CC-SG

CommandCenter Secure Gateway

Manuel de l'administrateur

Version 3.2

Copyright © 2007 Raritan, Inc.
CCA-0F-F
Octobre 2007
255-80-5140-00

Ce document contient des informations propriétaires protégées par droits de copyright. Tous droits réservés. Aucune partie de ce document ne peut être photocopiée, reproduite ou traduite dans une autre langue sans l'accord écrit préalable de Raritan, Inc.

© Copyright 2007 Raritan, Inc., CommandCenter®, Dominion®, Paragon® et le logo de la société Raritan sont des marques déposées ou non de Raritan Computer, Inc. Tous droits réservés. Java® est une marque déposée de Sun Microsystems, Inc. Internet Explorer® est une marque déposée de Microsoft Corporation. Netscape® et Netscape Navigator® sont des marques déposées de Netscape Communication Corporation. Toutes les autres marques déposées ou non sont détenues par leur propriétaire respectif.

Informations FCC (Etats-Unis seulement)

Cet équipement a été testé et certifié conforme aux limites d'un dispositif numérique de catégorie A selon l'article 15 du code de la Commission fédérale des communications des Etats-Unis (FCC). Ces limites visent à fournir une protection raisonnable contre les interférences nuisibles dans une installation commerciale. Cet équipement génère, utilise et peut émettre des émissions radioélectriques. S'il n'est pas installé et utilisé conformément aux instructions, il risque d'entraîner des interférences perturbant les communications radio. L'utilisation de l'équipement dans un environnement résidentiel peut générer des interférences nuisibles.

Informations VCCI (Japon seulement)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan n'est pas responsable des dégâts subis par ce produit suite à un accident, une catastrophe, une mauvaise utilisation, une modification du produit non effectuée par Raritan ou tout autre événement hors du contrôle raisonnable de Raritan ou ne découlant pas de conditions normales d'utilisation.

CE c UL us LISTED 1F61 I.T.E.

Table des matières

CC-SG - Notions fondamentales 15

Configuration et imposition des mots de passe forts 15
Mise à niveau de CC-SG vers une nouvelle version de firmware 16
Contrôle de l'alimentation d'un groupe de nœuds et surveillance de l'opération de gestion de l'alimentation 18
    Gestion de l'alimentation d'un groupe de noeuds 18
    Messages d'état de l'alimentation 19
Mise à niveau de plusieurs dispositifs dans un laps de temps limité 20
Affecter une vue personnalisée de noeuds par défaut à tous les utilisateurs 22

Chapitre 1 Introduction 1

Conditions préalables 1
Terminologie et sigles 2

Chapitre 2 Accès à CC-SG 5

Accès via un navigateur 5
Accès via un client lourd 6
    Installer le client lourd 6
    Utiliser le client lourd 7
Client Admin CC-SG 8

Chapitre 3 Mise en route 10

Confirmation de l'adresse IP 10
Définition de l'heure du serveur CC-SG 10
Vérification de la matrice de compatibilité 12
Vérification et mise à niveau des versions des applications 12

Chapitre 4 Configuration de CC-SG par paramétrage guidé 14

Avant d'utiliser le paramétrage guidé 15
Associations dans le paramétrage guidé 15
    Créer des catégories et des éléments 15
Paramétrage du dispositif 16
    Détecter et ajouter des dispositifs 16

Créer des groupes 18
Ajouter des groupes de dispositifs et de nœuds 18
Gestion des utilisateurs 21
Ajouter des groupes d'utilisateurs et des utilisateurs 21

Chapitre 5 Associations, catégories et éléments 24

A propos des associations 24
Terminologie relative aux associations 24
Associations – Définition des catégories et des éléments 25
Comment créer des associations 26
Gestionnaire des associations 26
Ajouter une catégorie 26
Modifier une catégorie 27
Supprimer une catégorie 27
Ajouter un élément 27
Modifier un élément 28
Supprimer un élément 28

Chapitre 6 Dispositifs, groupes de dispositifs et ports 29

Affichage des dispositifs 30
Onglet Dispositifs 30
Ecran Profil du dispositif 31
Icônes de dispositif et de port 31
Options de tri des ports 32
Options clic bouton droit de l'onglet Dispositifs 32
Recherche de dispositifs 33
Caractères joker de recherche 33
Exemple de caractères joker 33
Détection des dispositifs 34
Ajout d'un dispositif 35
Ajouter un dispositif KVM ou série 35
Ajouter un dispositif PowerStrip 37
Modification d'un dispositif 37
Modification d'un dispositif PowerStrip 38
Suppression d'un dispositif 38
Configuration des ports 39
Configurer un port série 39
Configurer un port KVM 39

Raritan.
When you're ready to take control®

Modification d'un port 40
Suppression d'un port 41
Copie en bloc de catégories et d'éléments de dispositifs 41
Mise à niveau d'un dispositif 42
Sauvegarde de la configuration du dispositif 42
Restauration de la configuration du dispositif 43
A propos de la restauration des configurations de dispositifs 43
Restaurer la configuration d'un dispositif (KX, KSX, KX101, SX, IP-Reach) 44
Restaurer toutes les données de configuration hormis les paramètres réseau sur un dispositif KX2 44
Restaurer uniquement les paramètres de dispositif ou les données de l'utilisateur ou du groupe de l'utilisateur sur un dispositif KX2 45
Restaurer toutes les données de configuration sur un dispositif KX2 45
Copie de la configuration du dispositif 46
Redémarrage du dispositif 46
Envoi d'une commande ping au dispositif 47
Suspension de la gestion 47
Reprise de la gestion 47
Gestionnaire d'alimentation des dispositifs 48
Démarrage d'admin 48
Vue topologique 49
Déconnexion des utilisateurs 49
Accès spécial aux dispositifs du système Paragon II 50
Paragon II System Controller (P2-SC) 50
Administration des unités IP-Reach et UST-IP 50
Gestionnaire des groupes de dispositifs 51
Ajouter un groupe de dispositifs 51
Modifier un groupe de dispositifs 54
Supprimer un groupe de dispositifs 55

Chapitre 7 Barrettes d'alimentation gérées 56

Processus de configuration de la gestion de l'alimentation dans CC-SG 56
Configuration des barrettes d'alimentation connectées à des dispositifs KX, KX2 et P2SC 57
Ajouter un dispositif PowerStrip connecté à un dispositif KX, KX2 ou P2SC 57
Déplacer une barrette de KX, KX2 ou P2SC vers un port différent 58
Supprimer une barrette d'alimentation connectée à un dispositif KX, KX2 ou P2SC 58
Configuration des barrettes d'alimentation connectées à des dispositifs SX 3.0 et KSX 58
Ajouter une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX 59
Supprimer une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX 60
Modifier une association de dispositif ou de port d'une barrette d'alimentation (SX 3.0, KSX) 60
Configuration des barrettes d'alimentation connectées à un dispositif SX 3.1 61
Ajouter un dispositif PowerStrip connecté à un dispositif SX 3.1 61
Déplacer la barrette d'alimentation d'un dispositif SX 3.1 vers un port différent 62

Supprimer une barrette d'alimentation connectée à un dispositif SX 3.1 62
Configuration des prises d'une barrette d'alimentation 63

Chapitre 8 Nœuds, groupes de nœuds et interfaces 65

Affichage des nœuds 65
Onglet Nœuds 66
Profil du nœud 66
Icônes associées aux nœuds et aux interfaces 67
Vue d'ensemble des nœuds et des interfaces 67
A propos des nœuds 67
Noms des nœuds 67
A propos des interfaces 68
Ajout d'un nœud 68
Nœuds créés par configuration de ports 69
Ajout d'une interface 69
Interfaces de connexions en bande 71
Interfaces pour connexions KVM hors bande, série hors bande 71
Interfaces pour connexions de gestion de l'alimentation par processeur DRAC, RSA et ILO 72
Interfaces pour connexions par barrette d'alimentation gérée 72
Interfaces pour connexions de gestion d'alimentation IPMI 73
Interface Navigateur Web 74
Résultats de l'ajout d'une interface 76
Modification d'une interface 76
Suppression d'une interface 77
Ajouter une interface aux signets 77
Modification d'un nœud 78
Suppression d'un nœud 79
Copie en bloc de catégories et d'éléments de nœuds 79
Connexion à un nœud 80
Envoi d'une commande ping à un nœud 80
Conversation 80
A propos des groupes de nœuds 82
Ajout d'un groupe de nœuds 83
Sélectionner les nœuds 83
Décrire les nœuds 84
Modification d'un groupe de nœuds 86
Suppression d'un groupe de nœuds 87

Chapitre 9 Utilisateurs et groupes d'utilisateurs 88

Onglet Utilisateurs 89
Groupes d'utilisateurs par défaut 90
Groupe CC Super-User 90
Groupe System Administrators 90

Groupe CC Users 91
Ajout d'un groupe d'utilisateurs 91
Modification d'un groupe d'utilisateurs 93
Suppression d'un groupe d'utilisateurs 94
Ajout d'un utilisateur 94
Modification d'un utilisateur 95
Suppression d'un utilisateur 96
Affectation d'un utilisateur à un groupe 97
Suppression d'un utilisateur d'un groupe 98
Votre profil utilisateur 98
A propos de mon profil 98
Changer votre mot de passe 98
Modifier votre préférence de recherche par défaut 99
Modifier la taille de police par défaut dans CC-SG 99
Modifier votre adresse électronique 99
Modifier le nom d'utilisateur du super utilisateur CC-SG 99
Déconnexion des utilisateurs 100
Copie en bloc d'utilisateurs 100

Chapitre 10 Stratégies de contrôle d'accès 102

Contrôle des accès à l'aide de stratégies 102
Ajout d'une stratégie 103
Modification d'une stratégie 105
Suppression d'une stratégie 106
Prise en charge de support virtuel 107
Support virtuel : définition 108
Affectation de stratégies à des groupes d'utilisateurs 110

Chapitre 11 Vues personnalisées pour dispositifs et nœuds 111

Types de vues personnalisées 111
Vue par catégorie 111
Filtrer par groupe de noeuds 111
Filtrer par groupe de dispositifs 112
Utilisation de vues personnalisées dans le client Admin 112
Vues personnalisées pour les nœuds 112
Vues personnalisées pour les dispositifs 115

Chapitre 12 Authentification à distance 119

A propos de l'authentification et de l'autorisation (AA) 119
Flux d'authentification 119
Comptes utilisateur 120

Noms distincts pour LDAP et AD 120
Définir un nom distinct pour AD 121
Définir un nom distinct pour LDAP 121
Définir un nom d'utilisateur pour AD 121
Définir un nom distinct de base 121
Définition des modules pour l'authentification et l'autorisation 121
Définition de l'ordre des serveurs AA externes 122
A propos d'AD et de CC-SG 122
Ajout d'un module AD dans CC-SG 122
Paramètres généraux AD 123
Paramètres avancés AD 124
Paramètres de groupe AD 126
Paramètres d'approbation AD 127
Modification d'un module AD 128
Importation des groupes d'utilisateurs AD 129
Synchronisation d'AD avec CC-SG 130
Synchroniser tous les groupes d'utilisateurs avec AD 131
Synchroniser tous les modules AD 132
Activer ou désactiver la synchronisation quotidienne de tous les modules AD 133
Modifier l'heure de synchronisation AD quotidienne 133
A propos de LDAP et de CC-SG 134
Ajout d'un module LDAP (Netscape) dans CC-SG 134
Paramètres généraux LDAP 134
Paramètres avancés LDAP 135
Paramètres de configuration Sun One LDAP (iPlanet) 136
Paramètres de configuration OpenLDAP (eDirectory) 137
A propos de TACACS+ et de CC-SG 137
Ajout d'un module TACACS+ 137
Paramètres généraux TACACS+ 138
A propos de RADIUS et de CC-SG 138
Ajout d'un module RADIUS 138
Paramètres généraux RADIUS 139
Authentification à deux facteurs à l'aide de RADIUS 139

Chapitre 13 Rapports 140

Utilisation des rapports 140
Trier les données d'un rapport 140
Redimensionner la largeur des colonnes d'un rapport 140
Afficher les détails d'un rapport 141
Parcourir des rapports de plusieurs pages 141
Imprimer l'affichage d'un rapport 141
Enregistrer un rapport dans un fichier 141
Purger les données d'un rapport de CC-SG 142
Afficher ou masquer les filtres de rapport 142

Rapport Journal d'audit 142
Rapport Journal d'erreurs 143
Rapport d'accès 144
Rapport de disponibilité 145
Rapport Utilisateurs actifs 145
Rapport Utilisateurs verrouillés 146
Rapport Données d'utilisateurs 146
Rapport Utilisateurs dans les groupes 147
Rapport Données de groupes 147
Rapport sur le groupe d'utilisateurs AD 148
Rapport Gestion du parc 148
Rapport sur le parc du nœud 149
Rapport sur les nœuds actifs 149
Rapport sur la création de nœuds 150
Rapport Interrogation des ports 150
Rapport Ports actifs 152
Rapports programmés 152
Rapport Mise à niveau du firmware d'un dispositif 153
Rapport Synchronisation CC-NOC 153

Chapitre 14 Maintenance du système 155

Mode de maintenance 155
Tâches programmées et mode de maintenance 155
Entrer en mode de maintenance 156
Quitter le mode de maintenance 156
Sauvegarde de CC-SG 156
Enregistrement et suppression des fichiers de sauvegarde 158
Enregistrer un fichier de sauvegarde 158
Supprimer un fichier de sauvegarde 158
Restauration de CC-SG 159
Réinitialisation de CC-SG 161
Redémarrage de CC-SG 161
Mise à niveau de CC-SG 162
Arrêt de CC-SG 163
Redémarrage de CC-SG après un arrêt 164
Mise hors tension de CC-SG 164
Fermeture d'une session CC-SG 165
Se déconnecter de CC-SG 165
Quitter CC-SG 165

Chapitre 15 Administration avancée 166

Configuration d'un message du jour 166
Configuration des applications d'accès aux nœuds 167
A propos des applications d'accès aux nœuds 167
Vérification et mise à niveau des versions des applications 167
Ajouter une application 168
Supprimer une application 169
Configuration des applications par défaut 169
A propos des applications par défaut 169
Afficher les affectations d'applications par défaut 169
Définir l'application par défaut d'une interface ou d'un type de port 169
Gestion du firmware d'un dispositif 170
Télécharger un firmware 170
Supprimer un firmware 170
Configuration du réseau CC-SG 171
A propos de la configuration réseau 171
A propos des ports LAN CC-SG 172
Mode principal/de sauvegarde : définition 173
Mode actif/actif : définition 176
Configurations DHCP recommandées pour CC-SG 178
Configuration de l'activité d'enregistrement 179
Purger le journal interne de CC-SG 179
Configuration de la date et de l'heure du serveur CC-SG 180
Configuration du modem 181
Configurer CC-SG 181
Configurer le modem du PC client 181
Configurer la connexion à distance 182
Configurer la connexion de rappel 182
Se connecter à CC-SG par modem 183
Modes de connexion : Direct et Proxy 185
A propos des modes de connexion 185
Pour configurer le mode Direct pour toutes les connexions clientes 185
Pour configurer le mode Proxy pour toutes les connexions clientes 185
Pour configurer une combinaison des modes Direct et Proxy 186
Paramètres du dispositif 186
Configuration de SNMP 187
A propos de SNMP et de CC-SG 187
Fichiers MIB 187
Pour configurer SNMP dans CC-SG 187
Configuration des clusters CC-SG 189
Cluster CC-SG : définition 189
Exigences pour les clusters CC-SG 189
A propos des clusters CC-SG et CC-NOC 189
Créer un cluster 190

Raritan.
When you're ready to take control®

Supprimer un nœud CC-SG secondaire 191
Supprimer un nœud CC-SG primaire 191
Récupérer un nœud CC-SG défaillant 192
Paramètres de cluster avancés 192
Gestionnaire de sécurité 193
Authentification à distance 193
Chiffrement AES 193
Configurer le protocole de connexion du navigateur : HTTP ou HTTPS/SSL 194
Paramétrer le numéro de port pour l'accès SSH à CC-SG 194
Paramètres de connexion 195
Configurer le minuteur d'inactivité 198
Portail 198
Certificats 200
Liste de contrôle d'accès 204
Gestionnaire des notifications 206
Configurer un serveur SMTP externe 206
Gestionnaire des tâches 207
Types de tâches 207
Programmer des tâches séquentielles 207
Envoyer des notifications de tâches par e-mail 208
Rapports programmés 208
Programmer une tâche 208
Programmer la mise à niveau du firmware d'un dispositif 211
Afficher une tâche, les détails d'une tâche et l'historique des tâches 213
CommandCenter NOC 214
Ajouter un CC-NOC 214
Modifier un CC-NOC 216
Lancer un CC-NOC 217
Supprimer un CC-NOC 217
Accès SSH à CC-SG 217
Commandes SSH 219
Astuces sur les commandes 221
Créer une connexion SSH à un dispositif SX 222
Utiliser SSH pour se connecter à un nœud via une interface série hors bande 223
Quitter une session SSH 224
Port d'administration série 224
A propos des programmes d'émulation de terminal 225

Interface API de services Web 225

Chapitre 16 Console de diagnostic 226

Accès à la console de diagnostic via un port VGA/clavier/souris 227
Accès à la console de diagnostic via SSH 227
A propos de la console d'état 229
Accès à la console d'état 229
A propos de la console d'administrateur 230
Accès à la console d'administrateur 230
Navigation dans la console d'administrateur 231
Modification de la configuration de la console de diagnostic 232
Modification de la configuration des interfaces réseau (Interfaces réseau) 233
Envoi d'une commande ping à une adresse IP (Interfaces réseau) 235
Utilisation de la détermination d'itinéraire (Interfaces réseau) 237
Modification des routes statiques (Interfaces réseau) 238
Consultation des fichiers journaux dans la console de diagnostic (Admin) 239
Redémarrage de CC-SG avec la console de diagnostic 244
Réamorçage de CC-SG avec la console de diagnostic 245
Mise hors tension du système CC-SG à partir de la console de diagnostic 246
Réinitialisation du mot de passe du super utilisateur CC avec la console de diagnostic 247
Réinitialisation de la configuration usine de CC-SG (Admin) 248
Paramètres des mots de passe de la console de diagnostic 251
Configuration des comptes 253
Affichage de l'état des disques (Utilitaires) 256
Affichage des processus exécutés sur CC-SG avec la console de diagnostic 257
Affichage de l'état de NTP (Utilitaires) 257

Annexe A Spécifications pour G1, V1 et E1 259

Modèle G1 259
- G1 - Spécifications générales 259
- G1 - Spécifications matérielles 259
- G1 - Impératifs d'environnement 260

Modèle V1 260
- V1 - Spécifications générales 260
- V1 - Spécifications matérielles 261
- V1 - Impératifs d'environnement 261

Modèle E1 262
- E1 - Spécifications générales 262
- E1 - Spécifications matérielles 262
- E1 - Impératifs d'environnement 263

Annexe B Configuration de CC-SG et du réseau 264

A propos de cette annexe 264
Ports ouverts requis pour les réseaux CC-SG : Synthèse 264
Canaux de communication CC-SG 266
CC-SG et dispositifs Raritan 267
Cluster CC-SG 267
Accès aux services d'infrastructure 268
Clients PC vers CC-SG 268
Clients PC vers nœuds 269
CC-SG et client pour IPMI, iLO/RILOE, DRAC, RSA 270
CC-SG et SNMP 270
CC-SG et CC-NOC 271
Ports internes CC-SG 271
Accès à CC-SG via un pare-feu compatible NAT 272

Annexe C Privilèges de groupe d'utilisateurs 273

Annexe D Traps SNMP 285

Annexe E Guide de dépannage 288

Configuration requise pour le navigateur client 288

Annexe F Authentification à deux facteurs 289

Authentification à deux facteurs - Environnements pris en charge 289
Authentification à deux facteurs - Configuration requise 289
Authentification à deux facteurs - Problèmes répertoriés 290

Annexe G FAQ 291

Annexe H Raccourcis clavier 299

Annexe I Conventions d'appellation 300

Index 301

Raritan.
When you're ready to take control®

CC-SG - Notions fondamentales

Ce chapitre présente quelques exemples d'utilisation courants pour permettre aux utilisateurs de se familiariser rapidement avec CC-SG. Notez que cette section contient des exemples courants, qui peuvent varier selon votre configuration et vos opérations.

Dans ce chapitre

Configuration et imposition des mots de passe forts 15
Mise à niveau de CC-SG vers une nouvelle version de firmware 16
Contrôle de l'alimentation d'un groupe de nœuds et surveillance de l'opération de gestion de l'alimentation.....18
Mise à niveau de plusieurs dispositifs dans un laps de temps limité 20
Affecter une vue personnalisée de noeuds par défaut à tous les utilisateurs 22

Configuration et imposition des mots de passe forts

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet **Paramètres de connexion**.
3. Cochez la case **Mots de passe forts obligatoires pour tous les utilisateurs**.
4. Sélectionnez la **longueur de mot de passe maximum**. Les mots de passe doivent contenir moins de caractères que le nombre maximum.
5. Sélectionnez une **profondeur d'historique du mot de passe**. Ce nombre indique le nombre de mots de passe conservés dans l'historique et non réutilisables. Par exemple, si le champ **Profondeur d'historique du mot de passe** indique 5, les utilisateurs ne peuvent pas réutiliser leurs 5 derniers mots de passe.
6. Sélectionnez une **fréquence d'expiration du mot de passe**. Tous les mots de passe expirent après un nombre défini de jours. Après l'expiration du mot de passe, les utilisateurs devront en choisir un nouveau à la connexion suivante.

7. Sélectionnez des **exigences du mot de passe fort** :
   - Les mots de passe doivent contenir au moins une lettre minuscule.
   - Les mots de passe doivent contenir au moins une lettre majuscule.
   - Les mots de passe doivent contenir au moins un nombre.
   - Les mots de passe doivent contenir au moins un caractère spécial (par exemple, un point d'exclamation ou une perluète).
8. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Reportez-vous à ***Paramètres de connexion*** (à la page 195) pour plus de détails sur la sécurité de connexion.

Mise à niveau de CC-SG vers une nouvelle version de firmware

Vous pouvez mettre à niveau le firmware de CC-SG lorsqu'une version plus récente est disponible. Les fichiers de firmware figurent dans la section Support du site Web Raritan.

Téléchargez le fichier de firmware sur votre PC client avant de procéder à la mise à niveau.

Il est recommandé d'effectuer une copie de sauvegarde de CC-SG avant d'effectuer la mise à niveau. Si vous utilisez un cluster CC-SG, vous devez d'abord supprimer celui-ci et mettre chaque nœud à niveau individuellement.

Remarque : si vous effectuez la mise à niveau de 3.0.2 à 3.1 et que vous utilisez Active Directory, consultez le fichier Lisezmoi de la version 3.1 pour prendre connaissance des instructions spéciales.

Important :

si vous devez mettre à niveau CC-SG et un périphérique ou groupes de périphériques, traitez CC-SG d'abord, puis le dispositif.

CC-SG redémarre dans le cadre du processus de mise à niveau de 3.1.1 à 3.2. N'INTERROMPEZ PAS le processus, ne redémarrez pas l'unité manuellement, ne mettez pas l'unité hors tension, n'effectuez pas d'alimentation cyclique lors de la mise à niveau.

➢ *Pour mettre à niveau CC-SG :*

1. Téléchargez le fichier de firmware sur votre PC client.

2. ***Entrez en mode de maintenance*** (voir "Entrer en mode de maintenance" à la page 156).
3. Lorsque CC-SG est en mode de maintenance, choisissez **Maintenance du système** > **Mettre à niveau**.
4. Cliquez sur **Parcourir**. Recherchez et sélectionnez le fichier de firmware de CC-SG, cliquez ensuite sur **Ouvrir**.
5. Cliquez sur **OK** pour télécharger ce fichier sur CC-SG.

   Une fois le fichier de firmware téléchargé sur CC-SG, un message de confirmation apparaît pour indiquer que CC-SG a entamé le processus de mise à niveau. Tous les utilisateurs sont alors déconnectés de CC-SG.
6. Cliquez sur **OK** pour quitter CC-SG et lui permettre de redémarrer. Vous devez attendre environ 8 minutes que CC-SG redémarre.
7. Fermez la fenêtre de votre navigateur, puis videz la mémoire cache de ce dernier.
8. Après 8 minutes, ouvrez une nouvelle fenêtre du navigateur et lancez CC-SG.
9. Choisissez **Aide** > **A propos de Raritan Secure Gateway**. Vérifiez le numéro de version pour vous assurer que la mise à niveau a abouti.
   - Si la version n'a pas été mise à niveau, répétez la procédure précédente.
   - Si la mise à niveau a abouti, passez à l'étape suivante.

Quittez le mode de maintenance (voir "Quitter le mode de maintenance" à la page 156).

Contrôle de l'alimentation d'un groupe de nœuds et surveillance de l'opération de gestion de l'alimentation

Gestion de l'alimentation d'un groupe de noeuds

Vous pouvez mettre sous tension/hors tension, effectuer une alimentation cyclique ou un arrêt approprié pour tous les noeuds associés à des interfaces d'alimentation d'un groupe de noeuds.

Cette fonction vous permet par exemple de mettre hors tension tous les noeuds d'un groupe afin de recâbler le rack sur lequel ils sont montés ou d'effectuer d'autres opérations de maintenance sur un groupe de noeuds.

Reportez-vous à la section Astuces relatives à la gestion de l'alimentation des noeuds à plusieurs interfaces pour plus d'informations sur le paramétrage des opérations de gestion de l'alimentation des noeuds comportant plusieurs interfaces de gestion d'alimentation.

1. Cliquez sur l'onglet **Noeuds**.
2. Dans le menu **Noeuds**, cliquez sur **Regrouper la gestion de l'alimentation**. L'écran **Regrouper la gestion de l'alimentation** apparaît.
3. Cliquez sur la flèche déroulante **Groupe de noeuds**, puis sélectionnez, dans la liste, le groupe dont vous souhaitez gérer l'alimentation.
4. Dans la liste **Disponible**, sélectionnez l'interface dont vous souhaitez gérer l'alimentation, puis cliquez sur **Ajouter** afin de transférer l'interface dans la liste **Sélectionné**. Répétez cette opération jusqu'à ce que vous ayez ajouté toutes les interfaces nécessaires à la liste **Sélectionné**. Pour supprimer une interface, cliquez dessus dans la liste **Sélectionné**, puis cliquez sur **Retirer**.
5. Vous devez ajouter les interfaces à la liste **Sélectionné** dans l'ordre selon lequel CC-SG doit effectuer l'opération d'alimentation. Sélectionnez une interface dans la liste **Sélectionné**, puis cliquez sur les flèches vers le haut et vers le bas pour déplacer les interfaces dans l'ordre souhaité.
6. Cliquez sur la flèche déroulante **Opération** et sélectionnez **Sous tension**, **Hors tension**, **Cycle d'alimentation** ou **Arrêt approprié** dans la liste.

7. Si vous avez sélectionné **Sous tension**, **Hors tension** ou **Arrêt approprié** dans le champ **Opération**, entrez le nombre de secondes, de 0 à 120, qui doivent s'écouler entre chaque interface dans le champ **Intervalle de séquence (en secondes)**.
8. Cliquez sur **OK** pour envoyer la requête d'opération via les interfaces sélectionnées. Un message de confirmation s'affiche à l'écran.
9. Une fenêtre Messages d'état de l'alimentation s'ouvre pour vous montrer l'état de l'opération de gestion de l'alimentation. Les messages alimentent la fenêtre au fur et à mesure de la réception de nouvelles informations sur l'opération de gestion de l'alimentation. Gardez cette fenêtre ouverte jusqu'à la fin des opérations de gestion de l'alimentation ; vous pouvez ainsi contrôler la progression.

   Reportez-vous à la section ***Messages d'état de l'alimentation*** (à la page 19) pour savoir comment CC-SG vous avertit de la réussite et de l'échec des opérations de gestion de l'alimentation.

Messages d'état de l'alimentation

La fenêtre Messages d'état de l'alimentation apparaît lors vous lancez une opération de gestion d'alimentation. Il est recommandé de garder cette fenêtre ouverte jusqu'à la fin des opérations de gestion de l'alimentation.

Vous pouvez redimensionner, réduire ou agrandir la fenêtre Messages d'état de l'alimentation. Vous pouvez sélectionner du texte, puis le copier et le coller dans la fenêtre.

Les messages de cette fenêtre sont mis à jour au fur et à mesure de la réception de nouvelles informations sur l'état de l'opération de gestion de l'alimentation.

Un nouveau message apparaît dans la fenêtre Messages d'état de l'alimentation :

- lorsque la demande d'opération de gestion de l'alimentation est envoyée ;
- si l'opération de gestion de l'alimentation échoue ;
- lorsque l'opération de gestion de l'alimentation aboutit ;
- si toutes les opérations de gestion de l'alimentation demandées aboutissent.

➢ *Pour obtenir des mises à jour d'état si vous fermez la fenêtre Messages d'état de l'alimentation :*

Si vous fermez la fenêtre d'état avant la fin de l'opération de gestion de l'alimentation :

- En cas d'échec d'une opération de gestion de l'alimentation, un message d'alerte apparaît et présente des informations sur l'opération.
- La barre d'état au bas de la fenêtre du navigateur affiche un message d'alerte lorsque l'opération entière aboutit.
- Des messages d'alerte n'apparaissent qu'en cas d'échec des opérations. Ils n'apparaissent pas si les opérations aboutissent.

Mise à niveau de plusieurs dispositifs dans un laps de temps limité

Vous pouvez programmer une tâche pour mettre à niveau plusieurs dispositifs de même type, tel que KX ou SX, au sein d'un groupe de dispositifs. Lorsque la tâche débute, un rapport Mise à niveau du firmware d'un dispositif est disponible dans le menu Rapports > Rapports programmés pour visualiser le statut de l'opération en temps réel. Ce rapport est également envoyé par courriel si l'option est paramétrée dans l'onglet Notification.

Reportez-vous au manuel d'utilisation Raritan de chaque dispositif pour obtenir une estimation de la durée de la mise à niveau.

➢ *Pour programmer une mise à niveau du firmware d'un dispositif :*

1. Choisissez Administration > Tâches.
2. Cliquez sur Nouveau.
3. Dans l'onglet Principale, entrez le nom et la description de la tâche. Le nom choisi identifiera la tâche et le rapport associé.
4. Ouvrez l'onglet Données de la tâche.
5. Indiquez les détails de la mise à niveau du dispositif :
   a. Exécution de la tâche : sélectionnez Mettre à niveau le firmware du dispositif.
   b. Groupe de dispositifs : sélectionnez le groupe contenant les dispositifs à mettre à niveau.

c. Type de dispositif : sélectionnez le type de dispositif à mettre à niveau. Si vous devez mettre à niveau plusieurs types de dispositifs, vous devez programmer une tâche pour chacun.

d. Mises à niveau simultanées : indiquez le nombre de dispositifs qui doivent démarrer la partie transfert de fichiers de la mise à niveau simultanément ; 10 au maximum. Dès qu'un transfert se termine, un nouveau démarre pour garantir que seul le nombre maximum de transferts simultanés a lieu.

e. Fichier de mise à niveau : sélectionnez la version de firmware cible de la mise à niveau. Seuls les fichiers de mise à jour disponibles adaptés au type de dispositif sélectionné sont présentés comme choix.

6. Définissez la période de la mise à niveau :

   a. Date/Heure de début : sélectionnez la date et l'heure de début de la tâche. Elles doivent être postérieures à la date et à l'heure en cours.

   b. Fenêtre de restriction de mise à niveau et Date/heure de début de la dernière mise à niveau : si toutes les mises à niveau doivent être exécutées sur une durée spécifique, utilisez ces champs pour indiquer la date et l'heure après lesquelles aucune nouvelle mise à niveau ne peut débuter. Sélectionnez Fenêtre de restriction de mise à niveau pour activer le champ Date/heure de début de la dernière mise à niveau.

7. Indiquez les dispositifs à mettre à niveau et leur séquence. Placez les dispositifs prioritaires en haut de la liste :

   a. Dans la liste Disponible, sélectionnez chaque dispositif à mettre à niveau et cliquez sur Ajouter pour le placer dans la liste Sélectionné.

   b. Dans la liste Sélectionné, choisissez un dispositif et utilisez les boutons fléchés pour le placer à l'endroit souhaité pour définir l'ordre de réalisation des mises à niveau.

8. Ouvrez l'onglet Nouvelle tentative. Indiquez si une nouvelle tentative doit être effectuée pour les mises à niveau ayant échoué.

   a. Nombre de nouvelles tentatives : entrez le nombre de fois où CC-SG doit tenter à nouveau une mise à niveau ayant échoué.

   b. Intervalle entre tentatives : entrez la durée qui doit s'écouler entre les tentatives. Les durées par défaut sont de 30, 60 et 90 minutes. Il s'agit des intervalles entre tentatives optima.

9. Ouvrez l'onglet Notification. Indiquez les adresses électroniques devant recevoir une notification de réussite ou d'échec. Par défaut, l'adresse électronique de l'utilisateur connecté est disponible. Les adresses électroniques des utilisateurs sont configurées dans le profil utilisateur.
   a. Cliquez sur Ajouter, entrez l'adresse électronique dans la fenêtre qui s'affiche, puis cliquez sur OK.
   b. Sélectionnez En cas d'échec si vous souhaitez envoyer un message si une mise à niveau échoue.
   c. Sélectionnez En cas de réussite si vous souhaitez envoyer un message lorsque toutes les mises à niveau aboutissent.
10. Cliquez sur OK pour enregistrer vos modifications.

Lorsque la tâche démarre, vous pouvez ouvrir le rapport Mise à niveau du firmware d'un dispositif à tout moment au cours de la période programmée pour voir le statut des opérations. Reportez-vous à ***Rapport Mise à niveau du firmware d'un dispositif*** (à la page 153) pour plus d'informations.

Affecter une vue personnalisée de noeuds par défaut à tous les utilisateurs

Si vous disposez du privilège CC Setup and Control (paramétrage et contrôle de CC), vous pouvez affecter une vue personnalisée par défaut à tous les utilisateurs.

1. Cliquez sur l'onglet Noeuds.
2. Choisissez Noeuds > Modifier la vue > Créer une vue personnalisée.
3. Cliquez sur la flèche déroulante **Nom** et sélectionnez la vue personnalisée que vous souhaitez affecter à tout le système.
4. Cochez la case **Pour tout le système**, puis cliquez sur **Enregistrer**.

Tous les utilisateurs qui se connectent à CC-SG voient l'onglet Noeuds trié selon la vue personnalisée sélectionnée. Les utilisateurs ont cependant la possibilité de changer la vue personnalisée.

Reportez-vous à ***Vues personnalisées*** (voir "Vues personnalisées pour dispositifs et nœuds" à la page 111) pour plus d'informations sur les types de vues personnalisées et obtenir des instructions sur leur création.

Chapitre 1 Introduction

Le manuel de l'administrateur CommandCenter Secure Gateway (CC-SG) présente des instructions pour l'administration et la gestion de votre unité CC-SG.

Ce guide est destiné aux administrateurs qui possèdent normalement tous les privilèges disponibles.

Les utilisateurs non administrateurs sont invités à se reporter au **manuel d'utilisation CommandCenter Secure Gateway** Raritan pour plus d'informations.

Dans ce chapitre

Conditions préalables.....1
Terminologie et sigles 2

Conditions préalables

Avant de configurer CC-SG conformément aux procédures détaillées dans ce document, reportez-vous au **guide de déploiement des solutions numériques** pour obtenir des instructions complètes sur le déploiement des dispositifs Raritan gérés par CC-SG.

Terminologie et sigles

Voici une liste des termes et sigles présents dans ce document :

Client d'accès – client HTML destiné aux utilisateurs standard souhaitant accéder à un nœud géré par CC-SG. Le client d'accès n'autorise pas l'utilisation des fonctions d'administration.

Client Admin – client Java pour CC-SG utilisable par les utilisateurs standard et les administrateurs. Il s'agit du seul client autorisant l'administration.

Associations – désigne la relation entre les catégories, les éléments de catégorie, et les ports ou dispositifs. Par exemple, si vous souhaitez associer la catégorie Emplacement à un dispositif, commencez par créer des associations avant d'ajouter des dispositifs et des ports dans CC-SG.

Catégorie – variable contenant un jeu de valeurs ou d'éléments. Un exemple de catégorie est Emplacement, qui peut contenir comme éléments New York City, Philadelphia, ou encore Data Center 1. Lorsque vous ajoutez des dispositifs ou des ports dans CC-SG, vous leur associez ce type d'informations. Il est conseillé de commencer par configurer correctement les associations avant d'ajouter les dispositifs et les ports. Type de SE est un autre exemple de catégorie, qui peut contenir des éléments tels que Windows, Unix ou Linux.

CIM (Module d'interface pour ordinateur) – désigne le matériel utilisé pour connecter un serveur cible et un dispositif Raritan. Chaque cible nécessite un module CIM, sauf le Dominion KX101 qui est relié directement à une cible et n'a par conséquent pas besoin de module CIM. Les serveurs cible doivent être mis sous tension et connectés aux CIM, lesquels doivent être connectés au dispositif Raritan AVANT d'ajouter celui-ci et de configurer les ports dans CC-SG. Sinon, le nom d'un CIM en blanc remplacera le nom du port CC-SG. Les serveurs doivent être redémarrés après avoir été connectés à un CIM.

CommandCenter NOC (CC NOC) – console de surveillance réseau qui permet l'audit et la surveillance de l'état des serveurs, de l'équipement et des dispositifs Raritan gérés par CC-SG.

Groupe de dispositifs – groupe défini de dispositifs accessibles à un utilisateur. Les groupes de dispositifs sont utilisés lors de la création des stratégies permettant de contrôler l'accès aux dispositifs présents dans ces groupes.

Dispositifs – désigne des produits Raritan, tels que Dominion KX, Dominion KX II, Dominion SX, Dominion KSX, IP-Reach, Paragon II System Controller, Paragon II UMT832 avec USTIP, gérés par CC-SG. Ces dispositifs contrôlent les systèmes et serveurs cible auxquels ils sont connectés. Consultez la matrice de compatibilité CC-SG sur le site Web du support Raritan pour obtenir la liste des dispositifs pris en charge.

Eléments – désigne les valeurs d'une catégorie. Par exemple, l'élément New York City appartient à la catégorie Emplacement. Autre exemple : l'élément Windows appartient à la catégorie Type de SE.

Port fantôme – lors de la gestion de dispositifs Paragon, un port fantôme peut se produire lorsqu'un CIM ou un serveur cible est supprimé du système ou mis hors tension (manuellement ou accidentellement). Reportez-vous au manuel d'utilisation de Paragon II pour plus d'informations.

Nom d'hôte – un nom d'hôte peut être indiqué si la prise en charge des serveurs DNS est activée. Reportez-vous à A propos du réseau dans le chapitre ***Administration avancée*** (à la page 166) pour plus d'informations. Le nom d'hôte et le nom de domaine complet qualifié (NDCQ = nom d'hôte + suffixe) associé ne peuvent pas dépasser 257 caractères. Il peut être constitué d'un nombre illimité de composants, s'ils sont séparés par « . ». Chaque composant doit avoir une taille maximale de 63 caractères, le premier d'entre eux étant obligatoirement alphabétique. Les autres caractères peuvent être alphabétiques, numériques ou
le signe « - » (trait d'union ou moins). Le dernier caractère d'un composant ne peut pas être le signe « - ». Même si le système conserve la casse des caractères entrés dans le système, le NDCQ n'est pas sensible à la casse lorsqu'il est utilisé.

iLO/RILOE – désigne les serveurs Integrated Lights Out/Remote Insight Lights Out de Hewlett Packard qui peuvent être gérés par CC-SG. Les cibles d'un dispositif iLO/RILOE sont mises sous/hors tension et recyclées directement. Les dispositifs iLO/RILOE ne peuvent pas être détectés par CC-SG ; il faut les ajouter manuellement en tant que nœuds.

Accès en bande – désigne le fait de passer par le réseau TCP/IP pour corriger ou dépanner une cible du réseau. Les dispositifs KVM et série sont accessibles à l'aide des applications en bande suivantes : RemoteDesktop Viewer, SSH Client, RSA Client, VNC Viewer.

Serveurs IPMI – serveurs Intelligent Platform Management Interface pouvant être contrôlés par CC-SG. Ils sont détectés automatiquement mais peuvent également être ajoutés manuellement.

Accès hors bande – utilisation d'applications telles que Raritan Remote Console (RRC), Raritan Console (RC) ou Multi-Platform Client (MPC) pour corriger ou dépanner un nœud KVM ou géré en série sur le réseau.

Stratégies – définissent les autorisations, le type d'accès et les nœuds et dispositifs auxquels un groupe d'utilisateurs a accès. Les stratégies sont appliquées à un groupe d'utilisateurs et sont dotées de plusieurs paramètres de contrôle, tels que la date et l'heure d'accès, afin de déterminer le niveau de contrôle.

Nœuds – désignent les systèmes cible, tels que les serveurs, les PC de bureau ou tout autre équipement réseau, auxquels les utilisateurs de CC-SG peuvent accéder.

Interfaces – fournissent un moyen d'accéder à un nœud, via une solution hors bande, telle qu'une connexion Dominion KX101, ou via une solution en bande, telle qu'un serveur VNC.

Groupe de nœuds – groupe défini de nœuds accessibles à un utilisateur. Les groupes de nœuds sont utilisés lors de la création des stratégies permettant de contrôler l'accès aux nœuds présents dans ces groupes.

Ports – points de connexion entre un dispositif Raritan et un nœud. Les ports n'existent que sur les dispositifs Raritan et identifient une voie d'accès du dispositif à un nœud.

SASL (Simple Authentication and Security Layer) – méthode utilisée pour ajouter la prise en charge de l'authentification aux protocoles basés sur les connexions.

SSH – clients, tels que PuTTY ou OpenSSH, qui fournissent une interface de ligne de commande à CC-SG. Seul un sous-ensemble des commandes CC-SG sont accessibles via SSH pour administrer des dispositifs et CC-SG lui-même.

Groupe d'utilisateurs – ensemble d'utilisateurs partageant le même niveau d'accès et les mêmes droits.

Raritan.
When you're ready to take control®

Chapitre 2 Accès à CC-SG

Vous pouvez accéder à CC-SG de plusieurs manières :

- **Navigateur** : CC-SG prend en charge de nombreux navigateurs Web. (Pour obtenir la liste complète des navigateurs pris en charge, reportez-vous à la matrice de compatibilité sur le site Web du support Raritan.
- **Client lourd** : vous pouvez installer un client lourd Java Web Start sur votre ordinateur client. Le client lourd fonctionne exactement comme le client par navigateur.
- **SSH** : les dispositifs distants connectés via le port série sont accessibles à l'aide de SSH. Reportez-vous à ***Administration avancée*** (à la page 166) pour plus d'informations.
- **Console de diagnostic** : elle permet uniquement des diagnostics et des réparations d'urgence, mais ne remplace pas l'interface utilisateur graphique par navigateur pour configurer et utiliser CC-SG. Reportez-vous à ***Administration avancée*** (à la page 166) pour plus d'informations.

Remarque : *les utilisateurs peuvent être connectés simultanément à l'aide du navigateur, du client autonome et du protocole SSH lors de l'accès à CC-SG.*

Dans ce chapitre

Accès via un navigateur.....5
Accès via un client lourd 6
Client Admin CC-SG.....8

Accès via un navigateur

1. Dans un navigateur Internet prise en charge, entrez l'URL : https://<adresse_IP>/admin, où <adresse_IP> indique l'adresse IP de CC-SG. Par exemple, **https://10.0.3.30/admin**.
2. Lorsque le message d'alerte de sécurité s'affiche, cliquez sur **Oui** pour continuer.
3. Le système vous avertit si la version de Java Runtime Environment installée sur votre machine n'est pas prise en charge. Dans la fenêtre qui s'affiche, indiquez si vous souhaitez télécharger la version de Java Runtime Environment correcte depuis le serveur CC-SG (le cas échéant) ou depuis le site Web de Sun Microsystems, ou si vous préférez continuer à utiliser la version incorrecte. Cliquez ensuite sur **OK**. La fenêtre de connexion s'affiche.

4. Si l'accord de service limité est activé, lisez-en le texte, puis cochez la case **Je comprends et j'accepte l'accord de service limité**.
5. Renseignez les champs **Nom d'utilisateur** et **Mot de passe**, puis cliquez sur **Connexion**.

Accès via un client lourd

Le client lourd CC-SG permet de se connecter à CC-SG en lançant une application Java Web Start au lieu d'exécuter un applet via un navigateur Web. Le client lourd offre l'avantage d'être plus performant qu'un navigateur en termes de vitesse et d'efficacité.

Installer le client lourd

➢ *Pour télécharger le client lourd depuis CC-SG :*

1. Lancez un navigateur Web et entrez l'URL : **http(s)://<adresse_IP>/install** où <adresse_IP> indique l'adresse IP de l'unité CC-SG.
   - Si un avertissement de sécurité apparaît, cliquez sur **Démarrer** pour continuer le téléchargement.
   - Si votre ordinateur client exécute Java version 1.4, une fenêtre **Desktop Integration** s'affiche. Si vous souhaitez que Java ajoute une icône de raccourci pour le client lourd sur votre bureau, cliquez sur **Yes** (Oui).
2. Une fois le téléchargement terminé, une nouvelle fenêtre apparaît vous permettant d'indiquer l'adresse IP de CC-SG.
3. Entrez l'adresse IP de l'unité CC-SG à laquelle vous souhaitez accéder dans le champ **Connexion par IP**. Après la connexion, cette adresse apparaîtra dans la liste déroulante **Connexion par IP**. Les adresses IP sont stockées dans un fichier de propriétés enregistré sur votre bureau.
4. Si CC-SG est configuré pour les connexions par navigateur sécurisées, vous devez cocher la case **Secure Socket Layer (SSL)**. Si CC-SG n'est pas configuré pour les connexions par navigateur sécurisées, vous devez désactiver la case **Secure Socket Layer (SSL)**. Ce paramètre doit être correct ; sinon, le client lourd ne pourra pas se connecter à CC-SG.

5. **Pour vérifier le paramètre dans CC-SG :** choisissez **Administration** > **Sécurité**. Dans l'onglet **Chiffrement**, observez l'option **Protocole de connexion du navigateur**. Si l'option **HTTPS/SSL** est sélectionnée, vous devez alors cocher la case **Secure Socket Layer (SSL)** dans la fenêtre de spécification de l'adresse IP du client lourd. Si l'option HTTP est sélectionnée, vous devez alors désactiver la case **Secure Socket Layer (SSL)** dans la fenêtre de spécification de l'adresse IP du client lourd.
6. Cliquez sur **Commencer**.
   - Un message vous avertit si la version de Java Runtime Environment installée sur votre machine n'est pas prise en charge. Suivez les invites pour télécharger une version prise en charge de Java, ou continuer avec la version installée.
7. L'écran de connexion s'affiche.
8. Si l'accord de service limité est activé, lisez-en le texte, puis cochez la case **Je comprends et j'accepte l'accord de service limité**.
9. Renseignez les champs **Nom d'utilisateur** et **Mot de passe**, puis cliquez sur **Connexion** pour continuer.

Utiliser le client lourd

Une fois le client lourd installé, il est accessible de deux façons sur votre ordinateur client. Elles sont déterminées par la version de Java utilisée.

➢ *Java 1.4.x*

Si votre ordinateur client exécute **Java version 1.4.x** et que vous avez cliqué sur **Yes** (oui) dans la fenêtre **Desktop Integration** (intégration au bureau) à l'installation du client lourd, vous pouvez double-cliquer sur l'icône de raccourci de votre bureau pour lancer le client lourd et accéder à CC-SG. Si vous n'avez pas d'icône de raccourci, vous pouvez en créer une à tout moment : recherchez **AMcc.jnlp** sur votre ordinateur client et créez un raccourci vers ce fichier.

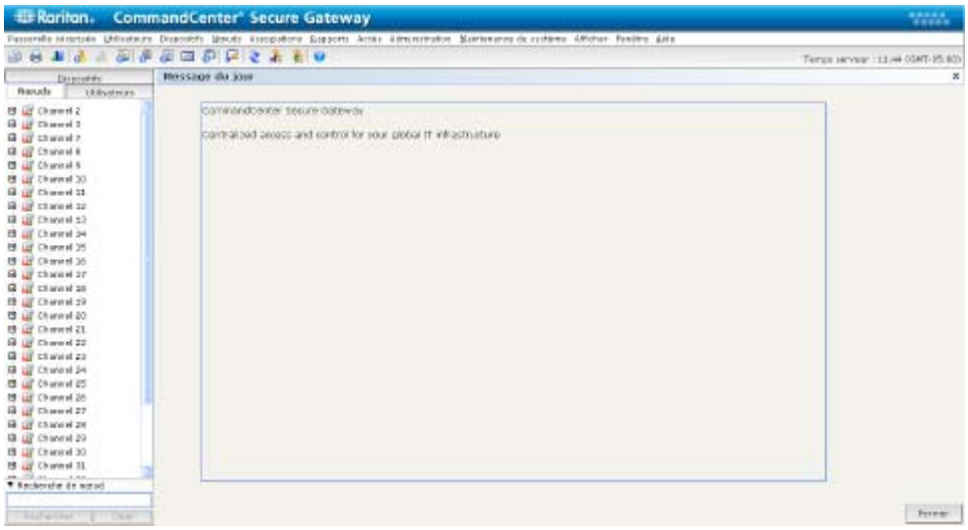
➢ *Java 1.5*

Si votre ordinateur client exécute **Java version 1.5**, vous pouvez :

- lancer le client lourd depuis le visualiseur du cache de l'application Java du panneau de configuration Java ;
- utiliser le visualiseur du cache de l'application Java du panneau de configuration Java afin d'installer une icône de raccourci sur votre bureau pour le client lourd.

Client Admin CC-SG

Si la connexion aboutit, la fenêtre du client Admin CC-SG s'affiche.



Raritan.
When you're ready to take control®

- **Onglet Nœuds** : cliquez sur l'onglet **Nœuds** pour afficher tous les nœuds cible connus sous la forme d'une arborescence. Cliquez sur un nœud pour afficher son profil. Les interfaces sont regroupées sous leurs nœuds parents. Cliquez sur les signes + et - pour développer ou réduire l'arborescence. Cliquez avec le bouton droit de la souris sur une interface et sélectionnez **Connecter** pour vous connecter à cette interface. Vous pouvez trier les nœuds par Nom (ordre alphabétique) ou par Etat (Disponible, Occupé, Indisponible). Cliquez avec le bouton droit de la souris dans l'arborescence, sélectionnez **Options de tri du nœud**, puis **Par nom de nœud** ou **Par état de nœud**.
- **Onglet Utilisateurs** : cliquez sur l'onglet **Utilisateurs** pour afficher tous les utilisateurs et groupes enregistrés sous la forme d'une arborescence. Cliquez sur les signes + et - pour développer ou réduire l'arborescence.
- **Onglet Dispositifs** : cliquez sur l'onglet **Dispositifs** pour afficher tous les dispositifs Raritan connus sous la forme d'une arborescence. Des icônes différentes sont associées aux différents types de dispositifs. Les ports sont regroupés sous leurs dispositifs parents. Cliquez sur les signes + et - pour développer ou réduire l'arborescence. Cliquez sur un port pour visualiser son profil. Pour vous connecter à un port, cliquez sur celui-ci avec le bouton droit de la souris et sélectionnez **Connecter**. Vous pouvez trier les ports par nom (ordre alphabétique) ou par état (Disponible, Occupé, Non disponible). Cliquez avec le bouton droit de la souris dans l'arborescence, sélectionnez **Options de tri des ports**, puis **Par nom de nœud** ou **Par état de nœud**.
- **Barre d'outils Commandes rapides** : cette barre d'outils propose des boutons de raccourci pour exécuter des commandes courantes.
- **Barre de menus Utilisation et configuration** : ces menus contiennent des commandes permettant d'utiliser et de configurer CC-SG. Vous pouvez également accéder à certaines de ces commandes en cliquant avec le bouton droit sur les icônes des onglets de sélection **Nœuds**, **Utilisateurs** et **Dispositifs**. L'affichage des menus et des éléments qu'ils contiennent dépend de vos droits d'accès d'utilisateur.
- **Temps serveur :** l'heure et le fuseau horaire qui apparaissent sont ceux configurés sur CC-SG dans le Gestionnaire de configuration. L'heure est utilisée pour programmer des tâches dans le Gestionnaire des tâches. Reportez-vous à ***Gestionnaire des tâches*** (à la page 207) pour plus d'informations. L'heure affichée peut être différente de celle utilisée par le PC client.

Chapitre 3 Mise en route

Lors de la première connexion à CC-SG, vous devez confirmer l'adresse IP, définir le temps serveur CC-SG et vérifier les versions de firmware et d'application installées. Il vous faudra peut-être mettre à niveau le firmware et les applications.

Une fois les configurations initiales effectuées, vous pouvez passer au chapitre ***Configuration de CC-SG par paramétrage guidé*** (à la page 14).

Dans ce chapitre

Confirmation de l'adresse IP 10
Définition de l'heure du serveur CC-SG.....10
Vérification de la matrice de compatibilité 12
Vérification et mise à niveau des versions des applications.....12

Confirmation de l'adresse IP

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **Configuration réseau**.
3. (Facultatif) Assurez-vous que les paramètres réseau sont corrects ou effectuez les modifications nécessaires. Reportez-vous à ***A propos de la configuration réseau*** (à la page 171) pour plus d'informations.
4. Cliquez sur **Mettre à jour la configuration** pour soumettre vos modifications.
5. Cliquez sur **Redémarrer maintenant** pour confirmer vos paramètres et redémarrer CC-SG.

Définition de l'heure du serveur CC-SG

L'heure et la date doivent être maintenues avec précision dans CC-SG afin de pouvoir gérer les dispositifs de manière fiable.

Important : la configuration de l'heure et de la date est utilisée pour programmer des tâches dans le Gestionnaire des tâches. Reportez-vous à *Gestionnaire des tâches* **(à la page 207) pour plus d'informations. Il peut y avoir un décalage entre l'heure réglée sur le client et celle réglée dans CC-SG.**

Seul le super utilisateur CC et les utilisateurs dotés de privilèges similaires peuvent configurer l'heure et la date.

Le changement de fuseau horaire est désactivé dans une configuration de clusters.

➢ *Pour configurer la date et l'heure du serveur CC-SG :*

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet **Heure/Date**.
   a. **Pour définir la date et l'heure manuellement : Date** – cliquez sur la flèche déroulante afin de sélectionner le **mois**, utilisez les flèches haut et bas pour sélectionner l'**année** et cliquez sur le **jour** dans la zone du calendrier. **Heure** – utilisez les flèches haut et bas afin de sélectionner les paramètres **Heure**, **Minutes** et **Secondes**, puis cliquez sur la flèche déroulante **Fuseau horaire** pour sélectionner le fuseau horaire applicable à CC-SG.
   b. **Pour définir la date et l'heure à l'aide du protocole NTP :** cochez la case **Activer le protocole de temps du réseau** au bas de la fenêtre et indiquez les adresses IP des **serveur principal (NTP)** et **serveur secondaire (NTP)** dans les champs correspondants.

   Remarque : Network Time Protocol (NTP) est le protocole utilisé pour synchroniser les données relatives à la date et à l'heure de l'ordinateur connecté à l'aide d'un serveur NTP référencé. Lorsque CC-SG est configuré à l'aide du protocole NTP, il peut synchroniser l'heure de son horloge sur celle du serveur de référence NTP publiquement disponible et conserver une heure correcte et cohérente.

3. Cliquez sur **Mettre à jour la configuration** pour appliquer les modifications relatives à l'heure et à la date à l'unité CC-SG.
4. Cliquez sur **Rafraîchir** pour recharger le nouveau temps serveur dans le champ **Heure actuelle**.

Choisissez **Maintenance du système** > **Redémarrer** pour redémarrer CC-SG.

Vérification de la matrice de compatibilité

La matrice de compatibilité répertorie les versions de firmware des dispositifs Raritan et les versions logicielles des applications compatibles avec la version actuelle de CC-SG. Lors de l'ajout d'un dispositif, de la mise à niveau du firmware d'un dispositif ou de la sélection de l'application à utiliser, CC-SG effectue une vérification à l'aide de ces données. Si la version du firmware ou la version logicielle est incompatible, CC-SG affiche un message d'avertissement avant que vous ne poursuiviez. Chaque version de CC-SG prend uniquement en charge les versions actuelles et antérieures de firmware des dispositifs Raritan au moment de la mise sur le marché. Vous pouvez également consulter la matrice de compatibilité sur le site Web du support Raritan.

➢ *Pour vérifier la matrice de compatibilité :*

- Dans le menu **Administration**, cliquez sur **Matrice de compatibilité**.

Vérification et mise à niveau des versions des applications

Vérifiez et mettez à niveau les versions des applications de CC-SG, telles que Raritan Console (RC) et Raritan Remote Client (RRC).

➢ *Pour vérifier la version d'une application :*

1. Choisissez **Administration** > **Applications**.
2. Sélectionnez le **nom de l'application** dans la liste. Notez le numéro figurant dans le champ **Version**. Certaines applications n'affichent pas automatiquement de numéro de version.

➢ *Pour mettre à niveau une application :*

Si la version n'est pas à jour, vous devez mettre à niveau l'application. Vous pouvez télécharger le fichier de mise à niveau de l'application depuis le site Web de Raritan. Pour obtenir la liste complète des versions d'application prises en charge, reportez-vous à la **matrice de compatibilité** sur le site Web du support Raritan.

1. Enregistrez le fichier d'application sur votre PC client.
2. Cliquez sur la flèche déroulante **Nom de l'application** et sélectionnez l'application que vous souhaitez mettre à niveau dans la liste. Si l'application n'apparaît pas, vous devez d'abord l'ajouter. ***Ajouter une application*** (à la page 168)

3. Cliquez sur **Parcourir**, recherchez et sélectionnez le fichier de mise à niveau de l'application dans la boîte de dialogue qui apparaît, puis cliquez sur **Ouvrir**.
4. Le nom de l'application s'affiche dans le champ **Nouveau fichier d'application** de l'écran **Gestionnaire des applications**.
5. Cliquez sur **Télécharger vers le serveur**. Une fenêtre indique la progression du téléchargement de la nouvelle application. Une fois le téléchargement terminé, une nouvelle fenêtre indique que l'application a été ajoutée à la base de données CC-SG et est prête à être utilisée.
6. Si le champ **Version** n'est pas automatiquement mis à jour, entrez-y le nouveau numéro de version. Le champ **Version** s'actualise automatiquement pour certaines applications.
7. Cliquez sur **Mettre à jour**.

Chapitre 4 Configuration de CC-SG par paramétrage guidé

Le paramétrage guidé est une méthode simple permettant d'effectuer les tâches de configuration initiales de CC-SG, une fois le réseau configuré. L'interface Paramétrage guidé vous guide à travers le processus de définition des associations, de détection et d'ajout de dispositifs à CC-SG, de création de groupes de dispositifs et de nœuds, de groupes d'utilisateurs, d'affectation de stratégies et de privilèges aux groupes d'utilisateurs, et d'ajout d'utilisateurs. Une fois le paramétrage guidé effectué, vous avez toujours la possibilité de modifier vos configurations individuellement.

Le paramétrage guidé se divise en quatre tâches :

- ***Associations*** (voir "Associations dans le paramétrage guidé" à la page 15) : permet de définir les catégories et éléments utilisés pour organiser vos équipements.
- ***Paramétrage du dispositif*** (à la page 16) : permet de détecter les dispositifs de votre réseau et de les ajouter à CC-SG. Autorise la configuration des ports de dispositif.
- ***Créer des groupes*** (à la page 18) : permet de classer les dispositifs et nœuds gérés par CC-SG dans des groupes et de créer des stratégies d'accès total pour chaque groupe.
- ***Gestion des utilisateurs*** (à la page 21) : permet d'ajouter des utilisateurs et des groupes d'utilisateurs à CC-SG, et de sélectionner les stratégies et les privilèges régissant l'accès des utilisateurs au sein de CC-SG et aux dispositifs et nœuds.

Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.

Dans ce chapitre

Avant d'utiliser le paramétrage guidé 15
Associations dans le paramétrage guidé 15
Paramétrage du dispositif 16
Créer des groupes 18
Gestion des utilisateurs 21

Avant d'utiliser le paramétrage guidé

Avant de procéder à la configuration de CC-SG, vous devez effectuer celle du système.

- Configurez et installez les appareils de la série Dominion et IP-Reach (dispositifs série et KVM), procédez notamment à l'affectation d'une adresse IP.

Associations dans le paramétrage guidé

Créer des catégories et des éléments

1. Dans la fenêtre Paramétrage guidé, cliquez sur **Associations**, puis sur **Create Categories** dans le panneau de gauche pour ouvrir le panneau correspondant.
2. Entrez le **nom de la catégorie** dans laquelle vous souhaitez organiser votre équipement, telle qu'Emplacement.
3. Dans le champ **Applicable à**, vous pouvez indiquer si la catégorie est disponible pour des dispositifs et/ou pour des nœuds. Cliquez sur le menu déroulant **Applicable à**, puis sélectionnez une valeur dans la liste.
4. Dans la table **Eléments**, entrez le nom d'un élément de la catégorie, tel que Raritan Etats-Unis.
   - Cliquez sur l'icône Ajouter une nouvelle ligne pour ajouter autant de rangées que nécessaire à la table **Eléments**.
   - Pour supprimer un élément de la table **Eléments**, sélectionnez la ligne correspondante, puis cliquez sur l'icône Supprimer la ligne .
5. Répétez ces étapes pour ajouter tous les éléments de la catégorie dans la table **Eléments**.
6. (Facultatif) Si vous souhaitez créer une autre catégorie, cliquez sur **Appliquer** pour enregistrer la catégorie en cours, puis répétez les étapes de cette section pour ajouter des catégories supplémentaires.
7. Une fois les catégories et éléments créés, cliquez sur **OK**. Le panneau Résumé des associations affiche la liste des catégories et des éléments que vous avez créés.
8. Cliquez sur **Continue** (continuer) pour démarrer la tâche suivante, **Paramétrage du dispositif**. Suivez les étapes de la section suivante.

Paramétrage du dispositif

Paramétrage du dispositif est la seconde tâche du paramétrage guidé. Elle vous permet de rechercher et de détecter des dispositifs sur votre réseau, et de les ajouter à CC-SG. Lorsque vous ajoutez des dispositifs, vous pouvez sélectionner un élément par catégorie pour l'associer au dispositif.

Important : assurez-vous qu'aucun autre utilisateur n'est connecté au dispositif lors de la configuration de CC-SG.

Détecter et ajouter des dispositifs

Le panneau **Détecter les dispositifs** s'ouvre lorsque vous cliquez sur **Continue** (continuer) à la fin de la tâche Associations. Vous pouvez également cliquer sur **Paramétrage du dispositif**, puis, dans l'arborescence **Tâches guidées** du panneau de gauche, sur **Détecter les dispositifs** pour ouvrir le panneau du même nom.

1. Dans les champs **Depuis l'adresse IP** et **Vers l'adresse IP**, entrez la plage d'adresses IP où vous souhaitez rechercher des dispositifs.
2. Dans le champ **Masque**, entrez le masque de sous-réseau dans lequel vous souhaitez rechercher des dispositifs.
3. Dans la liste **Types de dispositifs**, sélectionnez le type de dispositifs à rechercher dans la plage spécifiée. Maintenez la touche **Ctrl** enfoncée tout en cliquant sur les types de dispositifs souhaités pour en sélectionner plusieurs.
4. Cochez la case **Détection de diffusion** pour rechercher des dispositifs sur le sous-réseau où réside CC-SG. Pour détecter des dispositifs sur tous les sous-réseaux, désélectionnez **Détection de diffusion**.
5. Cliquez sur **Détecter**.
6. A la fin de la détection, un message de confirmation s'affiche. Cliquez sur **OK** dans le message de confirmation.
7. Si CC-SG a détecté des dispositifs du type spécifié et dans la plage d'adresses spécifiée, ils s'affichent dans une table de la section inférieure du panneau **Détecter les dispositifs**. Vous pouvez cliquer sur la flèche noire en haut du panneau pour masquer la section supérieure, et ainsi agrandir l'affichage des résultats de la détection dans la section inférieure du panneau.

8. Dans la table des dispositifs détectés, sélectionnez le dispositif à inclure à CC-SG, puis cliquez sur **Add** (ajouter). Le panneau **Ajouter un dispositif** s'ouvre. Le panneau **Ajouter un dispositif** varie légèrement selon le type de dispositif ajouté.
9. Vous pouvez modifier le **nom du dispositif** et la **description** en entrant de nouvelles données dans les champs correspondants.
10. Confirmez que l'adresse IP affectée lors de la préparation du dispositif à ajouter à CC-SG s'affiche dans le champ **Adresse IP ou nom d'hôte du dispositif**, ou entrez l'adresse correcte dans le champ, si nécessaire.
11. Le champ **Numéro de port TCP** est rempli automatiquement en fonction du type de dispositif.
12. Dans les champs correspondants, entrez les **nom d'utilisateur** et **mot de passe** créés lors de la préparation du dispositif à ajouter à CC-SG.
13. Dans le champ **Délai d'attente du test de détection de collision**, entrez le nombre de secondes qui doivent s'écouler avant expiration entre le dispositif et CC-SG.
14. Si vous ajoutez un dispositif Dominion SX, cochez la case **Accès local : Autorisé** pour autoriser l'accès local au dispositif. Désactivez la case **Accès local : Autorisé** pour interdire l'accès local au dispositif.
15. Si vous ajoutez un dispositif PowerStrip manuellement, cliquez sur la flèche déroulante **Nombre de prises** et sélectionnez le nombre de prises que le dispositif PowerStrip contient.
16. Si vous ajoutez un serveur IPMI, entrez l'**intervalle** à utiliser pour la vérification de la disponibilité. Dans le champ **Authentification**, précisez la méthode d'authentification configurée au niveau du serveur IPMI.
17. Si vous souhaitez configurer tous les ports disponibles sur le dispositif, cochez la case **Configurer tous les ports**. CC-SG ajoutera tous les ports du dispositif et créera un nœud pour chacun.
18. Dans la section **Associations de dispositifs** au bas du panneau, cliquez sur la flèche déroulante de la colonne Elément correspondant à chaque catégorie à affecter au dispositif, puis sélectionnez l'élément à associer au dispositif dans la liste.
19. Pour appliquer l'élément au dispositif et aux nœuds connectés à celui-ci, cochez la case **Appliquer aux nœuds**.
20. (Facultatif) Si vous souhaitez ajouter un autre dispositif, cliquez sur **Appliquer** pour enregistrer le dispositif en cours, puis répétez les étapes de cette section pour ajouter des dispositifs supplémentaires.

21. Une fois l'ajout des dispositifs terminé, cliquez sur **OK**. Le panneau **Résumé du dispositif** affiche la liste des dispositifs que vous avez ajoutés.
22. Cliquez sur **Continue** (Continuer) pour démarrer la tâche suivante, **Créer des groupes**. Suivez les étapes de la section suivante.

Créer des groupes

Créer des groupes est la troisième tâche du paramétrage guidé. Elle vous permet de définir des groupes de dispositifs et de nœuds, et de spécifier les membres de chacun de ces groupes. Les administrateurs peuvent gagner du temps en gérant des groupes de dispositifs et de nœuds similaires, au lieu de traiter chacun individuellement.

Ajouter des groupes de dispositifs et de nœuds

1. Le panneau **Groupes de dispositifs : Nouveau** s'ouvre lorsque vous cliquez sur **Continue** (continuer) à la fin de la tâche Paramétrage du dispositif. Vous pouvez également cliquer sur **Créer des groupes**, puis, dans l'arborescence **Tâches guidées** du panneau de gauche, sur **Ajouter des groupes de dispositifs** pour ouvrir le panneau **Groupes de dispositifs : Nouveau**.
2. Dans le champ **Nom du groupe**, entrez le nom du groupe de dispositifs à créer.
3. Vous pouvez ajouter des dispositifs à un groupe de deux façons : **Sélectionner les dispositifs** et **Décrire les dispositifs**. L'onglet Sélectionner les dispositifs vous permet de choisir dans la liste des dispositifs disponibles ceux que vous souhaitez affecter au groupe. L'onglet Décrire les dispositifs vous permet de spécifier des règles décrivant les dispositifs ; les dispositifs dont les paramètres respectent ces règles seront ajoutés au groupe.

Sélectionner les dispositifs

a. Cliquez sur l'onglet Sélectionner les dispositifs dans le panneau Ajouter des groupes de dispositifs.

b. Dans la liste **Disponible**, sélectionnez le dispositif à inclure au groupe, puis cliquez sur **Ajouter** pour le déplacer vers la liste **Sélectionné**. Les dispositifs de la liste **Sélectionné** seront ajoutés au groupe.

- Pour supprimer un dispositif du groupe, sélectionnez son nom dans la liste **Sélectionné**, puis cliquez sur **Retirer**.

- Vous pouvez rechercher un dispositif dans la liste **Disponible** ou dans la liste **Sélectionné**. Entrez les termes de la recherche dans le champ sous la liste, puis cliquez sur **Aller à**.

Décrire les dispositifs

a. Cliquez sur l'onglet **Décrire les dispositifs** dans le panneau **Ajouter des groupes de dispositifs**. Dans l'onglet Décrire les dispositifs, vous créez une table de règles décrivant les dispositifs à affecter au groupe.

b. Cliquez sur l'icône Ajouter une nouvelle ligne pour ajouter une rangée à la table.

c. Double-cliquez sur la cellule créée pour chaque colonne afin d'activer un menu déroulant. Dans chaque liste, sélectionnez les composants de règle à utiliser.

