CommandCenter Secure Gateway

Manuel de l'administrateur

Version 4.1

CCA-0I-v4.1-F

Décembre 2008

255-80-5140-00

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)

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 dommages 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

Chapitre 12 Authentification à distance 150

Chapitre 13 Rapports 171

Nouveautés du manuel de l'administrateur de CC-SG

Les sections suivantes ont changé ou des informations ont été ajoutées au manuel de l'administrateur CommandCenter Secure Gateway selon les améliorations ou modifications apportées à l'équipement et/ou à la documentation.

- ***Commuter l'état des nœuds primaire et secondaire*** (à la page 222)
- ***Récupérer un cluster*** (à la page 222)
- ***Supprimer un cluster*** (à la page 223)
- ***Configuration d'un voisinage*** (à la page 223)
- ***Chiffrement AES*** (à la page 228)
- ***Vérifier si votre navigateur accepte le chiffrement AES*** (à la page 229)
- ***Port d'administration série*** (à la page 261)
- ***Accéder à la console de diagnostic via SSH*** (à la page 264)
- ***A propos de la console d'état*** (à la page 265)
- ***Informations de la console d'état*** (à la page 266)
- ***Ecran de la console d'administrateur*** (à la page 273)
- ***Modifier les routes statiques*** (à la page 280)
- ***Effectuer des tests sur les disques ou sur le RAID*** (à la page 300)
- ***Programmer des tests sur les disques*** (à la page 302)
- ***Réparer ou reconstruire les disques RAID*** (à la page 304)
- ***Prendre un instantané du système*** (à la page 308)
- ***Modifier la résolution vidéo de la console de diagnostic*** (à la page 309)
- ***Ports ouverts requis pour les réseaux CC-SG : Synthèse*** (à la page 313)
- ***CC-SG et dispositifs Raritan*** (à la page 314)
- ***Clients PC vers CC-SG*** (à la page 316)
- ***Clients PC vers nœuds*** (à la page 317)
- ***Privilèges de groupe d'utilisateurs*** (à la page 321)
- ***Traps SNMP*** (à la page 330)
- ***Utilitaires de diagnostic*** (à la page 334)
- ***FAQ - Généralités*** (à la page 342)
- ***FAQ sur l'authentification*** (à la page 345)
- ***Conventions d'appellation*** (à la page 353)
- ***Messages d'amorçage de la console de diagnostic*** (à la page 356)

Reportez-vous aux notes de versions pour obtenir une explication plus détaillée des modifications appliquées à cette version de CommandCenter Secure Gateway.

CC-SG - Notions fondamentales

Cette section 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 application de 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 231) pour plus d'informations 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. Pour mettre à niveau CC-SG de la version 3.x à la version 4.1, vous devez effectuer tout d'abord la mise à niveau vers 4.0.

La version 4.0 ou supérieure de CC-SG n'est pas compatible avec le matériel G1. N'effectuez pas de mise à niveau d'une unité CC-SG G1 vers la version 4.0 ou supérieure.

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

Seuls les utilisateurs dotés du privilège CC Setup and Control (paramétrage et contrôle de CC) peuvent mettre à niveau CC-SG.

Vous devez sauvegarder CC-SG avant d'effectuer la mise à niveau et envoyer les fichiers de sauvegarde aux PC pour les conserver. Reportez-vous à ***Sauvegarde de CC-SG*** (à la page 186) et ***Enregistrer un fichier de sauvegarde*** (à la page 188).

Si vous utilisez un cluster CC-SG, vous devez le supprimer avant d'effectuer la mise à niveau. Mettez chaque nœud CC-SG à niveau individuellement, puis recréez le cluster.

Important : si vous devez mettre à niveau CC-SG et un dispositif ou un groupe de dispositifs, traitez CC-SG d'abord, puis le dispositif.

CC-SG sera réamorcé pendant la mise à niveau. N'INTERROMPEZ PAS la procédure, ne réamorcez 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. Connectez-vous au client Admin de CC-SG en utilisant un compte disposant du privilège CC Setup and Control.
3. Entrez en mode de maintenance. Reportez-vous à ***Passage en mode de maintenance*** (à la page 185).
4. Lorsque CC-SG est en mode de maintenance, choisissez Maintenance du système > Mettre à niveau.
5. Cliquez sur Parcourir. Recherchez et sélectionnez le fichier de firmware de CC-SG (.zip), cliquez ensuite sur Ouvrir.
6. 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 la mise à niveau. Tous les utilisateurs sont alors déconnectés de CC-SG.
7. Vous devez attendre la fin de la mise à niveau pour vous connecter de nouveau à CC-SG. Vous pouvez surveiller la mise à niveau dans la console de diagnostic.
   a. Accédez à cette dernière à l'aide du compte admin. Reportez-vous à ***Accéder à la console d'administrateur*** (à la page 272).
   b. Choisissez Admin > System Logfile Viewer. Sélectionnez sg/upgrade.log, puis choisissez Afficher pour consulter le journal de mise à niveau.
   c. Attentez la fin de la mise à niveau. Celle-ci est terminée lorsque le message indiquant la fin de la mise à niveau apparaît dans le journal de mise à niveau. Vous pouvez également attendre que le résultat du trap SNMP ccImageUpgradeResults affiche un message de réussite.
   d. Le serveur doit être réamorcé. Le processus de réamorçage commence lorsque le message indiquant le réamorçage de Linux apparaît dans le journal de mise à niveau. Le serveur est fermé, puis réamorcé.

   Remarque : pour les mises à niveau de CC-SG 3.x vers 4.0.x, le système sera réamorcé deux fois, ce qui est normal et attendu.

   e. Environ deux minutes après le réamorçage, vous pouvez accéder à nouveau à la console de diagnostic à l'aide du compte admin, et surveiller la progression de la mise à niveau. **Facultatif.**
8. Cliquez sur OK pour quitter CC-SG.

9. Effacez la mémoire cache du navigateur, puis fermez la fenêtre de ce dernier. Reportez-vous à ***Effacer la mémoire cache du navigateur*** (à la page 196).
10. Effacez la mémoire cache Java. Reportez-vous à ***Effacer la mémoire cache Java*** (à la page 196).
11. Lancez une nouvelle fenêtre du navigateur Web.
12. Connectez-vous au client Admin de CC-SG en utilisant un compte disposant du privilège CC Setup and Control.
13. 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.
14. Quittez le mode de maintenance. Reportez-vous à ***Sortie du mode de maintenance*** (à la page 186).

Effectuez une copie de sauvegarde de CC-SG. Reportez-vous à ***Sauvegarde de CC-SG*** (à la page 186).

Gestion de l'alimentation d'un groupe de nœuds et surveillance de la gestion de l'alimentation

Gestion de l'alimentation d'un groupe de nœuds

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

Cette fonction vous permet, par exemple, de mettre hors tension tous les nœuds 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 nœuds.

Reportez-vous à Astuces relatives à la gestion de l'alimentation des nœuds à plusieurs interfaces (dans le **manuel d'utilisation CommandCenter Secure Gateway**) pour plus d'informations sur le paramétrage des opérations de gestion de l'alimentation des nœuds comportant plusieurs interfaces de gestion d'alimentation.

1. Cliquez sur l'onglet Nœuds.
2. Choisissez Nœuds > Regrouper la gestion de l'alimentation. L'écran Regrouper la gestion de l'alimentation apparaît.
3. Cliquez sur la flèche déroulante Groupe de nœuds, puis sélectionnez, dans la liste, le groupe dont vous souhaitez gérer l'alimentation.

4. Dans la liste Disponible, sélectionnez l'interface sur laquelle vous souhaitez exécuter la gestion de l'alimentation et cliquez sur Ajouter pour placer 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. Organisez les interfaces dans la liste Sélectionné dans l'ordre où vous souhaitez voir CC-SG effectuer l'opération d'alimentation. Sélectionnez une interface dans la liste Sélectionné, puis cliquez sur les flèches haut et bas pour placer l'interface à l'endroit souhaité.
6. Cliquez sur la flèche déroulante Opération et sélectionnez Actif, Inactif, Cycle, Arrêt approprié ou Suspendre dans la liste.
7. Si vous avez sélectionné Sous tension, Hors tension, Arrêt approprié ou Suspendre 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 d'alimentation via les interfaces sélectionnées. Un message de confirmation apparaît.
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 ***Messages d'état de l'alimentation*** (à la page xxi) 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 s'ouvre 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 :

- 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. Cliquez sur 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 niveau 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. Indiquez si une nouvelle tentative doit être effectuée pour les mises à niveau ayant échoué.

   a. Cliquez sur l'onglet Nouvelle tentative.

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

   c. 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. 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 l'onglet Notification.

   b. Cliquez sur Ajouter, entrez l'adresse électronique dans la fenêtre qui s'ouvre, puis cliquez sur OK.

c. Sélectionnez En cas d'échec si vous souhaitez envoyer un message si une mise à niveau échoue.

d. 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 184).

Affectation d'une vue personnalisée de nœuds 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.

Pour affecter une vue personnalisée de nœuds par défaut à tous les utilisateurs :

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

Tous les utilisateurs qui se connectent à CC-SG voient l'onglet Nœuds trié selon la vue personnalisée sélectionnée. Les utilisateurs peuvent modifier la vue personnalisée.

Reportez-vous à ***Vues personnalisées*** (voir "Vues personnalisées pour dispositifs et nœuds" à la page 142) 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

Avant de configurer CC-SG conformément aux procédures de ce document, reportez-vous au **guide de déploiement CommandCenter Secure Gateway** pour obtenir des instructions plus 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 pouvant être employé par les utilisateurs standard et les administrateurs. Il s'agit du seul client autorisant l'administration.

Associations : relations entre les catégories, les éléments de catégorie, et les ports et/ou dispositifs. Par exemple, si vous souhaitez associer la catégorie Emplacement à un dispositif, créez 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) : 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 réamorcés 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 : 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 : valeurs d'une catégorie. Par exemple, l'élément New York City appartient à la catégorie Emplacement et l'élément Windows, 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 Paragon II de Raritan**.

Nom d'hôte : peut être indiqué si la prise en charge des serveurs DNS est activée. Reportez-vous à ***A propos de la configuration réseau*** (à la page 204).

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 : 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 : passage 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 (Intelligent Platform Management Interface) : serveurs 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 : elles définissent l'accès à un groupe d'utilisateurs au sein d'un réseau CC-SG. 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 : systèmes cible, tels que les serveurs, les PC de bureau et tout autre équipement réseau, auxquels les utilisateurs de CC-SG peuvent accéder.

Interfaces : différents moyens d'accéder à un nœud, via une solution hors bande, telle qu'une connexion Dominion KX2, 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 existent uniquement sur les dispositifs Raritan et identifient un chemin d'accès du dispositif vers 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 est accessible via SSH pour administrer des dispositifs et CC-SG lui-même.

Groupe d'utilisateurs : ensembles d'utilisateurs partageant le même niveau d'accès et les mêmes droits.

Configuration requise pour le navigateur client

Pour obtenir la liste complète des navigateurs pris en charge, consultez la matrice de compatibilité sur le site Web du support Raritan.

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 en obtenir la liste complète, consultez 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.
- 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 ***Console de diagnostic*** (à la page 264).

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

Dans ce chapitre

Accès par navigateur via le client Admin CC-SG

Le client Admin CC-SG est un client Java qui offre une interface utilisateur graphique pour les tâches administratives et d'accès, en fonction de vos autorisations.

1. Dans un navigateur Internet pris en charge, entrez l'adresse URL de l'unité CC-SG, puis tapez /admin : https://*Adresse IP*/admin, par exemple, ***https://10.0.3.30/admin*** (https://10.0.3.30/admin).

   Si la fenêtre d'avertissement d'incompatibilité JRE s'affiche, sélectionnez la version JRE correspondant à votre ordinateur client et installez-la. Lorsque JRE est installé, essayez à nouveau cette procédure. Reportez-vous à **Incompatibilité JRE** *(à la page 6).*

   Ou vous pouvez poursuivre sans installer de nouvelle version de JRE.

2. Si l'accord de service limité apparaît, lisez-en le texte, puis cochez la case Je comprends et j'accepte l'accord de service limité.

3. Entrez vos nom d'utilisateur et mot de passe, puis cliquez sur Connexion.
4. Si la connexion aboutit, la fenêtre du client Admin CC-SG s'affiche.

Incompatibilité JRE

Si la version minimum requise de JRE n'est pas installée sur votre ordinateur client, un message d'avertissement s'affiche avant que vous n'accédiez au client Admin CC-SG. La fenêtre d'avertissement d'incompatibilité JRE s'ouvre lorsque CC-SG ne retrouve pas le fichier JRE requis sur votre ordinateur client.

Dans ce cas, sélectionnez la version JRE correspondant à votre ordinateur client et installez-la, ou vous pouvez poursuivre sans installer de nouvelle version de JRE.

Vous devez relancer CC-SG lorsque JRE est installé.

Les administrateurs peuvent configurer la version minimum de JRE recommandée et le message qui s'affiche dans la fenêtre d'avertissement d'incompatibilité JRE. Reportez-vous à ***Configuration de paramètres JRE personnalisés*** (à la page 216).

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. La version minimum de Java requise pour exécuter le client lourd est 1.5.0.10.

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.
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 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, désactivez la case Secure Socket Layer (SSL) dans la fenêtre de spécification de l'adresse IP du client lourd.
6. Cliquez sur Démarrer.
   - 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. Entrez vos nom d'utilisateur et mot de passe dans les champs correspondants, puis cliquez sur Connexion pour continuer.

Utiliser le client lourd

La version minimum de Java requise pour exécuter le client lourd est 1.5.0.10. La version 1.6.0 de Java est également prise en charge.

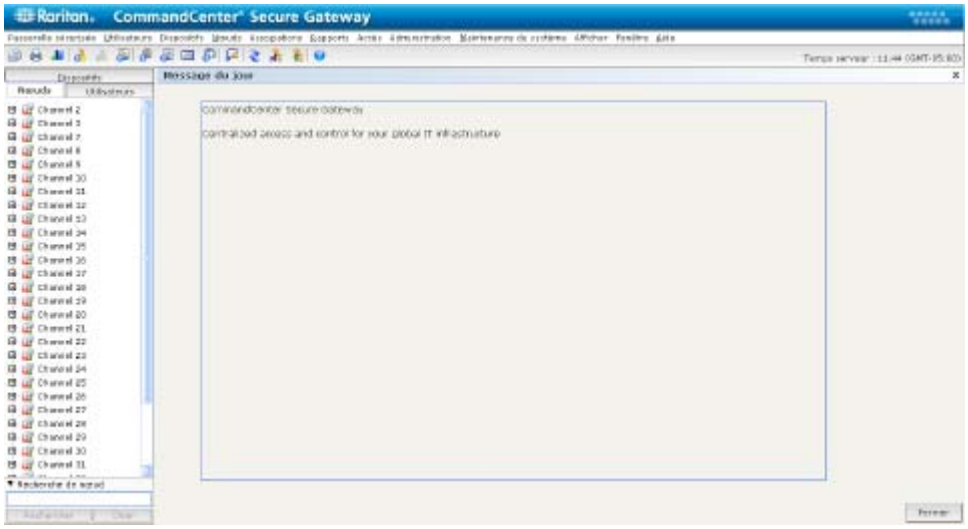
Une fois le client lourd installé, il est accessible de deux façons sur votre ordinateur client.

Pour accéder au client lourd :

- 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.

- Onglet Nœuds : cliquez sur l'onglet Nœuds pour afficher tous les nœuds cible connus sous forme d'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 forme d'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 forme d'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), par état (Disponible, Occupé, Non disponible) ou par numéro de port (ordre numérique). Cliquez avec le bouton droit de la souris dans l'arborescence, sélectionnez Options de tri du port, 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 de la souris 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 242). 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 terminées, passez au paramétrage guidé. Reportez-vous à ***Configuration de CC-SG par paramétrage guidé*** (à la page 14).

Dans ce chapitre

Confirmation de l'adresse IP

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet Configuration réseau.
3. 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 204). **Facultatif.**
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 du temps 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 242). 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 dans lequel vous utilisez CC-SG.

   a. 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, puis entrez les adresses IP des serveurs NTP principal et secondaire 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 :

- Choisissez Administration > Compatibility Matrix (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 des applications prises en charge, reportez-vous à la matrice de compatibilité sur le site Web du support Raritan.

Il est recommandé d'entrer en mode de maintenance avant de mettre à niveau les applications. Reportez-vous à ***Passage en mode de maintenance*** (à la page 185).

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. Reportez-vous à ***Ajouter une application*** (à la page 201).

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.

Remarque : les utilisateurs connectés pendant la mise à niveau doivent fermer leur session CC-SG, puis l'ouvrir à nouveau pour s'assurer que la nouvelle version de l'application est lancée.

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 : permet de définir les catégories et éléments utilisés pour organiser votre équipement. Reportez-vous à ***Associations dans le paramétrage guidé*** (à la page 15).
- Paramétrage du dispositif : permet de détecter les dispositifs de votre réseau et de les ajouter à CC-SG. Autorise la configuration des ports de dispositif. Reportez-vous à ***Paramétrage du dispositif*** (à la page 16).
- Créer des groupes : 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. Reportez-vous à ***Création de groupes*** (à la page 18).
- Gestion des utilisateurs : 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 ***Gestion des utilisateurs*** (à la page 20).

Reportez-vous à ***Conventions d'appellation*** (à la page 353) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.

Dans ce chapitre

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

Pour créer des catégories et des éléments par paramétrage guidé :

1. Dans la fenêtre Paramétrage guidé, cliquez sur Associations, puis sur Créer des catégories dans le panneau de gauche pour ouvrir le volet 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 une rangée à la table.
   - Pour supprimer un élément, sélectionnez sa rangée, 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. Pour 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. **Facultatif**
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 Continuer pour démarrer la tâche suivante, Paramétrage du dispositif. Suivez les étapes de la section suivante.

Paramétrage du dispositif

Le 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 Continuer à la fin de la tâche Associations. Vous pouvez également cliquer sur Paramétrage du dispositif, puis sur Détecter les dispositifs, dans l'arborescence Tâches guidées du panneau de gauche, pour ouvrir le volet du même nom.

Pour détecter et ajouter des dispositifs par paramétrage guidé :

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. Si CC-SG a détecté des dispositifs du type spécifié dans la plage d'adresses indiquée, ils s'affichent dans une table de la section inférieure du panneau Détecter les dispositifs. Cliquez 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.
7. Dans la table des dispositifs détectés, sélectionnez le dispositif à inclure à CC-SG, puis cliquez sur Ajouter. Le panneau Ajouter un dispositif s'ouvre. Le panneau Ajouter un dispositif varie légèrement selon le type de dispositif ajouté.
8. Vous pouvez modifier le nom du dispositif et la description en entrant de nouvelles données dans les champs correspondants.

9. 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.
10. Le champ Numéro de port TCP est renseigné automatiquement en fonction du type de dispositif.
11. 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.
12. 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.
13. Si vous ajoutez un dispositif Dominion SX, cochez la case Autoriser l'accès direct au dispositif pour autoriser l'accès local au dispositif. Désactivez la case Accès local : Autorisé pour interdire l'accès local au dispositif.
14. 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.
15. 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.
16. 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.
17. 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 dans la liste l'élément à associer au dispositif.
18. Pour appliquer l'élément au dispositif et aux nœuds connectés à celui-ci, cochez la case Appliquer aux nœuds.
19. Si vous souhaitez ajouter un autre dispositif, cliquez sur Appliquer pour enregistrer le dispositif en cours et répétez la procédure. **Facultatif.**
20. Une fois l'ajout des dispositifs terminé, cliquez sur OK. Le panneau Résumé du dispositif affiche la liste des dispositifs que vous avez ajoutés.
21. Cliquez sur Continuer pour démarrer la tâche suivante, Créer des groupes. Suivez les étapes de la section suivante.

Création de 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

Pour ajouter des groupes de dispositifs et des groupes de nœuds par paramétrage guidé :

1. Le panneau Groupe de dispositifs : Nouveau s'ouvre lorsque vous cliquez sur Continuer à la fin de la tâche Paramétrage du dispositif. Vous pouvez également cliquer sur Créer des groupes, puis sur Ajouter des groupes de dispositifs, dans l'arborescence Tâches guidées du panneau de gauche, pour ouvrir le panneau Groupe 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 Groupe de dispositifs : Nouveau.

   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.

   c. Pour supprimer un dispositif du groupe, choisissez son nom dans la liste Sélectionné, puis cliquez sur Retirer.

   d. 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.

4. 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.
5. Pour ajouter un autre groupe de dispositifs, cliquez sur Appliquer pour enregistrer le groupe actif, puis répétez cette procédure. **Facultatif.**
6. Une fois l'ajout des groupes de dispositifs terminé, cliquez sur OK. Le panneau Groupe de nœuds : Nouveau s'ouvre. Vous pouvez également cliquer sur Créer des groupes, puis sur Ajouter des groupes de nœuds, dans l'arborescence Tâches guidées du panneau de gauche, pour ouvrir le panneau Groupe de nœuds : Nouveau.
7. Dans le champ Nom du groupe, entrez le nom du groupe de nœuds à créer.
8. 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 Groupe de nœuds : Nouveau.

   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 Groupe de nœuds : Nouveau. 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. Reportez-vous à ***Stratégies de contrôle d'accès*** (à la page 137).

9. Activez 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 du groupe avec permission de contrôle.
10. Pour ajouter un autre groupe de nœuds, cliquez sur Appliquer pour enregistrer le groupe actif, puis répétez cette procédure. **Facultatif.**
11. 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.
12. Cliquez sur 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 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 volet du même nom.

Pour ajouter des groupes d'utilisateurs et des utilisateurs par paramétrage guidé :

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 64 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, choisissez son nom dans la liste Stratégies sélectionnées, puis cliquez sur Retirer.
8. Si vous souhaitez associer à distance des utilisateurs authentifiés avec des modules Active Directory, cliquez sur l'onglet Associations d'Active Directory lorsque cet onglet configuré AD n'est pas masqué. Cochez la case correspondant à chaque module Active Directory à associer au groupe d'utilisateurs.
9. Pour ajouter un autre groupe d'utilisateurs, cliquez sur Appliquer pour enregistrer le groupe actif, puis répétez cette procédure. **Facultatif.**
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.
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. 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 et des utilisateurs que vous avez ajoutés. **Facultatif.**

Chapitre 5 Associations, catégories et éléments

Dans ce chapitre

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 Eléments 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 : 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 : 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 à CC-SG, 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. Reportez-vous à ***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. Reportez-vous à ***Gestionnaire des associations*** (à la page 25).

Gestionnaire des associations

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

Remarque : par défaut, CC-SG laisse les noms de catégories par défaut « System Type » et « US States and territories » en anglais.

Ajouter une catégorie

Pour ajouter une catégorie :

1. Choisissez Associations > Association.
2. Cliquez sur Ajouter. La fenêtre Ajouter une catégorie s'ouvre.
3. Renseignez le champ Nom de la catégorie. Reportez-vous à ***Conventions d'appellation*** (à la page 353) 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 qu'une valeur de chaîne ne peut pas être remplacée par une valeur de nombre entier et inversement. Si vous devez effectuer ce type de modification, supprimez la catégorie et ajoutez-en une nouvelle.

Pour modifier une catégorie :

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'ouvre.
4. Entrez le nom de la nouvelle catégorie dans le 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 vos 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.

Pour supprimer une catégorie :

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'ouvre.
4. Cliquez sur Oui pour supprimer la catégorie.

Ajouter un élément

Pour 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 353) 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 vos modifications.

Modifier un élément

Pour modifier un élément :

1. Choisissez Associations > Association.
2. Cliquez sur la flèche déroulante Nom de la catégorie et sélectionnez la catégorie contenant l'élément à modifier.
3. Double-cliquez sur l'élément à modifier dans la liste des éléments.
4. Entrez la nouvelle valeur de l'élément dans cette liste. Les éléments sont sensibles à la casse.
5. Cliquez sur OK pour actualiser l'élément ou sur Fermer pour fermer la fenêtre.

Supprimer un élément

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

Pour supprimer un élément :

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.

Chapitre 6 Dispositifs, groupes de dispositifs et ports

Pour ajouter des dispositifs PowerStrip Raritan connectés à d'autres dispositifs Raritan à CC-SG, reportez-vous à ***Barrettes d'alimentation gérées*** (à la page 70).

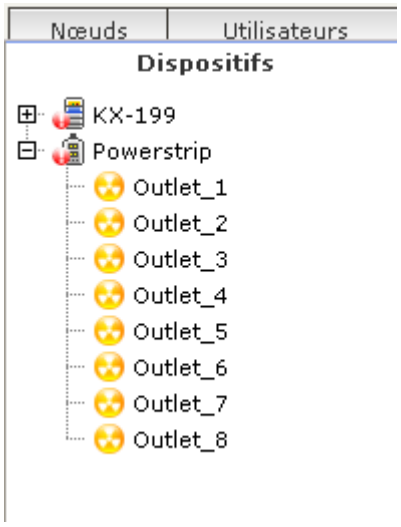
Remarque : pour configurer des dispositifs iLO/RILOE, IPMI, Dell DRAC, IBM RSA ou d'autres dispositifs non Raritan, utilisez l'option de menu Ajouter un nœud et ajoutez ces éléments comme interface. Reportez-vous à **Nœuds, groupes de nœuds et interfaces** *(à la page 80).*

Dans ce chapitre

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 + ou - pour développer ou masquer la liste des ports.

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

Icône	Signification
	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
	Châssis de lames disponible
	Châssis de lames non disponible
	Serveur de lames disponible
	Serveur de lames non disponible

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.

Pour trier les ports dans l'onglet Dispositifs :

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

Remarque : pour les serveurs lames sans commutateur KVM intégré, tels que les serveurs HP BladeSystem, le dispositif parent est le châssis de lames virtuel créé par CC-SG, non le dispositif KX2. Ces serveurs seront triés uniquement au sein du dispositif de châssis de lames virtuel afin qu'ils n'apparaissent pas dans l'ordre avec les autres ports KX2 à moins que vous ne rétablissiez ces ports de serveurs lames aux ports KX2 normaux. Reportez-vous à **Rétablir les ports de serveurs lames sur les ports KX2 normaux** *(à la page 50).*

Ecran Profil du dispositif

Lorsque vous sélectionnez un dispositif dans l'onglet Dispositifs, l'écran Profil du dispositif apparaît, qui affiche des informations sur le dispositif choisi.

Lorsqu'un dispositif est arrêté, les données de l'écran Profil du dispositif est en lecture seule. Vous pouvez supprimer un dispositif arrêté. Reportez-vous à ***Suppression d'un dispositif*** (à la page 40).

L'écran Profil du dispositif comprend des onglets présentant des informations sur le dispositif.

Onglet Associations

L'onglet Associations contient la totalité des catégories et éléments affectés au nœud. Vous pouvez modifier les associations en effectuant des sélections différentes. Reportez-vous à ***Associations, catégories et éléments*** (à la page 23).

Onglet Emplacement et contacts

L'onglet Emplacement et contacts contient des informations sur l'emplacement et les contacts d'un nœud, tels que des numéros de téléphone, dont vous pouvez avoir besoin lors du travail sur un nœud. Vous pouvez modifier les champs en entrant de nouvelles informations. Reportez-vous à ***Ajout d'un emplacement et de contacts à un profil de dispositif*** (à la page 39).

Onglet Notes

L'onglet Notes contient un outil permettant à un utilisateur de laisser des notes concernant un dispositif à l'intention d'autres utilisateurs. Toutes les notes apparaissent dans l'onglet avec la date, le nom d'utilisateur et l'adresse IP de leur auteur.

Si vous disposez du privilège Device, Port, and Node Management (gestion des dispositifs, des ports et des nœuds), vous pouvez effacer toutes les notes du profil du nœud en cliquant sur Effacer.

Reportez-vous à ***Ajout de notes à un profil de dispositif*** (à la page 39).

Onglet Commutateurs (Lames)

Les nœuds de châssis de lames, tels que IBM BladeCenter, comportent l'onglet Commutateurs (Lames). Cet onglet contient des données concernant les serveurs lames résidant dans le châssis de lames.

Outre la consultation des informations relatives aux lames, vous pouvez paramétrer les serveurs lames non configurés en sélectionnant les cases à cocher qui leur correspondent dans cet onglet.

Reportez-vous à ***Configuration des connecteurs sur un dispositif de châssis de lames*** (à la page 46).

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.

Pour ouvrir la vue topologique :

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.

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. Reportez-vous à ***Modifier votre préférence de recherche par défaut*** (à la page 134).

Pour rechercher un dispositif :

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

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 de dispositifs

La commande Détecter les dispositifs déclenche la recherche de tous les dispositifs 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 Include IPMI Agents (Inclure les agents IPMI) pour rechercher des cibles fournissant une 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. La page Ajouter un dispositif varie suivant les différents types de dispositifs. Reportez-vous aux instructions concernant l'ajout de chaque type de dispositif détecté par CC-SG.
   - Pour les dispositifs KVM ou série, reportez-vous à ***Ajouter un dispositif KVM ou série*** (à la page 35).
   - Pour les barrettes d'alimentation, reportez-vous à ***Ajouter un dispositif PowerStrip*** (à la page 37).
   - Pour les barrettes d'alimentation Dominion PX sur le réseau IP, reportez-vous à ***Ajouter un dispositif Dominion PX*** (voir "Ajouter un dispositif Dominion PX" à la page 37).
9. Cliquez sur Appliquer pour ajouter un dispositif détecté et continuer vers le dispositif détecté suivant. Cliquez sur OK pour ajouter le dispositif détecté actuel et arrêter le processus d'ajout des dispositifs détectés.

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 et pouvez fournir ces dernières à CC-SG. Pour rechercher des dispositifs à ajouter, utilisez l'option Détecter les dispositifs. Reportez-vous à ***Détection de dispositifs*** (à la page 33).

Pour ajouter des dispositifs PowerStrip Raritan connectés à d'autres dispositifs Raritan à CC-SG, reportez-vous à ***Barrettes d'alimentation gérées*** (à la page 70).

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. Suivant le type de dispositif sélectionné, la page Ajouter un dispositif est légèrement différente.

- Pour obtenir des instructions sur l'ajout de dispositifs KVM ou série, reportez-vous à ***Ajouter un dispositif KVM ou série*** (à la page 35).
- Pour obtenir des instructions sur l'ajout de barrettes d'alimentation, reportez-vous à ***Ajouter un dispositif PowerStrip*** (à la page 37).
- Pour obtenir des instructions sur l'ajout de dispositifs Dominion PX, reportez-vous à ***Ajouter un dispositif Dominion PX*** (voir "Ajouter un dispositif Dominion PX" à la page 37).

Ajouter un dispositif KVM ou série

Les dispositifs KVM et série peuvent prendre en charge le chiffrement AES 256 bits, que CC-SG supporte également depuis la version 4.1. Si le dispositif est paramétré sur le mode de chiffrement par défaut « auto-négocier », il négociera avec CC-SG afin de sélectionner un niveau de chiffrement approprié pour fonctionner avec CC-SG.

1. Renseignez le champ Nom du dispositif. Reportez-vous à ***Conventions d'appellation*** (à la page 353) 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 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. Il contient cinq chiffres au maximum. 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 dispositif 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. Entrez une brève description de ce dispositif dans le champ Description. **Facultatif.**

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 sera créé pour chaque port et une interface hors bande sera créée pour ce nœud, sauf s'il s'agit d'un nœud de châssis de lames.
   - Un nœud peut ou non être créé pour un dispositif de châssis de lames connecté à un port KX2, selon qu'une adresse IP ou un nom d'hôte pour le châssis de lame ont été entrés dans KX2. Consultez le manuel d'utilisation de KX II. Une interface de navigateur Web est affectée au nœud de châssis de lames dans CC-SG par défaut.
   - Un dispositif de châssis de lames virtuel sera créé pour les serveurs lames connectés directement aux ports KX2, si les groupes de ports de lames ont été configurés correctement pour ces serveurs lames dans KX2. Consultez le manuel d'utilisation de KX II.
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, catégories et éléments*** (à la page 23).
11. Pour chaque catégorie répertoriée, cliquez sur le menu déroulant Elément, puis sélectionnez dans la liste l'élément que vous souhaitez appliquer au dispositif. 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.
12. 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, catégories et éléments*** (à la page 23).
13. Une fois la configuration du dispositif terminée, cliquez sur Appliquer pour ajouter ce dispositif et ouvrir un nouvel écran Ajouter un dispositif vide qui vous permet de continuer à ajouter des dispositifs, ou cliquez sur OK pour ajouter ce dispositif sans passer à un nouvel écran Ajouter un dispositif.
14. 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 52).**

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 ***Barrette d'alimentation gérée*** (voir "Barrettes d'alimentation gérées" à la page 70).

Pour ajouter une unité Dominion PX qui n'est pas connectée à un autre dispositif Raritan, reportez-vous à ***Ajouter un dispositif Dominion PX*** (voir "Ajouter un dispositif Dominion PX" à la page 37).

Ajouter un dispositif Dominion PX

Les dispositifs Dominion PX sont des barrettes d'alimentation qui sont connectées à votre réseau IP uniquement. Un dispositif Dominion PX n'est pas géré par un autre dispositif Raritan. Si vous souhaitez ajouter une barrette d'alimentation qui est gérée par un autre dispositif Raritan, il existe une procédure différente. Reportez-vous à ***Barrette d'alimentation gérée*** (voir "Barrettes d'alimentation gérées" à la page 70).

1. Renseignez le champ Nom du dispositif. Reportez-vous à ***Conventions d'appellation*** (à la page 353) 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 pour le dispositif. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie et sigles*** (à la page 2).
3. Entrez le nom utilisé pour vous connecter à ce dispositif dans le champ Nom d'utilisateur. L'utilisateur doit disposer d'un accès administratif.
4. 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.

   Avertissement : CC-SG perdra la connectivité avec le dispositif Dominion PX si le nom d'utilisateur ou le mot de passe change. Si vous modifiez le mot de passe sur l'unité PX, vous devez changer le mot de passe pour le dispositif PX dans CC-SG. Reportez-vous à **Modification d'un dispositif** *(à la page 38).*
5. Entrez une brève description de ce dispositif dans le champ Description. **Facultatif.**
6. Cochez la case Configurer toutes les prises pour ajouter automatiquement toutes les prises de cette unité Dominion PX à l'onglet Dispositifs.
7. Une liste de catégories et d'éléments peut être configurée pour décrire et organiser le dispositif de façon optimale.

- Pour chaque catégorie répertoriée, sélectionnez dans la liste l'élément que vous souhaitez appliquer au dispositif. 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 d'autres. Reportez-vous à ***Associations, catégories et éléments*** (à la page 23).

8. Une fois la configuration du dispositif terminée, cliquez sur Appliquer pour ajouter ce dispositif et ouvrir un nouvel écran Ajouter un dispositif vide qui vous permet de continuer à ajouter des dispositifs, ou cliquez sur OK pour ajouter ce dispositif sans passer à un nouvel écran Ajouter un dispositif.

Modification d'un dispositif

Vous pouvez modifier un dispositif pour le renommer et changer ses propriétés, comme par exemple, modifier le nom d'utilisateur et le mot de passe d'un dispositif PX.

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 vos modifications.

Modification d'un dispositif PowerStrip ou d'un dispositif Dominion PX

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

Pour modifier un dispositif PowerStrip :

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 Outlet (prise) pour afficher toutes les prises de la barrette d'alimentation.
4. Si une prise est associée à un nœud, cliquez sur le lien hypertexte Nœud pour ouvrir le profil du nœud.

5. Si une prise est associée à un nœud, sélectionnez-la, puis cliquez sur Power Control (gestion de l'alimentation) afin d'ouvrir l'écran Gestion de l'alimentation pour le nœud associé.
6. Pour supprimer une prise, désactivez la case à cocher à côté de son nom.
7. Pour configurer une prise, cochez la case à côté de son nom.
8. Cliquez sur OK pour enregistrer vos modifications. Un message apparaît lorsque le dispositif a été modifié.

Ajout de notes à un profil de dispositif

L'onglet Notes vous permet d'ajouter des notes sur un dispositif à l'attention d'autres utilisateurs. Toutes les notes apparaissent dans l'onglet avec la date, le nom d'utilisateur et l'adresse IP de leur auteur.

Si vous disposez du privilège Device, Port, and Node Management (gestion des dispositifs, des ports et des nœuds), vous pouvez effacer toutes les notes qui s'affichent dans l'onglet Notes.

Pour ajouter des notes au profil du dispositif :

1. Sélectionnez un dispositif dans l'onglet Dispositifs. La page Profil du dispositif s'ouvre.
2. Cliquez sur l'onglet Notes.
3. Tapez votre note dans le champ Nouvelle note.
4. Cliquez sur Ajouter. Votre note apparaît dans la liste Notes.

Pour effacer toutes les notes :

1. Cliquez sur l'onglet Notes.
2. Cliquez sur Effacer les notes.
3. Cliquez sur Oui pour confirmer. Toutes les notes sont supprimées de l'onglet Notes.

Ajout d'un emplacement et de contacts à un profil de dispositif

Entrez des détails concernant l'emplacement du dispositif et les coordonnées de ceux qui administrent ou utilisent le dispositif.

Pour ajouter un emplacement et des contacts à un profil de dispositif :

1. Sélectionnez un dispositif dans l'onglet Dispositifs. La page Profil du dispositif s'ouvre.

2. Cliquez sur l'onglet Emplacement &Contacts.
3. Entrez des renseignements sur l'emplacement.
   - Service : 64 caractères au maximum.
   - Site : 64 caractères au maximum.
   - Emplacement : 128 caractères au maximum.
4. Entrez des renseignements sur les contacts.
   - Nom de la personne principale à contacter et Nom de la personne secondaire à contacter : 64 caractères au maximum.
   - Numéro de téléphone et de mobile : 32 caractères au maximum.
5. Cliquez sur OK pour enregistrer vos modifications.

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.

Pour supprimer un dispositif :

1. Cliquez sur l'onglet Dispositifs et sélectionnez le dispositif à supprimer.
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 de ports

Si tous les ports d'un dispositif n'ont pas été automatiquement ajoutés par l'activation de la case à cocher Configurer tous les ports lorsque vous avez ajouté le dispositif, utilisez l'écran Configurer les ports pour ajouter des ports un par un ou un ensemble de ports du dispositif dans CC-SG.

Une fois les ports configurés, un nœud est créé dans CC-SG pour chacun et l'interface par défaut est également générée. Reportez-vous à ***Nœuds créés par configuration de ports*** (à la page 42).

Configurer un port série

Pour configurer un port série :

1. Cliquez sur l'onglet Dispositifs et sélectionnez un dispositif série.
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 série 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 353) 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 choisissez dans la liste l'application que vous souhaitez utiliser lors de la connexion au port concerné. Pour autoriser CC-SG à sélectionner automatiquement l'application en fonction de votre navigateur, sélectionnez Détection automatique.
7. Cliquez sur OK pour ajouter le port.

Configurer un port KVM

Pour 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 353) 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 choisissez dans la liste l'application que vous souhaitez utiliser lors de la connexion au port concerné. Pour autoriser CC-SG à sélectionner automatiquement l'application en fonction de votre navigateur, sélectionnez Détection automatique.
7. Cliquez sur OK pour ajouter le port.

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 353).

Modification d'un port

Vous pouvez modifier différents paramètres pour les ports, tels que le nom, l'application d'accès et le port série. Les modifications que vous apportez dépendent du type du port et du type du dispositif.

Pour modifier un nom de port KVM ou série, ou une application d'accès :

Certains ports ne prennent en charge qu'une seule application d'accès, vous ne pouvez donc pas modifier cette préférence.

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 choisissez dans la liste l'application que vous souhaitez utiliser lors de la connexion au port concerné. Pour autoriser CC-SG à sélectionner automatiquement l'application en fonction de votre navigateur, sélectionnez Détection automatique.
4. Cliquez sur OK pour enregistrer vos modifications.

Pour modifier les paramètres du port série KSX2 ou KSX, tels que débit en bauds, le contrôle de flux ou les bits de parité/données :

1. Cliquez sur l'onglet Dispositifs et sélectionnez le port série que vous souhaitez modifier, ou sélectionnez simplement le dispositif contenant le port à modifier.
2. Choisissez Dispositifs >Gestionnaire des dispositifs > Démarrer Admin. La page administrative du dispositif s'ouvre.
3. Cliquez sur Configuration des ports.
4. Cliquez sur le port série que vous souhaitez modifier.
5. Modifiez les paramètres du port.
6. Cliquez sur OK pour enregistrer vos modifications. Fermez la page administrative et retournez dans CC-SG.

Pour modifier les paramètres d'un port série SX, tels que le débit en bauds, le contrôle de flux ou les bits de parité/données :

1. Cliquez sur l'onglet Dispositifs et sélectionnez le port à modifier. La page Profil du port s'ouvre.
2. Modifiez les paramètres du port.
3. Cliquez sur OK pour enregistrer vos modifications.

Suppression d'un port

La suppression d'un port entraîne le retrait de l'entrée correspondante d'un dispositif. Lorsqu'un port est arrêté, les données de l'écran Profil du port est en lecture seule. Vous pouvez supprimer un port arrêté.

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.

Pour supprimer un port :

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

Configuration d'un dispositif à châssis de lames connecté à KX2

Vue d'ensemble des châssis de lames

Il existe deux types de dispositifs de châssis de lames : l'un dispose d'un commutateur KVM intégré, qui peut fonctionner comme commutateur KVM à activation IP, et l'autre n'en dispose pas.

Châssis de lames à commutateur KVM intégré

Un châssis de lames à commutateur KVM intégré, comme ceux des séries Dell PowerEdge et IBM BladeCenter, est connecté à KX2 par un CIM. Comme un seul CIM est disponible pour accéder à tous les serveurs lames de ce châssis, lorsqu'un utilisateur accède à un serveur lame, il ne reste plus de chemin vers les autres.

Lors de la configuration de tous les ports KX2 dans CC-SG, le *châssis de lames* connecté au dispositif KX2 est paramétré. Reportez-vous à ***Ajouter un dispositif de châssis de lames*** (à la page 45). Les serveurs lames de ce type de châssis ne sont pas encore configurés, vous devez donc les paramétrer ultérieurement. Reportez-vous à ***Configuration des connecteurs sur un dispositif de châssis de lames*** (à la page 46).

Châssis de lames sans commutateur KVM intégré

Un châssis de lames sans commutateur KVM intégré, comme ceux des séries HP BladeSystem, permet à chaque serveur lame de se connecter à KX2 respectivement par un CIM. Comme chaque serveur lame de ce châssis dispose d'un CIM pour l'accès, lorsqu'un utilisateur accède à un serveur lame, les autres utilisateurs peuvent accéder aux autres serveurs lames.

Lors de la configuration de tous les ports KX2 dans CC-SG, les *serveurs lames* connectés au dispositif KX2 sont paramétrés. Si vous avez configuré correctement un groupe de ports de lames pour ces serveurs lames sur le dispositif KX2, CC-SG crée un châssis de lames *virtuel* au niveau des ports KX2 pour contenir ces serveurs lames. Reportez-vous à ***Ajouter un dispositif de châssis de lames*** (à la page 45). Sinon, ces serveurs lames apparaissent en tant que ports KX2 normaux dans l'onglet Dispositifs de CC-SG.

Ajouter un dispositif de châssis de lames

La procédure d'ajout des dispositifs de châssis de lames varie selon le type de châssis.

Un dispositif de châssis de lames affiche toujours deux noms dans l'onglet Dispositifs : le nom sans parenthèse est extrait du dispositif KX2, et celui entre parenthèses est le nom du châssis enregistré sur CC-SG.

Pour ajouter un dispositif de châssis de lames *avec* commutateur KVM intégré :

1. Configurez correctement le châssis de lames dans KX2. Consultez le manuel d'utilisation de KX II.
2. Configurez correctement le dispositif KX2 dans CC-SG. Reportez-vous à ***Ajouter un dispositif KVM ou série*** (à la page 35).
3. CC-SG détecte le dispositif de châssis de lames et ajoute son icône dans un ou deux onglets :
   - Dans l'onglet Dispositifs, le dispositif de châssis de lames apparaît sous le dispositif KX2 auquel il est connecté.
   - Dans l'onglet Nœuds, si vous avez entré l'adresse IP ou le nom d'hôte du châssis de lames sur le dispositif KX2, le châssis apparaît sous forme de nœud auquel est ajouté une interface de navigateur Web.

