à Mailbox Locator.

Adresse IP

Adresse IP (Internet Protocol) sous forme de nom symbolique ou en notation décimale à points.

maxclusters

Nombre maximal de grappes pouvant être configurées. La valeur par défaut du paramètre `maxclusters` est 100.

taille

Nombre maximal de grappes pouvant être configurées.

maxports

Valeur par défaut du nombre maximum de ports pour les grappes à créer. Ce paramètre peut être remplacé à l'aide des commandes **cluster set** ou **cluster add**. La valeur par défaut du paramètre `maxports` est 8.

taille

Nombre de ports.

fincount

Nombre de connexions devant être à l'état FIN avant que la collecte des données obsolètes commence. La valeur par défaut de fincount est 4000.

fincount

Valeur du paramètre fincount.

Remarque : Le paramètre fincount ne s'applique pas à CBR ni à Mailbox Locator.

fintimeout

Nombre de secondes durant lequel une connexion doit être gardée en mémoire avant que cette dernière ne soit mise à l'état FIN. La valeur par défaut du paramètre fintimeout est 60.

délai_fin

Valeur du paramètre fintimeout.

Remarque : Le paramètre fintimeout ne s'applique pas à CBR ni à Mailbox Locator.

maxservers

Nombre maximal par défaut de serveurs par port. Ce paramètre peut être remplacé à l'aide de la commande **cluster** ou **port**. La valeur par défaut de maxservers est 32.

taille

Nombre de serveurs

staletimeout

Nombre de secondes d'inactivité possible sur une connexion avant que cette dernière soit supprimée. La valeur par défaut pour FTP est de 900 et celle pour Telnet de 32 000 000. La valeur par défaut pour tous les autres ports est 300. Ce paramètre peut être remplacé à l'aide de la commande **cluster** ou **port**. Reportez-vous à «Utilisation de la valeur du délai d'attente» à la page 217, pour de plus amples informations.

Remarque : Pour Mailbox Locator, le paramètre staletimeout correspond au délai de déconnexion automatique après une période d'inactivité de ces protocoles. La valeur par défaut de staletimeout, pour Mailbox Locator, est de 60 secondes ; elle est supérieure aux délais d'inactivité de POP3 et IMAP. Pour plus d'informations sur le paramètre staletimeout pour Mailbox Locator, reportez-vous à la section «Remplacement du délai d'inactivité de POP3/IMAP» à la page 100.

délai d'expiration

Valeur du paramètre `staletimeout`.

stickytime

Valeur du délai de maintien de routage par défaut de toutes les futures grappes. Elle peut être remplacée par la commande **cluster** ou **port**. La valeur par défaut du paramètre `stickytime` est 0.

heure

Valeur du paramètre `stickytime` en secondes.

clientgateway

Clientgateway est une adresse IP utilisée pour NAT/NAPT ou Fonction CBR de Dispatcher. Il s'agit de l'adresse du routeur par lequel le trafic de retour est transmis de Network Dispatcher vers les clients. Clientgateway doit être associé à une valeur non nulle avant l'ajout d'un port à une méthode d'acheminement NAT/NAPT ou Fonction CBR de Dispatcher. Reportez-vous aux sections «Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)» à la page 52 et «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54 pour plus d'informations.

Remarque : Clientgateway ne s'applique qu'au composant Dispatcher.

adresse

Adresse de la passerelle client sous forme de nom symbolique ou en notation décimale à points. La valeur par défaut est 0.0.0.0.

weightbound

Valeur de la limite de pondération par défaut de tous les futurs ports. Ce paramètre peut être remplacé à l'aide des commandes **cluster** ou **port**. La valeur par défaut du paramètre `weightbound` est 20.

pondération

Valeur du paramètre pondération (`weightbound`).

porttype

Valeur du type de port par défaut pour tous les futurs ports. Ce paramètre peut être remplacé à l'aide des commandes **cluster** ou **port**.

Remarque : Le paramètre Porttype ne s'applique pas à CBR ni à Mailbox Locator.

type

La valeurs possibles sont **tcp**, **udp** et **both**.

wideportnumber

Port TCP inutilisé pour chaque machine Dispatcher. Le paramètre *wideportnumber* doit être le même pour toutes les machines Dispatcher.

La valeur par défaut du paramètre `wideportnumber` est 0, ce qui indique que la prise en charge du réseau étendu n'est pas utilisée.

Remarque : Le paramètre `Wideportnumber` ne s'applique pas à CBR ni à Mailbox Locator.

port

Valeur de **`wideportnumber`**.

sharedbandwidth

Quantité maximale de bande passante (en kilo-octets par seconde) pouvant être partagée au niveau de l'exécuteur. Pour plus d'informations sur la bande passante partagée, reportez-vous aux sections «Utilisation de règles basées sur la largeur de bande réservée et sur la largeur de bande partagée» à la page 185 et «Règle de largeur de bande partagée» à la page 186.

Remarque : Le concept de bande passante partagée ne concerne pas CBR ni Mailbox Locator.

taille

La taille de la **bande passante partagée** correspond à un entier. La valeur par défaut est zéro. Si la valeur est zéro, la bande passante ne peut pas être partagée au niveau de l'exécuteur.

start

Lance l'exécuteur.

Remarque : `Start` ne s'applique pas à Mailbox Locator.

status

Affiche l'état actuel des valeurs de l'exécuteur pouvant être définies ainsi que les valeurs par défaut.

stop

Arrête l'exécuteur. Pour Dispatcher, `stop` n'est *pas* un paramètre valide sous Windows 2000.

Remarque : `Stop` s'applique à Dispatcher et à CBR.

Exemples

- Pour afficher les compteurs internes de Dispatcher entrez :
`ndcontrol executor status`

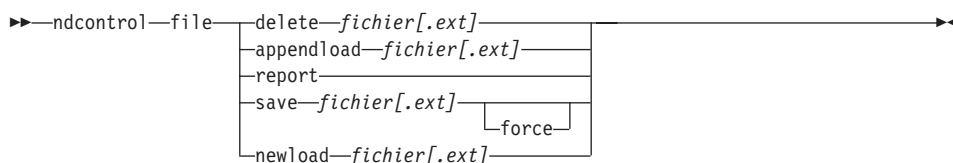
Etat de l'exécuteur :

Adresse de non-réacheminement	9.67.131.151
Adresse de la passerelle client	0.0.0.0
Décompte FIN	4,000
Délai de maintien de l'état FIN	60

Numéro de port du réseau étendu 2,001
 Largeur de bande partagée (Ko) 0
 Nombre maximal de ports par défaut par grappe . 8
 Nombre maximal de grappes 100
 Nombre maximal de serveurs par défaut par port 32
 Délai d'attente du port 300
 Délai de maintien de routage par défaut du port 0
 Limite de pondération par défaut du port 20
 Nombre maximal de grappes 100

- Pour affecter à l'adresse de non réacheminement la valeur 130.40.52.167, entrez :
`ndcontrol executor set nfa 130.40.52.167`
- Pour définir le nombre maximal de grappes, entrez :
`ndcontrol executor set maxclusters 4096`
- Pour lancer l'exécuteur, entrez :
`ndcontrol executor start`
- Pour arrêter l'exécuteur (**AIX, Linux et Solaris uniquement**), entrez :
`ndcontrol executor stop`

ndcontrol file — gestion des fichiers de configuration



delete

Supprime le fichier.

fichier[.ext]

Un fichier de configuration se compose de commandes ndcontrol.

Vous pouvez indiquer n'importe quelle extension de fichier (*.ext*) ou n'en indiquer aucune.

appendload

Pour mettre à jour la configuration actuelle, la commande appendload lance les commandes exécutables de votre fichier script.

report

Génère un rapport sur les fichiers disponibles.

save

Permet de sauvegarder la configuration actuelle de Network Dispatcher dans le fichier.

Remarque : Les fichiers sont sauvegardés dans des répertoires et chargés à partir de répertoires, où *composant* correspond à dispatcher, cbr ou ml (Mailbox Locator) :

- AIX : **/usr/lpp/nd/servers/configurations/composant**
- Linux : **/opt/nd/servers/configurations/composant**
- Solaris : **/opt/nd/servers/configurations/composant**
- Windows 2000 :

Chemin d'accès courant au répertoire d'installation —
c:\Program

Files\ibm\edge\nd\servers\configurations\composant

Chemin d'accès au répertoire d'installation natif —
c:\Program

Files\ibm\nd\servers\configurations\composant

force

Si vous voulez sauvegarder votre fichier dans un fichier existant du même nom, utilisez **force** pour supprimer le fichier existant avant de sauvegarder le nouveau fichier. Si vous n'utilisez pas l'option **force**, le fichier existant n'est pas remplacé.

newload

Permet de charger et d'exécuter un nouveau fichier de configuration dans Network Dispatcher. Le nouveau fichier de configuration remplace la configuration actuelle.

Exemples

- Pour supprimer un fichier :
`ndcontrol file delete fichier3`

Le fichier (fichier3) est supprimé.
- Chargement d'un nouveau fichier de configuration pour remplacer la configuration actuelle :
`ndcontrol file newload file1.sv`

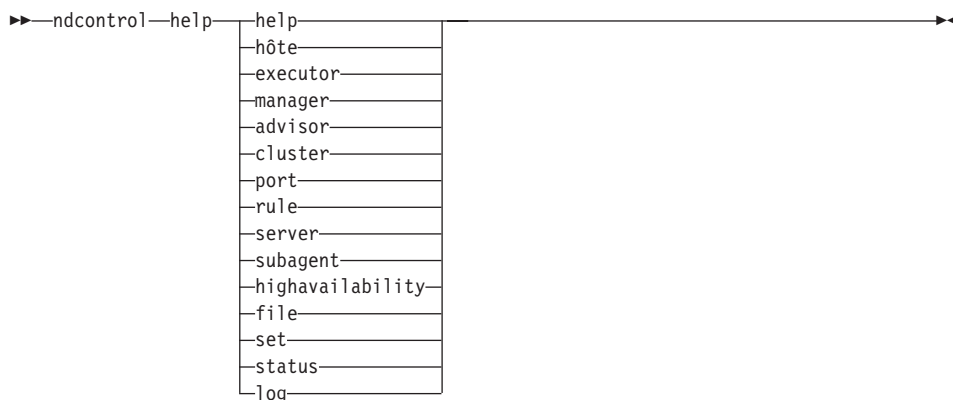
Le fichier (file1.sv) a été chargé dans le Dispatcher.
- Chargement et adjonction d'un fichier de configuration à la configuration actuelle :
`ndcontrol file appendload file2.sv`

Le fichier (file2.sv) a été chargé et ajouté à la configuration actuelle.
- Pour visualiser un rapport de vos fichiers (à savoir les fichiers que vous avez sauvegardés précédemment) :
`ndcontrol file report`

RAPPORT SUR LES FICHIERS :
fichier1.sauv
fichier2.sv
fichier3
- Pour sauvegarder votre configuration dans un fichier intitulé fichier3 :
`ndcontrol file save fichier3`

La configuration est sauvegardée dans fichier3.

ndcontrol help — Affichage ou impression de l'aide sur cette commande



Exemples

- Pour obtenir de l'aide sur la commande ndcontrol, entrez :
ndcontrol help

Cette commande génère des résultats similaires à l'exemple suivant :

ARGUMENTS DE LA COMMANDE HELP :

Syntaxe : help <option>

Exemple : help cluster

help	- Affichage des informations d'aide
advisor	- Aide sur la commande advisor
cluster	- Aide sur la commande cluster
port	- Aide sur la commande port
executor	- Aide sur la commande executor
file	- Aide sur la commande file
host	- Aide sur la commande host
log	- Aide sur la commande log
manager	- Aide sur la commande manager
metric	- Aide sur la commande metric
rule	- Aide sur la commande rule
server	- Aide sur la commande server
subagent	- Aide sur la commande subagent
set	- Aide sur la commande set
status	- Aide sur la commande status
highavailability	- Aide sur la commande highavailability

Il est à noter que les paramètres placés entre les signes <> sont des variables.

- L'aide affiche parfois des choix de variables en utilisant un | pour séparer les options disponibles :

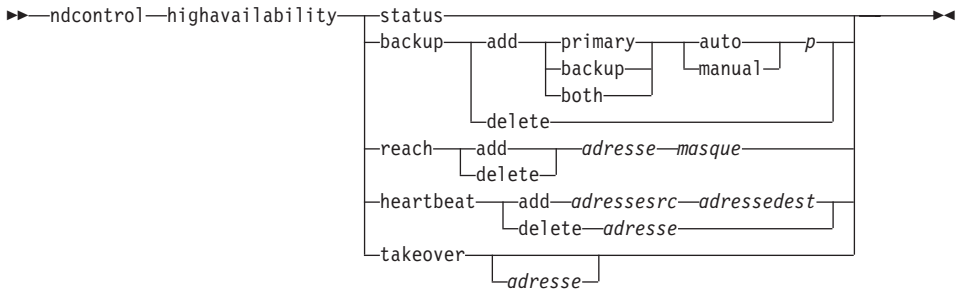
```
fintimeout <adresse de grappe>|all <heure>
```

```
-Change FIN timeout
```

```
(Utilisez "all" pour modifier toutes les grappes)
```

ndcontrol highavailability — Contrôle de la haute disponibilité

Remarque : Le schéma de syntaxe de haute-disponibilité ndcontrol ne s'applique pas à CBR ni à Mailbox Locator.



status

Renvoie un rapport sur la haute disponibilité. Les machines sont identifiées comme étant à l'un des trois états suivants :

Active Le réacheminement de paquets par un poste déterminé (principal, de sauvegarde, ou les deux) est en cours.

Standby

Le réacheminement de paquets par un poste déterminé (principal, de sauvegarde, ou les deux) n'est pas en cours ; celui-ci contrôle l'état d'un Dispatcher **actif**.

Inactive

Le réacheminement de paquets par un poste déterminé est en cours, et celui-ci ne tente pas d'établir une connexion avec son Dispatcher partenaire.

En outre, le mot clé **status** renvoie des informations relatives à divers sous-états:

Synchronisé

Un poste déterminé a établi une connexion avec un autre Dispatcher.

Autres sous-états

Ce poste essaie d'établir une connexion avec son Dispatcher partenaire, mais cette tentative n'a pas encore abouti.

machine de secours (backup)

Permet de sauvegarder des informations relatives au poste principal (primary) ou de sauvegarde (backup).

add

Permet de définir et d'exécuter les fonctions de haute-disponibilité relatives à ce poste.

machine principale (primary)

Identifie le répartiteur qui sert de poste *principal*.

machine de secours (backup)

Identifie la machine Dispatcher qui sert de poste de *sauvegarde*.

both

Identifie la machine Dispatcher qui joue le *double* rôle de poste principal et de sauvegarde. Il s'agit d'une fonction de la haute responsabilité réciproque qui associe, sur la base des grappes, les rôles de poste principale et de sauvegarde. Reportez-vous à la section «Haute disponibilité réciproque» à la page 51, pour de plus amples informations.

auto

Spécifie une stratégie de rétablissement *automatique* permettant au poste principal (primary) de reprendre l'acheminement des paquets dès qu'il est remis en service.

manual

Spécifie une stratégie de rétablissement *manuelle* qui ne permet au poste principal (primary) de reprendre le réacheminement des paquets que lorsque l'administrateur a émis une commande **takeover**.

p[port]

Port TCP non utilisé sur les deux postes, à utiliser par Dispatcher pour ses messages de cadence. Le *port* doit être identique pour le poste principal et pour le poste de sauvegarde.

delete

Supprime ce poste de la liste des postes à haute disponibilité, de sorte qu'il ne puisse plus servir de poste de sauvegarde (backup) ou principal (primary).

conseiller de contact (reach)

Ajoute ou supprime une adresse cible pour les répartiteurs principal et de sauvegarde. Le conseiller d'accessibilité envoie des *pings* à partir des deux répartiteurs pour déterminer le niveau d'accessibilité de leurs cibles.

Remarque : Lorsque vous configurez la cible d'accessibilité, vous devez également démarrer le conseiller reach. Il est démarré automatiquement par la fonction de gestionnaire.

add

Ajoute une adresse cible pour le conseiller d'accessibilité.

delete

Supprime une adresse cible du conseiller d'accessibilité.

adresse

Adresse IP (au format symbolique ou en notation décimale à points) du noeud cible.

masque

Masque de sous-réseau.

signal de présence (heartbeat)

Définit la session de communication entre les postes Dispatcher principal et de sauvegarde.

add

Indique au Dispatcher source l'adresse de son partenaire (adresse de destination).

addresesrc

Adresse source. Adresse (IP ou symbolique) de ce poste Dispatcher.

addressedest

Adresse de destination. Adresse (IP ou symbolique) de l'autre poste Dispatcher.

Remarque : srcaddress et dstaddress doivent correspondre aux NFA des machines pour au moins une paire de signaux de présence.

delete

Supprime la paire d'adresses des informations de cadence (heartbeat). Vous pouvez indiquer l'adresse de destination ou l'adresse source de la paire de signaux de présence.

adresse

Adresse (IP ou symbolique) de la destination ou de la source.

takeover

Configuration de haute disponibilité simple (Les machines Dispatcher occupent la fonction, soit de *postepincipale* soit de *sauvegarde*) :

- Demande à un Dispatcher en attente de passer à l'état actif et de commencer le routage des paquets, ce qui permet de forcer le Dispatcher actif à passer en attente. Cette commande doit être émise sur le poste en attente et ne fonctionne que dans le cas d'une stratégie **manuelle**. Le sous-état doit être *synchronisé*.

Configuration de haute disponibilité réciproque (le rôle de chaque machine Dispatcher est *double*) :

- La machine Dispatcher caractérisée par la fonction haute disponibilité réciproque contient deux grappes qui correspondent à celles de son partenaire. L'une des deux grappes joue le rôle de grappe principale (grappe de sauvegarde du partenaire), et l'autre de grappe de sauvegarde (grappe principale du partenaire). La commande takeover donne l'ordre à la machine Dispatcher de commencer le routage des

paquets en direction de la (des) grappe(s) de l'autre machine. Cette commande ne peut être émise que lorsque la (les) grappe (s) de la machine Dispatcher est (sont) en mode *d'attente* et que le sous-état est *synchronisé*. Ceci va contraindre la (les) grappe(s) active(s) du partenaire à passer en mode d'attente. La commande ne fonctionne que dans le cadre d'une stratégie **manuelle**. Reportez-vous à la section «Haute disponibilité réciproque» à la page 51, pour de plus amples informations.

Remarques :

1. Il est à noter que les rôles des deux postes (*principal* et *de sauvegarde*) ne changent pas. Seul leur *état* relatif (*actif* ou *en attente*) est modifié.
2. Il existe trois *scripts* possibles pour le passage à l'état actif : *goActive*, *goStandby* et *goInOp*. Reportez-vous à la section «Utilisation de scripts» à la page 178.

adresse

La valeur de l'adresse de relais est facultative. Elle ne doit être utilisée que lorsque la machine joue le *double* rôle de poste principal et de sauvegarde (configuration de haute disponibilité réciproque). L'adresse indiquée correspond au NFA de la machine Dispatcher chargée habituellement du trafic de cette grappe. Dans le cas où les deux grappes sont relayées, indiquez la propre adresse NFA du Dispatcher.

Exemples

- Pour vérifier l'état de la fonction de haute disponibilité d'une machine :
ndcontrol highavailability status

Résultat :

```
Etat de la haute disponibilité :
-----
Rôle .....principal
Stratégie de récupération .. manuelle
Etat ..... Actif
Sous-état..... Synchronisé
Hôte primaire..... 9.67.131.151
Port .....12,345
Cible privilégiée..... 9.67.134.223
```

Etat du signal de présence :

```
-----
Nombre ..... 1
```

Etat de l'accessibilité :

```
-----
Nombre ..... 1
```

- Pour ajouter les informations de sauvegarde à la machine principale via la stratégie de récupération automatique et le port 80 :
ndcontrol highavailability backup add primary auto 80

- Pour ajouter une adresse à laquelle le répartiteur doit pouvoir accéder :
`ndcontrol highavailability reach add 9.67.125.18`
- Pour ajouter aux machines principale et de secours des informations sur le signal de présence :
Machine principale (primary) -
`highavailability heartbeat add 9.67.111.3 9.67.186.8`
machine de secours (backup) - `highavailability heartbeat add 9.67.186.8 9.67.111.3`
- Pour indiquer au répartiteur en attente de devenir actif et obliger de la sorte la machine active à passer en attente :
`ndcontrol highavailability takeover`

ndcontrol host — configuration d'une machine éloignée

►►—ndcontrol—host:—*remote_host*—◄◄

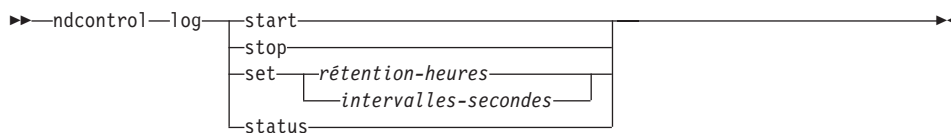
remote_host

Nom de la machine Network Dispatcher configurée à distance Lorsque vous tapez cette commande, assurez-vous qu'il ne reste pas d'espace entre **host:** et *remote_host*, par exemple :

```
ndcontrol host:remote_host
```

Après avoir tapé cette commande dans l'indicatif DOS, entrez toute commande ndcontrol valide que vous désirez envoyer à la machine Network Dispatcher éloignée.

ndcontrol log — Contrôle du fichier journal



start

Démarre la journalisation

stop

Arrête la journalisation

set

Définit les zones de journalisation. Pour plus d'informations sur la définition des zones pour la journalisation binaire, reportez-vous à la section «Utilisation de la journalisation binaire pour analyser les statistiques des serveurs» à la page 205.

retention

Nombre d'heures pendant lesquelles les fichiers journaux vont être conservés. La valeur de rétention par défaut est 24.

heures

Nombre d'heures.

intervalles

Nombre de secondes qui s'écoulent entre deux entrées de journal. La valeur par défaut est 60.

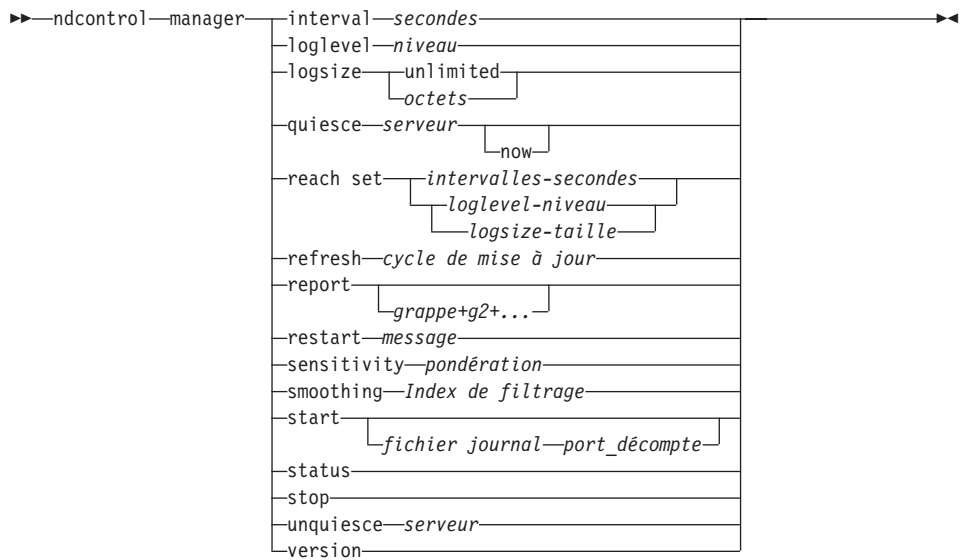
secondes

Nombre de secondes.

status

Affiche la rétention et les intervalles du journal.

ndcontrol manager — Contrôle du gestionnaire



interval

Définit la fréquence de mise à jour, par le gestionnaire, des pondérations des serveurs pour l'exécuteur, grâce à la mise à jour des critères utilisés par l'exécuteur pour acheminer les requêtes client.

secondes

Nombre positif représentant la fréquence (en secondes) de mise à jour, par le gestionnaire, des pondérations pour l'exécuteur. Valeur par défaut : 2

loglevel

Permet de définir le niveau de consignation pour le journal du gestionnaire et le journal du contrôleur de mesures.

niveau

Numéro du niveau (0 à 5). Plus le numéro est élevé, plus la quantité des informations consignées dans le journal du gestionnaire est importante. Valeur par défaut : 1. Les valeurs possibles sont les suivantes : 0 (Aucun), 1 (Minimal), 2 (De base), 3 (Modéré), 4 (Avancé), 5 (Prolixe).

logsize

Définit la taille maximale du journal du gestionnaire. Lorsque vous affectez une taille maximale au fichier journal, celui-ci se boucle ; lorsque le fichier atteint la taille indiquée, les entrées suivantes sont écrites à partir du haut du fichier pour écraser les entrées de journal précédentes. La taille du journal ne peut pas être moins élevée que la taille actuelle du journal. Les entrées de journal sont horodatées de sorte que vous pouvez

identifier l'ordre dans lequel elles sont consignées. Plus le niveau de journalisation est élevé, plus la taille du journal doit être choisie attentivement car l'espace peut être saturé rapidement lors d'une consignation à des niveaux plus élevés.

octets

Taille maximale (en octets) du fichier journal du gestionnaire. Vous pouvez indiquer un nombre positif supérieur à zéro, ou le mot **unlimited**. Il se peut que le fichier journal n'atteigne pas la taille maximale exacte avant l'écrasement, car la taille des entrées de journal elles-mêmes varie. La valeur par défaut est 1 Mo.

mettre au repos (quiesce)

N'indiquez plus de connexions à envoyer à un serveur sauf les nouvelles connexions ultérieures du client vers le serveur mis au repos si la connexion est associée à un délai de maintien de routage et que ce dernier n'est pas arrivé à expiration. Le gestionnaire affecte la valeur 0 à la pondération de ce serveur, pour chaque port pour lequel celui-ci est défini. Utilisez cette commande si vous voulez effectuer une intervention de maintenance rapide sur un serveur puis le réactiver. Si vous supprimez de la configuration un serveur mis au repos, puis que vous l'ajoutez de nouveau, son état ne sera plus celui dans lequel il se trouvait avant d'être mis au repos. Pour plus d'informations, voir «Mise au repos de la gestion des connexions avec maintien de routage» à la page 199.

serveur

Adresse IP du serveur sous forme de nom symbolique ou en notation décimale à points.

Ou, si vous utilisez le partitionnement du serveur, entrez le nom unique du serveur logique. Pour de plus amples informations, reportez-vous à «Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)» à la page 159.

now

N'utilisez l'option Mettre au repos "maintenant" que si le délai de maintien de routage est défini et que vous voulez que les nouvelles connexions soient envoyées à un autre serveur (différent du serveur mis au repos) avant que le délai de maintien de routage n'expire. Pour plus d'informations, voir «Mise au repos de la gestion des connexions avec maintien de routage» à la page 199.

reach set

Définit l'intervalle, le niveau de consignation et la taille du journal pour le conseiller d'accessibilité.

refresh

Définit le nombre d'intervalles avant qu'il soit demandé à l'exécuteur de mettre à jour les informations relatives aux nouvelles connexions et aux connexions actives.

cycle de mise à jour

Nombre positif représentant le nombre d'intervalles. Valeur par défaut : 2

report

Affiche un rapport d'analyse sur les statistiques.

grappe

Adresse de la grappe que vous souhaitez afficher dans le rapport.

L'adresse peut prendre la forme d'un nom symbolique ou d'une notation décimale. L'affichage par défaut est un rapport de gestionnaire portant sur toutes sur les grappes.

Remarque : Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

restart

Relance tous les serveurs (qui ne sont pas arrêtés) en leur affectant des valeurs de pondération normalisées (la moitié de la pondération maximale).

message

Message à consigner dans le fichier journal du gestionnaire.

sensitivity

Définit la sensibilité minimale à partir de laquelle les pondérations sont mises à jour. Cette valeur définit le moment où le gestionnaire doit modifier sa pondération pour le serveur en fonction des informations externes.

pondération

Nombre compris entre 1 et 100 à utiliser comme pourcentage de pondération. La valeur par défaut de 5 crée une sensibilité minimale de 5%.

smoothing

Définit un index pour lisser les variations des pondérations lors de l'équilibrage de charge. Plus l'index de filtrage est élevé, moins les pondérations des serveurs varient lorsque les conditions réseau sont modifiées. Plus cet index est faible, plus les pondérations des serveurs varient.

index

Nombre positif en virgule flottante. Valeur par défaut : 1,5.

start

Lance le gestionnaire.

fichier journal

Nom du fichier dans lequel les données de gestion sont consignées. Chaque enregistrement du journal est horodaté.

Le fichier par défaut est installé dans le répertoire **logs**. Reportez-vous à la section «Annexe F. Exemples de fichiers de configuration» à la page 387. Pour changer le répertoire dans lequel les fichiers journaux vont être stockés, reportez-vous à la section «Modification des chemins des fichiers journaux» à la page 216.

port_décompte

Port utilisé par Metric Server pour signaler les charges du système. Si vous indiquez un port de décompte, vous devez spécifier un nom de fichier journal. Le port de décompte par défaut est 10004.

status

Affiche l'état en cours de toutes les valeurs du gestionnaire qui peuvent être affectées globalement, ainsi que les valeurs par défaut associées.

stop

Arrête le gestionnaire.

unquiesce

Indique que le gestionnaire peut commencer à attribuer une pondération supérieure à 0 à un serveur préalablement mis au repos, sur chaque port pour lequel il est défini.

serveur

Adresse IP du serveur sous forme de nom symbolique ou en notation décimale à points.

version

Affiche la version en cours du gestionnaire.

Exemples

- Pour affecter la valeur de 5 secondes au délai séparant les mises à jour du gestionnaire, entrez :
`ndcontrol manager interval 5`
- Pour affecter au niveau de journalisation la valeur de 0, afin d'optimiser les performances, entrez :
`ndcontrol manager loglevel 0`
- Pour affecter à la taille de journal du gestionnaire la valeur de 1 000 000 octets, entrez :
`ndcontrol manager logsize 1000000`
- Pour indiquer qu'aucune autre connexion ne doit être envoyée au serveur à l'adresse 130.40.52.153, entrez :
`ndcontrol manager quiesce 130.40.52.153`

- Pour affecter la valeur 3 au nombre d'intervalles avant la mise à jour des pondérations, entrez :
ndcontrol manager refresh 3
- Pour obtenir une analyse statistique du gestionnaire, entrez :
ndcontrol manager report

Cette commande génère des résultats similaires à l'exemple suivant :

TABLE DES HOTES	ETAT
9.67.129.221	ACTIF
9.67.129.213	ACTIF
9.67.134.223	ACTIF

9.67.131.18	POND	ACTIV. % 48	NOUV. % 48	PORT % 4	SYSTEM % 0						
PORT: 80	ACT.	NV.	PND	CONNEXION	PDS	CONNEXION	PND	CHARGE	PND	CHARGE	
9.67.129.221	8	8	10	0	10	0	7	29	0	0	
9.67.134.223	11	11	10	0	10	0	12	17	0	0	
TOTAUX :	19	19		0		0		46		0	

9.67.131.18	POND	ACTIV. % 48	NOUV. % 48	PORT % 4	SYSTEM % 0						
PORT: 23	ACT	NV	PND	CONNEXION	PDS	CONNEXION	PND	CHARGE	PND	CHARGE	
9.67.129.213	10	10	10	0	10	0	10	71	0	0	
9.67.134.223	0	0	10	0	10	0	-9999	-1	0	0	
TOTAUX :	10	10		0		0		70		0	

CONSEILLER	PORT	DELA
reach	0	illimité
http	80	illimité
ftp	21	illimité

- Pour relancer tous les serveurs en leur affectant des pondérations normalisées et pour consigner un message dans le fichier journal du gestionnaire, entrez :
ndcontrol
manager restart Relance du gestionnaire pour mettre à jour le code

Cette commande génère des résultats similaires à l'exemple suivant :

320-14:04:54

Relance du gestionnaire pour mettre à jour le code

- Pour affecter la valeur 10 à la sensibilité aux modifications de pondération, entrez :

ndcontrol manager sensitivity 10

- Pour affecter la valeur 2 à l'index de lissage, entrez :

ndcontrol manager smoothing 2.0

- Pour lancer le gestionnaire et indiquer le fichier journal nommé ndmgr.log (les chemins ne peuvent pas être définis), entrez :

ndcontrol manager start ndmgr.log

- Pour afficher l'état en cours des valeurs associées au gestionnaire, entrez :

ndcontrol manager status

Cette commande génère des résultats similaires à l'exemple suivant :

Etat du

gestionnaire (manager) :

=====

Port du processus de décompte..... 10,004

Nom de fichier journal du gestionnaire..... manager.log

Niveau de consignation du gestionnaire..... 1

Taille maxi du journal du gestionnaire (octets).... unlimited

Niveau de sensibilité..... 0.05

Indice de lissage..... 1.5

Intervalle de mise à jour (secondes)..... 2

Cycle des mises à jour des pondérations 2

Niveau de journal à atteindre..... 1

Taille maximale du journal des contacts octets).... unlimited

Intervalle de mise à jour des contacts (secondes).. 7

- Pour arrêter le gestionnaire, entrez :

ndcontrol manager stop

- Pour indiquer qu'aucune autre nouvelle connexion ne doit être envoyée à un serveur à l'adresse 130.40.52.153, entrez (Remarque : Ne mettez le serveur au repos "maintenant" que si le délai de maintien de routage est défini et que vous voulez que les nouvelles connexions soient envoyées à un autre serveur avant expiration du délai de maintien de routage.):

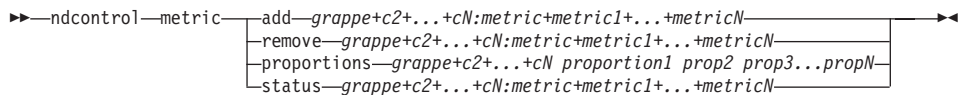
ndcontrol manager quiesce 130.40.52.153 now

- Pour indiquer qu'aucune autre nouvelle connexion ne doit être envoyée à un serveur à l'adresse 130.40.52.153, entrez (Remarque : si le délai de maintien de routage est défini, les nouvelles connexions qui auront lieu par la suite à partir du client seront envoyées à ce serveur jusqu'à expiration du délai de maintien de routage.):

ndcontrol manager quiesce 130.40.52.153

- Pour indiquer que le gestionnaire peut commencer à attribuer une pondération supérieure à 0 à un serveur à l'adresse 130.40.52.153 qui a préalablement été mis au repos, entrez :
`ndcontrol manager unquiesce 130.40.52.153`
- Pour afficher le numéro de version en cours du gestionnaire, entrez :
`ndcontrol manager version`

ndcontrol metric — configuration des mesures du système



add

Permet d'ajouter la mesure spécifiée.

grappe

Adresse de connexion des clients. Il peut s'agir du nom d'hôte de la machine ou de l'adresse IP en notation décimale à points. Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

Remarque : Pour Cisco Consultant, l'adresse de grappe correspond à l'adresse IP virtuelle (VIP) de la règle de contenu du propriétaire dans la configuration Cisco CSS Switch.

mesure

Nom de la mesure du système. Il doit s'agir du nom d'un fichier exécutable ou d'un fichier script du répertoire script du Metric Server.

remove

Supprime la mesure spécifiée.

proportions

Définit les proportions de toutes les mesures associées à cet objet.

status

Affiche les valeurs actuelles de cette mesure.