1. Cochez la case **Créer une stratégie d'accès total** pour le groupe si vous souhaitez définir, pour ce groupe de dispositifs, une stratégie autorisant l'accès permanent à tous les nœuds et dispositifs du groupe avec permission de contrôle.
2. (Facultatif) Si vous souhaitez ajouter un autre groupe de dispositifs, cliquez sur **Appliquer** pour enregistrer le groupe en cours, puis répétez les étapes de cette section pour ajouter des groupes de dispositifs supplémentaires.
3. Une fois l'ajout des groupes de dispositifs terminé, cliquez sur **OK**. Le panneau **Groupes de nœuds : Nouveau** s'ouvre. Vous pouvez également cliquer sur **Créer des groupes**, puis, dans l'arborescence **Tâches guidées** du panneau de gauche, sur **Ajouter des groupes de nœuds** pour ouvrir le panneau **Gestionnaire des groupes de nœuds**.
4. Dans le champ **Nom du groupe**, entrez le nom du groupe de nœuds à créer.
5. Vous pouvez ajouter des nœuds à un groupe de deux façons : **Sélectionner les nœuds** et **Décrire les nœuds**. L'onglet Sélectionner les nœuds vous permet de choisir dans la liste des nœuds disponibles ceux que vous souhaitez affecter au groupe. L'onglet Décrire les nœuds vous permet de spécifier des règles décrivant les nœuds ; les nœuds dont les paramètres respectent ces règles seront ajoutés au groupe.

Sélectionner les nœuds

a. Cliquez sur l'onglet **Sélectionner les nœuds** dans le panneau **Ajouter des groupes de nœuds**.

b. Dans la liste **Disponible**, sélectionnez le nœud à inclure au groupe, puis cliquez sur **Ajouter** pour le déplacer vers la liste **Sélectionné**. Les nœuds de la liste **Sélectionné** seront ajoutés au groupe.

c. Pour supprimer un nœud du groupe, sélectionnez son nom dans la liste **Sélectionné**, puis cliquez sur **Retirer**.

d. Vous pouvez rechercher un nœud dans la liste **Disponible** ou dans la liste **Sélectionné**. Entrez les termes de la recherche dans le champ sous la liste, puis cliquez sur **Aller à**.

Décrire les nœuds

a. Cliquez sur l'onglet **Décrire les nœuds** dans le panneau **Ajouter des groupes de nœuds**. Dans l'onglet Décrire les nœuds, vous créez une table de règles décrivant les nœuds à affecter au groupe.

b. Cliquez sur l'icône Ajouter une nouvelle ligne pour ajouter une rangée à la table.

c. Double-cliquez sur la cellule créée pour chaque colonne afin d'activer un menu déroulant. Dans chaque liste, sélectionnez les composants de règle à utiliser. ***Stratégies de contrôle d'accès*** (à la page 102).

d. Cochez la case **Créer une stratégie d'accès total** pour le groupe si vous souhaitez définir, pour ce groupe de nœuds, une stratégie autorisant l'accès permanent à tous les nœuds et dispositifs du groupe avec permission de contrôle.

e. (Facultatif) Si vous souhaitez ajouter un autre groupe de nœuds, cliquez sur **Appliquer** pour enregistrer le groupe en cours, puis répétez les étapes de cette section pour ajouter des groupes de nœuds supplémentaires.

1. Une fois l'ajout des groupes de nœuds terminé, cliquez sur **OK**. Le panneau **Résumé des groupes** affiche la liste des groupes que vous avez ajoutés.
2. Cliquez sur **Continue** (Continuer) pour démarrer la tâche suivante, **Gestion des utilisateurs**. Suivez les étapes de la section suivante.

Gestion des utilisateurs

Gestion des utilisateurs est la quatrième tâche du paramétrage guidé. Elle vous permet de sélectionner les **privilèges** et **stratégies** régissant l'accès et les activités des groupes d'utilisateurs. Les privilèges indiquent les activités que les membres d'un groupe d'utilisateurs peuvent exécuter dans CC-SG. Les stratégies indiquent les dispositifs et les nœuds que les membres d'un groupe d'utilisateurs peuvent afficher et modifier. Les stratégies sont basées sur des catégories et des éléments. Une fois les groupes d'utilisateurs créés, vous pouvez définir des utilisateurs individuels et les ajouter aux groupes.

Ajouter des groupes d'utilisateurs et des utilisateurs

Le panneau **Ajouter un groupe d'utilisateurs** s'ouvre lorsque vous cliquez sur **Continue** (continuer) à la fin de la tâche Créer des groupes. Vous pouvez également cliquer sur **Gestion des utilisateurs**, puis, dans l'arborescence **Tâches guidées** du panneau de gauche, sur **Ajouter un groupe d'utilisateurs** pour ouvrir le panneau du même nom.

1. Dans le champ **Nom du groupe d'utilisateurs**, entrez le nom du groupe à créer. Les noms de groupes d'utilisateurs peuvent contenir jusqu'à 32 caractères.
2. Dans le champ **Description**, entrez la description du groupe d'utilisateurs.
3. Cliquez sur l'onglet **Droits d'administrateur**, puis cochez les cases correspondant aux **privilèges** ou aux types d'activités CC-SG que vous souhaitez affecter au groupe d'utilisateurs.
4. Dans la section **Accès au nœud**, vous pouvez indiquer si le groupe d'utilisateurs doit avoir accès aux nœuds **en bande** et **hors bande**, et aux fonctions de **gestion de l'alimentation**. Cochez les cases correspondant aux types d'accès que vous souhaitez affecter au groupe.
5. Cliquez sur l'onglet **Stratégies**.
6. Dans la liste **Toutes les stratégies**, sélectionnez la **stratégie** à affecter au groupe d'utilisateurs, puis cliquez sur **Ajouter** pour la déplacer vers la liste **Stratégies sélectionnées**. Les éléments de la liste **Stratégies sélectionnées** seront affectés au groupe d'utilisateurs. Répétez cette étape pour ajouter des stratégies supplémentaires au groupe d'utilisateurs.

7. Pour supprimer une stratégie du groupe d'utilisateurs, sélectionnez son nom dans la liste **Stratégies sélectionnées**, puis cliquez sur **Supprimer**.
8. Pour associer des utilisateurs authentifiés à distance à des modules Active Directory, cliquez sur l'onglet **Active Directory Associations** (associations Active Directory). Cochez la case correspondant à chaque module Active Directory à associer au groupe d'utilisateurs.
9. (Facultatif) Si vous souhaitez ajouter un autre groupe d'utilisateurs, cliquez sur **Appliquer** pour enregistrer le groupe en cours, puis répétez les étapes de cette section pour ajouter des groupes d'utilisateurs supplémentaires.
10. Une fois l'ajout des groupes d'utilisateurs terminé, cliquez sur **OK**. Le panneau **Ajouter un utilisateur** s'ouvre. Vous pouvez également cliquer sur **Gestion des utilisateurs**, puis, dans l'arborescence **Tâches guidées** du panneau de gauche, sur **Ajouter un utilisateur** pour ouvrir le panneau du même nom.
11. Dans le champ **Nom d'utilisateur**, entrez le nom dont l'utilisateur à ajouter se servira pour se connecter à CC-SG.
12. Cochez la case **Connexion activée** pour autoriser l'utilisateur à se connecter à CC-SG.
13. Cochez la case **Authentification à distance** uniquement si vous souhaitez que l'utilisateur soit authentifié par un serveur externe, tel que TACACS+, RADIUS, LDAP ou AD. Si vous utilisez l'authentification à distance, le mot de passe n'est pas obligatoire. Les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe** sont désactivés si l'option **Authentification à distance** est cochée.
14. Dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**, entrez le mot de passe dont l'utilisateur se servira pour se connecter à CC-SG.
15. Cochez la case **Forcer la modification du mot de passe à la prochaine connexion** pour obliger l'utilisateur à changer le mot de passe affecté à l'ouverture de session suivante.
16. Cochez la case **Forcer la modification du mot de passe régulièrement** pour indiquer la fréquence à laquelle l'utilisateur devra changer le mot de passe.
17. Dans le champ **Période d'expiration (en jours)**, entrez le délai pendant lequel l'utilisateur pourra se servir du même mot de passe avant d'être obligé de le changer.

Raritan.
When you're ready to take control®

18. Entrez l'**adresse électronique** de l'utilisateur dans le champ correspondant.
19. Cliquez sur la flèche déroulante **Groupe(s) d'utilisateurs** et sélectionnez dans la liste le groupe d'utilisateurs auquel vous souhaitez affecter l'utilisateur.
20. (Facultatif) Si vous souhaitez ajouter un autre utilisateur, cliquez sur **Appliquer** pour enregistrer l'utilisateur en cours, puis répétez les étapes de cette section pour ajouter des utilisateurs supplémentaires.
21. Une fois l'ajout des utilisateurs terminé, cliquez sur **OK**. Le panneau **Résumé du groupe d'utilisateurs** affiche la liste des groupes d'utilisateurs que vous avez ajoutés.

Chapitre 5 Associations, catégories et éléments

Dans ce chapitre

A propos des associations.....24
Gestionnaire des associations.....26

A propos des associations

Vous pouvez paramétrer des associations afin de faciliter l'organisation de l'équipement géré par CC-SG. Chaque association comprend une catégorie, qui correspond au groupe organisationnel le plus élevé, et ses éléments associés, qui sont des sous-ensembles d'une catégorie. Imaginons par exemple que vos dispositifs Raritan servent à gérer des serveurs cible dans des centres de données situés en Amérique, en Asie-Pacifique et en Europe. Vous pourriez paramétrer une association organisant ces équipements par emplacement. Vous pouvez ensuite personnaliser CC-SG afin d'afficher vos dispositifs et nœuds Raritan en fonction de la catégorie choisie, Emplacement, et de ses éléments associés : Amérique, Asie-Pacifique et Europe, dans l'interface CC-SG. Vous pouvez personnaliser CC-SG afin d'organiser et d'afficher les serveurs comme vous le souhaitez.

Terminologie relative aux associations

- **Associations** – désigne les relations entre les catégories, les éléments d'une catégorie, et les nœuds et dispositifs.
- **Catégorie** – variable contenant un jeu de valeurs appelées éléments. Emplacement est un exemple de catégorie qui peut contenir les éléments Amérique et Asie-Pacifique. Type de SE est un autre exemple de catégorie, qui peut contenir des éléments tels que Windows, Unix ou Linux.
- **Eléments** – désigne les valeurs d'une catégorie. Par exemple, l'élément Amérique appartient à la catégorie Emplacement.

Associations – Définition des catégories et des éléments

Les dispositifs et nœuds Raritan sont organisés par catégories et par éléments. Chaque paire catégorie/élément est affectée à un dispositif et/ou à un nœud. Par conséquent, il est nécessaire de définir les catégories et les éléments avant d'ajouter un dispositif Raritan à CC-SG.

Une catégorie est un groupe d'éléments similaires. Par exemple, pour regrouper vos dispositifs Raritan par emplacement, vous pouvez définir une catégorie Emplacement, contenant un ensemble d'éléments, tels que New York, Philadelphie et La Nouvelle Orléans.

Les stratégies reposent également sur l'utilisation de catégories et d'éléments pour contrôler l'accès des utilisateurs aux serveurs. Par exemple, la paire catégorie/élément Emplacement/New York peut servir à créer une stratégie contrôlant l'accès des utilisateurs aux serveurs de New York.

Voici d'autres exemples d'associations type entre une catégorie et des éléments :

Catégorie	Eléments
Emplacement	New York, Philadelphie, La Nouvelle Orléans
Type de SE	Unix, Windows, Linux
Service	Ventes, Informatique, Technique

Les associations doivent être configurées simplement pour accomplir les objectifs de classement des serveurs/nœuds et d'accès des utilisateurs. Un nœud ne peut être affecté qu'à un seul élément d'une catégorie. Par exemple, un serveur cible ne peut pas être affecté en même temps aux éléments Windows et Unix de la catégorie Type de SE.

Voici une méthode pratique pour organiser vos systèmes lorsque les serveurs sont similaires et qu'ils doivent être organisés de manière aléatoire :

Catégorie	Elément
usergroup1	usergroup1node
usergroup2	usergroup2node
usergroup3	usergroup3node

Lorsque vous ajoutez des dispositifs et des nœuds, vous les reliez aux catégories et éléments que vous avez prédéfinis. Lorsque vous créez des groupes de nœuds et de dispositifs et que vous leur affectez des stratégies, vous utilisez vos catégories et éléments pour déterminer les nœuds et les dispositifs appartenant à chaque groupe.

Comment créer des associations

Vous disposez de deux méthodes pour créer des associations : le paramétrage guidé et le Gestionnaire des associations.

- Le **paramétrage guidé** combine plusieurs tâches de configuration dans une interface automatisée. Cette méthode est recommandée pour la configuration initiale de CC-SG. Une fois le paramétrage guidé effectué, vous avez toujours la possibilité de modifier vos configurations individuellement. ***Configuration de CC-SG par paramétrage guidé*** (à la page 14)
- Le **Gestionnaire des associations** vous permet de travailler sur les associations uniquement et n'automatise aucune tâche de configuration. Vous pouvez également utiliser le Gestionnaire des associations pour modifier celles-ci après le paramétrage guidé. ***Gestionnaire des associations*** (à la page 26)

Gestionnaire des associations

Le Gestionnaire des associations permet d'ajouter, de modifier ou de supprimer des catégories et des éléments.

Ajouter une catégorie

1. Choisissez **Associations** > **Association**.
2. Cliquez sur **Ajouter**. La fenêtre **Ajouter une catégorie** s'affiche.
3. Renseignez le champ **Nom de la catégorie**. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
4. Sélectionnez le type de données des éléments.
   - Sélectionnez **Chaîne** si la valeur est lue sous forme de texte.
   - Sélectionnez **Nombre entier** si la valeur est numérique.
5. Dans le champ Applicable à, sélectionnez si cette catégorie s'applique à des **dispositifs**, des **nœuds** ou des **dispositifs et nœuds**.
6. Cliquez sur **OK** pour créer la catégorie. Le nom de la nouvelle catégorie s'affiche dans le champ **Nom de la catégorie**.

Modifier une catégorie

Notez que la valeur Chaîne ne peut pas être remplacée par Nombre entier et inversement. Si vous devez effectuer ce type de modification, supprimez la catégorie et ajoutez-en une nouvelle.

1. Choisissez **Associations** > **Association**.
2. Cliquez sur la flèche déroulante **Nom de la catégorie** et sélectionnez la catégorie à modifier.
3. Cliquez sur **Modifier** dans le panneau **Catégorie** de l'écran pour modifier la catégorie. La fenêtre **Modifier une catégorie** s'affiche.
4. Modifiez la valeur du champ **Nom de la catégorie**.
5. Cliquez sur la flèche déroulante **Applicable à** pour indiquer si cette catégorie s'applique à **Dispositif**, **Nœud** ou **Les deux**.
6. Cliquez sur **OK** pour enregistrer les modifications. Le nom de la catégorie mise à jour s'affiche dans le champ **Nom de la catégorie**.

Supprimer une catégorie

Si vous supprimez une catégorie, tous les éléments créés dans celle-ci le sont également. La catégorie supprimée n'apparaît plus dans l'arborescence Nœuds ou Dispositifs une fois que l'écran a été rafraîchi ou que l'utilisateur se déconnecte et se reconnecte à CC-SG.

1. Choisissez **Associations** > **Association**.
2. Cliquez sur la flèche déroulante **Nom de la catégorie** et sélectionnez la catégorie à supprimer.
3. Cliquez sur **Supprimer** dans le panneau **Catégorie** de l'écran pour supprimer la catégorie. La fenêtre **Supprimer une catégorie** s'affiche.
4. Cliquez sur **Oui** pour supprimer la catégorie.

Ajouter un élément

1. Choisissez **Associations** > **Association**.
2. Cliquez sur la flèche déroulante **Nom de la catégorie** et sélectionnez la catégorie à laquelle vous souhaitez ajouter un nouvel élément.
3. Cliquez sur l'icône Ajouter une nouvelle ligne.
4. Entrez le nom du nouvel élément sur la ligne vide. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms. Le nom des éléments est sensible à la casse.

5. Cliquez sur **OK** pour enregistrer les modifications.

Modifier un élément

1. Dans le menu **Associations**, cliquez sur **Gestionnaire des associations**.
2. Cliquez sur la flèche déroulante **Nom de la catégorie** et sélectionnez la catégorie dont vous souhaiter modifier un élément.
3. Sélectionnez l'élément à modifier dans la liste **Eléments de la catégorie** et cliquez sur **Modifier**. La fenêtre **Modifier un élément** s'affiche.
4. Tapez le nouveau nom de l'élément dans le champ **Entrer la nouvelle valeur de l'élément**. Le nom des éléments est sensible à la casse.
5. Cliquez sur **OK** pour actualiser l'élément ou sur **Cancel (Annuler)** pour fermer la fenêtre. Le nouveau nom de l'élément s'affiche dans la liste **Eléments de la catégorie**.

Supprimer un élément

La suppression d'un élément le retire de toutes les associations ; les champs d'association sont alors vides.

1. Choisissez **Associations** > **Association**.
2. Cliquez sur la flèche déroulante **Nom de la catégorie** et sélectionnez la catégorie dont vous souhaiter supprimer un élément.
3. Sélectionnez l'élément à supprimer dans la liste **Eléments**, puis cliquez sur l'icône Supprimer la ligne.
4. Cliquez sur OK pour enregistrer vos modifications.

Raritan.
When you're ready to take control®

Chapitre 6 Dispositifs, groupes de dispositifs et ports

Pour ajouter des dispositifs PowerStrip Raritan connectés à d'autres dispositifs Raritan dans CC-SG, reportez-vous à ***Barrettes d'alimentation gérées*** (à la page 56) pour plus d'informations.

Remarque : *pour configurer des dispositifs iLO/RILOE, IPMI, Dell DRAC, IBM RSA ou d'autres dispositifs non Raritan, utilisez l'option de menu* ***Ajouter un nœud*** *et ajoutez ces éléments comme interface. Reportez-vous à* **Nœuds, groupes de nœuds et interfaces** *(à la page 65) pour plus d'informations.*

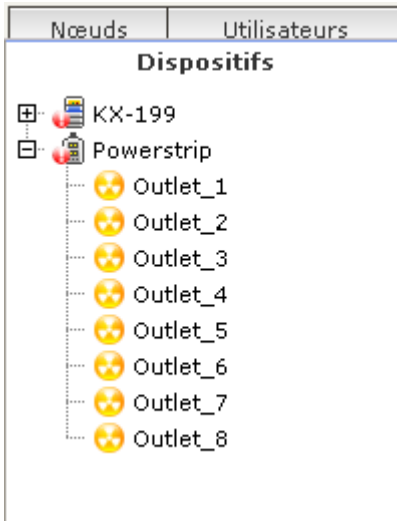
Dans ce chapitre

Affichage des dispositifs 30
Recherche de dispositifs 33
Détection des dispositifs 34
Ajout d'un dispositif 35
Modification d'un dispositif 37
Modification d'un dispositif PowerStrip 38
Suppression d'un dispositif 38
Configuration des ports 39
Modification d'un port 40
Suppression d'un port 41
Copie en bloc de catégories et d'éléments de dispositifs 41
Mise à niveau d'un dispositif 42
Sauvegarde de la configuration du dispositif 42
Restauration de la configuration du dispositif 43
Copie de la configuration du dispositif 46
Redémarrage du dispositif 46
Envoi d'une commande ping au dispositif 47
Suspension de la gestion 47
Reprise de la gestion 47
Gestionnaire d'alimentation des dispositifs 48
Démarrage d'admin 48
Vue topologique 49
Déconnexion des utilisateurs 49
Accès spécial aux dispositifs du système Paragon II 50
Gestionnaire des groupes de dispositifs 51

Affichage des dispositifs

Onglet Dispositifs

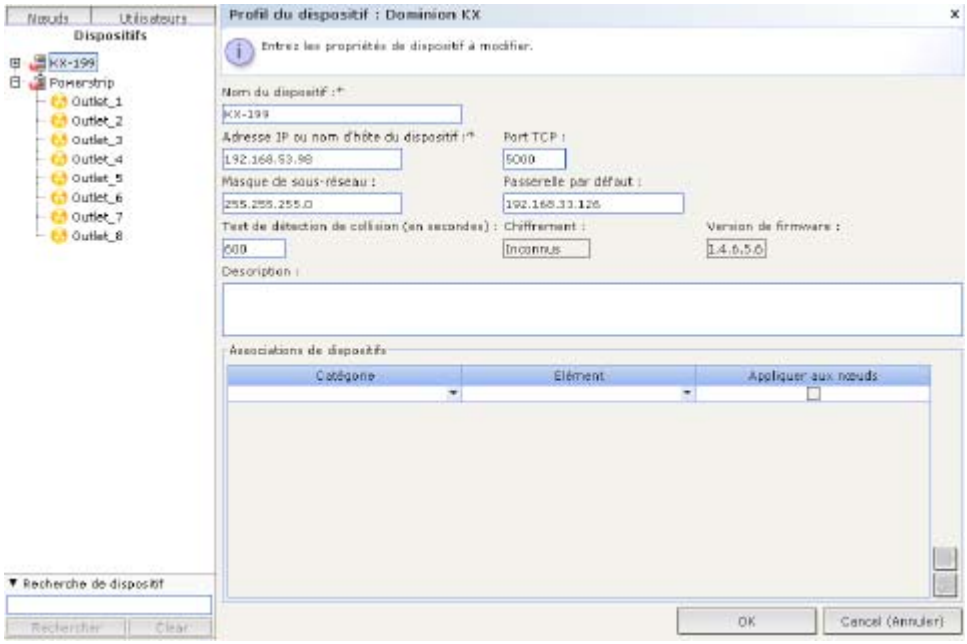
Cliquez sur l'onglet **Dispositifs** pour afficher tous les dispositifs dont CC-SG assure la gestion.



Les ports configurés de chaque dispositif sont imbriqués sous les dispositifs auxquels ils appartiennent. Dans la liste, le symbole + apparaît en regard des dispositifs dotés de ports configurés. Cliquez sur le symbole + pour développer ou masquer la liste des ports.

Ecran Profil du dispositif

Lorsque vous cliquez sur un dispositif sous l'onglet Dispositifs, l'écran **Profil du dispositif** apparaît, affichant des informations sur le dispositif sélectionné.



Icônes de dispositif et de port

Pour faciliter leur identification, les dispositifs et ports KVM, série et d'alimentation sont représentés par des icônes différentes dans l'arborescence Dispositifs. Placez le pointeur de la souris au-dessus d'une icône dans l'arborescence Dispositifs pour afficher une info-bulle contenant des informations sur le dispositif ou port.

Icône	Signification
	Dispositif disponible
	Port KVM disponible ou connecté
	Port KVM inactif
	Port série disponible
	Port série non disponible

	Port fantôme (reportez-vous au manuel d'utilisation de Paragon II Raritan pour plus d'informations sur le mode fantôme.)
	Dispositif suspendu
	Dispositif non disponible
	Barrette d'alimentation
	Port de prise

Options de tri des ports

Les ports configurés sont regroupés sous leurs dispositifs parents dans l'onglet Dispositifs. Vous pouvez modifier le mode de tri des ports. Les ports triés par état sont classés par ordre alphabétique au sein des groupes d'état de connexion. Les noms des dispositifs sont aussi classés en conséquence.

1. Choisissez **Dispositifs** > **Options de tri des ports**.
2. Sélectionnez **Par nom de port** ou **Par état de port** pour organiser les ports au sein des dispositifs dans l'ordre alphabétique des noms ou par état de disponibilité.

Options clic bouton droit de l'onglet Dispositifs

Vous pouvez cliquer avec le bouton droit sur un dispositif ou un port dans l'onglet Dispositifs pour afficher un menu des commandes disponibles pour la sélection.

Recherche de dispositifs

L'onglet Dispositifs offre la possibilité de rechercher des dispositifs dans l'arborescence. La recherche ne renvoie que des dispositifs et n'inclut pas de nom de port. La méthode de recherche peut être configurée dans **Mon profil** (voir "Modifier votre préférence de recherche par défaut" à la page 99).

➢ *Pour rechercher un dispositif :*

- Au bas de l'onglet Dispositifs, entrez une chaîne de recherche dans le champ **Recherche de dispositif** et appuyez sur **ENTREE**.
- Les ***caractères joker*** (voir "Caractères joker de recherche" à la page 33) sont pris en charge dans la chaîne de recherche.

Caractères joker de recherche

Caractère joker	Description
?	Indique un caractère quelconque.
[-]	Indique un caractère dans une plage.
*	Indique zéro caractère ou plus.

Exemple de caractères joker

Exemple	Description
KX?	Permet de trouver **KX1** et **KXZ**, mais pas **KX1Z**.
KX*	Permet de trouver **KX1**, **KX**, **KX1** et **KX1Z**.
KX[0-9][0-9]T	Permet de trouver **KX95T**, **KX66T**, mais pas **KXZ** et **KX5PT**.

Détection des dispositifs

La commande Détecter les dispositifs déclenche la recherche de tous les dispositifs Raritan de votre réseau. Une fois les dispositifs détectés, vous pouvez les ajouter à CC-SG s'ils ne sont pas encore gérés.

➢ *Pour détecter des dispositifs :*

1. Choisissez **Dispositifs** > **Détecter les dispositifs**.
2. Dans les champs **Depuis l'adresse IP** et **Vers l'adresse IP**, entrez la plage d'adresses IP où vous pensez trouver les dispositifs. La valeur entrée dans le champ **Vers l'adresse IP** doit être supérieure à celle du champ **Depuis l'adresse IP**. Indiquez le masque à appliquer à la plage. Si aucun masque n'est spécifié, l'adresse de diffusion **255 255 255 255** est envoyée ; elle émet sur l'ensemble des réseaux locaux. Pour détecter des dispositifs sur des sous-réseaux, un masque doit obligatoirement être spécifié.
3. Cochez la case **Détection de diffusion** pour rechercher des dispositifs sur le sous-réseau où réside CC-SG. Pour détecter des dispositifs sur différents sous-réseaux, désactivez la case **Détection de diffusion**.
4. Pour rechercher un type de dispositif particulier, sélectionnez-le dans la liste **Types de dispositifs**. Par défaut, tous les types de dispositifs sont sélectionnés. Pour sélectionner plusieurs types de dispositifs, cliquez dessus tout en appuyant sur la touche Ctrl.
5. Cochez la case **Inclure des agents IPMI** pour détecter des cibles offrant la gestion de l'alimentation IPMI.
6. Cliquez sur **Détecter** pour démarrer la recherche. A tout moment de l'opération, vous pouvez cliquer sur **Arrêter** pour interrompre le processus de détection. Les dispositifs détectés apparaissent dans une liste.
7. Pour ajouter des dispositifs détectés à CC-SG, sélectionnez-les dans la liste, puis cliquez sur **Ajouter**. Dans l'écran Ajouter un dispositif qui apparaît, certaines données sont déjà indiquées.

   Si vous avez sélectionné plusieurs dispositifs à ajouter, vous pouvez cliquer sur **Précédent** et sur **Ignorer** au bas de l'écran pour parcourir les écrans Ajouter un dispositif des unités à inclure.
8. Renseignez les champs **Nom d'utilisateur** et **Mot de passe** pour permettre à CC-SG d'authentifier le dispositif lors de communications à venir.
9. Sélectionnez les **catégories** et **éléments** à appliquer au dispositif.

10. Pour appliquer une catégorie et un élément aux nœuds connectés au dispositif, cochez la case **Appliquer aux nœuds** correspondante.
11. (Facultatif) Modifiez les champs **Nom du dispositif**, **Délai d'attente du test de détection de collision(s)**, **Accès local** (si disponible pour le type de dispositif), **Description**, **Configurer tous les ports** et **Associations de dispositifs**.
12. Lorsque la configuration du dispositif est terminée, cliquez sur **Appliquer** pour ajouter celui-ci et ouvrir l'écran Ajouter un dispositif correspondant à l'élément détecté suivant. Ou, cliquez sur **OK** pour ajouter le dispositif sans passer aux autres dispositifs détectés.

    Si la version de firmware d'un dispositif n'est pas compatible avec CC-SG, un message apparaît. Cliquez sur **Oui** pour ajouter le dispositif à CC-SG ou sur **Non** pour annuler l'opération. Vous pouvez mettre à niveau le firmware du dispositif après avoir ajouté ce dernier à CC-SG. Reportez-vous à **Mettre les dispositifs à niveau** pour plus d'informations.

Ajout d'un dispositif

Les dispositifs doivent être ajoutés à CC-SG avant de configurer des ports ou d'ajouter des interfaces fournissant l'accès aux nœuds connectés aux ports. L'écran **Ajouter un dispositif** permet d'ajouter les dispositifs dont vous connaissez les propriétés.

Pour ajouter des dispositifs PowerStrip Raritan connectés à d'autres dispositifs Raritan dans CC-SG, reportez-vous à ***Configuration de la gestion de l'alimentation*** (voir "Barrettes d'alimentation gérées" à la page 56) pour plus d'informations.

➢ *Pour ajouter un dispositif à CC-SG :*

1. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Ajouter un dispositif**.
2. Cliquez sur la flèche déroulante **Type de dispositif** et sélectionnez, dans la liste, le type de dispositif que vous ajoutez. Si vous sélectionnez **PowerStrip**, l'aspect de l'écran Ajouter un dispositif varie légèrement.

Ajouter un dispositif KVM ou série

1. Renseignez le champ **Nom du dispositif**. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.

2. Renseignez le champ **Adresse IP ou nom d'hôte** du dispositif. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2).
3. Entrez le numéro du port de communication TCP utilisé pour communiquer avec le dispositif dans le champ **Numéro de port TCP**. Le numéro ne doit pas dépasser 5 caractères numériques. Le numéro de port par défaut de la plupart des dispositifs Raritan est 5000.
4. Entrez le nom utilisé pour vous connecter à ce dispositif dans le champ **Nom d'utilisateur**. L'utilisateur doit disposer d'un accès administratif.
5. Entrez le mot de passe permettant d'accéder à ce dispositif dans le champ **Mot de passe**. L'utilisateur doit disposer d'un accès administratif.
6. Entrez le temps (en secondes) qui doit s'écouler avant expiration entre le nouveau dispositif et CC-SG dans le champ **Délai d'attente du test de détection de collision(s)**.
7. Lorsque vous ajoutez un dispositif Dominion SX, la case à cocher Autoriser l'accès au port local permet d'accorder ou de refuser l'accès au port local au dispositif. Cochez cette case pour accorder aux utilisateurs l'accès direct à ce dispositif pendant qu'il est géré par CC-SG.
8. (Facultatif) Entrez une brève description de ce dispositif dans le champ **Description**.
9. Cochez la case **Configurer tous les ports** pour ajouter automatiquement tous les ports de ce dispositif à l'onglet Dispositifs et créer un nœud pour chaque port du dispositif dans l'onglet Nœuds.
   - Les nœuds et ports correspondants seront configurés avec le même nom.
   - Un nœud est créé pour chaque port et une interface hors bande est créée pour ce nœud.
10. Une liste de **catégories** et d'**éléments** peut être configurée pour décrire et organiser de façon optimale le dispositif concerné et les nœuds qui lui sont connectés. Reportez-vous à ***Associations*** (voir "Associations, catégories et éléments" à la page 24) pour plus d'informations.

a. Pour chaque **catégorie** listée, cliquez sur le menu déroulant **Elément**, puis sélectionnez l'élément que vous souhaitez appliquer au dispositif correspondant. Sélectionnez l'élément vide du champ **Elément** lorsque vous ne souhaitez pas utiliser une catégorie.

   Pour affecter l'élément aux nœuds associés, ainsi qu'au dispositif, cochez la case **Appliquer aux nœuds**.

   Si les valeurs **Catégorie** ou **Elément** que vous souhaitez utiliser n'apparaissent pas, vous pouvez en ajouter via le menu **Associations**. Reportez-vous à ***Associations*** (voir "Associations, catégories et éléments" à la page 24) pour plus d'informations.

11. Lorsque la configuration du dispositif est terminée, cliquez sur **Appliquer** pour l'ajouter et ouvrir un nouvel écran Ajouter un dispositif vide afin de poursuivre l'ajout des dispositifs. Ou, cliquez sur **OK** pour ajouter le dispositif sans afficher de nouvel écran Ajouter un dispositif.
12. Si la version de firmware du dispositif n'est pas compatible avec CC-SG, un message apparaît. Cliquez sur **Oui** pour ajouter le dispositif à CC-SG. Vous pouvez mettre à niveau le firmware du dispositif après avoir ajouté ce dernier à CC-SG. Reportez-vous à ***Mise à niveau d'un dispositif*** (à la page 42) pour plus d'informations.

Ajouter un dispositif PowerStrip

L'ajout d'un dispositif PowerStrip à CC-SG varie selon le dispositif Raritan auquel la barrette d'alimentation est connectée physiquement. Reportez-vous à ***Barrettes d'alimentation gérées*** (à la page 56) pour plus d'informations.

Modification d'un dispositif

Vous pouvez modifier un dispositif pour le renommer et changer ses propriétés.

➢ *Pour modifier un dispositif :*

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif à modifier.
2. Dans l'écran Profil du dispositif, modifiez les paramètres selon les besoins.
3. Cliquez sur **OK** pour enregistrer les modifications.

Modification d'un dispositif PowerStrip

Vous pouvez modifier un dispositif PowerStrip géré afin de le renommer, de changer ses propriétés et d'afficher l'état de la configuration des prises.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif PowerStrip à modifier.
2. Entrez les nouvelles propriétés du dispositif dans les champs appropriés de l'écran. Si nécessaire, modifiez les catégories et éléments associés au dispositif.
3. Cliquez sur l'onglet **Outlets** (prises) pour afficher toutes les prises de la barrette d'alimentation.
4. Si une prise est associée à un nœud, vous pouvez cliquer sur le lien hypertexte **Nœud** pour ouvrir le profil du nœud.
5. Si une prise est associée à un nœud, vous pouvez sélectionner la prise, puis cliquez sur **Power Control** (gestion de l'alimentation) afin d'ouvrir l'écran Gestion de l'alimentation pour le nœud associé.
6. Cliquez sur **OK** pour enregistrer les modifications. Un message apparaît lorsque le dispositif a été modifié.

Suppression d'un dispositif

Vous pouvez supprimer un dispositif pour annuler sa gestion par CC-SG.

Important : la suppression d'un dispositif entraîne celle de tous les ports configurés pour lui. Toutes les interfaces associées à ces ports seront retirées des nœuds. En l'absence d'autre interface pour ces nœuds, ceux-ci seront supprimés de CC-SG.

Remarque : *vous devez suspendre les dispositifs KSX avant de les supprimer de CC-SG. Pour ce faire, cliquez avec le bouton droit sur le dispositif sous l'onglet Dispositifs, puis cliquez sur* ***Suspendre la gestion****. Cliquez sur* ***Oui*** *dans le message de confirmation qui apparaît. Le dispositif KSX redémarrera. Une fois le dispositif suspendu, vous pouvez le supprimer de CC-SG.*

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif à modifier.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Supprimer un dispositif**.

3. Cliquez sur **OK** pour supprimer le dispositif. Un message apparaît lorsque le dispositif a été supprimé.

Configuration des ports

Si les ports d'un dispositif n'ont pas tous été automatiquement inclus par l'activation de la case **Configurer tous les ports** lors de l'ajout du dispositif dans l'écran **Ajouter un dispositif**, vous pouvez utiliser l'écran Configurer les ports pour ajouter des ports individuels ou un ensemble de ports du dispositif à CC-SG. Vous devez configurer les ports avant l'ajout aux nœuds de toute interface hors bande.

Configurer un port série

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez un dispositif série.
2. Choisissez **Dispositifs** > **Gestionnaire des ports** > **Configurer les ports**.
3. Cliquez sur un en-tête de colonne pour classer les ports par cet attribut dans l'ordre croissant. Cliquez de nouveau sur l'en-tête pour classer les ports dans l'ordre décroissant.
4. Cliquez sur le bouton **Configurer** qui correspond au port série à configurer.
5. Renseignez le champ **Nom du port**. Pour une plus grande facilité d'utilisation, il est conseillé de nommer le port d'après la cible qui lui est connectée. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
6. Renseignez le champ **Nom de nœud** pour créer un nœud avec une interface hors bande depuis ce port. Pour une plus grande facilité d'utilisation, il est conseillé de nommer le nœud d'après la cible qui est connectée au port. Ceci signifie que vous allez entrer le même nom dans les champs **Nom du port** et **Nom de nœud**.
7. Cliquez sur le menu déroulant **Application d'accès** et sélectionnez dans la liste l'application à utiliser lors de la connexion au port concerné. Pour autoriser CC-SG à choisir automatiquement l'application correcte en fonction de votre navigateur, sélectionnez **Auto-Detect** (détection automatique).
8. Cliquez sur **OK** pour ajouter le port.

Configurer un port KVM

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez un dispositif KVM.

2. Choisissez **Dispositifs** > **Gestionnaire des ports** > **Configurer les ports**.
   - Cliquez sur un en-tête de colonne pour classer les ports par cet attribut dans l'ordre croissant. Cliquez de nouveau sur l'en-tête pour classer les ports dans l'ordre décroissant.
3. Cliquez sur le bouton **Configurer** qui correspond au port KVM à configurer.
4. Renseignez le champ **Nom du port**. Pour une plus grande facilité d'utilisation, il est conseillé de nommer le port d'après la cible qui lui est connectée. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
5. Renseignez le champ **Nom de nœud** pour créer un nœud avec une interface hors bande depuis ce port. Pour une plus grande facilité d'utilisation, il est conseillé de nommer le nœud d'après la cible qui est connectée au port. Ceci signifie que vous allez entrer le même nom dans les champs **Nom du port** et **Nom de nœud**.
6. Cliquez sur le menu déroulant **Application d'accès** et sélectionnez dans la liste l'application à utiliser lors de la connexion au port concerné. Pour autoriser CC-SG à choisir automatiquement l'application correcte en fonction de votre navigateur, sélectionnez **Auto-Detect** (détection automatique).
7. Cliquez sur **OK** pour ajouter le port.

Modification d'un port

Vous pouvez modifier des ports pour modifier le nom ou l'application d'accès.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le port à modifier.
2. Le cas échéant, modifiez la valeur du champ **Nom du port**.
3. Cliquez sur le menu déroulant **Application d'accès** et sélectionnez dans la liste l'application à utiliser lors de la connexion au port concerné. Pour autoriser CC-SG à choisir automatiquement l'application correcte en fonction de votre navigateur, sélectionnez **Auto-Detect** (détection automatique).
4. Cliquez sur **OK** pour enregistrer les modifications.

Suppression d'un port

La suppression d'un port entraîne le retrait de l'entrée correspondante d'un dispositif.

Important : si vous supprimez un port associé à un nœud, l'interface hors bande KVM ou série fournie par le port sera retirée du nœud. Si le nœud ne dispose d'aucune autre interface, il sera également retiré de CC-SG.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez supprimer les ports.
2. Choisissez **Dispositifs** > **Gestionnaire des ports** > **Supprimer des ports**.
3. Cochez le port à supprimer du dispositif.
4. Cliquez sur **OK** pour supprimer le port sélectionné. Un message apparaît lorsque le port a été supprimé.

Copie en bloc de catégories et d'éléments de dispositifs

La commande Copier en bloc permet de copier les catégories et les éléments affectés d'un dispositif vers plusieurs autres dispositifs. Notez que les catégories et les éléments sont les seules propriétés copiées lors de cette opération.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez un dispositif dans l'arborescence Dispositifs.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Copier en bloc**.
3. Dans la liste **Tous les dispositifs**, sélectionnez les dispositifs vers lesquels vous copiez les catégories et les éléments du dispositif indiqué dans le champ **Nom du dispositif**.
4. Cliquez sur le bouton **>** pour ajouter un dispositif à la liste **Dispositifs sélectionnés**.
5. Pour supprimer un dispositif de la liste **Dispositifs sélectionnés**, sélectionnez-le et cliquez sur le bouton **<**.
6. Cliquez sur **OK** pour copier en bloc. Un message apparaît lorsque les catégories et les éléments du dispositif ont été copiés.

Mise à niveau d'un dispositif

Vous pouvez mettre à niveau un dispositif lorsqu'une nouvelle version de firmware est disponible.

Important : consultez la matrice de compatibilité pour vous assurer que la nouvelle version du firmware du dispositif est compatible avec celle du firmware de CC-SG. Si vous devez mettre à niveau CC-SG et un périphérique ou groupes de périphériques, traitez CC-SG d'abord, puis le dispositif.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez un dispositif dans l'arborescence Dispositifs.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Mettre le dispositif à jour**.
3. **Nom du firmware** : sélectionnez le firmware approprié dans la liste. Raritan ou votre revendeur vous fournira cette information.
4. Cliquez sur **OK** pour mettre à niveau le dispositif.
   - La mise à niveau des dispositifs SX et KX prend environ 20 minutes.
   - Si la version de firmware du dispositif n'est pas compatible avec CC-SG, un message apparaît. Cliquez sur **Oui** pour mettre à niveau le dispositif. Cliquez sur **Non** pour annuler la mise à niveau.
5. Un message apparaît. Cliquez sur **Oui** pour redémarrer le dispositif. Un message apparaît lorsque le dispositif a été mis à niveau.
6. Pour garantir que votre navigateur charge tous les fichiers à niveau, fermez la fenêtre du navigateur, puis connectez-vous à CC-SG dans une nouvelle fenêtre.

Sauvegarde de la configuration du dispositif

Vous pouvez sauvegarder tous les fichiers de configuration utilisateur et système pour un dispositif donné. En cas d'incident sur le dispositif, vous pouvez restaurer les configurations précédentes depuis CC-SG à l'aide du fichier de sauvegarde créé. Chaque dispositif peut sauvegarder différents composants de la configuration. Reportez-vous au manuel d'utilisation du dispositif à sauvegarder pour plus d'informations.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif à sauvegarder.

2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Sauvegarder la configuration du dispositif**.
3. Renseignez le champ **Nom de la sauvegarde** pour identifier cette sauvegarde.
4. (Facultatif) Entrez une brève description de la sauvegarde dans le champ **Description**.
5. Cliquez sur **OK** pour sauvegarder la configuration du dispositif. Un message apparaît lorsque la configuration du dispositif a été sauvegardée.

Remarque : *lorsque vous sauvegardez un dispositif SX 3.0.1, les configurations des barrettes d'alimentation connectées ne sont pas sauvegardées. Si vous restaurez le dispositif SX 3.0.1 à partir de la sauvegarde, vous devez reconfigurer les barrettes d'alimentation.*

Restauration de la configuration du dispositif

A propos de la restauration des configurations de dispositifs

Les types de dispositifs suivants permettent la restauration d'une sauvegarde complète de leur configuration.

- KX
- KSX
- KX101
- SX
- IP-Reach

Les dispositifs KX2 vous permettent de choisir les composants d'une sauvegarde à restaurer.

- **Protégé** : la totalité du contenu du fichier de sauvegarde sélectionné, hormis les paramètres réseau (paquet personnalisé) est restaurée sur le dispositif.
- **Complet** : la totalité du contenu du fichier de sauvegarde sélectionné est restauré sur le dispositif.
- **Personnalisé** : vous permet de restaurer les paramètres du dispositif et/ou les paramètres d'utilisateur et de groupe d'utilisateurs.

Restaurer la configuration d'un dispositif (KX, KSX, KX101, SX, IP-Reach)

Vous pouvez restaurer une configuration de sauvegarde complète sur des dispositifs KX, KSX, KX101, SX et IP-Reach.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez restaurer une configuration de sauvegarde.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Configuration** > **Restaurer**.
3. Dans la table **Sauvegardes disponibles**, sélectionnez la configuration de sauvegarde à restaurer sur le dispositif.
4. Cliquez sur **OK**.
5. Cliquez sur **Oui** pour redémarrer le dispositif. Un message apparaît lorsque toutes les données ont été restaurées.

Restaurer toutes les données de configuration hormis les paramètres réseau sur un dispositif KX2

L'option de restauration Protégé vous permet de rétablir toutes les données de configuration, hormis les paramètres réseau, dans un fichier de sauvegarde sur un dispositif KX2.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez restaurer une configuration de sauvegarde.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Configuration** > **Restaurer**.
3. Dans la table **Sauvegardes disponibles**, sélectionnez la configuration de sauvegarde à restaurer sur le dispositif.
4. **Type de restauration** : sélectionnez **Protégé**.
5. Cliquez sur **OK**.
6. Cliquez sur **Oui** pour redémarrer le dispositif. Un message apparaît lorsque toutes les données de configuration utilisateur et système ont été restaurées.

Restaurer uniquement les paramètres de dispositif ou les données de l'utilisateur ou du groupe de l'utilisateur sur un dispositif KX2

L'option de restauration Personnalisé vous permet de rétablir les paramètres de dispositif et/ou les données de l'utilisateur ou du groupe de l'utilisateur.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez restaurer une configuration de sauvegarde.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Configuration** > **Restaurer**.
3. Dans la table **Sauvegardes disponibles**, sélectionnez la configuration de sauvegarde à restaurer sur le dispositif.
4. **Type de restauration** : sélectionnez **Personnalisé**.
5. **Restaurer les options** : sélectionnez les composants à restaurer sur le dispositif : Paramètres du dispositif, Données de l'utilisateur et du groupe de l'utilisateur
6. Cliquez sur **OK**.
7. Cliquez sur **Oui** pour redémarrer le dispositif. Un message apparaît lorsque les données ont été restaurées.

Restaurer toutes les données de configuration sur un dispositif KX2

L'option de restauration Complet vous permet de rétablir toutes les données de configuration dans un fichier de sauvegarde sur un dispositif KX2.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez restaurer une configuration de sauvegarde.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Configuration** > **Restaurer**.
3. Dans la table **Sauvegardes disponibles**, sélectionnez la configuration de sauvegarde à restaurer sur le dispositif.
4. **Type de restauration** : sélectionnez **Complet**.
5. Cliquez sur **OK**.
6. Cliquez sur **Oui** pour redémarrer le dispositif. Un message apparaît lorsque toutes les données de configuration utilisateur et système ont été restaurées.

Copie de la configuration du dispositif

Vous pouvez copier les configurations d'un dispositif à un autre ou plusieurs dispositifs

Remarque : *la copie de configurations n'est possible qu'entre unités Dominion SX possédant le même nombre de ports.*

1. Cliquez sur l'onglet Dispositifs et sélectionnez dans l'arborescence le dispositif dont vous souhaitez copier la configuration vers d'autres dispositifs.
2. Choisissez Dispositifs > Gestionnaire des configurations > Configuration > Copier la configuration.
3. Si vous avez utilisé l'option Sauvegarder la configuration sur le dispositif, vous pouvez copier la configuration en sélectionnant Depuis la configuration sauvegardée, puis en effectuant un choix dans le menu déroulant des configurations enregistrées.
4. Mettez en surbrillance les dispositifs vers lesquels vous souhaitez copier la configuration dans la colonne Dispositifs disponibles et cliquez sur la flèche droite pour les déplacer vers la colonne Copier la configuration dans. La flèche gauche permet de supprimer les dispositifs sélectionnés de la colonne Copier la configuration dans.
5. Cliquez sur OK pour copier la configuration vers les dispositifs de la colonne Copier la configuration dans.
6. Lorsque le message vous invitant à redémarrer le dispositif apparaît, cliquez sur Oui. Un message apparaît lorsque la configuration du dispositif a été copiée.

Redémarrage du dispositif

La fonction Redémarrer le dispositif permet de redémarrer un dispositif.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif à redémarrer.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Redémarrer le dispositif**.
3. Cliquez sur **OK** pour redémarrer le dispositif.
4. Cliquez sur Oui pour confirmer que tous les utilisateurs accédant au dispositif seront déconnectés.

Envoi d'une commande ping au dispositif

Cette commande permet de déterminer si un dispositif est disponible sur le réseau.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif devant recevoir la commande ping.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Envoyer une commande ping au dispositif**. L'écran **Envoyer une commande ping** au dispositif s'affiche et présente le résultat de la commande ping.

Suspension de la gestion

Vous pouvez suspendre un dispositif afin d'interrompre temporairement sa gestion par CC-SG sans perdre les données de configuration stockées dans CC-SG.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez suspendre la gestion par CC-SG.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Suspendre la gestion**. L'icône du dispositif dans l'arborescence indique son état suspendu.

Reprise de la gestion

Vous pouvez reprendre la gestion par CC-SG d'un dispositif suspendu pour qu'il repasse sous le contrôle de CC-SG.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif suspendu dans l'arborescence.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Reprendre la gestion**. L'icône du dispositif dans l'arborescence indique son état actif.

Gestionnaire d'alimentation des dispositifs

Le Gestionnaire d'alimentation des dispositifs permet d'afficher l'état d'un dispositif PowerStrip (notamment la tension, le courant et la température), et de gérer toutes les prises de celui-ci. Le Gestionnaire d'alimentation des dispositifs offre une vue des prises axée sur la barrette d'alimentation.

Avant d'utiliser le Gestionnaire, une connexion physique doit être établie entre la barrette d'alimentation et une unité Dominion SX ou KSX. Lorsque vous ajoutez la barrette d'alimentation, vous devez définir le dispositif Raritan fournissant la connexion. Elle sera ainsi associée au port série Dominion SX ou au port d'alimentation dédié Dominion KSX assurant sa gestion.

1. Dans l'onglet **Dispositifs**, sélectionnez un dispositif PowerStrip.
2. Choisissez **Dispositifs** > **Gestionnaire d'alimentation des dispositifs**.
3. Les prises sont répertoriées dans le panneau **Etat des prises**. Si vous ne parvenez pas à visualiser toutes les prises, faites défiler la liste.
   - Sélectionnez la case d'option **Actif** ou **Inactif** pour chaque prise afin de la mettre sous tension ou hors tension.
   - Cliquez sur **Réactiver** pour redémarrer le dispositif connecté à la prise.

Démarrage d'admin

Si elle est disponible, la commande **Démarrer Admin** vous permet d'accéder à l'interface administrateur du dispositif sélectionné.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez lancer l'interface administrateur.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Démarrer Admin**. L'interface administrateur du dispositif sélectionné apparaît.

Vue topologique

La commande Vue topologique permet d'afficher la configuration structurelle de tous les appareils connectés de votre configuration.

Tant que vous ne fermez pas la vue topologique, celle-ci remplace l'écran Profil du dispositif qui apparaît normalement lorsqu'un dispositif est sélectionné.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez afficher la vue topologique.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Vue topologique**. L'écran **Vue topologique** s'affiche pour le dispositif sélectionné.
   - Cliquez sur + ou sur – pour développer ou réduire la vue.

Déconnexion des utilisateurs

Les administrateurs peuvent mettre fin à la session de n'importe quel utilisateur sur un dispositif. Cela vaut pour les utilisateurs effectuant n'importe quel type d'opération sur un dispositif : connexion à des ports, sauvegarde de la configuration d'un dispositif, restauration de la configuration d'un dispositif ou mise à niveau du firmware d'un dispositif.

Les mises à niveau de firmware et les opérations de sauvegarde et de restauration de configuration peuvent aller à leur terme avant que la session de l'utilisateur sur le dispositif ne soit arrêtée. Il sera mis fin immédiatement à tous les autres types d'opération.

Vous pouvez fermer la session des utilisateurs directement connectés à un dispositif, ainsi que ceux qui sont connectés à ce dispositif par le biais de CC-SG (valable uniquement pour les dispositifs Dominion SX).

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif duquel vous souhaitez déconnecter un ou plusieurs utilisateurs.
2. Choisissez Dispositifs > Gestionnaire des dispositifs > Déconnecter utilisateurs.
3. Dans la table **Déconnecter les utilisateurs**, sélectionnez les utilisateurs dont vous souhaitez interrompre la session.
4. Cliquez sur **Déconnecter** pour les déconnecter du dispositif.

Accès spécial aux dispositifs du système Paragon II

Paragon II System Controller (P2-SC)

Les utilisateurs de dispositifs du système Paragon II peuvent ajouter leurs dispositifs P2-SC à l'arborescence des dispositifs CC-SG et les configurer par l'intermédiaire de l'application P2-SC Admin depuis CC-SG. Reportez-vous au **manuel d'utilisation de Paragon II System Controller** de Raritan pour plus d'informations sur l'utilisation de l'application P2-SC Admin.

Lorsque vous ajoutez le dispositif du système Paragon (le système Paragon comprend le dispositif P2-SC, les unités UMT connectées et les unités IP-Reach connectées) à CC-SG, celui-ci s'affiche dans l'arborescence des dispositifs.

➢ *Pour accéder à Paragon II System Controller :*

1. Cliquez sur l'onglet **Dispositifs**, puis sélectionnez le dispositif Paragon II System Controller.
2. Cliquez avec le bouton droit de la souris sur le dispositif Paragon II System Controller, puis cliquez sur **Démarrer Admin** pour lancer l'application Paragon II System Controller dans une nouvelle fenêtre de navigateur. Vous pouvez ensuite configurer les unités PII UMT.

Administration des unités IP-Reach et UST-IP

Vous pouvez également effectuer des diagnostics administratifs sur les dispositifs IP-Reach et UST-IP connectés à votre système Paragon directement depuis l'interface de CC-SG.

Lorsque vous ajoutez le dispositif du système Paragon dans CC-SG, celui-ci s'affiche dans l'arborescence des dispositifs.

➢ *Pour accéder à l'écran Admin de station utilisateur distante :*

1. Cliquez sur l'onglet **Dispositifs**, puis sélectionnez le dispositif **Paragon II System Controller**.
2. Avec le bouton droit de la souris, cliquez sur le dispositif **Paragon II System Controller** et sélectionnez **Admin de station utilisateur distante**. L'écran Admin de station utilisateur distante s'affiche, dressant la liste de toutes les unités IP-Reach et UST-IP connectées.

3. En regard de la ligne correspondant au dispositif avec lequel vous souhaitez travailler, cliquez sur le bouton **Démarrer Admin** pour activer Raritan Remote Console et afficher l'écran bleu de configuration du dispositif dans une nouvelle fenêtre.

Gestionnaire des groupes de dispositifs

Le Gestionnaire des groupes de dispositifs permet d'ajouter, de modifier et de supprimer des groupes de dispositifs. Lorsque vous ajoutez un nouveau groupe de dispositifs, vous pouvez lui créer une stratégie d'accès total. Reportez-vous à ***Stratégies de contrôle d'accès*** (à la page 102) pour plus d'informations.

Ajouter un groupe de dispositifs

1. Choisissez **Associations** > **Groupes de dispositifs**. La fenêtre Gestionnaire des groupes de dispositifs s'affiche. Les groupes de dispositifs existants apparaissent dans le panneau de gauche.
2. Cliquez sur l'icône Nouveau groupe dans la barre d'outils. Le panneau **Groupe de dispositifs : Nouveau** s'affiche.
3. Dans le champ **Nom du groupe**, entrez le nom du groupe de dispositifs à créer. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
4. Vous pouvez ajouter des dispositifs à un groupe de deux façons : **Sélectionner les dispositifs** et **Décrire les dispositifs**. L'onglet Sélectionner les dispositifs vous permet de choisir dans la liste des dispositifs disponibles ceux que vous souhaitez affecter au groupe. L'onglet Décrire les dispositifs vous permet de spécifier des règles décrivant les dispositifs ; les dispositifs dont les paramètres respectent ces règles seront ajoutés au groupe.

➢ *Sélectionner les dispositifs*

a. Cliquez sur l'onglet Sélectionner les dispositifs.

b. Dans la liste **Disponible**, sélectionnez le dispositif à inclure au groupe, puis cliquez sur **Ajouter** pour le déplacer vers la liste **Sélectionné**. Les dispositifs de la liste **Sélectionné** seront ajoutés au groupe.

- Pour supprimer un dispositif du groupe, sélectionnez son nom dans la liste **Sélectionné**, puis cliquez sur **Retirer**.

- Vous pouvez rechercher un dispositif dans la liste **Disponible** ou dans la liste **Sélectionné**. Entrez les termes de la recherche dans le champ sous la liste, puis cliquez sur **Aller à**.

➢ *Décrire les dispositifs*

a. Cliquez sur l'onglet **Décrire les dispositifs** dans le panneau **Groupe de dispositifs : Nouveau**. Dans l'onglet Décrire les dispositifs, vous créez une table de règles décrivant les dispositifs à affecter au groupe.

b. Cliquez sur l'icône Ajouter une nouvelle ligne pour ajouter une rangée à la table.

c. Double-cliquez sur la cellule créée pour chaque colonne afin d'activer un menu déroulant. Dans chaque liste, sélectionnez les composants de règle à utiliser.

1. **Préfixe** – laissez cette option vide ou sélectionnez **NOT**. Dans ce cas, la règle recherchera des valeurs en opposition au reste de l'expression.
2. **Catégorie** – sélectionnez un attribut à évaluer dans la règle. Toutes les catégories que vous avez créées dans le **Gestionnaire des associations** seront disponibles ici.
3. **Opérateur** – sélectionnez une opération de comparaison à effectuer entre la catégorie et les éléments. Trois opérateurs sont disponibles : **=** (est égal à), **LIKE** (utilisé pour trouver l'élément dans un nom) et **<>** (est différent de).
4. **Elément** – sélectionnez une valeur à comparer à l'attribut de catégorie. Seuls les éléments associés à la catégorie sélectionnée seront affichés ici (par exemple, si l'évaluation porte sur une catégorie Service, les éléments Emplacement n'apparaîtront pas ici).
5. **Nom de la règle** – il s'agit d'un nom affecté à la règle de cette ligne. Il n'est pas modifiable, il est utilisé pour écrire des descriptions dans le champ **Expression abrégée**.
6. Pour ajouter une autre règle, cliquez sur **Ajouter une nouvelle ligne**, puis effectuez les configurations nécessaires. La configuration de plusieurs règles permettra des descriptions plus précises en fournissant des critères multiples d'évaluation des dispositifs.

7. La table de règles ne présente que des critères d'évaluation des nœuds. Pour écrire la description du groupe de dispositifs, ajoutez les règles par **nom de règle** dans le champ **Expression abrégée**. Si la description ne requiert qu'une seule règle, il vous suffit d'entrer le nom de cette dernière dans le champ. Si plusieurs règles sont évaluées, entrez-les dans le champ à l'aide d'opérateurs logiques décrivant les règles les unes par rapport aux autres :

   & - opérateur AND. Un nœud doit satisfaire aux règles des deux côtés de cet opérateur pour que la description (ou la section d'une description) soit vérifiée.

   | - opérateur OR. Un dispositif ne doit satisfaire qu'une des règles de chaque côté de cet opérateur pour que la description (ou la section d'une description) soit vérifiée.

   (et **)** - opérateurs de regroupement. Ceci décompose la description en sous-section contenue entre les parenthèses. La section entre parenthèses est évaluée avant que le reste de la description ne soit comparé au nœud. Les groupes entre parenthèses peuvent être imbriqués dans un autre groupe entre parenthèses.

   Exemple 1 : si vous souhaitez décrire les dispositifs appartenant au service technique, créez une règle indiquant Service = Technique. Elle deviendra Rule0. Entrez ensuite Rule0 dans le champ **Expression abrégée**.

   Exemple 2 : vous souhaitez décrire un groupe de dispositifs appartenant au service technique, ou situés à Philadelphie, et indiquer que toutes les machines doivent disposer d'un Go de mémoire ; vous devez donc créer trois règles. Service = Technique (Rule0) Emplacement = Philadelphie (Rule1) Mémoire = 1Go (Rule2). Ces règles doivent être organisées les unes par rapport aux autres. Puisque le dispositif peut appartenir au service technique ou être situé à Philadelphie, utilisez l'opérateur OR, |, pour joindre les deux : Rule0|Rule1. Cette comparaison est placée entre parenthèses pour être effectuée en premier : (Rule0|Rule1). Enfin, puisque les dispositifs doivent satisfaire cette comparaison ET disposer d'un Go de mémoire, nous utilisons le connecteur AND, **&**, pour joindre cette section à Rule2 : (Rule0|Rule1)&Rule2. Entrez cette expression finale dans le champ **Expression abrégée**.

- Pour supprimer une ligne de la table, sélectionnez cette ligne, puis cliquez sur l'icône Supprimer la ligne sélectionnée .
- Pour afficher la liste des dispositifs dont les paramètres suivent les règles définies, cliquez sur **Affichage des dispositifs**.
  a. Cliquez sur **Valider** si une description a été écrite dans le champ **Expression abrégée**. Si la description est formée de manière incorrecte, vous recevez un message d'avertissement. Si la description est correctement formée, une forme normalisée de l'expression apparaît dans le champ **Expression normalisée**.
  b. Cliquez sur **Affichage des dispositifs** pour visualiser les nœuds satisfaisant l'expression. Une fenêtre **Dispositifs du groupe de dispositifs Résultats** apparaît présentant les dispositifs groupés par l'expression en cours. Vous pouvez ainsi vérifier si la description est écrite correctement. Dans le cas contraire, vous pouvez retourner à la table des règles ou au champ **Expression abrégée** pour effectuer des modifications.
  c. Cochez la case **Créer une stratégie d'accès total pour le groupe** si vous souhaitez définir, pour ce groupe de dispositifs, une stratégie autorisant l'accès permanent à tous les dispositifs du groupe avec permission de contrôle.
  d. (Facultatif) Si vous souhaitez ajouter un autre groupe de dispositifs, cliquez sur **Appliquer** pour enregistrer le groupe en cours, puis répétez les étapes de cette section pour ajouter des groupes de dispositifs supplémentaires. Une fois l'ajout des groupes de dispositifs terminé, cliquez sur **OK** pour enregistrer vos modifications.

Modifier un groupe de dispositifs

1. Choisissez **Associations** > **Groupes de dispositifs**. La fenêtre Gestionnaire des groupes de dispositifs s'affiche.
2. Les groupes de dispositifs existants apparaissent dans le panneau de gauche. Sélectionnez le groupe de dispositifs à renommer. Le panneau des détails du groupe de dispositifs s'affiche.
3. (Facultatif) Entrez le nouveau nom du groupe de dispositifs dans le champ **Nom du groupe**.
4. La modification des dispositifs inclus dans le groupe s'effectue à l'aide des onglets Sélectionner les dispositifs ou Décrire les dispositifs. Reportez-vous à **Ajouter un groupe de dispositifs** (à la page 51) pour plus d'informations.
5. Cliquez sur **OK** pour enregistrer les modifications.

Supprimer un groupe de dispositifs

1. Choisissez **Associations** > **Groupes de dispositifs**. La fenêtre Gestionnaire des groupes de dispositifs s'affiche.
2. Les groupes de dispositifs existants apparaissent dans le panneau de gauche. Sélectionnez le groupe de dispositifs à supprimer. Le panneau des détails du groupe de dispositifs s'affiche.
3. Choisissez **Groupes** > **Supprimer**.
4. Le panneau Supprimer le groupe de dispositifs s'affiche. Cliquez sur **Supprimer**.
5. Cliquez sur **Oui** dans le message de confirmation qui s'affiche.

Chapitre 7 Barrettes d'alimentation gérées

Dans CC-SG, les barrettes d'alimentation doivent être connectées à un des dispositifs suivants :

- Dominion KX
- Dominion KX2
- Dominion SX 3.0
- Dominion SX 3.1
- Dominion KSX
- Paragon II System Controller (P2SC)

Pour configurer des barrettes d'alimentation dans CC-SG, vous devez savoir à quel dispositif Raritan elles sont physiquement connectées.

Dans ce chapitre

Processus de configuration de la gestion de l'alimentation dans CC-SG.56
Configuration des barrettes d'alimentation connectées à des dispositifs KX, KX2 et P2SC 57
Configuration des barrettes d'alimentation connectées à des dispositifs SX 3.0 et KSX.....58
Configuration des barrettes d'alimentation connectées à un dispositif SX 3.1 61
Configuration des prises d'une barrette d'alimentation.....63

Processus de configuration de la gestion de l'alimentation dans CC-SG

1. Réalisez tous les branchements physiques entre le dispositif, la barrette d'alimentation et les nœuds alimentés par celle-ci. Reportez-vous aux guides de configuration rapide de RPC et Dominion PX, et au guide de déploiement CC-SG pour plus d'informations sur les connexions physiques entre barrettes d'alimentation, dispositifs et nœuds.
2. Ajoutez le dispositif de gestion à CC-SG. La procédure varie pour les différents dispositifs Raritan. Reportez-vous à la section correspondant au dispositif auquel la barrette d'alimentation est connectée :
   - ***Configuration des barrettes d'alimentation connectées à des dispositifs KX, KX2 et P2SC*** (à la page 57)

- ***Configuration des barrettes d'alimentation connectées à des dispositifs SX 3.0 et KSX*** (à la page 58)
- ***Configuration des barrettes d'alimentation connectées à un dispositif SX 3.1*** (à la page 61).

3. ***Configurez des prises*** (voir "Configuration des prises d'une barrette d'alimentation" à la page 63).
4. Associez chaque prise au nœud qu'elle alimente : ***Ajouter une interface de barrettes d'alimentation gérées au nœud*** (voir "Interfaces pour connexions par barrette d'alimentation gérée" à la page 72)

Configuration des barrettes d'alimentation connectées à des dispositifs KX, KX2 et P2SC

CC-SG détecte automatiquement les barrettes d'alimentation connectées à des dispositifs KX et KX2. Vous pouvez effectuer les tâches suivantes dans CC-SG pour configurer et gérer des barrettes d'alimentation connectées à des dispositifs KX et KX2.

- Ajouter un dispositif PowerStrip connecté à un dispositif KX ou KX2
- Déplacer une barrette de KX ou KX2 vers un port différent
- Supprimer une barrette d'alimentation connectée à un dispositif KX ou KX2

Ajouter un dispositif PowerStrip connecté à un dispositif KX, KX2 ou P2SC

Lorsque vous ajoutez à CC-SG un dispositif KX ou KX2 connecté à une barrette d'alimentation, celle-ci est ajoutée automatiquement. Elle apparaît dans l'onglet Dispositifs, sous le dispositif KX ou KX2 auquel elle est connectée.

Etapes suivantes :

1. ***Configurez des prises*** (voir "Configuration des prises d'une barrette d'alimentation" à la page 63).
2. Associez chaque prise au nœud qu'elle alimente : ***Ajouter une interface de barrettes d'alimentation gérées au nœud*** (voir "Interfaces pour connexions par barrette d'alimentation gérée" à la page 72)

Déplacer une barrette de KX, KX2 ou P2SC vers un port différent

Lorsque vous déplacez physiquement une barrette d'alimentation d'un dispositif ou port KX, KX2 ou P2SC à un autre, CC-SG la détecte automatiquement et met à jour son association au dispositif correct. Vous n'avez pas à ajouter la barrette d'alimentation à CC-SG séparément.

Remarque : *lorsque vous retirez physiquement une barrette d'alimentation d'un port P2SC sans la connecter à un autre, CC-SG ne la supprime pas du port précédent. Vous devez effectuer une réinitialisation de base de données partielle ou complète de l'unité UMT à laquelle la barrette d'alimentation est connectée pour retirer celle-ci de l'onglet Dispositifs. Reportez-vous au guide Raritan*

Supprimer une barrette d'alimentation connectée à un dispositif KX, KX2 ou P2SC

Vous ne pouvez pas supprimer une barrette d'alimentation connectée à un dispositif KX ou KX2 de CC-SG. Vous devez déconnecter physiquement la barrette d'alimentation du dispositif KX ou KX2 pour la supprimer de CC-SG. La barrette d'alimentation et toutes les prises configurées disparaissent alors de l'onglet Dispositifs.

Configuration des barrettes d'alimentation connectées à des dispositifs SX 3.0 et KSX

Vous pouvez effectuer les tâches suivantes dans CC-SG pour configurer et gérer des barrettes d'alimentation connectées à des dispositifs SX 3.0 ou KSX.

Remarque : *les barrettes d'alimentation doivent être physiquement connectées au port d'alimentation d'un dispositif KSX.*

- Ajouter une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX
- Supprimer une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX
- Modifier une association de dispositif ou de port d'une barrette d'alimentation (SX 3.0, KSX)

Ajouter une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX

1. ***Ajoutez le dispositif SX 3.0 ou KSX à CC-SG*** (voir "Ajouter un dispositif KVM ou série" à la page 35).
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Ajouter un dispositif**.
3. Sélectionnez **PowerStrip** dans le menu déroulant **Type de dispositif**.
4. Renseignez le champ **Nom de la barrette d'alimentation**. Maintenez le curseur au-dessus du champ pour voir le nombre de caractères autorisé dans le nom. Les espaces sont interdits.
5. Cliquez sur le menu déroulant **Nombre de prises**, puis sélectionnez le nombre de prises dont est dotée la barrette d'alimentation.
6. Cliquez sur le menu déroulant **Dispositif de gestion**, puis sélectionnez le dispositif SX 3.0 ou KSX connecté à la barrette d'alimentation.
7. Cliquez sur le menu déroulant **Port de gestion**, puis sélectionnez dans la liste le port du dispositif SX 3.0 ou KSX auquel la barrette d'alimentation est connectée.
8. (Facultatif) Entrez une brève description de cette barrette d'alimentation dans le champ **Description**.
9. (Facultatif) Cochez la case **Configurer toutes les prises** pour ajouter automatiquement chaque prise de la barrette d'alimentation à l'onglet **Dispositifs**. Si vous ne configurez pas toutes les prises immédiatement, vous pouvez ***les configurer ultérieurement*** (voir "Configuration des prises d'une barrette d'alimentation" à la page 63).
10. (Facultatif) Pour chaque **catégorie** listée, cliquez sur le menu déroulant **Elément**, puis sélectionnez l'élément que vous souhaitez appliquer au dispositif correspondant. Sélectionnez l'élément vide du champ **Elément** lorsque vous ne souhaitez pas utiliser une catégorie. Reportez-vous à ***Associations*** (voir "Associations, catégories et éléments" à la page 24) pour plus d'informations.
11. Lorsque la configuration de la barrette d'alimentation est terminée, cliquez sur **Appliquer** pour l'ajouter et ouvrir un nouvel écran Ajouter un dispositif vide afin de poursuivre l'ajout des dispositifs. Ou, cliquez sur **OK** pour ajouter la barrette d'alimentation sans afficher un nouvel écran Ajouter un dispositif.