Remarque : pour ce type de châssis de lames, vous devez configurer les serveurs lames ultérieurement. Reportez-vous à **Configuration des connecteurs sur un dispositif de châssis de lames** *(à la page 46).*

Pour ajouter un dispositif de châssis de lames *sans* commutateur KVM intégré :

1. Configurez correctement un groupe de ports de lames pour les serveurs lames dans KX2. Consultez le manuel d'utilisation de KX II.
2. Configurez correctement le dispositif KX2 dans CC-SG. Reportez-vous à ***Ajouter un dispositif KVM ou série*** (à la page 35).
3. CC-SG crée automatiquement un châssis de lames *virtuel* et ajoute l'icône de celui-ci dans un onglet. Notez qu'un châssis de lames virtuel n'apparaît jamais sous forme de nœud dans l'onglet Nœuds.
   - Dans l'onglet Dispositifs, le châssis de lames virtuel apparaît sous le dispositif KX2 comme conteneur virtuel des serveurs lames, qui apparaissent sous le châssis virtuel.

Remarque : si vous n'avez pas configuré le groupe de ports de lames pour les serveurs lames avant de paramétrer les ports KX2 dans CC-SG, vous pouvez choisir Dispositifs > Gestionnaire des dispositifs > Démarrer Admin pour définir le groupe de ports de lames. Configurez ensuite les serveurs lames dans CC-SG. Reportez-vous à **Configuration des connecteurs sur un dispositif de châssis de lames** *(à la page 46).*

Configuration des connecteurs sur un dispositif de châssis de lames

Si les serveurs lames ou les connecteurs ne sont pas encore configurés dans CC-SG, vous devez les paramétrer en suivant la procédure de cette section. Sinon, les serveurs lames n'apparaissent pas dans les onglets Dispositifs et Nœuds. Une interface KVM hors bande est automatiquement ajoutée à un nœud de serveur lame.

Pour configurer des connecteurs à partir du profil du châssis de lames :

1. Dans l'onglet Dispositifs, cliquez sur le + en regard du dispositif KX2 connecté au dispositif de châssis de lames.
2. Sélectionnez le dispositif de châssis de lames dont vous souhaitez configurer les connecteurs.
3. Dans l'écran Profil du dispositif, sélectionnez l'onglet Commutateurs (Lames).
4. Cochez la case de chaque connecteur à configurer, puis cliquez sur OK.

Pour configurer les commutateurs dans l'écran Configurer les ports :

1. Dans l'onglet Dispositifs, cliquez sur le + en regard du dispositif KX2 connecté au dispositif de châssis de lames.
2. Sélectionnez le dispositif de châssis de lames dont vous souhaitez configurer les connecteurs.
3. Choisissez Dispositifs > Gestionnaire des ports > Configurer les ports.
   - Pour configurer plusieurs connecteurs avec les noms par défaut affichés à l'écran, cochez la case de chaque connecteur à configurer, puis cliquez sur OK pour leur définir un nom par défaut.
   - Pour configurer les commutateurs individuellement, cliquez sur le bouton Configurer placé en regard de chacun. Entrez ensuite un nom de commutateur dans le champ Nom du port, puis un nom de nœud dans le champ Nom du nœud. L'application d'accès par défaut est définie suivant l'application par défaut sélectionnée pour « Châssis de commutateur (Châssis de lames) : KVM » dans le gestionnaire d'applications. Pour la modifier, cliquez sur le menu déroulant Application d'accès pour sélectionner celle que vous préférez dans la liste. Cliquez sur OK pour configurer le connecteur.

Pour configurer des connecteurs à l'aide de la commande Configurer les commutateurs (lames) :

1. Dans l'onglet Dispositifs, cliquez sur le + en regard du dispositif KX2 connecté au dispositif de châssis de lames.
2. Sélectionnez le dispositif de châssis de lames dont vous souhaitez configurer les connecteurs.
3. Choisissez Nœuds > Configurer les commutateurs (lames).
   - Pour configurer plusieurs connecteurs avec les noms par défaut affichés à l'écran, cochez la case de chaque connecteur à configurer, puis cliquez sur OK pour leur définir un nom par défaut.
   - Pour configurer les commutateurs individuellement, cliquez sur le bouton Configurer placé en regard de chacun. Entrez ensuite un nom de commutateur dans le champ Nom du port, puis un nom de nœud dans le champ Nom du nœud. L'application d'accès par défaut est définie suivant l'application par défaut sélectionnée pour « Châssis de commutateur (Châssis de lames) : KVM » dans le gestionnaire d'applications. Pour la modifier, cliquez sur le menu déroulant Application d'accès pour sélectionner celle que vous préférez dans la liste. Cliquez sur OK pour configurer le connecteur.

Modification de l'état du serveur lame

Cette section s'applique uniquement aux châssis de lames à commutateur KVM intégré, comme ceux des séries Dell PowerEdge et IBM BladeCenter.

Si l'état Installé pour le serveur lame ou le connecteur correspondant n'est pas activé sur le dispositif KX2, CC-SG affiche toujours l'état « Non disponible » pour le port du serveur lame. Lorsque vous êtes certain que certains connecteurs de lames sont actifs avec des serveurs lames installés, vous devriez modifier leur état sur le dispositif KX2 afin que CC-SG reflète celui-ci correctement.

Pour modifier l'état d'un serveur lame :

1. Cliquez sur l'onglet Dispositifs et sélectionnez le dispositif KX2 pour lequel vous souhaitez modifier l'état d'un connecteur de lame.
2. Choisissez Dispositifs > Gestionnaire des dispositifs > Démarrer Admin. Le client Admin KX2 s'ouvre.
3. Sélectionnez Paramètres du dispositif > Configuration des ports.
4. Cliquez sur le port du châssis de lames que vous souhaitez configurer.
5. Faites défiler la page jusqu'à la section des connecteurs de lames. Cochez la case Installé en regard des connecteurs de lames actifs avec serveurs lames installés.
6. Cliquez sur OK pour enregistrer les modifications.

Suppression des connecteurs sur un dispositif de châssis de lames

Vous pouvez supprimer les serveurs lames ou connecteurs inutilisés pour les faire disparaître des onglets Dispositifs et Nœuds.

Pour supprimer un connecteur à partir de l'écran Supprimer des ports :

1. Dans l'onglet Dispositifs, cliquez sur le + en regard du dispositif KX2 connecté au dispositif de châssis de lames.
2. Sélectionnez le dispositif de châssis de lames dont vous souhaitez supprimer les connecteurs.
3. Choisissez Dispositifs > Gestionnaire des ports > Supprimer les ports.
4. Cochez la case de chaque connecteur à supprimer, puis cliquez sur OK.

Pour supprimer un connecteur à l'aide de la commande Supprimer le commutateur (la lame) :

1. Dans l'onglet Dispositifs, cliquez sur le + en regard du dispositif KX2 connecté au dispositif de châssis de lames.
2. Sélectionnez le + en regard du dispositif de châssis de lames dont vous souhaitez supprimer les connecteurs.
3. Cliquez avec le bouton droit sur le connecteur de lame à supprimer.
4. Sélectionnez Supprimer le commutateur, puis cliquez sur OK pour effectuer la suppression.

Modifier un dispositif de châssis de lames

Vous pouvez modifier un dispositif de châssis de lames afin de le renommer, de changer ses propriétés et d'afficher l'état de la configuration des connecteurs.

Pour modifier un châssis de lames :

1. Dans l'onglet Dispositifs, cliquez sur le + en regard du dispositif KX2 connecté au dispositif de châssis de lames.
2. Sélectionnez le dispositif de châssis de lames à modifier.
3. Entrez les nouvelles propriétés du dispositif dans les champs appropriés de l'écran. Si nécessaire, modifiez les catégories et éléments associés au dispositif.
4. Cliquez sur l'onglet Commutateurs (Lames) pour afficher tous les connecteurs de ce dispositif de châssis de lames.
5. Si un connecteur a été configuré comme un nœud, vous pouvez cliquer sur le lien hypertexte Nœud pour ouvrir le profil du nœud. **Facultatif.**
6. Cliquez sur OK pour enregistrer vos modifications. Un message apparaît lorsque le dispositif a été modifié.

Supprimer un dispositif de châssis de lames

Vous pouvez supprimer un dispositif de châssis de lames connecté à un dispositif KX2 de CC-SG. Lorsque la suppression est effectuée, le dispositif de châssis de lames et tous les serveurs lames ou connecteurs configurés disparaissent de l'onglet Dispositifs et de l'onglet Nœuds.

Pour supprimer un dispositif de châssis de lames :

1. Cliquez sur l'onglet Dispositifs et sélectionnez le dispositif KX2 dont vous souhaitez supprimer le dispositif de châssis de lames.
2. Choisissez Dispositifs > Gestionnaire des ports > Supprimer les ports.

3. Cochez la case du port du châssis que vous souhaitez supprimer.
4. Cliquez sur OK pour supprimer le port de châssis sélectionné. Un message vous demande de confirmer la suppression du dispositif de châssis de lames ainsi que de tous ses serveurs lames.

Déplacer un dispositif de châssis de lames vers un port différent

Lorsque vous déplacez un dispositif de châssis de lames d'un dispositif KX2 ou port vers un autre dispositif KX2 ou port, CC-SG ne peut pas détecter et mettre automatiquement à jour les données de configuration du dispositif de châssis de lames sur le nouveau port. Vous devez configurer à nouveau le dispositif de châssis de lames sur CC-SG.

Pour déplacer un dispositif de châssis de lames vers un dispositif KX2 ou port différent :

1. Supprimez le dispositif de châssis de lames de CC-SG. Reportez-vous à ***Supprimer un dispositif de châssis de lames*** (à la page 49).
2. Déconnectez et reconnectez le châssis de lames à un autre dispositif KX2 ou port.
3. Ajoutez le dispositif de châssis de lames dans CC-SG. Reportez-vous à ***Ajouter un dispositif de châssis de lames*** (à la page 45).

Rétablir les ports de serveurs lames sur les ports KX2 normaux

Cette section s'applique uniquement aux châssis de lames sans commutateur KVM intégré, comme ceux des séries HP BladeSystem.

Vous pouvez reconfigurer des serveurs lames sous le châssis de lames virtuel comme ports KX2 normaux dans l'onglet Dispositifs.

Pour rétablir des serveurs lames sur des ports KX2 normaux :

1. Dans l'onglet Dispositifs, sélectionnez le dispositif KX2 dont vous souhaitez reconfigurer les serveurs lames comme ports KVM normaux.
2. Changez le groupe de ports de lames pour ces serveurs en groupe de ports non-lames.
   a. Dans CC-SG, choisissez Dispositifs > Gestionnaire des dispositifs > Démarrer Admin. Le client Admin KX2 s'ouvre.
   b. Cliquez sur Port Group Management (Gestion des groupes de ports).
   c. Cliquez sur le groupe de ports de lames dont vous souhaitez modifier la propriété.

d. Désélectionnez la case à cocher Blade Server Group (Groupe de serveurs lames).

e. Cliquez sur OK.

f. Quittez le client Admin KX2.

3. Le châssis de lames virtuel disparaît de l'onglet Dispositifs. Vous pouvez maintenant reconfigurer les ports du serveur lame comme ports KX2 normaux dans CC-SG. Reportez-vous à ***Configurer un port KVM*** (à la page 41).

Copie en bloc pour les associations, emplacement et contacts de dispositifs

La commande Copier en bloc permet de copier les catégories, éléments, emplacement et informations de contact d'un dispositif vers plusieurs autres dispositifs. Notez que les informations sélectionnées constituent la seule propriété copiée lors de cette opération. Lorsque le même type d'informations existe sur certains des dispositifs sélectionnés, l'exécution de la commande Copier en bloc REMPLACERA les données existantes par les nouvelles informations attribuées.

Pour copier en bloc des associations, emplacement et informations de contact de dispositifs :

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 Dispositifs disponibles, sélectionnez les dispositifs vers lesquels vous copiez les associations, emplacement et informations de contact du dispositif indiqué dans le champ Nom du dispositif.
4. Cliquez sur le bouton > pour ajouter un dispositif à la liste Dispositifs sélectionnés.
5. Sélectionnez le dispositif et cliquez sur < pour le retirer de la liste Dispositifs sélectionnés.
6. Dans l'onglet Associations, cochez la case Copier les associations pour copier tous les éléments et les catégories du dispositif.
   - Vous pouvez modifier, ajouter ou supprimer toutes les données de cet onglet. Les données modifiées seront copiées sur plusieurs dispositifs dans la liste Dispositifs sélectionnés, ainsi que le dispositif actuel affiché dans le champ Nom du dispositif. **Facultatif.**
7. Dans l'onglet Emplacement et contacts, cochez la case des données que vous souhaitez copier :

- Cochez la case Copier les informations d'emplacement pour copier les données affichées dans la section Emplacement.
- Cochez la case Copier les informations de contact pour copier les données affichées dans la section Contacts.
- Vous pouvez modifier, ajouter ou supprimer les données de ces onglets. Les données modifiées seront copiées sur plusieurs dispositifs dans la liste Dispositifs sélectionnés, ainsi que le dispositif actuel affiché dans le champ Nom du dispositif. **Facultatif.**

8. Cliquez sur OK pour copier en bloc. Un message apparaît lorsque les données sélectionnées ont été copiées.

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.

Pour mettre à niveau un dispositif :

1. Cliquez sur l'onglet Dispositifs et sélectionnez un dispositif dans l'arborescence Dispositifs.
2. Choisissez Dispositifs > Gestionnaire des dispositifs > Mettre à niveau un dispositif.
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.

Mise à niveau de la configuration d'un 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.

Le nombre maximum de fichiers de sauvegarde pouvant être stockés sur CC-SG est de 3 par dispositif. Si vous avez besoin de sauvegardes supplémentaires, vous pouvez enregistrer un fichier de sauvegarde sur votre réseau, puis le supprimer de CC-SG. Ou vous pouvez décider d'autoriser CC-SG à supprimer le fichier de sauvegarde le plus ancien pour vous. Cette option apparaîtra sous forme d'alerte lorsque vous tenterez d'effectuer une quatrième sauvegarde. Reportez-vous à ***Restaurer toutes les données de configuration d'un dispositif KX2, KSX2 ou KX2-101*** (voir "Restaurer toutes les données de configuration d'un dispositif KX2, KSX2 ou KX2-101." à la page 56).

Chaque dispositif peut sauvegarder différents composants de la configuration. Reportez-vous au manuel d'utilisation du dispositif à sauvegarder pour plus d'informations.

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.

Pour sauvegarder la configuration d'un dispositif :

1. Cliquez sur l'onglet Dispositifs et sélectionnez le dispositif à sauvegarder.
2. Choisissez Dispositifs > Gestionnaire des configurations > Configuration > Sauvegarde.
3. Renseignez le champ Nom de la sauvegarde pour identifier cette sauvegarde.
4. Entrez une brève description de la sauvegarde dans le champ Description. **Facultatif.**
5. Cliquez sur OK pour sauvegarder la configuration du dispositif. Un message apparaît lorsque la configuration du dispositif a été sauvegardée.

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, KSX2 et KX2-101 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. Vous pouvez utiliser l'option Protégé pour restaurer la sauvegarde d'un dispositif sur un autre du même modèle (KX2, KSX2 et KX2-101 uniquement).
- 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 de données 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.

Pour restaurer une configuration de dispositif de sauvegarde complète :

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 à l'exception des paramètres réseau sur un dispositif KX2, KSX2 ou KX2-101

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, KSX2 ou KX2-101. Vous pouvez utiliser l'option Protégé pour restaurer la sauvegarde d'un dispositif sur un autre du même modèle (KX2, KSX2 et KX2-101 uniquement).

Pour restaurer toutes les données de configuration à l'exception des paramètres réseau sur un dispositif KX2, KSX2 ou KX2-101 :

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, KSX2 ou KX2-101

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.

Pour restaurer uniquement les paramètres de dispositif ou les données de l'utilisateur ou du groupe de l'utilisateur sur un dispositif KX2, KSX2 ou KX2-101 :

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 d'un dispositif KX2, KSX2 ou KX2-101.

L'option de restauration Complet vous permet de rétablir toutes les données de configuration dans un fichier de sauvegarde sur un dispositif KX2, KSX2 ou KX2-101.

Pour restaurer toutes les données de configuration d'un dispositif KX2, KSX2 ou KX2-101 :

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.

Enregistrer, télécharger et supprimer les fichiers de sauvegarde d'un dispositif

Vous pouvez enregistrer les fichiers de sauvegarde d'un dispositif dans la page Restaurer la configuration du dispositif sur un emplacement du réseau ou d'un ordinateur local. Si vous devez faire de place pour stocker de nouvelles sauvegardes sur CC-SG, vous pouvez supprimer les fichiers de sauvegarde d'un dispositif. Vous pouvez également télécharger les fichiers de sauvegarde enregistrés sur votre réseau pour les replacer dans CC-SG afin de restaurer la configuration d'un dispositif.

Pour enregistrer un fichier de sauvegarde de dispositif de CC-SG :

1. Cliquez sur l'onglet Dispositifs et sélectionnez un dispositif.
2. Choisissez Dispositifs > Gestionnaire des dispositifs > Configuration > Restaurer.

3. Sélectionnez le fichier de sauvegarde de dispositif à enregistrer. Cliquez sur Enregistrer dans le fichier.
4. Allez l'emplacement où vous souhaitez enregistrer le fichier. Cliquez sur Enregistrer.

Pour supprimer un fichier de sauvegarde de dispositif de CC-SG :

1. Cliquez sur l'onglet Dispositifs et sélectionnez un dispositif.
2. Choisissez Dispositifs > Gestionnaire des dispositifs > Configuration > Restaurer.
3. Sélectionnez le fichier de sauvegarde à supprimer. Cliquez sur Supprimer.
4. Cliquez sur Oui pour confirmer.

Pour télécharger un fichier de sauvegarde de dispositif vers CC-SG :

1. Cliquez sur l'onglet Dispositifs et sélectionnez un dispositif.
2. Choisissez Dispositifs > Gestionnaire des dispositifs > Configuration > Restaurer.
3. Cliquez sur Télécharger vers le serveur. Recherchez et sélectionnez le fichier de sauvegarde du dispositif. Son extension est .rfp. Cliquez sur Ouvrir.

   Le fichier de sauvegarde de dispositif est téléchargé vers CC-SG et apparaît sur la page.

Copie de la configuration d'un dispositif

Les types de dispositifs suivants vous permettent de copier des configurations d'un dispositif à un autre ou à plusieurs autres.

- SX
- KX2
- KSX2
- KX2-101

La configuration peut être copiée uniquement entre les mêmes modèles comportant un nombre identique de ports. Par exemple, vous pouvez copier la configuration d'un dispositif KX2-864 vers d'autres unités KX2-864 uniquement.

La commande Copier la configuration copie toutes les données de configuration (paramètres du dispositif, données d'utilisateur et de groupe d'utilisateurs) à l'exception des paramètres réseau (paquet personnalisé).

Pour copier la configuration d'un dispositif :

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. Sélectionner la méthode de copie de configuration.
   - Pour copier les données de configuration actuelles, sélectionnez Copier depuis le dispositif.
   - Pour copier les données de configuration dans un fichier de sauvegarde enregistré auparavant sur CC-SG, sélectionnez Copier depuis le fichier de sauvegarde, puis le fichier dans la liste déroulante. Lorsqu'aucun fichier de sauvegarde n'est disponible, cette option est désactivée.
4. Cliquez sur la flèche déroulante Groupe de dispositifs et sélectionnez un groupe dans la liste. Tous les dispositifs du groupe sélectionné s'affichent dans la colonne Disponible.
5. Mettez en surbrillance les dispositifs vers lesquels vous souhaitez copier la configuration dans la colonne Disponible et cliquez sur la flèche droite pour les déplacer vers la colonne Sélectionné. La flèche gauche retire les dispositifs activés de la colonne Sélectionné.
6. Cliquez sur OK pour copier la configuration vers les dispositifs de la colonne Sélectionné.

7. 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 d'un dispositif

La fonction Redémarrer le dispositif permet de redémarrer un dispositif.

Pour 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 à un dispositif

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

Pour envoyer une commande ping à un dispositif :

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 d'un dispositif par CC-SG

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

Pour suspendre la gestion d'un dispositif par 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.

Pour reprendre la gestion par CC-SG d'un dispositif suspendu :

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.

Pour afficher le gestionnaire d'alimentation des dispositifs :

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.

Lancement de la page administrative d'un dispositif

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

Pour lancer la page administrative d'un dispositif :

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.

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).

Pour déconnecter les utilisateurs d'un dispositif :

1. Cliquez sur l'onglet Dispositifs et sélectionnez le dispositif dont vous souhaitez déconnecter les 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 à partir de CC-SG :

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 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 137).

Vue d'ensemble des groupes de dispositifs

Les groupes de dispositifs permettent d'organiser les dispositifs dans un ensemble. Le groupe sert de base à une stratégie autorisant ou refusant l'accès à cet ensemble particulier de dispositifs. Reportez-vous à ***Ajout d'une stratégie*** (à la page 138). Les dispositifs peuvent être groupés manuellement, par la méthode Sélectionner, ou en créant une expression booléenne décrivant un ensemble d'attributs communs, par la méthode Décrire.

Si vous avez utilisé Paramétrage guidé pour créer des catégories et des éléments pour les nœuds, certaines formes d'organisation des dispositifs 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, catégories et éléments*** (à la page 23) pour plus d'informations sur la création des catégories et des éléments.

Pour afficher des groupes de dispositifs :

- Choisissez Associations > Groupes de dispositifs. La fenêtre Gestionnaire des groupes de dispositifs apparaît. La liste des groupes de dispositifs existants s'affiche sur la gauche, tandis que les informations relatives au groupe de dispositifs sélectionné apparaissent dans le panneau principal.
  - La liste des groupes de dispositifs existants est affichée sur la gauche. Cliquez sur un groupe de dispositifs pour afficher les informations le concernant dans le Gestionnaire des groupes de dispositifs.
  - Si le groupe a été formé arbitrairement, l'onglet Sélectionner les dispositifs est affiché. Il présente une liste des dispositifs 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 dispositifs apparaît. Il présente les règles régissant la sélection des dispositifs du groupe.
  - Pour rechercher un dispositifs dans la liste du groupe, entrez une chaîne dans le champ de recherche au bas de la liste, puis cliquez sur Rechercher. La méthode de recherche est configurée dans l'écran Mon profil. Reportez-vous à ***Utilisateurs et groupes d'utilisateurs*** (à la page 123).

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

- Choisissez Rapports > Dispositifs > Données des groupes de dispositifs. Une liste des groupes de dispositifs existants s'affiche. Double-cliquez sur une ligne pour afficher les dispositifs d'un groupe.

Ajouter un groupe de dispositifs

Pour 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 353) 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.

Pour ajouter un groupe de dispositifs à l'aide de l'option Sélectionner les dispositifs :

1. Cliquez sur l'onglet Sélectionner les dispositifs dans le panneau Groupe de dispositifs : Nouveau.
2. 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, choisissez 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.

3. 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.
4. Pour ajouter un autre groupe de dispositifs, cliquez sur Appliquer pour enregistrer le groupe actif, puis répétez cette procédure. **Facultatif.**
5. Une fois l'ajout des groupes de dispositifs terminé, cliquez sur OK pour enregistrer vos modifications.

Pour ajouter un groupe de dispositifs à l'aide de l'option Décrire les dispositifs :

1. Cliquez sur l'onglet Décrire les dispositifs dans le panneau Groupe de dispositifs : Nouveau. Dans l'onglet Décrire les dispositifs, vous pouvez créer une table de règles décrivant les dispositifs à affecter au groupe.
2. Cliquez sur l'icône Ajouter une nouvelle ligne  pour ajouter une rangée à la table.
3. 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.
   - 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 sont disponibles ici. Si un châssis de lames a été configuré dans le système, une catégorie Châssis du commutateur (Châssis de lames) est disponible par défaut.
   - 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. Il n'est pas modifiable ; il est utilisé pour écrire des descriptions dans le champ Expression abrégée.

4. Pour ajouter une autre règle, cliquez sur l'icône 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.
5. 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, entrez 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 : si 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 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. Pour effectuer cette comparaison en premier, placez-la entre parenthèses : (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.

Remarque : un espace doit être placé avant et après les opérateurs & et |. Sinon, le champ Expression abrégée revient à l'expression par défaut, c'est-à-dire Rule0 & Rule1 & Rule2 etc., lorsque vous supprimez une règle de la table.

- Pour supprimer une ligne de la table, sélectionnez cette ligne, puis cliquez sur l'icône de suppression de ligne  .
- Pour afficher la liste des dispositifs dont les paramètres suivent les règles définies, cliquez sur Affichage des dispositifs.

6. 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.
7. Cliquez sur Affichage des dispositifs pour visualiser les nœuds satisfaisant l'expression. Une fenêtre Dispositifs du groupe de dispositifs Résultats apparaît et présente 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.
8. 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.
9. Pour ajouter un autre groupe de dispositifs, cliquez sur Appliquer pour enregistrer le groupe actif, puis répétez cette procédure. **Facultatif.**
10. Une fois l'ajout des groupes de dispositifs terminé, cliquez sur OK pour enregistrer vos modifications.

Méthode Décrire et méthode Sélectionner

Utilisez la méthode Décrire lorsque vous souhaitez baser votre groupe sur un attribut du nœud ou des dispositifs, tel que les catégories et les éléments. L'avantage de cette méthode réside dans le fait que lorsque vous ajoutez d'autres dispositifs ou nœuds avec les mêmes attributs que ceux décrits, ils seront placés automatiquement dans le groupe.

Utilisez la méthode Sélectionner lorsque vous souhaitez simplement créer manuellement un groupe de nœuds particuliers. Les nouveaux nœuds et dispositifs ajoutés à CC-SG ne sont pas placés automatiquement dans ces groupes. Vous devez les placer vous-même dans le groupe après leur ajout à CC-SG.

Ces deux méthodes ne peuvent pas être combinées.

Lorsqu'un groupe est créé avec une méthode, vous devez utiliser celle-ci pour le modifier. Si vous changez de méthodes, les paramètres actuels du groupe seront remplacés.

Modifier un groupe de dispositifs

Pour 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. Entrez le nouveau nom du groupe de dispositifs dans le champ Nom du groupe. **Facultatif.**
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.
5. Cliquez sur OK pour enregistrer vos modifications.

Supprimer un groupe de dispositifs

Pour 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

Il existe deux manières de configurer la gestion de l'alimentation à l'aide de barrettes d'alimentation dans CC-SG.

1. Toutes les barrettes de la marque Raritan prises en charge peuvent être connectées à un autre dispositif Raritan et ajoutées à CC-SG comme dispositif Powerstrip. Les barrettes d'alimentation Raritan comprennent les barrettes Dominion PX et RPC. Consultez la matrice de compatibilité pour obtenir la liste des versions prises en charge. Pour configurer ce type de barrettes d'alimentation gérées dans CC-SG, vous devez savoir à quel dispositif Raritan elles sont physiquement connectées. Reportez-vous à ***Configuration de barrettes d'alimentation gérées par un autre dispositif dans CC-SG*** (à la page 72).
2. Les barrettes d'alimentation Dominion PX peuvent être connectées directement au réseau IP et ajoutées à CC-SG comme dispositifs PX. Si des barrettes PX sont connectées directement au réseau IP, elles n'ont pas besoin d'être connectées à un autre dispositif Raritan.

Avec les deux méthodes, vous devez ajouter des interfaces de barrettes d'alimentation gérées à des nœuds afin de créer des associations d'alimentation entre les prises et les nœuds qu'elles alimentent. Reportez-vous à ***Interfaces de connexions par barrettes d'alimentation gérées*** (voir "Interfaces des connexions par barrettes d'alimentation gérées" à la page 108).

Remarque concernant Dominion PX

Quelle que soit la méthode choisie pour configurer une unité PX, vous devez configurer toutes les associations d'alimentation avec la même méthode, c'est-à-dire comme barrette d'alimentation du dispositif géré ou comme dispositif PX, mais non les deux.

De plus, vous pouvez connecter l'unité PX à un dispositif de gestion et configurer les associations d'alimentation, et également relier la même unité PX au réseau IP afin d'utiliser le client Web PX pour afficher et rassembler des données concernant l'alimentation. Reportez-vous au **manuel d'utilisation de Dominion PX** de Raritan, figurant dans la section Support du site Web de Raritan sous Firmware and Documentation.

Dans ce chapitre

Configuration de barrettes d'alimentation gérées par un autre dispositif dans CC-SG

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

- Dominion KX
- Dominion KX2
- Dominion KX2-101
- Dominion SX 3.0
- Dominion SX 3.1
- Dominion KSX
- Dominion KSX2
- Paragon II/Paragon II System Controller (P2SC)

Vous devez savoir à quel dispositif Raritan la barrette d'alimentation gérée est connectée physiquement.

Remarque : une barrette d'alimentation Dominion PX peut également être connectée à votre réseau IP, mais à aucun autre dispositif Raritan. Reportez-vous à **Barrettes d'alimentation gérées** *(à la page 70) pour en savoir plus sur la configuration de la gestion de l'alimentation pour ces barrettes.*

Pour configurer des barrettes d'alimentation gérées 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, KX2-101, KSX2 et P2SC*** (à la page 73)
   - ***Configuration des barrettes d'alimentation connectées à des dispositifs SX 3.0 et KSX*** (à la page 74)
   - ***Configuration des barrettes d'alimentation connectées à un dispositif SX 3.1*** (à la page 76).
3. Configurez des prises. Reportez-vous à ***Configuration des prises d'une barrette d'alimentation*** (à la page 78).

4. Associez chaque prise au nœud qu'elle alimente. Reportez-vous à ***Interfaces de connexions par barrettes d'alimentation gérées*** (voir "Interfaces des connexions par barrettes d'alimentation gérées" à la page 108).

Configuration des barrettes d'alimentation connectées à des dispositifs KX, KX2, KX2-101, KSX2 et P2SC

CC-SG détecte automatiquement les barrettes d'alimentation connectées à des dispositifs KX, KX2, KX2-101, KSX2 et P2SC. Vous pouvez effectuer les tâches suivantes dans CC-SG pour configurer et gérer des barrettes d'alimentation connectées à ces dispositifs.

- ***Ajouter un dispositif PowerStrip connecté à un dispositif KX, KX2, KX2-101, KSX2 ou P2SC*** (à la page 73)
- ***Déplacer une barrette d'alimentation de KX, KX2, KX2-101, KSX2 ou P2SC vers un port différent*** (à la page 74)
- ***Supprimer une barrette d'alimentation connectée à un dispositif KX, KX2, KX2-101, KSX2 ou P2SC*** (à la page 74)

Ajouter un dispositif PowerStrip connecté à un dispositif KX, KX2, KX2-101, KSX2 ou P2SC

Lorsque vous ajoutez à CC-SG un dispositif KX, KX2, KX2-101, KSX2 ou P2SC connecté à une barrette d'alimentation, celle-ci est ajoutée automatiquement. Elle apparaît dans l'onglet Dispositifs, sous le dispositif auquel elle est connectée.

Etapes suivantes :

1. Configurez des prises. Reportez-vous à ***Configuration des prises d'une barrette d'alimentation*** (à la page 78).
2. Associez chaque prise au nœud qu'elle alimente. Reportez-vous à ***Interfaces de connexions par barrettes d'alimentation gérées*** (voir "Interfaces des connexions par barrettes d'alimentation gérées" à la page 108).

Déplacer une barrette d'alimentation de KX, KX2, KX2-101, KSX2 ou P2SC vers un port différent

Lorsque vous déplacez physiquement une barrette d'alimentation d'un dispositif ou port KX, KX2, KX2-101, KSX2 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 ***manuel d'utilisation de P2SC de Raritan****.*

Supprimer une barrette d'alimentation connectée à un dispositif KX, KX2, KX2-101, KSX2 ou P2SC

Vous ne pouvez pas supprimer une barrette d'alimentation connectée à un dispositif KX, KX2, KX2-101, KSX2 ou P2SC de CC-SG. Vous devez déconnecter physiquement la barrette d'alimentation du dispositif 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*** (à la page 74)
- ***Supprimer une barrette d'alimentation connectée à un dispositif SX 3.0 ou KSX*** (à la page 76)
- ***Modifier une association de dispositif ou de port d'une barrette d'alimentation (SX 3.0, KSX)*** (à la page 76)

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. Reportez-vous à ***Ajouter un dispositif KVM ou série*** (à la page 35).

2. Choisissez Dispositifs > Gestionnaire des dispositifs > Ajouter un dispositif.
3. Cliquez sur le menu déroulant Type de dispositif et sélectionnez PowerStrip.
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. Entrez une brève description de cette barrette d'alimentation dans le champ Description. **Facultatif.**
9. 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. Reportez-vous à ***Configuration des prises d'une barrette d'alimentation*** (à la page 78). **Facultatif.**
10. Pour chaque catégorie répertoriée, cliquez sur le menu déroulant Elément, puis sélectionnez l'élément que vous souhaitez appliquer au dispositif. Sélectionnez l'élément vide du champ Elément lorsque vous ne souhaitez pas utiliser une catégorie. Reportez-vous à ***Associations, catégories et éléments*** (à la page 23). **Facultatif.**
11. Une fois la configuration de la barrette d'alimentation terminée, cliquez sur Appliquer pour ajouter ce dispositif et ouvrir un nouvel écran Ajouter un dispositif vide qui vous permet de continuer à ajouter des dispositifs, ou cliquez sur OK pour ajouter cette barrette sans passer à un nouvel écran Ajouter un dispositif.

Etapes suivantes :

1. Configurez des prises. Reportez-vous à ***Configuration des prises d'une barrette d'alimentation*** (à la page 78).
2. Associez chaque prise au nœud qu'elle alimente. Reportez-vous à ***Interfaces de connexions par barrettes d'alimentation gérées*** (voir "Interfaces des connexions par barrettes d'alimentation gérées" à la page 108).

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

Vous pouvez supprimer visuellement une barrette d'alimentation connectée à un dispositif SX 3.0, KSX ou P2SC même si elle est toujours physiquement présente. Si vous déconnectez physiquement 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. Dans 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. Sous l'onglet Dispositifs, sélectionnez la barrette d'alimentation qui a été déplacée.
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 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 une barrette d'alimentation connectée à un dispositif SX 3.1*** (à la page 77)
- ***Déplacer la barrette d'alimentation d'un dispositif SX 3.1 vers un port différent*** (à la page 78)
- ***Supprimer une barrette d'alimentation connectée à un dispositif SX 3.1*** (à la page 78)

Ajouter une barrette d'alimentation connectée 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. Reportez-vous à ***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 :

1. Ajoutez le dispositif SX 3.1 à CC-SG. Reportez-vous à ***Ajouter un dispositif KVM ou série*** (à la page 35).
2. Configurez les ports du dispositif SX 3.1. Reportez-vous à ***Configuration de ports*** (à la page 40).
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 de la souris, 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. Reportez-vous à ***Configuration des prises d'une barrette d'alimentation*** (à la page 78).
2. Associez chaque prise au nœud qu'elle alimente. Reportez-vous à ***Interfaces de connexions par barrettes d'alimentation gérées*** (voir "Interfaces des connexions par barrettes d'alimentation gérées" à la page 108).

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 et l'ajouter au nouveau port SX 3.1. Reportez-vous à ***Supprimer une barrette d'alimentation connectée à un dispositif SX 3.1*** (à la page 78) et ***Ajouter une barrette d'alimentation connectée à un dispositif SX 3.1*** (à la page 77).

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

Vous pouvez supprimer visuellement une barrette d'alimentation connectée à un dispositif SX 3.1 même si elle est toujours connectée physiquement. Si vous déconnectez physiquement 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.

Pour supprimer une barrette d'alimentation connectée à un dispositif SX 3.1 :

1. Dans 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

Avant d'associer des prises de barrettes d'alimentation à des nœuds, vous devez configurer ces prises en ajoutant une interface de barrettes d'alimentation gérées au nœud. Reportez-vous à ***Interfaces pour connexions par barrette d'alimentation gérée*** (voir "Interfaces des connexions par barrettes d'alimentation gérées" à la page 108).

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.
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.
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.
2. Cliquez sur le + en regard de la barrette d'alimentation.
3. Choisissez Dispositifs > Gestionnaire des ports > Supprimer les 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** de Raritan pour plus d'informations sur la connexion aux nœuds.

Dans ce chapitre

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. 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 à tout moment.

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 353) 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 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 disposer de plusieurs interfaces, mais d'une seule 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.

Certaines interfaces fonctionnent uniquement en mode Direct même si vous configurez CC-SG pour fonctionner en mode Proxy. Ces interfaces comprennent ILO, RDP, DRAC, Navigateur Web et VMware Viewer. Reportez-vous à ***A propos des modes de connexion*** (à la page 213).

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 pour dispositifs et nœuds*** (à la page 142) pour en savoir plus sur les divers modes d'affichage de l'onglet Nœuds.

Profil du nœud

Cliquez sur un nœud dans l'onglet Nœuds pour ouvrir la page Profil du nœud. Celle-ci comprend des onglets présentant des informations sur le nœud.

Onglet Interfaces

L'onglet Interfaces contient toutes les interfaces du nœud. Vous pouvez ajouter, modifier et supprimer des interfaces dans cet onglet, et sélectionner l'interface par défaut. Les nœuds prenant en charge le support virtuel comportent une colonne supplémentaire indiquant si l'option Support virtuel est activée.

Onglet Associations

L'onglet Associations contient la totalité des catégories et éléments affectés au nœud. Vous pouvez modifier les associations en effectuant des sélections différentes.

Reportez-vous à ***Associations, catégories et éléments*** (à la page 23).

Onglet Emplacement et contacts

L'onglet Emplacement et contacts contient des informations sur l'emplacement et les contacts d'un nœud, tels que des numéros de téléphone, dont vous pouvez avoir besoin lors du travail sur un nœud. Vous pouvez modifier les champs en entrant de nouvelles informations.

Reportez-vous à ***Ajout d'un emplacement et de contacts à un profil de nœud*** (à la page 91).

Onglet Notes

L'onglet Notes contient un outil permettant à un utilisateur de laisser des notes concernant un dispositif à l'intention d'autres utilisateurs. Toutes les notes apparaissent dans l'onglet avec la date, le nom d'utilisateur et l'adresse IP de leur auteur.

Si vous disposez du privilège Device, Port, and Node Management (gestion des dispositifs, des ports et des nœuds), vous pouvez effacer toutes les notes du profil du nœud. Cliquez sur le bouton Effacer.

Reportez-vous à ***Ajout de notes à un profil de nœud*** (à la page 91).

Onglet Audit

Les motifs d'accès à un nœud apparaissent dans l'onglet Audit. Les utilisateurs doivent entrer un motif d'accès avant la connexion à un nœud si l'audit des nœuds a été activé pour le groupe d'utilisateurs.

L'onglet Audit est masqué si la fonction est désactivée, ou si aucun motif d'accès n'a été entré.

Reportez-vous à ***Configuration de l'audit des accès pour des groupes d'utilisateurs*** (voir "Configuration de l'audit des accès des groupes d'utilisateurs" à la page 129).

Onglet Données de système de contrôle

Les nœuds de serveur de système de contrôle, tels que Virtual Center de VMware, comprennent l'onglet Données de système de contrôle. Celui-ci contient des informations du serveur de système de contrôle qui est mis à jour lorsque l'onglet est ouvert. Vous pouvez accéder à une vue topologique de l'infrastructure virtuelle, effectuer un lien vers des profils de nœuds associés ou vous connecter au système de contrôle et ouvrir l'onglet Résumé.

Onglet Données d'hôte virtuel

Les nœuds d'hôte virtuel, tels que les serveurs ESX de VMware, comprennent l'onglet Données d'hôte virtuel. Celui-ci contient des informations du serveur d'hôte virtuel mises à jour lorsque l'onglet est ouvert. Vous pouvez accéder à une vue topologique de l'infrastructure virtuelle, effectuer un lien vers des profils de nœuds associés ou vous connecter à l'hôte virtuel et ouvrir l'onglet Résumé. Si vous disposez du privilège Device, Port, and Node Management (gestion des dispositifs, des ports et des nœuds), vous pouvez réamorcer le serveur d'hôte virtuel et forcer son réamorçage.

Onglet Données de machine virtuelle

Les nœuds de machine virtuelle, tels que les machines virtuelles de VMware, comprennent l'onglet Données de machine virtuelle. Celui-ci contient des informations de la machine virtuelle mises à jour lorsque l'onglet est ouvert. Vous pouvez accéder à une vue topologique de l'infrastructure virtuelle, effectuer un lien vers des profils de nœuds associés ou vous connecter à l'hôte virtuel et ouvrir l'onglet Résumé.

Onglet Commutateurs (Lames)

Les nœuds de châssis de lames, tels que IBM BladeCenter, comportent l'onglet Commutateurs (Lames). Cet onglet contient des données concernant les serveurs lames résidant dans le châssis de lames.

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.

Comptes de service

Vue d'ensemble des comptes de service

Les comptes de service sont des références de connexion particulières que vous pouvez affecter à plusieurs interfaces. Vous pouvez gagner du temps en affectant un compte de service à un ensemble d'interfaces qui requièrent souvent un changement de mot de passe. Vous pouvez mettre à jour les références de connexion dans le compte de service et la modification est reportée dans toutes les interfaces qui utilisent ce compte.

Les comptes de service ne peuvent pas être utilisés pour les interfaces hors bande ou de barrettes d'alimentation gérées.

- Pour les interfaces DRAC, iLO et RSA, les références de connexion s'appliquent à la carte de processeur intégrée, non au système d'exploitation sous-jacent.
- Pour les interfaces RDP, SSH et Telnet, les références de connexion s'appliquent au système d'exploitation.
- Pour les interfaces VNC, les références de connexion s'appliquent au serveur VNC.
- Pour les interfaces Navigateur Web, les références de connexion s'appliquent au formulaire disponible à l'URL définie dans l'interface.

Pour afficher les comptes de service :

- Choisissez Nœuds > Comptes de service. La page Comptes de service s'ouvre.
- Cliquez sur un en-tête de colonne pour trier la table par cet attribut dans l'ordre croissant. Cliquez de nouveau sur l'en-tête pour trier la table dans l'ordre décroissant. **Facultatif.**

Champ	Description
Nom du compte de service	Ce nom permet d'identifier le compte de service dans les boîtes de dialogue de l'interface et sur la page Attribuer les comptes de service.
Nom d'utilisateur	Ce nom d'utilisateur est employé dans les références de connexion lorsque le compte de service est affecté à une interface.
Mot de passe	Ce mot de passe est utilisé dans les références de connexion lorsque le compte de service est affecté à une interface.
Mot de passe de confirmation	Ce champ permet de s'assurer que le mot de passe est entré correctement.
Description	Cette description peut contenir les informations supplémentaires que vous souhaitez ajouter à propos du compte de service.

Ajouter, modifier et supprimer des comptes de service

Pour ajouter un compte de service :

1. Choisissez Nœuds > Comptes de service. La page Comptes de service s'ouvre.
2. Cliquez sur l'icône Ajouter une nouvelle ligne  pour ajouter une rangée à la table.
3. Renseignez le champ Nom du compte de service.
4. Renseignez le champ Nom d'utilisateur.
5. Renseignez le champ Mot de passe.
6. Entrez à nouveau le mot de passe dans le champ Mot de passe de confirmation.
7. Entrez une description du compte de service dans le champ Description.
8. Cliquez sur OK.

Pour modifier un compte de service :

1. Choisissez Nœuds > Comptes de service. La page Comptes de service s'ouvre.
2. Recherchez le compte de service que vous souhaitez modifier.
3. Modifiez les champs. Vous ne pouvez pas changer le nom du compte de service.

Remarque : CC-SG met à jour toutes les interfaces associées au compte de service pour leur permettre d'utiliser les nouvelles références de connexion lorsque vous modifiez le nom d'utilisateur ou le mot de passe.

4. Cliquez sur OK.

Pour supprimer un compte de service :

1. Choisissez Nœuds > Comptes de service. La page Comptes de service s'ouvre.
2. Sélectionnez le compte de service à supprimer.
3. Cliquez sur le bouton Supprimer la ligne. 
4. Cliquez sur OK.

