CommandCenter®
Secure Gateway

CC-SG

Manuel de l'administrateur

Version 3.1

CCA-0D-F

Janvier 2007

255-80-5140-00

Cette page est laissée intentionnellement blanche.

Copyright et marques

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.

Homologations au 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.

*Pour toute assistance en Amérique du Nord ou du Sud, prenez contact avec l'équipe de support technique Raritan par téléphone au (732) 764-8886, par fax au (732) 764-8887, ou par e-mail à l'adresse suivante : **tech@raritan.com**.*

Contactez l'assistance technique – du lundi au vendredi, de 8h00 à 20h00 (heure de la côte Est des Etats-Unis).

Pour toute assistance dans le reste du monde, consultez la dernière page de ce manuelafin d'obtenir les coordonnées des bureaux régionaux de Raritan.

Consignes de sécurité

Pour éviter tout risque d'électrocution fatale et de dommages éventuels à l'équipement Raritan :

- N'utilisez de câble d'alimentation à 2 fils dans aucune configuration du produit.
- Testez les prises CA de l'ordinateur et de l'écran pour vérifier qu'elles sont correctement connectées et mises à la terre.
- Utilisez uniquement des prises mises à la terre pour l'ordinateur comme pour l'écran. Si vous utilisez un onduleur de secours, débranchez l'ordinateur, l'écran et l'appareil de l'alimentation.

Consignes de sécurité pour montage en rack

Pour les produits Raritan qui doivent être montés en rack, prenez les précautions suivantes :

- La température de fonctionnement dans un environnement de rack fermé peut être supérieure à la température ambiante. Ne dépassez pas la température ambiante maximum recommandée des appareils (reportez-vous à l'Annexe A : Spécifications).
- Assurez-vous que la circulation d'air dans l'environnement de rack est suffisante.
- Montez l'équipement dans le rack avec précaution de façon à éviter tout chargement bancal des composants mécaniques.
- Branchez l'équipement au circuit d'alimentation avec précaution afin d'éviter une surcharge des circuits.
- Mettez tout l'équipement correctement à la terre sur le circuit terminal, notamment les raccords d'alimentation tels que les barrettes d'alimentation (autres que celles branchées directement).

Table des matières

Figures

Cette page est laissée intentionnellement blanche.

Chapitre 1 : Introduction

Nous vous félicitons d'avoir acheté CommandCenter Secure Gateway (CC-SG), la méthode pratique et sécurisée de Raritan pour gérer plusieurs serveurs Unix, pare-feu, routeurs, équilibreurs de charge, dispositifs de gestion de l'alimentation et serveurs Windows.

CC-SG permet de centraliser la gestion et l'administration à l'aide d'un ensemble d'appareils de série et KVM. Il est conçu pour être utilisé dans différents environnements, des centres de données à haute densité aux entreprises gérant d'importants bureaux éloignés, en passant par les prestataires de services.

Lorsque CC-SG est utilisé conjointement aux appareils de gestion par niveau de port Dominion ou IP-Reach, l'administration des dispositifs cible (qualifiés de « nœuds ») est rationalisée et simplifiée, ce qui facilite celle des équipements des centres de données grâce à la connexion au réseau IP et la présentation des ports de console série et KVM de tous les nœuds présents sur le réseau géré.

Conditions préalables

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

Public visé

Ce document est destiné aux administrateurs qui disposent normalement de tous les privilèges disponibles. Reportez-vous à l'**Annexe C : Privilèges de groupe d'utilisateurs**. Les autres utilisateurs possèdent généralement moins de droits, par exemple seul le droit d'accès aux nœuds leur est attribué. Ces utilisateurs peuvent consulter le **Manuel d'utilisation de CommandCenter Secure Gateway** pour plus d'informations.

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.
- **Associations** – désigne la relation entre les catégories, les éléments de catégorie, et les ports ou dispositifs. Par exemple, si vous souhaitez associer la catégorie Emplacement à un dispositif, commencez par créer des associations avant d'ajouter des dispositifs et des ports dans CC-SG.
- **Catégorie** – variable contenant un jeu de valeurs ou d'éléments. Un exemple de catégorie est Emplacement, qui peut contenir comme éléments New York City, Philadelphia, ou encore Data Center 1. Lorsque vous ajoutez des dispositifs ou des ports dans CC-SG, vous leur associez ce type d'informations. Il est conseillé de commencer par configurer correctement les associations avant d'ajouter les dispositifs et les ports. Type de SE est un autre exemple de catégorie, qui peut contenir des éléments tels que Windows®, Unix® ou Linux®.
- **CIM** (Module d'interface pour ordinateur) – désigne le matériel utilisé pour connecter un serveur cible et un dispositif Raritan. Chaque cible nécessite un module CIM, sauf le Dominion KX101 qui est relié directement à une cible et n'a par conséquent pas besoin d'un module CIM. Les serveurs cible doivent être mis sous tension et connectés aux CIM, lesquels doivent être connectés au dispositif Raritan AVANT d'ajouter celui-ci et de configurer les ports dans CC-SG. Sinon, le nom d'un CIM en blanc remplacera le nom du port CC-SG. Les serveurs doivent être redémarrés après avoir été connectés à un CIM.
- **CommandCenter NOC (CC NOC)** – console de surveillance réseau qui permet l'audit et la surveillance de l'état des serveurs, de l'équipement et des dispositifs Raritan gérés par CC-SG.
- **Groupe de dispositifs** – groupe défini de dispositifs accessibles à un utilisateur. Les groupes de dispositifs sont utilisés lors de la création des stratégies permettant de contrôler l'accès aux dispositifs présents dans ces groupes.

- **Dispositifs** – désigne des produits de Raritan, tels que Dominion KX116, Dominion SX48, Dominion KSX440, IP-Reach, Paragon II System Controller, Paragon II UMT832, etc., gérés par CC-SG. Ces dispositifs contrôlent les systèmes et serveurs cible auxquels ils sont connectés.
- **Director Client** – client Java pour CC-SG utilisable par les utilisateurs standard et les administrateurs. Il s'agit du seul client autorisant l'administration.
- **Eléments** – désigne les valeurs d'une catégorie. Par exemple, l'élément New York City appartient à la catégorie Emplacement. Autre exemple : l'élément Windows appartient à la catégorie Type de SE.
- **Port fantôme** – un port fantôme peut se produire lors de la gestion de dispositifs Paragon et lors de la suppression du système ou de la mise hors tension (manuelle ou accidentelle) d'un CIM ou d'un serveur cible. Reportez-vous au *Manuel d'utilisation de Paragon II* pour plus d'informations.
- **Nom d'hôte** – un nom d'hôte est utilisable si la prise en charge des serveurs DNS est activée. Reportez-vous à **Gestionnaire de configuration** dans le **Chapitre 12 : Administration avancée** pour plus d'informations. Le nom d'hôte et le nom de domaine complet qualifié (NDCQ = nom d'hôte + suffixe) associé ne peuvent pas dépasser 257 caractères. Il peut être constitué d'un nombre illimité de composants, à condition qu'ils soient séparés par « . ». Chaque composant doit avoir une taille maximale de 63 caractères, le premier d'entre eux étant obligatoirement alphabétique. Les autres caractères peuvent être alphabétiques, numériques ou le signe « - » (trait d'union ou moins). Le dernier caractère d'un composant ne peut pas être le signe « - ». Même si le système conserve la casse des caractères entrés dans le système, le NDCQ n'est pas sensible à la casse lorsqu'il est utilisé.
- **iLO/RILOE** – désigne les serveurs Integrated Lights Out/Remote Insight Lights Out de Hewlett Packard qui peuvent être gérés par CC-SG. Les cibles d'un dispositif iLO/RILOE sont mises sous/hors tension et recyclées directement. Les dispositifs iLO/RILOE ne peuvent pas être détectés par CC-SG ; il faut les ajouter manuellement en tant que nœuds.
- **Accès en bande** – désigne le fait de passer par le réseau TCP/IP pour corriger ou dépanner une cible du réseau. Les dispositifs KVM et série sont accessibles à l'aide des applications en bande suivantes : **RemoteDesktop Viewer**, **SSH Client**, **RSA Client**, **VNC Viewer**.
- **Serveurs IPMI** (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** – définissent les autorisations, le type d'accès et les nœuds et dispositifs auxquels un groupe d'utilisateurs a accès. Les stratégies sont appliquées à un groupe d'utilisateurs et sont dotées de plusieurs paramètres de contrôle, tels que la date et l'heure d'accès, afin de déterminer le niveau de contrôle.
- **Nœuds** – désigne les systèmes cible, tels que les serveurs, les PC de bureau ou tout autre équipement réseau, auxquels les utilisateurs de CC-SG peuvent accéder.
- **Interfaces** – fournissent un moyen d'accéder à un nœud, via une solution hors bande, telle qu'une connexion Dominion KX101, ou via une solution en bande, telle qu'un serveur VNC.
- **Groupe de nœuds** – groupe défini de nœuds accessibles à un utilisateur. Les groupes de nœuds sont utilisés lors de la création des stratégies permettant de contrôler l'accès aux nœuds présents dans ces groupes.
- **Ports** – points de connexion entre un dispositif Raritan et un nœud. Les ports n'existent que sur les dispositifs Raritan et identifient une voie d'accès du dispositif à un nœud.
- **SASL** (Simple Authentication and Security Layer) – méthode utilisée pour ajouter la prise en charge de l'authentification aux protocoles basés sur les connexions.
- **SSH** – clients, tels que Putty ou OpenSSH, qui fournissent une interface de ligne de commande à CC-SG. SSH ne comprend qu'un sous-ensemble des commandes CC-SG pour administrer des dispositifs et CC-SG lui-même. Reportez-vous au **Chapitre 12 : Administration avancée** pour plus d'informations.
- **Groupe d'utilisateurs** – ensemble d'utilisateurs partageant le même niveau d'accès et les mêmes droits. Par exemple, le groupe d'utilisateurs par défaut **System Administrators** (administrateurs système) dispose d'un accès total à l'ensemble des tâches de configuration et des nœuds cible.

Chapitre 2 : Accès à CC-SG

Une fois son adresse IP configurée, l'unité CC-SG peut être placée à son emplacement final. Effectuez toutes les connexions matérielles nécessaires pour que l'unité soit opérationnelle.

Vous pouvez accéder à CC-SG de plusieurs manières, chacune d'elles étant décrite dans ce chapitre :

- **Navigateur** : CC-SG prend en charge de nombreux navigateurs Web. (Pour obtenir une liste complète des navigateurs et plates-formes pris en charge, reportez-vous à la **Matrice de compatibilité** sur **http://www.raritan.com/support**. Dans la page **Support** (Assistance), cliquez sur **Firmware Upgrades** (Mises à niveau de firmware), puis sur **CommandCenter Secure Gateway**.)
- **Client lourd** : vous pouvez installer un client lourd Java Web Start sur votre ordinateur client. Le client lourd fonctionne exactement comme le client par navigateur.
- **SSH** : les dispositifs distants connectés via le port série sont accessibles à l'aide de SSH. Reportez-vous à **Chapitre 12 : Administration avancée** pour plus d' informations.
- **Console de diagnostic** : elle permet uniquement des diagnostics et des réparations d'urgence, mais ne remplace pas l'interface utilisateur graphique par navigateur pour configurer et utiliser CC-SG. Reportez-vous à **Chapitre 12 : Administration avancée** pour plus d' informations.

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

Accès via un navigateur

1. Dans un navigateur Internet prise en charge, entrez l'URL : **https://<adresse_IP>/admin**, où **<adresse_IP>** indique l'adresse IP de CC-SG. Par exemple, **https://10.20.3.30/admin**. Lorsque le message d'alerte de sécurité s'affiche, cliquez sur **Oui** pour continuer. Le protocole SSL est toujours activé dans CC-SG. Lorsque vous vous connectez via Internet Explorer, le message d'alerte de sécurité s'affiche car le certificat racine de l'AC n'est pas installé dans le navigateur.
2. Le système vous avertit si la version de Java Runtime Environment installée sur votre machine n'est pas prise en charge. Dans la fenêtre qui s'affiche, indiquez si vous souhaitez télécharger la version de Java Runtime Environment correcte depuis le serveur CC-SG (le cas échéant) ou depuis le site Web de Sun Microsystems, ou si vous préférez continuer à utiliser la version incorrecte. Cliquez ensuite sur **OK**. La fenêtre de connexion s'affiche.

Figure 1 Fenêtre Connexion

3. 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**.
4. Saisissez vos **Nom d'utilisateur** et **Mot de passe**, puis cliquez sur **Connexion**.

Accès via un client lourd

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

Installer le client lourd

1. Pour télécharger le client lourd depuis CC-SG, lancez un navigateur Web et entrez l'URL : **/install: https://<IP address/install>**, où <adresse_IP> indique l'adresse IP de CC-SG.
2. Si un avertissement de sécurité apparaît, cliquez sur **Démarrer** pour continuer le téléchargement.
3. Si votre ordinateur client exécute Java version 1.4, une fenêtre **Desktop Integration** s'affiche. Si vous souhaitez que Java ajoute une icône de raccourci pour le client lourd sur votre bureau, cliquez sur Oui.
4. Une fois le téléchargement terminé, une nouvelle fenêtre apparaît vous permettant d'indiquer l'adresse IP de CC-SG.

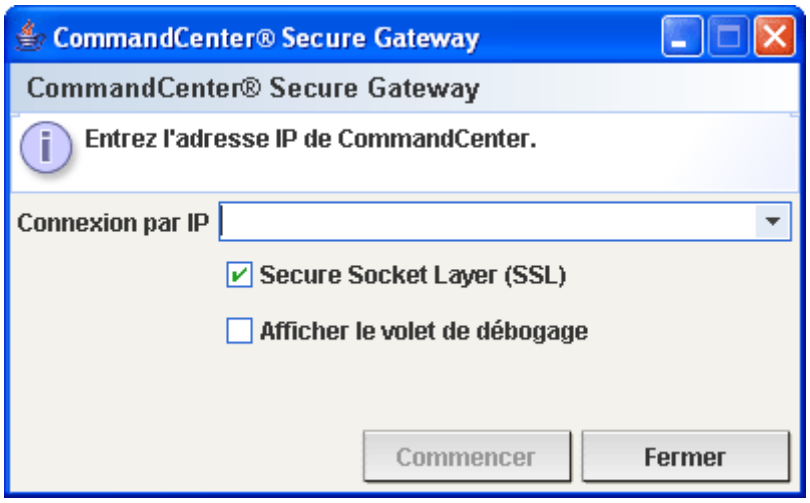

Figure 2 Fenêtre de spécification de l'adresse IP du client lourd

5. 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.
6. 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.
   - **Pour vérifier le paramètre dans CC-SG** : dans le menu **Administration**, cliquez sur **Sécurité**. Dans l'onglet **Généralités**, observez le champ **Protocole de connexion du navigateur**. Si l'option **HTTPS/SSL** est sélectionnée, vous devez alors cocher la case **Secure Socket Layer SSL** dans la fenêtre de spécification de l'adresse IP du client lourd. Si l'option **HTTP** est sélectionnée, vous devez alors désactiver la case **Secure Socket Layer SSL** dans la fenêtre de spécification de l'adresse IP du client lourd.
7. 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.

8. L'écran de connexion apparaît ; le client lourd ressemble à son homologue par navigateur et se comporte comme lui. 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

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

- **Java 1.4.x**

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

- **Java 1.5**

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

a. lancer le client lourd depuis le visualiseur du cache de l'application Java du panneau de configuration Java ;
b. 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.

Composants de la fenêtre CC-SG

Si la connexion aboutit, la fenêtre de l'application CC-SG s'affiche.

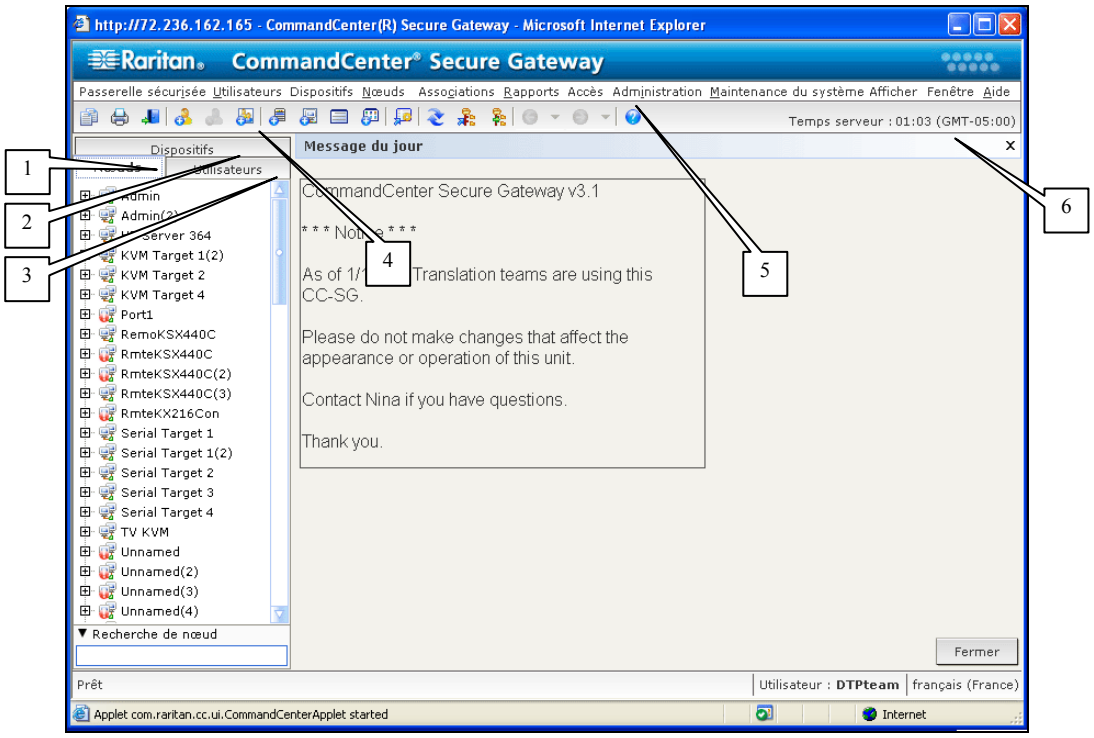

Figure 3 Composants de la fenêtre CC-SG

1. **Onglet Nœuds** : cliquez sur l'onglet **Nœuds** pour afficher tous les nœuds cible connus sous la forme d'une arborescence. Cliquez sur un nœud pour visualiser son profil. Les interfaces sont regroupées sous leurs nœuds parents. Cliquez sur les signes + et - pour développer ou réduire l'arborescence. Pour vous connecter à une interface, cliquez sur celle-ci avec le bouton droit de la souris et sélectionnez **Connecter**. Vous pouvez trier les nœuds par nom (ordre alphabétique) ou par état (Disponible, Occupé, Non disponible). Cliquez avec le bouton droit sur l'arborescence, sélectionnez **Options de tri du nœud**, puis **Par nom de nœud** ou **Par état de nœud**.
2. **Onglet Utilisateurs** : cliquez sur l'onglet **Utilisateurs** pour afficher tous les utilisateurs et groupes enregistrés sous la forme d'une arborescence. Cliquez sur les signes + et - pour développer ou réduire l'arborescence.
3. **Onglet Dispositifs** : cliquez sur l'onglet **Dispositifs** pour afficher tous les dispositifs Raritan connus sous la forme d'une arborescence. Des icônes différentes sont associées aux différents types de dispositifs. Les ports sont regroupés sous leurs dispositifs parents. Cliquez sur les signes + et - pour développer ou réduire l'arborescence. Cliquez sur un port pour visualiser son profil. Pour vous connecter à un port, cliquez sur celui-ci avec le bouton droit de la souris et sélectionnez **Connecter**. Vous pouvez trier les ports par nom (ordre alphabétique) ou par état (Disponible, Occupé, Non disponible). Cliquez avec le bouton droit sur l'arborescence, sélectionnez **Options de tri des ports**, puis **Par nom de port** ou **Par état de port**.
4. **Barre d'outils Commandes rapides** : cette barre d'outils propose des boutons de raccourci pour exécuter des commandes courantes.
5. **Barre de menus Utilisation et configuration** : ces menus contiennent des commandes permettant d'utiliser et de configurer CC-SG. Vous pouvez également accéder à certaines de ces commandes en cliquant avec le bouton droit sur les icônes des onglets de sélection **Nœuds**, **Utilisateurs** et **Dispositifs**. L'affichage des menus et des éléments qu'ils contiennent dépend de vos droits d'accès d'utilisateur.
6. **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 Gestion des tâches dans le **Chapitre 12 : Administration avancée** pour plus d'informations. L'heure affichée peut être différente de celle utilisée par le client.

Vérification de l'adresse IP, de la version du firmware et des versions d'application

Une fois connecté, vous devez confirmer l'adresse IP, définir l'heure du serveur CC-SG et vérifier les versions du firmware et des applications installées. Il vous faudra peut-être mettre à niveau le firmware et les applications.

Confirmer l'adresse IP

1. Dans le menu Administration, cliquez sur Configuration pour ouvrir l'écran Gestionnaire de configuration.
2. Cliquez sur l'onglet **Configuration réseau**.

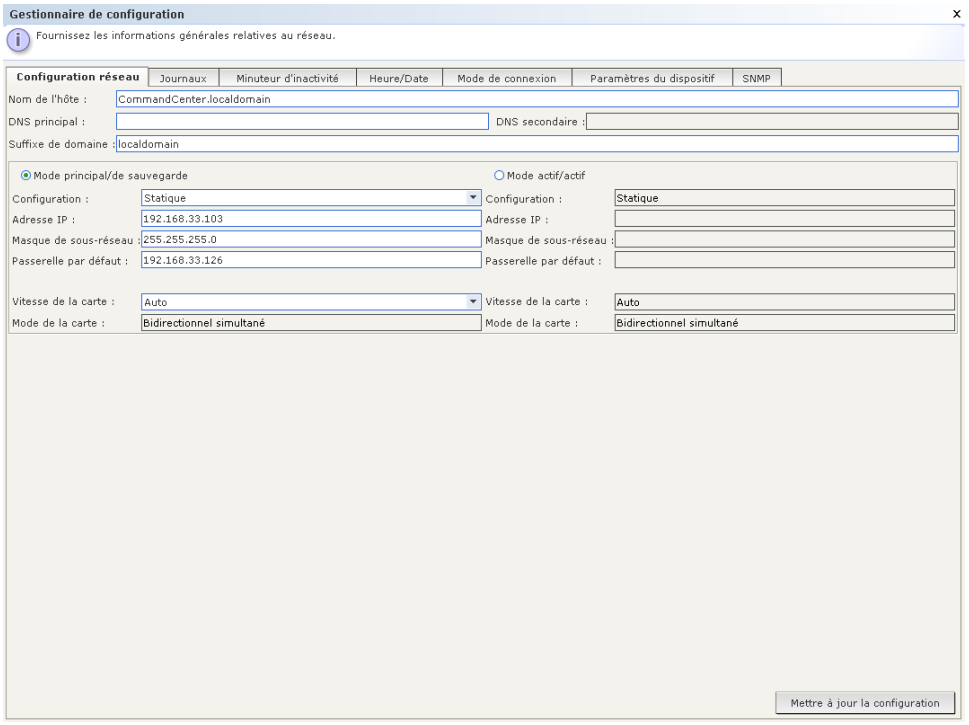

Figure 4 Confirmer l'adresse IP

3. Assurez-vous que les paramètres réseau sont corrects ou effectuez les modifications nécessaires.
4. Cliquez sur **Mettre à jour la configuration** pour soumettre vos modifications.
5. Cliquez sur **OK** dans la fenêtre de confirmation qui s'affiche pour valider vos paramètres, vous déconnecter et redémarrer CC-SG.
6. Accédez à CC-SG à l'aide de la nouvelle adresse IP.

Définir l'heure du serveur CC-SG

1. Connectez-vous à CC-SG.
2. Dans le menu **Administration**, cliquez sur **Configuration** pour ouvrir l'écran **Gestionnaire de configuration**.
3. Cliquez sur l'onglet **Heure/Date**.

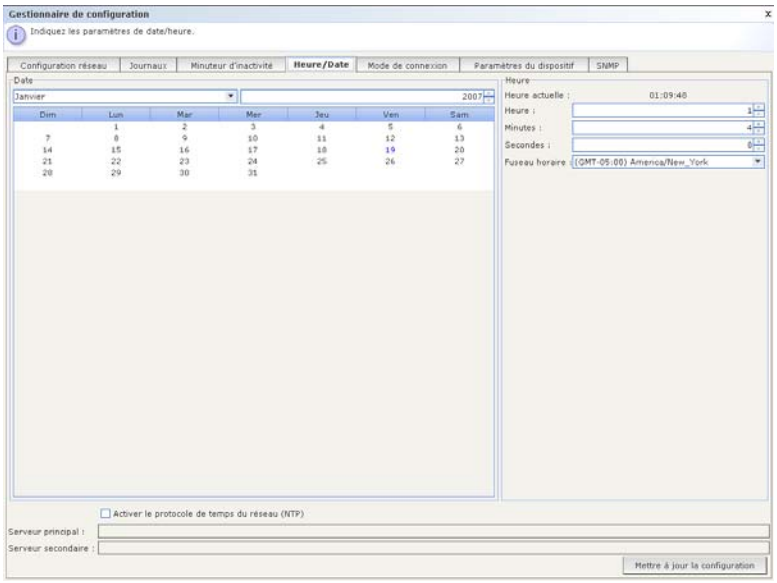

Figure 5 Configuration de l'heure et de la date

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

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

6. Cliquez sur **Mettre à jour la configuration** pour appliquer les modifications relatives à l'heure et à la date à l'unité CC-SG.
7. Cliquez sur **Rafraîchir** pour recharger le nouveau temps serveur dans le champ **Heure actuelle**.
8. Dans le menu **Maintenance du système**, cliquez sur **Redémarrer** pour relancer CC-SG.

Vérifier et mettre à niveau la version du firmware de CC-SG

1. Connectez-vous à CC-SG.
2. Dans le menu **Aide**, cliquez sur **A propos de Raritan Secure Gateway**. Une fenêtre pop-up contenant le numéro de version du firmware apparaît. Cliquez sur **OK**.
3. Si la version n'est pas à jour, vous devez mettre à niveau votre firmware. Vous pouvez télécharger le fichier de mise à niveau du firmware depuis le site Web de Raritan ou le copier depuis un CD Raritan. Enregistrez le fichier de mise à niveau du firmware sur votre PC client.

***Remarque** : avant de mettre à niveau CC-SG, vous devez passer en mode de maintenance. Reportez-vous à **Mode de maintenance** dans le **Chapitre 11 : Maintenance du système** pour plus d'informations.*

4. Dans le menu Maintenance du système, cliquez sur Mode de maintenance, puis sur Entrer en mode de maintenance.
5. Dans les champs correspondants de l'écran **Entrer en mode de maintenance**, tapez le message qui apparaîtra aux utilisateurs qui vont être déconnectés de CC-SG, et le délai (en minutes) du passage en mode de maintenance, puis cliquez sur **OK**.
6. Cliquez sur **OK** dans la boîte de dialogue de confirmation.
7. Un second message de confirmation apparaîtra lorsque CC-SG passera en mode de maintenance. Cliquez sur **OK**.
8. Dans le menu Maintenance du système, cliquez sur Mettre à niveau.

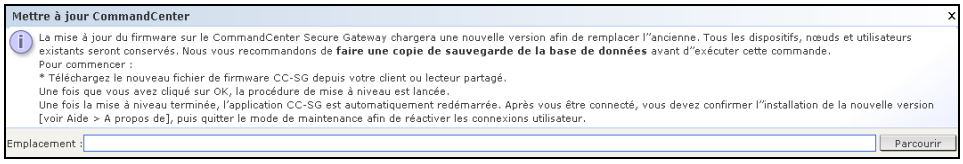

Figure 6 Mettre à niveau CC-SG

9. Cliquez sur **Parcourir**, recherchez et sélectionnez le fichier de mise à niveau du firmware dans la boîte de dialogue Ouvrir qui apparaît, puis cliquez sur **Ouvrir**.
10. Cliquez sur **OK** dans l'écran Mettre à jour CommandCenter.

***Remarque** : si vous avez obtenu le firmware sous forme de fichier zip, décompressez-le, puis suivez les instructions fournies dans le fichier LISEZMOI.*

Vérifier et mettre à niveau les 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).

1. Dans le menu **Administration**, cliquez sur **Applications**.

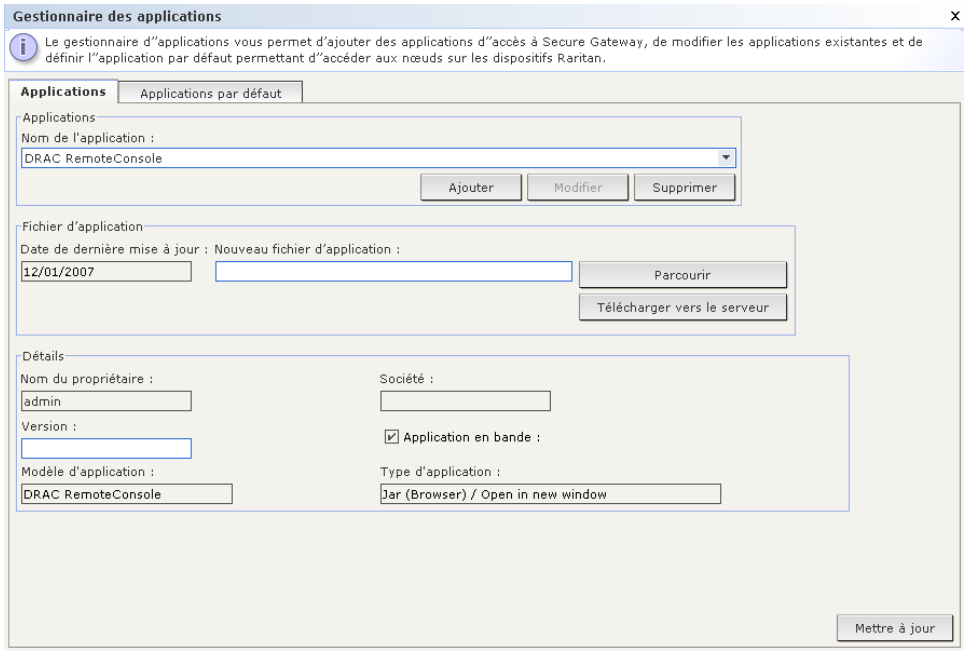

Figure 7 Gestionnaire des applications de CC-SG

2. Cliquez sur la flèche déroulante **Nom de l'application** et sélectionnez une application dans la liste. Notez le numéro figurant dans le champ **Version**.
3. 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 ou le copier depuis un CD Raritan. Enregistrez le fichier de mise à niveau de l'application sur votre PC client. (Pour obtenir une liste complète des versions d'application prises en charge, reportez-vous à la **Matrice de compatibilité** sur **http://www.raritan.com/support**. Dans la page **Support** (Assistance), cliquez sur **Firmware Upgrades** (Mises à niveau de firmware), puis sur **CommandCenter Secure Gateway**.)
4. Cliquez sur la flèche déroulante **Nom de l'application** et sélectionnez l'application que vous souhaitez mettre à niveau dans la liste.
5. 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**.
6. Le nom de l'application s'affiche dans le champ **Nouveau fichier d'application** de l'écran **Gestionnaire des applications**.
7. Cliquez sur **Télécharger vers le serveur**. Une fenêtre de progression 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 qu'elle peut être configurée et connectée à un port spécifique.
8. Si nécessaire, entrez le nouveau numéro de version dans le champ **Version**. Le champ **Version** s'actualise automatiquement pour certaines applications.
9. Cliquez sur **Mettre à jour**.
10. Cliquez sur Fermer pour fermer l'écran Gestionnaire des applications.

Mise hors tension de CC-SG

Si une panne d'alimentation en courant alternatif se produit sur une unité V1 alors qu'elle est en marche et exécute CC-SG, celle-ci se rappellera de son dernier état avant la coupure. Une fois l'alimentation rétablie, l'unité V1 redémarre automatiquement. En revanche, si la coupure d'alimentation se produit lorsque l'unité V1 est hors tension, cette dernière restera hors tension lorsque le courant sera rétabli.

Important : ne maintenez pas le bouton d'alimentation enfoncé pour forcer la mise hors tension de CC-SG. Pour mettre CC-SG hors tension, nous vous recommandons de suivre la procédure décrite ci-dessous.

Pour mettre CC-SG hors tension, procédez comme suit :

1. Retirez le cache, puis enfoncez fermement le bouton d'alimentation. Sur les unités G1, le bouton d'alimentation se trouve à l'arrière de l'unité.
2. Patientez environ une minute, le temps que CC-SG s'éteigne normalement.

***Remarque** : les utilisateurs connectés à CC-SG via la console de diagnostic recevront un court message à diffusion générale au moment de la mise hors tension de l'unité CC-SG. Les utilisateurs connectés à CC-SG via un navigateur Web ou SSH ne recevront pas de message lors de la mise hors tension de l'unité CC-SG.*

3. Si vous devez retirer le câble d'alimentation, attendez la fin du processus de mise sous 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.

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.

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

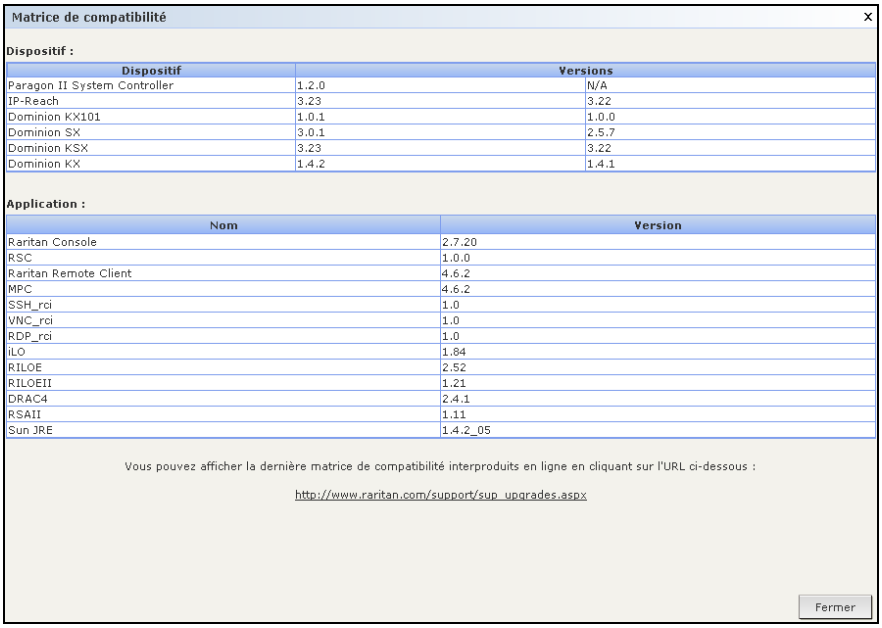

Figure 8 Matrice de compatibilité

Cette page est laissée intentionnellement blanche.

Chapitre 3 : Configuration de CC-SG par paramétrage guidé

Préparation de la configuration de CC-SG par 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 et à la création d'un compte administrateur de CC-SG.

Vue d'ensemble du paramétrage guidé

Le paramétrage guidé est une méthode simple permettant d'effectuer les tâches de configuration initiales de CC-SG, une fois le système 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.

Démarrage du paramétrage guidé

Dans le menu **Administration**, cliquez sur **Paramétrage guidé**. La fenêtre **Paramétrage guidé** apparaît. Le panneau gauche de la fenêtre répertorie les **tâches guidées** sous la forme d'une arborescence. Le côté droit de la fenêtre affiche le panneau correspondant à la tâche active.