Etapes suivantes :

1. ***Configurez des prises*** (voir "Configuration des prises d'une barrette d'alimentation" à la page 63).
2. Associez chaque prise au nœud qu'elle alimente : ***Ajouter une interface de barrettes d'alimentation gérées au nœud*** (voir "Interfaces pour connexions par barrette d'alimentation gérée" à la page 72)

Supprimer une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX

Vous pouvez supprimer une barrette d'alimentation connectée à un dispositif SX 3.0, KSX ou P2SC même si elle est toujours physiquement présente. Si vous déconnectez la barrette d'alimentation du dispositif SX 3.0, KSX ou P2SC auquel elle est associée, elle apparaît toujours sous celui-ci dans l'onglet Dispositifs. Pour la retirer de l'affichage, vous devez la supprimer.

1. Sous l'onglet Dispositifs, sélectionnez la barrette d'alimentation à supprimer.
2. Choisissez Dispositifs > Gestionnaire des dispositifs >Supprimer un dispositif.
3. Cliquez sur OK pour supprimer la barrette d'alimentation. Un message apparaît lorsque la barrette d'alimentation a été supprimée. L'icône de la barrette d'alimentation est retirée de l'onglet Dispositifs.

Modifier une association de dispositif ou de port d'une barrette d'alimentation (SX 3.0, KSX)

Si une barrette d'alimentation est physiquement déplacée d'un dispositif ou port SX 3.0 ou KSX à un autre, vous devez modifier l'association dans son profil dans CC-SG.

1. Dans l'onglet Dispositifs, sélectionnez la barrette d'alimentation déplacée d'un dispositif ou port SX 3.0 ou KSX à un autre.
2. Cliquez sur le menu déroulant **Dispositif de gestion**, puis sélectionnez le dispositif SX 3.0 ou KSX connecté à la barrette d'alimentation.
3. Cliquez sur le menu déroulant **Port de gestion**, puis sélectionnez dans la liste le port du dispositif SX 3.0 ou KSX auquel la barrette d'alimentation est connectée.
4. Cliquez sur **OK**.

Configuration des barrettes d'alimentation connectées à un dispositif SX 3.1

Vous pouvez effectuer les tâches suivantes dans CC-SG pour configurer et gérer des barrettes d'alimentation connectées à des dispositifs SX 3.1.

- Ajouter un dispositif PowerStrip connecté à un dispositif SX 3.1
- Déplacer la barrette d'alimentation d'un dispositif SX 3.1 vers un port différent
- Supprimer une barrette d'alimentation connectée à un dispositif SX 3.1

Ajouter un dispositif PowerStrip connecté à un dispositif SX 3.1

La procédure d'ajout d'une barrette d'alimentation connectée à un dispositif SX 3.1 varie si celui-ci a été ajouté à CC-SG ou non.

Si la barrette d'alimentation est connectée au dispositif SX 3.1 et que celui-ci n'a pas encore été ajouté à CC-SG :

1. ***Ajoutez le dispositif SX 3.1 à CC-SG*** (voir "Ajouter un dispositif KVM ou série" à la page 35).
2. CC-SG détecte la barrette d'alimentation et l'ajoute automatiquement. Elle apparaît dans l'onglet Dispositifs, sous le dispositif SX 3.1 auquel elle est connectée.

Si le dispositif SX 3.1 a déjà été ajouté à CC-SG et que la barrette d'alimentation est connectée ultérieurement au dispositif SX 3.1 :

1. ***Ajoutez le dispositif SX 3.1 à CC-SG*** (voir "Ajouter un dispositif KVM ou série" à la page 35).
2. ***Configurer les ports du dispositif SX 3.1*** (voir "Configuration des ports" à la page 39).
3. Dans l'onglet **Dispositifs**, sélectionnez le dispositif SX 3.1 auquel la barrette d'alimentation est connectée.
4. Cliquez sur le + en regard de l'icône du dispositif pour développer la liste des ports.
5. Avec le bouton droit, cliquez sur le port SX 3.1 auquel la barrette d'alimentation est connectée et sélectionnez Ajouter une barrette d'alimentation dans le menu contextuel.

6. Entrez le nombre de prises dont est dotée la barrette d'alimentation, puis cliquez sur **OK**.

Etapes suivantes :

1. ***Configurez des prises*** (voir "Configuration des prises d'une barrette d'alimentation" à la page 63).
2. Associez chaque prise au nœud qu'elle alimente : ***Ajouter une interface de barrettes d'alimentation gérées au nœud*** (voir "Interfaces pour connexions par barrette d'alimentation gérée" à la page 72)

Déplacer la barrette d'alimentation d'un dispositif SX 3.1 vers un port différent

Lorsque vous déplacez physiquement une barrette d'alimentation d'un dispositif ou port SX 3.1 à un autre, vous devez ***supprimer la barrette d'alimentation de l'ancien port SX 3.1*** (voir "Supprimer une barrette d'alimentation connectée à un dispositif SX 3.1" à la page 62) et ***l'ajouter au nouveau port SX 3.1*** (voir "Ajouter un dispositif PowerStrip connecté à un dispositif SX 3.1" à la page 61).

Supprimer une barrette d'alimentation connectée à un dispositif SX 3.1

Vous pouvez supprimer une barrette d'alimentation connectée à un dispositif SX 3.1 même si elle est toujours physiquement présente. Si vous déconnectez la barrette d'alimentation du dispositif SX 3.1 auquel elle est associée, elle apparaît toujours sous celui-ci dans l'onglet Dispositifs. Pour la retirer de l'affichage, vous devez la supprimer.

1. Sous l'onglet **Dispositifs**, sélectionnez la barrette d'alimentation à supprimer.
2. Choisissez **Dispositifs** > **Gestionnaire des dispositifs** > **Supprimer un dispositif**.
3. Cliquez sur **OK** pour supprimer la barrette d'alimentation. Un message apparaît lorsque la barrette d'alimentation a été supprimée. L'icône de la barrette d'alimentation est retirée de l'onglet Dispositifs.

Configuration des prises d'une barrette d'alimentation

Vous devez configurer les prises d'une barrette d'alimentation avant d'associer chaque prise à un nœud par l'***ajout d'une interface de barrettes d'alimentation gérée au nœud*** (voir "Interfaces pour connexions par barrette d'alimentation gérée" à la page 72).

➢ *Pour configurer des prises dans le profil d'une barrette d'alimentation :*

1. Dans l'onglet **Dispositifs**, cliquez sur le + en regard du dispositif connecté à la barrette d'alimentation pour développer tous les ports.
2. Sélectionnez la barrette d'alimentation dont vous souhaitez configurer les prises.
3. Dans l'écran Profil du dispositif : PowerStrip, sélectionnez l'onglet **Outlets** (prises).
4. Cochez la case de chaque prise à configurer, puis cliquez sur **OK**.

Les prises sont affichées sous l'icône Barrette d'alimentation dans l'onglet **Dispositifs**.

➢ *Pour configurer les prises dans l'écran Configurer les ports :*

1. Dans l'onglet **Dispositifs**, cliquez sur le + en regard du dispositif connecté à la barrette d'alimentation pour développer tous les ports.
2. Sélectionnez la barrette d'alimentation dont vous souhaitez configurer les prises.
3. Choisissez **Dispositifs** > **Gestionnaire des ports** > **Configurer les ports**.
   - Pour configurer plusieurs prises avec les noms par défaut affichés à l'écran, cochez la case de chaque prise à configurer, puis cliquez sur **OK** pour valider.
   - Pour configurer chaque prise séparément, cliquez sur le bouton **Configurer** en regard, puis entrez le nom de la prise dans le champ **Nom du port**. Cliquez sur **OK** pour configurer le port.

➢ *Pour supprimer une prise :*

1. Dans l'onglet **Dispositifs**, cliquez sur le + en regard du dispositif connecté à la barrette d'alimentation pour développer tous les ports.

2. Cliquez sur + en regard de la barrette d'alimentation pour développer toutes les prises.
3. Choisissez **Dispositifs** > **Gestionnaire des ports**, **Supprimer des ports**.
4. Cochez la case de chaque prise à supprimer, puis cliquez sur **OK**.

Chapitre 8 Nœuds, groupes de nœuds et interfaces

Cette section explique comment visualiser, configurer et modifier des nœuds et les interfaces associées, et comment créer des groupes de nœuds. La connexion aux nœuds est présentée brièvement. Reportez-vous au **manuel d'utilisation de CommandCenter Secure Gateway** pour plus d'informations sur la connexion aux nœuds.

Dans ce chapitre

Affichage des nœuds 65
Vue d'ensemble des nœuds et des interfaces 67
Ajout d'un nœud 68
Nœuds créés par configuration de ports 69
Ajout d'une interface 69
Résultats de l'ajout d'une interface 76
Modification d'une interface 76
Suppression d'une interface 77
Ajouter une interface aux signets 77
Modification d'un nœud 78
Suppression d'un nœud 79
Copie en bloc de catégories et d'éléments de nœuds 79
Connexion à un nœud 80
Envoi d'une commande ping à un nœud 80
Conversation 80
A propos des groupes de nœuds 82
Ajout d'un groupe de nœuds 83
Modification d'un groupe de nœuds 86
Suppression d'un groupe de nœuds 87

Affichage des nœuds

Dans CC-SG, vous pouvez afficher tous les nœuds dans l'onglet Nœuds et sélectionner un nœud pour visualiser son profil.

Onglet Nœuds

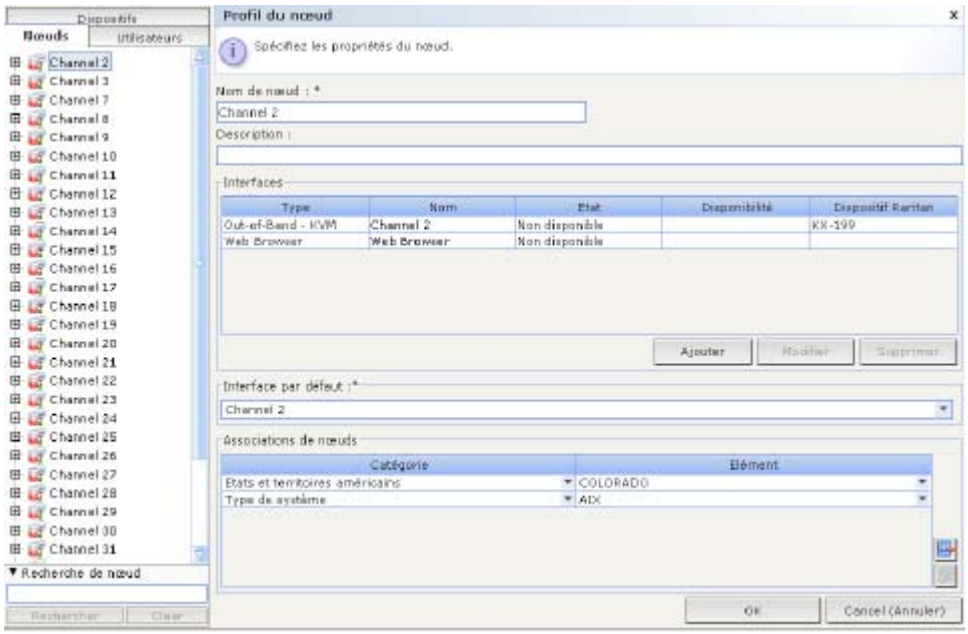
Lorsque vous cliquez sur l'onglet Nœuds, tous les nœuds auxquels vous avez accès apparaissent dans une arborescence.

Les nœuds sont classés par ordre alphabétique, en fonction de leur nom, ou regroupés selon leur disponibilité. Les nœuds triés par état sont classés par ordre alphabétique au sein des groupes de disponibilité. Pour passer d'une méthode de tri à l'autre, cliquez avec le bouton droit de la souris dans l'arborescence, cliquez sur **Options de tri du nœud**, puis sur **Par nom de nœud** ou **Par état de nœud**.

Reportez-vous à ***Vues personnalisées*** (voir "Vues personnalisées pour dispositifs et nœuds" à la page 111) pour plus d'informations sur l'affichage de l'onglet Nœuds en divers modes.

Profil du nœud

Cliquez sur un nœud dans l'onglet pour ouvrir l'écran **Profil du nœud**, qui inclut des informations sur le nœud, ses interfaces, l'interface par défaut, et les catégories et éléments qui lui sont affectés. Les nœuds prenant en charge le support virtuel comportent une colonne supplémentaire indiquant si l'option Support virtuel est activée.



Raritan.
When you're ready to take control®

Icônes associées aux nœuds et aux interfaces

Afin de faciliter leur identification, les nœuds sont associés à différentes icônes dans l'arborescence. Placez le pointeur de la souris au-dessus d'une icône dans l'arborescence Nœuds pour afficher une info-bulle contenant des informations sur le nœud.

Icône	Signification
	Nœud disponible : au moins une des interfaces du nœud est **active**.
	Nœud non disponible : aucune interface du nœud n'est **active**.

Vue d'ensemble des nœuds et des interfaces

A propos des nœuds

Chaque nœud représente une cible accessible via CC-SG, par des méthodes En bande (adresse IP directe) ou hors bande (connexion à un dispositif Raritan). Par exemple, un nœud peut être un serveur dans un rack connecté à un dispositif KVM sur IP Raritan, un serveur doté d'une carte HP iLO, un PC du réseau exécutant VNC, ou un élément d'une infrastructure réseau avec une connexion de gestion série à distance.

Vous pouvez ajouter manuellement des nœuds à CC-SG après avoir ajouté les dispositifs auxquels ils sont connectés. Toutefois, les nœuds peuvent également être créés automatiquement, en cochant la case **Configurer tous les ports** dans l'écran Ajouter un dispositif lorsque vous ajoutez un dispositif. Cette option permet à CC-SG d'ajouter automatiquement tous les ports du dispositif, et d'inclure un nœud et une interface KVM hors bande ou série pour chaque port. Vous pouvez toujours modifier ces nœuds, ports et interfaces ultérieurement.

Noms des nœuds

Le nom d'un nœud doit être unique. CC-SG vous présentera quelques options si vous tentez d'ajouter manuellement un nœud en lui donnant un nom existant. Lorsque CC-SG ajoute des nœuds automatiquement, un système de numérotation permet de garantir que les noms sont uniques.

Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.

A propos des interfaces

Dans CC-SG, l'accès aux nœuds s'effectue via des interfaces. Vous devez ajouter au moins une interface à chaque nouveau nœud. Vous pouvez ajouter différents types d'interfaces à un nœud pour offrir diverses méthodes d'accès, telles que KVM, série ou gestion d'alimentation hors bande, ou SSH/RDP/VNC ou DRAC/RSA/ILO en bande, selon le type du nœud.

Un nœud peut être doté de plusieurs interfaces. Il ne peut disposer que d'une interface série ou KVM hors bande. Par exemple, un serveur Windows peut disposer d'une interface KVM hors bande via ses ports clavier, souris et écran, et d'une interface d'alimentation pour gérer la prise à laquelle il est connecté.

Ajout d'un nœud

➢ *Pour ajouter un nœud à CC-SG :*

1. Cliquez sur l'onglet **Nœuds**.
2. Choisissez Nœuds > **Ajouter un nœud**.
3. Renseignez le champ **Nom de nœud**. Les noms de nœud dans CC-SG doivent tous être uniques. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
4. (Facultatif) Entrez une brève description de ce nœud dans le champ **Description**.
5. Vous devez configurer au moins une interface. Cliquez sur **Ajouter** dans la zone **Interfaces** de l'écran Ajouter un nœud pour définir une interface. Reportez-vous à ***Ajout d'une interface*** (à la page 69) pour plus d'informations.
6. (Facultatif) Une liste de **catégories** et d'**éléments** peut être configurée pour décrire et organiser le nœud de façon optimale. Reportez-vous à ***Associations*** (voir "Associations, catégories et éléments" à la page 24) pour plus d'informations.
   - Pour chaque **catégorie** listée, cliquez sur le menu déroulant **Elément**, puis sélectionnez l'élément que vous souhaitez appliquer au nœud correspondant.
   - Sélectionnez l'élément vide du champ **Elément** lorsque vous ne souhaitez pas utiliser une catégorie.

- Si les valeurs **Catégorie** ou **Elément** que vous souhaitez utiliser n'apparaissent pas, vous pouvez en ajouter via le menu **Associations**. Reportez-vous à ***Associations*** (voir "Associations, catégories et éléments" à la page 24) pour plus d'informations.

7. Cliquez sur **OK** pour enregistrer les modifications. Le nœud sera ajouté à la liste.

Nœuds créés par configuration de ports

Lorsque vous configurez les ports d'un dispositif, un nœud est automatiquement créé pour chaque port. Une interface est également créée pour chaque nœud.

Lorsqu'un nœud est automatiquement créé, il reçoit le nom du port auquel il est associé. S'il existe déjà un nœud de ce nom, une extension est ajoutée au nom ; par exemple, Channel1(1). L'extension est le nombre entre parenthèses. Elle n'est pas incluse dans le décompte des caractères du nom du nœud. Si vous modifiez le nom du nœud, le nouveau nom sera limité au nombre maximum de caractères. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations.

Ajout d'une interface

1. Pour un nœud existant : cliquez sur l'onglet **Nœuds**, puis sélectionnez le nœud auquel vous souhaitez ajouter une interface. Dans l'écran **Profil du nœud** qui apparaît, cliquez sur **Ajouter** dans la section **Interfaces**.

   Si vous ajoutez un nouveau nœud : cliquez sur **Ajouter** dans la section **Interfaces** de l'écran **Ajouter un nœud**.

   La fenêtre **Ajouter une interface** s'affiche.

2. Cliquez sur le menu déroulant **Type d'interface** et sélectionnez le type de la connexion au nœud :

   Connexions en bande (voir "Interfaces de connexions en bande" à la page 71)

   - **KVM DRAC en bande** : sélectionnez cette option pour créer une connexion KVM à un serveur Dell DRAC via l'interface DRAC. Vous devrez ensuite configurer une interface d'alimentation DRAC.
   - **KVM processeur iLO en bande** : sélectionnez cette option pour créer une connexion KVM à un serveur HP via une interface iLO ou RILOE.

- **RDP en bande** : sélectionnez cette option pour créer une connexion KVM à un nœud à l'aide du protocole RDP (par exemple, la connexion Bureau à distance d'un serveur Windows).
- **KVM RSA en bande** : sélectionnez cette option pour créer une connexion KVM à un serveur IBM RSA via son interface RSA. Vous devrez ensuite configurer une interface d'alimentation RSA.
- **SSH en bande** : sélectionnez cette option pour créer une connexion SSH à un nœud.
- **VNC en bande** : sélectionnez cette option pour créer une connexion KVM à un nœud via le logiciel de serveur VNC.

Connexions hors bande (voir "Interfaces pour connexions KVM hors bande, série hors bande" à la page 71)

- **KVM hors bande** : sélectionnez cette option pour créer une connexion KVM à un nœud via un dispositif KVM Raritan (KX, KX101, KSX, IP-Reach, Paragon II).
- **Série hors bande** : sélectionnez cette option pour créer une connexion série à un nœud via un dispositif série Raritan (SX, KSX).

Connexions de gestion d'alimentation (voir "Interfaces pour connexions de gestion de l'alimentation par processeur DRAC, RSA et ILO" à la page 72)

- **Gestion de l'alimentation - DRAC** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un serveur Dell DRAC.
- **Gestion de l'alimentation - Processeur iLO** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un serveur iLO/RILOE HP.
- **Gestion de l'alimentation - IPMI** (voir "Interfaces pour connexions de gestion d'alimentation IPMI" à la page 73) : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un nœud via une connexion IPMI.
- **Gestion de l'alimentation - RSA** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un serveur RSA.

Connexions par barrettes d'alimentation gérées (voir "Interfaces pour connexions par barrette d'alimentation gérée" à la page 72)

- **Barrette d'alimentation gérée** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un nœud alimenté via une barrette Raritan, telle que Dominion PX.

Connexions par navigateur Web (voir "Interface Navigateur Web" à la page 74)

- **Navigateur Web** : sélectionnez cette option pour créer une connexion à un dispositif intégrant un serveur Web.

3. Un nom par défaut apparaît dans le champ **Nom** en fonction du type d'interface sélectionné. Vous pouvez le modifier. Ce nom apparaîtra en regard de l'interface dans la liste des nœuds. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.

Interfaces de connexions en bande

1. Entrez l'adresse IP ou le nom de l'hôte de l'interface dans le champ **Adresse IP/nom d'hôte**.
2. (Facultatif) Entrez un port TCP pour la connexion dans le champ correspondant.
3. Entrez le nom d'utilisateur pour cette connexion dans le champ correspondant.
4. (Facultatif) Entrez le mot de passe pour cette connexion dans le champ correspondant.
5. (Facultatif) Entrez une description de cette interface dans le champ **Description**.
6. Cliquez sur **OK** pour enregistrer les modifications.

Interfaces pour connexions KVM hors bande, série hors bande

1. **Nom de l'application** : sélectionnez l'application à utiliser pour la connexion au nœud à l'aide de l'interface de la liste. Pour autoriser CC-SG à choisir automatiquement l'application en fonction de votre navigateur, sélectionnez **Auto-Detect** (détection automatique).
2. **Nom de dispositif Raritan** : sélectionnez le dispositif Raritan fournissant l'accès au nœud. Notez qu'un dispositif doit avoir été ajouté à CC-SG pour apparaître dans cette liste.

3. **Nom de port Raritan** : sélectionnez le port du dispositif Raritan fournissant l'accès au nœud. Le port doit être configuré dans CC-SG pour apparaître dans la liste. Pour les connexions série, les champs **Débit en bauds**, **Parité** et **Contrôle du flux** seront renseignés en fonction de la configuration du port.
4. (Facultatif) Entrez une description de cette interface dans le champ **Description**.
5. Cliquez sur **OK** pour enregistrer les modifications.

Interfaces pour connexions de gestion de l'alimentation par processeur DRAC, RSA et ILO

1. Entrez l'adresse IP ou le nom de l'hôte de l'interface dans le champ **Adresse IP/nom d'hôte**.
2. (Facultatif) Entrez un port TCP pour la connexion dans le champ correspondant.
3. Entrez le nom d'utilisateur pour cette connexion dans le champ correspondant.
4. (Facultatif) Entrez le mot de passe pour cette connexion dans le champ correspondant.
5. (Facultatif) Entrez une description de cette interface dans le champ **Description**.
6. Cliquez sur **OK** pour enregistrer les modifications.

Interfaces pour connexions par barrette d'alimentation gérée

Lorsque vous créez une interface pour barrette d'alimentation gérée indiquant un dispositif de gestion KX, la prise spécifiée sera renommée à l'aide du nom du nœud associé.

1. **Dispositif de gestion** :sélectionnez le dispositif Raritan auquel la barrette d'alimentation est connectée. Le dispositif doit être ajouté à CC-SG.
2. **Port de gestion** :sélectionnez le port du dispositif Raritan auquel la barrette d'alimentation est connectée.
3. **Nom de la barrette d'alimentation** : sélectionnez la barrette alimentant le nœud. La barrette doit être configurée dans CC-SG pour apparaître dans la liste.
4. **Nom de prise** : sélectionnez le nom de la prise sur laquelle le nœud est branché.

5. (Facultatif) Entrez une description de cette interface dans le champ **Description**.
6. Cliquez sur **OK** pour enregistrer les modifications.

Interfaces pour connexions de gestion d'alimentation IPMI

1. Entrez l'adresse IP ou le nom de l'hôte de l'interface dans le champ **Adresse IP/nom d'hôte**.
2. Entrez le numéro de port UDP de l'interface dans le champ correspondant.
3. **Authentification** : sélectionnez un schéma d'authentification pour la connexion à l'interface.
4. Entrez une valeur pour l'interface dans le champ **Intervalle de vérification (en secondes)**.
5. Entrez le nom d'utilisateur pour cette interface dans le champ correspondant.
6. (Facultatif) Entrez le mot de passe pour cette interface dans le champ correspondant.
7. (Facultatif) Entrez une description de cette interface dans le champ **Description**.
8. Cliquez sur **OK** pour enregistrer les modifications.

Interface Navigateur Web

Vous pouvez ajouter une interface Navigateur Web pour créer une connexion à un dispositif intégrant un serveur Web, tel qu'un Dominion PX. ***Exemple : Ajouter une interface Navigateur Web à un nœud PX*** (à la page 76). Une interface Navigateur Web permet également la connexion à une application Web quelconque, telle que celle associée à une carte de processeur RSA, DRAC ou ILO.

Il est possible qu'une interface Navigateur Web n'autorise pas la connexion automatique si l'application Web requiert des données autres que le nom d'utilisateur et le mot de passe ; un ID de session par exemple.

Les utilisateurs doivent être dotés du ***privilège Node In-Band Access*** (voir "Ajout d'un groupe d'utilisateurs" à la page 91) (accès en bande au nœud) pour accéder à une interface Navigateur Web.

DNS doit être configuré pour résoudre les URL. Les adresses IP ne requièrent la configuration de DNS.

1. Le nom par défaut d'une interface Navigateur Web est Web Browser. Vous pouvez modifier le nom dans le champ Nom. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
2. Entrez l'URL ou le nom du domaine de l'application Web dans le champ URL. Notez que vous devez entrer l'URL à laquelle l'application Web doit lire le nom d'utilisateur et le mot de passe. L'URL ne doit pas dépasser 120 caractères. Suivez les exemples ci-après pour corriger les formats :
   - http(s)://192.168.1.1/login.asp
   - http(s)://www.example.com/cgi/login
   - http(s)://example.com/home.html
3. (Facultatif) Entrez les nom d'utilisateur et mot de passe autorisant l'accès à cette interface.

   Remarque : laissez les champs vides pour les applications Web DRAC, ILO et RSA ou la connexion échouera.

4. Entrez le nom des champs Nom d'utilisateur et Mot de passe utilisés dans l'écran de connexion pour l'application Web dans les champs Champ du nom d'utilisateur et Champ du mot de passe. Vous devez visualiser la source HTML de l'écran de connexion pour trouver le nom des champs, et non leur libellé. ***Astuces pour ajouter une interface Navigateur Web*** (à la page 75).

5. (Facultatif) Entrez une description de cette interface dans le champ **Description**.
6. Cliquez sur **OK** pour enregistrer les modifications.

Astuces pour ajouter une interface Navigateur Web

Pour configurer l'interface Navigateur Web, vous devez collecter quelques informations de la source HTML pour identifier les noms réels des champs Nom d'utilisateur et Mot de passe. Chaque éditeur implémente différemment ces champs d'authentification et leurs noms varient d'un dispositif à l'autre, ainsi que d'une version de firmware à une autre. Aussi, il n'existe pas de méthode unique pour trouver le nom des champs. La procédure ci-dessous décrit une méthode possible.

Demandez l'assistance d'un ingénieur informatique ou d'un administrateur système pour repérer et identifier les noms de champ corrects.

➢ *Astuce pour repérer le nom des champs :*

1. Dans le code source HTML de la page de connexion de l'application Web, recherchez le libellé du champ, tel que Nom d'utilisateur et Mot de passe.
2. Examinez ensuite le code adjacent pour trouver une balise ressemblant à : `name="user"`

   Le mot entre guillemets est le nom du champ.

Exemple : Ajouter une interface Navigateur Web à un nœud PX

Une barre d'alimentation gérée Dominion PX peut être ajoutée à CC-SG en tant que nœud. Vous pouvez ensuite ajouter une interface Navigateur Web au nœud pour permettre aux utilisateurs d'accéder à l'application d'administration Web de Dominion PX.

➢ *Utilisez les valeurs suivantes pour ajouter une interface Navigateur Web à un nœud Dominion PX :*

URL : `<ADRESSE IP DOMINION PX>/auth.asp`

Nom d'utilisateur : nom d'utilisateur de l'administrateur Dominion PX

Mot de passe : mot de passe de l'administrateur Dominion PX

Champ du nom d'utilisateur = `login`

Champ du mot de passe = `password`

Résultats de l'ajout d'une interface

Lorsque vous ajoutez une interface à un nœud, elle apparaît dans la table **Interfaces** table et dans le menu déroulant **Interface par défaut** de l'écran **Ajouter un nœud** ou **Profil du nœud**. Vous pouvez cliquer sur le menu déroulant pour sélectionner l'interface à utiliser par défaut lors de la connexion au nœud.

Après enregistrement des modifications apportées à l'écran **Ajouter un nœud** ou **Profil du nœud**, le nom de l'interface apparaît également dans la liste Nœuds, imbriqué sous le nœud auquel elle donne accès.

Lorsque vous ajoutez une interface pour barrette d'alimentation gérée indiquant un dispositif de gestion KX, la prise spécifiée sera renommée à l'aide du nom du nœud associé.

Modification d'une interface

➢ *Pour modifier une interface :*

1. Cliquez sur l'onglet **Nœuds**.
2. Cliquez sur le nœud doté de l'interface à modifier.
3. Dans la table **Interfaces**, sélectionnez la ligne correspondant à l'interface à modifier.

4. Cliquez sur **Modifier**.
5. Modifiez les champs selon les besoins. Reportez-vous à ***Ajout d'une interface*** (à la page 69) pour plus d'informations sur les champs.
6. Cliquez sur **OK** pour enregistrer les modifications.

Suppression d'une interface

➢ *Pour supprimer une interface d'un nœud :*

1. Cliquez sur l'onglet **Nœuds**.
2. Cliquez sur le nœud doté de l'interface à supprimer.
3. Dans la table **Interfaces**, sélectionnez la ligne correspondant à l'interface à supprimer.
4. Cliquez sur **Supprimer**. Un message de confirmation apparaît.
5. Cliquez sur **Oui** pour supprimer l'interface.

Ajouter une interface aux signets

Si vous accédez fréquemment à un noeud via une interface particulière, vous pouvez l'ajouter à vos signets pour qu'elle soit à votre disposition dans le navigateur.

➢ *Pour ajouter une interface aux signets dans un navigateur :*

1. Sous l'onglet Noeuds, sélectionnez l'interface à ajouter aux signets. Vous devez développer le noeud pour visualiser les interfaces.
2. Choisissez Noeuds > Interface noeud signet.
3. Sélectionnez Copier URL dans Presse-papiers.
4. Cliquez sur OK. L'URL est copiée dans le Presse-papiers.
5. Ouvrez une nouvelle fenêtre de navigateur et collez l'URL dans le champ d'adresse.
6. Appuyez sur ENTREE pour vous connecter à l'URL.
7. Ajoutez l'URL à vos signets (ou à vos Favoris) dans le navigateur.

➢ *Pour ajouter une interface à vos signets dans Internet Explorer (ajouter une interface à vos Favoris) :*

1. Sous l'onglet Noeuds, sélectionnez l'interface à ajouter aux signets. Vous devez développer le noeud pour visualiser les interfaces.

2. Choisissez Noeuds > Interface noeud signet.
3. Sélectionnez Ajouter signet (IE uniquement).
4. Un nom par défaut apparaît dans le champ Nom du signet. Vous pouvez le modifier. Ce nom apparaît dans la liste de vos Favoris dans Internet Explorer.
5. Cliquez sur OK. La fenêtre Ajout de Favoris s'affiche.
6. Cliquez sur OK pour ajouter le signet à votre liste de Favoris.

➢ *Pour accéder au signet d'une interface :*

1. Ouvrez une fenêtre de navigateur.
2. Choisissez le signet de l'interface dans la liste de votre navigateur.
3. Lorsque le client d'accès CC-SG apparaît, connectez-vous en tant qu'utilisateur ayant accès à l'interface. La connexion avec l'interface s'ouvre.

Modification d'un nœud

Vous pouvez modifier un nœud pour remplacer son nom, sa description, ses interfaces, son interface par défaut ou ses associations.

➢ *Pour modifier un nœud :*

1. Cliquez sur l'onglet **Nœuds** et sélectionnez le nœud à modifier. L'écran Profil du nœud apparaît.
2. Modifiez les champs selon les besoins.
   - **Nom de nœud** : le nom du nœud qui apparaît dans l'écran Profil du nœud et dans l'onglet Nœuds. Les noms de nœud dans CC-SG doivent tous être uniques.
   - **Description** : description du nœud permettant aux utilisateurs d'identifier celui-ci.
   - **Interfaces** : permet d'ajouter, de modifier ou de supprimer une interface.
   - **Interface par défaut** : l'interface utilisée par défaut pour la connexion à un nœud.
   - **Associations de nœuds** : une liste de **catégories** et d'**éléments** configurée pour décrire et organiser le nœud de façon optimale.
3. Cliquez sur **OK** pour enregistrer les modifications.

Suppression d'un nœud

La suppression d'un nœud entraîne son retrait de l'onglet Nœuds. Le nœud ne sera plus accessible aux utilisateurs. Lorsque vous supprimez un nœud, tous les interfaces, associations et ports associés le sont également.

➢ *Pour supprimer un nœud :*

1. Sous l'onglet **Nœuds**, sélectionnez le nœud à supprimer.
2. Choisissez **Nœuds** > **Supprimer un nœud**. L'écran **Supprimer un nœud** s'affiche.
3. Cliquez sur **OK** pour supprimer le nœud.
4. Cliquez sur **Oui** pour confirmer que la suppression du nœud efface également toutes les interfaces et les ports associés. La liste de tous les objets supprimés apparaît lorsque la suppression est terminée.

Copie en bloc de catégories et d'éléments de nœuds

La commande Copier en bloc permet de copier les catégories et les éléments affectés d'un nœud vers plusieurs autres nœuds. Les catégories et les éléments sont les seules propriétés copiées lors de cette opération.

1. Cliquez sur l'onglet **Nœuds** et sélectionnez un nœud.
2. Choisissez **Nœuds** > **Copier en bloc**.
3. Dans la liste **Tous les nœuds**, sélectionnez les nœuds vers lesquels vous copiez les catégories et les éléments du nœud indiqué dans le champ **Nom du nœud**.
   - Cliquez sur le bouton flèche droite pour ajouter un nœud à la liste **Nœuds**.
   - Pour retirer un nœud de la liste **Nœuds sélectionnés**, sélectionnez-le, puis cliquez sur le bouton flèche gauche.
4. Cliquez sur **OK** pour copier en bloc. Un message apparaît lorsque les catégories et les éléments du nœud ont été copiés.

Connexion à un nœud

Une fois le nœud doté d'une interface, vous pouvez vous y connecter via l'interface de différentes façons. Reportez-vous au **manuel d'utilisation de CommandCenter Secure Gateway** de Raritan pour plus d'informations.

➢ *Pour effectuer la connexion à un nœud :*

1. Cliquez sur l'onglet **Nœuds**.
2. Sélectionnez le nœud auquel vous souhaitez vous connecter et :
   - Dans la table **Interfaces**, cliquez sur le nom de l'interface à l'aide de laquelle vous souhaitez vous connecter.
   - Dans l'onglet **Nœuds**, développez la liste d'interfaces sous le nœud auquel vous souhaitez vous connecter. Double-cliquez sur le nom de l'interface à l'aide de laquelle vous souhaitez vous connecter.

Envoi d'une commande ping à un nœud

Vous pouvez envoyer une commande ping à un nœud depuis CC-SG pour vous assurer que la connexion est active.

➢ *Pour envoyer une commande ping à un nœud :*

1. Cliquez sur l'onglet **Nœuds** et sélectionnez le nœud devant recevoir la commande ping.
2. Choisissez **Nœuds** > **Nœud ping**. Le résultat de l'exécution de la commande ping apparaît à l'écran.

Conversation

La fonction de conversation permet aux utilisateurs connectés au même nœud de communiquer. Vous devez être connecté à un nœud pour démarrer une session de conversation le concernant. Seuls les utilisateurs du même nœud peuvent communiquer.

➢ *Pour démarrer une session de conversation :*

1. Choisissez **Nœuds** > **Conversation** > **Démarrer la session de conversation**.

Raritan.
When you're ready to take control®

2. Tapez un message dans le champ en bas à gauche, puis cliquez sur **Envoyer**. Le message apparaît alors dans le champ en haut à gauche pour pouvoir être lu par tous les utilisateurs.

➢ *Pour participer à une session de conversation en cours :*

- Choisissez **Nœuds** > **Conversation** > **Afficher la session de conversation**.

➢ *Pour mettre fin à une session de conversation :*

1. Cliquez sur **Fermer** dans la session de conversation. Un message de confirmation apparaît.
   - Cliquez sur **Oui** pour fermer la session de conversation de tous les participants.
   - Cliquez sur **Non** pour quitter la session de conversation et la maintenir pour les autres participants.

A propos des groupes de nœuds

Les groupes de nœuds permettent d'organiser les nœuds dans un ensemble. Le groupe sert de base à une stratégie autorisant ou refusant l'accès à cet ensemble particulier de nœuds. Reportez-vous à ***Ajouter une stratégie*** (voir "Ajout d'une stratégie" à la page 103) pour plus d'informations. Les nœuds peuvent être groupés manuellement ou en créant une expression booléenne décrivant un ensemble d'attributs communs.

Si vous avez utilisé Paramétrage guidé pour créer des catégories et des éléments pour les nœuds, certaines formes d'organisation des nœuds par attributs communs ont déjà été créées. CC-SG crée automatiquement des stratégies d'accès par défaut reposant sur ces éléments. Reportez-vous à ***Associations*** (voir "Associations, catégories et éléments" à la page 24) pour plus d'informations sur la création des catégories et des éléments.

➢ *Pour visualiser des groupes de nœuds :*

- Choisissez **Associations** > **Groupes de nœuds**. La fenêtre **Gestionnaire des groupes de nœuds** s'affiche. La liste des groupes de nœuds existants s'affiche sur la gauche, tandis que les informations relatives au groupe de nœuds sélectionné apparaissent dans le panneau principal.
  - La liste des groupes de nœuds existants est affichée sur la gauche. Cliquez sur un groupe de nœuds pour afficher les informations le concernant dans le Gestionnaire des groupes de nœuds.
  - Si le groupe a été formé arbitrairement, l'onglet **Sélectionner les nœuds** est affiché. Il présente une liste des nœuds du groupe et de ceux qui n'en font pas partie.
  - Si le groupe a été formé d'après des attributs communs, l'onglet **Décrire les nœuds** est affiché. Il présente les règles régissant la sélection des nœuds du groupe.
  - Pour rechercher un nœud dans la liste du groupe, entrez une chaîne dans le champ **Recherche de nœud** au bas de la liste, puis cliquez sur **Aller à**. La méthode de recherche est configurée dans l'écran **Mon profil**. Reportez-vous à ***Configurer des utilisateurs et des groupes d'utilisateurs*** (voir "Utilisateurs et groupes d'utilisateurs" à la page 88) pour plus d'informations.

- Pour visualiser un groupe basé sur des attributs, cliquez sur **Afficher les nœuds** pour faire apparaître la liste des nœuds présents dans le groupe. Une fenêtre **Nœuds du groupe de nœuds** affiche les nœuds et tous leurs attributs.

Ajout d'un groupe de nœuds

➢ *Pour ajouter un groupe de nœuds :*

1. Choisissez **Associations** > **Groupes de nœuds**. La fenêtre **Gestionnaire des groupes de nœuds** s'affiche.
2. Choisissez **Groupes** > **Ajouter**. Un modèle de groupe de nœuds apparaît.
3. Dans le champ **Nom du groupe**, entrez le nom du groupe de nœuds à créer. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
4. Vous pouvez ajouter des nœuds à un groupe de deux façons : **Sélectionner les nœuds** et **Décrire les nœuds**. La méthode Sélectionner les nœuds permet d'affecter arbitrairement des nœuds au groupe en les sélectionnant dans la liste des nœuds disponibles. La méthode Décrire les nœuds permet de définir des règles de description des nœuds ; les nœuds correspondant à la description sont ajoutés au groupe.

Sélectionner les nœuds

1. Cliquez sur l'onglet **Sélectionner les nœuds**.
2. Cliquez sur le menu déroulant **Nom du dispositif** et sélectionnez un dispositif pour filtrer la liste **Disponible** et n'afficher que les nœuds avec interfaces à partir de ce dispositif.
3. Dans la liste **Disponible**, sélectionnez les nœuds à inclure au groupe, puis cliquez sur **Ajouter** pour les déplacer vers la liste **Sélectionné**. Les nœuds de la liste **Sélectionné** seront ajoutés au groupe.
4. Pour supprimer un nœud du groupe, sélectionnez son nom dans la liste **Sélectionné**, puis cliquez sur **Retirer**.
5. Vous pouvez rechercher un nœud dans la liste **Disponible** ou dans la liste **Sélectionné**. Entrez les termes de la recherche dans le champ sous la liste, puis cliquez sur **Aller à**.

6. Si vous comptez créer une stratégie autorisant l'accès permanent aux nœuds de ce groupe, cochez la case **Créer une stratégie d'accès total** pour le groupe.
7. Lorsque l'opération est terminée, cliquez sur **Ajouter** pour créer le groupe de nœuds. Le groupe est ajouté à la liste des groupes de nœuds à gauche.

Décrire les nœuds

1. Cliquez sur l'onglet **Sélectionner les nœuds**.
2. Cliquez sur **Ajouter une nouvelle ligne** afin d'inclure une rangée pour une nouvelle règle dans la table. Les règles se présentent sous la forme d'une expression qui peut être comparée aux nœuds.
3. Double-cliquez sur chaque colonne d'une ligne pour transformer la cellule voulue en menu déroulant, puis sélectionnez la valeur souhaitée pour chaque composant :
   - **Préfixe** – laissez cette option vide ou sélectionnez **NOT**. Dans ce cas, la règle recherchera des valeurs en opposition au reste de l'expression.
   - **Catégorie** – sélectionnez un attribut à évaluer dans la règle. Toutes les catégories que vous avez créées dans le **Gestionnaire des associations** seront disponibles ici. Les options **Nom de nœud** et **Type d'interface** sont également présentes.
   - **Opérateur** – sélectionnez une opération de comparaison à effectuer entre la catégorie et les éléments. Trois opérateurs sont disponibles : **=** (est égal à), **LIKE** (utilisé pour trouver l'élément dans un nom) et **<>** (est différent de).
   - **Elément** – sélectionnez une valeur à comparer à l'attribut de catégorie. Seuls les éléments associés à la catégorie sélectionnée seront affichés ici (par exemple, si l'évaluation porte sur une catégorie Service, les éléments Emplacement n'apparaîtront pas ici).

     Nom de la règle – il s'agit d'un nom affecté à la règle de cette ligne. Ces valeurs ne sont pas modifiables. Utilisez-les pour écrire des descriptions dans le champ **Expression abrégée**.

     Par exemple, la règle Service = Technique décrit tous les nœuds dont la **catégorie** Service est définie sur Technique. C'est exactement ce qui se produit lorsque vous configurez les associations au cours de l'opération **Ajouter un nœud**.

4. Pour ajouter une autre règle, cliquez à nouveau sur **Ajouter une nouvelle ligne**, puis effectuez les configurations nécessaires. La configuration de plusieurs règles permettra des descriptions plus précises en fournissant des critères multiples d'évaluation des nœuds.
   - Si vous souhaitez retirer une règle, mettez-la en surbrillance dans la table, puis cliquez sur **Supprimer la ligne**.
5. La table de règles ne présente que des critères d'évaluation des nœuds. Pour écrire la description du groupe de nœuds, ajoutez les règles par **nom de règle** dans le champ **Expression abrégée**. Si la description ne requiert qu'une seule règle, il vous suffit d'entrer le nom de cette dernière dans le champ. Si plusieurs règles sont évaluées, entrez-les dans le champ à l'aide d'opérateurs logiques décrivant les règles les unes par rapport aux autres :
   - **&** - opérateur AND. Un nœud doit satisfaire aux règles des deux côtés de cet opérateur pour que la description (ou la section d'une description) soit vérifiée.
   - | - opérateur OR. Un nœud ne doit satisfaire qu'une des règles de chaque côté de cet opérateur pour que la description (ou la section d'une description) soit vérifiée.
   - **(** et **)** - opérateurs de regroupement. Ceci décompose la description en sous-section contenue entre les parenthèses. La section entre parenthèses est évaluée avant que le reste de la description ne soit comparé au nœud. Les groupes entre parenthèses peuvent être imbriqués dans un autre groupe entre parenthèses.

     Exemple 1 : si vous souhaitez décrire les nœuds appartenant au service technique, créez une règle indiquant Service = Technique. Elle deviendra Rule0. Entrez ensuite Rule0 dans le champ **Expression abrégée**.

     Exemple 2 : vous souhaitez décrire un groupe de nœuds appartenant au service technique OU situés à Philadelphie, et indiquer que toutes les machines doivent disposer d'un Go de mémoire ; vous devez donc créer trois règles.

- Service = Service technique (Rule0)
- Emplacement = Philadelphie (Rule1)
- Mémoire = 1Go (Rule2)

Ces règles doivent être organisées les unes par rapport aux autres. Puisque le nœud peut appartenir au service technique ou être situé à Philadelphie, utilisez l'opérateur OR, |, pour joindre les deux : Rule0|Rule1. Pour effectuer cette comparaison en premier, placez-la entre parenthèses : (Rule0|Rule1). Enfin, puisque les nœuds doivent satisfaire cette comparaison ET disposer d'un Go de mémoire, nous utilisons le connecteur AND, **&**, pour joindre cette section à Rule2 : (Rule0|Rule1)&Rule2. Entrez cette expression finale dans le champ **Expression abrégée**.

6. Cliquez sur **Valider** si une description a été écrite dans le champ **Expression abrégée**. Si la description est formée de manière incorrecte, un avertissement apparaît. Si la description est correctement formée, une forme normalisée de l'expression apparaît dans le champ **Expression normalisée**.
7. Cliquez sur **Afficher les nœuds** pour visualiser les nœuds satisfaisant l'expression. Une fenêtre **Nœuds du groupe de nœuds** apparaît présentant les nœuds groupés par l'expression en cours. Vous pouvez ainsi vérifier si la description est écrite correctement. Dans le cas contraire, vous pouvez retourner à la table des règles ou au champ **Expression abrégée** pour effectuer des modifications.
8. Si vous comptez créer une stratégie autorisant l'accès permanent aux nœuds de ce groupe, cochez la case **Créer une stratégie d'accès total pour le groupe**.
9. Lorsque la description des nœuds appartenant au groupe est terminée, cliquez sur **Ajouter** pour créer le groupe de nœuds. Le groupe est ajouté à la liste des groupes de nœuds à gauche.

Modification d'un groupe de nœuds

Modifiez un groupe de nœuds pour changer sa composition ou sa description.

➢ *Pour modifier un groupe de nœuds :*

1. Choisissez **Associations** > **Groupes de nœuds**. La fenêtre **Gestionnaire des groupes de nœuds** s'ouvre.

2. Cliquez sur le nœud à modifier dans la liste des groupes de nœuds. Les informations relatives au nœud choisi s'affichent dans la fenêtre **Groupes de nœuds**.
3. Reportez-vous aux instructions des sections **Sélectionner les nœuds** et **Décrire les nœuds** ci-dessus pour plus d'informations sur la configuration d'un groupe de nœuds.
4. Cliquez sur **OK** pour enregistrer les modifications.

Suppression d'un groupe de nœuds

1. Choisissez **Associations** > **Groupes de nœuds**. La fenêtre **Gestionnaire des groupes de nœuds** s'affiche.
2. Dans la liste des groupes de nœuds à gauche, sélectionnez le nœud à supprimer.
3. Choisissez **Groupes** > **Supprimer**.

Chapitre 9 Utilisateurs et groupes d'utilisateurs

Les comptes **utilisateur** sont créés pour affecter aux utilisateurs un nom d'utilisateur et un mot de passe pour accéder à CC-SG.

Un **groupe d'utilisateurs** définit un ensemble de privilèges pour ses membres. Vous ne pouvez pas affecter de privilèges aux utilisateurs eux-mêmes, uniquement aux groupes d'utilisateurs. Tous les utilisateurs doivent appartenir à un groupe d'utilisateurs au moins.

CC-SG gère une liste d'utilisateurs et une liste de groupes d'utilisateurs centralisées pour l'authentification et l'autorisation.

La configuration de l'authentification externe par CC-SG est décrite dans ***Authentification à distance*** (à la page 119).

La création de stratégies d'accès pour les affecter à des groupes d'utilisateurs est décrite dans ***Stratégies de contrôle d'accès*** (à la page 102).

Dans ce chapitre

Onglet Utilisateurs....89
Groupes d'utilisateurs par défaut....90
Ajout d'un groupe d'utilisateurs....91
Modification d'un groupe d'utilisateurs....93
Suppression d'un groupe d'utilisateurs....94
Ajout d'un utilisateur....94
Modification d'un utilisateur....95
Suppression d'un utilisateur....96
Affectation d'un utilisateur à un groupe....97
Suppression d'un utilisateur d'un groupe....98
Votre profil utilisateur....98
Déconnexion des utilisateurs....100
Copie en bloc d'utilisateurs....100

Onglet Utilisateurs

Cliquez sur l'onglet **Utilisateurs** pour afficher tous les utilisateurs et groupes de CC-SG.

Les utilisateurs sont imbriqués sous les groupes d'utilisateurs dont ils sont membres. Les groupes auxquels des utilisateurs sont affectés apparaissent dans la liste avec un symbole + en regard de leur nom. Cliquez sur le symbole + pour développer ou masquer la liste des utilisateurs d'un groupe. Les utilisateurs actifs, connectés actuellement à CC-SG, apparaissent en gras.

L'onglet Utilisateurs offre la possibilité d'effectuer des recherches d'utilisateurs dans l'arborescence.

Groupes d'utilisateurs par défaut

CC-SG est configuré avec trois groupes d'utilisateurs par défaut : **CC-Super User** (super utilisateur CC), **System Administrators** (administrateurs système) et **CC Users** (utilisateurs CC).

Groupe CC Super-User

Le groupe **CC Super-User** dispose des droits complets d'administration et d'accès. Ce groupe ne peut contenir qu'un seul utilisateur membre. Le nom d'utilisateur par défaut est **admin**. Vous pouvez le modifier. Vous ne pouvez pas supprimer le groupe CC Super-User. Vous ne pouvez pas modifier les privilèges affectés au groupe CC Super-User, ajouter des membres ou supprimer le seul membre du groupe. Les mots de passe forts sont systématiquement appliqués pour le membre du groupe CC Super-User. Les exigences du mot de passe fort sont :

- Les mots de passe doivent contenir au moins une lettre minuscule.
- Les mots de passe doivent contenir au moins une lettre majuscule.
- Les mots de passe doivent contenir au moins un nombre.
- Les mots de passe doivent contenir au moins un caractère spécial (par exemple, un point d'exclamation ou une perluète).

Groupe System Administrators

Le groupe **System Administrators** dispose des droits complets d'administration et d'accès. Contrairement au groupe CC Super-User, vous pouvez modifier les privilèges, et ajouter ou supprimer des membres.

Groupe CC Users

Le groupe **CC Users** dispose d'un accès aux nœuds en bande ou hors bande. Vous pouvez modifier les privilèges, et ajouter ou supprimer des membres.

Important : de nombreuses commandes de menu ne sont accessibles qu'après la sélection du groupe d'utilisateurs ou de l'utilisateur approprié.

Ajout d'un groupe d'utilisateurs

La création de groupes d'utilisateurs vous permet d'organiser par la suite les utilisateurs lors de leur ajout. A la création d'un groupe d'utilisateurs, un ensemble de privilèges lui est affecté. Les utilisateurs affectés au groupe hériteront de ces privilèges. Par exemple, si vous créez un groupe et lui affectez le privilège **User Management** (gestion des utilisateurs), tous les utilisateurs affectés au groupe pourront afficher et exécuter les commandes du menu **Gestionnaire des utilisateurs**. Reportez-vous à l'***annexe C : Privilèges de groupe d'utilisateurs*** (voir "Privilèges de groupe d'utilisateurs" à la page 273) pour plus d'informations sur chaque privilège.

La configuration des groupes d'utilisateurs se compose de quatre étapes de base :

- dénomination du groupe et saisie d'une description ;
- sélection des privilèges dont disposera le groupe d'utilisateurs ;
- sélection des types d'interfaces dont le groupe d'utilisateurs peut se servir pour accéder aux nœuds ;
- sélection des stratégies décrivant les nœuds accessibles au groupe d'utilisateurs.

➢ *Pour ajouter un groupe :*

1. Choisissez **Utilisateurs** > **Gestionnaire des groupes d'utilisateurs** > **Ajouter un groupe d'utilisateurs**. L'écran **Ajouter un groupe d'utilisateurs** s'affiche.
2. Renseignez le champ **Nom du groupe d'utilisateurs**. Le nom d'un groupe d'utilisateurs doit être unique. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
3. (Facultatif) Entrez une brève description de ce groupe dans le champ **Description**.

4. Cliquez sur l'onglet **Droits d'administrateur**.
5. Cochez la case correspondant à chaque privilège que vous souhaitez affecter au groupe d'utilisateurs.
6. Sous la table des privilèges figure la zone **Accès au nœud** contenant les privilèges de trois types d'accès au nœud : **Node Out-of-Band Access** (accès hors bande au nœud), **Node In-Band Access** (accès en bande au nœud) et **Node Power Control** (gestion de l'alimentation des nœuds). Cochez la case correspondant à chaque type d'accès au nœud que vous souhaitez affecter au groupe d'utilisateurs.
7. Cliquez sur l'onglet **Stratégies de dispositif/nœud**. Une table de stratégies apparaît.

   La table **Toutes les stratégies** répertorie toutes les stratégies disponibles dans CC-SG. Chaque stratégie représente une règle autorisant ou refusant l'accès à un groupe de nœuds. Reportez-vous à ***Configurer des stratégies et des groupes de nœuds*** (voir "Stratégies de contrôle d'accès" à la page 102) pour plus d'informations sur les stratégies et comment les créer.
8. Dans la liste **Toutes les stratégies**, sélectionnez la stratégie à affecter au groupe d'utilisateurs, puis cliquez sur **Ajouter** pour la déplacer vers la liste **Stratégies sélectionnées**. Les stratégies de la liste **Stratégies sélectionnées** autoriseront ou non l'accès aux nœuds ou aux dispositifs qu'elles contrôlent.

   Répétez cette étape pour ajouter des stratégies supplémentaires au groupe d'utilisateurs.

   - Pour accorder simplement au groupe l'accès à tous les nœuds disponibles, sélectionnez l'option **Full Access Policy** (stratégie d'accès total) dans la liste **Toutes les stratégies**, puis cliquez sur **Ajouter**.
   - Pour supprimer une stratégie du groupe d'utilisateurs, sélectionnez son nom dans la liste **Stratégies sélectionnées**, puis cliquez sur **Supprimer**.
9. (Facultatif) Lorsque les stratégies du groupe sont configurées, cliquez sur **Appliquer** pour enregistrer le groupe et en créer un autre. Répétez les opérations de cette section chaque fois que vous souhaitez ajouter des groupes d'utilisateurs.
10. Cliquez sur **OK** pour enregistrer les modifications.

Modification d'un groupe d'utilisateurs

La modification d'un groupe d'utilisateurs permet de remplacer les privilèges et les stratégies du groupe.

Remarque : *vous ne pouvez pas modifier les privilèges ou les stratégies du groupe* ***CC-Super User****.*

➢ *Pour modifier un groupe :*

1. Cliquez sur l'onglet **Utilisateurs** de gauche.
2. Cliquez sur le groupe d'utilisateurs dans l'onglet **Utilisateurs**. L'écran **Profil du groupe d'utilisateurs** apparaît.
3. (Facultatif) Entrez le nouveau nom du groupe d'utilisateurs dans le champ **Nom du groupe d'utilisateurs**.
4. (Facultatif) Entrez une nouvelle description de ce groupe dans le champ **Description**.
5. Cliquez sur l'onglet **Droits d'administrateur**.
6. Cochez la case correspondant à chaque privilège que vous souhaitez affecter au groupe d'utilisateurs. Désactivez un privilège pour le retirer du groupe.
7. Dans la zone **Accès au nœud**, cliquez sur le menu déroulant pour chaque type d'interface d'accès autorisée au groupe et sélectionnez **Contrôler**.
8. Cliquez sur le menu déroulant pour chaque type d'interface d'accès non autorisée au groupe et sélectionnez **Refuser**.
9. Cliquez sur l'onglet **Stratégies**. Deux tables de stratégies apparaissent.
10. Pour chaque stratégie que vous souhaitez ajouter au groupe, sélectionnez-la dans la table **Toutes les stratégies**, puis cliquez sur **Ajouter** pour déplacer la stratégie vers la liste **Stratégies sélectionnées**. Les stratégies de la liste **Stratégies sélectionnées** autoriseront ou non aux utilisateurs l'accès au nœud (ou aux dispositifs) qu'elles contrôlent.
11. Pour supprimer une stratégie du groupe d'utilisateurs, sélectionnez son nom dans la liste **Stratégies sélectionnées**, puis cliquez sur **Supprimer**.
12. Cliquez sur **OK** pour enregistrer les modifications.

Suppression d'un groupe d'utilisateurs

Vous pouvez supprimer un groupe d'utilisateurs s'il ne compte aucun membre.

➢ *Pour supprimer un groupe d'utilisateurs :*

1. Cliquez sur l'onglet **Utilisateurs** de gauche.
2. Cliquez sur le groupe d'utilisateurs à supprimer dans l'onglet **Utilisateurs**.
3. Choisissez **Utilisateurs** > **Gestionnaire des groupes d'utilisateurs** > **Supprimer un groupe d'utilisateurs**.
4. Cliquez sur **OK** pour supprimer le groupe d'utilisateurs.

Ajout d'un utilisateur

Lorsque vous ajoutez un utilisateur à CC-SG, vous devez indiquer un groupe pour accorder à l'utilisateur les privilèges d'accès affectés au groupe.

➢ *Pour ajouter un utilisateur :*

1. Dans l'onglet **Utilisateurs**, sélectionnez le groupe auquel vous souhaitez ajouter un utilisateur.
2. Choisissez **Utilisateurs** > **Gestionnaire des utilisateurs** > **Ajouter un utilisateur**.
3. Dans le champ **Nom d'utilisateur**, entrez le nom dont l'utilisateur à ajouter se servira pour se connecter à CC-SG. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
4. Cochez la case **Connexion activée** pour autoriser l'utilisateur à se connecter à CC-SG.
5. Cochez la case **Authentification à distance** uniquement si vous souhaitez que l'utilisateur soit authentifié par un serveur externe, tel que TACACS+, RADIUS, LDAP ou AD. Si vous utilisez l'authentification à distance, un mot de passe n'est pas nécessaire ; les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe** sont alors désactivés.
6. Dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**, entrez le mot de passe dont l'utilisateur se servira pour se connecter à CC-SG.

Remarque : reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des mots de passe.

Si les mots de passe forts sont activés, le mot de passe entré doit être conforme aux règles établies. La barre d'information en haut de l'écran affichera des messages pour vous rappeler les exigences en matière de mot de passe. Reportez-vous à ***Administration avancée*** (à la page 166) pour plus d'informations sur les mots de passe forts.

7. Cochez la case **Forcer la modification du mot de passe à la prochaine connexion** pour obliger l'utilisateur à changer le mot de passe affecté à l'ouverture de session suivante.
8. Cochez la case **Forcer la modification du mot de passe régulièrement** pour indiquer la fréquence à laquelle l'utilisateur devra changer le mot de passe.
9. Si vous cochez cette case, dans le champ **Période d'expiration (en jours)**, entrez le délai pendant lequel l'utilisateur pourra se servir du même mot de passe avant d'être obligé de le changer.
10. Entrez l'**adresse électronique** de l'utilisateur dans le champ correspondant. Elle sera utilisée pour envoyer des notifications utilisateur.
11. Cliquez sur le menu déroulant **Groupes d'utilisateurs** et sélectionnez le groupe auquel l'utilisateur sera ajouté.
12. Lorsque la configuration de l'utilisateur est terminée, cliquez sur **Appliquer** pour ajouter celui-ci et en créer un autre, ou cliquez sur **OK** pour ajouter l'utilisateur sans en créer d'autre. Les utilisateurs créés apparaîtront dans l'onglet **Utilisateurs**, imbriqués sous les groupes auxquels ils appartiennent.

Modification d'un utilisateur

Vous ne pouvez pas modifier un utilisateur pour remplacer le groupe auquel il appartient. Reportez-vous à ***Ajouter un utilisateur à un groupe*** (voir "Affectation d'un utilisateur à un groupe" à la page 97) pour plus d'informations.

➢ *Pour modifier un utilisateur :*

1. Dans l'onglet **Utilisateurs**, cliquez sur le symbole + pour développer le groupe contenant l'utilisateur à modifier, puis sélectionnez l'utilisateur. L'écran **Profil utilisateur** apparaît.

2. Désactivez la case **Connexion activée** pour empêcher l'utilisateur de se connecter à CC-SG. Cochez la case **Connexion activée** pour autoriser l'utilisateur à se connecter à CC-SG.
3. Cochez la case **Authentification à distance** uniquement si vous souhaitez que l'utilisateur soit authentifié par un serveur externe, tel que TACACS+, RADIUS, LDAP ou AD. Si vous utilisez l'authentification à distance, un mot de passe n'est pas nécessaire ; les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe** sont alors désactivés.
4. Dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**, entrez le mot de passe remplaçant celui de l'utilisateur.

   Remarque : si les mots de passe forts sont activés, le mot de passe entré doit être conforme aux règles établies. La barre d'information en haut de l'écran vous rappellera les exigences en matière de mot de passe. Reportez-vous à ***Administration avancée*** (à la page 166) pour plus d'informations sur les mots de passe forts.

5. Cochez la case **Forcer la modification du mot de passe à la prochaine connexion** pour obliger l'utilisateur à changer le mot de passe affecté à l'ouverture de session suivante.
6. Dans le champ **Adresse électronique**, ajoutez une adresse ou modifiez celle configurée pour l'utilisateur. Elle sera utilisée pour envoyer des notifications utilisateur.
7. Cliquez sur **OK** pour enregistrer les modifications.

Suppression d'un utilisateur

La suppression d'un utilisateur entraîne son retrait définitif de CC-SG. Cette opération permet de supprimer des comptes utilisateur devenus inutiles.

Cette procédure supprime toutes les instances d'un utilisateur, même s'il figure dans plusieurs groupes. Reportez-vous à ***Supprimer un utilisateur d'un groupe*** (voir "Suppression d'un utilisateur d'un groupe" à la page 98) pour retirer un utilisateur d'un groupe mais non de CC-SG.

➢ *Pour supprimer un utilisateur :*

1. Dans l'onglet **Utilisateurs**, cliquez sur le symbole + pour développer le groupe contenant l'utilisateur à supprimer, puis sélectionnez l'utilisateur. L'écran **Profil utilisateur** apparaît.

2. Choisissez **Utilisateurs** > **Gestionnaire des utilisateurs** > **Supprimer un utilisateur**.
3. Cliquez sur **OK** pour supprimer définitivement l'utilisateur de CC-SG.

Affectation d'un utilisateur à un groupe

La commande Affecter des utilisateurs à un groupe permet d'affecter des utilisateurs à un groupe dont ils ne sont pas encore membres. Les utilisateurs affectés ainsi seront ajoutés à leur nouveau groupe tout en restant dans leurs groupes précédents éventuels. Pour déplacer un utilisateur, utilisez cette commande conjointement à la commande **Supprimer un utilisateur du groupe** décrite dans la section suivante.

➢ *Pour affecter un utilisateur à un groupe :*

1. Dans l'onglet **Utilisateurs**, sélectionnez le groupe d'utilisateurs auquel vous souhaitez affecter des utilisateurs.
2. Choisissez **Utilisateurs** > **Gestionnaire des groupes d'utilisateurs** > **Affecter des utilisateurs à un groupe**.
3. Le groupe d'utilisateurs sélectionné apparaît dans le champ **Nom du groupe d'utilisateurs**.
4. Les utilisateurs non affectés au groupe cible apparaissent dans la liste **Utilisateurs hors groupe**.
   - Dans la liste, sélectionnez les utilisateurs à ajouter, puis cliquez sur **>** pour les déplacer dans la liste **Utilisateurs dans le groupe**.
   - Cliquez sur le bouton **>>** pour déplacer tous les utilisateurs non membres du groupe vers la liste **Utilisateurs dans le groupe**.
   - Pour supprimer des personnes du groupe cible, sélectionnez les utilisateurs à retirer dans la liste **Utilisateurs dans le groupe**, puis cliquez sur le bouton **<**.
   - Cliquez sur le bouton **<<** pour retirer tous les utilisateurs de la liste **Utilisateurs dans le groupe**.
5. Lorsque tous les utilisateurs ont été déplacés vers la colonne appropriée, cliquez sur **OK**. Les membres de la liste **Utilisateurs dans le groupe** sont alors ajoutés au groupe d'utilisateurs sélectionné.

Suppression d'un utilisateur d'un groupe

Lorsque vous supprimez un utilisateur d'un groupe, le retrait ne concerne que le groupe spécifié. L'utilisateur reste dans tous les autres groupes affectés. La suppression d'un utilisateur d'un groupe n'entraîne pas son retrait de CC-SG.

Si un utilisateur n'appartient qu'à un seul groupe, la suppression est impossible. Vous ne pouvez le supprimer que de CC-SG.

➢ *Pour supprimer un utilisateur d'un groupe :*

1. Dans l'onglet **Utilisateurs**, cliquez sur le symbole + pour développer le groupe contenant l'utilisateur à supprimer, puis sélectionnez l'utilisateur. L'écran **Profil utilisateur** apparaît.
2. Choisissez **Utilisateurs** > **Gestionnaire des utilisateurs** > **Supprimer un utilisateur du groupe**. L'écran **Supprimer un utilisateur** s'affiche.
3. Cliquez sur **OK** pour supprimer l'utilisateur du groupe.

Votre profil utilisateur

A propos de mon profil

Mon profil permet à tous les utilisateurs de visualiser des détails sur leur compte, d'en modifier certains et de personnaliser les paramètres d'utilisation. C'est la seule façon de modifier le nom du compte **admin**.

➢ *Pour visualiser votre profil :*

- Choisissez **Passerelle sécurisée** > **Mon profil**. L'écran **Mon profil** apparaît, affichant les détails de votre compte.

Changer votre mot de passe

1. Choisissez **Passerelle sécurisée** > **Mon profil**.
2. Cochez la case **Modifier le mot de passe**.
3. Entrez votre mot de passe actuel dans le champ **Ancien mot de passe**.
4. Entrez votre nouveau mot de passe dans le champ **Nouveau mot de passe**. Un avis apparaît si un mot de passe fort est obligatoire.
5. Entrez une nouvelle fois votre nouveau mot de passe dans le champ **Confirmer le nouveau mot de passe**.

6. Cliquez sur **OK** pour enregistrer les modifications.

Modifier votre préférence de recherche par défaut

1. Choisissez **Passerelle sécurisée** > **Mon profil**.
2. Dans la zone **Préférence de recherche**, sélectionnez la méthode que vous souhaitez privilégier pour la recherche de nœuds, d'utilisateurs et de dispositifs.
   - **Filtre par résultats de recherche** – permet d'utiliser des caractères joker et limite l'affichage des nœuds, des utilisateurs ou des dispositifs à tous les noms contenant les critères de recherche.
   - **Trouver la chaîne correspondante** – ne prend pas en charge l'utilisation des caractères joker et met en surbrillance la correspondance la plus proche parmi les nœuds, utilisateurs ou dispositifs au fur et à mesure de votre saisie. La liste est limitée aux éléments contenant les critères de recherche après l'activation du bouton **Rechercher**.
3. Cliquez sur **OK** pour enregistrer les modifications.

Modifier la taille de police par défaut dans CC-SG

1. Choisissez **Passerelle sécurisée** > **Mon profil**.
2. Cliquez sur le menu déroulant **Taille de police** pour régler la taille de la police d'affichage du client CC-SG standard.
3. Cliquez sur **OK** pour enregistrer les modifications.

Modifier votre adresse électronique

1. Choisissez **Passerelle sécurisée** > **Mon profil**.
2. Entrez une nouvelle adresse dans le champ **Adresse électronique** pour ajouter ou remplacer l'adresse que CC-SG doit utiliser pour vous envoyer des notifications.
3. Cliquez sur **OK** pour enregistrer les modifications.

Modifier le nom d'utilisateur du super utilisateur CC-SG

Vous devez vous connecter à CC-SG sous le compte du super utilisateur CC pour modifier son nom d'utilisateur. Le nom d'utilisateur par défaut du super utilisateur CC est **admin**.

1. Choisissez **Passerelle sécurisée** > **Mon profil**.
2. Modifiez la valeur du champ **Nom d'utilisateur**.

3. Cliquez sur **OK** pour enregistrer les modifications.

Déconnexion des utilisateurs

Vous pouvez fermer la session CC-SG des utilisateurs actifs, individuellement ou par groupe d'utilisateurs.