Modifier le mot de passe d'un compte de service

Pour modifier le mot de passe d'un compte de service :

1. Choisissez Nœuds > Comptes de service. La page Comptes de service s'ouvre.
2. Recherchez le compte de service dont vous souhaitez modifier le mot de passe.
3. Entrez le nouveau mot de passe dans le champ Mot de passe.
4. Entrez à nouveau le mot de passe dans le champ Mot de passe de confirmation.
5. Cliquez sur OK.

Remarque : CC-SG met à jour toutes les interfaces associées au compte de service pour leur permettre d'utiliser les nouvelles références de connexion lorsque vous modifiez le nom d'utilisateur ou le mot de passe.

Affecter des comptes de service à des interfaces

Vous pouvez affecter un compte de service à plusieurs interfaces. Chaque interface associée au compte de service utilise les mêmes données de connexion.

CC-SG met à jour toutes les interfaces associées au compte de service pour leur permettre d'utiliser les nouvelles références de connexion lorsque vous modifiez le nom d'utilisateur ou le mot de passe.

Vous pouvez également sélectionner un compte de service lorsque vous configurez une interface. Reportez-vous à ***Ajout, modification et suppression d'interfaces*** (à la page 105).

Vous devez disposer du privilège Device, Port, and Node Management (gestion des dispositifs, des ports et des nœuds) pour affecter des comptes de service à des interfaces. Reportez-vous à ***Ajout, modification et suppression de groupes d'utilisateurs*** (voir "Ajout, modification et suppression des groupes d'utilisateurs" à la page 126).

Pour affecter un compte de service à des interfaces :

1. Choisissez Nœuds > Attribuer les comptes de service. La page Attribuer les comptes de service s'ouvre.
2. Dans le champ Nom du compte de service, sélectionnez le compte de service que vous souhaitez affecter aux nœuds.
3. Dans la liste Disponible, sélectionnez les interfaces auxquelles vous souhaitez affecter le compte de service. Appuyez sur la touche Ctrl ou Maj tout en cliquant pour sélectionner plusieurs interfaces en même temps.

   *Conseil : entrez le nom d'un nœud dans le champ de recherche pour le mettre en surbrillance dans la liste. Tapez * après un nom partiel pour mettre en surbrillance tous les noms similaires de la liste.*

   Cliquez sur les en-têtes de colonne pour trier les listes dans l'ordre alphabétique.
4. Cliquez sur Ajouter pour placer les interfaces sélectionnées dans la liste Sélectionné.
5. Cliquez sur OK. Le compte de service est affecté à tous les nœuds de la liste Sélectionné.

Remarque : CC-SG met à jour toutes les interfaces associées au compte de service pour leur permettre d'utiliser les nouvelles références de connexion lorsque vous modifiez le nom d'utilisateur ou le mot de passe.

Ajout, modification et suppression de nœuds

Ajouter 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 353) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
4. Entrez une brève description de ce nœud dans le champ Description. **Facultatif.**
5. Vous devez configurer au moins une interface. Cliquez sur Ajouter dans la zone Interfaces de l'écran Ajouter un nœud pour ajouter une interface. Reportez-vous à ***Ajouter une interface*** (à la page 105).
6. Une liste de catégories et d'éléments peut être configurée pour décrire et organiser le nœud de façon optimale. Reportez-vous à ***Associations, catégories et éléments*** (à la page 23). **Facultatif.**
   - Pour chaque catégorie répertoriée, cliquez sur le menu déroulant Elément, puis sélectionnez dans la liste l'élément que vous souhaitez appliquer au nœud.

   Remarque : par défaut, CC-SG laisse les noms de catégories par défaut « System Type » et « US States and territories » en anglais.

   - 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 les ajouter via le menu Associations. Reportez-vous à ***Associations, catégories et éléments*** (à la page 23).
7. Cliquez sur OK pour enregistrer vos modifications. Le nœud sera ajouté à la liste.

Important : Si vous déplacez un châssis de lames d'un port KX II à un autre, les interfaces ajoutées au nœud du châssis dans CC-SG seront perdues dans ce dernier. Toutes les autres informations seront conservées.

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 353).

Modifier 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.
3. Cliquez sur OK pour enregistrer vos modifications.

Remarque : La modification du nom de nœud d'un châssis de lames ne change pas le nom du châssis. Pour modifier le nom du châssis, vous devez utiliser l'écran Profil du dispositif. Reportez-vous à **Modifier un dispositif de châssis de lames** *(à la page 49).*

Supprimer 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.

Ajout d'un emplacement et de contacts à un profil de nœud

Entrez des détails concernant l'emplacement du nœud et les coordonnées de ceux qui administrent ou utilisent le nœud.

Pour ajouter un emplacement et des contacts à un profil de nœud :

1. Sélectionnez un nœud dans l'onglet Nœuds. La page Profil du nœud s'ouvre.
2. Cliquez sur l'onglet Emplacement &Contacts.
3. Entrez des renseignements sur l'emplacement.
   - Service : 64 caractères au maximum.
   - Site : 64 caractères au maximum.
   - Emplacement : 128 caractères au maximum.
4. Entrez des renseignements sur les contacts.
   - Nom de la personne principale à contacter et Nom de la personne secondaire à contacter : 64 caractères au maximum.
   - Numéro de téléphone et de mobile : 32 caractères au maximum.
5. Cliquez sur OK pour enregistrer vos modifications.

Ajout de notes à un profil de nœud

L'onglet Notes vous permet d'ajouter des notes sur un nœud à l'attention d'autres utilisateurs. Toutes les notes apparaissent dans l'onglet avec la date, le nom d'utilisateur et l'adresse IP de leur auteur.

Si vous disposez du privilège Device, Port, and Node Management (gestion des dispositifs, des ports et des nœuds), vous pouvez effacer toutes les notes qui s'affichent dans l'onglet Notes.

Pour ajouter des notes au profil du nœud :

1. Sélectionnez un nœud dans l'onglet Nœuds. La page Profil du nœud s'ouvre.
2. Cliquez sur l'onglet Notes.
3. Tapez votre note dans le champ Nouvelle note.
4. Cliquez sur Ajouter. Votre note apparaît dans la liste Notes.

Pour effacer toutes les notes :

1. Cliquez sur l'onglet Notes.
2. Cliquez sur Effacer les notes.

3. Cliquez sur Oui pour confirmer. Toutes les notes sont supprimées de l'onglet Notes.

Configuration de l'infrastructure virtuelle dans CC-SG

Terminologie de l'infrastructure virtuelle

CC-SG utilise la terminologie suivante pour les composants de l'infrastructure virtuelle.

Terme	Définition	Exemple
Système de contrôle	Serveur de gestion. Le système de contrôle gère un ou plusieurs hôtes virtuels.	Centre virtuel VMware
Hôte virtuel	Matériel physique contenant une ou plusieurs machines virtuelles.	ESX VMware
Machine virtuelle	« Serveur » virtuel résidant sur un hôte virtuel. Une machine virtuelle peut être déplacée d'un hôte virtuel à un autre.	Machine virtuelle VMware ou VM
Interface VI Client	Les nœuds du système de contrôle de l'hôte virtuel utilisent une interface VI Client qui permet d'accéder à l'application client de l'infrastructure du système de virtualisation.	Accès Web à l'infrastructure virtuelle VMware
Interface du visualiseur VMW	Les nœuds de la machine virtuelle disposent d'une interface du visualiseur VMW qui permet d'accéder à l'application du visualiseur de la machine virtuelle.	Console à distance de la machine virtuelle VMware
Interface d'alimentation VMW	Les nœuds de la machine virtuelle disposent d'une interface d'alimentation VMW qui permet de gérer l'alimentation du nœud via CC-SG.	S/O

Vue d'ensemble des nœuds virtuels

Vous pouvez configurer votre infrastructure virtuelle pour l'accès à CC-SG. La page Virtualisation offre deux outils assistants, l'assistant Ajouter un système de contrôle et l'assistant Ajouter un hôte virtuel, qui vous aident à ajouter des systèmes de contrôle, des hôtes virtuels et leurs machines virtuelles correctement.

Une fois la configuration terminée, tous les systèmes de contrôle, hôtes virtuels et machines virtuelles sont accessibles sous forme de nœuds dans CC-SG. Chaque type de nœud virtuel est configuré avec une interface d'accès et une autre d'alimentation.

- Les nœuds de système de contrôle et d'hôte virtuel sont configurés avec une interface VI Client. Celle-ci permet d'accéder au client d'infrastructure du système de virtualisation. Pour les centres de contrôle VMware, l'interface VI Client permet d'accéder au serveur de centre de contrôle via l'accès Web à l'infrastructure virtuelle VMware. Pour les serveurs ESX VMware, l'interface VI Client permet d'accéder au serveur ESX via l'accès Web à l'infrastructure virtuelle VMware.
- Les nœuds de machine virtuelle sont configurés avec une interface du visualiseur VMW et une interface d'alimentation VMW. L'interface du visualiseur VMW permet d'accéder à l'application du visualiseur de la machine virtuelle. Pour les machines virtuelles VMware, l'interface du visualiseur VMW permet d'accéder à la console à distance de la machine virtuelle. L'interface d'alimentation VMW permet de gérer l'alimentation du nœud via CC-SG.

Ajouter un système de contrôle comprenant des hôtes et des machines virtuels

Lorsque vous ajoutez un système de contrôle, un assistant vous aide à ajouter les hôtes et machines virtuels inclus dans ce système.

Pour ajouter un système de contrôle comprenant des hôtes et machines virtuels :

1. Choisissez Nœuds > Virtualisation.
2. Cliquez sur Ajouter un système de contrôle.
3. Nom d'hôte/Adresse IP : entrez l'adresse IP ou le nom d'hôte du système de contrôle. 64 caractères au maximum.
4. Protocole de connexion : définissez des communications HTTP ou HTTPS entre le système de contrôle et CC-SG.
5. Port TCP : indiquez le port TCP. Le port par défaut est 443.
6. Intervalle de vérification (en secondes) : entrez la durée en secondes qui doit s'écouler avant expiration entre le système de contrôle et CC-SG.

7. Entrez des informations d'authentification :
   - Pour utiliser un compte de service pour l'authentification, cochez la case Utiliser les informations d'identification du compte de service. Sélectionnez le compte de service à utiliser dans le menu Nom du compte de service.

     ou

   - Entrez un nom d'utilisateur et un mot de passe pour l'authentification. 64 caractères au maximum chacun.
8. Pour autoriser les utilisateurs qui accèdent à ce système de contrôle à se connecter automatiquement à l'interface VI Client, cochez la case Activer la signature unique pour le client VI. **Facultatif.**
9. Cliquez sur Suivant. CC-SG détecte les hôtes et machines virtuels du système de contrôle.
   - Cliquez sur un en-tête de colonne pour trier la table par cet attribut dans l'ordre croissant. Cliquez de nouveau sur l'en-tête pour trier la table dans l'ordre décroissant. **Facultatif.**
10. Ajoutez des machines virtuelles à CC-SG. Un nœud sera créé pour chaque machine virtuelle. Chaque hôte virtuel sera également configuré. Seul un nœud d'hôte virtuel sera ajouté, même si l'hôte virtuel est associé à plusieurs machines virtuelles.
    - Pour ajouter une machine virtuelle :
      - Cochez la case Configurer en regard de la machine virtuelle à ajouter.
      - Pour ajouter une interface VNC, RDP ou SSH au nœud d'hôte virtuel et au nœud de machine virtuelle, cochez les cases en regard de la machine virtuelle. **Facultatif.**
    - Pour ajouter toutes les machines virtuelles :
      - Cochez la case supérieure de la colonne Configurer pour sélectionner toutes les machines virtuelles.
      - Pour ajouter une interface VNC, RDP ou SSH à tous les nœuds d'hôtes virtuels et à tous les nœuds de machines virtuelles, cochez la case supérieure des colonnes VNC, RDP ou SSH. **Facultatif.**
    - Pour ajouter plusieurs machines virtuelles :

- Utilisez Ctrl+clic ou Maj+clic pour sélectionner les machines virtuelles que vous souhaitez ajouter.
- Dans la section Activer/Désactiver les lignes sélectionnées, cochez la case Machine virtuelle.
- Pour ajouter une interface VNC, RDP ou SSH aux nœuds d'hôtes virtuels et aux nœuds de machines virtuelles qui seront créés, cochez les cases VNC, RDP ou SSH dans la section Activer/Désactiver les lignes sélectionnées. **Facultatif.**
- Cliquez sur Activer.

11. Cliquez sur Suivant. CC-SG affiche la liste des types d'interfaces qui seront ajoutés. Vous pouvez ajouter des noms et des références de connexion pour chaque type.
12. Pour chaque type d'interface, entrez un nom et des références de connexion. Ceux-ci seront partagés par toutes les interfaces ajoutées à chaque nœud de machine virtuelle et d'hôte virtuel configurés. **Facultatif.**

Laissez ces champs vides si vous préférez ajouter des noms et des références de connexion à chaque interface individuellement.

L'interface prendra le nom du nœud si le champ est laissé vide.

---

a. Entrez des noms pour les interfaces. 32 caractères au maximum.
   - Interfaces client VI de l'hôte virtuel
   - Interfaces du visualiseur VMware
   - Interfaces d'alimentation virtuelles
   - Interfaces RDP, VNC et SSH, le cas échéant.

b. Entrez des références de connexion, le cas échéant. Certains types d'interface n'ont pas besoin de ces références :
   - Pour utiliser un compte de service, cochez la case Utiliser les informations d'identification du compte de service, puis sélectionnez le nom du compte de service.

   ou

   - Entrez un nom d'utilisateur et un mot de passe pour le type d'interface. 64 caractères au maximum chacun.

13. Cliquez sur OK.

CC-SG crée :

- Un nœud pour chaque machine virtuelle. Chaque nœud de machine virtuelle dispose d'une interface du visualiseur VMW, d'une interface d'alimentation VMW et d'autres interfaces en bande que vous avez définies. Les nœuds de machine virtuelle reprennent le nom de leur machine provenant des systèmes d'hôte virtuel.
- Un nœud pour chaque hôte virtuel. Chaque nœud d'hôte virtuel dispose d'une interface VI Client. Les nœuds d'hôte virtuel sont nommés d'après leur adresse IP ou le nom de l'hôte.
- Un nœud pour le système de contrôle. Chaque nœud de système de contrôle dispose d'une interface VI Client. Les nœuds de système de contrôle sont nommés Centre virtuel VMware.

Ajouter un hôte virtuel comprenant des machines virtuelles

Lorsque vous ajoutez un hôte virtuel, un assistant vous aide à ajouter les machines virtuelles incluses dans cet hôte.

Pour ajouter un hôte virtuel comprenant des machines virtuelles :

1. Choisissez Nœuds > Virtualisation.
2. Cliquez sur Ajouter un hôte virtuel.
3. Choisissez Nœuds > Virtualisation.
4. Cliquez sur Ajouter un hôte virtuel.
5. Nom d'hôte/Adresse IP : entrez l'adresse IP ou le nom d'hôte de l'hôte virtuel. 64 caractères au maximum.
6. Protocole de connexion : définissez des communications HTTP ou HTTPS entre l'hôte virtuel et CC-SG.
7. Port TCP : indiquez le port TCP. Le port par défaut est 443.
8. Intervalle de vérification (en secondes) : entrez la durée en secondes qui doit s'écouler avant expiration entre l'hôte virtuel et CC-SG.
9. Entrez des informations d'authentification :
   - Pour utiliser un compte de service pour l'authentification, cochez la case Utiliser les informations d'identification du compte de service. Sélectionnez le compte de service à utiliser dans le menu Nom du compte de service.

     ou

   - Entrez un nom d'utilisateur et un mot de passe pour l'authentification. 64 caractères au maximum chacun.
10. Pour autoriser les utilisateurs qui accèdent à cet hôte virtuel à se connecter automatiquement à l'interface VI Client, cochez la case Activer la signature unique pour le client VI. **Facultatif.**

11. Cliquez sur Suivant. CC-SG détecte les machines virtuelles de l'hôte virtuel.
    - Cliquez sur un en-tête de colonne pour trier la table par cet attribut dans l'ordre croissant. Cliquez de nouveau sur l'en-tête pour trier la table dans l'ordre décroissant. **Facultatif.**
12. Ajoutez des machines virtuelles à CC-SG. Un nœud sera créé pour chaque machine virtuelle. Chaque hôte virtuel sera également configuré. Seul un nœud d'hôte virtuel sera ajouté, même si l'hôte virtuel est associé à plusieurs machines virtuelles.
    - Pour ajouter une machine virtuelle :
      - Cochez la case Configurer en regard de la machine virtuelle à ajouter.
      - Pour ajouter une interface VNC, RDP ou SSH au nœud d'hôte virtuel et au nœud de machine virtuelle, cochez les cases en regard de la machine virtuelle. **Facultatif.**
    - Pour ajouter toutes les machines virtuelles :
      - Cochez la case supérieure de la colonne Configurer pour sélectionner toutes les machines virtuelles.
      - Pour ajouter une interface VNC, RDP ou SSH à tous les nœuds d'hôtes virtuels et à tous les nœuds de machines virtuelles, cochez la case supérieure des colonnes VNC, RDP ou SSH. **Facultatif.**
    - Pour ajouter plusieurs machines virtuelles :
      - Utilisez Ctrl+clic ou Maj+clic pour sélectionner les machines virtuelles que vous souhaitez ajouter.
      - Dans la section Activer/Désactiver les lignes sélectionnées, cochez la case Machine virtuelle.
      - Pour ajouter une interface VNC, RDP ou SSH aux nœuds d'hôtes virtuels et aux nœuds de machines virtuelles qui seront créés, cochez les cases VNC, RDP ou SSH dans la section Activer/Désactiver les lignes sélectionnées. **Facultatif.**
      - Cliquez sur Activer.
13. Cliquez sur Suivant. CC-SG affiche la liste des types d'interfaces qui seront ajoutés. Vous pouvez ajouter des noms et des références de connexion pour chaque type.
14. Pour chaque type d'interface, entrez un nom et des références de connexion. Ceux-ci seront partagés par toutes les interfaces ajoutées à chaque nœud de machine virtuelle et d'hôte virtuel configurés. **Facultatif.**

Laissez ces champs vides si vous préférez ajouter des noms et des références de connexion à chaque interface individuellement.

L'interface prendra le nom du nœud si le champ est laissé vide.

a. Entrez des noms pour les interfaces. 32 caractères au maximum.
   - Interfaces VI Client
   - Interfaces du visualiseur VMware
   - Interfaces d'alimentation virtuelles
   - Interfaces RDP, VNC et SSH, le cas échéant.

b. Entrez des références de connexion, le cas échéant. Certains types d'interface n'ont pas besoin de ces références :
   - Pour utiliser un compte de service, cochez la case Utiliser les informations d'identification du compte de service, puis sélectionnez le nom du compte de service.

   ou

   - Entrez un nom d'utilisateur et un mot de passe pour le type d'interface. 64 caractères au maximum chacun.

15. Cliquez sur OK.

    CC-SG crée :

    - Un nœud pour chaque machine virtuelle. Chaque nœud de machine virtuelle dispose d'une interface du visualiseur VMW, d'une interface d'alimentation VMW et d'autres interfaces en bande que vous avez définies. Les nœuds de machine virtuelle reprennent le nom de leur machine provenant des systèmes d'hôte virtuel.
    - Un nœud pour chaque hôte virtuel. Chaque nœud d'hôte virtuel dispose d'une interface VI Client. Les nœuds d'hôte virtuel sont nommés d'après leur adresse IP ou le nom de l'hôte.

Modifier les systèmes de contrôle, hôtes virtuels et machines virtuelles

Vous pouvez modifier les systèmes de contrôle, hôtes virtuels et machines virtuelles configurés dans CC-SG afin de changer leurs propriétés. Vous pouvez supprimer des nœuds de machine virtuelle de CC-SG en désactivant la case à cocher Configurer de cette machine.

Pour modifier des systèmes de contrôle, hôtes virtuels et machines virtuelles :

1. Choisissez Nœuds > Virtualisation.
2. Cliquez sur un en-tête de colonne pour trier la table par cet attribut dans l'ordre croissant. Cliquez de nouveau sur l'en-tête pour trier la table dans l'ordre décroissant. **Facultatif.**

3. Sélectionnez le système de contrôle ou l'hôte virtuel que vous souhaitez modifier.
4. Cliquez sur Modifier.
5. Modifiez les données selon vos besoins. Reportez-vous à ***Ajouter un système de contrôle comprenant des hôtes et des machines virtuels*** (à la page 93) et ***Ajouter un hôte virtuel comprenant des machines virtuelles*** (à la page 96) pour obtenir une description complète des champs.
6. Cliquez sur Suivant.
7. Supprimez une ou plusieurs machines virtuelles de CC-SG.
   - Pour supprimer une machine virtuelle, désactivez la case à cocher Configurer.
   - Pour supprimer plusieurs machines virtuelles, utilisez Ctrl+clic ou Maj+clic pour sélectionner plusieurs machines virtuelles. Cochez ensuite la case Machine virtuelle dans la section Activer/Désactiver les lignes sélectionnées, et cliquez sur Désactiver.
8. Pour ajouter des interfaces VNC, RDP ou SSH au nœud d'hôte virtuel et au nœud de machine virtuelle, cochez les cases en regard de chaque machine.

   Vous ne pouvez pas retirer les interfaces SSH, VNC et RDP des nœuds de machine virtuelle ou d'hôte virtuel de cette page. Vous devez supprimer les interfaces du profil de nœud. Reportez-vous à **Supprimer une interface** *(à la page 113).*
9. Cliquez sur Suivant. Si vous décidez de supprimer des machines virtuelles, un message d'alerte s'affiche.
10. Pour chaque type d'interface, entrez un nom et des références de connexion. Ceux-ci seront partagés par toutes les interfaces ajoutées à chaque nœud de machine virtuelle et d'hôte virtuel configurés. **Facultatif.** Vous pouvez laisser ces champs vides si vous préférez ajouter des noms et des références de connexion à chaque interface individuellement.
    a. Entrez des noms pour les interfaces (32 caractères maximum).
       - Interfaces client VI de l'hôte virtuel
       - Interfaces du visualiseur VMware
       - Interfaces d'alimentation virtuelles
       - Interfaces RDP, VNC et SSH, le cas échéant.
    b. Entrez des références de connexion :

- Pour utiliser un compte de service, cochez la case Utiliser les informations d'identification du compte de service, puis sélectionnez le nom du compte de service.

ou

- Entrez un nom d'utilisateur et un mot de passe pour le type d'interface. 64 caractères au maximum chacun.

11. Cliquez sur OK.

Supprimer des systèmes de contrôle et des hôtes virtuels

Vous pouvez supprimer des systèmes de contrôle et des hôtes virtuels de CC-SG.

Lorsque vous supprimez un système de contrôle, les hôtes et machines virtuels qui lui sont associés ne sont pas supprimés.

Lorsque vous supprimez un hôte virtuel, les systèmes de contrôle et machines virtuelles qui lui sont associés ne sont pas supprimés.

Les nœuds de machine virtuelle ne sont pas automatiquement supprimés lorsque les systèmes de contrôles ou les hôtes virtuels qui leur sont associés le sont. Reportez-vous à ***Supprimer un nœud de machine virtuelle*** (à la page 100).

Pour supprimer des systèmes de contrôle et des hôtes virtuels :

1. Choisissez Nœuds > Virtualisation.
2. Sélectionnez dans la liste les systèmes de contrôle et les hôtes virtuels que vous souhaitez supprimer. Appuyez sur la touche Ctrl tout en cliquant pour sélectionner plusieurs éléments.
3. Cliquez sur Supprimer.

Supprimer un nœud de machine virtuelle

Il existe deux manières de supprimer des nœuds de machine virtuelle :

- Utilisez la fonction Supprimer un nœud. Reportez-vous à ***Supprimer un nœud*** (à la page 90).
- Désactivez la case à cocher Configurer pour la machine virtuelle. Reportez-vous à ***Modifier les systèmes de contrôle, hôtes virtuels et machines virtuelles*** (à la page 98).

Supprimer une infrastructure virtuelle

Suivez la procédure ci-après pour supprimer une infrastructure virtuelle entière de CC-SG, système de contrôle, hôtes et machines virtuels compris.

Pour supprimer une infrastructure virtuelle :

1. Supprimez tous les nœuds de machine virtuelle en désactivant la case à cocher Configurer pour chaque machine. Reportez-vous à ***Modifier les systèmes de contrôle, hôtes virtuels et machines virtuelles*** (à la page 98).
2. Supprimez le système de contrôle et les hôtes virtuels. Reportez-vous à ***Supprimer des systèmes de contrôle et des hôtes virtuels*** (à la page 100).

   Tous les composants de l'infrastructure virtuelle sont supprimés : les nœuds de système de contrôle, d'hôte virtuel et de machine virtuelle, et leurs interfaces.

Synchronisation de l'infrastructure virtuelle dans CC-SG

La synchronisation assure que CC-SG dispose d'informations à jour sur votre infrastructure virtuelle. Elle met à jour des informations spécifiques à chaque nœud de machine virtuelle et des données sur la topologie de l'infrastructure.

Vous pouvez configurer une synchronisation quotidienne automatique de tous les systèmes de contrôle et des hôtes virtuels configurés. Vous pouvez également effectuer à tout moment une synchronisation de systèmes de contrôle et d'hôtes virtuels sélectionnés.

Synchroniser l'infrastructure virtuelle

Vous pouvez effectuer une synchronisation de CC-SG avec votre infrastructure virtuelle.

Lorsque vous sélectionnez un système de contrôle à synchroniser, les hôtes virtuels qui lui sont associés seront également synchronisés, que vous les sélectionnez ou non.

Pour synchroniser l'infrastructure virtuelle :

1. Choisissez Nœuds > Virtualisation.
2. Dans la liste de nœuds, sélectionnez les nœuds à synchroniser. Appuyez sur la touche Ctrl tout en cliquant pour sélectionner plusieurs éléments.

3. Cliquez sur Synchroniser. Si l'infrastructure virtuelle a été modifiée depuis la dernière synchronisation, les données sont mises à jour dans CC-SG.
   - La colonne Configuré dans Secure Gateway affiche le nombre de machines ou hôtes virtuels configurés dans CC-SG.
   - La colonne Date de la dernière synchronisation affiche les date et heure de la synchronisation.
   - La colonne Etat de nœud présente le statut du nœud virtuel.

Activer ou désactiver la synchronisation quotidienne de l'infrastructure virtuelle

Vous pouvez configurer une synchronisation automatique de CC-SG avec votre infrastructure virtuelle. Cette synchronisation se produit tous les jours à l'heure spécifiée.

Pour activer la synchronisation quotidienne de l'infrastructure virtuelle :

1. Choisissez Nœuds > Virtualisation.
2. Cochez la case Activer la synchronisation automatique quotidienne.
3. Entrez l'heure à laquelle vous souhaitez lancer la synchronisation quotidienne dans le champ Heure de début.
4. Cliquez sur Mettre à jour.

Pour désactiver la synchronisation quotidienne de l'infrastructure virtuelle :

1. Choisissez Nœuds > Virtualisation.
2. Désactivez la case à cocher Activer la synchronisation automatique quotidienne.
3. Cliquez sur Mettre à jour.

Réamorcer ou forcer le réamorçage d'un nœud d'hôte virtuel

Vous pouvez réamorcer ou forcer le réamorçage d'un serveur d'hôte virtuel. Une opération de réamorçage effectue un redémarrage normal du serveur d'hôte virtuel lorsqu'il est en mode de maintenance. Une opération de réamorçage forcé oblige le serveur d'hôte virtuel à redémarrer même s'il n'est pas en mode de maintenance.

Pour accéder à ces commandes, vous devez disposer des privilèges Node In-Band Access (accès en bande au nœud) et Node Power Control (gestion de l'alimentation des nœuds). Vous devez également appartenir à un groupe d'utilisateurs disposant d'une stratégie d'accès au nœud que vous souhaitez réamorcer ou dont vous souhaitez forcer le réamorçage.

Pour réamorcer ou forcer le réamorçage d'un nœud d'hôte virtuel :

1. Sélectionnez le nœud d'hôte virtuel que vous souhaitez réamorcer ou dont vous souhaitez forcer le réamorçage.
2. Cliquez sur l'onglet Données d'hôte virtuel.
3. Cliquez sur Redémarrer ou sur Forcer le rédémarrage.

Accès à la vue topologique virtuelle

La vue topologique est une arborescence qui présente les relations du système de contrôle, des hôtes et machines virtuels associés au nœud sélectionné.

Vous devez disposer du privilège Device, Port, and Node Management (gestion des dispositifs, des ports et des nœuds) pour ouvrir la vue topologique.

Pour ouvrir la vue topologique à partir du profil du nœud virtuel :

1. Dans le profil du nœud, cliquez sur l'onglet contenant des données de virtualisation sur le nœud : onglet Données de machine virtuelle, Données d'hôte virtuel ou Système de contrôle, suivant le type du nœud.
2. Cliquez sur le lien Vue topologique. La vue topologique s'ouvre dans une nouvelle fenêtre. Les nœuds virtuels configurés dans CC-SG apparaissent sous forme de liens.
   - Double-cliquez sur le lien d'un nœud pour ouvrir le profil du nœud virtuel.
   - Double-cliquez sur le lien d'une interface pour vous connecter au nœud.

- Double-cliquez sur un lien d'interface d'alimentation virtuelle pour ouvrir la page Gestion de l'alimentation pour ce nœud.

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 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.

   ou

   - 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 laquelle vous souhaitez vous connecter ou cliquez avec le bouton droit sur l'interface et sélectionnez 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 auquel vous souhaitez envoyer une commande ping.
2. Choisissez Nœuds > Nœud ping. Le résultat de l'exécution de la commande ping apparaît à l'écran.

Ajout, modification et suppression d'interfaces

Ajouter une interface

Remarque : les interfaces pour nœuds virtuels, tels que le système de contrôle, les hôtes et machines virtuels, peuvent être ajoutées uniquement à l'aide des outils Virtualisation sous Nœuds > Virtualisation. Reportez-vous à **Configuration de l'infrastructure virtuelle dans CC-SG** *(à la page 92).*

Pour ajouter 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'ouvre.

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

   Connexions en bande :

   - 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.

     Reportez-vous à ***Interfaces de connexions en bande*** (à la page 107).

Connexions hors bande :

- 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).

  Reportez-vous à ***Interfaces pour connexions KVM hors bande, série hors bande*** (à la page 107).

Connexions de gestion d'alimentation :

- 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 : 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.

  Reportez-vous à ***Interfaces pour connexions de gestion de l'alimentation par DRAC, RSA et processeur ILO*** (à la page 108) et ***Interfaces pour connexions de gestion d'alimentation IPMI*** (à la page 109).

Connexions par barrettes d'alimentation gérées :

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

  Reportez-vous à ***Interfaces des connexions par barrettes d'alimentation gérées*** (à la page 108).

Connexions par navigateur Web :

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

  Reportez-vous à ***Interface Navigateur Web*** (à la page 110).

3. Un nom par défaut apparaît dans le champ Nom en fonction du type d'interface sélectionné. Vous pouvez le modifier. Ce nom apparaît en regard de l'interface dans la liste des nœuds. Reportez-vous à ***Conventions d'appellation*** (à la page 353) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.

Interfaces de connexions en bande

Les connexions en bande comprennent RDP, VNC, SSH, KVM RSA, KVM processeur iLO, KVM DRAC et TELNET.

Telnet n'est pas une méthode d'accès sécurisé. Tous les noms d'utilisateur, mots de passe et trafic sont transmis en texte clair.

Pour ajouter une interface pour les 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. Entrez un port TCP pour la connexion dans le champ correspondant. **Facultatif.**
3. Pour les interfaces RDP, sélectionnez Console ou Utilisateur distant. Lorsqu'un utilisateur de console accède à un nœud, tous les autres utilisateurs sont déconnectés. Plusieurs utilisateurs distants peuvent accéder à un nœud simultanément.
4. Entrez des informations d'authentification :
   - Pour utiliser un compte de service pour l'authentification, cochez la case Utiliser les informations d'identification du compte de service. Sélectionnez le compte de service à utiliser dans le menu Nom du compte de service.

   ou

   - Entrez un nom d'utilisateur et un mot de passe pour l'authentification. Pour les interfaces VNC, seul un mot de passe est requis.
5. Sélectionnez la présentation de clavier correspondant à votre langue.
6. Entrez une description de cette interface dans le champ Description. **Facultatif.**
7. Cliquez sur OK pour enregistrer vos modifications.

Interfaces pour connexions KVM hors bande, série hors bande

Pour ajouter une interface 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 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. Entrez une description de cette interface dans le champ Description. **Facultatif.**
5. Cliquez sur OK pour enregistrer vos modifications.

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

Pour ajouter une interface pour connexions de gestion de l'alimentation par DRAC, RSA et processeur ILO :

1. Entrez l'adresse IP ou le nom de l'hôte de l'interface dans le champ Adresse IP/nom d'hôte.
2. Entrez un port TCP pour la connexion dans le champ correspondant. **Facultatif.**
3. Entrez des informations d'authentification :
   - Pour utiliser un compte de service pour l'authentification, cochez la case Utiliser les informations d'identification du compte de service. Sélectionnez le compte de service à utiliser dans le menu Nom du compte de service.

   ou

   - Entrez un nom d'utilisateur et un mot de passe pour l'authentification.
4. Entrez une description de cette interface dans le champ Description. **Facultatif.**
5. Cliquez sur OK pour enregistrer vos modifications.

Interfaces des connexions par barrettes d'alimentation gérées

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.

Pour ajouter une interface de connexions par barrettes d'alimentation gérées :

1. Dispositif de gestion :

- Sélectionnez le dispositif Raritan auquel la barrette d'alimentation est connectée. Le dispositif doit être ajouté à CC-SG.

ou

- Sélectionnez Dominion PX si cette interface de gestion d'alimentation utilise un dispositif PX sur le réseau IP qui n'est connecté à aucun autre dispositif Raritan.

2. Port de gestion : sélectionnez le port Raritan auquel la barrette d'alimentation est connectée. Ce champ est désactivé lorsque vous sélectionnez PX comme dispositif de gestion.
3. Nom de la barrette d'alimentation : sélectionnez la barrette ou le dispositif PX alimentant le nœud. La barrette ou le dispositif PX doivent être configurés dans CC-SG pour apparaître dans la liste.
4. Nom de prise : sélectionnez le nom de la prise sur laquelle le nœud est branché. **Facultatif.**
5. Entrez une description de cette interface dans le champ Description.
6. Cliquez sur OK pour enregistrer vos modifications.

Remarque : une interface de barrette d'alimentation gérée peut être ajoutée à un nœud de châssis de lames mais pas à un nœud de serveur lame.

Interfaces pour connexions de gestion d'alimentation IPMI

Pour ajouter une interface 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 des informations d'authentification :

   - Pour utiliser un compte de service pour l'authentification, cochez la case Utiliser les informations d'identification du compte de service. Sélectionnez le compte de service à utiliser dans le menu Nom du compte de service.

   ou

   - Entrez un nom d'utilisateur et un mot de passe pour l'authentification. **Facultatif.**

6. Entrez une description de cette interface dans le champ Description.
7. Cliquez sur OK pour enregistrer vos 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. Reportez-vous à ***Exemple : Ajout d'une interface Navigateur Web à un nœud PX*** (à la page 112). Si vous avez attribué une URL ou une adresse IP à un châssis de lames sur le dispositif KX2, une interface Navigateur Web est ajoutée automatiquement.

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 (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 pas la configuration de DNS.

Pour ajouter une interface navigateur Web :

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 353) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
2. Entrez un port TCP pour la connexion dans le champ correspondant. Si vous utilisez HTTPS dans l'URL, vous devez paramétrer le port TCP sur 443. **Facultatif.**
3. 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 entrer des formats corrects :
   - http(s)://192.168.1.1/login.asp
   - http(s)://www.example.com/cgi/login
   - http(s)://example.com/home.html
4. Entrez des informations d'authentification : **Facultatif.**

- Pour utiliser un compte de service pour l'authentification, cochez la case Utiliser les informations d'identification du compte de service. Sélectionnez le compte de service à utiliser dans le menu Nom du compte de service.

ou

- Entrez un nom d'utilisateur et un mot de passe pour l'authentification. Entrez les nom d'utilisateur et mot de passe autorisant l'accès à cette interface.

Remarque : n'entrez pas d'informations d'authentification pour les applications Web DRAC, ILO et RSA sous peine de voir la connexion échouer.

5. Entrez le nom des champs pour le nom d'utilisateur et le mot de passe utilisés dans l'écran de connexion pour l'application Web dans le champ du nom d'utilisateur et dans le 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. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 111).
6. Entrez une description de cette interface dans le champ Description. **Facultatif.**
7. Cliquez sur OK pour enregistrer vos 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. Reportez-vous à la procédure ci-dessous pour prendre connaissance d'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 : Ajout d'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 : `<DOMINION PX IP ADDRESS>/auth.asp`

Port TCP : 80

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 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 des interfaces apparaît également dans la liste Nœuds, imbriqué sous le nœud auquel elles donnent 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 et sélectionnez le nœud doté de l'interface à modifier. La page Profil du nœud s'ouvre.
2. Dans l'onglet Interfaces, sélectionnez la ligne correspondant à l'interface à modifier.
3. Cliquez sur Modifier.

4. Modifiez les champs selon les besoins. Reportez-vous à ***Ajout d'une interface*** (voir "Ajouter une interface" à la page 105) pour plus d'informations sur les champs. Certains champs sont accessibles en lecture seule.
5. Cliquez sur OK pour enregistrer vos modifications.

Supprimer une interface

Vous pouvez supprimer n'importe quelle interface d'un nœud à l'exception des suivantes :

- une interface VMW Viewer ou VMW Power sur un nœud de machine virtuelle ;
- une interface Navigateur Web sur un châssis de lames à commutateur KVM intégré, associée à une URL ou une adresse IP sur le dispositif KX2.

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, cliquez sur 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.

Ajout d'une interface aux signets

Si vous accédez fréquemment à un nœud 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 Nœuds, sélectionnez l'interface à ajouter aux signets. Vous devez développer le nœud pour visualiser les interfaces.
2. Choisissez Nœuds > Interface nœud 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 Entrée 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 Nœuds, sélectionnez l'interface à ajouter aux signets. Vous devez développer le nœud pour visualiser les interfaces.
2. Choisissez Nœuds > Interface nœud signet.
3. Sélectionnez Ajouter signet (IE uniquement).
4. Un nom par défaut apparaît dans le champ Nom du signet. Vous pouvez modifier le nom qui apparaîtra dans votre liste de Favoris dans Internet Explorer.
5. Cliquez sur OK. La fenêtre Ajout de Favoris s'ouvre.
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.

Pour obtenir des URL de signet pour tous les nœuds :

- Vous pouvez obtenir des URL de signet pour tous les nœuds dans le rapport sur le parc du nœud. Reportez-vous à ***Rapport sur le parc du nœud*** (à la page 180).

Configuration de l'accès par port direct à un nœud

Vous pouvez configurer l'accès par port direct à un nœud à l'aide de la fonction Interface nœud signet.

Reportez-vous à ***Ajout d'une interface aux signets*** (à la page 113).

Copie en bloc pour les associations, emplacements et contacts de nœuds

La commande Copier en bloc permet de copier les catégories, éléments, emplacement et informations de contact d'un nœud vers plusieurs autres nœuds. Notez que les informations sélectionnées constituent la seule propriété copiée lors de cette opération. Lorsque le même type d'informations existe sur certains des nœuds sélectionnés, l'exécution de la commande Copier en bloc REMPLACERA les données existantes par les nouvelles informations attribuées.

Pour copier en bloc des associations, emplacement et informations de contact de nœuds :

1. Cliquez sur l'onglet Nœuds et sélectionnez un nœud.
2. Choisissez Nœuds > Copier en bloc.
3. Dans la liste Nœuds disponibles, sélectionnez les nœuds vers lesquels vous copiez les associations, emplacement et informations de contact du nœud indiqué dans le champ Nom du nœud.
4. Cliquez sur le bouton > pour ajouter un nœud à la liste Nœuds sélectionnés.
5. Sélectionnez le nœud et cliquez sur < pour le retirer de la liste Nœuds sélectionnés.
6. Dans l'onglet Associations, cochez la case Copier les associations de nœuds pour copier tous les éléments et les catégories du nœud.
   - Vous pouvez modifier, ajouter ou supprimer toutes les données de cet onglet. Les données modifiées seront copiées sur plusieurs nœuds dans la liste Nœuds sélectionnés, ainsi que le nœud actuel affiché dans le champ Nom du nœud. **Facultatif.**
7. Dans l'onglet Emplacement et contacts, cochez la case des données que vous souhaitez copier :
   - Cochez la case Copier les informations d'emplacement pour copier les données affichées dans la section Emplacement.
   - Cochez la case Copier les informations de contact pour copier les données affichées dans la section Contacts.
   - Vous pouvez modifier, ajouter ou supprimer toutes les données de cet onglet. Les données modifiées seront copiées sur plusieurs nœuds dans la liste Nœuds sélectionnés, ainsi que le nœud actuel affiché dans le champ Nom du nœud. **Facultatif.**
8. Cliquez sur OK pour copier en bloc. Un message apparaît lorsque les données sélectionnées ont été copiées.

Utilisation de 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.
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.

Ajout, modification et suppression des groupes de nœuds

Vue d'ensemble 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 ***Ajout d'une stratégie*** (à la page 138). Les nœuds peuvent être groupés manuellement, par la méthode Sélectionner, ou en créant une expression booléenne décrivant un ensemble d'attributs communs, par la méthode Décrire.

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, catégories et éléments*** (à la page 23) 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 apparaît. 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 apparaît. 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 Rechercher. La méthode de recherche est configurée dans l'écran Mon profil. Reportez-vous à ***Utilisateurs et groupes d'utilisateurs*** (à la page 123).
  - 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.

Ajouter un groupe de nœuds

Pour ajouter un groupe de nœuds :

1. Choisissez Associations > Groupes de nœuds. La fenêtre Gestionnaire des groupes de nœuds apparaît.
2. Choisissez Groupes > Nouveau. 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 353) 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.

Méthode Décrire et méthode Sélectionner

Utilisez la méthode Décrire lorsque vous souhaitez baser votre groupe sur un attribut du nœud ou des dispositifs, tel que les catégories et les éléments. L'avantage de cette méthode réside dans le fait que lorsque vous ajoutez d'autres dispositifs ou nœuds avec les mêmes attributs que ceux décrits, ils seront placés automatiquement dans le groupe.

Utilisez la méthode Sélectionner lorsque vous souhaitez simplement créer manuellement un groupe de nœuds particuliers. Les nouveaux nœuds et dispositifs ajoutés à CC-SG ne sont pas placés automatiquement dans ces groupes. Vous devez les placer vous-même dans le groupe après leur ajout à CC-SG.

Ces deux méthodes ne peuvent pas être combinées.

Lorsqu'un groupe est créé avec une méthode, vous devez utiliser celle-ci pour le modifier. Si vous changez de méthodes, les paramètres actuels du groupe seront remplacés.

Sélectionner les nœuds

Pour ajouter un groupe de nœuds à l'aide de l'option 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.
   - Pour supprimer un nœud du groupe, sélectionnez son nom dans la liste Sélectionné, puis cliquez sur Retirer.
   - 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.
4. 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.
5. Lorsque l'opération est terminée, cliquez sur OK pour créer le groupe de nœuds. Le groupe est ajouté à la liste des groupes de nœuds à gauche.

Décrire les nœuds

Pour ajouter un groupe de nœuds à l'aide de l'option Décrire les nœuds :

1. Cliquez sur l'onglet Sélectionner les nœuds.
2. Cliquez sur l'icône Ajouter une nouvelle ligne  afin d'ajouter 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 Interface sont également présentes. Si un châssis de lames a été configuré dans le système, une catégorie Châssis du commutateur (Châssis de lames) est disponible par défaut.

- 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 l'icône 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.
   - Pour retirer une règle, mettez-la en surbrillance dans la table, puis cliquez sur l'icône 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 : si 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 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. Pour effectuer cette comparaison en premier, placez-la entre parenthèses : (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.