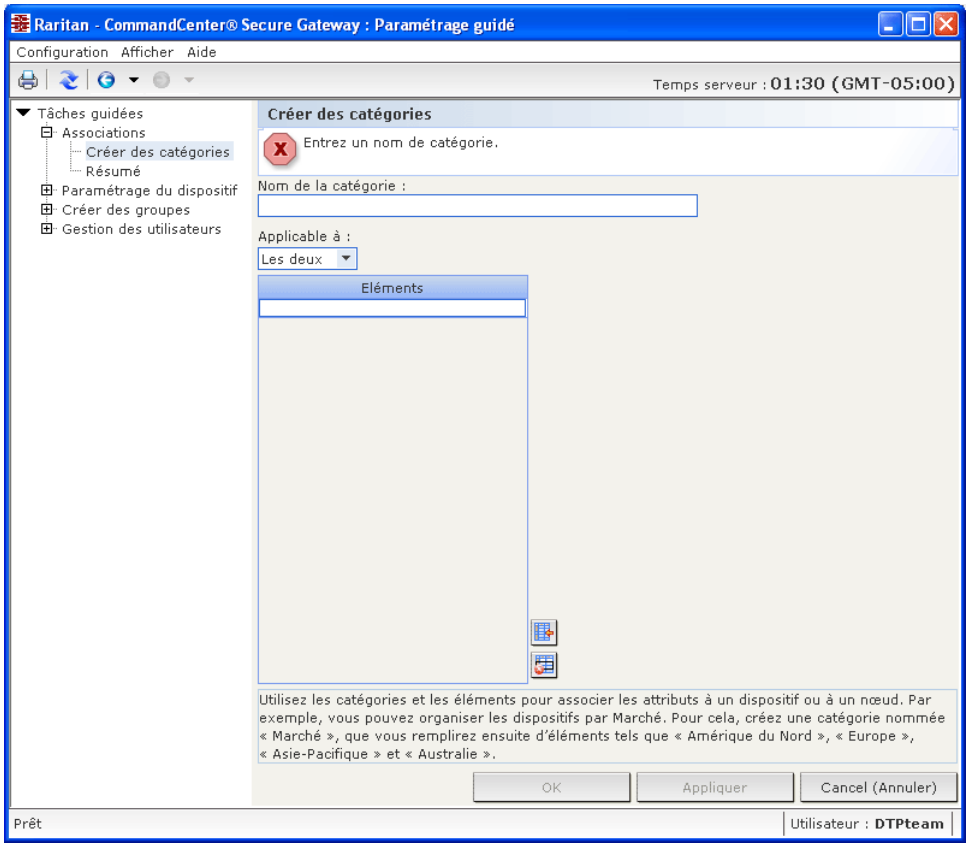

Figure 9 Fenêtre Paramétrage guidé

Le paramétrage guidé se divise en quatre tâches, expliquées dans les sections suivantes :

- **Associations** : permet de définir les catégories et éléments utilisés pour organiser vos équipements.

- **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.
- **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.
- **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.

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 les sous-ensembles de la Catégorie. Par exemple, pour organiser les équipements par emplacement, vous pouvez créer une catégorie appelée Emplacement et des éléments pour l'emplacement de chaque serveur, tels que Philadelphie, New York et La Nouvelle Orléans.

Créer des catégories et des éléments

1. Dans la fenêtre **Paramétrage guidé**, le panneau par défaut est **Créer des catégories**. Cliquez sur **Associations**, puis sur **Créer des catégories** dans le panneau de gauche pour ouvrir le panneau du même nom.

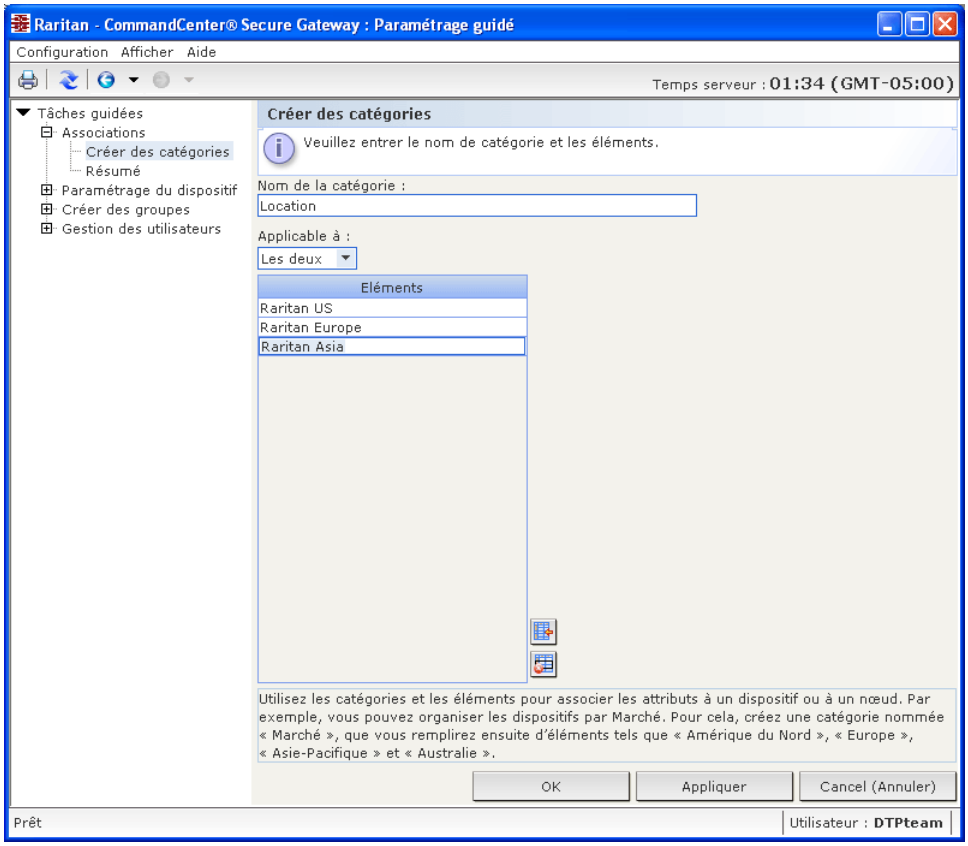

Figure 10 Paramétrage guidé – Créer des catégories et des éléments

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, pour des nœuds ou pour les deux. 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 le nombre de rangées nécessaires à la table **Eléments**.
- Pour supprimer un élément de la table **Eléments**, sélectionnez la ligne correspondante, puis cliquez sur l'icône Supprimer la ligne.

5. Répétez ces étapes pour ajouter tous les éléments de la catégorie dans la table **Eléments**.
6. Si vous souhaitez créer une autre catégorie, cliquez sur **Appliquer** pour enregistrer la catégorie en cours, puis répétez les étapes de cette section pour ajouter des catégories supplémentaires.
7. Une fois les catégories et éléments créés, cliquez sur **OK**. Le panneau Résumé des associations affiche la liste des catégories et des éléments que vous avez créés.
8. Cliquez sur **Continue** (continuer) pour démarrer la tâche suivante, **Paramétrage du dispositif**. Suivez les étapes de la section suivante.

Paramétrage du dispositif

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

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

Détecter et ajouter des dispositifs

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

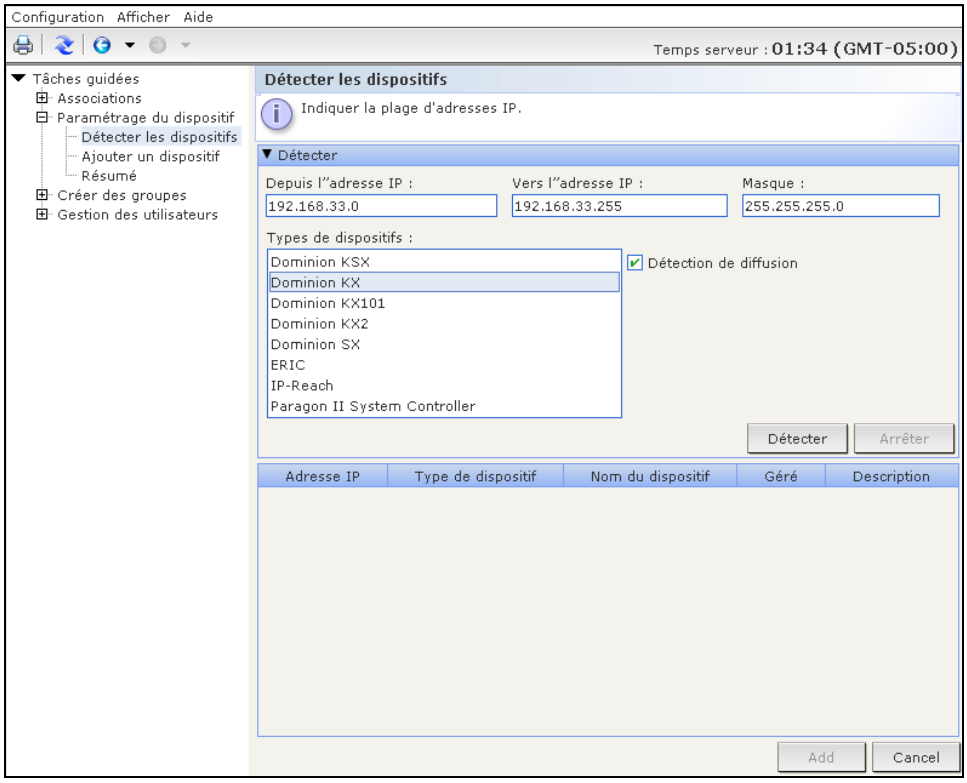

Figure 11 Paramétrage guidé – Détecter les dispositifs

2. Dans les champs **Depuis l'adresse IP** et **Vers l'adresse IP**, entrez la plage d'adresses IP où vous souhaitez rechercher des dispositifs.
3. Dans le champ **Masque**, entrez le masque de sous-réseau dans lequel vous souhaitez rechercher des dispositifs.
4. 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.
5. 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**.
6. Cliquez sur **Détecter**.
7. A la fin de la détection, un message de confirmation s'affiche. Cliquez sur **OK** dans le message de confirmation.
8. Si CC-SG a détecté des dispositifs du type spécifié et dans la plage d'adresses spécifiée, ils s'affichent dans une table de la section inférieure du panneau **Détecter les dispositifs**. Vous pouvez cliquer sur la flèche noire en haut du panneau pour masquer la section supérieure, et ainsi agrandir l'affichage des résultats de la détection dans la section inférieure du panneau.

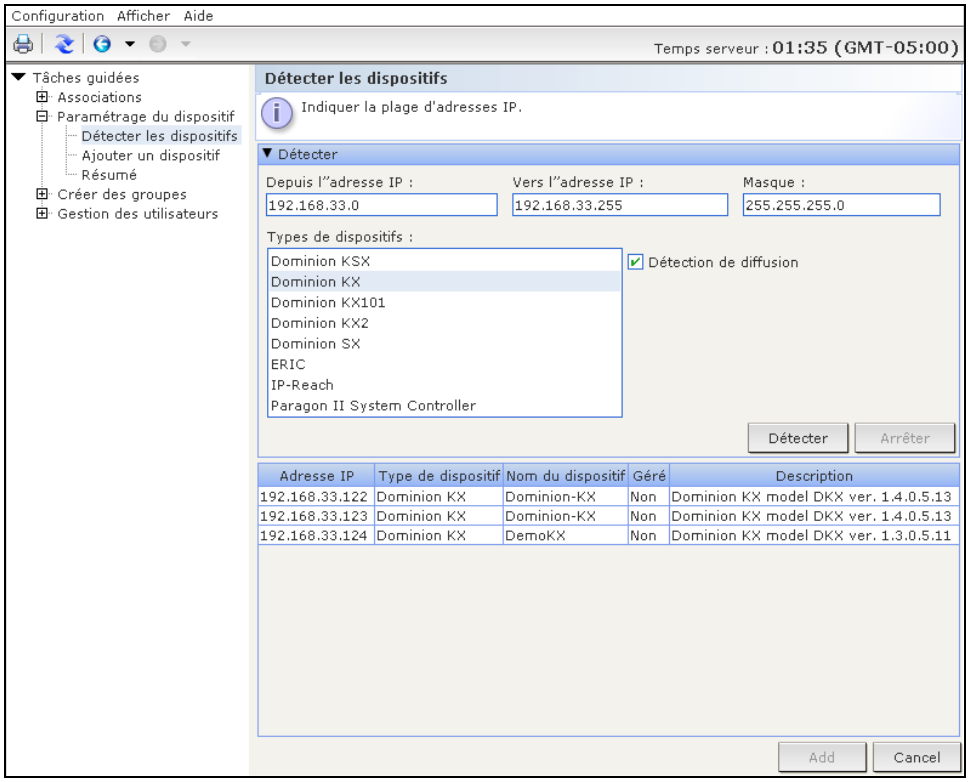

Figure 12 Paramétrage guidé – Résultats de la détection des dispositifs

9. Dans la table des dispositifs détectés, sélectionnez le dispositif à inclure à CC-SG, puis cliquez sur **Add** (ajouter). Le panneau **Ajouter un dispositif** s'ouvre. Le panneau **Ajouter un dispositif** varie légèrement selon le type de dispositif ajouté.

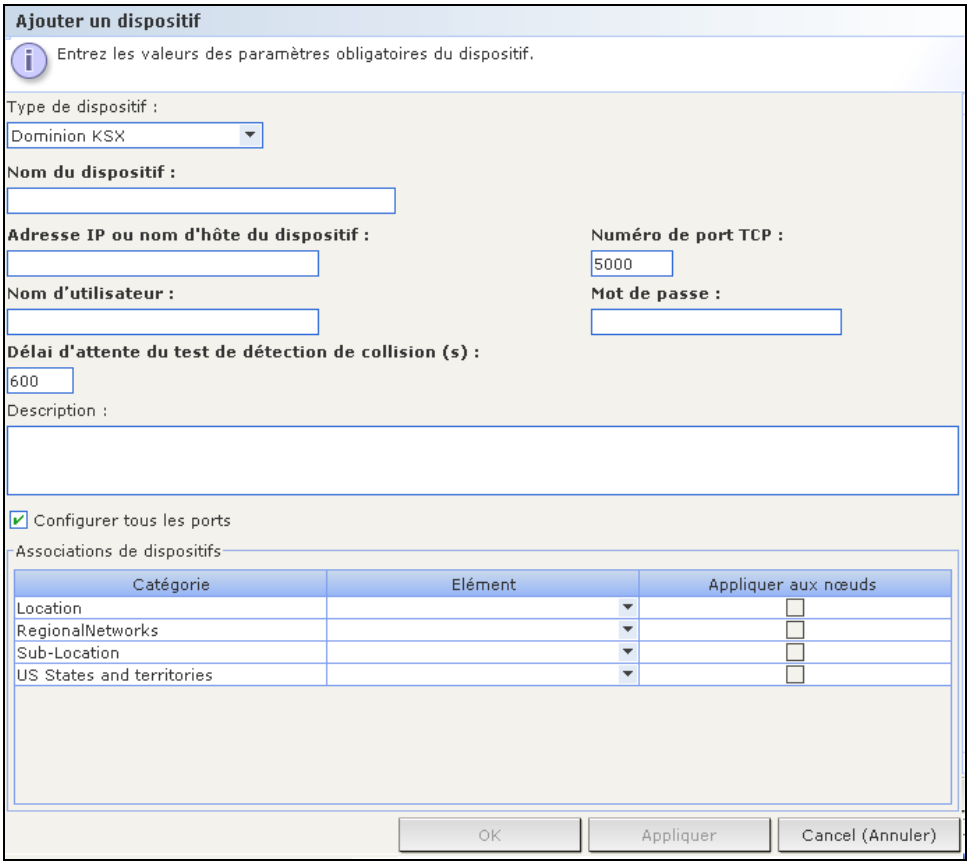

Figure 13 Paramétrage guidé – Ajouter un dispositif

10. Vous pouvez modifier le **nom du dispositif** et la **description** en entrant de nouvelles données dans les champs correspondants.
11. 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.
12. Le champ **Numéro de port TCP** est rempli automatiquement en fonction du type de dispositif.
13. 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.
14. 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.
15. Si vous ajoutez un dispositif Dominion SX, cochez la case **Accès local : Autorisé** pour autoriser l'accès local au dispositif. Désactivez la case **Accès local : Autorisé** pour interdire l'accès local au dispositif.
16. 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.
17. 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.
18. 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.
19. Dans la section **Associations de dispositifs** au bas du panneau, cliquez sur la flèche déroulante de la colonne Elément correspondant à chaque catégorie à affecter au dispositif, puis sélectionnez l'élément à associer au dispositif dans la liste.

20. Pour appliquer l'élément au dispositif et aux nœuds connectés à celui-ci, cochez la case **Appliquer aux nœuds**.
21. Si vous souhaitez ajouter un autre dispositif, cliquez sur **Appliquer** pour enregistrer le dispositif en cours, puis répétez les étapes de cette section pour ajouter des dispositifs supplémentaires.
22. Une fois l'ajout des dispositifs terminé, cliquez sur **OK**. Le panneau **Résumé du dispositif** affiche la liste des dispositifs que vous avez ajoutés.
23. Cliquez sur **Continue** (continuer) pour démarrer la tâche suivante, **Créer des groupes**. Suivez les étapes de la section suivante.

Créer des groupes

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

Ajouter des groupes de dispositifs et de nœuds

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

Sélectionner les dispositifs

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

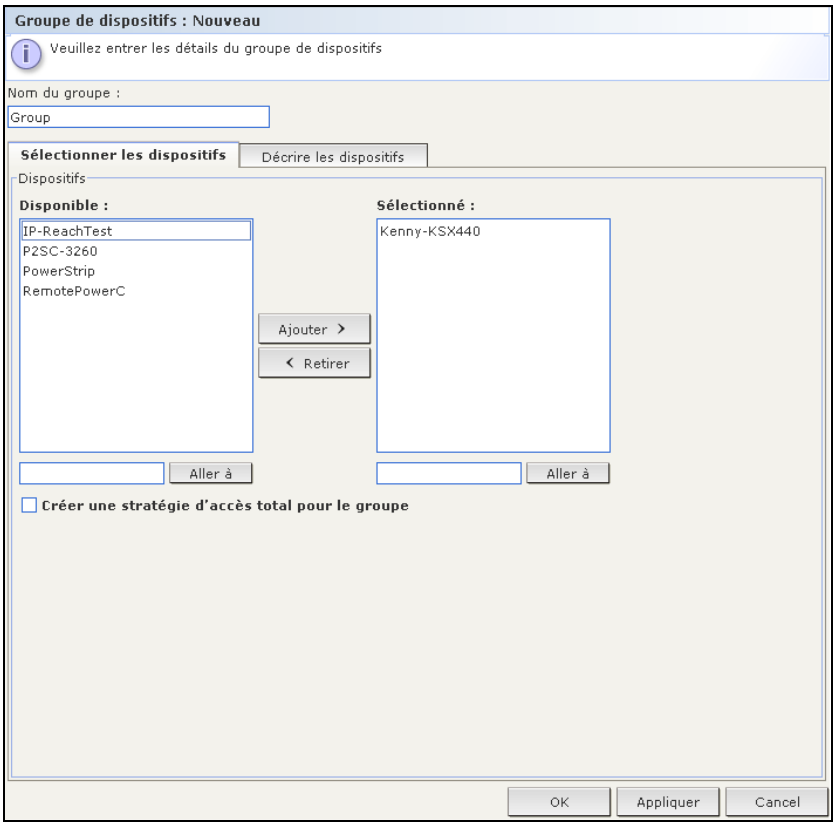

Figure 14 Paramétrage guidé – Ajouter des groupes de dispositifs, Sélectionner les dispositifs

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

- Pour supprimer un dispositif du groupe, sélectionnez son nom dans la liste **Sélectionné**, puis cliquez sur **Retirer**.
- Vous pouvez rechercher un dispositif dans la liste **Disponible** ou dans la liste **Sélectionné**. Entrez les termes de la recherche dans le champ sous la liste, puis cliquez sur **Aller à**.

Décrire les dispositifs

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

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

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

d. 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.

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

f. Une fois l'ajout des groupes de dispositifs terminé, cliquez sur **OK**. Le panneau **Groupes de nœuds : Nouveau** s'ouvre. Vous pouvez également cliquer sur **Créer des groupes**, puis sur **Ajouter des groupes de nœuds** dans l'arborescence **Tâches guidées** du panneau gauche pour ouvrir le panneau **Groupes de nœuds : Nouveau**.

g. Dans le champ **Nom du groupe**, entrez le nom du groupe de nœuds à créer.

h. Vous pouvez ajouter des nœuds à un groupe de deux façons : **Sélectionner les nœuds** et **Décrire les nœuds**. L'onglet **Sélectionner les nœuds** vous permet de choisir dans la liste des nœuds disponibles ceux que vous souhaitez affecter au groupe. L'onglet **Décrire les nœuds** vous permet de spécifier des règles décrivant les nœuds ; les nœuds dont les paramètres respectent ces règles seront ajoutés au groupe.

Sélectionner les nœuds

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

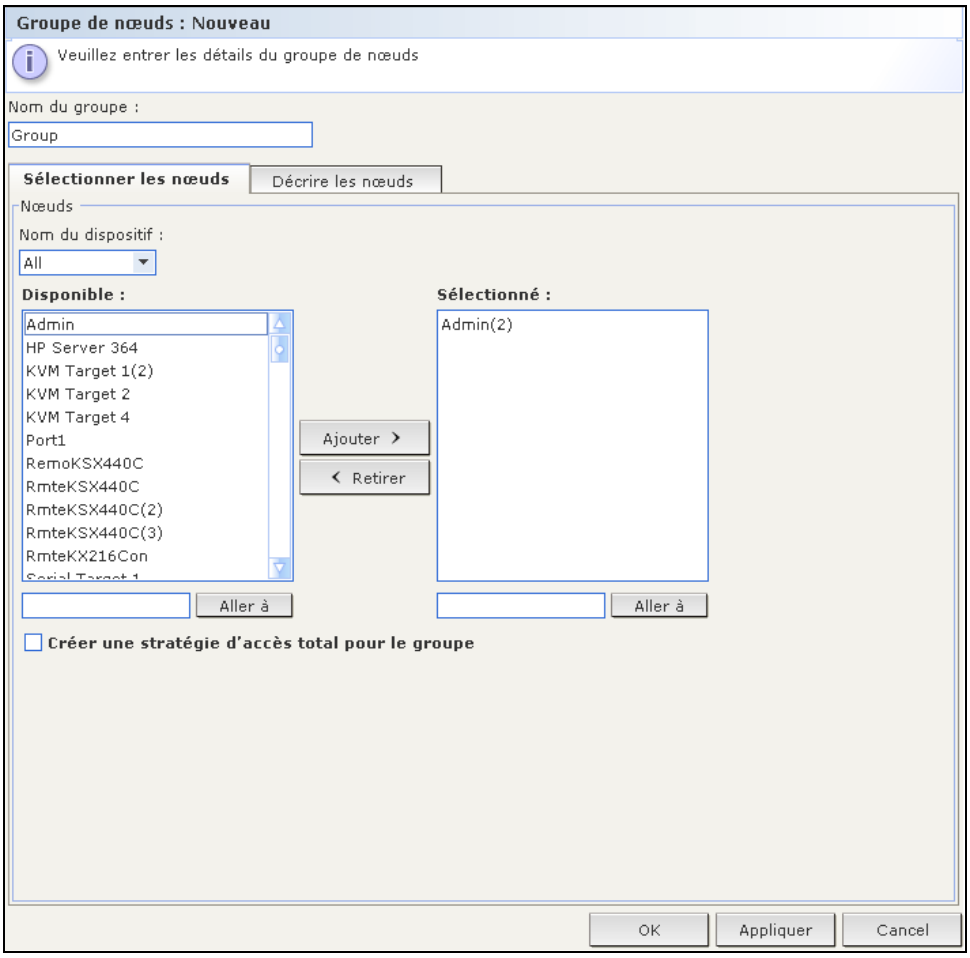

Figure 15 Paramétrage guidé – Ajouter des groupes de nœuds, Sélectionner les nœuds

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

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

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

Décrire les nœuds

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

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

c. Double-cliquez sur la cellule créée pour chaque colonne afin d'activer un menu déroulant. Dans chaque liste, sélectionnez les composants de règle à utiliser. Reportez-vous au **Chapitre 8 : Stratégies** pour plus d'informations.

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

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

f. 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.

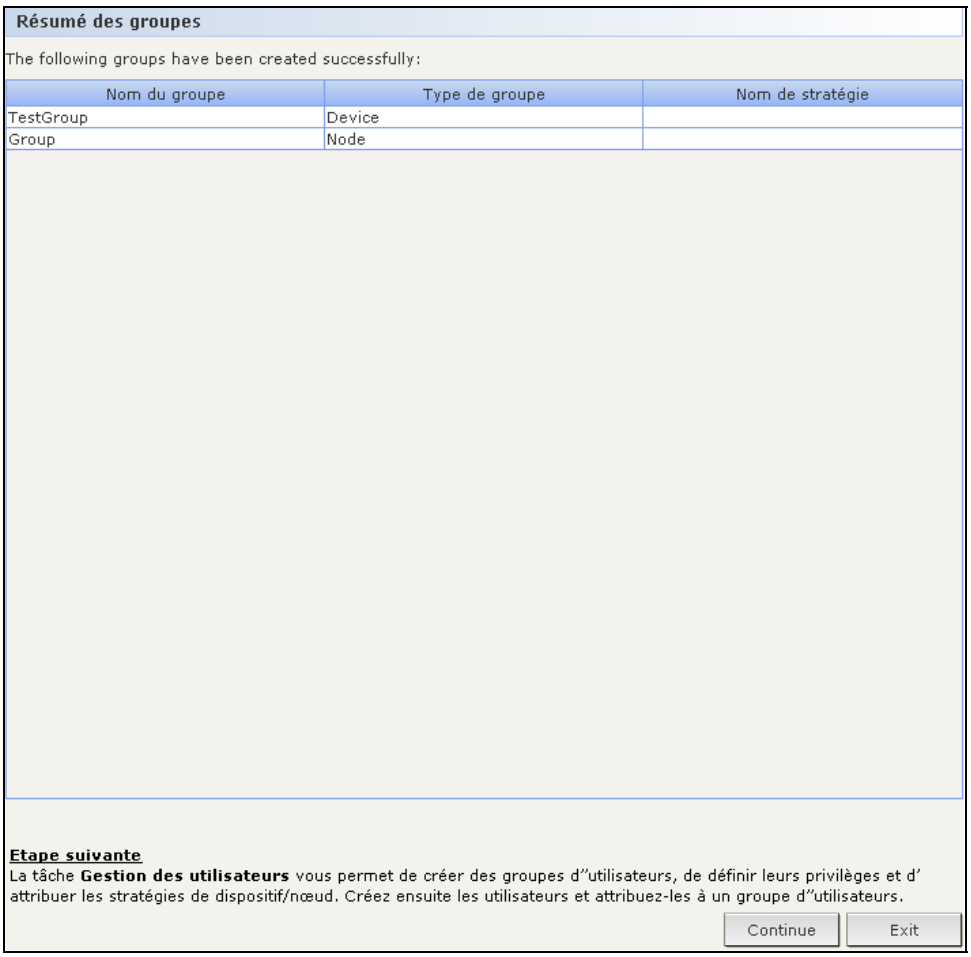

Figure 16 Paramétrage guidé – Résumé des groupes

g. Cliquez sur **Continue** (continuer) pour démarrer la tâche suivante, **Gestion des utilisateurs**. Suivez les étapes de la section suivante.

Gestion des utilisateurs

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

Ajouter des groupes d'utilisateurs et des utilisateurs

1. Le panneau **Ajouter un groupe d'utilisateurs** s'ouvre lorsque vous cliquez sur **Continue** (continuer) à la fin de la tâche Créer des groupes. Vous pouvez également cliquer sur **Gestion des utilisateurs**, puis, dans l'arborescence **Tâches guidées** du panneau gauche, sur **Ajouter un groupe d'utilisateurs** pour ouvrir le panneau du même nom.
2. Dans le champ **Nom du groupe d'utilisateurs**, entrez le nom du groupe à créer.
3. Dans le champ **Description**, entrez la description du groupe d'utilisateurs.
4. 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.

5. 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.

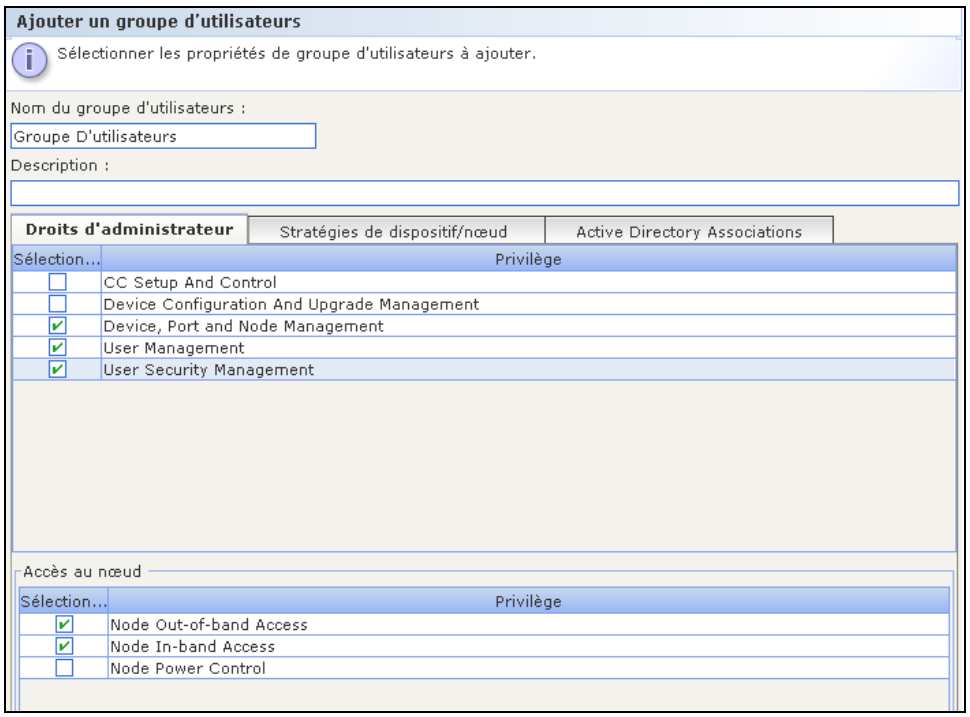

Figure 17 Ecran Ajouter un groupe d'utilisateurs – Droits d'administrateur

6. Cliquez sur l'onglet **Stratégies**.

7. 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.

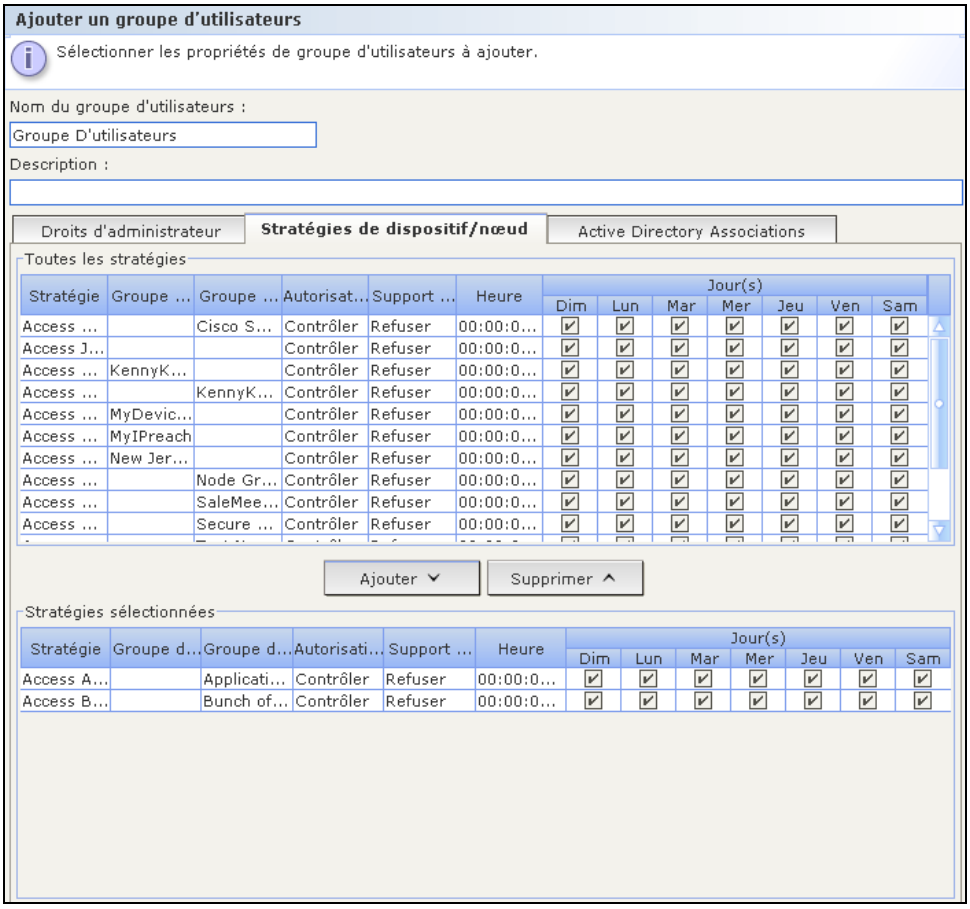

Figure 18 Ecran Ajouter un groupe d'utilisateurs – Stratégies

8. Pour supprimer une stratégie du groupe d'utilisateurs, sélectionnez son nom dans la liste **Stratégies sélectionnées**, puis cliquez sur **Supprimer**.
9. Pour associer des utilisateurs authentifiés à distance à des modules Active Directory, cliquez sur l'onglet **Active Directory Associations** (associations Active Directory). Cochez la case correspondant à chaque module Active Directory à associer au groupe d'utilisateurs.
10. Si vous souhaitez ajouter un autre groupe d'utilisateurs, cliquez sur **Appliquer** pour enregistrer le groupe en cours, puis répétez les étapes de cette section pour ajouter des groupes d'utilisateurs supplémentaires.
11. 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 gauche, sur **Ajouter un utilisateur** pour ouvrir le panneau du même nom.
12. Dans le champ **Nom d'utilisateur**, entrez le nom dont l'utilisateur à ajouter se servira pour se connecter à CC-SG.
13. Cochez la case **Connexion activée** pour autoriser l'utilisateur à se connecter à CC-SG.
14. 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.

15. 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.
16. 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.
17. 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.
18. 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.
19. Entrez l'**adresse électronique** de l'utilisateur dans le champ correspondant.
20. Cliquez sur la flèche déroulante **Groupe(s) d'utilisateurs** et sélectionnez dans la liste le groupe d'utilisateurs auquel vous souhaitez affecter l'utilisateur.
21. 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.
22. Une fois l'ajout des utilisateurs terminé, cliquez sur **OK**. Le panneau **Résumé du groupe d'utilisateurs** affiche la liste des groupes d'utilisateurs que vous avez ajoutés.

Chapitre 4 : Création d'associations

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 les sous-ensembles de la Catégorie. Imaginons par exemple que vos dispositifs Raritan servent à gérer des serveurs cible dans des centres de données situés à New York, Philadelphie et La Nouvelle Orléans. 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 : New York, Philadelphie et La Nouvelle Orléans, dans l'interface CC-SG. La figure ci-dessous présente une vue personnalisée créée à l'aide de cet exemple. Vous pouvez personnaliser CC-SG afin d'organiser et d'afficher les serveurs comme vous le souhaitez.

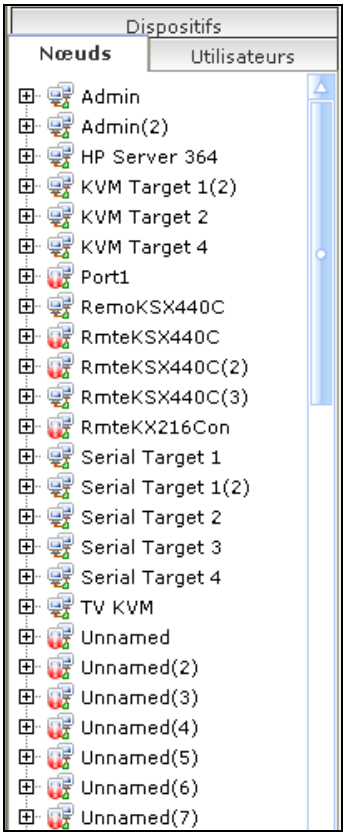

Figure 19 Exemple d'association dans CC-SG

Terminologie relative aux associations

Pour comprendre le concept des associations, prenez connaissance des définitions suivantes :

- **Associations** – désigne les relations entre les catégories, les éléments d'une catégorie, et les nœuds et dispositifs. Imaginons que vous souhaitiez associer la catégorie Emplacement à un dispositif. Dans ce cas, vous devez d'abord créer les associations, ou les modifier ultérieurement, avant d'ajouter les dispositifs et les ports dans CC-SG.
- **Catégorie** – variable contenant un jeu de valeurs appelées Eléments. Un exemple de catégorie est Emplacement, qui peut contenir comme éléments New York et Philadelphie. Type de SE est un autre exemple de catégorie, qui peut contenir des éléments tels que Windows, Unix ou Linux. Lorsque vous ajoutez des dispositifs à CC-SG, vous leur associez ces informations.
- **Eléments** – désigne les valeurs d'une catégorie. Par exemple, l'élément New York appartient à la catégorie Emplacement.