Exemples

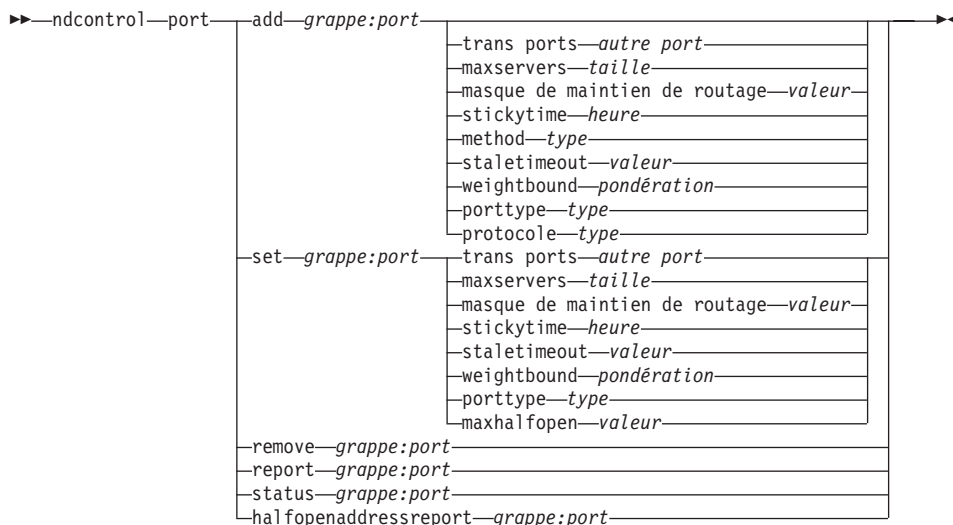
- Pour ajouter une mesure de système, entrez :
`sscontrol metric add site1:metric1`
- Pour définir les proportions d'un nom de site disposant de deux mesures de système, entrez :
`sscontrol metric proportions site1 0 100`
- Pour afficher l'état en cours des valeurs associées à la mesure spécifiée, entrez :
`sscontrol metric status site1:metric1`

Cette commande génère des résultats similaires à l'exemple suivant :

```
Etat
des mesures :
-----
Grappe ..... 10.10.10.20
```

Nom de la mesure metric1
Proportion de la mesure 50
 Serveur plm3
 Données de mesure -1

ndcontrol port — Configuration des ports



add

Ajoute un port à une grappe. Avant d'ajouter un serveur à un port, vous devez ajouter un port à une grappe. Si aucun port n'est destiné à une grappe, toutes les requêtes client seront traitées en local. Cette commande permet d'ajouter plusieurs ports à la fois.

Remarque : Pour le composant Mailbox Locator de Network Dispatcher, vous devez associer l'adresse IP de grappe à un alias sur l'ordinateur avant d'ajouter un port. La commande **add port** tente de lancer un proxy Java qui relie à la grappe. Par conséquent, l'adresse IP doit exister dans la pile IP.

Sous Windows, cela signifie qu'elle doit figurer dans la configuration des fonctions de gestion réseau. La commande **cluster configure** ne suffit pas, car elle ne simule que la définition d'adresse IP et le proxy ne peut pas établir un lien avec cette fausse adresse IP. Sous tous les autres systèmes d'exploitation, la commande **cluster configure** est appropriée, car elle utilise `ifconfig` pour l'alias de l'adresse IP.

grappe

Adresse de la grappe sous forme de nom symbolique ou en notation décimale à point. Vous pouvez utiliser le signe deux-points (:) comme caractère générique. Par exemple, la commande `ndcontrol port add :80` permet d'ajouter le port 80 à toutes les grappes.

Remarque : Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

port

Numéro du port. Le numéro de port 0 (zéro) est utilisé pour indiquer un port générique.

Remarque : Chaque port supplémentaire doit être séparé du précédent par le signe plus (+).

trans ports

Trans ports permet d'étendre la fonction d'affinité/maintien de routage à des ports multiples de façon à ce que les requêtes des clients reçues sur différents ports continuent à être envoyées au même serveur lors des requêtes suivantes. En ce qui concerne la valeur trans ports, indiquez le numéro *autre port* avec lequel vous souhaitez partager la fonction d'affinité trans ports. Pour utiliser cette fonction, les ports doivent :

- partager la même adresse de grappe
- partager les mêmes serveurs
- avoir le même (non nul) délai de maintien de routage
- avoir le même masque de maintien de routage

Pour supprimer la fonction trans ports, remplacez la valeur trans ports sur son propre numéro de port. Pour plus d'informations sur la fonction de l'affinité trans ports, reportez-vous à «Affinité trans ports» à la page 197.

Remarque : Trans ports s'applique uniquement au composant Dispatcher.

autre port

Valeur de trans ports. La valeur par défaut est la même que celle de son numéro de *port*.

maxservers

Nombre maximal de serveurs. La valeur par défaut du paramètre maxservers est 32. Nombre de serveurs autorisés sur un port.

taille

Valeur de maxservers.

Masque de maintien de routage

La fonction de masque d'adresse de l'affinité regroupe les requêtes des clients entrants, en fonction de leurs adresses de sous-réseaux communes. Lorsqu'une requête client établit une connexion avec un port pour la première fois, toutes les adresses ultérieures des clients possédant la même adresse de sous-réseau (indiquée par la partie masquée de l'adresse) seront acheminées vers ce même serveur. Se reporter à la section «Masque d'adresse de l'affinité» à la page 198, pour plus d'informations.

Remarque : Le mot clé du masque de maintien de routage s'applique uniquement au composant Dispatcher.

valeur

La valeur du masque de maintien de routage correspond au nombre de bits à poids fort, parmi les adresse IP 32 bits, que vous souhaitez masquer. Les valeurs possibles sont 8, 16, 24 et 32. La valeur par défaut est 32 et elle désactive la fonction du masque d'adresse d'affinité.

stickytime

Délai entre la fermeture d'une connexion et l'ouverture d'une nouvelle connexion au cours de laquelle un client sera renvoyé au même serveur utilisé lors de la première connexion. Passé le délai de maintien de routage, le client peut être envoyé à un serveur autre que le premier.

Composant Dispatcher :

- Méthode d'acheminement CBR de Dispatcher
 - Lorsque vous définissez un délai de routage différent de zéro, le type d'affinité par défaut (none) doit être associé à la commande rule. L'affinité basée sur les règles (cookie passif, URI) ne peut pas être utilisée lorsqu'un délai de maintien de routage est défini pour le port.
 - La définition d'une valeur de délai de maintien de routage activant l'affinité SSL ID, vous ne pouvez pas ajouter de règle Contenu au port.
- Méthodes d'acheminement MAC et NAT de Dispatcher
 - Lorsque vous définissez un délai de routage différent de zéro, vous ne pouvez pas associer de type d'affinité à la règle. L'affinité basée sur les règles ne peut pas être utilisée lorsqu'un délai de maintien de routage est défini pour le port.
 - La définition d'une valeur de délai de maintien de routage active l'affinité de l'adresse IP.
- La valeur de délai de maintien de routage doit être de 1 si vous utilisez l'API Server Directed Affinity.

Composant CBR : lorsque vous définissez un délai de routage différent de zéro, le type d'affinité par défaut (none) doit être associé à la commande rule. L'affinité basée sur les règles (cookie passif, URI, cookie actif) ne peut pas être utilisée lorsqu'un délai de maintien de routage est défini pour le port.

heure

Délai de maintien de routage du port (en secondes). la valeur Zéro signifie que le port n'est pas maintenu.

method

Il s'agit de la méthode d'acheminement. Les méthodes d'acheminement

possibles sont les suivantes : MAC, NAT/NAPT ou CBR (routage par contenu). Il se peut que vous n'ajoutiez *pas* de méthode d'acheminement NAT/NAPT ou CBR si vous n'indiquez pas d'abord une adresse IP non nulle pour le paramètre clientgateway de la commande ndcontrol executor. Reportez-vous aux sections «Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)» à la page 52 et «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54 pour plus d'informations.

Remarque : Si le serveur dorsal se trouve sur le même sous-réseau que l'adresse de retour et que vous utilisez la méthode d'acheminement CBR ou NAT/NAPT, vous devez définir l'adresse de routeur en tant qu'adresse de serveur dorsal.

type

Il s'agit du type de la méthode d'acheminement. Les valeurs possibles sont les suivantes : mac, nat ou cbr. La valeur par défaut est mac (acheminement MAC).

staletimeout

Nombre de secondes d'inactivité possible sur une connexion avant que cette dernière soit supprimée. Pour Dispatcher ou le composant CBR, la valeur par défaut est 900 pour le port 21 (FTP) et 32,000,000 pour le port 23 (Telnet). Pour tous les autres ports, la valeur par défaut est 300. Le paramètre staletimeout peut également être défini au niveau de l'exécuteur ou de la grappe. Reportez-vous à «Utilisation de la valeur du délai d'attente» à la page 217, pour de plus amples informations.

Remarque : Pour Mailbox Locator, le paramètre staletimeout correspond au délai de déconnexion automatique après une période d'inactivité de ces protocoles. La valeur par défaut de staletimeout, pour Mailbox Locator, est de 60 secondes ; elle est supérieure aux délais d'inactivité de POP3 et IMAP. Pour plus d'informations sur le paramètre staletimeout pour Mailbox Locator, reportez-vous à la section «Remplacement du délai d'inactivité de POP3/IMAP» à la page 100.

valeur

Valeur du paramètre **staletimeout** (en secondes).

weightbound

Définit la pondération maximale des serveurs sur ce port. Cela a une incidence sur le degré de différence possible entre le nombre des demandes transmises par l'exécuteur à chaque serveur. La valeur par défaut est 20.

pondération

Nombre compris entre 1 et 100 représentant la limite de pondération maximale.

porttype

Type de port.

Remarque : Le paramètre Porttype ne s'applique qu'à Dispatcher.

type

La valeurs possibles sont **tcp**, **udp** et **both**. La valeur par défaut est (tcp/udp).

Protocole

Type de protocole proxy (POP3 ou IMAP). Le paramètre protocol est requis lors de l'ajout d'un port pour Mailbox Locator.

Remarque : Il ne s'applique qu'à Mailbox Locator.

type

Les valeurs possibles sont **POP3** ou **IMAP**.

maxhalfopen

Nombre maximal de connexions partielles. Ce paramètre permet de détecter les refus de service éventuelles qui génèrent un nombre élevé de connexions TCP partielles sur les serveurs.

Une valeur positive indique qu'il sera procédé à une vérification pour déterminer si le nombre de connexions partielles en cours dépasse la limite autorisée. Si tel est le cas, un script d'alerte est appelé. Pour de plus amples informations, reportez-vous à «Détection d'attaque de refus de service» à la page 204.

Remarque : Le paramètre maxhalfopen ne s'applique qu'à Dispatcher.

valeur

Valeur de maxhalfopen. La valeur par défaut est zéro (aucune vérification n'est effectuée).

set

Définit les zones d'un port.

remove

Supprime ce port.

report

Génère un rapport sur ce port.

status

Affiche l'état des serveurs sur ce port. Pour visualiser l'état de tous les ports, n'indiquez pas de *port* dans cette commande. N'oubliez pas les deux-points.

nbSecondes

Durée en secondes avant la réinitialisation des connexions partielles.

halfopenaddressreport

Génère des entrées dans le journal (halfOpen.log) pour toutes les adresses client (jusqu'à environ 8000 paires d'adresses) qui ont accédé à des serveurs disposant de connexions partielles. De plus, les données statistiques sont affichées dans la ligne de commande, telles que le nombre total, moyen ou plus élevé de connexions partielles, et le temps moyen de connexion partiel (en secondes). Pour de plus amples informations, reportez-vous à «Détection d'attaque de refus de service» à la page 204.

Exemples

- Pour ajouter les ports 80 et 23 à l'adresse de grappe 130.40.52.153, entrez :
`ndcontrol port add 130.40.52.153:80+23`
- Pour ajouter un port générique à l'adresse de grappe 130.40.52.153, entrez :
`ndcontrol port set 130.40.52.153:0`
- Dans le cas de Mailbox Locator, pour ajouter le port 20 du protocole POP3 à l'adresse de grappe 9.37.60.91, entrez :
`mlcontrol port add 9.37.60.91:20 protocol pop3`
- Pour affecter la pondération maximale de 10 au port 80 à l'adresse de grappe 130.40.52.153, entrez :
`ndcontrol port set 130.40.52.153:80 weightbound 10`
- Pour porter à 60 secondes la valeur de délai de maintien de routage des ports 80 et 23 de l'adresse de grappe 130.40.52.153, entrez :
`ndcontrol port set 130.40.52.153:80+23 stickytime 60`
- Pour définir l'affinité trans ports du port 80 au port 23, à l'adresse de grappe 130.40.52.153, entrez :
`ndcontrol port set 130.40.52.153:80 crossport 23`
- Pour supprimer le port 23 de l'adresse de grappe 130.40.52.153, entrez :
`ndcontrol port remove 130.40.52.153:23`
- Pour obtenir l'état du port 80 à l'adresse de grappe 9.67.131.153, entrez :
`ndcontrol port status 9.67.131.153:80`

Cette commande génère des résultats similaires à l'exemple suivant :

Etat du port :

Numéro du port 80

```

Adresse de grappe ..... 9.67.131.153
Nombre de serveurs ..... 2
Délai d'expiration ..... 30
Limite de pondération ..... 20
Nombre maximal de serveurs ..... 32
Délai de maintien de routage ..... 0
Type de port ..... tcp/udp
Méthode d'acheminement ..... acheminement MAC
Bits du masque de rappel ..... 32
Affinité trans ports ..... 80
Nombre maximal de connexions partielles 0

```

- Pour obtenir le rapport d'adresses partielles pour le port 80 à l'adresse de grappe 9.67.127.121, entrez :

```
ndcontrol port halfopenaddressreport 9.67.127.121:80
```

Cette commande génère des résultats similaires à l'exemple suivant :

Rapport

- Connexions partielles créé :

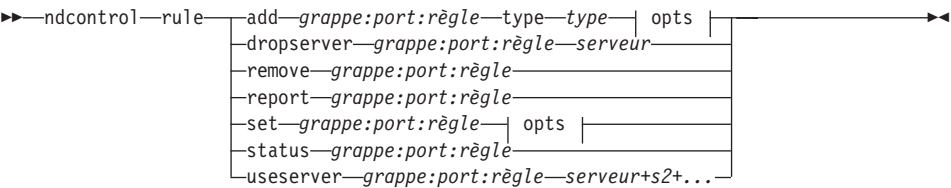
```

Rapport - Adresses avec connexions partielles pour grappe:port = 9.67.127.121:80
Rapport - Adresses avec connexions partielles pour grappe:port ... 0
Nombre total de connexions partielles consignées ..... 0
Plus grand nombre de connexions partielles consignées ..... 0
Nombre moyen de connexions partielles consignées ..... 0
Temps moyen de connexion partielle (en secondes) consignées ..... 0
Nombre total de connexions partielles reçues ..... 0

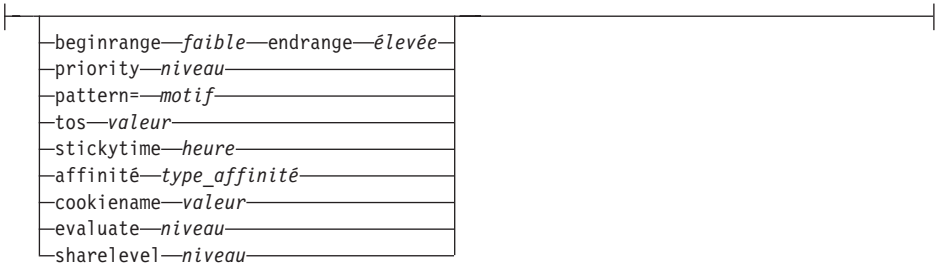
```

ndcontrol rule — configuration des règles

Remarque : Les schémas des syntaxes de commandes de règles ne s'appliquent pas à Mailbox Locator.



opts :



add

Ajoute cette règle à un port.

grappe

Adresse de la grappe sous forme de nom symbolique ou en notation décimale à point. Vous pouvez utiliser le signe deux-points (:) comme caractère générique. Par exemple, la commande suivante `ndcontrol rule add :80:RuleA type type`, permet d'ajouter RuleA au port 80 pour toutes les grappes.

Remarque : Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

port

Numéro du port. Vous pouvez utiliser le signe deux-points (:) comme caractère générique. Par exemple, la commande suivante `ndcontrol rule add clusterA::RuleA type type` permet d'ajouter RuleA à tous les ports pour ClusterA.

Remarque : Chaque port supplémentaire doit être séparé du précédent par le signe plus (+).

règle

Nom choisi pour la règle. Ce nom peut contenir tout caractère alphanumérique, des traits de soulignement, des traits d'union ou des points. Il peut comporter de 1 à 20 caractères, et ne doit contenir aucun espace.

Remarque : Chaque règle supplémentaire doit être séparée de la précédente par le signe plus (+).

type

Type de règle.

type

Les différents *types* de règles possibles sont les suivants :

ip La règle est définie en fonction de l'adresse IP du client.

time La règle est définie en fonction de l'heure.

connection

La règle est définie en fonction du nombre de connexions par seconde du port. Cette règle ne fonctionne que si le gestionnaire est en cours d'exécution.

active La règle est définie en fonction du nombre total de connexions actives sur le port. Cette règle ne fonctionne que si le gestionnaire est en cours d'exécution.

port La règle est définie en fonction du port client.

Remarque : Port ne s'applique pas à CBR.

service

Cette règle est fondée sur la zone d'octets type de service (TOS) de l'en-tête IP.

Remarque : la règle Service s'applique uniquement au composant Dispatcher.

reservedbandwidth

Cette règle est fonction du nombre de kilo-octets par seconde de largeur de bande délivrés par un ensemble de serveurs. Pour plus d'informations, reportez-vous aux sections «Utilisation de règles basées sur la largeur de bande réservée et sur la largeur de bande partagée» à la page 185 et «Règle de largeur de bande réservée» à la page 186.

Remarque : Reservedbandwidth ne s'applique qu'au composant Dispatcher.

sharedbandwidth

Cette règle est fonction du nombre de kilo-octets par seconde de largeur de bande partagés au niveau de l'exécuteur ou de la grappe. Pour plus d'informations, reportez-vous aux sections «Utilisation de règles basées sur la largeur de bande réservée et sur la largeur de bande partagée» à la page 185 et «Règle de largeur de bande partagée» à la page 186.

Remarque : Sharedbandwidth ne s'applique qu'au composant Dispatcher.

true Cette règle est toujours vraie. Considérez-la comme une instruction else en logique de programmation.

content

Cette règle décrit une expression régulière qui sera comparée aux URL demandées par les clients. Elle ne fonctionne que pour Dispatcher et CBR.

beginrange

Valeur de début de la fourchette utilisée pour déterminer si la règle est vraie.

faible

Dépend du type de règle. Le type de valeur et les valeurs par défaut sont précisés ci-après par type de règle :

ip Adresse du client sous forme de nom symbolique ou en notation décimale à point. La valeur par défaut est 0.0.0.0.

time Entier. La valeur par défaut est 0 (minuit).

connection

Entier. Valeur par défaut : 0.

active Entier. Valeur par défaut : 0.

port Entier. Valeur par défaut : 0.

reservedbandwidth

Entier (kilo-octets par seconde). Valeur par défaut : 0.

endrange

Valeur de fin de la fourchette utilisée pour déterminer si la règle est vraie.

élevée

Dépend du type de règle. Le type de valeur et les valeurs par défaut sont précisés ci-après par type de règle :

ip Adresse du client sous forme de nom symbolique ou en notation décimale à point. La valeur par défaut est 255.255.255.254.

time Entier. La valeur par défaut est 24 (minuit).

Remarque : Lors de la définition des intervalles de temps (début et fin d'une fourchette horaire), notez que chaque valeur doit être un entier représentant seulement l'heure. Les subdivisions de l'heure ne sont pas indiquées. Pour cette raison, pour indiquer une heure, par exemple entre 3:00 et 4:00 du matin, attribuez la valeur **3** à *beginrange* (début) et **3** à *endrange* (fin). Cela signifiera toutes les minutes comprises entre 3:00 et 3:59. Si vous indiquez **3** au paramètre *beginrange* et **4** au paramètre *endrange*, vous couvrirez la période de deux heures allant de 3:00 à 4:59.

connections

Entier. La valeur par défaut est 2 à la puissance 32 moins 1.

active Entier. La valeur par défaut est 2 à la puissance 32 moins 1.

port Entier. La valeur par défaut est 65535.

reservedbandwidth

Entier (kilo-octets par seconde). La valeur par défaut est 2 à la puissance 32 moins 1.

priority

Ordre dans lequel les règles sont consultées.

niveau

Entier. Si vous ne spécifiez pas la priorité de la première règle que vous ajoutez, Dispatcher lui affecte par défaut la valeur 1. Une règle ajoutée par la suite se verra affecter par défaut une priorité égale à la priorité la plus basse existante + 10. Supposons que vous avez une règle dont la priorité est 30. Vous ajoutez une nouvelle règle et définissez sa priorité à 25 (priorité *supérieure* à 30). Vous ajoutez ensuite une troisième règle, sans lui affecter de priorité. La priorité de la troisième règle sera de 40 (30 + 10).

pattern

Indique le motif à utiliser pour une règle type de contenu.

motif

Motif à utiliser. Pour plus d'informations sur les valeurs acceptées, reportez-vous à la section «Annexe C. Syntaxe des règles de contenu (modèle)» à la page 323.

tos

Indique la valeur de "type de service" (TOS) utilisée par la règle type **service**.

Remarque : TOS s'applique uniquement au composant Dispatcher.

valeur

Chaîne de 8 caractères à utiliser pour la valeur TOS. Les caractères valides

sont : 0 (zéro binaire), 1 (un binaire), et x (peu importe). Par exemple : 0xx1010x. Pour plus d'informations, reportez-vous à la section «Utilisation de règles basées sur le type de services (TOS)» à la page 184.

stickytime

Indique le délai de maintien de routage à utiliser pour une règle. Lorsque vous attribuez la valeur "activecookie" au paramètre affinity dans la commande rule, vous devez affecter une valeur différente de zéro au délai de maintien de routage pour activer ce type d'affinité. Le délai de maintien de routage de la commande rule ne s'applique pas aux types d'affinité "passivecookie" ou "uri".

Pour de plus amples informations, reportez-vous à «Affinité de cookie actif» à la page 200.

Remarque : La règle de délai de maintien de routage s'applique uniquement au composant CBR.

heure

Heure en secondes

Affinity

Indique le type d'affinité à utiliser pour une règle : cookie actif, cookie passif, URI ou aucune affinité.

Le type d'affinité "activecookie" permet l'équilibrage de charge du trafic Web et une affinité avec le même serveur en fonction des cookies générés par Network Dispatcher.

Le type d'affinité "passivecookie" permet l'équilibrage de charge du trafic Web et une affinité avec le même serveur en fonction des cookies d'auto-identification générés par les serveurs. Vous devez utiliser le paramètre cookienam avec l'affinité de cookie passif.

Le type d'affinité "URI" permet l'équilibrage de charge du trafic Web vers des serveurs Caching Proxy dans le but d'augmenter la mémoire cache.

Pour plus d'informations, reportez-vous aux sections «Affinité de cookie actif» à la page 200, «Affinité de cookie passif» à la page 202 et «Affinité d'URI» à la page 203.

Remarque : L'affinité s'applique aux règles configurées avec la méthode d'acheminement CBR de Dispatcher et au composant CBR.

type_affinité

Les valeurs possibles pour le type d'affinité sont les suivantes : none (valeur par défaut), activecookie, passivecookie ou uri.

cookienam

Nom arbitraire défini par l'administrateur qui agit comme identificateur pour Network Dispatcher. Il s'agit du nom que Network Dispatcher doit

rechercher dans la demande d'en-tête HTTP client. Le nom de cookie et la valeur associée sert d'identificateur à Network Dispatcher, lui permettant d'envoyer les demandes suivantes d'un site Web au même serveur. Le nom de cookie n'est applicable qu'avec l'affinité de cookie passif.

Pour de plus amples informations, reportez-vous à «Affinité de cookie passif» à la page 202.

Remarque : Le nom de cookie s'applique aux règles configurées avec la méthode d'acheminement CBR de Dispatcher et au composant CBR.

valeur

Valeur du nom de cookie.

evaluate

Cette option est disponible pour le composant Dispatcher uniquement. Indique s'il faut évaluer la condition de règle sur tous les serveurs sur un port ou sur tous les serveurs de la règle. C'est option n'est valide que pour les règles qui fondent leurs décisions sur des caractéristiques des serveurs, telles que les règles de type connection, active et reservedbandwidth. Pour plus d'informations, reportez-vous à la section «Option d'évaluation de serveur» à la page 190.

niveau

Les valeurs acceptées sont port ou rule. La valeur par défaut est port.

sharelevel

Ce paramètre ne s'applique qu'à la règle relative à la largeur de bande partagée. Indique si la largeur de bande est partagé au niveau de la grappe ou au niveau de l'exécuteur. Le partage de la largeur de bande au niveau de la grappe permet à un ou des ports de partager une quantité maximale de largeur de bande sur plusieurs ports dans la même grappe. Le partage de la largeur de bande au niveau de l'exécuteur permet à une ou à des grappes dans la configuration Dispatcher de partager une quantité maximale de largeur de bande. Pour plus d'informations, reportez-vous à la section «Règle de largeur de bande partagée» à la page 186.

niveau

Les valeurs acceptées sont executor ou cluster.

dropserver

Supprime un serveur d'un jeu de règles.

serveur

Adresse IP de la machine serveur TCP sous forme de nom symbolique ou en notation décimale à point.

Ou, si vous utilisez le partitionnement du serveur, entrez le nom unique du serveur logique. Pour de plus amples informations, reportez-vous à «Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)» à la page 159.

Remarque : Chaque serveur supplémentaire doit être séparé du précédent par le signe plus (+).

remove

Supprime une ou plusieurs règles séparées entre elles par des signes plus.

report

Affiche les valeurs internes d'une ou plusieurs règles.

set

Définit les valeurs de cette règle.

status

Affiche les valeurs paramétrables d'une ou plusieurs règles.

useserver

Insère des serveurs dans un jeu de règles.

Exemples

- Pour ajouter une règle qui sera toujours vraie, ne spécifiez pas de valeur de début ni de fin. Entrez :
`ndcontrol rule add 9.37.67.100:80:trule type true priority 100`
- Pour créer une règle qui interdit l'accès à une série d'adresses IP, en l'occurrence, celles qui commencent par "9:", entrez :
`ndcontrol rule add 9.37.131.153:80:ni type ip b 9.0.0.0 e 9.255.255.255`
- Pour créer une règle qui limitera l'utilisation d'un serveur donné de 11:00 à 15:00, entrez :
`ndcontrol rule add cluster1:80:timerule type time beginrange 11 endrange 14`
`ndcontrol rule useserver cluster1:80:timerule server05`
- Pour créer une règle fondée sur le contenu de la zone d'octets TOS, dans l'en-tête IP, entrez :
`ndcontrol rule add 9.67.131.153:80:tosrule type service tos 0xx1001x`
- Pour créer une règle basée sur la largeur de bande réservée qui allouera un ensemble de serveurs (évalués dans la règle) pour délivrer des données jusqu'à 100 kilo-octets par seconde :
`ndcontrol rule add 9.67.131.153:80:rbwrule type reservedbandwidth`
`beginrange 0 endrange 100 evaluate rule`

- Pour créer une règle basée sur la largeur de bande partagée qui va rechercher la largeur de bande inutilisée au niveau de la grappe, (Remarque : vous devez d'abord spécifier la quantité maximale de largeur de bande (en kilo-octets par seconde) pouvant être partagée au niveau de la grappe à l'aide de la commande `ndcontrol cluster`), entrez :

```
ndcontrol cluster set 9.67.131.153 sharedbandwidth 200
```

```
ndcontrol rule add 9.67.131.153:80:shbwrule type sharedbandwidth  
sharelevel cluster
```

ndcontrol server — Configuration des serveurs



add

Permet d'ajouter ce serveur.

grappe

Adresse de la grappe sous forme de nom symbolique ou en notation décimale à point. Vous pouvez utiliser le signe deux-points (:) comme caractère générique. Par exemple, la commande `ndcontrol server add :80:ServerA` permet d'ajouter ServerA au port 80 sur toutes les grappes.

Remarque : Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

port

Numéro du port. Vous pouvez utiliser le signe deux-points (:) comme caractère générique. Par exemple, la commande `ndcontrol server add ::ServerA`, permet d'ajouter ServerA à toutes les grappes sur tous les ports.

Remarque : Chaque port supplémentaire doit être séparé du précédent par le signe plus (+).

serveur

Le **serveur** est l'adresse IP unique de la machine serveur TCP sous forme de nom symbolique ou en notation décimale à point.

Ou, si vous utilisez un nom unique qui ne se résout pas en adresse IP, vous devez fournir le paramètre **address** du serveur dans la commande **ndcontrol server add**. Pour de plus amples informations, reportez-vous à «Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)» à la page 159.

Remarque : Chaque serveur supplémentaire doit être séparé du précédent par le signe plus (+).

address

Adresse IP unique de la machine serveur TCP sous forme de nom d'hôte ou en notation décimale à point. S'il n'est pas possible de résoudre le serveur, vous devez fournir l'adresse de la machine serveur physique. Pour de plus amples informations, reportez-vous à «Partitionnement du serveur : serveurs logiques configurés pour un serveur physique (adresse IP)» à la page 159.

adresse

Valeur de l'adresse du serveur.

collocated

L'option Co-implanté permet d'indiquer si Dispatcher est installé sur l'un des serveurs dont il équilibre les charges. Elle ne s'applique pas à la plate-forme Windows 2000.

Remarque : Le paramètre **collocated** n'est valide que si vous utilisez les méthodes d'acheminement **mac** ou **nat** de Dispatcher. Mailbox Locator, Site Selector et Cisco Consultant peuvent être co-implantés sur toutes les plate-formes mais ne requièrent pas ce mot clé. Pour plus d'informations, voir «Utilisation de serveurs implantés au même endroit» à la page 162.

valeur

Valeur de Co-implanté : oui ou non. Elle est fixée à non par défaut.

sticky

Permet à un serveur de remplacer sur son port les paramètres de maintien de routage. Lorsque la valeur par défaut est "oui," le serveur garde l'affinité normale définie sur le port. Lorsque cette valeur est "non," le client ne sera *pas* renvoyé à ce serveur lors de sa prochaine requête à ce port et ce, indépendamment des paramètres de maintien de routage du port. Ceci peut s'avérer utile quand vous utilisez des règles. Pour plus d'informations, voir «Substitution d'affinité de règle» à la page 199.

valeur

Valeur du maintien de routage : oui ou non. Elle est fixée à non par défaut.

weight

Nombre compris entre 0 et 100 (mais qui ne doit pas dépasser la valeur de pondération du port spécifiée) représentant la pondération relative à ce serveur. L'affectation de la valeur zéro à la pondération empêche l'envoi de nouvelles demandes au serveur mais ne met pas fin aux connexions actuellement actives à ce serveur. La valeur par défaut correspond à la moitié de la valeur de pondération maximale du port indiqué. Si le gestionnaire est en cours d'exécution, ce paramètre est rapidement remplacé.

valeur

Valeur de la pondération du serveur.

fixedweight

L'option fixedweight vous permet d'indiquer si vous souhaitez, ou non, que le gestionnaire modifie la pondération du serveur. Si vous fixez sur oui la valeur fixedweight, le gestionnaire en activité ne sera pas autorisé à modifier la pondération du serveur. Pour plus d'informations, voir «Pondérations fixées par le gestionnaire» à la page 143.

valeur

Valeur de fixedweight : oui ou non. La valeur par défaut est non.

mapport

Mappe le numéro du port de destination de la demande client (pour Dispatcher) au numéro de port du serveur que Dispatcher utilise pour équilibrer la charge de la demande du client. Permet à Network Dispatcher de recevoir une demande de client sur un port et de la transmettre à un autre port de la machine serveur. Le paramètre mapport permet d'équilibrer la charge des demandes d'un client sur un serveur sur lequel peuvent s'exécuter plusieurs démons serveur.

Remarque : Mapport s'applique à Dispatcher (avec les méthodes d'acheminement nat ou cbr) ainsi qu'à CBR. Pour Dispatcher, reportez-vous aux sections «Réacheminement NAT/NAPT de Dispatcher (méthode d'acheminement nat)» à la page 52 et «Fonction CBR de Dispatcher (méthode d'acheminement cbr)» à la page 54. Pour CBR, reportez-vous à la section «Equilibrage de charge client-proxy dans SSL et proxy-serveur dans HTTP» à la page 80.

valeur du port

Valeur du numéro de port de mappage. La valeur par défaut est le numéro de port de destination de la demande du client.

router

Si vous définissez un réseau étendu, il s'agit de l'adresse du routeur vers le serveur éloigné. La valeur par défaut est 0, correspondant à un serveur local. Notez que, lorsqu'une adresse de routeur est définie avec une valeur autre que zéro (ce qui désigne un serveur éloigné), elle ne peut pas être redéfinie par 0 pour rechanger le serveur en serveur local. Le serveur doit être supprimé, puis ajouté à nouveau sans adresse de routeur spécifiée. De même, un serveur local (adresse de routeur = 0) ne peut pas être changé en serveur éloigné en changeant l'adresse du routeur. Le serveur doit être supprimé, puis ajouté de nouveau. Pour de plus amples informations, reportez-vous à «Configuration du support de réseau étendu pour Dispatcher» à la page 164.

Remarque : Le routeur ne concerne que Dispatcher. Si vous utilisez les méthodes d'acheminement NAT ou CBR, indiquez l'adresse de routeur lors de l'ajout d'un serveur à la configuration.

adr

Adresse du routeur.

cookievalue

Cookievalue est une valeur arbitraire qui représente le côté serveur de la paire de valeur nom de cookie/cookie. La valeur de cookie, associée au nom de cookie, sert d'identificateur permettant à Network Dispatcher d'envoyer les demandes client suivantes au même serveur. Pour de plus amples informations, reportez-vous à «Affinité de cookie passif» à la page 202.

Remarque : Cookievalue est valide pour Dispatcher (avec la méthode d'acheminement CBR) et pour CBR.

valeur

Il s'agit de n'importe quelle valeur arbitraire. Par défaut, il n'y a pas de valeur de cookie.

returnaddress

Adresse IP ou nom d'hôte unique. Il s'agit d'une adresse configurée sur la machine Dispatcher que Dispatcher utilise comme adresse source lors de l'équilibrage de charge des demandes du client sur le serveur. Elle permet de garantir que le serveur renverra le paquet à la machine Dispatcher pour traiter le contenu de la demande, au lieu de l'envoyer directement au client. (Dispatcher transmettra ensuite le paquet IP au client.) Vous devez indiquer la valeur d'adresse de retour lors de l'ajout du serveur. L'adresse de retour ne peut pas être modifiée sauf si vous supprimez le serveur et l'ajoutez à nouveau. Elle ne peut pas être identique à l'adresse de grappe, de serveur ou NFA.