Remarque : un espace doit être placé avant et après les opérateurs & et |. Sinon, le champ Expression abrégée revient à l'expression par défaut, c'est-à-dire Rule0 & Rule1 & Rule2 etc., lorsque vous supprimez une règle de la table.

---

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, qui présente 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 OK pour créer le groupe de nœuds. Le groupe est ajouté à la liste des groupes de nœuds à gauche.

Modifier 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 ou Décrire les nœuds pour plus d'informations sur la configuration d'un groupe de nœuds.
4. Cliquez sur OK pour enregistrer vos modifications.

Supprimer un groupe de nœuds

Pour supprimer un groupe de nœuds :

1. Choisissez Associations > Groupes de nœuds. La fenêtre Gestionnaire des groupes de nœuds s'ouvre.
2. Dans la liste des groupes de nœuds à gauche, sélectionnez le nœud à supprimer.
3. Choisissez Groupes > Supprimer.
4. Le panneau Supprimer un groupe de nœuds s'affiche. Cliquez sur Supprimer.
5. Cliquez sur Oui dans le message de confirmation qui s'affiche.

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.

Vous pouvez également configurer CC-SG pour utiliser l'authentification externe. Reportez-vous à ***Authentification à distance*** (à la page 150).

Vous devez également créer des stratégies d'accès que vous pouvez affecter aux groupes d'utilisateurs. Reportez-vous à ***Stratégies de contrôle d'accès*** (à la page 137).

Dans ce chapitre

Onglet Utilisateurs

Cliquez sur l'onglet Utilisateurs pour afficher tous les groupes d'utilisateurs et utilisateurs 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 + pour développer ou réduire la liste. 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, modification et suppression des groupes d'utilisateurs

Ajouter un groupe d'utilisateurs

La création de groupes d'utilisateurs vous permet d'organiser 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 ***Privilèges de groupe d'utilisateurs*** (à la page 321).

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 353) pour plus d'informations sur les règles CC-SG relatives à la longueur des noms.
3. Entrez une brève description de ce groupe dans le champ Description. **Facultatif.**
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 ***Stratégies de contrôle d'accès*** (à la page 137) pour plus d'informations sur les stratégies et leur mode de création.

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. 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. **Facultatif.**

10. Cliquez sur OK pour enregistrer vos modifications.

Modifier 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 d'utilisateurs :

1. Cliquez sur l'onglet Utilisateurs.
2. Cliquez sur le groupe d'utilisateurs dans l'onglet Utilisateurs. L'écran Profil du groupe d'utilisateurs apparaît.
3. Renseignez le champ Nom du groupe d'utilisateurs. **Facultatif.**
4. Entrez une nouvelle description de ce groupe dans le champ Description. **Facultatif.**
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. Lorsque vous souhaitez ajouter une stratégie au groupe, sélectionnez-la dans la table Toutes les stratégies, puis cliquez sur Ajouter pour la déplacer 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, choisissez son nom dans la liste Stratégies sélectionnées et cliquez sur Supprimer.
12. Cliquez sur OK pour enregistrer vos modifications.

Supprimer 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.
2. Cliquez sur le groupe d'utilisateurs à supprimer.
3. Choisissez Utilisateurs > Gestionnaire des groupes d'utilisateurs > Supprimer un groupe d'utilisateurs.
4. Cliquez sur OK pour supprimer le groupe d'utilisateurs.

Configuration de l'audit des accès des groupes d'utilisateurs

Vous pouvez exiger des membres d'un groupe d'utilisateurs qu'ils entrent le motif d'accès au nœud avant que l'accès soit accordé. Une boîte de dialogue apparaît à tous les utilisateurs des groupes sélectionnés. Les utilisateurs doivent entrer le motif de l'accès avant l'établissement de la connexion au nœud. Cette fonction s'applique à tous les types d'accès avec tous les types d'interfaces, notamment la gestion de l'alimentation.

Les motifs d'accès sont consignés dans le journal d'audit et dans l'onglet d'audit du profil du nœud.

Pour configurer l'audit des accès des groupes d'utilisateurs :

1. Choisissez Utilisateurs > Audit des nœuds.
2. Cochez la case Saisie obligatoire des informations d'accès par les utilisateurs lors de la connexion à un nœud.
3. Dans le champ Message aux utilisateurs, entrez le message qui apparaîtra aux utilisateurs lors de la tentative d'accès à un nœud. Un message par défaut est fourni. 256 caractères au maximum.
4. Pour placer les groupes d'utilisateurs dans la liste Sélectionné afin d'activer l'audit des accès, cliquez sur les boutons fléchés. Utilisez Ctrl+clic pour sélectionner plusieurs éléments.

   *Conseil : entrez le nom d'un groupe d'utilisateurs dans le champ Rechercher pour le mettre en surbrillance dans la liste. Tapez * après un nom partiel pour mettre en surbrillance tous les noms similaires dans la liste.*

   Cliquez sur les en-têtes de colonne pour trier les listes par ordre alphabétique.
5. Cliquez sur Mettre à jour.

Ajout, modification et suppression des utilisateurs

Ajouter 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 353) 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 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 353) 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 199) 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 son 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. Entrez le numéro de téléphone de l'utilisateur dans le champ correspondant.
12. Cliquez sur le menu déroulant Groupes d'utilisateurs et sélectionnez le groupe auquel l'utilisateur sera ajouté.

- Suivant le groupe d'utilisateurs sélectionné, la case Demander à l'utilisateur d'entrer des informations lorsqu'il se connecte à un nœud peut être cochée ou non. Si elle est cochée, l'utilisateur doit entrer des informations lorsqu'il accède à un nœud. Reportez-vous à ***Configuration de l'audit des accès pour des groupes d'utilisateurs*** (voir "Configuration de l'audit des accès des groupes d'utilisateurs" à la page 129).

13. 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.

Modifier un utilisateur

Vous ne pouvez pas modifier un utilisateur pour remplacer le groupe auquel il appartient. Reportez-vous à ***Affectation d'un utilisateur à un groupe*** (à la page 132).

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 à cocher Connexion activée pour empêcher cet utilisateur de se connecter à CC-SG. Cochez la case Connexion activée pour autoriser cet 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 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 199) 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 vos modifications.

Supprimer 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 133) 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 ce dernier. 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

Utilisez cette commande pour affecter un utilisateur à un autre groupe. Les utilisateurs affectés ainsi seront ajoutés au 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.

Pour affecter un utilisateur à un groupe :

1. Dans l'onglet Utilisateurs, sélectionnez le groupe d'utilisateurs auquel vous souhaitez affecter un utilisateur.
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.
   - Sélectionnez les utilisateurs à retirer de la liste Utilisateurs dans le groupe, puis cliquez sur le bouton < pour les retirer.

- 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 ce dernier L'écran Profil utilisateur apparaît.
2. Choisissez Utilisateurs > Gestionnaire des utilisateurs > Supprimer un utilisateur du groupe. L'écran Supprimer un utilisateur apparaît.
3. Cliquez sur OK pour supprimer l'utilisateur du groupe.

Votre profil utilisateur

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 CC Super User.

Pour visualiser votre profil :

Choisissez Passerelle sécurisée > Mon profil. L'écran Mon profil apparaît et affiche les détails de votre compte.

Changer votre mot de passe

1. Choisissez Passerelle sécurisée > Mon profil.
2. Cochez la case Changer le mot de passe (authentification locale uniquement).
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 message 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 vos 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 vos 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 vos 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 vos 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 vos 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, puis sélectionnez ce dernier.
   - 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 des 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 recevant les affiliations disposent déjà d'affiliations de groupe, celles-ci 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 ce dernier.
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 > pour déplacer le nom d'un utilisateur vers la liste Utilisateurs sélectionnés.
   - Cliquez sur >> pour déplacer tous les utilisateurs vers la liste Utilisateurs sélectionnés.
   - Choisissez l'utilisateur dans la liste Utilisateurs sélectionnés, puis cliquez sur < pour le retirer.
   - 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

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 141).

CC-SG inclut 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 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*** (voir "Ajouter un groupe de nœuds" à la page 118).
- Créez des groupes de dispositifs afin d'organiser les dispositifs pour lesquels vous souhaitez créer des règles d'accès. Reportez-vous à ***Ajout d'un groupe de dispositifs*** (voir "Ajouter un groupe de dispositifs" à la page 64).
- 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 138).
- Appliquez la stratégie à un groupe d'utilisateurs. Reportez-vous à ***Affectation de stratégies à des groupes d'utilisateurs*** (à la page 141).

Dans ce chapitre

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. Reportez-vous à **Modes de connexion : Direct et Proxy** *(à la page 213).*

Pour ajouter une stratégie :

1. Choisissez Associations > Stratégies. La fenêtre Gestionnaire des stratégies s'ouvre.
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 353) 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 type.
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 de dispositifs sélectionnés aux heures et jours indiqués :
    - Lecture-Ecriture donne accès en lecture et en 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 à ce moment. Ils prendront effet à la session suivante.

Pour 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 ***Mode de maintenance*** (à la page 185).

Pour modifier une stratégie :

1. Dans le menu Associations, cliquez sur Stratégies. La fenêtre Gestionnaire des stratégies s'ouvre.
2. Cliquez sur la flèche déroulante Nom de stratégie, puis choisissez dans la liste la stratégie à modifier.
3. 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. **Facultatif.**
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 de dispositifs sélectionnés aux heures et jours indiqués :
    - Lecture-Ecriture donne accès en lecture et en 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

Vous pouvez supprimer une stratégie qui n'est plus utile.

Pour supprimer une stratégie :

1. Choisissez Associations > Stratégies. La fenêtre Gestionnaire des stratégies s'ouvre.
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 KX2, KSX2 et KX2-101 compatibles. Pour obtenir des instructions détaillées sur l'accès aux supports virtuels avec votre dispositif, reportez-vous à :

- **Manuel d'utilisation de Dominion KX II**
- **Manuel d'utilisation de Dominion KSX II**
- **Manuel d'utilisation de Dominion KXII-101**

Reportez-vous à ***Ajout d'une stratégie*** (à la page 138) pour plus d'informations sur la création de stratégies d'autorisation de support virtuel à des groupes d'utilisateurs dans CC-SG.

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 ***Utilisateurs et groupes d'utilisateurs*** (à la page 123) 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

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 nœuds

Seuls les groupes de nœuds que vous spécifiez sont affichés dans la liste des nœuds lorsque la vue personnalisée Filtrer par groupe de nœuds est appliquée. Le premier niveau d'organisation est le nom du groupe de nœuds. Un nœud apparaît plusieurs fois dans la liste s'il appartient à plusieurs groupes de nœuds définis dans la vue personnalisée. Les nœuds 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 nœuds

Pour ajouter une vue personnalisée pour les nœuds :

1. Cliquez sur l'onglet Nœuds.
2. Choisissez Nœuds > Modifier la vue > 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'ouvre.
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 nœuds pour créer une vue personnalisée qui affiche uniquement les groupes de nœuds spécifiés.
   - Sélectionnez Vue par catégorie pour créer une vue personnalisée qui affiche les nœuds en fonction des catégories spécifiées.
6. Cliquez sur OK.
7. Dans la section Détails de vue personnalisée :
   a. Dans la liste Disponible, sélectionnez l'élément à inclure dans la vue personnalisée, puis cliquez sur Ajouter afin de l'ajouter à la liste. Répétez cette opération pour tous les éléments dont vous avez besoin.
   b. Organisez les éléments dans la liste Sélectionné dans l'ordre dans lequel chaque groupe doit apparaître dans l'onglet Nœuds. Sélectionnez un élément, puis cliquez sur les flèches haut et bas afin de placer l'élément dans l'ordre qui vous convient.
   c. Si vous devez supprimer un élément de la liste, sélectionnez-le, puis cliquez sur Retirer.
8. Cliquez sur Enregistrer. 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 nœuds

Pour appliquer une vue personnalisée à la liste de nœuds :

1. Choisissez Nœuds > Modifier la vue > Vue personnalisée. L'écran Vue personnalisée s'affiche.
2. Cliquez sur la flèche déroulante Nom et sélectionnez une vue personnalisée dans la liste.
3. Cliquez sur Appliquer la vue.

ou

- Choisissez Nœuds > 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 nœuds

1. Cliquez sur l'onglet Nœuds.
2. Choisissez Nœuds > Modifier la vue > Créer une vue personnalisée. L'écran Vue personnalisée s'affiche.
3. Cliquez sur la flèche déroulante Nom et 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'ouvre.
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 l'élément à inclure dans la vue personnalisée, puis cliquez sur Ajouter afin de l'ajouter à la liste. Répétez cette opération pour tous les éléments dont vous avez besoin.
   b. Organisez les éléments dans la liste Sélectionné dans l'ordre dans lequel chaque groupe doit apparaître dans l'onglet Nœuds. Sélectionnez un élément, puis cliquez sur les flèches haut et bas afin de placer l'élément dans l'ordre qui vous convient.
   c. Si vous devez supprimer un élément de la liste, sélectionnez-le, puis cliquez sur Retirer.

2. Cliquez sur Enregistrer. 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 nœuds

Pour supprimer une vue personnalisée pour les nœuds :

1. Cliquez sur l'onglet Nœuds.
2. Choisissez Nœuds > Modifier la vue > Créer une vue personnalisée. L'écran Vue personnalisée s'affiche.
3. Cliquez sur la flèche déroulante Nom et 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 message de confirmation Supprimer une vue personnalisée s'affiche.
5. Cliquez sur Oui.

Affecter une vue personnalisée par défaut à des nœuds

Pour affecter une vue personnalisée par défaut aux nœuds :

1. Cliquez sur l'onglet Nœuds.
2. Choisissez Nœuds > Modifier la vue > Créer une vue personnalisée. L'écran Vue personnalisée s'affiche.
3. Cliquez sur la flèche déroulante Nom et 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.

Affectation d'une vue personnalisée de nœuds 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.

Pour affecter une vue personnalisée de nœuds par défaut à tous les utilisateurs :

1. Cliquez sur l'onglet Nœuds.
2. Choisissez Nœuds > Modifier la vue > Créer une vue personnalisée.

3. Cliquez sur la flèche déroulante Nom et sélectionnez la vue personnalisée que vous souhaitez affecter par défaut à tout le système.
4. Cochez la case Vue système, puis cliquez sur Enregistrer.

Tous les utilisateurs qui se connectent à CC-SG voient l'onglet Nœuds trié selon la vue personnalisée sélectionnée. Les utilisateurs peuvent modifier 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. Choisissez Dispositifs > Modifier la vue > 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 l'élément à inclure dans la vue personnalisée, puis cliquez sur Ajouter afin de l'ajouter à la liste. Répétez cette opération pour tous les éléments dont vous avez besoin.
   b. Organisez les éléments dans la liste Sélectionné dans l'ordre dans lequel chaque groupe doit apparaître dans l'onglet Nœuds. Sélectionnez un élément, puis cliquez sur les flèches haut et bas afin de placer l'élément dans l'ordre qui vous convient.
   c. Si vous devez supprimer un élément de la liste, sélectionnez-le, puis cliquez sur Retirer.
8. Cliquez sur Enregistrer. 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. Choisissez Dispositifs > Modifier la vue > Vue personnalisée. L'écran Vue personnalisée s'affiche.
2. Cliquez sur la flèche déroulante Nom et 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. Choisissez Dispositifs > Modifier la vue > Créer une vue personnalisée. L'écran Vue personnalisée s'affiche.
3. Cliquez sur la flèche déroulante Nom et 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'ouvre.
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 l'élément à inclure dans la vue personnalisée, puis cliquez sur Ajouter afin de l'ajouter à la liste. Répétez cette opération pour tous les éléments dont vous avez besoin.

b. Organisez les éléments dans la liste Sélectionné dans l'ordre dans lequel chaque groupe doit apparaître dans l'onglet Nœuds. Sélectionnez un élément, puis cliquez sur les flèches haut et bas afin de placer l'élément dans l'ordre qui vous convient.

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

2. Cliquez sur Enregistrer. 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

Pour supprimer une vue personnalisée pour les 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 et 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 message de confirmation Supprimer une vue personnalisée s'affiche.
5. Cliquez sur Oui.

Affecter une vue personnalisée par défaut à des dispositifs

Pour affecter une vue personnalisée par défaut aux 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 et 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.

Pour affecter une vue personnalisée par défaut des dispositifs 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 par défaut 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 peuvent modifier la vue personnalisée.

Chapitre 12 Authentification à distance

Dans ce chapitre

Vue d'ensemble 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.

Les mises en place LDAP utilisent LDAP v3.

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 ***Utilisateurs et groupes d'utilisateurs*** (à la page 123) 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 un utilisateur de CC-SG est associé 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, indiquez 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. Cliquez sur 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. Cliquez sur 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.

Vue d'ensemble d'AD et 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.

N'ajoutez pas de modules AD en double. Si le message « Vous n'êtes membre d'aucun groupe » apparaît à vos utilisateurs lorsqu'ils tentent de se connecter, vous avez peut-être configuré des modules AD en double. Vérifiez les modules que vous avez configurés pour déterminer s'ils décrivent des zones de domaine superposées.

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 *Configuration du réseau CC-SG* **(à la page 204).**

Pour ajouter un module AD 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 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.

N'ajoutez pas de modules AD en double. Si le message « Vous n'êtes membre d'aucun groupe » apparaît à vos utilisateurs lorsqu'ils tentent de se connecter, vous avez peut-être configuré des modules AD en double. Vérifiez les modules que vous avez configurés pour déterminer s'ils décrivent des zones de domaine superposées.

1. Entrez le domaine AD à interroger dans le champ Domaine. Par exemple, si le domaine AD est installé dans le domaine xyz.com, entrez xyz.com dans le champ Domaine. 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 des serveurs DNS primaire et secondaire respectivement dans les champs Primary DNS Server IP Address (Adresse IP du serveur DNS primaire) et Secondary DNS Server IP Address (Adresse IP du serveur DNS secondaire), ou cochez la case Utiliser le DNS par défaut de CC-SG pour utiliser le serveur DNS configuré dans la section Gestionnaire de configuration de CC-SG. Reportez-vous à ***Administration avancée*** (à la page 199).
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 peut 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. La longueur maximum est de 32 caractères alphanumériques.
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.

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 Confiances s'ouvre.

Paramètres de confiance AD

Dans l'onglet Confiances, 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 Confiances. Si vous avez configuré plusieurs domaines AD, tous les autres domaines sont affichés dans l'onglet Confiances.
2. Pour chaque domaine de la colonne Partenaire de confiance, cliquez sur le menu déroulant Sens de confiance, puis sélectionnez le sens de l'approbation que vous souhaitez établir entre les domaines. Les sens de confiance sont mis à jour dans tous les modules AD lorsque vous modifiez l'un d'entre eux.
   - Entrant : les données provenant du domaine sont approuvées.
   - Sortant : les données arrivant dans le domaine sélectionné sont approuvées.
   - Bidirectionnel : les données sont approuvées dans les deux sens par chaque domaine.
   - Désactivé : 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 Autorisation si vous souhaitez que CC-SG utilise le module AD pour l'autorisation 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. Cliquez sur 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 154), ***Paramètres avancés AD*** (à la page 155), ***Paramètres de groupe AD*** (à la page 157) et ***Paramètres de confiance AD*** (à la page 158).
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 vos 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 ***Synchroniser tous les groupes d'utilisateurs avec AD*** (à la page 162) et ***Synchroniser tous les modules AD*** (à la page 163).

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 157).

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 ***Synchroniser tous les groupes d'utilisateurs avec AD*** (à la page 162) et ***Synchroniser tous les modules AD*** (à la page 163).

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. Reportez-vous à **Administration avancée** *(à la page 199).*

Pour importer des groupes d'utilisateurs AD :

1. Choisissez Administration > Sécurité.

2. Cliquez sur l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés apparaissent 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 Associations de 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 ***Synchroniser tous les modules AD*** (à la page 163). 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 (Active Directory) :** 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. Reportez-vous à ***Synchroniser tous les modules AD*** (à la page 163).
  2. **Tous les groupes d'utilisateurs :**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. Reportez-vous à ***Synchroniser tous les groupes d'utilisateurs avec AD*** (à la page 162).

Synchroniser tous les groupes d'utilisateurs avec AD

Il est recommandé de synchroniser tous les groupes d'utilisateurs si vous avez modifié un groupe ; si vous avez déplacé par exemple un groupe d'utilisateurs 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 Associations de Active Directory.)

Si vous avez apporté des changements aux utilisateurs ou aux contrôleurs de domaine, synchronisez tous les modules AD. Reportez-vous à ***Synchroniser tous les modules AD*** (à la page 163).

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. Choisissez Administration > Sécurité.
2. Cliquez sur l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés apparaissent dans une table.
3. Sélectionnez le serveur AD dont vous souhaitez synchroniser les groupes d'utilisateurs avec ceux de CC-SG.
4. Dans la liste Synchronisation sur demande, sélectionnez Tous les groupes d'utilisateurs, puis cliquez sur le bouton fléché.
5. 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.

   Un message de confirmation s'affiche lorsque tous les groupes d'utilisateurs importés dans le module sélectionné sont synchronisés.

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. Choisissez Administration > Sécurité.
2. Cliquez sur l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés apparaissent dans une table.
3. 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.

Lors du changement du mot de passe d'un utilisateur dans MSFT Windows Server 2003 AD, l'ancien mot de passe et le nouveau sont valables pendant 30 minutes environ. Pendant cette période, l'utilisateur peut se connecter à CC-SG avec l'un de ces deux mots de passe car AD conserve l'ancien mot de passe dans la mémoire cache pendant 30 minutes avant de finaliser la mise à jour du nouveau mot de passe.

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. Cliquez sur l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés apparaissent 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. Cliquez sur l'onglet Authentification. Tous les serveurs d'autorisation et d'authentification configurés apparaissent 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. Sélectionnez 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 vos 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 123).

Ajout d'un module TACACS+

Pour ajouter 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 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. Renseignez le champ Port d'authentification.
4. Renseignez les champs Clé partagée et Confirmez la clé partagée. La longueur maximum est de 128 caractères alphanumériques.
5. Cliquez sur OK pour enregistrer vos 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 123).

Ajout d'un module RADIUS

Pour ajouter 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. Renseignez le champ Numéro de port. Le numéro de port par défaut est 1812.
4. Renseignez le champ Port d'authentification.
5. Renseignez les champs Clé partagée et Confirmez la clé partagée.
6. Cliquez sur OK pour enregistrer vos 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, les utilisateurs se connectent à CC-SG en commençant par saisir leur nom d'utilisateur dans le champ correspondant, puis leur 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 340).**

Chapitre 13 Rapports

Dans ce chapitre

Utilisation des rapports

Le filtre par défaut de n'importe quel rapport est la stratégie utilisateur. Par exemple, les nœuds ou dispositifs pour lesquels l'utilisateur ne dispose d'aucune permission d'accès ne s'afficheront pas dans les 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 Entrée pour afficher les détails.

Tous les détails du rapport sélectionné s'affichent dans une boîte de dialogue, pas seulement les détails que vous pouvez voir dans l'écran du rapport. Par exemple, l'écran Rapport d'accès n'affiche pas les options Type d'interface et Message, mais celles-ci sont disponibles dans la boîte de dialogue Détails d'accès aux nœuds.

Parcourir des rapports de plusieurs pages

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

Imprimer un rapport

CC-SG comporte deux options d'impression. Vous pouvez imprimer une page de rapport telle qu'elle apparaît à l'écran (imprimer une capture d'écran) ou l'intégralité d'un rapport, avec tous les détails sur chaque élément.

Remarque : les options d'impression fonctionnent pour toutes les pages CC-SG.

Pour imprimer une capture d'écran d'un rapport :

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

Pour imprimer tous les détails d'un rapport :

1. Générez le rapport à imprimer. Veillez à sélectionner Toutes dans le champ Entrées à afficher.
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. Par exemple, l'écran Rapport d'accès n'affiche pas les colonnes Type et Message, mais celles-ci sont disponibles après l'enregistrement et l'ouverture du rapport d'accès dans Excel.

1. Générez le rapport que vous souhaitez enregistrer dans un fichier.
2. Cliquez sur Enregistrer dans le fichier.
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 données apparaissant dans les rapports Journal d'audit et Journal d'erreurs. La purge de ces rapports supprime toutes les données répondant aux critères de recherche utilisés. Par exemple, si vous recherchez toutes les entrées de journal d'audit du 26 au 27 mars 2008, seuls ces enregistrements seront purgés. Les entrées antérieures au 26 mars ou postérieures au 27 mars resteront dans le journal d'audit.

Les données purgées sont définitivement supprimées de CC-SG.

Pour purger les données d'un rapport de CC-SG :

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 et Heure de début et Date et Heure de fin. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute) 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 Type de message, Message, Nom d'utilisateur et Adresse IP de l'utilisateur. Les caractères joker sont acceptés dans ces champs, sauf dans le champ Type de message.
   - Pour limiter le rapport à un type de message, effectuez une sélection dans le champ Type de message.
   - 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. Dans le champ Entrées à afficher, sélectionnez le nombre d'entrées à afficher dans l'écran du rapport.
5. Cliquez sur Appliquer pour générer le rapport.
   - Pour purger les enregistrements du rapport, cliquez sur Purger. Reportez-vous à ***Purger les données d'un rapport de CC-SG*** (à la page 173).

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 et Heure de début et Date et Heure de fin. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute) 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. Dans le champ Entrées à afficher, sélectionnez le nombre d'entrées à afficher dans l'écran du rapport.
5. Cliquez sur Appliquer pour générer le rapport.
   - Cliquez sur Purger pour supprimer le journal d'erreurs. Reportez-vous à ***Purger les données d'un rapport de CC-SG*** (à la page 173).

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 Dispositifs ou Nœuds.

3. Définissez la période couverte par le rapport dans les champs Date et Heure de début et Date et Heure de fin. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute) 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 entrant des paramètres supplémentaires dans les champs Nom du dispositif, Nom du nœud, Nom d'utilisateur et Adresse IP de l'utilisateur. Les caractères joker sont acceptés dans ces champs.
   - Pour limiter le rapport à un dispositif particulier, renseignez le champ Nom(s) du dispositif.
   - Pour limiter le rapport à un nœud particulier, entrez le nom du port dans le champ Nom(s) de nœud.
   - Pour limiter le rapport aux activités d'un utilisateur particulier, entrez le nom de ce dernier dans le champ Nom(s) d'utilisateur.
   - Pour limiter le rapport aux activités d'une adresse IP particulière, entrez l'adresse IP de l'utilisateur dans le champ Adresse(s) IP.
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.

Pour générer le rapport de disponibilité :

1. Choisissez Rapports > Rapport de disponibilité.
2. Sélectionnez 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. Reportez-vous à ***Paramètres de verrouillage*** (à la page 232).

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 de tous les 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 de tous les utilisateurs :

- Choisissez Rapports > Utilisateurs > Données de tous les utilisateurs.
  - Le champ Nom d'utilisateur affiche le nom d'utilisateur de tous les utilisateurs de CC-SG.
  - 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 ***Ajouter un utilisateur*** (à la page 129).

- 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 ***Ajouter un utilisateur*** (à la page 129).
- 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 ***Privilèges de groupe d'utilisateurs*** (à la page 321).
- 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 sur les données des groupes d'utilisateurs

Le rapport Données des groupes d'utilisateurs affiche les données relatives aux utilisateurs et aux groupes auxquels ils sont associés.

Pour générer le rapport Données des groupes d'utilisateurs :

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

Rapport sur le parc de dispositifs

Le rapport sur le parc de dispositifs affiche des données relatives aux dispositifs gérés actuellement par CC-SG.

Pour générer le rapport sur le parc de dispositifs :

- Choisissez Rapports > Dispositifs > Rapport sur le parc de dispositifs. Le rapport est généré pour tous les dispositifs.

Pour filtrer les données du rapport par type de dispositif :

- Sélectionnez un type de dispositif, 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.

Rapport Données des groupes de dispositifs

Le rapport Données des groupes de dispositifs affiche les informations de groupe de dispositifs.

Pour générer le rapport Données des groupes de dispositifs :

1. Choisissez Rapports > Dispositifs > Données des groupes de dispositifs.
2. Double-cliquez sur une ligne pour afficher la liste des dispositifs d'un groupe.

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 :		
	Disponible	
	Non disponible	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 :		

Type d'état	Etat du port	Définition
	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. 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** de Raritan. **Facultatif.**
4. Sélectionnez Ports suspendus ou Ports verrouillés pour inclure les ports suspendus ou verrouillés. Les ports suspendus surviennent lorsque la gestion CC-SG d'un dispositif est suspendue. Les ports verrouillés surviennent lorsqu'un dispositif est en cours de mise à niveau. **Facultatif.**
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 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 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, sélectionnez un paramètre dans le menu correspondant.
   - 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.

Pour obtenir des URL de signet pour les nœuds :

1. Générez le rapport sur le parc du nœuds, puis double-cliquez sur un nœud pour afficher la boîte de dialogue des détails.
2. Cliquez sur Enregistrer dans le fichier. Toutes les informations du rapport sont enregistrées dans un fichier .csv.
3. La colonne URL contient des liens directs vers chaque nœud. Vous pouvez utiliser ces informations pour créer une page Web de liens vers chaque nœud, au lieu de créer des signets individuels pour chacun. Reportez-vous à ***Ajouter une interface aux signets*** (voir "Ajout d'une interface aux signets" à la page 113).

Rapport sur les nœuds actifs

Le rapport sur les nœuds actifs indique les nom et type de chaque interface active, le mode de connexion, le dispositif associé, un horodateur, l'utilisateur actuel 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 :

- Choisissez Rapports > Utilisateurs > Nœuds actifs. Le rapport est généré si des nœuds sont actifs.

Pour déconnecter un nœud d'une session active :

- Dans le rapport Nœuds actifs, sélectionnez le nœud à déconnecter, puis cliquez sur Déconnecter.

Rapport sur la création des 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. Sélectionnez Tous les nœuds ou Doublons potentiels. La seconde option limite le rapport aux nœuds marqués comme doublons potentiels.

3. Si vous sélectionnez Tous les nœuds, définissez la période couverte par le rapport dans les champs Date et Heure de début et Date et Heure de fin. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
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 Données des groupes de nœuds

Le rapport Données des groupes de nœuds affiche les informations de groupe de nœuds.

Pour générer le rapport Données des groupes de nœuds :

1. Choisissez Rapports > Utilisateurs > Données de groupes de nœuds.
2. Double-cliquez sur une ligne pour afficher la liste des nœuds d'un groupe.

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 AD 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.

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. Les rapports programmés peuvent être consultés au format HTML uniquement. Reportez-vous à ***Gestionnaire des tâches*** (à la page 242).

Pour accéder aux rapports programmés :

1. Choisissez Rapports > Rapports programmés.
2. Sélectionnez un type de rapport.
3. Sélectionnez un propriétaire du rapport.
4. 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.
5. Définissez la période couverte par le rapport dans les champs Date et Heure de début et Date et Heure de fin. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
6. Cliquez sur Appliquer. La liste des rapports programmés est générée.

Pour afficher un rapport programmé :

1. Sélectionnez le rapport dans la liste.
2. Cliquez sur Afficher un rapport.

Remarque : un rapport manuel Journal d'audit, Journal d'erreurs et Rapport d'accès présente toutes les entrées tandis qu'un rapport généré à partir d'une tâche programmée affiche 10 000 lignes au maximum.

Pour supprimer un rapport programmé :

1. Sélectionnez les rapports à supprimer. Utilisez Ctrl+clic et Maj+clic pour sélectionner plusieurs rapports.
2. Cliquez sur Supprimer les rapports.
3. Cliquez sur Oui pour confirmer.

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 183) pour plus d'informations sur l'affichage du rapport.

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 249).** Vous pouvez 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, puis 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

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 242). Lorsque l'unité CC-SG quitte le mode de maintenance, les tâches programmées sont exécutées dès que possible.

Passage en mode de maintenance

1. Choisissez Maintenance du système > Mode de maintenance > Entrer en mode de maintenance.

2. Mot de passe : entrez votre mot de passe. Seuls les utilisateurs dotés du privilège CC Setup and Control peuvent accéder au mode de maintenance.
3. Message à diffusion générale : entrez le message à afficher aux utilisateurs qui seront déconnectés de CC-SG.
4. Entrer en mode de maintenance après (mn) : entrez le nombre de minutes (de 0 à 720) qui doivent s'écouler avant que CC-SG entre en mode de maintenance. Si vous entrez zéro, le mode de maintenance démarre immédiatement.

   Si vous définissez plus de 10 minutes, le message à diffusion générale apparaît aux utilisateurs immédiatement, puis à 10 et 5 minutes avant que l'événement ne se produise.
5. Cliquez sur OK.
6. Cliquez sur OK dans la boîte de dialogue de confirmation.

Sortie du mode de maintenance

1. Choisissez Maintenance du système > Mode de maintenance > Quitter le mode de maintenance.
2. Cliquez sur OK pour quitter le mode de maintenance.
3. 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.

Pour sauvegarder CC-SG :

1. Choisissez Maintenance du système > Sauvegarde.
2. Renseignez le champ Nom de la sauvegarde.
3. Entrez une brève description de cette sauvegarde dans le champ Description. **Facultatif.**
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 une sauvegarde des données critiques uniquement 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. Pour enregistrer une copie de ce fichier de sauvegarde sur un serveur externe, cochez la case Sauvegarde vers un site distant. **Facultatif.**
6. Sélectionnez un protocole utilisé 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 Adresse IP/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. Dans le champ Nom de fichier, nommez la sauvegarde sur le serveur distant.
13. Cliquez sur Enregistrer comme valeur par défaut si vous souhaitez enregistrer les paramètres actuels du serveur distant comme valeurs par défaut. **Facultatif.**

14. Cliquez sur OK.

    Un message 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. Reportez-vous à ***Restauration de CC-SG*** (à la page 189).

Important : la configuration du voisinage est incluse dans le fichier de sauvegarde de CC-SG alors n'oubliez pas de noter ses paramètres au moment de la sauvegarde. Cela vous aidera à déterminer si le fichier de sauvegarde est approprié pour l'unité CC-SG que vous restaurerez.

Enregistrement et suppression des fichiers de sauvegarde

L'écran Restaurer CommandCenter permet d'enregistrer et de supprimer des sauvegardes sur CC-SG. 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 pour copier le fichier de sauvegarde 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

Vous pouvez restaurer CC-SG à l'aide d'un fichier de sauvegarde que vous avez créé.

Important : la configuration du voisinage est incluse dans le fichier de sauvegarde de CC-SG alors n'oubliez pas de noter ses paramètres au moment de la sauvegarde. Cela vous aidera à déterminer si le fichier de sauvegarde est approprié pour l'unité CC-SG que vous restaurerez.

Pour restaurer CC-SG :

1. Choisissez Maintenance du système > Restaurer. L'écran Restaurer CommandCenter affiche la liste des fichiers de sauvegarde disponibles pour CC-SG. Celle-ci répertorie le type de la sauvegarde, sa date, une description, la version de CC-SG d'origine et la taille du fichier de sauvegarde.
2. Pour restaurer depuis une sauvegarde stockée en dehors du système CC-SG, vous devez d'abord téléverser le fichier de sauvegarde sur CC-SG. **Facultatif.**
   a. Cliquez sur Télécharger vers le serveur.
   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 téléverser ce fichier sur CC-SG. Cette opération terminée, le fichier de sauvegarde apparaît dans la table Sauvegardes disponibles.
3. Sélectionnez le fichier de 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.

- Restaurer les données : configuration de CC-SG, configuration des dispositifs et des nœuds, et données utilisateur.
- Restaurer les journaux : journaux d'erreur et rapports d'événement stockés dans CC-SG.
- Restaurer le firmware de CC : fichiers de firmware stockés utilisés pour la mise à jour du serveur CC-SG.
- Restaurer les binaires de firmware : fichiers de firmware stockés utilisés pour la mise à jour des dispositifs Raritan gérés par CC-SG.
- Restaurer les applications : 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 (mn). Ceci permet aux utilisateurs de terminer leur travail et de se déconnecter.

   Si vous définissez plus de 10 minutes, le message à diffusion générale apparaît aux utilisateurs immédiatement, puis à 10 et 5 minutes avant que l'événement ne se produise.
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. CC-SG attend le temps indiqué avant de restaurer sa configuration à partir 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, ou rétablir d'autres composants à leurs paramètres par défaut usine. Vous devez effectuer une sauvegarde et enregistrer le fichier de sauvegarde à un autre emplacement avant d'utiliser les options de réinitialisation.

Il est recommandé d'utiliser les options par défaut sélectionnées.

Option	Description
Base de données complète	Cette option supprime la base de données CC-SG existante et constitue une nouvelle version en la chargeant avec les valeurs par défaut usine. Les paramètres réseau, SNMP et de console de diagnostic, et le firmware ne font pas partie de la base de données CC-SG. Les paramètres IP-ACL sont rétablis par une réinitialisation de la base de données complète que l'option IP ACL Tables soit sélectionnée ou non. La configuration du voisinage est supprimée lors de la réinitialisation, l'unité CC-SG ne « se souvient » donc plus avoir été membre du voisinage. Lorsque la base de données est supprimée, tous les dispositifs, nœuds et utilisateurs sont retirés. Tous les serveurs d'authentification et d'autorisation sont retirés. Votre compte Super utilisateur CC est rétabli à sa valeur par défaut. Une fois l'opération de réinitialisation terminée, vous devez vous connecter à l'aide des nom d'utilisateur et mot de passe par défaut admin/raritan.
Enregistrer les paramètres de personnalité	Cette option peut être activée uniquement lorsque vous sélectionnez Full CC-SG Database Reset (Réinitialisation de la base de données CC-SG complète). Elle permet d'enregistrer certaines options configurées précédemment lorsque la base de données CC-SG est reconstruite. ▪ Communication sécurisée entre les clients PC et CC-SG ▪ Imposition des mots de passe forts ▪ Connexions directes ou Proxy aux nœuds hors bande ▪ Paramètre de délai d'inactivité

Option	Description
Paramètres réseau	Cette option rétablit les paramètres réseau aux valeurs par défaut usine. ▪ Nom de l'hôte : CommandCenter ▪ Nom de domaine : localdomain ▪ Mode : Principal/de sauvegarde ▪ Configuration : Statique ▪ Adresse IP : 192.168.0.192 ▪ Masque réseau : 255.255.255.0 ▪ Passerelle : néant ▪ DNS principal : néant ▪ DNS secondaire : néant ▪ Vitesse de carte : Auto
Configuration SNMP	Cette option rétablit les paramètres SNMP aux valeurs par défaut usine. ▪ Port : 161 ▪ Communauté en lecture seule : public ▪ Communauté en lecture/écriture : privé ▪ Contact système, Nom, Emplacement : néant ▪ Configuration des traps SNMP ▪ Destinations des traps SNMP
Firmware par défaut	Cette option rétablit tous les fichiers de firmware de dispositif aux valeurs par défaut usine. Cette option ne modifie pas la base de données CC-SG.
Télécharger le firmware dans la base de données après réinitialisation	Cette option charge les fichiers de firmware de la version de CC-SG actuelle dans la base de données CC-SG.
Console de diagnostic	Cette option rétablit les paramètres de console de diagnostic aux valeurs par défaut usine.
Tables IP-LCA	Cette option retire toutes les entrées de la table IP-ACL. Les paramètres IP-ACL sont rétablis par une réinitialisation de la base de données complète que l'option IP ACL Tables soit sélectionnée ou non.

Pour réinitialiser CC-SG :

1. Avant de procéder à la réinitialisation, sauvegardez CC-SG et enregistrez le fichier de sauvegarde à un emplacement distant. Reportez-vous à ***Sauvegarde de CC-SG*** (à la page 186).
2. Choisissez Maintenance du système > Réinitialiser.

3. Sélectionnez les options de réinitialisation.
4. Tapez votre mot de passe CC-SG.
5. Message à diffusion générale : entrez le message à afficher aux utilisateurs qui seront déconnectés de CC-SG.
6. Entrez le nombre de minutes (de 0 à 720) qui doivent s'écouler avant que CC-SG n'exécute l'opération de réinitialisation.

   Si vous définissez plus de 10 minutes, le message à diffusion générale apparaît aux utilisateurs immédiatement, puis à 10 et 5 minutes avant que l'événement ne se produise.
7. Cliquez sur OK. Un message apparaît pour confirmer la réinitialisation.

NE METTEZ PAS hors tension, N'EFFECTUEZ PAS d'alimentation cyclique ou N'INTERROMPEZ PAS CC-SG pendant la réinitialisation. Ces opérations peuvent entraîner la perte des données de CC-SG.

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 720) qui doivent s'écouler avant que CC-SG redémarre.

   Si vous définissez plus de 10 minutes, le message à diffusion générale apparaît aux utilisateurs immédiatement, puis à 10 et 5 minutes avant que l'événement ne se produise.
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. Pour mettre à niveau CC-SG de la version 3.x à la version 4.1, vous devez effectuer tout d'abord la mise à niveau vers 4.0.

La version 4.0 ou supérieure de CC-SG n'est pas compatible avec le matériel G1. N'effectuez pas de mise à niveau d'une unité CC-SG G1 vers la version 4.0 ou supérieure.

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

Seuls les utilisateurs dotés du privilège CC Setup and Control (paramétrage et contrôle de CC) peuvent mettre à niveau CC-SG.

Vous devez sauvegarder CC-SG avant d'effectuer la mise à niveau et envoyer les fichiers de sauvegarde aux PC pour les conserver. Reportez-vous à ***Sauvegarde de CC-SG*** (à la page 186) et ***Enregistrer un fichier de sauvegarde*** (à la page 188).

Si vous utilisez un cluster CC-SG, vous devez le supprimer avant d'effectuer la mise à niveau. Mettez chaque nœud CC-SG à niveau individuellement, puis recréez le cluster.

Important : si vous devez mettre à niveau CC-SG et un dispositif ou un groupe de dispositifs, traitez CC-SG d'abord, puis le dispositif.

CC-SG sera réamorcé pendant la mise à niveau. N'INTERROMPEZ PAS la procédure, ne réamorcez 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. Connectez-vous au client Admin de CC-SG en utilisant un compte disposant du privilège CC Setup and Control.
3. Entrez en mode de maintenance. Reportez-vous à ***Passage en mode de maintenance*** (à la page 185).
4. Lorsque CC-SG est en mode de maintenance, choisissez Maintenance du système > Mettre à niveau.
5. Cliquez sur Parcourir. Recherchez et sélectionnez le fichier de firmware de CC-SG (.zip), cliquez ensuite sur Ouvrir.
6. 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 la mise à niveau. Tous les utilisateurs sont alors déconnectés de CC-SG.

7. Vous devez attendre la fin de la mise à niveau pour vous connecter de nouveau à CC-SG. Vous pouvez surveiller la mise à niveau dans la console de diagnostic.
   a. Accédez à cette dernière à l'aide du compte admin. Reportez-vous à ***Accéder à la console d'administrateur*** (à la page 272).
   b. Choisissez Admin > System Logfile Viewer. Sélectionnez sg/upgrade.log, puis choisissez Afficher pour consulter le journal de mise à niveau.
   c. Attentez la fin de la mise à niveau. Celle-ci est terminée lorsque le message indiquant la fin de la mise à niveau apparaît dans le journal de mise à niveau. Vous pouvez également attendre que le résultat du trap SNMP ccImageUpgradeResults affiche un message de réussite.
   d. Le serveur doit être réamorcé. Le processus de réamorçage commence lorsque le message indiquant le réamorçage de Linux apparaît dans le journal de mise à niveau. Le serveur est fermé, puis réamorcé.

   Remarque : pour les mises à niveau de CC-SG 3.x vers 4.0.x, le système sera réamorcé deux fois, ce qui est normal et attendu.

   e. Environ deux minutes après le réamorçage, vous pouvez accéder à nouveau à la console de diagnostic à l'aide du compte admin, et surveiller la progression de la mise à niveau. **Facultatif.**
8. Cliquez sur OK pour quitter CC-SG.
9. Effacez la mémoire cache du navigateur, puis fermez la fenêtre de ce dernier. Reportez-vous à ***Effacer la mémoire cache du navigateur*** (à la page 196).
10. Effacez la mémoire cache Java. Reportez-vous à ***Effacer la mémoire cache Java*** (à la page 196).
11. Lancez une nouvelle fenêtre du navigateur Web.
12. Connectez-vous au client Admin de CC-SG en utilisant un compte disposant du privilège CC Setup and Control.
13. 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.