- **Dispositifs** – désigne des produits Raritan, tels que Dominion KX, Dominion SX, Dominion KSX, IP-Reach, Paragon II System Controller, Paragon II UMT832 avec USTIP, etc., gérés par CC-SG. Ces dispositifs contrôlent les systèmes cible, ou nœuds, auxquels ils sont connectés.
- **Nœuds** – désigne les systèmes ou serveurs cible accessibles et gérés par CC-SG. Dans CC-SG, cliquez sur un nœud pour y accéder et le gérer via des interfaces.

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, à un nœud ou aux deux. 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 semblables. Par exemple, pour regrouper vos dispositifs Raritan par emplacement, vous pouvez définir une catégorie Emplacement, contenant un ensemble d'éléments, tels que New York, Philadelphie et La Nouvelle Orléans.

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

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

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

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

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

CATÉGORIE	ELÉMENT
usergroup1	usergroup1node
usergroup2	usergroup2node
usergroup3	usergroup3node

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

Comment créer des associations

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

- Le **paramétrage guidé** combine plusieurs tâches de configuration dans une interface automatisée. Cette méthode est recommandée pour la configuration initiale de CC-SG. Une fois le paramétrage guidé effectué, vous avez toujours la possibilité de modifier vos configurations individuellement. Reportez-vous à Chapitre 3 : Configuration de CC-SG par paramétrage guidé pour plus d'informations.
- Le **Gestionnaire des associations** vous permet de travailler sur les associations uniquement et n'automatise aucune tâche de configuration. Reportez-vous à la section **Gestionnaire des associations** dans les pages suivantes pour plus d'informations.

Gestionnaire des associations

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

Ajouter une catégorie

1. Dans le menu Associations, cliquez sur Association. L'écran Gestionnaire des associations s'affiche.

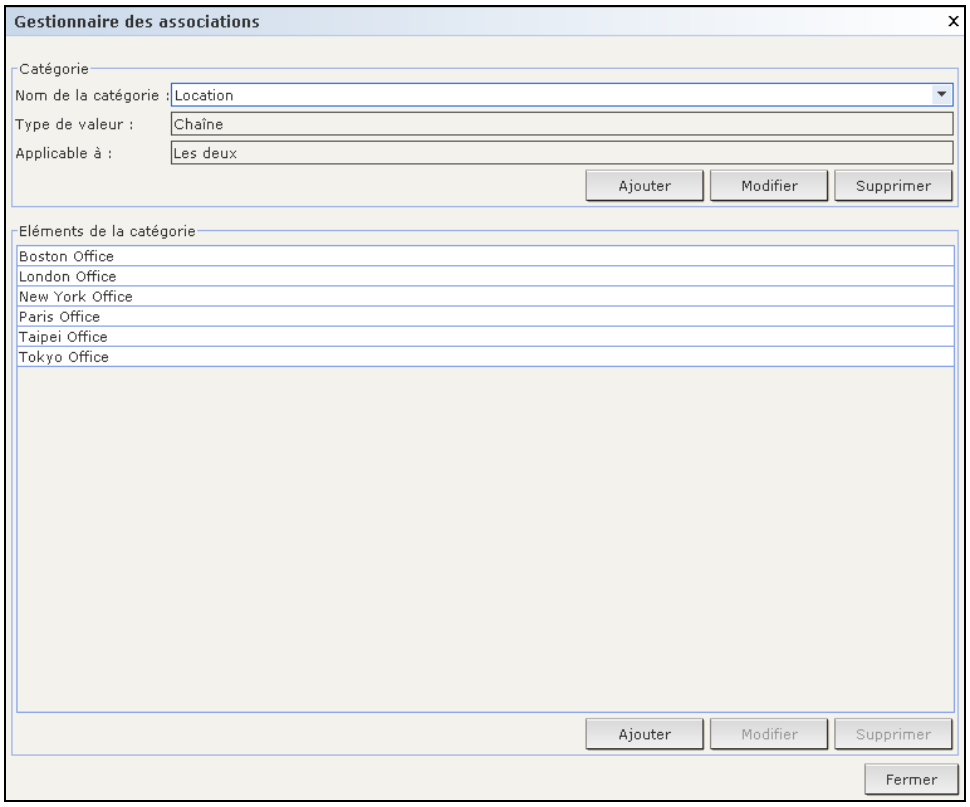

Figure 20 Ecran Gestionnaire des associations

2. Cliquez sur **Ajouter** dans le panneau **Catégorie** pour ajouter une nouvelle catégorie. La fenêtre **Ajouter une catégorie** s'affiche.

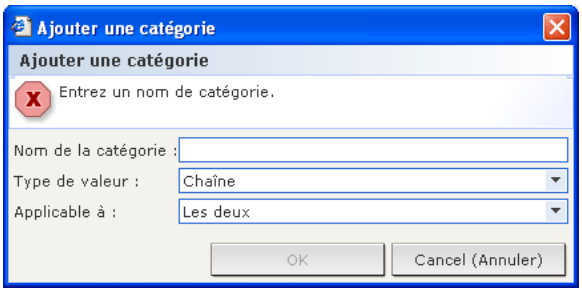

Figure 21 Fenêtre Ajouter une catégorie

3. Entrez un nom pour la catégorie dans le champ **Nom de la catégorie**. Le nom ne doit pas dépasser 31 caractères.
4. Cliquez sur la flèche déroulante **Type de valeur** et sélectionnez **Chaîne** ou **Nombre entier**.
5. Cliquez sur la flèche déroulante **Applicable à** et sélectionnez le type de dispositif auquel s'applique cette catégorie : **Dispositif**, **Nœud** ou **Les deux**.
6. Cliquez sur **OK** pour créer la catégorie ou sur **Cancel** (Annuler) pour quitter l'application sans procéder à la création. Le nom de la nouvelle catégorie s'affiche dans le champ **Nom de la catégorie**.

Modifier une catégorie

1. Dans le menu Associations, cliquez sur Association. L'écran Gestionnaire des associations s'affiche.
2. Cliquez sur la flèche déroulante **Nom de la catégorie** et sélectionnez la catégorie à modifier.
3. Cliquez sur **Modifier** dans le panneau **Catégorie** de l'écran pour modifier la catégorie. La fenêtre **Modifier une catégorie** s'affiche.

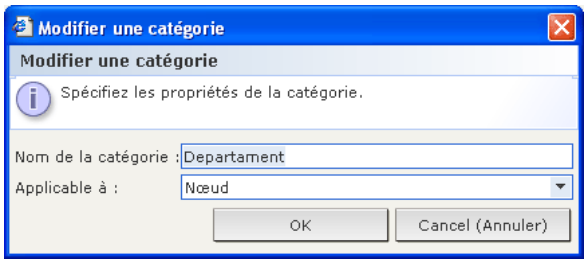

Figure 22 Fenêtre Modifier une catégorie

4. Entrez le nouveau nom de la 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**. Notez que la valeur Chaîne ne peut pas être remplacée par Nombre entier et inversement. Si vous devez effectuer ce type de modification, supprimez la catégorie et ajoutez-en une nouvelle.
6. Cliquez sur **OK** pour enregistrer les modifications. Le nom de la catégorie mise à jour s'affiche dans le champ **Nom de la catégorie**.

Supprimer une catégorie

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

1. Dans le menu Associations, cliquez sur Association. L'écran Gestionnaire des associations s'affiche.
2. Cliquez sur la flèche déroulante **Nom de la catégorie** et sélectionnez la catégorie à supprimer.
3. Cliquez sur **Supprimer** dans le panneau **Catégorie** de l'écran pour supprimer la catégorie. La fenêtre **Supprimer une catégorie** s'affiche.

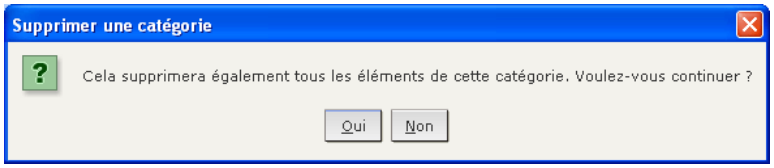

Figure 23 Fenêtre Supprimer une catégorie

4. Cliquez sur **Oui** pour supprimer la catégorie.

Ajouter un élément

1. Dans le menu Associations, cliquez sur Association. L'écran Gestionnaire des associations s'affiche.

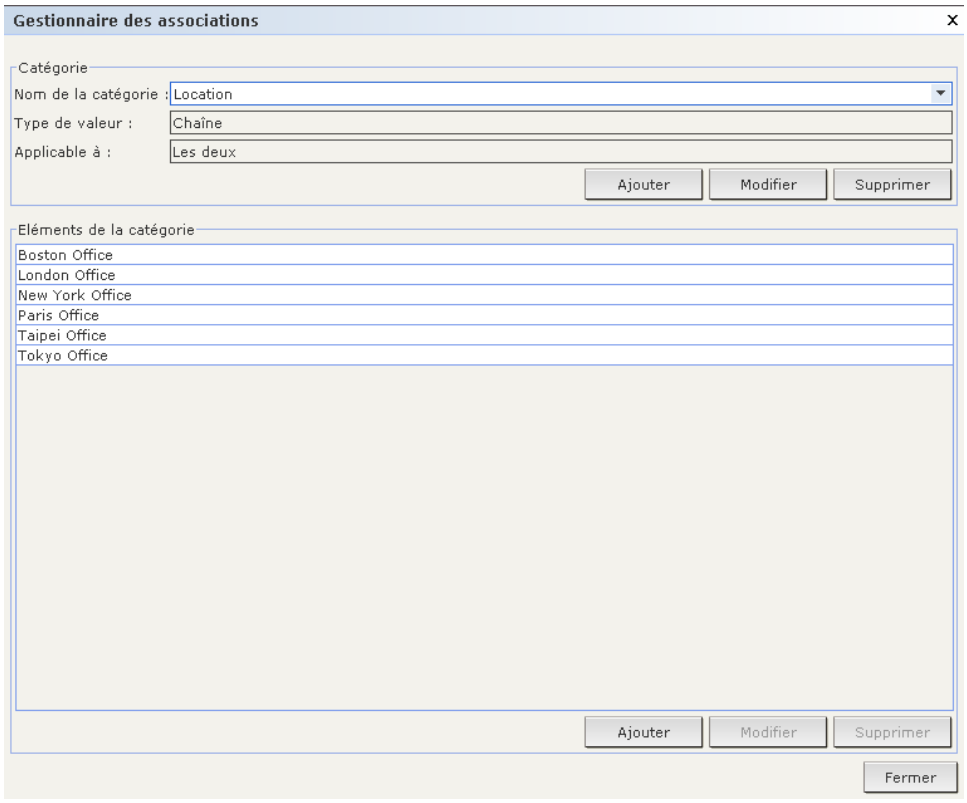

Figure 24 Ecran Gestionnaire des associations

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 **Ajouter** dans le panneau **Eléments de la catégorie** pour ajouter un nouvel élément. La fenêtre **Ajouter un élément** s'affiche.

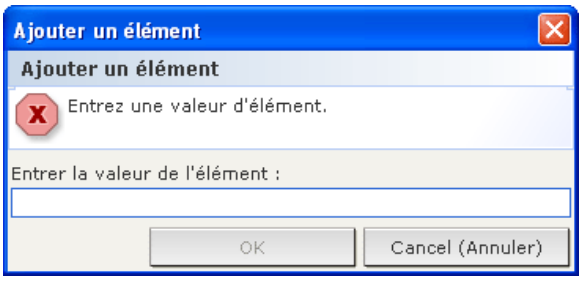

Figure 25 Fenêtre Ajouter un élément

4. Tapez le nom du nouvel élément dans le champ **Entrer la valeur de l'élément**.
5. Cliquez sur **OK** pour ajouter l'élément ou sur **Cancel** (Annuler) pour fermer la fenêtre. Le nouvel élément s'affiche dans le panneau **Eléments de la catégorie**.

Modifier un élément

1. Dans le menu **Associations**, cliquez sur **Association**. L'écran **Gestionnaire des associations** s'affiche.
2. Cliquez sur la flèche déroulante **Nom de la catégorie** et sélectionnez la catégorie dont vous souhaiter modifier un élément.
3. Sélectionnez l'élément à modifier dans la liste **Eléments de la catégorie** et cliquez sur **Modifier** dans le panneau **Eléments de la catégorie**. La fenêtre **Modifier un élément** s'affiche.

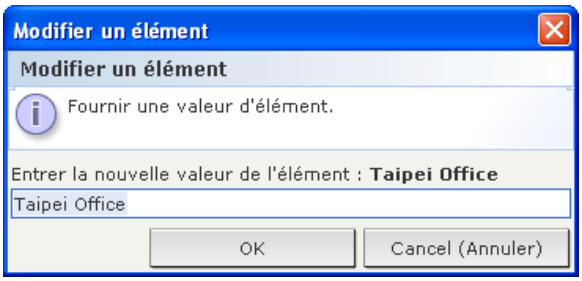

Figure 26 Fenêtre Modifier un élément

4. Tapez le nouveau nom de l'élément dans le champ **Entrer la nouvelle valeur de l'élément**.
5. Cliquez sur **OK** pour actualiser l'élément ou sur **Cancel** (Annuler) pour fermer la fenêtre. Le nouveau nom de l'élément s'affiche dans la liste **Elément de catégorie**.

Supprimer un élément

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

1. Dans le menu **Associations**, cliquez sur **Association**. L'écran **Gestionnaire des associations** s'affiche.
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 de la catégorie** et cliquez sur **Supprimer** dans le panneau **Eléments de la catégorie**. La fenêtre **Supprimer un élément** s'affiche.

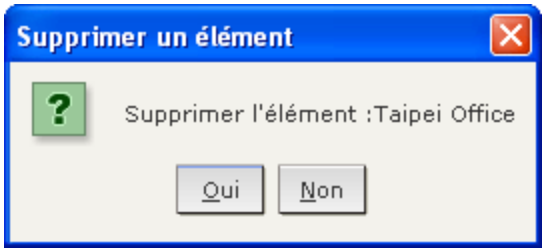

Figure 27 Fenêtre Supprimer un élément

4. Cliquez sur **Oui** pour supprimer l'élément ou sur **Non** pour fermer la fenêtre. Le nom de l'élément est retiré de la liste **Eléments de la catégorie**.

***Remarque** : la suppression d'un élément le retire de toutes les associations de catégorie de dispositifs et de nœuds. Les champs des éléments pré-associés sont alors vides.*

Cette page est laissée intentionnellement blanche.

Chapitre 5 : Ajout de dispositifs et de groupes de dispositifs

Vous devez ajouter les dispositifs Raritan, tels que les dispositifs de la série Dominion et les unités IP-Reach, à CC-SG avant d'utiliser ce dernier pour les configurer et les gérer. Le menu Dispositifs offre toutes les fonctions relatives aux dispositifs et aux ports. Vous pouvez également accéder à certaines fonctions en cliquant avec le bouton droit sur un dispositif ou un port sous l'onglet Dispositifs, puis en effectuant une sélection dans le menu qui apparaît.

***Remarque** : Pour configurer des dispositifs iLO/RILOE, IPMI, Dell DRAC, IBM RSA ou d'autres dispositifs « génériques », utilisez l'option de menu **Ajouter un nœud** et ajoutez ces éléments comme interface de connexion. Reportez-vous au **Chapitre 6 : Configuration des nœuds et des interfaces** pour plus d'informations.*

Onglet Dispositifs

Cliquez sur l'onglet **Dispositifs** pour afficher l'arborescence correspondante.

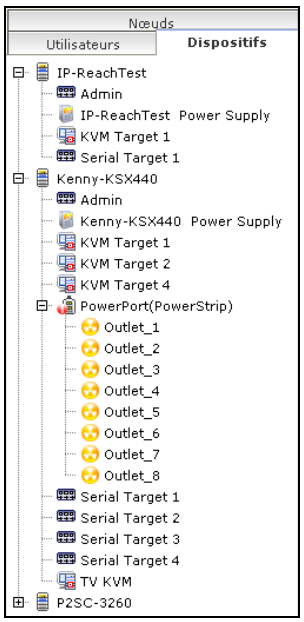

Figure 28 Arborescence Dispositifs

L'onglet Dispositifs affiche un ensemble de dispositifs et leurs ports configurés. Les ports sont imbriqués sous les dispositifs auxquels ils appartiennent. Dans la liste, le symbole + apparaît en regard des dispositifs dotés de ports configurés. Cliquez sur le symbole + pour développer ou masquer la liste des ports.

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
	Dispositif suspendu
	Dispositif non disponible
	Barrette d'alimentation
	Port de prise

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

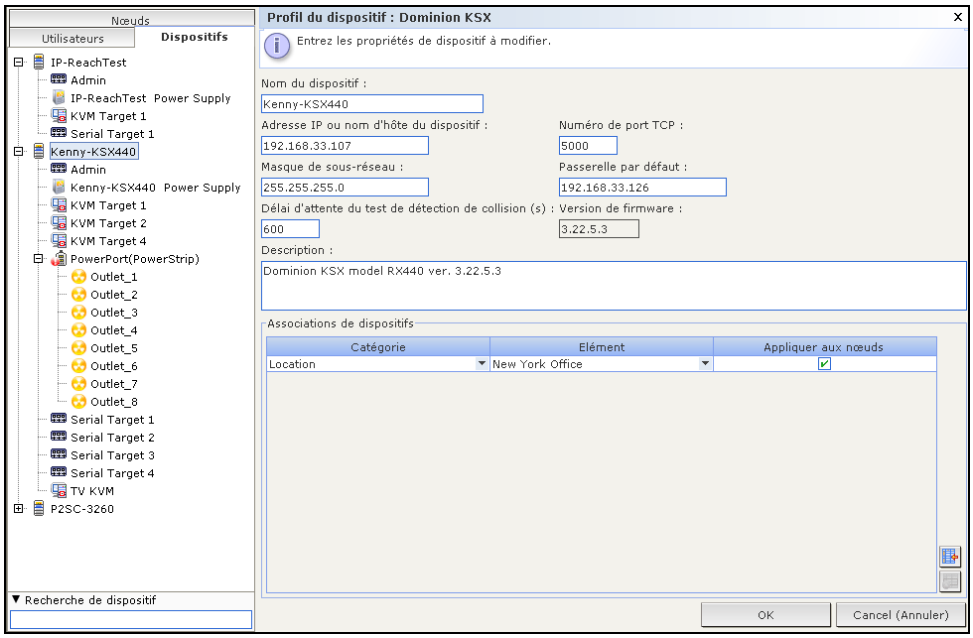

Figure 29 Onglet Dispositifs et écran Profil du dispositif

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 via l'écran **Mon profil** décrit plus tard dans le **Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs**.

Pour rechercher un dispositif, au bas de l'arborescence Dispositifs, entrez une chaîne dans le champ **Recherche de dispositif**, et appuyez sur **ENTREE**. Les caractères joker sont pris en charge dans la chaîne de recherche :

CARACTÈRE JOKER	DESCRIPTION
?	Indique un caractère quelconque.
[-]	Indique un caractère dans une plage.
*	Indique zéro caractère ou plus.

Par exemple :

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**.

Important : un grand nombre de commandes de la barre de menus sont accessibles en cliquant avec le bouton droit de la souris sur un dispositif ou un port dans l'arborescence Dispositifs, puis en sélectionnant une commande dans le menu de raccourcis qui s'affiche.

Ajout d'un dispositif

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

Pour ajouter un dispositif à CC-SG :

1. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, puis sur **Ajouter un dispositif**. L'écran **Ajouter un dispositif** s'affiche.

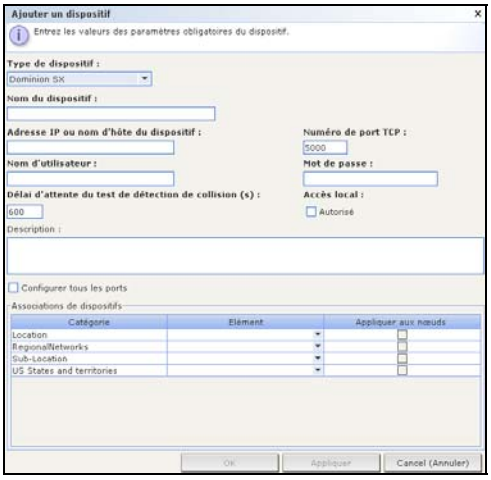

Figure 30 Ecran Ajouter un dispositif

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

Ajouter un dispositif KVM ou série

3. Renseignez le champ **Nom du dispositif**.
4. Renseignez le champ **Adresse IP ou nom d'hôte du dispositif**. Pour connaître les règles des noms d'hôte, reportez-vous à **Terminology/Acronyms** dans le **Chapitre 1 : Introduction**.
5. Entrez le port de communication TCP utilisé pour communiquer avec le dispositif dans le champ **Numéro de port TCP**. Le numéro de port par défaut de la plupart des dispositifs Raritan est 5000.
6. Entrez le nom utilisé pour vous connecter à ce dispositif dans le champ **Nom d'utilisateur**. Si vous avez suivi le **Guide de déploiement des solutions numériques Raritan** pour préparer les dispositifs à ajouter à CC-SG, entrez le nom d'utilisateur de l'administrateur CC-SG configuré sur le dispositif.
7. Entrez le mot de passe permettant d'accéder à ce dispositif dans le champ **Mot de passe**. Si vous avez suivi le **Guide de déploiement des solutions numériques Raritan** pour préparer les dispositifs à ajouter à CC-SG, entrez le mot de passe de l'utilisateur administrateur CC-SG configuré sur le dispositif.
8. 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)**.
9. Le cas échéant, cochez la case **Autorisé** sous **Accès local** pour accorder aux utilisateurs l'accès direct à ce dispositif pendant qu'il est géré par CC-SG.
10. Si vous le souhaitez, entrez une brève description de ce dispositif dans le champ **Description**.
11. 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. Si cette case est cochée à l'ajout du dispositif, un nœud est créé pour chaque port, et une interface hors bande est créée pour ce nœud.

12. 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 au **Chapitre 4 : Création d'associations** pour plus d'informations.

    Pour configurer les **catégories** et les **éléments** :

    a. Pour chaque **catégorie** répertoriée, cliquez sur le menu déroulant **Elément**, puis sélectionnez dans la liste l'élément à appliquer au dispositif. Sélectionnez l'élément vide dans le champ **Elément** pour chaque catégorie que vous ne souhaitez pas utiliser.
    b. Pour affecter l'élément aux nœuds associés, ainsi qu'au dispositif, cochez la case **Appliquer aux nœuds**.

    Si les valeurs **Catégorie** ou **Elément** que vous souhaitez utiliser n'apparaissent pas, vous pouvez en ajouter via le menu **Associations**. Reportez-vous au **Chapitre 4 : Création d'associations** pour plus d'informations.
13. Lorsque la configuration du dispositif est terminée, cliquez sur **Appliquer** pour l'ajouter et ouvrir un nouvel écran **Ajouter un dispositif** vide afin de poursuivre l'ajout des dispositifs. Ou, cliquez sur **OK** pour ajouter le dispositif sans afficher un nouvel écran **Ajouter un dispositif**.
14. Si la version du firmware du dispositif n'est pas compatible avec CC-SG, un message vous en avertit et vous demande si vous souhaitez continuer. 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 **Mettre le dispositif à niveau** plus loin dans ce chapitre.

Ajouter un dispositif PowerStrip

Lorsque vous ajoutez un dispositif PowerStrip, vous pouvez autoriser CC-SG à configurer automatiquement ses prises. Une fois les prises configurées, vous pouvez associer chacune au nœud qu'elle alimente par l'ajout d'une interface d'alimentation au nœud. Reportez-vous au **Chapitre 6 : Configuration des nœuds et des interfaces** pour plus d'informations. Vous pouvez également ne pas autoriser CC-SG à configurer les prises et effectuer l'opération vous-même ultérieurement.

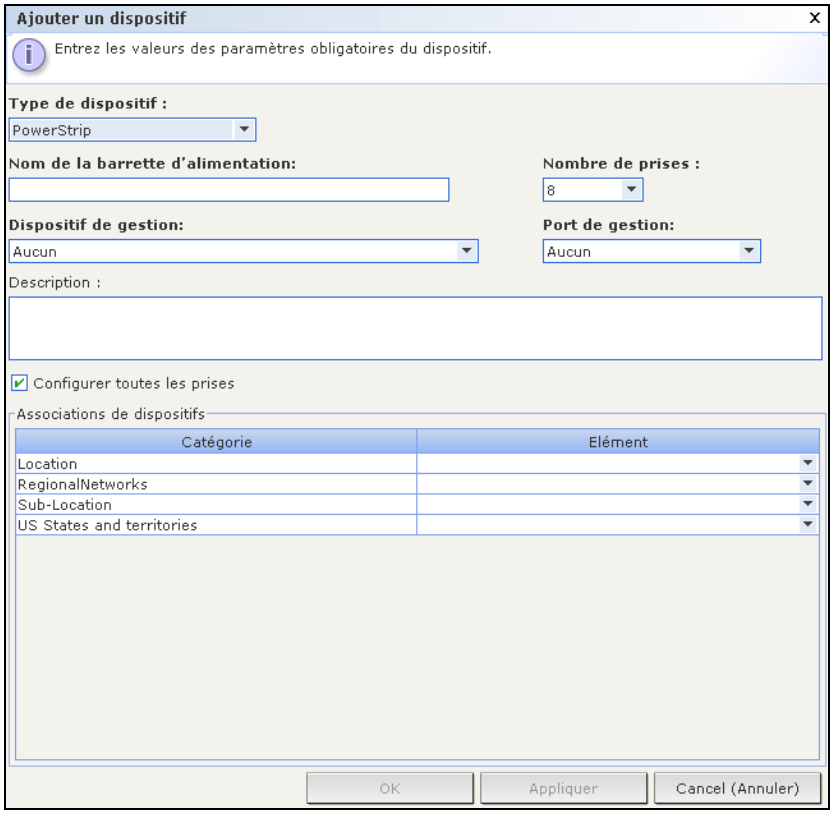

Figure 31 Ajouter un dispositif PowerStrip

3. Renseignez le champ Nom de la barrette d'alimentation.
4. Cliquez sur le menu déroulant **Nombre de prises**, puis sélectionnez le nombre de prises dont est dotée la barrette d'alimentation.

5. Cliquez sur le menu déroulant **Dispositif de gestion**, puis sélectionnez dans la liste le dispositif que vous utiliserez pour gérer la barrette d'alimentation.
6. Cliquez sur le menu déroulant **Port de gestion**, puis sélectionnez dans la liste le port du dispositif de gestion auquel la barrette d'alimentation est connectée.
7. Si vous le souhaitez, entrez une brève description de la barrette d'alimentation dans le champ **Description**.
8. Cochez la case **Configurer toutes les prises** pour ajouter automatiquement chaque prise du dispositif à l'onglet **Dispositifs**.
9. Une liste de catégories et d'éléments peut être configurée pour décrire et organiser de façon optimale la barrette d'alimentation concernée et les nœuds qui lui sont connectés. Reportez-vous au **Chapitre 4 : Création d'associations** pour plus d'informations.
    - Pour chaque **catégorie** répertoriée, cliquez sur le menu déroulant **Elément**, puis sélectionnez dans la liste l'élément à appliquer au dispositif. Sélectionnez l'élément vide dans le champ **Elément** pour chaque catégorie que vous ne souhaitez pas utiliser.

    Si les valeurs **Catégorie** ou **Elément** que vous souhaitez utiliser n'apparaissent pas, vous pouvez en ajouter via le menu **Associations**. Reportez-vous au **Chapitre 4 : Création d'associations** pour plus d'informations.
10. Lorsque la configuration du dispositif est terminée, cliquez sur **Appliquer** pour l'ajouter et ouvrir un nouvel écran **Ajouter un dispositif** vide afin de poursuivre l'ajout des dispositifs. Ou, cliquez sur **OK** pour ajouter la barrette d'alimentation sans afficher un nouvel écran **Ajouter un dispositif**.

Détection des dispositifs

La commande Détecter les dispositifs déclenche la recherche de tous les dispositifs de votre réseau. La recherche détecte automatiquement tous les dispositifs Raritan, récemment ajoutés ou déjà présents sur votre réseau, tels que des unités Paragon II System Controller, IP-Reach, Dominion KX, Dominion KX101, Dominion KSX, Dominion SX et des unités eRIC. Une fois les dispositifs détectés, vous pouvez les ajouter à CC-SG s'ils ne sont pas encore gérés.

1. Dans le menu **Dispositifs**, cliquez sur Détecter les dispositifs. L'écran **Détecter** les dispositifs s'affiche.

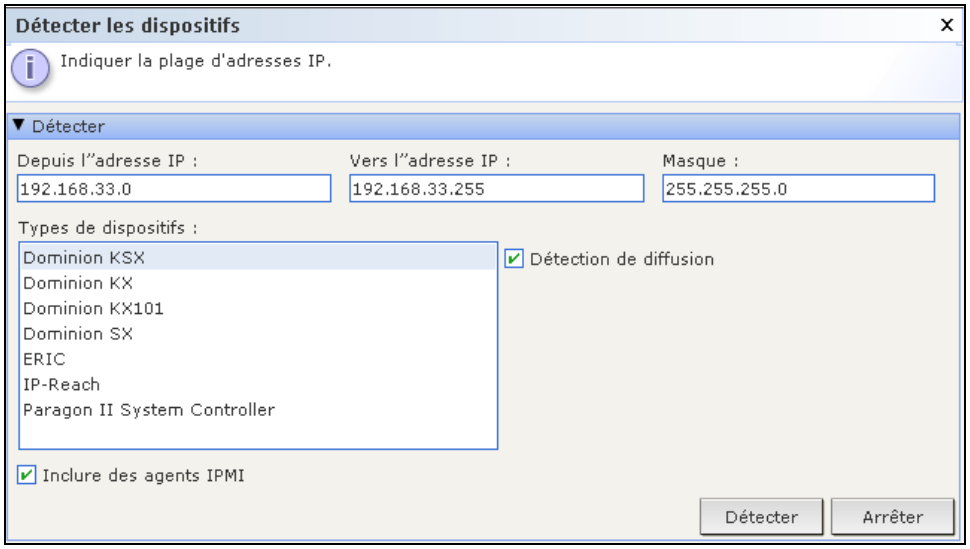

Figure 32 Ecran Détecter les dispositifs

2. Dans les champs **Depuis l'adresse IP** et **Vers l'adresse IP**, entrez la plage d'adresses IP où vous pensez trouver les dispositifs. La valeur entrée dans le champ **Vers l'adresse IP** doit être supérieure à celle du champ **Depuis l'adresse IP**. Indiquez le masque à appliquer à la plage. Si aucun masque n'est spécifié, l'adresse de diffusion **255.255.255.255** est envoyée ; elle émet sur l'ensemble des réseaux locaux. Pour détecter des dispositifs sur des sous-réseaux, un masque doit obligatoirement être spécifié.

3. Cochez la case **Détection de diffusion** pour rechercher des dispositifs sur le sous-réseau où réside CC-SG. Pour détecter des dispositifs sur différents sous-réseaux, désactivez la case **Détection de diffusion**.
4. Pour rechercher un type de dispositif particulier, sélectionnez-le dans la liste **Types de dispositifs**. Par défaut, tous les types de dispositifs sont sélectionnés. Pour sélectionner plusieurs types de dispositifs, cliquez dessus tout en appuyant sur la touche **Ctrl**.
5. Cochez la case **Inclure des agents IPMI** pour détecter des cibles offrant la gestion de l'alimentation IPMI.
6. Cliquez sur **Détecter** pour démarrer la recherche. A tout moment de l'opération, vous pouvez cliquer sur **Arrêter** pour interrompre le processus de détection. Les dispositifs détectés apparaissent dans une liste.

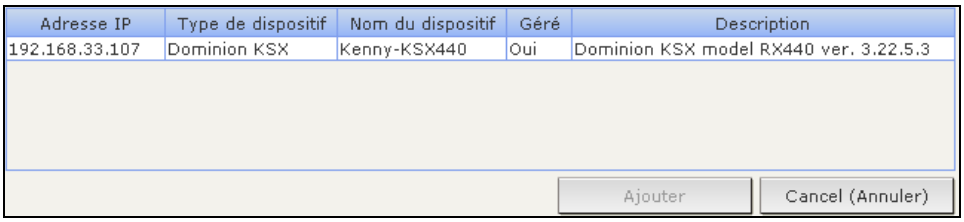

Figure 33 Fenêtre de la liste des dispositifs détectés

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.

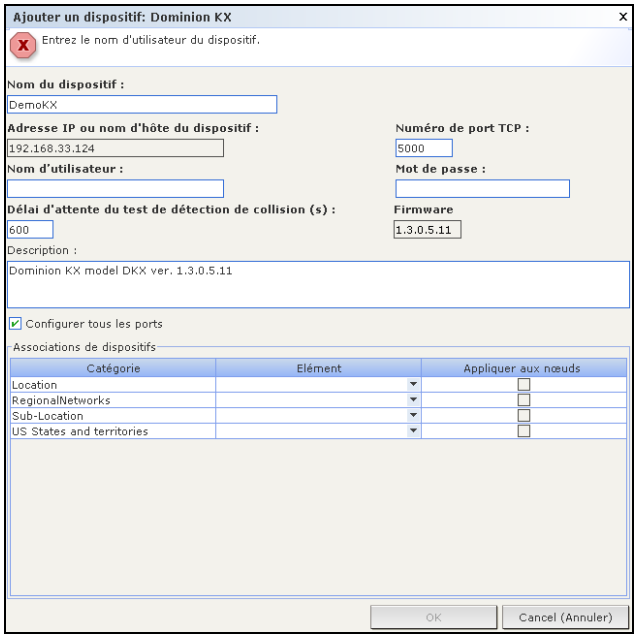

Figure 34 Ajouter un dispositif détecté

8. Entrez le **nom d'utilisateur** et le **mot de passe** (qui ont été créés spécifiquement pour CC-SG dans le dispositif) dans les champs correspondants afin de permettre à CC-SG d'authentifier le dispositif lors d'une communication future. Sélectionnez les **catégories** et **éléments** à appliquer au dispositif. Pour appliquer une catégorie et un élément aux nœuds connectés au dispositif, cochez la case **Appliquer aux nœuds** correspondante.
9. Si vous le souhaitez, vous pouvez modifier les champs **Nom du dispositif**, **Délai d'attente du test de détection de collision (s)**, **Accès local** (si disponible pour le type de dispositif), **Description**, **Configurer tous les ports** et **Associations de dispositifs** en fonction de vos besoins.

10. Lorsque la configuration du dispositif est terminée, cliquez sur **Appliquer** pour ajouter celui-ci et ouvrir l'écran **Ajouter un dispositif** correspondant à l'élément détecté suivant. Ou, cliquez sur **OK** pour ajouter le dispositif sans passer aux autres dispositifs détectés.
11. Si la version du firmware d'un dispositif n'est pas compatible avec CC-SG, un message vous en avertit et vous demande si vous souhaitez continuer. Cliquez sur **Oui** pour ajouter le dispositif à CC-SG ou sur **Non** pour annuler l'opération. Vous pouvez mettre à niveau le firmware du dispositif après avoir ajouté ce dernier à CC-SG. Pour plus d'informations, reportez-vous à **Mettre le dispositif à niveau** plus loin dans ce chapitre.

Modification d'un dispositif

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

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif à modifier. L'écran **Profil du dispositif** apparaît.

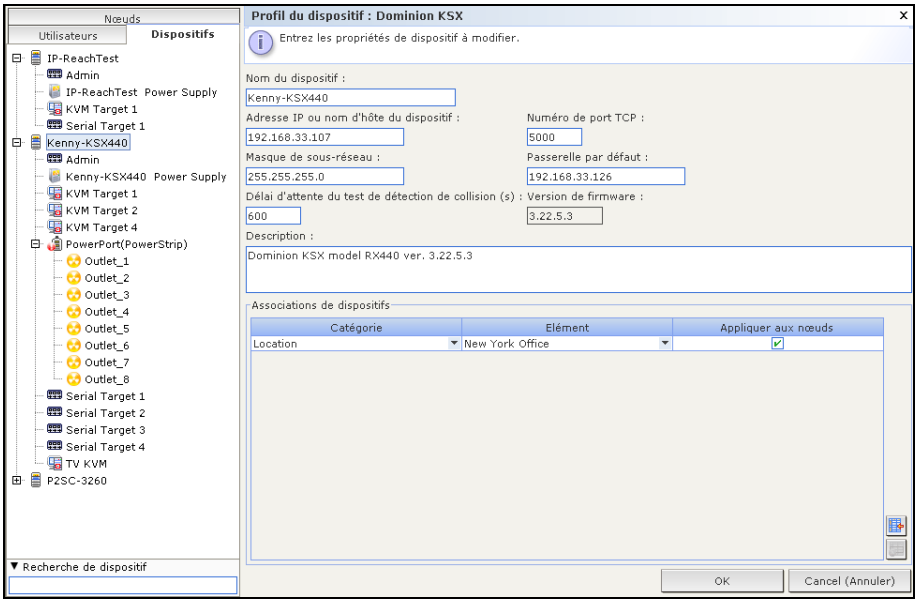

Figure 35 Ecran Profil du dispositif

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 **OK** pour enregistrer les modifications. Le message **Le dispositif a été mis à jour** confirme la modification du dispositif.