➢ *Pour déconnecter des utilisateurs :*

1. Dans l'onglet **Utilisateurs**, cliquez sur le symbole + pour développer le groupe contenant l'utilisateur à déconnecter de CC-SG, puis sélectionnez l'utilisateur.
   - Pour sélectionner plusieurs utilisateurs, maintenez la touche **Maj** et cliquez sur des utilisateurs supplémentaires.
2. Choisissez **Utilisateurs** > **Gestionnaire des utilisateurs** > **Déconnecter les utilisateurs**. L'écran **Déconnecter les utilisateurs** apparaît et affiche la liste des utilisateurs sélectionnés.
3. Cliquez sur **OK** pour déconnecter les utilisateurs de CC-SG.

➢ *Pour déconnecter tous les utilisateurs d'un groupe :*

1. Dans l'onglet **Utilisateurs**, sélectionnez le groupe d'utilisateurs que vous souhaitez déconnecter de CC-SG.
   - Pour déconnecter plusieurs groupes, maintenez la touche **Maj** et cliquez sur des groupes supplémentaires.
2. Choisissez **Utilisateurs** > **Gestionnaire des groupes d'utilisateurs** > **Déconnecter les utilisateurs**. L'écran **Déconnecter les utilisateurs** apparaît et affiche la liste des utilisateurs actifs des groupes sélectionnés.
3. Cliquez sur **OK** pour déconnecter les utilisateurs de CC-SG.

Copie en bloc d'utilisateurs

Vous pouvez utiliser la commande Copier en bloc pour copier les affiliations de groupe d'un utilisateur à un autre, ou à une liste d'utilisateurs. Si les utilisateurs cible appartiennent déjà à des groupes, ces affiliations seront supprimées.

➢ *Pour copier en bloc des utilisateurs :*

1. Dans l'onglet **Utilisateurs**, cliquez sur le symbole + pour développer le groupe contenant l'utilisateur dont vous souhaitez copier les stratégies et les privilèges, puis sélectionnez l'utilisateur.

2. Choisissez **Utilisateurs** > **Gestionnaire des utilisateurs** > **Copier en bloc**. Le champ **Nom d'utilisateur** affiche l'utilisateur dont vous copiez les stratégies et privilèges.
3. Dans la liste **Tous les utilisateurs**, sélectionnez les utilisateurs qui doivent adopter les stratégies et privilèges de l'utilisateur indiqué dans le champ **Nom d'utilisateur**.
   - Cliquez sur le bouton **>** pour déplacer le nom d'un utilisateur vers la liste **Utilisateurs sélectionnés**.
   - Cliquez sur le bouton **>>** pour déplacer tous les utilisateurs vers la liste **Utilisateurs sélectionnés**.
   - Pour supprimer un utilisateur de la liste **Utilisateurs sélectionnés**, sélectionnez-le et cliquez sur le bouton **<**.
   - Cliquez sur **<<** pour retirer tous les utilisateurs de la liste **Utilisateurs dans le groupe**.
4. Cliquez sur **OK** pour copier.

Chapitre 10 Stratégies de contrôle d'accès

Dans ce chapitre

Contrôle des accès à l'aide de stratégies 102
Ajout d'une stratégie 103
Modification d'une stratégie.....105
Suppression d'une stratégie 106
Prise en charge de support virtuel 107
Affectation de stratégies à des groupes d'utilisateurs 110

Contrôle des accès à l'aide de stratégies

Les stratégies sont des règles définissant les nœuds et dispositifs accessibles aux utilisateurs, quand ils peuvent y accéder et si des autorisations de support virtuel sont activées, le cas échéant. La méthode la plus simple pour créer des stratégies consiste à classer les nœuds et dispositifs en groupes, puis à définir des stratégies autorisant ou refusant l'accès aux nœuds et aux dispositifs de chaque groupe. Une fois la stratégie créée, vous l'affectez à un groupe d'utilisateurs. Reportez-vous à ***Affectation de stratégies à des groupes d'utilisateurs*** (à la page 110).

CC-SG inclut également une **stratégie d'accès total**. Si vous souhaitez accorder aux utilisateurs l'accès à tous les nœuds, il vous suffit d'affecter la **stratégie d'accès total** à tous les groupes d'utilisateurs.

Si vous avez effectué le **paramétrage guidé**, certaines stratégies de base ont peut-être déjà été créées. Reportez-vous à ***Configuration de CC-SG par paramétrage guidé*** (à la page 14) pour plus d'informations.

➢ *Pour contrôler l'accès à l'aide de stratégies :*

- Créez des groupes de nœuds afin d'organiser les nœuds pour lesquels vous souhaitez créer des règles d'accès. Reportez-vous à ***Ajout d'un groupe de nœuds*** (à la page 83).
- Créez des groupes de dispositifs afin d'organiser les dispositifs pour lesquels vous souhaitez créer des règles d'accès. Reportez-vous à ***Ajouter un groupe de dispositifs*** (à la page 51).
- Créez une stratégie pour un groupe de nœuds (ou de dispositifs) indiquant quand l'accès à celui-ci est possible. Reportez-vous à ***Ajout d'une stratégie*** (à la page 103).
- Appliquez la stratégie à un groupe d'utilisateurs. Reportez-vous à ***Affectation de stratégies à des groupes d'utilisateurs*** (à la page 110).

Ajout d'une stratégie

Si vous créez une stratégie qui interdit l'accès (**Refuser**) à un groupe de nœuds ou de dispositifs, vous devez également en créer une qui en autorise l'accès (**Contrôler**). Les utilisateurs ne reçoivent pas automatiquement de droits **Contrôler** lorsque la stratégie **Refuser** n'est pas en vigueur.

Remarque : lorsque CC-SG est en mode Proxy ou Les deux, vous ne pouvez donner aux utilisateurs accès à Support virtuel. **Modes de connexion : Direct et Proxy** *(à la page 185)*

➢ *Pour ajouter une stratégie :*

1. Choisissez **Associations** > **Stratégies**. La fenêtre **Gestionnaire des stratégies** s'affiche.
2. Cliquez sur **Ajouter**. Une fenêtre de dialogue s'affiche vous demandant d'entrer un nom pour la stratégie.
3. Renseignez le champ **Entrer le nom de la stratégie**. Reportez-vous à ***Conventions d'appellation*** (à la page 300) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
4. Cliquez sur **OK**. La nouvelle stratégie est ajoutée à la liste **Nom de stratégie** dans l'écran Gestionnaire des stratégies.
5. Cliquez sur la flèche déroulante **Groupe de dispositifs**, puis sélectionnez le groupe dont l'accès est régi par cette stratégie.
6. Cliquez sur la flèche déroulante **Groupe de nœuds**, puis sélectionnez le groupe dont l'accès est régi par cette stratégie.
7. Si cette stratégie ne concerne qu'un type de groupe, ne sélectionnez qu'une valeur pour ce groupe.
8. Cliquez sur la flèche déroulante **Jours**, puis sélectionnez les jours de la semaine concernés par cette stratégie : **Tous** les jours, **Jour de la semaine** (lundi à vendredi uniquement) et **Week-end** (samedi et dimanche uniquement), ou **Personnalisé** (sélectionnez des jours spécifiques).
9. Sélectionnez **Personnalisé** pour choisir votre propre ensemble de jours. Les cases à cocher correspondant aux différents jours de la semaine sont alors activées.
10. Cochez les cases correspondant aux jours concernés par cette stratégie.

11. Dans le champ **Heure de début**, entrez l'heure à laquelle cette stratégie entre en vigueur. L'heure saisie doit respecter le format 24 heures.
12. Dans le champ **Heure de fin**, entrez l'heure à laquelle cette stratégie prend fin. L'heure saisie doit respecter le format 24 heures.
13. Dans le champ **Autorisation d'accès au nœud/dispositif**, sélectionnez **Contrôler** pour que cette stratégie autorise l'accès au groupe de nœuds ou de dispositifs sélectionné aux heures et jours désignés. Sélectionnez **Refuser** pour que cette stratégie interdise l'accès au groupe de nœuds ou de dispositifs sélectionné aux heures et jours désignés.
14. Si vous avez sélectionné **Contrôler** dans le champ **Autorisation d'accès au nœud/dispositif**, la section Autorisation de support virtuel est activée. Dans le champ **Autorisation de support virtuel**, sélectionnez une option pour autoriser ou refuser l'accès aux supports virtuels disponibles dans les groupes de nœuds ou dispositifs sélectionnés aux heures et jours indiqués :
    - **Lecture-Ecriture** donne accès en lecture et écriture aux supports virtuels.
    - **Lecture seule** donne uniquement accès en lecture aux supports virtuels.
    - **Refuser** interdit tout accès aux supports virtuels.
15. Cliquez sur **Mettre à jour** pour ajouter la nouvelle stratégie à CC-SG, puis cliquez sur **Oui** dans le message de confirmation qui apparaît.

Modification d'une stratégie

Lorsque vous modifiez une stratégie, les changements n'affectent pas les utilisateurs connectés à CC-SG au moment de la modification. Ils prendront effet à la session suivante.

Si vous souhaitez que vos changements prennent effet immédiatement, entrez en mode de maintenance, puis modifiez les stratégies. Lorsque vous entrez en mode de maintenance, tous les utilisateurs actuels sont déconnectés de CC-SG jusqu'à la sortie du mode de maintenance. Les utilisateurs peuvent alors se reconnecter. Reportez-vous à ***A propos du mode de maintenance*** (voir "Mode de maintenance" à la page 155) pour plus d'informations.

➢ *Pour modifier une stratégie :*

1. Dans le menu **Associations**, cliquez sur **Stratégies**. La fenêtre **Gestionnaire des stratégies** s'affiche.
2. Cliquez sur la flèche déroulante **Nom de stratégie**, puis choisissez dans la liste la stratégie à modifier.
3. (Facultatif) Pour modifier le nom de la stratégie, cliquez sur **Modifier**. Une fenêtre **Modifier une stratégie** apparaît. Entrez un nouveau nom dans le champ, puis cliquez sur **OK** pour renommer la stratégie.
4. Cliquez sur la flèche déroulante **Groupe de dispositifs**, puis sélectionnez le groupe dont l'accès est régi par cette stratégie.
5. Cliquez sur la flèche déroulante **Groupe de nœuds**, puis sélectionnez le groupe dont l'accès est régi par cette stratégie.
6. Si cette stratégie ne concerne qu'un type de groupe, ne sélectionnez qu'une valeur pour ce type.
7. Cliquez sur la flèche déroulante **Jours**, puis sélectionnez les jours de la semaine concernés par cette stratégie : **Tous** (tous les jours), **Jour de la semaine** (lundi à vendredi uniquement) et **Week-end** (samedi et dimanche uniquement), ou **Personnalisé** (sélectionnez des jours spécifiques).
8. Sélectionnez **Personnalisé** pour choisir votre propre ensemble de jours. Les cases à cocher correspondant aux différents jours de la semaine sont alors activées.
9. Cochez les cases correspondant aux jours concernés par cette stratégie.

10. Dans le champ **Heure de début**, entrez l'heure à laquelle cette stratégie entre en vigueur. L'heure saisie doit respecter le format 24 heures.
11. Dans le champ **Heure de fin**, entrez l'heure à laquelle cette stratégie prend fin. L'heure saisie doit respecter le format 24 heures.
    - Dans le champ **Autorisation d'accès au nœud/dispositif** :
    - Sélectionnez **Contrôler** pour que cette stratégie autorise l'accès au groupe de nœuds ou de dispositifs sélectionné aux heures et jours désignés.
    - Sélectionnez **Refuser** pour que cette stratégie interdise l'accès au groupe de nœuds ou de dispositifs sélectionné aux heures et jours désignés.
12. Si vous avez sélectionné **Contrôler** dans le champ **Autorisation d'accès au nœud/dispositif**, la section Autorisation de support virtuel est activée. Dans le champ **Autorisation de support virtuel**, sélectionnez une option pour autoriser ou refuser l'accès aux supports virtuels disponibles dans les groupes de nœuds ou dispositifs sélectionnés aux heures et jours indiqués :
    - **Lecture-Ecriture** donne accès en lecture et écriture aux supports virtuels.
    - **Lecture seule** donne uniquement accès en lecture aux supports virtuels.
    - **Refuser** interdit tout accès aux supports virtuels.
13. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.
14. Cliquez sur **Oui** dans le message de confirmation qui s'affiche.

Suppression d'une stratégie

➢ *Pour supprimer une stratégie :*

1. Choisissez **Associations** > **Stratégies**. La fenêtre **Gestionnaire des stratégies** s'affiche.
2. Cliquez sur la flèche déroulante **Nom de stratégie**, puis choisissez dans la liste la stratégie à supprimer.
3. Cliquez sur **Supprimer**.
4. Cliquez sur **Oui** dans le message de confirmation qui s'affiche.

Prise en charge de support virtuel

CC-SG permet la prise en charge de supports virtuels pour les nœuds connectés aux dispositifs KX II compatibles. Pour obtenir des instructions détaillées sur l'accès aux supports virtuels, reportez-vous au manuel d'utilisation de Dominion KX II. Reportez-vous à ***Ajout d'une stratégie*** (à la page 103) pour plus d'informations sur la création de stratégies d'autorisation de support virtuel à des groupes d'utilisateurs dans CC-SG.

Support virtuel : définition

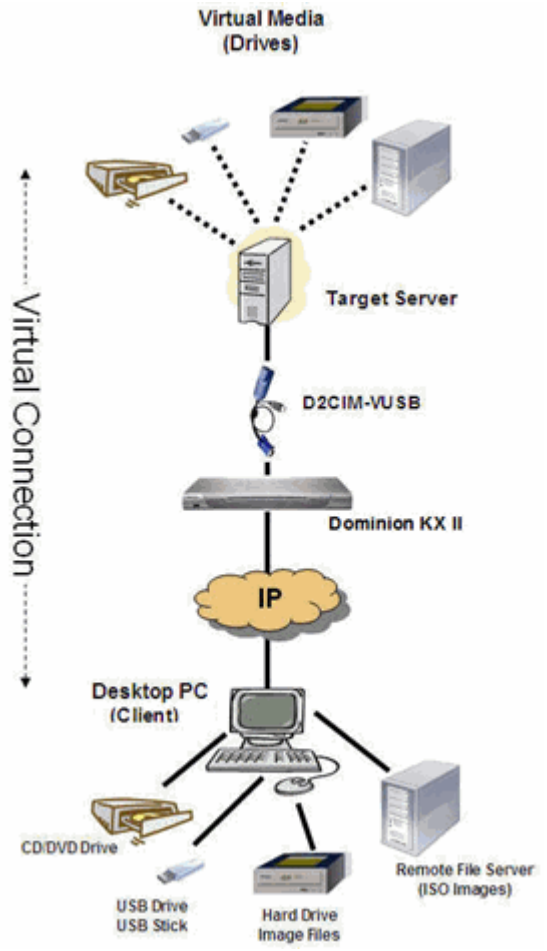
La fonction Support virtuel prolonge les capacités KVM en permettant aux serveurs cible KVM d'accéder à distance aux supports des serveurs de fichiers de PC clients et réseau. Grâce à cette fonction, les supports montés sur les serveurs de fichiers de PC clients et réseau sont intégrés virtuellement au serveur cible. Le serveur cible peut alors accéder en lecture et en écriture au support comme s'il lui était connecté physiquement. Les supports virtuels possibles sont les suivants : lecteurs de CD et de DVD internes et USB, mémoires de stockage de grande capacité USB, disques durs de PC et images ISO (images disque).

Les supports virtuels permettent d'effectuer des tâches supplémentaires à distances, telles que :

- transférer des fichiers ;
- exécuter des diagnostics ;
- installer des applications ou des correctifs ;
- installer complètement le système d'exploitation.

Ce contrôle KVM étendu élimine la plupart des accès au centre de données, permettant un gain de temps et d'argent, et rendant ainsi les supports virtuels très puissants.

Raritan.
When you're ready to take control®


Virtual Media
(Drives)
Virtual Connection
Target Server
D2CIM-VUSB
Dominion KX II
IP
Desktop PC
(Client)
CD/DVD Drive
USB Drive
USB Stick
Hard Drive
Image Files
Remote File Server
(ISO Images)

Tous les modèles CommandCenter Secure Gateway prennent en charge la fonction Support virtuel. Les avantages de la fonction Support virtuel : montage des lecteurs/supports à distance sur le serveur cible pour prendre en charge l'installation des logiciels et les diagnostics, sont maintenant disponibles dans tous les modèles CommandCenter Secure Gateway.

Chaque unité CommandCenter Secure Gateway est équipée de la fonction Support virtuel pour autoriser la gestion à distance des tâches à l'aide d'une vaste gamme de lecteurs de CD ou de DVD, USB, et d'images internes et distants. Contrairement à d'autres solutions, CommandCenter Secure Gateway prend en charge l'accès par support virtuel des disques durs et des images montées à distance pour une flexibilité et une productivité accrues.

Les sessions sur support virtuel sont sécurisées à l'aide de chiffrement 128 bits AES ou RC4.

Le nouveau module d'interface pour ordinateur D2CIM-VUSB prend en charge les sessions sur support virtuel pour les serveurs cible KVM disposant de l'interface USB 2.0. Ce nouveau module prend également en charge la synchronisation de souris absolue, ainsi que la mise à jour de firmware à distance.

Affectation de stratégies à des groupes d'utilisateurs

Les stratégies doivent être affectées à un groupe d'utilisateurs avant de prendre effet. Une fois la stratégie affectée à un groupe d'utilisateurs, elle contrôlera l'accès des membres. Reportez-vous à ***Configurer des utilisateurs et des groupes d'utilisateurs*** (voir "Utilisateurs et groupes d'utilisateurs" à la page 88) pour plus d'informations sur l'affectation de stratégies à un groupe d'utilisateurs.

Chapitre 11: Vues personnalisées pour dispositifs et nœuds

L'option Vues personnalisées vous permet d'indiquer différents modes d'affichage des nœuds et des dispositifs dans le panneau de gauche, à l'aide de catégories, de groupes de nœuds et de groupes de dispositifs.

Dans ce chapitre

Types de vues personnalisées 111
Utilisation de vues personnalisées dans le client Admin.....112

Types de vues personnalisées

Il existe trois types de vues personnalisées : Vue par catégorie, Filtrer par groupe de nœuds et Filtrer par groupe de dispositifs.

Vue par catégorie

Tous les nœuds et dispositifs décrits par les catégories que vous spécifiez apparaissent dans la liste des nœuds ou des dispositifs lorsqu'une vue personnalisée Vue par catégorie est appliquée. Les nœuds et les dispositifs auxquels aucune catégorie n'a été affectée s'affichent également comme non associés.

Filtrer par groupe de noeuds

Seuls les groupes de noeuds que vous spécifiez sont affichés dans la liste des noeuds lorsque la vue personnalisée Groupe de noeuds est appliquée. Le premier niveau d'organisation est le nom du groupe de noeuds. Un noeud apparaît plusieurs fois dans la liste s'il appartient à plusieurs groupes de noeuds définis dans la vue personnalisée. Les noeuds n'appartenant pas à un groupe spécifié par la vue personnalisée ne figurent pas dans la liste.

Filtrer par groupe de dispositifs

Seuls les groupes de dispositifs que vous spécifiez sont affichés dans la liste des dispositifs lorsque la vue personnalisée Filtrer par groupe de dispositifs est appliquée. Le premier niveau d'organisation est le nom du groupe de dispositifs. Un dispositif apparaît plusieurs fois dans la liste s'il appartient à plusieurs groupes de dispositifs définis dans la vue personnalisée. Les dispositifs n'appartenant pas à un groupe spécifié par la vue personnalisée ne figurent pas dans la liste.

Utilisation de vues personnalisées dans le client Admin

Vues personnalisées pour les nœuds

Ajouter une vue personnalisée à des noeuds

➢ *Ajouter une vue personnalisée à des noeuds*

1. Cliquez sur l'onglet **Noeuds**.
2. Dans le menu **Noeuds**, cliquez sur **Modifier la vue**, puis sur **Créer une vue personnalisée**. L'écran **Vue personnalisée** s'affiche.
3. Dans le panneau **Vue personnalisée**, cliquez sur **Ajouter**. La fenêtre **Ajouter une vue personnalisée** s'affiche.
4. Tapez le nom de la nouvelle vue dans le champ **Nom de la vue personnalisée**.
5. Dans la section Type de vue personnalisée :
   - Sélectionnez **Filtrer par groupe de noeuds** pour créer une vue personnalisée qui affiche uniquement les groupes de noeuds spécifiés.
   - Sélectionnez **Vue par catégorie** pour créer une vue personnalisée qui affiche les noeuds en fonction des catégories spécifiées.
6. Cliquez sur **OK**.
7. Dans la section **Détails de vue personnalisée** :
   a. Dans la liste Disponible, sélectionnez un élément à inclure à la vue personnalisée, puis cliquez sur **Ajouter** pour le déplacer dans la liste Sélectionné. Répétez cette opération pour tous les éléments dont vous avez besoin.

b. Placez les éléments dans la liste **Sélectionné** dans l'ordre dans lequel chaque groupe doit apparaître sous l'onglet Noeuds. Sélectionnez un élément, puis cliquez sur les boutons fléchés pour placer les éléments dans l'ordre souhaité.

c. Si vous devez supprimer un élément de la liste, sélectionnez-le, puis cliquez sur **Retirer**.

8. Cliquez sur **Enregistrer** pour enregistrer la vue personnalisée. Un message confirme l'ajout de la vue personnalisée.
9. Pour appliquer la nouvelle vue personnalisée, cliquez sur **Appliquer la vue**.

Appliquer une vue personnalisée à des noeuds

➢ *Pour appliquer une vue personnalisée à la liste de noeuds*

1. Dans le menu **Noeuds**, cliquez sur **Modifier la vue**, puis sur **Vue personnalisée**. L'écran **Vue personnalisée** s'affiche.
2. Cliquez sur la flèche déroulante **Nom**, puis sélectionnez une vue personnalisée dans la liste.
3. Cliquez sur **Appliquer la vue** pour appliquer la vue personnalisée.

OU

- Choisissez Noeuds > Modifier la vue. Toutes les vues personnalisées définies apparaissent comme options dans le menu contextuel. Choisissez la vue personnalisée à appliquer.

Modifier une vue personnalisée pour des noeuds

1. Cliquez sur l'onglet **Noeuds**.
2. Dans le menu **Noeuds**, cliquez sur **Modifier la vue**, puis sur **Créer une vue personnalisée**. L'écran **Vue personnalisée** s'affiche.
3. Cliquez sur la flèche déroulante **Nom**, puis sélectionnez une vue personnalisée dans la liste. Les détails des éléments inclus, ainsi que leur ordre, sont affichés dans le panneau **Détails de vue personnalisée**.

➢ *Pour renommer une vue personnalisée :*

1. Dans le panneau **Vue personnalisée**, cliquez sur **Modifier**. La fenêtre **Modifier une vue personnalisée** s'affiche.

2. Renseignez le champ **Entrer le nouveau nom de la vue personnalisée**, puis cliquez sur **OK**. Le nom de la nouvelle vue apparaît dans le champ **Nom** de l'écran Vue personnalisée.

➢ *Pour modifier le contenu de la vue personnalisée :*

1. Dans la section **Détails de vue personnalisée** :
   a. Dans la liste Disponible, sélectionnez un élément à inclure à la vue personnalisée, puis cliquez sur **Ajouter** pour le déplacer dans la liste Sélectionné. Répétez cette opération pour tous les éléments dont vous avez besoin.
   b. Placez les éléments dans la liste **Sélectionné** dans l'ordre dans lequel chaque groupe doit apparaître sous l'onglet Noeuds. Sélectionnez un élément, puis cliquez sur les boutons fléchés pour placer les éléments dans l'ordre souhaité.
   c. Si vous devez supprimer un élément de la liste, sélectionnez-le, puis cliquez sur **Retirer**.
2. Cliquez sur **Enregistrer** pour enregistrer la vue personnalisée. Un message confirme l'ajout de la vue personnalisée.
3. Pour appliquer la nouvelle vue personnalisée, cliquez sur **Appliquer la vue**.

Supprimer une vue personnalisée pour des noeuds

1. Cliquez sur l'onglet **Noeuds**.
2. Dans le menu **Noeuds**, cliquez sur **Modifier la vue**, puis sur **Créer une vue personnalisée**. L'écran **Vue personnalisée** s'affiche.
3. Cliquez sur la flèche déroulante **Nom**, puis sélectionnez une vue personnalisée dans la liste. Les détails des éléments inclus, ainsi que leur ordre, sont affichés dans le panneau **Détails de vue personnalisée**.
4. Dans le panneau **Vue personnalisée**, cliquez sur **Supprimer**. Une demande de confirmation **Supprimer une vue personnalisée** s'affiche.
5. Cliquez sur **Oui** dans le message de confirmation.

Affecter une vue personnalisée par défaut à des noeuds

1. Cliquez sur l'onglet **Noeuds**.
2. Dans le menu **Noeuds**, cliquez sur **Modifier la vue**, puis sur **Créer une vue personnalisée**. L'écran **Vue personnalisée** s'affiche.

3. Cliquez sur la flèche déroulante **Nom**, puis sélectionnez une vue personnalisée dans la liste.
4. Dans le panneau **Vue personnalisée**, cliquez sur **Définir comme valeur par défaut**. A la connexion suivante, la vue personnalisée sélectionnée sera utilisée par défaut.

Affecter une vue personnalisée de noeuds par défaut à tous les utilisateurs

Si vous disposez du privilège CC Setup and Control (paramétrage et contrôle de CC), vous pouvez affecter une vue personnalisée par défaut à tous les utilisateurs.

1. Cliquez sur l'onglet Noeuds.
2. Choisissez Noeuds > Modifier la vue > Créer une vue personnalisée.
3. Cliquez sur la flèche déroulante **Nom** et sélectionnez la vue personnalisée que vous souhaitez affecter à tout le système.
4. Cochez la case **Pour tout le système**, puis cliquez sur **Enregistrer**.

Tous les utilisateurs qui se connectent à CC-SG voient l'onglet Noeuds trié selon la vue personnalisée sélectionnée. Les utilisateurs ont cependant la possibilité de changer la vue personnalisée.

Vues personnalisées pour les dispositifs

Ajouter une vue personnalisée pour les dispositifs

➢ *Pour ajouter une vue personnalisée pour les dispositifs*

1. Cliquez sur l'onglet Dispositifs.
2. Dans le menu Dispositifs, cliquez sur **Modifier la vue**, puis sur **Créer une vue personnalisée**.L'écran **Vue personnalisée** s'affiche.
3. Dans le panneau **Vue personnalisée**, cliquez sur **Ajouter**. La fenêtre **Ajouter une vue personnalisée** s'affiche.
4. Tapez le nom de la nouvelle vue dans le champ **Nom de la vue personnalisée**.
5. Dans la section Type de vue personnalisée :
   - Sélectionnez **Filtrer par groupe de dispositifs** pour créer une vue personnalisée qui affiche uniquement les groupes de dispositifs spécifiés.
   - Sélectionnez **Vue par catégorie** pour créer une vue personnalisée qui affiche les dispositifs en fonction des catégories spécifiées.

6. Cliquez sur **OK**.
7. Dans la section **Détails de vue personnalisée** :
   a. Dans la liste Disponible, sélectionnez un élément à inclure à la vue personnalisée, puis cliquez sur **Ajouter** pour le déplacer dans la liste Sélectionné. Répétez cette opération pour tous les éléments dont vous avez besoin.
   b. Placez les éléments dans la liste **Sélectionné** dans l'ordre dans lequel chaque groupe doit apparaître sous l'onglet Noeuds. Sélectionnez un élément, puis cliquez sur les boutons fléchés pour placer les éléments dans l'ordre souhaité.
   c. Si vous devez supprimer un élément de la liste, sélectionnez-le, puis cliquez sur **Retirer**.
8. Cliquez sur **Enregistrer** pour enregistrer la vue personnalisée. Un message confirme l'ajout de la vue personnalisée.
9. Pour appliquer la nouvelle vue personnalisée, cliquez sur **Appliquer la vue**.

Appliquer une vue personnalisée pour des dispositifs

➢ *Pour appliquer une vue personnalisée à la liste de dispositifs*

1. Dans le menu Dispositifs, cliquez sur **Modifier la vue**, puis sur **Vue personnalisée**. L'écran **Vue personnalisée** s'affiche.
2. Cliquez sur la flèche déroulante **Nom**, puis sélectionnez une vue personnalisée dans la liste.
3. Cliquez sur **Appliquer la vue** pour appliquer la vue personnalisée.

OU

Choisissez Dispositifs > Modifier la vue. Toutes les vues personnalisées définies apparaissent comme options dans le menu contextuel. Choisissez la vue personnalisée à appliquer.

Modifier une vue personnalisée pour des dispositifs

1. Cliquez sur l'onglet **Dispositifs**.
2. Dans le menu Dispositifs, cliquez sur **Modifier la vue**, puis sur **Créer une vue personnalisée**.L'écran **Vue personnalisée** s'affiche.

3. Cliquez sur la flèche déroulante **Nom**, puis sélectionnez une vue personnalisée dans la liste. Les détails des éléments inclus, ainsi que leur ordre, sont affichés dans le panneau **Détails de vue personnalisée**.

➢ *Pour renommer une vue personnalisée :*

1. Dans le panneau **Vue personnalisée**, cliquez sur **Modifier**. La fenêtre **Modifier une vue personnalisée** s'affiche.
2. Renseignez le champ **Entrer le nouveau nom de la vue personnalisée**, puis cliquez sur **OK**. Le nom de la nouvelle vue apparaît dans le champ **Nom** de l'écran Vue personnalisée.

➢ *Pour modifier le contenu de la vue personnalisée :*

1. Dans la section **Détails de vue personnalisée** :
   a. Dans la liste Disponible, sélectionnez un élément à inclure à la vue personnalisée, puis cliquez sur **Ajouter** pour le déplacer dans la liste Sélectionné. Répétez cette opération pour tous les éléments dont vous avez besoin.
   b. Placez les éléments dans la liste **Sélectionné** dans l'ordre dans lequel chaque groupe doit apparaître sous l'onglet Noeuds. Sélectionnez un élément, puis cliquez sur les boutons fléchés pour placer les éléments dans l'ordre souhaité.
   c. Si vous devez supprimer un élément de la liste, sélectionnez-le, puis cliquez sur **Retirer**.
2. Cliquez sur **Enregistrer** pour enregistrer la vue personnalisée. Un message confirme l'ajout de la vue personnalisée.
3. Pour appliquer la nouvelle vue personnalisée, cliquez sur **Appliquer la vue**.

Supprimer une vue personnalisée pour des dispositifs

1. Cliquez sur l'onglet Dispositifs.
2. Choisissez Dispositifs > **Modifier la vue** > **Créer une vue personnalisée**. L'écran **Vue personnalisée** s'affiche.
3. Cliquez sur la flèche déroulante **Nom**, puis sélectionnez une vue personnalisée dans la liste. Les détails des éléments inclus, ainsi que leur ordre, sont affichés dans le panneau **Détails de vue personnalisée**.

4. Dans le panneau **Vue personnalisée**, cliquez sur **Supprimer**. Une demande de confirmation **Supprimer une vue personnalisée** s'affiche.
5. Cliquez sur **Oui** dans le message de confirmation.

Affecter une vue personnalisée par défaut à des dispositifs

1. Cliquez sur l'onglet Dispositifs.
2. Choisissez Dispositifs > **Modifier la vue** > **Créer une vue personnalisée**. L'écran **Vue personnalisée** s'affiche.
3. Cliquez sur la flèche déroulante **Nom**, puis sélectionnez une vue personnalisée dans la liste.
4. Dans le panneau **Vue personnalisée**, cliquez sur **Définir comme valeur par défaut**. A la connexion suivante, la vue personnalisée sélectionnée sera utilisée par défaut.

Affecter une vue personnalisée de dispositifs par défaut à tous les utilisateurs

Si vous disposez du privilège Device, Port and Node Management (gestion des dispositifs, des ports et des nœuds), vous pouvez affecter une vue personnalisée par défaut à tous les utilisateurs.

1. Cliquez sur l'onglet Dispositifs.
2. Choisissez Dispositifs > Modifier la vue > Créer une vue personnalisée.
3. Cliquez sur la flèche déroulante **Nom** et sélectionnez la vue personnalisée que vous souhaitez affecter à tout le système.
4. Cochez la case **Pour tout le système**, puis cliquez sur **Enregistrer**.

Tous les utilisateurs qui se connectent à CC-SG voient l'onglet Dispositifs trié selon la vue personnalisée sélectionnée. Les utilisateurs ont cependant la possibilité de changer la vue personnalisée.

Chapitre 12 Authentification à distance

Dans ce chapitre

A propos de l'authentification et de l'autorisation (AA) 119
Noms distincts pour LDAP et AD 120
Définition des modules pour l'authentification et l'autorisation 121
Définition de l'ordre des serveurs AA externes 122
A propos d'AD et de CC-SG 122
Ajout d'un module AD dans CC-SG 122
Modification d'un module AD 128
Importation des groupes d'utilisateurs AD 129
Synchronisation d'AD avec CC-SG 130
A propos de LDAP et de CC-SG 134
Ajout d'un module LDAP (Netscape) dans CC-SG 134
A propos de TACACS+ et de CC-SG 137
Ajout d'un module TACACS+ 137
A propos de RADIUS et de CC-SG 138
Ajout d'un module RADIUS 138

A propos de l'authentification et de l'autorisation (AA)

Les utilisateurs de CC-SG peuvent être authentifiés et autorisés localement sur l'unité CC-SG, ou authentifiés à distance à l'aide des serveurs de répertoires pris en charge mentionnés ci-après :

- Active Directory (AD) de Microsoft
- Lightweight Directory Access Protocol (LDAP) de Netscape
- TACACS+
- RADIUS

Vous pouvez utiliser un nombre quelconque de serveurs à distance pour l'authentification externe. Vous pouvez par exemple configurer trois serveurs AD, deux serveurs iPlanet (LDAP) et trois serveurs RADIUS.

Seul AD peut être utilisé pour l'autorisation à distance des utilisateurs.

Flux d'authentification

Lorsque l'authentification à distance est activée, l'authentification et l'autorisation suivent les étapes mentionnées ci-après :

1. L'utilisateur se connecte à CC-SG à l'aide des nom d'utilisateur et mot de passe appropriés.

2. CC-SG se connecte au serveur externe et envoie le nom d'utilisateur et le mot de passe.
3. Le nom d'utilisateur et le mot de passe sont acceptés ou refusés et renvoyés. Si l'authentification est rejetée, la tentative de connexion échoue.
4. Si l'authentification aboutit, une autorisation est effectuée. CC-SG vérifie que le nom d'utilisateur entré correspond à un groupe créé dans CC-SG ou importé d'AD, et accorde des privilèges suivant la stratégie affectée.

Lorsque l'authentification à distance est désactivée, l'authentification et l'autorisation sont effectuées localement sur CC-SG.

Comptes utilisateur

Des comptes utilisateur doivent être ajoutés au serveur d'authentification pour permettre l'opération à distance. Vous devez créer les utilisateurs sur CC-SG pour tous les serveurs d'authentification, sauf si l'authentification et l'autorisation s'effectuent à l'aide d'AD. Les noms d'utilisateur doivent être identiques sur le serveur d'authentification et sur CC-SG, même si les mots de passe peuvent être différents. Le mot de passe local CC-SG n'est utilisé que si l'authentification à distance est désactivée. Reportez-vous à ***Configurer des utilisateurs et des groupes d'utilisateurs*** (voir "Utilisateurs et groupes d'utilisateurs" à la page 88) pour plus d'informations sur l'ajout d'utilisateurs qui seront authentifiés à distance.

Remarque *: si l'authentification à distance est activée, les utilisateurs doivent s'adresser à leurs administrateurs pour modifier leur mot de passe sur le serveur distant. Les mots de passe des utilisateurs authentifiés à distance ne sont pas modifiables sur CC-SG.*

Noms distincts pour LDAP et AD

La configuration des utilisateurs authentifiés à distance sur les serveurs LDAP ou AD requiert la saisie des noms d'utilisateur et des recherches au format Nom distinct. Le format Nom distinct est décrit dans **RFC2253** (http://www.rfc-editor.org/rfc/rfc2253.txt).

Pour configurer CC-SG, vous devez savoir comment entrer les noms distincts et l'ordre où chaque composant du nom doit être répertorié.

Définir un nom distinct pour AD

La structure d'un nom distinct pour AD se présente comme suit. Vous n'avez pas à indiquer un **nom courant** et une **unité organisationnelle** :

- nom courant (cn), unité organisationnelle (ou), composant de domaine (dc)

Définir un nom distinct pour LDAP

La structure d'un nom distinct pour Netscape LDAP et eDirectory LDAP se présente comme suit :

- id utilisateur (uid), unité organisationnelle (ou), organisation (o)

Définir un nom d'utilisateur pour AD

Lors de l'authentification des utilisateurs CC-SG sur un serveur AD à l'aide des données **cn=administrator,cn=users,dc=xyz,dc=com** dans **username**, si une unité CC-SG est associée à un groupe AD importé, l'accès est accordé à l'utilisateur avec ces références de connexion. Notez que vous pouvez indiquer plusieurs noms courants, unités organisationnelles et composants de domaine.

Définir un nom distinct de base

La saisie d'un nom distinct (ND) permet également d'indiquer l'emplacement de départ de la recherche des utilisateurs. Renseignez le champ **ND de base** pour indiquer un conteneur AD où figurent les utilisateurs. Par exemple, entrez : **ou=DCAdmins,ou=IT,dc=xyz,dc=com** pour rechercher tous les utilisateurs dans les unités organisationnelles **DCAdmins** et **IT** sous le domaine **xyz.com**.

Définition des modules pour l'authentification et l'autorisation

Lorsque vous avez ajouté tous les serveurs externes comme modules dans CC-SG, vous pouvez décider si CC-SG doit les utiliser pour l'authentification et/ou l'autorisation.

➢ *Pour définir des modules d'authentification et d'autorisation :*

1. Choisissez Administration > Sécurité.
2. Choisissez l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification externes configurés s'affichent dans une table.
3. Pour chaque serveur listé :

a. Cochez la case **Authentification** si vous souhaitez que CC-SG utilise le serveur pour l'authentification des utilisateurs.

b. Cochez la case **Autorisation** si vous souhaitez que CC-SG utilise le serveur pour l'autorisation des utilisateurs. Seuls les serveurs AD peuvent être utilisés pour l'autorisation.

4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Définition de l'ordre des serveurs AA externes

CC-SG interrogera les serveurs d'autorisation et d'authentification externes configurés dans l'ordre spécifié. Si la première option sélectionnée n'est pas disponible, CC-SG essaie la deuxième, la troisième, et ainsi de suite, jusqu'à ce l'opération aboutisse.

➢ *Pour établir l'ordre dans lequel CC-SG utilise les serveurs d'authentification et d'autorisation externes :*

1. Choisissez Administration > Sécurité.
2. Choisissez l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification externes configurés s'affichent dans une table.
3. Sélectionnez un serveur dans la liste, puis cliquez sur les flèches haut et bas pour définir la priorité de la séquence d'engagement.
4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

A propos d'AD et de CC-SG

CC-SG prend en charge l'authentification et l'autorisation des utilisateurs importés d'un contrôleur de domaine AD, même si ceux-ci ne sont pas définis localement dans CC-SG. Les utilisateurs sont ainsi gérés exclusivement sur le serveur AD. Une fois votre serveur AD configuré en tant que module dans CC-SG, ce dernier peut rechercher un domaine particulier dans tous les contrôleurs. Vous pouvez synchroniser vos modules AD dans CC-SG avec vos serveurs AD pour vous assurer que CC-SG dispose des données d'autorisation les plus récentes sur vos groupes d'utilisateurs AD.

Ajout d'un module AD dans CC-SG

Important : créez les groupes d'utilisateurs AD appropriés et affectez-leur des utilisateurs AD avant de commencer cette procédure. Assurez-vous également que le serveur de noms de domaine CC-SG et le suffixe de domaine sont configurés dans le Gestionnaire de

configuration. Reportez-vous à *Configurer le réseau CC-SG* **(voir "Configuration du réseau CC-SG" à la page 171).**

➢ *Pour ajouter un module AD dans CC-SG :*

1. Choisissez Administration > Sécurité.
2. Choisissez l'onglet Authentification.
3. Cliquez sur **Ajouter** pour ouvrir la fenêtre Ajouter un module.
4. Cliquez sur le menu déroulant **Type de module** et sélectionnez **AD** dans la liste.
5. Entrez le nom du serveur AD dans le champ **Nom du module**.
   - Le nombre maximum de caractères est de 31.
   - Tous les caractères imprimables peuvent être utilisés.
   - Le nom de module est facultatif. Il se définit uniquement pour distinguer ce module de serveur AD de ceux que vous configurez dans CC-SG. Ce nom n'est pas lié à celui du serveur AD.
6. Cliquez sur **Suivant** pour continuer. L'onglet **Généralités** s'ouvre.

Paramètres généraux AD

Dans l'onglet **Généralités**, vous devez ajouter les données qui permettront à CC-SG de lancer des requêtes sur le serveur AD.

1. Entrez le domaine AD à interroger dans le champ **Domain** (domaine). Par exemple, si le domaine AD est installé dans le domaine xyz.com, entrez **xyz.com** dans le champ **Domain**. CC-SG et le serveur AD que vous souhaitez interroger doivent être configurés sur le même domaine ou sur des domaines différents approuvés.

   Remarque : CC-SG recherche le domaine souhaité sur tous les contrôleurs de domaine connus.

2. Entrez l'adresse IP du serveur de noms de domaine dans le champ **DNS Server IP Address** (adresse IP du serveur DNS). Vous pouvez également cocher la case **Use default CC-SG DNS** (utiliser le serveur DNS CC-SG par défaut) afin d'utiliser le serveur de noms de domaine configuré dans la section Gestionnaire de configuration de CC-SG. Reportez-vous à ***Administration avancée*** (à la page 166) pour plus d'informations.
3. Cochez la case **Liaison anonyme** si vous souhaitez vous connecter au serveur AD sans indiquer de nom d'utilisateur et de mot de passe. Dans ce cas, vérifiez si le serveur AD autorise les requêtes anonymes.

Remarque : par défaut, Windows 2003 N'AUTORISE PAS les requêtes anonymes. Les serveurs Windows 2000 autorisent certaines opérations anonymes dont les résultats de requête sont basés sur les autorisations affectées à chaque objet.

4. Si vous n'utilisez pas de liaison anonyme, entrez le nom d'utilisateur du compte utilisateur à l'aide duquel vous souhaitez interroger le serveur AD dans le champ **Nom d'utilisateur**. Le format requis dépend de la version et de la configuration d'AD. Utilisez l'un des formats suivants :

   Un utilisateur nommé User Name dont le nom de connexion est UserN dans le domaine raritan.com sera entré comme suit :

   - cn=UserName,cn=users,dc=Raritan,dc=com
   - **UserName@raritan.com**
   - Raritan/UserName

   Remarque : l'utilisateur défini doit être autorisé à exécuter des requêtes de recherche dans le domaine AD. Par exemple, l'utilisateur doit appartenir à un groupe dans AD dont l'option **Group scope** (portée de groupe) est paramétrée sur **Global** et l'option **Group type** (type de groupe) sur **Security** (sécurité).

5. Entrez le mot de passe du compte utilisateur à employer pour interroger le serveur AD dans les champs **Mot de passe** et **Confirmer le mot de passe**.
6. Cliquez sur **Tester la connexion** pour tester la connexion au serveur AD à l'aide des paramètres fournis. Un message doit s'afficher pour confirmer la réussite de la connexion. Si aucune confirmation ne s'affiche, vérifiez soigneusement les paramètres et essayez à nouveau.
7. Cliquez sur **Suivant** pour continuer. L'onglet **Options avancées** s'ouvre.

Paramètres avancés AD

➢ *Pour configurer les paramètres AD avancés :*

1. Cliquez sur l'onglet Options avancées.
2. Entrez le numéro du port d'écoute du serveur AD. Le port par défaut est **389**. Si vous utilisez des connexions sécurisées pour LDAP (étape 3, ci-après), vous aurez peut-être à modifier ce port. Le port standard des connexions LDAP sécurisées est **636**.

Raritan.
When you're ready to take control®

3. Cochez la case **Connexion sécurisée pour LDAP** afin d'utiliser un canal sécurisé pour la connexion. Lorsque cette case est cochée, CC-SG utilise LDAP sur SSL pour se connecter à AD. Il est possible que cette option ne soit pas prise en charge par votre configuration AD.
4. Spécifiez le **ND de base** (au niveau de l'annuaire) sur lequel la requête de recherche sera exécutée pour l'authentification. CC-SG peut effectuer une recherche récurrente vers le bas à partir de ce ND de base.

Exemple	Description
dc=raritan,dc=com	La requête de recherche de l'entrée utilisateur est exécutée sur toute la structure de répertoires.
cn=Administrators,cn=Users,dc=raritan,dc=com	La requête de recherche de l'entrée utilisateur est exécutée uniquement dans le sous-répertoire Administrators (entrée).

5. Entrez les attributs de l'utilisateur dans le champ **Filtre** afin de limiter la recherche exclusivement aux entrées répondant à ces critères. Le filtre par défaut est **objectclass=user**, ce qui signifie que seules les entrées de type **user** (utilisateur) sont recherchées.
6. Spécifiez le mode d'exécution de la requête de recherche.
   - Cochez la case **Utiliser la liaison** si l'utilisateur se connectant à partir de l'applet est autorisé à effectuer des requêtes de recherche sur le serveur AD. Toutefois, si un modèle de nom d'utilisateur est indiqué dans le champ **Lier le modèle de nom d'utilisateur**, il doit être fusionné au nom d'utilisateur fourni dans l'applet. Le résultat est utilisé pour la connexion au serveur AD.

     Exemple : si vous avez **cn={0},cn=Users,dc=raritan,dc=com** et que **TestUser** a été indiqué dans l'applet, CC-SG utilise alors **cn=TestUser,cn-Users,dc=raritan,dc=com** pour la connexion au serveur AD.

- Cochez la case **Utiliser la liaison après une recherche** afin d'employer le nom d'utilisateur et le mot de passe spécifiés dans l'onglet **Généralités** pour la connexion au serveur AD. L'entrée est recherchée dans le ND de base et trouvée si elle répond aux critères de filtrage indiqués et si l'attribut « samAccountName » est égal au nom d'utilisateur entré dans l'applet. Une seconde tentative de connexion, ou liaison, est alors effectuée à l'aide du nom d'utilisateur et du mot de passe fournis dans l'applet. Cette seconde liaison assure que l'utilisateur a indiqué le mot de passe correct.

7. Cliquez sur **Suivant** pour continuer. L'onglet **Groupes** s'ouvre.

Paramètres de groupe AD

Dans l'onglet Groupes, vous pouvez définir la provenance exacte des groupes d'utilisateurs AD à importer.

Important : vous devez définir les paramètres de groupe avant d'importer des groupes du serveur AD.

1. Cliquez sur l'onglet **Groupes**.
2. Spécifiez le **ND de base** (au niveau du répertoire) utilisé pour rechercher les groupes contenant l'utilisateur à autoriser.

Exemple	Description
dc=raritan,dc=com	La requête de recherche de l'utilisateur dans le groupe est exécutée sur toute la structure de répertoires.
cn=Administrators,cn=Users,dc=raritan,dc=com	La requête de recherche de l'utilisateur dans le groupe est exécutée uniquement dans le sous-répertoire Administrators (entrée).

3. Entrez les attributs de l'utilisateur dans le champ **Filtre** afin de limiter la recherche de l'utilisateur du groupe exclusivement aux entrées répondant à ces critères.

   Par exemple, si vous indiquez le ND de base **cn=Groups,dc=raritan,dc=com** et le filtre **(objectclass=group)**, toutes les entrées de l'entrée **Groups** de type **group** sont retournées.

4. Cliquez sur **Suivant** pour continuer. L'onglet **Trusts** (approbations) s'ouvre.

Paramètres d'approbation AD

Dans l'onglet Trusts, vous pouvez définir des relations de confiance entre des domaines existants et le nouveau domaine AD. De telles relations rendent les ressources accessibles aux utilisateurs authentifiés dans plusieurs domaines. Ces relations peuvent être entrantes, sortantes, bidirectionnelles ou désactivées. Il vous faut définir des relations d'approbation si vous souhaitez que des modules AD représentant des forêts différentes dans AD aient accès aux données de chacun. Les approbations configurées dans CC-SG doivent correspondre à celles configurées dans AD.

1. Cliquez sur l'onglet **Trusts** (approbations). Si vous avez configuré plusieurs domaines AD, tous les autres domaines sont affichés dans l'onglet **Trusts**.
2. Pour chaque domaine de la colonne **Trust Partner** (partenaire approuvé), cliquez sur le menu déroulant **Trust Direction** (direction de l'approbation), puis sélectionnez le sens de l'approbation que vous souhaitez établir entre les domaines. Les directions d'approbation sont mises à jour dans tous les modules AD lorsque vous modifiez l'un d'entre eux.
   - **Incoming** (entrante) : les données provenant du domaine sont approuvées. Dans la figure ci-dessus, le module AD 2 accepte les données provenant du module AD 1.
   - **Outgoing** (sortante) : les données arrivant dans le domaine sélectionné sont approuvées. Dans la figure ci-dessus, le module AD 1 accepte les données provenant du module AD 2.
   - **Bidirectional** (bidirectionnelle) : les données sont approuvées dans les deux sens par chaque domaine.
   - **Disabled** (désactivée) : les données ne sont pas échangées entre les domaines.
3. Cliquez sur **Appliquer** pour enregistrer vos modifications, puis cliquez sur **OK** pour enregistrer le module AD et quitter la fenêtre.

   Le nouveau module AD apparaît dans l'écran Gestionnaire de sécurité, sous External AA Servers (serveurs AA externes).
4. Cochez la case **Authentification** si vous souhaitez que CC-SG utilise le module AD pour l'authentification des utilisateurs. Cochez la case **Authentification** si vous souhaitez que CC-SG utilise le module AD pour l'authentification des utilisateurs.
5. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Modification d'un module AD

Une fois les modules AD configurés, vous pouvez les modifier à tout moment.

➢ *Pour modifier un module AD :*

1. Choisissez Administration > Sécurité.
2. Choisissez l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification externes configurés s'affichent dans une table.
3. Sélectionnez le module AD que vous souhaitez modifier, puis cliquez sur **Modifier**.
4. Cliquez sur chaque onglet de la fenêtre Modifier un module pour visualiser les paramètres configurés. Effectuez les changements nécessaires. Reportez-vous à ***Paramètres généraux AD*** (à la page 123), ***Paramètres avancés AD*** (à la page 124), ***Paramètres de groupe AD*** (à la page 126) et ***Paramètres d'approbation AD*** (à la page 127) pour plus d'informations.
5. Si vous modifiez les données de connexion, cliquez sur **Tester la connexion** afin de tester la connexion au serveur AD à l'aide des paramètres définis. Un message doit s'afficher pour confirmer la réussite de la connexion. Si aucune confirmation ne s'affiche, vérifiez soigneusement les paramètres et essayez à nouveau.
6. Cliquez sur **OK** pour enregistrer les modifications.
7. Vous devez synchroniser les groupes d'utilisateurs AD que vous avez modifiés. Vous pouvez également synchroniser tous les modules AD pour synchroniser tous leurs groupes et utilisateurs. Reportez-vous à ***Synchronisation des groupes d'utilisateurs AD*** (voir "Synchroniser tous les groupes d'utilisateurs avec AD" à la page 131) et ***Synchronisation de tous les modules AD*** (voir "Synchroniser tous les modules AD" à la page 132) pour plus d'informations.

Raritan.
When you're ready to take control®

Importation des groupes d'utilisateurs AD

Vous devez définir des paramètres de groupe dans le module AD avant d'importer des groupes du serveur AD. Reportez-vous à ***Paramètres de groupe AD*** (à la page 126).

Après avoir changé des groupes ou utilisateurs importés, vous devez synchroniser les groupes d'utilisateurs AD modifiés pour mapper les groupes importés aux groupes appropriés sur AD, et synchroniser tous les modules AD pour en synchroniser tous les groupes et utilisateurs. Reportez-vous à ***Synchronisation des groupes d'utilisateurs AD*** (voir "Synchroniser tous les groupes d'utilisateurs avec AD" à la page 131) et ***Synchronisation de tous les modules AD*** (voir "Synchroniser tous les modules AD" à la page 132) pour plus d'informations.

Vous pouvez importer les groupes imbriqués depuis AD.

Remarque : *assurez-vous que le serveur de noms de domaine CC-SG et le suffixe de domaine sont configurés dans le Gestionnaire de configuration avant d'importer des groupes d'utilisateurs AD.* **Administration avancée** *(à la page 166)*

➢ *Pour importer des groupes d'utilisateurs AD :*

1. Choisissez Administration > Sécurité.
2. Choisissez l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés s'affichent dans une table.
3. Sélectionnez le serveur AD dont vous souhaitez importer les groupes d'utilisateurs AD.
4. Cliquez sur **Importer les groupes d'utilisateurs AD** pour extraire une liste de valeurs de groupes d'utilisateurs stockées sur le serveur AD. Si un ou plusieurs des groupes d'utilisateurs ne sont pas encore sur l'unité CC-SG, vous pouvez les importer ici et leur affecter une stratégie d'accès.
5. Sélectionnez les groupes à importer dans CC-SG.
   - Le nom des groupes d'utilisateurs importés peut comporter jusqu'à 64 caractères.
   - Pour rechercher des groupes d'utilisateurs, entrez une chaîne de recherche dans le champ **Search for User Group** (rechercher un groupe d'utilisateurs), puis cliquez sur **Aller à**.
   - Cliquez sur un en-tête de colonne pour trier la liste des groupes d'utilisateurs selon les données de cette colonne.

- Cliquez sur **Sélectionner tout** pour choisir tous les groupes pour l'importation.
- Cliquez sur **Désélectionner tout** pour désélectionner tous les groupes d'utilisateurs choisis.

6. Dans la colonne **Stratégies**, sélectionnez une stratégie d'accès CC-SG dans la liste pour l'affecter au groupe sélectionné.
7. Cliquez sur **Importer** pour importer les groupes d'utilisateurs sélectionnés.

*Conseil : pour vérifier si le groupe a bien été importé et afficher les droits dont disposent ses membres, cliquez sur l'onglet **Utilisateurs**, puis sélectionnez le groupe en question pour ouvrir l'écran Profil du groupe d'utilisateurs. Vérifiez les informations des onglets **Droits d'administrateur** et **Stratégies de dispositif/nœud**. Cliquez sur l'onglet **Active Directory Associations** (associations Active Directory) pour consulter les informations relatives au module AD associé au groupe d'utilisateurs.*

Synchronisation d'AD avec CC-SG

Il existe plusieurs méthodes pour synchroniser les données que compte CC-SG avec votre serveur AD.

- Synchronisation quotidienne de tous les modules : vous pouvez activer la synchronisation programmée pour permettre à CC-SG de synchroniser quotidiennement tous les modules AD à l'heure que vous choisissez. Reportez-vous à ***Synchronisation de tous les modules AD*** (voir "Synchroniser tous les modules AD" à la page 132). Cette synchronisation n'est nécessaire que si vous utilisez AD pour l'autorisation.
- Synchronisation sur demande : vous pouvez exécuter deux types de synchronisation à tout moment.
  1. ***Tous les modules du répertoire actif*** (voir "Synchroniser tous les modules AD" à la page 132) : cette option effectue la même opération que la synchronisation quotidienne de tous les modules, mais vous pouvez l'utiliser pour synchroniser à tout moment sur demande. Cette synchronisation n'est nécessaire que si vous utilisez AD pour l'autorisation.

2. ***Tous les groupes d'utilisateurs*** (voir "Synchroniser tous les groupes d'utilisateurs avec AD" à la page 131) : utilisez cette option lorsque vous avez modifié un groupe d'utilisateurs. La synchronisation de tous les groupes d'utilisateurs vous permet de mapper des groupes d'utilisateurs importés et locaux à des groupes identifiés dans un module AD. La synchronisation des groupes d'utilisateurs ne met pas à jour les données d'accès dans CC-SG. Vous devez synchroniser tous les modules AD, en attendant l'exécution de la synchronisation quotidienne ou en exécutant la synchronisation sur demande de tous les modules, pour mettre à jour les données d'accès.

Synchroniser tous les groupes d'utilisateurs avec AD

Il est recommandé de synchroniser tous les groupes d'utilisateurs si vous avez modifié un groupe. Par exemple, si vous savez qu'un groupe d'utilisateurs a été déplacé d'un module AD à un autre. (Vous pouvez également modifier l'association AD d'un groupe d'utilisateurs manuellement, dans Profil du groupe d'utilisateurs, onglet Active Directory Associations.)

Si vous avez apporté des changements aux utilisateurs ou aux contrôleurs de domaine, ***synchronisez tous les modules AD*** (voir "Synchroniser tous les modules AD" à la page 132).

Lorsque vous synchronisez des groupes d'utilisateurs AD, CC-SG extrait les groupes pour le module AD sélectionné, compare leurs noms aux groupes d'utilisateurs déjà importés d'AD, puis identifie les paires identiques. CC-SG présente ces dernières et vous permet de sélectionner les groupes AD à associer à CC-SG. Les données d'accès dans CC-SG ne sont pas mises à jour. La synchronisation des groupes d'utilisateurs AD n'effectue que le mappage des noms de groupes d'AD à CC-SG.

➢ *Pour synchroniser tous les groupes d'utilisateurs avec AD :*

1. ***Entrez en mode de maintenance*** (voir "Entrer en mode de maintenance" à la page 156).
2. Choisissez Administration > Sécurité.
3. Choisissez l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés s'affichent dans une table.
4. Sélectionnez le serveur AD dont vous souhaitez synchroniser les groupes d'utilisateurs avec ceux de CC-SG.
5. Dans la liste Synchronisation sur demande, sélectionnez Tous les groupes d'utilisateurs, puis cliquez sur le bouton fléché.

6. La liste de tous les groupes d'utilisateurs figurant dans le module AD dont les noms correspondent à des groupes de CC-SG apparaît. Sélectionnez les groupes d'utilisateurs à synchroniser, puis cliquez sur OK.
7. Un message de confirmation s'affiche lorsque tous les groupes d'utilisateurs importés dans le module sélectionné sont synchronisés.
8. ***Quittez le mode de maintenance*** (voir "Quitter le mode de maintenance" à la page 156).

Synchroniser tous les modules AD

Il est recommandé de synchroniser tous les modules AD chaque fois que vous modifiez ou supprimez un utilisateur dans AD, modifiez des autorisations d'utilisateur dans AD ou apportez des changements à un contrôleur de domaine.

Lorsque vous synchronisez tous les modules AD, CC-SG extrait les groupes d'utilisateurs de tous les modules AD configurés, compare leurs noms aux groupes d'utilisateurs importés dans CC-SG ou associés au module AD dans CC-SG, puis rafraîchit la mémoire cache locale de CC-SG. Cette dernière contient tous les contrôleurs de chaque domaine, les groupes d'utilisateurs associés aux modules dans CC-SG et les données de tous les utilisateurs AD connus. Si des groupes d'utilisateurs ont été supprimés des modules AD, CC-SG retire également toutes les associations à ces groupes de sa mémoire cache locale. Ainsi, CC-SG dispose des données de groupes d'utilisateurs AD les plus récentes.

➢ *Pour synchroniser tous les modules AD :*

1. ***Entrez en mode de maintenance*** (voir "Entrer en mode de maintenance" à la page 156).
2. Choisissez **Administration** > **Sécurité**.
3. Choisissez l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés s'affichent dans une table.
4. Dans la liste Synchronisation sur demande, sélectionnez Tous les modules du répertoire actif, puis cliquez sur le bouton fléché. Un message de confirmation apparaît lorsque tous les modules AD sont synchronisés.
5. ***Quittez le mode de maintenance*** (voir "Quitter le mode de maintenance" à la page 156).

Activer ou désactiver la synchronisation quotidienne de tous les modules AD

➢ *Pour activer la synchronisation quotidienne de tous les modules AD :*

1. Choisissez **Administration** > **Sécurité**.
2. Choisissez l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés s'affichent dans une table.
3. Cochez la case Synchronisation quotidienne de tous les modules.
4. Dans le champ **Durée de synchronisation**, cliquez sur les flèches haut et bas pour sélectionner l'heure à laquelle CC-SG doit effectuer la synchronisation quotidienne de tous les modules AD.
5. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

➢ *Pour désactiver la synchronisation quotidienne de tous les modules AD :*

1. Choisissez **Administration** > **Sécurité**.
2. Choisissez l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés s'affichent dans une table.
3. Désactivez la case Synchronisation quotidienne de tous les modules.
4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Modifier l'heure de synchronisation AD quotidienne

Lorsque la synchronisation quotidienne est activée, vous pouvez indiquer l'heure à laquelle l'opération a lieu automatiquement. Par défaut, elle se produit à 23 h 30.

➢ *Pour modifier l'heure de synchronisation AD quotidienne :*

1. Choisissez **Administration** > **Sécurité**.
2. Choisissez l'onglet Authentification. Assurez-vous que la case Synchronisation quotidienne de tous les modules est cochée.
3. Dans le champ **Durée de synchronisation** au bas de l'écran, cliquez sur les flèches haut et bas pour sélectionner l'heure à laquelle CC-SG doit effectuer la synchronisation quotidienne de tous les modules AD.
4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

A propos de LDAP et de CC-SG

Une fois CC-SG lancé et le nom d'utilisateur et le mot de passe saisis, une requête est transmise directement au serveur LDAP ou par l''intermédiaire de CC-SG. Si le nom d'utilisateur et le mot de passe correspondent à ceux figurant dans le répertoire LDAP, l'utilisateur est authentifié. Les autorisations de l'utilisateur sont alors vérifiées à l'aide des groupes d'utilisateurs locaux sur le serveur LDAP.

Ajout d'un module LDAP (Netscape) dans CC-SG

➢ *Pour ajouter un module LDAP (Netscape) dans CC-SG :*

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet Authentification.
3. Cliquez sur **Ajouter…** pour ouvrir la fenêtre Ajouter un module.
4. Cliquez sur le menu déroulant **Type de module** et sélectionnez LDAP dans la liste.
5. Entrez le nom du serveur LDAP dans le champ **Nom du module**.
6. Cliquez sur **Suivant** pour continuer. L'onglet **Généralités** s'ouvre.

Paramètres généraux LDAP

1. Cliquez sur l'onglet **Généralités**.
2. Entrez l'adresse IP ou le nom d'hôte du serveur LDAP dans le champ **Adresse IP/nom d'hôte**. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2).
3. Tapez la valeur du port dans le champ **Port**. Le port par défaut est 389.
4. Cochez la case **Connexion sécurisée pour LDAP** si vous utilisez un serveur LDAP sécurisé.
5. Cochez la case **Liaison anonyme** si votre serveur LDAP autorise les requêtes anonymes. Dans ce cas, vous n'avez à entrer ni nom d'utilisateur ni mot de passe.

Remarque : par défaut, Windows 2003 N'AUTORISE PAS les requêtes anonymes. Les serveurs Windows 2000 autorisent certaines opérations anonymes dont les résultats de requête sont basés sur les autorisations affectées à chaque objet.

6. Si vous n'utilisez pas de liaison anonyme, renseignez le champ **Nom d'utilisateur**. Entrez un nom distinct (ND) afin d'indiquer les références de connexion utilisées pour interroger le serveur LDAP. Pour former le ND, entrez le nom courant, l'unité organisationnelle et le domaine. Par exemple, tapez **uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot**. Séparez les valeurs par des virgules, mais n'utilisez aucun espace avant ou après la virgule. La valeur peut inclure des espaces, par exemple **Command Center**.
7. Entrez le mot de passe dans les champs **Mot de passe** et **Confirmer le mot de passe**.
8. Pour indiquer l'emplacement de départ de la recherche des utilisateurs, entrez un nom distinct dans le champ **ND de base**. Par exemple, les critères **ou=Administrators,ou=TopologyManagement,o=NetscapeRoot** inspectent toutes les unités organisationnelles sous le domaine.
9. Pour limiter la recherche à des types particuliers d'objets, renseignez le champ **Filtre**. Par exemple, le critère **(objectclass=person)** limite la recherche aux objets de personne uniquement.
10. Cliquez sur **Tester la connexion** pour effectuer un essai de connexion au serveur LDAP à l'aide des paramètres donnés. Un message doit s'afficher pour confirmer la réussite de la connexion. Dans le cas contraire, vérifiez soigneusement les paramètres et essayez à nouveau.
11. Cliquez sur **Suivant** pour passer à l'onglet **Options avancées** afin de définir des options de configuration avancées pour le serveur LDAP.

Paramètres avancés LDAP

1. Cliquez sur l'onglet **Options avancées**.
2. Sélectionnez **Base 64** pour envoyer le mot de passe au serveur LDAP avec chiffrement. Sélectionnez **Texte brut** pour envoyer le mot de passe au serveur LDAP sous forme de texte brut.
3. **Digest par défaut** : sélectionnez le chiffrement par défaut des mots de passe utilisateur.
4. Entrez les paramètres d'attributs d'utilisateur et d'appartenance au groupe dans les champs **Attribut d'utilisateur** et **Attribut d'appartenance au groupe**. Ces valeurs doivent être issues de votre schéma de répertoires LDAP.
5. Entrez le modèle de liaison dans le champ **Lier le modèle de nom d'utilisateur**.

- Cochez **Utiliser la liaison** si vous souhaitez que CC-SG envoie le nom d'utilisateur et le mot de passe entrés lors de la connexion au serveur LDAP pour l'authentification. Si la case **Utiliser la liaison** n'est pas cochée, CC-SG recherche le nom d'utilisateur sur le serveur LDAP. S'il le trouve, il récupère l'objet LDAP et compare localement le mot de passe associé à celui entré.
- Sur certains serveurs LDAP, le mot de passe ne peut pas être récupéré dans le cadre de l'objet LDAP. Cochez la case **Utiliser la liaison après une recherche** pour indiquer à CC-SG de lier de nouveau le mot de passe à l'objet LDAP et le renvoyer au serveur pour authentification.

6. Cliquez sur **OK** pour enregistrer les modifications. Le nouveau module LDAP apparaît dans l'écran Gestionnaire de sécurité, sous External AA Servers (serveurs AA externes).
7. Cochez la case **Authentification** si vous souhaitez que CC-SG utilise le module LDAP pour l'authentification des utilisateurs.
8. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Paramètres de configuration Sun One LDAP (iPlanet)

Si vous utilisez un serveur Sun One LDAP pour l'authentification à distance, utilisez cet exemple de paramètres :

Nom du paramètre	Paramètres SUN One LDAP
Adresse IP/nom d'hôte	**<Adresse IP du serveur de répertoires>**
Nom d'utilisateur	**CN=<ID utilisateur valide>**
Mot de passe	**<Mot de passe>**
ND de base	**O=<Organisation>**
Filtre	**(objectclass=person)**
Mots de passe (écran Options avancées)	**Texte brut**
Mot de passe (Digest par défaut) (Options avancées)	**SHA**
Utiliser la liaison	**non coché**
Utiliser la liaison après une recherche	**coché**

Paramètres de configuration OpenLDAP (eDirectory)

Si vous utilisez un serveur OpenLDAP pour l'authentification à distance, utilisez cet exemple :

Nom du paramètre	Paramètres Open LDAP
Adresse IP/nom d'hôte	<Adresse IP du serveur de répertoires>
Nom d'utilisateur	CN=<ID utilisateur valide>, O=<Organisation>
Mot de passe	<Mot de passe>
Base utilisateur	O=accounts, O=<Organisation>
Filtre utilisateur	(objectclass=person)
Mots de passe (écran Options avancées)	Base64
Mot de passe (Digest par défaut) (Options avancées)	crypté
Utiliser la liaison	non coché
Utiliser la liaison après une recherche	coché

A propos de TACACS+ et de CC-SG

Les utilisateurs CC-SG authentifiés à distance par un serveur TACACS+ doivent être créés sur le serveur TACACS+ et sur l'unité CC-SG. Les noms d'utilisateur doivent être identiques sur le serveur TACACS+ et sur CC-SG, même si les mots de passe peuvent être différents. Reportez-vous à ***Utilisateurs et groupes d'utilisateurs*** (à la page 88) pour plus d'informations.

Ajout d'un module TACACS+

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet Authentification.
3. Cliquez sur **Ajouter** pour ouvrir la fenêtre Ajouter un module.
4. Choisissez le **type de module**> TACACS+.

5. Entrez le nom du serveur TACACS+ dans le champ **Nom du module**.
6. Cliquez sur **Suivant**. L'onglet **Généralités** s'ouvre.

Paramètres généraux TACACS+

1. Entrez l'adresse IP ou le nom d'hôte du serveur TACACS+ dans le champ **Adresse IP/nom d'hôte**. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2).
2. Entrez le numéro du port d'écoute du serveur TACACS+ dans le champ **Numéro de port**. Le numéro de port par défaut est **49**.
3. Entrez le port d'authentification dans le champ **Port d'authentification**.
4. Renseignez les champs **Clé partagée** et **Confirmez la clé partagée**.
5. Cliquez sur **OK** pour enregistrer les modifications. Le nouveau module TACACS+ apparaît dans l'écran Gestionnaire de sécurité, sous External AA Servers (serveurs AA externes).
6. Cochez la case **Authentification** si vous souhaitez que CC-SG utilise le module TACACS+ pour l'authentification des utilisateurs.
7. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

A propos de RADIUS et de CC-SG

Les utilisateurs CC-SG authentifiés à distance par un serveur RADIUS doivent être créés sur le serveur RADIUS et sur l'unité CC-SG. Les noms d'utilisateur doivent être identiques sur le serveur RADIUS et sur CC-SG, même si les mots de passe peuvent être différents. Reportez-vous à ***Utilisateurs et groupes d'utilisateurs*** (à la page 88) pour plus d'informations sur l'ajout d'utilisateurs qui seront authentifiés à distance.