14. Quittez le mode de maintenance. Reportez-vous à ***Sortie du mode de maintenance*** (à la page 186).
15. Effectuez une copie de sauvegarde de CC-SG. Reportez-vous à ***Sauvegarde de CC-SG*** (à la page 186).

Effacer la mémoire cache du navigateur

Ces instructions peuvent varier légèrement pour différentes versions de navigateur.

Pour effacer la mémoire cache du navigateur dans Internet Explorer 6.0 ou supérieur :

1. Choisissez Outils > Options Internet.
2. Dans l'onglet Général, cliquez sur Supprimer les fichiers, puis sur OK pour confirmer.

Dans FireFox 2.0 :

1. Choisissez Outils > Effacer les données privées.
2. Assurez-vous que l'option Cache est sélectionnée, puis cliquez sur Effacer les données privées maintenant.

Effacer la mémoire cache Java

Ces instructions peuvent varier légèrement pour différentes versions Java et différents systèmes d'exploitation.

Dans Windows XP avec Java 1.6 :

1. Choisissez Panneau de configuration > Java.
2. Sur l'onglet Général, cliquez sur Paramètres.
3. Dans la boîte de dialogue qui s'ouvre, cliquez sur Supprimer les fichiers.
4. Assurez-vous que les cases Applications et Applets sont cochées, puis cliquez sur OK.

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 720) qui doivent s'écouler avant l'arrêt de CC-SG.

   Si vous définissez plus de 10 minutes, le message à diffusion générale apparaît aux utilisateurs immédiatement, puis à 10 et 5 minutes avant que l'événement ne se produise.
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 ***Redémarrer CC-SG avec la console de diagnostic*** (à la page 286).
- 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 hors tension CC-SG, il est recommandé d'utiliser la commande CC-SG System Power OFF (Mise hors tension du système CC-SG) de la console de diagnostic. Reportez-vous à *Mettre hors tension le système CC-SG à partir de la console de diagnostic* **(à la page 288).**

Pour mettre CC-SG hors tension :

1. Retirez le cache, puis enfoncez fermement le bouton d'alimentation.
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 pour mettre fin à la session tout en gardant la fenêtre du client ouverte. Reportez-vous à ***Se déconnecter de CC-SG*** (à la page 198).
- Quittez pour mettre fin à la session et fermer la fenêtre du client. Reportez-vous à ***Quitter CC-SG*** (à la page 198).

Se déconnecter de CC-SG

1. Choisissez Passerelle sécurisée > Déconnexion. La fenêtre Déconnexion s'ouvre.
2. Cliquez sur Oui pour vous déconnecter de CC-SG. Une fois la déconnexion effectuée, la fenêtre de connexion de CC-SG s'ouvre.

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

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. Cochez la case Afficher le Message du jour pour tous les utilisateurs pour que le message apparaisse à tous les utilisateurs à la connexion. **Facultatif.**
3. Cochez la case 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 une police pour le texte du message.

c. Cliquez sur le menu déroulant Taille de police et sélectionnez une taille pour le texte 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 vos 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 des applications prises en charge, reportez-vous à la matrice de compatibilité sur le site Web du support Raritan.

Il est recommandé d'entrer en mode de maintenance avant de mettre à niveau les applications. Reportez-vous à ***Passage en mode de maintenance*** (à la page 185).

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. Reportez-vous à ***Ajouter une application*** (à la page 201).
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.

Remarque : les utilisateurs connectés pendant la mise à niveau doivent fermer leur session CC-SG, puis l'ouvrir à nouveau pour s'assurer que la nouvelle version de l'application est lancée.

Ajouter une application

Lorsque vous ajoutez une application dans CC-SG, vous devez indiquer les types de dispositifs qui fonctionnent avec elle. Si un dispositif fournit l'accès KVM et série, il figure deux fois dans la liste, une pour chaque méthode.

Pour ajouter une application :

1. Choisissez Administration > Applications.

2. Cliquez sur Ajouter. La fenêtre de dialogue Ajouter une application s'ouvre.
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.
7. L'application sélectionnée se charge dans CC-SG.

Supprimer une application

Pour 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

Pour 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

Pour 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. Reportez-vous à ***Mise à niveau d'un dispositif*** (à la page 52).

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.

Pour télécharger un firmware sur CC-SG :

1. Choisissez Administration > Firmware.
2. Cliquez sur Ajouter pour ajouter un nouveau fichier de firmware. Une fenêtre de recherche s'ouvre.
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

Pour 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.

Important : pour changer l'adresse IP d'une unité CC-SG qui est déjà *membre d'un voisinage* **(voir "Voisinage : définition" à la page 223), vous devez en premier lieu la retirer de la configuration du voisinage. Sinon, vous ne serez pas en mesure de supprimer CC-SG du voisinage.**

A propos de la configuration réseau

CC-SG offre deux modes de configuration du réseau :

- **Mode principal/de sauvegarde :** reportez-vous à ***Mode principal/de sauvegarde : définition*** (à la page 205).
- **Mode actif/actif :** reportez-vous à ***Mode actif/actif : définition*** (à la page 208).

Important : il est fortement recommandé d'utiliser le mode principal/de sauvegarde pour les nouveaux déploiements.

CC-SG autorise également les adresses IP statiques ou DHCP. Reportez-vous à ***Configurations DHCP recommandées pour CC-SG*** (à la page 210) pour une utilisation optimale de DHCP avec votre unité CC-SG.

A propos des ports LAN CC-SG

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 V1 :

Modèle	Nom du réseau local principal	Emplacement du réseau local principal	Nom du réseau local secondaire	Emplacement du réseau local secondaire
V1-0 ou V1-1	LAN1	Port LAN gauche	LAN2	Port LAN droit

Ports LAN E1 :

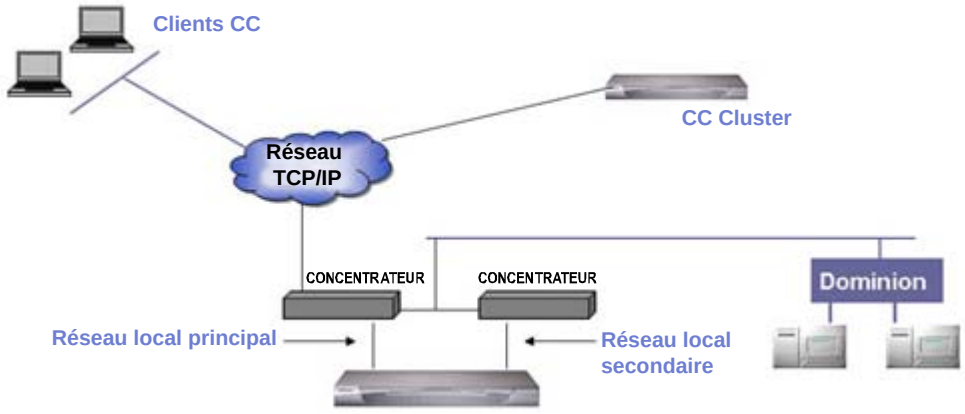
Modèle	Nom du réseau local principal	Emplacement du réseau local principal	Nom du réseau local secondaire	Emplacement du réseau local secondaire
E1-0	Sans libellé	Port LAN supérieur d'un ensemble de 2 ports au centre du panneau arrière de l'unité	Sans libellé	Port LAN inférieur d'un ensemble de 2 ports au centre du panneau arrière de l'unité
E1-1	LAN1	Port LAN gauche	LAN2	Port LAN droit

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.

Important : il est fortement recommandé d'utiliser le mode principal/de sauvegarde pour les nouveaux déploiements.

Reportez-vous à ***A propos des ports LAN CC-SG*** (à la page 205) 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.
- Vous pouvez connecter chaque port LAN à un commutateur ou concentrateur différent du même sous-réseau pour des questions de fiabilité. **Facultatif.**

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 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 210).

   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. Si votre commutateur utilise une vitesse de ligne d'1 Giga, sélectionnez Auto.
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 immédiatement redémarrer CC-SG automatiquement.

- Cliquez sur Redémarrer plus tard pour redémarrer CC-SG manuellement ultérieurement. Reportez-vous à ***Redémarrage de CC-SG*** (à la page 193).
  - Cliquez sur Annuler pour retourner au panneau Configuration réseau sans enregistrer vos modifications. Vous devez cliquer sur Mettre à jour la configuration, puis cliquez sur Redémarrer maintenant ou Redémarrer plus tard pour enregistrer vos modifications.

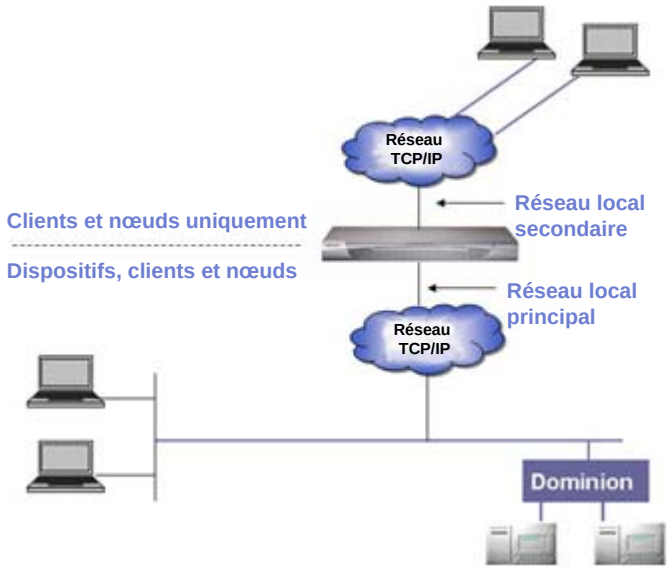
Remarque : si l'unité CC-SG est configurée avec DHCP, vous pouvez y accéder via le nom d'hôte après enregistrement auprès du serveur DNS.

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 205) 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 si nécessaire. Reportez-vous à ***Modifier les routes statiques*** (à la page 280).

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 210).

   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. Si votre commutateur utilise une vitesse de ligne d'1 Giga, sélectionnez Auto.
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 des serveurs d'enregistrement externes et indiquer 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. Reportez-vous à **Purger les données d'un rapport de CC-SG** *(à la page 173).*

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 242). 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 dans lequel vous utilisez CC-SG.

   a. 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, puis entrez les adresses IP des serveurs NTP principal et secondaire 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.

Modes de connexion : Direct et Proxy

A propos des modes de connexion

CC-SG offre trois modes de connexion en bande et hors bande : Direct, Proxy et Les deux.

- 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 Proxy n'utilise pas SSL entre CC-SG et le dispositif KXII pour les données KVM, si AES est activé dans le dispositif KXII.
- 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. Certaines interfaces fonctionnent uniquement en mode Direct même si vous configurez CC-SG pour fonctionner en mode Proxy. Ces interfaces comprennent ILO, RDP, DRAC, Navigateur Web et VMware Viewer. Reportez-vous à *A propos des interfaces* **(à la page 81).**

Configurer le mode Direct pour toutes les connexions clientes

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.

Configurer le mode Proxy pour toutes les connexions clientes

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.

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.

Pour configurer une combinaison des modes Direct et Proxy :

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

Vous pouvez configurer certains paramètres s'appliquant à tous les dispositifs et le numéro de port par défaut de chaque type de dispositif.

Pour configurer le numéro de port par défaut des dispositifs :

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet Paramètres du dispositif.
3. Sélectionnez un type de dispositif dans la table et double-cliquez sur la valeur Port par défaut.
4. Tapez la nouvelle valeur de port par défaut.
5. Cliquez sur Mettre à jour la configuration pour enregistrer vos modifications.

Pour configurer le délai d'attente des dispositifs :

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet Paramètres du dispositif.
3. Tapez un nouveau délai d'attente dans le champ Test de détection de collision (s). Les valeurs admises sont comprises entre 30 et 50 000 secondes.
4. Cliquez sur Mettre à jour la configuration pour enregistrer vos modifications.

Pour activer ou désactiver un message d'avertissement pour toutes les opérations d'alimentation :

Cochez la case Afficher un message d'avertissement pour toutes les opérations d'alimentation pour activer un message avertissant l'utilisateur avant une opération d'alimentation demandée. Seul l'utilisateur qui a déclenché l'opération voit le message. Il peut annuler ou confirmer l'opération en cliquant Oui ou Non dans le message.

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet Paramètres du dispositif.
3. Cochez la case Afficher un message d'avertissement pour toutes les opérations d'alimentation pour activer le message d'avertissement. Désélectionnez la case à cocher pour désactiver le message d'avertissement.
4. Cliquez sur Mettre à jour la configuration pour enregistrer vos modifications.

Configuration de paramètres JRE personnalisés

CC-SG affichent un message d'avertissement aux utilisateurs qui tentent d'accéder à CC-SG sans la version JRE minimum que vous spécifiez. Vérifiez dans la matrice de compatibilité la version JRE minimum prise en charge. Choisissez Administration > Compatibility Matrix (matrice de compatibilité).

Si un utilisateur tente de se connecter à CC-SG sans la version JRE spécifiée, la fenêtre Avertissement d'incompatibilité JRE s'ouvre. La fenêtre comprend plusieurs options pour télécharger les versions JRE minimum par défaut. Vous pouvez inclure au message du texte et des liens vers les options de téléchargement. Les utilisateurs peuvent télécharger une nouvelle version de JRE ou continuer l'accès à CC-SG avec la version installée.

Pour activer ou désactiver un JRE personnalisé pour la connexion :

1. Effectuez une sauvegarde de CC-SG et enregistrez le fichier obtenu à un emplacement distant avant d'activer ou de désactiver cette fonction. Reportez-vous à ***Sauvegarde de CC-SG*** (à la page 186).
2. Choisissez Administration > Configuration.
3. Cliquez sur l'onglet JRE personnalisé.
4. Cochez la case Activer la connexion du JRE personnalisé pour activer l'option. Désélectionnez la case à cocher pour désactiver l'option.
5. Entrez la version JRE minimum dans le champ Demander le JRE minimum. Vous devez entrer le numéro de version complet, comprenant au moins trois parties. Par exemple, 1.6.0 est un numéro de version correct. 1.6 est incorrect. Pour les versions JRE de mise à jour, utilisez un trait de soulignement. Par exemple, 1.6.0_5 est un numéro de version correct pour JRE version 1.6.0 mise à jour 5.
6. Cliquez sur Mettre à jour.

Pour personnaliser le message de la fenêtre Avertissement d'incompatibilité JRE :

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet JRE personnalisé.
3. A l'aide de code HTML, entrez le message qui apparaît dans la fenêtre Avertissement d'incompatibilité JRE.
4. Cliquez sur Mettre à jour.

Pour restaurer le message et la version JRE minimum par défaut :

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet JRE personnalisé.
3. Cliquez sur Restaurer le paramètre par défaut.
4. Cliquez sur Mettre à jour.

Pour effacer le message et la version JRE minimum par défaut :

1. Choisissez Administration > Configuration. Cliquez sur l'onglet JRE personnalisé.
2. Cliquez sur Effacer.

Configuration de SNMP

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 RFC 1213.

Pour configurer SNMP dans CC-SG :

1. Choisissez Administration > Configuration.
2. Cliquez sur l'onglet SNMP.
3. Cochez la case Activer le démon SNMP pour activer les opérations SNMP.
4. 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.

5. Cliquez sur Mettre à jour la configuration de l'agent pour enregistrer vos modifications.
6. Cochez la case Activer les traps SNMP pour autoriser l'envoi de traps SNMP de CC-SG à un hôte SNMP.
7. Dans la section 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. Tapez la chaîne Communauté et la version (v1 ou v2) utilisées par les hôtes SNMP dans la section Destination des traps.
9. 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. Utilisez la case à cocher dans l'en-tête de la colonne Sélectionné pour activer tous les traps, ou pour désactiver toutes les cases à cocher. Consultez les fichiers MIB pour obtenir la liste des traps SNMP fournis. Pour plus d'informations, reportez-vous à Fichiers MIB.
10. 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.
11. Cliquez sur Mettre à jour la configuration des traps pour enregistrer vos modifications.

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. Reportez-vous à ***Traps SNMP*** (à la page 330). Le fichier MIB personnalisé se trouve sur le site Web du support Raritan.

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 (V1 ou E1).
- Votre 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 204).
- 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.

Accéder à un cluster CC-SG

Lorsqu'un cluster est créé, les utilisateurs peuvent accéder directement au nœud primaire ou s'ils dirigent leur navigateur vers le nœud secondaire, ils seront redirigés. Le réacheminement ne fonctionne pas pour un applet Admin Client déjà téléchargé puisque le navigateur Web doit être fermé et une nouvelle session doit être ouverte et dirigée vers le nouveau système primaire. L'accès SSH à une unité CC-SG doit être dirigé spécifiquement vers le nœud primaire.

Créer un cluster

Il est recommandé de sauvegarder votre configuration sur les deux unités CC-SG avant de créer un cluster.

Pour créer un cluster :

1. Choisissez Administration > Configuration des clusters.
2. L'unité CC-SG à laquelle vous accédez actuellement affiche le champ d'adresse IP/nom d'hôte de l'unité primaire Secure Gateway, qui indique qu'elle deviendra nœud primaire.
3. Définissez un nœud secondaire, ou de sauvegarde, dans le champ d'adresse IP/nom d'hôte de l'unité Secure Gateway de sauvegarde. Vérifiez que l'unité CC-SG spécifiée utilise la même version de firmware et le même type de matériel que le nœud primaire. Utilisez une de ces méthodes pour la définition :
   - Cliquez sur Détecter les unités Secure Gateway pour analyser et afficher toutes les unités CC-SG dans le sous-ensemble auquel vous accédez actuellement. Cliquez ensuite sur une unité CC-SG avec l'état Autonome dans la table des unités CC-SG détectées pour la sélectionner.
   - Vous pouvez également spécifier une unité CC-SG, dans un sous-ensemble différent, par exemple, en entrant une adresse IP ou un nom d'hôte dans le champ d'adresse IP/nom d'hôte de l'unité Secure Gateway de sauvegarde. Cliquez ensuite sur Vérifier la sauvegarde pour vous assurer que l'unité utilise la même version de firmware et le même type de matériel que le nœud primaire.
4. Renseignez le champ Nom du cluster.
5. Entrez un nom d'utilisateur et un mot de passe valides pour le nœud de sauvegarde dans les champs de nom d'utilisateur et de mot de passe pour l'unité Secure Gateway de sauvegarde.
6. Cliquez sur Créer un cluster. Un message apparaît.
7. Cliquez sur Oui.

Important : une fois le processus de création de cluster entamé, n'exécutez aucune autre fonction dans CC-SG avant la fin.

8. Continuez à cliquer sur OK pour tous les messages à l'écran. Le nœud de sauvegarde redémarre et le processus dure plusieurs minutes.
9. Lorsque la création du cluster est terminée, un message indique que le nœud de sauvegarde a été lié.

Configurer les paramètres d'un cluster

Vous ne pouvez pas modifier le fuseau horaire dans la configuration d'un cluster.

Pour configurer les paramètres d'un cluster :

1. Choisissez Administration > Configuration des clusters.
2. Dans l'onglet Configuration, modifiez ou configurez les paramètres.
   - Le cas échéant, modifiez le nom du cluster.
   - Dans le champ Intervalle de temps, entrez la fréquence à laquelle CC-SG doit vérifier sa connexion avec les autres nœuds. Les valeurs autorisées sont comprises entre 5 et 20 secondes.

   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.

   - 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. Les valeurs autorisées sont comprises entre 2 et 10 tests.
3. Cliquez sur Mettre à jour pour enregistrer vos modifications.

Commuter l'état des nœuds primaire et secondaire

Vous pouvez échanger les rôles des nœuds primaire et secondaire le nœud secondaire, ou de sauvegarde, est en attente.

Un nœud CC-SG en attente ne reçoit pas de mises à jour du nœud primaire. Tous les changements qui se sont produits depuis l'entrée en état d'attente seront donc perdus lors de la permutation entre les nœuds primaire et secondaire.

Pour permuter entre les nœuds primaire et secondaire

1. Choisissez Administration > Configuration des clusters.
2. Dans l'onglet Configuration, cliquez sur Basculer primaire et sauvegarde.

Récupérer un cluster

Lorsqu'un cluster est brisé à cause d'une défaillance ou lorsque le nœud secondaire défaillant passe à l'état En attente, vous pouvez reconstruire le cluster pour récupérer l'état des nœuds primaire et secondaire.

Si la communication est interrompue entre les nœuds primaire et secondaire, le nœud secondaire prend le rôle du nœud primaire. Lorsque la connectivité est rétablie, vous risquez d'avoir deux nœuds primaires. Il est impossible de récupérer le cluster avec deux nœuds primaires. Dans ce cas, connectez-vous à chaque nœud primaire pour supprimer le cluster et le créer à nouveau.

Pour récupérer un cluster :

1. Choisissez Administration > Configuration des clusters.
2. Cliquez sur l'onglet Restauration. Vous pouvez faire reconstruire le cluster automatiquement à l'heure spécifiée ou le reconstruire immédiatement.
   - Cliquez sur Rebuild Now (Reconstruire maintenant) pour récupérer immédiatement le cluster.
   - Cochez la case Enable Automatic Rebuild (Activer la reconstruction automatique) et indiquez une heure pour l'opération dans les champs From Time (Heure de début) et To Time (Heure de fin). Cliquez sur Mettre à jour pour enregistrer les modifications.

Remarque : lorsque les unités CC-SG en cluster n'utilisent pas le même fuseau horaire, lorsqu'une défaillance du nœud primaire se produit et que le nœud secondaire devient nœud primaire, l'heure indiquée pour la reconstruction automatique utilise toujours le fuseau horaire de l'ancien nœud primaire.

Supprimer un cluster

La suppression d'un cluster retire entièrement les données entrées dans celui-ci et restaure l'état Autonome des nœuds CC-SG primaire et secondaire. De plus, toutes les données de configuration, à l'exception des paramètres réseau (paquet personnalisé), du nœud secondaire sont réinitialisées aux valeurs par défaut, dont le mot de passe du super utilisateur CC.

Si la communication est interrompue entre les nœuds primaire et secondaire, le nœud secondaire prend le rôle du nœud primaire. Lorsque la connectivité est rétablie, vous risquez d'avoir deux nœuds primaires. Il est impossible de récupérer le cluster avec deux nœuds primaires. Dans ce cas, connectez-vous à chaque nœud primaire pour supprimer le cluster et le créer à nouveau.

Pour supprimer un cluster :

1. Choisissez Administration > Configuration des clusters.
2. Cliquez sur Delete Cluster (Supprimer le cluster).
3. Cliquez sur Yes (Oui) pour supprimer l'état des nœuds primaire et secondaire.
4. Un message apparaît lorsque le cluster est supprimé.

Configuration d'un voisinage

Voisinage : définition

Un voisinage est un ensemble de 10 unités CC-SG maximum. Après le paramétrage du voisinage dans Admin Client, les utilisateurs peuvent accéder à plusieurs unités CC-SG du même voisinage par une connexion unique à l'aide du client d'accès.

Avant le paramétrage ou la gestion de la configuration du voisinage, gardez à l'esprit les critères de celui-ci :

- Une unité CC-SG n'appartient qu'à un seul voisinage.
- Toutes les unités CC-SG d'un même voisinage doivent utiliser la même version du firmware.
- Les unités CC-SG du voisinage doivent être des unités CC-SG autonomes ou des nœuds primaires d'unités CC-SG en cluster.

Créer un voisinage

Vous pouvez vous connecter à une unité CC-SG dans laquelle vous souhaitez créer un voisinage et qui n'est pas encore membre d'un voisinage. Après la création d'un voisinage, tous ses membres partagent les mêmes données de voisinage. Si l'un des membres est le nœud primaire d'unités CC-SG en cluster, l'adresse IP ou le nom d'hôte du nœud secondaire, ou de sauvegarde, s'affiche également dans la configuration du voisinage.

Pour créer un voisinage :

1. Choisissez Administration > Voisinage.
2. Renseignez le champ Nom du voisinage.
3. Cliquez sur Créer le voisinage.
4. L'adresse IP ou le nom d'hôte de l'unité CC-SG actuelle s'affiche déjà dans la table d'adresse IP/nom d'hôte de l'unité Secure Gateway. Vous pouvez cliquer sur la flèche déroulante pour basculer entre les noms d'hôte complets ou courts, ou l'adresse IP.
5. Ajoutez une ou plusieurs unités CC-SG dans la table.
   a. Cliquez sur la ligne vide suivante ou appuyez sur Tab ou sur les touches de direction haut/bas.
   b. Entrez l'adresse IP ou le nom d'hôte de la nouvelle unité CC-SG que vous souhaitez ajouter et appuyez sur Entrée. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie et sigles*** (à la page 2).
   c. Répétez les étapes précédentes jusqu'à avoir ajouté toutes les unités CC-SG.
6. Cliquez sur Suivant.
   - Si une ou plusieurs unités CC-SG sont introuvables, un message apparaît et ces unités sont surlignées en jaune dans la table. Retirez ces unités ou modifiez leurs adresses IP ou noms d'hôte, puis cliquez à nouveau sur Suivant.
7. CC-SG affiche une liste des unités CC-SG, ainsi que de leur version de firmware et état dans la table Configuration du voisinage.

   Remarque : les unités CC-SG qui ne répondent pas aux **critères du voisinage** *(voir "Voisinage : définition" à la page 223) sont automatiquement désactivées.*
8. Ajustez les configurations de voisinage, le cas échéant. **Facultatif.**

- Pour modifier le nom d'une unité Secure Gateway de CC-SG, cliquez dessus, entrez-en un nouveau et appuyez sur Entrée. Le nom par défaut un nom d'hôte CC-SG court. Le nom apparaît aux utilisateurs du client d'accès lors du passage d'un membre à un autre du voisinage ; chaque nom doit donc être unique.
- Pour désactiver une unité CC-SG, désélectionnez la case Activer placée en regard de cette unité. Les unités C-SG désactivées fonctionnent de manière autonome et n'apparaissent pas comme membres du voisinage aux utilisateurs du client d'accès.
- Cliquez sur un en-tête de colonne pour trier la table par cet attribut dans l'ordre croissant. Cliquez de nouveau sur l'en-tête pour trier la table dans l'ordre décroissant.

9. Pour retourner à l'écran précédent, cliquez sur Précédent et répétez les étapes antérieures. **Facultatif.**
10. Cliquez sur Terminer.

Remarque : Raritan vous recommande :

(1) de configurer les mêmes paramètre et texte Accord de service limité pour tous les membres du voisinage. Reportez-vous à **Portail** *(à la page 234).*

(2) D'utiliser un certificat fiable/officiel pour chaque membre du voisinage si SSL est activé.

Modifier un voisinage

Après le paramétrage de la configuration d'un voisinage sur une unité CC-SG, toutes les unités CC-SG du même voisinage partagent les données de ce dernier. Vous pouvez donc vous connecter à n'importe quelle unité CC-SG du voisinage pour changer la configuration de ce dernier.

Remarque : toutes les modifications apportées aux membres d'un voisinage sont transmises lorsque vous cliquez sur Envoyer la mise à jour dans le panneau Configuration du voisinage. Toutefois, les utilisateurs actuellement connectés au voisinage ne verront pas ces changements tant qu'ils ne se seront pas déconnectés, puis connectés à nouveau.

Ajouter un membre de voisinage

Pour ajouter une unité CC-SG dans le voisinage

1. Choisissez Administration > Voisinage.
2. Cliquez sur Ajouter un membre. La boîte de dialogue correspondante apparaît.

3. Ajoutez des unités CC-SG. Le nombre d'unités CC-SG à ajouter dépend du nombre de membres existants du voisinage. Un voisinage contient 10 membres au maximum.
   a. Cliquez sur la ligne vide suivante ou appuyez sur Tab ou sur les touches de direction haut/bas.
   b. Entrez l'adresse IP ou le nom d'hôte de l'unité CC-SG que vous souhaitez ajouter. Pour connaître les règles des noms d'hôte, reportez-vous à ***Terminologie et sigles*** (à la page 2).
   c. Répétez les étapes précédentes jusqu'à avoir ajouté toutes les unités CC-SG.
   d. Cliquez sur OK.
4. Si de nouvelles unités CC-SG répondent aux critères du voisinage et sont détectées, elles s'affichent dans la table Configuration du voisinage. Sinon, un message apparaît et vous renvoie dans la boîte de dialogue Ajouter un membre. Modifiez celle-ci si nécessaire.
5. Cochez la case Actif en regard du nom de chaque nouvelle unité CC-SG.
6. Pour modifier le nom d'une unité Secure Gateway de CC-SG, cliquez dessus, entrez-en un nouveau et appuyez sur Entrée. Le nom par défaut un nom d'hôte CC-SG court. **Facultatif.**
7. Cliquez sur Envoyer la mise à jour pour enregistrer les modifications et transmettre les dernières données de voisinage aux autres membres.

Gérer la configuration du voisinage

Vous pouvez désactiver ou renommer les unités CC-SG dans la configuration du voisinage. La désactivation d'une unité CC-SG la rend indisponible dans la liste des membres du voisinage du client d'accès. Vous pouvez également actualiser les données de tous les membres, telles que la version du firmware ou l'état de l'unité, dans la configuration du voisinage.

Pour désactiver ou renommer les unités CC-SG dans le voisinage, ou extraire les dernières données

1. Choisissez Administration > Voisinage.
2. Cliquez sur un en-tête de colonne pour trier la table par cet attribut dans l'ordre croissant. Cliquez de nouveau sur l'en-tête pour trier la table dans l'ordre décroissant. **Facultatif.**
3. Vous pouvez gérer les membres maintenant.
   - Pour désactiver une unité CC-SG, désélectionnez la case Actif placée en regard de cette unité.

- Pour modifier le nom d'une unité Secure Gateway, cliquez dessus, entrez-en un nouveau et appuyez sur Entrée. Ce nom doit être unique.
- Pour extraire les données à jour de toutes les unités CC-SG, cliquez sur Rafraîchir les données de membre.
- Pour toujours mettre fin aux sessions de connexion existantes des utilisateurs lorsqu'ils passent à une autre unité CC-SG, cochez la case Déconnecter les sessions actives lors du changement de Secure Gateway. Sinon, désactivez-la.

4. Cliquez sur Envoyer la mise à jour pour enregistrer les modifications et transmettre les dernières données de voisinage aux autres membres.

Supprimer un membre de voisinage

Lorsqu'une unité CC-SG d'un voisinage n'est plus appropriée, vous pouvez la retirer ou la désactiver dans la configuration du voisinage. Sinon, elles pourraient être indisponibles aux utilisateurs du client d'accès Client qui tentent d'y accéder. Par exemple, un membre de voisinage n'est plus approprié lorsque vous :

- paramétrez l'unité CC-SG comme nœud CC-SG de sauvegarde dans une configuration en cluster, puisque cet état ne répond pas aux ***critères du voisinage*** (voir "Voisinage : définition" à la page 223) ;
- réinitialisez l'unité CC-SG, celle-ci supprime la configuration de son voisinage et récupère les valeurs par défaut usine.

Lorsque vous supprimez des membres, vérifiez qu'un minimum de deux unités CC-SG demeurent dans le voisinage. Sinon, CC-SG supprimera ce dernier.

Pour supprimer une unité CC-SG du voisinage

1. Choisissez Administration > Voisinage.
2. Cliquez sur l'unité CC-SG à supprimer puis sur Supprimer le membre. Répétez cette étape précédente jusqu'à avoir retiré toutes les unités CC-SG souhaitées.
3. Cliquez sur Envoyer la mise à jour pour enregistrer les modifications et transmettre les dernières données de voisinage aux autres membres.

Important : pour changer l'adresse IP d'une unité CC-SG qui est déjà *membre d'un voisinage* **(voir "Voisinage : définition" à la page 223), vous devez en premier lieu la retirer de la configuration du voisinage. Sinon, vous ne serez pas en mesure de supprimer CC-SG du voisinage.**

Actualiser un voisinage

Vous pouvez extraire le dernier état de tous les membres d'un voisinage immédiatement dans le panneau Configuration du voisinage.

1. Choisissez Administration > Voisinage.
2. Cliquez sur Rafraîchir les données de membre.
3. Cliquez sur Envoyer la mise à jour pour enregistrer les modifications et transmettre les dernières données de voisinage aux autres membres.

Supprimer un voisinage

Pour supprimer un voisinage :

1. Connectez-vous à une unité CC-SG dont vous souhaitez supprimer la configuration de voisinage.
2. Choisissez Administration > Voisinage.
3. Cliquez sur Supprimer le voisinage.
4. Cliquez sur Oui pour confirmer la suppression.

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 150) 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 AES-128 ou AES-256 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

CC-SG prend en charge AES-128 et AES-256. 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.

Remarque : Internet Explorer 6 ne prend pas en charge les chiffrements AES-128 et AES-256.

Chiffrement AES -256 bits : conditions préalables et configurations prises en charge

Le chiffrement AES-256 est pris en charge uniquement sur les navigateurs Web suivants :

- Firefox 2.0.0.x et supérieur
- Internet Explorer 7

Remarque : Internet Explorer 7 prend en charge les chiffrements AES-128 et AES-256 dans Windows Vista uniquement. Il ne prend en charge le chiffrement AES dans Windows XP.

Outre la prise en charge par le navigateur utilisé, le chiffrement AES-256 nécessite l'installation des fichiers Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6.

Pour activer le chiffrement AES-256 avec votre navigateur

1. Téléchargez JCE Unlimited Strength Jurisdiction Policy Files 6 du site ***http://java.sun.com/javase/downloads/index.jsp*** (http://java.sun.com/javase/downloads/index.jsp).
2. Extrayez les fichiers dans votre répertoire Java sous `\lib\securiry\`. Par exemple, `C:\Program Files\Java 1.6.0\lib\security\`.

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.
   - Cliquez sur la flèche déroulante Longueur de clé pour sélectionner le niveau de chiffrement 128 ou 256.
   - Le champ Port CC-SG affiche 80.
   - 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.

Pour configurer le protocole de connexion du navigateur :

1. Choisissez Administration > Sécurité.
2. Ouvrez l'onglet Chiffrement.
3. Sélectionnez l'option HTTP ou HTTPS/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.

Définir 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 252).

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 vous 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. Vous pouvez activer cette fonction pour les utilisateurs authentifiés localement, pour les utilisateurs authentifiés à distance ou pour tous les utilisateurs.

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. Cliquez sur l'onglet Paramètres de connexion.
3. Cochez la case Verrouillage activé pour les utilisateurs locaux pour activer le verrouillage des utilisateurs authentifiés localement. Cochez la case Verrouillage activé pour les utilisateurs distants pour activer le verrouillage des utilisateurs authentifiés à distance.
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. 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. **Facultatif.**
7. 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. **Facultatif.**
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. Désélectionnez la case Verrouillage activé pour les utilisateurs locaux pour désactiver le verrouillage des utilisateurs authentifiés localement. Désélectionnez la case Verrouillage activé pour les utilisateurs distants pour désactiver le verrouillage des utilisateurs authentifiés à distance.
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 la case Super utilisateur pour autoriser plusieurs connexions simultanées avec le compte Super utilisateur CC.

- Cochez la case Administrateurs système pour autoriser plusieurs connexions simultanées des comptes du groupe d'utilisateurs System Administrators.
- Cochez la case 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. Cochez la case 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.

Pour 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 Exporter. 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.

Pour 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'ouvre.
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 l'écran Administration > Sécurité > Chiffrement, AES-128 est la valeur par défaut. Si le chiffrement AES n'est pas obligatoire, DES 3 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.

Pour 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 l'écran Administration > Sécurité > Chiffrement, AES-128 est la valeur par défaut. Si le chiffrement AES n'est pas obligatoire, DES 3 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 vous souhaitez 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 vous souhaitez 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. Reportez-vous à ***Gestionnaire des tâches*** (à la page 242). 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 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. **Facultatif.**
6. Entrez le mot de passe du nom de compte dans les champs Mot de passe et Entrez à nouveau le mot de passe. **Facultatif.**
7. Entrez une adresse e-mail valide 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 des prises
- Effacer les journaux
- Redémarrer le 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)
- Générer tous les rapports

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. Vous pouvez indiquer où l'e-mail est envoyé et choisir un envoi sécurisé via SSL dans le Gestionnaire des notifications. Reportez-vous à ***Gestionnaire des notifications*** (à la page 241).

Rapports programmés

Les rapports programmés sont envoyés par courrier électronique aux destinataires définis. Vous pouvez spécifier CSV ou HTML pour la version du rapport envoyé par courriel.

Tous les rapports avec un état Terminé sont stockés au format HTML 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 183).

Rechercher et afficher des tâches

Vous pouvez afficher les tâches dans une liste filtrée par les critères que vous choisissez. Pour chaque tâche, vous pouvez afficher des détails et un historique.

Remarque : 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 de la tâche que vous souhaitez afficher.
3. Filtrez la liste davantage en sélectionnant une ou plusieurs tâches, un ou plusieurs états ou un ou plusieurs propriétaires (Ctrl+clic).
4. Cliquez sur Afficher les tâches pour visualiser la liste de tâches.

Pour afficher l'historique d'une tâche :

- Sélectionnez la tâche et cliquez sur Historique des tâches.

Pour afficher les détails d'une tâche :

- Double-cliquez sur une tâche pour ouvrir une boîte de dialogue contenant les détails de la tâche.

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 246) pour plus d'informations 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 CommandCenter :** reportez-vous à ***Sauvegarde de CC-SG*** (à la page 186)
   - **Sauvegarder la configuration du dispositif :** reportez-vous à ***Sauvegarde de la configuration d'un dispositif*** (voir "Mise à niveau de la configuration d'un dispositif" à la page 53)
   - **Copier la configuration du dispositif :** reportez-vous à ***Copie de la configuration du dispositif*** (voir "Copie de la configuration d'un dispositif" à la page 58)
   - **Regrouper la gestion de l'alimentation :** reportez-vous à ***Gestion de l'alimentation d'un groupe de nœuds*** (à la page xx)
   - **Gestion de l'alimentation des prises :** reportez-vous au **manuel d'utilisation CC-SG**.
   - **Effacer les journaux :** reportez-vous à ***Configuration de l'activité d'enregistrement*** (à la page 210).
   - **Redémarrer les dispositifs :** reportez-vous à ***Redémarrage d'un dispositif*** (à la page 59)
   - **Restaurer la configuration du dispositif :** reportez-vous à ***Restauration des configurations de dispositifs*** (à la page 54) (ne s'applique pas aux groupes de dispositifs)
   - **Mise à niveau du firmware du dispositif (dispositif individuel ou groupe de dispositifs) :** reportez-vous à ***Programmer la mise à niveau du firmware d'un dispositif*** (à la page 246).

- **Générer tous les rapports :** reportez-vous à ***Rapports*** (à la page 171).

6. Cliquez sur l'onglet Périodicité. L'onglet Périodicité est désactivé pour les tâches de mise à niveau du firmware du dispositif.
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 Chaque jour si vous souhaitez que la tâche se répète chaque jour de la semaine. Cliquez sur la case d'option 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 s'ouvre, 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 vos modifications.

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. Cliquez sur 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 niveau 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. Indiquez si une nouvelle tentative doit être effectuée pour les mises à niveau ayant échoué.

   a. Cliquez sur l'onglet Nouvelle tentative.

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

   c. 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. 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 l'onglet Notification.

   b. Cliquez sur Ajouter, entrez l'adresse électronique dans la fenêtre qui s'ouvre, puis cliquez sur OK.

c. Sélectionnez En cas d'échec si vous souhaitez envoyer un message si une mise à niveau échoue.

d. 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 184).

Modifier une tâche programmée

Vous pouvez modifier une tâche programmée avant son exécution.

Pour modifier une tâche programmée :

1. Sélectionnez la tâche à modifier.
2. Cliquez sur Modifier.
3. Modifiez les spécifications de la tâche selon vos besoins. Reportez-vous à ***Programmer une tâche*** (à la page 244) et ***Programmer la mise à niveau du firmware d'un dispositif*** (à la page 246) pour obtenir une description des onglets.
4. Cliquez sur Mettre à jour pour enregistrer vos modifications.

Reprogrammer une tâche

La fonction Enregistrer sous du Gestionnaire des tâches vous permet de reprogrammer une tâche terminée que vous souhaitez exécuter à nouveau. Il s'agit également d'une manière pratique de créer une tâche similaire à une tâche terminée.

Pour reprogrammer une tâche :

1. Choisissez Administration > Tâches.
2. Sur la page Gestionnaire des tâches, sélectionnez la tâche à reprogrammer. Utilisez les critères de filtre pour rechercher la tâche.
3. Cliquez sur Enregistrer sous.
4. Dans la fenêtre Enregistrer la tâche sous qui s'ouvre, les onglets sont alimentés à l'aide des informations de la tâche configurée précédemment.
5. Modifiez les spécifications de la tâche selon vos besoins. Reportez-vous à ***Programmer une tâche*** (à la page 244) et ***Programmer la mise à niveau du firmware d'un dispositif*** (à la page 246) pour obtenir une description des onglets.

6. Cliquez sur OK pour enregistrer vos modifications.

Programmer une tâche similaire à une autre

Vous pouvez utiliser une tâche configurée précédemment comme modèle pour programmer une nouvelle tâche dotée de spécifications similaires.

Pour programmer une tâche similaire à une autre :

- Reportez-vous à ***Reprogrammer une tâche*** (à la page 248).

Supprimer une tâche

Vous pouvez supprimer une tâche pour la retirer du Gestionnaire des tâches. Vous ne pouvez pas supprimer une tâche en cours d'exécution.

Pour supprimer une tâche :

- Sélectionnez la tâche, puis cliquez sur Supprimer.

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 si vous souhaitez 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 courriel 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. Actuellement, seule l'option « CC-NOC 5.2 ou supérieur » est disponible.

4. Entrez un nom descriptif pour 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 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. 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 184).*

7. 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.

8. 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.
9. 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.
10. Cliquez sur Suivant.
11. Entrez 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. Echangez les codes de passe oralement ou par écrit.

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 cinq 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. Sélectionnez 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.

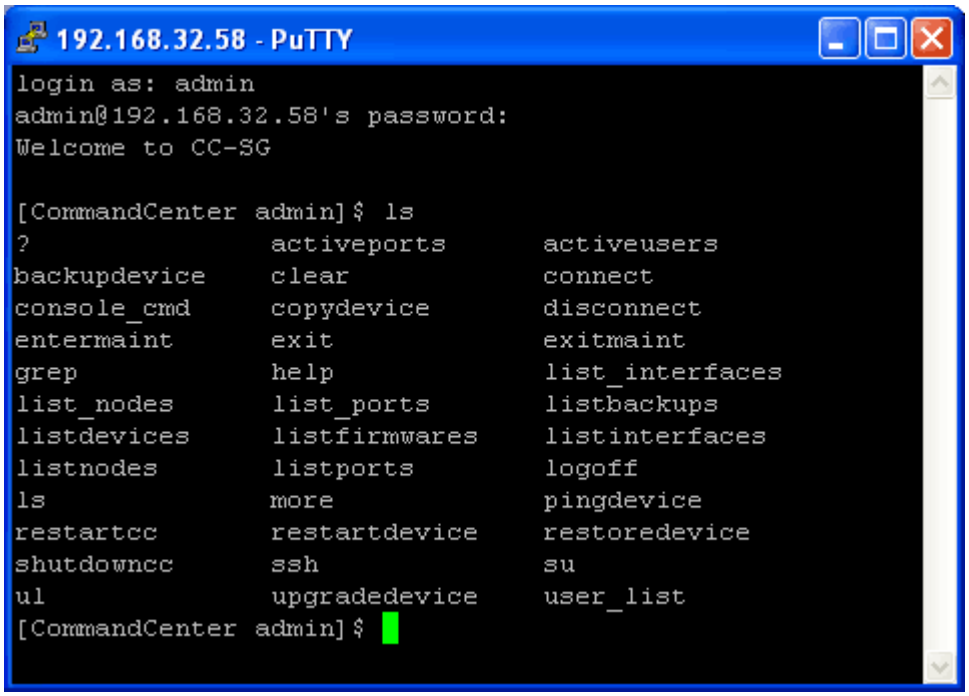
Les administrateurs qui utilisent SSH pour accéder à CC-SG ne peuvent pas déconnecter un utilisateur SSH CC Super-User, mais ils peuvent déconnecter tous les autres utilisateurs du client SSH, administrateurs système compris.