Modifier un dispositif PowerStrip

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

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

Suppression d'un dispositif

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

Important : la suppression d'un dispositif entraîne la suppression 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.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif à supprimer.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, puis sur **Supprimer un dispositif**. L'écran **Supprimer un dispositif** s'affiche.

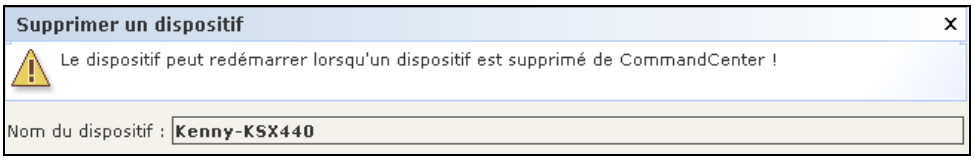

Figure 36 Ecran Supprimer un dispositif

3. Cliquez sur **OK** pour supprimer le dispositif ou sur **Cancel** (Annuler) pour quitter sans rien supprimer. Le message **Le dispositif a été supprimé** confirme que le dispositif a bien été supprimé.

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

Configuration des ports

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

Configurer un port série

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez un dispositif série dans l'arborescence Dispositifs.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des ports**, puis sur **Configurer les ports**. L'écran Configurer les ports s'affiche.

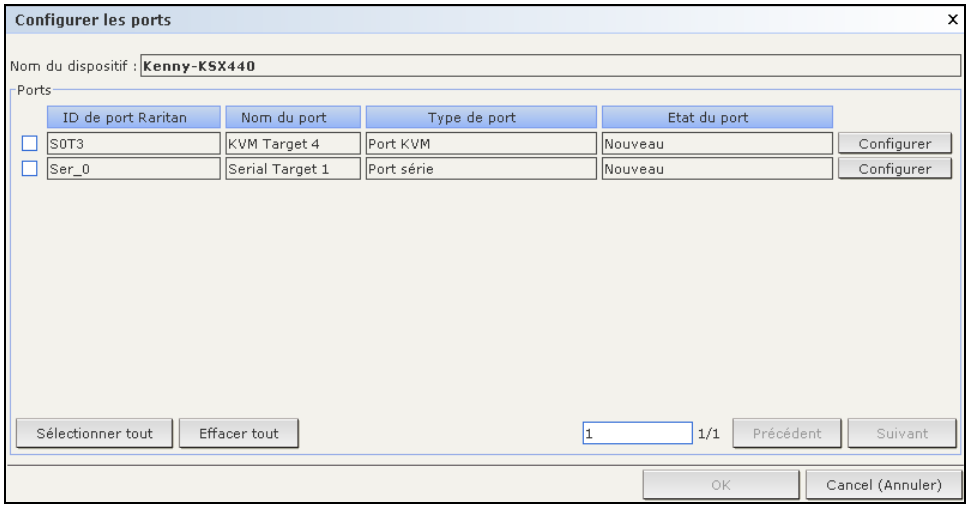

Figure 37 Ecran Configurer les ports

- 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. L'écran Configurer le port série s'affiche.

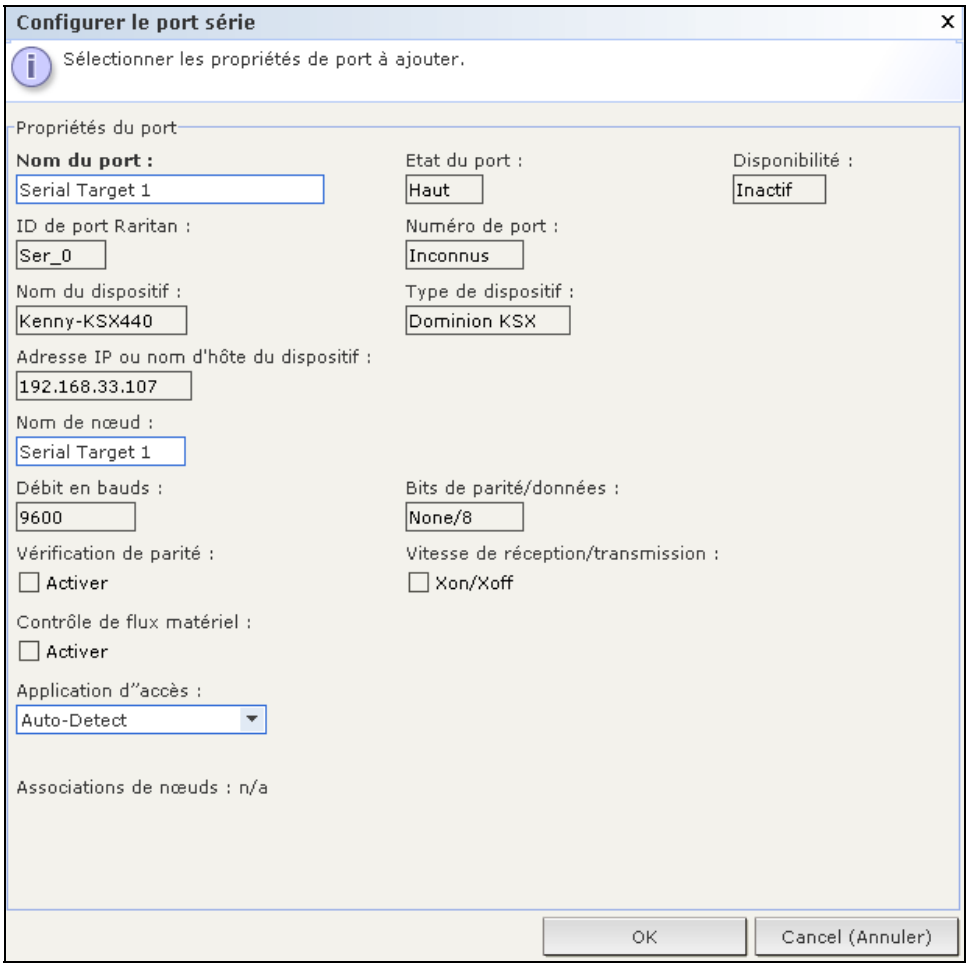

Figure 38 Ecran Configurer le port série

4. Entrez un nom pour le port dans 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.
5. Renseignez le champ **Nom de nœud** pour créer un nœud avec une interface hors bande depuis ce port. Pour une plus grande facilité d'utilisation, il est conseillé de nommer le nœud d'après la cible qui est connectée au port. Ceci signifie que vous allez entrer le même nom dans les champs **Nom du port** et **Nom de nœud**.
6. Cliquez sur le menu déroulant **Application d'accès** et sélectionnez dans la liste l'application à utiliser lors de la connexion au port concerné. Pour autoriser CC-SG à choisir automatiquement l'application correcte en fonction de votre navigateur, sélectionnez **Auto-Detect** (détection automatique).
7. Cliquez sur **OK** pour ajouter le port.

Configurer un port KVM

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez un dispositif KVM dans l'arborescence Dispositifs.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des ports**, puis sur **Configurer les ports**. L'écran Configurer les ports s'affiche.

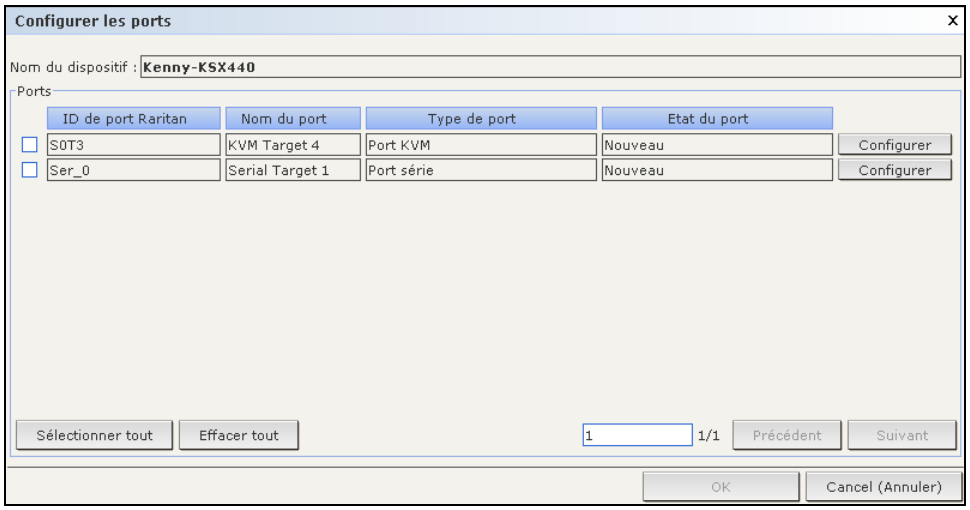

Figure 39 Ecran Configurer les ports

- 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. L'écran Configurer le port KVM s'affiche.

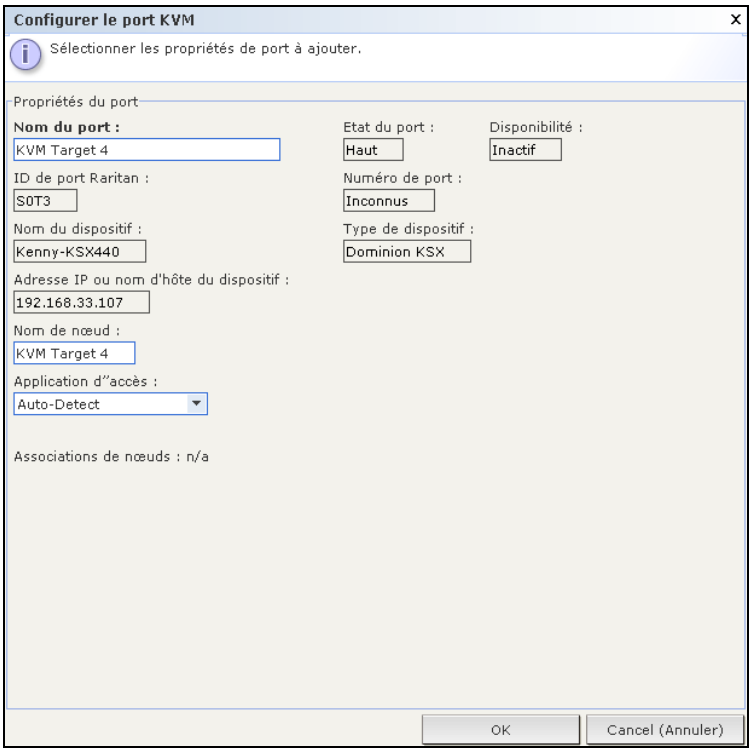

Figure 40 Ecran Configurer le port KVM

4. Entrez un nom pour le port dans 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.

5. Renseignez le champ **Nom de nœud** pour créer un nœud avec une interface hors bande depuis ce port. Pour une plus grande facilité d'utilisation, il est conseillé de nommer le nœud d'après la cible qui est connectée au port. Ceci signifie que vous allez entrer le même nom dans les champs **Nom du port** et **Nom de nœud**.
6. Cliquez sur le menu déroulant **Application d'accès** et sélectionnez dans la liste l'application à utiliser lors de la connexion au port concerné. Pour autoriser CC-SG à choisir automatiquement l'application correcte en fonction de votre navigateur, sélectionnez **Auto-Detect** (détection automatique).
7. Cliquez sur **OK** pour ajouter le port.

Modifier des ports

Vous pouvez modifier des ports configurés pour les renommer ou remplacer l'application associée.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le port à modifier. L'écran **Profil du port** apparaît.

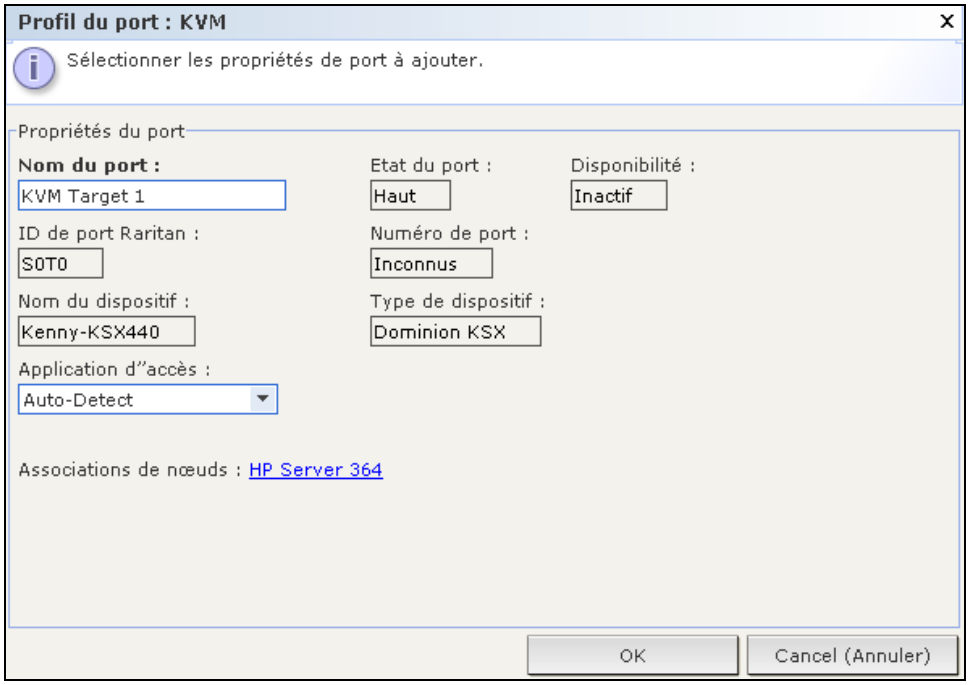

Figure 41 Profil de port

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

Supprimer des ports

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

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

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez supprimer les ports.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des ports**, puis sur **Supprimer des ports**. L'écran **Supprimer des ports** s'affiche.

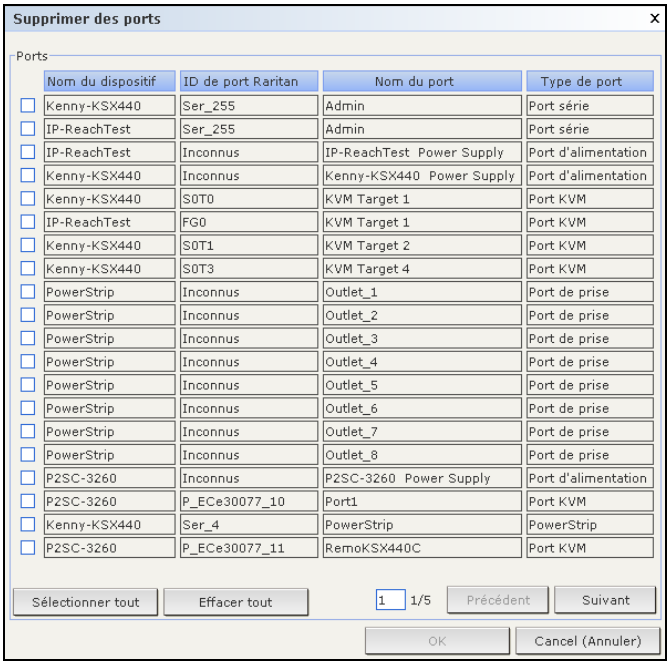

Figure 42 Ecran Supprimer des ports

3. Cochez le port à supprimer du dispositif.
4. Cliquez sur **OK** pour supprimer le port sélectionné. Le message **Le port a été supprimé** confirme que le port a bien été supprimé.

Gestion des dispositifs

Une fois le dispositif ajouté à CC-SG, plusieurs fonctions de gestion, outre la configuration des ports, peuvent être exécutées.

Copier en bloc des catégories et des éléments de dispositifs

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

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez un dispositif dans l'arborescence Dispositifs.
2. Dans le menu Dispositifs, cliquez sur Gestionnaire des dispositifs, puis sur Copier en bloc. L'écran Copier en bloc s'affiche.
3. Dans la liste **Tous les dispositifs**, sélectionnez les dispositifs vers lesquels vous copiez les catégories et les éléments du dispositif indiqué dans le champ **Nom du dispositif**.
4. Cliquez sur le **bouton >** (flèche droite) pour ajouter un dispositif à la liste **Dispositifs sélectionnés**.

5. Pour supprimer un dispositif de la liste **Dispositifs sélectionnés**, sélectionnez-le et cliquez sur le **bouton <** (flèche gauche).
6. Cliquez sur **OK** pour effectuer une copie en bloc ou sur **Cancel** (Annuler) pour quitter sans rien copier. Le message **Le dispositif a été copié** confirme que les catégories et les éléments du dispositif ont bien été copiés.

Mettre le dispositif à niveau

L'écran **Mettre le dispositif à jour** permet de télécharger de nouvelles versions de firmware pour un dispositif.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez un dispositif dans l'arborescence Dispositifs.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, puis sur **Mettre le dispositif à jour**. L'écran **Mettre le dispositif à jour** s'affiche.

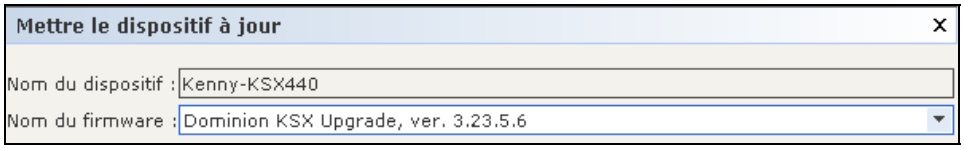

Figure 43 Ecran Mettre le dispositif à jour

3. Cliquez sur la flèche déroulante **Nom du firmware** et 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 du firmware du dispositif n'est pas compatible avec CC-SG, un message vous en avertit et vous demande si vous souhaitez continuer. Reportez-vous au **Chapitre 2 : Accès à CC-SG** pour plus d'informations. Cliquez sur **Oui** pour mettre à niveau le dispositif.
5. Un message de **redémarrage** apparaît. Cliquez sur **Oui** pour redémarrer le dispositif.
6. Le message **Le dispositif a été mis à jour** confirme la mise à niveau du dispositif.

Sauvegarder la configuration du dispositif

Vous pouvez sauvegarder tous les fichiers de configuration utilisateur et système pour un dispositif donné. En cas d'incident sur le dispositif, vous pouvez restaurer les configurations précédentes depuis CC-SG à l'aide du fichier de sauvegarde créé.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif à sauvegarder.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, **Configuration**, puis sur **Sauvegarde**. L'écran **Sauvegarder la configuration du dispositif** s'affiche.

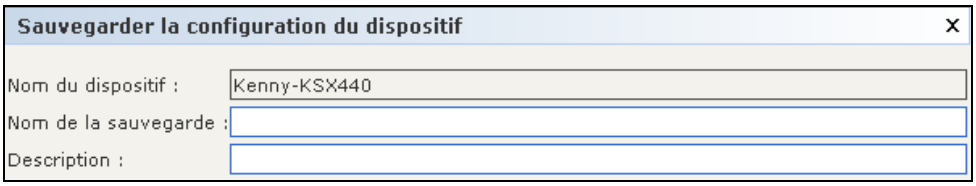

Figure 44 Ecran Sauvegarder la configuration du dispositif

3. Renseignez le champ **Nom de la sauvegarde** pour identifier cette sauvegarde.
4. Si vous le souhaitez, entrez une brève description de la sauvegarde dans le champ **Description**.
5. Cliquez sur **OK** pour sauvegarder la configuration du dispositif. Le message **La configuration du dispositif a été sauvegardée** confirme que la configuration du dispositif a bien été sauvegardée.

Restaurer la configuration du dispositif

Vous pouvez restaurer sur un dispositif une configuration sauvegardée précédemment.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez restaurer une configuration sauvegardée.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, **Configuration**, puis sur **Restaurer**. L'écran **Restaurer la configuration du dispositif** s'affiche.

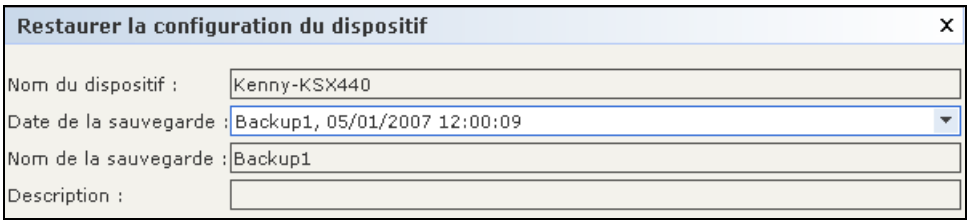

Figure 45 Ecran Restaurer la configuration du dispositif

3. Cliquez sur la flèche déroulante **Date de la sauvegarde** et sélectionnez dans la liste la date à laquelle vous avez effectué la dernière sauvegarde du dispositif. Le nom et la description de la sauvegarde apparaissent dans les champs correspondants.
4. Cliquez sur **OK** pour restaurer la sauvegarde.
5. Lorsque le message vous invitant à redémarrer le dispositif apparaît, cliquez sur **Oui**. Le message **La configuration du dispositif a été restaurée** confirme que toutes les données de configuration utilisateur et système ont bien été restaurées.

Copier la configuration du dispositif

Cette commande permet de copier des configurations d'un dispositif vers un ou plusieurs autres.

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

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

Redémarrer le dispositif

La fonction Redémarrer le dispositif permet de redémarrer un dispositif.

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif à redémarrer.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, puis sur **Redémarrer le dispositif**. L'écran **Redémarrer le dispositif** s'affiche.

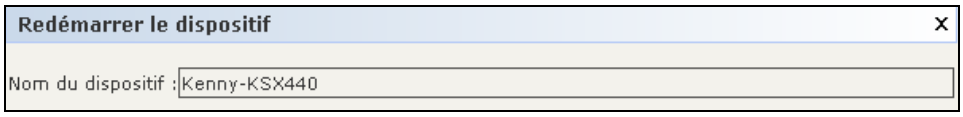

Figure 46 Ecran Redémarrer le dispositif

3. Cliquez sur **OK** pour redémarrer le dispositif. Le message **Le dispositif a été redémarré** confirme que le dispositif a bien été redémarré.

Envoyer une commande ping au dispositif

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

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif auquel la commande ping doit être envoyée.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, puis sur **Envoyer une commande ping au dispositif**. L'écran **Envoyer une commande ping au dispositif** s'affiche et présente le résultat de la commande ping.

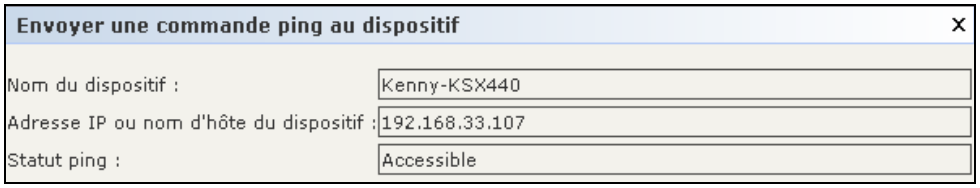

Figure 47 Ecran Envoyer une commande ping au dispositif

Suspendre la gestion

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

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

Reprendre la gestion

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

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif suspendu dans l'arborescence.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, puis sur **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 ne permet pas la mise sous et hors tension des nœuds individuellement, mais il offre une vue des prises axée sur la barrette d'alimentation.

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

1. Dans l'arborescence **Dispositifs**, sélectionnez un dispositif PowerStrip.
2. Dans le menu **Dispositifs**, sélectionnez **Gestionnaire d'alimentation des dispositifs**. L'écran **Gestionnaire d'alimentation des dispositifs** s'affiche.
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.
4. Sélectionnez la case d'option **Actif** ou **Inactif** pour chaque prise afin de la mettre sous tension ou hors tension.
5. Cliquez sur **Réactiver** pour redémarrer le dispositif connecté à la prise.
6. Cliquez sur **Fermer** pour fermer l'écran **Gestionnaire d'alimentation des dispositifs**.

Démarrer Admin

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

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

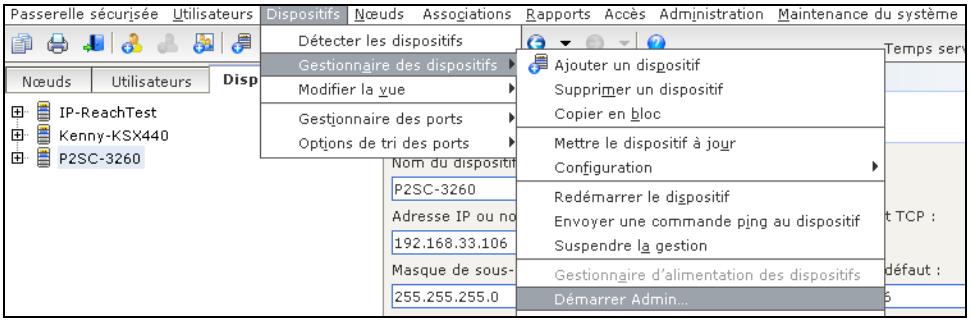

Figure 48 Démarrer Admin pour un dispositif KX

Vue topologique

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

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif dont vous souhaitez afficher la vue topologique.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, puis sur **Vue topologique**. L'écran **Vue topologique** s'affiche pour le dispositif sélectionné.

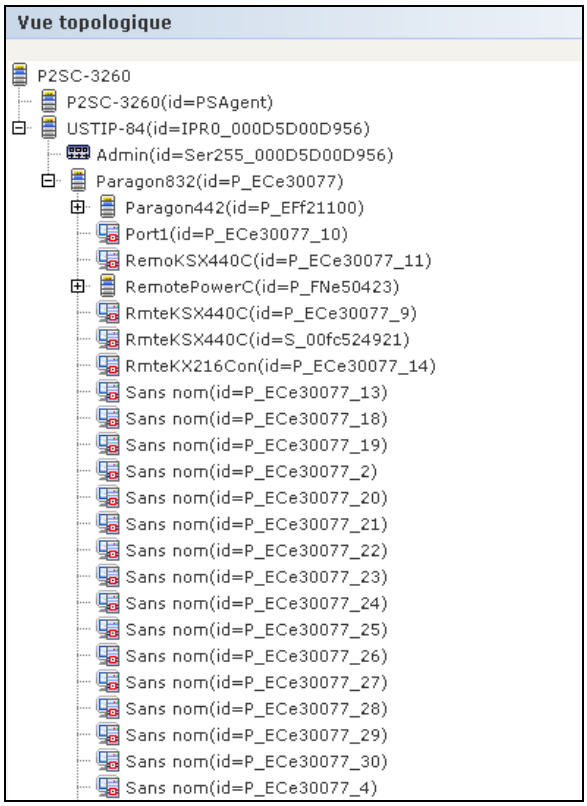

Figure 49 Vue topologique

3. Vous pouvez parcourir la vue topologique de la même manière que l'arborescence Dispositifs. Cliquez sur + ou sur – pour développer ou réduire la vue.
4. Cliquez sur **Fermer** pour fermer l'écran **Vue topologique**.

***Remarque** : 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.*

Déconnecter 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.

***Remarque** : 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.*

1. Cliquez sur l'onglet **Dispositifs** et sélectionnez le dispositif duquel vous souhaitez déconnecter un ou plusieurs utilisateurs.
2. Dans le menu **Dispositifs**, cliquez sur **Gestionnaire des dispositifs**, puis sur **Déconnecter utilisateurs**. L'écran **Déconnecter des utilisateurs** s'affiche.

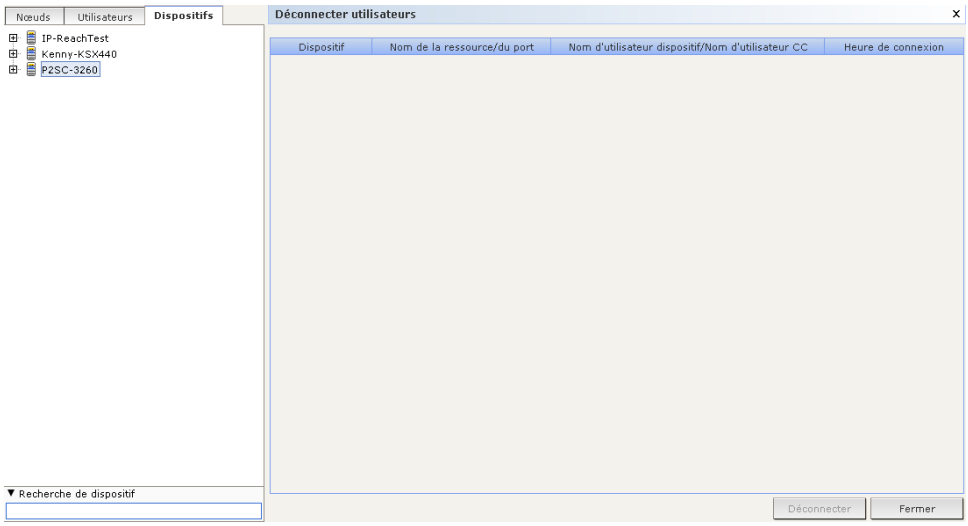

Figure 50 Déconnecter les utilisateurs

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.

***Remarque** : 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).*

Affichage des dispositifs

CC-SG offre différentes options pour afficher les dispositifs dans l'onglet **Dispositifs**.

Arborescence

Sélectionnez **Tree View** (arborescence) pour afficher les dispositifs dans l'arborescence Dispositifs groupés dans la vue par défaut. La sélection de **Tree View** vous ramènera également systématiquement à la vue standard depuis une **vue personnalisée**. Reportez-vous à **Vues personnalisée** plus loin dans ce chapitre pour plus d'informations.

1. Dans le menu **Dispositifs**, cliquez sur **Modifier la vue**, puis sur **Tree View** (arborescence). La vue standard de l'arborescence Dispositifs s'affiche.

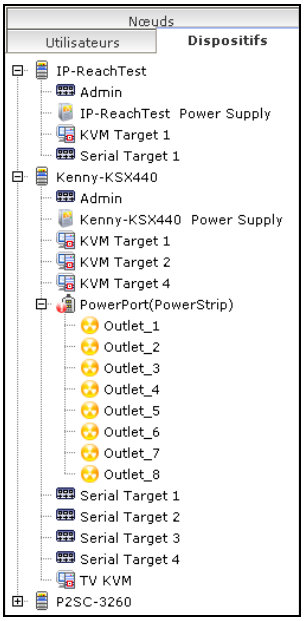

Figure 51 Ecran Vue standard de l'arborescence Dispositifs

Les ports configurés sont regroupés sous leurs dispositifs parents. Pour modifier l'affichage des ports, cliquez sur le menu **Dispositifs**, puis sur **Options de tri des ports**. Sélectionnez **Par nom de port** ou **Par état de port** pour organiser les ports au sein des dispositifs dans l'ordre alphabétique des noms ou par état de disponibilité. 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.

Vue personnalisée

Vous pouvez personnaliser l'arborescence Dispositifs en organisant les dispositifs de façon à ce qu'ils apparaissent sous une forme particulière. Vous pouvez par exemple afficher les dispositifs par pays, par fuseau horaire ou selon tout autre critère permettant de les différencier. Reportez-vous au **Chapitre 4 : Création d'associations** pour plus d'informations sur l'ajout de catégories à CC-SG.

1. Cliquez sur l'onglet **Dispositifs**.

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

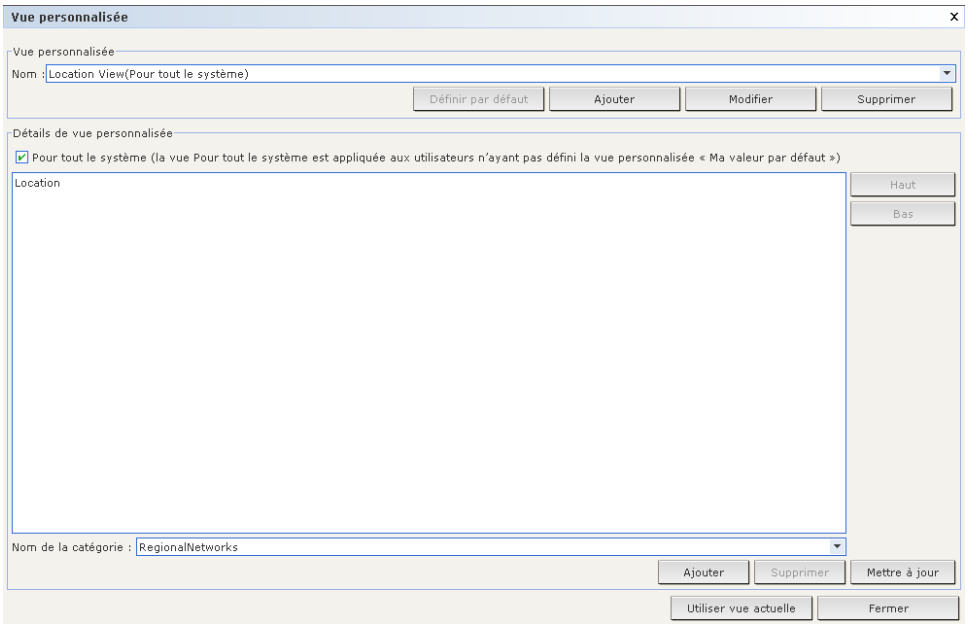

Figure 52 Ecran Vue personnalisée

3. Pour personnaliser la vue, cliquez sur la flèche déroulante **Nom** et sélectionnez une vue personnalisée qui a déjà été enregistrée dans la base de données. Les détails des catégories de la vue s'affichent dans le champ **Détails de vue personnalisée**.
4. Cliquez sur **Utiliser vue actuelle** de manière que l'arborescence Dispositifs représente la vue personnalisée sélectionnée.
5. Cliquez sur **Définir par défaut** si vous souhaitez que la vue personnalisée sélectionnée s'affiche lorsque vous vous connectez à CC-SG.
6. Cochez la case **Pour tout le système** pour en faire la vue par défaut de tous les utilisateurs n'affichant pas leur propre vue personnalisée par défaut.

Sélectionner une vue personnalisée

Pour remplacer rapidement la vue Arborescence en cours par une vue personnalisée déjà créée :

1. Cliquez sur l'onglet **Dispositifs**.
2. Dans le menu **Dispositifs**, cliquez sur **Modifier la vue**, puis sélectionnez le nom de la vue personnalisée figurant sous **Créer une vue personnalisée**. L'arborescence est alors remplacée par la vue personnalisée sélectionnée.

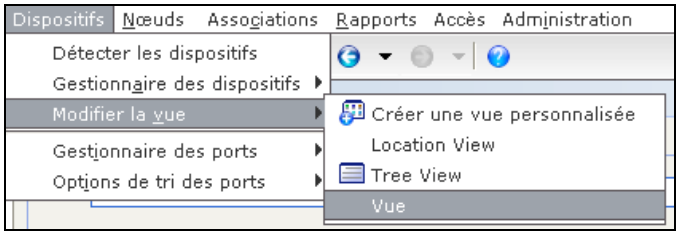

Figure 53 Sélectionner une vue personnalisée

Ajouter une vue personnalisée

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

3. Dans le panneau **Vue personnalisée**, cliquez sur **Ajouter**. La fenêtre **Ajouter une vue personnalisée** s'affiche.
4. Entrez un nom pour la nouvelle vue personnalisée et cliquez sur **OK**, ou cliquez sur **Cancel** (Annuler) pour fermer la fenêtre. Le nom de la nouvelle vue apparaît dans le champ **Nom**.
5. Cliquez sur la flèche déroulante dans la partie inférieure du panneau **Détails de vue personnalisée**. Cette liste contient les catégories que vous pouvez utiliser pour filtrer les vues personnalisées. Sélectionnez un détail dans la liste déroulante et cliquez sur le bouton **Ajouter** pour inclure ce détail dans le panneau **Détails de vue personnalisée**. Vous pouvez sélectionner autant de détails que vous le souhaitez.
6. Pour réorganiser les détails dans le panneau **Détails de vue personnalisée**, sélectionnez un détail et utilisez les boutons **Haut** et **Bas** de façon à organiser les détails dans l'ordre selon lequel les dispositifs doivent être triés. Pour supprimer un détail de la liste, sélectionnez-le et cliquez sur le bouton **Supprimer** du panneau **Détails de vue personnalisée**.
7. Cliquez sur **Mettre à jour** pour mettre la vue personnalisée à jour. Le message **La vue personnalisée a été mise à jour** confirme que la vue personnalisée a bien été mise à jour.
8. Cliquez sur **Utiliser vue actuelle** de manière que l'arborescence Dispositifs représente la vue personnalisée sélectionnée.