Ajout d'un module RADIUS

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet Authentification.
3. Cliquez sur **Ajouter** pour ouvrir la fenêtre Ajouter un module.
4. Cliquez sur le menu déroulant **Type de module** et sélectionnez RADIUS dans la liste.
5. Entrez le nom du serveur RADIUS dans le champ **Nom du module**.

6. Cliquez sur **Suivant** pour continuer. L'onglet **Généralités** s'ouvre.

Paramètres généraux RADIUS

1. Cliquez sur l'onglet **Généralités**.
2. Entrez l'adresse IP ou le nom d'hôte du serveur RADIUS dans le champ **Adresse IP/nom d'hôte**. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2).
3. Entrez le numéro de port dans le champ **Numéro de port**. Le numéro de port par défaut est 1812.
4. Entrez le port d'authentification dans le champ **Port d'authentification**.
5. Renseignez les champs **Clé partagée** et **Confirmez la clé partagée**.
6. Cliquez sur **OK** pour enregistrer les modifications.
7. Le nouveau module RADIUS apparaît dans l'écran Gestionnaire de sécurité, sous External AA Servers (serveurs AA externes). Cochez la case **Authentification** si vous souhaitez que CC-SG utilise le module RADIUS pour l'authentification des utilisateurs.
8. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Authentification à deux facteurs à l'aide de RADIUS

Grâce à l'utilisation conjointe d'un serveur RSA RADIUS prenant en charge l'authentification à deux facteurs et d'un gestionnaire d'authentification RSA, CC-SG peut utiliser des modèles d'authentification à deux facteurs avec des jetons dynamiques.

Dans un tel environnement, l'utilisateur se connecte à CC-SG en commençant par saisir son nom d'utilisateur dans le champ correspondant. Puis l'utilisateur entre son mot de passe fixe, suivi par la valeur de jeton dynamique dans le champ **Mot de passe**.

La configuration de CC-SG est identique à l'authentification distante RADIUS standard décrite plus haut. Reportez-vous à ***Authentification à deux facteurs*** (à la page 289) pour plus d'informations.

Chapitre 13 Rapports

Dans ce chapitre

Utilisation des rapports....140
Rapport Journal d'audit....142
Rapport Journal d'erreurs....143
Rapport d'accès....144
Rapport de disponibilité....145
Rapport Utilisateurs actifs....145
Rapport Utilisateurs verrouillés....146
Rapport Données d'utilisateurs....146
Rapport Utilisateurs dans les groupes....147
Rapport Données de groupes....147
Rapport sur le groupe d'utilisateurs AD....148
Rapport Gestion du parc....148
Rapport sur le parc du nœud....149
Rapport sur les nœuds actifs....149
Rapport sur la création de nœuds....150
Rapport Interrogation des ports....150
Rapport Ports actifs....152
Rapports programmés....152
Rapport Mise à niveau du firmware d'un dispositif....153
Rapport Synchronisation CC-NOC....153

Utilisation des rapports

Trier les données d'un rapport

- Cliquez sur un en-tête pour trier les données de rapport selon les valeurs de cette colonne. Les données sont alors organisées par ordre alphabétique, numérique ou chronologique croissant.
- Cliquez de nouveau sur l'en-tête de colonne pour trier les données par ordre décroissant.

Redimensionner la largeur des colonnes d'un rapport

Les largeurs de colonne choisies deviennent la vue par défaut du rapport à la connexion et à l'exécution de rapports suivantes.

1. Maintenez le pointeur de la souris sur le séparateur de colonnes dans la zone des en-têtes de colonne jusqu'à ce qu'il prenne la forme d'une double flèche.

2. Cliquez et faites glisser la flèche vers la gauche ou la droite pour changer la largeur des colonnes.

Afficher les détails d'un rapport

- Double-cliquez sur une ligne pour afficher les détails du rapport.
- Lorsqu'une ligne est en surbrillance, appuyez sur ENTREE pour afficher les détails.

Parcourir des rapports de plusieurs pages

- Cliquez sur les icônes de flèche au bas du rapport pour parcourir les pages du rapport.

Imprimer l'affichage d'un rapport

Vous pouvez imprimer le rapport tel qu'il apparaît à l'écran. Pour imprimer tous les détails du rapport, ***enregistrez le rapport dans un fichier*** (voir "Enregistrer un rapport dans un fichier" à la page 141), puis imprimez le fichier.

1. Générez le rapport à imprimer.
2. Choisissez Passerelle sécurisée > Imprimer.

Enregistrer un rapport dans un fichier

Vous pouvez enregistrer un rapport dans un fichier .CSV, qui peut être ouvert dans Excel. Lorsque vous enregistrez un rapport dans un fichier, tous ses détails sont sauvegardés et non uniquement ceux affichés à l'écran.

1. Générez le rapport que vous souhaitez enregistrer dans un fichier.
2. Cliquez sur Enregistrer dans le fichier. (Ou, cliquez sur Gérer les données du rapport, puis sur Enregistrer.)
3. Entrez le nom du fichier et choisissez l'emplacement où vous souhaitez l'enregistrer.
4. Cliquez sur Enregistrer.

Purger les données d'un rapport de CC-SG

Vous pouvez purger les enregistrements consignés dans les rapports Journal d'audit et Journal d'erreurs. La purge de ces rapports suppriment définitivement toutes les données présentes dans le journal d'audit ou le journal d'erreurs.

1. Générez le rapport dont vous souhaitez supprimer les données de CC-SG.
2. Cliquez sur Purger.
3. Cliquez sur Oui pour confirmer.

Afficher ou masquer les filtres de rapport

En haut de l'écran de certains rapports figure un ensemble de critères de filtrage. Vous pouvez masquer la section de filtre, ce qui permet à la zone du rapport de s'étendre.

➢ *Pour afficher ou masquer les filtres de rapport :*

- Cliquez sur la barre d'outils Filtre en haut de l'écran pour masquer cette section.
- Cliquez à nouveau sur la barre d'outils Filtre pour afficher la section.

Rapport Journal d'audit

Le rapport **Journal d'audit** affiche les journaux d'audit et les accès à CC-SG. Il répertorie des opérations telles que l'ajout, la modification ou la suppression de dispositifs ou de ports, ainsi que d'autres modifications.

CC-SG conserve un journal d'audit des événements suivants :

- lancement de CC-SG
- arrêt de CC-SG
- connexion d'un utilisateur à CC-SG
- déconnexion d'un utilisateur de CC-SG
- lancement d'une connexion à un nœud

➢ *Pour générer un rapport Journal d'audit :*

1. Choisissez Rapports > Journal d'audit.

2. Définissez la période couverte par le rapport dans les champs **Date de début** et **Date de fin**. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
3. Vous pouvez limiter les données contenues dans le rapport en renseignant les champs **Message**, **Nom d'utilisateur** et **Adresse IP de l'utilisateur**. Les caractères joker sont acceptés dans ces champs.
   - Pour limiter le rapport en fonction du texte du message associé à une activité, renseignez le champ **Message**.
   - Pour limiter le rapport aux activités d'un utilisateur particulier, entrez le nom de ce dernier dans le champ **Nom d'utilisateur**.
   - Pour limiter le rapport aux activités d'une adresse IP particulière, entrez l'adresse IP de l'utilisateur dans le champ **Adresse IP de l'utilisateur**.
4. Cliquez sur Appliquer pour générer le rapport.
   - Cliquez sur **Purger (voir** "Purger les données d'un rapport de CC-SG" **à la page 142)** pour supprimer le journal d'audit.

Rapport Journal d'erreurs

CC-SG stocke les messages d'erreurs dans une série de fichiers Journal d'erreurs qui peuvent être consultés et utilisés pour faciliter le dépannage de problèmes. Le journal d'erreur contient un sous-ensemble des entrées du journal d'audit associées à une erreur.

➢ *Pour générer le rapport Journal d'erreurs :*

1. Choisissez Rapports > Journal d'erreurs.
2. Définissez la période couverte par le rapport dans les champs **Date de début** et **Date de fin**. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
3. Vous pouvez limiter les données contenues dans le rapport en renseignant les champs **Message**, **Nom d'utilisateur** et **Adresse IP de l'utilisateur**. Les caractères joker sont acceptés dans ces champs.
   - Pour limiter le rapport en fonction du texte du message associé à une activité, renseignez le champ **Message**.
   - Pour limiter le rapport aux activités d'un utilisateur particulier, entrez le nom de ce dernier dans le champ **Nom d'utilisateur**.

- Pour limiter le rapport aux activités d'une adresse IP particulière, entrez l'adresse IP de l'utilisateur dans le champ **Adresse IP de l'utilisateur**.

4. Cliquez sur Appliquer pour générer le rapport.
   - Cliquez sur ***Purger*** (voir "Purger les données d'un rapport de CC-SG" à la page 142) pour supprimer le journal d'erreurs.

Rapport d'accès

Le rapport d'accès permet de consulter les informations relatives aux dispositifs et ports utilisés (à quel moment et par quel utilisateur).

➢ *Pour générer le rapport d'accès :*

1. Choisissez Rapports > Rapport d'accès.
2. Sélectionnez Nœuds ou Dispositifs.
3. Définissez la période couverte par le rapport dans les champs **Date de début** et **Date de fin**. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
4. Vous pouvez limiter les données contenues dans le rapport en renseignant les champs **Nom du dispositif**, **Nom de nœud**, **Nom d'utilisateur** et **Adresse IP de l'utilisateur**.
   - Pour limiter le rapport à un dispositif particulier, renseignez le champ **Nom du dispositif**.
   - Pour limiter le rapport à un nœud particulier, renseignez le champ **Nom de nœud**.
   - Pour limiter le rapport aux activités d'un utilisateur particulier, entrez le nom de ce dernier dans le champ **Nom d'utilisateur**.
   - Pour limiter le rapport aux activités d'une adresse IP particulière, entrez l'adresse IP de l'utilisateur dans le champ **Adresse IP de l'utilisateur**.
5. Dans le champ Entrées à afficher, sélectionnez le nombre d'entrées à afficher dans l'écran du rapport.
6. Cliquez sur Appliquer pour générer le rapport.

Rapport de disponibilité

Le rapport de disponibilité affiche l'état de toutes les connexions à des dispositifs ou nœuds. Ce rapport vous donne les informations de disponibilité complètes de tous les dispositifs ou nœuds de votre réseau géré CC-SG. Les informations figurant dans le rapport sont les suivantes :

➢ *Pour générer le rapport de disponibilité :*

1. Choisissez Rapports > Rapport de disponibilité.
2. Sélectionnez l'option Nœuds ou Dispositifs.
3. Cliquez sur Appliquer.

Rapport Utilisateurs actifs

Le rapport Utilisateurs actifs affiche les utilisateurs actifs et les sessions utilisateur en cours. Vous pouvez sélectionner des utilisateurs actifs dans le rapport et les déconnecter de CC-SG.

➢ *Pour générer le rapport Utilisateurs actifs :*

- Choisissez Rapports > Utilisateurs > Utilisateurs actifs.

➢ *Pour déconnecter un utilisateur d'une session active dans CC-SG :*

1. Dans le rapport Utilisateurs actifs, sélectionnez le nom de l'utilisateur à déconnecter.
2. Cliquez sur **Déconnexion**.

Rapport Utilisateurs verrouillés

Le rapport Utilisateurs verrouillés affiche les utilisateurs actuellement verrouillés de CC-SG en raison d'un trop grand nombre de tentatives de connexion ayant échoué. Vous pouvez les déverrouiller à partir de ce rapport. ***Paramètres de verrouillage*** (à la page 196)

➢ *Pour générer le rapport Utilisateurs verrouillés :*

- Choisissez Rapports > Utilisateurs > Utilisateurs verrouillés.

➢ *Pour déverrouiller l'accès d'un utilisateur à CC-SG :*

- Sélectionnez le nom de l'utilisateur à déverrouiller, puis cliquez sur **Déverrouiller l'utilisateur**.

Rapport Données d'utilisateurs

Le rapport Données d'utilisateurs affiche certaines données relatives à tous les utilisateurs de la base de données CC-SG.

➢ *Pour générer le rapport Données d'utilisateurs :*

- Choisissez Rapports > Utilisateurs > Données d'utilisateurs.
  - Le champ **Nom d'utilisateur** affiche le nom d'utilisateur de tous les utilisateurs de CC-SG.
  - Le champ **Téléphone** affiche le numéro de rappel automatique de l'utilisateur. Cette option est disponible uniquement pour les utilisateurs de systèmes CC-SG G1 avec modem.
  - Le champ **Activé** affiche **vrai** si l'utilisateur peut se connecter à CC-SG, **faux** dans le cas contraire, suivant que la case **Connexion activée** est cochée ou non dans le profil utilisateur. Reportez-vous à ***Ajout d'un utilisateur*** (à la page 94) pour plus d'informations.
  - The Le champ **Expiration du mot de passe** affiche le nombre de jours pendant lesquels l'utilisateur peut conserver le même mot de passe avant d'être forcé de le changer. Reportez-vous à ***Ajout d'un utilisateur*** (à la page 94) pour plus d'informations.
  - Le champ **Groupes** affiche les groupes auxquels l'utilisateur appartient.

- Le champ **Droits d'administrateur** affiche les privilèges CC-SG attribués à l'utilisateur. Reportez-vous à l'***annexe C : Privilèges de groupe d'utilisateurs*** (voir "Privilèges de groupe d'utilisateurs" à la page 273) pour plus d'informations.
- Le champ **E-mail** affiche l'adresse électronique de l'utilisateur définie dans le profil utilisateur.
- Le champ **Type d'utilisateur** indique **local** ou **distant**, suivant la méthode d'accès de l'utilisateur.

Rapport Utilisateurs dans les groupes

Le rapport Utilisateurs dans les groupes affiche les données relatives aux utilisateurs et aux groupes auxquels ils sont associés.

➢ *Pour générer le rapport Utilisateurs dans les groupes :*

- Choisissez Rapports > Utilisateurs > Utilisateurs dans les groupes.
- Double-cliquez sur le groupe d'utilisateurs pour afficher les stratégies affectées.

Rapport Données de groupes

Le rapport Groupes affiche des informations relatives aux groupes d'utilisateurs, de nœuds et de dispositifs. Vous pouvez afficher les groupes d'utilisateurs par nom et par description, les groupes de nœuds et les groupes de dispositifs par nom, le tout dans le même écran.

➢ *Pour générer le rapport Données de groupes :*

- Choisissez Rapports > Utilisateurs > Données de groupes.
  - Cliquez sur le bouton … en regard d'une ligne pour afficher les stratégies associées au groupe d'utilisateurs, la liste des nœuds répondant à la règle de groupe de nœuds ou la liste de dispositifs répondant à la règle de groupe de dispositifs.

Rapport sur le groupe d'utilisateurs AD

Le rapport sur les groupes d'utilisateurs AD présente tous les utilisateurs des groupes importés dans CC-SG à partir de serveurs Active Directory configurés pour l'authentification et pour l'autorisation. Il ne répertorie pas les utilisateurs ajoutés localement, via CC-SG, aux groupes d'utilisateurs AD.

➢ *Pour générer le rapport sur le groupe des utilisateurs AD :*

1. Choisissez Rapports > Répertoire actif > Rapport sur le groupe d'utilisateurs AD.
2. La liste **Serveur AD** répertorie tous les serveurs AD configurés sur CC-SG pour l'authentification et l'autorisation. Cochez la case correspondant à chaque serveur AD que CC-SG doit inclure dans le rapport.
3. Dans la section **Groupes d'utilisateurs AD**, la liste **Disponible** présente tous les groupes d'utilisateurs importés dans CC-SG à partir des serveurs AD cochés dans la liste **Serveur AD**. Sélectionnez les groupes d'utilisateurs à inclure dans le rapport, puis cliquez sur **Ajouter** pour les déplacer vers la liste **Sélectionné**.
4. Cliquez sur **Appliquer** pour générer le rapport.

Rapport Gestion du parc

Le rapport **Gestion du parc** affiche des données relatives aux dispositifs gérés actuellement par CC-SG.

➢ *Pour générer le rapport Gestion du parc :*

1. Choisissez Rapports > Dispositifs > Rapport Gestion du parc. Le rapport **Gestion du parc** est généré pour tous les dispositifs.
   - Pour filtrer les données du rapport par type de dispositif, cliquez sur la flèche déroulante **Type de dispositif**, sélectionnez un type dans la liste, puis cliquez sur **Appliquer**. Le rapport est généré à nouveau à l'aide du filtre sélectionné.
   - Les dispositifs dont la version n'est pas conforme à la matrice de compatibilité sont affichés en rouge dans le champ **Nom du dispositif**.

- Cliquez sur **Actualiser** pour générer un nouveau rapport. La génération du rapport peut demander plusieurs minutes, en fonction de la taille de la configuration de votre système.

Rapport sur le parc du nœud

Le rapport sur le parc du nœud affiche les nom, nom et type d'interface, nom et type de dispositif, et groupe de tous les nœuds gérés par CC-SG. Vous pouvez également filtrer le rapport afin de n'inclure que les données relatives aux nœuds associés à un groupe, type d'interface, type de dispositif ou dispositif particulier.

➢ *Pour générer le rapport sur le parc du nœud :*

1. Choisissez Rapports > Nœuds > Rapport sur le parc du nœud.
2. Sélectionnez les critères de filtrage que vous souhaitez appliquer au rapport : Tous les nœuds, Groupe de nœuds, Groupe de dispositifs ou Dispositifs.
   - Si vous sélectionnez Groupe de nœuds, Type d'interface ou Groupe de dispositifs, cliquez sur la flèche déroulante correspondante, puis choisissez un paramètre dans la liste.
   - Si vous sélectionnez Dispositifs, choisissez dans la liste Disponible les dispositifs dont vous souhaitez inclure le parc de nœud dans le rapport, puis cliquez sur Ajouter pour les déplacer vers la liste Sélectionné.
3. Cliquez sur Appliquer pour générer le rapport. Le rapport sur le parc du nœud est généré.

Rapport sur les nœuds actifs

Le rapport sur les nœuds actifs indique les nom et type de chaque interface active, l'utilisateur actuel, un horodateur et l'adresse IP de l'utilisateur pour chaque nœud à connexion active. Vous pouvez consulter la liste des nœuds actifs et déconnecter des nœuds à partir de ce rapport.

➢ *Pour générer le rapport sur les nœuds actifs :*

1. Choisissez Rapports > Utilisateurs > Nœuds actifs. Le rapport est généré si des nœuds sont actifs.
   - Pour déconnecter un nœud à partir d'une session en cours, sélectionnez-le, puis cliquez sur **Déconnecter**.

Rapport sur la création de nœuds

Le rapport sur la création de nœuds répertorie toutes les tentatives de création de nœuds, réussies ou non, pendant une période donnée. Vous pouvez décider d'afficher toutes les tentatives de création de nœuds ou simplement les doublons potentiels.

➢ *Pour générer le rapport sur la création de nœuds :*

1. Choisissez Rapports > Utilisateurs > Création du nœud.
2. Définissez la période couverte par le rapport dans les champs Date de début et Date de fin. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
3. Sélectionnez Tous les nœuds ou Doublons potentiels pour indiquer si vous souhaitez limiter le rapport aux nœuds marqués comme doublons potentiels.
4. Cliquez sur Appliquer. Le rapport sur la création de nœuds est généré.
   - Le champ Résultat indique Success (réussite), Failed (échec) ou Potential Duplicate (doublon potentiel) pour décrire l'issue de la tentative de création de nœud.

Rapport Interrogation des ports

Le rapport Interrogation des ports affiche tous les ports en fonction de leur état.

➢ *Pour générer le rapport Interrogation des ports :*

1. Choisissez Rapports > Ports > Interrogation des ports.
2. Dans la section **Etat/Disponibilité du port**, sélectionnez les états à inclure dans le rapport. Si vous cochez plusieurs cases, les ports à tous les états sélectionnés sont inclus. Vous devez sélectionner au moins une option Disponibilité lorsque qu'une option Etat est indiquée.

Type d'état	Etat du port	Définition
	Tous	Tous les ports.
Etat :		

Type d'état	Etat du port	Définition
	Up (actif)	
	Down (inactif)	La connexion au port n'est pas possible car le dispositif est arrêté et non disponible.
Disponibilité :		
	Inactif	Le port a été configuré et la connexion au port est possible.
	Connecté	
	Occupé	Un utilisateur est connecté à ce port.
	Sous tension	
	Hors tension	
Non configuré :		
	Nouveau	Un serveur cible est connecté au port, mais ce dernier n'est pas configuré.
	Inutilisé	Aucun serveur cible n'est connecté au port qui n'est pas configuré.

3. (Facultatif) Sélectionnez **Ports fantômes** pour inclure les ports de ce type. Un port fantôme peut survenir lorsqu'un CIM ou un serveur cible est retiré du système Paragon ou mis hors tension (manuellement ou par mégarde). Reportez-vous au **manuel d'utilisation de Paragon II** pour plus d'informations.
4. (Facultatif) Sélectionnez Ports suspendus ou Ports verrouillés pour inclure les ports suspendus ou verrouillés. Les ports suspendus surviennent lorsqu'un dispositif est suspendu. Les ports verrouillés surviennent lorsqu'un dispositif est en cours de mise à niveau.
5. Dans le champ Entrées à afficher, sélectionnez le nombre de lignes de données à afficher dans l'écran du rapport.

   Remarque : cette préférence ne s'applique pas lorsque l'état est généré dans le cadre d'une tâche.

6. Cliquez sur **Appliquer** pour générer le rapport.

Rapport Ports actifs

Le rapport Ports actifs affiche les ports hors bande actuellement utilisés. Vous pouvez consulter la liste des ports actifs et déconnecter des ports à partir de ce rapport.

➢ *Pour générer le rapport Ports actifs :*

- Choisissez Rapports > Ports > Ports actifs.

➢ *Pour déconnecter un port d'une session en cours :*

- Dans le rapport Ports actifs, sélectionnez le port à déconnecter, puis cliquez sur **Déconnecter**.

Rapports programmés

L'écran Rapports programmés affiche les rapports programmés dans le Gestionnaire des tâches. Il affiche les rapports de mise à niveau du firmware d'un dispositif et de redémarrage d'un dispositif. Tous les rapports programmés peuvent être consultés au format HTML. Reportez-vous à ***Gestionnaire des tâches*** (à la page 207) pour plus d'informations.

➢ *Pour accéder aux rapports programmés :*

1. Choisissez Rapports > Rapports programmés.
2. Cliquez sur **Obtenir les rapports** pour afficher la liste complète de tous les rapports programmés créés par tous les propriétaires. Par défaut, tous les rapports programmés dans l'heure précédente sont affichés.
   - Pour visualiser un rapport, sélectionnez-le dans la liste et cliquez sur **Afficher le rapport**.
   - (Facultatif) Filtrez les rapports affichés :

   a. Entrez des paramètres.

- Sélectionnez un **type de rapport**.
- Sélectionnez un **propriétaire du rapport**.
- Modifiez les dates de début et de fin dans les champs **Rapports générés entre**.
- Entrez un **nom du rapport** pour filtrer sur le nom. Vous pouvez entrer le nom entier ou une partie du nom. Les correspondances ne respectent pas la casse. Les caractères joker ne sont pas autorisés.

b. Cliquez sur **Obtenir les rapports** pour visualiser la liste filtrée.

Rapport Mise à niveau du firmware d'un dispositif

Le rapport Mise à niveau du firmware d'un dispositif figure dans la liste Rapports programmés. Ce rapport généré lors de l'exécution d'une tâche de mise à niveau du firmware d'un dispositif. Affichez le rapport pour obtenir des informations d'état en temps réel sur la tâche. Une fois la tâche terminée, les informations du rapport sont statiques.

Reportez-vous à ***Rapports programmés*** (à la page 152) pour plus d'informations sur l'affichage des rapports.

Rapport Synchronisation CC-NOC

Le rapport Synchronisation CC-NOC répertorie toutes les cibles, ainsi que leurs adresses IP, auxquelles l'unité CC-SG est abonnée et qui sont contrôlées par une unité CC-NOC à une date de détection particulière. Les nouvelles cibles découvertes dans la plage configurée sont également affichées ici. Reportez-vous à ***Ajouter une unité CC-NOC*** (voir "Ajouter un CC-NOC" à la page 214) pour plus d'informations. Vous pouvez également purger des cibles de la base de données CC-SG à partir de ce rapport.

➢ *Pour générer le rapport Synchronisation CC-NOC :*

1. Choisissez Rapports > Synchronisation CC-NOC.
2. Sélectionnez une **dernière date détectée** et cliquez sur **Obtenir des cibles**. Les cibles découvertes à la **dernière date de détection** ou avant cette date sont affichées sous **Cibles détectées**.
   - Pour purger une cible de la base de données CC-SG, sélectionnez-la, puis cliquez sur **Purger**.
   - Pour purger la liste entière de cibles de la base de données CC-SG, cliquez sur **Effacer tout**.

Chapitre 14 Maintenance du système

Dans ce chapitre

Mode de maintenance 155
Entrer en mode de maintenance 156
Quitter le mode de maintenance 156
Sauvegarde de CC-SG 156
Enregistrement et suppression des fichiers de sauvegarde 158
Restauration de CC-SG 159
Réinitialisation de CC-SG 161
Redémarrage de CC-SG 161
Mise à niveau de CC-SG 162
Arrêt de CC-SG 163
Redémarrage de CC-SG après un arrêt 164
Mise hors tension de CC-SG 164
Fermeture d'une session CC-SG 165

Mode de maintenance

Ce mode limite l'accès à l'unité CC-SG pour permettre à un administrateur d'effectuer diverses opérations sans être interrompu ; la mise à niveau de CC-SG par exemple.

Les utilisateurs en cours, hormis l'administrateur qui a déclenché le mode de maintenance, sont avertis et déconnectés après l'expiration d'un délai configurable. En mode de maintenance, les autres administrateurs sont autorisés à se connecter à CC-SG ; en revanche, les autres utilisateurs non-administrateurs ne le peuvent pas. Un trap SNMP est généré chaque fois que l'unité CC-SG passe en mode de maintenance ou en sort.

Remarque : *le mode de maintenance n'est disponible que sur les unités CC-SG autonomes et non dans une configuration en cluster. La mise à niveau de CC-SG est désactivée jusqu'au passage en mode de maintenance.*

Tâches programmées et mode de maintenance

Les tâches programmées ne peuvent pas être exécutées lorsque CC-SG est en mode de maintenance. Reportez-vous à ***Gestionnaire des tâches*** (à la page 207) pour plus d'informations sur les tâches programmées. Lorsque l'unité CC-SG quitte le mode de maintenance, les tâches programmées sont exécutées dès que possible.

Entrer en mode de maintenance

1. Entrez en mode de maintenance :
   a. Choisissez Maintenance du système > Mode de maintenance > Entrer en mode de maintenance.
   b. Mot de passe : entrez votre mot de passe. Seuls les utilisateurs dotés du privilège CC Setup and Control peuvent accéder au mode de maintenance.
   c. Message à diffusion générale : entrez le message à afficher aux utilisateurs qui seront déconnectés de CC-SG.
   d. Entrer en mode de maintenance après (mn) : entrez le nombre de minutes, de 0 à 30, qui doivent s'écouler avant que CC-SG entre en mode de maintenance. Si vous entrez zéro, le mode de maintenance démarre immédiatement.
   e. Cliquez sur OK.
   f. Cliquez sur OK dans la boîte de dialogue de confirmation.

Quitter le mode de maintenance

1. Quittez le mode de maintenance :
   a. Choisissez Maintenance du système > Mode de maintenance > Quitter le mode de maintenance.
   b. Cliquez sur **OK** pour quitter le mode de maintenance.

   Un message s'affiche lorsque CC-SG a quitté le mode de maintenance. Tous les utilisateurs peuvent maintenant accéder normalement à CC-SG.

Sauvegarde de CC-SG

Il est recommandé d'entrer en mode de maintenance avant de sauvegarder CC-SG. Ainsi, aucune modification ne peut être apportée à la base de données au cours de la sauvegarde.

1. Choisissez **Maintenance du système** > **Sauvegarde**.
2. Renseignez le champ **Nom de la sauvegarde**.
3. (Facultatif) Entrez une brève description de cette sauvegarde dans le champ **Description**.

4. Sélectionnez un **type de sauvegarde**.
   - **Personnalisé** : permet de définir les composants à ajouter à la sauvegarde en les cochant dans la zone **Options de sauvegarde** en dessous. Cochez les options que vous souhaitez inclure dans la sauvegarde.
   - **Données** : configuration de CC-SG, configuration des dispositifs et des nœuds, et données utilisateur. (Standard)
   - **Journaux** : journaux d'erreur et rapports d'événement stockés dans CC-SG.
   - **Fichiers de firmware de CC** : fichiers de firmware stockés utilisés pour la mise à jour du serveur CC-SG.
   - **Fichiers de firmware des dispositifs** : fichiers de firmware stockés utilisés pour la mise à jour des dispositifs Raritan gérés par CC-SG.
   - **Fichiers d'application** : applications stockées utilisées par CC-SG pour connecter les utilisateurs aux nœuds.
   - **Complet** : crée une sauvegarde de la totalité des **données**, **journaux**, fichiers de firmware et **fichiers d'application** stockés dans CC-SG. Ceci produit les fichiers de sauvegarde les plus volumineux.
   - **Standard** : crée uniquement une sauvegarde des **données** critiques dans CC-SG. Cette sauvegarde inclut des données sur la configuration de CC-SG, la configuration des dispositifs et des nœuds et la configuration des utilisateurs. Ceci produit les fichiers de sauvegarde les plus petits.
5. (Facultatif) Si vous souhaitez enregistrer une copie de ce fichier de sauvegarde sur un serveur externe, cochez la case **Sauvegarde vers un site distant**.
6. Sélectionnez le **protocole** à utiliser pour la connexion à un serveur distant, **FTP** ou **SFTP**.
7. Entrez l'adresse IP ou le nom d'hôte du serveur dans le champ **Nom d'hôte**.
8. Si vous n'utilisez pas le port par défaut pour le protocole sélectionné (FTP : 21, SFTP : 22), entrez le port de communication utilisé dans le champ **Numéro de port**.
9. Entrez un nom d'utilisateur pour le serveur distant dans le champ correspondant.
10. Entrez un mot de passe pour le serveur distant dans le champ correspondant.

11. Dans le champ **Répertoire**, indiquez le répertoire utilisé pour stocker la sauvegarde sur le serveur distant. Vous devez indiquer le chemin d'accès absolu au répertoire.
12. Cliquez sur **OK**.

    Un message de confirmation apparaît à la fin de la sauvegarde. Le fichier de sauvegarde est enregistré dans le système de fichiers CC-SG et sur un serveur distant également, si cela est spécifié dans le champ **Sauvegarde vers un site distant**. Cette sauvegarde peut être restaurée ultérieurement.

Enregistrement et suppression des fichiers de sauvegarde

Vous pouvez également enregistrer et supprimer des sauvegardes stockées sur le système CC-SG à partir de l'écran **Restaurer CommandCenter**. L'enregistrement de sauvegardes vous permet de conserver une copie du fichier de sauvegarde sur un autre PC. Vous pouvez créer une archive des fichiers de sauvegarde. Les fichiers de sauvegarde enregistrés à un autre emplacement peuvent être téléchargés sur d'autres unités CC-SG, puis restaurés pour copier une configuration d'une unité CC-SG à une autre.

La suppression des sauvegardes inutiles permet un gain d'espace sur CC-SG.

Enregistrer un fichier de sauvegarde

1. Choisissez **Maintenance du système** > **Restaurer Command Center**.
2. Dans la table **Sauvegardes disponibles**, sélectionnez la sauvegarde à enregistrer sur votre PC.
3. Cliquez sur **Enregistrer dans le fichier**. Une boîte de dialogue Enregistrer apparaît.
4. Entrez le nom du fichier et choisissez l'emplacement où vous souhaitez l'enregistrer.
5. Cliquez sur Enregistrer.

   Le fichier de sauvegarde est copié à l'emplacement indiqué.

Supprimer un fichier de sauvegarde

1. Dans la table **Sauvegardes disponibles**, sélectionnez la sauvegarde à supprimer.
2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation apparaît.

3. Cliquez sur **OK** pour supprimer la sauvegarde du système CC-SG.

Restauration de CC-SG

➢ *Pour restaurer CC-SG :*

1. Choisissez **Maintenance du système** > **Restaurer**. L'écran **Restaurer CommandCenter** affiche une table de sessions de sauvegarde disponibles pour CC-SG. Cette table répertorie le type de la sauvegarde, sa date, une description, la version de CC-SG utilisée et la taille du fichier de sauvegarde.
2. (Facultatif) Pour restaurer depuis une sauvegarde stockée en dehors du système CC-SG, vous devez d'abord téléverser le fichier de sauvegarde sur CC-SG.
   a. Cliquez sur **Télécharger vers le serveur**. Un écran de dialogue Ouvrir apparaît.
   b. Recherchez le fichier de sauvegarde et sélectionnez-le dans la fenêtre de dialogue. Vous pouvez extraire le fichier de n'importe quel emplacement du réseau du client.
   c. Cliquez sur **Ouvrir** pour télécharger ce fichier sur CC-SG. Cette opération terminée, le fichier de sauvegarde apparaît dans la table **Sauvegardes disponibles**.
3. Sélectionnez la sauvegarde à restaurer dans la table **Sauvegardes disponibles**.
4. Le cas échéant, sélectionnez le type de restauration que vous souhaitez effectuer à partir de cette sauvegarde :
   - **Standard** : restaure uniquement les **données** critiques dans CC-SG. Ceci inclut des données sur la configuration de CC-SG, la configuration des dispositifs et des nœuds et la configuration des utilisateurs.
   - **Complet** : restaure la totalité des **données**, **journaux**, fichiers de firmware et **fichiers d'application** stockés dans le fichier de sauvegarde. Une sauvegarde complète doit avoir été effectuée pour ce fichier.
   - **Personnalisé** : permet de définir les composants de la sauvegarde à restaurer dans CC-SG en les cochant dans la zone **Restaurer les options**. Cochez les options que vous souhaitez inclure dans la restauration .
   - **Données** : configuration de CC-SG, configuration des dispositifs et des nœuds, et données utilisateur.

- **Journaux** : journaux d'erreur et rapports d'événement stockés dans CC-SG.
- **Fichiers de firmware de CC** : fichiers de firmware stockés utilisés pour la mise à jour du serveur CC-SG.
- **Fichiers de firmware des dispositifs** : fichiers de firmware stockés utilisés pour la mise à jour des dispositifs Raritan gérés par CC-SG.
- **Fichiers d'application** : applications stockées utilisées par CC-SG pour connecter les utilisateurs aux nœuds.

5. Entrez le nombre de minutes, de 0 à 60, qui doivent s'écouler avant que CC-SG n'exécute l'opération de restauration dans le champ **Restaurer après**. Ceci permet aux utilisateurs de terminer leur travail et de se déconnecter.
6. Dans le champ **Message à diffusion générale**, entrez un message pour prévenir les autres utilisateurs de CC-SG qu'une restauration va avoir lieu.
7. Cliquez sur **Restaurer**. Après cela, CC-SG attendra le temps indiqué dans le champ **Restaurer après** avant de récupérer la configuration issue de la sauvegarde sélectionnée. Lorsque la restauration se produit, tous les autres utilisateurs sont déconnectés.

Réinitialisation de CC-SG

Vous pouvez réinitialiser CC-SG pour purger la base de données. Lorsque la base de données est purgée, tous les dispositifs, nœuds et utilisateurs sont retirés. Tous les serveurs d'authentification et d'autorisation sont retirés.

Cette opération ne réinitialise pas les données de configuration système, telles que l'adresse IP de CC-SG. Les actions suivants ont lieu lorsque vous réinitialisez CC-SG :

- réinitialisation de la base de données CC-SG
- réinitialisation de la configuration SNMP
- réinitialisation au firmware par défaut
- chargement du firmware par défaut dans la base de données CC-SG
- réinitialisation de la console de diagnostic aux valeurs par défaut

Vous devez effectuer une sauvegarde et enregistrer le fichier de sauvegarde à un autre emplacement avant de réinitialiser CC-SG.

➢ *Pour réinitialiser CC-SG :*

1. Choisissez **Maintenance du système** > **Réinitialiser**.
2. Tapez votre **mot de passe** CC-SG.
3. Message à diffusion générale : entrez le message à afficher aux utilisateurs qui seront déconnectés de CC-SG.
4. Entrez le nombre de minutes, de 0 à 30, qui doivent s'écouler avant que CC-SG n'exécute l'opération de réinitialisation.
5. Cliquez sur **OK** pour réinitialiser CC-SG. Un message apparaît pour confirmer la réinitialisation.

Redémarrage de CC-SG

La commande de redémarrage permet de relancer le logiciel CC-SG. Le redémarrage déconnecte tous les utilisateurs actifs de CC-SG.

Le redémarrage n'entraîne pas une alimentation cyclique de l'unité CC-SG. Pour effectuer un réamorçage complet, vous devez accéder à la console de diagnostic ou à l'interrupteur d'alimentation de l'unité CC-SG.

1. Choisissez **Maintenance du système** > **Redémarrer**.
2. Renseignez le champ **Mot de passe**.

3. Message à diffusion générale : entrez le message à afficher aux utilisateurs qui seront déconnectés de CC-SG.
4. Redémarrer après (mn) : entrez le nombre de minutes, de 0 à 30, qui doivent s'écouler avant que CC-SG redémarre.
5. Cliquez sur **OK** pour redémarrer CC-SG.

Mise à niveau de CC-SG

Vous pouvez mettre à niveau le firmware de CC-SG lorsqu'une version plus récente est disponible. Les fichiers de firmware figurent dans la section Support du site Web Raritan.

Téléchargez le fichier de firmware sur votre PC client avant de procéder à la mise à niveau.

Il est recommandé d'effectuer une copie de sauvegarde de CC-SG avant d'effectuer la mise à niveau. Si vous utilisez un cluster CC-SG, vous devez d'abord supprimer celui-ci et mettre chaque nœud à niveau individuellement.

Remarque : si vous effectuez la mise à niveau de 3.0.2 à 3.1 et que vous utilisez Active Directory, consultez le fichier Lisezmoi de la version 3.1 pour prendre connaissance des instructions spéciales.

Important :

si vous devez mettre à niveau CC-SG et un périphérique ou groupes de périphériques, traitez CC-SG d'abord, puis le dispositif.

CC-SG redémarre dans le cadre du processus de mise à niveau de 3.1.1 à 3.2. N'INTERROMPEZ PAS le processus, ne redémarrez pas l'unité manuellement, ne mettez pas l'unité hors tension, n'effectuez pas d'alimentation cyclique lors de la mise à niveau.

➢ *Pour mettre à niveau CC-SG :*

1. Téléchargez le fichier de firmware sur votre PC client.
2. ***Entrez en mode de maintenance*** (voir "Entrer en mode de maintenance" à la page 156).
3. Lorsque CC-SG est en mode de maintenance, choisissez **Maintenance du système** > **Mettre à niveau**.
4. Cliquez sur **Parcourir**. Recherchez et sélectionnez le fichier de firmware de CC-SG, cliquez ensuite sur **Ouvrir**.
5. Cliquez sur **OK** pour télécharger ce fichier sur CC-SG.

Une fois le fichier de firmware téléchargé sur CC-SG, un message de confirmation apparaît pour indiquer que CC-SG a entamé le processus de mise à niveau. Tous les utilisateurs sont alors déconnectés de CC-SG.

6. Cliquez sur **OK** pour quitter CC-SG et lui permettre de redémarrer. Vous devez attendre environ 8 minutes que CC-SG redémarre.
7. Fermez la fenêtre de votre navigateur, puis videz la mémoire cache de ce dernier.
8. Après 8 minutes, ouvrez une nouvelle fenêtre du navigateur et lancez CC-SG.
9. Choisissez **Aide** > **A propos de Raritan Secure Gateway**. Vérifiez le numéro de version pour vous assurer que la mise à niveau a abouti.
   - Si la version n'a pas été mise à niveau, répétez la procédure précédente.
   - Si la mise à niveau a abouti, passez à l'étape suivante.
10. ***Quittez le mode de maintenance*** (voir "Quitter le mode de maintenance" à la page 156).

Arrêt de CC-SG

Cette opération permet de fermer le logiciel CC-SG, mais elle n'entraîne pas la mise hors tension de l'unité CC-SG.

Lorsque CC-SG est arrêté, tous les utilisateurs sont déconnectés. Les utilisateurs ne peuvent se reconnecter qu'après le redémarrage de CC-SG, via la console de diagnostic ou la réactivation de CC-SG.

➢ *Pour arrêter CC-SG :*

1. Choisissez **Maintenance du système** > **Arrêter CommandCenter**.
2. Renseignez le champ **Mot de passe**.
3. Dans le champ **Message à diffusion générale**, acceptez le message par défaut ou entrez le message à afficher sur l'écran de tous les utilisateurs actuellement connectés (vous pouvez, par exemple, accorder quelques minutes aux utilisateurs pour terminer les tâches en cours dans CC-SG et leur indiquer quand le système sera à nouveau disponible). Tous les utilisateurs seront déconnectés lors de l'arrêt de CC-SG.
4. Dans le champ **Arrêter après (mn)**, entrez le nombre de minutes, de 0 à 60, qui doivent s'écouler avant l'arrêt de CC-SG.
5. Cliquez sur **OK** pour arrêter CC-SG.

Redémarrage de CC-SG après un arrêt

Après avoir arrêté CC-SG, redémarrez l'unité de l'une des deux façons suivantes :

- Par le biais de la console de diagnostic : reportez-vous à ***Console de diagnostic*** (à la page 226) pour plus d'informations.
- Réinitialisez l'alimentation de l'unité CC-SG.

Mise hors tension de CC-SG

Si l'unité CC-SG perd son alimentation en cours d'exécution, elle mémorise le dernier état d'alimentation. Une fois l'alimentation rétablie, l'unité CC-SG redémarre automatiquement. En revanche, si la coupure d'alimentation se produit lorsque l'unité CC-SG est hors tension, cette dernière restera hors tension lorsque le courant sera rétabli.

Important : ne maintenez pas le bouton d'alimentation enfoncé pour forcer la mise hors tension de CC-SG. Pour mettre CC-SG hors tension, nous vous recommandons de suivre la procédure décrite ci-dessous.

➢ *Pour mettre CC-SG hors tension :*

1. Retirez le cache, puis enfoncez fermement le bouton d'alimentation. Sur les unités G1, le bouton d'alimentation se trouve à l'arrière de l'unité.
2. Patientez environ une minute, le temps que CC-SG s'éteigne normalement.

   Remarque : les utilisateurs connectés à CC-SG via la console de diagnostic recevront un court message à diffusion générale au moment de la mise hors tension de l'unité CC-SG. Les utilisateurs connectés à CC-SG via un navigateur Web ou SSH ne recevront pas de message lors de la mise hors tension de l'unité CC-SG.

3. Si vous devez retirer le câble d'alimentation, attendez la fin du processus de mise hors tension. Cette étape est indispensable pour que CC-SG mette fin à toutes les transactions, ferme les bases de données et mette les lecteurs de disques en sécurité en vue de la coupure d'alimentation.

Fermeture d'une session CC-SG

Il existe deux méthodes pour fermer une session CC-SG.

Déconnectez-vous (voir "Se déconnecter de CC-SG" à la page 165) pour mettre fin à la session tout en gardant la fenêtre du client ouverte.

Quittez (voir "Quitter CC-SG" à la page 165) pour mettre fin à la session et fermer la fenêtre du client.

Se déconnecter de CC-SG

1. Choisissez **Passerelle sécurisée** > **Déconnexion**. La fenêtre **Déconnexion** s'affiche.
2. Cliquez sur **Oui** pour vous déconnecter de CC-SG. Une fois la déconnexion effectuée, la fenêtre de connexion de CC-SG s'affiche.

Quitter CC-SG

1. Choisissez **Passerelle sécurisée** > **Quitter**.
2. Cliquez sur **Oui** pour quitter CC-SG.

Chapitre 15 Administration avancée

Dans ce chapitre

Configuration d'un message du jour....166
Configuration des applications d'accès aux nœuds....167
Configuration des applications par défaut....169
Gestion du firmware d'un dispositif....170
Configuration du réseau CC-SG....171
Configuration de l'activité d'enregistrement....179
Configuration de la date et de l'heure du serveur CC-SG....180
Configuration du modem....181
Modes de connexion : Direct et Proxy....185
Paramètres du dispositif....186
Configuration de SNMP....187
Configuration des clusters CC-SG....189
Gestionnaire de sécurité....193
Gestionnaire des notifications....206
Gestionnaire des tâches....207
CommandCenter NOC....214
Accès SSH à CC-SG....217
Port d'administration série....224
Interface API de services Web....225

Configuration d'un message du jour

Le message du jour vous permet de présenter un message à tous les utilisateurs à la connexion. Vous devez disposer du privilège **CC Setup and Control** pour configurer le message du jour.

➢ *Pour configurer le message du jour :*

1. Choisissez **Administration** > **Paramétrage du Message du jour**.
2. (Facultatif) Sélectionnez **Afficher le Message du jour pour tous les utilisateurs** pour que le message apparaisse à tous les utilisateurs à la connexion.
3. Sélectionnez **Contenu du Message du jour** si vous souhaitez entrer un message dans CC-SG, ou **Fichier du Message du jour** pour le charger depuis un fichier existant.
   - Si vous sélectionnez **Contenu du Message du jour** :
   a. Entrez un message dans la boîte de dialogue fournie.

b. Cliquez sur le menu déroulant **Nom de la police** et sélectionnez la police d'affichage du message.

c. Cliquez sur le menu déroulant **Taille de police** et sélectionnez la taille d'affichage du message.

- Si vous sélectionnez **Fichier du Message du jour** :

a. Cliquez sur **Parcourir** pour rechercher le fichier de message.

b. Sélectionnez le fichier dans la fenêtre de dialogue qui apparaît, puis cliquez sur **Ouvrir**.

c. Cliquez sur **Aperçu** pour vérifier le contenu du fichier.

4. Cliquez sur **OK** pour enregistrer les modifications.

Configuration des applications d'accès aux nœuds

A propos des applications d'accès aux nœuds

CC-SG offre diverses applications que vous pouvez utiliser pour accéder aux nœuds. Vous pouvez utiliser le Gestionnaire d'applications pour afficher des applications, en ajouter de nouvelles, en supprimer et définir l'application par défaut pour chaque type de dispositif.

➢ *Pour afficher les applications disponibles dans CC-SG :*

1. Choisissez **Administration** > **Applications**.
2. Cliquez sur le menu déroulant Nom de l'application pour afficher la liste des applications disponibles dans CC-SG.

Vérification et mise à niveau des versions des applications

Vérifiez et mettez à niveau les versions des applications de CC-SG, telles que Raritan Console (RC) et Raritan Remote Client (RRC).

➢ *Pour vérifier la version d'une application :*

1. Choisissez **Administration** > **Applications**.
2. Sélectionnez le **nom de l'application** dans la liste. Notez le numéro figurant dans le champ **Version**. Certaines applications n'affichent pas automatiquement de numéro de version.

➢ *Pour mettre à niveau une application :*

Si la version n'est pas à jour, vous devez mettre à niveau l'application. Vous pouvez télécharger le fichier de mise à niveau de l'application depuis le site Web de Raritan. Pour obtenir la liste complète des versions d'application prises en charge, reportez-vous à la **matrice de compatibilité** sur le site Web du support Raritan.

1. Enregistrez le fichier d'application sur votre PC client.
2. Cliquez sur la flèche déroulante **Nom de l'application** et sélectionnez l'application que vous souhaitez mettre à niveau dans la liste. Si l'application n'apparaît pas, vous devez d'abord l'ajouter. ***Ajouter une application*** (à la page 168)
3. Cliquez sur **Parcourir**, recherchez et sélectionnez le fichier de mise à niveau de l'application dans la boîte de dialogue qui apparaît, puis cliquez sur **Ouvrir**.
4. Le nom de l'application s'affiche dans le champ **Nouveau fichier d'application** de l'écran **Gestionnaire des applications**.
5. Cliquez sur **Télécharger vers le serveur**. Une fenêtre indique la progression du téléchargement de la nouvelle application. Une fois le téléchargement terminé, une nouvelle fenêtre indique que l'application a été ajoutée à la base de données CC-SG et est prête à être utilisée.
6. Si le champ **Version** n'est pas automatiquement mis à jour, entrez-y le nouveau numéro de version. Le champ **Version** s'actualise automatiquement pour certaines applications.
7. Cliquez sur **Mettre à jour**.

Ajouter une application

Lorsque vous ajoutez une application dans CC-SG, vous devez indiquer les types de dispositifs avec lesquels l'application fonctionnera. Si un dispositif fournit l'accès KVM et série, il figure deux fois dans la liste, une pour chaque méthode.

1. Choisissez **Administration** > **Applications**.
2. Cliquez sur **Ajouter**. La fenêtre de dialogue **Ajouter une application** s'affiche.
3. Renseignez le champ **Nom de l'application**.
4. Dans la liste **Disponible**, sélectionnez les dispositifs Raritan avec lesquels l'application fonctionnera, puis cliquez sur **Ajouter** pour les déplacer vers la liste **Sélectionné**.

- Pour ne plus autoriser l'utilisation d'un dispositif avec l'application, choisissez-le dans la liste **Sélectionné**, puis cliquez sur **Retirer**.

5. Cliquez sur **OK**. Une boîte de dialogue Ouvrir apparaît.
6. Recherchez et sélectionnez le fichier d'application (généralement un fichier .jar ou .cab), puis cliquez sur **Ouvrir**.

   L'application sélectionnée se charge dans CC-SG.

Supprimer une application

1. Choisissez **Administration** > **Applications**.
2. Sélectionnez une application dans le menu déroulant **Nom de l'application**.
3. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation apparaît.
4. Cliquez sur **Oui** pour supprimer l'application.

Configuration des applications par défaut

A propos des applications par défaut

Vous pouvez spécifier l'application que CC-SG doit utiliser par défaut pour chaque type de dispositif.

Afficher les affectations d'applications par défaut

1. Choisissez **Administration** > **Applications**.
2. Cliquez sur l'onglet **Applications par défaut** pour afficher et modifier les applications par défaut actuelles de divers interfaces et types de ports. Les applications répertoriées ici serviront de valeur par défaut lors de la configuration d'un nœud pour autoriser l'accès via une interface sélectionnée.

Définir l'application par défaut d'une interface ou d'un type de port

1. Choisissez **Administration** > **Applications**.
2. Cliquez sur l'onglet **Applications par défaut**.
3. Sélectionnez l'interface ou le type de port dont vous souhaitez définir l'application par défaut.

4. Double-cliquez sur la flèche **Application** indiquée sur cette ligne. La valeur devient un menu déroulant. Les valeurs grisées ne sont pas modifiables.
5. Sélectionnez l'application à utiliser par défaut lors de la connexion à l'interface ou au type de port choisis.
   - **Détection automatique** : CC-SG sélectionne automatiquement une application appropriée en fonction du navigateur du client.
6. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Gestion du firmware d'un dispositif

CC-SG stocke le firmware des dispositifs Raritan pour mettre à niveau les dispositifs qu'il contrôle. Le gestionnaire des firmware permet de télécharger et de supprimer les fichiers de firmware des dispositifs dans CC-SG. Une fois le fichier de firmware téléchargé, vous pouvez y accéder pour effectuer la mise à niveau du dispositif. ***Mise à niveau d'un dispositif*** (à la page 42)

Télécharger un firmware

Vous pouvez télécharger différentes versions de firmware de dispositif sur CC-SG. Lorsqu'une nouvelle version est disponible, elle est postée sur le site Web de Raritan.

1. Choisissez **Administration** > **Firmware**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau fichier de firmware. Une fenêtre de recherche s'affiche.
3. Recherchez et sélectionnez le fichier de firmware à télécharger sur CC-SG, cliquez ensuite sur **Ouvrir**. Une fois le téléchargement terminé, le nouveau firmware apparaît dans le champ **Nom du firmware**.

Supprimer un firmware

1. Choisissez **Administration** > **Firmware**.
2. Cliquez sur la flèche déroulante **Nom du firmware** et sélectionnez le firmware à supprimer.
3. Cliquez sur **Supprimer**. Un message de confirmation apparaît.
4. Cliquez sur **Oui** pour supprimer le firmware.

Configuration du réseau CC-SG

Vous pouvez configurer les paramètres de votre réseau géré CC-SG dans le Gestionnaire de configuration.

A propos de la configuration réseau

CC-SG offre deux modes de configuration du réseau :

- ***Mode principal/de sauvegarde*** (voir "Mode principal/de sauvegarde : définition" à la page 173)
- ***Mode actif/actif*** (voir "Mode actif/actif : définition" à la page 176)

CC-SG autorise également les adresses IP statiques ou DHCP. Reportez-vous à ***Configurations DHCP recommandées pour CC-SG*** (à la page 178) pour une utilisation optimale de DHCP avec de votre unité CC-SG.

A propos des ports LAN CC-SG

Une unité CC-SG fournit deux ports LAN principaux : réseau local principal et réseau local secondaire. Les modes principal/de sauvegarde et actif/actif requièrent une connexion aux ports LAN CC-SG de différentes façons.

Reportez-vous aux tables ci-dessous pour vérifier l'emplacement des ports de réseaux locaux principal et secondaire sur votre modèle CC-SG.

Ports LAN G1

Modèle	Nom du réseau local principal	Emplacement du réseau local principal	Nom du réseau local secondaire	Emplacement du réseau local secondaire
G1	LAN0	Port LAN droit	LAN1	Port LAN gauche

Ports LAN V1

Modèle	Nom du réseau local principal	Emplacement du réseau local principal	Nom du réseau local secondaire	Emplacement du réseau local secondaire
V1	LAN1	Port LAN gauche	LAN2	Port LAN droit

Raritan.
When you're ready to take control®

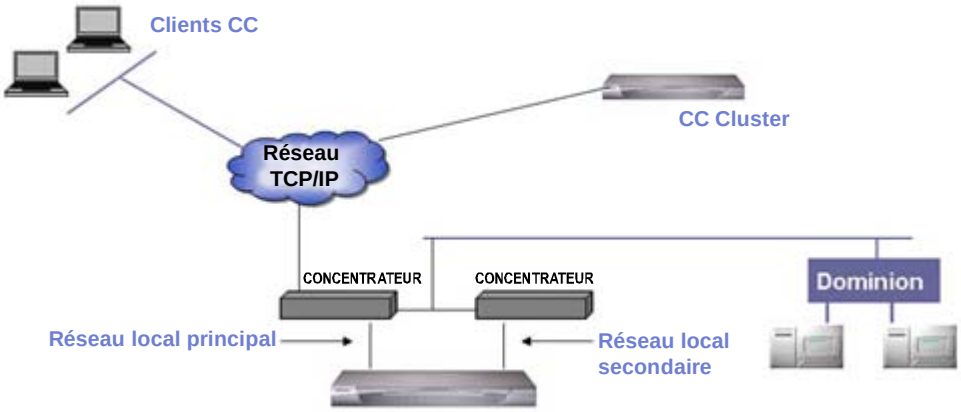
Ports LAN E1

Modèle	Nom du réseau local principal	Emplacement du réseau local principal	Nom du réseau local secondaire	Emplacement du réseau local secondaire
E1	Sans libellé.	Port LAN supérieur d'un ensemble de 2 ports au centre du panneau arrière de l'unité	Sans libellé.	Port LAN inférieur d'un ensemble de 2 ports au centre du panneau arrière de l'unité

Mode principal/de sauvegarde : définition

Le mode principal/de sauvegarde vous permet d'utiliser deux ports LAN CC-SG pour implémenter le basculement et la redondance réseau. Dans ce mode, seul un port LAN est actif à la fois.

Reportez-vous à ***A propos des ports LAN CC-SG*** (à la page 172) pour obtenir l'emplacement des ports LAN principal et secondaire sur chaque modèle CC-SG.



Si le réseau principal est connecté et reçoit un signal d'intégrité de liens, CC-SG utilise ce port LAN pour toutes les communications. Si le réseau local principal perd l'intégrité de liens LAN et que le réseau local secondaire est connecté, CC-SG bascule son adresse IP affectée sur le réseau local secondaire. Le réseau local secondaire est utilisé jusqu'à la remise en service du réseau local principal. Lorsque le réseau local principal est remis en service, CC-SG y retourne automatiquement.

Tant qu'une connexion de réseau local est viable, un client ne remarque aucune interruption de service au cours d'une défaillance.

➢ *Configuration du mode principal/de sauvegarde*

Lors de l'implémentation du mode principal/de sauvegarde pour votre réseau CC-SG :

- Les deux ports LAN CC-SG doivent être connectés au même sous-réseau local.
- (Facultatif) Vous pouvez connecter chaque port LAN à un commutateur ou concentrateur différent du même sous-réseau pour des questions de fiabilité.

➢ *Pour configurer le mode principal/de sauvegarde dans CC-SG :*

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **Configuration réseau**.
3. Sélectionnez **Mode principal/de sauvegarde**.
4. Tapez le nom de l'hôte CC-SG dans le champ Nom de l'hôte. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2). Lorsque vous cliquez sur **Mettre à jour la configuration** pour enregistrer la configuration, le champ **Nom de l'hôte** est actualisé pour refléter le nom de domaine complètement qualifié (NDCQ) si un DNS et un suffixe de domaine ont été configurés.
5. Cliquez sur la flèche déroulante **Configuration** et sélectionnez **DHCP** ou **Statique**.

   DHCP :

   - Si vous choisissez DHCP, les champs DNS principal, DNS secondaire, Suffixe de domaine, Adresse IP, Masque de sous-réseau et Passerelle par défaut sont automatiquement remplis (si votre serveur DHCP est configuré pour fournir ces données) une fois la configuration réseau enregistrée et l'unité CC-SG redémarrée.

- A l'aide de ces données fournies par le serveur DHCP, CC-SG s'enregistre de manière dynamique auprès du serveur DNS si les mises à jour dynamiques sont autorisées.
- Reportez-vous à ***Configurations DHCP recommandées pour CC-SG*** (à la page 178) pour plus d'informations.

Statique :

- Si vous choisissez **Statique**, entrez des serveurs DNS principal et DNS secondaire, un suffixe de domaine, une adresse IP, un masque de sous-réseau et une passerelle par défaut dans les champs appropriés.

6. Cliquez sur la flèche déroulante **Vitesse de la carte** et sélectionnez une vitesse de ligne dans la liste. Assurez-vous que votre sélection est conforme avec le paramètre de port de carte de votre commutateur.
7. Si vous avez sélectionné **Auto** dans le champ **Vitesse de la carte**, le champ **Mode de la carte** est désactivé, l'option **Bidirectionnel simultané** étant sélectionnée automatiquement. Si vous avez indiqué une vitesse de carte différente d'Auto, cliquez sur la flèche déroulante **Mode de la carte** et sélectionnez un mode duplex dans la liste.
8. Cliquez sur **Mettre à jour la configuration** pour enregistrer vos modifications. Les modifications ne seront pas appliquées tant que CC-SG n'aura pas été redémarré.
   - Cliquez sur **Redémarrer maintenant** pour redémarrer automatiquement CC-SG immédiatement.
   - Cliquez sur **Redémarrer plus tard** pour ***redémarrer CC-SG*** (voir "Redémarrage de CC-SG" à la page 161) manuellement ultérieurement.
     - Cliquez sur **Annuler** pour retourner au panneau Configuration réseau sans enregistrer vos modifications. Vous devez cliquer sur **Mettre à jour la configuration**, puis sur **Redémarrer maintenant** ou **Redémarrer plus tard** pour enregistrer vos modifications.

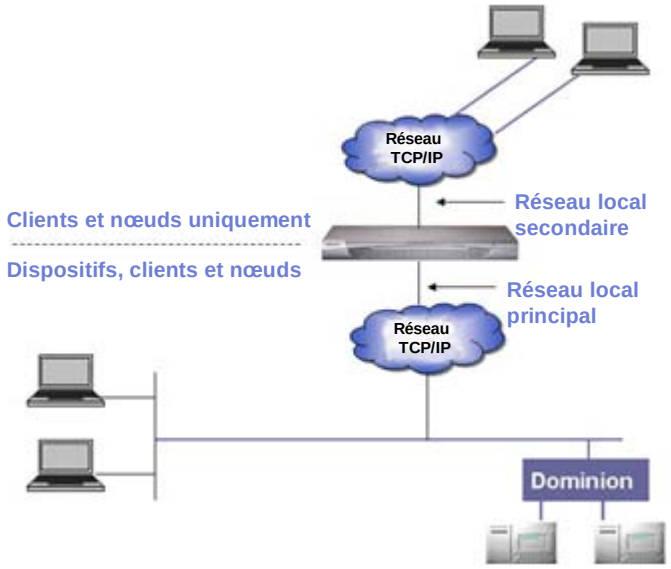
Remarque : *si l'unité CC-SG est configurée avec DHCP, vous pouvez y accéder via le nom d'hôte après enregistrement auprès du serveur DNS.*

Mode actif/actif : définition

Le mode actif/actif vous permet d'utiliser CC-SG pour gérer des dispositifs et des nœuds figurant sur deux réseaux distincts. Dans ce mode, CC-SG gère le trafic entre deux domaines IP séparés. Le mode actif/actif ne propose pas le basculement. Si les deux connexions de réseau local échouent, les utilisateurs n'ont plus accès.

Reportez-vous à ***A propos des ports LAN CC-SG*** (à la page 172) pour obtenir l'emplacement des ports LAN principal et secondaire sur chaque modèle CC-SG.

Remarque : *le clustering ne peut pas être configuré en mode actif/actif.*



➢ *Configuration du mode actif/actif*

Lors de l'implémentation du mode actif/actif pour votre réseau CC-SG :

- Chaque port LAN CC-SG doit être connecté à un sous-réseau différent.
- Les dispositifs Raritan doivent être connectés au réseau local principal uniquement.
- Les clients et les nœuds peuvent être connectés au réseau local principal ou secondaire.
- Définissez au plus une passerelle par défaut dans le panneau Configuration réseau de CC-SG. Utilisez la console de diagnostic pour ***ajouter des routes statiques supplémentaires*** (voir "Modification des routes statiques (Interfaces réseau)" à la page 238) si nécessaire.

➢ *Pour configurer le mode actif/actif dans CC-SG :*

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet Configuration réseau.
3. Sélectionnez Mode actif/actif.
4. Tapez le nom de l'hôte CC-SG dans le champ Nom de l'hôte. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2). Lorsque vous cliquez sur Mettre à jour la configuration pour enregistrer la configuration, le champ Nom de l'hôte est actualisé pour refléter le nom de domaine complètement qualifié (NDCQ) si un DNS et un suffixe de domaine ont été configurés.
5. Configure le réseau local principal dans la colonne de gauche et le réseau local secondaire dans la colonne de droite :
6. Cliquez sur la flèche déroulante Configuration et sélectionnez DHCP ou Statique.

   DHCP :

   - Si vous choisissez DHCP, les champs DNS principal, DNS secondaire, Suffixe de domaine, Adresse IP, Masque de sous-réseau et Passerelle par défaut sont automatiquement remplis (si votre serveur DHCP est configuré pour fournir ces données) une fois la configuration réseau enregistrée et l'unité CC-SG redémarrée.

- A l'aide de ces données fournies par le serveur DHCP, CC-SG s'enregistre de manière dynamique auprès du serveur DNS si les mises à jour dynamiques sont autorisées.
- Reportez-vous à ***Configurations DHCP recommandées pour CC-SG*** (à la page 178) pour plus d'informations.

Statique :

- Si vous choisissez Statique, entrez des serveurs DNS principal et DNS secondaire, un suffixe de domaine, une adresse IP et un masque de sous-réseau dans les champs appropriés.
- N'indiquez qu'une passerelle par défaut, pas deux.

7. Cliquez sur la flèche déroulante Vitesse de la carte et sélectionnez une vitesse de ligne dans la liste. Assurez-vous que votre sélection est conforme avec le paramètre de port de carte de votre commutateur.
8. Si vous avez sélectionné Auto dans le champ Vitesse de la carte, le champ Mode de la carte est désactivé, l'option Bidirectionnel simultané étant sélectionnée automatiquement. Si vous avez indiqué une vitesse de carte différente d'Auto, cliquez sur la flèche déroulante Mode de la carte et sélectionnez un mode duplex dans la liste.
9. Cliquez sur Mettre à jour la configuration pour enregistrer vos modifications. CC-SG redémarre.

Configurations DHCP recommandées pour CC-SG

Etudiez les configurations DHCP recommandées suivantes. Assurez-vous que votre serveur DHCP est paramétré correctement avant de configurer CC-SG pour utiliser DHCP.

- Configurez le serveur DHCP pour allouer l'adresse IP de CC-SG de manière statique.
- Configurez les serveurs DHCP et DNS pour enregistrer automatiquement l'unité CC-SG avec le serveur DNS lorsque le serveur DHCP alloue une adresse IP à CC-SG.
- Configurez le serveur DNS pour accepter les demandes d'enregistrement DDNS (Dynamic Domain Name System) non authentifiées de CC-SG.

Configuration de l'activité d'enregistrement

Vous pouvez configurer CC-SG afin d'envoyer des rapports à de serveurs d'enregistrement externes. Vous pouvez configurer le niveau des messages consignés dans chacun des journaux.

➢ *Pour configurer l'activité d'enregistrement de CC-SG :*

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **Journaux**.
3. Pour affecter un serveur d'enregistrement externe à l'usage de CC-SG, entrez l'adresse IP dans le champ **Adresse du serveur** sous **Serveur principal**.
4. Cliquez sur la flèche déroulante **Niveau de transfert** et sélectionnez un niveau de gravité d'événement. Tous les événements de ce niveau ou d'un niveau supérieur seront envoyés au serveur d'enregistrement.
5. Pour configurer un second serveur d'enregistrement externe, répétez les étapes 3 et 4 pour les champs figurant sous **Serveur secondaire**.
6. Sous **Journal CommandCenter**, cliquez sur le menu déroulant **Niveau de transfert** et sélectionnez un niveau de gravité. Tous les événements de ce niveau ou d'un niveau supérieur seront envoyés au journal interne de CC-SG.
7. Cliquez sur **Mettre à jour la configuration** pour enregistrer vos modifications.

Purger le journal interne de CC-SG

Vous pouvez purger le journal interne de CC-SG. Cette opération ne supprime aucun événement consigné sur vos serveurs d'enregistrement externes.

Remarque : *les rapports Journal d'audit et Journal d'erreurs sont basés sur le journal interne de CC-SG. Si vous purgez ce dernier, ces deux rapports le seront également. Vous pouvez également purger ces rapports individuellement.* **Purger les données d'un rapport de CC-SG** *(à la page 142)*

➢ *Pour purger le journal interne de CC-SG :*

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **Journaux**.
3. Cliquez sur **Purger**.

4. Cliquez sur **Oui**.

Configuration de la date et de l'heure du serveur CC-SG

L'heure et la date doivent être maintenues avec précision dans CC-SG afin de pouvoir gérer les dispositifs de manière fiable.

Important : la configuration de l'heure et de la date est utilisée pour programmer des tâches dans le Gestionnaire des tâches. Reportez-vous à *Gestionnaire des tâches* **(à la page 207) pour plus d'informations. Il peut y avoir un décalage entre l'heure réglée sur le client et celle réglée dans CC-SG.**

Seul le super utilisateur CC et les utilisateurs dotés de privilèges similaires peuvent configurer l'heure et la date.

Le changement de fuseau horaire est désactivé dans une configuration de clusters.

➢ *Pour configurer la date et l'heure du serveur CC-SG :*

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet **Heure/Date**.
   a. **Pour définir la date et l'heure manuellement : Date** – cliquez sur la flèche déroulante afin de sélectionner le **mois**, utilisez les flèches haut et bas pour sélectionner l'**année** et cliquez sur le **jour** dans la zone du calendrier. **Heure** – utilisez les flèches haut et bas afin de sélectionner les paramètres **Heure**, **Minutes** et **Secondes**, puis cliquez sur la flèche déroulante **Fuseau horaire** pour sélectionner le fuseau horaire applicable à CC-SG.
   b. **Pour définir la date et l'heure à l'aide du protocole NTP :** cochez la case **Activer le protocole de temps du réseau** au bas de la fenêtre et indiquez les adresses IP des **serveur principal (NTP)** et **serveur secondaire (NTP)** dans les champs correspondants.

   Remarque : Network Time Protocol (NTP) est le protocole utilisé pour synchroniser les données relatives à la date et à l'heure de l'ordinateur connecté à l'aide d'un serveur NTP référencé. Lorsque CC-SG est configuré à l'aide du protocole NTP, il peut synchroniser l'heure de son horloge sur celle du serveur de référence NTP publiquement disponible et conserver une heure correcte et cohérente.
3. Cliquez sur **Mettre à jour la configuration** pour appliquer les modifications relatives à l'heure et à la date à l'unité CC-SG.

4. Cliquez sur **Rafraîchir** pour recharger le nouveau temps serveur dans le champ **Heure actuelle**.
5. Choisissez **Maintenance du système** > **Redémarrer** pour redémarrer CC-SG.

Configuration du modem

Cet écran vous permet d'accéder à une unité G1 CC-SG depuis une machine cliente via une connexion par ligne commutée. Cette méthode d'accès à CC-SG peut être utilisée dans les cas d'urgence.