Pour accéder à CC-SG via SSH :

1. Lancez un client SSH, tel que PuTTY.
2. Spécifiez l'adresse IP du CC-SG.
3. Spécifiez le numéro de port SSH. La valeur par défaut est 22. La configuration du port pour l'accès SSH s'effectue dans le Gestionnaire de sécurité. Reportez-vous à ***Gestionnaire de sécurité*** (à la page 228).
4. Ouvrez la connexion.
5. Connectez-vous en utilisant vos nom d'utilisateur et mot de passe CC-SG.
6. Une invite de commande apparaît.

Pour afficher toutes les commandes SSH :

- A l'invite, tapez ls pour afficher toutes les commandes disponibles.



Obtenir de l'aide sur les commandes SSH

Vous pouvez obtenir une aide limitée sur toutes les commandes à la fois. Vous pouvez également obtenir une aide détaillée sur une seule commande à la fois.

Pour obtenir de l'aide sur une seule commande SSH :

1. A l'invite, tapez la commande souhaitée, suivie d'un espace et de `-h`. Par exemple :

   ```
   connect -h
   ```

2. Des informations sur la commande, ses paramètres et son utilisateur apparaissent à l'écran.

Pour obtenir de l'aide sur toutes les commandes SSH :

1. A l'invite, tapez la commande suivante :

   ```
   help
   ```

2. Une brève description et un exemple apparaissent pour chaque commande SSH.

Commandes SSH et paramètres

Le tableau suivant répertorie toutes les commandes disponibles dans SSH. Vous devez disposer des privilèges appropriés dans CC-SG pour accéder à chaque commande.

Certaines commandes sont dotées de paramètres supplémentaires que vous devez taper pour exécuter la commande. Pour plus d'informations sur la saisie des commandes, reportez-vous à ***Astuces sur les commandes*** (à la page 257).

Pour lister les ports actifs :

```
activeports
```

Pour lister les utilisateurs actifs :

```
activeusers
```

Pour sauvegarder une configuration de dispositif :

```
backup device <[-host <hôte>] | [-id <id_dispositif>]>
nom_sauvegarde [description]
```

Pour effacer l'écran :

```
clear
```

Pour établir la connexion à un port série :

Si <nom_port> ou <nom_dispositif> contient des espaces, il doit être entouré de guillemets.

```
connect [-d <nom_dispositif>] [-e <car_echap>] <[-i
<id_interface>] | [-n <nom_port>] | [id_port]>
```

Pour copier la configuration d'un dispositif à un autre. Dispositifs SX avec le même nombre de ports uniquement :

```
copydevice <[-b <id_sauvegarde>] |
[hôte_dispositif_source]> hôte_dispositif_cible
```

Pour fermer une connexion de port :

```
disconnect <[-u <nomutilisateur>] [-p <id_port>] [-id
<id_connexion>]>
```

Pour entrer en mode de maintenance :

```
entermaint minutes [message]
```

- **Pour quitter le mode de maintenance :**

```
exitmaint
```

- **Pour rechercher du texte dans le flux de sortie redirigé :**

```
grep terme_recherche
```

- **Pour afficher l'écran d'aide sur toutes les commandes :**

```
help
```

- **Pour répertorier les sauvegardes de configuration du dispositif disponibles :**

```
listbackups <[-id <id_dispositif>] | [hôte]>
```

- **Pour lister les dispositifs disponibles :**

```
listdevices
```

- **Pour répertorier les versions de firmware disponibles pour la mise à niveau :**

```
listfirmwares <[-id <id_dispositif>] | [hôte] >
```

- **Pour lister toutes les interfaces :**

```
listinterfaces [-id <id_nœud>]
```

- **Pour lister tous les nœuds :**

```
listnodes
```

- **Pour lister tous les ports :**

```
listports [[-id <id_dispositif>] | [hôte]
```

- **Pour déconnecter un utilisateur :**

```
logoff  [-u <nomutilisateur>] message
```

- **Pour lister toutes les commandes :**

```
ls
```

- **Pour spécifier la pagination :**

```
more [-p <taille_page>]
```

- **Pour envoyer une commande ping à un dispositif :**

```
pingdevice <[-id <id_dispositif>] | [hôte]>
```

Pour redémarrer CC-SG :

```
restartcc minutes [message]
```

Pour redémarrer un dispositif :

```
restartdevice <[-id <id_dispositif>] | [hôte]>
```

Pour restaurer une configuration de dispositif :

```
restoredevice <[-host <hôte>] | [-id <id_dispositif>]>
[id_sauvegarde]
```

Pour arrêter CC-SG :

```
shutdowncc minutes [message]
```

Pour ouvrir une connexion SSH à un dispositif SX :

```
ssh  [-e <car_echap>] <[-id <id_dispositif>] | [hôte]>
```

Pour modifier un utilisateur :

```
su [-u <nom_utilisateur>]
```

Pour mettre à niveau le firmware d'un dispositif :

```
upgradedevice <[-id <id_dispositif>] | [hôte]>
```

Pour lister tous les utilisateurs actuels :

```
userlist
```

Pour quitter la session SSH :

```
exit
```

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 et sigles*** (à la page 2).
- Les commandes `copydevice` et `restartdevice` ne s'appliquent qu'à certains dispositifs Raritan. Dominion SX et les serveurs IPMI ne sont pas pris en charge par ces commandes.
- Les éléments d'une commande figurant entre crochets sont facultatifs. Vous n'êtes pas obligé de les utiliser.
- Certaines commandes contiennent deux segments séparés par le signe Or : |

  Vous devez entrer un des éléments indiqués de la commande, pas les deux.
- Les éléments de commande figurant entre chevrons indiquent le texte que vous devez taper. Ne tapez pas les chevrons. Par exemple :

Syntaxe de commande	Valeur de l'ID du dispositif	Vous devez taper
`ssh -id <id_dispositif>`	100	`ssh -id 100`

- Le caractère d'échappement par défaut est un tilde suivi d'un point. Par exemple :

  `~.`

  Reportez-vous à ***Mettre fin aux connexions SSH*** (à la page 260) pour plus d'informations sur l'utilisation du caractère d'échappement et la commande exit.

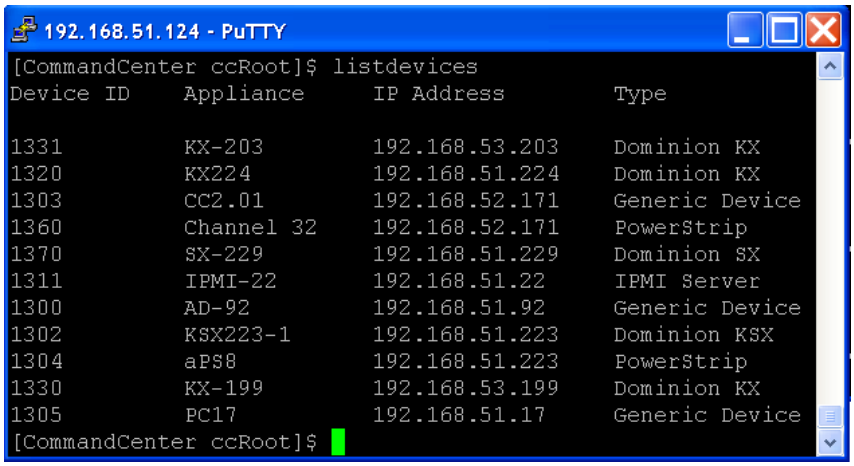
L'utilisation du caractère d'échappement dans le terminal ou le client Linux peut poser problème. Raritan vous recommande de définir un nouveau caractère d'échappement lors de l'établissement d'une connexion au port. La commande est `connect [-e <caractère_échapp>] [id_port]`. Par exemple, pour utiliser m comme caractère d'échappement lors de la connexion à un port dont l'id est 2360, entrez `connect -e m 2360`.

Créer une connexion SSH à un dispositif série

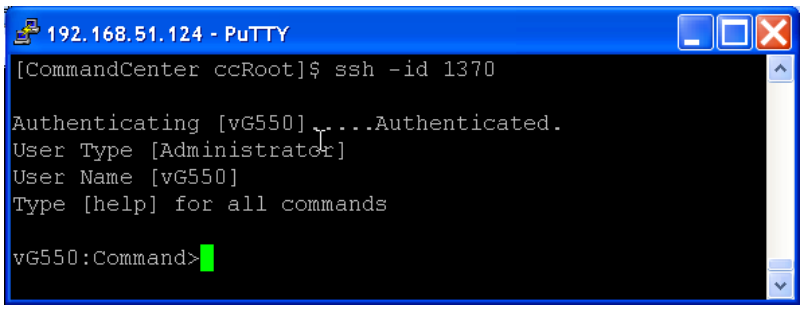
Vous pouvez créer une connexion SSH à un dispositif série pour effectuer des opérations administratives sur ce dernier. Une fois la connexion établie, les commandes administratives prises en charge par le dispositif série sont disponibles.

Remarque : avant de vous connecter, assurez-vous que le dispositif série a été ajouté à l'unité CC-SG.

1. Tapez `listdevices` pour vérifier que le dispositif série a été ajouté à CC-SG.



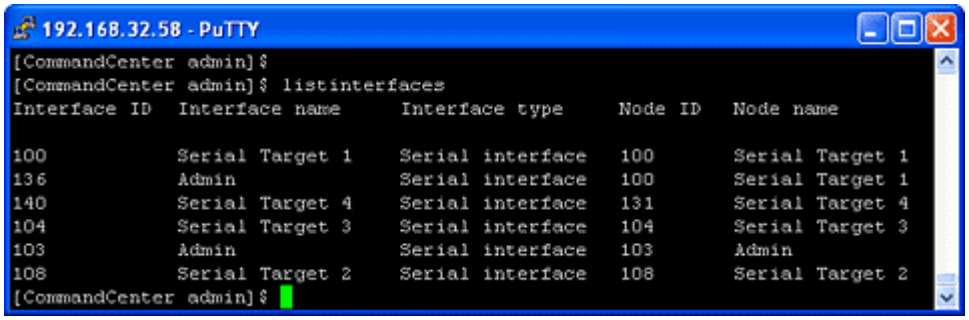
2. Connectez-vous au dispositif en tapant `ssh -id <id_dispositif>`.
   Par exemple, à partir de la figure ci-dessus, vous pouvez vous connecter à SX-229 en entrant `ssh -id 1370`.



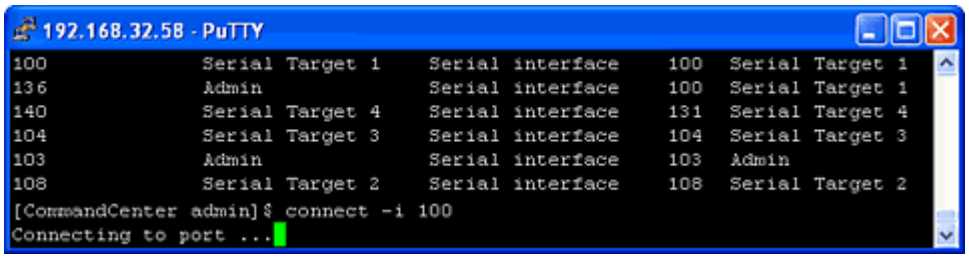
Utiliser SSH pour se connecter à un nœud via une interface série hors bande

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. 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.

Commande	Alias	Description
`help`	`?,h`	Imprime l'écran d'aide.

Mettre fin aux connexions SSH

Vous pouvez établir des connexions SSH à CC-SG uniquement, ou établir une connexion à CC-SG, puis à un port, dispositif ou nœud géré par CC-SG. Il existe plusieurs manières de terminer ces connexions, selon la partie à laquelle vous souhaitez mettre fin.

Pour mettre fin entièrement à la connexion SSH à CC-SG :

Cette commande termine la connexion SSH dans son intégralité, connexions établies à des port, dispositif ou nœud via CC-SG comprises.

- A l'invite, tapez la commande suivante et appuyez sur la touche Entrée :

```
exit
```

Pour mettre fin à une connexion à un port, dispositif ou nœud en restant connecté à CC-SG :

Vous pouvez utiliser le caractère d'échappement pour mettre fin à une connexion à un port, dispositif ou nœud en gardant la connexion à CC-SG ouverte.

Le caractère d'échappement par défaut est un tilde suivi d'un point.

- A l'invite, tapez la commande suivante et appuyez sur Entrée :

```
~.
```

L'utilisation du caractère d'échappement dans le terminal ou le client Linux peut poser problème. Raritan vous recommande de définir un nouveau caractère d'échappement lors de l'établissement d'une connexion au port. La commande est `connect [-e <caractère_échapp>] [id_port]`. Par exemple, pour utiliser m comme caractère d'échappement lors de la connexion à un port dont l'id est 2360, entrez `connect -e m 2360`.

Port d'administration série

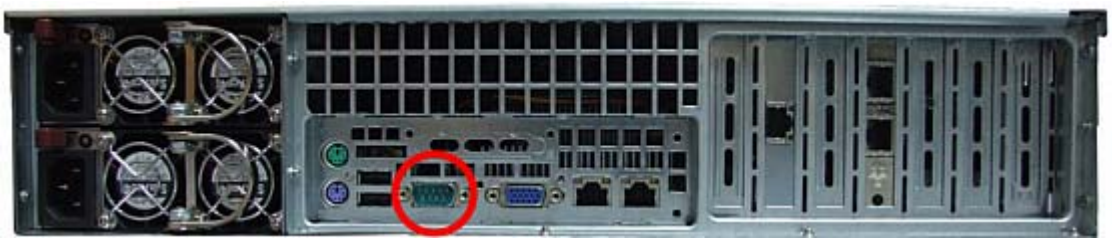
Le port d'administration série sur CC-SG peut être connecté directement à un dispositif série Raritan, tel que Dominion SX ou KSX.

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 V1 :

Port d'administration série E1 :

- OU -



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.

Recherche de votre numéro de série CC-SG

Pour trouver votre numéro de série CC-SG :

1. Connectez-vous au client Admin.

2. Choisissez Aide > A propos de Raritan Secure Gateway.
3. Une nouvelle fenêtre s'ouvre présentant votre numéro de série CC-SG.

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.

Vous devez accepter l'accord de licence d'utilisateur final avant d'ajouter un client API de services Web à CC-SG. Vous pouvez ajouter jusqu'à cinq clients WS-API. Reportez-vous au manuel SDK des services Web CC-SG pour plus d'informations sur l'utilisation de l'interface API.

Pour ajouter une interface API de services Web :

1. Sélectionnez Accès > Ajouter une API de services Web. Cette option n'est disponible qu'aux utilisateurs disposant du privilège CC Setup and Control.
2. Prenez connaissance de l'accord de licence d'utilisateur final.
   - Vous pouvez copier et coller le texte pour l'enregistrer, ou choisir Passerelle sécurisée > Imprimer.
   - Une fois la configuration terminée, cet accord de licence sera également disponible dans le menu Accès.
3. Cliquez sur Accepter. La fenêtre Configuration de l'API de services Web s'ouvre.
4. Entrez les données demandées sur le client de services Web.
   - Nom de client de services Web : 64 caractères au maximum.
   - Adresse IP/nom d''hôte : 64 caractères au maximum.
   - Port de services Web HTTPS : champ en lecture seule. CC-SG utilise le port 9443 lorsque l'établissement des approbations est généré.
   - Nom de fournisseur avec licence : 64 caractères au maximum.
   - Certifier le nom du fournisseur : ouvre la page de certification des fournisseurs Raritan.
   - URL de l''application cliente : lorsque l'URL est spécifiée, une option de menu est disponible pour autoriser l'accès à l'application cliente de services Web depuis CC-SG.
5. Générez un certificat auto-signé.

a. Mode de chiffrement : si l'option Chiffrement AES obligatoire entre le client et le serveur est sélectionnée dans l'écran Administration > Sécurité > Chiffrement, AES-128 est la valeur par défaut. Si le chiffrement AES n'est pas obligatoire, DES 3 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.

6. Cliquez sur Générer le certificat. Le texte apparaît dans la zone Certificat.
7. Cliquez sur Enregistrer dans le fichier pour sauvegarder le certificat dans un fichier .P12.
8. Cliquez sur Ajouter pour enregistrer vos modifications.

Chapitre 16 Console de diagnostic

La console de diagnostic est une interface basée sur des menus, non graphique, qui fournit un accès local à CC-SG. Elle est accessible depuis un port série ou KVM. Reportez-vous à ***Accéder à la console de diagnostic via un port VGA/clavier/souris*** (à la page 264). Vous pouvez également y accéder depuis un client SSH (Secure Shell), tel que PuTTY ou OpenSSH Client. Reportez-vous à ***Accéder à la console de diagnostic via SSH*** (à la page 264).

La console de diagnostic comporte deux interfaces :

1. Console d'état : reportez-vous à ***A propos de la console d'état*** (à la page 265).
2. Console d'administrateur : reportez-vous à ***A propos de la console d'administrateur*** (à la page 272).

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

Accéder 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 Entrée pour afficher une invite de connexion à l'écran.

Accéder 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.
3. Spécifiez 23 pour le port. Le port SSH par défaut est 22. Si vous ne le remplacez pas par 23, le client SSH accède à l'interface de ligne de commande de CC-SG, et non à la console de diagnostic.

4. Cliquez sur le bouton permettant la connexion. Une fenêtre s'ouvre pour vous demander vos identifiants de connexion.

Console d'état

A propos de la console d'état

- La console d'état permet de vérifier 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.
- Vous pouvez configurer l'unité CC-SG pour qu'elle présente les informations de la console d'état via une interface Web. Vous devez activer les options relatives à la console d'état Web. Reportez-vous à ***Accéder à la console d'état depuis le navigateur Web*** (voir "Accéder à la console d'état depuis un navigateur Web" à la page 265). Les informations de la console d'état via le Web peuvent être protégées par un compte et un mot de passe.

Accès à la console d'état

Les informations de la console d'état sont visibles de différentes façons : port VGA/clavier/souris, SSH ou navigateur Web.

Accéder à la console d'état via un port VGA/clavier/souris ou SSH

Pour accéder à la console d'état via un port VGA/clavier/souris ou SSH :

1. Accédez à la console de diagnostic. Reportez-vous à ***Accès à la console de diagnostic*** (à la page 264).
2. A l'invite de connexion, tapez status.
3. Les données système actuelles s'affichent.

Accéder à la console d'état depuis un navigateur Web

Pour récupérer les informations de console d'état sur le Web, vous devez activer les options pertinentes de la console de diagnostic, et le serveur Web doit être disponible et fonctionnel.

1 : Activer les options relatives à la console d'état Web dans la console de diagnostic :

1. Choisissez Operation > Diagnostic Console Config (configuration de la console de diagnostic).
2. Dans la liste Ports, sélectionnez Web.

3. Dans la liste Status, cochez la case en regard de Web.
4. Cliquez sur Save (Enregistrer).

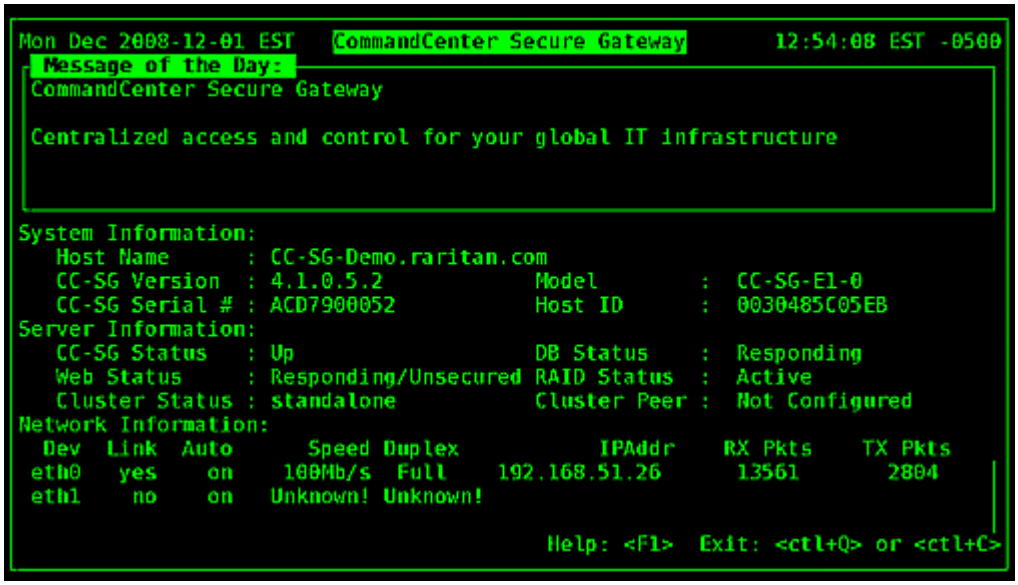
2: Accéder à la console d'état depuis un navigateur Web :

1. Dans un navigateur Internet pris en charge, entrez l'URL : `http(s)://<adresse_IP>/status/` où `<adresse_IP>` indique l'adresse IP de l'unité CC-SG. Notez que la barre oblique (/) suivant /status est obligatoire. Par exemple, `https://10.20.3.30/status/`.
2. Une page d'état s'ouvre. Elle contient les mêmes informations que la console d'état.

Informations de la console d'état

Console d'état via un port VGA/clavier/souris ou SSH

Après que vous avez tapé status à l'invite de connexion, la console d'état en lecture seule apparaît.



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. Les informations de cet écran sont actualisées toutes les cinq secondes environ.

La console d'état se compose de quatre zones principales :

- Titre CC-SG, date et heure
- Message du jour
- Etat du système, du serveur et du réseau
- Rappel des touches de navigation

Titre CC-SG, date et heure

Le titre CC-SG est permanent et indique aux utilisateurs qu'ils sont connectés à une unité CC-SG.

La date et l'heure en haut de l'écran indiquent la dernière interrogation des données sur l'unité CC-SG. La date et l'heure reflètent les valeurs de temps enregistrées sur le serveur CC-SG.

Message du jour

La zone Message du jour (MOTD) affiche les cinq premières lignes du MOTD entrées dans le client Admin de CC-SG. Chaque ligne contient 78 caractères au maximum et ne prend en charge aucun formatage spécial.

Etat du système, du serveur et du réseau

Cette zone de l'écran donne des informations sur l'état de divers composants CC-SG. Le tableau suivant explique les informations et les états de CC-SG et de sa base de données :

Informations	Description
Host Name (Nom de l'hôte)	Nom de domaine complètement qualifié de CC-SG (NDCQ). Il se compose du nom d'hôte de l'unité et du nom de domaine associé.
CC-SG Version (Version de CC-SG)	Version de firmware actuelle de CC-SG. Il s'agit d'une valeur à cinq chiffres.
CC-SG Serial #	Numéro de série de CC-SG.
Model (Modèle)	Type de modèle de CC-SG.
Host ID (ID d'hôte)	Nombre pour l'octroi d'une licence à l'unité CC-SG.
CC-SG Status (Etat de CC-SG)	Etat du serveur CC-SG, qui traite la plupart des demandes des utilisateurs. Les états disponibles sont les suivants :

Informations	Description	
	Up (Disponible)	CC-SG est disponible et accepte les demandes des utilisateurs.
	Down (Non disponible)	CC-SG peut être arrêté ou en cours de redémarrage. Si l'état Down se poursuit, essayez de redémarrer CC-SG.
	Restarting (Redémarrage)	CC-SG est en cours de redémarrage.
DB Status (Etat de la BD)	Le serveur CC-SG utilise une base de données (BD) interne dans le cadre de ses opérations. Cette base de données doit être disponible et réactive pour permettre le fonctionnement de CC-SG. Les états disponibles sont les suivants :	
	Responding (Réponse)	La base de données CC-SG est disponible.
	Up (Disponible)	Certains sous-programmes de la base de données sont en cours d'exécution, mais elle ne répond pas aux demandes locales.
	Restoring (Restauration)	CC-SG est en cours d'auto-restauration et les interrogations de la base de données sont interrompues pour le moment.
	Down (Non disponible)	Le serveur de base de données n'a pas encore démarré.
Web Status (Etat Web)	L'accès au serveur CC-SG s'effectue essentiellement par le Web. Ce champ indique l'état du serveur Web et les états disponibles sont les suivants :	
	Responding/ Unsecured (Réponse/Non sécurisé)	Le serveur Web est disponible et répond aux demandes http (non sécurisées).
	Responding/ Secured (Réponse/Sécurisé)	Le serveur Web est disponible et répond aux demandes https (sécurisées).

Informations	Description	
	Up (Disponible)	Certains processus du serveur Web sont en cours d'exécution, mais les demandes locales restent sans réponse.
	Down (Non disponible)	Le serveur Web n'est pas disponible pour le moment.
RAID Status (Etat Raid)	CC-SG stocke ses données sur deux disques en miroir (RAID-1). Les états disponibles pour les disques RAID sont les suivants :	
	Active (Actif)	Le RAID est entièrement opérationnel.
	Degraded (Altéré)	Un ou plusieurs lecteurs de disque rencontrent des problèmes. Contactez l'assistance technique Raritan pour obtenir de l'aide.
Cluster Status (Etat du cluster)	CC-SG peut fonctionner conjointement à un autre CC-SG pour former un cluster. Reportez-vous à ***Configuration des clusters CC-SG*** (à la page 219). Si le champ affiche « standalone » (autonome), l'unité CC-SG ne se trouve pas dans une configuration en cluster. Sinon, le champ affiche l'état du cluster.	
Cluster Peer (Pair sur cluster)	Si l'unité CC-SG se trouve dans une configuration en cluster, le champ affiche l'adresse IP de l'autre unité du cluster.	
Network Information (Informations relatives au réseau)	Pour chaque interface réseau, une table déroulante est disponible pour l'affichage des informations.	
	Dev	Nom interne de l'interface.
	Link (Lien)	Etat de l'intégrité de liens, c'est-à-dire, indique si ce port est connecté à un port de commutateur Ethernet opérationnel via un câble intact.
	Auto	Indique si la négociation automatique est appliquée à ce port.
	Speed (Vitesse)	Vitesse de fonctionnement de cette interface : 10, 100 ou 1000 Mbits par seconde.

Informations	Description	
	Duplex	Indique si l'interface est Full-duplex (bidirectionnelle simultanée) ou Half-duplex (bidirectionnelle non simultanée).
	IPAddr	Adresse Ipv4 actuelle de cette interface.
	RX -Pkts	Nombre de paquets IP reçus sur cette interface depuis l'amorçage de CC-SG.
	TX -Pkts	Nombre de paquets IP transmis sur cette interface depuis l'amorçage de CC-SG.

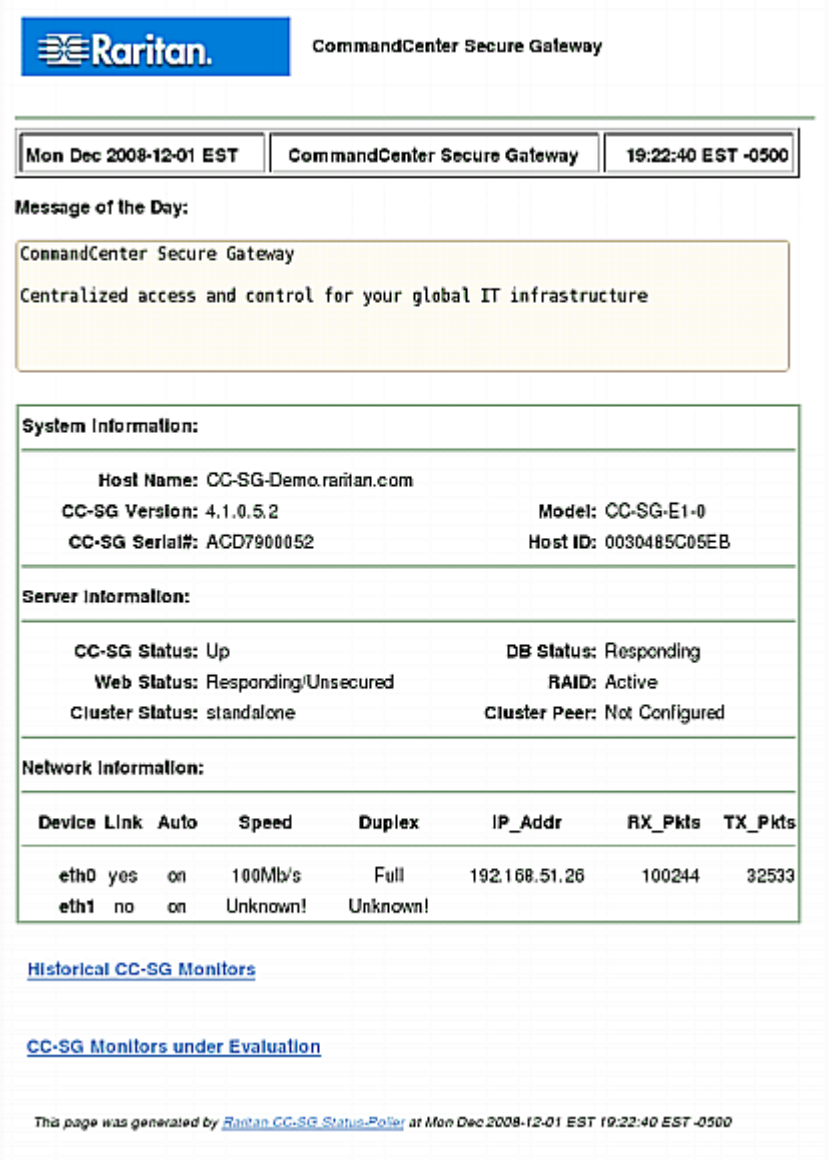
Rappel des touches de navigation

La ligne inférieure de l'écran affiche les combinaisons de touches pour l'appel de l'aide et la fermeture de la console d'état. La console d'état ignore les saisies au clavier autres que les touches décrites ci-dessous.

- Appuyez sur F1 pour appeler l'écran d'aide, qui affiche les options disponibles, ainsi que la version de la console de diagnostic.
- Appuyez sur Ctrl+L pour effacer l'écran actuel et le retracer avec les informations à jour. Vous pouvez actualiser l'écran une fois par seconde au maximum.
- Appuyez sur Ctrl+Q ou Ctrl+C pour quitter la console d'état.
- Vous pouvez utiliser les touches fléchées pour faire défiler l'écran Network Information horizontalement et verticalement lorsque les données qu'il contient dépassent l'affichage.

Console d'état depuis un navigateur Web

Après que vous vous êtes connecté à la console d'état depuis le navigateur Web, la page Web de la console d'état en lecture seule apparaît.



La page Web affiche les mêmes informations que la console d'état et actualise également celles-ci toutes les cinq secondes environ. Pour en savoir plus sur les liens des moniteurs CC-SG au bas de la page Web, reportez-vous à ***Afficher les rapports d'évolution des données d'historique*** (à la page 298) et ***Surveillance des disques CC-SG*** (à la page 336).

Console d'administrateur

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

Important : le compte admin de la console de diagnostic est distinct des compte et mot de passe admin CC Super User 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.

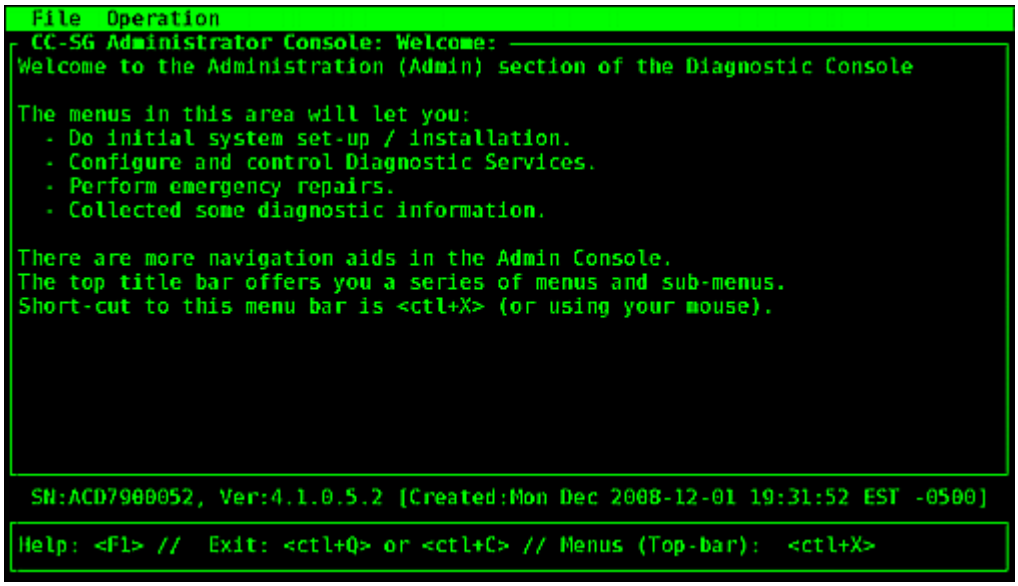
Accéder à la console d'administrateur

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.

Pour accéder à la console d'administrateur :

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 292) pour plus d'informations sur la définition de la force du mot de passe.

L'écran principal de la console d'administrateur apparaît.



Ecran de la console d'administrateur

L'écran de la console d'administrateur se compose de quatre zones principales.

- **Barre de menus :**

  Vous pouvez exécuter les fonctions de la console d'administrateur en activant la barre de menus. Appuyez sur Ctrl+X pour activer la barre de menus ou cliquez sur une option à l'aide de la souris si vous accédez à la console d'administrateur via le client SSH.

  Le menu File (Fichier) offre une autre option pour quitter la console de diagnostic. Le menu Operation offre quatre commandes de menu qui peuvent comporter un ou plusieurs sous-menus. Pour en savoir plus sur chaque commande de menu et sous-menu, reportez-vous aux autres sections relatives à la console d'administrateur.

- **Zone d'affichage principal :**

  Le contenu varie en fonction de l'opération sélectionnée.

- **Barre d'état :**

  La barre d'état se trouve juste au-dessus de la barre des touches de navigation. Elle affiche certaines informations système importantes, telles que le numéro de série, la version de firmware de CC-SG, et l'heure de chargement ou de mise à jour des données affichées dans la zone d'affichage principal. Des captures d'écran contenant ces informations peuvent être utiles lorsque vous signalez des problèmes à l'assistance technique Raritan.

- **Barre des touches de navigation** :

  Reportez-vous à ***Naviguer dans la console d'administrateur*** (à la page 274).

Naviguer dans la console d'administrateur

Utilisez des combinaisons de touches pour naviguer dans la console d'administrateur. 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+X	Activer la barre de menus. Sélectionnez des commandes dans le menu pour effectuer diverses opérations dans la console d'administrateur.
F1	Appeler l'écran d'aide, qui affiche les options disponibles, ainsi que la version de la console de diagnostic.
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.
Barre d'espacement	Sélectionner l'option en cours.
Entrée	Sélectionner l'option en cours.
Touche fléchée	Passer à des champs différents au sein d'une option.

Modifier 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 SSH. Pour accéder à la console d'état, un mécanisme supplémentaire, via le Web, est également disponible.

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 clients SSH, vous pouvez configurer le numéro de port à utiliser, s'il n'est pas encore employé par un autre service CC-SG. Pour l'accès Web à la console d'état, vous pouvez spécifier un compte, distinct des autres comptes du système, pour limiter l'accès. Sinon, n'importe quel utilisateur pouvant accéder à CC-SG via le Web peut accéder à la page Web de la console d'état.

Important : veillez à ne pas verrouiller tous les accès Administrateur ou Assistance sur site.

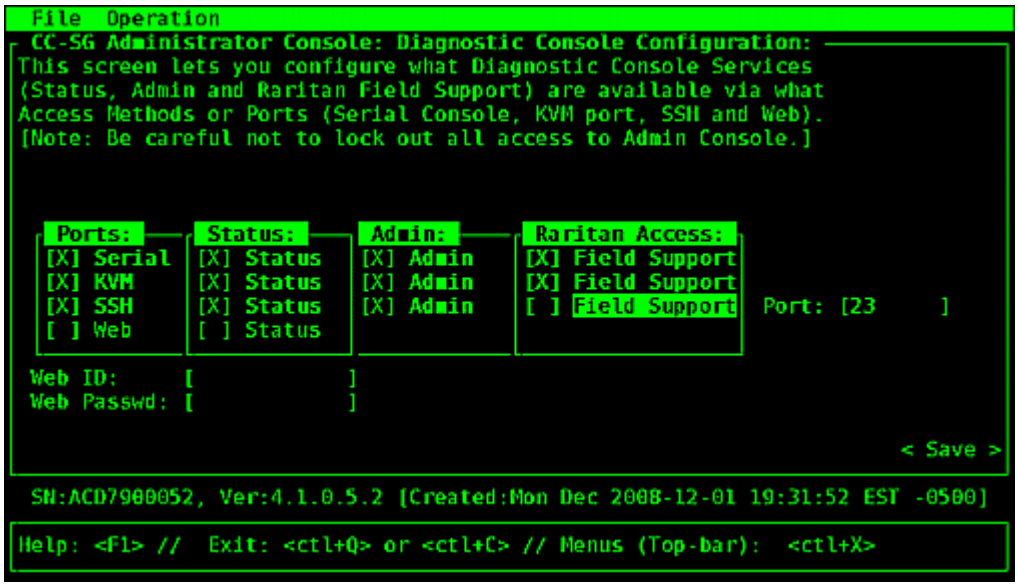
Pour modifier la configuration de la console de diagnostic :

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 quatre mécanismes d'accès à la console de diagnostic : port série (COM1), console KVM, SSH (réseau IP) et Web. 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.

   Si les options Web et Status sont activées, la page Web de la console d'état est toujours disponible si le serveur Web est disponible et fonctionnel. Pour limiter l'accès à la page Web de la console d'état, tapez un compte et un mot de passe.
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).

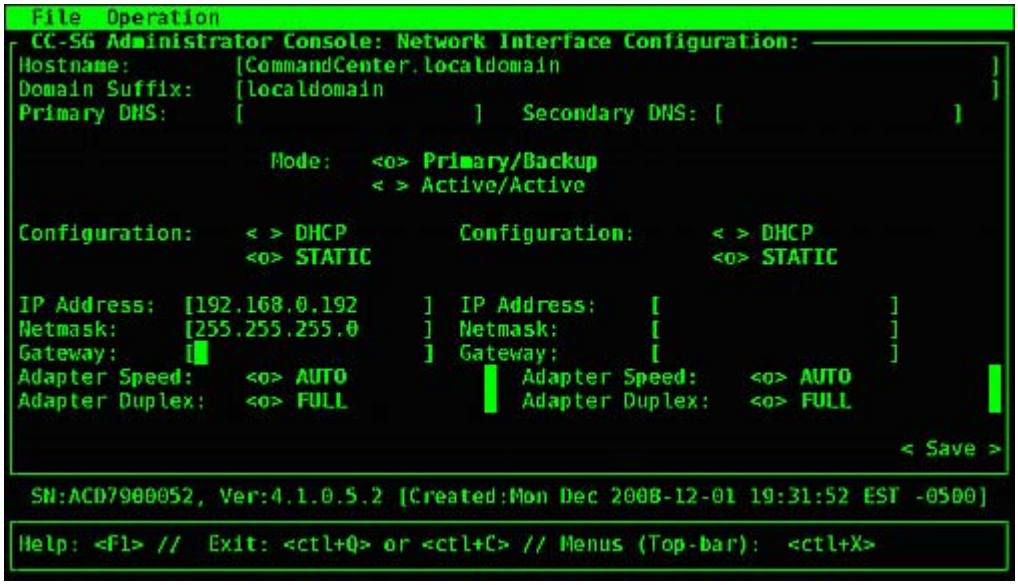


Modifier la configuration des interfaces réseau (Interfaces réseau)

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 (Client Admin) pour les paramétrer. Si vous souhaitez poursuivre, cliquez sur YES.



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 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 204).
   - 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, tapez une adresse IP (obligatoire), un masque réseau (obligatoire), une passerelle par défaut (facultatif), des DNS principal (facultatif) et secondaire (facultatif), et un nom de domaine dans le suffixe de domaine (facultatif).
   - Même si DHCP est utilisé pour déterminer la configuration IP d'une interface, vous devez indiquer une adresse IP et un masque réseau formatés correctement.

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 fléchées permettent d'y accéder. Appuyez sur la barre d'espacement pour sélectionner l'option affichée. Pour les vitesses de ligne de 1 Go, sélectionnez AUTO.
6. Si vous n'avez pas sélectionné AUTO dans le champ Adapter Speed, cliquez sur Adapter Duplex et utilisez les touches fléchées 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. Cliquez sur 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, appuyez sur ALT+F1. Six sessions de terminal sont disponibles de F1 à F6.

Envoyer une commande ping

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. Sélectionnez : **Facultatif.**

Option	Description
Show other received ICMP packets	Sortie détaillée, qui répertorie d'autres paquets ICMP reçus en plus des paquets ECHO_RESPONSE. Survient rarement.

Option	Description
No DNS Resolution	Ne résout pas les adresses des noms d'hôte.
Record Route	Enregistre la route. Active 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. 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. **Facultatif.**
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 ***Modifier les routes statiques*** (à la page 280).
6. Appuyez sur CTRL+C pour mettre fin à la session.

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.

Utiliser la détermination d'itinéraire

La détermination d'itinéraire (traceroute) 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. Sélectionnez : **Facultatif.**

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. 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. **Facultatif.**
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 ».

Modifier les routes statiques

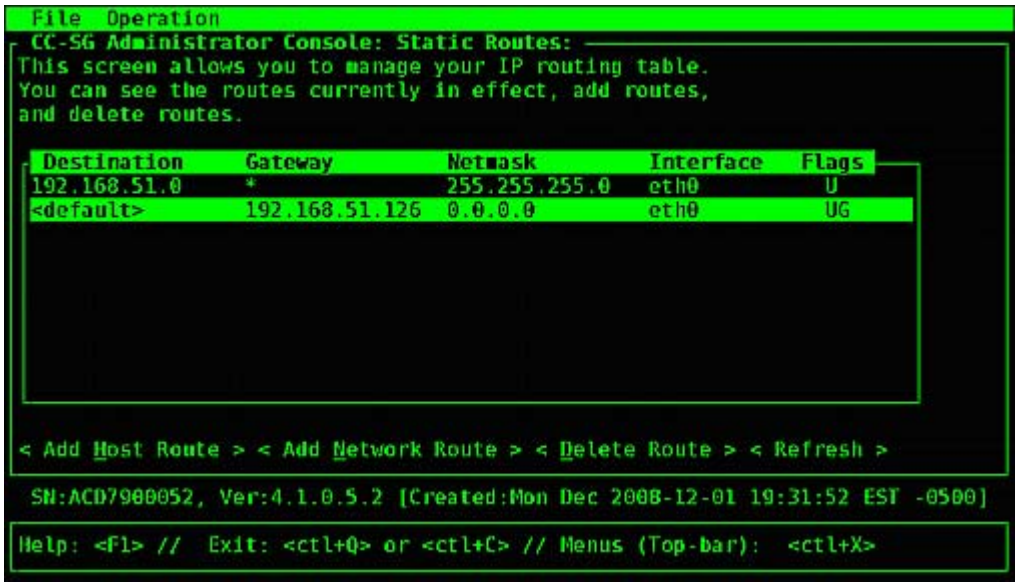
Dans Static Routes, vous pouvez consulter le tableau de l'acheminement IP actuel et modifier, ajouter ou supprimer des routes. L'utilisation et le placement précis des routes statiques peuvent réellement améliorer les performances de votre réseau, vous permettant ainsi de conserver de la bande passante 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 204). 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'ouvre. Vous pouvez ajouter une route IP associée au tableau d'acheminement en sélectionnant Add Host Route (Ajouter une route jusqu'à l'hôte) ou Add Network Route (Ajouter une route réseau). Les éléments du tableau d'acheminement peuvent être sélectionnés, et vous pouvez supprimer une route du tableau en choisissant Delete Route. Le bouton Refresh met à jour les informations d'acheminement du tableau ci-dessus.
   - L'option Add Host Route exige une adresse IP d'hôte de destination, et une adresse IP de passerelle et/ou un nom d'interface, comme illustré dans la console d'état.
   - L'option Add Network Route est similaire, mais exige un réseau de destination et un masque de réseau.
   - Avec chaque élément sélectionné ou mis en surbrillance dans la table, vous pouvez choisir Delete Route pour supprimer la route. La seule exception est la route associée à l'hôte et l'interface en cours, que CC-SG ne vous autorise pas à supprimer.