Remarque : Le paramètre `returnaddress` ne s'applique qu'à Dispatcher. Si vous utilisez les méthodes d'acheminement NAT ou CBR, indiquez l'adresse de retour lors de l'ajout d'un serveur à la configuration.

adr

Valeur de l'adresse de retour.

advisorrequest

Le conseiller HTTP utilise la chaîne `advisor request` pour interroger l'état des serveurs. Elle n'est valide que pour les serveurs qui sont traités par le conseiller HTTP. Vous devez démarrer le conseiller HTTP pour activer cette valeur. Pour de plus amples informations, reportez-vous à «Option de demande/réponse (URL) de conseiller HTTP» à la page 161.

Remarque : `Advisorrequest` s'applique aux composants Dispatcher et CBR.

chaîne

Valeur de la chaîne utilisée par le conseiller HTTP. La valeur par défaut est `HEAD / HTTP/1.0`.

Remarque : Si la chaîne comporte un espace —

- Lorsque vous lancez la commande à partir de l'invite du shell **ndcontrol**>>, vous devez mettre la chaîne entre guillemets. Par exemple : **server set grappe:port:serveur advisorrequest "head / http/2.0"**
- Lorsque vous lancez la commande **ndcontrol** à partir de l'invite du système d'exploitation, vous devez placer les caractères `"\"` et `\""` respectivement avant et après le texte. Par exemple : **ndcontrol server set grappe:port:serveur advisorrequest "\"head / http/2.0\""**

advisorresponse

Chaîne `advisor response` que le conseiller HTTP recherche dans la réponse HTTP. Elle n'est valide que pour les serveurs qui sont traités par le conseiller HTTP. Vous devez démarrer le conseiller HTTP pour activer cette valeur. Pour de plus amples informations, reportez-vous à «Option de demande/réponse (URL) de conseiller HTTP» à la page 161.

Remarque : `Advisorresponse` s'applique aux composants Dispatcher et CBR.

chaîne

Valeur de la chaîne utilisée par le conseiller HTTP. La valeur par défaut est `null`.

Remarque : Si la chaîne comporte un espace —

- Lorsque vous lancez la commande à partir de l'invite du shell **ndcontrol**>>, vous devez mettre la chaîne entre guillemets.
- Lorsque vous lancez la commande **ndcontrol** à partir de l'invite du système d'exploitation, vous devez placer les caractères "\" et \"\" respectivement avant et après le texte.

down

Marque ce serveur comme étant arrêté. Cette commande permet d'interrompre toutes les connexions actives à ce serveur et d'empêcher l'envoi d'autres connexions ou paquets à ce serveur.

remove

Permet de supprimer ce serveur.

report

Génère un rapport sur ce serveur.

set

Permet de définir des valeurs pour ce serveur.

status

Affichage de l'état des serveurs.

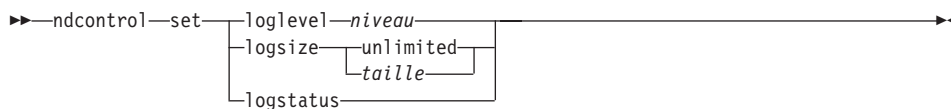
up Marque ce serveur comme étant activé. Dispatcher envoie désormais de nouvelles connexions à ce serveur.

Exemples

- Pour ajouter le serveur 27.65.89.42 au port 80 sur une grappe à l'adresse 130.40.52.153, entrez :
`ndcontrol server add 130.40.52.153:80:27.65.89.42`
- Pour fixer le serveur, à l'adresse 27.65.89.42, dans la position Maintien de routage (fonction de substitution d'affinité de règle), entrez :
`ndcontrol server set 130.40.52.153:80:27.65.89.42 sticky no`
- Pour marquer le serveur 27.65.89.42 comme étant arrêté, entrez :
`ndcontrol server down 130.40.52.153:80:27.65.89.42`
- Pour supprimer le serveur 27.65.89.42 de tous les ports de toutes les grappes, entrez :
`ndcontrol server remove ::27.65.89.42`
- Pour fixer le serveur, à l'adresse 27.65.89.42, dans la position co-implanté (le serveur et Network Dispatcher sont situés sur la même machine) :
`ndcontrol server set 130.40.52.153:80:27.65.89.42 collocated yes`
- Pour affecter la valeur 10 à la pondération du serveur 27.65.89.42 au port 80 sur une grappe à l'adresse 130.40.52.153, entrez :
`ndcontrol server set 130.40.52.153:80:27.65.89.42 weight 10`

- Pour marquer le serveur 27.65.89.42 comme étant activé, entrez :
ndcontrol server up 130.40.52.153:80:27.65.89.42
- Pour ajouter un serveur éloigné :
ndcontrol server add 130.40.52.153:80:130.60.70.1 router 130.140.150.0
- Pour permettre au conseiller HTTP d'interroger une demande d'URL HTTP HEAD / HTTP/2.0 pour le serveur 27.65.89.42 sur le port HTTP 80, entrez :
ndcontrol server set 130.40.52.153:80:27.65.89.42
advisorequest "\"HEAD / HTTP/2.0\""

ndcontrol set — Configuration du journal du serveur



loglevel

Niveau auquel le ndserver consigne ses activités.

niveau

La valeur par défaut de **loglevel** est 0. La fourchette va de 0 à 5. Les valeurs possibles sont les suivantes : 0 (Aucun), 1 (Minimal), 2 (De base), 3 (Modéré), 4 (Avancé), 5 (Prolixe).

logsize

Nombre maximal d'octets à consigner dans le fichier journal.

taille

La taille de fichier journal par défaut est 1 Mo.

logstatus

Affiche les paramètres du journal du serveur (niveau de journalisation et taille du journal)

ndcontrol status — Affichage de l'exécution ou non du gestionnaire et des conseillers

➤—ndcontrol—status—➤

Exemples

- Pour visualiser les éléments en cours d'exécution, entrez :
ndcontrol status

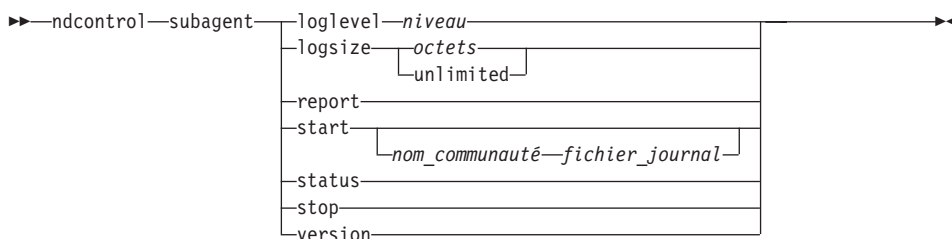
Cette commande génère des résultats similaires à l'exemple suivant :

L'exécuteur (executor) a été lancé.
Le gestionnaire (manager) a été lancé

CONSEILLER	PORT	DELAI
reach	0	illimité
http	80	illimité
ftp	21	illimité

ndcontrol subagent — Configuration du sous-agent SNMP

Remarque : Les schémas des syntaxes de commande de sous-agent Ndcontrol ne s'appliquent pas à CBR ni à Mailbox Locator.



loglevel

Niveau auquel le sous-agent consigne ses activités dans un fichier.

niveau

Numéro du niveau (0 à 5). Plus le numéro est élevé, plus la quantité des informations consignées dans le journal du gestionnaire est importante. Valeur par défaut : 1. Les valeurs possibles sont les suivantes : 0 (Aucun), 1 (Minimal), 2 (De base), 3 (Modéré), 4 (Avancé), 5 (Prolixe).

logsize

Taille maximale en octets à consigner dans le journal du sous-agent. La valeur par défaut est 1 Mo. Lorsque vous affectez une taille maximale au fichier journal, celui-ci se boucle ; lorsque le fichier atteint la taille indiquée, les entrées suivantes sont écrites à partir du haut du fichier pour écraser les entrées de journal précédentes. La taille du journal ne peut pas être moins élevée que la taille actuelle du journal. Les entrées de fichier sont horodatées, ce qui permet de déterminer l'ordre dans lequel elles ont été créées. Plus le niveau de journalisation est élevé, plus la taille du journal doit être choisie attentivement car l'espace peut être saturé rapidement lors d'une consignation à des niveaux plus élevés.

octets

Taille maximale (en octets) du fichier journal du sous-agent. Vous pouvez indiquer un nombre positif supérieur à zéro, ou le mot **unlimited**. Il se peut que le fichier journal n'atteigne pas la taille maximale exacte avant l'écrasement, car la taille des entrées de journal elles-mêmes varie. La valeur par défaut est unlimited.

report

Affiche un rapport d'analyse sur les statistiques.

start

Lance le sous-agent.

nom_communauté

Nom de la valeur SNMP du nom de communauté que vous pouvez utiliser comme mot de passe de sécurité. La valeur par défaut est public.

fichier journal

Nom du fichier dans lequel les données du sous-agent SNMP sont consignées. Chaque enregistrement du journal est horodaté. La valeur par défaut est subagent.log. Le fichier par défaut est installé dans le répertoire **logs**. Reportez-vous à la section «Annexe F. Exemples de fichiers de configuration» à la page 387. Pour changer le répertoire dans lequel les fichiers journaux vont être stockés, reportez-vous à la section «Modification des chemins des fichiers journaux» à la page 216.

status

Affiche l'état en cours de toutes les valeurs du sous-agent SNMP qui peuvent être affectées globalement, ainsi que les valeurs par défaut associées.

version

Affiche la version en cours du sous-agent.

Exemples

- Pour lancer le sous-agent avec le nom de communauté bigguy, entrez la commande suivante :
`ndcontrol subagent start bigguy bigguy.log`

Annexe C. Syntaxe des règles de contenu (modèle)

La présente annexe décrit comment utiliser la syntaxe de règle de contenu (modèle) pour le composant CBR et la méthode d'acheminement CBR de Dispatcher. Elle contient en outre des scénarios et des exemples de syntaxe.

Syntaxe de règle de contenu (modèle) :

Ne s'applique que si vous avez sélectionné le type de règle Contenu.

Entrez la syntaxe voulue en tenant compte des restrictions suivantes :

- Le motif ne doit pas contenir d'espace.
- Caractères tenant lieu de caractères spéciaux lorsqu'ils ne sont pas précédés d'une barre oblique inverse (\) :
 - * caractère générique (correspond à n'importe quel caractère)
 - (parenthèse gauche utilisée pour un regroupement logique
 -) parenthèse droite utilisée pour un regroupement logique
 - & ET logique
 - | OU logique
 - ! NON logique

Mots clés réservés

Les mots clés réservés sont toujours suivis d'un signe égal «=».

Méthode

Méthode HTTP de la demande, par exemple GET, POST, etc.

URI Chemin de la demande d'URL

Version

Version spécifique de la demande, HTTP/1.0 ou HTTP/1.1

Hôte valeur de l'hôte : en-tête.

Remarque : Facultatif dans les protocoles HTTP/1.0

<clé> Tout nom d'en-tête HTTP valide pouvant être recherché par HTTP. Par exemple, User-Agent, Connection, Referer, etc.

Un navigateur demandant la page

<http://www.entreprise.com/path/webpage.htm> peut obtenir des résultats du type suivant :

Méthode=GET

URI=/chemin/page Web.htm

Version=/HTTP/1.1

Hôte=www.entreprise.com

Connexion=signal de présence

Référenceur=<http://www.entreprise.com/chemin/pagewebparente.htm>

Remarque : Le shell du système d'exploitation peut interpréter les caractères spéciaux tels que "&" et les convertir en texte de remplacement avant leur évaluation avec **cbrcontrol**.

Par exemple, la commande suivante n'est valide qu'avec l'invite **cbrcontrol>>**.

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

Pour que cette commande fonctionne à partir de l'invite du système d'exploitation lorsque vous utilisez des caractères spéciaux, placez le motif entre guillemets (" ") comme suit :

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

Si vous omettez les guillemets, le motif sera peut-être tronqué lors de la sauvegarde de la règle dans CBR. Les guillemets ne sont pas pris en charge avec l'invite **cbrcontrol>>**.

Ci-dessous, se trouve un ensemble de scénarios et des exemples d'utilisation des syntaxes de modèle

Scénario 1 :

La configuration d'une grappe implique un ensemble de serveurs Web pour le contenu HTML standard, un autre ensemble de serveurs Web avec WebSphere Application Server pour les demandes de servlet, un autre ensemble de serveurs Lotus Notes pour les fichiers NSF, etc. Pour effectuer la différence entre les pages demandées, l'accès aux données du client est requis. Il est également nécessaire de les envoyer aux serveurs appropriés. Les règles de correspondance de modèle de contenu permettent d'effectuer une séparation, nécessaire à l'accomplissement de ces tâches. Plusieurs règles sont configurées afin que la séparation des demandes nécessaire se produise automatiquement.

Par exemple, les commandes suivantes provoquent les trois divisions indiquées :

```
>>rule add cluster1:80:servlets type content pattern uri=*/servlet/*priority 1
>>rule uses cluster1:80:servlets server1+server2

>>rule add cluster1:80:notes type content pattern uri=*.nsf* priority 2
>>rule uses cluster1:80:notes server3+server4

>>rule add cluster1:80:regular type true priority 3
>>rule uses cluster1:80:regular server5+server6
```

Si une demande de fichier NSF est reçue par Network Dispatcher, la règle servlets est vérifiée mais ne correspond pas. La demande est ensuite vérifiée par la règle notes qui trouve une correspondance. L'équilibrage de charge du client est effectué entre le serveur 3 et le serveur 4.

Scénario 2

Le contrôle par le site Web principal de plusieurs groupes internes constitue un autre scénario classique. Par exemple, l'ensemble de serveurs et le contenu de `www.company.com/software` sont différents de ceux de `www.company.com/hardware`. Étant donné que les demandes dépendent toutes de la grappe `www.company.com` racine, les règles de contenu sont requises pour trouver les différences d'URI et pour effectuer l'équilibrage de charge. La règle du scénario peut être du type suivant :

```
>>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
```

Scénario 3

Pour certaines associations, l'ordre de recherche des règles est important. Par exemple, dans le scénario 2, les clients ont été séparés en fonction d'un répertoire dans leur chemin de demande. Cependant, le répertoire cible peut apparaître à plusieurs niveaux du chemin et la signification est différente en fonction de l'emplacement. Par exemple, la cible de `www.company.com/pcs/fixes/software` est différente de celle de `www.company.com/mainframe/fixes/software`. Les règles doivent être définies pour prendre en compte cette possibilité et ne doivent pas inclure trop de scénarios en même temps. Par exemple, la recherche générique du test «`uri=*/software/*` » est trop large. D'autres règles peuvent être structurées de la manière suivante :

Vous pouvez associer plusieurs recherches afin de restreindre la recherche :

```
>>rule add cluster1:80:pcs type content pattern (uri=/pcs/*)&(uri=*/software/*)
>>rule uses cluster 1:80:pcs server1
```

Dans le cas où il n'est pas possible d'utiliser des combinaisons, l'ordre est important :

```
>>rule add cluster1:80:pc1 type content pattern uri=/pcs/*  
>>rule uses cluster1:80:pc1 server2
```

La deuxième règle permet de détecter l'apparition de «pcs» dans des répertoires ultérieurs du chemin et non le premier.

```
>>rule add cluster1:80:pc2 type content pattern uri=/*/pcs/*  
>>rule uses cluster1:80:pc2 server3
```

Dans la plupart des cas, vous pouvez compléter les règles par une règle par défaut **toujours vrai** afin de détecter tous les éléments non pris en compte par les autres règles. Un serveur peut également renvoyer un message du type «Ce site est actuellement indisponible, faites une nouvelle tentative ultérieurement» dans les scénarios pour lesquels aucun autre serveur ne peut renvoyer de réponse pour ce client.

```
>>rule add cluster1:80:sorry type true priority 100  
>>rule uses cluster1:80:sorry server5
```

Annexe D. Guide des commandes Site Selector

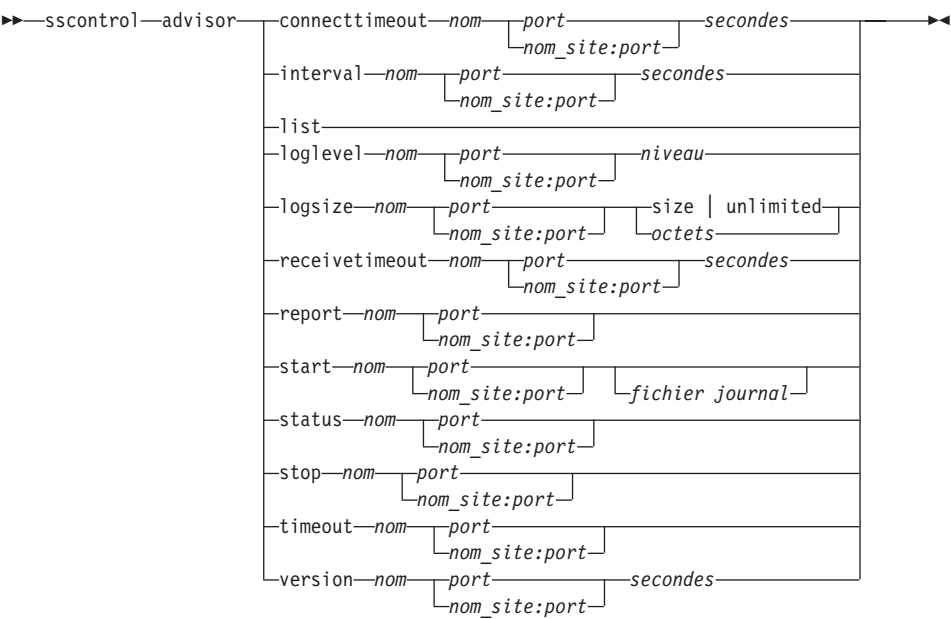
La présente annexe explique comment utiliser les commandes **sscontrol** Site Selector ci-après :

- «sscontrol advisor — Contrôle du conseiller» à la page 328
- «sscontrol file — Gestion des fichiers de configuration» à la page 334
- «sscontrol help — Affichage ou impression de l'aide sur cette commande» à la page 336
- «sscontrol manager — Contrôle du gestionnaire» à la page 337
- «sscontrol metric — Configuration des mesures du système» à la page 342
- «sscontrol nameserver — Contrôle de NameServer» à la page 343
- «sscontrol rule — Configuration des règles» à la page 344
- «sscontrol server — Configuration des serveurs» à la page 348
- «sscontrol set — Configuration du journal du serveur» à la page 350
- «sscontrol sitename — Configuration d'un nom de site» à la page 351
- «sscontrol status — Affiche si le gestionnaire et les conseillers sont en cours d'exécution» à la page 355

Vous pouvez entrer une version abrégée des paramètres de commandes **sscontrol**. Il suffit d'entrer les lettres spécifiques des paramètres. Par exemple, pour obtenir l'aide correspondant à la commande **file save**, entrez **sscontrol he f** à la place de **sscontrol help file**.

Remarque : Les valeurs des paramètres de commande doivent être saisies en anglais. Les seules exceptions s'appliquent aux noms d'hôte (utilisés dans les commandes **cluster** et **server**) et aux noms de fichiers (utilisés dans les commandes **file**).

sscontrol advisor — Contrôle du conseiller



connecttimeout

Permet de définir le délai d'attente à l'expiration duquel un signal qu'une connexion à un serveur a échoué. Pour plus d'informations, reportez-vous à la section «Délai de connexion du conseiller et délai de réception pour les serveurs» à la page 148.

nom

Nom du conseiller. Les valeurs possibles sont les suivantes : **http**, **ftp**, **ssl**, **smtp**, **imap**, **pop3**, **nntp**, **telnet**, **connect**, **ping**, **WLM** et **WTE**. Les noms des conseillers personnalisés sont au format xxxx, ADV_xxxx étant le nom de la classe mettant en oeuvre le conseiller personnalisé.

port

Numéro du port contrôlé par le conseiller.

secondes

Il s'agit d'un entier positif représentant le délai d'attente à l'expiration duquel le conseiller signale qu'une connexion à un serveur a échoué. La valeur par défaut est trois fois la valeur spécifiée pour l'intervalle du conseiller.

interval

Définit la fréquence à laquelle le conseiller demande des informations aux serveurs.

secondes

Il s'agit d'un entier positif qui représente le nombre de secondes entre les demandes envoyées aux serveurs pour connaître leurs états en cours.
Valeur par défaut : 7.

list

Affiche la liste des conseillers qui fournissent des informations au gestionnaire.

loglevel

Définit le niveau de consignation relatif à un journal de conseiller.

niveau

Valeur du niveau (0 à 5). La valeur par défaut est 1. Plus la valeur est élevée, plus la quantité d'informations consignée dans le journal du conseiller est importante. Les valeurs possibles sont les suivantes :

- 0 correspond à Aucun
- 1 correspond à Minimal
- 2 correspond à De base
- 3 correspond à Modéré
- 4 correspond à Avancé
- 5 correspond à Prolixe

.

logsize

Définit la taille maximale d'un journal de conseiller. Lorsque vous affectez une taille maximale au fichier journal, celui-ci fonctionne en boucle, c'est-à-dire que lorsqu'il atteint la taille indiquée, les nouvelles entrées sont écrites à partir du haut du fichier et remplacent les entrées existantes. La valeur indiquée par logsize ne peut pas être inférieure à la taille actuelle du fichier journal. Les entrées du journal sont horodatées, ce qui permet de déterminer l'ordre dans lequel elles ont été enregistrées. Plus le niveau de journalisation est élevé, plus la taille du journal doit être choisie avec soin car l'espace peut être saturé rapidement.

taille | unlimited

Taille maximale (en octets) du fichier journal du conseiller. Vous pouvez indiquer un nombre positif supérieur à zéro, ou **unlimited**. Il se peut que le fichier journal n'atteigne pas la taille maximale exacte avant le remplacement des entrées existantes, car la taille des entrées de journal elles-mêmes varie. La valeur par défaut est 1 Mo.

receivetimeout

Permet de définir le délai à l'expiration duquel un conseiller signale que la réception d'un envoi provenant d'un serveur a échoué. Pour plus d'informations, reportez-vous à la section «Délai de connexion du conseiller et délai de réception pour les serveurs» à la page 148.

secondes

Il s'agit d'un entier positif qui représente le délai en secondes à l'expiration duquel le conseiller signale que la réception d'un envoi provenant d'un serveur a échoué. La valeur par défaut est trois fois la valeur spécifiée pour l'intervalle du conseiller.

report

Affiche un rapport sur l'état du conseiller.

start

Lance le conseiller. Il existe des conseillers pour chaque protocole. Les ports par défaut sont les suivants :

Nom du conseiller	Protocole	Port
Connect	Non disp.	Défini par l'utilisateur
db2	privé	50000
ftp	FTP	21
http	HTTP	80
imap	IMAP	143
nntp	NNTP	119
PING	PING	0
pop3	POP3	110
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23

nom

Indique le nom du conseiller.

nom_site:port

Le nom de site est facultatif dans les commandes du conseiller, mais la valeur de port est requise. Par défaut, le conseiller démarre sur tous les sites disponibles configurés. Si vous indiquez un nom de site, le conseiller démarre uniquement sur le site précisé. Les noms de site supplémentaires sont séparés par le signe plus (+).

fichier journal

Nom du fichier dans lequel les données de gestion sont consignées. Chaque enregistrement du journal est horodaté.

Le fichier par défaut est *nom_conseiller_port.log*, par exemple, **http_80.log**. Pour changer le répertoire dans lequel les fichiers journaux seront enregistrés, reportez-vous à la section «Modification des chemins des fichiers journaux» à la page 216.

Vous ne pouvez lancer qu'un conseiller par nom de site.

status

Affiche l'état et les valeurs par défaut en cours pour toutes les valeurs globales d'un conseiller.

stop

Arrête le conseiller.

timeout

Définit le nombre de secondes pendant lesquelles le gestionnaire considère que les informations provenant du conseiller sont valides. Si le gestionnaire considère que les informations du conseiller sont antérieures à ce délai, il n'utilise pas ces informations pour déterminer les pondérations relatives aux serveurs sur le port contrôlé par le conseiller. Il est fait exception à ce délai lorsque le conseiller a informé le gestionnaire qu'un serveur spécifique est hors service. Le gestionnaire utilise ces informations relatives au serveur même après le dépassement du délai imparti pour les informations du conseiller.

secondes

Nombre positif représentant le nombre de secondes, ou **Unlimited**. La valeur par défaut est unlimited.

version

Affiche la version en cours du conseiller.

Exemples

- Pour définir le délai d'attente (30 secondes) à l'expiration duquel un conseiller HTTP (pour le port 80) signale qu'une connexion à un serveur a échoué, entrez :

```
sscontrol advisor  
connecttimeout http 80 30
```

- Pour définir un intervalle de 6 secondes pour le conseiller FTP (pour le port 21), entrez :

```
sscontrol advisor interval ftp 21 6
```

- Pour afficher la liste des conseillers qui fournissent des informations au gestionnaire, entrez :

```
sscontrol advisor list
```

Cette commande génère des résultats similaires à l'exemple suivant :

ADVISOR	SITENAME:PORT	TIMEOUT
http	80	unlimited
ftp	21	unlimited

- Pour attribuer la valeur 0 au niveau de consignation du journal du conseiller http pour le site monSite afin d'optimiser les performances, entrez :

```
sscontrol advisor loglevel http monSite:80 0
```

- Pour attribuer la valeur 5000 octets à la taille du journal du conseiller ftp pour le site monSite, entrez :

```
sscontrol  
advisor logsize ftp monSite:21 5000
```


- Pour définir le délai d'attente (60 secondes) à l'expiration duquel un conseiller HTTP (pour le port 80) signale que la réception d'un envoi provenant d'un serveur a échoué, entrez :

```
sscontrol advisor receivetimeout http 80 60
```

- Pour afficher un rapport sur l'état du conseiller ftp (pour le port 21), entrez :

```
sscontrol advisor report ftp 21
```

Cette commande génère des résultats similaires à l'exemple suivant :

Rapport du conseiller :

Nom du conseiller http

Numéro du port 80

Nom du site monSite

Adresse du serveur 9.67.129.230

Charge 8

- Pour lancer le conseiller à l'aide du fichier ftpadv.log, entrez :

```
sscontrol advisor start ftp 21 ftpadv.log
```

- Pour afficher l'état actuel des valeurs associées au conseiller http, entrez :

```
sscontrol advisor status http 80
```

Cette commande génère des résultats similaires à l'exemple suivant :

Etat du conseiller :

Intervalle (secondes)..... 7

Délai (secondes) Illimité

Délai de connexion (secondes)..... 21

Délai de réception (secondes)..... 21

Nom du fichier journal du conseiller Http_80.log

Niveau de consignation 1

Taille maximale du journal (octets) Illimité

- Pour arrêter le conseiller http sur le port 80, entrez :

```
sscontrol advisor stop http 80
```

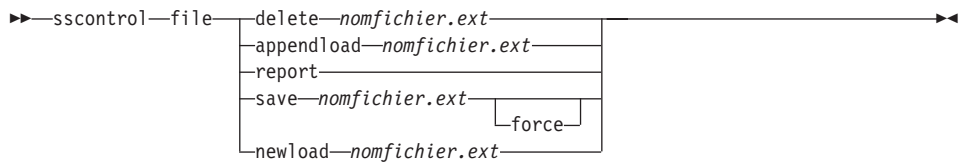
- Pour définir un délai d'attente de 5 secondes pour les informations du conseiller, entrez :

```
sscontrol advisor timeout ftp 21 5
```

- Pour rechercher le numéro de version en cours du conseiller ssl, entrez :

```
sscontrol advisor version ssl 443
```

sscontrol file — Gestion des fichiers de configuration



delete

Supprime le fichier

nomfichier.ext

Fichier de configuration.

Vous pouvez indiquer n'importe quelle extension de fichier (*.ext*) ou n'en indiquer aucune.

appendload

Ajoute un fichier de configuration à la configuration en cours et le charge dans Site Selector.

report

Génère un rapport sur les fichiers disponibles.

save

Sauvegarde la configuration en cours de Site Selector dans le fichier.

Remarque : Les fichiers sont sauvegardés dans les répertoires suivants et chargés à partir de ces mêmes répertoires :

- AIX : `/usr/lpp/nd/servers/configurations/ss`
- Linux : `/opt/nd/servers/configurations/ss`
- Solaris : `/opt/nd/servers/configurations/ss`
- Windows 2000 :

Chemin d'accès courant au répertoire d'installation —

c:\Program Files\ibm\edge\nd\servers\configurations\composant

Chemin d'accès au répertoire d'installation natif —

c:\Program Files\ibm\nd\servers\configurations\composant

force

Si vous voulez sauvegarder votre fichier dans un fichier existant du même nom, utilisez **force** pour supprimer le fichier existant avant de sauvegarder le nouveau fichier. Si vous n'utilisez pas l'option **force**, le fichier existant n'est pas remplacé.

newload

Charge un nouveau fichier de configuration dans Site Selector. Le nouveau fichier de configuration remplacera la configuration actuelle.

Exemples

- Pour supprimer un fichier, entrez :
`sscontrol file delete fichier3`

Le fichier (fichier3) est supprimé.
- Pour charger un nouveau fichier de configuration pour remplacer la configuration actuelle, entrez :
`sscontrol file newload fichier1.sv`

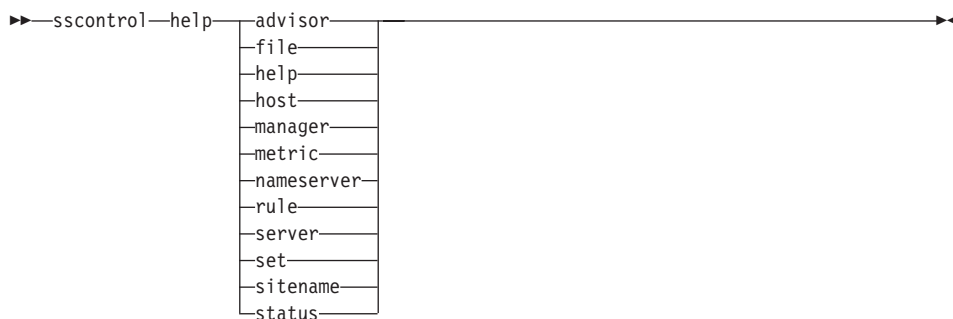
Le fichier (fichier1.sv) a été chargé dans le Dispatcher.
- Pour charger et ajouter un fichier de configuration à la configuration actuelle, entrez :
`sscontrol file appendload fichier2.sv`

Le fichier (fichier2.sv) a été ajouté à la configuration actuelle et chargé.
- Pour visualiser un rapport de vos fichiers (à savoir les fichiers que vous avez sauvegardés précédemment), entrez :
`sscontrol file report`

RAPPORT SUR LES FICHIERS :
fichier1.sauv
fichier2.sv
fichier3
- Pour sauvegarder votre configuration dans un fichier intitulé fichier3, entrez :
`sscontrol file save fichier3`

La configuration est sauvegardée dans fichier3.

sscontrol help — Affichage ou impression de l'aide sur cette commande



Exemples

- Pour obtenir l'aide sur la commande sscontrol, entrez :
sscontrol help

Cette commande génère des résultats similaires à l'exemple suivant :

ARGUMENTS DE LA COMMANDE HELP :

Syntaxe : help <option>

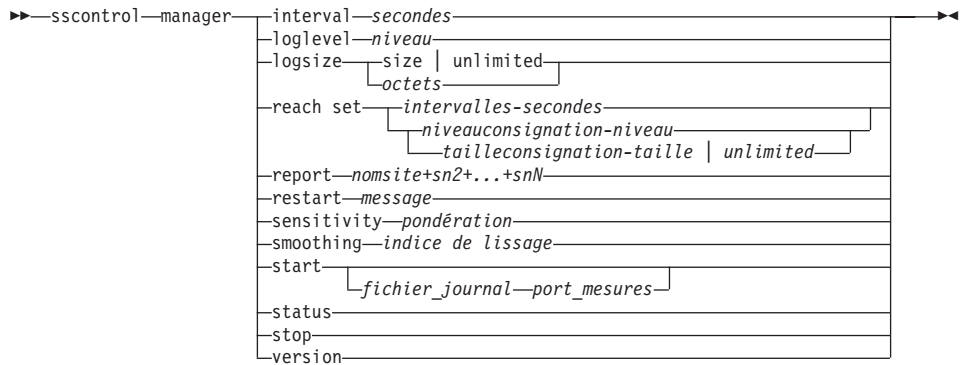
Exemple: help name

help	- Affichage des informations d'aide
advisor	- Aide sur la commande advisor
file	- Aide sur la commande file
host	- Aide sur la commande host
manager	- Aide sur la commande manager
metric	- Aide sur la commande metric
sitename	- Aide sur la commande sitename
nameserver	- Aide sur la commande nameserver
server	- Aide sur la commande server
subagent	- Aide sur la commande subagent
set	- Aide sur la commande set
status	- Aide sur la commande status

Les paramètres entre caractères < > sont des variables.

- L'aide affiche parfois des choix de variables en utilisant le caractère | pour séparer les options disponibles :
logsize <nombre d'octets | unlimited>
- Nombre maximal d'octets à consigner dans le journal

sscontrol manager — Contrôle du gestionnaire



interval

Définit la fréquence de mise à jour, par le gestionnaire, des pondérations des serveurs.

secondes

Nombre entier positif représentant la fréquence (en secondes) de mise à jour des pondérations par le gestionnaire. Valeur par défaut : 2

loglevel

Permet de définir le niveau de consignation pour le journal du gestionnaire et le journal du contrôleur de mesures.

niveau

Valeur du niveau (0 à 5). Plus la valeur est élevée, plus la quantité des informations consignées dans le journal du gestionnaire est importante. Valeur par défaut : 1. Les valeurs possibles sont les suivantes :

- 0 correspond à Aucun
- 1 correspond à Minimal
- 2 correspond à De base
- 3 correspond à Modéré
- 4 correspond à Avancé
- 5 correspond à Prolixe

logsize

Définit la taille maximale du journal du gestionnaire. Lorsque vous attribuez une taille maximale au fichier journal, ce dernier fonctionne en boucle. Lorsque le fichier atteint la taille indiquée, les entrées suivantes sont écrites à partir du haut du fichier et remplacent les entrées existantes. La valeur indiquée par *logsize* ne peut pas être inférieure à la taille actuelle du fichier journal. Les entrées du journal sont horodatées, ce qui permet de déterminer l'ordre dans lequel elles ont été enregistrées.