Les modèles V1 et E1 de CC-SG ne disposent pas de modem et n'en permettent pas la configuration.

Configurer CC-SG

1. Choisissez Administration > Configuration. Lorsque l'écran Gestionnaire de configuration s'affiche, cliquez sur l'onglet Modem.
2. Entrez l'adresse IP de l'unité CC-SG dans le champ Adresse du serveur.
3. Dans le champ Adresse du client, entrez l'adresse IP du client qui doit se connecter par ligne commutée à l'unité CC-SG.
4. Dans le champ Téléphone du client, entrez le numéro de rappel composé par l'unité CC-SG pour se connecter au client, en cas de numérotation de rappel.
5. Cliquez sur Mettre à jour la configuration pour enregistrer vos modifications.

Configurer le modem du PC client

Branchez une ligne téléphonique sur l'unité G1 CC-SG, qui contient un modem intégré. Vous pouvez retirer les câbles de réseau local.

Sur le client de numérotation, connectez un modem à la machine cliente, un ordinateur Windows XP par exemple. Branchez une ligne téléphonique au modem client. Redémarrez la machine cliente ; le modem connecté est détecté en tant que nouveau matériel. Installez le modem sur le client comme suit (en supposant qu'il s'agit d'une machine cliente Windows XP) :

1. Choisissez **Panneau de configuration** > **Options de modems et téléphonie**.
2. Cliquez sur l'onglet **Modems**.

3. Cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Options avancées**.
5. Dans le champ **Commandes d'initialisation supplémentaires**, tapez une commande d'initialisation qui sera utilisée par votre modem pour définir l'indicateur « Carrier detection » (Ecoute de porteuse). Par exemple, tapez **at&c** pour un modem télécopieur SoftK56. Il est nécessaire d'indiquer à Windows de ne pas fermer le processus de connexion de modem démarré lorsque la connexion est interrompue par la partie appelante (accès entrant). Cliquez sur **OK** pour enregistrer les modifications.

Configurer la connexion à distance

La procédure suivante illustre la création d'une connexion entrante à distance à CC-SG depuis un ordinateur client Windows XP :

1. Choisissez **Démarrer** > **Favoris réseau**.
2. Cliquez avec le bouton droit de la souris dans la fenêtre et sélectionnez **Propriétés**.
3. Sous **Gestion du réseau** dans la fenêtre **Connexions réseau**, cliquez sur **Créer une nouvelle connexion**.
4. Cliquez sur **Suivant**, **Connexion au réseau d'entreprise**, **Connexion d'accès à distance**.
5. Entrez le nom de la connexion à CC-SG.
6. Tapez le numéro de téléphone utilisé pour la connexion à CC-SG et cliquez sur **Suivant**. Il NE S'AGIT PAS du numéro de rappel configuré dans le champ **Téléphone du client** de l'onglet **Modem** du **Gestionnaire de configuration** sur CC-SG.
7. La connexion à CC-SG ne requiert pas de carte à puce. Si vous n'en utilisez pas, cliquez sur **Ne pas utiliser ma carte à puce** pour cette connexion, puis sur **Suivant**.
8. Cliquez sur **Mon utilisation uniquement** dans l'écran suivant pour réserver la connexion à vous seul.
9. Cliquez sur **Terminer** dans le dernier écran pour enregistrer vos modifications.

Configurer la connexion de rappel

Si l'unité CC-SG utilise une connexion de rappel, vous devez utiliser un fichier de script. Pour définir un fichier de script de rappel :

1. Choisissez **Démarrer** > **Favoris réseau**.

2. Cliquez sur **Afficher les connexions réseau** sous **Gestion du réseau**.
3. Cliquez avec le bouton droit sur la connexion **CommandCenter**, puis sur **Propriétés**.
4. Cliquez sur l'onglet **Sécurité**.
5. Cliquez sur **Afficher une fenêtre de terminal**.
6. Cliquez sur **Exécuter le script**, puis sur **Parcourir** pour entrer le script de connexion à distance, **call-back.scp** par exemple.
7. Cliquez sur **OK**.

Exemple de fichier de script de rappel :

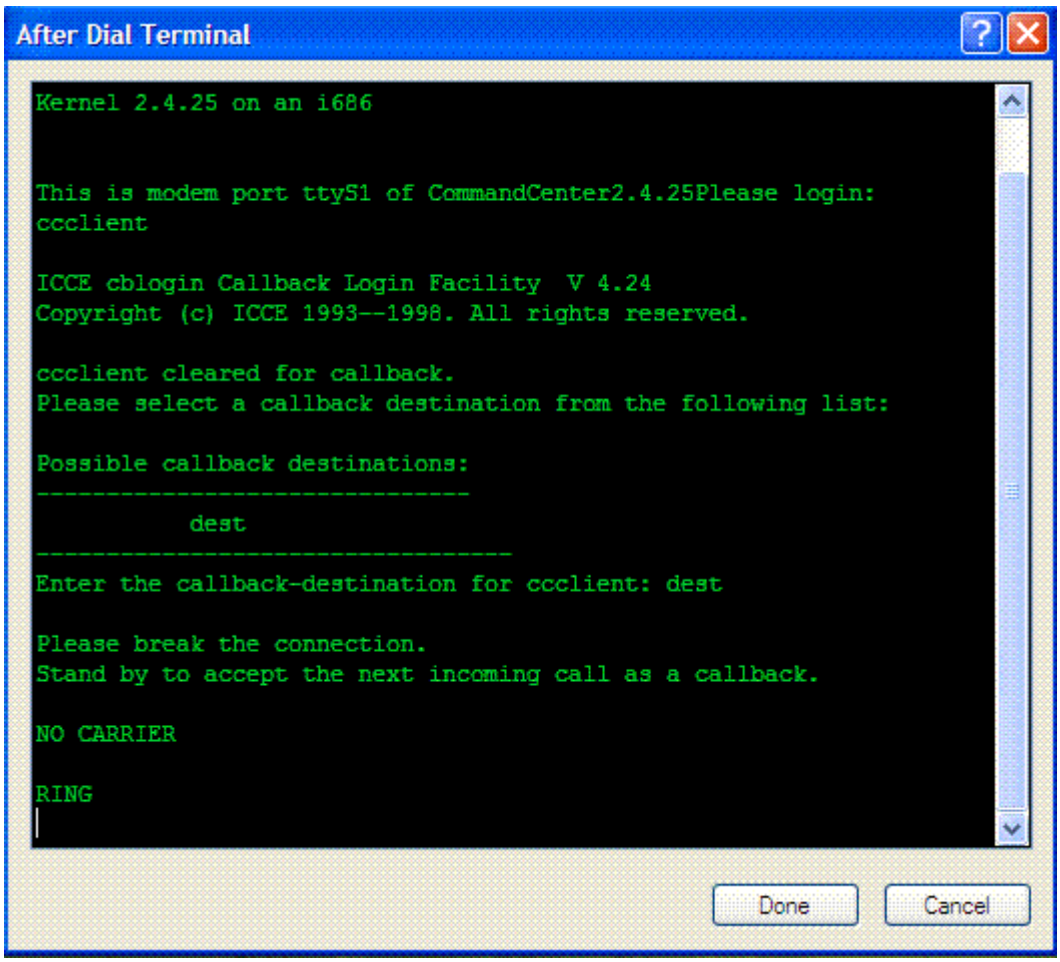
```
proc main
delay 1
waitfor "ogin:"
transmit "ccclient^M"
waitfor "client:"
transmit "dest^M"
waitfor "callback."
transmit "ATH^M"
waitfor "RING"
transmit "ATA^M"
waitfor "CONNECT"
waitfor "ogin:"
transmit "ccclient^M"
endproc
```

Se connecter à CC-SG par modem

➢ *Pour se connecter à CC-SG via un modem :*

1. Choisissez **Démarrer** > **Favoris réseau**.
2. Cliquez sur **Afficher les connexions réseau**.
3. Double-cliquez sur la connexion d'accès à distance que vous avez créée.
4. Tapez le nom d'utilisateur **ccclient** et le mot de passe **cbupass**.

5. Si le champ n'est pas encore renseigné, entrez le numéro de téléphone de connexion à CC-SG. Il NE S'AGIT PAS du numéro de rappel.
6. Cliquez sur **Composer**. Si vous utilisez la fonction de rappel, le modem compose le numéro de l'unité CC-SG, qui compose à son tour celui du PC client.
7. Si l'option **Afficher une fenêtre de terminal** a été cochée comme décrit dans **Configurer la connexion de rappel** (à la page 182), un terminal après numérotation apparaît.



8. Patientez 1 à 2 minutes. Puis, dans un navigateur pris en charge, entrez l'adresse IP de CC-SG configurée dans le champ **Adresse du serveur** de l'onglet **Modem** du **Gestionnaire de configuration** sur CC-SG, et connectez-vous à CC-SG.

Modes de connexion : Direct et Proxy

A propos des modes de connexion

CC-SG offre trois modes de connexion hors bande pour les ports de dispositifs Raritan : Direct, Proxy et Les deux, qui est une combinaison de Direct et Proxy.

- Le mode Direct vous permet de vous connecter directement à un nœud ou port, sans transmettre de données via CC-SG. Le mode Direct offre généralement des connexions plus rapides.
- Le mode Proxy vous permet de vous connecter à un nœud ou port en transmettant toutes les données via CC-SG. Le mode Proxy augmente la charge du serveur CC-SG, ce qui peut ralentir les connexions. Toutefois, le mode Proxy est recommandé si la sécurité de la connexion est plus importante. Vous n'avez qu'à garder les ports TCP (80, 443 et 2400) de l'unité CC-SG ouverts dans votre pare-feu.
- Le mode Les deux vous permet de configurer CC-SG afin d'utiliser une combinaison des modes Direct et Proxy. Dans ce mode, le mode Proxy est le mode par défaut, mais vous pouvez configurer CC-SG pour utiliser le mode Direct lorsque les connexions sont établies à l'aide d'adresses IP clientes de plages spécifiques.

Important : lorsque CC-SG est en mode Proxy ou Les deux, vous ne pouvez donner aux utilisateurs accès à la fonction Support virtuel.

Pour configurer le mode Direct pour toutes les connexions clientes

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **Mode de connexion**.
3. Sélectionnez **Mode direct**.
4. Cliquez sur **Mettre à jour la configuration**.

Pour configurer le mode Proxy pour toutes les connexions clientes

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **Mode de connexion**.
3. Sélectionnez **Mode Proxy**.
4. Cliquez sur **Mettre à jour la configuration**.

Pour configurer une combinaison des modes Direct et Proxy

Lorsque vous configurez CC-SG afin d'utiliser une combinaison des modes Direct et Proxy, le mode Proxy est le mode de connexion par défaut, et le mode Direct n'est utilisé que pour les adresses IP de clients spécifiées.

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **Mode de connexion**.
3. Sélectionnez **Les deux**.
4. Dans les champs **Adresse réseau** et **Masque réseau**, indiquez la plage des adresses IP clientes que doivent se connecter aux nœuds et ports via le mode Direct, puis cliquez sur **Ajouter**.
5. Cliquez sur **Mettre à jour la configuration**.

Paramètres du dispositif

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **Paramètres du dispositif**.
3. Pour mettre à jour le port par défaut du dispositif, sélectionnez un type de dispositif dans le tableau et double-cliquez sur la valeur du paramètre Port par défaut. Tapez la nouvelle valeur du port par défaut et appuyez sur la touche **Entrée**.
4. Pour mettre à jour le délai d'attente d'un dispositif, modifiez la valeur du champ **Test de détection de collision(s)**.
5. Cliquez sur **Mettre à jour la configuration** pour enregistrer vos modifications. Un message de confirmation s'affichera à l'écran, indiquant la mise à jour de tous les paramètres du dispositif associé.

Configuration de SNMP

A propos de SNMP et de CC-SG

Le protocole simplifié de gestion de réseau (SNMP, de l'anglais Simple Network Management Protocol) permet à CC-SG d'envoyer des traps SNMP (notifications d'événements) à un gestionnaire SNMP du réseau. Vous devez être formé à la gestion d'une infrastructure SNMP pour configurer le fonctionnement de CC-SG avec SNMP.

CC-SG prend également en charge les opérations GET/SET SNMP avec les solutions tierces, comme HP OpenView. Pour cela, vous devez fournir les informations d'identifiant d'agents SNMP, telles que celles des objets de groupe système MIB-II : sysContact, sysName et sysLocation. Ces identifiants fournissent des informations de contact, d'administration et d'emplacement concernant le nœud géré. Pour plus d'informations, reportez-vous à la norme RFC 1213.

Fichiers MIB

Etant donné que CC-SG envoie ses propres traps Raritan, vous devez mettre à jour tous les gestionnaires SNMP à l'aide d'un fichier MIB personnalisé contenant les définitions des traps Raritan. ***Traps SNMP*** (à la page 285). Le fichier MIB personnalisé se trouve sur le site Web du support Raritan.

Pour configurer SNMP dans CC-SG

1. Choisissez **Administration** > **Configuration**.
2. Cliquez sur l'onglet **SNMP**.
3. Pour identifier l'agent SNMP exécuté sur CC-SG auprès des solutions de gestion d'entreprise tierces, renseignez les champs de la section **Configuration de l'agent**. Tapez le **port** de l'agent **(161** étant la valeur par défaut).Tapez une chaîne **Communauté en lecture seule** (**public** par défaut) et une chaîne **Communauté en lecture/écriture** (**private** par défaut). Vous pouvez entrer plusieurs chaînes de communauté ; séparez-les par une virgule. Entrez un **contact système**, un **nom du système** et un **emplacement du système** pour fournir des informations sur le nœud géré.
4. Cliquez sur **Mettre à jour la configuration de l'agent** pour enregistrer vos modifications.
5. Sélectionnez **Activer les traps SNMP** pour autoriser l'envoi de traps SNMP de CC-SG à un hôte SNMP.

6. Cochez les cases en regard des traps que CC-SG doit envoyer à vos hôtes SNMP. Sous **Sources des traps**, les traps SNMP sont répertoriés en deux catégories différentes : **Journal système**, contenant les notifications sur l'état de l'unité CC elle-même, par exemple une défaillance du disque dur ; et **Journal de l'application**, contenant les notifications générées par les événements de l'application CC, par exemple les modifications apportées à un compte utilisateur. Pour activer les traps par type, cochez les cases **Journal système** et **Journal de l'application**. Chaque trap peut être activé ou désactivé en cochant la case correspondante. Les boutons **Sélectionner tout** et **Effacer tout** permettent d'activer tous les traps ou de désactiver toutes les cases. Consultez les fichiers MIB pour obtenir la liste des traps SNMP fournis. Reportez-vous à **Fichiers MIB** pour plus d'informations.
7. Dans le panneau **Destinations des traps**, entrez l'adresse IP de l'**hôte** et le numéro de **port** utilisés par les hôtes SNMP. Le port par défaut est **162**.
8. Dans le panneau **Destination des traps**, entrez la chaîne **Communauté** et la **version** (**v1** ou **v2**) utilisées par les hôtes SNMP.
9. Cliquez sur **Ajouter** pour ajouter cet hôte de destination à la liste des hôtes configurés. Vous pouvez inclure dans cette liste autant de gestionnaires que vous le souhaitez.
10. Cliquez sur **Mettre à jour la configuration des traps** pour enregistrer vos modifications.

Raritan.
When you're ready to take control®

Configuration des clusters CC-SG

Cluster CC-SG : définition

Un cluster CC-SG utilise deux nœuds CC-SG, un nœud primaire et un nœud secondaire, pour la sécurité des sauvegardes en cas de défaillance du nœud CC-SG primaire. Ces deux nœuds partagent des données communes pour des connexions et des utilisateurs actifs, et toutes les données relatives à l'état sont répliquées entre ces deux nœuds.

Les dispositifs compris dans un cluster CC-SG doivent disposer de l'adresse IP du nœud CC-SG primaire pour informer ce dernier en cas d'événements de changement d'état. En cas de défaillance du nœud primaire, le nœud secondaire reprend immédiatement la totalité des fonctions de celui-ci. Cette fonction requiert l'initialisation de l'application CC-SG et des sessions utilisateur. Toutes les sessions provenant du nœud CC-SG primaire seront fermées. Les dispositifs connectés au nœud primaire détecteront que ce dernier ne répond pas et répondront alors aux requêtes émanant du nœud secondaire.

Exigences pour les clusters CC-SG

- Les nœuds primaire et secondaire d'un cluster doivent utiliser la même version de firmware, sur une version matérielle identique (G1, V1 ou E1).
- L'unité CC-SG doit être en mode **Principal/Sauvegarde** pour être utilisée avec la fonction de cluster. Cette opération ne fonctionne pas avec une configuration Actif/Actif. Reportez-vous à ***A propos de la configuration réseau*** (à la page 171) pour plus d'informations.
- Les paramètres de date, heure et fuseau horaire ne sont pas répliquées du nœud primaire au nœud secondaire. Vous devez configurer ces paramètres dans chaque CC-SG avant de créer le cluster.

A propos des clusters CC-SG et CC-NOC

Dans une configuration de cluster, seul le nœud primaire communique avec CC-NOC. Lorsqu'une unité CC-SG devient nœud primaire, elle envoie son adresse IP, en plus de celle du nœud secondaire, à CC-NOC.

Créer un cluster

En cas de basculement, l'administrateur doit envoyer un e-mail à tous les utilisateurs CC-SG pour les prévenir d'utiliser l'adresse IP du nouveau nœud CC-SG primaire.

Si la communication est interrompue entre les nœuds primaire et secondaire, le nœud secondaire prend le rôle du nœud primaire. Lorsque la connectivité sera rétablie, vous pouvez avoir deux nœuds primaires. Le cas échéant, retirez l'un d'entre eux et réinitialisez-le comme nœud secondaire.

Important : il est recommandé de sauvegarder votre configuration sur les deux unités CC-SG avant de créer un cluster.

➢ *1. Définir un nœud CC-SG primaire*

1. Choisissez **Administration** > **Configuration des clusters**.
2. Cliquez sur **Découvrir les appareils CommandCenter** pour analyser et afficher tous les appareils CC-SG dans le sous-ensemble que vous utilisez actuellement. Vous pouvez également ajouter un CC-SG, d'un sous-réseau différent par exemple, en spécifiant une adresse IP dans **Adresse de CommandCenter** au bas de la fenêtre, puis en cliquant sur **Ajouter un appareil CommandCenter**.
3. Renseignez le champ **Nom du cluster**. Si vous n'entrez pas de nom maintenant, un nom par défaut sera fourni, tel que **cluster192.168.51.124**, à la création du cluster.
4. Cliquez sur **Créer un cluster**. Un message apparaît.
5. Cliquez sur **Oui**. L'unité CC-SG que vous utilisez actuellement devient le nœud primaire.

➢ *2. Définir un nœud CC-SG secondaire*

1. Cliquez sur **Découvrir les appareils CommandCenter** pour analyser et afficher tous les appareils CC-SG dans le sous-ensemble que vous utilisez actuellement. Vous pouvez également ajouter un CC-SG, d'un sous-réseau différent par exemple, en spécifiant une adresse IP dans **Adresse de CommandCenter** au bas de la fenêtre. Cliquez sur **Ajouter un appareil CommandCenter**.
2. Pour ajouter un nœud secondaire, ou nœud CC-SG de sauvegarde, sélectionnez une unité CC-SG à l'état **Autonome** dans le tableau Configuration des clusters. Le numéro de version doit correspondre à celui du nœud primaire.

3. Entrez un nom d'utilisateur et un mot de passe valides pour le nœud de sauvegarde dans les champs **Nom d'utilisateur de sauvegarde** et **Mot de passe**.
4. Cliquez sur **Lier cluster de sauvegarde**.
5. Un message de confirmation apparaît. Cliquez sur **Oui** pour affecter l'état secondaire au nœud sélectionné.

   Important : une fois le processus de liaison entamé, n'exécutez aucune autre fonction dans CC-SG avant la fin.

6. Le tout nouveau nœud secondaire redémarre. Cette procédure peut durer plusieurs minutes. Une fois le redémarrage effectué, un message de confirmation s'affiche.
7. Choisissez **Administration** > **Configuration des clusters** pour visualiser le tableau Configuration des clusters mis à jour.

Supprimer un nœud CC-SG secondaire

Lorsque vous supprimez un nœud secondaire, ou de sauvegarde, vous supprimez la désignation Nœud secondaire. L'unité secondaire CC-SG n'est pas effacée de votre configuration.

➢ *Pour supprimer l'état de nœud secondaire d'une unité CC-SG :*

1. Sélectionnez le nœud secondaire CC-SG dans le tableau Configuration des clusters.
2. Cliquez sur **Supprimer le cluster de sauvegarde**.
3. Cliquez sur **Oui** pour supprimer l'état de nœud secondaire.

Supprimer un nœud CC-SG primaire

Lorsque vous supprimez un cluster, vous ne retirez pas l'unité primaire CC-SG de votre configuration ; cette action élimine simplement la désignation Nœud primaire. Supprimer le cluster est disponible uniquement en l'absence de nœuds de sauvegarde.

➢ *Pour supprimer l'état de nœud primaire d'une unité CC-SG :*

1. Sélectionnez le nœud primaire CC-SG dans le tableau Configuration des clusters.
2. Cliquez sur **Supprimer le cluster**.
3. Cliquez sur **Oui** pour supprimer l'état de nœud primaire.

Récupérer un nœud CC-SG défaillant

Si un nœud est défaillant et qu'un basculement se produit, l'état En attente du nœud indique sa récupération. Lorsqu'un nœud passe au mode En attente, il peut être démarré en mode Autonome ou en mode Sauvegarde.

1. Sélectionnez le nœud En attente dans le tableau Configuration des clusters.
2. Ajoutez-le en tant que nœud de sauvegarde en cliquant sur **Lier nœud en attente**.
3. Un message de confirmation apparaît. Cliquez sur **Oui** pour affecter l'état secondaire au nœud sélectionné.
4. Le nœud secondaire redémarre. Cette procédure peut durer plusieurs minutes. Une fois le redémarrage effectué, un message de confirmation s'affiche.

Paramètres de cluster avancés

Vous ne pouvez pas modifier le fuseau horaire dans la configuration d'un cluster.

➢ *Pour configurer les paramètres de cluster avancés :*

1. Sélectionnez le nœud primaire.
2. Cliquez sur **Options avancées**. La fenêtre **Paramètres avancés** s'affiche.
3. Dans le champ **Intervalle de temps**, entrez la fréquence à laquelle CC-SG doit vérifier sa connexion avec l'autre nœud.

   Remarque : un intervalle de temps court augmente le trafic réseau généré par les tests de détection de collision consécutifs. Les clusters dont les nœuds sont très éloignés l'un de l'autre peuvent nécessiter des intervalles plus longs.

4. Dans le champ **Seuil de défaillance**, entrez le nombre de tests de détection de collision consécutifs qui doivent être exécutés sans réponse avant qu'un nœud CC-SG ne soit considéré comme défaillant.
5. Dans le champ **Récupération après**, entrez le nombre de tests de détection de collision consécutifs qui doivent être renvoyés avec succès avant qu'une connexion défaillante ne soit considérée comme étant récupérée.

6. Cliquez sur **OK** pour enregistrer les modifications.

Gestionnaire de sécurité

Le Gestionnaire de sécurité permet d'administrer l'accès fourni par CC-SG aux utilisateurs. Dans le Gestionnaire de sécurité, vous pouvez configurer des méthodes d'authentification, l'accès SSL, le chiffrement AES, les règles de mot de passe fort et de verrouillage, le portail de connexion, les certificats et les listes de contrôle d'accès.

Authentification à distance

Reportez-vous à ***Authentification à distance*** (à la page 119) pour obtenir des instructions détaillées sur la configuration des serveurs d'authentification à distance.

Chiffrement AES

Vous pouvez configurer CC-SG afin de rendre obligatoire le chiffrement 128 bits AES entre votre client et le serveur CC-SG. Lorsque le chiffrement AES est requis, tous les utilisateurs doivent accéder à CC-SG à l'aide d'un client AES. Si ce chiffrement est obligatoire et que vous essayez d'accéder à CC-SG avec un navigateur non-AES, vous ne pourrez pas vous connecter à CC-SG.

Vérifier si votre navigateur accepte le chiffrement AES

Si vous ne savez pas si votre navigateur utilise AES, vérifiez auprès de son fabricant.

Vous pouvez également essayer de consulter le site Web suivant à l'aide du navigateur dont vous souhaitez tester la méthode de chiffrement : ***https://www.fortify.net/sslcheck.html***
https://www.fortify.net/sslcheck.html. Ce site Web peut détecter la méthode de chiffrement de votre navigateur et afficher un rapport. Raritan n'est pas affilié avec ce site Web.

Rendre le chiffrement AES obligatoire entre le client et CC-SG

Dans le Gestionnaire de sécurité, vous pouvez configurer CC-SG afin de rendre obligatoire le chiffrement AES pour des sessions entre le client et le serveur CC-SG.

1. Choisissez **Administration** > **Sécurité**.
2. Ouvrez l'onglet **Chiffrement**.

3. Cochez la case **Chiffrement AES obligatoire entre le client et le serveur**.
4. Un message apparaît pour vous prévenir que vos clients doivent utiliser le chiffrement AES pour se connecter à CC-SG lorsque cette option est sélectionnée. Cliquez sur **OK** pour confirmer.
   - Le champ **Longueur de clé** affiche 128. Le chiffrement 128 bits sera obligatoire entre votre client et le serveur CC-SG.
   - Le champ **Protocole de connexion du navigateur** indique que HTTPS/SSL est sélectionné.
5. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Configurer le protocole de connexion du navigateur : HTTP ou HTTPS/SSL

Dans le Gestionnaire de sécurité, vous pouvez configurer CC-SG afin d'utiliser des connexions HTTP standard de clients, ou pour rendre les connexions HTTPS/SSL obligatoires. Vous devez redémarrer CC-SG pour que les modifications apportées à ce paramètre entrent en vigueur.

1. Choisissez **Administration** > **Sécurité**.
2. Ouvrez l'onglet **Chiffrement**.
3. Sélectionnez l'option **HTTP** ou **HTTP/SSL** pour spécifier le protocole de connexion du navigateur que vos clients doivent utiliser pour se connecter à CC-SG.
4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Paramétrer le numéro de port pour l'accès SSH à CC-SG

Dans le Gestionnaire de sécurité, vous pouvez définir le numéro du port que vous souhaitez utiliser pour l'accès SSH à CC-SG. Reportez-vous à **Accès SSH à CC-SG** (à la page 217) pour plus d'informations.

➢ *Pour définir le numéro de port pour l'accès SSH à CC-SG :*

1. Choisissez **Administration** > **Sécurité**.
2. Dans l'onglet **Chiffrement**, entrez le numéro de port pour l'accès à CC-SG via SSH dans le champ **Port de serveur SSH**.
3. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Paramètres de connexion

L'onglet **Paramètres de connexion** permet de configurer les options **Paramètres de mot de passe fort** et **Paramètres de verrouillage**.

Afficher les paramètres de connexion

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet **Paramètres de connexion**.

Mots de passe forts obligatoires pour tous les utilisateurs

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet **Paramètres de connexion**.
3. Cochez la case **Mots de passe forts obligatoires pour tous les utilisateurs**.
4. Sélectionnez la **longueur de mot de passe maximum**. Les mots de passe doivent contenir moins de caractères que le nombre maximum.
5. Sélectionnez une **profondeur d'historique du mot de passe**. Ce nombre indique le nombre de mots de passe conservés dans l'historique et non réutilisables. Par exemple, si le champ **Profondeur d'historique du mot de passe** indique 5, les utilisateurs ne peuvent pas réutiliser leurs 5 derniers mots de passe.
6. Sélectionnez une **fréquence d'expiration du mot de passe**. Tous les mots de passe expirent après un nombre défini de jours. Après l'expiration du mot de passe, les utilisateurs devront en choisir un nouveau à la connexion suivante.
7. Sélectionnez des **exigences du mot de passe fort** :
   - Les mots de passe doivent contenir au moins une lettre minuscule.
   - Les mots de passe doivent contenir au moins une lettre majuscule.
   - Les mots de passe doivent contenir au moins un nombre.
   - Les mots de passe doivent contenir au moins un caractère spécial (par exemple, un point d'exclamation ou une perluète).
8. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

A propos des mots de passe CC-SG

Tous les mots de passe doivent remplir tous les critères configurés par l'administrateur. Une fois les règles de mot de passe fort définies, tous les mots de passe suivants doivent les respecter. Tous les utilisateurs existants doivent modifier leurs mots de passe à la connexion suivante si les nouveaux critères sont plus forts que les précédents. Les règles de mot de passe fort ne s'appliquent qu'aux profils utilisateur enregistrés en local. Les règles de mot de passe sur un serveur d'authentification doivent être gérées par le serveur d'authentification.

En outre, une séquence identique de quatre caractères ne peut pas figurer à la fois dans le nom d'utilisateur et le mot de passe.

Les règles de mot de passe fort exigent que les utilisateurs respectent des instructions strictes lors de la création de mots de passe afin que ces derniers soient plus difficiles à deviner, et donc plus sûrs, en théorie. Les mots de passe forts ne sont pas activés par défaut dans CC-SG. Un mot de passe respectant tous les paramètres en matière de mot de passe fort est toujours obligatoire pour le super utilisateur CC.

Vous pouvez utiliser la fonction **Message du jour** pour prévenir les utilisateurs que les règles de mot de passe fort vont changer et indiquer les nouveaux critères.

Paramètres de verrouillage

Les administrateurs peuvent verrouiller les utilisateurs de CC-SG, de CC-NOC et de SSH après un nombre donné d'échecs de tentative de connexion. Cette fonction s'applique aux utilisateurs authentifiés et autorisés localement par CC-SG. Elle ne s'applique pas aux utilisateurs qui sont authentifiés à distance par des serveurs externes. Reportez-vous à ***Configuration de l'authentification à distance*** (voir "Authentification à distance" à la page 119) pour plus d'informations.

Remarque *: par défaut, le compte* ***admin*** *est verrouillé pendant cinq minutes après trois échecs des tentatives de connexion. Pour* ***admin****, le nombre d'échecs de connexion avant et après verrouillage n'est pas configurable.*

➢ *Pour activer le verrouillage :*

1. Choisissez Administration > Sécurité.
2. Ouvrez l'onglet Paramètres de connexion.
3. Cochez la case Verrouillage activé.

4. Par défaut, trois échecs de connexion sont autorisés avant le verrouillage d'un utilisateur. Vous pouvez remplacer cette valeur par un chiffre compris entre 1 et 10.
5. Choisissez une stratégie de verrouillage :
   - Verrouiller pour la période : indiquez un délai, en minutes, pendant lequel l'utilisateur est verrouillé avant de pouvoir se connecter à nouveau. Le paramètre par défaut est de 5 minutes. Vous pouvez spécifier une période allant d'une minute à 1440 minutes (24 heures). Une fois le délai passé, l'utilisateur peut à nouveau se connecter. Pendant la période de verrouillage, l'administrateur peut à tout moment supplanter cette valeur et autoriser l'utilisateur à se reconnecter à CC-SG.
   - Verrouiller jusqu'à ce que l'Admin autorise l'accès : les utilisateurs sont verrouillés jusqu'à ce qu'un administrateur déverrouille leur compte.
6. (Facultatif) Renseignez le champ E-mail de notification de verrouillage. Une notification est envoyée à cette adresse lorsque le verrouillage se produit. Si le champ est vide, aucune notification n'est envoyée.
7. (Facultatif) Renseignez le champ Numéro de téléphone de l'administrateur. Ce numéro de téléphone sera affiché dans le message de notification envoyé lorsque le verrouillage se produit.
8. Cliquez sur Mettre à jour pour enregistrer vos modifications.

➢ *Pour désactiver le verrouillage :*

Lorsque vous désactivez un verrouillage, tous les utilisateurs verrouillés de CC-SG sont autorisés à se connecter.

1. Choisissez Administration > Sécurité.
2. Ouvrez l'onglet Paramètres de connexion.
3. Désactivez la case à cocher Verrouillage activé.
4. Cliquez sur Mettre à jour pour enregistrer vos modifications.

Autoriser les connexions simultanées par utilisateur

Vous pouvez autoriser plusieurs sessions simultanées sur CC-SG avec un même nom d'utilisateur.

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet **Paramètres de connexion**.

- Cochez **Super utilisateur** pour autoriser plusieurs connexions simultanées avec le compte Super utilisateur CC.
- Cochez **Administrateurs système** pour autoriser plusieurs connexions simultanées des comptes du groupe d'utilisateurs **System Administrators**.
- Cochez **Tous les autres utilisateurs** pour autoriser des connexions simultanées par tous les autres utilisateurs.

3. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Configurer le minuteur d'inactivité

Vous pouvez configurer le minuteur d'inactivité afin de spécifier combien de temps une session CC-SG peut rester inactive avant que l'utilisateur ne soit déconnecté de CC-SG.

Lorsqu'un utilisateur a ouvert des connexions à des nœuds, la session est considérée comme active et l'utilisateur ne sera pas déconnecté après l'expiration du minuteur d'inactivité.

➢ *Pour configurer le minuteur d'inactivité :*

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet **Paramètres de connexion**.
3. Entrez le délai d'inactivité souhaité dans le champ **Délai d'inactivité**.
4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Portail

Les paramètres de portail permettent aux administrateurs de configurer un logo et un accord d'accès pour accueillir les utilisateurs lorsqu'ils accèdent à CC-SG.

➢ *Pour configurer les paramètres de portail :*

1. Choisissez **Administration** > **Sécurité**.
2. Ouvrez l'onglet **Portail**.

Logo

Un petit fichier graphique peut être téléchargé dans CC-SG pour servir de bannière sur la page de connexion. La taille maximum du logo est de 998x170 pixels.

➢ *Pour télécharger un logo :*

1. Cliquez sur **Parcourir** dans la zone **Logo** de l'onglet Portail. Une boîte de dialogue Ouvrir apparaît.
2. Sélectionnez le fichier graphique que vous souhaitez utiliser comme logo dans la boîte de dialogue, puis cliquez sur **Ouvrir**.
3. Cliquez sur **Aperçu** pour prévisualiser le logo. Le fichier graphique sélectionné apparaît sur la droite.
4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Accord de service limité

Vous pouvez configurer un message qui apparaîtra sur la gauche des champs de l'écran de connexion. Ceci est destiné à servir d'accord de service limité, ou de déclaration que les utilisateurs acceptent lorsqu'ils accèdent à CC-SG. L'acceptation de l'accord de service limité par l'utilisateur est consignée dans les fichiers journaux et dans le rapport de journal d'audit.

➢ *Pour ajouter un accord de service limité à l'écran de connexion de CC-SG :*

1. Sélectionnez **Demander l'acceptation de l'accord de service limité** pour obliger les utilisateurs à cocher la case d'acceptation de l'écran de connexion avant de saisir leurs données de connexion.
2. Entrez votre message :
   a. Sélectionnez **Message de l'accord de service limité** si vous souhaitez entrer directement le texte de la bannière.
      - Tapez le texte de l'accord dans le champ prévu à cet effet. La longueur maximum du message est de 10 000 caractères.
      - Cliquez sur le menu déroulant **Police** et sélectionnez une police pour le message.
      - Cliquez sur le menu déroulant **Taille** et sélectionnez une taille de police pour le message.
   b. Sélectionnez **Fichier de l'accord de service limité** pour charger un message à partir d'un fichier texte (.TXT).

- Cliquez sur **Parcourir**. Une fenêtre de dialogue s'affiche.
- Dans cette fenêtre, sélectionnez le fichier texte contenant le message que vous souhaitez utiliser, puis cliquez sur **Ouvrir**. La longueur maximum du message est de 10 000 caractères.
- Cliquez sur **Aperçu** pour prévisualiser le texte du fichier. L'aperçu apparaît dans le champ de message de la bannière au-dessus.

3. Cliquez sur **Mettre à jour** pour enregistrer vos modifications. Les mises à jour apparaîtront sur l'écran de connexion la prochaine fois que l'utilisateur accède à CC-SG.

Certificats

Dans l'onglet Certificat, vous pouvez générer une demande de signature de certificat (CSR) à envoyer à une autorité de certification pour demander un certificat d'identité générique, générer un certificat auto-signé, ou importer et exporter des certificats et leurs clés privées.

Tâches relatives aux certificats

***Remarque** : le bouton **Exporter** au bas de l'écran devient **Importer** ou **Générer**, selon l'option de certificat sélectionnée.*

➢ *Exporter le certificat et la clé privée actuels*

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet **Certificat**.
3. Cliquez sur **Exporter le certificat et la clé privée actuels**.
4. Cliquez sur **Export**.

   Le certificat s'affiche dans le panneau **Certificat** ; la clé privée, dans le panneau **Clé privée**.
5. Dans chaque panneau, sélectionnez le texte et appuyez sur les touches CTRL+C pour le copier. Vous pouvez alors le coller où vous le souhaitez.

➢ *Générer une demande de signature de certificat et importer des certificat et clé privée collés*

La demande de signature de certificat est soumise au serveur de certificats qui émet un certificat signé. Un certificat racine est également exporté de ce serveur et enregistré dans un fichier. Après avoir reçu le certificat signé de l'autorité de certification, vous pouvez importer les certificat signé, certificat racine et clé privée.

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet **Certificat**.
3. Cliquez sur **Générer une demande de signature de certificat**, puis sur **Générer**.La fenêtre Générer une demande de signature de certificat s'affiche.
4. Entrez les données demandées dans les champs.
   a. Mode de chiffrement : si l'option **Chiffrement AES obligatoire entre le client et le serveur** est sélectionnée dans Administration > Sécurité > Chiffrement, AES-128 est la valeur par défaut. Si le chiffrement AES n'est pas obligatoire, 3DES est la valeur par défaut.
   b. Longueur de la clé privée : 1024 est la valeur par défaut.
   c. Période de validité (en jours) : 4 chiffres maximum.
   d. Code de pays : la balise CSR est le nom du pays.
   e. Etat ou province : 64 caractères au maximum. Entrez le nom complet de l'Etat ou le nom de la province. N'utilisez pas d'abréviation.
   f. Ville/Localité : la balise CSR est le nom de la localité. 64 caractères au maximum.
   g. Nom de société déposé : la balise CSR est le nom de l'organisation. 64 caractères au maximum.
   h. Nom de division/service : la balise CSR est le nom de l'unité organisationnelle. 64 caractères au maximum.
   i. Nom de domaine complètement qualifié : la balise CSR est le nom courant. La société indiquée le champ Nom de société déposé doit posséder le nom de domaine pour les demandes de signature de certificat. Sinon le service de signature rejettera la demande.
   j. Mot de passe challenge : 64 caractères au maximum.

k. Adresse électronique de l'administrateur : entrez l'adresse électronique de l'administrateur chargé de la demande de certificat.

5. Cliquez sur **OK** pour générer la demande de signature de certificat. Celle-ci et la clé privée apparaissent dans les champs correspondants de l'écran **Certificat**.
6. Sélectionnez le texte de la case Demande de certificat et appuyez sur les touches CTRL+C pour le copier. Dans un éditeur ASCII, tel que le Bloc-notes, copiez et collez la demande de signature de certificat dans un fichier et enregistrez celui-ci avec une extension **.cer**.
7. Sélectionnez le texte de la case Clé privée et appuyez sur les touches CTRL+C pour le copier. Dans un éditeur ASCII, tel que le Bloc-notes, copiez et collez la clé privée dans un fichier et enregistrez celui-ci avec une extension **.txt**.
8. Envoyez le **fichier .cer** au serveur de certificats pour obtenir un certificat signé.
9. Téléchargez ou exportez le certificat racine du serveur et enregistrez-le dans un fichier avec l'extension **.cer**. Il s'agit d'un certificat différent du certificat signé qui sera émis par le serveur de certificats à l'étape suivante.
10. Cliquez sur **Parcourir** à côté de **Fichier de l'AC** et sélectionnez le fichier du certificat racine.
11. Lorsque vous avez reçu le certificat signé du serveur, cliquez sur **Importer le certificat et la clé privée copiés**.
12. Copiez le texte du certificat signé et appuyez sur les touches CTRL+V pour le coller dans la case Certificat.
13. Copiez le texte de la clé privée enregistrée précédemment dans un fichier .txt et appuyez sur les touches CTRL+V pour le coller dans la case Clé privée.
14. Tapez **raritan** dans le champ **Mot de passe** si la demande de signature de certificat a été générée par CC-SG. Si une application différente a généré la demande, utilisez le mot de passe associé à cette application.

***Remarque** : si le certificat importé est signé par une autorité de certification (AC) racine et sous-racine, l'utilisation d'un certificat racine ou sous-racine uniquement échouera. Pour résoudre ce problème, copiez et collez les certificats racine et sous-racine dans un fichier, puis importez ce dernier.*

➢ *Générer un certificat auto-signé*

1. Choisissez **Administration** > **Sécurité**.
2. Cliquez sur l'onglet **Certificat**.
3. Cliquez sur **Générer un certificat auto-signé**, puis sur **Générer**. La fenêtre **Générer un certificat auto-signé** s'affiche.
4. Entrez les données demandées dans les champs.
   a. Mode de chiffrement : si l'option **Chiffrement AES obligatoire entre le client et le serveur** est sélectionnée dans Administration > Sécurité > Chiffrement, AES-128 est la valeur par défaut. Si le chiffrement AES n'est pas obligatoire, 3DES est la valeur par défaut.
   b. Longueur de la clé privée : 1024 est la valeur par défaut.
   c. Période de validité (en jours) : 4 chiffres maximum.
   d. Code de pays : la balise CSR est le nom du pays.
   e. Etat ou province : 64 caractères au maximum. Entrez le nom complet de l'Etat ou le nom de la province. N'utilisez pas d'abréviation.
   f. Ville/Localité : la balise CSR est le nom de la localité. 64 caractères au maximum.
   g. Nom de société déposé : la balise CSR est le nom de l'organisation. 64 caractères au maximum.
   h. Nom de division/service : la balise CSR est le nom de l'unité organisationnelle. 64 caractères au maximum.
   i. Nom de domaine complètement qualifié : la balise CSR est le nom courant. La société indiquée le champ Nom de société déposé doit posséder le nom de domaine pour les demandes de signature de certificat. Sinon le service de signature rejettera la demande.
   j. Mot de passe challenge : 64 caractères au maximum.
   k. Adresse électronique de l'administrateur : entrez l'adresse électronique de l'administrateur chargé de la demande de certificat.

5. Cliquez sur **OK** pour générer le certificat. Le certificat et la clé privée s'affichent sous forme cryptée dans les champs correspondants de l'écran **Certificat**.

Liste de contrôle d'accès

Une liste de contrôle d'accès IP définit des plages d'adresses IP de client pour lesquelles vous souhaitez refuser ou autoriser l'accès à CC-SG. Chaque entrée de la liste de contrôle d'accès devient une règle qui détermine si un utilisateur d'un certain groupe, avec une adresse IP particulière, peut accéder à CC-SG. Vous pouvez également définir des règles à appliquer à tout le système CC-SG (sélectionnez Système au lieu d'un groupe d'utilisateurs) au niveau du système d'exploitation. Lorsque vous avez créé des règles, vous pouvez les classer dans la liste afin de définir l'ordre dans lequel elles sont appliquées. Les règles au sommet de la liste ont priorité sur celles des positions inférieures.

➢ *Pour afficher une liste de contrôle d'accès :*

1. Choisissez Administration > Sécurité.
2. Cliquez sur l'onglet Liste de contrôle d'accès.

➢ *Pour ajouter une règle à la liste de contrôle d'accès :*

1. Choisissez Administration > Sécurité.
2. Cliquez sur l'onglet Liste de contrôle d'accès.
3. Cliquez sur l'icône Ajouter une nouvelle ligne pour ajouter une rangée à la table.
4. Indiquez une plage d'adresses IP auxquelles appliquer la règle en entrant la valeur de la première adresse IP dans le champ De l'adresse IP et celle de la dernière dans le champ A l'adresse IP.
5. Cliquez sur la flèche déroulante Groupe pour sélectionner le groupe d'utilisateurs auquel la règle doit être appliquée. Sélectionnez Système pour appliquer la règle à tout le système CC-SG.
6. Cliquez sur la flèche déroulante Action et sélectionnez Autoriser ou Refuser pour indiquer si les utilisateurs spécifiés dans la plage d'adresses IP peuvent accéder à CC-SG.
7. Cliquez sur Mettre à jour pour enregistrer vos modifications.

➢ *Pour ajouter une règle à la liste de contrôle d'accès pour autoriser ou refuser l'accès au niveau du système d'exploitation :*

1. Choisissez Administration > Sécurité.
2. Cliquez sur l'onglet Liste de contrôle d'accès.
3. Cliquez sur l'icône Ajouter une nouvelle ligne pour ajouter une rangée à la table.
4. Indiquez une plage d'adresses IP auxquelles appliquer la règle en entrant la valeur de la première adresse IP dans le champ De l'adresse IP et celle de la dernière dans le champ A l'adresse IP.
5. Choisissez Groupe > Système.
6. Cliquez sur la flèche déroulante Action et sélectionnez Autoriser ou Refuser pour indiquer si les utilisateurs spécifiés dans la plage d'adresses IP peuvent accéder à CC-SG.
7. Cliquez sur Mettre à jour pour enregistrer vos modifications.

➢ *Pour modifier l'ordre dans lequel CC-SG applique les règles :*

1. Choisissez Administration > Sécurité.
2. Cliquez sur l'onglet Liste de contrôle d'accès.
3. Sélectionnez une règle que vous souhaitez faire monter ou descendre dans la liste.
4. Cliquez sur les touches fléchées haut et bas jusqu'à ce que la règle soit bien positionnée.
5. Cliquez sur Mettre à jour pour enregistrer vos modifications.

➢ *Pour retirer une règle de la liste de contrôle d'accès :*

1. Choisissez Administration > Sécurité.
2. Cliquez sur l'onglet Liste de contrôle d'accès.
3. Sélectionnez la règle que vous souhaitez retirer, puis cliquez sur l'icône Supprimer la ligne.
4. Cliquez sur Mettre à jour pour enregistrer vos modifications.

Gestionnaire des notifications

Utilisez le gestionnaire des notifications pour configurer un serveur SMTP externe de manière à envoyer des notifications de CC-SG. Les notifications servent à envoyer par courrier électronique des rapports programmés, des rapports de verrouillage d'utilisateurs, l'état des tâches programmées qui ont échoué ou abouti. ***Gestionnaire des tâches*** (à la page 207) Après avoir configuré le serveur SMTP, vous pouvez choisir d'envoyer un e-mail de test au destinataire désigné pour le prévenir du résultat du test.

Configurer un serveur SMTP externe

1. Choisissez **Administration** > **Notifications**.
2. Cochez la case **Activer notification SMTP**.
3. Renseignez le champ **Hôte SMTP**. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2).
4. Entrez un numéro de port SMTP valide dans le champ **Port SMTP**.
5. Entrez un nom de compte valide permettant la connexion au serveur SMTP dans le champ **Nom du compte**.
6. Entrez le mot de passe du nom de compte dans les champs **Mot de passe** et **Entrez à nouveau le mot de passe**.
7. Entrez une adresse e-mail dans le champ **De** afin d'indiquer que les messages proviennent de CC-SG.
8. Dans le champ **Tentatives d'envoi**, entrez le nombre de fois où les messages électroniques doivent être renvoyés en cas d'échec.
9. Dans le champ **Intervalle de tentative d'envoi (en minutes)**, entrez le nombre de minutes, entre 1 et 60, qui doivent s'écouler entre les tentatives d'envoi.
10. Cochez **Utiliser SSL** si vous souhaitez un envoi sécurisé des messages via Secure Sockets Layer (SSL).
11. Cliquez sur **Tester la configuration** pour envoyer un message de test au compte SMTP spécifié. Assurez-vous que le message est bien arrivé.
12. Cliquez sur **Mettre à jour la configuration** pour enregistrer vos modifications.

Gestionnaire des tâches

Utilisez le gestionnaire des tâches pour programmer des tâches CC-SG quotidiennes, hebdomadaires, mensuelles ou annuelles. Une tâche peut être programmée pour une exécution unique ou périodique à un jour de la semaine particulier et à un intervalle défini. Par exemple, vous pouvez programmer des sauvegardes de dispositif toutes les trois semaines le vendredi ou planifier l'envoi d'un rapport particulier par e-mail à un ou plusieurs destinataires tous les lundis.

***Remarque** : le Gestionnaire des tâches utilise l'heure du serveur définie dans CC-SG pour la programmation, et non celle de votre PC client. L'heure du serveur s'affiche dans l'angle supérieur droit de chaque écran CC-SG.*

Types de tâches

Les tâches suivantes peuvent être programmées :

- Sauvegarder CC-SG
- Sauvegarde de la configuration du dispositif (dispositif individuel ou groupe de dispositifs)
- Copie de la configuration du dispositif (dispositif individuel ou groupe de dispositifs)
- Regrouper la gestion de l'alimentation
- Gestion de l'alimentation
- Purger des journaux
- Redémarrer un dispositif
- Restauration de la configuration du dispositif (ne s'applique pas aux groupes de dispositifs)
- Mise à niveau du firmware du dispositif (dispositif individuel ou groupe de dispositifs)
- Génération de tous les rapports (formats HTML ou CSV)

Programmer des tâches séquentielles

Nous vous recommandons de programmer des tâches de manière séquentielle afin de confirmer qu'un comportement attendu s'est effectivement produit. Vous pouvez, par exemple, programmer une tâche Mettre à niveau le firmware du dispositif pour un groupe de dispositifs donné et la faire immédiatement suivre d'une tâche Rapport de gestion du parc afin de confirmer que les versions correctes du firmware ont été mises à niveau.

Envoyer des notifications de tâches par e-mail

Une fois la tâche effectuée, un e-mail peut être envoyé à un destinataire particulier. Dans le ***Gestionnaire des notifications*** (à la page 206), vous pouvez spécifier la destination et le mode d'envoi du message, par exemple s'il est envoyé de manière sécurisée via SSL.

Rapports programmés

Les rapports programmés sont envoyés par courrier électronique aux destinataires définis.

Tous les rapports avec un état **Terminé** sont stockés sur CC-SG pendant 30 jours. Vous pouvez afficher les rapports terminés au format HTML en sélectionnant **Rapports programmés** dans le menu **Rapports**. Reportez-vous à ***Rapports programmés*** (à la page 152) pour plus d'informations.

Programmer une tâche

Cette section présente la plupart des tâches programmables. Reportez-vous à ***Programmer la mise à niveau du firmware d'un dispositif*** (à la page 211) pour en savoir plus sur ces mises à niveau.

➢ *Pour programmer une tâche :*

1. Choisissez **Administration** > **Tâches**.
2. Cliquez sur **Nouveau**.
3. Dans l'onglet **Principale**, entrez un nom (1 à 32 caractères alphanumériques ou soulignés, aucun espace) et une description pour la tâche.
4. Cliquez sur l'onglet **Données de la tâche**.
5. Cliquez sur le menu déroulant **Exécution de la tâche** et sélectionnez la tâche que vous souhaitez programmer. Notez que les champs obligatoires varient suivant la tâche sélectionnée. Reportez aux sections suivantes pour en savoir plus sur chaque tâche :
   - ***Sauvegarder CC-SG*** (voir "Sauvegarde de CC-SG" à la page 156)
   - ***Sauvegarder la configuration du dispositif*** (voir "Sauvegarde de la configuration du dispositif" à la page 42)
   - ***Copier la configuration du dispositif*** (voir "Copie de la configuration du dispositif" à la page 46)

- ***Regrouper la gestion de l'alimentation*** (voir "Gestion de l'alimentation d'un groupe de noeuds" à la page 18)
- Gérer l'alimentation : reportez-vous au manuel d'utilisation de CC-SG.
- ***Purger des journaux*** (voir "Configuration de l'activité d'enregistrement" à la page 179)
- ***Redémarrer un dispositif*** (voir "Redémarrage du dispositif" à la page 46)
- ***Restaurer la configuration du dispositif*** (voir "Restauration de la configuration du dispositif" à la page 43) (ne s'applique pas aux groupes de dispositifs)
- ***Générer tous les rapports*** (voir "Rapports" à la page 140)
- ***Mettre à niveau le firmware du dispositif*** (voir "Programmer la mise à niveau du firmware d'un dispositif" à la page 211) (dispositif individuel ou groupe de dispositifs)

6. Cliquez sur l'onglet **Périodicité**. L'onglet **Périodicité** est désactivé pour les ***tâches de mise à niveau du firmware du dispositif*** (voir "Programmer la mise à niveau du firmware d'un dispositif" à la page 211).
7. Dans le champ **Période**, cliquez sur la case d'option correspondant à la fréquence souhaitée de la tâche programmée.
   a. **Une fois :** utilisez les flèches haut et bas pour sélectionner l'**heure de début** de la tâche.
   b. **Périodique :** utilisez les flèches haut et bas pour sélectionner l'**heure de début** de la tâche. Entrez le nombre d'exécutions souhaitées de la tâche dans le champ **Nombre de répétitions**. Entrez le délai qui doit s'écouler entre les répétitions dans le champ **Intervalle de répétition**. Cliquez sur le menu déroulant et sélectionnez l'unité de temps dans la liste.
   c. **Quotidienne :** cliquez sur la case d'option en regard de **Chaque jour** si vous souhaitez que la tâche se répète 7 jours par semaine. Cliquez sur la case d'option en regard de **Chaque jour de la semaine** si vous souhaitez que la tâche se répète chaque jour, du lundi au vendredi.
   d. **Hebdomadaire :** utilisez les flèches haut et bas pour sélectionner le nombre de semaines qui doivent s'écouler entre les exécutions de la tâche, puis cochez la case en regard de chaque jour où la tâche doit avoir lieu les semaines où elle est exécutée.

e. **Mensuelle :** entrez la date d'exécution dans le champ **Jours**, puis cochez la case en regard de chaque mois où la tâche doit avoir lieu à la date spécifiée.

f. **Annuelle :** cliquez sur le menu déroulant et sélectionnez le mois d'exécution de la tâche dans la liste. Utilisez les flèches haut et bas pour sélectionner le jour du mois d'exécution de la tâche.

8. Pour les tâches **quotidiennes**, **hebdomadaires**, **mensuelles** et **annuelles**, vous devez ajouter une heure de début et de fin dans la section **Plage de périodicité**. Utilisez les flèches haut et bas pour sélectionner l'heure de début (champ **Commence à**) et la **date de début**. Cliquez sur la case d'option en regard de **Pas de date de fin** si la tâche doit avoir lieu indéfiniment. Ou, cliquez sur la case d'option en regard de **Date de fin**, puis utilisez les flèches haut et bas pour sélectionner la date à laquelle la tâche ne doit plus se produire.

9. Cliquez sur l'onglet **Nouvelle tentative**.

10. Si une tâche échoue, CC-SG peut réessayer ultérieurement comme indiqué dans l'onglet **Nouvelle tentative**. Entrez le nombre de fois où CC-SG peut exécuter à nouveau la tâche dans le champ Nombre de nouvelles tentatives. Entrez le délai qui doit s'écouler entre les tentatives dans le champ **Intervalle entre tentatives**. Cliquez sur le menu déroulant et sélectionnez l'unité de temps dans la liste.

Important : si vous programmez une tâche pour mettre à niveau des dispositifs SX ou KX, définissez un intervalle entre tentatives de plus de 20 minutes, car l'opération prend environ 20 minutes.

---

11. Cliquez sur l'onglet **Notification**.

12. Indiquez les adresses électroniques auxquelles une notification doit être envoyée en cas de réussite ou d'échec d'une tâche. Par défaut, l'adresse électronique de l'utilisateur connecté est disponible. Les adresses électroniques des utilisateurs sont configurées dans le profil utilisateur. Pour ajouter une autre adresse, cliquez sur **Ajouter**, entrez l'adresse électronique dans la fenêtre qui apparaît, puis cliquez sur **OK**. Par défaut, un e-mail est envoyé si l'exécution de la tâche aboutit. Pour prévenir les destinataires de l'échec des tâches, cochez la case **En cas d'échec**.

13. Cliquez sur **OK** pour enregistrer les modifications.

Raritan.
When you're ready to take control®

Programmer la mise à niveau du firmware d'un dispositif

Vous pouvez programmer une tâche pour mettre à niveau plusieurs dispositifs de même type, tel que KX ou SX, au sein d'un groupe de dispositifs. Lorsque la tâche débute, un rapport Mise à niveau du firmware d'un dispositif est disponible dans le menu Rapports > Rapports programmés pour visualiser le statut de l'opération en temps réel. Ce rapport est également envoyé par courriel si l'option est paramétrée dans l'onglet Notification.

Reportez-vous au manuel d'utilisation Raritan de chaque dispositif pour obtenir une estimation de la durée de la mise à niveau.

➢ *Pour programmer une mise à niveau du firmware d'un dispositif :*

1. Choisissez Administration > Tâches.
2. Cliquez sur Nouveau.
3. Dans l'onglet Principale, entrez le nom et la description de la tâche. Le nom choisi identifiera la tâche et le rapport associé.
4. Ouvrez l'onglet Données de la tâche.
5. Indiquez les détails de la mise à niveau du dispositif :
   a. Exécution de la tâche : sélectionnez Mettre à niveau le firmware du dispositif.
   b. Groupe de dispositifs : sélectionnez le groupe contenant les dispositifs à mettre à niveau.
   c. Type de dispositif : sélectionnez le type de dispositif à mettre à niveau. Si vous devez mettre à niveau plusieurs types de dispositifs, vous devez programmer une tâche pour chacun.
   d. Mises à niveau simultanées : indiquez le nombre de dispositifs qui doivent démarrer la partie transfert de fichiers de la mise à niveau simultanément ; 10 au maximum. Dès qu'un transfert se termine, un nouveau démarre pour garantir que seul le nombre maximum de transferts simultanés a lieu.
   e. Fichier de mise à niveau : sélectionnez la version de firmware cible de la mise à niveau. Seuls les fichiers de mise à jour disponibles adaptés au type de dispositif sélectionné sont présentés comme choix.
6. Définissez la période de la mise à niveau :

a. Date/Heure de début : sélectionnez la date et l'heure de début de la tâche. Elles doivent être postérieures à la date et à l'heure en cours.

b. Fenêtre de restriction de mise à niveau et Date/heure de début de la dernière mise à niveau : si toutes les mises à niveau doivent être exécutées sur une durée spécifique, utilisez ces champs pour indiquer la date et l'heure après lesquelles aucune nouvelle mise à niveau ne peut débuter. Sélectionnez Fenêtre de restriction de mise à niveau pour activer le champ Date/heure de début de la dernière mise à niveau.

7. Indiquez les dispositifs à mettre à niveau et leur séquence. Placez les dispositifs prioritaires en haut de la liste :

   a. Dans la liste Disponible, sélectionnez chaque dispositif à mettre à niveau et cliquez sur Ajouter pour le placer dans la liste Sélectionné.

   b. Dans la liste Sélectionné, choisissez un dispositif et utilisez les boutons fléchés pour le placer à l'endroit souhaité pour définir l'ordre de réalisation des mises à niveau.

8. Ouvrez l'onglet Nouvelle tentative. Indiquez si une nouvelle tentative doit être effectuée pour les mises à niveau ayant échoué.

   a. Nombre de nouvelles tentatives : entrez le nombre de fois où CC-SG doit tenter à nouveau une mise à niveau ayant échoué.

   b. Intervalle entre tentatives : entrez la durée qui doit s'écouler entre les tentatives. Les durées par défaut sont de 30, 60 et 90 minutes. Il s'agit des intervalles entre tentatives optima.

9. Ouvrez l'onglet Notification. Indiquez les adresses électroniques devant recevoir une notification de réussite ou d'échec. Par défaut, l'adresse électronique de l'utilisateur connecté est disponible. Les adresses électroniques des utilisateurs sont configurées dans le profil utilisateur.

   a. Cliquez sur Ajouter, entrez l'adresse électronique dans la fenêtre qui s'affiche, puis cliquez sur OK.

   b. Sélectionnez En cas d'échec si vous souhaitez envoyer un message si une mise à niveau échoue.

   c. Sélectionnez En cas de réussite si vous souhaitez envoyer un message lorsque toutes les mises à niveau aboutissent.

10. Cliquez sur OK pour enregistrer vos modifications.

Raritan.
When you're ready to take control®

Lorsque la tâche démarre, vous pouvez ouvrir le rapport Mise à niveau du firmware d'un dispositif à tout moment au cours de la période programmée pour voir le statut des opérations. Reportez-vous à ***Rapport Mise à niveau du firmware d'un dispositif*** (à la page 153) pour plus d'informations.

Afficher une tâche, les détails d'une tâche et l'historique des tâches

Si une tâche est modifiée ou mise à jour, son historique antérieur n'est plus valable et la date de dernière exécution reste vide.

➢ *Pour afficher une tâche :*

1. Choisissez **Administration** > **Tâches**.
2. Pour rechercher des tâches, utilisez les boutons haut et bas pour sélectionner la période qui doit être couverte par la recherche. Vous pouvez filtrer la liste davantage en sélectionnant une ou plusieurs tâches, un ou plusieurs états ou un ou plusieurs propriétaires (**Ctrl+clic**). Cliquez sur **Afficher les tâches** pour visualiser la liste de tâches.
   - Pour effacer une tâche, sélectionnez-la, puis cliquez sur **Supprimer**.

   Remarque : vous ne pouvez pas supprimer une tâche en cours d'exécution.

   - Pour afficher l'historique d'une tâche, sélectionnez-la et cliquez sur **Historique des tâches**.
   - Pour afficher les détails d'une tâche, double-cliquez dessus.
   - Pour changer une tâche programmée, sélectionnez-la, puis cliquez sur **Modifier** pour ouvrir la fenêtre Modifier la tâche. Modifiez les spécifications de la tâche selon vos besoins, puis cliquez sur **Mettre à jour**. Reportez-vous à **Programmer une tâche** pour obtenir une description des onglets.
   - Pour créer une tâche en fonction d'une tâche configurée précédemment, sélectionnez la tâche à copier, puis cliquez sur **Enregistrer sous** pour ouvrir la fenêtre Enregistrer la tâche sous. Les informations de la tâche configurée précédemment sont indiquées dans les onglets. Modifiez les spécifications de la tâche selon vos besoins, puis cliquez sur **Mettre à jour**. Reportez-vous à ***Programmer une tâche*** (à la page 208) et à ***Programmer la mise à niveau du firmware d'un dispositif*** (à la page 211) pour obtenir une description des onglets.

CommandCenter NOC

L'ajout d'un CommandCenter NOC (CC-NOC) à votre configuration permet de développer vos capacités de gestion des cibles. Vous bénéficiez en effet de services de surveillance, de création de rapports et d'alerte pour vos systèmes cible série et KVM. Reportez-vous à la documentation CommandCenter NOC Raritan pour plus d'informations sur l'installation et le fonctionnement de votre console CC-NOC.

Pour créer une connexion valide entre l'unité CC-SG et la console CC-NOC, vous devriez synchroniser les paramètres de date et d'heure de chacune. Elles doivent être configurées pour utiliser un serveur NTP.

Ajouter un CC-NOC

Vous devez fournir les codes de passe générés à l'administrateur qui doit les intégrer à CC-NOC dans les cinq minutes. Evitez de transmettre ces codes par e-mail ou tout autre moyen électronique pour empêcher une interception éventuelle par des systèmes automatisés. Il est recommandé de les transmettre par téléphone ou par écrit à des intervenants de confiance.

1. Dans le menu **Accès**, cliquez sur **Configuration CC-NOC**.
2. Cliquez sur **Ajouter**.
3. Sélectionnez la version de logiciel CC-NOC à ajouter et cliquez sur **Suivant**. La version 5.1 comporte moins de fonctionnalités d'intégration que la version 5.2 et les versions ultérieures, et ne nécessite qu'un nom et une adresse IP. Consultez le site Web du support Raritan pour en savoir plus sur CC-NOC 5.1.
4. Entrez un nom descriptif de la console CC-NOC dans le champ **Nom du CC-NOC**. La longueur maximum est de 50 caractères alphanumériques.
5. Entrez l'adresse IP ou le nom d'hôte de la console CC-NOC dans le champ **Adresse IP/nom d'hôte du CC-NOC**. Ce champ est obligatoire. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2).

6. Pour extraire des informations quotidiennes sur les cibles de la base de données CC-NOC, tapez une plage de détection dans les champs **Plage IP de** et **Plage IP à**. CC-SG demande que CC-NOC lui envoie des événements pour les dispositifs de cette plage d'adresses IP. Celle-ci est associée à la plage de détection configurée dans la console CC-NOC. Pour plus de détails, reportez-vous au **manuel de l'administrateur du CommandCenter NOC** de Raritan. Entrez une plage en gardant les règles suivantes à l'esprit :

Plage d'adresses IP	Description
Si la plage CC-SG entrée ici est un sous-ensemble de la plage configurée dans CC-NOC…	…alors, CC-NOC retourne toutes les informations connues des dispositifs cible inclus dans cette plage.
Si la plage CC-SG entrée ici comporte une liste partielle (intersection non null) de la plage configurée dans CC-NOC…	…alors, CC-NOC retourne toutes les informations connues des dispositifs cible inclus dans la plage d'intersection.
Si la plage CC-SG est un surensemble de la plage configurée dans CC-NOC…	…alors, CC-NOC retourne toutes les informations connues des dispositifs cible inclus dans cette plage. CC-NOC retourne essentiellement les cibles définies dans la plage de CC-NOC.
Si la plage CC-SG ne chevauche pas la plage configurée dans CC-NOC…	…alors, CC-NOC ne retourne aucune information de dispositifs cible.

Remarque : utilisez le rapport Synchronisation CC-NOC pour visualiser les cibles auxquelles l'unité CC-SG est abonnée. Le rapport affiche également les nouvelles cibles détectées par CC-NOC. Reportez-vous à ***Rapport Synchronisation CC-NOC*** (à la page 153) pour plus d'informations.

1. Indiquez une **durée de synchronisation** pour programmer l'extraction des informations cible de la base de données CC-NOC. Les bases de données sont alors actualisées au fur et à mesure que les cibles sont détectées ou deviennent non gérées. La valeur par défaut est l'heure en cours sur l'ordinateur client. Vous pouvez programmer la synchronisation pendant les heures creuses pour ne pas affecter les autres processus.

2. Dans le champ **Intervalle de test de détection de collision**, entrez la fréquence (en secondes) à laquelle CC-SG envoie un message de détection de collision à la console CC-NOC. Ceci confirme si celle-ci est toujours active et disponible. La valeur par défaut est **60** secondes. Les valeurs autorisées sont comprises entre **30 et 120** secondes.
3. Dans le champ **Tentatives de test de détection de collision en cas d'échec**, entrez le nombre de tests de détection de collision consécutifs qui doivent être exécutés sans réponse avant qu'un nœud CC-NOC ne soit considéré comme défaillant. La valeur par défaut est **2** tests de détection de collision. Les valeurs autorisées sont comprises entre **2 et 4** tests.
4. Cliquez sur **Suivant**.
5. Copiez et collez les codes de passe dans les champs CC-NOC si vous êtes l'administrateur concerné, ou soumettez les deux codes à l'administrateur.

Important : pour améliorer la sécurité, vous devez entrer les codes de passe dans la console CC-NOC dans les cinq minutes suivant leur génération sur CC-SG. Ceci réduit la possibilité pour les intrus de pénétrer dans le système par une attaque de force. Evitez de transmettre ces codes par e-mail ou tout autre moyen électronique pour empêcher une interception éventuelle par des systèmes automatisés. Il est recommandé de les transmettre par téléphone ou par écrit à des intervenants de confiance.

Une fois l'échange de certificats terminé, un canal sécurisé est établi entre le CC-NOC et l'unité CC-SG. Les données du CC-NOC sont copiées sur l'unité CC-SG. Cliquez sur **OK** pour terminer la procédure. Si celle-ci ne prend pas fin dans les **5** minutes, le délai expire, les données ne sont pas enregistrées sur l'unité CC-SG et les certificats stockés sont supprimés. Vous devez répéter la procédure.

Remarque : *CommandCenter NOC ne peut être ajouté qu'à des unités CC-SG autonomes ou à des nœuds primaires d'unités CC-SG en cluster.*

Modifier un CC-NOC

➢ *Pour modifier un CC-NOC :*

1. Choisissez **Accès** > **Configuration CC-NOC**.
2. Mettez en surbrillance un CC-NOC dans la liste et cliquez sur **Modifier**.

3. Modifiez la configuration selon vos besoins.

Lancer un CC-NOC

➢ *Pour lancer un CC-NOC à partir de l'unité CC-SG :*

1. Choisissez **Accès** > **Configuration CC-NOC**.
2. Dans l'écran Configuration CC-NOC, sélectionnez un CC-NOC disponible.
3. Cliquez sur **Lancer**. Le système se connecte alors à une unité CC-NOC configurée.

Supprimer un CC-NOC

1. Choisissez **Accès** > **Configuration CC-NOC**.
2. Sélectionnez le CC-NOC à retirer de CC-SG, puis cliquez sur **Supprimer**. Un message de confirmation apparaît.
3. Cliquez sur **Oui** pour supprimer le CC-NOC. Un message apparaît lorsque le CC-NOC a été supprimé.

Accès SSH à CC-SG

Utilisez des clients Secure Shell (SSH), tels que Putty ou OpenSHH Client, pour accéder à une interface de ligne de commande vers un serveur SSH (v2) sur CC-SG. Seul un sous-ensemble des commandes CC-SG est accessible via SSH pour administrer des dispositifs et CC-SG lui-même.