Même si vous pouvez supprimer toutes les autres routes, passerelle par défaut comprise, cette opération peut considérablement affecter la communication avec CC-SG.



Consulter des fichiers journaux dans la console de diagnostic

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, lorsque l'utilisateur entre dans la zone de liste des fichiers journaux par exemple, ou à la sélection d'une nouvelle option de tri. Le nom des fichiers est précédé 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

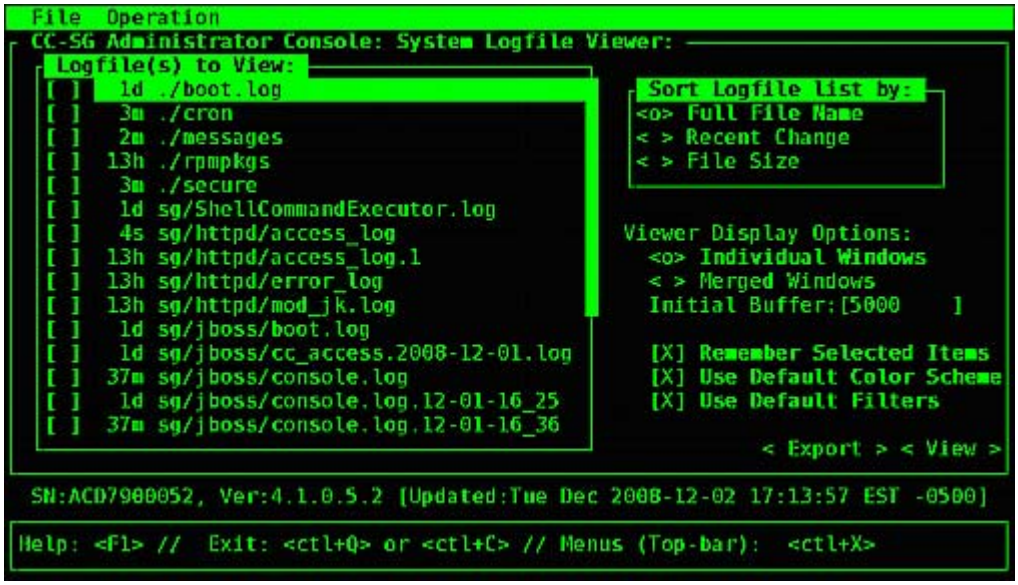
Tailles de fichier :

- B = octets
- K = Kilo-octets (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.



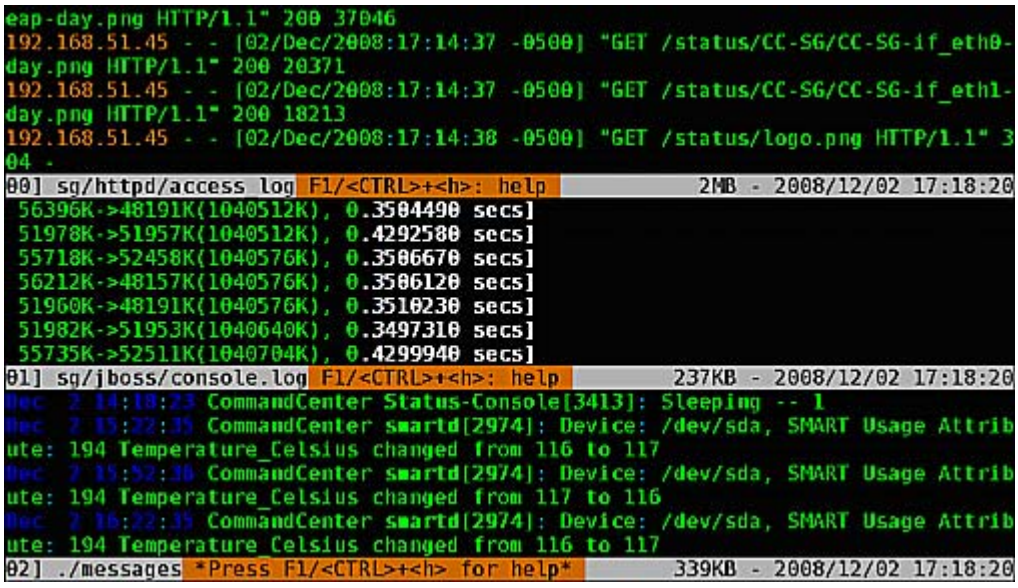
Pour trier les fichiers journaux de la liste de consultation :

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. 5 000 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.

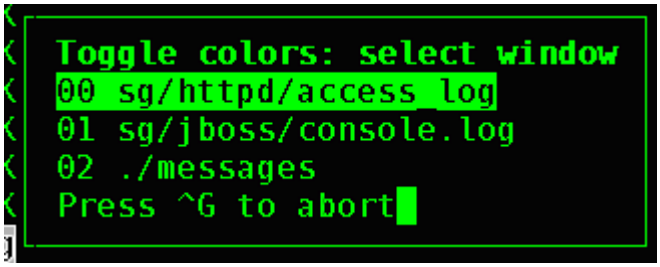
Option	Description
Use Default Filters	Si cette case est cochée, des filtres sont automatiquement appliqués à certains fichiers journaux.
Export	Cette option rassemble tous les fichiers journaux sélectionnés et les rend disponibles par accès Web pour qu'ils puissent être extraits et transmis à l'assistance 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 :



- Lorsque vous visualisez les fichiers journaux, appuyez sur les touches 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.

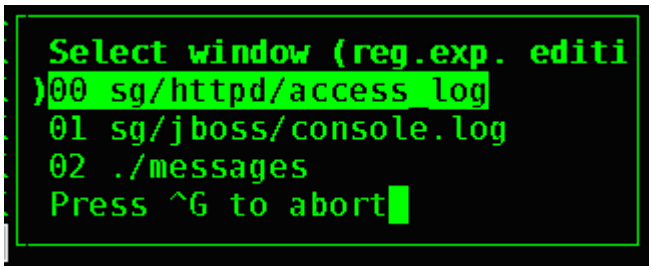


- Entrez I pour afficher les informations système.

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.

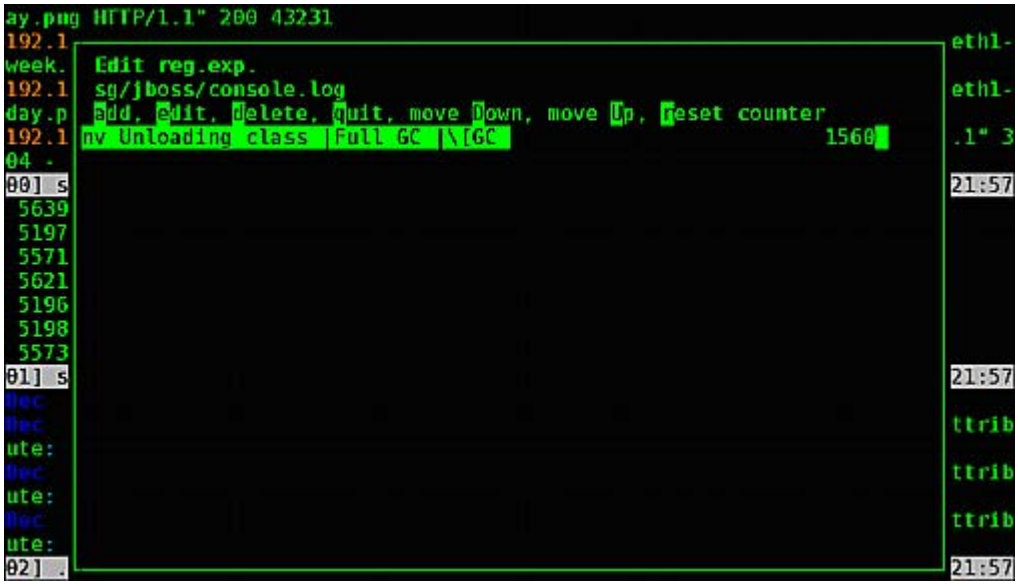
Pour filtrer un fichier journal à l'aide d'une expression standard :

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.



Redémarrer CC-SG avec la console de diagnostic

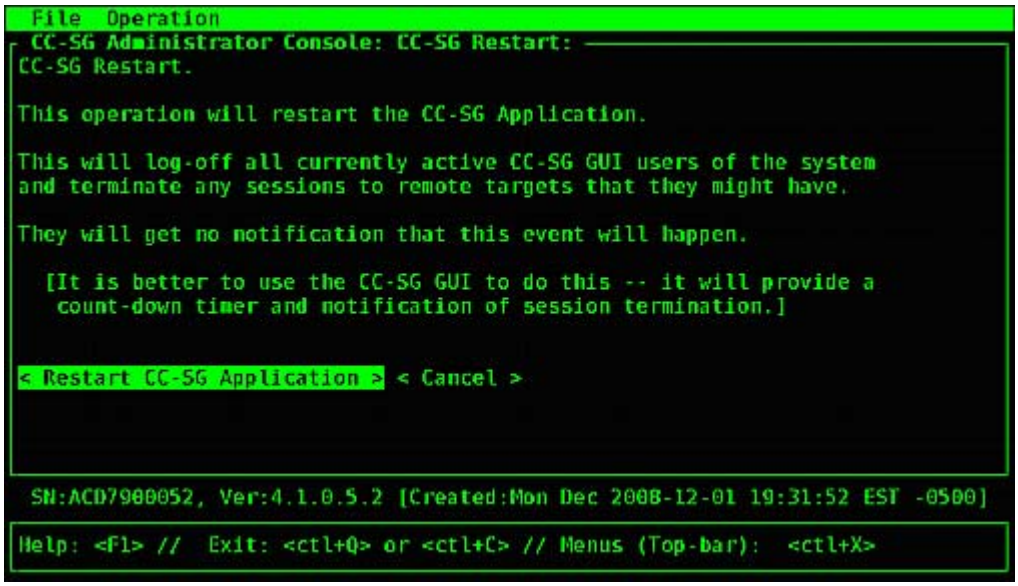
Le redémarrage de CC-SG déconnectera tous ses utilisateurs actuels et mettra fin à leurs sessions sur les serveurs cible distants.

Important : il est FORTEMENT recommandé de redémarrer l'unité CC-SG dans le client Admin, 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 193). Les utilisateurs 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.



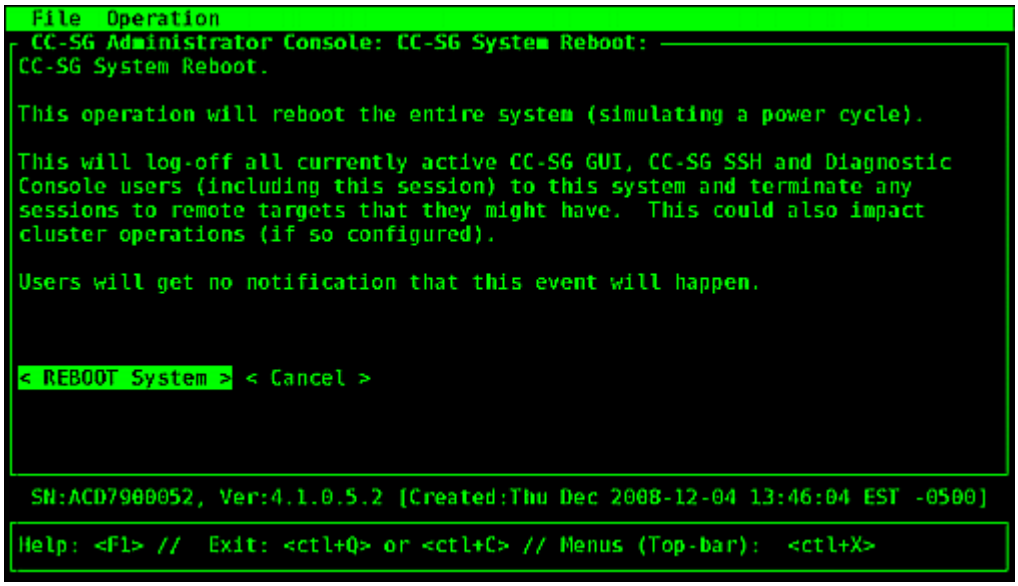
Réamorcer CC-SG avec la console de diagnostic

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 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 réamorcer CC-SG. Confirmez le réamorçage dans l'écran suivant pour continuer.



Mettre hors tension le système CC-SG à partir de la console de diagnostic

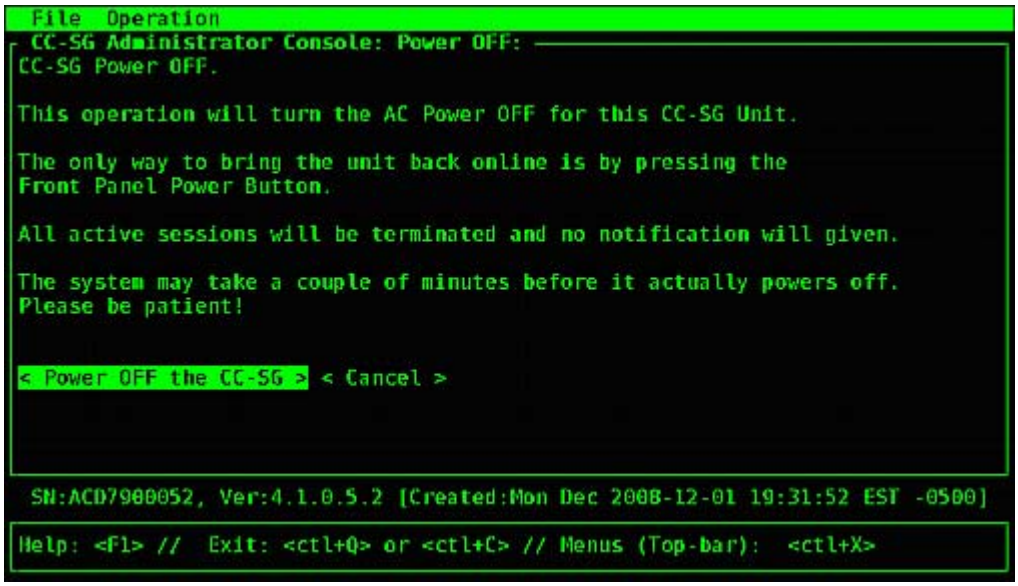
Cette option permet de mettre hors tension l'unité CC-SG. Les utilisateurs connectés ne recevront aucune notification. Les utilisateurs de CC-SG, SSH et la console de diagnostic (cette session comprise) seront déconnectés. Toutes les connexions aux serveurs cible distants seront interrompues.

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 Entrée pour couper l'alimentation de l'unité CC-SG. Confirmez la mise hors tension dans l'écran suivant pour continuer.



Réinitialiser le 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.

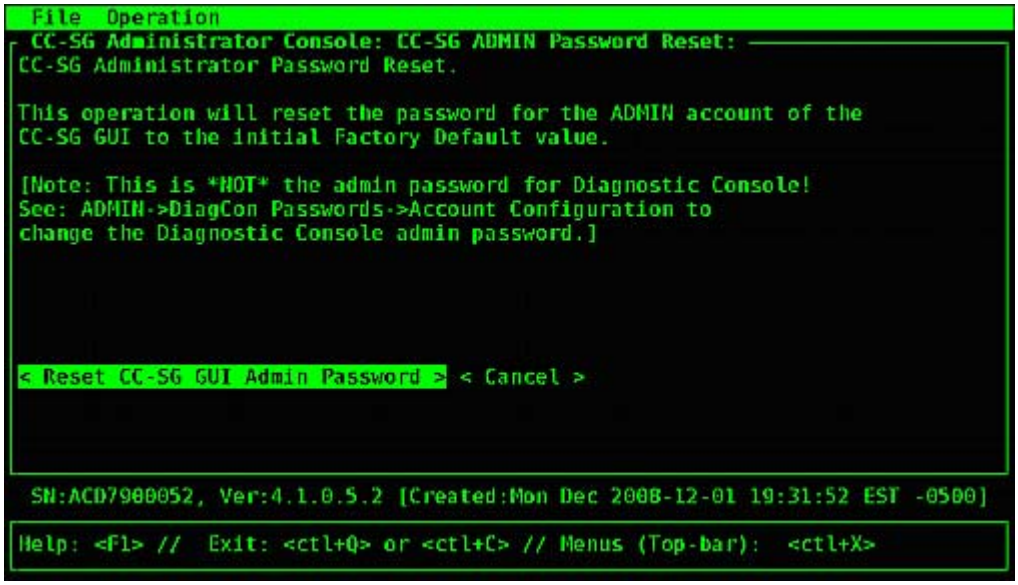
Mot de passe par défaut usine : raritan

Remarque : il ne s'agit pas du mot de passe de l'utilisateur admin de la console de diagnostic. Reportez-vous à **Paramètres des mots de passe de la console de diagnostic** *(à la page 292).*

▶ Pour réinitialiser le mot de passe admin de l'interface CC-SG :

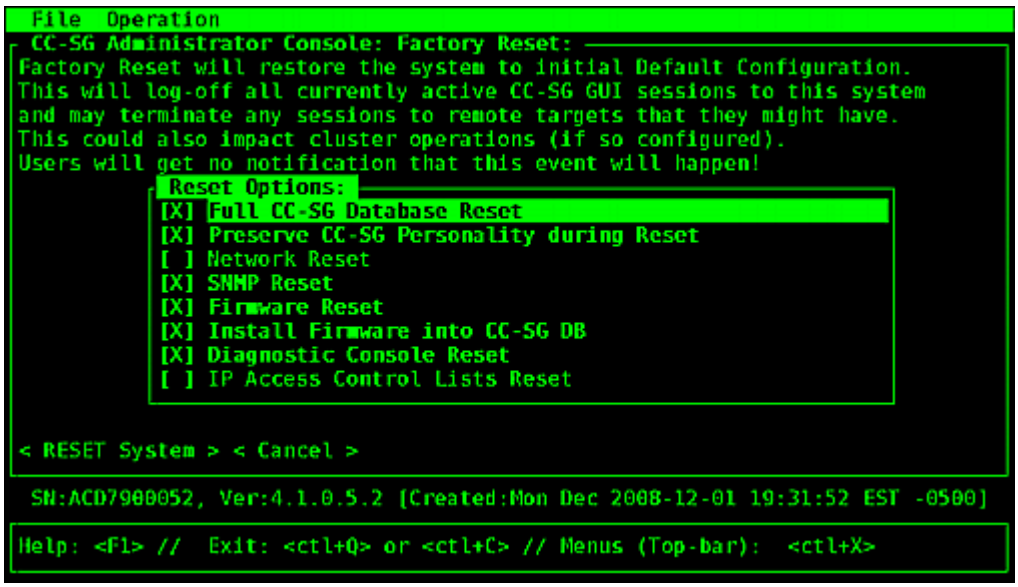
1. Choisissez Operation > Admin > CC-SG ADMIN Password Reset.

2. Cliquez sur Reset CC-SG GUI Admin Password ou appuyez sur Entrée pour rétablir le mot de passe admin par défaut usine. Confirmez la réinitialisation du mot de passe dans l'écran suivant pour continuer.



Réinitialiser 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 recommandé d'utiliser les options par défaut sélectionnées.

Option	Description
Full CC-SG Database Reset	Cette option supprime la base de données CC-SG existante et constitue une nouvelle version en la chargeant avec les valeurs par défaut usine. Les paramètres réseau, SNMP et de console de diagnostic, et le firmware ne font pas partie de la base de données CC-SG. Les paramètres IP-ACL sont rétablis par une réinitialisation de la base de données complète que l'option IP ACL Tables soit sélectionnée ou non. La configuration du voisinage est supprimée lors de la réinitialisation, l'unité CC-SG ne « se souvient » donc plus avoir été membre du voisinage.
Preserve CC-SG Personality during Reset	Cette option est activée lorsque vous sélectionnez Full CC-SG Database Reset. Lorsque la base de données CC-SG est reconstituée, certaines options configurées précédemment sont enregistrées. ▪ Communication sécurisée entre les clients PC et CC-SG ▪ Imposition des mots de passe forts ▪ Connexions directes ou Proxy aux nœuds hors bande ▪ Paramètre de délai d'inactivité
Network Reset	Cette option rétablit les paramètres réseau aux valeurs par défaut usine. ▪ Nom de l'hôte : CommandCenter ▪ Nom de domaine : localdomain ▪ Mode : Principal/de sauvegarde ▪ Configuration : Statique ▪ Adresse IP : 192.168.0.192 ▪ Masque réseau : 255.255.255.0 ▪ Passerelle : néant ▪ DNS principal : néant ▪ DNS secondaire : néant ▪ Vitesse de carte : Auto
SNMP Reset	Cette option rétablit les paramètres SNMP aux valeurs par défaut usine. ▪ Port : 161 ▪ Communauté en lecture seule : public ▪ Communauté en lecture/écriture : privé ▪ Contact système, Nom, Emplacement : néant ▪ Configuration des traps SNMP ▪ Destinations des traps SNMP

Option	Description
Firmware Reset	Cette option rétablit tous les fichiers de firmware de dispositif aux valeurs par défaut usine. Cette option ne modifie pas la base de données CC-SG.
Install Firmware into CC-SG DB	Cette option charge les fichiers de firmware de la version de CC-SG actuelle dans la base de données CC-SG.
Diagnostic Console Reset	Cette option rétablit les paramètres de console de diagnostic aux valeurs par défaut usine.
IP Access Control Lists Reset	Cette option retire toutes les entrées de la table IP-ACL. Les paramètres IP-ACL sont rétablis par une réinitialisation de la base de données complète que l'option IP Access Control Lists reset soit sélectionnée ou non. Reportez-vous à ***Liste de contrôle d'accès*** (voir "Liste de contrôle d''accès" à la page 239).

Pour réinitialiser CC-SG à la configuration usine :

1. Choisissez Operation > Admin > Factory Reset.
2. Sélectionnez les options de réinitialisation.
3. Cliquez sur Reset System.
4. Un message d'avertissement et une barre de progression apparaissent à l'écran. La barre de progression indique l'état de réinitialisation en cours et vous ne pouvez pas contrôler CC-SG avant la fin de la réinitialisation.

NE METTEZ PAS hors tension, N'EFFECTUEZ PAS d'alimentation cyclique ou N'INTERROMPEZ PAS CC-SG pendant la réinitialisation. Ces opérations peuvent entraîner la perte des données de CC-SG.

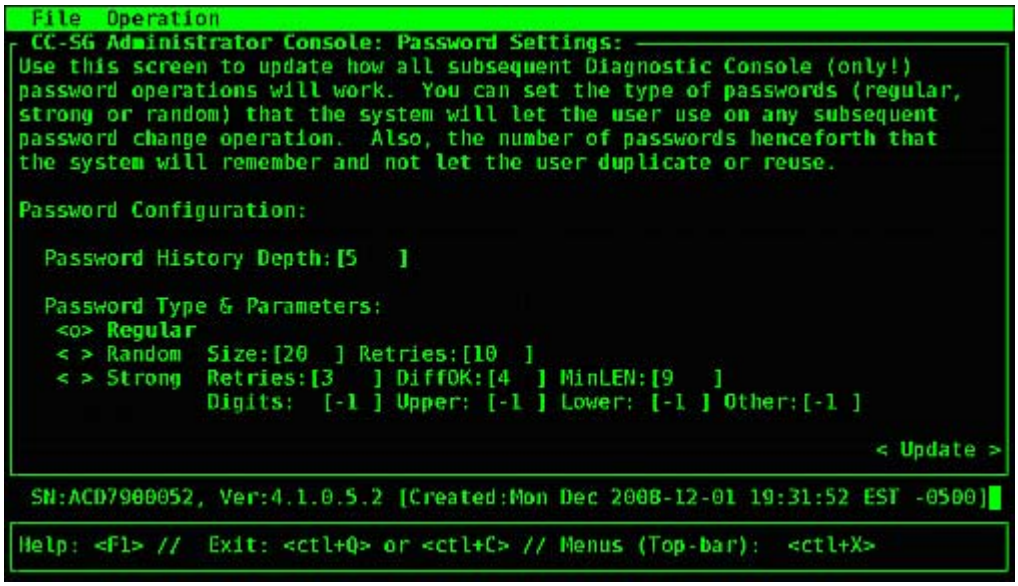
Paramètres des mots de passe de la console de diagnostic

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 des comptes). 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.

Pour configurer les mots de passe de la console de diagnostic :

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.



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.

Paramètre de mot de passe	Description
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 entre 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 de console de diagnostic

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.

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 zone inférieure 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.
Expire	(Lecture seule). Il s'agit du jour où ce compte doit changer de mot de passe.

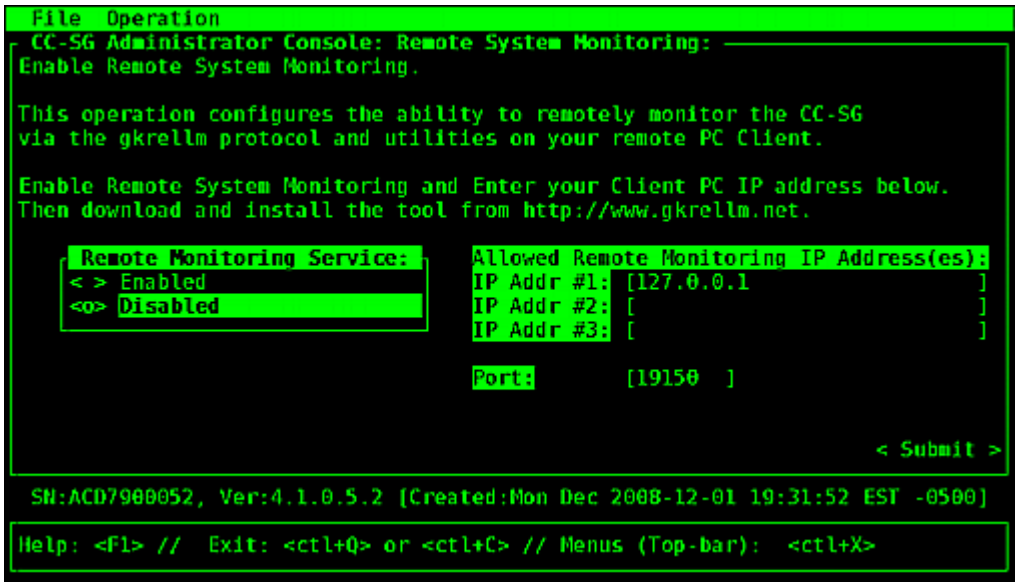
Paramètre	Description
Mode	Option configurable si le compte est désactivé (aucune connexion autorisée) ou activé (jeton d'authentification obligatoire), ou si l'accès est autorisé et qu'aucun mot de passe n'est requis. (Ne verrouillez pas les comptes Admin et FS1 en même temps, vous ne pourriez plus 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.
Warning	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.

Configurer la surveillance du système à distance

Vous pouvez habiliter la fonction de surveillance du système à distance à utiliser l'outil GKrellM. Cet outil offre une vue graphique de l'utilisation des ressources sur l'unité CC-SG. Il est similaire à l'onglet Performances du Gestionnaire des tâches Windows.

1: Activer la surveillance du système à distance pour l'unité CC-SG :

1. Choisissez Operation > Utilities > Remote System Monitoring.



2. Sélectionnez Enabled dans le champ Remote Monitoring Service.
3. Entrez l'adresse IP du PC client que vous souhaitez autoriser à surveiller l'unité CC-SG dans le champ Allowed Remote Monitoring IP Addresses (adresses IP autorisées pour la surveillance à distance). Vous pouvez entrer jusqu'à trois adresses IP.
4. Le port par défaut de l'outil GKrellM est 19150. Vous pouvez le modifier.
5. Sélectionnez Submit.

2: Télécharger le logiciel client de surveillance du système à distance :

1. Accédez à www.gkrellm.net.
2. Téléchargez et installez le paquet approprié pour votre PC client.

3: Configurer le client de surveillance du système à distance pour fonctionner avec CC-SG :

Suivez les instructions du fichier Read Me pour définir l'unité CC-SG comme cible de la surveillance.

Les utilisateurs Windows doivent utiliser la ligne de commande pour repérer le répertoire d'installation de Gkrellm, puis exécuter les commandes indiquées dans le fichier Read Me.

Afficher les rapports d'évolution des données d'historique

L'évolution des données d'historique collecte des informations sur l'utilisation du processeur et de la mémoire, l'espace du tas Java et le trafic réseau. Ces informations sont compilées dans un rapport visualisable sous forme de page Web depuis CC-SG. Le rapport contient l'état de l'unité CC-SG et des liens vers des données d'historique.

1: Activer l'affichage de l'évolution des données d'historique :

1. Choisissez Operation > Diagnostic Console Config (configuration de la console de diagnostic).
2. Dans la liste Ports, sélectionnez Web.
3. Dans la liste Status, cochez la case en regard de Web.
4. Cliquez sur Save (Enregistrer).

2: Afficher les rapports d'évolution des données d'historique :

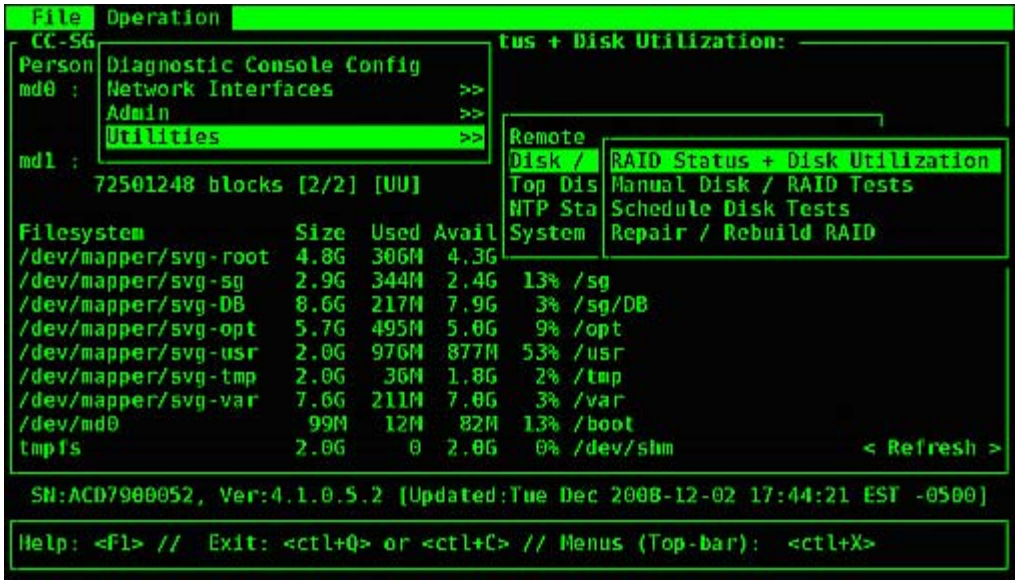
1. Dans un navigateur Internet pris en charge, entrez l'URL : `http(s)://<adresse_IP>/status/` où `<adresse_IP>` indique l'adresse IP de l'unité CC-SG. Notez que la barre oblique (/) suivant /status est obligatoire. Par exemple, `https://10.20.3.30/status/`.
2. Une page d'état s'ouvre. Elle contient les mêmes informations que la console d'état. Reportez-vous à ***Console d'état*** (à la page 265).
   - Cliquez sur le lien Historical CC-SG Monitors pour afficher des informations sur l'utilisation du processeur et de la mémoire, l'espace du tas Java et le trafic réseau. Cliquez sur chaque graphique pour afficher ses détails dans une nouvelle page.

Afficher l'état du RAID et l'utilisation des disques

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 des disques de CC-SG :

1. Choisissez Operation > Utilities > Disk / RAID Utilities > RAID Status + Disk Utilization.



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.

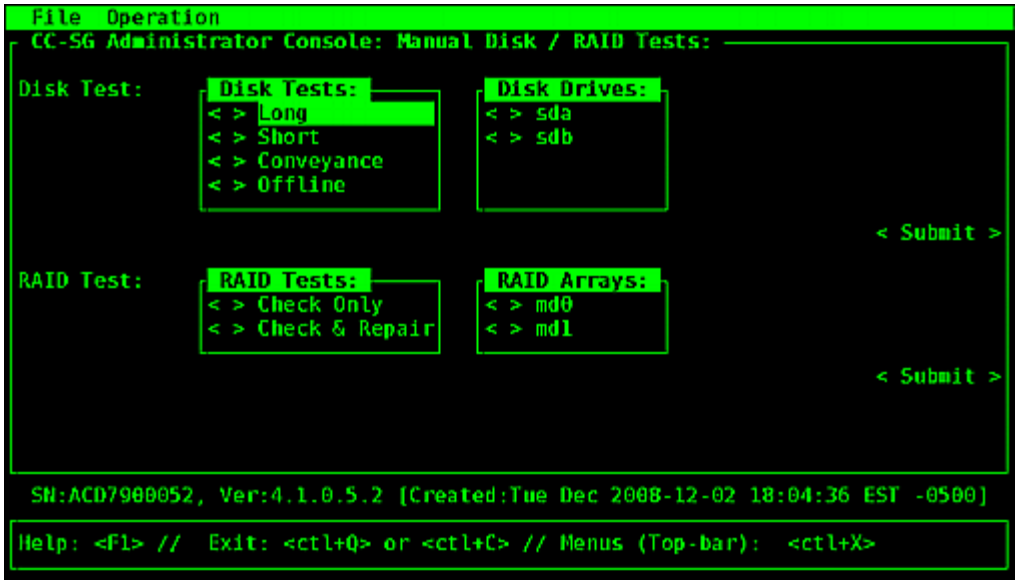
Remarque : les disques durs sont entièrement synchronisés et la protection totale du RAID-1 est disponible lorsqu'un écran semblable à celui présenté ci-dessus s'affiche. L'état des tableaux md0 et md1 est [UU]).

Effectuer des tests sur les disques ou sur le RAID

Vous pouvez effectuer manuellement des tests de lecteurs de disque SMART, ou des opérations de vérification et de réparation de RAID.

Pour effectuer un test de lecteur de disque, ou une opération de vérification et de réparation de RAID :

1. Choisissez Operation > Utilities > Disk/RAID Utilities > Manual Disk/RAID Tests.



2. Pour effectuer un test de lecteur de disque SMART :
   a. Dans la section Disk Test, sélectionnez le type de test et le lecteur de disque à tester.
   b. Sélectionnez Submit.
   c. Le test est programmé et un écran d'informations SMART s'affiche.
   d. Lorsque la durée requise s'est écoulée comme l'indique l'écran, vous pouvez afficher les résultats dans l'écran Repair/Rebuild RAID (Réparer/Reconstruire le RAID). Reportez-vous à ***Réparer ou reconstruire les disques RAID*** (à la page 304).
3. Pour effectuer une opération de test et de réparation du RAID :
   a. Dans la section RAID Test, sélectionnez le type de test et la matrice de disques RAID à tester. La matrice md0 est une petite partition d'amorçage, alors que la matrice md1 couvre le reste du système.
   b. Sélectionnez Submit.

c. Vous pouvez suivre la progression du test dans l'écran RAID Status+Disk Utilization (Etat du RAID+Utilisation des disques). Reportez-vous à ***Afficher l'état du RAID et l'utilisation des disques*** (à la page 299). **Facultatif.**

d. A la fin du test, vous pouvez afficher les résultats dans l'écran Repair/Rebuild RAID. Reportez-vous à ***Réparer ou reconstruire les disques RAID*** (à la page 304). Si une valeur non nulle apparaît dans la colonne Mis-Match (Conflit) pour la matrice donnée, indiquant la présence d'un problème éventuel, contactez l'assistance technique Raritan pour obtenir de l'aide.

Programmer des tests sur les disques

Vous pouvez programmer l'exécution périodique de tests SMART sur les lecteurs de disque. Le firmware du lecteur de disque effectue ces tests et vous pouvez afficher leurs résultats dans l'écran Repair/Rebuild. Reportez-vous à ***Réparer ou reconstruire les disques RAID*** (à la page 304).

Les tests SMART peuvent être exécutés pendant que l'unité CC-SG fonctionne et est en cours d'utilisation. Leur impact est marginal sur les performances de l'unité CC-SG, mais les activités de celle-ci peuvent considérablement ralentir l'exécution des tests SMART. Il est donc recommandé de ne pas programmer de tests fréquents.

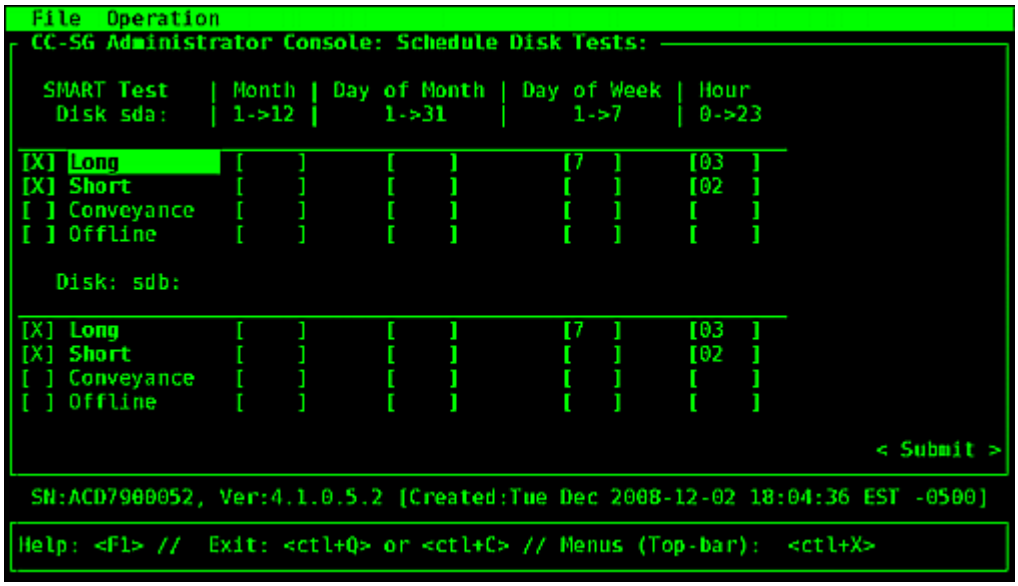
Lors de la programmation des tests SMART, tenez compte des instructions suivantes :

- Un seul test à la fois peut être exécuté sur un lecteur donné.
- La programmation d'un autre test ne sera pas possible si un lecteur est en cours de test.
- Si deux tests sont programmés pour la même plage horaire, le test le plus long est prioritaire.
- Le test est exécuté « dans » l'heure spécifiée, pas forcément au début de l'heure.
- Ne programmez pas de tests SMART au cours de périodes d'activité de disque important, par exemple lors des charges CC-SG lourdes ou d'opération de nettoyage se produisant chaque jour à minuit et à midi.

Remarque : par défaut, l'exécution d'un test court est programmée sur CC-SG à 2 h chaque jour et un test long à 3 h tous les dimanche. Ces tests programmés s'appliquent aux deux lecteurs de disque.

Pour modifier la programmation des tests de disque :

1. Choisissez Operation > Utilities > Disk/RAID Utilities > Schedule Disk Tests (Programmer des tests de disque).



2. Cliquez ou utilisez les touches fléchées pour vous déplacer, et appuyez sur la barre d'espacement pour sélectionner un type de test en le marquant d'un X. Les divers types de tests ont une durée différente.
   - Un test court prend environ deux minutes lorsque la charge du système est légère.
   - Un test d'acheminement prend environ cinq minutes.
   - Un test long prend environ 50 minutes.
   - Un test hors ligne dure jusqu'à 50 minutes.
3. Indiquez la date et l'heure d'exécution de ce test. Renseignez les champs Mois, Jour du mois, Jour de la semaine et Heure.
   - Le champ Jour du mois utilise les valeurs 1 pour le lundi à 7 pour le dimanche.
   - L'heure doit être indiquée au format 24 heures.

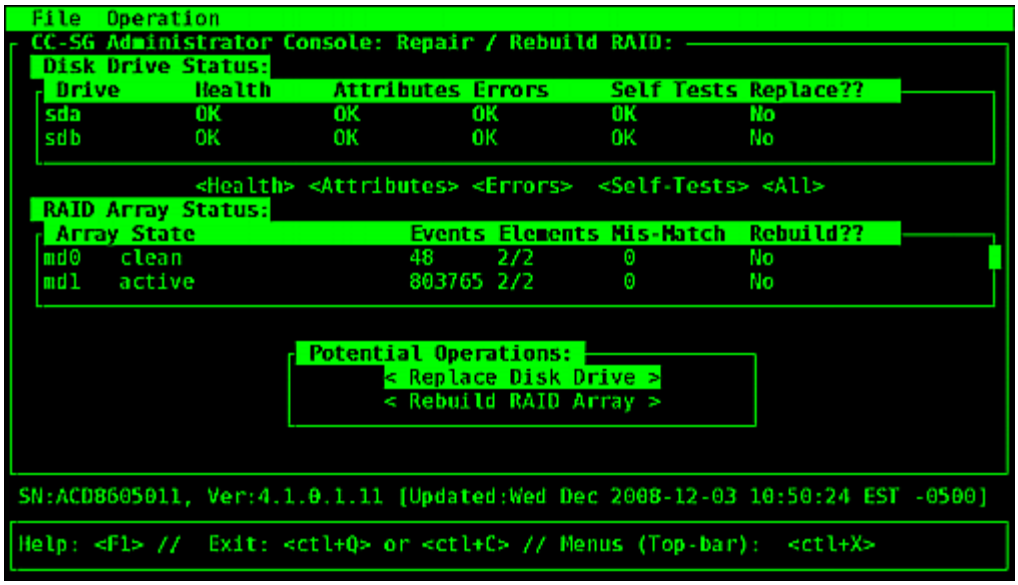
   Remarque : un champ vide correspond à toutes les valeurs.
4. Sélectionnez Submit.

Réparer ou reconstruire les disques RAID

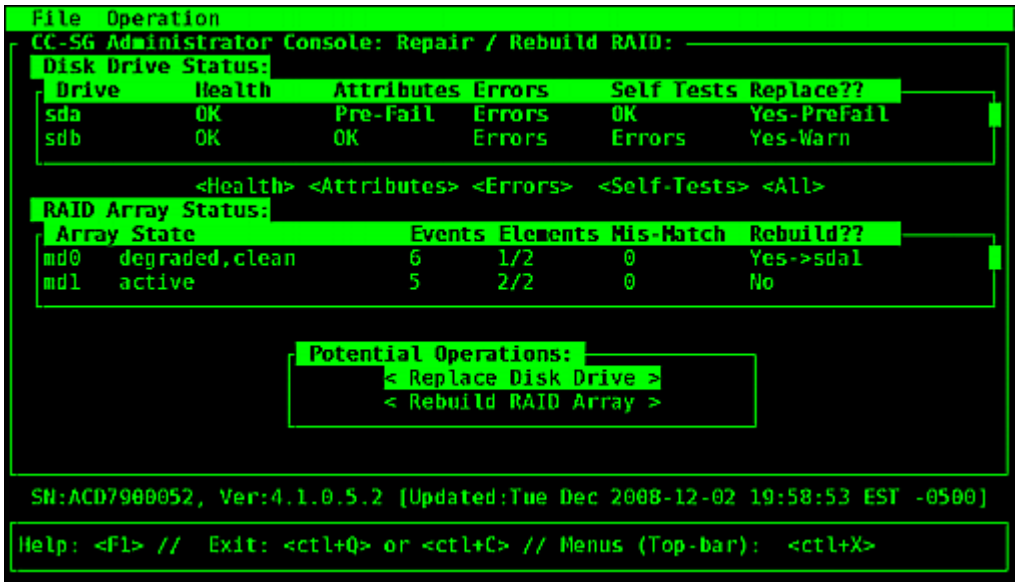
Cette option affiche des informations d'état détaillées pour les lecteurs de disque et les matrices RAID, et indique si vous devez remplacer un lecteur de disque ou reconstruire une matrice RAID-1 en miroir. Avant de remplacer ou de permuter à chaud un lecteur de disque, procurez une unité de remplacement auprès de Raritan.