Plus le niveau de journalisation est élevé, plus la taille du journal doit être choisie avec soin car l'espace peut être saturé rapidement.

octets

Taille maximale (en octets) du fichier journal du gestionnaire. Vous pouvez indiquer un nombre positif supérieur à zéro, ou **unlimited**. Il se peut que le fichier journal n'atteigne pas la taille maximale exacte avant le remplacement des entrées existantes, car la taille des entrées de journal elles-même varie. La valeur par défaut est 1 Mo.

reach set

Définit l'intervalle, le niveau de consignation et la taille du journal pour le conseiller d'accessibilité.

report

Affiche un rapport d'analyse sur les statistiques.

nom_site

Nom du site à afficher dans le rapport. Il s'agit d'un nom d'hôte ne pouvant être résolu qui sera demandé par le client. Le nom de site doit être un nom de domaine qualifié complet.

Remarque : Les noms de site supplémentaires sont séparés par le signe plus (+).

restart

Relance tous les serveurs (qui ne sont pas arrêtés) en leur affectant des valeurs de pondération normalisées (la moitié de la pondération maximale).

message

Message à consigner dans le fichier journal du gestionnaire.

sensitivity

Définit la sensibilité minimale à partir de laquelle les pondérations sont mises à jour. Cette valeur définit le moment où le gestionnaire doit modifier sa pondération pour le serveur en fonction des informations externes.

pondération

Nombre compris entre 0 et 100 indiquant le pourcentage de pondération. La valeur par défaut 5 crée une sensibilité minimale de 5%.

smoothing

Définit un indice de lissage des variations des pondérations lors de l'équilibrage de charge. Plus l'indice de lissage est élevé, moins les pondérations des serveurs varient lorsque les conditions réseau sont modifiées. Plus cet indice est faible, plus les pondérations des serveurs varient.

indice

Nombre positif en virgule flottante. Valeur par défaut : 1,5.

start

Lance le gestionnaire

fichier journal

Nom du fichier dans lequel les données de gestion sont consignées. Chaque enregistrement du journal est horodaté.

Le fichier par défaut se trouve dans le répertoire **logs**. Reportez-vous à la section «Annexe F. Exemples de fichiers de configuration» à la page 387. Pour changer le répertoire dans lequel les fichiers journaux vont être enregistrés, reportez-vous à la section «Modification des chemins des fichiers journaux» à la page 216.

port_mesures

Port sur lequel Metric Server renvoie l'état des charges du système. Si vous indiquez un port de décompte, vous devez spécifier un nom de fichier journal. Le port de décompte par défaut est 10004.

status

Affiche l'état et les valeurs par défaut en cours pour toutes les valeurs globales du gestionnaire.

stop

Arrête le gestionnaire.

version

Affiche la version en cours du gestionnaire.

Exemples

- Pour définir un délai de 5 secondes entre les mises à jour du gestionnaire, entrez :
`sscontrol manager interval 5`
- Pour affecter au niveau de journalisation la valeur de 0, afin d'optimiser les performances, entrez :
`sscontrol manager loglevel 0`
- Pour définir une taille de journal du gestionnaire de 1 000 000 octets, entrez :
`sscontrol manager logsize 1000000`
- Pour obtenir une analyse statistique du gestionnaire, entrez :
`sscontrol manager report`

Cette commande génère des résultats similaires à l'exemple suivant :

SERVEUR	ETAT
9.67.129.221	ACTIF
9.67.129.213	ACTIF
9.67.134.223	ACTIF

LEGENDE ETAT GESTIONNAIRE

CPU	Charge de la CPU
MEM	Charge de la mémoire
SYS	Mesure du système
NOW	Pondération actuelle
NEW	Nouvelle pondération
WT	Pondération

monSite	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				
TOTAUX :	10 10 -1 -1 -1 0				

ADVISOR	SITENAME:PORT	TIMEOUT
http	80	unlimited

- Pour relancer tous les serveurs en leur affectant des pondérations normalisées et pour consigner un message dans le fichier journal du gestionnaire, entrez :
sscontrol manager restart Relance du gestionnaire pour mettre à jour

Cette commande génère des résultats similaires à l'exemple suivant :

320-14:04:54

Relance du gestionnaire pour mettre à jour le code

- Pour affecter la valeur 10 à la sensibilité aux modifications de pondération, entrez :
sscontrol manager sensitivity 10
- Pour affecter la valeur 2 à l'indice de lissage, entrez :
sscontrol manager smoothing 2.0

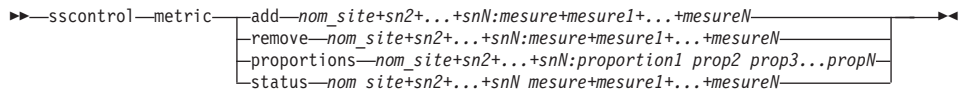
- Pour lancer le gestionnaire et indiquer le fichier journal nommé ndmgr.log (les chemins ne peuvent pas être définis), entrez :
sscontrol manager start ndmgr.log
- Pour afficher l'état en cours des valeurs associées au gestionnaire, entrez :
sscontrol manager status

Cette commande génère des résultats similaires à l'exemple suivant :

```
Etat du
gestionnaire :
=====
Port de mesures..... 10004
Nom du fichier journal du gestionnaire..... manager.log
Niveau de consignation du gestionnaire..... 1
Taille maxi du journal du gestionnaire (octets)... unlimited
Niveau de sensibilité..... 5
Indice de lissage..... 1.5
Intervalle de mise à jour (secondes)..... 2
Cycle de mise à jour des pondérations..... 2
Niveau du journal de contacts..... 1
Taille maximale du journal de contact (octets)... unlimited
Intervalle de mise à jour des contacts (secondes). 7
```

- Pour arrêter le gestionnaire, entrez :
sscontrol manager stop
- Pour afficher le numéro de version en cours du gestionnaire, entrez :
sscontrol manager version

sscontrol metric — Configuration des mesures du système



add

Permet d'ajouter la mesure spécifiée.

nom_site

Nom du site configuré. Les noms de site supplémentaires sont séparés par le signe plus (+).

measure

Nom de la mesure du système. Il doit s'agir du nom d'un fichier exécutable ou d'un fichier script du répertoire script de Metric Server.

remove

Supprime la mesure spécifiée.

proportions

Ce paramètre détermine la correspondance des mesures entre elles lorsqu'elles sont regroupées en une seule charge système pour un serveur.

status

Affiche les valeurs serveur actuelles de cette mesure.

Exemples

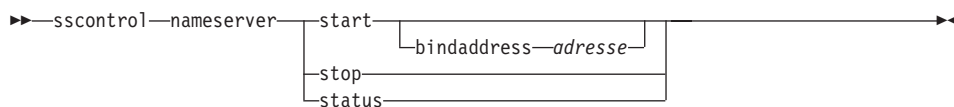
- Pour ajouter une mesure de système, entrez :
`sscontrol metric add sitel:metric1`
- Pour définir les proportions pour un nom de site disposant de deux mesures de système, entrez :
`sscontrol metric proportions sitel 0 100`
- Pour afficher l'état en cours des valeurs associées à la mesure spécifiée, entrez :
`sscontrol metric status sitel:metric1`

Cette commande génère des résultats similaires à l'exemple suivant :

Etat des mesures :

```
Nom du site..... sitel
Nom de la mesure..... metric1
Proportion de la mesure..... 50
  Serveur ..... 9.37.56.100
Données de mesure... -1
```

sscontrol nameserver — Contrôle de NameServer



start

Démarre le serveur de noms

bindaddress

Démarre le serveur de noms lié à l'adresse indiquée. Le serveur de noms ne répond qu'aux demandes destinées à cette adresse.

adresse

Adresse (IP ou symbolique) configurée sur le dispositif Site Selector.

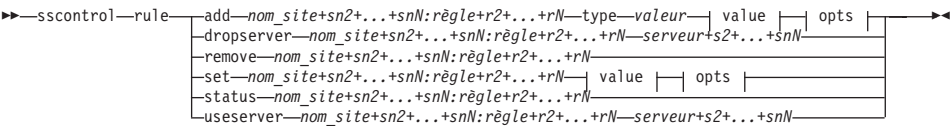
stop

Arrête le serveur de noms

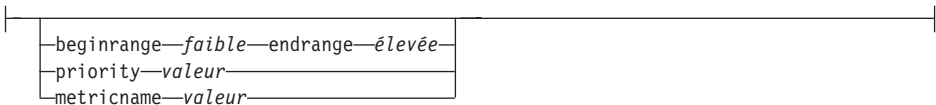
status

Affiche l'état du serveur de noms

sscontrol rule — Configuration des règles



opts :



add

Ajoute cette règle à un nom de site.

nom_site

Nom d'hôte ne pouvant être résolu qui sera demandé par le client. Le nom de site doit être un nom de domaine qualifié complet. Les noms de site supplémentaires sont séparés par le signe plus (+).

règle

Nom choisi pour la règle. Ce nom peut contenir tout caractère alphanumérique, des traits de soulignement, des traits d'union ou des points. Il peut comporter de 1 à 20 caractères, et ne doit contenir aucun espace.

Remarque : Chaque règle supplémentaire doit être séparée de la précédente par le signe plus (+).

type

Type de règle

type

Les différents *types* de règles possibles sont les suivants :

ip La règle est définie en fonction de l'adresse IP du client.

metricall

La règle est basée sur la valeur de mesure actuelle pour tous les serveurs de l'ensemble de serveurs.

metricavg

La règle est basée sur la moyenne des valeurs de mesure actuelles pour tous les serveurs de l'ensemble de serveurs.

time La règle est définie en fonction de l'heure.

true Cette règle est toujours vraie. Considérez-la comme une instruction else en logique de programmation.

beginrange

Valeur de début de la fourchette utilisée pour déterminer si la règle est vraie.

faible

Dépend du type de règle. Le type de valeur et les valeurs par défaut sont précisés ci-après par type de règle :

ip Adresse du client sous forme de nom symbolique ou en notation décimale à point. La valeur par défaut est 0.0.0.0.

time Entier. La valeur par défaut est 0 (minuit).

metricall

Entier. Valeur par défaut : 100.

metricavg

Entier. Valeur par défaut : 100.

endrange

Valeur de fin de la fourchette utilisée pour déterminer si la règle est vraie.

élevée

Dépend du type de règle. Le type de valeur et les valeurs par défaut sont précisés ci-après par type de règle :

ip Adresse du client sous forme de nom symbolique ou en notation décimale à point. La valeur par défaut est 255.255.255.254.

time Entier. La valeur par défaut est 24 (minuit).

Remarque : Lors de la définition des intervalles de temps (début et fin d'une fourchette horaire), notez que chaque valeur doit être un entier représentant seulement l'heure. Les subdivisions de l'heure ne sont pas indiquées. Pour cette raison, pour indiquer une heure, par exemple entre 3 h et 4 h du matin, attribuez la valeur 3 à beginrange (début) et 3 à endrange (fin). Cela signifiera toutes les minutes comprises entre 3 h et 3 h 59. Si vous indiquez la valeur 3 pour le paramètre beginrange et la valeur 4 pour le paramètre endrange, vous couvrirez la période de deux heures allant de 3 h à 4 h 59.

metricall

Entier. La valeur par défaut est 2 à la puissance 32 moins 1.

metricavg

Entier. La valeur par défaut est 2 à la puissance 32 moins 1.

priority

L'ordre suivant lequel les règles sont consultées.

niveau

Entier. Si vous ne spécifiez pas la priorité de la première règle que vous ajoutez, Site Selector lui affectera par défaut la valeur 1. Une règle ajoutée par la suite se verra affecter par défaut une priorité égale à la priorité la plus basse existante + 10. Supposons que vous ayez une règle dont la priorité est 30. Vous ajoutez une nouvelle règle et définissez sa priorité à 25 (priorité *supérieure* à 30). Vous ajoutez ensuite une troisième règle, sans lui affecter de priorité. La priorité de la troisième règle sera de 40 (30 + 10).

metricname

Nom de la mesure calculée pour une règle

dropserver

Supprime un serveur d'un jeu de règles.

serveur

Adresse IP de la machine serveur TCP sous forme de nom symbolique ou en notation décimale à point.

Remarque : Les noms de site supplémentaires sont séparés par le signe plus (+).

remove

Supprime une ou plusieurs règles séparées entre elles par des signes plus.

set

Définit les valeurs de cette règle.

status

Affiche toutes les valeurs d'une ou de plusieurs règles.

useserver

Insère un serveur dans un jeu de règles.

Exemples

- Pour ajouter une règle qui sera toujours vraie, ne spécifiez pas de valeur de début ni de fin. Entrez :

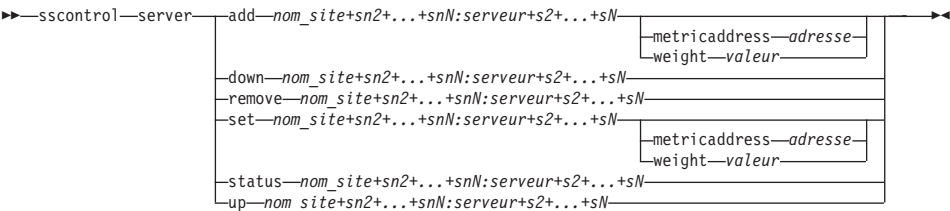
```
sscontrol  
rule add sitename:rulename type true priority 100
```
- Pour créer une règle qui interdit l'accès à une plage d'adresses IP, en l'occurrence celles qui commencent par "9:", entrez :

```
sscontrol rule add sitename:rulename type ip b 9.0.0.0 e 9.255.255.255
```

- Pour créer une règle qui limitera l'utilisation d'un serveur donné de 11:00 à 15:00, entrez :

```
sscontrol rule add sitename:rulename type time beginrange 11 endrange 14  
sscontrol rule useserver sitename:rulename server05
```

sscontrol server — Configuration des serveurs



add
Permet d'ajouter ce serveur.

nom_site
Nom d'hôte ne pouvant être résolu demandé par le client. Le nom de site doit être un nom de domaine qualifié complet. Les noms de site supplémentaires sont séparés par le signe plus (+).

serveur
Adresse IP de la machine serveur TCP sous forme de nom symbolique ou en notation décimale à point.

Remarque : Chaque serveur supplémentaire doit être séparé du précédent par le signe plus (+).

metricaddress
Adresse du serveur de mesures

adresse
Adresse du serveur sous forme d'adresse symbolique ou en notation décimale à points.

weight
Nombre compris dans la fourchette 0–100 (mais qui ne doit pas dépasser la valeur de limite de pondération maximale pour le nom de site indiqué) représentant la pondération pour ce serveur. L'affectation de la valeur zéro à la pondération empêche l'envoi de nouvelles demandes au serveur. La valeur par défaut correspond à la moitié de la pondération maximale pour le nom de site indiqué. Si le gestionnaire est en cours d'exécution, ce paramètre est rapidement remplacé.

valeur
Valeur de pondération du serveur

down
Marque ce serveur comme étant arrêté. Empêche la transmission de toute autre demande à ce serveur.

remove

Permet de supprimer ce serveur.

set

Permet de définir des valeurs pour ce serveur.

status

Affiche l'état des serveurs.

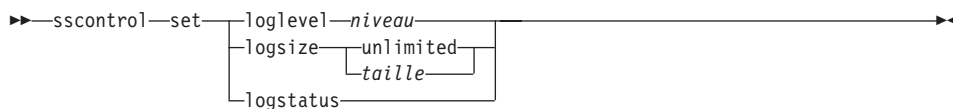
up

Marque ce serveur comme étant activé. Site Selector envoie désormais de nouvelles demandes à ce serveur.

Exemples

- Pour ajouter le serveur avec l'adresse 27.65.89.42 à un site dont le nom est site1, entrez :
`sscontrol server add site1:27.65.89.42`
- Pour marquer le serveur 27.65.89.42 comme étant arrêté, entrez :
`sscontrol server down site1:27.65.89.42`
- Pour supprimer le serveur avec l'adresse pour les sites, entrez :
`sscontrol server remove :27.65.89.42`
- Pour marquer le serveur 27.65.89.42 comme étant activé, entrez :
`sscontrol server up site1:27.65.89.42`

sscontrol set — Configuration du journal du serveur



loglevel

Niveau de journalisation de ses activités par le serveur ssserver.

niveau

La valeur par défaut de **loglevel** est 0. Les valeurs possibles sont les suivantes :

- 0 correspond à Aucun
- 1 correspond à Minimal
- 2 correspond à De base
- 3 correspond à Modéré
- 4 correspond à Avancé
- 5 correspond à Prolixe

logsize

Nombre maximal d’octets à consigner dans le fichier journal.

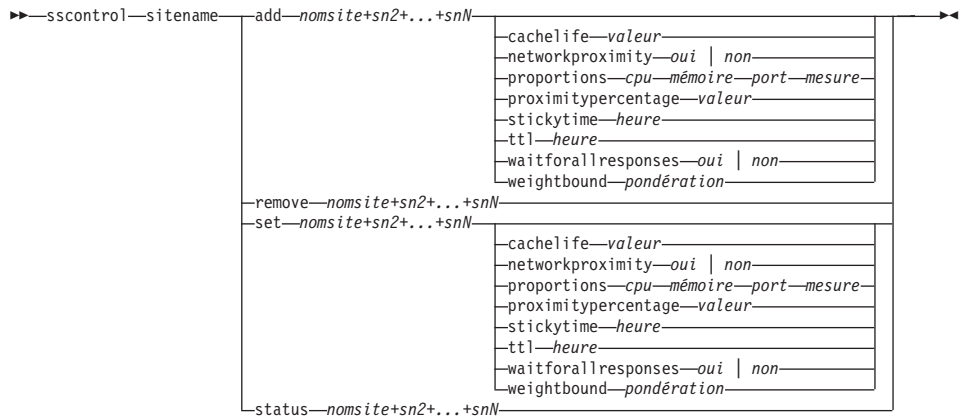
taille

La taille de fichier journal par défaut est 1 Mo.

logstatus

Affiche les paramètres du journal du serveur (niveau de journalisation et taille du journal).

sscontrol sitename — Configuration d'un nom de site



add

Ajoute un nouveau nom de site

nom_site

Nom d'hôte ne pouvant être résolu, demandé par le client. Les noms de site supplémentaires sont séparés par le signe plus (+).

cachelife

Période pendant laquelle une réponse de proximité reste valide et enregistrée dans la mémoire cache. La valeur par défaut est 1800. Pour de plus amples informations, reportez-vous à «Utilisation de la fonction de proximité réseau (Network Proximity)» à la page 112.

valeur

Nombre positif représentant la période (en nombre de secondes) pendant laquelle une réponse de proximité reste valide et enregistrée dans la mémoire cache.

networkproximity

Détermine la proximité du réseau de chaque serveur par rapport au client demandeur. Tient compte de cette réponse de proximité pour la décision d'équilibrage de charge. Active ou désactive la fonction de proximité. Pour de plus amples informations, reportez-vous à «Utilisation de la fonction de proximité réseau (Network Proximity)» à la page 112.

valeur

Les options sont oui ou non. La valeur par défaut est non qui signifie que la fonction de proximité du réseau est désactivée.

proportions

Définit le niveau d'importance de la CPU, de la mémoire, du port (donnée provenant des conseillers) et des mesures système pour le serveur de

mesures. Les proportions sont utilisées par le gestionnaire pour définir les pondérations du serveur. Chacune de ces valeurs est exprimée en pourcentage du total et, par conséquent, leur somme doit toujours être égale à 100.

cpu Pourcentage de l'unité centrale utilisé sur chaque serveur avec équilibrage de charge (donnée provenant de l'agent Metric Server).

mémoire Pourcentage de mémoire utilisé (donnée provenant de l'agent Metric Server) sur chaque serveur avec équilibrage de charge.

port Donnée provenant des conseillers en mode écoute sur ce port.

système Donnée provenant de Metric Server.

proximitypercentage

Définit l'importance de la réponse de proximité, par rapport au bon fonctionnement du serveur (pondération du gestionnaire). Pour de plus amples informations, reportez-vous à la section «Utilisation de la fonction de proximité réseau (Network Proximity)» à la page 112.

valeur

Valeur par défaut : 50

stickytime

Délai pendant lequel un client va recevoir l'ID serveur renvoyé pour la première demande. Le délai de maintien de routage par défaut est 0 (le nom de site n'est pas conservé).

heure

Nombre entier positif différent de zéro, représentant la période (en nombre de secondes) pendant laquelle le client reçoit l'ID serveur renvoyé pour la première demande.

ttl Définit la durée de vie. Indique la période pendant laquelle la réponse résolue reste en mémoire cache sur un autre serveur de noms. La valeur par défaut est 5.

valeur

Nombre positif représentant la période (en nombre de secondes) pendant laquelle la réponse résolue reste en mémoire cache sur le serveur de noms.

waitforallresponses

Permet de définir s'il est nécessaire d'attendre toutes les réponses de proximité des serveurs avant de répondre à la demande du client. Pour de plus amples informations, reportez-vous à «Utilisation de la fonction de proximité réseau (Network Proximity)» à la page 112.

valeur

Les valeurs possibles sont oui ou non. La valeur par défaut est oui.

weightbound

Nombre correspondant à la pondération maximale pouvant être définie pour les serveurs sur ce site. La valeur de limite de pondération définie pour le nom de site peut être remplacée pour des serveurs individuels à l'aide de la valeur de **pondération du serveur**. La valeur de limite de pondération par défaut pour le nom de site est égale à 20.

pondération

Valeur de la limite de pondération

set

Définit les propriétés du nom de site.

remove

Supprime le nom de site.

status

Affiche l'état en cours d'un nom de site spécifique.

Exemples

- Pour ajouter un nom de site, entrez :
`sscontrol sitename add 130.40.52.153`
- Pour activer la fonction de proximité du réseau, entrez :
`sscontrol sitename set monSite networkproximity yes`
- Pour définir une durée de vie de 1900000 secondes pour la mémoire cache, entrez :
`sscontrol sitename set monSite cachelife 1900000`
- Pour définir un pourcentage de proximité de 45, entrez :
`sscontrol sitename set monSite proximitypercentage 45`
- Pour empêcher un nom de site d'attendre toutes les réponses avant de répondre, entrez :
`sscontrol sitename set monSite waitforallresponses no`
- Pour définir une durée de vie de 7 secondes, entrez :
`sscontrol sitename set monSite ttl 7`
- Pour définir le niveau d'importance pour CpuLoad, MemLoad, Port et System Metric, entrez respectivement, :
`sscontrol sitename set monSite proportions 50 48 1 1`
- Pour supprimer un nom de site, entrez :
`sscontrol sitename remove 130.40.52.153`
- Pour afficher l'état du nom de site monSite, entrez :
`sscontrol sitename
status monSite`

Cette commande génère des résultats similaires à l'exemple suivant :

```
Etat
SiteName :
-----
SiteName ..... monSite
WeightBound ..... 20
TTL ..... 5
StickyTime ..... 0
Nombre de serveurs..... 1
Proportion accordée à CpuLoad ..... 49
Proportion accordée à MemLoad..... 50
Proportion accordée au port..... 1
Proportion accordée aux mesures du système... 0
Conseiller fonctionnant sur le port..... 80
Utilisation de la fonction de proximité..... N
```

sscontrol status — Affiche si le gestionnaire et les conseillers sont en cours d'exécution

»—sscontrol—status—«

Exemples

- Pour visualiser les programmes en cours d'exécution, entrez :
sscontrol status

Cette commande génère des résultats similaires à l'exemple suivant :

```
      NameServer
a été lancé.
      Le gestionnaire (manager) a été lancé
-----
| ADVISOR | SITENAME:PORT | TIMEOUT |
-----
|   http |           80 | unlimited |
-----
```

Annexe E. Guide des commandes Consultant for Cisco CSS Switches

La présente annexe explique comment utiliser les commandes **lbcontrol** pour Consultant for Cisco CSS Switches :

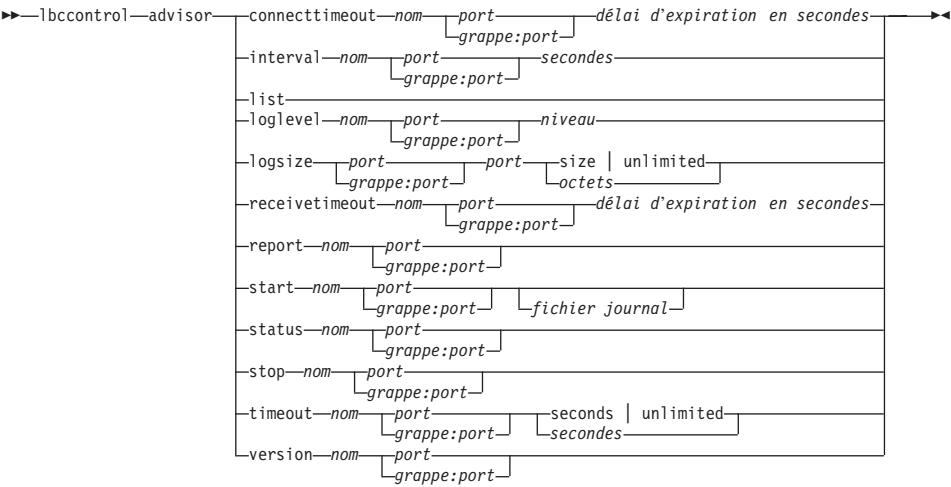
- «**lbcontrol advisor** — Contrôle du conseiller» à la page 358
- «**lbcontrol cluster** — Configuration des grappes» à la page 363
- «**lbcontrol executor** — Contrôle de l'exécuteur» à la page 365
- «**lbcontrol file** — Gestion des fichiers de configuration» à la page 367
- «**lbcontrol help** — Affichage ou impression de l'aide relative à cette commande» à la page 369
- «**lbcontrol host** — Configuration d'une machine éloignée» à la page 370
- «**lbcontrol log** — Contrôle du fichier journal binaire» à la page 371
- «**lbcontrol manager** — Contrôle du gestionnaire» à la page 372
- «**lbcontrol metric** — Configuration des mesures du système» à la page 378
- «**lbcontrol port** — Configuration des ports» à la page 380
- «**lbcontrol server** — Configuration des serveurs» à la page 382
- «**lbcontrol set** — Configuration du journal du serveur» à la page 384
- «**lbcontrol status** — Indique par affichage si le gestionnaire et les conseillers sont en cours d'exécution» à la page 385

Vous pouvez entrer une version abrégée des paramètres de commandes **lbcontrol**. Il suffit d'entrer les lettres uniques des paramètres. Par exemple, pour l'aide correspondant à la commande **file save**, entrez **lbcontrol he f** à la place de **lbcontrol help file**.

Le préfixe "lbc" signifie load-balancing consultant (consultant d'équilibrage de la charge).

Remarque : Les valeurs des paramètres de commande doivent être saisies en anglais. Les seules exceptions s'appliquent aux noms d'hôte (utilisés dans les commandes **cluster** et **server**) et aux noms de fichiers (utilisés dans les commandes **file**).

lbccontrol advisor — Contrôle du conseiller



connecttimeout

Permet de définir la période pendant laquelle un conseiller attend avant de signaler qu’une connexion à un serveur a échoué. Pour plus d’informations, reportez-vous à la section «Délai de connexion du conseiller et délai de réception pour les serveurs» à la page 148.

nom

Nom du conseiller. Les valeurs possibles sont les suivantes : **http**, **ftp**, **ssl**, **smtp**, **imap**, **pop3**, **nntp**, **telnet**, **connect**, **ping** et **WTE**. Le nom des conseillers personnalisés est au format `xxxx`, `ADV_xxxx` étant le nom de la classe qui met en oeuvre le conseiller personnalisé.

port

Numéro du port contrôlé par le conseiller.

délai d'expiration en secondes

Il s’agit d’un entier positif représentant la période en secondes pendant laquelle le conseiller attend avant de signaler qu’une connexion à un serveur a échoué. La valeur par défaut est trois fois la valeur spécifiée pour l’intervalle du conseiller.

interval

Définit la fréquence à laquelle le conseiller demande des informations aux serveurs.

secondes

Il s’agit d’un entier positif qui représente le nombre de secondes entre les demandes envoyées aux serveurs pour connaître leurs états en cours. La valeur par défaut est 15.

list

Affiche la liste des conseillers qui fournissent des informations au gestionnaire.

loglevel

Définit le niveau de consignation relatif à un journal de conseiller.

niveau

Numéro du niveau (0 à 5). La valeur par défaut est 1. Plus le numéro est élevé, plus la quantité d'informations consignée dans le journal du conseiller est importante. Les valeurs possibles sont les suivantes : 0 (Aucun), 1 (Minimal), 2 (De base), 3 (Modéré), 4 (Avancé), 5 (Prolixe).

logsize

Définit la taille maximale d'un journal de conseiller. Lorsque vous attribuez une taille maximale au fichier journal, ce dernier est traité par procédé de boucle. Lorsque le fichier atteint la taille indiquée, les entrées suivantes sont écrites à partir du haut du fichier pour écraser les entrées de journal précédentes. La taille du journal ne peut pas être inférieure à la taille actuelle du journal. Les entrées du journal sont horodatées, ce qui permet de déterminer l'ordre dans lequel elles ont été enregistrées. Plus le niveau de journalisation est élevé, plus la taille du journal doit être choisie attentivement car l'espace peut être saturé rapidement.

nombre d'enregistrements

Taille maximale (en octets) du fichier journal du conseiller. Vous pouvez indiquer un nombre positif supérieur à zéro, ou le mot **unlimited**. Il se peut que le fichier journal n'atteigne pas la taille maximale exacte avant le remplacement des entrées existantes, car la taille des entrées de journal elles-même varie. La valeur par défaut est 1 Mo.

receivetimeout

Permet de définir le délai à l'expiration duquel un conseiller signale que la réception d'un envoi provenant d'un serveur a échoué. Pour plus d'informations, reportez-vous à la section «Délai de connexion du conseiller et délai de réception pour les serveurs» à la page 148.

délai d'expiration en secondes

Il s'agit d'un entier positif qui représente le délai en secondes à l'expiration duquel le conseiller signale que la réception d'un envoi provenant d'un serveur a échoué. La valeur par défaut est trois fois la valeur spécifiée pour l'intervalle du conseiller.

report

Affiche un rapport sur l'état du conseiller.

start

Lance le conseiller. Il existe des conseillers pour chaque protocole. Les ports par défaut sont les suivants :

Nom du conseiller	Protocole	Port
connect	ICMP	12345
db2	privé	50000
ftp	FTP	21
http	HTTP	80
ibmproxy	HTTP (via Caching Proxy)	80
imap	IMAP	143
nntp	NNTP	119
ping	PING	0
pop3	POP3	110
smtp	SMTP	25
ssl	SSL	443
telnet	Telnet	23
WLM	privé	10007

Remarque : Le conseiller FTP doit est activé uniquement pour le port de contrôle FTP (21). Ne lancez pas un conseiller FTP sur le port de données FTP (20).

fichier journal

Nom du fichier dans lequel les données de gestion sont consignées. Chaque enregistrement est horodaté.

Le fichier par défaut se présente sous la forme *nomconseiller_port.log*, par exemple, **http_80.log**. Pour changer le répertoire dans lequel les fichiers journaux vont être stockés, reportez-vous à la section «Modification des chemins des fichiers journaux» à la page 216.

Définissez les proportions du gestionnaire pour vous assurer que les informations du conseiller sont utilisées.

status

Affiche l'état en cours de toutes les valeurs globales du conseiller ainsi que leurs valeurs par défaut.

stop

Arrête le conseiller.

timeout

Définit le nombre de secondes pendant lesquelles le gestionnaire considère que les informations provenant du conseiller sont valides. Si le gestionnaire considère que les informations du conseiller sont antérieures à ce délai, il n'utilise pas ces informations pour déterminer les pondérations relatives aux serveurs sur le port contrôlé par le serveur. Il est fait exception à ce délai lorsque le conseiller informe le gestionnaire qu'un serveur spécifique est hors service. Le gestionnaire utilise ces informations relatives au serveur même après le dépassement du délai imparti pour les informations du conseiller.

secondes

Nombre positif représentant le nombre de secondes, ou le mot **unlimited**. La valeur par défaut est unlimited.

version

Affiche la version en cours du conseiller.

Exemples

- Pour définir le délai d'attente (30 secondes) à l'expiration duquel un conseiller HTTP (pour le port 80) signale qu'une connexion à un serveur a échoué, entrez :
`lbcontrol advisor connecttimeout http 80 30`
- Pour définir un intervalle de 6 secondes pour le conseiller FTP (pour le port 21), entrez :
`lbcontrol advisor interval ftp 21 6`
- Pour afficher la liste des conseillers qui fournissent des informations au gestionnaire, entrez :
`lbcontrol advisor list`

Cette commande génère des résultats similaires à l'exemple suivant :

ADVISOR	PORT	TIMEOUT	

http	80	unlimited	
ftp	21	unlimited	

- Pour remplacer le niveau de consignation du journal du conseiller par 0, afin d'optimiser les performances, entrez :
`lbcontrol advisor loglevel http 80 0`
- Pour remplacer la taille du journal du conseiller par 5000 octets, entrez :
`lbcontrol advisor logsize ftp 21 5000`

- Pour définir la durée (60 secondes) pendant laquelle un conseiller HTTP (pour le port 80) attend avant de signaler qu'une réception d'un envoi provenant d'un serveur a échoué, entrez :

```
lbcontrol advisor receivetimeout http 80 60
```

- Pour afficher un rapport sur l'état du conseiller ftp (pour le port 21), entrez :

```
lbcontrol advisor report ftp 21
```

Cette commande génère des résultats similaires à l'exemple suivant :

Rapport du conseiller :

Nom du conseiller Ftp

Numéro du port 21

Adresse de grappe 9.67.131.18

Adresse du serveur 9.67.129.230

Charge 8

Adresse de grappe 9.67.131.18

Adresse du serveur 9.67.131.215

Charge -1

- Pour lancer le conseiller à l'aide du fichier ftpadv.log, entrez :

```
lbcontrol advisor start ftp 21 ftpadv.log
```

- Pour afficher l'état actuel des valeurs associées au conseiller http :

```
lbcontrol advisor status http 80
```

Cette commande génère des résultats similaires à l'exemple suivant :

Etat du conseiller (advisor) :

Intervalle (secondes) 15

Délai d'expiration (secondes) Illimité

Délai d'expiration de connexion (secondes)... 21

Délai d'expiration de réception (secondes)... 21

Nom du fichier journal du conseiller Http_80.log

Niveau de consignation 1

Taille maximale du journal (octets) Illimité

- Pour arrêter le conseiller http au port 80, entrez :

```
lbcontrol advisor stop http 80
```

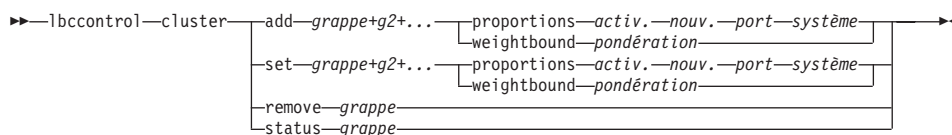
- Pour affecter la valeur de 5 secondes au délai d'attente des informations du conseiller, entrez :

```
lbcontrol advisor timeout ftp 21 5
```

- Pour rechercher le numéro de version en cours du conseiller ssl, entrez :

```
lbcontrol advisor version ssl 443
```

lbcontrol cluster — Configuration des grappes



add

Ajoute cette grappe. Vous devez définir au moins une grappe.

weightbound

Définit la pondération maximale des serveurs sur ce port. Cette option a une incidence sur le degré de différence possible entre le nombre de demandes transmises par Cisco CSS Switch à chaque serveur. La valeur par défaut est 10.

pondération

Valeur de la limite de pondération.

set

Définit les caractéristiques de la grappe.

proportions

Définit le niveau d'importance des connexions actives (*activ.*), des nouvelles connexions (*nouv.*), des informations en provenance des conseillers (*port*) et des informations provenant du Metric Server (*système*) permettant au gestionnaire de définir les pondérations des serveurs. Chacune des valeurs décrites ci-après est exprimée en pourcentage de la valeur totale, et par conséquent, leur somme est toujours égale à 100. Pour plus d'informations, reportez-vous à la section «Proportion de l'importance accordée aux données d'état» à la page 141.

activ.