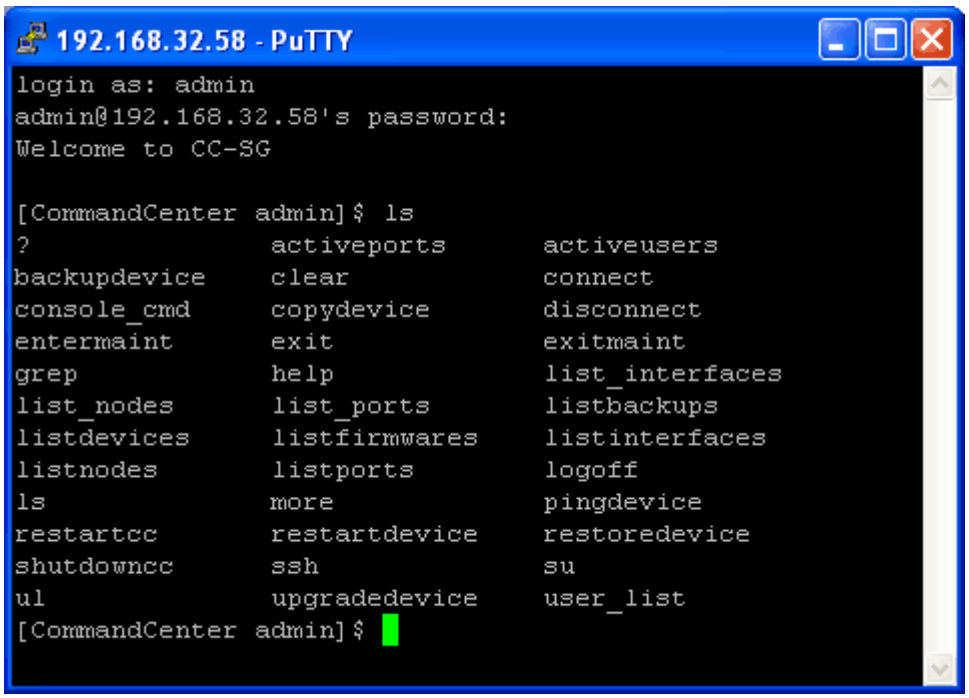
L'utilisateur du client SSH est authentifié par l'unité CC-SG dans laquelle des stratégies d'authentification et d'autorisation sont appliquées au client SSH. Les commandes disponibles pour le client SSH sont déterminées par les autorisations des groupes d'utilisateurs auxquels l'utilisateur du client SSH appartient.

Les administrateurs qui utilisent SSH pour accéder à CC-SG ne peuvent pas déconnecter un utilisateur SSH CC Super-User, mais ils peuvent déconnecter tous les autres utilisateurs du client SSH, administrateurs système compris.

➢ *Pour accéder à CC-SG via SSH :*

1. Lancez un client SSH, tel que PuTTY.

2. Entrez l'adresse IP de CC-SG et **22** pour le port, puis ouvrez la connexion. La configuration du port pour l'accès SSH s'effectue dans le Gestionnaire de sécurité. Reportez-vous à ***Configuration de la sécurité*** (voir "Gestionnaire de sécurité" à la page 193) pour plus d'informations.
3. Connectez-vous en utilisant vos nom d'utilisateur et mot de passe CC-SG.
4. Une invite de commande apparaît. Tapez **ls** pour afficher toutes les commandes disponibles. Vous pouvez taper **?** ou **help** pour afficher la description et le format de saisie de toutes les commandes.



Commandes SSH

Le tableau suivant décrit toutes les commandes disponibles dans SSH. Vous devez disposer des privilèges appropriés dans CC-SG pour accéder à chaque commande.

Tapez la commande suivie du commutateur **-h** pour afficher l'aide de cette commande, par exemple **listfirmwares -h**.

Commande Description
`activeports` Répertorie les ports actifs.
`activeusers` Répertorie les utilisateurs actifs.
`backup device <[-host <hôte>] | [-id <id_dispositif>]> nom_sauvegarde [description]` Sauvegarde la configuration du dispositif.
`clear` Efface l'écran.
`connect [-d <nom_dispositif>] [-e <car_echap>] <[-i <id_interface>] | [-n <nom_port>] | [id_port]>` Etablit la connexion à un port série. Si <nom_port> ou <nom_dispositif> contient des espaces, il doit être entouré de guillemets.
`copydevice <[-b <id_sauvegarde>] | [hôte_dispositif_source]> hôte_dispositif_cible` Copie la configuration du dispositif.
`disconnect <[-u <nomutilisateur>] [-p <id_port>] [-id <id_connexion>]>` Ferme la connexion du port.
`entermaint minutes [message]` Place CC-SG en mode de maintenance.
`exitmaint` Sort CommandCenter du mode de maintenance.
`grep terme_recherche` Recherche du texte dans le flux de sortie redirigé.

`help` Affiche l'écran d'aide.
`listbackups <[-id <id_dispositif>] | [hôte]>` Répertorie les sauvegardes de configuration du dispositif disponibles.
`listdevices` Répertorie les dispositifs disponibles.
`listfirmwares <[-id <id_dispositif>] | [hôte]>` Répertorie les versions de firmware disponibles pour la mise à niveau.
`listinterfaces [-id <id_nœud>]` Répertorie toutes les interfaces.
`listnodes` Répertorie tous les nœuds.
`listports [[-id <id_dispositif>] | [hôte]` Répertorie tous les ports.
`logoff [-u <nomutilisateur>] message` Déconnecte l'utilisateur.
`ls` Répertorie les commandes.
`more [-p <taille_page>]` Effectue la pagination.
`pingdevice <[-id <id_dispositif>] | [hôte]>` Envoie une commande ping au dispositif.
`restartcc minutes [message]` Redémarre CC-SG.
`restartdevice <[-id <id_dispositif>] | [hôte]>` Redémarre le dispositif.
`restoredevice <[-host <hôte>] | [-id <id_dispositif>]> [id_sauvegarde]` Restaure la configuration du dispositif.
`shutdowncc minutes [message]` Arrête CC-SG.
`ssh [-e <car_echap>] <[-id <id_dispositif>] | [hôte]>` Ouvre une connexion SSH à un dispositif SX.

`su [-u <nom_utilisateur>]` Modifie un utilisateur.
`upgradedevice <[-id <id_dispositif>] | [hôte]>` Met à niveau le firmware du dispositif.
`exit` Ferme une session SSH.

Astuces sur les commandes

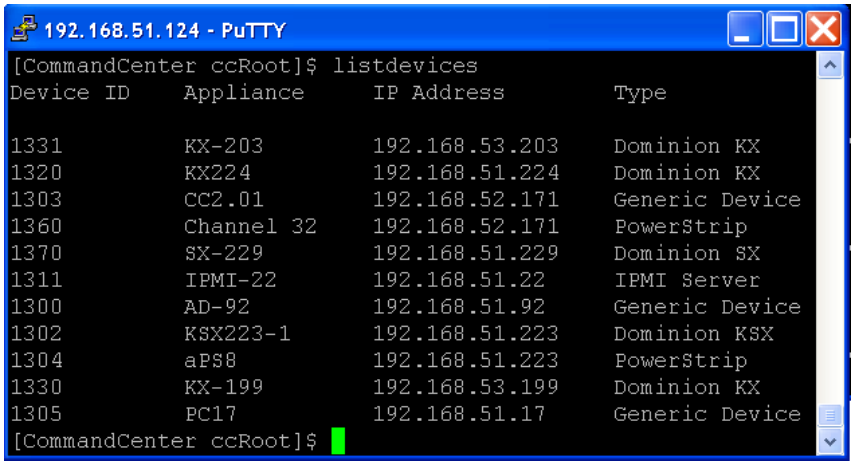
- Pour les commandes transmettant une adresse IP, par exemple `upgradedevice`, vous pouvez remplacer l'adresse IP par un nom d'hôte. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2).
- Les commandes `copydevice` et `restartdevice` s'appliquent seulement à quelques dispositifs Raritan, par exemple Dominion SX. Les serveurs IPMI, les dispositifs génériques ne sont pas pris en charge par ces commandes.

Créer une connexion SSH à un dispositif SX

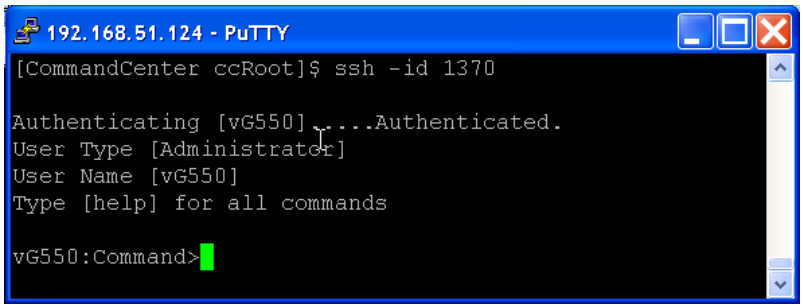
Vous pouvez créer une connexion SSH à un dispositif SX pour effectuer des opérations administratives sur ce dernier. Une fois la connexion établie, les commandes administratives prises en charge par le dispositif SX sont disponibles.

***Remarque** : avant de vous connecter, assurez-vous que le dispositif SX a été ajouté à l'unité CC-SG.*

1. Tapez `listdevices` pour vérifier que le dispositif SX a été ajouté à CC-SG.



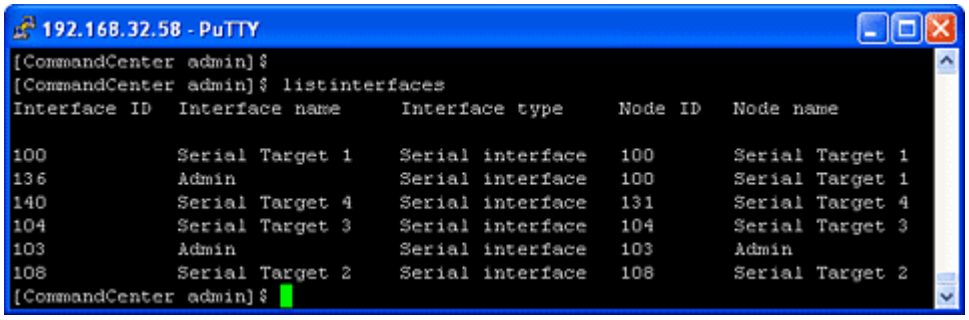
2. Connectez-vous au dispositif SX en tapant `ssh -id <id dispositif>`. Par exemple, à partir de la figure ci-dessus, vous pouvez vous connecter à SX-229 en entrant `ssh –id 1370`.



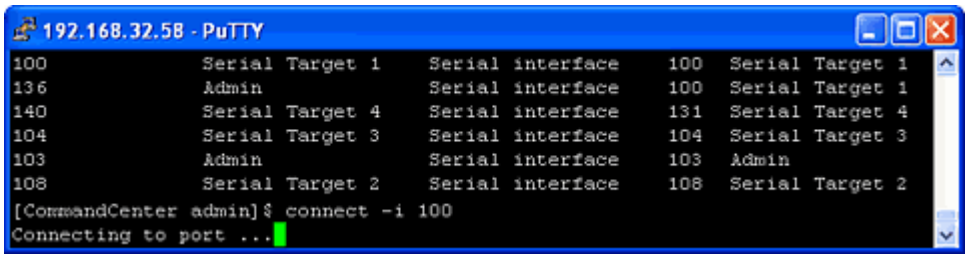
Utiliser SSH pour se connecter à un nœud via une interface série hors bande

Vous pouvez utiliser SSH pour vous connecter à un nœud via son interface série hors bande associée. La connexion SSH est établie en mode Proxy.

1. Tapez `listinterfaces` pour afficher l'ID des nœuds et les interfaces associées.



2. Tapez `connect -i <id_interface>` pour vous connecter au nœud associé à l'interface.



3. Une fois connecté au nœud, appuyez sur les touches d'échappement par défaut « ~ » suivi d'un point « . ». A l'invite qui apparaît, vous pouvez entrer des commandes ou alias spécifiques.

Commande	Alias	Description
`quit`	`q`	Met fin à la connexion et retourne à l'invite SSH.
`get_write`	`gw`	Obtient un accès en écriture. Permet à l'utilisateur SSH d'exécuter des commandes sur le serveur alors que l'utilisateur du navigateur peut uniquement observer les procédures.
`get_history`	`gh`	Extrait l'historique. Affiche les dernières commandes et résultats du serveur cible.

`send_break`	`sb`	Envoie une rupture. Interrompt la boucle dans le serveur cible émanant de l'utilisateur du navigateur.
`help`	`?,h`	Imprime l'écran d'aide.

Quitter une session SSH

Pour mettre fin entièrement à la connexion SSH à CC-SG, tapez `exit`.

Port d'administration série

Le port d'administration série sur CC-SG peut être connecté directement à un dispositif série Raritan, tel que Dominion SX ou KSX.

Vous pouvez vous connecter à l'unité SX ou KSX via l'adresse IP à l'aide d'un programme d'émulation de terminal, tel que HyperTerminal ou PuTTY. Définissez le débit en bauds dans le programme d'émulation de terminal sur celui de l'unité SX ou KSX.

➢ *Port d'administration série G1 :*

➢ *Port d'administration série V1 :*

➢ *Port d'administration série E1 :*

A propos des programmes d'émulation de terminal

HyperTerminal est disponible sous de nombreux systèmes d'exploitation Windows. HyperTerminal n'est pas disponible sous Windows Vista.

PuTTY est un programme libre téléchargeable depuis Internet.

Interface API de services Web

L'interface API de services Web (WS API) n'est pas disponible actuellement pour activation. Reportez-vous à http://www.raritan.com/web-services-api pour obtenir des informations à jour sur cette fonction.

Chapitre 16 Console de diagnostic

La console de diagnostic est une interface standard, non graphique, qui fournit un accès local à CC-SG. Elle est ***accessible à partir d'un port série ou KVM*** (voir "Accès à la console de diagnostic via un port VGA/clavier/souris" à la page 227), ou d'un ***client Secure Shell (SSH)*** (voir "Accès à la console de diagnostic via SSH" à la page 227), par exemple PuTTY ou OpenSSH Client.

Elle comprend deux interfaces : la ***console d'état*** (voir "A propos de la console d'état" à la page 229) et la ***console d'administration*** (voir "A propos de la console d'administrateur" à la page 230).

Remarque : *lorsque vous accédez à la console de diagnostic via SSH, les consoles d'état et d'administration héritent des paramètres d'apparence de votre client SSH et des associations de clavier. Ces paramètres peuvent être différents de ceux présentés dans cette documentation.*

Dans ce chapitre

Accès à la console de diagnostic via un port VGA/clavier/souris.....227
Accès à la console de diagnostic via SSH 227
A propos de la console d'état 229
Accès à la console d'état.....229
A propos de la console d'administrateur.....230
Accès à la console d'administrateur 230
Navigation dans la console d'administrateur 231
Modification de la configuration de la console de diagnostic 232
Modification de la configuration des interfaces réseau (Interfaces réseau) 233
Envoi d'une commande ping à une adresse IP (Interfaces réseau).....235
Utilisation de la détermination d'itinéraire (Interfaces réseau).....237
Modification des routes statiques (Interfaces réseau).....238
Consultation des fichiers journaux dans la console de diagnostic (Admin) 239
Redémarrage de CC-SG avec la console de diagnostic 244
Réamorçage de CC-SG avec la console de diagnostic 245
Mise hors tension du système CC-SG à partir de la console de diagnostic 246
Réinitialisation du mot de passe du super utilisateur CC avec la console de diagnostic.....247
Réinitialisation de la configuration usine de CC-SG (Admin) 248
Paramètres des mots de passe de la console de diagnostic.....251
Configuration des comptes 253
Affichage de l'état des disques (Utilitaires).....256
Affichage des processus exécutés sur CC-SG avec la console de diagnostic 257
Affichage de l'état de NTP (Utilitaires).....257

Accès à la console de diagnostic via un port VGA/clavier/souris

1. Branchez un moniteur VGA plus un clavier et une souris PS2 à l'arrière de l'unité CC-SG.
2. Appuyez sur RETOUR pour afficher une invite de connexion à l'écran.

Accès à la console de diagnostic via SSH

1. Lancez un client SSH, tel que PuTTY, sur un PC client disposant d'une connexion réseau à CC-SG.

2. Entrez l'adresse IP de l'unité CC-SG, ou son nom d'hôte IP (si elle a été enregistrée avec un serveur DNS), et spécifiez 23 pour le port.
3. Cliquez sur le bouton permettant la connexion. Une fenêtre s'ouvre pour vous demander vos identifiants de connexion.

➢ *Pour accéder à la console d'état*

L'accès à la console d'état ne nécessite pas de mot de passe, mais il est possible d'en imposer l'usage.

- A l'invite de connexion, tapez **status**. La console d'état en lecture seule apparaît.

```
+-------------------------------------------------------------------------------+
¦Mon Dec 11 EST          CommandCenter Secure Gateway                  22:27:58¦
¦+ Message of the Day: ----------------------------------------------------------+¦
¦¦CommandCenter Secure Gateway                                                  ¦¦
¦¦                                                                              ¦¦
¦¦Centralized access and control for your global IT infrastructure               ¦¦
¦¦                                                                              ¦¦
¦¦                                                                              ¦¦
¦+-------------------------------------------------------------------------------+¦
¦System Information:                                                            ¦
¦   Host Name      : CommandCenter.localdomain                                  ¦
¦   CC-SG Version  : 3.1.0.5.1          Model         :  CC-SG-V1               ¦
¦   CC-SG Serial # : ACC6500009         Host ID       :  00304856F118           ¦
¦Server Information:                                                            ¦
¦   CC-SG Status   : Up                 DB Status     :  Responding             ¦
¦   Web Status     : Responding/Unsecured                                       ¦
¦   Cluster Status : standalone         Cluster Peer  :  Not Configured         ¦
¦Network Information:                                                           ¦
¦  Dev  Link  Auto      Speed Duplex          IPAddr    RX Pkts    TX Pkts     ¦
¦ eth0   yes    on    100Mb/s  Full    192.168.0.192      55285         11     ¦
¦ eth1    no    on   Unknown! Unknown!                                         ¦
¦                                                                               ¦
¦                                                                               ¦
¦                                        Help: <F1>  Exit: <ctl+Q> or <ctl+C>¦
+-------------------------------------------------------------------------------+
```

Cet écran affiche de manière dynamique des informations sur l'état du système et indique si la console CC-SG et ses sous-composants fonctionnent.

L'heure affichée dans le coin supérieur droit de l'écran indique la dernière interrogation des données sur l'unité CC-SG.

Les informations de cet écran sont actualisées toutes les 5 secondes environ.

- Appuyez sur les touches **Ctrl-L** pour effacer l'écran actuel et recharger des informations à jour. Vous pouvez actualiser l'écran une fois par seconde au maximum.
- Appuyez sur les touches **Ctrl-Q** ou **Ctrl-C** pour quitter l'écran.
- La console d'état n'accepte aucune autre saisie ni navigation d'écran. Toutes les autres saisies sont ignorées.

Le tableau suivant décrit les états de CC-SG et de sa base de données :

Etat	Description
Etat de CC-SG : Up (actif)	CC-SG est disponible.
Etat de CC-SG : Down (inactif)	CC-SG peut être en cours de réamorçage. Si l'état Down se poursuit, essayez de redémarrer CC-SG.
Etat de CC-SG : Restarting (redémarrage)	CC-SG est en cours de redémarrage.
Etat de la BD : Responding (réponse)	La base de données de CC-SG est disponible.
Etat de la BD : Down (inactif)	CC-SG peut être en cours de réamorçage.

A propos de la console d'état

La console d'état permet de déterminer l'état de CC-SG, des différents services utilisés par CC-SG et du réseau connecté.

Par défaut, la console d'état ne nécessite pas de mot de passe.

Accès à la console d'état

➢ *Pour accéder à la console d'état :*

1. Tapez **status** à l'invite de **connexion**.
2. Les données système actuelles s'affichent.

A propos de la console d'administrateur

La console d'administrateur vous permet de définir certains paramètres initiaux, d'établir la configuration réseau initiale, de déboguer des fichiers journaux, d'effectuer des diagnostics limités et de redémarrer CC-SG.

Les identifiants de connexion par défaut à la console d'administrateur sont :

- Nom d'utilisateur : **admin**
- Mot de passe : **raritan**

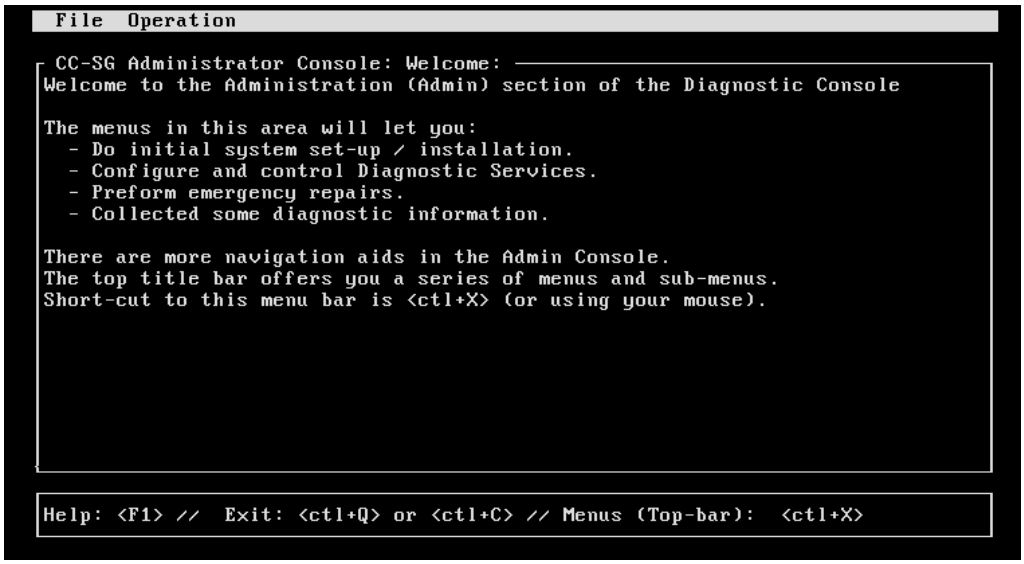
Le compte de la console de diagnostic **admin** est distinct des compte et mot de passe CC Super User **admin** utilisés dans le client Admin CC-SG Java et le client d'accès HTML. La modification d'un de ces mots de passe n'affecte pas l'autre.

Accès à la console d'administrateur

Toutes les informations affichées dans la console d'administrateur sont statiques. Si des changements sont apportés à la configuration via l'interface graphique CC-SG ou la console de diagnostic, vous devez vous reconnecter à la console d'administrateur pour voir apparaître ces modifications.

1. A l'invite de connexion, tapez **admin**.
2. Tapez le mot de passe CC-SG. Le mot de passe par défaut est **raritan**. A la première connexion, ce mot de passe expire et vous devez en choisir un nouveau. Entrez ce mot de passe et, à l'invite, tapez un nouveau mot de passe. Reportez-vous à ***Paramètres des mots de passe de la console de diagnostic*** (à la page 251) pour en savoir plus sur la définition de la force du mot de passe.

L'écran principal de la console d'administrateur apparaît.



Navigation dans la console d'administrateur

Le tableau suivant vous indique les diverses méthodes de navigation au sein des menus de la console de diagnostic. Pour certaines sessions, la souris peut également servir pour la navigation. Toutefois, elle ne fonctionne pas nécessairement sur tous les clients SSH ou sur la console KVM.

APPUYEZ SUR	POUR
CTRL+C ou CTRL+Q	Quitter la console de diagnostic.
CTRL+L	Effacer l'écran et retracer les informations (qui ne sont pas mises à jour ni rafraîchies).
TAB	Passer à l'option disponible suivante.
ESPACE	Sélectionner l'option en cours.
ENTREE	Sélectionner l'option en cours.
FLECHE	Passer à des champs différents au sein d'une option.

Modification de la configuration de la console de diagnostic

La console de diagnostic est accessible via un port série (COM1), un port VGA/clavier/souris (KVM) ou à partir de clients Secure Shell (SSH). Pour chaque type de port, vous pouvez décider si des connexions **status** ou **admin** sont autorisées et si le personnel d'assistance sur site peut également accéder à la console de diagnostic depuis le port. Pour les SSH, vous pouvez également configurer le numéro de port à utiliser, s'il n'est pas encore employé par un autre service CC-SG.

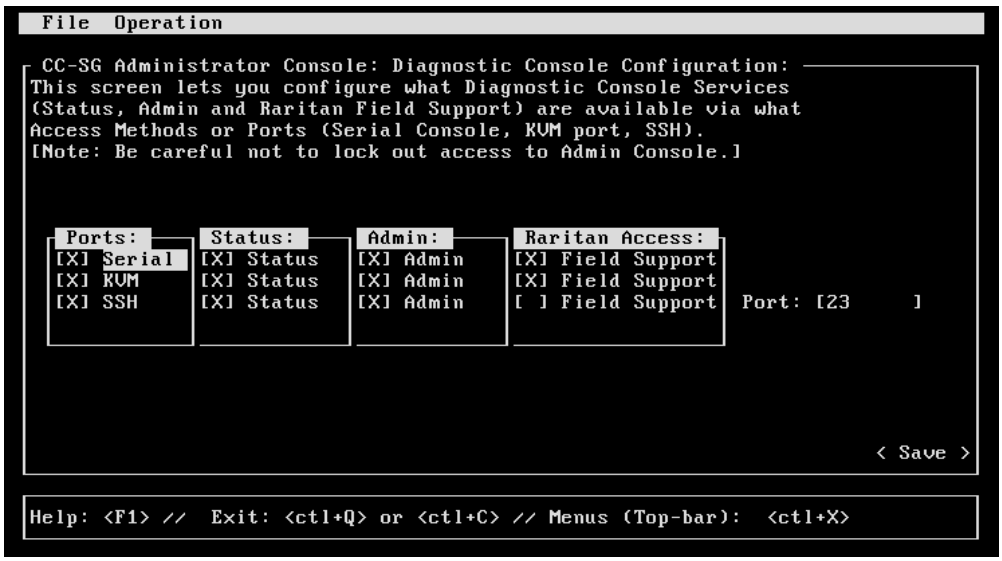
Important : veillez à ne pas verrouiller complètement tous les accès Administrateur ou Assistance sur site.

➢ *Pour modifier la configuration de la console de diagnostic :*

1. Choisissez **Operation** > **Diagnostic Console Config** (configuration de la console de diagnostic).
2. Définissez le mode de configuration et d'accès de la console de diagnostic.

   Il existe trois mécanismes d'accès à la console de diagnostic : port série (COM1), console KVM, SSH (réseau IP). La console de diagnostic offre trois services : Affichage d'état (Status Display), Console d'administration (Admin Console), Assistance sur site Raritan (Raritan Field Support). Cet écran permet de sélectionner les services disponibles via les différents mécanismes d'accès.

3. Entrez le numéro de port que vous souhaitez définir pour l'accès SSH à la console de diagnostic dans le champ **Port**. Le port par défaut est **23**.



4. Cliquez sur **Save** (Enregistrer).

Modification de la configuration des interfaces réseau (Interfaces réseau)

Dans la configuration d'interface réseau, vous pouvez effectuer des tâches de paramétrage initiales, telles que la définition du nom d'hôte et de l'adresse IP de CC-SG.

1. Choisissez **Operation** > **Network Interfaces** (interfaces réseau) > **Network Interface Config** (configuration de l'interface réseau).

2. Si les interfaces réseau sont déjà configurées, vous verrez un message d'**avertissement** indiquant que vous devez utiliser l'interface graphique CC-SG (Director Client de l'administrateur) pour les paramétrer. Si vous souhaitez poursuivre, cliquez sur **YES**.

```
 File  Operation

 CC-SG Administrator Console: Network Interface Configuration:
Hostname:        [CommandCenter.localdomain                                  ]
Domain Suffix:   [localdomain                                                ]
Primary DNS:     [                  ]   Secondary DNS: [                  ]

                    Mode:   <o> Primary/Backup
                            < > Active/Active

Configuration:    < > DHCP         Configuration:      < > DHCP
                  <o> STATIC                           <o> STATIC

IP Address:  [192.168.0.192     ]  IP Address:    [                  ]
Netmask:     [255.255.255.0     ]  Netmask:       [                  ]
Gateway:     [                  ]  Gateway:       [                  ]
Adapter Speed:    <o> AUTO            Adapter Speed:    <o> AUTO
Adapter Duplex:   <o> FULL            Adapter Duplex:   <o> FULL


                                                                   < Save >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

3. Entrez le nom d'hôte dans le champ **Host Name**. Après enregistrement, ce champ est mis à jour pour refléter le nom de domaine complet (NDCQ), le cas échéant. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie/Sigles*** (voir "Terminologie et sigles" à la page 2).

4. Dans le champ **Mode**, sélectionnez **Primary/Backup Mode** (mode principal/sauvegarde) ou **Active/Active Mode.** Reportez-vous à ***A propos de la configuration réseau*** (à la page 171) pour en savoir plus.

   - Dans le champ Configuration, sélectionnez DHCP ou Static.
   - Si vous choisissez DHCP et que votre serveur DHCP a été configuré correctement, les informations de DNS, le suffixe de domaine, l'adresse IP, la passerelle par défaut et le masque de sous-réseau sont automatiquement indiqués lorsque vous enregistrez et que vous quittez, puis rouvrez la console d'administrateur.
   - Si vous choisissez **Static**, renseignez les champs **IP Address** (obligatoire), **Netmask**(obligatoire), **Default Gateway** (facultatif), **Primary DNS** (facultatif), **Secondary DNS**(facultatif), et entrez un nom de domaine dans le champ **Domain Suffix** (facultatif).

Raritan.
When you're ready to take control®

- Même si DHCP est utilisé pour déterminer la configuration IP d'une interface, une **adresse IP** et un **masque réseau** formatés correctement doivent être fournis.

5. Dans **Adapter Speed**, sélectionnez une vitesse de ligne. Les autres valeurs 10, 100 et 1000 Mbps figurent dans une liste déroulante (où une seule valeur est visible à la fois) ; les touches ✙✙ permettent d'y accéder, et la barre d'espacement permet de sélectionner l'option affichée.
6. Si vous n'avez pas choisi **AUTO** pour **Adapter Speed**, cliquez sur **Adapter Duplex** et utilisez les touches ✙✙ pour sélectionner un mode duplex (**FULL** ou **HALF**) dans la liste, le cas échéant. Même s'il est toujours possible de sélectionner un mode duplex, il ne prend effet que si la valeur du champ **Adapter Speed** n'est pas **AUTO**.
7. Si vous avez sélectionné l'option **Active/Active Mode**, répétez ces étapes pour la seconde interface réseau.
8. Sélectionnez **Save** (enregistrer). L'unité CC-SG redémarre, déconnecte tous les utilisateurs de l'interface CC-SG et met fin à leur session. Un écran d'**avertissement** apparaît pour informer de la reconfiguration réseau imminente et de son impact pour les utilisateurs de l'interface CC-SG. Cliquez sur <**YES**> pour continuer.

   La progression du système peut être surveillée sur l'écran d'état de la console de diagnostic. Sur le port KVM, une autre session de terminal peut être sélectionnée par la saisie de <**ALT**>+<**F2**> et la connexion sous le nom **status**.Pour retourner à la session de terminal d'origine, tapez <**ALT**>+<**F1**>. Six sessions de terminal sont disponibles de <**F1**> à <**F6**>.

Envoi d'une commande ping à une adresse IP (Interfaces réseau)

Utilisez la commande ping pour vérifier si la connexion entre l'ordinateur CC-SG et une adresse IP particulière fonctionne correctement.

***Remarque** : certains sites bloquent explicitement les requêtes ping. Assurez-vous que la cible et le réseau concerné autorisent les commandes ping en cas d'échec de celles-ci.*

1. Choisissez Operation > Network Interfaces > Ping.
2. Dans le champ Ping Target, entrez l'adresse IP ou le nom d'hôte (si DNS est configuré correctement sur l'unité CC-SG) de la cible que vous souhaitez vérifier.
3. (Facultatif) Sélectionnez :

Option	Description
Show other received ICMP packets	Sortie détaillée, qui répertorie d'autres paquets ICMP reçus en plus des paquets ECHO_RESPONSE. Survient rarement.
No DNS Resolution	Ne résout pas les adresses des noms d'hôte.
Record Route	Enregistre la route. Définit l'option de route de l'enregistrement IP, qui stockera la route du paquet dans l'en-tête IP.
Use Broadcast Address	Autorise l'envoi d'une commande ping à un message à diffusion générale.
Adaptive Timing	Commande ping adaptable. L'intervalle interpaquets s'adapte à la durée aller-retour, afin qu'il n'existe pas plus d'une inspection sans réponse sur le réseau. L'intervalle minimum est de 200 millisecondes.

4. (Facultatif) Entrez des valeurs pour le nombre de secondes d'exécution de la commande ping, le nombre de requêtes ping envoyées et la taille des paquets ping (la valeur par défaut est 56, qui donne 64 octets de données ICMP lorsqu'elle est combinée aux 8 octets des données d'en-tête ICMP). Si les champs restent vides, les valeurs par défaut sont utilisées.
5. Cliquez sur Ping. Si les résultats affichent une série de réponses, la connexion fonctionne. La durée vous indique la vitesse de la connexion. Si une erreur d'« expiration » s'affiche à la place d'une réponse, la connexion entre votre ordinateur et le domaine ne fonctionne pas. Reportez-vous à ***Utilisation de la détermination d'itinéraire*** (voir "Modification des routes statiques (Interfaces réseau)" à la page 238) pour plus d'informations.
6. Appuyez sur CTRL+C pour mettre fin à la session ping.

Remarque : lorsque vous appuyez sur Ctrl+Q, un résumé statistique apparaît pour la session en cours et l'envoi de la commande ping à la destination se poursuit.

Utilisation de la détermination d'itinéraire (Interfaces réseau)

La détermination d'itinéraire est souvent utilisée pour le dépannage du réseau. En affichant une liste des routeurs traversés, elle vous permet d'identifier le chemin emprunté par votre ordinateur pour atteindre une destination particulière sur le réseau. Elle répertorie tous les routeurs traversés jusqu'à sa destination ou son échec et son rejet. De plus, elle vous indique la durée du « saut » d'un routeur à un autre. Vous pouvez ainsi identifier les problèmes d'acheminement ou les pare-feu qui peuvent bloquer l'accès à un site.

➢ *Pour exécuter une détermination d'itinéraire sur une adresse IP ou un nom d'hôte :*

1. Choisissez **Operation** > **Network Interfaces** > **Traceroute**.
2. Entrez l'adresse IP ou le nom d'hôte de la cible que vous souhaitez vérifier dans le champ **Traceroute Target**.
3. (Facultatif) Sélectionnez :

Option	Description
Verbose	Sortie détaillée, qui répertorie les paquets ICMP reçus, autres que TIME_EXCEEDED et UNREACHABLE.
No DNS Resolution	Ne résout pas les adresses des noms d'hôte.
Use ICMP (vs. normal UDP)	Utilisez ICMP ECHO au lieu des datagrammes UDP.

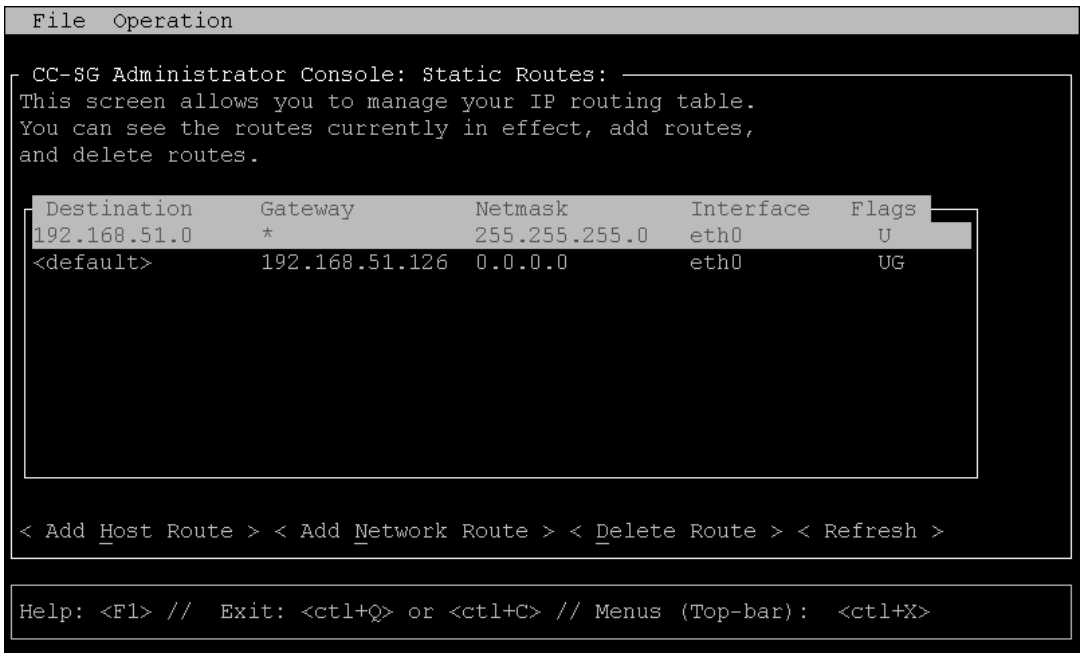
4. (Facultatif) Entrez des valeurs pour le nombre de sauts que la commande de détermination d'itinéraire utilisera dans les paquets d'inspection sortants (la valeur par défaut est 30), le port de destination UDP à utiliser dans les inspections (la valeur par défaut est 33434) et la taille des paquets de détermination d'itinéraire. Si les champs restent vides, les valeurs par défaut sont utilisées.
5. Cliquez sur **Traceroute** dans le coin inférieur droit de la fenêtre.
6. Appuyez sur **Ctrl+C** ou **Ctrl+Q** pour mettre fin à la session de détermination d'itinéraire. Une invite **Return?** apparaît ; appuyez sur **ENTREE** pour retourner au menu Traceroute. L'invite **Return?** s'affiche également lorsque l'opération Traceroute se termine à cause d'événements « destination atteinte » ou « nombre de sauts dépassé ».

Modification des routes statiques (Interfaces réseau)

Dans Static Routes, vous pouvez consulter le tableau de l'acheminement IP actuel et modifier, ajouter ou supprimer des routes. L'utilisation et le placement précis des routes statiques peuvent réellement améliorer les performances de votre réseau, vous permettant ainsi de conserver de la bande passante pour des applications de gestion importantes. Ils peuvent également être utiles pour les paramètres Réseau actif/actif où chaque interface est reliée à un domaine IP distinct. Reportez-vous à ***A propos de la configuration réseau*** (à la page 171) pour plus d'informations. Cliquez avec la souris ou utilisez les touches **TAB** et fléchées pour naviguer, et appuyez sur la touche **Entrée** pour sélectionner une valeur.

➢ *Pour visualiser ou modifier des routes statiques :*

1. Choisissez **Operation** > **Network Interfaces** > **Static Routes**.
2. Le tableau d'acheminement IP actuel s'affiche. Vous pouvez ajouter une route hôte ou réseau, ou supprimer une route. Le bouton **Refresh** met à jour les informations d'acheminement du tableau ci-dessus.



Consultation des fichiers journaux dans la console de diagnostic (Admin)

Vous pouvez visualiser un fichier journal ou en consulter plusieurs simultanément via LogViewer, qui permet la consultation de plusieurs fichiers à la fois, pour examiner l'activité du système.

La liste des fichiers journaux n'est mise à jour qu'à l'activation de la liste associée (par exemple, lorsque l'utilisateur entre dans la zone de liste des fichiers journaux) ou à la sélection d'une nouvelle option de tri. Les noms de fichier sont précédés d'un horodateur indiquant la dernière réception de données par le fichier journal ou sa taille.

➢ *Abréviations d'horodateur et de taille de fichier :*

Horodateurs :

- s = secondes
- m = minutes
- h = heures
- d = jours

Tailles de fichier :

- B = octets
- K = Kilooctets (1 000 octets)
- M = Mégaoctets (1 000 000 octets)
- G = Gigaoctets (1 000 000 000 octets)

➢ *Pour afficher les fichiers journaux :*

1. Choisissez **Operation** > **Admin** > **System Logfile Viewer**.
2. L'écran Logviewer se divise en quatre zones principales.
   - Liste des fichiers journaux disponibles actuellement dans le système. Si la liste ne tient pas dans la fenêtre d'affichage, vous pouvez la faire défiler à l'aide des touches fléchées.
   - Critères de tri de la liste des fichiers journaux. Les fichiers journaux peuvent être triés en fonction de leur nom entier, de la date de modification la plus récente ou de la taille la plus grande.
   - Options d'affichage du visualiseur.
   - Sélecteur Export/View (exporter/afficher).

3. Cliquez ou utilisez les touches fléchées pour vous déplacer, et appuyez sur la **BARRE D'ESPACEMENT** pour sélectionner un fichier journal en le signalant d'un **X**. Vous pouvez visualiser plusieurs fichiers journaux à la fois.

```
 File  Operation

 CC-SG Administrator Console: System Logfile Viewer:
  Logfile(s) to View:                                  Sort Logfile list by:
  [ ]  10h ./boot.log                                  <o> Full File Name
  [ ]   9m ./cron                                      < > Recent Change
  [ ]   7m ./messages                                  < > File Size
  [ ]  16h ./pgsql
  [ ]  10h ./rpmpkgs
  [ ]  38m ./secure
  [ ]  16h sg/ShellCommandExecutor.log                 Viewer Display Options:
  [ ]   2s sg/httpd/access_log                           <o> Individual Windows
  [ ]  10h sg/httpd/access_log.1                         < > Merged Windows
  [ ]  10h sg/httpd/error_log                            Initial Buffer:[5000    ]
  [ ]   1d sg/install/anaconda.log
  [ ]   1d sg/install/ccinstall.log                      [X] Remember Selected Items
  [ ]   1d sg/install/dmi.log                            [X] Use Default Color Scheme
  [ ]   1d sg/install/install.log                        [X] Use Default Filters
  [ ]   1d sg/install/install.log.syslog
                                                                   < Export > < View >

 Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

➢ *Pour trier les fichiers journaux de la liste de consultation :*

Les options **Sort Logfile list by** contrôlent l'ordre dans lequel les fichiers journaux s'affichent dans la liste **Logfile to View**.

Option	Description
Individual Windows	Affiche les journaux sélectionnés dans des sous-fenêtres distinctes.
Merged Windows	Fusionne les journaux sélectionnés dans une fenêtre d'affichage.
Initial Buffer	Paramètre la mémoire tampon ou la taille de l'historique initiales. **5000** est la valeur par défaut. Ce système est configuré pour mettre en mémoire tampon toutes les nouvelles informations qui se présentent.

Remember Selected Items	Si cette case est cochée, les sélections de fichier journal actuelles (le cas échéant) seront conservées. Sinon, la sélection est réinitialisée chaque fois qu'une nouvelle liste de fichiers journaux est générée. Ceci est utile si vous souhaitez parcourir les fichiers.
Use Default Color Scheme	Si cette case est cochée, certains fichiers journaux seront affichés avec un jeu de couleurs standard. Remarque : des commandes multitail peuvent être utilisées pour modifier le jeu de couleurs lorsque les fichiers journaux sont ouverts.
Use Default Filters	Si cette case est cochée, des filtres sont automatiquement appliqués à certains fichiers journaux.
Export	Cette option rassemble tous les fichiers journaux sélectionnés et les rend disponibles par accès Web pour qu'ils puissent être extraits et transmis à l'assistance technique Raritan. L'accès au contenu de ce paquet n'est pas disponible au client. Les fichiers journaux exportés sont disponibles jusqu'à 10 jours, puis le système les supprime automatiquement.
View	Affiche les journaux sélectionnés.

Lorsque l'option **View** est sélectionnée avec Individual Windows, LogViewer s'affiche :

```
15:30:54,366 INFO  [ChannelSocket] JK: ajp13 listening on /0.0.0.0:8009
15:30:54,378 INFO  [JkMain] Jk running ID=0 time=0/26  config=null
15:30:54,480 INFO  [Http11Protocol] Starting Coyote HTTP/1.1 on http-9443
15:30:54,756 INFO  [Http11Protocol] Starting Coyote HTTP/1.1 on http-0.0.0.0-808
0
15:30:54,801 INFO  [Server] JBoss (MX MicroKernel) [4.0.3 (build: CVSTag=JBoss_4
_0_3 date=200510042324)] Started in 57s:149ms
00] sg/jboss/console.log F1/<CTRL>+<h>: help          118KB - 2006/12/13 15:32:54
3/bin ; USER=root ; COMMAND=/data/raritan/jboss/ccscripts/root-scripts/iptables_
ports.sh
Dec 13 15:30:55 CommandCenter httpd: httpd startup succeeded
Dec 13 15:30:55 CommandCenter MonitorCC[14617]: Starting httpd: ^[[60G[  ^[[0;32
mOK^[[0;39m
Dec 13 15:30:56 CommandCenter MonitorCC[14617]: startAll: Done --  JBoss:47 HTTP
D:1
01] ./messages *Press F1/<CTRL>+<h> for help*         935KB - 2006/12/13 15:32:54

02] sg/httpd/access_log F1/<CTRL>+<h>: help           538KB - 2006/12/13 15:32:54
```

- Lorsque vous visualisez les fichiers journaux, tapez **Q, CTRL-Q** ou **CTRL+C** pour retourner à l'écran précédent.
- Si vous le souhaitez, vous pouvez modifier les couleurs d'un fichier journal pour repérer ce qui est important. Entrez **c** pour changer les couleurs d'un fichier journal et sélectionnez un journal dans la liste.

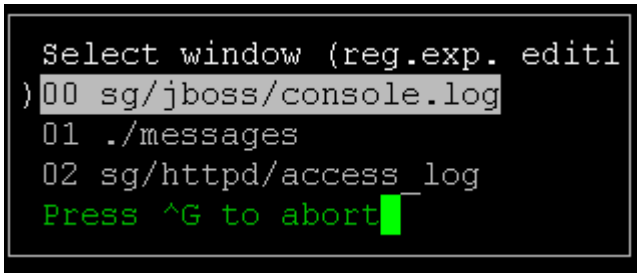
```
Toggle colors: select window
00 sg/jboss/console.log
01 ./messages
02 sg/httpd/access_log
Press ^G to abort
```

- Entrez **i** pour afficher les informations système.

Remarque : *la charge du système est statique depuis le début de cette session de la console d'administrateur. Utilisez l'utilitaire TOP pour surveiller dynamiquement les ressources du système.*

➢ *Pour filtrer un fichier journal à l'aide d'une expression standard :*

1. Entrez **e** pour ajouter ou modifier une expression standard et sélectionnez un journal dans la liste si vous avez décidé d'en consulter plusieurs.



2. Entrez **a** pour ajouter une expression standard. Par exemple, pour afficher des informations sur les messages **WARN** dans le fichier journal **sg/jboss/console.log**, entrez **WARN** et sélectionnez **match**.

Remarque : cet écran présente également le schéma de filtre par défaut de console.log, qui retire la plupart des messages de tas Java.

Redémarrage de CC-SG avec la console de diagnostic

Vous pouvez redémarrer CC-SG, qui déconnectera tous ses utilisateurs actuels et mettra fin à leurs sessions sur les serveurs cible distants.

Important : il est FORTEMENT recommandé de redémarrer l'unité CC-SG dans le client Admin Java, à moins qu'il ne soit absolument indispensable de la redémarrer à partir de la console de diagnostic. Reportez-vous à *Redémarrage de CC-SG* **(à la page 161) pour plus d'informations. Les utilisateurs ne NE SERONT PAS PREVENUS du redémarrage de CC-SG dans la console de diagnostic.**

➢ *Pour redémarrer CC-SG avec la console de diagnostic :*

1. Choisissez **Operation** > **Admin** > **CC-SG Restart**.
2. Cliquez sur **Restart CC-SG Application** ou appuyez sur la touche **ENTRÉE**.Confirmez le redémarrage dans l'écran suivant pour continuer.

```
 File  Operation

 CC-SG Administrator Console: CC-SG Restart:
CC-SG Restart.

This operation will restart the CC-SG Application.

This will log-off all currently active CC-SG GUI users of the system
and terminate any sessions to remote targets that they might have.

They will get no notification that this event will happen.

  [It is better to use the CC-SG GUI to do this -- it will provide a
   count-down timer and notification of session termination.]


< Restart CC-SG Application > < Cancel >


Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Réamorçage de CC-SG avec la console de diagnostic

Cette option entraîne un réamorçage complet de CC-SG, qui simule un cycle d'alimentation. Les utilisateurs ne recevront aucune notification. Les utilisateurs de CC-SG, SSH et la console de diagnostic (cette session comprise) seront déconnectés. Toutes les connexions aux serveurs cible distants seront également interrompues.

➢ *Pour réamorcer CC-SG*

1. Choisissez **Operation** > **Admin** > **CC-SG System Reboot**.
2. Cliquez sur **REBOOT System** ou appuyez sur la touche **ENTRÉE** pour réinitialiser CC-SG. Confirmez le réamorçage dans l'écran suivant pour continuer.

```
 File  Operation

 CC-SG Administrator Console: CC-SG System Reboot:
CC-SG System Reboot.

This operation will reboot the entire system (simulating a power cycle).

This will log-off all currently active CC-SG GUI, CC-SG SSH and Diagnostic
Console users (including this session) to this system and terminate any
sessions to remote targets that they might have.  This could also impact
cluster operations (if so configured).

Users will get no notification that this event will happen.



< REBOOT System > < Cancel >


Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Mise hors tension du système CC-SG à partir de la console de diagnostic

Cette option permet de mettre hors tension l'unité CC-SG. Les utilisateurs connectés ne recevront aucune notification. Les utilisateurs de CC-SG, SSH et la console de diagnostic (cette session comprise) seront déconnectés. Toutes les connexions aux serveurs cible distants seront également interrompues.

Le seul moyen de remettre l'unité CC-SG sous tension consiste à appuyer sur le bouton d'alimentation du panneau avant.

➢ *Pour mettre l'unité CC-SG hors tension :*

1. Choisissez **Operation** > **Admin** > **CC-SG System Power OFF**.
2. Cliquez sur **Power OFF the CC-SG** ou appuyez sur **ENTREE** pour couper l'alimentation de l'unité CC-SG. Confirmez la mise hors tension dans l'écran suivant pour continuer.

```
 File  Operation

┌ CC-SG Administrator Console: Power OFF: ──────────────────────────────────
CC-SG Power OFF.

This operation will turn the AC Power OFF for this CC-SG Unit.

The only way to bring the unit back online is by pressing the
Front Panel Power Button.

All active sessions will be terminated and no notification will given.

The system may take a couple of minutes before it actually powers off.
Please be patient!


< Power OFF the CC-SG > < Cancel >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Réinitialisation du mot de passe du super utilisateur CC avec la console de diagnostic

Cette option permet de réinitialiser le mot de passe du compte du super utilisateur CC à la valeur par défaut usine.

Mot de passe par défaut usine : **raritan**

Remarque : *il ne s'agit pas du mot de passe de l'utilisateur admin de la console de diagnostic. Reportez-vous à* **Mots de passe de la console de diagnostic (Admin)** *(voir "Paramètres des mots de passe de la console de diagnostic" à la page 251) pour plus d'informations.*

➢ *Pour réinitialiser le mot de passe admin de l'interface CC-SG :*

1. Choisissez Operation > Admin > CC-SG ADMIN Password Reset.
2. Cliquez sur Reset CC-SG GUI Admin Password ou appuyez sur ENTREE pour rétablir le mot de passe admin par défaut usine. Confirmez la réinitialisation du mot de passe dans l'écran suivant pour continuer.

```
 File  Operation

┌ CC-SG Administrator Console: CC-SG ADMIN Password Reset: ──────────────
CC-SG Administrator Password Reset.

This operation will reset the password for the ADMIN account of the
CC-SG GUI to the initial Factory Default value.

[Note: This is *NOT* the admin password for Diagnostic Console!
See: ADMIN->DiagCon Passwords->Account Configuration to
change the Diagnostic Console admin password.]

< Reset CC-SG GUI Admin Password > < Cancel >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Réinitialisation de la configuration usine de CC-SG (Admin)

Cette option réinitialisera tout ou partie du système CC-SG à ses valeurs par défaut usine. Tous les utilisateurs de CC-SG actifs seront déconnectés sans notification et le traitement SNMP sera interrompu. Il est fortement recommandé de faire passer CC-SG en **mode de maintenance** avant de commencer cette opération. Si possible, réinitialisez CC-SG depuis le client Admin de l'administrateur, plutôt qu'avec la console de diagnostic. L'option de réinitialisation du client Admin peut exécuter toutes les fonctions répertoriées ici, sauf la réinitialisation des valeurs de réseau.

1. Choisissez **Operation** > **Admin** > **Factory Reset**. L'écran suivant présentant 7 options de réinitialisation (**Reset Options**) apparaît.

```
 File  Operation

 CC-SG Administrator Console: Factory Reset:
Factory Reset.

This operation will restore the system to initial Factory Configuration.
This will log-off all currently active CC-SG GUI sessions to this system
and may terminate any sessions to remote targets that they might have.
This could also impact cluster operations (if so configured).
Users will get no notification that this event will happen.
          Reset Options:
          [X] Full CC-SG Database Reset
          [X] Preserve CC-SG Personality during Reset
          [X] Network Reset
          [X] SNMP Reset
          [X] Firmware Reset
          [X] Install Firmware into CC-SG DB
          [X] Diagnostic Console Reset

< RESET System > < Cancel >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Option	Description
Full CC-SG Database Reset	La sélection de cette option supprime entièrement la base de données CC-SG existante et crée une version nouvelle en la chargeant avec les valeurs par défaut usine.

Preserve CC-SG Personality during Reset	Cette option n'est valide et active que si l'option précédente est également sélectionnée. Lors de la reconstitution de la base de données CC-SG (dans l'option précédente), les valeurs suivantes seront migrées vers la nouvelle version de la base de données (si elles sont lisibles et disponibles ; sinon, les valeurs par défaut seront utilisées). Le système tente de conserver les informations suivantes : La valeur par défaut apparaît entre crochets. Communication sécurisée [non sécurisée] entre les clients PC et CC-SG Vérification des mots de passe forts [désactivée] : sélectionne si l'application du mot de passe fort est activée. Connexions directe et Proxy [Directe] indique si des connexions directes ou Proxy sont utilisées par les clients PC vers les nœuds hors bande. Minuteur d'inactivité [1800] : délai après lequel les sessions inactives sont déconnectées. Paramètres du modem [10.0.0.1/10.0.0.2/<none>] : paramètre d'adresse IP du serveur, d'adresse IP du client et numéro de téléphone de rappel du modem.

Network Reset	Cette option rétablit les paramètres réseau par défaut usine : Nom d'hôte = CommandCenter Nom de domaine = localdomain Mode = Principal/Sauvegarde Configuration = Statique Adresse IP = 192.168.0.192 Masque réseau = 255.255.255.0 Passerelle = <none> DNS principal = <none> DNS secondaire = <none> Vitesse de carte = Auto
SNMP Reset	Réinitialise la configuration SNMP aux valeurs par défaut usine. Port : 161 Communauté en lecture seule : public Communauté en lecture/écriture : private Contact système, Nom, Emplacement : <empty> Configuration des traps SNMP Destinations des traps SNMP
Firmware Reset	Retire les fichiers de firmware téléchargés et restaure les versions par défaut dans le référentiel de système de fichiers, mais ne modifie pas la BD CC-SG.
Install Firmware into CC-SG DB	Charge les fichiers de firmware trouvés dans le référentiel de système de fichiers dans la BD CC-SG.
Diagnostic Console Reset	Restaure la configuration, les paramètres de compte et les valeurs par défaut usine de la console de diagnostic.

Paramètres des mots de passe de la console de diagnostic

Cette option permet de configurer la force des mots de passe (status et admin), ainsi que leurs attributs, tels que le paramétrage du nombre maximum de jours devant s'écouler avant la modification du mot de passe (effectuée via le menu de configuration de compte). L'opération de ces menus s'applique uniquement aux comptes (status et admin) et aux mots de passe de la console de diagnostic. Elle n'a aucun effet sur les comptes ou mots de passe habituels de l'interface utilisateur graphique de CC-SG.

➢ *Configuration des mots de passe*

1. Choisissez **Operation** > **Admin** > **DiagCon Passwords** > **Password Configuration**.
2. Dans le champ Password History Depth, entrez le nombre de mots de passe à garder en mémoire. Le paramètre par défaut est **5**.

```
 File  Operation

┌ CC-SG Administrator Console: Password Settings: ──────────────────────────
Use this screen to update how all subsequent Diagnostic Console (only!)
password operations will work.  You can set the type of passwords (regular,
strong or random) that the system will let the user use on any subsequent
password change operation.  Also, the number of passwords henceforth that
the system will remember and not let the user duplicate or reuse.

Password Configuration:

  Password History Depth:[5   ]

  Password Type & Parameters:
   <o> Regular
   < > Random  Size:[20  ] Retries:[10  ]
   < > Strong  Retries:[3   ] DiffOK:[4  ] MinLEN:[9   ]
               Digits:  [-1 ] Upper: [-1 ] Lower: [-1 ] Other:[-1 ]

                                                                < Update >
└──────────────────────────────────────────────────────────────────────────

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

3. Sélectionnez **Regular**, **Random** ou **Strong** pour les mots de passe **admin** et **status** (s'ils sont activés).

Paramètre de mot de passe	Description
Regular	Il s'agit de mots de passe standard. Les mots de passe doivent contenir plus de quatre caractères avec peu de restrictions. Il s'agit de la configuration de mot de passe par défaut du système.
Random	Fournit des mots de passe générés de manière aléatoire. Configure la taille (size) maximum de mots de passe en bits (le minimum est 14, le maximum, 70 ; la valeur par défaut est 20) et le nombre de tentatives (retries) (la valeur par défaut est 10), c'est-à-dire le nombre de fois que le système vous demandera si vous acceptez le nouveau mot de passe. Vous pouvez accepter (en tapant le nouveau de passe deux fois) ou rejeter le mot de passe aléatoire. Vous ne pouvez pas choisir votre propre mot de passe.

Strong	Impose des mots de passe forts. **Retries** représente le nombre d'invites que vous recevez avant l'affichage d'un message d'erreur. **DiffOK** indique le nombre de caractères pouvant être identiques dans le nouveau mot de passe et l'ancien. **MinLEN** est la longueur minimum de caractères requise dans le mot de passe. Indiquez dans les champs Digits (chiffres), Upper (majuscules), Lower (minuscules) et Other (spéciaux), les caractères nécessaires dans le mot de passe. Les nombres positifs représentent le « crédit » maximum de cette classe de caractères pouvant être pris en compte dans l'évaluation de la « simplicité ». Les nombres négatifs impliquent que le mot de passe DOIT comporter un nombre minimum de caractères d'une classe donnée. Ainsi, -1 indique que chaque mot de passe doit comporter au moins un chiffre.

Configuration des comptes

Par défaut, le compte **status** ne nécessite pas de mot de passe, mais vous pouvez le configurer pour qu'il en requiert un. D'autres aspects du mot de passe **admin** peuvent être configurés et les comptes d'assistance sur site, activés ou désactivés.

➢ *Pour configurer des comptes :*

1. Choisissez **Operation** > **Admin** > **DiagCon Passwords** > **Account Configuration**.

2. Dans l'écran qui apparaît, vous pouvez consulter les paramètres de chaque compte, **Status**, **Admin**, **FS1** et **FS2**.

```
 File  Operation

┌ CC-SG Administrator Console: Account Settings: ──────────────────────────────
Account Configuration:
Field: \ User: Status:        Admin:         FS1:           FS2:
User Name:     status         admin          fs1            fs2
Last Changed:  Dec 12, 2006   Dec 12, 2006   Dec 13, 2006   Dec 13, 2006
Expire:        Never          Never          Never          Never

Mode:          < > Disabled                  < > Disabled   <o> Disabled
               < > Enabled                   <o> Enabled    < > Enabled
               <o> NoPassword
Min Days:      [0      ]      [0      ]
Max Days:      [99999  ]      [99999  ]
Warn:          [7      ]      [7      ]
Max # Logins:  [-1     ]      [2      ]      [1      ]      [0      ]
Update Param:   <UPDATE>       <UPDATE>       <UPDATE>       <UPDATE>
New Password:  <New Password> <New Password>

                                   < RESET to Factory Password Configuration >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Cet écran est divisé en trois zones principales :

- Celle du haut affiche des informations en lecture seule sur les comptes du système.
- La section du milieu présente les différents paramètres pertinents pour chaque ID, ainsi qu'un jeu de boutons, afin de permettre la mise à jour de ces paramètres ou la définition de nouveaux mots de passe pour les comptes.
- La dernière zone sert à restaurer les paramètres usine pour la configuration du mot de passe (c'est-à-dire les paramètres du système au moment de son expédition).

3. Si vous souhaitez rendre le mot de passe obligatoire pour le compte **Status**, sélectionnez **Enabled** sous ce dernier.

4. Pour les comptes **Admin** et **Status**, vous pouvez configurer :

Paramètre	Description
User \ User Name	(Lecture seule). Il s'agit du nom d'utilisateur ou de l'ID actuel du compte.
Last Changed	(Lecture seule). Il s'agit de la date de dernière modification du mot de passe pour ce compte.

Raritan.
When you're ready to take control®

Expire	(Lecture seule). Indique le jour où ce compte doit changer de mot de passe.
Mode	Option configurable si le compte est désactivé (aucune connexion autorisée) ou activé (jeton d'authentification obligatoire), ou si l'accès est autorisé et qu'aucun mot de passe n'est requis. (Ne verrouillez pas les comptes Admin et FS1 en même temps, vous ne pourriez plus utiliser la console de diagnostic.)
Min Days	Nombre minimum de jours après lesquels un mot de passe peut être à nouveau changé. La valeur par défaut est **0**.
Max Days	Nombre maximum de jours pendant lesquels le mot de passe sera effectif. La valeur par défaut est **99999**.
Avertissement	Nombre de jours pendant lesquels des messages d'avertissement sont affichés avant expiration du mot de passe.
Max # of Logins	Nombre maximum de connexions simultanées autorisées par le compte. Les chiffres négatifs indiquent qu'il n'existe aucune restriction (**-1** est la valeur par défaut pour la connexion status). **0** signifie que personne ne peut se connecter. Un chiffre positif définit le nombre d'utilisateurs pouvant se connecter simultanément (**2** est la valeur par défaut pour la connexion admin).
UPDATE	Enregistre les modifications effectuées pour cet ID.
New Password	Entrez un nouveau mot de passe pour ce compte.

Affichage de l'état des disques (Utilitaires)

Cette option affiche l'état des disques CC-SG, par exemple leur taille, s'ils sont actifs, l'état de RAID-1 et la quantité d'espace actuellement utilisée par différents systèmes de fichiers.

➢ *Pour afficher l'état du disque de CC-SG :*

1. Choisissez **Operation** > **Utilities** > **Disk Status**.
2. Cliquez sur **Refresh** ou appuyez sur **Entrée** pour actualiser l'affichage. Le rafraîchissement de l'écran est particulièrement utile lors de la mise à niveau ou de l'installation, et lorsque vous souhaitez voir la progression des disques RAID au fur et à mesure de leurs reconstruction et synchronisation.

```
 File  Operation

 CC-SG Administrator Console: Disk Status:
Personalities : [raid1]
md1 : active raid1 sdb2[1] sda2[0]
      78043648 blocks [2/2] [UU]

md0 : active raid1 sdb1[1] sda1[0]
      104320 blocks [2/2] [UU]

Filesystem            Size  Used Avail Use% Mounted on
/dev/mapper/svg-root  4.9G  115M  4.5G   3% /
/dev/md0               99M  9.0M   85M  10% /boot
/dev/mapper/svg-opt   5.8G  334M  5.2G   6% /opt
/dev/mapper/svg-sg    2.9G  195M  2.6G   7% /sg
/dev/mapper/svg-DB    8.7G  286M  8.0G   4% /sg/DB
/dev/mapper/svg-tmp   2.0G  339M  1.6G  18% /tmp
/dev/mapper/svg-usr   2.0G  580M  1.3G  31% /usr
/dev/mapper/svg-var   7.7G  133M  7.2G   2% /var
                                                    < Refresh >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

Remarque : *les disques durs sont entièrement synchronisés et la protection totale du RAID-1 est disponible lorsqu'un écran semblable à celui présenté ci-dessus s'affiche. L'état des tableaux* ***md0*** *et* ***md1*** *est* ***[UU]****).*

Raritan.
When you're ready to take control®

Affichage des processus exécutés sur CC-SG avec la console de diagnostic

L'option Top Display présente la liste des processus actuellement exécutés sur CC-SG, les attributs de ces processus, ainsi que l'état général du système.

➢ *Pour afficher les processus exécutés sur CC-SG :*

1. Choisissez **Operation** > **Utilities** > **Top Display**.
2. Affichez le nombre des processus exécutés, en veille, le total des processus et ceux qui sont arrêtés.

```
top - 20:19:27 up 1 day, 23:33,  6 users,  load average: 0.55, 0.27, 0.20
Tasks: 117 total,   1 running, 116 sleeping,   0 stopped,   0 zombie
Cpu(s):  5.6% us,  8.6% sy,  0.0% ni, 85.7% id,  0.0% wa,  0.0% hi,  0.0% si
Mem:   2076088k total,  1351804k used,   724284k free,   245720k buffers
Swap:  2031608k total,        0k used,  2031608k free,   795588k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
20271 sg        16   0  275m  26m  11m S  1.7  1.3   0:14.09 jsvc
 4990 root      23   0  5452 3460 1780 S  0.3  0.2   4:30.55 status-poller.p
12634 admin     16   0  2584  960  748 R  0.3  0.0   0:00.01 top
    1 root      16   0  2280  544  468 S  0.0  0.0   0:00.79 init
    2 root      34  19     0    0    0 S  0.0  0.0   0:00.24 ksoftirqd/0
    3 root       5 -10     0    0    0 S  0.0  0.0   0:00.68 events/0
    4 root       5 -10     0    0    0 S  0.0  0.0   0:00.00 khelper
    5 root      15 -10     0    0    0 S  0.0  0.0   0:00.00 kacpid
   25 root       5 -10     0    0    0 S  0.0  0.0   0:00.00 kblockd/0
   35 root      15   0     0    0    0 S  0.0  0.0   0:00.12 pdflush
   36 root      15   0     0    0    0 S  0.0  0.0   0:01.13 pdflush
   38 root      13 -10     0    0    0 S  0.0  0.0   0:00.00 aio/0
   26 root      15   0     0    0    0 S  0.0  0.0   0:00.00 khubd
   37 root      15   0     0    0    0 S  0.0  0.0   0:00.02 kswapd0
  111 root      25   0     0    0    0 S  0.0  0.0   0:00.00 kseriod
  181 root       5 -10     0    0    0 S  0.0  0.0   0:00.00 ata/0
  183 root      22   0     0    0    0 S  0.0  0.0   0:00.00 scsi_eh_0
```

3. Entrez **h** pour afficher un écran d'aide pour la commande top. La touche d'aide **F1** ne fonctionne pas ici.

Affichage de l'état de NTP (Utilitaires)

Cette option affiche l'état du démon de temps NTP s'il est configuré et exécuté sur CC-SG. Le démon NTP peut être configuré uniquement dans l'interface utilisateur graphique de l'administrateur de CC-SG, Director Client.