Modifier une vue personnalisée

1. Cliquez sur l'onglet **Dispositifs**.
2. Dans le menu **Dispositifs**, cliquez sur **Modifier la vue**, puis sur **Créer une vue personnalisée**. L'écran **Vue personnalisée** s'affiche.
3. Cliquez sur la flèche déroulante **Nom** du panneau **Vue personnalisée** et sélectionnez la vue personnalisée à modifier. Cliquez sur **Modifier**. La fenêtre **Modifier une vue personnalisée** s'affiche.
4. Entrez un nouveau nom pour la vue personnalisée et cliquez sur **OK** pour confirmer, ou sur **Cancel** (Annuler) pour fermer la fenêtre.
5. Cliquez sur la flèche déroulante dans la partie inférieure du panneau **Détails de vue personnalisée**. Cette liste contient les catégories que vous pouvez utiliser pour filtrer les vues personnalisées. Sélectionnez un détail dans la liste déroulante et cliquez sur le bouton **Ajouter** pour inclure ce détail dans le panneau **Détails de vue personnalisée**. Vous pouvez sélectionner autant de détails que vous le souhaitez.
6. Pour réorganiser les détails dans le panneau **Détails de vue personnalisée**, sélectionnez un détail et utilisez les boutons **Haut** et **Bas** de façon à organiser les détails dans l'ordre selon lequel les dispositifs doivent être triés. Pour supprimer un détail de la liste, sélectionnez-le et cliquez sur le bouton **Supprimer** du panneau **Détails de vue personnalisée**.
7. Cliquez sur **Mettre à jour** pour mettre la vue personnalisée à jour. Le message **La vue personnalisée a été mise à jour** confirme que la vue personnalisée a bien été mise à jour.
8. Cliquez sur **Utiliser vue actuelle** de manière que l'arborescence Dispositifs représente la vue personnalisée sélectionnée.

Supprimer une vue personnalisée

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

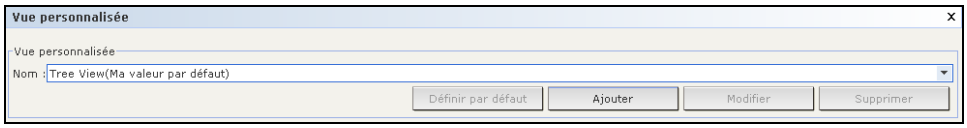

Figure 54 Ecran Vue personnalisée

3. Cliquez sur la flèche déroulante **Nom** du panneau **Vue personnalisée** et sélectionnez la vue personnalisée à supprimer.
4. Cliquez sur le bouton **Supprimer** dans le panneau **Vue personnalisée**. La fenêtre **Supprimer une vue personnalisée** s'affiche.
5. Cliquez sur **Oui** pour supprimer la vue personnalisée.

Accès spécial aux dispositifs du système Paragon II

Paragon II System Controller (P2-SC)

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

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

Pour accéder à Paragon II System Controller :

1. Cliquez sur l'onglet **Dispositifs**, puis sélectionnez le dispositif Paragon II System Controller.
2. Cliquez avec le bouton droit de la souris sur le dispositif Paragon II System Controller, puis 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.

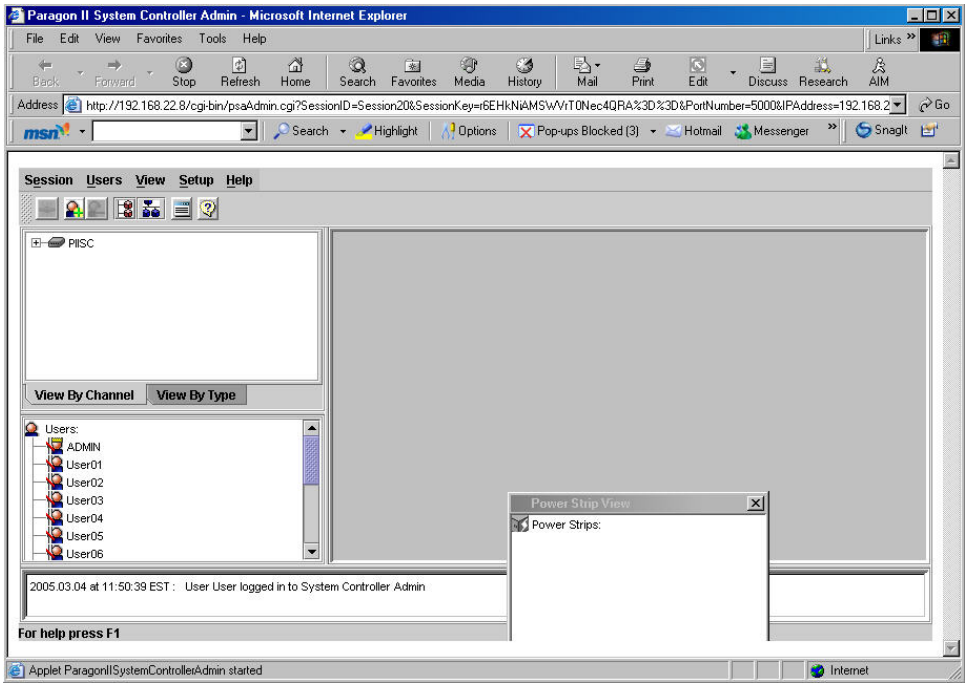

Figure 55 Fenêtre de l'application Paragon Manager

Administration des unités IP-Reach et UST-IP

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

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

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

1. Cliquez sur l'onglet **Dispositifs**, puis sélectionnez le dispositif Paragon II System Controller.
2. Avec le bouton droit de la souris, cliquez sur le dispositif Paragon II System Controller, puis cliquez sur **Lancer l'Admin de station utilisateur**. 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.

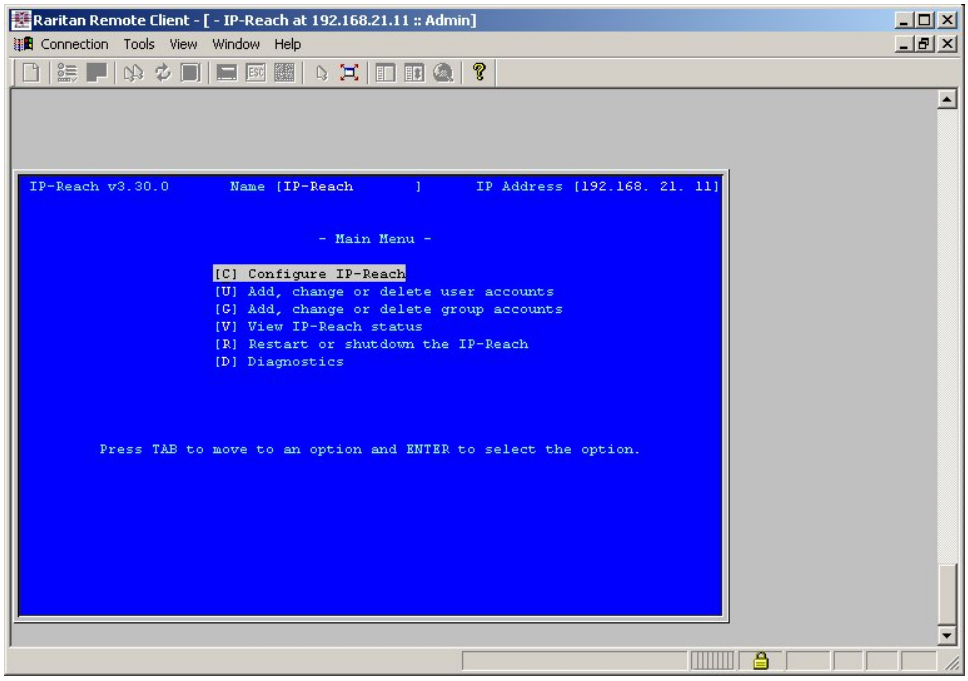

Figure 56 Ecran d'administration de l'unité IP-Reach

Gestionnaire des groupes de dispositifs

L'écran 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 au **Chapitre 8 : Stratégies** pour plus d'informations.

Ajouter un groupe de dispositifs

1. Dans le menu **Associations**, cliquez sur **Groupes de dispositifs**. La fenêtre Gestionnaire des groupes de dispositifs s'affiche. Les groupes de dispositifs existants apparaissent dans le panneau gauche.

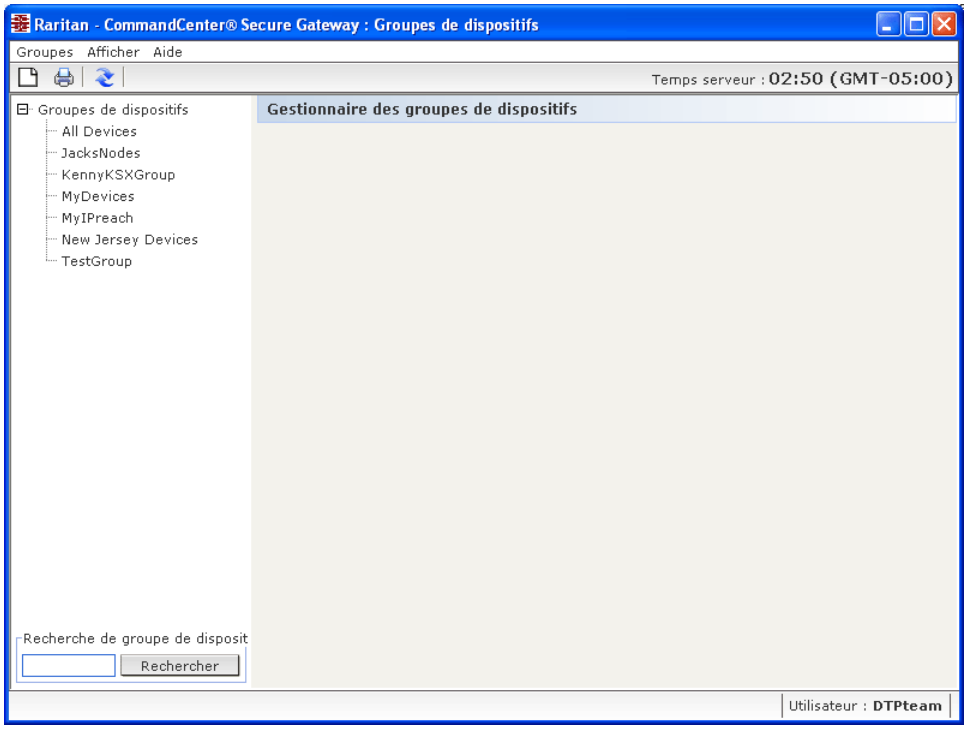

Figure 57 Gestionnaire des groupes de dispositifs

2. Cliquez sur l'icône Nouveau groupe dans la barre d'outils. Le panneau **Groupe de dispositifs : Nouveau** s'affiche.

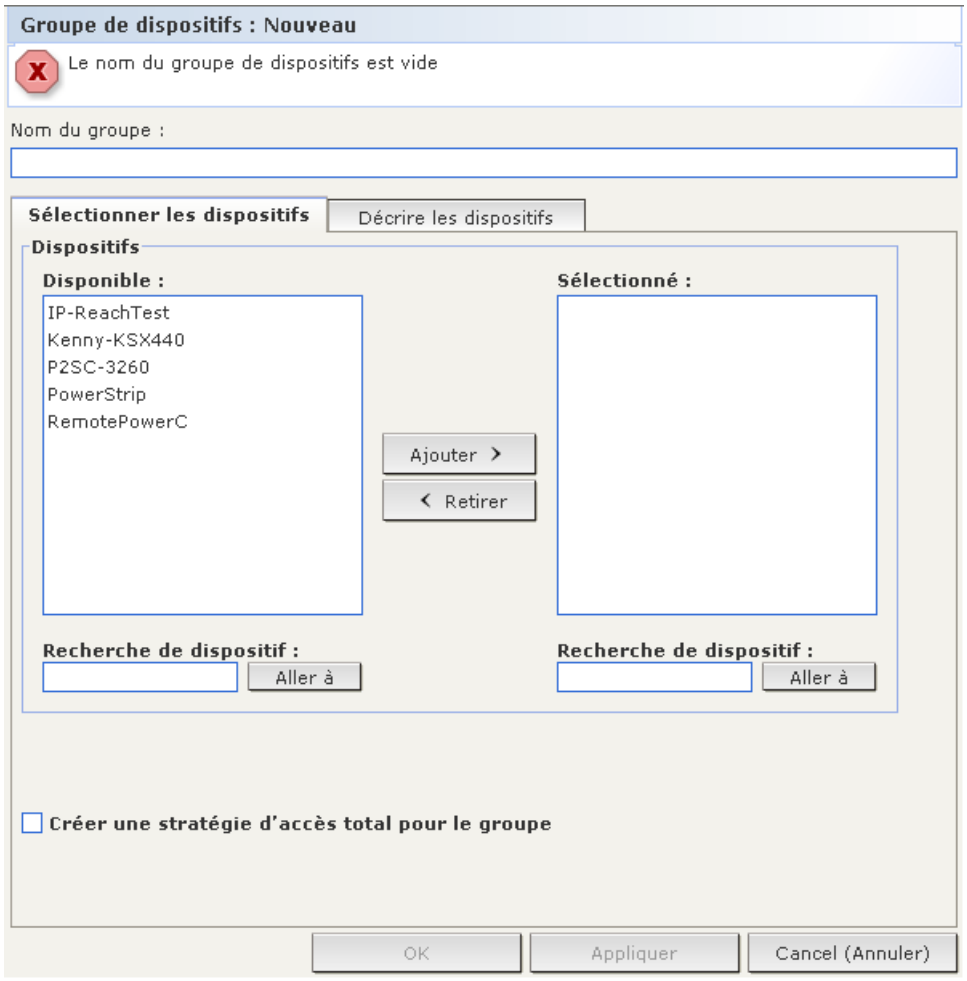

Figure 58 Panneau Groupes de dispositifs : Nouveau, onglet Sélectionner les dispositifs

3. Dans le champ **Nom du groupe**, entrez le nom du groupe de dispositifs à créer.
4. Vous pouvez ajouter des dispositifs à un groupe de deux façons : **Sélectionner les dispositifs** et **Décrire les dispositifs**. L'onglet Sélectionner les dispositifs vous permet de choisir dans la liste des dispositifs disponibles ceux que vous souhaitez affecter au groupe. L'onglet Décrire les dispositifs vous permet de spécifier des règles décrivant les dispositifs ; les dispositifs dont les paramètres respectent ces règles seront ajoutés au groupe.

Sélectionner les dispositifs

a. Cliquez sur l'onglet Sélectionner les dispositifs 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.

- Pour supprimer un dispositif du groupe, sélectionnez son nom dans la liste **Sélectionné**, puis cliquez sur **Retirer**.
- Vous pouvez rechercher un dispositif dans la liste **Disponible** ou dans la liste **Sélectionné**. Entrez les termes de la recherche dans le champ sous la liste, puis cliquez sur **Aller à**.

Décrire les dispositifs

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

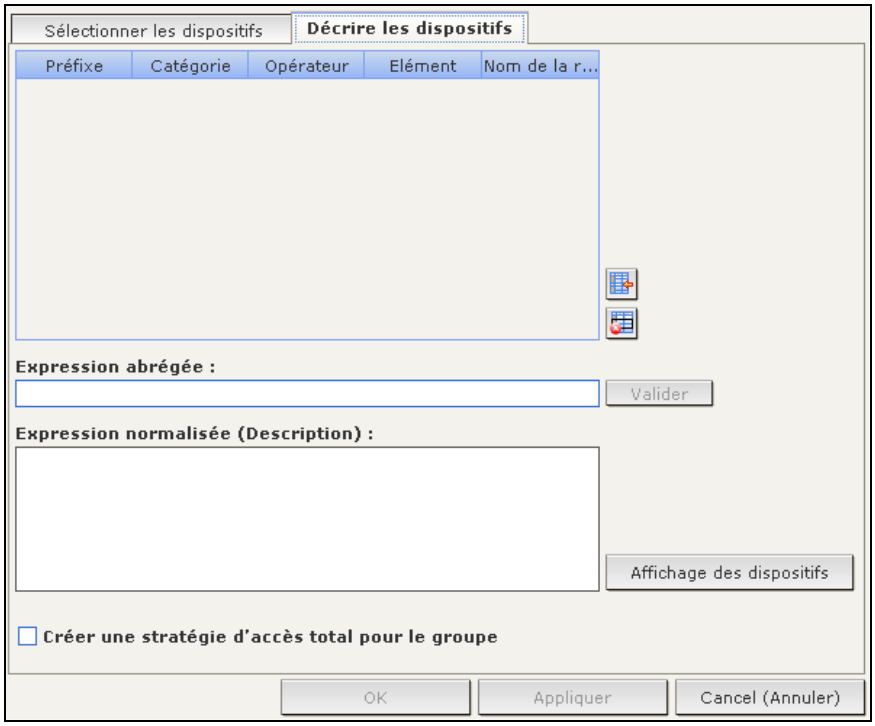

Figure 59 Onglet Décrire les dispositifs

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.

- **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.
- **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**.

Par exemple, la règle Service = Technique décrit tous les dispositifs 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 dispositif**.

d. Pour ajouter une autre règle, cliquez sur **Ajouter une nouvelle ligne**, puis effectuez les configurations nécessaires. La configuration de plusieurs règles permettra des descriptions plus précises en fournissant des critères multiples d'évaluation des dispositifs.

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

- **&** - opérateur AND. Un nœud doit satisfaire aux règles des deux côtés de cet opérateur pour que la description (ou la section d'une description) soit vérifiée.
- | - opérateur OR. Un dispositif ne doit satisfaire qu'une des règles de chaque côté de cet opérateur pour que la description (ou la section d'une description) soit vérifiée.
- **(** et **)** – opérateurs de regroupement. Ceci décompose la description en sous-section contenue entre les parenthèses. La section entre parenthèses est évaluée avant que le reste de la description ne soit comparé au nœud. Les groupes entre parenthèses peuvent être imbriqués dans un autre groupe entre parenthèses.

Par exemple : 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**.

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

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

f. 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**.

g. Cliquez sur **Affichage des dispositifs** pour visualiser les nœuds satisfaisant l'expression. Une fenêtre **Dispositifs du groupe de dispositifs Résultats** apparaît présentant les dispositifs groupés par l'expression en cours. Vous pouvez ainsi vérifier si la description est écrite correctement. Dans le cas contraire, vous pouvez retourner à la table des règles ou au champ **Expression abrégée** pour effectuer des modifications.

h. 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.

i. Si vous souhaitez ajouter un autre groupe de dispositifs, cliquez sur **Appliquer** pour enregistrer le groupe en cours, puis répétez les étapes de cette section pour ajouter des groupes de dispositifs supplémentaires. Si vous avez terminé, cliquez sur **OK** pour enregistrer le groupe et quitter le panneau **Groupe de dispositifs : Nouveau**.

Modifier un groupe de dispositifs

1. Dans le menu **Associations**, cliquez sur **Groupes de dispositifs**. La fenêtre Gestionnaire des groupes de dispositifs s'affiche.

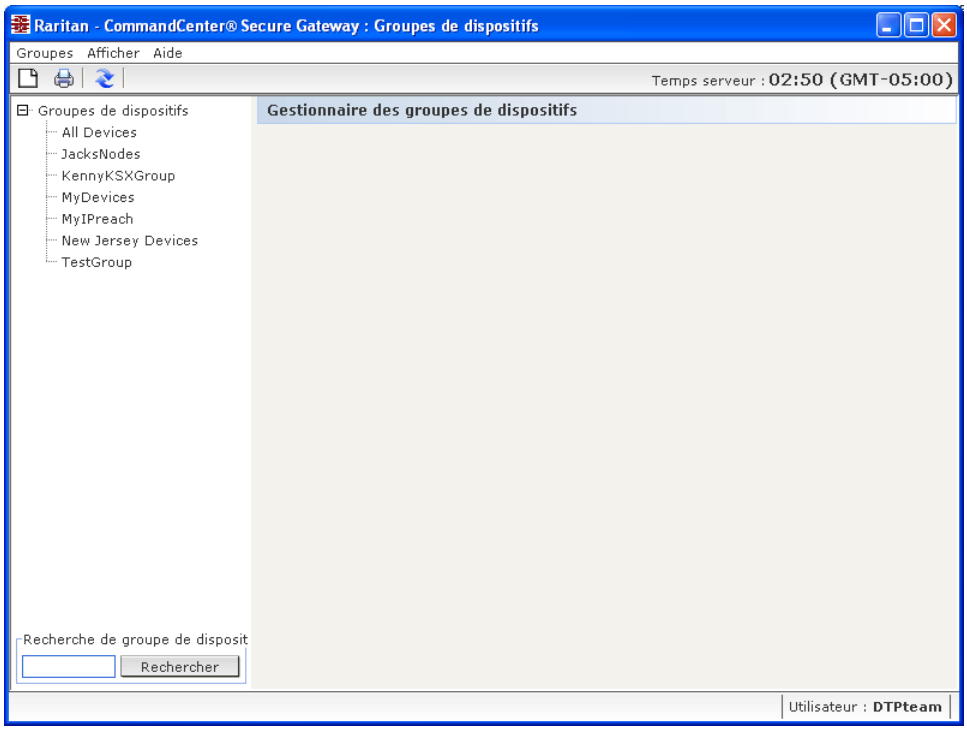

Figure 60 Ecran Gestionnaire des groupes de dispositifs

2. Les groupes de dispositifs existants apparaissent dans le panneau gauche. Sélectionnez le groupe de dispositifs à renommer. Le panneau des détails du groupe de dispositifs s'affiche.
3. Pour renommer le groupe, entrez un nouveau nom dans le champ **Nom du groupe**.
4. La modification des dispositifs inclus dans le groupe s'effectue à l'aide des onglets **Sélectionner les dispositifs** ou **Décrire les dispositifs**. Reportez-vous à **Ajouter un groupe de dispositifs** dans la section précédente pour plus d'informations.
5. Cliquez sur **OK** pour enregistrer les modifications.

Supprimer un groupe de dispositifs

1. Dans le menu **Associations**, cliquez sur **Groupes de dispositifs**. La fenêtre Gestionnaire des groupes de dispositifs s'affiche.

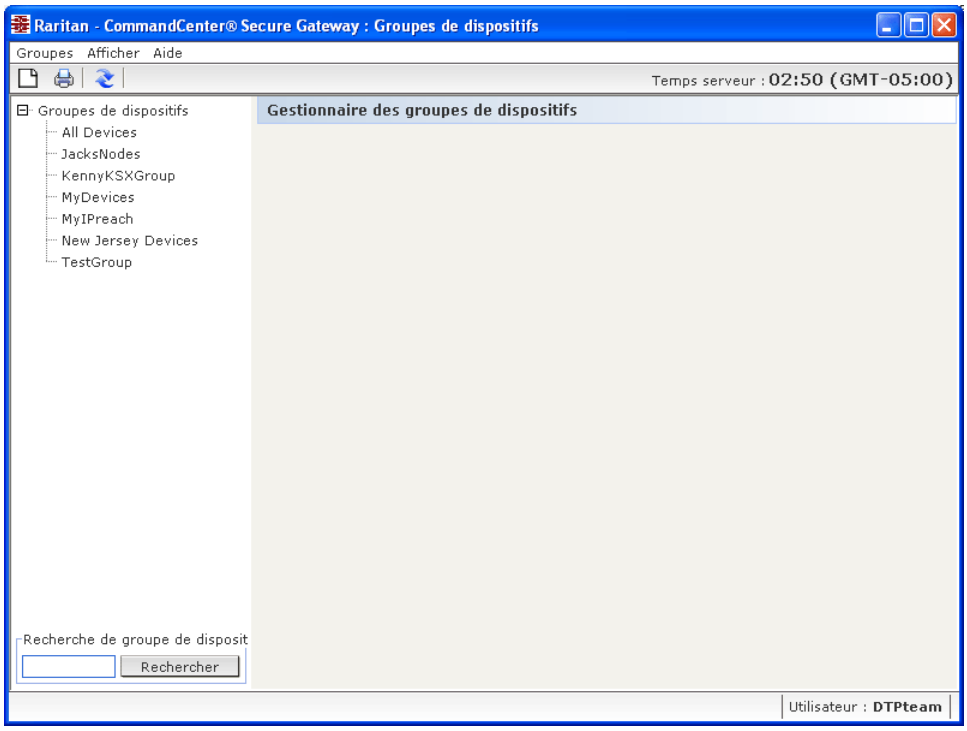

Figure 61 Ecran Gestionnaire des groupes de dispositifs

2. Les groupes de dispositifs existants apparaissent dans le panneau gauche. Sélectionnez le groupe de dispositifs à supprimer. Le panneau des détails du groupe de dispositifs s'affiche.
3. Dans le menu **Groupes**, cliquez sur **Supprimer**.

Figure 62 Fenêtre Supprimer un groupe de dispositifs

4. Le panneau **Supprimer le groupe de dispositifs** s'affiche. Cliquez sur **Supprimer**.

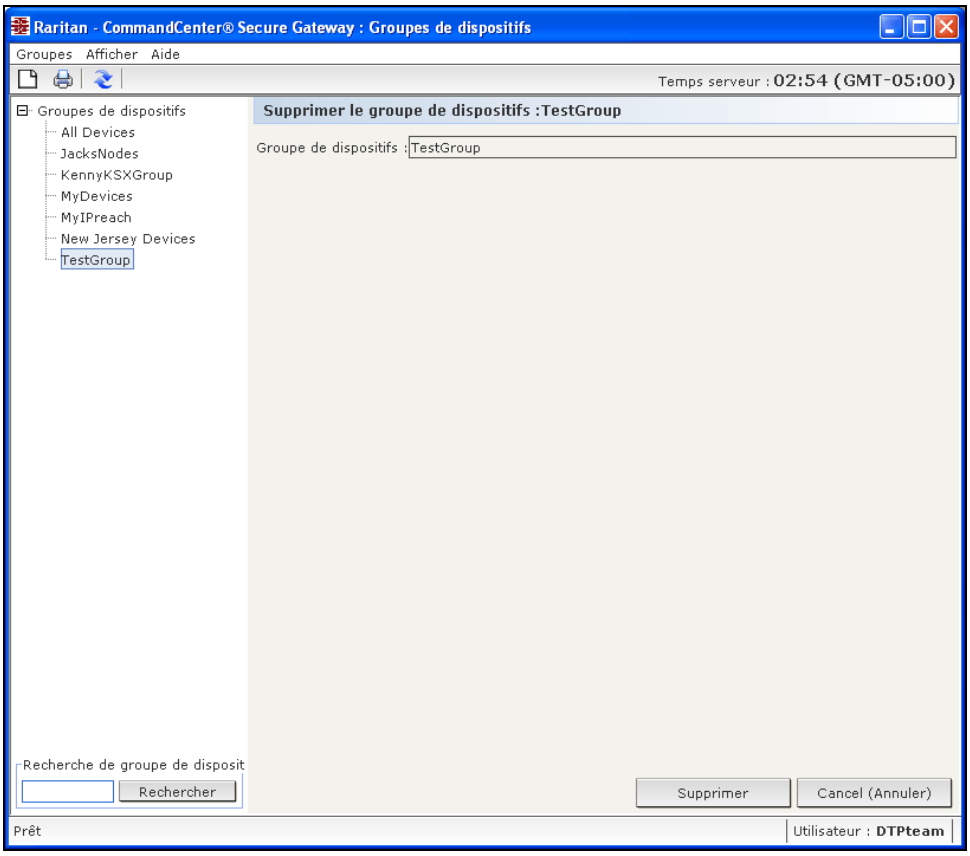

Figure 63 Panneau Supprimer le groupe de dispositifs

5. Cliquez sur **Oui** dans le message de confirmation qui s'affiche.

Chapitre 6 : Configuration des nœuds et des interfaces

Ce chapitre explique comment afficher, configurer et modifier les nœuds et les interfaces associées. Reportez-vous au **Manuel d'utilisation de CommandCenter Secure Gateway** pour plus d'informations sur la connexion des nœuds.

Affichage des nœuds

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

Arborescence Nœuds

Lorsque vous cliquez sur l'onglet **Nœuds**, l'arborescence correspondante affiche les nœuds disponibles. 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**.

Profil du nœud

Cliquez sur un nœud dans l'arborescence pour ouvrir l'écran **Profil du nœud**, qui inclut des informations sur le nœud, ses interfaces, l'interface par défaut, et les catégories et éléments qui lui sont affectés.

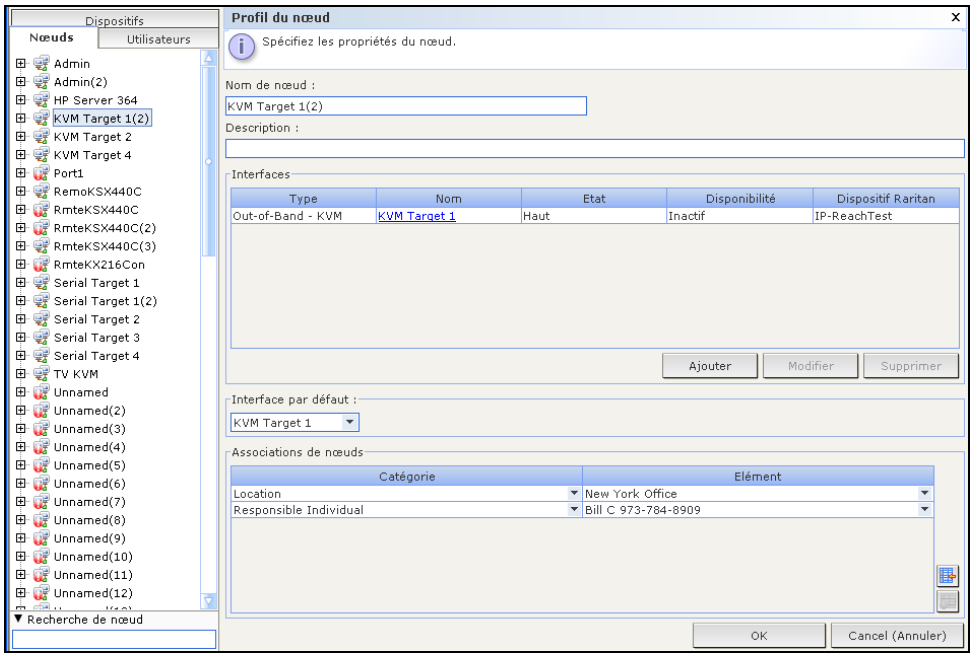

Figure 64 Onglet Nœuds et écran Profil du nœud

Icônes associées aux nœuds et aux interfaces

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

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

Vue d'ensemble des nœuds et des interfaces

A propos des nœuds

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

Vous pouvez ajouter manuellement des nœuds à CC-SG après avoir ajouté les dispositifs auxquels ils sont connectés. Toutefois, les nœuds peuvent également être créés automatiquement, en cochant la case **Configurer tous les ports** dans l'écran **Ajouter un dispositif** lorsque vous ajoutez un dispositif. Cette option permet à CC-SG d'ajouter automatiquement tous les ports du dispositif, et d'inclure un nœud et une interface KVM hors bande ou série pour chaque port. Vous avez toujours la possibilité de modifier ces nœuds, ports et interfaces ultérieurement, comme le décrit le présent chapitre. Reportez-vous au **Chapitre 3 : Configuration de CC-SG par paramétrage guidé** ou au **Chapitre 5 : Ajout de dispositifs et de groupes de dispositifs** pour plus d'informations.

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.

A propos des interfaces

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

Un nœud peut disposer de plusieurs interfaces, mais d'une seule interface série ou KVM hors bande. Par exemple, un PC exécutant Windows Server 2003 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.

Important : un grand nombre de commandes de la barre de menus décrites dans cette section sont accessibles en cliquant avec le bouton droit de la souris sur un nœud et en sélectionnant une commande dans le menu de raccourcis qui apparaît.

Ajout d'un nœud

Pour ajouter un nœud à CC-SG :

1. Cliquez sur l'onglet **Nœuds**.
2. Dans le menu **Nœuds**, cliquez sur **Ajouter un nœud**. L'écran **Profil du nœud** apparaît.

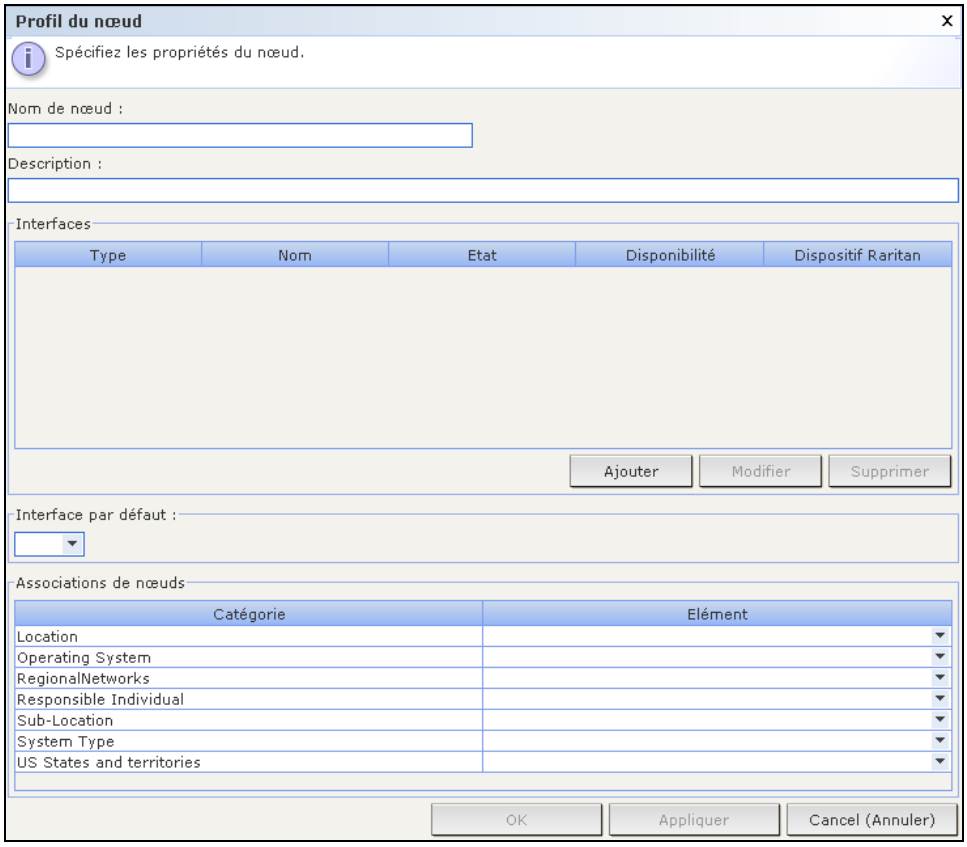

Figure 65 Ecran pour ajouter un nœud

3. Renseignez le champ **Nom de nœud**. Les noms de nœud dans CC-SG doivent tous être uniques.
4. Si vous le souhaitez, entrez une brève description de ce nœud dans le champ **Description**.
5. Vous devez configurer au moins une interface. Cliquez sur **Ajouter** dans la zone **Interfaces** de l'écran **Ajouter un nœud** pour définir une interface. Reportez-vous à la section **Ajout d'une interface** ci-après pour plus d'informations sur cette procédure.
6. Une liste de **catégories** et d'**éléments** peut être configurée pour décrire et organiser le nœud de façon optimale. Reportez-vous au **Chapitre 4 : Création d'associations** pour plus d'informations.
   - Pour chaque **catégorie** répertoriée, cliquez sur le menu déroulant **Elément**, puis sélectionnez dans la liste l'élément à appliquer au nœud. Sélectionnez l'élément vide dans le champ **Elément** pour chaque catégorie que vous ne souhaitez pas utiliser.
   - Si les valeurs **Catégorie** ou **Elément** que vous souhaitez utiliser n'apparaissent pas, vous pouvez en ajouter via le menu **Associations**. Reportez-vous au **Chapitre 4 : Création d'associations** pour plus d'informations.
7. Cliquez sur **OK** pour enregistrer le nœud. Le nœud sera ajouté à la liste.

Ajout d'une interface

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

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

   Connexions en bande

   - **DRAC KVM** : 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.
   - **RDP** : 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).
   - **RSA KVM** : 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** : sélectionnez cette option pour créer une connexion SSH à un nœud.
   - **VNC** : sélectionnez cette option pour créer une connexion KVM à un nœud via le logiciel de serveur VNC.
   - **iLO/RILOE KVM** : sélectionnez cette option pour créer une connexion KVM à un serveur HP via une interface iLO ou RILOE.