Nombre compris entre 0 et 100 représentant la proportion de pondération à attribuer aux nouvelles connexions. Valeur par défaut : 50.

nouv.

Nombre compris entre 0 et 100 représentant la proportion de pondération à attribuer aux nouvelles connexions. Valeur par défaut : 50.

port

Nombre compris entre 0 et 100 représentant la proportion de pondération à attribuer aux informations provenant des conseillers. Valeur par défaut : 0.

système

Nombre compris entre 0 et 100 représentant la proportion de pondérations à attribuer aux informations provenant des mesures système. La valeur par défaut est 0.

remove

Supprime cette grappe.

status

Affiche l'état en cours d'une grappe spécifique.

Exemples

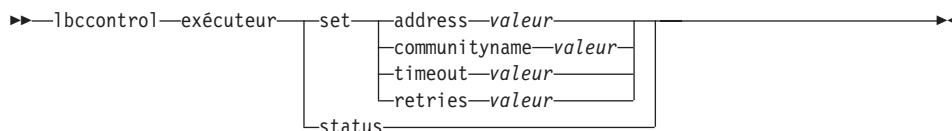
- Pour ajouter l'adresse de grappe 130.40.52.153, entrez :
`lbcontrol cluster add 130.40.52.153`
- Pour supprimer l'adresse de grappe 130.40.52.153, entrez :
`lbcontrol cluster remove 130.40.52.153`
- Pour définir l'importance relative affectée aux données reçues par le gestionnaire :
`lbcontrol cluster proportions 60 35 5 0`
- Pour visualiser l'état de l'adresse de grappe 9.67.131.167, entrez :
`lbcontrol cluster status 9.67.131.167`

Cette commande génère des résultats similaire à l'exemple suivant :

Etat de la grappe (cluster) :

```
-----  
Adresse ..... 9.67.131.167  
Nombre de ports cibles ..... 3  
Limite de pondération par défaut du port ..... 10  
Proportion accordée aux connexions actives .. 49  
Proportion accordée aux nouvelles connexions ..... 49  
Proportion accordée aux connexions spécifiques du port ... 2  
Proportion accordée aux mesures du système ..... 0
```

lbcontrol executor — Contrôle de l'exécuteur



set

Définit les zones de l'exécuteur.

address

Adresse IP ou nom d'hôte permettant de se connecter à Cisco CSS Switch à des fins administratives. Pour obtenir plus d'informations, reportez-vous à la brochure *Cisco Content Services Switch Basic Configuration Guide*.

valeur

Adresse IP valide ou nom d'hôte.

communityname

Nom de communauté SNMP utilisé dans les communications SNMP avec Cisco CSS Switch. Pour obtenir plus d'informations, reportez-vous à la brochure *Cisco Content Services Switch Basic Configuration Guide*.

valeur

La valeur par défaut est public avec un accès en lecture-écriture.

timeout

Nombre de secondes après lesquelles les requêtes SNMP provenant de Cisco Consultant et destinées à Cisco CSS Switch arrivent à expiration. Cisco Consultant utilise SNMP pour rassembler des informations à partir de Cisco CSS Switch. Si les messages `manager.log` indiquent des délais d'expiration fréquents, vous pouvez régler cette valeur afin de compenser.

valeur

La valeur par défaut est 3.

retries

Nombre de fois où Cisco Consultant émet une requête SNMP vers Cisco CSS Switch. Si les messages `manager.log` indiquent des erreurs de requête SNMP fréquentes, vous pouvez régler cette valeur pour compensation.

valeur

La valeur par défaut est 2.

status

Affiche l'état actuel des valeurs de l'exécuteur pouvant être définies ainsi que les valeurs par défaut.

Exemples

- Pour afficher les compteurs internes de Cisco Consultant :

```
lbcontrol executor status
```

```
Etat de l'exécuteur :
```

```
-----
```

```
adresse ..... 9.67.131.151
```

```
nom de la communauté ..... public
```

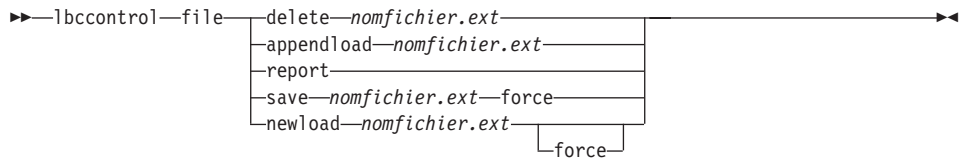
```
délai ..... 3
```

```
nombre de tentatives ..... 2
```

- Pour attribuer à l'adresse la valeur 130.40.52.167 :

```
lbcontrol executor set address 130.40.52.167
```

lbcontrol file — Gestion des fichiers de configuration



delete

Supprime le fichier.

nomfichier.ext

Fichier de configuration.

Vous pouvez indiquer n'importe quelle extension de fichier (.ext) ou n'en indiquer aucune

appendload

Ajoute un fichier de configuration à la configuration en cours et le charge dans Cisco Consultant.

report

Génère un rapport sur les fichiers disponibles.

save

Sauvegarde la configuration en cours de Cisco Consultant dans le fichier.

Remarque : Les fichiers sont sauvegardés dans les répertoires suivants et chargés à partir de ces mêmes répertoires :

- AIX : /usr/lpp/nd/servers/configurations/lbc
- Linux : /opt/nd/servers/configurations/lbc
- Solaris : /opt/nd/servers/configurations/lbc
- Windows 2000 :

Chemin d'accès courant au répertoire d'installation —

c:\Program Files\ibm\edge\nd\servers\configurations\composant

Chemin d'accès au répertoire d'installation natif —

c:\Program Files\ibm\nd\servers\configurations\composant

force

Si vous voulez sauvegarder votre fichier dans un fichier existant du même nom, utilisez **force** pour supprimer le fichier existant avant de sauvegarder le nouveau fichier. Si vous n'utilisez pas l'option force, le fichier existant n'est pas remplacé.

newload

Charge un nouveau fichier de configuration dans Cisco Consultant. Le nouveau fichier de configuration remplace la configuration actuelle.

Exemples

- Pour supprimer un fichier :
`lbcontrol file delete fichier3`

Le fichier (fichier3) est supprimé.
- Chargement d'un nouveau fichier de configuration pour remplacer la configuration actuelle :
`lbcontrol file newload fichier1.sv`

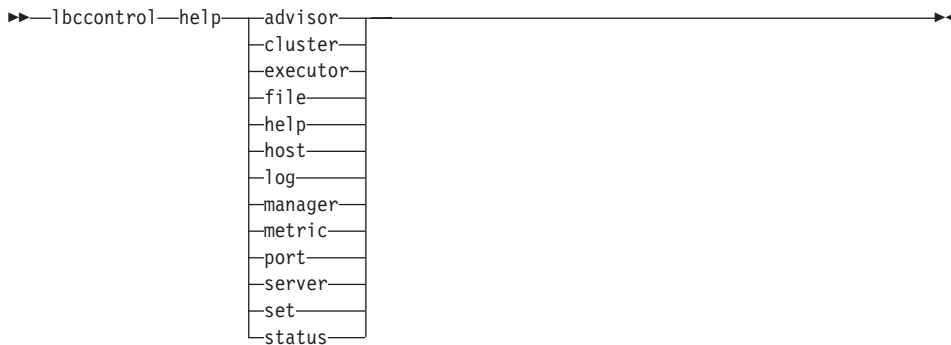
Le fichier (fichier1.sv) a été chargé dans Dispatcher.
- Chargement et adjonction d'un fichier de configuration à la configuration actuelle :
`lbcontrol file appendload fichier2.sv`

Le fichier (fichier2.sv) a été chargé et ajouté à la configuration actuelle.
- Pour visualiser un rapport de vos fichiers (à savoir les fichiers que vous avez sauvegardés précédemment) :
`lbcontrol file report`

RAPPORT SUR LES FICHIERS :
fichier1.sauv
fichier2.sv
fichier3
- Pour sauvegarder votre configuration dans un fichier intitulé fichier3 :
`lbcontrol file save fichier3`

La configuration est sauvegardée dans fichier3.

lbcontrol help — Affichage ou impression de l'aide relative à cette commande



Examples

- Pour obtenir de l'aide sur la commande `lbcontrol`, entrez :
`lbcontrol help`

Cette commande génère des résultats similaires à l'exemple suivant :

ARGUMENTS DE LA COMMANDE HELP :

Syntaxe : `help <option>`

Exemple : help cluster

```

executor      - Aide sur la commande executor
cluster      - Aide sur la commande cluster
port         - Aide sur la commande port
rule         - Aide sur la commande rule
subagent     - Aide sur la commande subagent
manager      - Aide sur la commande manager
metric       - Aide sur la commande metric
advisor      - Aide sur la commande advisor
file         - Aide sur la commande file
host         - Aide sur la commande host
log          - Aide sur la commande log
set          - Aide sur la commande set
status       - Aide sur la commande status
help         - Impression du texte d'aide dans son intégralité

```

Les paramètres entres les caractères < > sont des variables.

lbcontrol host — Configuration d'une machine éloignée

►►—lbcontrol—host:—*hôte_éloigné*—◄◄

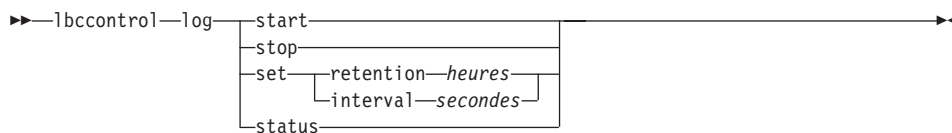
hôte_éloigné

Nom de la machine Cisco Consultant en cours de configuration. Lorsque vous entrez cette commande, n'insérez pas de caractère d'espacement entre **host:** et *hôte_éloigné*, par exemple :

```
lbcontrol  
host:hôte_éloigné
```

Exécutez cette commande à partir d'une invite, puis entrez une commande lbcontrol valide à appliquer à la machine Cisco Consultant éloignée.

lbccontrol log — Contrôle du fichier journal binaire



start

Lance la journalisation

stop

Arrête la journalisation

set

Définit les zones de journalisation. Pour plus d'informations sur la définition des zones pour la journalisation binaire, reportez-vous à la section «Utilisation de la journalisation binaire pour analyser les statistiques des serveurs» à la page 205.

rétenion

Nombre d'heures pendant lesquelles les fichiers journaux binaires vont être conservés. La valeur de rétention par défaut est 24.

heures

Nombre d'heures.

interval

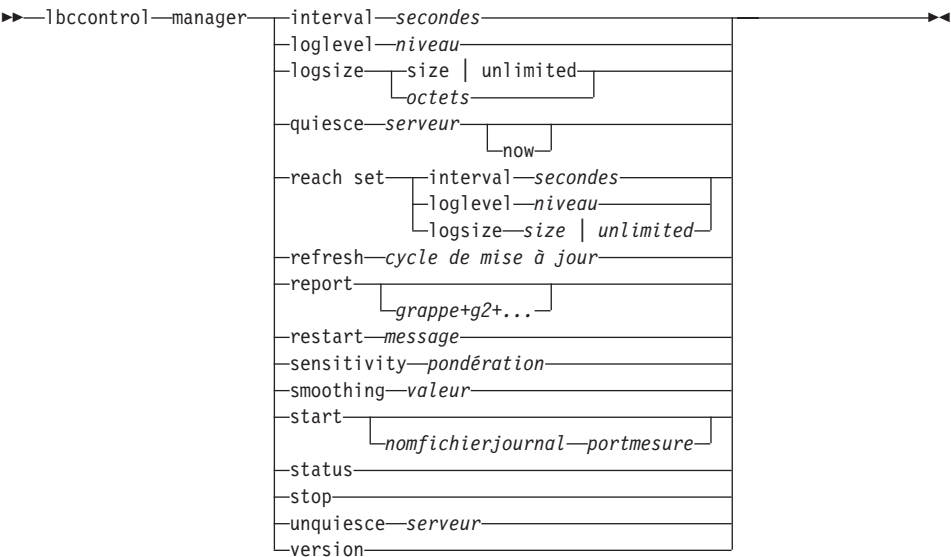
Nombre de secondes qui s'écoulent entre deux entrées de journal. La valeur par défaut est 60.

secondes

Nombre de secondes.

status

Affiche la rétention et les intervalles du journal.



interval
Définit la fréquence de mise à jour, par le gestionnaire, des pondérations des serveurs en fonction de la mise à jour par Cisco CSS Switch, des critères utilisés par Cisco CSS Switch pour acheminer les demandes client.

seconde
Nombre entier positif représentant la fréquence (en secondes) de mise à jour, par le gestionnaire, des pondérations pour Cisco CSS Switch. La valeur par défaut est 15 et l'intervalle minimal est 10. Si vous tentez d'attribuer à l'intervalle du gestionnaire une valeur inférieure à 10 secondes, la valeur 10 secondes est attribuée à l'intervalle. Nous vous recommandons d'utiliser l'intervalle du gestionnaire par défaut qui est de 15 secondes car Cisco CSS Switch ne tire pas profit de mises à jour plus rapides.

loglevel
Permet de définir le niveau de consignation relatif au journal du gestionnaire.

niveau
Numéro du niveau (0 à 5). Plus le numéro est élevé, plus la quantité des informations consignées dans le journal du gestionnaire est importante. Valeur par défaut : 1. Les valeurs possibles sont les suivantes : 0 (Aucun), 1 (Minimal), 2 (De base), 3 (Modéré), 4 (Avancé), 5 (Proluxe).

logsize

Définit la taille maximale du journal du gestionnaire. Lorsque vous attribuez une taille maximale au fichier journal, ce dernier est traité par procédé de boucle. Lorsque le fichier atteint la taille indiquée, les entrées suivantes sont écrites à partir du haut du fichier pour écraser les entrées de journal précédentes. La taille du journal ne peut pas être inférieure à la taille actuelle du journal. Les entrées du journal sont horodatées, ce qui permet de déterminer l'ordre dans lequel elles ont été enregistrées. Plus le niveau de journalisation est élevé, plus la taille du journal doit être choisie attentivement car l'espace peut être saturé rapidement.

octets

Taille maximale (en octets) du fichier journal du gestionnaire. Vous pouvez indiquer un nombre positif supérieur à zéro, ou le mot **unlimited**. Il se peut que le fichier journal n'atteigne pas la taille maximale exacte avant l'écrasement, car la taille des entrées de journal elles-mêmes varie. La valeur par défaut est 1 Mo.

quiesce

Indique de ne plus envoyer de connexions à un serveur. Le gestionnaire attribue la valeur 0 à la pondération de ce serveur, pour chaque port pour lequel le serveur est défini puis envoie une commande `suspend` à Cisco CSS Switch. Utilisez cette commande lorsque vous voulez placer un serveur au repos pour des opérations de maintenance rapides puis activez-le à nouveau. Si vous supprimez de la configuration un serveur mis en attente et que vous l'ajoutez à nouveau, il ne conserve pas l'état qui lui était attribué avant sa mise en attente.

serveur

Adresse IP du serveur sous forme d'adresse symbolique ou en notation décimal à points.

conseiller de contact (reach)

Définit l'intervalle, le niveau de consignation et la taille du journal pour le conseiller d'accessibilité.

refresh

Définit le nombre d'intervalles avant qu'il ne soit demandé à Cisco CSS Switch de régénérer les informations relatives aux nouvelles connexions et aux connexions actives.

cycle de mise à jour

Nombre positif représentant le nombre d'intervalles. La valeur par défaut est 1.

report

Affiche un rapport d'analyse sur les statistiques.

grappe

Adresse de la grappe que vous souhaitez afficher dans le rapport.

L'adresse peut prendre la forme d'un nom symbolique ou d'une notation décimale. L'affichage par défaut est un rapport de gestionnaire portant sur toutes sur les grappes.

Remarque : Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

restart

Relance tous les serveurs (qui ne sont pas arrêtés) en leur affectant des valeurs de pondération normalisées (la moitié de la pondération maximale).

message

Message à consigner dans le fichier journal du gestionnaire.

sensitivity

Définit la sensibilité minimale à partir de laquelle les pondérations sont mises à jour. Ce paramètre définit le moment où le gestionnaire doit modifier sa pondération pour le serveur, en fonction des informations externes.

pondération

Nombre compris entre 0 et 100 à utiliser comme pourcentage de pondération. La valeur par défaut de 5 crée une sensibilité minimale de 5%.

smoothing

Définit un index pour lisser les variations des pondérations lors de l'équilibrage de charge. Plus l'index de filtrage est élevé, moins les pondérations des serveurs varient lorsque les conditions réseau sont modifiées. Plus cet index est faible, plus les pondérations des serveurs varient.

valeur

Nombre positif en virgule flottante. Valeur par défaut : 1,5.

start

Lance le gestionnaire.

nomfichierjournal

Nom du fichier dans lequel les données de gestion sont consignées. Chaque enregistrement du journal est horodaté.

Le fichier par défaut se trouve dans le répertoire **logs**. Reportez-vous à la section «Annexe F. Exemples de fichiers de configuration» à la page 387. Pour obtenir des informations sur le mode de modification du répertoire dans lequel les fichiers journaux sont enregistrés, reportez-vous à la section «Modification des chemins des fichiers journaux» à la page 216.

portmeasure

Port sur lequel le système Metric Server va communiquer. Si vous indiquez un port de décompte, vous devez spécifier un nom de fichier journal. Le port de décompte par défaut est 10004.

status

Affiche l'état en cours de toutes les valeurs globales du gestionnaire et leurs valeurs par défaut.

stop

Arrête le gestionnaire.

unquiesce

Indique que le gestionnaire peut commencer à attribuer une pondération supérieure à 0 à un serveur préalablement mis au repos sur chaque port pour lequel il est défini. Le gestionnaire envoie une commande active à Cisco CSS Switch.

serveur

Adresse IP du serveur sous forme de nom symbolique ou en notation décimale à points.

version

Affiche la version en cours du gestionnaire.

Exemples

- Pour affecter la valeur de 5 secondes au délai séparant les mises à jour du gestionnaire, entrez :
`lbcontrol manager interval 5`
- Pour affecter au niveau de journalisation la valeur de 0, afin d'optimiser les performances, entrez :
`lbcontrol manager loglevel 0`
- Pour affecter à la taille de journal du gestionnaire la valeur de 1 000 000 octets, entrez :
`lbcontrol manager logsize 1000000`
- Pour indiquer qu'aucune autre connexion ne doit être envoyée au serveur à l'adresse 130.40.52.153, entrez :
`lbcontrol manager quiesce 130.40.52.153`
- Pour attribuer la valeur 3 au nombre d'intervalles avant la régénération des pondérations :
`lbcontrol manager refresh 3`
- Pour obtenir une analyse statistique du gestionnaire, entrez :
`lbcontrol manager report`

Cette commande génère des résultats similaires à l'exemple suivant :

lbccontrol>>rapport du gestionnaire

TABLE DES NOTES				ETAT	
serveur6				ACTIF	
serveur5				ACTIF	
serveur4				ACTIF	
serveur3				ACTIF	
serveur2				ACTIF	
serveur1				ACTIF	

9.67.154.35		POND.		ACTIV. % 49		NOUV. % 50		PORT % 1		SYSTEME % 0	
PORT :	80	ACTU.	NV.	PND	CONNEXIONS	PND	CONNEXIONS	PND	CHARGE	PND	CHARGE
serveur1	4	4	5	0	5	0	3	301	-9999	-1	
serveur2	5	5	5	0	5	0	6	160	-9999	-1	
TOTAUX :	9	9		0		0		461		-2	

9.67.154.35		POND.		ACTIV. % 49		NOUV. % 50		PORT % 1		SYSTEME % 0	
PORT :	443	ACTU.	NV.	PND	CONNEXIONS	PND	CONNEXIONS	PND	CHARGE	PND	CHARGE
serveur3	4	4	5	0	5	0		0	-9999	-1	
serveur4	5	5	5	0	5	0	0	0	-9999	-1	
TOTAUX :	9	9		0		0		0		-2	

9.67.154.34		POND.		ACTIV. % 49		NOUV. % 50		PORT % 1		SYSTEME % 0	
PORT :	80	ACTU.	NV.	PND	CONNEXIONS	PND	CONNEXIONS	PND	CHARGE	PND	CHARGE
serveur5	5	5	5	0	5	0	5	160	-9999	-1	
serveur6	0	0	5	0	5	0	-9999	-1	-9999	-1	
TOTAUX :	5	5		0		0		159		-2	

ADVISOR	PORT	TIMEOUT
http	80	unlimited

- Pour relancer tous les serveurs en leur affectant des pondérations normalisées et pour consigner un message dans le fichier journal du gestionnaire, entrez :

```
lbcontrol manager restart Restarting the manager to update code
```

Cette commande génère des résultats similaires à l'exemple suivant :

```
320-14:04:54
```

```
Relance du gestionnaire pour mettre à jour le code
```

- Pour affecter la valeur 10 à la sensibilité aux modifications de pondération, entrez :

```
lbcontrol manager sensitivity 10
```

- Pour affecter la valeur 2 à l'index de lissage, entrez :

```
lbcontrol manager smoothing 2.0
```

- Pour lancer le gestionnaire et indiquer le fichier journal nommé ndmgr.log (les chemins ne peuvent pas être définis), entrez :

```
lbcontrol manager start ndmgr.log
```

- Pour afficher l'état en cours des valeurs associées au gestionnaire, entrez :

```
lbcontrol manager status
```

Cette commande génère des résultats similaires à l'exemple suivant :

```
Etat du
```

```
gestionnaire (manager) :
```

```
=====
```

```
Port de mesure ..... 10004
```

```
Nom de fichier journal de gestionnaire ..... manager.log
```

```
Niveau de consignation du gestionnaire ..... 1
```

```
Taille maxi du journal du gestionnaire (octets) ..... unlimited
```

```
Niveau de sensibilité ..... 0.05
```

```
Indice de lissage ..... 1.5
```

```
Intervalle de mise à jour (secondes) ..... 2
```

```
Cycle des mises à jour des pondérations ..... 1
```

```
Niveau de journal des contacts ..... 1
```

```
Taille maximale du journal des contacts (octets) ..... unlimited
```

```
Intervalle de mise à jour des contacts (secondes) ..... 7
```

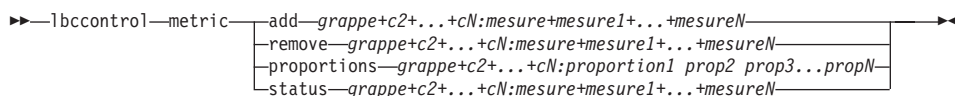
- Pour arrêter le gestionnaire, entrez :

```
lbcontrol manager stop
```

- Pour afficher le numéro de version en cours du gestionnaire, entrez :

```
lbcontrol manager version
```

lbcontrol metric — Configuration des mesures du système



add

Ajoute une mesure.

grappe

Adresse de connexion des clients. Il peut s'agir du nom d'hôte de la machine ou de l'adresse IP en notation décimale à points. Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

Remarque : Pour Cisco Consultant, l'adresse de grappe correspond à l'adresse IP virtuelle (VIP) de la règle de contenu du propriétaire dans la configuration Cisco CSS Switch.

mesure

Mesure du système. Voici les différents types de mesure :

- cpuload
- memload
- port
- mesures du système

remove

Supprime cette mesure.

proportions

Définit les proportions des mesures associées à cet objet.

status

Affiche les valeurs actuelles de cette mesure.

Exemples

- Pour ajouter une mesure de système, entrez :
`lbcontrol metric add 10.10.10.20:metric1`
- Pour définir les proportions d'une grappe associée à deux mesures de système, entrez :
`lbcontrol metric proportions 10.10.10.20 48 52`
- Pour afficher l'état en cours des valeurs associées à la mesure spécifiée, entrez :
`lbcontrol metric status 10.10.10.20:metric1`

Cette commande génère des résultats similaires à l'exemple suivant :

Etat des mesures :

Grappe 10.10.10.20

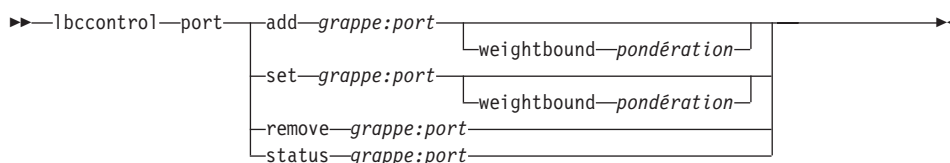
Nom de la mesure..... metric1

Proportion de la mesure..... 52

 Serveur 9.37.56.100

 Données de mesure... -1

lbcontrol port — Configuration des ports



add

Ajoute un port à une grappe. Avant d'ajouter un serveur à un port, vous devez ajouter un port à une grappe. Si aucun port n'est associé à une grappe, les demandes client sont traitées en local. Cette commande permet d'ajouter plusieurs ports à la fois.

weightbound

Définit la pondération maximale des serveurs sur ce port. Cette option a une incidence sur le degré de différence possible entre le nombre de demandes transmises par Cisco CSS Switch à chaque serveur. La valeur par défaut est 10.

pondération

Nombre compris entre 1 et 10 représentant la limite de pondération maximale.

set

Définit les zones d'un port.

remove

Supprime ce port.

status

Affiche l'état des serveurs sur ce port. Si vous voulez voir le statut de tous les ports, n'indiquez pas de *port* avec cette commande et n'oubliez pas le caractère deux-points.

Exemples

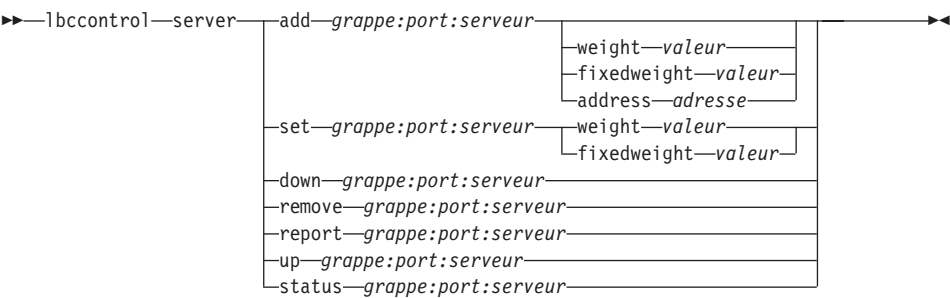
- Pour ajouter les ports 80 et 23 à l'adresse de grappe 130.40.52.153, entrez :
`lbcontrol port add 130.40.52.153:80+23`
- Pour affecter la pondération maximale de 10 au port 80 à l'adresse de grappe 130.40.52.153, entrez :
`lbcontrol port set 130.40.52.153:80 weightbound 10`
- Pour supprimer le port 23 de l'adresse de grappe 130.40.52.153, entrez :
`lbcontrol port remove 130.40.52.153:23`
- Pour obtenir l'état du port 80 à l'adresse de grappe 9.67.131.153, entrez :
`lbcontrol port status 9.67.131.153:80`

Cette commande génère des résultats similaires à l'exemple suivant :

Etat du port :

Numéro du port	80
Adresse de grappe	9.67.131.153
Nombre de serveurs	2
Limite de pondération	10

lbcontrol server — Configuration des serveurs



add
Permet d’ajouter ce serveur.

grappe
Adresse de la grappe sous forme de nom symbolique ou en notation décimale à point.

Remarque : Chaque grappe supplémentaire doit être séparée de la précédente par le signe plus (+).

port
Numéro du port.

Remarque : Chaque port supplémentaire doit être séparé du précédent par le signe plus (+).

serveur
Adresse IP unique du serveur TCP sous forme de nom symbolique ou en notation décimale à point. Si vous utilisez un nom unique qui ne se résout pas en adresse IP, vous devez fournir l’attribut d’adresse lorsque vous entrez la commande **lbcontrol server add**.

weight
Nombre compris entre 0 et 10 représentant la pondération de ce serveur. L’affectation de la valeur zéro à la pondération empêche l’envoi de nouvelles demandes au serveur mais ne met pas fin aux connections actuellement actives à ce serveur. La valeur par défaut correspond à la moitié de la pondération maximale du port indiqué. Ce paramètre est rapidement remplacé lorsque le gestionnaire est en cours d’exécution et que fixedweight a pour valeur non.

valeur
Valeur de pondération.

fixedweight

L'option **fixedweight** permet d'indiquer si vous souhaitez que le gestionnaire modifie la pondération du serveur. Si vous fixez sur oui la valeur **fixedweight**, le gestionnaire en activité ne sera pas autorisé à modifier la pondération du serveur. Pour plus d'informations, reportez-vous à la section «Pondérations fixées par le gestionnaire» à la page 143.

valeur

Valeur de la pondération fixe. La valeur par défaut est non.

address

Adresse IP unique du serveur TCP sous forme de nom symbolique ou en notation décimale à point. Si la valeur du nom du serveur n'est pas résolue (par exemple, un nom de serveur logique), vous devez fournir l'adresse du serveur physique.

valeur

Identificateur unique du serveur. S'il n'est pas possible de résoudre le serveur, vous devez fournir l'attribut de l'adresse.

down

Marque ce serveur comme étant arrêté. Cisco CSS Switch arrête d'envoyer des connexions à ce serveur.

remove

Permet de supprimer ce serveur.

report

Génère un rapport sur ce serveur.

set

Permet de définir des valeurs pour ce serveur.

up Marque ce serveur comme étant activé. Cisco CSS Switch envoie désormais les nouvelles connexions à ce serveur.

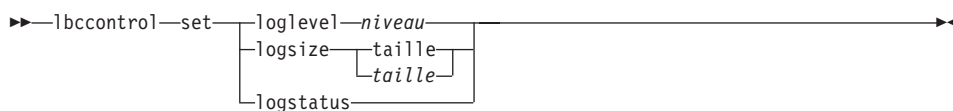
status

Affichage de l'état des serveurs.

Exemples

- Pour ajouter le serveur 27.65.89.42 au port 80 sur une grappe à l'adresse 130.40.52.153, entrez :
`lbcontrol server add 130.40.52.153:80:27.65.89.42`
- Pour supprimer le serveur 27.65.89.42 de tous les ports de toutes les grappes, entrez :
`lbcontrol server remove ::27.65.89.42`
- Pour affecter la valeur 10 à la pondération du serveur 27.65.89.42 au port 80 sur une grappe à l'adresse 130.40.52.153, entrez :
`lbcontrol server set 130.40.52.153:80:27.65.89.42 weight 10`

lbcontrol set — Configuration du journal du serveur



loglevel

Niveau auquel le serveur lbserver journalise ses activités.

niveau

La valeur par défaut de **loglevel** est 1. La fourchette va de 0 à 5. Les valeurs possibles sont les suivantes : 0 (Aucun), 1 (Minimal), 2 (De base), 3 (Modéré), 4 (Avancé), 5 (Prolixe).

logsize

Nombre maximal d'octets à journaliser dans le fichier journal.

taille

La taille de fichier journal par défaut est 1 Mo.

logstatus

Affiche les paramètres du journal du serveur (niveau de journalisation et taille du journal).

lbcontrol status — Indique par affichage si le gestionnaire et les conseillers sont en cours d'exécution

►►—lbcontrol—status—◀◀

Exemples

- Pour visualiser les éléments en cours d'exécution, entrez :
lbcontrol status

Cette commande génère des résultats similaires à l'exemple suivant :

Le gestionnaire (manager) a été lancé

ADVISOR	PORT	TIMEOUT

http	80	unlimited
ftp	21	unlimited

Annexe F. Exemples de fichiers de configuration

La présente annexe contient des exemples de fichiers de configuration pour le composant Dispatcher de Network Dispatcher.

Exemples de fichiers de configuration Network Dispatcher

Les exemples de fichiers se trouvent dans le répertoire
.../nd/servers/samples/.