➢ *Pour afficher l'état du démon NTP sur CC-SG :*

1. Choisissez **Operation** > **Utilities** > **NTP Status Display**.

- NTP n'est pas activé ou configuré correctement :

```
 File  Operation

 CC-SG Administrator Console: NTP Status:

NTP Daemon does not appear to be running

                                                          < Refresh >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

- NTP est configuré ou exécuté correctement :

```
 File  Operation

 CC-SG Administrator Console: NTP Status:
NTP Daemon PID=17735
synchronised to NTP server (81.0.239.181) at stratum 3
   time correct to within 143 ms
   polling server every 64 s

-----------

client    127.127.1.0
client    81.0.239.181
client    152.118.24.8
     remote           local      st poll reach  delay   offset    disp
==============================================================================
=127.127.1.0     127.0.0.1       10   64  377 0.00000  0.000000 0.03061
*81.0.239.181    192.168.51.40    2   64  377 0.13531 -0.026990 0.05887
=152.118.24.8    192.168.51.40    3   64  377 0.39163 -0.039222 0.07307

                                                          < Refresh >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```


Raritan.
When you're ready to take control®

Annexe A Spécifications pour G1, V1 et E1

Dans ce chapitre

Modèle G1 259
Modèle V1 260
Modèle E1 262

Modèle G1

G1 - Spécifications générales

Facteur de forme	1U
Dimensions (PxLxH)	563 mm x 440 mm x 44 mm
Poids	10,92 kg
Alimentation	Détection automatique des alimentations redondantes permutables à chaud, 110/220 V, 2.0A
Temps moyen entre défaillances (MTBF)	38 269 heures
Port d'administration KVM	(Clavier/souris DB15 + PS2)
Port d'administration série	DB9
Port de console	S/O

G1 - Spécifications matérielles

Processeur	Intel® Pentium® III 1 GHz
Mémoire	512 Mo
Interfaces réseau	(2) 10/100 Ethernet (RJ45)
Disque dur et contrôleur	RAID 1 avec (2) IDE de 40 Go à 7200 tr/min
Lecteur CD/ROM	CD/ROM 40x lecture seule

G1 - Impératifs d'environnement

En fonctionnement	
Humidité résiduelle	20 à 85 %
Altitude	Fonctionne correctement aux altitudes comprises entre 0 et 10 000 pieds (0 à 3 000 m), stockage à 40 000 pieds (12 000 m) (estimation)
Vibrations	5-55-5 Hz, 0,38mm, 1 minute par cycle, 30 minutes par axe (X, Y, Z)
Chocs	S/O
A l'arrêt	
Température	0 à 30° C (32 à 104° F)
Humidité résiduelle	10 à 90 %
Altitude	Fonctionne correctement aux altitudes comprises entre 0 et 10 000 pieds (0 à 3 000 m), stockage à 40 000 pieds (12 000 m) (estimation)
Vibrations	5-55-5 Hz, 0,38mm, 1 minute par cycle, 30 minutes par axe (X, Y, Z)
Chocs	S/O

Modèle V1

V1 - Spécifications générales

Facteur de forme	1U
Dimensions (PxLxH)	615 mm x 485 mm x 44 mm
Poids	10,80 kg
Alimentation	Alimentation simple (1 x 300 watts)
Température de fonctionnement	10 à 35° C (50 à 95° F)
Temps moyen entre défaillances (MTBF)	36 354 heures

Port d'administration KVM	(Clavier/souris DB15 + PS2 ou USB)
Port d'administration série	DB9
Port de console	(2) ports USB 2.0

V1 - Spécifications matérielles

Processeur	AMD Opteron 146
Mémoire	2 Go
Interfaces réseau	(2) 10/100/1000 Ethernet (RJ45)
Disque dur et contrôleur	RAID 1 avec (2) SATA de 80 Go à 7200 tr/min
Lecteur CD/ROM	DVD-ROM

V1 - Impératifs d'environnement

En fonctionnement	
Humidité résiduelle	8 à 90 %
Altitude	Fonctionne correctement aux altitudes comprises entre 0 et 3 048 m, stockage à 12 192 m (estimation)
Vibrations	5-55-5 HZ, 0,38 mm, 1 minute par cycle ; 30 minutes par axe (X,Y,Z)
Chocs	S/O
A l'arrêt	
Température	-40 à +60° C (-40° à 140° F)
Humidité résiduelle	5 à 95 %
Altitude	Fonctionne correctement aux altitudes comprises entre 0 et 3 048 m, stockage à 12 192 m (estimation)

Vibrations	5-55-5 HZ, 0,38mm,1 minute par cycle ; 30 minutes par axe (X,Y,Z)
Chocs	S/O

Modèle E1

E1 - Spécifications générales

Facteur de forme	2U
Dimensions (PxLxH)	687 mm x 475 mm x 88 mm
Poids	20 kg
Alimentation	Alimentation 2U 500W permutable à chaud SP502-2S
Température de fonctionnement	0 à 50° C
Temps moyen entre défaillances (MTBF)	53 564 heures
Port d'administration KVM	Ports clavier et souris PS/2, 1 port VGA
Port d'administration série	Port série Fast UART 16550
Port de console	(2) ports USB 2.0

E1 - Spécifications matérielles

Processeur	(2) processeurs AMD Opteron 250 2,4 GHz 1 Mo
Mémoire	4 Go
Interfaces réseau	Adaptateur serveur double port Intel PRO/1000 PT
Disque dur et contrôleur	Cache 16 Mo avec (2) WD740ADFD SATA de 74 Go à 10K tr/min
Lecteur CD/ROM	DVD-ROM

Raritan.
When you're ready to take control®

E1 - Impératifs d'environnement

En fonctionnement	
Humidité résiduelle	5 à 90 %, sans condensation
Altitude	Niveau de la mer à 213 360.00 cm
Vibrations	Balayage de 10 à 500 Hz à une accélération constante de 0,5 g pendant une heure, sur chaque axe perpendiculaire X, Y et Z
Chocs	5 g pendant 11 ms avec demi-onde sinusoïdale pour chaque axe perpendiculaire X, Y et Z
A l'arrêt	
Température	-40° à 70° C
Humidité résiduelle	5 à 90 %, sans condensation
Altitude	Niveau de la mer à 1 219 200.00 cm
Vibrations	Balayage de 10 à 300 Hz à une accélération constante de 2 g pendant une heure, sur chaque axe perpendiculaire X, Y et Z
Chocs	30 g pendant 11 ms avec demi-onde sinusoïdale pour chaque axe perpendiculaire X, Y et Z

Annexe B Configuration de CC-SG et du réseau

Dans ce chapitre

A propos de cette annexe.....264
Ports ouverts requis pour les réseaux CC-SG : Synthèse 264
Canaux de communication CC-SG.....266

A propos de cette annexe

Cette annexe indique la configuration réseau requise (adresses, protocoles et ports) d'un déploiement CC-SG standard. Elle comporte des informations relatives au mode de configuration de votre réseau pour l'accès externe (le cas échéant), ainsi que pour la mise en application de la sécurité interne et de la stratégie d'acheminement (le cas échéant). Ces données sont destinées à l'administrateur d'un réseau TCP/IP, dont le rôle et les responsabilités peuvent s'étendre au-delà de ceux d'un administrateur CC-SG, et qui souhaite intégrer CC-SG et ses composants aux stratégies d'accès de sécurité et d'acheminement d'un site.

Les tableaux qui suivent indiquent les protocoles et ports nécessaires à CC-SG et à ses composants associés.

Ports ouverts requis pour les réseaux CC-SG : Synthèse

Les ports suivants doivent être ouverts :

Numéro de port	Protocole	Usage
80	TCP	Accès HTTP à CC-SG
443	TCP	Accès HTTPS (SSL) à CC-SG
8080	TCP	CC-SG <-> Client PC
2400	TCP	Accès au nœud (mode Proxy et accès en bande)

5000	TCP	Accès au nœud (mode direct) Ces ports doivent être ouverts par dispositif Raritan accessible en externe. Les autres ports du tableau doivent être ouverts uniquement pour accéder à CC-SG.
51000	TCP	Accès cible SX (mode direct)

Exceptions possibles :

le port 80 peut être abandonné si l'accès à CC-SG est toujours effectué via des adresses HTTPS ;

les ports 5000 et 51000 peuvent être abandonnés si le mode Proxy de CC-SG est utilisé pour toutes les connexions depuis les pare-feu.

Ainsi, une configuration minimum nécessite l'ouverture de trois (3) ports uniquement [443, 8080 et 2400] pour permettre un accès externe à CC-SG.

Canaux de communication CC-SG

Les canaux de communication sont partitionnés comme suit :

- CC-SG vers dispositifs Raritan
- CC-SG vers cluster CC-SG (facultatif)
- CC-SG vers services d'infrastructure
- Clients vers CC-SG
- Clients vers cibles (mode direct)
- Clients vers cibles (mode Proxy)
- Clients vers cibles (en bande)
- CC-SG vers CC-NOC

Pour chaque canal de communication, les tableaux des sections suivantes :

- représentent les **adresses IP** symboliques utilisées par les parties en communication. Ces adresses doivent être autorisées sur tous les chemins de communication entre les entités ;
- indiquent la **direction** de la communication. Ceci peut être important pour les stratégies particulières à votre site. Pour un rôle CC-SG donné, le chemin entre les parties en communication correspondantes doit être disponible, ainsi que pour les autres chemins de réacheminement qui pourraient être utilisés dans le cas d'une défaillance de réseau ;
- fournissent les **numéro de port** et **protocole** utilisés par CC-SG ;
- indiquent si le port est **configurable**, ce qui signifie que l'interface utilisateur graphique ou la console de diagnostic fournit un champ dans lequel vous pouvez remplacer le numéro de port par défaut indiqué à cause de conflits avec d'autres applications du réseau ou pour des raisons de sécurité.

CC-SG et dispositifs Raritan

Un des rôles principaux de CC-SG consiste à gérer et à contrôler des dispositifs Raritan (par exemple, Dominion KX, KSX, etc.). Généralement, CC-SG communique avec ces dispositifs sur un réseau TCP/IP (local, étendu ou VPN) et les protocoles TCP et UDP sont utilisés comme suit :

Direction de la communication	Numéro de port	Protocole	Configurable ?
CC-SG vers diffusion locale	5000	UDP	oui
CC-SG vers IP LAN distant	5000	UDP	oui
CC-SG vers dispositif Raritan	5000	TCP	oui
Dispositif Raritan vers CC-SG	5001	UDP	non

Cluster CC-SG

Lorsque la fonction facultative Cluster CC-SG est utilisée, les ports suivants doivent être disponibles pour les sous-réseaux en interconnexion. Sinon, il n'est pas nécessaire de les ouvrir.

Chaque CC-SG du cluster peut être sur un LAN distinct. Toutefois, l'interconnexion entre les unités doit être fiable et non soumise à des périodes d'encombrement.

Direction de la communication	Numéro de port	Protocole	Configurable ?
CC-SG vers diffusion locale	10000	UDP	non
CC-SG vers IP LAN distant	10000	UDP	non
CC-SG vers CC-SG	5432	TCP	non
CC-SG vers CC-SG	8732	TCP	non
CC-SG vers CC-SG	3232	TCP	non

Accès aux services d'infrastructure

CC-SG peut être configuré pour utiliser plusieurs services conformes aux normes de l'industrie comme DHCP, DNS et NTP. Pour que CC-SG communique avec ces serveurs facultatifs, les ports et protocoles suivants sont utilisés :

Direction de la communication	Numéro de port	Protocole	Configurable ?
Serveur DHCP vers CC-SG	68	UDP	Non
CC-SG vers serveur DHCP	67	UDP	Non
Serveur NTP vers CC-SG	123	UDP	Non
CC-SG vers DNS	53	UDP	Non

Clients PC vers CC-SG

Les clients PC se connectent à CC-SG via un de ces trois modes :

- Interfaces utilisateur graphiques Client Admin ou Client d'accès via un navigateur Web
- Interface de ligne de commande (CLI) via SSH
- Console de diagnostic

Direction de la communication	Numéro de port	Protocole	Configurable ?
Client PC vers interface utilisateur graphique CC-SG	443	TCP	non
Client PC vers interface utilisateur graphique CC-SG	80	TCP	non
Client PC vers interface utilisateur graphique CC-SG	8080	TCP	non
Client PC vers CLI SSH	22	TCP	oui

Client PC vers console de diagnostic	23	TCP	oui

Clients PC vers nœuds

L'autre rôle important de CC-SG consiste à connecter des clients PC à différents nœuds. Ceux-ci peuvent être des connexions de console en série ou KVM aux dispositifs Raritan (appelées connexions hors bande). Un autre mode consiste à utiliser les méthodes d'accès en bande (IBA), par exemple, Virtual Network Computer (VNC), Windows Remote Desktop (RDP) ou Secure Shell (SSH).

Un autre aspect de la communication entre client PC et cible implique que :

- le client PC est connecté directement à la cible (via un dispositif Raritan ou un accès en bande) ; il s'agit du **mode direct** ;
- ou, le client PC est connecté à la cible via CC-SG qui sert de pare-feu d'application ; il s'agit du **mode Proxy**.

Direction de la communication	Numéro de port	Protocole	Configurable ?
Client vers CC-SG via Proxy vers cible	2400 (sur CC-SG)	TCP	non
Client vers cible Raritan (mode direct)	5000 (sur dispositif)	TCP	oui
Client vers Dominion SX vers cible (mode direct)	51000	TCP	oui

CC-SG et client pour IPMI, iLO/RILOE, DRAC, RSA

Un autre rôle important de CC-SG est de gérer des dispositifs tiers, tels que des dispositifs iLO/RILOE ou des serveurs Integrated Lights Out/Remote Insight Lights Out de Hewlett Packard. Les cibles d'un dispositif iLO/RILOE sont mises sous/hors tension et réactivées directement. Les serveurs IPMI (Intelligent Platform Management Interface) peuvent également être contrôlés par CC-SG. Les cibles DRAC et RSA Dell peuvent aussi être gérées par CC-SG.

Direction de la communication	Numéro de port	Protocole	Configurable
CC-SG vers IPMI	623	UDP	non
CC-SG vers iLO/RILOE (utilise des ports HTTP)	80 ou 443	UDP	non
CC-SG vers DRAC	80 ou 443	UDP	non
CC-SG vers RSA	80 ou 443	UDP	non

CC-SG et SNMP

Le protocole SNMP (Simple Network Management Protocol) permet à CC-SG d'envoyer des traps SNMP (notifications d'événements) à un gestionnaire SNMP du réseau. CC-SG prend également en charge les opérations GET/SET SNMP avec les solutions de gestion d'entreprise tierces, comme HP OpenView.

Direction de la communication	Numéro de port	Protocole	Configurable ?
Gestionnaire SNMP vers CC-SG	161	UDP	oui
CC-SG vers gestionnaire SNMP	162	UDP	oui

Raritan.
When you're ready to take control®

CC-SG et CC-NOC

L'appareil facultatif CC-NOC peut être déployé conjointement à CC-SG. CC-NOC est une console de surveillance réseau Raritan qui permet l'audit et la surveillance du statut des serveurs, de l'équipement et des dispositifs Raritan gérés par CC-SG.

Direction de la communication	Numéro de port	Protocole	Configurable ?
CC-SG vers CC-NOC	9443	TCP	non

Ports internes CC-SG

CC-SG utilise plusieurs ports pour les fonctions internes. Sa fonction de pare-feu local bloque l'accès à ces derniers. Cependant, certains analyseurs externes peuvent détecter ceux-ci comme « bloqués » ou « filtrés ». L'accès externe à ces ports n'est pas obligatoire et peut être bloqué davantage. Les ports actuellement utilisés sont :

- 1088
- 1098
- 2222
- 4444
- 4445
- 8009
- 8083
- 8093

En plus de ces ports, CC-SG peut utiliser des ports TCP et UDP de la série 32xxx (ou supérieure). L'accès externe à ces ports n'est pas obligatoire et peut être bloqué.

Accès à CC-SG via un pare-feu compatible NAT

Si le pare-feu utilise la conversion NAT (Network Address Translation) en même temps que la conversion PAT (Port Address Translation), alors le mode Proxy doit être activé pour toutes les connexions utilisant ce pare-feu. De plus, ce pare-feu doit être configuré pour des connexions externes aux ports 80 (non-SSL)/443 (SSL), 8080 et 2400 pour être transmis à CC-SG (puisque le client PC initialise les sessions sur ces ports).

Remarque : *il n'est pas recommandé d'exécuter du trafic non-SSL via un pare-feu.*

Toutes les connexions en bande utilisent CC-SG comme connexion Proxy. Aucune autre configuration n'est nécessaire. Les connexions hors bande qui utilisent le pare-feu doivent être configurées pour utiliser le mode Proxy. Reportez-vous à ***Modes de connexion : direct et Proxy*** (à la page 185) pour en savoir plus. CC-SG se connecte aux différentes cibles (IBA ou OBA) pour répondre aux demandes du client PC. Toutefois, CC-SG mettra fin à la connexion TCP/IP entre le client PC et la cible qui passe par le pare-feu.

Raritan.
When you're ready to take control®

Annexe C Privilèges de groupe d'utilisateurs

Menu > Sous-menu	Option de menu	Privilège requis	Description
Passerelle sécurisée	**Ce menu est disponible pour tous les utilisateurs.**		
	Mon profil	Aucun*	
	Message du jour	Aucun*	
	Imprimer	Aucun*	
	Déconnexion	Aucun*	
	Quitter	Aucun*	
Utilisateurs	**Ce menu et l'arborescence Utilisateurs sont disponibles uniquement pour les utilisateurs disposant du privilège User Management (gestions des utilisateurs).**		
> Gestionnaire des utilisateurs	> Ajouter un utilisateur	User Management	
	(Modification des utilisateurs)	User Management	Via Profil utilisateur
	> Supprimer un utilisateur	User Management	
	> Supprimer un utilisateur du groupe	User Management	
	> Déconnecter l'utilisateur	User Management	
	> Copier en bloc	User Management	
> Gestionnaire des groupes d'utilisateurs	> Ajouter un groupe d'utilisateurs	User Management	
	(Modification des groupes d'utilisateurs)	User Management	Via Profil du groupe d'utilisateurs

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Supprimer un groupe d'utilisateurs	User Management	
	> Affecter des utilisateurs à un groupe	User Management	
	> Déconnecter les utilisateurs	User Management	
Dispositifs	**Ce menu et l'arborescence Dispositifs sont disponibles uniquement pour les utilisateurs disposant d'un des privilèges suivants :** Device, Port and Node Management Device Configuration and Upgrade Management		
	Détecter les dispositifs	Device, Port and Node Management	
> Gestionnaire des dispositifs	> Ajouter un dispositif	Device, Port and Node Management	
	(Modification des dispositifs)	Device, Port and Node Management	Via Profil du dispositif
	> Supprimer un dispositif	Device, Port and Node Management	
	> Copier en bloc	Device, Port and Node Management	
	> Mettre le dispositif à jour	Device Configuration and Upgrade Management	
>> Configuration	>> Sauvegarde	Device Configuration and Upgrade Management	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	>> Restaurer	Device Configuration and Upgrade Management	
	>> Copier la configuration	Device Configuration and Upgrade Management	
	> Redémarrer le dispositif	Device, Port and Node Management ou Device Configuration and Upgrade Management	
	> Envoyer une commande ping au dispositif	Device, Port and Node Management ou Device Configuration and Upgrade Management	
	> Suspendre la gestion	Device, Port and Node Management ou Device Configuration and Upgrade Management	
	> Gestionnaire d'alimentation des dispositifs	Device, Port and Node Management	
	> Démarrer Admin	Device, Port and Node Management ou Device Configuration and Upgrade Management	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Lancer l'Admin de station utilisateur		
	> Déconnecter utilisateurs	Device, Port and Node Management ou Device Configuration and Upgrade Management	
	> Vue topologique	Device, Port and Node Management	
> Modifier la vue	> Créer une vue personnalisée	Device, Port and Node Management ou Device Configuration and Upgrade Management	
	> Arborescence	Device, Port and Node Management ou Device Configuration and Upgrade Management	
> Gestionnaire des ports	> Connecter	Device, Port and Node Management	
	> Configurer les ports	Device, Port and Node Management	
	> Ajouter le port aux signets	Device, Port and Node Management	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Se déconnecter du port	Device, Port and Node Management	
	> Copier en bloc	Device, Port and Node Management	
	> Supprimer des ports	Device, Port and Node Management	
> Options de tri des ports	> Par nom de port	Device, Port and Node Management ou Device Configuration and Upgrade Management	
	> Par état de port	Device, Port and Node Management ou Device Configuration and Upgrade Management	
Nœuds	**Ce menu et l'arborescence Nœuds sont disponibles uniquement pour les utilisateurs disposant d'un des privilèges suivants :** Device, Port and Node Management Node In-Band Access (accès en bande au nœud) Node Out-of-Band Access (accès hors bande au nœud) Node Power Control		
	Ajouter un nœud	Device, Port and Node Management	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	(Modification des nœuds)	Device, Port and Node Management	Via Profil du nœud
	Supprimer un nœud	Device, Port and Node Management	
	<nomInterface>	In-Band Access ou Out-of-Band Access	
	Déconnecter	In-Band Access ou Out-of-Band Access	
	Power Control	Power Control	
	Regrouper la gestion de l'alimentation	Power Control	
> Options de tri du nœud	> Par nom de nœud	L'un des suivants : Device, Port and Node Management ou In-Band Access ou Out-of-Band Access ou Power Control	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Par état de nœud	L'un des suivants : Device, Port and Node Management ou Node In-Band Access ou Node Out-of-Band Access ou Node Power Control	
> Conversation	> Démarrer la session de conversation	Node In-Band Access ou Node Out-of-Band Access ou Node Power Control	
	> Afficher la session de conversation	Node In-Band Access ou Node Out-of-Band Access ou Node Power Control	
	> Terminer la session de conversation	Node In-Band Access ou Node Out-of-Band Access ou Node Power Control	

Menu > Sous-menu	Option de menu	Privilège requis	Description
> Modifier la vue	> Créer une vue personnalisée	L'un des suivants : Device, Port and Node Management ou Node In-Band Access ou Node Out-of-Band Access ou Node Power Control	
	> Arborescence	L'un des suivants : Device, Port and Node Management ou Node In-Band Access ou Node Out-of-Band Access ou Node Power Control	
Associations	**Ce menu est disponible uniquement pour les utilisateurs disposant du privilège User Security Management (gestion de la sécurité des utilisateurs).**		
	> Associations	User Security Management	Comporte la capacité d'ajouter, de modifier et de supprimer.

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Groupe de dispositifs	User Security Management	Comporte la capacité d'ajouter, de modifier et de supprimer.
	> Groupe de nœuds	User Security Management	Comporte la capacité d'ajouter, de modifier et de supprimer.
	> Stratégies	User Security Management	Comporte la capacité d'ajouter, de modifier et de supprimer.
Rapports	**Ce menu est disponible pour tous les utilisateurs.**		
	Journal d'audit	CC Setup and Control	
	Journal d'erreurs	CC Setup and Control	
	Rapport d'accès	CC Setup and Control	
	Rapport de disponibilité	Device, Port and Node Management ou Device Configuration and Upgrade Management	
> Utilisateurs	> Utilisateurs actifs	User Management	
	> Utilisateurs verrouillés	CC Setup and Control	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Données d'utilisateurs	Pour consulter les données de tous les utilisateurs : User Management Pour consulter vos propres données utilisateur : Aucun	
	> Utilisateurs dans groupes	User Management	
	> Données de groupes	User Security Management	
> Dispositifs	Gestion du parc	Device, Port and Node Management	
> Nœuds	> Rapport sur le parc du nœud	Device, Port and Node Management	
	> Nœuds actifs	Device, Port and Node Management	
	> Création du nœud	Device, Port and Node Management	
> Ports	> Interrogation des ports	Device, Port and Node Management	
	> Ports actifs	Device, Port and Node Management	
> Répertoire actif	Rapport sur le groupe d'utilisateurs AD		

Menu > Sous-menu	Option de menu	Privilège requis	Description
	Rapports programmés	CC Setup and Control	
	Synchronisation CC-NOC	CC Setup and Control	
Accès			
	Configuration CC-NOC	CC Setup and Control	
Administration	**Ce menu est disponible uniquement pour les utilisateurs disposant d'un des privilèges suivants :** CC Setup and Control Combinaison de Device, Port and Node Management (gestion des dispositifs, des ports et des nœuds), User Management (gestion des utilisateurs) et User Security Management (gestion de la sécurité des utilisateurs)		
	Paramétrage guidé	Tous les privilèges suivants : Device, Port and Node Management, User Management et User Security Management	
	Paramétrage du Message du jour	CC Setup and Control	
	Applications	CC Setup and Control	
	Firmware	Device, Port and Node Management	
	Configuration	CC Setup and Control	
	Sécurité	CC Setup and Control	
	Notifications	CC Setup and Control	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	Tâches	CC Setup and Control	
	Matrice de compatibilité	Device Configuration and Upgrade Management	
Maintenance du système			
	Sauvegarde	CC Setup and Control	
	Restaurer	CC Setup and Control	
	Réinitialiser	CC Setup and Control	
	Redémarrer	CC Setup and Control	
	Mettre à niveau	CC Setup and Control	
	Arrêter	CC Setup and Control	
> Mode de maintenance	> Entrer en mode de maintenance	CC Setup and Control	
	> Quitter le mode de maintenance	CC Setup and Control	
View		Aucun*	
Fenêtre		Aucun*	
Aide		Aucun*	

*Aucun indique qu'aucun privilège particulier n'est requis. Tous les utilisateurs ayant accès à CC-SG peuvent accéder à ces menus et commandes.

Annexe D Traps SNMP

CC-SG fournit les traps SNMP suivants :

Trap SNMP	Description
ccUnavailable	L'application CC-SG n'est pas disponible.
ccAvailablecustomerservice@cs.sephora.com	L'application CC-SG est disponible.
ccUserLogin	Un utilisateur CC-SG s'est connecté.
ccUserLogout	Un utilisateur CC-SG s'est déconnecté.
ccPortConnectionStarted	Une session CC-SG a démarré.
ccPortConnectionStopped	Une session CC-SG s'est arrêtée.
ccPortConnectionTerminated	Une session CC-SG s'est interrompue.
ccImageUpgradeStarted	La mise à niveau d'image CC-SG a commencé.
ccImageUpgradeResults	La mise à niveau d'image CC-SG est réalisée.
ccUserAdded	Un nouvel utilisateur a été ajouté à CC-SG.
ccUserDeleted	Un utilisateur a été supprimé de CC-SG.
ccUserModified	Un utilisateur CC-SG a été modifié.
ccUserAuthenticationFailure	Echec d'authentification d'utilisateur CC-SG.
ccLanCardFailure	CC-SG a détecté une défaillance de la carte LAN.
ccHardDiskFailure	CC-SG a détecté une défaillance du disque dur.
ccLeafNodeUnavailable	CC-SG a détecté un échec de connexion à un nœud feuille.

ccLeafNodeAvailable	CC-SG a détecté un nœud feuille joignable.
ccIncompatibleDeviceFirmware	CC-SG a détecté un dispositif avec un firmware incompatible.
ccDeviceUpgrade	CC-SG a mis à niveau le firmware sur un dispositif.
ccEnterMaintenanceMode	CC-SG est entré en mode de maintenance.
ccExitMaintenanceMode	CC-SG a quitté le mode de maintenance.
ccUserLockedOut	Un utilisateur CC-SG a été verrouillé.
ccDeviceAddedAfterCCNOCNotification	CC-SG a ajouté un dispositif après avoir reçu une notification de CC-NOC.
ccScheduledTaskExecutionFailure	Raison de l'échec de l'exécution d'une tâche programmée.
ccDiagnosticConsoleLogin	Un utilisateur s'est connecté à la console de diagnostic CC-SG.
ccDiagnosticConsoleLogout	Un utilisateur s'est déconnecté de la console de diagnostic CC-SG.
ccNOCAvailable	CC-SG a détecté que CC-NOC est disponible.
ccNOCUnavailable	CC-SG a détecté que CC-NOC n'est pas disponible.
ccUserGroupAdded	Un nouveau groupe d'utilisateurs a été ajouté à CC-SG.
ccUserGroupDeleted	Un groupe d'utilisateurs CC-SG a été supprimé.
ccUserGroupModified	Un groupe d'utilisateurs CC-SG a été modifié.
ccSuperuserNameChanged	Le nom du super utilisateur CC-SG a changé.
ccSuperuserPasswordChanged	Le mot de passe du super utilisateur CC-SG a changé.

ccLoginBannerChanged	La bannière de connexion CC-SG a changé.
ccMOTDChanged	Le message du jour CC-SG (MOTD) a changé.

Annexe E Guide de dépannage

Pour lancer CC-SG à partir de votre navigateur Web, il vous faut un plug-in Java. Si votre ordinateur ne dispose pas de la bonne version, CC-SG vous guidera dans la procédure d'installation. Si votre ordinateur ne dispose de plug-in Java, CC-SG ne peut pas être lancé automatiquement. Dans ce cas, vous devez désinstaller ou désactiver votre ancienne version de Java et fournir une connectivité de port série à CC-SG pour assurer un fonctionnement optimal.

- Si l'applet CC-SG ne se charge pas, vérifiez les paramètres de votre navigateur Web.
  - Dans Internet Explorer : vérifiez que le plug-in Java (Sun) est activé.
  - Ouvrez le plug-in Java dans le Panneau de configuration et réglez les paramètres dans votre navigateur.
- Si vous rencontrez des problèmes pour ajouter des dispositifs, vérifiez que les versions des firmware des dispositifs sont correctes.
- Si le câble de l'interface réseau reliant le dispositif et CC-SG est déconnecté, patientez pendant le test de détection de collision défini, puis rebranchez le câble d'interface réseau. Pendant la période de détection de collision configurée, le dispositif fonctionne en mode autonome et est accessible via RRC, MPC ou RC.
- Si vous recevez un message d'erreur indiquant que la version de votre client est différente de la version du serveur et que le comportement peut être imprévisible, vous devez redémarrer et vider la mémoire cache de votre navigateur.

Dans ce chapitre

Configuration requise pour le navigateur client 288

Configuration requise pour le navigateur client

Pour obtenir la liste complète des navigateurs pris en charge, reportez-vous à la **matrice de compatibilité** sur le site Web du support Raritan.

Annexe F Authentification à deux facteurs

CC-SG peut être configuré de manière à pointer sur un serveur RSA RADIUS prenant en charge l'authentification à deux facteurs via un gestionnaire d'authentification RSA. CC-SG se comporte comme un client RADIUS et envoie des demandes d'authentification d'utilisateur au serveur RSA RADIUS. La demande d'authentification inclut un ID utilisateur, un mot de passe fixe et un code de jeton dynamique.

Dans ce chapitre

Authentification à deux facteurs - Environnements pris en charge 289
Authentification à deux facteurs - Configuration requise.....289
Authentification à deux facteurs - Problèmes répertoriés.....290

Authentification à deux facteurs - Environnements pris en charge

Les composants d'authentification à deux facteurs ci-après fonctionnent avec CC-SG :

- RSA RADIUS Server 6.1 sous Windows Server 2003
- RSA Authentication Manager 6.1 sous Windows Server 2003
- Jeton matériel RSA Secure ID SID700.

  Les versions de produit RSA antérieures devraient également fonctionner avec CC-SG, mais elles n'ont pas été vérifiées.

Authentification à deux facteurs - Configuration requise

Les tâches ci-après doivent être effectuées pour la configuration de l'authentification à deux facteurs. Reportez-vous à la documentation RSA pour plus d'informations.

1. Importer des jetons.
2. Créer un utilisateur CC-SG et lui affecter un jeton.
3. Générer un mot de passe d'utilisateur.
4. Créer un hôte d'agent pour le serveur RADIUS.
5. Créer un hôte d'agent (type : serveur de communication) pour CC-SG.
6. Créer un client RADIUS CC-SG.

Authentification à deux facteurs - Problèmes répertoriés

Le mode RSA RADIUS « New PIN » nécessitant un mot de passe ou un numéro d'identification personnel de vérification ne fonctionne pas. Aussi, tous les utilisateurs de ce schéma doivent recevoir des mots de passe fixes.

Annexe G FAQ

Question	Réponse
Généralités	
Qu'est-ce que CC-SG ?	CC-SG est un dispositif de gestion réseau permettant d'ajouter et d'intégrer des serveurs et des équipements réseau généralement déployés dans un centre de données et connectés à un produit Raritan qui prend en charge le protocole IP.
A quoi sert CC-SG ?	La gestion de vos centres de données devient de plus en plus complexe à mesure que vous y déployez d'autres serveurs et dispositifs. CC-SG permet aux administrateurs ou aux responsables système d'accéder à l'ensemble des serveurs, équipements et utilisateurs, et de les gérer à partir d'un dispositif unique.
Qu'est-ce que CommandCenter NOC ?	CommandCenter NOC, ou CC-NOC, est un dispositif de surveillance réseau destiné à l'audit et à la surveillance de l'état des serveurs, de l'équipement et des dispositifs Raritan auxquels CC-SG permet d'accéder.
Quels sont les produits Raritan pris en charge par CC-SG ?	Reportez-vous à la matrice de comptabilité CC-SG sur le site Web du support Raritan.
Comment CC-SG s'intègre-t-il avec les autres produits Raritan ?	CC-SG utilise une technologie de recherche et de détection propriétaire unique qui identifie les dispositifs Raritan et s'y connecte à l'aide d'une adresse réseau connue. Une fois CC-SG connecté et configuré, les dispositifs qui lui sont reliés sont transparents et le fonctionnement et la gestion deviennent extrêmement simples.
L'accès par assistant numérique personnel est-il possible ?	Oui, dans la mesure où l'assistant numérique personnel dispose d'un navigateur Java et prend en charge le cryptage SSL 128 bits (ou de puissance inférieure dans certaines régions). Pour plus d'informations, prenez contact avec le support technique de Raritan. Aucun essai n'a été effectué dans ce domaine.

Question	Réponse
L'état de CC-SG est-il limité par l'état des dispositifs pour lesquels il fait office de proxy ?	Non. Le logiciel de CC-SG réside sur un serveur dédié. Par conséquent, vous pouvez toujours accéder à CC-SG même si le dispositif mandaté par CC-SG est mis hors tension.
Puis-je procéder à la mise à niveau vers de nouvelles versions du logiciel CC-SG lorsque celles-ci seront disponibles ?	Oui. Prenez contact avec le représentant commercial agréé Raritan ou directement avec Raritan, Inc.
Combien de nœuds et/ou d'unités Dominion et/ou d'unités IP-Reach peuvent être connectés à CC-SG ?	Le nombre de nœuds et/ou d'unités Dominion et/ou d'unités IP-Reach pouvant être connectés n'est pas spécifiquement limité. Mais il n'est cependant pas illimité : les performances du processeur et la quantité de mémoire sur le serveur hôte déterminent le nombre de nœuds auxquels il est réellement possible de se connecter.
Existe-t-il une manière d'optimiser les performances de Microsoft Internet Explorer si celui-ci est mon navigateur Web préféré ?	Pour améliorer les performances de Microsoft Internet Explorer lors de l'accès à la console, désactivez les options « Compilateur Java JIT activé », « Journalisation Java activée » et « Console Java activée ». Dans la barre de menus principale, sélectionnez **Outils > Options Internet > Avancées**. Faites défiler la liste des options jusqu'à ce que vous voyiez les éléments ci-dessus et assurez-vous qu'ils **ne sont pas** cochés.
Que faire si je ne parviens pas à ajouter un port série/de console à CC-SG ?	Si le dispositif de console/série est un produit Dominion, vérifiez que les conditions suivantes sont remplies : - l'unité Dominion est active ; - l'unité Dominion n'a pas atteint le nombre maximum de comptes utilisateur configurés.
Quelles sont les versions de Java prises en charge par CC-SG de Raritan ?	Pour en savoir plus sur la configuration Java minimum requise côtés serveur et client, consultez la matrice de compatibilité sur ***http://www.raritan.com/support*** (http://www.raritan.com/support). Cliquez sur Mises à niveau de firmware, puis sur CommandCenter Secure Gateway.

Question	Réponse
Un administrateur a ajouté un nouveau nœud à la base de données CC-SG et me l'a affecté. Comment puis-je l'afficher dans mon arborescence de nœuds ?	Pour mettre l'arborescence à jour et afficher le nœud nouvellement affecté, cliquez sur le bouton de raccourci **Actualiser** de la barre d'outils. Rappelez-vous que l'actualisation de CC-SG ferme toutes les sessions de console en cours.
Comment le Bureau Windows sera-t-il pris en charge à l'avenir ?	Il est possible d'accéder à CC-SG par-delà le pare-feu en configurant les ports correspondants sur le pare-feu. Les ports suivants sont les ports standard : 80 : pour l'accès HTTP via un navigateur Web 443 : pour l'accès HTTPS via un navigateur Web 8080 : pour les fonctions serveur de CC-SG 2400 : pour les connexions en Mode Proxy 5001 : pour la notification d'événements IPR/DKSX/DKX/P2-SC Si un pare-feu se trouve entre deux nœuds de cluster, les ports suivants doivent être ouverts pour que le cluster fonctionne correctement : 8732 : pour le test de détection de collision des nœuds du cluster 5432 : pour la réplication BD des nœuds du cluster
Quelles sont les instructions de conception pour les systèmes à grande échelle ? Contraintes ou hypothèses ?	Raritan propose deux modèles pour l'évolutivité du serveur : le modèle centre de données et le modèle réseau. Le modèle centre de données utilise Paragon pour gérer des milliers de systèmes dans un seul centre de données. Il s'agit de la méthode la plus efficace et la plus rentable pour gérer un emplacement unique. Il prend également en charge le modèle réseau avec IP-Reach et la station utilisateur à accès par IP (UST-IP). Le modèle réseau est géré par le biais du réseau TCP/IP et regroupe l'accès par l'intermédiaire de CC-SG. Les utilisateurs n'ont donc pas besoin de connaître les adresses IP ou la topologie des dispositifs d'accès. Il propose également une connexion unique pratique.

Question	Réponse
Authentification	
Combien de comptes utilisateur peut-on créer pour CC-SG ?	Vérifiez les limites associées à votre licence. Il n'existe pas de limite spécifique au nombre de comptes utilisateur que vous pouvez créer. Ce nombre n'est cependant pas illimité. La taille de la base de données, les performances du processeur et la quantité de mémoire sur le serveur qui héberge CC-SG déterminent le nombre de comptes utilisateur pouvant réellement être créés.
Puis-je attribuer une adresse de nœud spécifique à un utilisateur spécifique ?	Oui, si vous disposez de droits d'administrateur. Les administrateurs ont la possibilité d'affecter des nœuds spécifiques à chaque utilisateur.
Si nous disposons de plus de 1 000 utilisateurs, comment la gestion peut-elle être effectuée ? Active Directory est-il pris en charge ?	CC-SG fonctionne avec Microsoft Active Directory, Sun iPlanet ou Novell eDirectory. Si un compte utilisateur existe déjà sur un serveur d'authentification, CC-SG prend en charge l'authentification à distance à l'aide d'**AD/TACACS+ /RADIUS/LDAP**.
Quelles sont les options disponibles pour l'authentification avec des services d'annuaires et des outils de sécurité tels que LDAP, AD, RADIUS, etc. ?	CC-SG autorise l'authentification locale, ainsi que l'authentification à distance. Les serveurs d'authentification à distance pris en charge sont les suivants : AD, TACACS+, RADIUS et LDAP.
Sécurité	
Parfois, lorsque j'essaie de me connecter, un message m'indique que mon nom d'utilisateur est incorrect, même si je suis certain d'avoir saisi le nom d'utilisateur et le mot de passe exacts. Pourquoi ?	Un identifiant de session spécifique est transmis chaque fois que vous vous connectez à CC-SG. Cet identifiant possède une fonction d'expiration et, en conséquence, si vous ne vous connectez pas à l'unité avant l'expiration, l'identifiant de session n'est plus correct. Actualisez l'affichage de la page en maintenant la touche Maj enfoncée à partir de CC-SG. Vous pouvez également fermer la fenêtre de navigateur actuelle, ouvrir une nouvelle fenêtre de navigateur et vous reconnecter. Cette fonction est une garantie de sécurité supplémentaire ; de cette façon, personne ne peut afficher des informations enregistrées dans la mémoire cache Web pour accéder à l'unité.

Question	Réponse
Comment les mots de passe sont-ils sécurisés ?	Les mots de passe sont chiffrés à l'aide de la technologie de chiffrement MD5, qui utilise un hachage unidirectionnel. Cela permet de prévoir une sécurité complémentaire afin d'empêcher des utilisateurs non autorisés d'accéder à la liste de mots de passe.
Il m'arrive parfois, après avoir laissé mon poste de travail inactif pendant quelques instants, de recevoir un message indiquant que je ne suis plus connecté lorsque je clique sur un menu de CC-SG. Pourquoi ?	CC-SG surveille la durée de chaque session utilisateur. En cas d'inactivité pendant une période prédéfinie, CC-SG déconnecte l'utilisateur. La durée de la période est prédéfinie sur 60 minutes, mais peut être reconfigurée. Il est recommandé aux utilisateurs de **quitter** CC-SG lorsqu'ils terminent une session.
Raritan accède au serveur en tant qu'agent root. Cela peut occasionner des problèmes avec les organismes gouvernementaux. Les clients peuvent-ils accéder au serveur en tant qu'agents root ou Raritan propose-t-il une méthode d'audit/de comptabilité ?	Non, les utilisateurs n'ont pas accès au serveur en tant qu'agents root une fois que l'unité est livrée par Raritan, Inc.
Le chiffrement SSL est-il interne et externe (pas seulement réseau étendu mais également réseau local) ?	Les deux. La session est chiffrée sans tenir compte de l'origine, réseau local ou réseau étendu.
CC-SG prend-il en charge la liste CRL, c'est-à-dire la liste LDAP des certificats invalides ?	Non.
CC-SG prend-il en charge la demande de certificat client ?	Non.
Comptabilité	

Question	Réponse
L'heure des événements dans le rapport Journal d'audit semble incorrecte. Pourquoi ?	L'heure des événements est consignée selon les paramètres de date et d'heure de l'ordinateur client. Vous pouvez modifier ces derniers.
Les fonctions d'audit/enregistrement permettent-elles de savoir quel utilisateur a effectué une mise sous/hors tension ?	La mise hors tension directe n'est pas enregistrée, mais la gestion de l'alimentation par le biais de CC-SG peut être consignée dans des journaux d'audit.
Performances	
En tant qu'administrateur de CC-SG, j'ai ajouté plus de 500 nœuds que je me suis affectés. A présent, la connexion à CC-SG prend beaucoup de temps.	En tant qu'administrateur, lorsqu'un grand nombre de nœuds vous est affecté, CC-SG télécharge les informations pour tous les nœuds lors de la connexion, ce qui ralentit considérablement cette dernière. Nous vous recommandons de ne pas affecter un trop grand nombre de nœuds aux comptes administrateur utilisés essentiellement pour gérer la configuration/les paramètres de CC-SG.
Quelle est la bande passante utilisée par le client ?	Le niveau d'activité réseau d'un accès à distance à une console série sur TCP/IP est pratiquement le même que celui d'une session Telnet. Cependant, il existe une limite de la bande passante RS232 du port de console proprement dit, plus le temps système SSL/TCP/IP. Raritan Remote Client (RRC) gère l'accès à distance à une console KVM. Cette application permet de disposer d'une bande passante ajustable des réseaux locaux jusqu'aux utilisateurs connectés à distance.
Regroupement	
Est-il possible de placer un serveur spécifique dans plusieurs groupes ?	Oui. Tout comme un utilisateur, un dispositif peut appartenir à plusieurs groupes. Par exemple, un système Sun situé à New York City peut appartenir au groupe Sun : « TypeSE = Solaris » et au groupe New York City : « emplacement = NYC ».

Question	Réponse
Quel est l'impact d'une application bloquée par l'utilisation active du port de console, par exemple, certaines variantes UNIX n'autorisant pas l'administration sur des interfaces réseau ?	Une console est généralement considérée comme un chemin d'accès sûr et fiable de dernier recours. Certains systèmes UNIX permettent la connexion à la console en tant qu'agent root. Pour des raisons de sécurité, d'autres systèmes peuvent empêcher les connexions multiples afin que, si l'administrateur est connecté à la console, tout autre accès soit refusé. Enfin, à partir de la console, l'administrateur peut également désactiver les interfaces réseau si cela est nécessaire afin de bloquer tous les autres accès. L'activité normale de la commande sur la console n'a pas un impact plus important que la commande équivalente exécutée à partir d'une autre interface. Cependant, dans la mesure où elle ne dépend pas du réseau, un système trop surchargé pour répondre à une connexion réseau peut encore accepter la connexion de la console. Ainsi, un autre avantage de l'accès via la console est de permettre le dépannage et le diagnostic de problèmes de niveaux système et réseau.
Quelles sont les recommandations au sujet du déplacement/changement des modules d'interface pour ordinateur (CIM) au niveau physique avec des modifications apportées à la base de données logique ?	Chaque CIM a un numéro de série et un nom système cible. Nos systèmes considèrent qu'un CIM reste connecté à la cible correspondant à son nom en cas de déplacement de la connexion d'un commutateur à un autre. Ce mouvement se reflète automatiquement sur la configuration système et est répercuté dans CC-SG. En revanche, si le CIM est déplacé sur un autre serveur, un administrateur doit le renommer.
Interopérabilité	
Comment CC-SG s'intègre-t-il aux produits à châssis à lame ?	CC-SG peut prendre en charge tous les dispositifs disposant d'une interface KVM ou série sous forme d'intercommunication transparente.
Jusqu'à quel niveau CC-SG peut-il s'intégrer à des outils KVM tiers ? Jusqu'au niveau des ports KVM tiers ou simplement jusqu'au niveau du boîtier ?	L'intégration de commutateurs KVM tiers est généralement réalisée à l'aide de macros de clavier lorsque les fabricants KVM tiers ne rendent pas publics les protocoles de communication de leurs commutateurs KVM. Le degré d'intégration varie selon la fonction des commutateurs KVM tiers.

Question	Réponse
Comment puis-je atténuer la restriction de quatre chemins simultanés par l'intermédiaire du boîtier IP-Reach, incluant le calendrier de lancement pour un éventuel boîtier 8 chemins ?	Pour le moment, la meilleure mise en place possible consiste à regrouper les boîtiers IP-Reach à l'aide de CC-SG. A l'avenir, Raritan envisage d'augmenter le nombre de chemins d'accès simultanés par boîtier. Le développement de ces projets doit néanmoins être achevé, d'autres projets ayant été traités en priorité. Nous accueillons néanmoins avec plaisir tous les commentaires relatifs à la demande du marché et aux exemples d'utilisation d'une solution 8 chemins.
Autorisation	
L'autorisation est-elle possible avec RADIUS/TACACS/LDAP ?	LDAP et TACACS sont utilisés uniquement pour l'authentification à distance, non pour l'autorisation.
Expérience utilisateur	
En ce qui concerne la gestion de la console par l'intermédiaire d'un port réseau ou d'un port série local (COM2, par exemple) : la connexion est-elle gérée en local par CC-SG, ou perdue ?	La connexion à CC-SG par l'intermédiaire de la console CC-SG elle-même équivaut à obtenir le privilège racine du système d'exploitation (Linux) sur lequel CC-SG est exécuté. Syslog enregistre ce genre d'événements, mais ce que les utilisateurs saisissent au niveau de la console CC-SG est perdu.

Annexe H Raccourcis clavier

Les raccourcis clavier suivants peuvent être utilisés dans le client Admin Java.

Opération	Raccourci clavier
Actualiser	F5
Panneau d'impression	Ctrl + P
Aide	F1
Insérer une ligne dans le tableau Associations	Ctrl + I

Annexe I Conventions d'appellation

Cette annexe comporte des informations concernant les conventions d'appellation utilisées dans CC-SG. Respectez le nombre maximum de caractères lors de l'appellation de toutes les parties de votre configuration CC-SG.

Limites CC-SG	
Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom du dispositif	32
Groupe de dispositifs	40
Nom du port	32
Nom d'utilisateur	20
Nom du groupe d'utilisateurs	64
Mot de passe (non fort)	16
Mot de passe (fort)	Configurable Minimum : 8 Maximum : 64 Minimum par défaut : 8 Maximum par défaut : 16
Nom de la catégorie	64
Element Name (nom d'élément)	31
Nom de nœud	66
Nom du groupe de nœuds	40
Nom de stratégie	56

Index

A

A propos d'AD et de CC-SG • 122
A propos de cette annexe • 264
A propos de la configuration réseau • 10, 171, 189, 234, 238
A propos de la console d'administrateur • 226, 230
A propos de la console d'état • 226, 229
A propos de la restauration des configurations de dispositifs • 43
A propos de l'authentification et de l'autorisation (AA) • 119
A propos de LDAP et de CC-SG • 134
A propos de mon profil • 98
A propos de RADIUS et de CC-SG • 138
A propos de SNMP et de CC-SG • 187
A propos de TACACS+ et de CC-SG • 137
A propos des applications d'accès aux nœuds • 167
A propos des applications par défaut • 169
A propos des associations • 24
A propos des clusters CC-SG et CC-NOC • 189
A propos des groupes de nœuds • 82
A propos des interfaces • 68
A propos des modes de connexion • 185
A propos des mots de passe CC-SG • 196
A propos des nœuds • 67
A propos des ports LAN CC-SG • 172, 173, 176
A propos des programmes d'émulation de terminal • 225
Accès à CC-SG • 5
Accès à CC-SG via un pare-feu compatible NAT • 272
Accès à la console d'administrateur • 230
Accès à la console de diagnostic via SSH • 226, 227
Accès à la console de diagnostic via un port VGA/clavier/souris • 226, 227
Accès à la console d'état • 229
Accès aux services d'infrastructure • 268
Accès spécial aux dispositifs du système Paragon II • 50
Accès SSH à CC-SG • 194, 217
Accès via un client lourd • 6
Accès via un navigateur • 5
Activer ou désactiver la synchronisation quotidienne de tous les modules AD • 133
Administration avancée • 3, 5, 95, 96, 123, 129, 166
Administration des unités IP-Reach et UST-IP • 50
Affectation de stratégies à des groupes d'utilisateurs • 102, 110
Affectation d'un utilisateur à un groupe • 95, 97
Affecter une vue personnalisée de dispositifs par défaut à tous les utilisateurs • 118
Affecter une vue personnalisée de noeuds par défaut à tous les utilisateurs • 22, 115
Affecter une vue personnalisée par défaut à des dispositifs • 118
Affecter une vue personnalisée par défaut à des noeuds • 114
Affichage de l'état de NTP (Utilitaires) • 257
Affichage de l'état des disques (Utilitaires) • 256
Affichage des dispositifs • 30
Affichage des nœuds • 65
Affichage des processus exécutés sur CC-SG avec la console de diagnostic • 257
Afficher les affectations d'applications par défaut • 169
Afficher les détails d'un rapport • 141
Afficher les paramètres de connexion • 195
Afficher ou masquer les filtres de rapport • 142
Afficher une tâche, les détails d'une tâche et l'historique des tâches • 213
Ajout d'un dispositif • 35
Ajout d'un groupe de nœuds • 83, 102
Ajout d'un groupe d'utilisateurs • 74, 91
Ajout d'un module AD dans CC-SG • 122

Ajout d'un module LDAP (Netscape) dans CC-SG • 134
Ajout d'un module RADIUS • 138
Ajout d'un module TACACS+ • 137
Ajout d'un nœud • 68
Ajout d'un utilisateur • 94, 146
Ajout d'une interface • 68, 69, 77
Ajout d'une stratégie • 82, 102, 103, 107
Ajouter des groupes de dispositifs et de nœuds • 18
Ajouter des groupes d'utilisateurs et des utilisateurs • 21
Ajouter un CC-NOC • 153, 214
Ajouter un dispositif KVM ou série • 35, 59, 61
Ajouter un dispositif PowerStrip • 37
Ajouter un dispositif PowerStrip connecté à un dispositif KX, KX2 ou P2SC • 57
Ajouter un dispositif PowerStrip connecté à un dispositif SX 3.1 • 61, 62
Ajouter un élément • 27
Ajouter un groupe de dispositifs • 51, 54, 102
Ajouter une application • 12, 168
Ajouter une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX • 59
Ajouter une catégorie • 26
Ajouter une interface aux signets • 77
Ajouter une vue personnalisée à des noeuds • 112
Ajouter une vue personnalisée pour les dispositifs • 115
Appliquer une vue personnalisée à des noeuds • 113
Appliquer une vue personnalisée pour des dispositifs • 116
Arrêt de CC-SG • 163
Associations – Définition des catégories et des éléments • 25
Associations dans le paramétrage guidé • 14, 15
Associations, catégories et éléments • 24, 36, 37, 59, 68, 69, 82
Astuces pour ajouter une interface Navigateur Web • 74, 75
Astuces sur les commandes • 221
Authentification à deux facteurs • 139, 289
Authentification à deux facteurs - Configuration requise • 289
Authentification à deux facteurs - Environnements pris en charge • 289
Authentification à deux facteurs - Problèmes répertoriés • 290
Authentification à deux facteurs à l'aide de RADIUS • 139
Authentification à distance • 88, 119, 193, 196
Autoriser les connexions simultanées par utilisateur • 197
Avant d'utiliser le paramétrage guidé • 15

B

Barrettes d'alimentation gérées • 29, 35, 37, 56

C

Canaux de communication CC-SG • 266
Caractères joker de recherche • 33
CC-SG - Notions fondamentales • 15
CC-SG et CC-NOC • 271
CC-SG et client pour IPMI, iLO/RILOE, DRAC, RSA • 270
CC-SG et dispositifs Raritan • 267
CC-SG et SNMP • 270
Certificats • 200
Changer votre mot de passe • 98
Chiffrement AES • 193
Client Admin CC-SG • 8
Clients PC vers CC-SG • 268
Clients PC vers nœuds • 269
Cluster CC-SG • 267
Cluster CC-SG
définition • 189
CommandCenter NOC • 214
Commandes SSH • 219
Comment créer des associations • 26
Comptes utilisateur • 120
Conditions préalables • 1
Configuration de CC-SG et du réseau • 264
Configuration de CC-SG par paramétrage guidé • 10, 14, 26, 102
Configuration de la date et de l'heure du serveur CC-SG • 180

Configuration de l'activité d'enregistrement • 179, 209
Configuration de SNMP • 187
Configuration des applications d'accès aux nœuds • 167
Configuration des applications par défaut • 169
Configuration des barrettes d'alimentation connectées à des dispositifs KX, KX2 et P2SC • 56, 57
Configuration des barrettes d'alimentation connectées à des dispositifs SX 3.0 et KSX • 57, 58
Configuration des barrettes d'alimentation connectées à un dispositif SX 3.1 • 57, 61
Configuration des clusters CC-SG • 189
Configuration des comptes • 253
Configuration des ports • 39, 61
Configuration des prises d'une barrette d'alimentation • 57, 59, 60, 62, 63
Configuration du modem • 181
Configuration du réseau CC-SG • 123, 171
Configuration d'un message du jour • 166
Configuration et imposition des mots de passe forts • 15
Configuration requise pour le navigateur client • 288
Configurations DHCP recommandées pour CC-SG • 171, 175, 178
Configurer CC-SG • 181
Configurer la connexion à distance • 182
Configurer la connexion de rappel • 182, 184
Configurer le minuteur d'inactivité • 198
Configurer le modem du PC client • 181
Configurer le protocole de connexion du navigateur
HTTP ou HTTPS/SSL • 194
Configurer un port KVM • 39
Configurer un port série • 39
Configurer un serveur SMTP externe • 206
Confirmation de l'adresse IP • 10
Connexion à un nœud • 80
Console de diagnostic • 164, 226
Consultation des fichiers journaux dans la console de diagnostic (Admin) • 239
Contrôle de l'alimentation d'un groupe de nœuds et surveillance de l'opération de gestion de l'alimentation • 18
Contrôle des accès à l'aide de stratégies • 102
Conventions d'appellation • 14, 26, 27, 35, 39, 40, 51, 67, 68, 69, 71, 74, 83, 91, 94, 95, 103, 300
Conversation • 80
Copie de la configuration du dispositif • 46, 208
Copie en bloc de catégories et d'éléments de dispositifs • 41
Copie en bloc de catégories et d'éléments de nœuds • 79
Copie en bloc d'utilisateurs • 100
Créer des catégories et des éléments • 15
Créer des groupes • 14, 18
Créer un cluster • 190
Créer une connexion SSH à un dispositif SX • 222

D

Déconnexion des utilisateurs • 49, 100
Décrire les nœuds • 84
Définir l'application par défaut d'une interface ou d'un type de port • 169
Définir un nom distinct de base • 121
Définir un nom distinct pour AD • 121
Définir un nom distinct pour LDAP • 121
Définir un nom d'utilisateur pour AD • 121
Définition de l'heure du serveur CC-SG • 10
Définition de l'ordre des serveurs AA externes • 122
Définition des modules pour l'authentification et l'autorisation • 121
Démarrage d'admin • 48
Déplacer la barrette d'alimentation d'un dispositif SX 3.1 vers un port différent • 62
Déplacer une barrette de KX, KX2 ou P2SC vers un port différent • 58
Détecter et ajouter des dispositifs • 16
Détection des dispositifs • 34
Dispositifs, groupes de dispositifs et ports • 29

E

E1 - Impératifs d'environnement • 263
E1 - Spécifications générales • 262
E1 - Spécifications matérielles • 262
Ecran Profil du dispositif • 31
Enregistrement et suppression des fichiers de sauvegarde • 158
Enregistrer un fichier de sauvegarde • 158
Enregistrer un rapport dans un fichier • 141
Entrer en mode de maintenance • 17, 131, 132, 156, 162
Envoi d'une commande ping à un nœud • 80
Envoi d'une commande ping à une adresse IP (Interfaces réseau) • 235
Envoi d'une commande ping au dispositif • 47
Envoyer des notifications de tâches par e-mail • 208
Exemple
  Ajouter une interface Navigateur Web à un nœud PX • 74, 76
Exemple de caractères joker • 33
Exigences pour les clusters CC-SG • 189

F

FAQ • 291
Fermeture d'une session CC-SG • 165
Fichiers MIB • 187
Filtrer par groupe de dispositifs • 112
Filtrer par groupe de noeuds • 111
Flux d'authentification • 119

G

G1 - Impératifs d'environnement • 260
G1 - Spécifications générales • 259
G1 - Spécifications matérielles • 259
Gestion de l'alimentation d'un groupe de noeuds • 18, 209
Gestion des utilisateurs • 14, 21
Gestion du firmware d'un dispositif • 170
Gestionnaire d'alimentation des dispositifs • 48
Gestionnaire de sécurité • 193, 218
Gestionnaire des associations • 26
Gestionnaire des groupes de dispositifs • 51
Gestionnaire des notifications • 206, 208
Gestionnaire des tâches • 9, 10, 152, 155, 180, 206, 207
Groupe CC Super-User • 90
Groupe CC Users • 91
Groupe System Administrators • 90
Groupes d'utilisateurs par défaut • 90
Guide de dépannage • 288

I

Icônes associées aux nœuds et aux interfaces • 67
Icônes de dispositif et de port • 31
Importation des groupes d'utilisateurs AD • 129
Imprimer l'affichage d'un rapport • 141
Installer le client lourd • 6
Interface API de services Web • 225
Interface Navigateur Web • 71, 74
Interfaces de connexions en bande • 69, 71
Interfaces pour connexions de gestion d'alimentation IPMI • 70, 73
Interfaces pour connexions de gestion de l'alimentation par processeur DRAC, RSA et ILO • 70, 72
Interfaces pour connexions KVM hors bande, série hors bande • 70, 71
Interfaces pour connexions par barrette d'alimentation gérée • 57, 60, 62, 63, 70, 72
Introduction • 1

L

Lancer un CC-NOC • 217
Liste de contrôle d'accès • 204

M

Maintenance du système • 155
Messages d'état de l'alimentation • 19
Mise à niveau de CC-SG • 162
Mise à niveau de CC-SG vers une nouvelle version de firmware • 16
Mise à niveau de plusieurs dispositifs dans un laps de temps limité • 20
Mise à niveau d'un dispositif • 37, 42, 170
Mise en route • 10

Raritan.
When you're ready to take control®

Mise hors tension de CC-SG • 164
Mise hors tension du système CC-SG à partir de la console de diagnostic • 246
Mode actif/actif
définition • 171, 176
Mode de maintenance • 105, 155
Mode principal/de sauvegarde
définition • 171, 173
Modèle E1 • 262
Modèle G1 • 259
Modèle V1 • 260
Modes de connexion
Direct et Proxy • 103, 185, 272
Modification de la configuration de la console de diagnostic • 232
Modification de la configuration des interfaces réseau (Interfaces réseau) • 233
Modification des routes statiques (Interfaces réseau) • 177, 236, 238
Modification d'un dispositif • 37
Modification d'un dispositif PowerStrip • 38
Modification d'un groupe de nœuds • 86
Modification d'un groupe d'utilisateurs • 93
Modification d'un module AD • 128
Modification d'un nœud • 78
Modification d'un port • 40
Modification d'un utilisateur • 95
Modification d'une interface • 76
Modification d'une stratégie • 105
Modifier la taille de police par défaut dans CC-SG • 99
Modifier le nom d'utilisateur du super utilisateur CC-SG • 99
Modifier l'heure de synchronisation AD quotidienne • 133
Modifier un CC-NOC • 216
Modifier un élément • 28
Modifier un groupe de dispositifs • 54
Modifier une association de dispositif ou de port d'une barrette d'alimentation (SX 3.0, KSX) • 60
Modifier une catégorie • 27
Modifier une vue personnalisée pour des dispositifs • 116
Modifier une vue personnalisée pour des noeuds • 113
Modifier votre adresse électronique • 99
Modifier votre préférence de recherche par défaut • 33, 99
Mots de passe forts obligatoires pour tous les utilisateurs • 195

N

Navigation dans la console d'administrateur • 231
Nœuds créés par configuration de ports • 69
Nœuds, groupes de nœuds et interfaces • 29, 65
Noms des nœuds • 67
Noms distincts pour LDAP et AD • 120

O

Onglet Dispositifs • 30
Onglet Nœuds • 66
Onglet Utilisateurs • 89
Options clic bouton droit de l'onglet Dispositifs • 32
Options de tri des ports • 32

P

Paragon II System Controller (P2-SC) • 50
Paramétrage du dispositif • 14, 16
Paramétrer le numéro de port pour l'accès SSH à CC-SG • 194
Paramètres avancés AD • 124, 128
Paramètres avancés LDAP • 135
Paramètres d'approbation AD • 127, 128
Paramètres de cluster avancés • 192
Paramètres de configuration OpenLDAP (eDirectory) • 137
Paramètres de configuration Sun One LDAP (iPlanet) • 136
Paramètres de connexion • 16, 195
Paramètres de groupe AD • 126, 128, 129
Paramètres de verrouillage • 146, 196
Paramètres des mots de passe de la console de diagnostic • 230, 247, 251
Paramètres du dispositif • 186
Paramètres généraux AD • 123, 128

Paramètres généraux LDAP • 134
Paramètres généraux RADIUS • 139
Paramètres généraux TACACS+ • 138
Parcourir des rapports de plusieurs pages • 141
Port d'administration série • 224
Portail • 198
Ports internes CC-SG • 271
Ports ouverts requis pour les réseaux CC-SG Synthèse • 264
Pour configurer le mode Direct pour toutes les connexions clientes • 185
Pour configurer le mode Proxy pour toutes les connexions clientes • 185
Pour configurer SNMP dans CC-SG • 187
Pour configurer une combinaison des modes Direct et Proxy • 186
Prise en charge de support virtuel • 107
Privilèges de groupe d'utilisateurs • 91, 147, 273
Processus de configuration de la gestion de l'alimentation dans CC-SG • 56
Profil du nœud • 66
Programmer des tâches séquentielles • 207
Programmer la mise à niveau du firmware d'un dispositif • 208, 209, 211, 213
Programmer une tâche • 208, 213
Purger le journal interne de CC-SG • 179
Purger les données d'un rapport de CC-SG • 142, 143, 144, 179

Q

Quitter CC-SG • 165
Quitter le mode de maintenance • 17, 132, 156, 163
Quitter une session SSH • 224

R

Raccourcis clavier • 299
Rapport d'accès • 144
Rapport de disponibilité • 145
Rapport Données de groupes • 147
Rapport Données d'utilisateurs • 146
Rapport Gestion du parc • 148
Rapport Interrogation des ports • 150
Rapport Journal d'audit • 142
Rapport Journal d'erreurs • 143
Rapport Mise à niveau du firmware d'un dispositif • 22, 153, 213
Rapport Ports actifs • 152
Rapport sur la création de nœuds • 150
Rapport sur le groupe d'utilisateurs AD • 148
Rapport sur le parc du nœud • 149
Rapport sur les nœuds actifs • 149
Rapport Synchronisation CC-NOC • 153, 215
Rapport Utilisateurs actifs • 145
Rapport Utilisateurs dans les groupes • 147
Rapport Utilisateurs verrouillés • 146
Rapports • 140, 209
Rapports programmés • 152, 153, 208
Réamorçage de CC-SG avec la console de diagnostic • 245
Recherche de dispositifs • 33
Récupérer un nœud CC-SG défaillant • 192
Redémarrage de CC-SG • 161, 175, 244
Redémarrage de CC-SG après un arrêt • 164
Redémarrage de CC-SG avec la console de diagnostic • 244
Redémarrage du dispositif • 46, 209
Redimensionner la largeur des colonnes d'un rapport • 140
Réinitialisation de CC-SG • 161
Réinitialisation de la configuration usine de CC-SG (Admin) • 248
Réinitialisation du mot de passe du super utilisateur CC avec la console de diagnostic • 247
Rendre le chiffrement AES obligatoire entre le client et CC-SG • 193
Reprise de la gestion • 47
Restauration de CC-SG • 159
Restauration de la configuration du dispositif • 43, 209
Restaurer la configuration d'un dispositif (KX, KSX, KX101, SX, IP-Reach) • 44
Restaurer toutes les données de configuration hormis les paramètres réseau sur un dispositif KX2 • 44
Restaurer toutes les données de configuration sur un dispositif KX2 • 45

Restaurer uniquement les paramètres de dispositif ou les données de l'utilisateur ou du groupe de l'utilisateur sur un dispositif KX2 • 45
Résultats de l'ajout d'une interface • 76

S

Sauvegarde de CC-SG • 156, 208
Sauvegarde de la configuration du dispositif • 42, 208
Se connecter à CC-SG par modem • 183
Se déconnecter de CC-SG • 165
Sélectionner les nœuds • 83
Spécifications pour G1, V1 et E1 • 259
Stratégies de contrôle d'accès • 20, 51, 88, 92, 102
Support virtuel
définition • 108
Suppression d'un dispositif • 38
Suppression d'un groupe de nœuds • 87
Suppression d'un groupe d'utilisateurs • 94
Suppression d'un nœud • 79
Suppression d'un port • 41
Suppression d'un utilisateur • 96
Suppression d'un utilisateur d'un groupe • 96, 98
Suppression d'une interface • 77
Suppression d'une stratégie • 106
Supprimer un CC-NOC • 217
Supprimer un élément • 28
Supprimer un fichier de sauvegarde • 158
Supprimer un firmware • 170
Supprimer un groupe de dispositifs • 55
Supprimer un nœud CC-SG primaire • 191
Supprimer un nœud CC-SG secondaire • 191
Supprimer une application • 169
Supprimer une barrette d'alimentation connectée à un dispositif KX, KX2 ou P2SC • 58
Supprimer une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX • 60
Supprimer une barrette d'alimentation connectée à un dispositif SX 3.1 • 62
Supprimer une catégorie • 27
Supprimer une vue personnalisée pour des dispositifs • 117
Supprimer une vue personnalisée pour des noeuds • 114
Suspension de la gestion • 47
Synchronisation d'AD avec CC-SG • 130
Synchroniser tous les groupes d'utilisateurs avec AD • 128, 129, 131
Synchroniser tous les modules AD • 128, 129, 130, 131, 132

T

Tâches programmées et mode de maintenance • 155
Tâches relatives aux certificats • 200
Télécharger un firmware • 170
Terminologie et sigles • 2, 36, 134, 138, 139, 174, 177, 206, 214, 221, 234
Terminologie relative aux associations • 24
Traps SNMP • 187, 285
Trier les données d'un rapport • 140
Types de tâches • 207
Types de vues personnalisées • 111

U

Utilisateurs et groupes d'utilisateurs • 82, 88, 110, 120, 137, 138
Utilisation de la détermination d'itinéraire (Interfaces réseau) • 237
Utilisation de vues personnalisées dans le client Admin • 112
Utilisation des rapports • 140
Utiliser le client lourd • 7
Utiliser SSH pour se connecter à un nœud via une interface série hors bande • 223

V

V1 - Impératifs d'environnement • 261
V1 - Spécifications générales • 260
V1 - Spécifications matérielles • 261
Vérification de la matrice de compatibilité • 12
Vérification et mise à niveau des versions des applications • 12, 167
Vérifier si votre navigateur accepte le chiffrement AES • 193

Votre profil utilisateur • 98
Vue d'ensemble des nœuds et des interfaces • 67
Vue par catégorie • 111
Vue topologique • 49
Vues personnalisées pour dispositifs et nœuds • 22, 66, 111
Vues personnalisées pour les dispositifs • 115
Vues personnalisées pour les nœuds • 112

➢ *Etats-Unis/Canada/Amérique latine*

Lundi au vendredi
8 h à 20 h (heure de la côte Est)
Téléphone : 800-724-8090 ou 732-764-8886
Pour CommandCenter NOC : appuyez sur la touche 6, puis sur 1
Pour CommandCenter Secure Gateway : appuyez sur la touche 6, puis sur 2
Fax : 732-764-8887
E-mail pour CommandCenter NOC : tech-ccnoc@raritan.com
E-mail pour tous les autres produits : tech@raritan.com

➢ *Pékin*

Lundi au vendredi
9 h à 18 h (heure locale)
Téléphone : +86-10-88091890

➢ *Japon*

Lundi au vendredi
9 h 30 à 17 h 30 (heure locale)
Téléphone : +81-3-3523-5994
E-mail : support.japan@raritan.com

➢ *Europe*

Lundi au vendredi
8 h 30 à 17 h. GMT+1 (heure de l'Europe centrale)
Téléphone : +31-10-2844040
E-mail : tech.europe@raritan.com

➢ *Corée*

Lundi au vendredi
9 h à 18 h (heure locale)
Téléphone : +82-2-5578730

➢ *France*

Lundi au vendredi
8 h 30 à 17 h. GMT+1 (heure de l'Europe centrale)
Téléphone : +33-1-47-56-20-39

➢ *Melbourne, Australie*

Lundi au vendredi
9 h à 18 h (heure locale)
Téléphone : +61-3-9866-6887

➢ *Allemagne*

Lundi au vendredi
8 h 30 à 17 h. GMT+1 (heure de l'Europe centrale)
Téléphone : +49-20-17-47-98-0

➢ *Shanghai*

Lundi au vendredi
9 h à 18 h (heure locale)
Téléphone : +86-21-5425-2499

➢ *GuangZhou*

Lundi au vendredi
9 h à 18 h (heure locale)
Téléphone : +86-20-8755-5561

➢ *Taïwan*

Lundi au vendredi
9 h à 18 h. GMT -5 Standard -4 Heure d'été
Téléphone : +886-2-8919-1333
E-mail : tech.rap@raritan.com

➢ *Inde*

Lundi au vendredi
9 h à 18 h (heure locale)
Téléphone : +91-124-410-7881

➢ *Royaume-Uni*

Lundi au vendredi
8 h 30 à 17 h. GMT+1 (heure de l'Europe centrale)
Téléphone : +44-20-7614-77-00