Pour réparer ou reconstruire le RAID :

1. Choisissez Operation > Utilities > Disk/RAID Utilities > Repair/Rebuild RAID (Réparer/Reconstruire le RAID).
2. Si un élément ne présente pas la mention No dans la colonne Replace?? ou Rebuild??, contactez l'assistance technique Raritan pour obtenir de l'aide.
   - Un système fonctionnant correctement :



- Un système artificiel présentant plusieurs problèmes :



Le système met à jour les informations affichées lorsque vous alternez entre les zones Disk Drive Status (Etat du lecteur de disque), RAID Array Status (Etat de la matrice RAID) et Potential Operations (Opérations potentielles).

3. Vous pouvez sélectionner n'importe quel bouton sous la table de la section Disk Drive Status pour afficher des informations SMART détaillées. **Facultatif.**
4. Sélectionnez Replace Disk Drive ou Rebuild RAID Array, et suivez les instructions affichées jusqu'à la fin de l'opération.

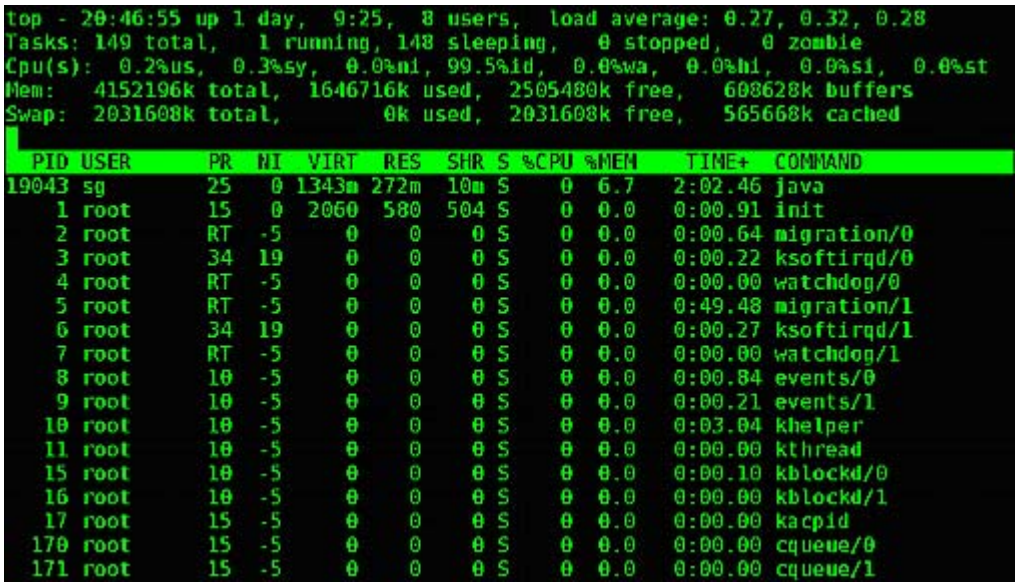
Afficher les processus exécutés sur CC-SG avec la console de diagnostic

L'option Top Display présente la liste des processus actuellement exécutés, leurs attributs, 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.



3. Entrez `h` pour afficher un écran d'aide pour la commande top. La touche d'aide F1 ne fonctionne pas ici.

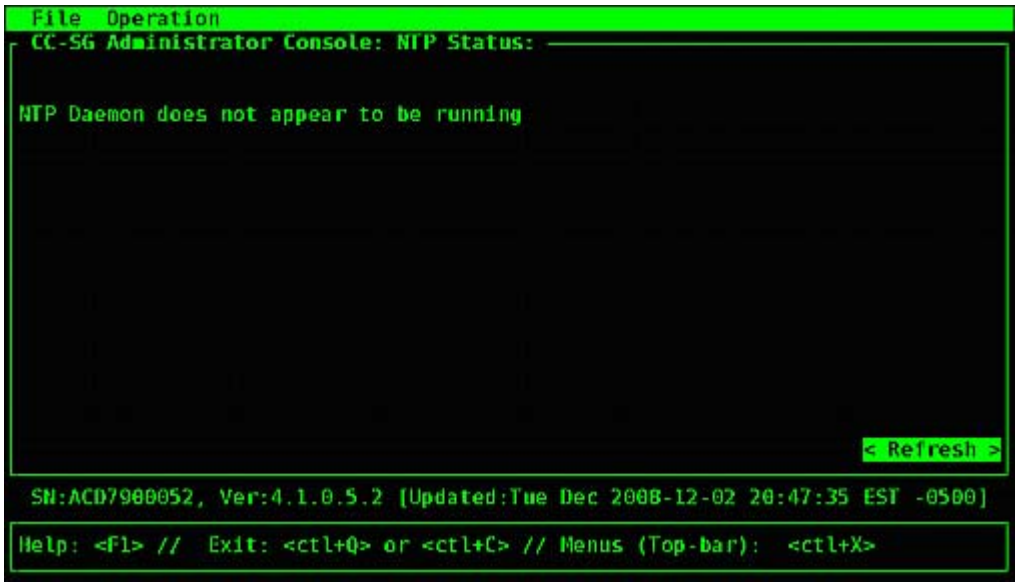
Afficher l'état NTP

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, Client Admin.

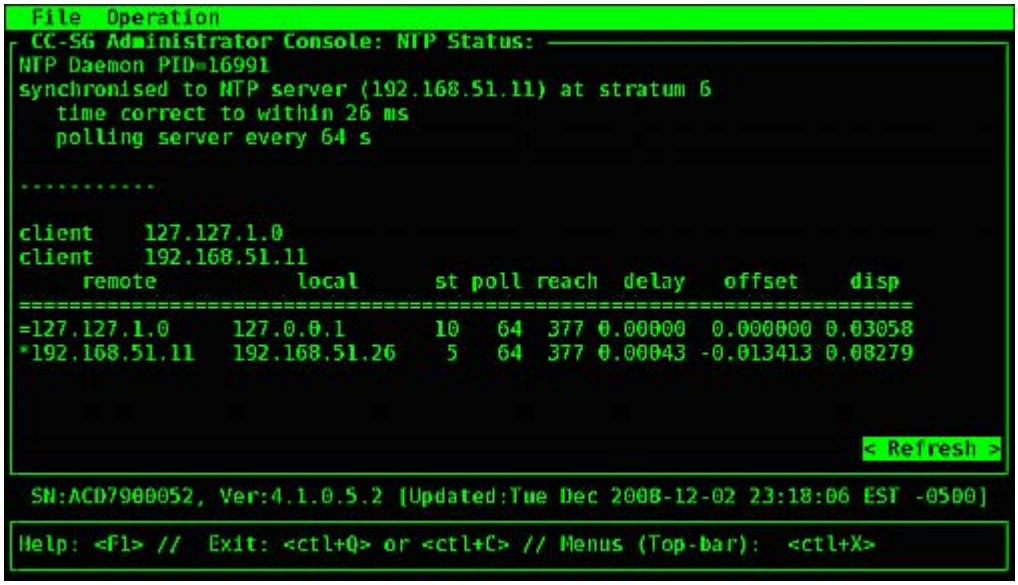
Pour afficher l'état du démon NTP sur CC-SG :

1. Choisissez Operation > Utilities > NTP Status Display.

- NTP n'est pas activé ou configuré correctement :



- NTP est configuré et s'exécute correctement :



Prendre un instantané du système

Si CC-SG ne fonctionne pas correctement, la capture des informations stockées dans CC-SG, telles que les journaux système, les configurations ou la base de données, peut se révéler très utile et vous pouvez la fournir à l'assistance technique Raritan à des fins d'analyse et de dépannage.

1: Prendre un instantané de CC-SG :

1. Choisissez Operation > Utilities > System Snapshot (Instantané du système).
2. Cliquez sur ou sélectionnez Yes. Le menu d'instantané du système s'ouvre.
3. Assurez-vous que chaque valeur %Used affichée est inférieure à 60 % pour garantir que l'espace disponible est suffisant pour l'opération d'instantané. Sinon, abandonner l'opération et effectuez l'opération de nettoyage, ou contactez l'assistance technique Raritan pour obtenir de l'aide.
4. Les options System Snapshot sont divisées en deux zones.
   - Snapshot Configuration (Configuration de l'instantané) affiche la liste des données CC-SG dont vous pouvez prendre un instantané.
   - Snapshot Operations (Opération d'instantané) affiche la liste des opérations possibles à l'activation de l'opération d'instantané.
5. Il n'est généralement pas nécessaire de modifier les sélections d'instantané par défaut sauf si l'assistance technique Raritan vous le demande. Dans ce cas, cliquez ou utilisez les touches fléchées pour vous déplacer, et appuyez sur la barre d'espacement pour sélectionner les opérations d'instantané souhaitées et les marquer d'un X.
6. Cliquez sur ou sélectionnez Submit pour poursuivre l'opération de prise d'instantané.
7. Une liste d'éléments défile rapidement pendant la prise de l'instantané. Il arrive parfois que CC-SG s'interrompt pendant quelques instants.
8. A la fin de la prise de l'instantané, CC-SG affiche les informations le concernant, notamment :
   - l'emplacement et le nom du fichier d'instantané CC-SG ;
   - la taille ;
   - la somme de contrôle MD5.

   Les informations d'instantané ne sont fournies qu'à titre indicatif et il n'est pas nécessaire de les noter.

9. Appuyez sur Entrée pour retourner au menu System Snapshot.

2: Récupérer le fichier d'instantané CC-SG :

1. Dans un navigateur Internet pris en charge, entrez l'URL : `http(s)://<adresse_IP>/upload/` où `adresse_IP` indique l'adresse IP de l'unité CC-SG. Notez que la barre oblique (/) suivant `/upload` est obligatoire. Par exemple, `https://10.20.3.30/upload/`.
2. La boîte de dialogue Enter Network Password (Entrer le mot de passe réseau) apparaît. Tapez le nom d'utilisateur et le mot de passe du compte admin de la console de diagnostic, et cliquez sur OK pour vous connecter.
3. Tous les fichiers d'instantané disponibles pris par CC-SG sont répertoriés.

   Remarque : CC-SG ne conserve les fichiers d'instantané que dix jours, vous devez donc les récupérer assez rapidement.

4. Cliquez sur le fichier d'instantané portant le nom approprié ou le fichier nommé snapshot car il s'agit du dernier créé. Les fichiers sont déjà compressés, chiffrés et signés, vous devez donc les transférer en mode binaire.
5. Lors de l'enregistrement du fichier avec IE, sauvegardez-le dans un fichier brut en choisissant Tous les fichiers dans la liste déroulante Type de fichier de la boîte de dialogue Enregistrer sous.

Modifier la résolution vidéo de la console de diagnostic

Raritan vous recommande de régler la résolution vidéo de la console de diagnostic pour permettre l'affichage correct du menu à l'écran.

Pour régler la résolution vidéo

1. ***Réamorcez CC-SG*** (voir "Réamorcer CC-SG avec la console de diagnostic" à la page 287).
2. Lorsque les messages ci-dessous apparaissent, appuyez sur n'importe quelle touche (Echap ou touche fléchée par exemple) dans les cinq secondes pour accéder au menu GRUB.

   ```
   Press any key to enter the menu (Appuyez sur une touche quelconque pour accéder au menu)
   ```

   ```
   Booting CentOS (x.x.x) in x seconds.... (Amorçage de CentOS dans x secondes)
   ```

3. Mettez en surbrillance l'option 1024x768 / 24-bit à l'aide des touches fléchées haut ou bas, et appuyez sur Entrée.

Annexe A Spécifications pour V1 et E1

Dans ce chapitre

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° - 35° (50°- 95°)
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 - 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	N/A
A l'arrêt	
Température	-40° - +60° (-40°-140°)

En fonctionnement	
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	N/A

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 - 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

En fonctionnement **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

Cette annexe indique la configuration réseau requise, notamment 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, ainsi que pour la mise en application de la sécurité interne et de la stratégie d'acheminement. Des détails sont fournis à l'intention d'un administrateur réseau TCP/IP. Le rôle et les responsabilités d'un administrateur TCP/IP peuvent s'étendre au-delà de ceux d'un administrateur CC-SG. Cette annexe aidera l'administrateur à intégrer CC-SG et ses composants aux stratégies d'accès de sécurité et d'acheminement d'un site.

Les tableaux indiquent les protocoles et ports nécessaires à CC-SG et à ses composants associés.

Dans ce chapitre

Ports ouverts requis pour les réseaux CC-SG : Synthèse

Les ports suivants doivent être ouverts :

Numéro de port	Protocole	Usage	Détails
80	TCP	Accès HTTP à CC-SG	Non chiffré.
443	TCP	Accès HTTPS (SSL) à CC-SG	SSL/AES-128/AES-256 chiffré.
8080	TCP	CC-SG à Client PC	SSL/AES-128/AES-256 chiffré si configuré.
2400	TCP	Accès au nœud (mode proxy)	Non chiffré.
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. AES-128/AES-256 chiffré si configuré.

Numéro de port	Protocole	Usage	Détails
80 et 443 pour les nœuds Système de contrôle 80, 443, 902 et 903 pour des nœuds d'hôte virtuel et de machine virtuelle	TCP	Accès au nœud virtuel	N/A
51000	TCP	Accès cible SX (mode direct)	AES-128/AES-256 chiffré si configuré.

Exceptions possibles aux ports ouverts requis :

le port 80 peut être fermé si l'accès à CC-SG est toujours effectué via des adresses HTTPS ;

les ports 5000 et 51000 peuvent être fermés si le mode proxy de CC-SG est utilisé pour toutes les connexions depuis les pare-feu.

Canaux de communication CC-SG

Chaque canal de communication est documenté. Pour chaque canal de communication, le tableau inclut :

- les adresses IP symboliques utilisées par les parties en communication. Ces adresses doivent être autorisées sur tous les chemins de communication entre les entités ;
- 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 ;
- les numéro de port et protocole utilisés par CC-SG ;
- si le port est configurable, ce qui signifie que le client Admin ou la console de diagnostic fournit un champ dans lequel vous pouvez remplacer le numéro de port par défaut indiqué s'il existe des conflits avec d'autres applications du réseau ou pour des raisons de sécurité.
- des détails sur la méthode de communication, le message transmis via le canal de communication ou son chiffrement.

CC-SG et dispositifs Raritan

Un des rôles principaux de CC-SG consiste à gérer et à contrôler des dispositifs Raritan, tels que la Dominion KX II. 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 ?	Détails
CC-SG vers diffusion locale	5000	UDP	oui	Détection de collision
CC-SG vers IP LAN distant	5000	UDP	oui	Détection de collision
CC-SG vers dispositif Raritan	5000	TCP	oui	Protocole RDM RC4/AES-128/AES-256 chiffré.
Dispositif Raritan vers CC-SG	5001	UDP	non	Détection de collision
CC-SG vers Dominion PX	623	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 ?	Détails
CC-SG vers diffusion locale	10000	UDP	non	Détection de collision
CC-SG vers IP LAN distant	10000	UDP	non	Détection de collision
CC-SG vers CC-SG	5432	TCP	non	De HA-JDBC sur le serveur principal au serveur PostgreSQL DB de sauvegarde. Non chiffré.
CC-SG vers CC-SG	8732	TCP	non	Echange de données de contrôle du clustering de synchronisation des serveurs principal-de sauvegarde. MD5 chiffré.

Direction de la communication	Numéro de port	Protocole	Configurable ?	Détails
CC-SG vers CC-SG	3232	TCP	non	Transfert des modifications de configuration de synchronisation SNMP principal-de sauvegarde. Non chiffré.

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. Ces ports et protocoles sont utilisés pour autoriser CC-SG à communiquer avec ces serveurs facultatifs.

Direction de la communication	Numéro de port	Protocole	Configurable ?	Détails
Serveur DHCP vers CC-SG	68	UDP	non	Norme IPv4 DHCP
CC-SG vers serveur DHCP	67	UDP	non	Norme IPv4 DHCP
Serveur NTP vers CC-SG	123	UDP	non	Norme NTP
CC-SG vers DNS	53	UDP	non	Norme DNS

Clients PC vers CC-SG

Les clients PC se connectent à CC-SG via un de ces trois modes :

- Client Admin ou Client d'accès via un navigateur Web. CC-SG prend en charge SSL v2, SSL v3 et TLS v1 pour les connexions de navigateur. Vous pouvez configurer ces méthodes de chiffrement dans votre navigateur.
- Interface de ligne de commande (CLI) via SSH
- Console de diagnostic

Direction de la communication	Numéro de port	Protocole	Configurable ?	Détails
Client PC vers CC-SG	443	TCP	non	Communication client-serveur. SSL/AES-128/AES-256 chiffré si configuré.

Direction de la communication	Numéro de port	Protocole	Configurable ?	Détails
Client PC vers CC-SG	80	TCP	non	Communication client-serveur. Non chiffré. Si SSL est activé, le port 80 est redirigé vers 443.
Client PC vers CC-SG	8080	TCP	non	Communication client-serveur. SSL/AES-128/AES-256 chiffré si configuré.
Client PC vers CLI SSH	22	TCP	oui	Communication client-serveur. SSL/AES-128/AES-256 chiffré si configuré.
Client PC vers console de diagnostic	23	TCP	oui	Communication client-serveur. SSL/AES-128/AES-256 chiffré si configuré.

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 des méthodes d'accès en bande, telles que VNC, RDP ou SSH.

Un autre aspect de la communication entre client PC et nœud implique que :

- le client PC se connecte directement au nœud via un dispositif Raritan ou un accès en bande. Il s'agit du mode direct ;
- le client PC se connecte au nœud 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 ?	Détails
Client vers CC-SG via Proxy vers nœud	2400 (sur CC-SG)	TCP	non	Communication client-serveur. Non chiffré.
Client vers dispositif Raritan vers nœud KVM hors bande (mode direct)	5000 (sur dispositif Raritan)	TCP	oui	Communication client-serveur. SSL/AES-128/AES-256 chiffré si configuré.

Direction de la communication	Numéro de port	Protocole	Configurable ?	Détails
Client vers dispositif Dominion SX Raritan vers nœud série hors bande (mode direct)	51000 (sur dispositif Raritan)	TCP	oui	Communication client-serveur. SSL/AES-128/AES-256 chiffré si configuré.

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 ?	Détails
CC-SG vers IPMI	623	TCP	non	Norme IPMI
CC-SG vers iLO/RILOE (utilise des ports HTTP)	80 ou 443	TCP	non	Norme fournisseur
CC-SG vers DRAC	80 ou 443	TCP	non	Norme fournisseur
CC-SG vers RSA	80 ou 443	TCP	non	Norme fournisseur

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 ?	Détails
Gestionnaire SNMP vers CC-SG	161	UDP	oui	Norme SNMP
CC-SG vers gestionnaire SNMP	162	UDP	oui	Norme SNMP

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 ?	Détails
CC-SG vers CC-NOC	9443	TCP	non	Services Web NOC. SSL/AES128 chiffré.

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. Le pare-feu doit être configuré pour des connexions externes aux ports 80 (non-SSL) ou 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.

Les connexions hors bande qui utilisent le pare-feu doivent être configurées sur le mode Proxy. Reportez-vous à ***Modes de connexion : Direct et Proxy*** (à la page 213). CC-SG se connecte aux différentes cibles 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.

Accès RDP aux nœuds

Le port 3389 doit être ouvert pour l'accès RDP aux nœuds.

Accès VNC aux nœuds

Le port 5800 ou 5900 doit être ouvert pour l'accès VNC aux nœuds.

Accès SSH aux nœuds

Le port 22 doit être ouvert pour l'accès SSH aux nœuds.

Port de surveillance du système à distance

Lorsque la fonction de surveillance du système à distance est activée, le port 19150 est ouvert par défaut. Reportez-vous à ***Configurer la surveillance du système à distance*** (à la page 297).

Annexe C Privilèges de groupe d'utilisateurs

Ce tableau indique les privilèges à affecter à un utilisateur pour lui permettre d'accéder à une option de menu CC-SG.

*Aucun indique qu'aucun privilège particulier n'est requis. Tous les utilisateurs ayant accès à CC-SG peuvent accéder à ces menus et commandes.

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*	
	Impression écran...	Aucun*	
	Déconnexion	Aucun*	
	Quitter	Aucun*	
Utilisateurs	Ce menu et l'arborescence Utilisateurs sont disponibles uniquement pour les utilisateurs disposant du privilège User Management (gestion 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	
	Audit des nœuds	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 (gestion des dispositifs, des ports et des nœuds) Device Configuration and Upgrade Management (gestion de la configuration et de la mise à niveau des dispositifs)		
	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	
	>> 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	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> 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 et Node Power Control	
	> Démarrer Admin	Device, Port, and Node Management ou Device Configuration and Upgrade Management	
	> Lancer l'Admin de station utilisateur	Device, Port, and Node Management	
	> 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 et Node Out-of-band Access	
	> Configurer les ports	Device, Port, and Node Management	
	> Se déconnecter du port	Device, Port, and Node Management	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Supprimer des ports	Device, Port, and Node Management	
	> Gestionnaire d'alimentation des ports	Device, Port, and Node Management et Node Power Control	
	> Ajouter une barrette d'alimentation	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	
	> Par numéro 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 (gestion de l'alimentation des nœuds)		
	Ajouter un nœud	Device, Port, and Node Management	
	(Modification des nœuds)	Device, Port, and Node Management	Via Profil du nœud
	Supprimer un nœud	Device, Port, and Node Management	
	<nomInterface>	Node In-Band Access ou Node Out-of-band Access	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	Déconnecter	L'un des suivants : Node In-Band Access ou Node Out-of-Band Access ou Device, Port, and Node Management ou Device Configuration and Upgrade Management	
	Virtualisation	Device, Port and Node Management	
	Copier en bloc	Device, Port and Node Management	
	Gestion de l'alimentation	Power Control	
	Comptes de service	Device, Port, and Node Management	
	Attribuer les comptes de service	Device, Port, and Node Management	
	Regrouper la gestion de l'alimentation	Power Control	
	Configurer les commutateurs (lames)	Device, Port, and Node Management	
	Nœud ping	Device, Port, and Node Management	
	Interface nœud signet	Node In-Band Access ou Out-of-Band Access	
> Options de tri du nœud	> Par nom de nœud	L'un des suivants : Device, Port, and Node Management ou Node In-Band Access ou Node 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	
> 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).		
	> Association	User Security Management	Comporte la capacité d'ajouter, de modifier et de supprimer.

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Groupes de dispositifs	User Security Management	Comporte la capacité d'ajouter, de modifier et de supprimer.
	> Groupes 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 les utilisateurs dotés d'un privilège d'administration quelconque, hormis ceux disposant du privilège User Security Management uniquement		
	Journal d'audit	CC Setup and Control	
	Journal d'erreurs	CC Setup and Control	
	Rapport d'accès	Device, Port, and Node Management	
	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	
	> Données de tous les utilisateurs	Pour consulter les données de tous les utilisateurs : User Management Pour consulter vos propres données utilisateur : Aucun	
	> Données des groupes d'utilisateurs	User Management	
> Dispositifs	> Rapport sur le parc du nœud	Device, Port, and Node Management ou Device Configuration and Upgrade Management	
	> Données des groupes de dispositifs	Device, Port, and Node Management	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	> Interrogation des ports	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	
	> Données des groupes de nœuds	Device, Port, and Node Management	
> Active Directory	Rapport sur le groupe d'utilisateurs AD	CC Setup and Control ou User Management	
	Rapports programmés	CC Setup and Control	
	Synchronisation CC-NOC	CC Setup and Control	
Accès			
	Configuration CC-NOC	CC Setup and Control	
	Ajouter une API de services Web	CC Setup and Control	
Administration	Ce menu est disponible uniquement pour les utilisateurs disposant d'un des privilèges suivants : CC Setup and Control (paramétrage et contrôle de CC) 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	

Menu > Sous-menu	Option de menu	Privilège requis	Description
	Firmware	Device Configuration and Upgrade Management	
	Configuration	CC Setup and Control	
	Configuration des clusters	CC Setup and Control	
	Voisinage	CC Setup and Control	
	Sécurité	CC Setup and Control	
	Notifications	CC Setup and Control	
	Tâches	CC Setup and Control	
	Matrice de compatibilité	Device, Port, and Node Management ou 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	
Afficher		Aucun*	
Fenêtre		Aucun*	
Aide		Aucun*	

Annexe D Traps SNMP

CC-SG fournit les traps SNMP suivants :

Trap SNMP	Description
ccUnavailable	L'application CC-SG n'est pas disponible.
ccAvailable	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	Motif de l'échec de l'exécution d'une tâche programmée.

Trap SNMP	Description
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 d'utilisateur 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.
ccDominionPXReplaced	Un dispositif Dominion PX a été remplacé par un autre.
ccSystemMonitorNotification	CC-SG manque de mémoire.
ccNeighborhoodActivated	Le voisinage CC-SG a été activé.
ccNeighborhoodUpdated	Le voisinage CC-SG a été mis à jour.
ccDominionPXFirmwareChanged	Une version de firmware Dominion PX a été modifiée.
ccClusterFailover	Défaillance du nœud CC-SG primaire et le nœud CC-SG de sauvegarde sert maintenant de nœud CC-SG primaire.
ccClusterBackupFailed	Défaillance du nœud CC-SG de sauvegarde.
ccClusterWaitingPeerDetected	Le nœud CC-SG primaire a détecté un pair en mode d'attente.
ccClusterOperation	Une opération de cluster a été exécutée.

Annexe E Guide de dépannage

Le lancement de CC-SG à partir de votre navigateur Web requiert 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 pas 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 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 vider la mémoire cache du navigateur et la mémoire Java, puis redémarrer le navigateur. Reportez-vous à ***Effacer la mémoire cache du navigateur*** (à la page 196) et ***Effacer la mémoire cache Java*** (à la page 196).
- En cas de problème d'accès à un port KX2 via l'interface MPC depuis Internet Explorer, effacez la mémoire cache du navigateur puis accédez à nouveau au port. Reportez-vous à ***Effacer la mémoire cache du navigateur*** (à la page 196).
- Si l'utilisation de la mémoire monte considérablement ou que la session de navigateur ne répond plus à vos actions, essayez d'augmenter la taille de tas Java pour votre client.
  a. Ouvrez le plug-in Java dans le Panneau de configuration.
  b. Cliquez sur l'onglet Java.
  c. Cliquez sur Afficher dans la zone de groupe Paramètres de l'applet Java Runtime.
  d. Sélectionnez la ligne correspondant à la version de Java en cours d'exécution et tapez `-Xmx<size>m` dans la colonne Paramètres d'exécution Java. Par exemple, tapez `-Xmx300m` pour augmenter la taille du tas Java au maximum de 300 Mo.

Annexe F Utilitaires de diagnostic

L'unité CC-SG est fournie avec quelques utilitaires de diagnostic qui peuvent se révéler très utiles pour vous ou pour l'assistance technique Raritan afin d'analyser et de déboguer la cause des problèmes de CC-SG.

Dans ce chapitre

Diagnostic de la mémoire

L'unité CC-SG est mise en œuvre avec le programme de diagnostic Memtest86+, qui peut être appelé depuis le menu GRUB. En cas de problèmes de mémoire, vous pouvez exécuter le test de diagnostic Memtest86+ pour les résoudre.

1: Exécuter le programme de diagnostic Memtest86+ :

1. ***Réamorcez CC-SG*** (voir "Réamorcer CC-SG avec la console de diagnostic" à la page 287).
2. Lorsque les messages ci-dessous apparaissent, appuyez sur n'importe quelle touche (Echap ou touche fléchée par exemple) dans les cinq secondes pour accéder au menu GRUB.

   ```
   Press any key to enter the menu (Appuyez sur une touche
   quelconque pour accéder au menu)

   Booting CentOS (x.x.x) in x seconds.... (Amorçage de
   CentOS dans x secondes)
   ```

3. Mettez en évidence l'option Memtest86+ vX.X (où vX.X indique la version active) à l'aide des touches fléchées haut ou bas et appuyez sur Entrée.
4. CC-SG charge et exécute le programme de diagnostic Memtest86+. Laissez le programme effectuer au moins un passage ; la colonne Pass indique alors 1. Pour effectuer un test plus complet, laissez le programme s'exécuter pendant plusieurs heures ou même toute la nuit.
5. Vérifiez les éléments suivants pour déterminer s'il existe des erreurs de mémoire.
   - Memory (Mémoire) : la quantité totale de mémoire doit correspondre à votre type de CC-SG : 512M pour G1, 2048M pour V1 et 4096M pour E1.
   - Errors (Erreurs) : la colonne doit indiquer 0.

- Error display area (Zone d'affichage d'erreur) : il s'agit de la zone en bas à droite, sous la rangée WallTime. Le programme ne doit rien afficher dans cette zone pour indiquer l'absence d'erreurs.

Si un des éléments précédents indique la présence d'erreurs de mémoire, vous pouvez :

- capturer l'écran de Memtest86+ contenant les erreurs de mémoire et contacter l'assistance technique Raritan pour obtenir de l'aide ;
- fermer CC-SG et réinstaller les modules DIMM de mémoire pour assurer que le contact est correct. Effectuez ensuite le test de diagnostic Memtest86+ pour vérifier si le problème de mémoire est résolu.

2: Interrompre le programme de diagnostic Memtest86+ :

1. Appuyez sur Echap.
2. CC-SG effectue une réinitialisation et un réamorçage.

Mode de débogage

Même si l'activation du mode de débogage est extrêmement utile pour le dépannage, il peut affecter le fonctionnement et les performances de CC-SG. **N'activez le mode de débogage que si l'assistance technique Raritan vous y invite**. Vous devez désactiver le mode de débogage une fois le dépannage terminé.

1 : Activer le mode de débogage :

1. Dans un navigateur Internet pris en charge, entrez l'URL : `http(s)://<adresse_IP>:8080/jmx-console/` où `<adresse_IP` indique l'adresse IP de l'unité CC-SG. Par exemple, `https://10.20.3.30:8080/jmx-console/`.
2. Tapez admin dans le champ Nom d'utilisateur.
3. Tapez le mot de passe du super utilisateur dans le champ Mot de passe.
4. Faites défiler l'affichage jusqu'à `com.raritan.cc.bl.logger`.
5. Cliquez sur cet hyperlien : `service=LoggerService`. La liste des options de débogage apparaît à l'écran.
6. Remplacez la valeur INFO de l'option de débogage demandée par l'assistance technique Raritan par DEBUG.
7. Cliquez sur Appliquer les modifications au bas de la fenêtre.
8. Reproduisez le problème et ***prenez un instantané*** (voir "Prendre un instantané du système" à la page 308).

2 : Désactiver le mode de débogage :

1. Ouvrez la fenêtre des options de débogage en suivant les quatre premières étapes de la section précédente.
2. Remplacez la valeur de l'option de débogage DEBUG par INFO.
3. Cliquez sur Appliquer les modifications au bas de la fenêtre.

Surveillance des disques CC-SG

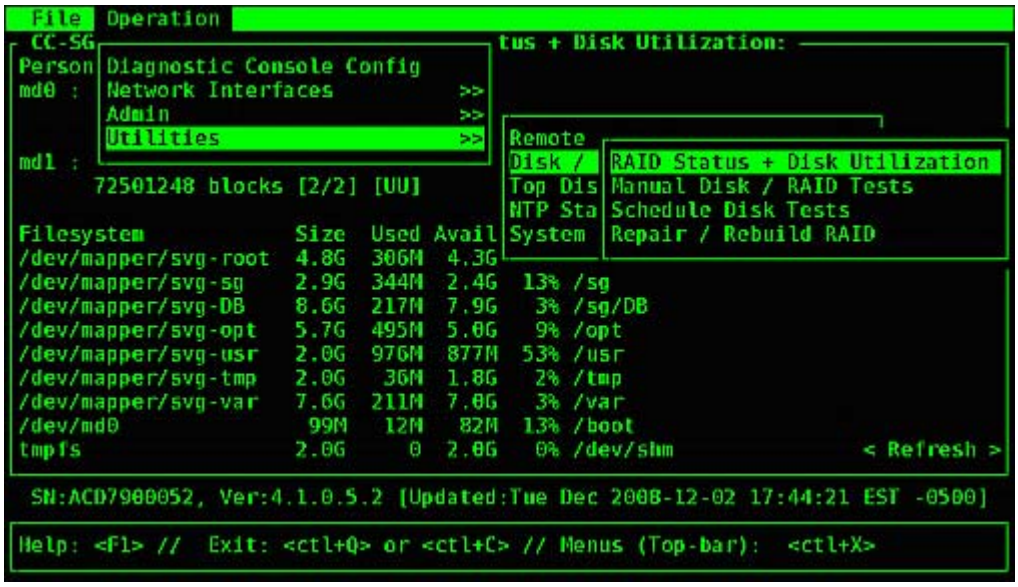
Si l'espace disque CC-SG est épuisé dans un ou plusieurs systèmes de fichiers, ceci peut nuire au fonctionnement et même entraîner la perte de certaines données techniques. Aussi, vous devez surveiller l'utilisation des disques CC-SG et entreprendre des actions correctives pour éviter ou résoudre d'éventuels problèmes. La surveillance des disques peut être effectuée via la console de diagnostic ou le navigateur Web. Si vous êtes un utilisateur expérimenté, vous pouvez vous servir de la ***surveillance à distance gkrellm*** (voir "Configurer la surveillance du système à distance" à la page 297).

Important : pour les unités CC-SG dans une configuration en cluster, vous devez surveiller les deux unités.

Pour surveiller l'espace disque via la console de diagnostic

1. Connectez-vous à la console de diagnostic et appelez l'***écran Disk Status*** (voir "Afficher l'état du RAID et l'utilisation des disques" à la page 299) (état des disques).
2. Vérifiez les informations relatives aux disques et effectuez les actions nécessaires.
   - Les deux partitions RAID doivent s'afficher sous la forme [UU] et non [U_] ou [_U]. Sinon, ceci signale une défaillance de disque et vous devez contacter l'assistance technique Raritan.

- Aucune des valeurs `Use%` des systèmes de fichiers (cinquième colonne à l'écran) ne doit être supérieure à 50 %. Différents systèmes de fichiers contiennent différentes données et les actions correctives sont également différentes.



Système de fichiers	Données	Action corrective
/sg/DB	Base de données CC-SG	Contactez l'assistance technique Raritan.

Système de fichiers	Données	Action corrective
/opt	Sauvegardes et instantanés CC-SG	1. Enregistrez les nouveaux fichiers d'instantané sur un PC client distant. Reportez-vous à ***Prendre un instantané du système*** (à la page 308) pour obtenir la procédure d'extraction. 2. Accédez au menu ***System Snapshot*** (voir "Prendre un instantané du système" à la page 308) (Instantané du système). 3. Sélectionnez la zone Pre-Clean-up SNAP (Instantané avant nettoyage). 4. Sélectionnez la zone Pre-Clean-up UPLOAD (Télécharger avant nettoyage). 5. Désélectionnez SNAP. 6. Désélectionnez Package & Export (Paquet & Exporter). 7. Cliquez sur ou sélectionnez Submit (Soumettre). 8. Si le problème d'espace persiste, utilisez le client Admin pour vous connecter à CC-SG, téléchargez les sauvegardes CC-SG sur un PC client puis supprimez-les de CC-SG.
/var	Fichiers journaux et mises à niveau système	Contactez l'assistance technique Raritan.
/tmp	Zone Scratch (zone de manœuvre) (utilisée par les instantanés)	1. Accédez au menu ***System Snapshot*** (voir "Prendre un instantané du système" à la page 308) (Instantané du système). 2. Désélectionnez SNAP. 3. Désélectionnez Package & Export (Paquet & Exporter). 4. Sélectionnez Clean-up /tmp (Nettoyer /tmp). 5. Cliquez sur ou sélectionnez Submit (Soumettre).

Pour surveiller l'espace disque via un navigateur Web

Cette méthode ne s'applique qu'à CC-SG version 4.0 ou supérieure. Vous devez activer les options relatives à la console d'état Web de la console de diagnostic avant de surveiller l'espace disque depuis le navigateur. Reportez-vous à ***Accéder à la console d'état depuis le navigateur Web*** (voir "Accéder à la console d'état depuis un navigateur Web" à la page 265).

1. Dans un navigateur Internet pris en charge, entrez l'URL : `http(s)://<adresse_IP>/status/` où `<adresse_IP>` indique l'adresse IP de l'unité CC-SG. Notez que la barre oblique (/) suivant /status est obligatoire. Par exemple, `https://10.20.3.30/status/`.
2. Une page d'état s'ouvre. Elle contient les mêmes informations que la console d'état.
3. Cliquez sur CC-SG Monitors (Moniteurs CC-SG) sous Evaluation au bas de la page.
4. Vérifiez les informations relatives aux disques et effectuez les actions nécessaires. Reportez-vous à la section précédente pour en savoir plus.

Remarque : pour les problèmes de systèmes de fichiers non répertoriés dans cette section, ou lorsque les actions correctives entreprises ne résolvent pas les problèmes, contactez l'assistance technique Raritan pour obtenir de l'aide.

Annexe G 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

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.

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 H FAQ

Dans ce chapitre

FAQ - Généralités

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 compatibilité sur le site Web de Raritan dans la section Support sous Firmware and Documentation.

Question	Réponse
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'adresses réseau connues. 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'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 IE 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 ?	Reportez-vous à la matrice de compatibilité sur le site Web de Raritan dans la section Support sous Firmware and Documentation.

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
L'unité CC-SG détecte-t-elle automatiquement la configuration du châssis de lames lorsque je déplace ce dernier d'un port KX2 à un autre ?	CC-SG ne détecte ni ne met à jour automatiquement la configuration du châssis de lames lorsque vous déplacez ce dernier vers un autre port ou dispositif KX2. La configuration est perdue et vous devez donc configurer à nouveau le châssis de lames dans CC-SG.
Comment puis-je fusionner les nœuds du serveur lame et de l'hôte virtuel s'ils se rapportent au même serveur ?	Configurez la fonction Virtualisation avant de configurer les connecteurs de lames. Lorsque vous configurez le connecteur de lames, entrez le même nom pour le nœud de l'hôte virtuel, et ajoutez cette interface au nœud existant lorsqu'un message apparaît.

FAQ sur l'authentification

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.

Question	Réponse
Pourquoi le message d'erreur « Nom d'utilisateur et/ou mot de passe incorrect(s) » apparaît-il après la saisie correcte d'un nom d'utilisateur et d'un mot de passe valides pour la connexion à CC-SG ?	Vérifiez le compte utilisateur dans AD. Si AD est défini pour une connexion à des ordinateurs spécifiques du domaine, il vous empêche de vous connecter à CC-SG. Dans ce cas, supprimez la restriction de connexion dans AD.

FAQ sur la sécurité

Question	Réponse
Sécurité	
Parfois, lorsque j'essaie de me connecter, un message m'indique que mes données de connexion sont incorrectes, 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.
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.

Question	Réponse
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.

FAQ sur la comptabilité

Question	Réponse
Comptabilité	
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.

FAQ sur les performances

Question	Réponse
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.

FAQ sur le regroupement

Question	Réponse
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 ? Que se passe-t-il, par exemple, si je déplace physiquement un module CIM avec serveur cible d'un port à un autre (sur le même dispositif ou sur un autre) ? Qu'arrive-t-il aux noms de port ? Qu'arrive-t-il au nœud ? Qu'arrive-t-il aux interfaces ?	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 dans les ports et interfaces de CC-SG ; les noms des ports et des interfaces sont mis à jour pour refléter la modification. L'interface apparaît sous le nœud associé au port. Toutefois, le nom du nœud ne change pas. Vous devez le renommer manuellement en le modifiant. Ce scénario suppose que tous les ports impliqués ont déjà été configurés. Si vous déplacez physiquement le serveur cible et le CIM vers un port différent et non configuré, vous pouvez alors configurer le port dans CC-SG et le nœud sera automatiquement créé.

FAQ sur l'interopérabilité

Question	Réponse
Interopérabilité	

Question	Réponse
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.
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.

FAQ sur l'autorisation

Question	Réponse
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.

FAQ sur l'expérience utilisateur

Question	Réponse
Expérience utilisateur	

Question	Réponse
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) : Qu'arrive-t-il à la connexion ? L'unité CC-SG capture-t-elle la gestion locale ou est-elle 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 cet événement, mais ce que les utilisateurs saisissent au niveau de la console CC-SG est perdu.

Annexe I 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 J 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.

Dans ce chapitre

Informations sur l'utilisateur

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom d'utilisateur	64
Mot de passe utilisateur (non fort)	6-16
Mot de passe utilisateur (fort)	Configurable Minimum : 8 Maximum : 16-64
Adresse électronique de l'utilisateur	60
Numéro de téléphone de l'utilisateur	32
Nom du groupe d'utilisateurs	64
Description des groupes d'utilisateurs	160

Informations sur le nœud

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom du nœud	64
Description du nœud	160

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Notes	256
Informations d'audit	256

Informations d'emplacement

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Service	64
Site	64
Emplacement	128

Informations de contact

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom du contact principal	64
Numéro de téléphone	32
Mobile	32
Nom du contact secondaire	64
Numéro de téléphone	32
Mobile	32

Comptes de service

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom du compte de service	64
Nom d'utilisateur	64
Mot de passe	64
Description	128

Informations sur le dispositif

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom du dispositif	64
Description du dispositif	160
Adresse IP/Nom d'hôte du dispositif	64
Nom d'utilisateur	64
Mot de passe	64
Notes	256

Informations sur le port

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom du port	32

Associations

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom de la catégorie	32
Nom d'élément	32
Nom du groupe de dispositifs	40
Nom du groupe de nœuds	40

Administration

Champ de CC-SG	Nombre de caractères autorisé par CC-SG
Nom du cluster	64
Nom du voisinage	64
Nom du module d'authentification	31
Nom de la sauvegarde	64
Description du fichier de sauvegarde	255
Message à diffusion générale	255

Annexe K Messages d'amorçage de la console de diagnostic

Avant la version 4.0, la console de diagnostic CC-SG affiche plusieurs messages à l'écran à chaque amorçage. Il s'agit de messages de diagnostic et d'avertissements Linux standard qui n'indiquent généralement pas un problème système. Le tableau offre une brève introduction à quelques messages fréquents.

Message	Description
hda:	Le message indique qu'un élément du système tente de communiquer avec le lecteur de DVD-ROM. Le message peut être appelé dans diverses situations. Par exemple : • Un utilisateur ouvre ou ferme le compartiment du lecteur de DVD-ROM. • Le système d'exploitation vérifie le lecteur de DVD-ROM et ne trouve aucun support lors de l'amorçage. D'autres scénarios appellent également le message, mais ils ne seront pas décrits dans la section.
avc:	Le message provient d'un système interne d'audit et de contrôle de sécurité -- sous-système SELinux. Le système émet des avertissements sans appliquer de politique de sécurité. Ils n'indiquent donc pas un problème système.
ipcontracks:	Le message apparaît systématiquement à l'amorçage de CC-SG et est donc normal.

Notez que CC-SG désactive ces messages depuis la version 4.0, mais ils sont toujours disponibles dans les journaux internes. Aussi, lorsque vous effectuez la mise à niveau de CC-SG de 3.x à 4.x, ces messages de la console de diagnostic disparaissent.

Index

A

B

C

D

E

F

G

I

L

M

N

O

P

Q

R

S

T

U

V

Etats-Unis/Canada/Amérique latine

Lundi - Vendredi
8h00 - 20h00, heure de la côte Est des Etats-Unis
Tél. : 800-724-8090 ou 732-764-8886
Pour CommandCenter NOC : appuyez sur 6, puis sur 1.
Pour CommandCenter Secure Gateway : appuyez sur 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

Chine

Beijing

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-10-88091890

Shanghai

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-21-5425-2499

Guangzhou

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-20-8755-5561

Inde

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +91-124-410-7881

Japon

Lundi - Vendredi
9h30 - 17h30, heure locale
Tél. : +81-3-3523-5994
E-mail : support.japan@raritan.com

Europe

Europe

Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +31-10-2844040
E-mail : tech.europe@raritan.com

Royaume-Uni

Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +44-20-7614-77-00

France

Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +33-1-47-56-20-39

Allemagne

Lundi - Vendredi
8h30 - 17h30, CET (UTC/GMT+1)
Tél. : +49-20-17-47-98-0
E-mail : rg-support@raritan.com

Melbourne, Australie

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +61-3-9866-6887

Taiwan

Lundi - Vendredi
9h00 - 18h00, UTC/GMT - Heure normale 5 - Heure avancée 4
Tél. : +886-2-8919-1333
E-mail : support.apac@raritan.com