Dispatcher Fichier de configuration—AIX, Red Hat Linux, et Solaris

```
#!/bin/ksh
#
# configuration.sample - Exemple de fichier de configuration pour
# le composant Dispatcher
#
#
# Ce script doit être lancé par l'utilisateur root.
#
# iam='whoami'

# if [ "$iam" != "root" ] if [ "$iam" != "root" ]
# then
# echo "Vous devez vous connecter en tant qu'utilisateur root pour exécuter ce script"
# exit 2
# fi

#
# Démarrez d'abord le serveur
#
# ndserver start
# sleep 5

#
# Lancez ensuite l'exécuteur
#
# ndcontrol executor start

#
# Il est possible d'arrêter le répartiteur à tout moment à l'aide
# des commandes "ndcontrol executor stop" et "ndserver stop"
# pour arrêter respectivement l'exécuteur et le serveur avant
# d'arrêter le logiciel Dispatcher.
#
# L'étape suivante dans la configuration du répartiteur est de définir
# l'adresse NFA (adresse de non-réacheminement) et les adresses de grappes.
#
# L'adresse NFA permet d'accéder à distance au répartiteur
# afin d'effectuer des opérations d'administration et de configuration.
```

```

# Cette adresse est obligatoire car le répartiteur doit acheminer
# des paquets vers les adresses de grappes.
#
# L'adresse de grappe (cluster) correspond au nom d'hôte (ou à l'adresse IP)
# auquel les clients éloignés se connecteront.
#
# Vous pouvez indifféremment utiliser les noms d'hôte et les adresses IP
# dans ce fichier.
#

# NFA=nomhôte.domaine.nom
# CLUSTER=www.votresociété.com

# echo "Chargement de l'adresse de non réacheminement"
# ndcontrol executor set nfa $NFA

#
# L'étape suivante dans la configuration du répartiteur consiste à créer
# une grappe. Le répartiteur acheminera les requêtes envoyées
# à l'adresse de grappe vers les serveurs associés
# à cette grappe. Vous pouvez configurer plusieurs adresses de
# grappes et leur associer plusieurs serveurs à l'aide du répartiteur.

# Utilisez une configuration similaire pour CLUSTER2, CLUSTER3, etc.
#

# echo "Chargement de la première adresse de grappe"
# ndcontrol cluster add $CLUSTER

#
# L'étape suivante consiste à définir les ports utilisés par cette grappe.
# Toute requête reçue par le répartiteur sur un port défini
# sera réacheminée vers le port correspondant de l'un
# des serveurs.
#

# echo "Création de ports pour la grappe : $CLUSTER"

# ndcontrol port add $CLUSTER:20+21+80

#
# La dernière étape consiste à associer chaque serveur
# aux ports de cette grappe.
# Vous pouvez utiliser indifféremment le nom
# d'hôte ou l'adresse IP des serveurs.
#

# SERVER1=server1name.domain.name
# SERVER1=nomserveur1.domaine.nom
# SERVER2=nomserveur2.domaine.nom
# SERVER3=nomserveur3.domaine.nom

# echo "Ajout des serveurs"
# ndcontrol server add $CLUSTER:20+21+80:
# $SERVER1+$SERVER2+$SERVER3

```



```

#
# Nous allons maintenant lancer les composants d'équilibrage de charge
# du répartiteur. Le premier composant s'appelle le gestionnaire.
# Les autres composants d'équilibrage de charge sont les
# conseillers. Si le gestionnaire et les conseillers ne fonctionnent pas,
# le répartiteur envoie des requêtes au format de permutation circulaire
# (round-robin). Une fois le gestionnaire lancé, les décisions de pondération
# basées sur le nombre de connexions nouvelles et actives sont utilisées, et
# les requêtes entrantes sont envoyées au meilleur serveur. Les conseillers
# fournissent au gestionnaire des informations supplémentaires sur la capacité
# du serveur à répondre aux requêtes, et à détecter si le serveur est actif
# ou non. Si un conseiller détecte qu'un serveur est arrêté, cela sera
# consigné (à condition que les proportions du gestionnaire soient définies
# pour inclure les entrées de conseiller) et aucune autre requête ne sera
# acheminée vers le serveur.

# La dernière étape de configuration des composants d'équilibrage de charge
# est la définition des proportions du gestionnaire. Ce dernier met à
# jour la pondération de chaque serveur en fonction de quatre règles :
# 1. Nombre de connexions actives sur chaque serveur.
# 2. Nombre de nouvelles connexions sur chaque serveur.
# 3. Informations fournies par les conseillers.
# 4. Informations fournies par le conseiller au niveau système.
# La somme de ces proportions doit être égale à 100. Par exemple,
# si l'on définit les proportions du gestionnaire de la façon suivante :
# ndcontrol manager proportions 48 48 0 0
# 48 % des informations proviendront des connexions nouvelles, 48%,
# des connexions actives, 4%, des conseillers et les entrées
# système ne seront pas prises en compte. #
#
# REMARQUE : par défaut, les proportions du gestionnaire sont définies à 50 50 0 0.
#

# echo "Lancement du gestionnaire (manager)..."
# ndcontrol manager start

# echo "Lancement du conseiller (advisor) FTP sur le port 21..."
# ndcontrol advisor start ftp 21
# echo "Lancement du conseiller (advisor) HTTP sur le port 80..."
# ndcontrol advisor start http 80
# echo "Lancement du conseiller (advisor) Telnet sur le port 23..."
# ndcontrol advisor start telnet 23
# echo "Lancement du conseiller (advisor) SMTP sur le port 25..."
# ndcontrol advisor start smtp 25
# echo "Lancement du conseiller (advisor) POP3 sur le port 110..."
# ndcontrol advisor start pop3 110
# echo "Lancement du conseiller (advisor) NNTP sur le port 119..."
# ndcontrol advisor start nntp 119
# echo "Lancement du conseiller (advisor) SSL sur le port 443..."
# ndcontrol advisor start ssl 443
#

# echo "Définition des proportions du gestionnaire..."
# ndcontrol manager proportions 58 40 2 0

```

```

#
# L'étape finale dans la configuration du répartiteur est d'affecter
# un alias à la Carte d'interface réseau (NIC).
#
# REMARQUE : N'utilisez pas cette commande dans un environnement
# haute disponibilité. Les scripts go* configureront les cartes NIC et
# le bouclage si nécessaire.
# ndcontrol cluster configure $CLUSTER

# Si votre adresse de grappe se trouve sur une autre carte NIC
# ou sur un sous-réseau autre que ceux de la NFA, utilisez le format
# suivant comme commande de configuration de grappe.
# ndcontrol cluster configure $CLUSTER tr0 0xfffff800
# tr0 étant votre carte NIC (tr1, la seconde carte réseau en anneau à jeton,
# en0 la première carte ethernet) et 0xfffff800 étant un masque
# de sous-réseau valide pour votre site.
#

#
# Les commandes suivantes permettent de définir les valeurs par défaut.
# Utilisez ces commandes pour modifier les valeurs par défaut.
# ndcontrol manager loglevel 1
# ndcontrol manager logsize 1048576
# ndcontrol manager sensitivity 5.000000
# ndcontrol manager interval 2
# ndcontrol manager refresh 2
#
# ndcontrol advisor interval ftp 21 5
# ndcontrol advisor loglevel ftp 21 1
# ndcontrol advisor logsize ftp 21 1048576
# ndcontrol advisor timeout ftp 21 unlimited
# ndcontrol advisor interval telnet 23 5
# ndcontrol advisor loglevel telnet 23 1
# ndcontrol advisor logsize telnet 23 1048576
# ndcontrol advisor timeout telnet 23 unlimited
# ndcontrol advisor interval smtp 25 5
# ndcontrol advisor loglevel smtp 25 1
# ndcontrol advisor logsize smtp 25 1048576
# ndcontrol advisor timeout smtp 25 unlimited
# ndcontrol advisor interval http 80 5
# ndcontrol advisor loglevel http 80 1
# ndcontrol advisor logsize http 80 1048576
# ndcontrol advisor timeout http 80 unlimited
# ndcontrol advisor interval pop3 110 5
# ndcontrol advisor loglevel pop3 110 1
# ndcontrol advisor logsize pop3 110 1048576
# ndcontrol advisor timeout pop3 110 unlimited
# ndcontrol advisor interval nntp 119 5
# ndcontrol advisor loglevel nntp 119 1
# ndcontrol advisor logsize nntp 119 1048576
# ndcontrol advisor timeout nntp 119 unlimited
# ndcontrol advisor interval ssl 443 5

```

```
# ndcontrol advisor loglevel ssl 443 1
# ndcontrol advisor logsize ssl 443 1048576
# ndcontrol advisor timeout ssl 443 unlimited
#
```

Dispatcher Fichier de configuration — Windows

Voici un exemple de fichier de configuration de Network Dispatcher intitulé **configuration.cmd.sample** à utiliser sous Windows.

```
@echo off
rem configuration.cmd.sample - Exemple de fichier de configuration pour
rem le composant Dispatcher.
rem

rem Démarrez ndserver à partir du panneau Services

rem

rem
rem Lancez ensuite l'exécuteur
rem
rem call ndcontrol executor start

rem

rem L'étape suivante dans la configuration du répartiteur est de définir
rem l'adresse NFA (adresse de non-réacheminement) et les
rem adresses de grappes.
rem

rem L'adresse NFA permet d'accéder à distance au répartiteur
rem afin d'effectuer des opérations d'administration de configuration.
rem Cette adresse est obligatoire car le répartiteur doit réacheminer
rem des paquets vers les adresses de grappes.

rem
rem L'adresse de grappe (CLUSTER) est le nom d'hôte (ou l'adresse IP)
rem à laquelle les clients éloignés se connecteront.
rem

rem Vous pouvez indifféremment utiliser les noms d'hôte et les adresses IP
rem dans ce fichier.
rem NFA=[adresse de non-réacheminement]
rem CLUSTER=[nom de la grappe]
rem

rem set NFA=nom_hôte.domaine.nom
rem set CLUSTER=www.votresociété.com

rem echo "Chargement de l'adresse de non réacheminement"
rem call ndcontrol executor set nfa %NFA%

rem
rem Les valeurs par défaut sont affectées aux commandes suivantes.
rem Utilisez ces commandes pour modifier les valeurs par défaut.
```

```

rem call ndcontrol executor set fintimeout 30
rem call ndcontrol executor set fincount 4000
rem
rem
rem L'étape suivante dans la configuration du répartiteur consiste à
créer
rem une grappe. Le répartiteur acheminera les requêtes envoyées
rem à l'adresse de grappe vers les serveurs associés
rem à cette grappe. Vous pouvez configurer plusieurs adresses de
rem grappes à l'aide du répartiteur.
rem Utilisez une configuration similaire pour CLUSTER2, CLUSTER3, etc.
rem

rem echo "Chargement de la première adresse de grappe"
rem call ndcontrol cluster add %CLUSTER%

rem
rem L'étape suivante consiste à définir les ports utilisés par cette grappe.
rem Toute requête reçue par le répartiteur sur un port défini
rem sera réacheminée vers le port correspondant
rem de l'un des serveurs.
rem

rem echo "Création des ports de la GRAPPE : %CLUSTER%"
rem call ndcontrol port add %CLUSTER%:20+21+80

rem
rem La dernière étape consiste à associer chaque serveur aux
rem ports définis pour la grappe. Vous pouvez utiliser indifféremment
rem le nom d'hôte ou l'adresse IP des machines serveurs.
rem

rem set SERVER1=nomserveur1.domaine.nom
rem set SERVER2=nomserveur2.domaine.nom
rem set SERVER3=nomserveur3.domaine.nom

rem echo "Ajout des serveurs"
rem call ndcontrol server add %CLUSTER%:20+21+80:
rem %SERVER1%+%SERVER2%+%SERVER3%

rem
rem Nous allons maintenant lancer les composants d'équilibrage de charge
rem du répartiteur. Le premier composant s'appelle le gestionnaire.
rem Les autres composants d'équilibrage de charge sont les
rem conseillers. Si le gestionnaire et les conseillers ne sont pas
rem actifs, le répartiteur envoie des requêtes au format de permutation circulaire
rem (round-robin). Une fois le gestionnaire lancé, les décisions de
rem pondération basées sur le nombre de connexions nouvelles et actives
rem sont utilisées et les requêtes entrantes sont envoyées au meilleur
rem serveur. Les conseillers permettent au gestionnaire de disposer d'informations
rem supplémentaires sur la capacité du serveur à répondre aux requêtes
rem et à détecter si un serveur est actif ou non. Si un conseiller
rem détecte qu'un serveur est arrêté, cela sera consigné (à condition que
rem les proportions du gestionnaire aient été définies pour inclure les

```

```
rem entrées du conseiller) et aucune requête ne sera acheminée vers le serveur.
rem La dernière étape de configuration des composants d'équilibrage de charge
rem est la définition des proportions du gestionnaire. Ce dernier met à
rem jour la pondération manager de chaque serveur sur
la base de quatre règles :
```

```
rem 1. Nombre de connexions actives sur chaque serveur.
rem 2. Nombre de nouvelles connexions pour chaque serveur.
rem 3. Informations fournies par les conseillers.
rem 4. Informations fournies par le conseiller au niveau système.
rem
rem La somme de ces proportions doit être égale à 100. Par exemple,
rem si l'on définit les proportions avec
rem ndcontrol cluster set <cluster> proportions 48 48 4 0
rem 48 % des informations proviendront des connexions nouvelles,
rem des connexions actives, 4 % des conseillers et les entrées
rem système ne seront pas prises en compte.
rem
rem REMARQUE : par défaut, les propriétés du gestionnaires sont
définies comme suit :
rem 50 50 0 0
```

```
rem echo "Lancement du gestionnaire (manager)..."
rem call ndcontrol manager start
```

```
rem echo "Lancement du conseiller (advisor) FTP sur le port 21..."
rem call ndcontrol advisor start ftp 21
rem echo "Lancement du conseiller (advisor) HTTP sur le port 80..."
rem call ndcontrol advisor start http 80
rem echo "Lancement du conseiller Telnet sur le port 23 ..."
rem call ndcontrol advisor start telnet 23
rem echo "Lancement du conseiller SMTP sur le port 25 ..."
rem call ndcontrol advisor start smtp 25
rem echo "Lancement du conseiller POP3 sur le port 110 ..."
rem call ndcontrol advisor start pop3 110
rem echo "Lancement du conseiller NNTP sur le port 119 ..."
rem call ndcontrol advisor start nntp 119
rem echo "Lancement du conseiller SSL sur le port 443 ..."
rem call ndcontrol advisor start ssl 443
rem
```

```
rem echo "Définition des proportions de la grappe..."
rem call ndcontrol cluster set %CLUSTER% proportions 58 40 2 0
```

```
rem
rem L'étape finale de configuration du répartiteur est
rem l'affectation d'un alias à la carte d'interface réseau (NIC).
rem
rem
rem REMARQUE : N'utilisez pas cette commande dans un environnement à
rem haute disponibilité. Les scripts go* configureront les cartes NIC
rem et le bouclage si nécessaire.
rem
rem
rem ndcontrol cluster configure %CLUSTER%
```

```

rem Si votre adresse de grappe se trouve sur une autre carte NIC
rem ou sur un sous-réseau autre que l'adresse NFA, utilisez la
rem commande de configuration de grappe suivante.
rem ndcontrol cluster configure %CLUSTER% tr0 0xfffff800
rem tr0 étant votre carte NIC (tr1 la seconde carte réseau en anneau
rem à jeton, en0 la première carte Ethernet) et 0xfffff800,
rem un masque de sous-réseau valide de votre site.
rem

rem
rem Les valeurs par défaut sont affectées aux commandes suivantes.
rem Utilisez ces commandes pour modifier les valeurs par défaut.
rem call ndcontrol manager loglevel 1
rem call ndcontrol manager logsize 1048576
rem call ndcontrol manager sensitivity 5.000000
rem call ndcontrol manager interval 2
rem call ndcontrol manager refresh 2
rem
rem
rem call ndcontrol advisor interval ftp 21 5
rem call ndcontrol advisor loglevel ftp 21 1
rem call ndcontrol advisor logsize ftp 21 1048576
rem call ndcontrol advisor timeout ftp 21 unlimited
rem call ndcontrol advisor interval telnet 23 5
rem call ndcontrol advisor loglevel telnet 23 1
rem call ndcontrol advisor logsize telnet 23 1048576
rem call ndcontrol advisor timeout telnet 23 unlimited
rem call ndcontrol advisor interval smtp 25 5
rem call ndcontrol advisor loglevel smtp 25 1
rem call ndcontrol advisor logsize smtp 25 1048576
rem call ndcontrol advisor timeout smtp 25 unlimited
rem call ndcontrol advisor interval http 80 5
rem call ndcontrol advisor loglevel http 80 1
rem call ndcontrol advisor logsize http 80 1048576
rem call ndcontrol advisor timeout http 80 unlimited
rem call ndcontrol advisor interval pop3 110 5
rem call ndcontrol advisor loglevel pop3 110 1
rem call ndcontrol advisor logsize pop3 110 1048576
rem call ndcontrol advisor timeout pop3 110 unlimited
rem call ndcontrol advisor interval nntp 119 5
rem call ndcontrol advisor loglevel nntp 119 1
rem call ndcontrol advisor logsize nntp 119 1048576
rem call ndcontrol advisor timeout nntp 119 unlimited
rem call ndcontrol advisor interval ssl 443 5
rem call ndcontrol advisor loglevel ssl 443 1
rem call ndcontrol advisor logsize ssl 443 1048576
rem call ndcontrol advisor timeout ssl 443 unlimited
rem

```

Conseiller type

Vous trouverez ci-dessous un exemple de fichier de conseiller intitulé **ADV_type**.

```
/**
 * ADV_type : Conseiller HTTP de Network Dispatcher
 *
 *
 * Cette classe définit un exemple de conseiller personnalisé pour Network Dispatcher.
 * Comme tous les conseillers, le conseiller personnalisé étend la fonction de
 * la base du conseiller, appelée ADV_Base. En fait, c'est cette base qui
 * effectue la plupart des fonctions du conseiller, telles que la communication
 * des charges à Network Dispatcher, qui seront utilisées dans l'algorithme
 * de pondération de Network Dispatcher. La base du conseiller effectue également
 * des opérations de connexion et de fermeture de socket, et fournit des
 * méthodes d'envoi et de réception qui seront utilisées par le conseiller.
 * Le conseiller n'est lui-même utilisé que pour l'envoi et la réception
 * de données vers/sur le port du serveur conseillé.
 * Les méthodes TCP de la base du conseiller sont programmées pour calculer la charge.
 * Un indicateur de constructeur de ADV_base
 * remplace, si vous le souhaitez, la charge existante par la nouvelle charge
 * renvoyée pour le conseiller.
 *
 * Remarque : En fonction d'une valeur définie dans le constructeur, la base
 * du conseiller fournit la charge à l'algorithme de pondération à un intervalle donné.
 * Si le véritable conseiller n'a pas terminé ses opérations afin de
 * renvoyer une charge valide, la base du conseiller utilise
 * la charge précédente.
 *
 * ATTRIBUTION DE NOM
 *
 * La convention d'attribution de nom est la suivante :
 *
 * - Le fichier doit se trouver dans les répertoires Network Dispatcher
 * suivants :
 *
 *     nd/servers/lib/CustomAdvisors/
 *     (nd\servers\lib\CustomAdvisors sous Windows 2000)
 *
 * - Le nom du conseiller doit être précédé de "ADV". Il peut
 * cependant n'être lancé qu'à partir du nom. Par exemple, le
 * conseiller peut être lancé avec "modèle".
 *
 * - Le nom du conseiller doit être en minuscules.
 *
 * En respectant ces règles, le chemin et le nom du conseiller
 * donné en exemple sont les suivants :
 *
 *     <répertoire de base>/lib/CustomAdvisors/ADV_sample.class
 *
 *
 * les conseillers, tout comme les autres éléments de Network
 * Dispatcher, doivent être compilés avec la version recommandée
 * de Java.
 * Pour pouvoir accéder aux classes de Network Dispatcher, vérifiez
```

```

* que le fichier ibmnd.jar
* (situé dans le sous-répertoire lib du
* répertoire de base) figure dans la classe d'environnement
* CLASSPATH du système.
*
*
* Méthodes fournies par ADV_Base :
*
* - ADV_Base (Constructeur) :
*
*   - Paramètres
*     - String sName = Nom du conseiller
*     - String sVersion = Version du conseiller
*     - int iDefaultPort = Numéro de port par défaut utilisé par le conseiller
*     - int iInterval = Intervalle que doivent utiliser les serveurs
*     - String sDefaultLogFileName = Non utilisé. indiquer "".
*     - boolean replace = True - remplacement de la valeur de la charge
*                               calculée par la base du conseiller
*                               False - ajout à la valeur de la charge calculée
*                               par la base du conseiller
*   - Return
*     - Les constructeurs n'ont pas de valeurs de retour.
*
* la base de conseiller étant basée sur une arborescence,
* le conseiller a de nombreuses autres méthodes
* d'utilisation à sa disposition. Ces méthodes peuvent
* être référencées en utilisant le paramètre CALLER dans
* getLoad().
*
* Ces méthodes sont les suivantes :
*
* - send - Envoie un paquet de données concernant la connexion
*          socket établie sur le port spécifié du serveur.
*   - Paramètres
*     - String sDataString - Les données à envoyer se présentent
*       sous forme de chaîne
*   - Return
*     - int RC - Indique si les données ont été correctement
*       envoyées ; un entier négatif indique une
*       erreur.
*
* - receive - Reçoit des informations de la connexion socket.
*   - Paramètres
*     - StringBuffer sbDataBuffer - Données reçues pendant l'appel
*       de réception
*   - Return
*     - int RC - Indique si les données ont été correctement
*       reçues ; un zéro indique que les données ont été
*       envoyées ; un entier négatif indique une erreur.
*
* Si la fonction fournie par la base du conseiller n'est pas
* suffisante, vous pouvez créer la fonction appropriée dans
* le conseiller et les méthodes fournies par la base du
* conseiller seront alors ignorées.
*

```



```

* Un point important est de savoir si
* la charge renvoyée doit être appliquée à la charge
* générée dans la base du conseiller, ou la remplacer ;
* il existe des exemples valides dans les deux cas.
*
* Cet exemple concerne principalement le conseiller HTTP
* Dispatcher. Il fonctionne très simplement :
* une demande d'envoi (demande http principale) est émise.
* Dès que la réponse est reçue, la méthode getLoad se termine,
* indiquant à la base du conseiller d'arrêter de chronométrer.
* La méthode est alors terminée. Les informations renvoyées
* ne sont pas analysées, la charge est fonction du temps
* nécessaire pour effectuer les opérations d'envoi et de réception.
*/

```

```

package CustomAdvisors;
import com.ibm.internet.nd.advisors.*;

public class ADV_sample extends ADV_Base implements ADV_MethodInterface
{
    Chaîne COPYRIGHT = "(C) Copyright IBM Corporation 1997, Tous
    droits réservés.\n";

    static final String  ADV_NAME          = "Type";
    static final int     ADV_DEF_ADV_ON_PORT = 80;
    static final int     ADV_DEF_INTERVAL  = 7;

    // Remarque : La plupart des protocoles de serveur
    // requièrent un retour chariot ("\r") et un passage à
    // la ligne ("\n") à la fin des messages. Si tel est le
    // cas, incluez-les dans la chaîne ci-dessous.
    static final String  ADV_SEND_REQUEST  =
        "HEAD / HTTP/1.0\r\nAccept: */*\r\nUser-Agent: " +
        "IBM_Network_Dispatcher_HTTP_Advisor\r\n\r\n";

    /**
     * Constructeur.
     *
     * Paramètres : Aucun, mais le constructeur de ADV_Base
     * comporte plusieurs paramètres qui doivent lui être transmis.
     *
     */
    public ADV_type()
    {
        super( ADV_NAME,
            "2.0.0.0-03.27.98",
            ADV_DEF_ADV_ON_PORT,
            ADV_DEF_INTERVAL,
            "", // not used
            false);
        super.setAdvisor( this );
    }

    /**

```

```

* ADV_AdvisorInitialize
*
* Toute initialisation spécifique au conseiller qui
* doit être mise en oeuvre après le démarrage de
* la base du conseiller.
* Cette méthode n'est appelée qu'une seule fois et n'est
* généralement pas utilisée.
*/
public void ADV_AdvisorInitialize()
{
    return;
}

/**
* getLoad()
*
* Cette méthode est appelée par la base du conseiller pour terminer
* l'opération du conseiller, basée sur des détails propres au protocole.
* Dans cet exemple de conseiller, une seule opération d'envoi
* et de réception est nécessaire ; si une logique plus
* complexe est nécessaire, il est possible d'émettre des
* envois et réceptions multiples. Par exemple, une réponse
* peut être reçue et sa syntaxe peut être analysée. Sur la base
* des informations obtenues, un autre ordre d'envoi et de
* réception peut alors être émis.
*
* Paramètres :
*
* - iConnectTime - la charge actuelle car elle fait référence au temps
*                  nécessaire à l'établissement d'une connexion
*                  avec le serveur sur le port spécifié.
*
* - caller - Une référence à la classe de la base du conseiller
*            dans laquelle les méthodes fournies par Network
*            Dispatcher doivent répondre à de simples demandes
*            TCP, principalement des demandes d'envoi et de
*            réception
*
* Résultats :
*
* - La charge - Valeur exprimée en millisecondes, pouvant être
*   ajoutée à la charge existante, ou la remplacer, suivant la
*   valeur de l'indicateur "replace" du constructeur.
*
* Plus la charge est importante, plus le serveur met de temps
* à répondre. Par conséquent, la pondération de l'équilibrage
* de charge restera dans Network Dispatcher.
*
* Si la valeur est négative, il s'agit d'une erreur. Une erreur
* du conseiller indique le serveur auquel le conseiller tente
* d'accéder n'est pas accessible et qu'une défaillance a été
* identifiée.
Network Dispatcher ne tentera pas d'équilibrer

```

```

*   la charge d'un serveur défaillant. Network Dispatcher
*   reprendra l'équilibrage de charge sur le serveur lorsqu'une
*   valeur positive sera reçue.
*
*   La valeur zéro n'est généralement pas renvoyée ; Network
*   Dispatcher traite une charge de zéro de manière spéciale.
*   Zéro est censé indiquer un état inconnu. Network Dispatcher
*   affecte donc une pondération élevée en retour.
*/
public int getLoad(int iConnectTime, ADV_Thread caller)
{
int iRc;
int iLoad = ADV_HOST_INACCESSIBLE;  // -1

// Send tcp request
iRc = caller.send(ADV_SEND_REQUEST);
if (iRc >= 0)
{
// Réception
StringBuffer sbReceiveData = new StringBuffer("");
iRc = caller.receive(sbReceiveData);

// En cas de bonne réception, une charge de zéro est renvoyée.
// Ceci s'explique par le fait que l'indicateur "replace" a la
// valeur false, qui indique que la charge élaborée dans le
// conseiller de base doit être utilisée.
// Etant donné que les données renvoyées n'ont pas été utilisées,
// aucune charge supplémentaire n'est requise.

// Remarque : La charge de la base du conseiller ne doit pas
// être égale à zéro. Par conséquent, aucune charge égale à zéro
// n'est renvoyée dans le but de calculer la pondération.
if (iRc >= 0)
{
iLoad = 0;
}
}
return iLoad;
}

} // End - ADV_type

```

Annexe G. Exemple de configuration de haute disponibilité à deux niveaux utilisant Dispatcher, CBR et Caching Proxy

Cette annexe décrit comment définir une configuration de haute disponibilité à deux niveaux regroupant les capacités de deux composants Network Dispatcher (Dispatcher et CBR) et Caching Proxy.

Configuration de la machine serveur

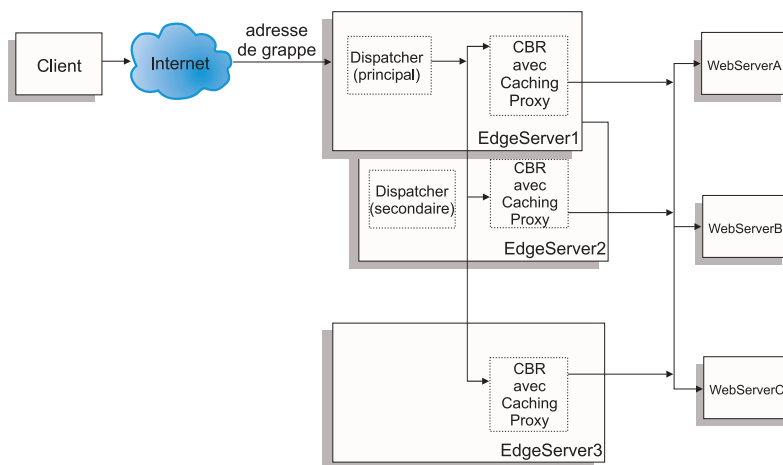


Figure 30. Exemple de configuration de haute disponibilité à deux niveaux utilisant Dispatcher, CBR et Caching Proxy

Le serveur suivant est configuré pour la figure 30 :

- **EdgeServer1** : machine Dispatcher primaire (haute disponibilité) co-implantée avec CBR et Caching Proxy équilibrant la charge des serveurs Web.
- **EdgeServer2** : machine Dispatcher de secours (haute disponibilité) co-implantée avec CBR et Caching Proxy.
- **EdgeServer3** : CBR et machine Caching Proxy.
- **ServeurWebA**, **ServeurWebB**, **ServeurWebC** : serveurs Web périphériques.

La figure 30 montre une représentation de base de l'équilibrage de la charge de plusieurs serveurs (**EdgeServer1**, **EdgeServer2**, **EdgeServer3**) sur plusieurs serveurs Web périphériques. Le composant CBR utilise Caching Proxy pour acheminer les demandes vers les serveurs Web périphériques en fonction de l'URL. Le composant Dispatcher permet d'équilibrer la charge des composants

CBR sur les serveurs Edge Server. La fonction haute disponibilité de Dispatcher permet d'assurer l'acheminement des demandes vers les serveurs périphériques même en cas de défaillance de la machine haute disponibilité primaire (EdgeServer1).

Instructions de configuration de base :

- Configurez Caching Proxy de la même façon sur tous les serveurs Edge Server. Pour améliorer l'accessibilité globale aux pages Web sur les serveurs périphériques, configurez Caching Proxy pour permettre le stockage en mémoire cache. Les serveurs Edge Server peuvent ainsi y placer les pages Web les plus souvent demandées. Pour plus d'informations sur la configuration de Caching Proxy, reportez-vous au manuel *IBM WebSphere Edge Server for Multiplatforms Administration Guide*.
- Définissez l'adresse de la grappe et les ports de la même façon dans les composants CBR et Dispatcher de Network Dispatcher.
- Configurez le composant CBR de la même façon sur tous les serveurs Edge Server. Utilisez les serveurs Web A, B et C sur les ports que vous souhaitez définir pour la grappe. Pour plus d'informations sur la configuration de CBR, reportez-vous au «Chapitre 7. Configuration du composant CBR» à la page 83.
- Configurez le composant Dispatcher de la même façon sur les serveurs Edge Server 1 et 2. Définissez tous les serveurs Edge Server comme serveurs des ports que vous souhaitez définir pour la grappe dont la charge est équilibrée par Dispatcher. Pour plus d'informations sur la configuration de Dispatcher, reportez-vous au «Chapitre 5. Configuration du composant Dispatcher» à la page 57.
- Configurez Edge Server 1 comme serveur de haute disponibilité primaire et Edge Server 2 comme serveur de haute disponibilité de secours. Pour plus d'informations, reportez-vous à la section «Haute disponibilité» à la page 173.

Remarque :

1. Vous devez mettre à jour le nom d'hôte (www.entreprise.com) associé à l'adresse de la grappe dans le fichier de configuration de Caching Proxy au niveau de l'instruction "Hostname".
2. Pour éviter l'affichage des adresses des serveurs périphériques dans l'URL, associez la valeur "yes" à l'instruction "SendRevProxyName" du fichier de configuration de Caching Proxy.
3. Pour assurer un stockage efficace en mémoire cache des pages Web, associez la valeur "ON" à l'instruction "Caching" et

augmentez la valeur affectée à l'instruction "CacheMemory" en fonction de la taille requise dans le fichier de configuration de Caching Proxy.

4. Pour effectuer le stockage en mémoire cache en fonction du nom d'URL des communications entrantes et non de l'adresse IP, ajoutez une ligne à l'instruction Proxy sous la section Mapping Rules du fichier de configuration de Caching Proxy. Lignes de l'exemple auxquelles font référence les remarques 1 à 4 ci-dessus :

```
Hostname          www.entreprise.com
SendRevProxyName  yes
Caching           ON
CacheMemory       128000 K
Proxy             /* http://www.entreprise.com/* www.entreprise.com
```

5. N'oubliez pas d'affecter un alias à l'adresse de grappe de la carte d'interface réseau de EdgeServer1 et à l'adresse de grappe de de l'unité de bouclage des autres serveurs Edge Server.
6. Si les serveurs Edge Server fonctionnent sous Linux, il est nécessaire d'installer un correctif pour ce dernier. Pour plus d'informations, reportez-vous à la section «Installation du correctif du noyau Linux (pour supprimer les réponses ARP sur l'interface de bouclage)» à la page 72.
7. Avec CBR, l'affinité de port (délai de maintien de routage) ne doit pas être utilisée conjointement aux règles Contenu, sinon, ces dernières ne sont pas appliquées lors du traitement des demandes envoyées aux serveurs Web périphériques.

Fichiers de configuration exemple :

Les fichiers de configuration exemple suivants sont identiques à ceux créés lors de la définition de la configuration de Edge Server comme illustré à la figure 30 à la page 401. Ils correspondent aux fichiers des composants Dispatcher et CBR de Network Dispatcher. Dans ces fichiers, une seule carte de réseau Ethernet est utilisée pour chaque machine Edge Server et toutes les adresses sont représentées dans un sous-réseau privé. Les fichiers de configuration exemple utilisent les adresses IP suivantes pour les machines spécifiées :

- EdgeServer1 (Edge Server haute disponibilité primaire) : 192.168.1.10
- EdgeServer2 (Edge Server haute disponibilité de secours) : 192.168.1.20
- EdgeServer3 (Edge Server de mise en cache des pages Web) : 192.168.1.30
- Adresse de la grappe du site Web : 192.168.1.11
- ServeurWebA à C (serveurs Web périphériques) : 192.168.1.71, 192.168.1.72 et 192.168.1.73

Fichier de configuration exemple du composant Dispatcher d'un serveur Edge Server haute disponibilité primaire :

```
ndcontrol executor start

ndcontrol cluster add 192.168.1.11 primaryhost 192.168.1.10

ndcontrol port add 192.168.1.11:80

ndcontrol server add 192.168.1.11:80:edgeserver1 address 192.168.1.10

ndcontrol server add 192.168.1.11:80:edgeserver2 address 192.168.1.20

ndcontrol server add 192.168.1.11:80:edgeserver3 address 192.168.1.30

ndcontrol manager start manager.log 10004

ndcontrol highavailability heartbeat add 192.168.1.10 192.168.1.20
ndcontrol highavailability backup add primary auto 4567
```

Fichier de configuration exemple du composant CBR des serveurs Edge Server :

```
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
```

Annexe H. Ressources supplémentaires

Accès à la ligne de commande

Dans plusieurs circonstances, vous pouvez utiliser les touches du clavier ou une combinaison de touches au lieu de manier votre souris pour certaines opérations. De nombreuses options de menu peuvent être appelées par le clavier.

Consultez la documentation de votre système d'exploitation pour obtenir des instructions relative à l'utilisation du clavier.

Obtention de l'aide en ligne

Network Dispatcher comprend une aide en ligne qui décrit les tâches que vous effectuerez lors de l'installation, de la planification, de la configuration et de l'utilisation du produit.

Pour obtenir l'aide relative à la fenêtre affichée, cliquez sur le point d'interrogation (?) dans le coin supérieur droit. Sélectionnez l'une des options suivantes :

Aide sur les zones

Aide contextuelle relative à la tâche effectuée.

Procédures

Liste des tâches liées à la fenêtre affichée.

Table des matières

Table des matières de toutes les informations d'aide.

Index Index alphabétique des rubriques d'aide.

Informations de référence

Pour des informations supplémentaires sur l'utilisation de Network Dispatcher, consultez les sites suivants :

- le site Web de WebSphere Edge Server :
<http://www.ibm.com/software/webservers/edgeserver>
- le site Web Network Dispatcher technote :
<http://www.ibm.com/software/webservers/edgeserver/support.html>
Cliquez sur **Search for Network Dispatcher hints and tips**.

Annexe I. Remarques

La mention de produits, de logiciels ou de services IBM dans le présent document n'implique aucunement l'intention d'IBM de les introduire dans tous les pays dans lesquels il intervient. Toute référence à un produit, un programme ou un service IBM n'est pas sensée établir ou impliquer que les produits, programmes ou services IBM peuvent être utilisés. Tout produit, programme ou service équivalent sur le plan fonctionnel aux produits, programmes ou services IBM peut être utilisé à leur place s'il fait partie de la propriété intellectuelle d'IBM ou est soumis à tout autre droit protégé légalement. L'évaluation et la vérification du fonctionnement conjointement à d'autres produits, exceptés ceux désignés expressément par IBM, relève de la responsabilité de l'utilisateur.

IBM peut détenir des brevets ou des demandes de brevet sur certains sujets décrits dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Vous pouvez adresser des demandes de licence à IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
La Défense 5
2, avenue Gambetta
92066 - Paris-La Défense CEDEX
France

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Le logiciel sous licence décrit dans le présent document et tous les éléments sous licence disponibles pour celui-ci sont fournis par IBM dans les conditions stipulées par le contrat de clientèle IBM.