   Connexions hors bande

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

   Connexions de gestion d'alimentation

   - **DRAC** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un serveur Dell DRAC.
   - **IPMI** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un nœud via une connexion IPMI.
   - **Managed PowerStrip** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un nœud alimenté via une barrette gérée en série Raritan.
   - **RSA** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un serveur RSA.
   - **iLO/RILOE** : sélectionnez cette option pour créer une connexion de gestion d'alimentation à un serveur iLO/RILOE HP.

3. Un nom par défaut apparaît dans le champ **Nom** en fonction de votre sélection. Le cas échéant, vous pouvez le remplacer par le nom de votre choix. Ce nom apparaîtra en regard de l'interface dans la liste des nœuds.

Pour les connexions en bande et de gestion d'alimentation DRAC, RSA et iLO/RILOE :

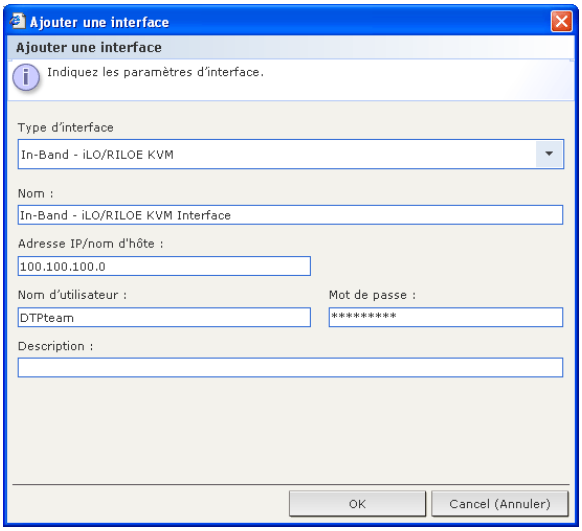

Figure 66 Ajouter une interface—In-Band iLO/RILOE KVM

a. Entrez l'adresse IP ou le nom de l'hôte de l'interface dans le champ **Adresse IP/nom d'hôte**.
b. Le cas échéant, entrez un **port TCP** pour la connexion dans le champ correspondant.
c. Entrez le **nom d'utilisateur** pour cette connexion dans le champ correspondant.
d. Le cas échéant, entrez le **mot de passe** pour cette connexion dans le champ correspondant.
e. Cliquez sur **OK** pour ajouter l'interface au nœud. Vous êtes alors redirigé vers l'écran **Ajouter un nœud** ou **Profil du nœud**.

Pour les connexions KVM hors bande, série hors bande :

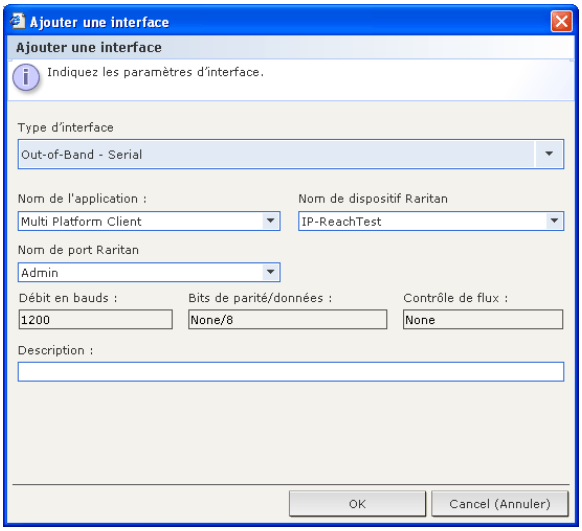

Figure 67 Configurer une connexion KVM hors bande

a. Cliquez sur le menu déroulant **Nom de l'application** et sélectionnez dans la liste l'application à utiliser lors de la connexion au nœud avec l'interface. Pour autoriser CC-SG à choisir automatiquement l'application en fonction de votre navigateur, sélectionnez **Auto-Detect** (détection automatique).

b. Cliquez sur le menu déroulant **Nom de dispositif Raritan** et sélectionnez le dispositif Raritan permettant l'accès au nœud. Notez qu'un dispositif doit avoir été ajouté à CC-SG pour apparaître dans cette liste.

c. Cliquez sur le menu déroulant **Nom de port Raritan** et sélectionnez le port sur le dispositif Raritan permettant 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.

d. Cliquez sur **OK** pour ajouter l'interface au nœud. Vous êtes alors redirigé vers l'écran **Ajouter un nœud** ou **Profil du nœud**.

Pour les connexions Managed Power Strip :

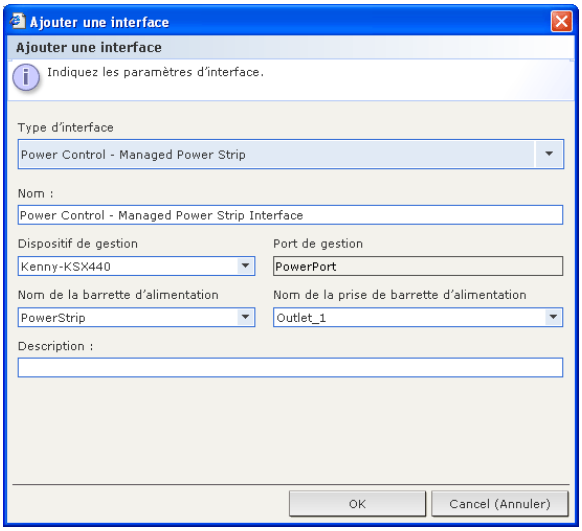

Figure 68 Configurer une interface de gestion d'alimentation Managed Power Strip

a. Cliquez sur le menu déroulant **Dispositif de gestion** et sélectionnez le dispositif Raritan qui gère la barrette servant à alimenter le nœud. Le dispositif sélectionné doit avoir été ajouté à CC-SG pour que les options appropriées soient disponibles.

b. Cliquez sur le menu déroulant **Nom de la barrette d'alimentation** et sélectionnez la barrette qui alimente le nœud. La barrette doit être configurée dans CC-SG pour apparaître dans la liste.

c. Cliquez sur **Nom de la prise de barrette d'alimentation** et sélectionnez la prise sur laquelle le nœud est branché.

d. Si vous le souhaitez, vous pouvez également entrer une description de l'interface de gestion de l'alimentation dans le champ **Description**.

e. Cliquez sur **OK** pour ajouter l'interface au nœud. Vous êtes alors redirigé vers l'écran **Ajouter un nœud** ou **Profil du nœud**.

Pour les connexions de gestion d'alimentation IPMI :

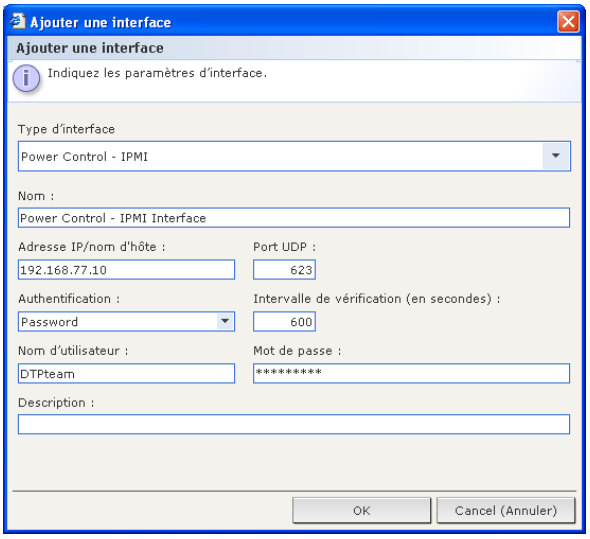

Figure 69 Configurer une interface de gestion d'alimentation IPMI

a. Entrez l'adresse IP ou le nom de l'hôte de l'interface dans le champ **Adresse IP/nom d'hôte**.
b. Entrez le **port UDP** de l'interface dans le champ correspondant.
c. Cliquez sur le menu déroulant **Authentification** et sélectionnez un schéma d'authentification pour la connexion à l'interface.
d. Entrez une valeur pour l'interface dans le champ **Intervalle de vérification (en secondes)**.
e. Entrez le **nom d'utilisateur** pour cette interface dans le champ correspondant.
f. Le cas échéant, entrez le **mot de passe** pour cette interface dans le champ correspondant.
g. Cliquez sur **OK** pour ajouter l'interface au nœud. Vous êtes alors redirigé vers l'écran **Ajouter un nœud** ou **Profil du nœud**.

Résultats de l'ajout d'une interface

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

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

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** pour plus d'informations.

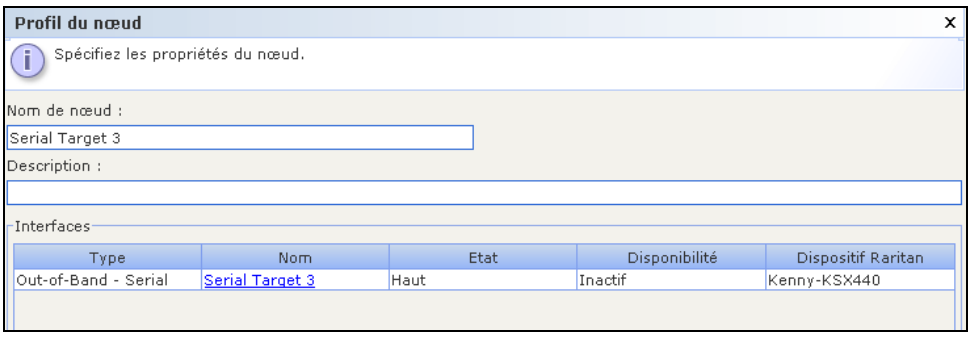

Figure 70 Se connecter à l'interface configurée d'un nœud

1. Cliquez sur l'onglet **Nœuds**.
2. Sélectionnez le nœud auquel vous souhaitez vous connecter. L'écran **Profil du nœud** apparaît.
3. Dans la table **Interfaces**, cliquez sur le nom de l'interface à l'aide de laquelle vous souhaitez vous connecter.

Ou :

1. Dans l'onglet Nœuds, cliquez sur le symbole + en regard du nœud auquel vous souhaitez vous connecter afin de développer la liste des interfaces.
2. Double-cliquez sur le nom de l'interface à l'aide de laquelle vous souhaitez vous connecter.

Modification d'une interface

Pour modifier une interface :

1. Cliquez sur l'onglet **Nœuds**.
2. Cliquez sur le nœud doté de l'interface à modifier. L'écran **Profil du nœud** apparaît.
3. Dans la table **Interfaces**, sélectionnez la ligne correspondant à l'interface à modifier.
4. Cliquez sur **Modifier**. L'écran **Modifier une interface** s'affiche.

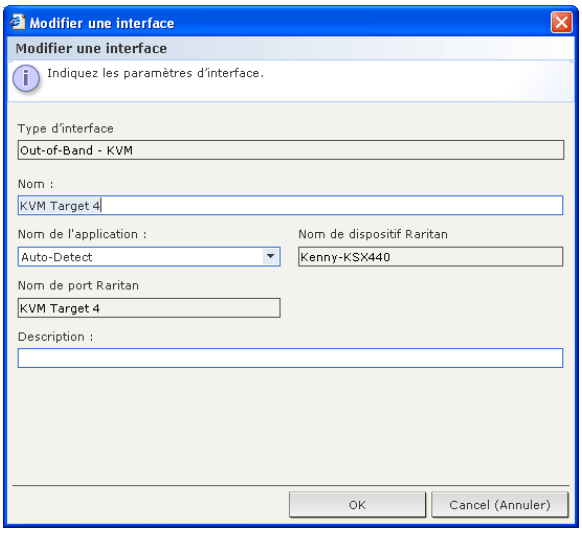

Figure 71 Modifier une interface

5. Vous ne pouvez pas modifier le type d'une interface existante. Vous pouvez modifier les valeurs des champs **Nom d'interface**, **Description** et autres, pour le type. Reportez-vous à la section **Ajout d'une interface** ci-dessus pour plus d'informations.

Suppression d'une interface

Pour supprimer une interface d'un nœud :

1. Cliquez sur l'onglet **Nœuds**.
2. Cliquez sur le nœud doté de l'interface à supprimer. L'écran **Profil du nœud** apparaît.
3. Dans la table **Interfaces**, sélectionnez la ligne correspondant à l'interface à supprimer.
4. Cliquez sur **Supprimer**. Il vous sera demandé de confirmer votre décision.
5. Cliquez sur **Oui** pour supprimer l'interface.

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.

1. Cliquez sur l'onglet **Nœuds** et sélectionnez le nœud auquel la commande ping doit être envoyée.
2. Dans le menu **Nœuds**, cliquez sur **Nœud ping**. Le résultat de l'exécution de la commande ping apparaît à l'écran.

Modification d'un nœud

Les nœuds existants apparaissent sous l'onglet **Nœuds** et sont modifiables. Pour modifier un nœud :

1. Cliquez sur l'onglet **Nœuds** et sélectionnez le nœud à modifier. L'écran **Profil du nœud** apparaît.

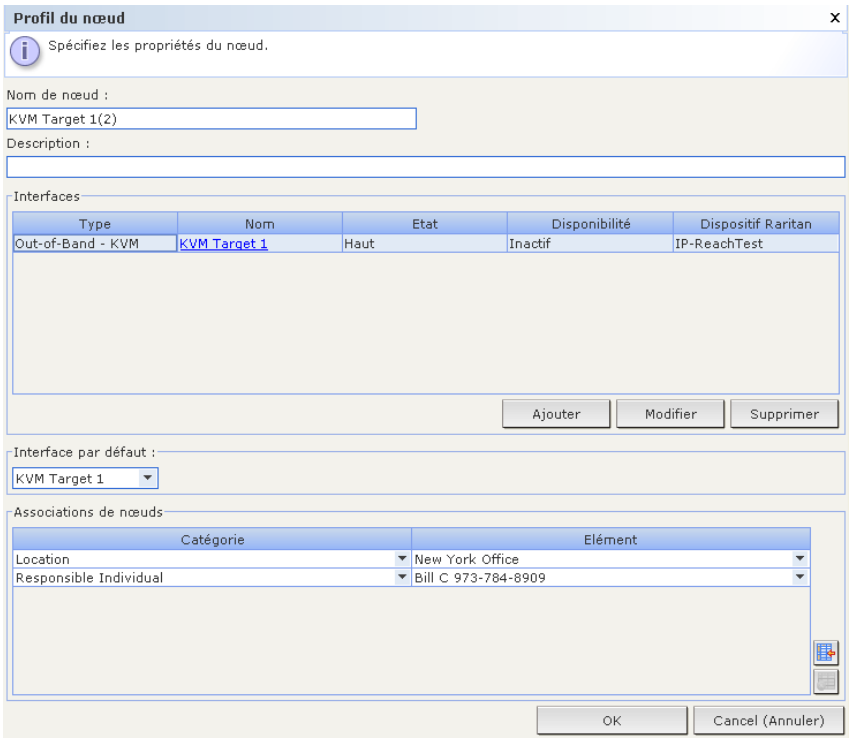

Figure 72 Ecran pour modifier un nœud

2. Si vous le souhaitez, entrez un nouveau nom dans le champ **Nom de nœud**. Les noms de nœud dans CC-SG doivent tous être uniques.
3. Si vous le souhaitez, entrez une nouvelle description brève de ce nœud dans le champ **Description**.
4. Cliquez sur **Ajouter** dans la zone **Interfaces** pour ajouter une nouvelle interface. Reportez-vous à la section **Ajout d'une interface** ci-dessus pour plus d'informations sur cette procédure.

5. Sélectionnez un nœud dans la table **Interfaces**, puis cliquez sur **Modifier** ou sur **Supprimer** pour modifier ou supprimer l'interface du nœud. Reportez-vous aux sections **Modification d'une interface** et **Suppression d'une interface** ci-dessus pour plus d'informations sur ces procédures.
6. Une liste de **catégories** et d'**éléments** peut être configurée pour décrire et organiser le nœud de façon optimale. Une catégorie permet de classer un nœud, et un élément est une valeur spécifique de cette classification. Par exemple, si le nœud représente un PC appartenant au service technique, pour une catégorie appelée Service, un élément appelé Technique peut être choisi.

   Pour **configurer** des **catégories** et des **éléments** pour le nœud :

   a. Pour chaque **catégorie** de la liste à laquelle vous souhaitez affecter une valeur, double-cliquez sur le champ **Elément** en regard de la catégorie en question. Le champ devient un menu déroulant.
   b. Cliquez sur le menu déroulant et sélectionnez la valeur **Elément** souhaitée. Sélectionnez **Aucun** si vous ne souhaitez pas utiliser cette catégorie.

   Si les valeurs **Catégorie** ou **Elément** que vous souhaitez n'apparaissent pas, vous pouvez en ajouter via le menu **Associations**. Reportez-vous au **Chapitre 4 : Création d'associations** pour plus d'informations sur la création de catégories et d'éléments.
7. Cliquez sur **OK** lorsque la configuration du nœud est terminée.

Suppression d'un nœud

La suppression d'un nœud entraîne son retrait de la liste Nœuds. Le nœud ne sera plus accessible aux utilisateurs et perdra toutes ses interfaces et associations précédentes.

Pour supprimer un nœud :

1. Cliquez sur l'onglet **Nœuds**.
2. Cliquez avec le bouton droit sur le nœud à effacer et sélectionnez **Supprimer un nœud**. L'écran **Supprimer un nœud** apparaît et affiche le nom du nœud sélectionné.

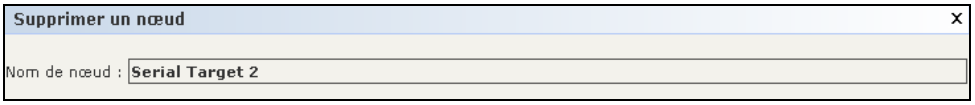

Figure 73 Supprimer un nœud

3. Cliquez sur **OK** pour supprimer le nœud ou sur **Cancel** (Annuler) pour quitter sans rien supprimer.

Conversation

La fonction 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 sur le même nœud peuvent converser les uns avec les autres.

Pour participer à une session de conversation :

1. Cliquez sur l'onglet **Nœuds**.
2. Cliquez avec le bouton droit sur le nœud auquel vous êtes connecté et sélectionnez **Conversation**, puis **Démarrer la session de conversation** si aucune session n'a encore été créée. Un session de conversation est alors créée.

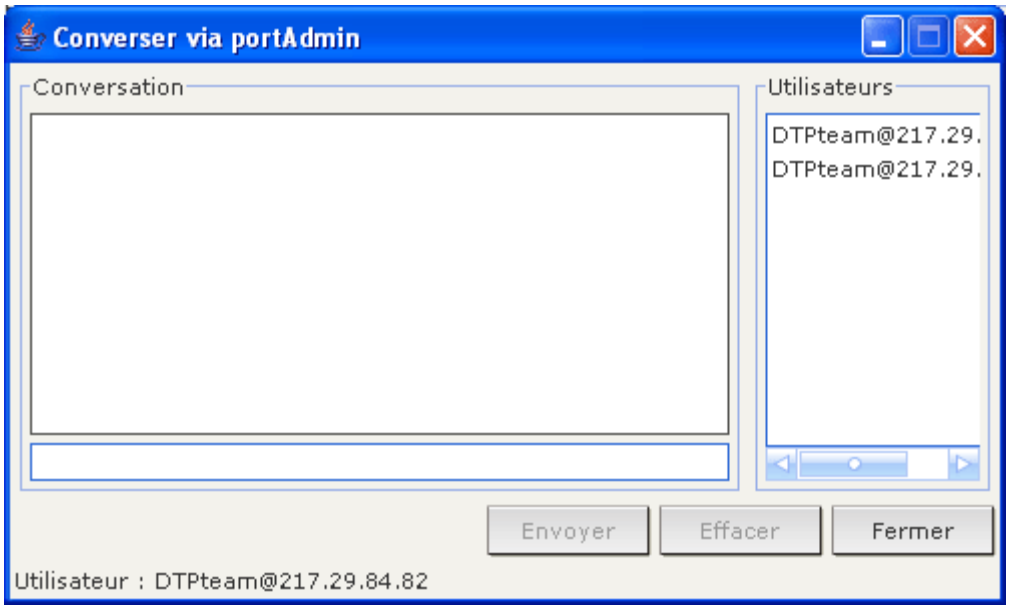

Figure 74 Session de conversation pour un nœud

Si une session est en cours, cliquez sur le nœud avec le bouton droit, sélectionnez **Conversation**, puis **Afficher la session de conversation** pour vous joindre à celle-ci.

La fenêtre de conversation apparaît alors avec les champs de message à gauche et la liste des participants à droite.

3. Tapez un message dans le champ prévu à cet effet (en bas à gauche), puis appuyez sur **<Entrée>** ou cliquez sur **Envoyer**. Le message apparaît alors dans le champ de conversation (en haut à gauche) pour pouvoir être lu par tous les utilisateurs.
4. Cliquez sur **Effacer** pour supprimer un message entré dans le champ de nouveau message, mais qui n'a pas encore été envoyé. Le champ de conversation ne sera pas effacé.
5. Cliquez sur **Fermer** pour quitter ou terminer la session de conversation.
6. Il vous sera demandé si vous souhaitez fermer la session de conversation. Cliquez sur **Oui** pour fermer la session de conversation de tous les participants ; cliquez sur **Non** pour quitter la session en la laissant ouverte pour les autres.

Vous pouvez également fermer la session de conversation de tous les participants depuis l'onglet **Nœuds**. Pour ce faire, cliquez avec le bouton droit sur le nœud associé à la session, sélectionnez **Conversation**, puis **Terminer la session de conversation**.

Groupes de nœuds

Les groupes de nœuds permettent aux administrateurs de créer des groupes logiques de nœuds arbitrairement ou en fonction de leurs catégories et éléments, et de les utiliser pour la création de stratégies d'accès. Reportez-vous au **Chapitre 8 : Stratégies** pour plus d'informations sur la création des groupes de nœuds et leur application à des stratégies.

Pour accéder à la fenêtre **Groupes de nœuds** depuis la liste Nœuds, cliquez avec le bouton droit et sélectionnez **Groupes de nœuds**.

Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs

Le terme **Utilisateurs** désigne les utilisateurs et administrateurs individuels se connectant à CC-SG pour accéder à des nœuds et gérer des dispositifs. Les **groupes d'utilisateurs** sont des organisations qui définissent un ensemble de privilèges pour leurs membres ; les utilisateurs eux-mêmes n'ont aucun privilège. En règle générale, tous les utilisateurs doivent appartenir à un groupe d'utilisateurs.

CC-SG assure la gestion de ses propres listes centralisées d'utilisateurs et de groupes d'utilisateurs à des fins d'authentification et d'autorisation, décrites dans le présent chapitre. Si vous utilisez des schémas d'authentification externes (par exemple, RADIUS ou Active Directory), les groupes d'utilisateurs et les stratégies (reportez-vous au **Chapitre 8 : Stratégies**) doivent tout de même être créés sur CC-SG. La configuration de l'authentification externe par CC-SG est décrite au **Chapitre 9 : Authentification à distance**.

Arborescence Utilisateurs

Cliquez sur l'onglet **Utilisateurs** pour afficher l'arborescence correspondante.

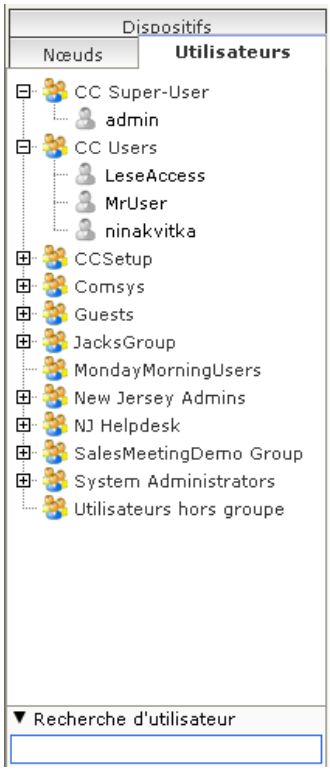

Figure 75 Arborescence Utilisateurs

L'arborescence Utilisateurs affiche 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 le symbole pour développer ou masquer la liste des utilisateurs membres. Les utilisateurs actifs, connectés actuellement à CC-SG, apparaissent en gras.

L'arborescence Utilisateurs offre la possibilité d'effectuer des recherches d'utilisateurs. La méthode de recherche peut être configurée via l'écran **Mon profil** décrit plus loin dans le présent chapitre.

Groupes d'utilisateurs spéciaux

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.

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.

Utilisateurs hors groupe

Les **utilisateurs hors groupe** ne disposent d'aucun privilège, aucun utilisateur ne peut être créé ni placé manuellement dans ce groupe. Les utilisateurs sont affectés à ce groupe s'ils ont été retirés de tous leurs groupes d'utilisateurs existants.

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

Un grand nombre de commandes de la barre de menus décrites dans cette section sont accessibles en cliquant avec le bouton droit de la souris sur un groupe d'utilisateurs ou un utilisateur et en sélectionnant une commande dans le menu de raccourcis qui apparaît.

Ajout de groupes d'utilisateurs

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

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

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

Pour créer un groupe d'utilisateurs :

1. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des groupes d'utilisateurs**, puis **Ajouter un groupe d'utilisateurs**. L'écran **Ajouter un groupe d'utilisateurs** s'affiche.

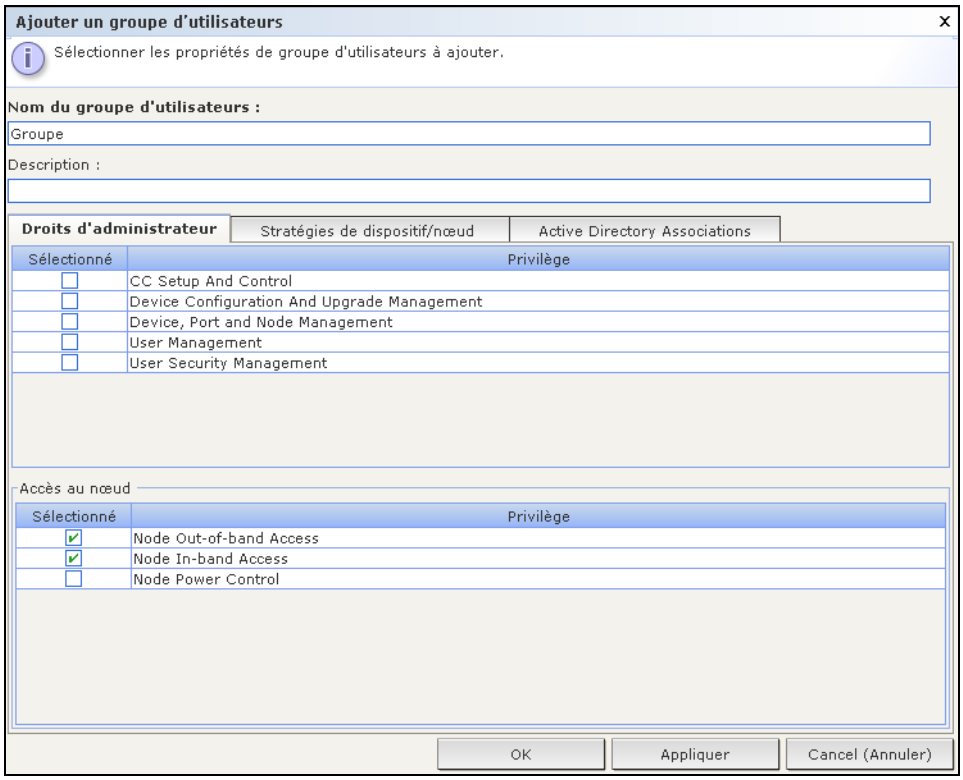

Figure 76 Ecran Ajouter un groupe d'utilisateurs

2. Renseignez le champ **Nom du groupe d'utilisateurs**. Le nom d'un groupe d'utilisateurs doit être unique.
3. Si vous le souhaitez, entrez une brève description du groupe dans le champ **Description**.
4. Cliquez sur l'onglet **Droits d'administrateur**.
5. Cochez la case correspondant à chaque privilège que vous souhaitez affecter au groupe d'utilisateurs.
6. Sous la table des privilèges figure la zone **Accès au nœud** contenant les privilèges de trois types d'accès au nœud : **Node Out-of-Band Access** (accès hors bande au nœud), **Node In-Band Access** (accès en bande au nœud) et **Node Power Control** (gestion de l'alimentation des nœuds). Cochez la case correspondant à chaque type d'accès au nœud que vous souhaitez affecter au groupe d'utilisateurs.

7. Cliquez sur l'onglet **Stratégies de dispositif/nœud**. Une table de stratégies apparaît.

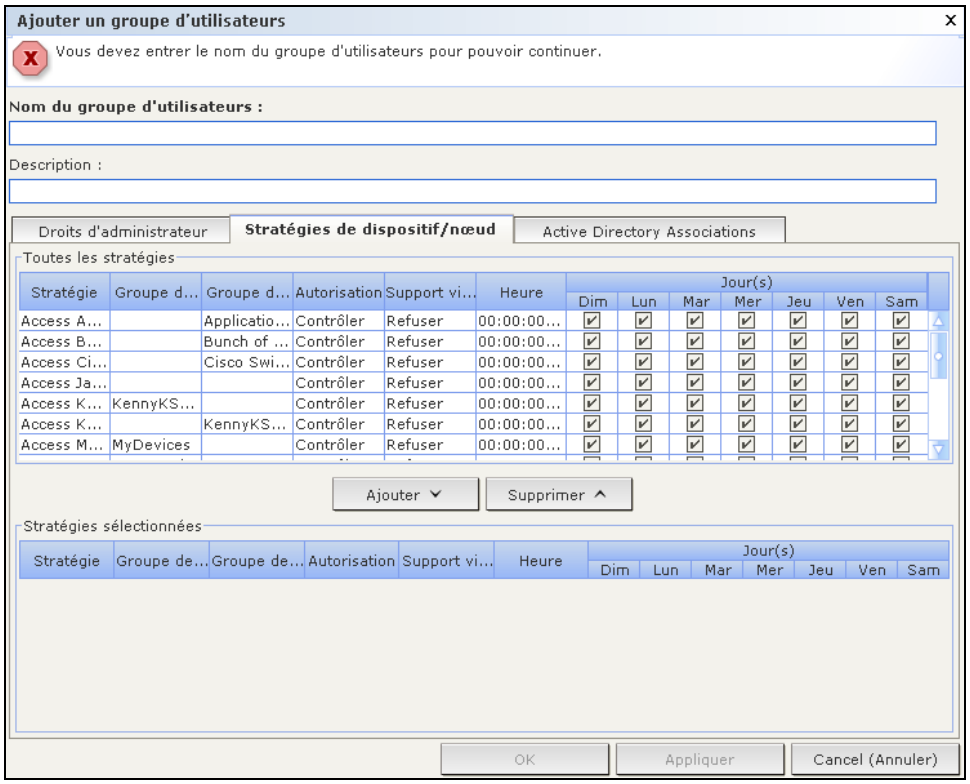

Figure 77 Onglet Stratégies de l'écran Ajouter un groupe d'utilisateurs

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 au **Chapitre 8 : Stratégies** pour plus d'informations sur les stratégies et comment les créer.

8. Dans la liste **Toutes les stratégies**, sélectionnez la stratégie à affecter au groupe d'utilisateurs, puis cliquez sur **Ajouter** pour la déplacer vers la liste **Stratégies sélectionnées**. Les stratégies de la liste **Stratégies sélectionnées** autoriseront ou non aux utilisateurs l'accès au nœud (ou aux dispositifs) qu'elles contrôlent.
9. Répétez cette étape pour ajouter des stratégies supplémentaires au groupe d'utilisateurs.
10. 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**.
11. Pour supprimer une stratégie du groupe d'utilisateurs, sélectionnez son nom dans la liste **Stratégies sélectionnées**, puis cliquez sur **Supprimer**.
12. Lorsque la configuration des stratégies du groupe est terminée, cliquez sur **Appliquer** pour enregistrer le groupe et en créer un autre, ou sur **OK** pour enregistrer le groupe d'utilisateurs sans en créer d'autres. Si vous cliquez sur **Appliquer**, répétez les étapes de cette section pour ajouter des groupes d'utilisateurs supplémentaires.

Modification d'un groupe d'utilisateurs

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

***Remarque** : vous ne pouvez pas modifier les privilèges et les stratégies des groupes **CC Super-User** et **Utilisateurs hors groupe**.*

Pour modifier un groupe :

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.

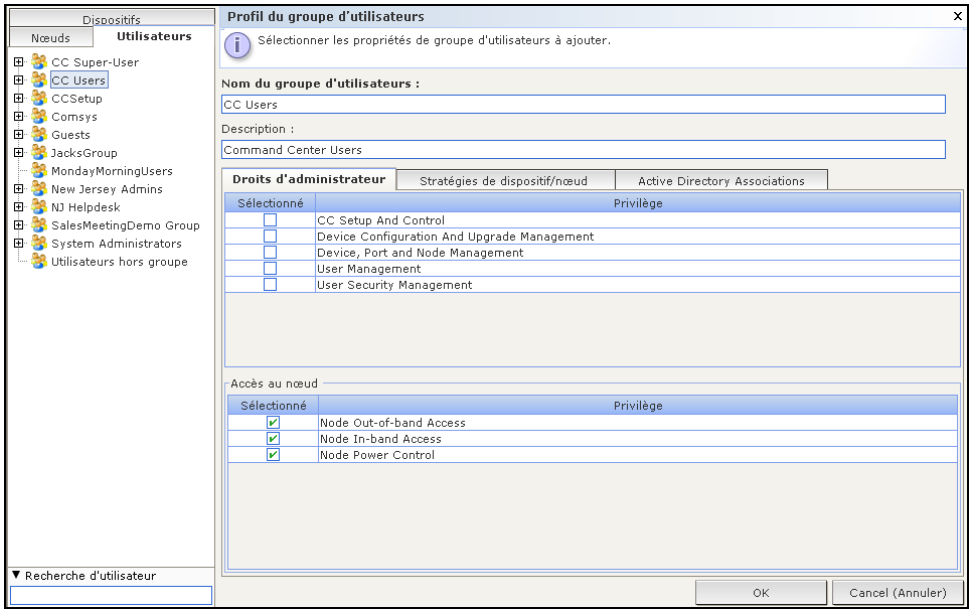

Figure 78 Modifier le groupe sélectionné

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

Suppression d'un groupe d'utilisateurs

La suppression d'un groupe d'utilisateurs entraîne son retrait de CC-SG. Les utilisateurs du groupe supprimé restent dans tous les autres groupes auxquels ils ont été affectés. Si les utilisateurs du groupe supprimé ne figuraient dans aucun autre groupe, ils sont affectés au groupe Utilisateurs hors groupe, qui ne dispose d'aucun privilège.

Pour supprimer un groupe d'utilisateurs :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur le groupe d'utilisateurs à supprimer dans l'onglet **Utilisateurs**.
3. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des groupes d'utilisateurs**, puis **Supprimer un groupe d'utilisateurs**. L'écran Supprimer un groupe d'utilisateurs s'affiche.

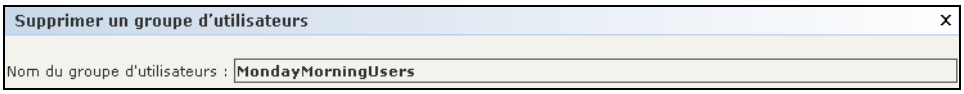

Figure 79 Supprimer un groupe d'utilisateurs

4. Cliquez sur **OK** pour supprimer le groupe d'utilisateurs ou sur **Cancel** (Annuler) pour quitter sans rien supprimer.

Si vous cliquez sur OK, un message d'état apparaît pour confirmer la suppression du groupe.

Ajout d'un utilisateur

Ajoutez des utilisateurs à un groupe pour leur affecter des privilèges d'accès dans CC-SG. La capacité d'un utilisateur à accéder à des nœuds ou à gérer des dispositifs dépend du groupe dont il est membre.

Pour ajouter un utilisateur :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Dans l'onglet **Utilisateurs**, cliquez sur le groupe auquel l'utilisateur doit être ajouté (vous ne pouvez pas ajouter d'utilisateur sans sélectionner de groupe).
3. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des utilisateurs**, puis **Ajouter un utilisateur**. L'écran **Ajouter un utilisateur** s'affiche.