Le présent document n'est pas destiné à une utilisation en environnement de production, il est fourni en l'état, sans garantie d'aucune sorte et toutes les garanties y sont dénoncées, y compris la garantie de qualité marchande et de bon fonctionnement dans un but donné.

Ce produit comprend le logiciel informatique créé et distribué par CERN. Ce texte doit figurer intégralement dans chaque produit comprenant le logiciel informatique CERN inclus ou en faisant partie.

Marques

Les termes qui suivent sont des marques d'International Business Machines Corporation dans certains pays.

AIX

IBM

IBMLink

LoadLeveler

NetView

OS/2

WebSphere

Lotus est une marque de Lotus Development Corporation dans certains pays.

Domino est une marque de Lotus Development Corporation dans certains pays.

Tivoli est une marque de Tivoli Systems, Inc dans certains pays.

Java et toutes les marques et logos incluant Java sont des marques de Sun Microsystems, Inc. dans certains pays.

Solaris est une marque de Sun Microsystems, Inc. dans certains pays.

Microsoft et Windows 2000 sont des marques de Microsoft Corporation dans certains pays.

Cisco est une marque de Cisco Systems, Inc. dans certains pays.

HP est une marque de Hewlett-Packard dans certains pays.

Linux est une marque de Linus Torvalds.

Red Hat est une marque enregistrée de Red Hat, Inc.

UNIX est une marque enregistrée de The Open Group dans certains pays.

D'autres sociétés sont propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

Glossaire

A

ACK : Bit de contrôle n'occupant aucun espace séquentiel, qui indique que la zone d'accusé de réception de ce segment précise le prochain numéro de séquence à recevoir par l'émetteur de ce segment, d'où accusant réception de tous les numéros de séquence précédents.

adresse : Code unique affecté à chaque unité ou poste de travail connecté à un réseau. Une adresse IP standard est une zone d'adresse 32 bits. Cette zone est constituée de deux parties : la première correspond à l'adresse réseau et la seconde au numéro d'hôte.

adresse à contacter : Dans le cadre des fonctions de haute disponibilité de Dispatcher, adresse du poste cible auquel le conseiller doit envoyer des pings pour vérifier si ce poste répond.

adresse cible : Adresse du poste partenaire de haute disponibilité auquel des signaux de présence et des réponses sont envoyés.

adresse de grappe : Sous Dispatcher, adresse à laquelle les clients se connectent.

adresse de non-réacheminement (nfa) : Adresse IP principale du poste Network Dispatcher, utilisée pour l'administration et la configuration.

Adresse de retour : Adresse IP ou nom d'hôte unique. Ils sont configurés sur la machine Dispatcher et utilisés par Dispatcher comme adresse source lors de l'équilibrage de charge des demandes client sur le serveur.

adresse du serveur : Code unique attribué à chaque ordinateur fournissant des services partagés à d'autres ordinateurs d'un réseau ; par exemple, un serveur de fichiers, un serveur d'impression ou un serveur de messagerie. Une adresse IP standard est une zone d'adresse 32 bits. Il peut s'agir de l'adresse IP en notation décimale ou du nom d'hôte.

adresse IP : Adresse Internet Protocol. Adresse unique 32 bits, indiquant l'emplacement réel de chaque unité ou poste de travail d'un réseau. Elle est également désignée par adresse Internet.

adresse MAC : Concept du domaine des réseaux locaux ou de l'émulation de réseaux locaux.

adresse source : Dans le cadre des fonctions de haute disponibilité de Dispatcher, adresse du poste partenaire de haute disponibilité envoyant des signaux de présence.

affinité trans ports : L'affinité trans ports se définit comme l'extension à plusieurs ports de la fonction affinité (maintien de routage). Voir également délai de maintien de routage.

agent : (1) En gestion de systèmes, utilisateur qui, pour une interaction particulière, a assumé un rôle d'agent. (2) Entité représentant un ou plusieurs objets gérés (a) en émettant des notifications relatives aux objets et (b) en traitant les demandes d'opérations de gestion émises par les gestionnaires pour modifier ou consulter les objets.

alias : Autre nom attribué à un serveur. Grâce à l'alias, le serveur est indépendant du nom de sa machine hôte. L'alias doit être défini dans le serveur de noms de domaine.

alias de bouclage : Seconde adresse IP associée à l'interface de bouclage. Cette adresse présente l'avantage de ne pas apparaître sur une interface réelle.

API : Interface de programme d'application (Application programming interface). Interface (conventions d'appellation) par laquelle un programme d'application accède au système d'exploitation et autres services. L'API est définie au niveau du code source et apporte un niveau d'abstraction entre l'application et le noyau (ou autres utilitaires privilégiés) afin de garantir la portabilité du code.

assistant : Dans une application, dialogue utilisant des instructions étape par étape pour guider l'utilisateur dans une tâche spécifique.

C

Caching Proxy : Serveur proxy de mise en mémoire cache pouvant contribuer à accélérer les temps de réponse grâce à des schémas de mise en mémoire cache extrêmement efficaces. Un filtrage PICS souple aide les administrateurs réseau à contrôler l'accès aux informations du Web à un emplacement central.

CBR : Abréviation de Content Based Routing. Composant de Network Dispatcher. CBR utilise Caching Proxy pour équilibrer la charge des demandes entrantes, en fonction du contenu de la page Web qui utilise des types de règle précis, sur des serveurs HTTP ou HTTPS.

cbrcontrol : Fournit l'interface du composant Content Based Router de Network Dispatcher.

cbrserver : Dans Content Based Router, traite les demandes de l'exécuteur, du gestionnaire et des conseillers.

CGI : Abréviation de Common Gateway Interface. Norme permettant l'échange d'informations entre un serveur Web et un programme externe. Ce dernier peut être écrit dans n'importe quel langage pris en charge par le système d'exploitation et permet d'effectuer des tâches qui ne sont généralement pas exécutées par le serveur, par exemple, le traitement des formulaires.

Cisco Consultant : Composant d'IBM Network Dispatcher. Cisco Consultant utilise la technologie Network Dispatcher pour fournir en temps réel des informations sur l'équilibrage de charge à Cisco Content Services Switch.

Cisco CSS Switch : Il s'agit de l'un des relais CSS 11000 series de Cisco, utilisé pour l'acheminement des paquets et le routage du contenu.

client : Système ou processus informatique demandant un service à un autre système ou processus informatique. Par exemple, un poste de travail ou un ordinateur personnel demandant des documents HTML à un serveur Web Lotus Domino Go est un client de ce serveur.

cohabitation : Lorsque vous ne disposez pas d'une machine dédiée, Dispatcher est installé sur la machine dont il assure l'équilibrage de charge.

Remarque : La co-implantation s'applique uniquement aux systèmes d'exploitation AIX, Red Hat Linux et Solaris.

Co-implantation d'adresses multiples : Dans une configuration de co-implantation d'adresses multiples, le client peut indiquer un adresse de serveur co-implanté différente de celle de non-acheminement (NFA). Voir aussi Co-implantation.

conseiller : Fonction de Network Dispatcher. Les conseillers collectent et analysent les informations renvoyées par chaque serveur, puis en informent le gestionnaire.

conseiller de contact (reach) : Sous Dispatcher, conseiller qui lance des pings vers une cible déterminée, puis indique si cette cible répond ou non.

Conversion d'adresses réseau : NAT ou Network Address Translator, Virtual LAN. Périphérique en cours de développement permettant d'étendre les adresses Internet déjà utilisées. Il permet l'utilisation d'adresses dupliquées dans une entreprise et d'une adresse unique à l'extérieur.

D

délai de maintien de routage : Délai entre la fermeture d'une connexion et l'ouverture d'une nouvelle connexion au cours de laquelle un client sera renvoyé au même serveur utilisé lors de la première connexion. Passé le délai de maintien de routage, le client peut être envoyé à un serveur autre que le premier.

délai d'expiration : Intervalle de temps alloué à une opération.

démon : Contrôleur de disque et d'exécution. Programme non impliqué explicitement, qui attend certaines conditions pour agir. L'idée est que le logiciel n'a pas besoin de savoir que le démon est actif (bien que le programme effectue souvent une opération uniquement parce qu'il appellera implicitement un démon).

Dispatcher : Composant d'Network Dispatcher qui permet l'équilibrage efficace du trafic TCP ou UDP entre des groupes de serveurs reliés. La machine Dispatcher correspond au serveur qui exécute le code Dispatcher.

E

état down (hors service) : Interruption de toutes les connexions actives à un serveur et arrêt de l'envoi de nouvelles connexions ou de nouveaux paquets à ce serveur.

état FIN : Etat d'une transaction terminée. Une fois qu'une transaction est à l'état FIN, le programme récupérateur d'Network Dispatcher peut libérer la mémoire réservée à la connexion.

état up (en service) : Permettre à un serveur de recevoir de nouvelles connexions.

Ethernet : Type standard de réseau local (lan). Il permet à plusieurs systèmes d'accéder à tout moment au support de transmission sans coordination préalable, évite les conflits à l'aide des fonctions de détection et de report de porteur et résout les conflits éventuels en utilisant les options de détection et de transmission des collisions. Les protocoles de logiciels utilisés par les systèmes Ethernet varient, mais incluent TCP/IP.

Evolutivité : Capacité d'adaptation d'un système à une intensité d'utilisation, de volume ou de demande supérieure ou inférieure. Par exemple, un système évolutif peut s'adapter efficacement pour gérer de petits ou grands réseaux exécutant des tâches dont la complexité est variable.

exécuteur : Fonctions de Dispatcher. L'exécuteur achemine des demandes aux serveurs TCP ou UDP et contrôle également le nombre des connexions nouvelles, actives et terminées, puis regroupe les connexions terminées ou réinitialisées afin de récupérer de l'espace mémoire. L'exécuteur fournit les connexions nouvelles et actives au gestionnaire. Dans Cisco Consultant, l'exécuteur détient les informations de configuration ainsi que les informations nécessaires à la connexion à Cisco CSS Switch.

F

FIN : Bit de contrôle occupant un seul numéro de séquence, qui indique que l'émetteur n'enverra aucun autre contrôle ou donnée occupant un espace séquentiel.

FQDN : Abréviation de Fully Qualified Domain Name. Nom complet d'un système, comprenant son nom d'hôte local et son nom de domaine avec un domaine de niveau supérieur (tld). Par exemple, "venera" est un nom d'hôte et "venera.isi.edu" est un nom FQDN. Le nom FQDN doit permettre de déterminer l'adresse Internet unique de n'importe quel hôte présent sur Internet. Ce processus, appelé "résolution de nom", utilise le système DNS (Domain Name System).

FTP (File Transfer Protocol) : Protocole d'application permettant le transfert de fichiers à destination et en provenance d'ordinateurs en réseau. Le protocole FTP requiert un ID utilisateur et, le cas échéant, un mot de passe permettant l'accès aux fichiers d'un système hôte éloigné.

G

gestionnaire : Fonctions réseau de Dispatcher. Le gestionnaire définit des pondérations basées sur les compteurs internes de l'exécuteur et sur les informations renvoyées par les conseillers. L'exécuteur utilise ensuite les pondérations pour effectuer un équilibrage de charge.

Gestionnaire de paquets Red Hat (RPM) : Gestionnaire de paquets Red Hat (Red Hat Package Manager).

grappe : Sous Dispatcher, groupe de serveurs TCP ou UDP utilisés pour le même but et identifiés par un seul nom d'hôte. Voir aussi cellule.

GRE : Abréviation de Generic Routing Encapsulation. Protocole permettant de transmettre un protocole réseau arbitraire A à un autre protocole arbitraire B en encapsulant les paquets du protocole A dans des paquets GRE, qui sont à leur tour intégrés à des paquets du protocole B.

H

haute disponibilité : Fonction de Dispatcher permettant à un Dispatcher de prendre le contrôle d'un autre si ce dernier est défaillant pour une raison quelconque.

haute disponibilité réciproque : La haute disponibilité réciproque permet à deux machines Dispatcher de jouer, l'une pour l'autre, le rôle de machine principale et de secours. Voir aussi machine de secours (backup), haute disponibilité, machine principale.

hôte : Ordinateur connecté à un réseau, fournissant un point d'accès à ce réseau. Il peut s'agir d'un client et/ou d'un serveur.

HTML : Abréviation de Hypertext Markup Language. Langage permettant de créer des documents hypertexte. Ces derniers comportent des liens avec d'autres documents contenant des informations

complémentaires sur le terme ou le sujet mis en évidence. HTML contrôle, par exemple, le format du texte et de la position des zones d'entrée de formulaire, ainsi que les liens navigables.

HTTP (Hypertext Transfer Protocol) : Protocole permettant de transférer et d'afficher des documents hypertexte.

I

ICMP : Abréviation d'Internet Control Message Protocol. Protocole qui permet la génération de messages d'erreur, de test et d'information relatifs aux conditions de transmission entre un serveur hôte et une passerelle vers Internet.

IMAP : Abréviation d'Internet Message Access Protocol. Protocole permettant au client d'accéder à des messages électroniques placés dans un serveur et de les manipuler. Il permet la manipulation à distance de dossiers de messages (boîtes aux lettres), suivant un procédé équivalent à celle des boîtes aux lettres locales.

interface de bouclage : Interface qui ignore les fonctions de communication non nécessaires lorsque les informations sont adressées à une entité du même système.

Internet : Ensemble mondial de réseaux interconnectés utilisant la série de protocoles Internet et permettant un accès public.

intranet : Réseau privé sécurisé intégrant des normes et applications Internet (par exemple, des navigateurs Web) à l'infrastructure de gestion de réseau informatique existante d'une entreprise.

IP : Abréviation de Internet Protocol. Protocole sans connexion, acheminant des données via un réseau ou des réseaux interconnectés. Le protocole IP sert d'intermédiaire entre les couches de protocole supérieures et la couche physique.

IPSEC : Abréviation de Internet Protocol Security. Norme de développement pour la sécurité au niveau de la couche réseau ou de traitement des paquets transmis lors des communications réseau.

journalisation binaire : Permet de stocker les informations du serveur dans des fichiers binaires et de traiter ces fichiers afin d'analyser les informations du serveur recueillies.

L

largeur de bande : Différence entre la fréquence la plus élevée et la fréquence la plus basse d'une voie de transmission ; quantité de données pouvant être envoyée par un circuit de communication particulier par seconde.

lbc : Abréviation de load-balancing Consultant

lbccontrol : Dans Cisco Consultant, fournit l'interface de Cisco CSS Switch.

lbcserver : Dans Cisco Consultant, contient les informations de configuration et exécute les commandes.

M

machine de secours (backup) : Dans le cadre des fonctions de haute disponibilité de Dispatcher, partenaire de la machine principale (primary). Elle contrôle l'état de la machine principale (primary) et la remplace si nécessaire. Voir aussi haute disponibilité, machine principale

machine principale (primary) : Dans le cadre des fonctions de haute disponibilité de Dispatcher, poste qui démarre en tant que poste d'acheminement actif des paquets. Son partenaire, la machine de secours (backup), contrôle l'état de la machine principale et la remplace si nécessaire. Voir aussi machine de secours (backup), haute disponibilité.

Mailbox Locator : Composant de Network Dispatcher. Dans le cas des protocoles IMAP et POP3, le proxy CBR choisit un serveur approprié en fonction de l'ID utilisateur et du mot de passe.

masque de réseau : Dans le cadre de la gestion de sous-réseaux Internet, masque de 32 bits permettant d'identifier les bits d'adresse de sous-réseau de la partie hôte d'une adresse IP.

masque de sous-réseau : Dans le cadre de la gestion de sous-réseaux Internet, masque de 32 bits permettant d'identifier les bits d'adresse de sous-réseau de la partie hôte d'une adresse IP.

mesure : Processus ou commande qui renvoie une valeur numérique pouvant être utilisée lors de l'équilibrage de charge sur le réseau, par exemple, le nombre d'utilisateurs connectés.

mettre au repos : Mettre fin à un processus en permettant l'arrêt normal des opérations.

MIB : (1) Abréviation de Management Information Base. Ensemble d'objets accessibles via un protocole de gestion de réseau. (2) Définition des informations de gestion indiquant les informations accessibles à partir d'un hôte ou d'une passerelle, ainsi que les opérations autorisées.

mlcontrol : Fournit l'interface du composant Mailbox Locator de Network Dispatcher.

mlserver : Dans Mailbox Locator, contient les informations de configuration et exécute les commandes.

N

ndcontrol : Fournit l'interface du composant Dispatcher de Network Dispatcher.

ndserver : Dans Dispatcher, traite les demandes adressées à l'exécuteur, au gestionnaire et aux conseillers à partir de la ligne de commande.

Network Address Port Translation : NAT, également appelé mappage de port. Il permet la configuration de plusieurs démons de serveurs dans un serveur physique unique qui écoutent sur différents numéros de ports.

NIC : Abréviation de Network Interface Card. Carte à circuit installé sur un ordinateur pour établir des connexions physiques à un réseau.

NNTP : Abréviation de Network News Transfer Protocol. Protocole TCP/IP permettant le transfert d'éléments d'informations.

noeud géré : Dans le cadre des communications Internet, poste de travail, serveur ou routeur contenant un agent de gestion de réseau. Dans le cadre du protocole IP (Internet Protocol), le noeud géré contient généralement un agent SNMP.

nom de site : Un nom de site est un nom d'hôte impossible à résoudre, qui sera demandé par le client. Par exemple, un site Web a 3 serveurs (1.2.3.4, 1.2.3.5 et 1.2.3.6) configurés pour le nom de site *www.dnsload.com*. Lorsqu'un client demande ce nom de site, l'une des trois adresses IP du serveur est renvoyée en tant que résolution. Le nom de site doit être un nom de domaine complet, comme *dnsload.com*. Un nom de site incomplet tel que *dnsload* n'est pas un nom de site valide.

nom d'hôte : Nom symbolique attribué à un hôte. Les noms d'hôte sont résolus à des adresses IP via un serveur de noms de domaine.

notation décimale : Représentation syntaxique d'un entier 32 bits constitué de quatre nombres de 8 bits, écrits dans la base 10 et séparés par des points. Elle sert à représenter des adresses IP.

P

paquet : Unité de données acheminées entre une source et une cible sur Internet ou tout autre réseau de commutation de paquets.

pare-feu : Ordinateur qui relie un réseau privé tel qu'une entreprise à un réseau public tel qu'Internet. Il contient des programmes limitant l'accès entre deux réseaux. Voir aussi *passerelle de proxy*.

passerelle : Unité fonctionnelle permettant d'interconnecter deux ordinateurs réseau ayant des architectures différentes.

PICS : Abréviation de Platform for Internet Content Selection. Abréviation de Platform for Internet Content Selection. Les clients prenant en charge PICS permettent aux utilisateurs de déterminer les "rating services" (services de contrôle d'accès) qu'ils souhaitent utiliser et, pour chacun de ces rating services, s'il est acceptable ou non.

ping : Commande qui envoie des paquets de demande d'écho ICMP (Internet Control Message Protocol) à un hôte, à une passerelle ou à un routeur, en espérant recevoir une réponse.

POP3 : Abréviation de Post Office Protocol 3. Protocole permettant l'échange de courrier réseau et l'accès aux boîtes aux lettres.

port : Nombre qui identifie une unité de communication abstraite. Les serveurs Web utilisent par défaut le port 80.

poste de gestion de réseau : Dans le cadre du protocole SNMP (Simple Network Management Protocol), poste exécutant des protocoles d'application de gestion qui surveillent et contrôlent les éléments de réseau.

poste serveur : Serveur relié par Dispatcher à d'autres serveurs dans un seul serveur virtuel. Dispatcher équilibre le trafic entre les postes serveur. Synonyme de serveur groupé.

poste serveur TCP : Serveur relié par Network Dispatcher à d'autres serveurs dans un seul serveur virtuel. Network Dispatcher équilibre le trafic TCP entre les postes serveur TCP. Synonyme de serveur groupé.

priorité : Dans le cadre de l'équilibrage de charge basé sur des règles, niveau d'importance accordé à une règle donnée. Dispatcher évalue les règles du premier niveau de priorité jusqu'au dernier.

Protocole : Ensemble de règles régissant le fonctionnement des éléments d'un système de communication si des communications sont établies. Les protocoles peuvent déterminer les détails de niveau inférieur des interfaces entre des machines, par exemple, l'ordre de transmission des bits d'un octet ; ils peuvent également déterminer les échanges de haut niveau entre les programmes d'application, par exemple, le transfert de fichier.

proximité réseau : Proximité de deux entités connectées en réseau (par exemple, un client et un serveur), déterminée par Site Selector par la mesure de la durée de la procédure aller-retour.

Q

QoS (Quality of Service) : Propriétés de performances d'un service réseau, notamment le débit, le délai de transmission et la priorité. Certains protocoles permettent aux paquets ou aux flots de données d'inclure des spécifications QoS.

R

règle : Dans le cadre de l'équilibrage de charge basé sur des règles, mécanisme de regroupement de serveurs permettant de choisir un serveur en fonction des informations autres que l'adresse de destination ou le port.

Réseau local (LAN) : Réseau local (Local Area Network). Réseau informatique d'unités connectés entre elles, à des fins de communication, dans une zone de taille limitée. Ce réseau local peut être connecté à un réseau plus étendu.

réseau privé : Réseau distinct sur lequel Dispatcher communique avec des serveurs groupés pour des raisons de performances.

RMI : Abréviation de Remote Method Invocation. Partie de la bibliothèque de langages de programmation Java qui permet à un programme Java d'être exécuté sur une machine et d'accéder aux objets et aux méthodes d'un autre programme Java exécuté sur une autre machine.

router : Périphérique chargé d'acheminer des paquets entre des réseaux. La décision d'acheminement dépend des informations de la couche réseau et des tables de routage, souvent élaborées par des logiciels de routage.

S

script CGI : Programme CGI écrit dans un langage de script tel que Perl ou REXX qui utilise l'interface CGI (Common Gateway Interface) pour effectuer des tâches qui ne sont généralement pas exécutées par le serveur, par exemple, le traitement des formulaires.

serveur : Ordinateur fournissant des services partagés à d'autres ordinateurs d'un réseau ; par exemple, un serveur de fichiers, un serveur d'impression ou un serveur de messagerie.

serveur de noms de domaines : DNS. Service de requête global de données réparties et répliquées, généralement utilisé sur Internet pour la conversion des noms d'hôte en adresses Internet. Type de nom

d'hôte utilisé sur Internet, bien que le terme approprié soit "nom de domaine complet". DNS peut être configuré pour utiliser une série de serveurs de noms, en fonction des domaines figurant dans le nom recherché, jusqu'à ce qu'une valeur soit trouvée.

serveur groupé : Serveur relié par Dispatcher à d'autres serveurs dans un seul serveur virtuel. Network Dispatcher équilibre le trafic TCP ou UDP entre ces serveurs groupés.

service : Fonction fournie par un ou plusieurs noeuds, par exemple, HTTP, FTP, Telnet.

shell : Logiciel acceptant et traitant des lignes de commande à partir du poste de travail d'un utilisateur. Le shell Korn constitue un des nombreux shells UNIX disponibles.

signal de présence (heartbeat) : Paquet simple transmis entre deux postes Dispatcher en mode haute disponibilité, utilisé par le poste Dispatcher de secours pour surveiller l'état du poste Dispatcher actif.

Site Selector : Composant Network Dispatcher pour l'équilibrage de charge utilisant le système DNS. Site Selector équilibre la charge sur des serveurs faisant partie d'un réseau étendu (WAN) en utilisant des mesures et des pondérations recueillies à l'aide du composant Metric Server qui s'exécute sur ces serveurs.

SMTP : Abréviation de Simple Mail Transfer Protocol. Dans la série des protocoles, protocole d'application permettant le transfert de messages entre les utilisateurs de l'environnement Internet. Le protocole SMTP indique les séquences d'échange et le format des messages. Il considère que TCP (Transmission Control Protocol) est le protocole sous-jacent.

SNMP : Abréviation de Simple Network Management Protocol. Protocole Internet standard défini par les spécifications STD 15, RFC 1157 et conçu pour gérer les noeuds d'un réseau IP. SNMP ne se limite pas à TCP/IP. Il peut être utilisé pour gérer et surveiller différents types d'équipements, notamment les ordinateurs, les routeurs, les concentrateurs et les chargeurs automatiques de disques.

SPARC : Architecture de processeur modulable.

sscontrol : Fournit l'interface du composant Site Selector de Network Dispatcher.

SSL : Abréviation de Secure Sockets Layer. Plan de sécurité courant développé par Netscape Communications Corp. conjointement avec RSA Data Security Inc. SSL permet l'authentification du serveur par le client, ainsi que le chiffrement de l'ensemble des données et demandes. L'URL d'un serveur sécurisé protégé par SSL commence par https (et non http).

ssserver : Dans Site Selector, gère les demandes adressées au nom de site, au gestionnaire et aux conseillers à partir de la ligne de commande.

stratégie : Dans le cadre des fonctions de haute disponibilité de Dispatcher, mot clé permettant d'indiquer le mode de récupération d'espace à la suite de la défaillance de la machine active.

superutilisateur : Droits non restreints permettant d'accéder à une partie du système d'exploitation AIX, Red Hat Linux ou Solaris, et de modifier celle-ci, et généralement associés à l'utilisateur qui gère le système.

SYN : Bit de contrôle du segment entrant, occupant un seul numéro de séquence, utilisé au début d'une connexion, afin d'indiquer la position de début de la numérotation des séquences.

Système Metric Server : Précédemment appelé Server Monitor Agent (SMA). Metric server fournit au gestionnaire Network Dispatcher des mesures spécifiques au système.

T

TCP : Abréviation de Transmission Control Protocol. Protocole de communication utilisé sur le réseau Internet. TCP permet un échange d'informations hôte à hôte fiable. Il utilise IP comme protocole sous-jacent.

TCP/IP : Abréviation de Transmission Control Protocol/Internet Protocol. Une série de protocoles permettant la communication entre les réseaux, quelles que soient les techniques de communication utilisées dans chaque réseau.

Telnet : Protocole d'émulation de terminal ; protocole d'application TCP/IP destiné au service de connexion éloigné. Telnet permet à un utilisateur d'un site d'accéder à un hôte éloigné comme si le poste de l'utilisateur était connecté directement à cet hôte éloigné.

TTL : Durée (en nombre de secondes) pendant laquelle un client peut enregistrer en mémoire cache la réponse de résolution de nom.

type de règle : Dans le cadre de l'équilibrage de charge basé sur des règles, indicateur des informations devant être évaluées pour déterminer si une règle est vraie.

Type de service (TOS) : Type de service (Type of service). Zone d'octets de 1, dans l'en-tête IP du paquet SYN.

U

UDP : Abréviation de User Datagram Protocol. Dans la série des protocoles Internet, protocole fournissant un service de datagramme sans connexion et non fiable. Il permet à un programme d'application d'une machine ou d'un processus d'envoyer un datagramme à un programme d'application d'une autre machine ou d'un autre processus. UDP utilise le protocole IP (Internet Protocol) pour transmettre des datagrammes.

URI : Universal Resource Identifier. Adresse codée de toute ressource disponible sur le Web (par exemple, un document HTML, une image, un clip video, un programme).

URL : Uniform Resource Locator. Méthode standard permettant d'indiquer l'emplacement d'un objet, généralement une page Web sur Internet. Les adresses URL possèdent la forme des adresses utilisées sur Internet. Elles sont utilisées dans des documents HTML afin de spécifier la cible d'un lien hypertexte qui correspond en général à un autre document HTML (pouvant être stocké sur une autre machine).

V

valeur de début : Dans le cadre de l'équilibrage de charge basé sur des règles, valeur inférieure indiquée pour une règle. La valeur par défaut dépend du type de règle.

valeur de fin : Dans le cadre de l'équilibrage de charge basé sur des règles, valeur supérieure indiquée pour une règle. Cette valeur dépend du type de règle.

valeur par défaut : Valeur, attribut ou option utilisé si aucune valeur n'est indiquée de façon explicite.

voie d'acheminement : Chemin du trafic de réseau entre l'origine et la destination.

VPN : Abréviation de Virtual Private Network (VPN). Réseau composé d'un ou plusieurs tunnels IP sécurisés reliant deux réseaux ou plus.

W

WAN : Wide Area Network. Réseau fournissant des services de communication dans une zone plus étendue que celle prise en charge par un réseau local ou métropolitain et qui peut être utilisé pour fournir des fonctions de transmission publiques.

WAP : Abréviation de Wireless Application Protocol. Norme internationale ouverte pour les applications utilisant des communications sans fil, par exemple l'accès Internet à partir d'un téléphone mobile.

WAS : Abréviation de Websphere Application Server.

Web : Réseau de serveurs HTTP contenant des programmes et des fichiers dont la plupart correspond à des documents hypertexte qui contiennent des liens avec d'autres documents des serveurs HTTP. Désigné également par World Wide Web.

WLM : Abréviation de Workload Manager. Conseiller fourni avec Dispatcher. Le conseiller WLM est conçu pour travailler uniquement avec les serveurs sur gros systèmes OS/390 exécutant le composant MVS Workload Manager (WLM).

Index

Nombres

2MI (Remote Method
Invocation) 213

A

accessibilité 405
Administration à distance 22, 213
adresse de non-acheminement
définition 63, 275, 365, 366
affichage
compteurs internes 274, 366
état
serveurs d'un port 301, 380
une grappe ou toutes les
grappes 270, 364
liste
conseillers fournissant
actuellement des
mesures 264, 332, 361
numéro de version
conseiller 265, 332, 333
gestionnaire 293, 339, 341,
375, 377
paramètres globaux et leurs
valeurs par défaut
pour le gestionnaire 292,
339, 341, 375, 377
pour un conseiller 265, 331,
333
rapport statistique 291, 338, 339,
373, 375
rapport sur l'état d'un
conseiller 264, 330, 333, 359
affinité (maintien de routage)
affinité trans port 197, 198
affinité trans ports 297
cookie actif 200, 307
cookie passif 200, 202, 307
délai de maintien de routage 55,
56, 195, 197, 298, 307
fonctionnement 195
ID SSL (acheminement CBR) 55,
56
mailbox locator 99
maintien de routage (substitution
d'affinité de règle) 199, 312
masque d'adresse de
l'affinité 198

affinité (maintien de routage) (*suite*)
masque de maintien de
routage 197, 198, 297
mettre au repos maintenant 288,
292
mise au repos maintenant 199
option de règle 200
SDA (Server Directed
Affinity) 196
substitution d'affinité de
règle 199
URI 200, 203, 307
affinité d'URI 200, 203, 307
affinité de cookie actif 200, 307
affinité de cookie passif 200, 202,
307
affinité dirigée par le serveur
(SDA) 161, 196
affinité trans port 197
affinité trans ports 297
aide, en ligne 405
aide en ligne 405
aide sur les zones 405
AIX
configuration requise 12
installation 13
ajout
grappe 270, 364
port à une grappe 65, 301, 380
serveur à un port 66, 316, 349,
383
alias
carte d'interface réseau 63, 92
unité de bouclage 67
correctif du noyau Linux 68,
72
apCnsvchits 208
apSvcConnections 208
arrêt
Cisco Consultant 227
conseiller 263, 331, 333
exécuteur 275
gestionnaire 292, 339, 341, 375,
377
assistant, configuration
Dispatcher 4

C

Caching Proxy 79
configuration pour utiliser
CBR 88
carte d'interface réseau
alias 63
Ethernet (pour Solaris) 61
mappage (pour
Windows 2000) 64
carte d'interface réseau Ethernet
ibmnd.conf
configuration Solaris 61
CBR
alias pour la carte d'interface
réseau 92
avec Caching Proxy
configuration 94
connexions SSL 80
conseiller ssl2http 81
mot clé mapport 80
Présentation générale 78
commande ifconfig 92
configuration
Configuration du poste
CBR 88
présentation des tâches 83
configuration matérielle et
logicielle requises 77
échec de cbrcontrol 247
échec de la commande cbrcontrol
sous Solaris 247
échec de ndadmin 247
erreur de syntaxe ou de
configuration 248
incident d'exécution 247
lancement et arrêt 225
non-équilibre des
requêtes 247
paramètres de l'équilibrage de
charge 140
planification 77
tableau de résolution des
incidents 232
utilisation du composant
Dispatcher 54
CBR (Content Based Routing)
configuration
Configuration du poste
CBR 88

- CBR (Content Based Routing) *(suite)*
 - configuration *(suite)*
 - présentation des tâches 83
- Cisco Consultant
 - commandes 357
 - configuration
 - exemple 45
 - installation de la machine
 - CSS 132
 - présentation des tâches 129
 - configuration matérielle et logicielle requises 123
 - définition de l'équilibrage de charge
 - délai d'attente pour le serveur du conseiller 358
 - échec de lbcccontrol 251
 - échec de ndadmin 251
 - échec du lancement 251
 - exécuteur 124
 - gestionnaire 124
 - impossible de créer un registre sur le port 14099 251
 - lancement 227
 - lancement et arrêt 227
 - lbcccontrol 124
 - lbcsrvr 124
 - ndadmin 124
 - paramètres de l'équilibrage de charge
 - délai d'attente pour le serveur du conseiller 359, 361, 362
 - délai de rapport du conseiller 361, 362
 - planification 123
 - tableau de résolution des incidents 234
 - utilisation 227
- clavier 405
- clé privée
 - pour authentification distante 213
- clé publique
 - pour authentification distante 213
- clés
 - ndkeys 157, 214
- co-implantation, Network Dispatcher et le serveur 166
- co-implantation, Network Dispatcher et serveur 60, 66
- co-implantation d'adresses multiples 66
- co-implanté (mot clé) 316
- co-implanter, Network Dispatcher et le serveur 162, 312, 316
- Collecte des données obsolètes 218
- collocated (mot clé) 163
- commande cbrcontrol
 - advisor 260
 - executor 271
 - file 276
 - grappe 266
 - help 278
 - hôte 285
 - journal 286
 - manager 287
 - metric 294
 - port 296
 - rule 303
 - serveur 311
 - set 318
 - status 319
- commande ifconfig 68, 92, 166
- commande lbcccontrol
 - conseiller 358
 - exécuteur 365
 - file 367
 - gestionnaire 372
 - grappe 363
 - help 369
 - host 370
 - log 371
 - metric 378
 - port 380
 - serveur 382
 - set 384
 - status 385
- commande mlcontrol
 - advisor 260
 - executor 271
 - file 276
 - grappe 266
 - help 278
 - hôte 285
 - journal 286
 - manager 287
 - metric 294
 - port 296
 - serveur 311
 - set 318
 - status 319
- commande ndcontrol
 - advisor 260
 - conseiller 66, 67
 - exécuteur 63
 - executor 271
 - file 276
 - gestionnaire 66, 67
- commande ndcontrol *(suite)*
 - grappe 266
 - help 278
 - highavailability 280
 - hôte 285
 - invite 258
 - journal 286
 - manager 287
 - metric 294
 - port 65, 296
 - réduction des paramètres de commande 258
 - rule 303
 - serveur 66, 311
 - set 318
 - status 319
 - subagent 320
- commande netstat 70
- commande route 70, 71
- commandes
 - cbrcontrol
 - advisor 260
 - executor 271
 - file 276
 - grappe 266
 - help 278
 - hôte 285
 - journal 286
 - manager 287
 - metric 294
 - port 296
 - rule 303
 - serveur 311
 - set 318
 - status 319
 - Cisco Consultant 357
 - ifconfig 65, 166
 - affectation d'alias à l'unité de bouclage 68
 - lbcccontrol
 - conseiller 358
 - exécuteur 365
 - file 367
 - gestionnaire 372
 - grappe 363
 - help 369
 - host 370
 - log 371
 - metric 378
 - port 380
 - serveurs, configuration 382
 - set 384
 - status 385
 - mlcontrol
 - advisor 260

- commandes (*suite*)
 - mlcontrol (*suite*)
 - executor 271
 - file 276
 - grappe 266
 - help 278
 - hôte 285
 - journal 286
 - manager 287
 - metric 294
 - port 296
 - serveur 311
 - set 318
 - status 319
 - ndconfig 65, 167
 - ndcontrol
 - advisor 260
 - contrôle du conseiller 66, 67
 - contrôle du gestionnaire 66, 67
 - définition d'un port 65
 - définition d'un serveur 66
 - définition de l'adresse de non-acheminement 63, 275, 365, 366
 - executor 271
 - file 276
 - grappe 266
 - haute disponibilité,
 - contrôle 280
 - help 278
 - hôte 285
 - invite 258
 - journal 286
 - manager 287
 - metric 294
 - port 296
 - rule 303
 - serveur 311
 - set 318
 - sous-agent, configuration
 - SNMP 320
 - status 319
 - netstat
 - contrôle des adresses IP et des alias 70
 - Site Selector 327
 - sscontrol
 - advisor 328
 - file 334
 - help 336
 - manager 337
 - mesure 342
 - nameserver 343
 - rule 344
- commandes (*suite*)
 - sscontrol (*suite*)
 - server 348
 - set 350
 - sitename 351
 - status 355
 - voie d'acheminement
 - suppression d'une voie supplémentaire 70, 71
 - composant Dispatcher
 - affichage d'un écran bleu lors du lancement de l'exécuteur 244
 - affichage incorrect de l'interface graphique 243
 - charge des demandes non équilibrée 239
 - comportement imprévu lors du chargement d'un fichier de configuration volumineux 246
 - configuration
 - configuration d'un réseau privé 191
 - configuration de la machine Network Dispatcher 60
 - présentation des tâches 57
 - configuration matérielle et logicielle requises 47
 - connexion à une machine éloignée 241
 - disparition des fenêtres d'aide 243
 - dysfonctionnement de MS IIS et de SSL 241
 - dysfonctionnement de SNMP 240
 - dysfonctionnement des conseillers 240
 - échec de ndadmin 241
 - échec de ndcontrol 241
 - erreur lors du lancement de ndserver sous Solaris 2.7 242
 - erreur lorsque Caching Proxy est installé 243
 - évitement du trafic retour avec Network Dispatcher par la fonction Path MTU Discovery 244
 - fonction CBR (content-based routing) 54
 - fonction haute disponibilité de Network Dispatcher inopérante en mode réseau étendu 245
 - fonction haute disponibilité inopérante 240
- composant Dispatcher (*suite*)
 - impossible d'ajouter un signal de présence 240
 - impossible d'ouvrir la fenêtre d'aide 242
 - incident d'exécution 239
 - indication par les conseillers que tous les serveurs sont en panne 245
 - lancement 217
 - lancement incorrect de l'interface graphique 242
 - NAT / NAPT 52
 - non réponse du serveur 239
 - paramètres de l'équilibrage de charge 140
 - délai de rapport du conseiller 148
 - délai du serveur du conseiller 148
 - index de filtrage 145
 - Intervalles conseiller 148
 - intervalles gestionnaire 144
 - pondérations 142
 - proportion de l'importance accordée aux données d'état 141
 - seuil de sensibilité 144
 - planification 47
 - réacheminement MAC 52
 - routes supplémentaires (Windows 2000) 240
 - tableau de résolution des incidents 229
 - transmission d'un cadre impossible 243
 - utilisation 217
- composants du produit 48
 - configuration
 - assistant 4
 - CBR (Content Based Routing) 83
 - Cisco Consultant 129
 - composant Dispatcher 57
 - définition d'une grappe 133
 - définition des serveurs faisant l'objet d'un équilibrage de charge 133
 - définition du niveau d'importance des informations de la grappe 134
 - lancement du gestionnaire 134
 - Mailbox Locator 101
 - mappage entre Consultant et CSS 125

- configuration (*suite*)
 - méthodes
 - assistant (CBR) 87
 - assistant (Dispatcher) 60
 - assistant (Mailbox Locator) 104
 - assistant (Site Selector) 118
 - GUI (CBR) 86
 - interface graphique (Cisco Consultant) 131
 - interface graphique (Dispatcher) 59
 - interface graphique (Mailbox Locator) 103
 - interface graphique (Site Selector) 117
 - ligne de commande (CBR) 84
 - ligne de commande (Cisco Consultant) 130
 - ligne de commande (Dispatcher) 58
 - ligne de commande (Mailbox Locator) 102
 - ligne de commande (Site Selector) 116
 - scripts (CBR) 85
 - scripts (Cisco Consultant) 131
 - scripts (Dispatcher) 58
 - scripts (Mailbox Locator) 103
 - scripts (Site Selector) 117
 - port 133
 - Site Selector 115
 - système Metric Server 134
 - tâches avancées 137
 - test 135
 - vérification 71
- Configuration
 - fichiers exemple 387
- configuration logicielle requise
 - composant Dispatcher 47
- Configuration logicielle requise
 - CBR 77
 - Cisco Consultant 123
 - Mailbox Locator 97
 - Site Selector 109
- configuration matérielle requise
 - composant Dispatcher 47
- Configuration matérielle requise
 - CBR 77
 - Cisco Consultant 123
 - Mailbox Locator 97
 - Site Selector 109
- configuration requise
 - AIX 12
 - Linux 17
 - Solaris 20
 - Windows 2000 22
- connecttimeout
 - Cisco Consultant 358
 - Site Selector 328
- connexion/déconnexion 11
- connexions, définition du
 - pourcentage d'importance 141, 270
- connexions actives 208
- connexions SSL
 - configuration de ibmproxy 80
 - conseiller 150
 - incident d'activation 241
 - pour CBR 80
- conseiller Caching Proxy 150
- conseiller DB2 151
- conseiller ftp 260, 328
- conseiller http 260, 328
- conseiller personnalisé 151
- conseiller ssl2http 81, 150
- conseiller WAS (WebSphere Application Server) 152
- conseiller Workload manager (WLM) 155
- conseillers
 - cbrcontrol 260
 - Cisco Consultant
 - affichage de l'état 360, 362
 - arrêt 360, 362
 - délai de connexion du serveur 358, 361
 - délai de rapport 361, 362
 - délai de réception du serveur 359, 362
 - intervalle 358, 361
 - lancement 360, 362
 - Liste 359, 360
 - noms 358
 - port 358
 - rapport sur l'état de 362
 - version de 361, 362
 - composant Dispatcher 146
 - arrêt 263
 - conseiller Caching Proxy 150
 - conseiller self 151, 172
 - conseiller ssl2http 81, 150
 - délai de connexion du serveur 148, 264
 - délai de rapport 148, 263
 - délai de réception du serveur 148, 264
- conseillers (*suite*)
 - composant Dispatcher (*suite*)
 - dépassement du délai de connexion du serveur 260
 - dépassement du délai de réception du serveur 262
 - détection d'erreur rapide 149
 - intervalle 148, 264
 - lancement 67, 263
 - lancement/arrêt 147
 - liste 149, 264
 - noms 260
 - personnaliser 151
 - port 267
 - rapport sur l'état de 264
 - report 265
 - version de 265
 - demande/réponse de conseiller HTTP 161
 - exemples de fichiers de configuration 395
 - lancement 134
 - lbcccontrol 358
 - liste 262
 - Liste 360
 - mlcontrol 260
 - ndcontrol 260
 - option d'URL, conseiller HTTP 161
 - restriction sous Linux 146
 - Site Selector
 - arrêt 331, 333
 - délai de connexion du serveur 328, 332
 - délai de rapport 332, 333
 - délai de réception du serveur 329, 333
 - interval 328
 - intervalle 332
 - lancement 331, 333
 - list 329
 - liste 331, 332
 - loglevel 329
 - noms 328
 - port 260, 328
 - rapport sur l'état de 330, 333
 - version de 332, 333
 - sscontrol 328, 336
- conseillers, composant Network Dispatcher
 - lancement 66
 - liste 361
 - rapport sur l'état de 359
- Content Based Routing 29

- Content Based Routing (*suite*)
 - configuration matérielle et
 - logicielle requises 77
 - paramètres de l'équilibrage de
 - charge 140
 - planification 77
 - tableau de résolution des
 - incidents 232
 - utilisation 225
 - utilisation du composant
 - Dispatcher 54
- conversion d'adresse réseau
 - (NAT) 52

D

- Décompte fin 218
- default.cfg 62, 91, 105, 119
- définition
 - adresse de grappe 65
 - adresse de non-
 - acheminement 60, 63, 275, 365, 366
 - fréquence d'interrogation de
 - l'exécuteur par le
 - gestionnaire 144, 291, 373, 375
 - grappe 270, 364
 - indice de lissage 145, 292, 338, 340, 374, 377
 - intervalle de temps
 - interrogation des serveurs par
 - le conseiller 264, 332, 358, 361
 - mise à jour de l'exécuteur par
 - le gestionnaire 144, 290, 337, 339, 372, 375
 - niveau de journalisation
 - pour le conseiller 215, 264, 332, 359, 361
 - pour le gestionnaire 337, 372
 - nom du fichier journal 331, 360
 - pour le gestionnaire 339, 374
 - pondération maximale
 - pour les serveurs d'un port
 - spécifique 143, 301, 380
 - pondération pour un
 - serveur 290, 293, 316, 349, 375, 383
 - port à une grappe 65, 301, 380
 - pourcentage d'importance de
 - l'équilibrage de charge 270
 - sensibilité aux mises à jour de
 - pondération 144, 292, 338, 340, 374, 377
 - serveur à un port 66, 316, 349, 383

- définition (*suite*)
 - taille maximale du journal
 - pour le conseiller 215, 264, 329, 332, 359, 361
 - pour le gestionnaire 290, 337, 339, 373, 375
 - délai d'attente 217, 268, 272, 299
 - délai FIN
 - modification 218
 - désinstallation
 - sous AIX 14
 - sous Linux 18
 - sous Solaris 21
 - sous Windows 2000 24
 - détection d'attaque de refus de
 - service 204
 - halfopenaddressreport 301
 - maxhalfopen 300
 - diagnostic des incidents
 - affichage d'un écran bleu lors du
 - lancement de l'exécuteur
 - Network Dispatcher 244
 - affichage incorrect de l'interface
 - graphique 243
 - ajout impossible d'un port 249
 - arrêt de la commande
 - cbrserver 248
 - CBR ne fonctionne pas 247
 - ce message d'erreur s'affiche
 - lorsque l'on tente de visualiser
 - l'aide en ligne 242
 - charges non indiquées par Metric
 - Server 252
 - comportement imprévu lors du
 - chargement d'un fichier de
 - configuration volumineux 246
 - disparition des panneaux
 - d'aide 243
 - dysfonctionnement de Dispatcher,
 - de Microsoft IIS et de SSL 241
 - échec de démarrage de sserver
 - sous Windows 2000 250
 - échec de la commande cbrcontrol
 - ou ndadmin 247
 - échec de la commande cbrcontrol
 - sous Solaris 247
 - échec de la commande lbcccontrol
 - ou ndadmin 251
 - échec de la commande mlcontrol
 - ou ndadmin 249
 - échec de la commande ndcontrol
 - ou ndadmin 241
 - échec de la commande sscontrol
 - ou ndadmin 250

- diagnostic des incidents (*suite*)
 - échec du lancement de
 - lbserver 251
 - équilibrage de charge de Site
 - Selector incorrect 251
 - erreur de syntaxe ou de
 - configuration 248
 - erreur lors de l'exécution de
 - Dispatcher lorsque Caching
 - Proxy est installé 243
 - évitement du trafic retour avec
 - Network Dispatcher par la
 - fonction Path MTU
 - Discovery 244
 - fonction haute disponibilité de
 - Dispatcher inopérante 240
 - fonction haute disponibilité de
 - Network Dispatcher inopérante
 - en mode réseau étendu 245
 - impossible d'ajouter un signal de
 - présence 240
 - impossible de créer un registre
 - sur le port 14099 251
 - incidents courants et
 - solutions 239, 241, 247, 248, 250, 251, 252
 - indication par les conseillers que
 - tous les serveurs sont en
 - panne 245
 - IOException Metric Server sous
 - Windows 2000 252
 - journal de Metric Server indique
 - qu'une signature est nécessaire
 - pour accéder à l'agent 252
 - lancement incorrect de l'interface
 - graphique 242
 - Les conseillers ne fonctionnent
 - pas 240
 - Les requêtes de Dispatcher ne
 - sont pas acheminées 239
 - message d'erreur incorrect lors
 - du lancement de ndserver sous
 - Solaris 2.7 242
 - Network Dispatcher ne peut pas
 - traiter et transmettre de
 - cadre 243
 - non-équilibrage des
 - requêtes 247
 - non exécution de
 - Dispatcher 239
 - non exécution de Mailbox
 - Locator 248
 - non exécution de Site
 - Selector 250

- diagnostic des incidents (*suite*)
 - non réponse du composant
 - Dispatcher et du serveur 239
 - numéros de port utilisés par CBR 236
 - numéros de port utilisés par Cisco Consultant 238
 - numéros de port utilisés par Dispatcher 235
 - numéros de port utilisés par Mailbox Locator 237
 - numéros de port utilisés par Site Selector 237
 - permutation circulaire non effectuée par Site Selector (Solaris) 250
 - réception d'une erreur Mailbox Locator lors d'une tentative d'ajout de port 249
 - route supplémentaire 240
 - SNMP ne fonctionne pas 240
- diagrammes de syntaxe
 - Exemples 254
 - lecture 253
 - paramètres 253
 - ponctuation 253
 - symboles 253
- Dispatcher
 - configuration
 - configuration des serveurs TCP 67
- DPID2 220

E

- Environnement d'exécution Java (JRE) 13, 18, 20
- Équilibrage basé sur des règles
 - Heure 309
- équilibrage basé sur des règles 180
 - adresse du client IP 344, 346
 - Adresse du client IP 182, 304, 309
 - Connexions actives d'un port 183, 304
 - Contenu de la demande 189
 - contenu de la requête 54
 - Contenu de la requête 305
 - heure 344, 347
 - Heure 183, 304
 - largeur de bande partagée 185, 186, 305, 310
 - largeur de bande réservée 185, 186, 304, 309
 - mesure de tous les serveurs 187
 - metricall 344

- équilibrage basé sur des règles (*suite*)
 - metricavg 344
 - moyenne des mesures 188
 - nombre de connexions par seconde 183
 - Nombre de connexions par seconde 304
 - option d'évaluation 190
 - option d'évaluation de serveur 190
 - Port du client 184, 304
 - toujours vrai 346
 - toujours vraie 345
 - toujours vraies 188, 305, 309
 - type de service (TOS) 184, 304, 309
- équilibrage en fonction des règles
 - sélection de règles, par composant 181
- état, affichage
 - serveurs d'un port
 - spécifique 301, 380
 - toutes les grappes 364
 - une seule grappe 364
- exécuteur
 - arrêt 275
 - lancement 275, 365
 - lbcontrol 365
- executor
 - cbrcontrol 271
 - mlcontrol 271
 - ndcontrol 271
- Exemple de lancement rapide 1
- exemples
 - gestion de serveurs locaux 37, 38, 40, 41, 43, 45
- Exemples
 - Démarrage 1
- exemples de fichiers de configuration
 - conseiller 395
- exploitation de Network Dispatcher 213

F

- fichier de mappage d'adresses
 - exemple 192
- fichiers de configuration
 - exemple 387
 - composant Dispatcher (AIX) 387
 - composant Dispatcher (Windows) 391
- file
 - cbrcontrol 276

- file (*suite*)
 - lbcontrol 367
 - mlcontrol 276
 - ndcontrol 276
 - sscontrol 334
- Firewall 24

G

- gestion de Network Dispatcher 213
- gestionnaire
 - arrêt 292, 339, 341, 375, 377
 - lancement 66, 67, 134, 292, 339, 341, 374, 377
 - lbcontrol 372
 - pondération fixée 143
 - proportions 141, 363
 - version de 293, 339, 341, 375, 377
- goActive 178
- goldle 179
- goInOp 179
- goStandby 179
- grappe
 - affichage
 - état de cette grappe 270, 364
 - ajout 270, 364
 - cbrcontrol 266
 - configuration de l'adresse 63
 - définition 63, 133, 270, 364
 - définition du niveau
 - d'importance des informations 67, 134
 - générique 63
 - lbcontrol 363
 - mlcontrol 266
 - modification du délai FIN
 - pour 218
 - modification du nombre FIN
 - pour 218
 - ndcontrol 266
 - proportions 266
 - suppression 270, 353, 363, 364
- grappe générique 63
 - avec Caching Proxy pour le proxy transparent 194
 - pour combiner les configurations serveurs 193
 - pour équilibrer la charge des pare-feux 193
- Grappe générique 270
- GRE (Generic Routing Encapsulation)
 - OS/390 171
 - Support de réseau étendu 171
- GUI 5

GUI (*suite*)

résolution 243

H

handicap 405

haute disponibilité 46, 50, 173

Configuration 173

hôte primaire 268

ndcontrol 280

réci-proque 51, 174, 268, 270, 282

scripts 178

goActive 178

goIdle 179

goInOp 179

goStandby 179

highavailChange 179

Haute disponibilité 29

primaryhost 270

haute disponibilité réci-proque 51,
173, 174

de relais 177

primaryhost 268, 270

scripts 178

help

cbrcontrol 278

lbcontrol 369

mlcontrol 278

ndcontrol 278

highavailChange 179

host

lbcontrol 370

hôte

cbrcontrol 285

mlcontrol 285

ndcontrol 285

hôte primaire 174

I

ibmnd.conf

configuration Solaris 61

ibmproxy 80, 88

conseiller 150

ifconfig, commande 65

imap

remplacement 100

indice de lissage, définition 145,
292, 338, 340, 374, 377

installation

Network Dispatcher 11

sous AIX 13

sous Linux 18

sous Solaris 21

sous Windows 2000 23, 24

Interface graphique 5

intervalle, définition de la fréquence

interrogation de l'exécuteur par
le gestionnaire 144, 291, 373,
375

interrogation des serveurs par le
conseiller 264, 332, 358, 361

mise à jour des pondérations par
le gestionnaire pour
l'exécuteur 144, 290, 337, 339,
372, 375

J

journal

binaire, pour les statistiques des

serveurs 206, 286

cbrcontrol 286

fichier, définition du nom

pour le conseiller 331, 360

pour le gestionnaire 339, 374

mlcontrol 286

ndcontrol 286

niveau, définition

pour le conseiller 215, 264,
332, 359, 361

pour le gestionnaire 215,
337, 372

pour le serveur 215

pour le sous-agent 215

taille, définition

pour le conseiller 215, 264,
329, 332, 359, 361

pour le gestionnaire 215,

290, 337, 339, 373, 375

pour le serveur 215

pour le sous-agent 215

utilisation des journaux Cisco

Consultant 227

utilisation des journaux de

CBR 225

utilisation des journaux Mailbox

Locator 226

utilisation des journaux Metric

Server 228

utilisation des journaux Network

Dispatcher 215

utilisation des journaux Site

Selector 227

journalisation binaire pour les
statistiques des serveurs 206, 216

L

lancement

Cisco Consultant 227

conseiller 66, 67, 263, 331, 333

Dispatcher 4

lancement (*suite*)

exécuteur 63, 275, 365

gestionnaire 66, 67, 292, 339,
341, 374, 377

Metric Server 227

serveur 62, 63

Site Selector 226

lancement et arrêt

CBR 225

Dispatcher 217

Mailbox Locator 226

lbserver

échec du lancement 238, 251

lien explicite 191

ligne de commande

accès 405

exemple de configuration 4

Linux

configuration requise 17

correctif du noyau

versions 2.2.12, 2.2.13 75

versions 2.4.x 73

installation 18

log

binaire, pour les statistiques

serveur 371

lbcontrol 371

M

Mailbox Locator

ajout impossible d'un port 249

arrêt de la commande

mlserver 248

configuration

installation de la

machine 105

présentation des tâches 101

configuration matérielle et

logicielle requises 97

délai d'inactivité 268, 272, 299

échec de mlcontrol 249

échec de ndadmin 249

erreur proxy lors d'une tentative
d'ajout de port 249

incident d'exécution 248

lancement et arrêt 226

mlserver 98

paramètres de l'équilibrage de
charge 140

planification 97

Présentation générale 98

protocole de proxy 300, 301

staletimeout (délai

d'expiration) 268, 272, 299

- Mailbox Locator (*suite*)
 - tableau de résolution des incidents 233
 - utilisation 226
- maintien de routage (affinité)
 - affinité trans port 197, 198
 - affinité trans ports 297
 - cookie actif 200, 307
 - cookie passif 200, 202, 307
 - délai de maintien de routage 55, 56, 195, 197, 298, 307
 - fonctionnement 195
 - maintien de routage (substitution d'affinité de règle) 199, 312
 - masque d'adresse de l'affinité 198
 - masque de maintien de routage 197, 198, 297
 - mettre au repos maintenant 288, 292
 - mise au repos maintenant 199
 - SDA (Server Directed Affinity) 196
 - substitution d'affinité de règle 199
 - URI 200, 307
- manager
 - cbrcontrol 287
 - mlcontrol 287
 - ndcontrol 287
 - sscontrol 337
- mappage entre Consultant et CSS 125
- marquage d'un serveur à l'état défaillant 316, 348, 349
- en service 317, 349
- marques 409
- Marques 409
- masque d'adresse de l'affinité 198
- Masque d'adresse de l'affinité 297
- mesure
 - sscontrol 342
- mesures du système
 - configuration 294, 342, 378
 - définition du pourcentage d'importance 141, 266, 267, 363
- méthode d'acheminement
 - cbr 54
 - mac 52, 53
 - mac, nat ou cbr 298
 - MAC, NAT ou CBR 56
 - NAT 52
- méthode d'acheminement cbr 54
- méthode d'acheminement cbr (*suite*)
 - délai de maintien de routage 55, 56
- méthode d'acheminement mac 52
- Méthode d'acheminement NAT 52
- metric
 - cbrcontrol 294
 - lbcontrol 378
 - mlcontrol 294
 - ndcontrol 294
- Metric Server
 - lancement et arrêt 227
 - présentation générale 157
 - utilisation 227
- migration 11
- mise à l'état de repos d'un serveur 199, 288, 290, 292, 375
- modification
 - décompte FIN 218
 - délai d'expiration 218
 - délai FIN 218
- N**
- nameserver
 - sscontrol 343
- NAPT (network address port translation) 52
- ndconfig 167
 - commande 65
- ndkeys 158, 214
- ndserver
 - lancement 4
- Network Dispatcher
 - avantages 29
 - configuration
 - CBR 83
 - Cisco Consultant 129
 - composant Dispatcher 60, 88, 105, 119
 - Mailbox Locator 101
 - Site Selector 115
 - configuration logicielle
 - requis 47, 77, 97, 109, 123
 - configuration matérielle
 - requis 47, 77, 97, 109, 123
 - Exemple de lancement rapide 1
 - fonctions 27, 35
 - identification des incidents 229
 - installation 11
 - présentation générale 27, 35
 - remarques relatives à la planification 47, 109
 - tâches de configuration
 - avancées 137
- Network Dispatcher (*suite*)
 - utilisation et gestion 213, 226, 227
 - Utilisation et gestion 213
 - niveau d'importance des informations 134
 - nombre maximal FIN
 - modification 218
 - notices 407
 - nouvelles connexions 208
 - nouvelles connexions, définition du pourcentage d'importance 141, 267, 363
 - nouvelles fonctions, version 2.0
 - prise en charge de la nouvelle norme NLS chinoise 31
 - nouvelles fonctions, version 2.0
 - Programmes d'exit utilisateur améliorés 34**
 - Affinité d'URI 33
 - affinité de type cookie passif 33
 - amélioration de l'utilisation de CBR 32
 - Cisco Consultant 31
 - Composant CBR de Dispatcher 33
 - Conseiller DB2 35
 - Conseillers propres aux grappes ou aux sites 34
 - Demande/réponse de conseiller HTTP 34
 - Détection des refus de service 34
 - Mailbox Locator 32
 - NAT et NAPT 32
 - Partitionnement du serveur 34
 - pris en charge de Red Hat Linux Version 7.1 30
 - prise en charge de AIX version 5.1 30
 - prise en charge de SuSE Linux version 7.1 30
 - Proportions spécifiques pour les grappes 33
 - Site Selector 31
 - support multilingue sous Linux et Solaris 30
 - système Metric Server 31
- O**
- option de menu Contrôler 218
- options de proximité 112
- OS/390
 - support GRE 171

P

- paramètres, affichage de toutes les valeurs globales
 - pour le gestionnaire 292, 339, 341, 375, 377
 - pour un conseiller 265, 331, 333
- paramètres de l'équilibrage de charge (optimisation) 140
- planification
 - CBR 77
 - Cisco Consultant 123
 - composant Dispatcher 47
 - Mailbox Locator 97
 - Site Selector 109
- planification de l'installation 27, 47, 109
- pondération
 - définition
 - limite pour tous les serveurs d'un port 143, 301, 380
 - pour un serveur 316, 349, 383
 - exemple xml 209
 - mode de définition par le gestionnaire 143, 210
- pondération maximale, définition
 - pour les serveurs d'un port spécifique 143, 301, 380
- pop3
 - remplacement 100
- port
 - cbrcontrol 296
 - configuration 133
 - lbcontrol 380
 - mlcontrol 296
 - ndcontrol 296
- port générique 65, 301
 - conseiller ping 150
 - pour acheminer le trafic destiné à un port non configuré 195
- ports
 - affichage
 - état des serveurs sur ce port 301, 380
 - ajout 301, 380
 - définition de la pondération maximale 143, 301, 380
 - définition pour une grappe 65, 301, 380
 - génériques 65
 - pour les conseillers 260, 328
 - suppression 301, 380
- pourcentage d'importance pour l'équilibrage de charge, définition 141, 270

R

- présentation générale
 - configuration de CBR 83
 - configuration de Mailbox Locator 101
 - configuration de Site Selector 115
 - configuration du composant Dispatcher 57
- Présentation générale
 - configuration de Cisco Consultant 129
- primaryhost 270
- procédures 405
- proximité réseau 112

R

- rapport d'analyse des statistiques, affichage 291, 338, 339, 373, 375
- redémarrage de tous les serveurs avec des pondérations normalisées 291, 338, 340, 374, 377
- références de commandes
 - comment lire 253
- règle de contenu 54, 189
- réseau privé, utilisation avec Dispatcher 191
- résolution, interface graphique 243
- résolution des incidents 229
 - affichage d'un écran bleu lors du lancement de l'exécuteur Network Dispatcher 244
 - affichage incorrect de l'interface graphique 243
 - ajout impossible d'un port 249
 - arrêt de la commande cbrserver 248
 - CBR ne fonctionne pas 247
 - ce message d'erreur s'affiche lorsque l'on tente de visualiser l'aide en ligne 242
 - charges non indiquées par Metric Server 252
 - comportement imprévu lors du chargement d'un fichier de configuration volumineux 246
 - disparition des panneaux d'aide 243
 - dysfonctionnement de Dispatcher, de Microsoft IIS et de SSL 241
 - échec de démarrage de sserver sous Windows 2000 250
 - échec de la commande cbrcontrol ou ndadmin 247

résolution des incidents (*suite*)

- échec de la commande cbrcontrol sous Solaris 247
- échec de la commande lbcontrol ou ndadmin 251
- échec de la commande mlcontrol ou ndadmin 249
- échec de la commande ndcontrol ou ndadmin 241
- échec de la commande sserver ou ndadmin 250
- échec du lancement de lbserver 251
- équilibrage de charge de Site Selector incorrect 251
- erreur de syntaxe ou de configuration 248
- erreur lors de l'exécution de Dispatcher lorsque Caching Proxy est installé 243
- évitement du trafic retour avec Network Dispatcher par la fonction Path MTU Discovery 244
- fonction haute disponibilité de Dispatcher inopérante 240
- fonction haute disponibilité de Network Dispatcher inopérante en mode réseau étendu 245
- impossible d'ajouter un signal de présence 240
- impossible de créer un registre sur le port 14099 251
- incidents courants et solutions 239, 241, 247, 248, 250, 251, 252
- indication par les conseillers que tous les serveurs sont en panne 245
- IOException Metric Server sous Windows 2000 252
- journal de Metric Server indique qu'une signature est nécessaire pour accéder à l'agent 252
- lancement incorrect de l'interface graphique 242
- Les conseillers ne fonctionnent pas 240
- Les requêtes de Dispatcher ne sont pas acheminées 239
- message d'erreur incorrect lors du lancement de ndserver sous Solaris 2.7 242

- résolution des incidents (*suite*)
 - Network Dispatcher ne peut pas traiter et transmettre de cadre 243
- non-équilibre des requêtes 247
- non exécution de Dispatcher 239
- non exécution de Mailbox Locator 248
- non exécution de Site Selector 250
- non réponse du composant Dispatcher et du serveur 239
- numéros de port utilisés par CBR 236
- numéros de port utilisés par Cisco Consultant 238
- numéros de port utilisés par Dispatcher 235
- numéros de port utilisés par Mailbox Locator 237
- numéros de port utilisés par Site Selector 237
- permutation circulaire non effectuée par Site Selector (Solaris) 250
- réception d'une erreur Mailbox Locator lors d'une tentative d'ajout de port 249
- route supplémentaire 240
- SNMP ne fonctionne pas 240
- ressources 405
- route supplémentaire 70, 71
- routes, supplémentaires 70
- routes, suppression des routes supplémentaires 71
- rule
 - cbrcontrol 303
 - ndcontrol 303
 - sscontrol 344

S

- sauvegarde, haute-disponibilité 50, 280
 - Configuration 173
- scripts 178
 - exit utilisateur 145
 - goActive 178
 - goIdle 179
 - goInOp 179
 - goStandby 179
 - highavailChange 179
- scripts d'exit utilisateur 145

- scripts d'exit utilisateur (*suite*)
 - détection de refus de service 204
 - managerAlert 146
 - managerClear 146
 - serverDown 145
 - serverUp 145
- SDA (Server Directed Affinity) 161, 196
- Secure Sockets Layer 66
- sensibilité aux mises à jour de pondération, définition 144, 292, 338, 340, 374, 377
- server
 - sscontrol 348
- serveur
 - adresse 312, 383
 - advisorrequest 315
 - advisorresponse 315
 - ajout 316, 349, 383
 - cbrcontrol 311
 - co-implanté 312, 316
 - cookievalue 314
 - définition de la pondération 316, 349, 383
 - définition sur un port 66, 316, 349, 383
 - fixedweight 313
 - lbcontrol 382
 - logique 159
 - mapport 80, 313
 - marqué défaillant 316, 348, 349
 - marqué en service 317, 349
 - mise à l'état de repos 199, 288, 290, 292, 375
 - mlcontrol 311
 - ndcontrol 311
 - partitionnement 159
 - physiques 159
 - pondération 313
 - réactivation 293, 375
 - redémarrage global avec des pondérations normalisées 291, 338, 340, 374, 377
 - returnaddress 314
 - rouage non maintenu (substitution d'affinité de règle) 312, 316
 - router 314
 - suppression 316, 349, 383
- serveur marqué défaillant 316, 348, 349
- serveur marqué en service 317, 349
- serveurs de liaison 65, 66, 146, 166

- set
 - cbrcontrol 318
 - lbcontrol 384
 - mlcontrol 318
 - ndcontrol 318
 - sscontrol 350
- Simple Network Management Protocol (SNMP) 219
- Site Selector
 - commandes 327
 - configuration
 - installation de la machine 119
 - présentation des tâches 115
 - configuration matérielle et logicielle requises 109
 - échec de démarrage de sserver sous Windows 2000 250
 - échec de ndadmin 250
 - échec de sscontrol 250
 - équilibre de charge incorrect avec des chemins en double 251
 - équilibre de la charge des machines Dispatcher HA 180
 - exemple de configuration 43
 - incident d'exécution 250
 - lancement et arrêt 226
 - paramètres de l'équilibre de charge 140
 - planification 109
 - présentation générale 42
 - tableau de résolution des incidents 233
 - trafic à permutation circulaire à partir des clients Solaris non exécuté 250
 - utilisation 226
- sitename
 - sscontrol 351
- SNMP 215, 219
- Solaris
 - apr publish, commande 65
 - configuration de la machine Dispatcher 61
 - configuration requise 20
 - installation 21
 - sous-agents 215
 - ndcontrol 320
 - Sous-agents 219
 - spécifique d'une grappe proportions 351
 - sscontrol, commande
 - advisor 328
 - file 334

sscontrol, commande (*suite*)

- help 336
- manager 337
- mesure 342
- nameserver 343
- rule 344
- server 348
- set 350
- sitename 351
- status 355

SSL 66

status

- cbrcontrol 319
- lbcontrol 385
- mlcontrol 319
- ndcontrol 319

substitution d'affinité de règle

- serveur 199, 312, 316

support de réseau étendu 164

- Exemple de configuration 168
- utilisation d'une machine
 - Dispatcher éloignée 164
- utilisation de conseillers éloignés 166
- utilisation de GRE 171

suppression

- grappe 270, 353, 363, 364
- port d'une grappe 301, 380
- serveur d'un port 316, 349, 383
- voie d'acheminement supplémentaire 71

supprimer

- grappe 270, 353, 363, 364
- port d'une grappe 301, 380
- serveur d'un port 316, 349, 383
- voie d'acheminement supplémentaire 71

système Metric Server

- charges non indiquées par Metric Server 252
- IOException Metric Server sous Windows 2000 252
- journal de Metric Server indique qu'une signature est nécessaire pour accéder à l'agent 252
- lancement 134
- tableau de résolution des incidents 234

T

tableaux de résolution des incidents

- CBR 232
- Cisco Consultant 234
- composant Dispatcher 229
- Mailbox Locator 233

tableaux de résolution des incidents (*suite*)

- Site Selector 233
- système Metric Server 234

test

- configuration 135

V

vérification

- voie d'acheminement supplémentaire 70

version, affichage

- conseiller 265, 332, 333
- gestionnaire 293, 339, 341, 375, 377

W

Windows 2000

- commande de configuration de grappe 64
- configuration de la machine
 - Dispatcher 62
- configuration requise 22
- installation 23
- ndconfig, commande 65



GC11-1312-04



Spine information:



WebSphere Edge Server pour
multiplateforme

Network Dispatcher - Guide d'administration

Version 2.0