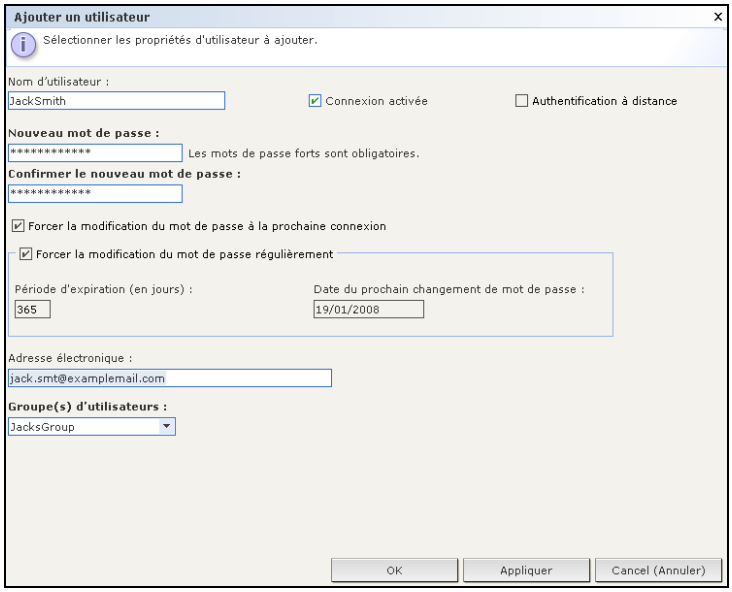

Figure 80 Ajouter un utilisateur

4. Dans le champ correspondant, entrez le **nom d'utilisateur** de l'utilisateur à ajouter. Il se servira de ce nom pour se connecter à CC-SG.
5. Cochez la case **Connexion activée** pour autoriser l'utilisateur à se connecter à CC-SG.

6. Cochez la case **Authentification à distance** uniquement si vous souhaitez que l'utilisateur soit authentifié par un serveur externe, tel que TACACS+, RADIUS, LDAP ou AD. Si vous utilisez l'authentification à distance, un mot de passe n'est pas nécessaire ; les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe** sont alors désactivés.
7. 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** : 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 au **Chapitre 12 : Administration** avancée pour plus d'informations sur les mots de passe forts.*

8. 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.
9. 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.
    a. 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. Pour modifier le groupe auquel vous ajoutez l'utilisateur, cliquez sur le menu déroulant **Groupe(s) d'utilisateurs** et sélectionnez un nouveau groupe.
12. Lorsque la configuration de l'utilisateur est terminée, cliquez sur **Appliquer** pour ajouter celui-ci et en créer un autre, ou cliquez sur **OK** pour ajouter l'utilisateur sans en créer d'autre. Les utilisateurs créés apparaîtront dans l'onglet **Utilisateurs**, imbriqués sous les groupes auxquels ils appartiennent.

Modification d'un utilisateur

Pour modifier un utilisateur :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur le symbole + en regard du groupe de l'utilisateur à modifier.
3. Cliquez sur l'utilisateur à modifier. L'écran **Profil utilisateur** apparaît.

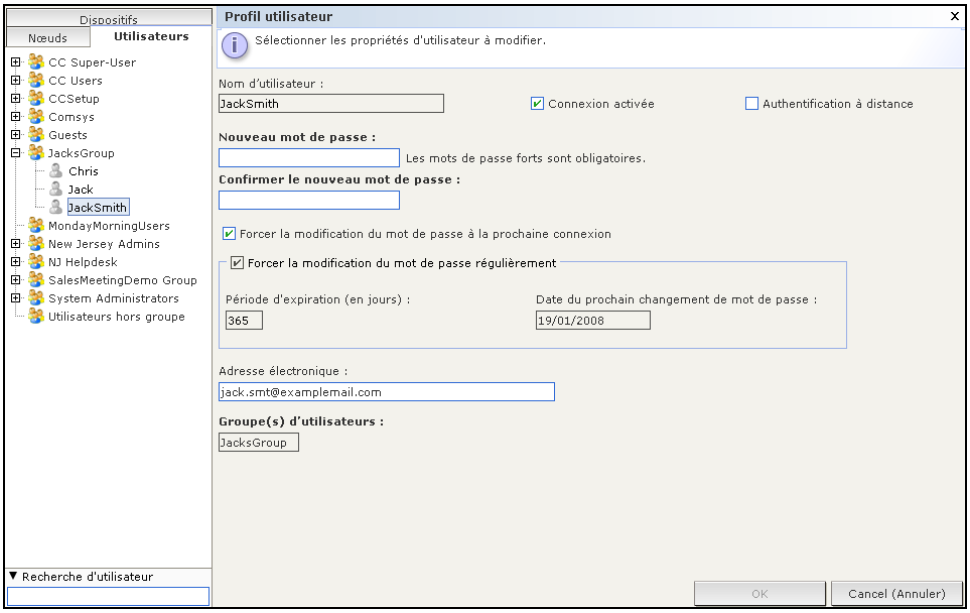

Figure 81 Modifier un utilisateur sélectionné

4. Désactivez la case **Connexion activée** pour empêcher l'utilisateur de se connecter à CC-SG. Cochez la case **Connexion activée** pour autoriser l'utilisateur à se connecter à CC-SG.
5. Cochez la case **Authentification à distance** uniquement si vous souhaitez que l'utilisateur soit authentifié par un serveur externe, tel que TACACS+, RADIUS, LDAP ou AD. Si vous utilisez l'authentification à distance, un mot de passe n'est pas nécessaire ; les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe** sont alors désactivés.
6. Dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**, entrez le mot de passe 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 au **Chapitre 12 : Administration avancée** 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. Dans le champ **Adresse électronique**, ajoutez une adresse ou modifiez celle configurée pour l'utilisateur. Elle sera utilisée pour envoyer des notifications utilisateur.
9. Lorsque la modification de l'utilisateur est terminée, cliquez sur **OK** pour enregistrer les modifications apportées à l'utilisateur ou sur **Cancel** (Annuler) pour quitter sans enregistrer.

***Remarque** : vous ne pouvez pas modifier un utilisateur pour remplacer le groupe auquel il appartient. Reportez-vous à **Affectation d'utilisateurs à un groupe** ci-dessous pour plus d'informations.*

Suppression d'un utilisateur

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

Pour supprimer un utilisateur :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur le symbole + en regard du groupe de l'utilisateur à supprimer.
3. Cliquez sur l'utilisateur à supprimer.
4. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des utilisateurs**, puis **Supprimer un utilisateur**. L'écran **Supprimer un utilisateur** s'affiche.

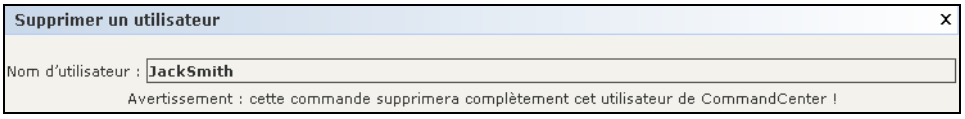

Figure 82 Supprimer un utilisateur

5. Cliquez sur **OK** pour supprimer définitivement l'utilisateur de CC-SG, ou cliquez sur **Cancel** (Annuler) pour quitter sans rien supprimer.

***Remarque** : cette commande supprime toutes les instances d'un utilisateur, même s'il figure dans plusieurs groupes. Reportez-vous à **Suppression d'utilisateurs d'un groupe** ci-dessous si vous souhaitez simplement retirer un utilisateur d'un groupe.*

Affectation d'utilisateurs à un groupe

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

Pour affecter un utilisateur à un groupe :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur le groupe auquel vous souhaitez affecter des utilisateurs.
3. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des groupes d'utilisateurs**, puis **Affecter des utilisateurs à un groupe**. L'écran **Affecter des utilisateurs à un groupe** s'affiche.

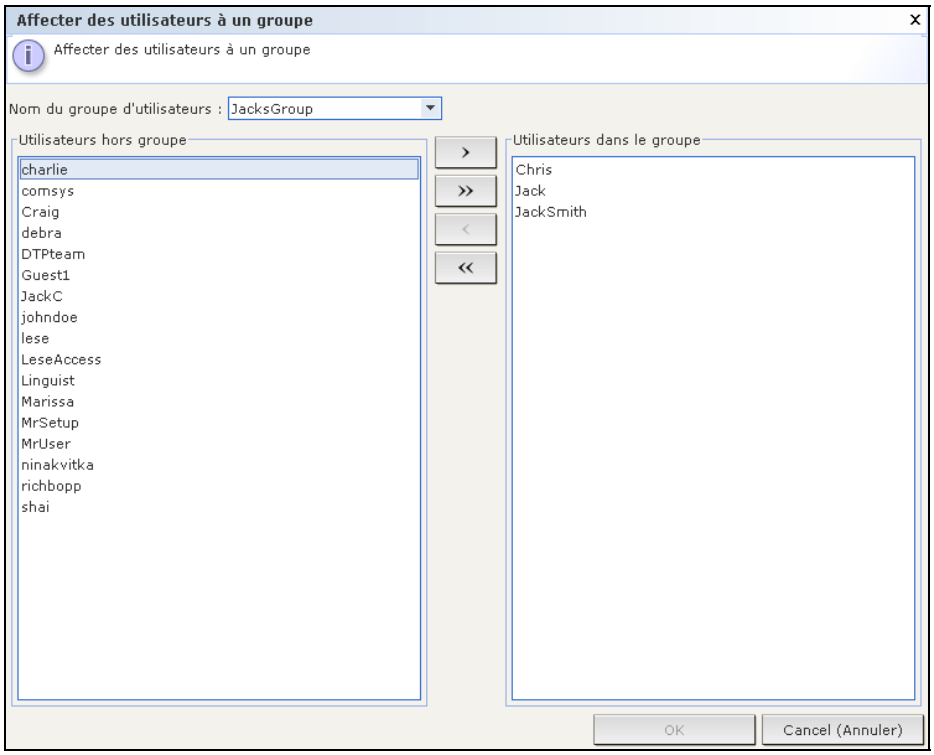

Figure 83 Ecran Affecter des utilisateurs à un groupe

4. Les utilisateurs non affectés au groupe cible apparaissent dans la liste **Utilisateurs hors groupe**. Sélectionnez dans cette colonne les utilisateurs à ajouter, puis cliquez sur le bouton > pour les déplacer vers la liste **Utilisateurs dans le groupe**.
5. Cliquez sur le bouton >> pour déplacer tous les utilisateurs non membres du groupe vers la liste **Utilisateurs dans le groupe**.
6. Pour supprimer des personnes du groupe cible, sélectionnez les utilisateurs à retirer dans la liste **Utilisateurs dans le groupe**, puis cliquez sur le bouton <.
7. Cliquez sur le bouton << pour retirer tous les utilisateurs de la liste **Utilisateurs dans le groupe**.
8. 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'utilisateurs d'un groupe

La commande **Supprimer un utilisateur du groupe** permet de retirer un utilisateur sélectionné du groupe sous lequel il figure. Cette commande ne retire pas l'utilisateur de ses autres groupes ni de CC-SG.

Pour supprimer un utilisateur d'un groupe :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur le symbole + en regard du groupe d'où l'utilisateur doit être supprimé.

3. Cliquez sur l'utilisateur à retirer.
4. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des utilisateurs**, puis **Supprimer un utilisateur du groupe**. Dans l'écran **Supprimer un utilisateur du groupe** qui s'affiche, l'utilisateur et le groupe d'où il doit être retiré sont indiqués.

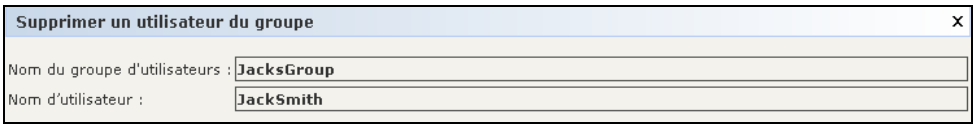

Figure 84 Supprimer un utilisateur d'un groupe

5. Cliquez sur **OK** pour supprimer l'utilisateur du groupe ou sur **Cancel** (Annuler) pour quitter sans rien supprimer.

***Remarque** : si vous supprimez d'un groupe un utilisateur qui n'appartient à aucun autre groupe, l'utilisateur sera ajouté au groupe **Utilisateurs hors groupe**.*

Autres fonctions utilisateur et groupe d'utilisateurs

Mon profil

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

Pour modifier votre profil :

1. Dans le menu **Passerelle sécurisée**, cliquez sur **Mon profil**. L'écran **Mon profil** apparaît, affichant les détails de votre compte.

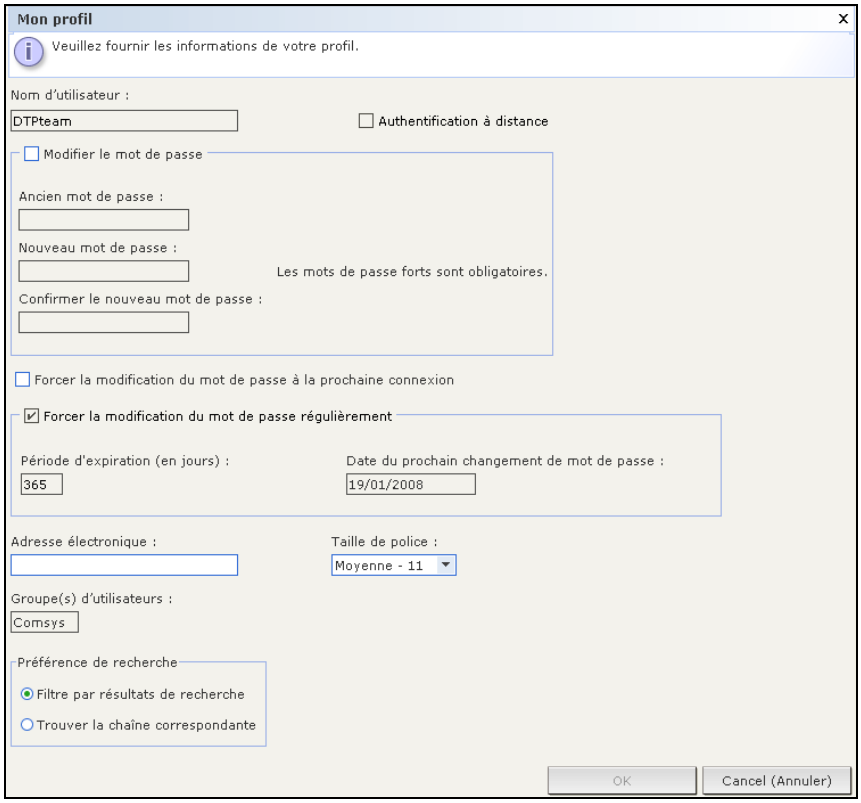

Figure 85 Ecran Mon profil

2. Si vous êtes connecté sur le compte **admin**, vous pouvez entrer un nouveau nom dans le champ **Nom d'utilisateur** pour renommer votre compte.

3. Cochez la case **Modifier le mot de passe** si vous souhaitez modifier votre mot de passe.
   a. Entrez votre mot de passe actuel dans le champ **Ancien mot de passe**.
   b. Entrez votre nouveau mot de passe dans le champ **Nouveau mot de passe**. Un avis apparaît si un mot de passe fort est obligatoire.
   c. Entrez une nouvelle fois votre nouveau mot de passe dans le champ **Confirmer le nouveau mot de passe**.
4. 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.
5. Cliquez sur le menu déroulant **Taille de police** pour régler la taille de la police d'affichage du client CC-SG standard.
6. 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**.
7. Lorsque la modification de votre profil est terminée, cliquez sur **OK** pour enregistrer les modifications ou sur **Cancel** (Annuler) pour quitter sans enregistrer.

Déconnecter les utilisateurs

Cette commande permet de déconnecter les utilisateurs actifs de CC-SG. Elle permet également de fermer la session de tous les utilisateurs actifs d'un groupe.

Pour déconnecter des utilisateurs :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur le symbole + en regard du groupe des utilisateurs à déconnecter.
3. Cliquez sur l'utilisateur à déconnecter. Pour déconnecter plusieurs utilisateurs, maintenez la touche **Ctrl** enfoncée et cliquez sur les autres utilisateurs.
4. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des utilisateurs**, puis **Déconnecter le ou les utilisateur(s)**. L'écran **Déconnecter les utilisateurs** apparaît et affiche la liste des utilisateurs sélectionnés.
5. Cliquez sur **OK** pour déconnecter les utilisateurs de CC-SG ou sur **Cancel** (Annuler) pour abandonner l'opération.

Pour déconnecter tous les utilisateurs d'un groupe :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur le groupe des utilisateurs à déconnecter. Pour déconnecter plusieurs groupes d'utilisateurs, maintenez la touche **Ctrl** enfoncée et cliquez sur les autres groupes.
3. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des groupes d'utilisateurs**, puis **Déconnecter les utilisateurs**. L'écran **Déconnecter les utilisateurs** apparaît et affiche la liste des utilisateurs actifs des groupes sélectionnés.
4. Cliquez sur **OK** pour déconnecter les utilisateurs de CC-SG ou sur **Cancel** (Annuler) pour abandonner l'opération.

Copier en bloc

Pour gagner du temps, la commande **Copier en bloc** peut être utilisée pour cloner les privilèges et les stratégies d'un utilisateur pour d'autres utilisateurs en déplaçant ces derniers vers les mêmes groupes que l'utilisateur choisi. Pour copier en bloc :

1. Cliquez sur l'onglet **Utilisateurs**.
2. Cliquez sur le symbole + en regard du groupe de l'utilisateur à copier.
3. Cliquez sur l'utilisateur à copier.
4. Dans le menu **Utilisateurs**, sélectionnez **Gestionnaire des utilisateurs**, puis **Copier en bloc**. L'écran **Copier en bloc** s'affiche.

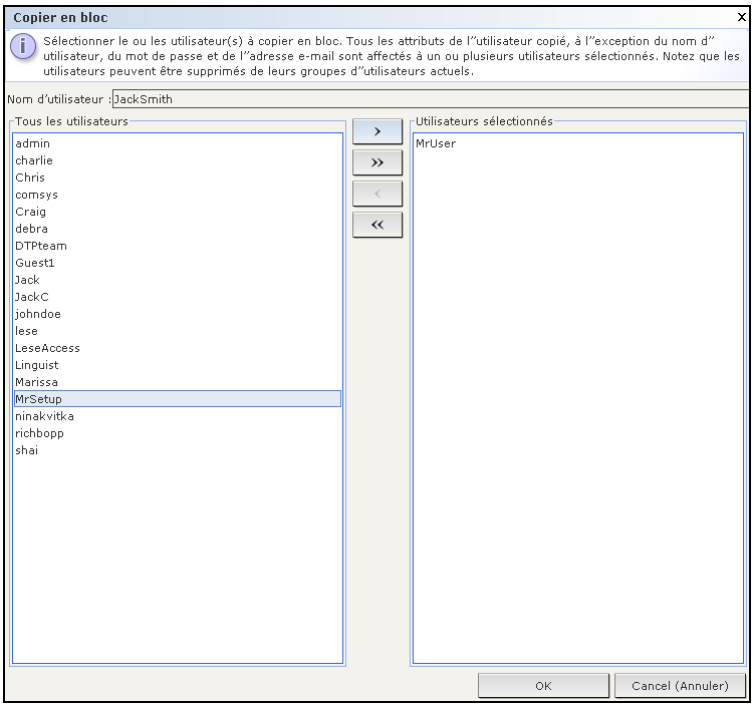

Figure 86 Ecran Copier en bloc

5. Dans la liste **Tous les utilisateurs**, sélectionnez les utilisateurs qui doivent adopter les privilèges et stratégies de l'utilisateur indiqué dans le champ **Nom d'utilisateur**.
6. Cliquez sur le bouton > pour déplacer le nom d'un utilisateur vers la liste **Utilisateurs sélectionnés**.
7. Cliquez sur le bouton >> pour déplacer tous les utilisateurs vers la liste **Utilisateurs sélectionnés**.
8. Pour retirer un utilisateur de la liste **Utilisateurs sélectionnés**, sélectionnez-le et cliquez sur le **bouton** <.
9. Cliquez sur le bouton << pour retirer tous les utilisateurs de la liste **Utilisateurs sélectionnés**.
10. Cliquez sur **OK** pour copier les propriétés de l'utilisateur. Les utilisateurs copiés seront déplacés de leurs groupes actuels vers les groupes dont l'utilisateur sélectionné est membre.

Chapitre 8 : Stratégies

Contrôle des accès à l'aide de stratégies

La configuration de nouvelles stratégies autorisant l'accès utilisateur à des nœuds est facultative, mais primordiale pour tirer profit de la capacité de CC-SG à contrôler cet accès. 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 souhaitez renforcer votre contrôle sur l'accès des utilisateurs aux nœuds, vous devez créer des stratégies afin de définir des règles pour celui-ci. Comme tous les privilèges, les stratégies sont affectées à des groupes d'utilisateurs afin d'appliquer ces règles d'accès aux membres de ces groupes.

Si vous avez effectué le **paramétrage guidé** (reportez-vous au **Chapitre 3: Configuration de CC-SG par paramétrage guidé**), certaines stratégies de base ont sans doute déjà été créées. Vous pouvez maintenant appliquer ces stratégies à des groupes d'utilisateurs existants. Si vous n'avez pas utilisé le **paramétrage guidé** ni créé les stratégies nécessaires, suivez la procédure ci-dessous. Vous allez :

- créer des groupes de nœuds afin d'organiser les nœuds pour lesquels vous souhaitez créer des règles d'accès ;
- créer des groupes de dispositifs si vous souhaitez créer des règles d'accès pour les dispositifs Raritan qui fournissent des interfaces aux nœuds ;
- créer une stratégie pour un nœud (ou dispositif) indiquant quand l'accès à celui-ci est possible ;
- appliquer cette stratégie à un groupe d'utilisateurs.

Résumé des stratégies

Le diagramme suivant offre une représentation visuelle de la mise en place de la sécurité à l'aide de CC-SG :

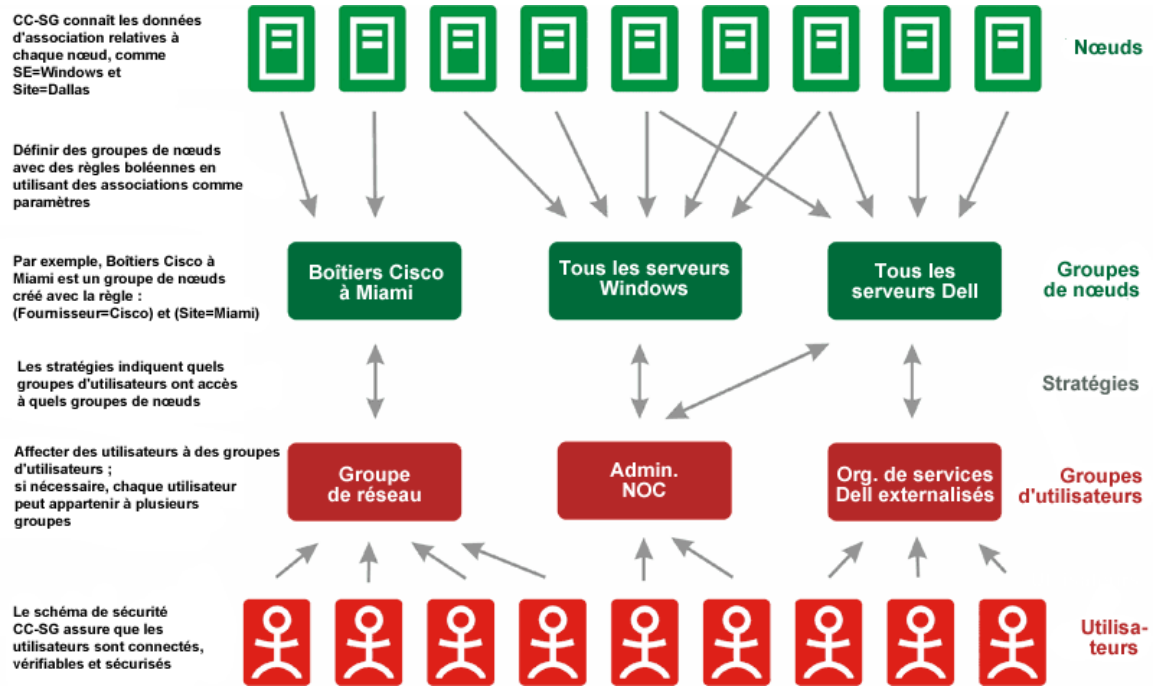

Figure 87 Résumé de stratégie

Groupes de nœuds

Les groupes de nœuds permettent d'organiser les nœuds dans un ensemble. Chaque groupe sert ensuite de base à une stratégie autorisant ou refusant l'accès à cet ensemble particulier de nœuds. Les nœuds peuvent être regroupés arbitrairement ou par un jeu d'attributs communs.

De plus, si vous avez utilisé le Gestionnaire des associations 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 au **Chapitre 4 : Associations** pour plus d'informations sur la création des catégories et des éléments.

Pour visualiser les groupes de nœuds existants :

Dans le menu **Associations**, cliquez sur **Groupes de nœuds**. La fenêtre **Gestionnaire des groupes de nœuds** s'affiche. La liste des groupes de nœuds existants s'affiche sur la gauche, tandis que les informations relatives au groupe de nœuds sélectionné apparaissent dans le panneau principal.

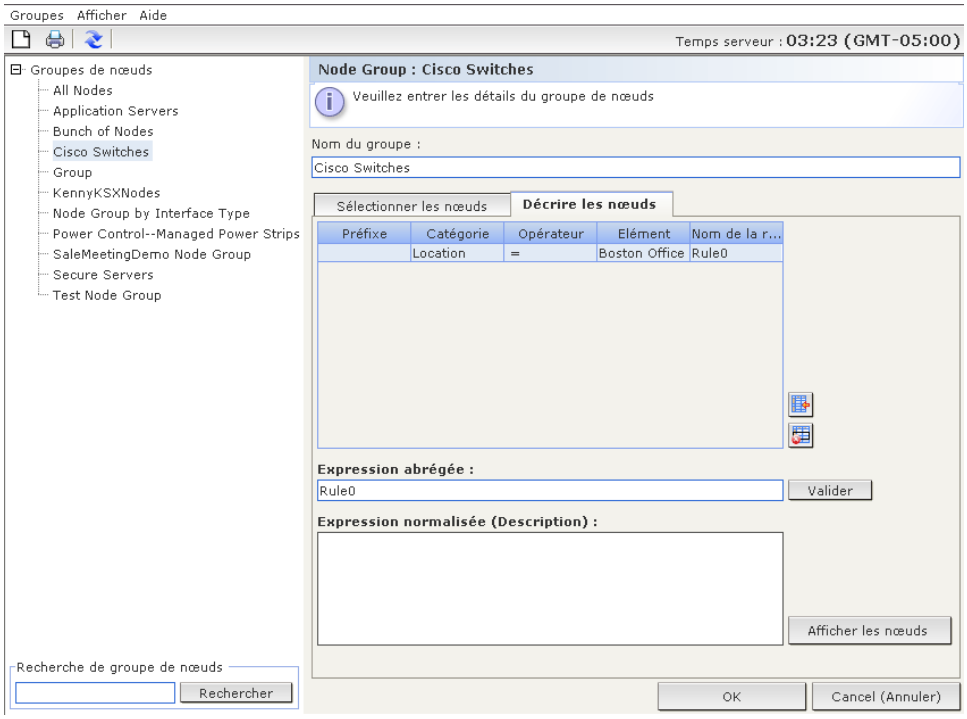

Figure 88 Gestionnaire des groupes de nœuds

1. La liste des groupes de nœuds existants est affichée sur la gauche. Cliquez sur un groupe de nœuds pour afficher les informations le concernant dans le Gestionnaire des groupes de nœuds.
   Si le groupe a été formé arbitrairement, l'onglet **Sélectionner les nœuds** est affiché. Il présente une liste des nœuds du groupe et de ceux qui n'en font pas partie.
   Si le groupe a été formé d'après des attributs communs, l'onglet **Décrire les nœuds** est affiché. Il présente les règles régissant la sélection des nœuds du groupe.
2. Pour rechercher un nœud dans la liste du groupe, entrez une chaîne dans le champ **Recherche de nœud** au bas de la liste, puis cliquez sur **Aller à**. La méthode de recherche est configurée dans l'écran **Mon profil**. Reportez-vous au **Chapitre 7 : Utilisateurs et groupes d'utilisateurs** pour plus d'informations.

3. 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.

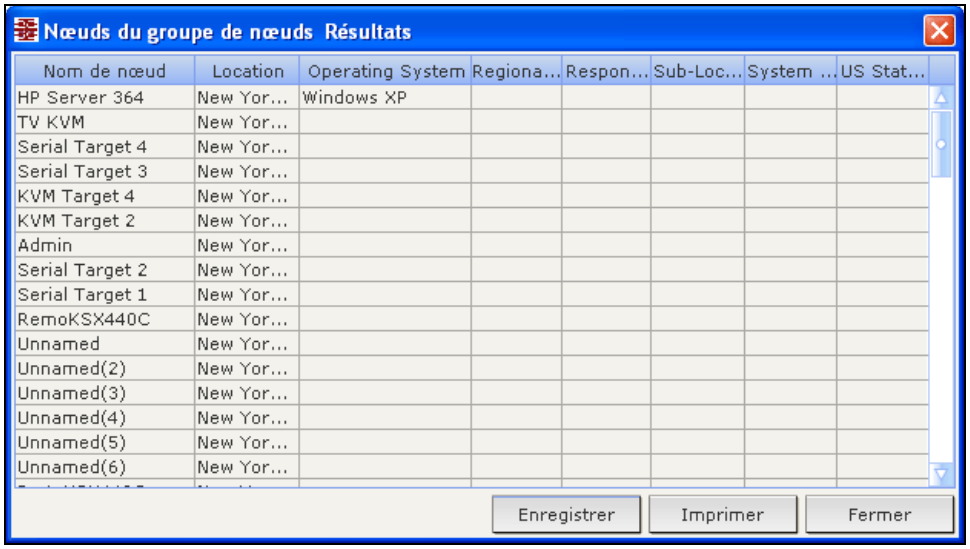

Figure 89 Nœuds d'un groupe basé sur des attributs

Ajouter des groupes de nœuds

Pour ajouter un nouveau groupe de nœuds :

1. Dans le menu **Associations**, cliquez sur **Groupes de nœuds**. La fenêtre **Gestionnaire des groupes de nœuds** s'affiche.
2. Dans le menu **Groupes**, sélectionnez **Nouveau**. Un modèle de groupe de nœuds apparaît.
3. Dans le champ **Nom du groupe**, entrez le nom du groupe de nœuds à créer.

Vo]us pouvez ajouter des nœuds à un groupe de deux façons : **Sélectionner les nœuds** et **Décrire les nœuds**. La méthode Sélectionner les nœuds permet d'affecter arbitrairement des nœuds au groupe en les sélectionnant dans la liste des nœuds disponibles. La méthode Décrire les nœuds permet de définir des règles de description des nœuds ; les nœuds correspondant à la description sont ajoutés au groupe.

Sélectionner les nœuds

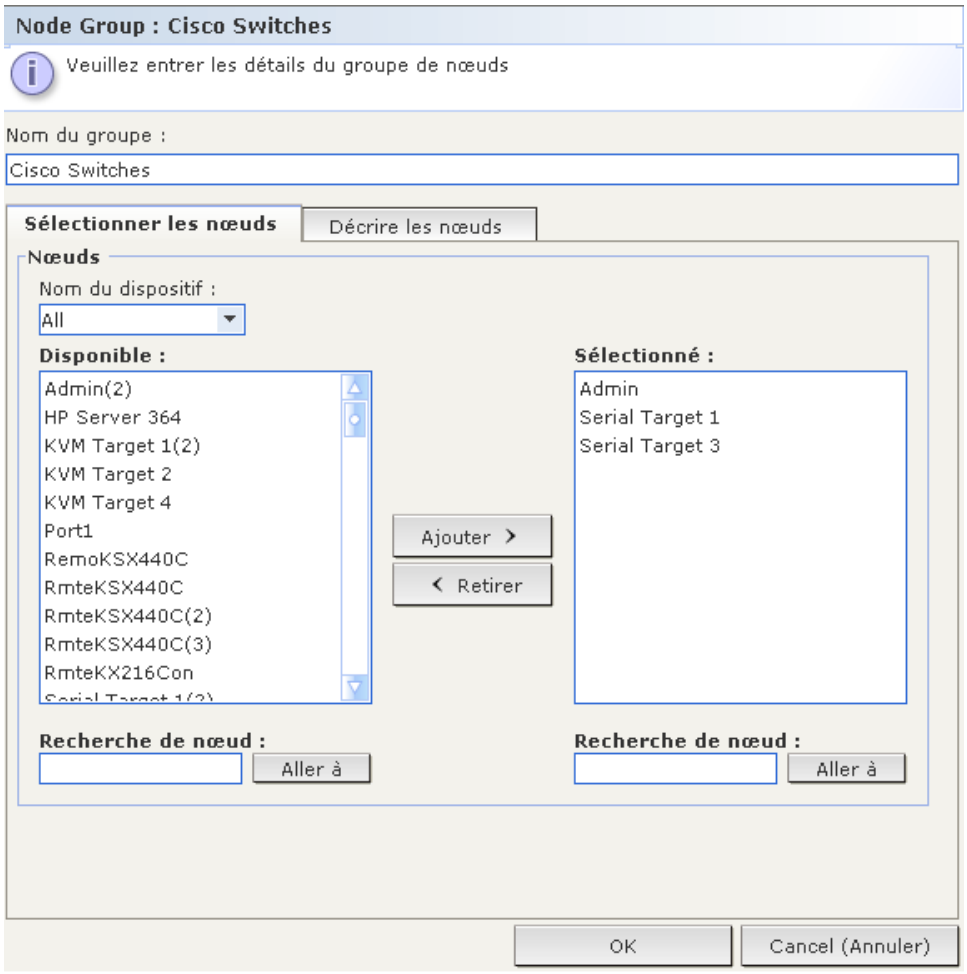

Figure 90 Ajouter des nœuds à l'aide de la méthode Sélectionner les nœuds

1. Cliquez sur l'onglet **Sélectionner les nœuds**.
2. Cliquez sur le menu déroulant **Nom du dispositif** et sélectionnez un dispositif pour filtrer la liste **Disponible** et n'afficher que les nœuds avec interfaces à partir de ce dispositif.
3. Dans la liste **Disponible**, sélectionnez les nœuds à inclure au groupe, puis cliquez sur **Ajouter** pour les déplacer vers la liste **Sélectionné**. Les nœuds de la liste **Sélectionné** seront ajoutés au groupe.
4. Pour supprimer un nœud du groupe, sélectionnez son nom dans la liste **Sélectionné**, puis cliquez sur **Retirer**.
5. Vous pouvez rechercher un nœud dans la liste **Disponible** ou dans la liste **Sélectionné**. Entrez les termes de la recherche dans le champ sous la liste, puis cliquez sur **Aller à**.
6. Si vous comptez créer une stratégie autorisant l'accès permanent aux nœuds de ce groupe, cochez la case **Créer une stratégie d'accès total pour le groupe**.
7. Lorsque l'ajout est terminé, cliquez sur **Ajouter** pour créer le groupe de nœuds. Le groupe est ajouté à la liste des groupes de nœuds à gauche.

Décrire les nœuds

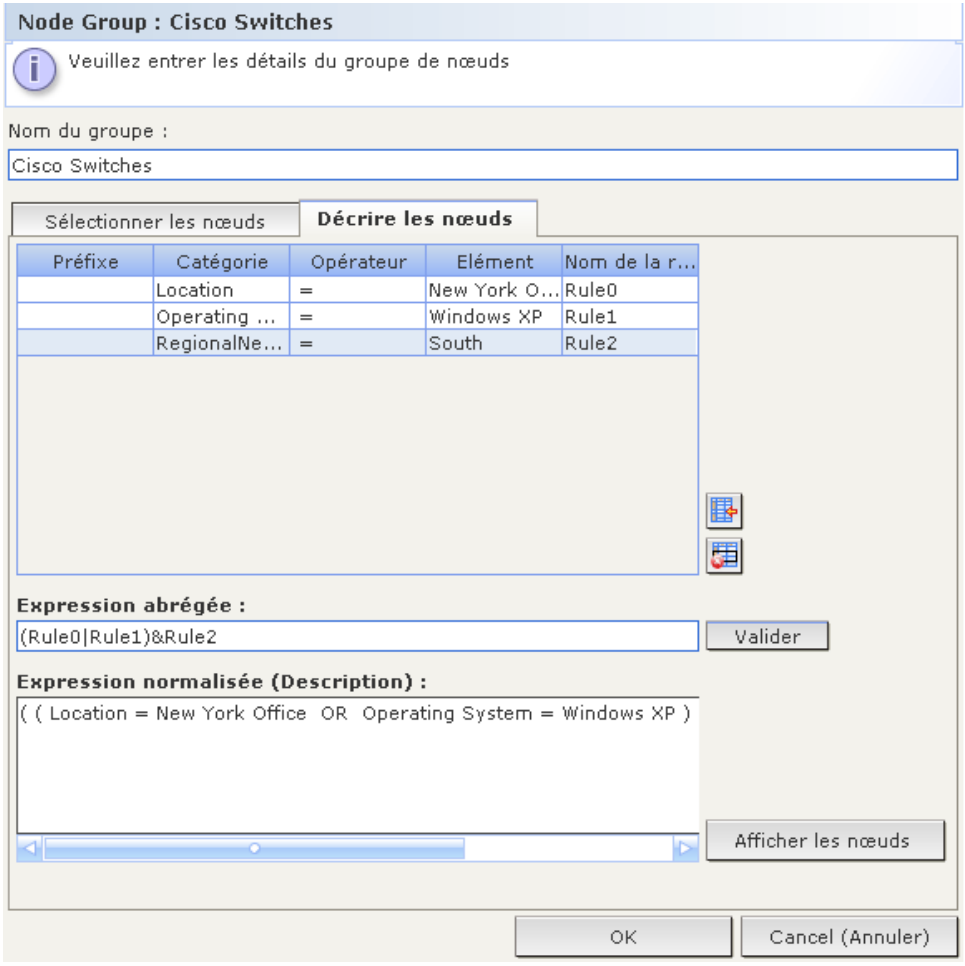

Figure 91 Décrire un groupe de nœuds avec plusieurs règles

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

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

4. Pour ajouter une autre règle, cliquez à nouveau sur **Ajouter une nouvelle ligne**, puis effectuez les configurations nécessaires. La configuration de plusieurs règles permettra des descriptions plus précises en fournissant des critères multiples d'évaluation des nœuds.
5. Si vous souhaitez retirer une règle, mettez-la en surbrillance dans la table, puis cliquez sur **Supprimer la ligne**.
6. 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.

   Par exemple : si vous souhaitez simplement décrire les nœuds appartenant au service technique, créez une règle indiquant `Service = Technique` ; elle deviendra Rule0. Il vous suffit ensuite d'entrer Rule0 dans le champ **Expression abrégée**.

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

7. 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**.
8. Cliquez sur **Afficher les nœuds** pour visualiser les nœuds satisfaisant l'expression. Une fenêtre **Nœuds du groupe de nœuds** apparaît présentant les nœuds groupés par l'expression en cours. Vous pouvez ainsi vérifier si la description est écrite correctement. Dans le cas contraire, vous pouvez retourner à la table des règles ou au champ **Expression abrégée** pour effectuer des modifications.
9. 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**.
10. Lorsque la description des nœuds appartenant au groupe est terminée, cliquez sur **Ajouter** pour créer le groupe de nœuds. Le groupe est ajouté à la liste des groupes de nœuds à gauche.

Modifier un groupe de nœuds

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

1. Dans le menu **Associations**, cliquez sur **Groupes de nœuds**. La fenêtre **Gestionnaire des groupes de nœuds** s'affiche.

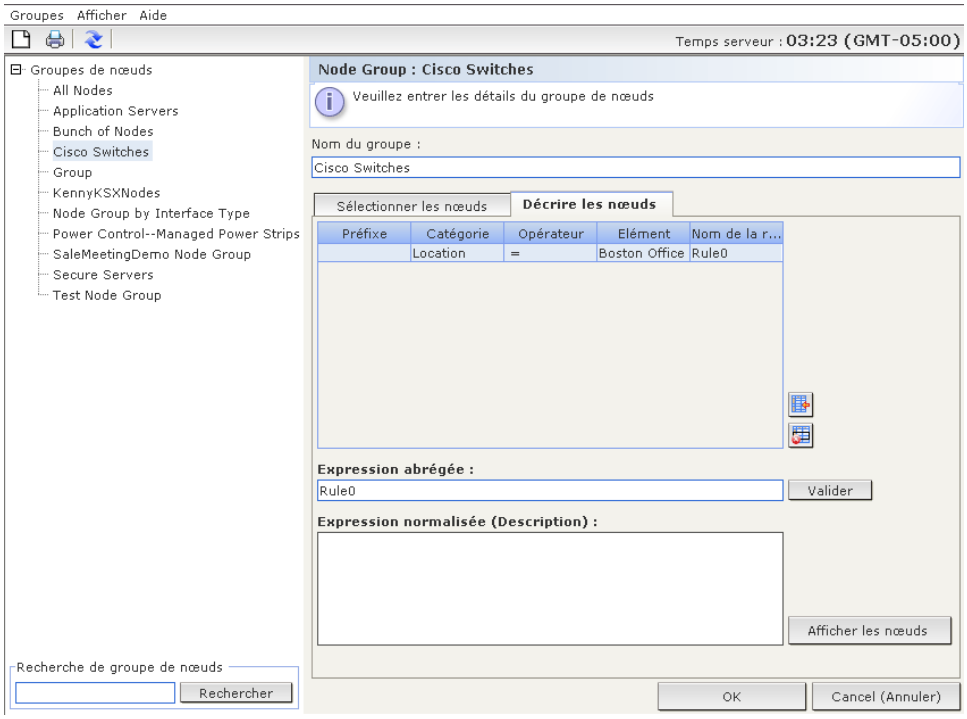

Figure 92 Modifier un groupe de nœuds

2. Dans la liste des groupes de nœuds à gauche, cliquez sur le nœud à modifier. Les informations relatives au nœud choisi s'affichent dans la fenêtre **Node Group** (groupe de nœuds).
3. Reportez-vous aux instructions des sections **Sélectionner les nœuds** et **Décrire les nœuds** ci-dessus pour plus d'informations sur la configuration d'un groupe de nœuds.
4. Cliquez sur **Modifier** lorsque la modification du groupe de nœuds est terminée.

Supprimer un groupe de nœuds

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

Groupes de dispositifs

Les groupes de dispositifs fonctionnent de la même manière que les groupes de nœuds, à la différence près qu'ils servent à organiser les dispositifs Raritan en ensembles qui seront gérés par des stratégies.

Reportez-vous au **Chapitre 5 : Ajout de dispositifs et de groupes de dispositifs, Gestionnaire des groupes de dispositifs** pour plus d'informations.

Gestionnaire des stratégies

Une fois vos groupes de nœuds et de dispositifs créés, ils peuvent servir de base à la création d'une stratégie d'accès : règle indiquant si les utilisateurs peuvent ou non accéder aux nœuds ou dispositifs du groupe (ou groupe de dispositifs), ainsi que les périodes où elle est en vigueur.

Ajouter une stratégie

Pour créer une stratégie :

1. Dans le menu **Associations**, cliquez sur **Stratégies**. La fenêtre **Gestionnaire des stratégies** s'affiche.

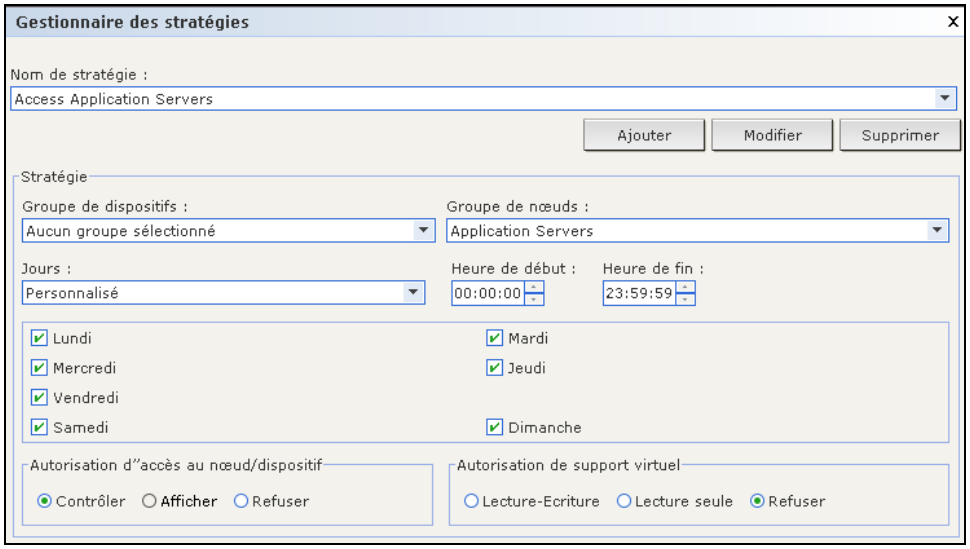

Figure 93 Gestionnaire des stratégies

2. Cliquez sur **Ajouter**. Une fenêtre de dialogue s'affiche vous demandant d'entrer un nom pour la stratégie.

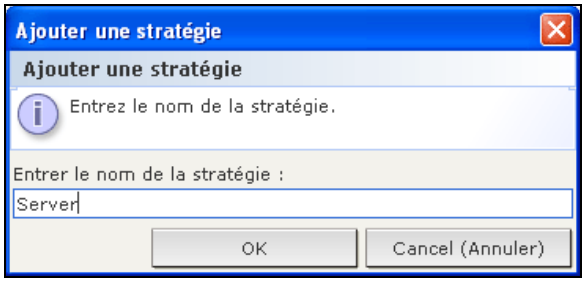

Figure 94 Ajouter une stratégie

3. Renseignez le champ **Entrer le nom de la stratégie**.
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 de dispositifs dont l'accès est régi par cette stratégie.
   Cliquez sur la flèche déroulante **Groupe de nœuds**, puis sélectionnez le groupe de nœuds dont l'accès est régi par cette stratégie.
   Si cette stratégie ne concerne qu'un type de groupe, ne sélectionnez qu'une valeur pour ce groupe.
6. 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).
   a. Sélectionnez **Personnalisé** pour choisir votre propre ensemble de jours. Les cases à cocher correspondant aux différents jours de la semaine sont alors activées.
   b. Cochez les cases correspondant aux jours concernés par cette stratégie.
7. 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.
8. Dans le champ **Heure de fin**, entrez l'heure à laquelle cette stratégie prend fin. L'heure saisie doit respecter le format 24 heures.
9. 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.
10. Cliquez sur **Mettre à jour** pour ajouter la nouvelle stratégie à CC-SG, puis cliquez sur **Oui** dans le message de confirmation qui apparaît.

Remarque : *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.*

Modifier une stratégie

Lorsque vous modifiez une stratégie, les changements n'affectent pas les utilisateurs connectés à CC-SG au moment de la modification. Ils prendront effet à la session suivante. Si vous souhaitez que vos changements prennent effet immédiatement, entrez en mode de maintenance, puis modifiez les stratégies. Lorsque vous entrez en mode de maintenance, tous les utilisateurs actuels sont déconnectés de CC-SG jusqu'à la sortie du mode de maintenance. Les utilisateurs peuvent alors se reconnecter. Reportez-vous au **Chapitre 11 : Maintenance du système, Mode de maintenance** pour plus d'informations.

Pour modifier une stratégie :

1. Dans le menu **Associations**, cliquez sur **Stratégies**. La fenêtre **Gestionnaire des stratégies** s'affiche.
2. Cliquez sur la flèche déroulante **Nom de stratégie**, puis choisissez dans la liste la stratégie à modifier.
3. Pour modifier le nom de la stratégie, cliquez sur **Modifier**. Une fenêtre **Modifier une stratégie** apparaît. Entrez un nouveau nom dans le champ, puis cliquez sur **OK** pour renommer la stratégie.
4. Cliquez sur la flèche déroulante **Groupe de dispositifs**, puis sélectionnez le groupe de dispositifs dont l'accès est régi par cette stratégie.
   Cliquez sur la flèche déroulante **Groupe de nœuds**, puis sélectionnez le groupe de nœuds dont l'accès est régi par cette stratégie.
   Si cette stratégie ne concerne qu'un type de groupe, ne sélectionnez qu'une valeur pour ce type.
5. 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).
   a. Sélectionnez **Personnalisé** pour choisir votre propre ensemble de jours. Les cases à cocher correspondant aux différents jours de la semaine sont alors activées.
   b. Cochez les cases correspondant aux jours concernés par cette stratégie.
6. 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.

7. Dans le champ **Heure de fin**, entrez l'heure à laquelle cette stratégie prend fin. L'heure saisie doit respecter le format 24 heures.
8. 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.
9. Si vous avez sélectionné **Contrôler** dans le champ **Autorisation d'accès au nœud/dispositif**, la section **Autorisation de support virtuel** est activée. Si vous souhaitez que cette stratégie permette l'**autorisation de support virtuel**, sélectionnez l'autorisation **Lecture-Ecriture** ou **Lecture seule**. Si vous souhaitez que cette stratégie interdise l'**autorisation de support virtuel**, sélectionnez **Refuser**.
10. Cliquez sur **Mettre à jour** pour enregistrer les modifications apportées à la stratégie, puis cliquez sur **Oui** dans le message de confirmation qui apparaît.

Supprimer une stratégie

Pour supprimer une stratégie :

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

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 au **Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs** pour plus d'informations sur l'affectation de stratégies à un groupe d'utilisateurs.

Chapitre 9 : Configuration de l'authentification à istance

Authentification et 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 autant de serveurs RADIUS, TACACS+ et LDAP distants que nécessaire pour l'authentification externe. Vous pouvez par exemple configurer trois serveurs AD, deux serveurs iPlanet (LDAP) et trois serveurs RADIUS.

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 locale 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 de 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. Pour plus d'informations sur l'ajout d'utilisateurs à authentifier à distance, reportez-vous au **Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs**.

***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 ND complet est décrit dans **RFC2253**. Dans le cadre de ce document, vous devez savoir comment entrer les noms distincts et la séquence de chacun de leurs composants dans la liste.

Les noms distincts pour AD suivent la structure ci-après. Il n'est pas obligatoire de définir à la fois un **nom courant** et une **unité organisationnelle** :

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

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

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

Nom d'utilisateur

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

ND 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**.

Configurations AD

Ajouter un module AD dans 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.

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 au Chapitre 12 : Gestionnaire de configuration pour plus d'informations.

Pour ajouter un module AD dans CC-SG :

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** apparaît, qui affiche l'onglet **Généralités**.
2. Cliquez sur **Ajouter…** pour ouvrir la fenêtre **Ajouter un module**.

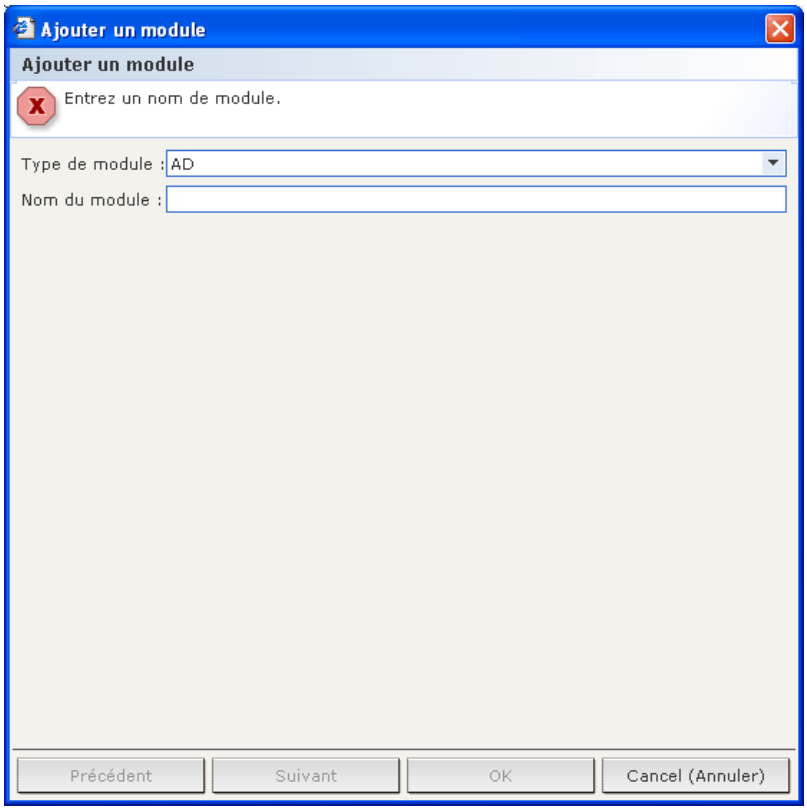

Figure 95 Ajouter un module

3. Cliquez sur le menu déroulant **Type de module** et sélectionnez AD dans la liste.
4. Entrez le nom du serveur AD dans le champ **Nom du module**. 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.
5. 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.

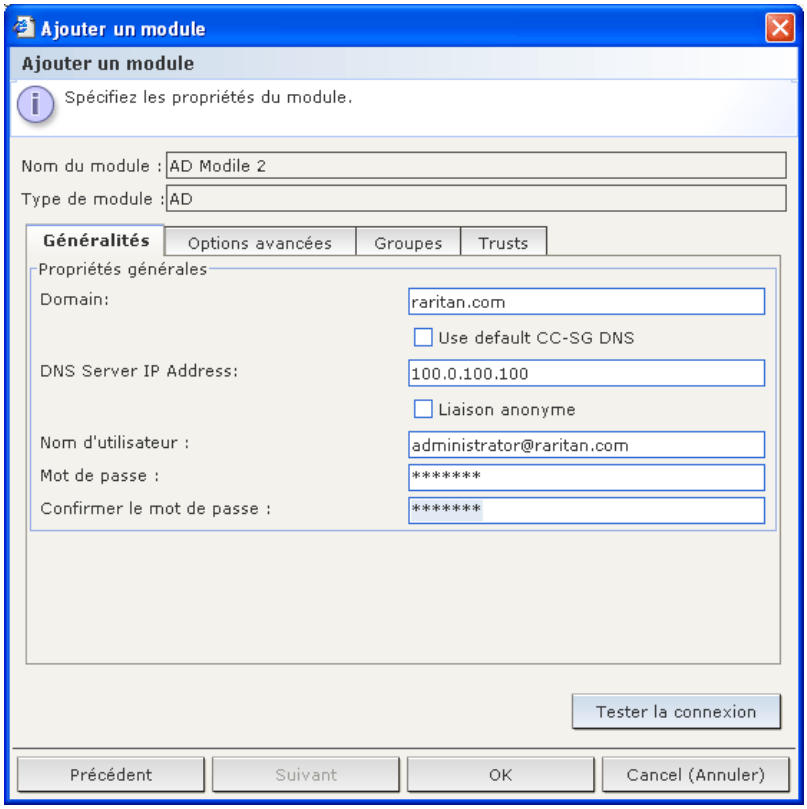

Figure 96 Paramètres généraux AD

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

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

2. Entrez l'adresse IP du serveur de noms de domaine dans le champ **DNS Server IP Address** (adresse IP du serveur DNS). Vous pouvez également cocher la case **Use default CC-SG DNS** (utiliser le serveur DNS CC-SG par défaut) afin d'utiliser le serveur de noms de domaine configuré dans la section Gestionnaire de configuration de CC-SG. Reportez-vous au **Chapitre 12 : Gestionnaire de configuration** pour plus d'informations.
3. Cochez la case **Liaison anonyme** si vous souhaitez vous connecter au serveur AD sans indiquer de nom d'utilisateur et de mot de passe. Dans ce cas, vérifiez si le serveur AD autorise les requêtes anonymes.

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

4. Si vous n'utilisez pas de liaison anonyme, entrez le nom d'utilisateur du compte utilisateur à l'aide duquel vous souhaitez interroger le serveur AD dans le champ **Nom d'utilisateur** au format suivant : **nomd'utilisateur@domaine.com**. L'utilisateur défini doit être autorisé à exécuter des requêtes de recherche dans le domaine AD. Par exemple, l'utilisateur doit appartenir à un groupe dans AD dont l'option **Group scope** (portée de groupe) est paramétrée sur **Global** et l'option **Group type** (type de groupe) sur **Security** (sécurité).

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

Paramètres avancés AD

1. Si vous souhaitez configurer des paramètres avancés, cliquez sur l'onglet **Options avancées**.

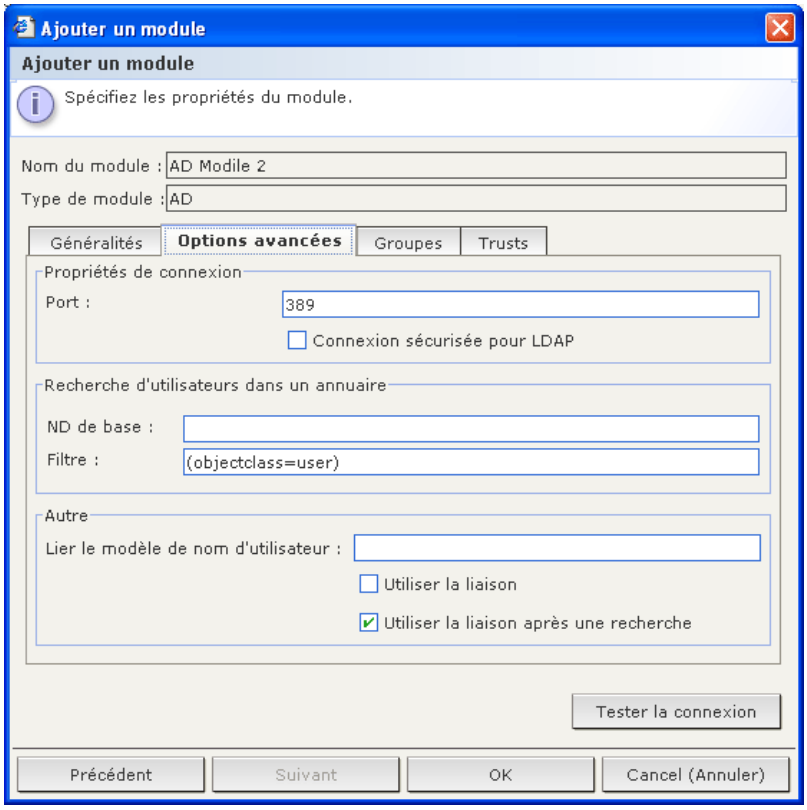

Figure 97 Paramètres avancés AD

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. Si vous cochez la case **Utiliser la liaison**, CC-SG tente de se connecter, ou de **se lier**, au serveur AD directement avec le nom d'utilisateur et le mot de passe fournis dans l'applet. 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.
   Par 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. Ne cochez la case **Utiliser la liaison** que si l'utilisateur se connectant à partir de l'applet est autorisé à effectuer des requêtes de recherche sur le serveur AD.
7. 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.
8. 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**.

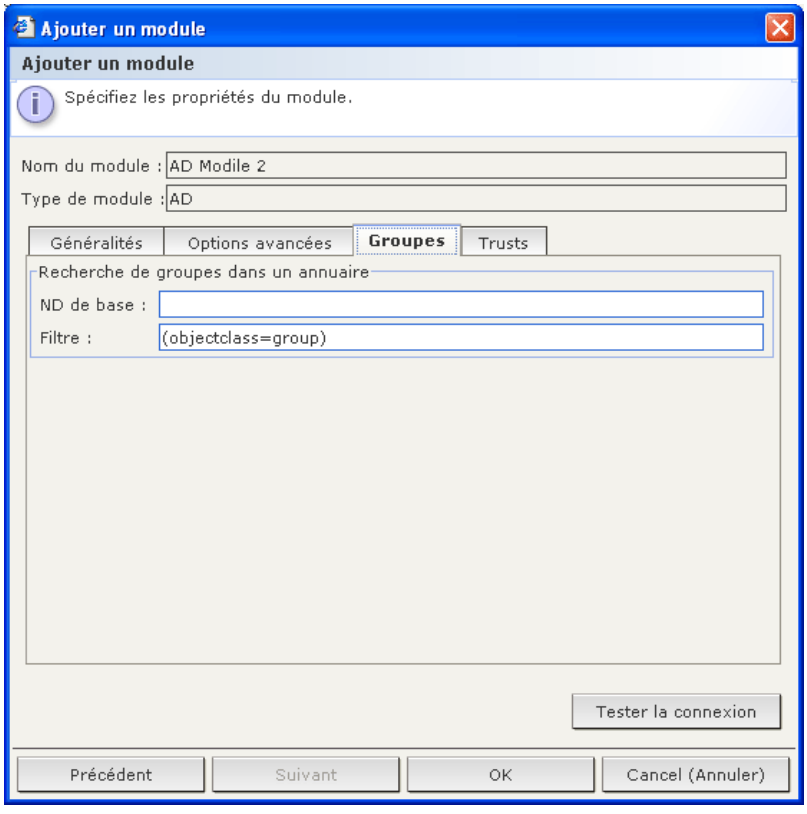

Figure 98 Paramètres de groupe AD

2. Spécifiez le **ND de base** (au niveau de l'annuaire) utilisé pour rechercher les groupes contenant l'utilisateur à autoriser.

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

3. Entrez les attributs de l'utilisateur dans le champ **Filtre** afin de limiter la recherche de l'utilisateur du groupe exclusivement aux entrées répondant à ces critères. Par exemple, si vous indiquez le ND de base **cn=Groups,dc=raritan,dc=com** et le filtre (**objectclass=group**), toutes les entrées de l'entrée **Groups** de type **group** sont retournées.
4. Cliquez sur **Suivant** pour continuer. L'onglet **Trusts** (approbations) s'ouvre.

Paramètres d'approbation AD

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

1. Cliquez sur l'onglet **Trusts** (approbations). Si vous avez configuré plusieurs domaines AD, tous les autres domaines sont affichés dans l'onglet **Trusts**.

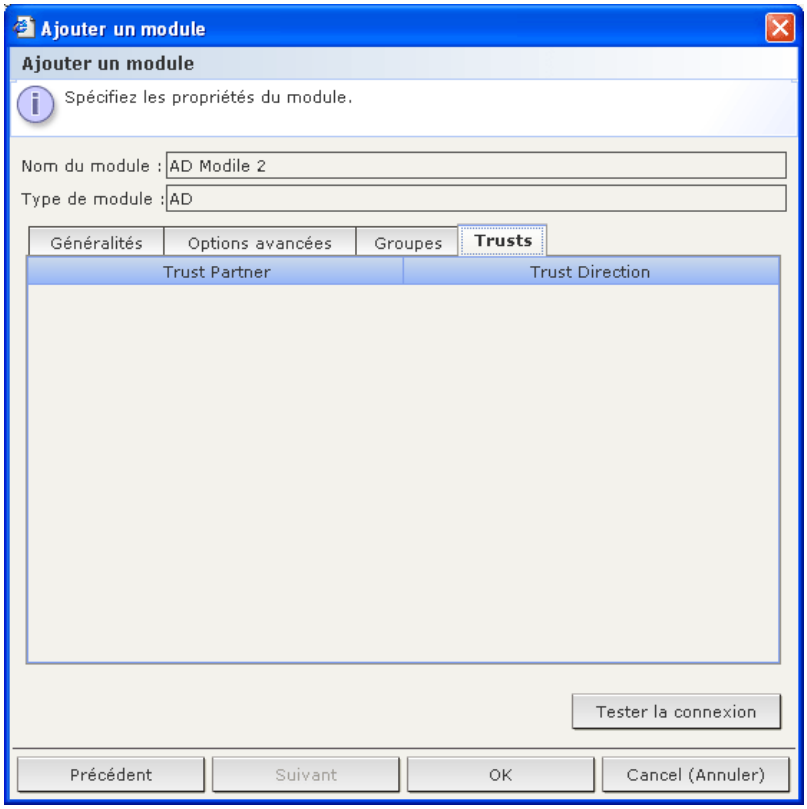

Figure 99 Paramètres d'approbation AD

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

Modifier les modules AD

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

1. Dans le menu **Administration**, cliquez sur **Sécurité**.
2. Sélectionnez le module AD que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Cliquez sur chaque onglet de la fenêtre **Modifier un module** pour visualiser les paramètres configurés. Effectuez les changements nécessaires. Reportez-vous aux sections précédentes **Paramètres généraux AD**, **Paramètres avancés AD**, **Paramètres de groupe AD** et **Paramètres d'approbation AD** pour plus d'informations.
4. 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.
5. Cliquez sur **OK** pour enregistrer les modifications. 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 les groupes d'utilisateurs AD** et **Synchroniser tous les modules AD** pour plus d'informations.

Importer les 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 104. Après avoir changé des groupes ou utilisateurs importés, vous devez synchroniser les groupes d'utilisateurs AD modifiés. Vous pouvez également synchroniser tous les modules AD pour en synchroniser tous les groupes et utilisateurs. Reportez-vous à **Synchroniser les groupes d'utilisateurs AD** et **Synchroniser tous les modules AD** pour plus d'informations.

***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 au **Chapitre 12 : Gestionnaire de configuration** pour plus d'informations.*

1. Dans le menu **Administration**, cliquez sur **Sécurité**.
2. Sélectionnez le module AD depuis lequel vous souhaitez importer des groupes d'utilisateurs AD.

3. 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.
4. Cochez les cases en regard des groupes à importer dans CC-SG. Cliquez sur un en-tête de colonne pour trier la liste des groupes d'utilisateurs selon les données de cette colonne. 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 **Sélectionner tout** pour choisir tous les groupes pour l'importation. Cliquez sur **Désélectionner tout** pour désélectionner tous les groupes d'utilisateurs choisis.
5. Dans la colonne **Stratégies**, cliquez sur le champ, puis choisissez une stratégie d'accès CC-SG dans la liste pour l'affecter au groupe sélectionné. Ces stratégies doivent déjà exister. Reportez-vous à **Chapitre 8 : Stratégies** pour plus d'informations.
6. Cliquez sur **Importer** pour importer les groupes d'utilisateurs sélectionnés.
7. Pour vérifier si le groupe a bien été importé et afficher les droits dont disposent ses membres, cliquez sur l'onglet **Utilisateurs**, puis sélectionnez le groupe en question pour ouvrir l'écran **Profil du groupe d'utilisateurs**. Vérifiez les informations des onglets **Droits d'administrateur** et **Stratégies de dispositif/nœud**. Cliquez sur l'onglet **Active Directory Associations** (associations Active Directory) pour consulter les informations relatives au module AD associé au groupe d'utilisateurs.

Synchroniser les groupes d'utilisateurs AD

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 importés d'AD, puis identifie les paires identiques. CC-SG présente ces dernières et vous permet de sélectionner les groupes à importer. Ainsi, CC-SG importe les données de groupes d'utilisateurs AD les plus récentes. De plus, il synchronise automatiquement tous les modules AD une fois par jour. Reportez-vous à **Définir l'heure de synchronisation AD**, ci-après, pour plus d'informations.

1. Dans le menu **Administration**, cliquez sur **Sécurité**.
2. Sélectionnez le module AD dont vous souhaitez synchroniser les groupes d'utilisateurs avec le serveur AD.
3. Cliquez sur **Synchronize AD User Groups** (synchroniser les groupes d'utilisateurs AD).
4. Un message de confirmation s'affiche lorsque tous les groupes d'utilisateurs importés dans le module sélectionné sont synchronisés.

Synchroniser tous les modules AD

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, puis rafraîchit la mémoire cache locale de CC-SG. Cette dernière contient tous les contrôleurs de chaque domaine, les groupes d'utilisateurs de tous les modules et les données de tous les utilisateurs AD connus. Si des groupes d'utilisateurs ont été supprimés des modules AD, CC-SG les retire également de sa mémoire cache locale. Ainsi, CC-SG dispose des données de groupes d'utilisateurs AD les plus récentes.

1. Vous devez passer en mode de maintenance avant de pouvoir synchroniser tous les modules AD. Tous les utilisateurs seront déconnectés de CC-SG quand celui-ci sera en mode de maintenance. Dans le menu **Maintenance du système**, cliquez sur **Mode de maintenance**, puis sur **Entrer en mode de maintenance**.
2. Dans les champs correspondants de l'écran **Entrer en mode de maintenance**, tapez le message qui apparaîtra aux utilisateurs qui vont être déconnectés de CC-SG, et le nombre de minutes devant s'écouler avant le passage en mode de maintenance, puis cliquez sur **OK**.
3. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

4. Un second message de confirmation apparaîtra lorsque CC-SG passera en mode de maintenance. Cliquez sur **OK**.
5. Lorsque CC-SG est en mode de maintenance, dans le menu **Administration**, cliquez sur **Sécurité**.
6. Cliquez sur **Synchronize all AD Modules** (synchroniser tous les modules AD).

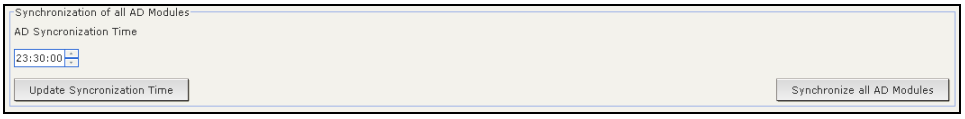

Figure 100 Synchronisation de tous les modules AD

7. Un message de confirmation apparaît lorsque tous les modules AD sont synchronisés.
8. Pour quitter le mode de maintenance, dans le menu **Maintenance du système**, cliquez sur **Mode de maintenance**, puis sur **Quitter le mode de maintenance**.
9. Dans l'écran qui s'affiche, cliquez sur **OK**. Un second message de confirmation apparaîtra lorsque CC-SG quittera le mode de maintenance. Cliquez sur **OK**.

Définir l'heure de synchronisation AD

Par défaut, CC-SG synchronise tous les modules AD configurés chaque jour à 23h30. Vous pouvez modifier l'heure à laquelle cette synchronisation automatique se produit.

1. Dans le menu **Administration**, cliquez sur **Sécurité**.
2. Dans le champ **AD Synchronization Time** (heure de synchronisation AD) 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.

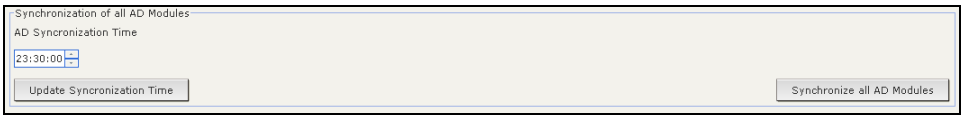

Figure 101 Synchronisation de tous les modules AD

3. Cliquez sur **Update Synchronization Time** (mettre à jour l'heure de synchronisation) pour enregistrer vos modifications.

Configuration AD — Mettre à niveau à partir de CC-SG 3.0.2

Si vous avez effectué la mise à niveau de CC-SG de la version 3.0.2 à la version 3.1, vous devez reconfigurer vos modules AD avant que vos utilisateurs AD ne puissent se connecter à CC-SG. CC-SG 3.1 requiert la définition d'un serveur de noms de domaine et d'un nom de domaine pour chaque module AD. Cette configuration permet à CC-SG de rechercher un domaine particulier dans tous les contrôleurs de domaine.

Important : CC-SG sera toujours en mode de maintenance après la mise à niveau vers 3.1. Vous devez donc vous connecter à l'aide du compte CC Super-User pour effectuer cette opération. Le compte CC Super-User par défaut pour la mise à niveau de systèmes à partir de 3.0.2 est ccroot/raritan0.

Pour reconfigurer les modules AD :

1. Dans le menu **Administration**, cliquez sur **Sécurité**.
2. Sélectionnez le module AD que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Dans l'onglet **Généralités**, entrez le serveur de noms de domaine et le nom de domaine pour le module AD dans les champs correspondants. Reportez-vous à **Paramètres généraux AD** pour plus d'informations.

4. 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.
5. Cliquez sur **OK** pour enregistrer les modifications.
6. Si vous souhaitez configurer les paramètres avancés, de groupe ou d'approbation, cliquez sur l'onglet correspondant pour afficher les options. Reportez-vous aux sections précédentes **Paramètres avancés AD**, **Paramètres de groupe AD** et **Paramètres d'approbation AD** pour plus d'informations. Cliquez sur **OK** pour enregistrer les modifications dans ces onglets.
7. Répétez ces étapes pour reconfigurer tous les modules AD.
8. Lorsque vous avez reconfiguré tous les modules AD, vous pouvez synchroniser vos groupes d'utilisateurs AD importés avec les serveurs AD. Reportez-vous à **Synchroniser les groupes d'utilisateurs AD** pour plus d'informations.
9. Après avoir synchronisé les groupes d'utilisateurs AD de tous les modules, vous devez synchroniser tous les modules AD. Reportez-vous à **Synchroniser tous les modules AD** pour plus d'informations. Suivant votre configuration AD, la synchronisation peut prendre jusqu'à 30 secondes par contrôleur de domaine. Si des contrôleurs de domaine sont hors ligne pendant la synchronisation, l'opération peut durer plus longtemps.

***Remarque** : reportez-vous aux sections ci-après pour vous familiariser avec la synchronisation des groupes d'utilisateurs AD dans CC-SG 3.1 : **Synchroniser tous les modules AD** et **Définir l'heure de synchronisation AD**. Pour des instructions concernant la génération d'un rapport contenant des informations relatives aux groupes d'utilisateurs AD, reportez-vous au **Chapitre 10 : Génération de rapports, Rapport sur le groupe d'utilisateurs AD**.*

Ajout d'un module LDAP (Netscape) dans 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.

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** apparaît, qui affiche l'onglet **Généralités**.
2. Cliquez sur **Ajouter…** pour ouvrir la fenêtre **Ajouter un module**.

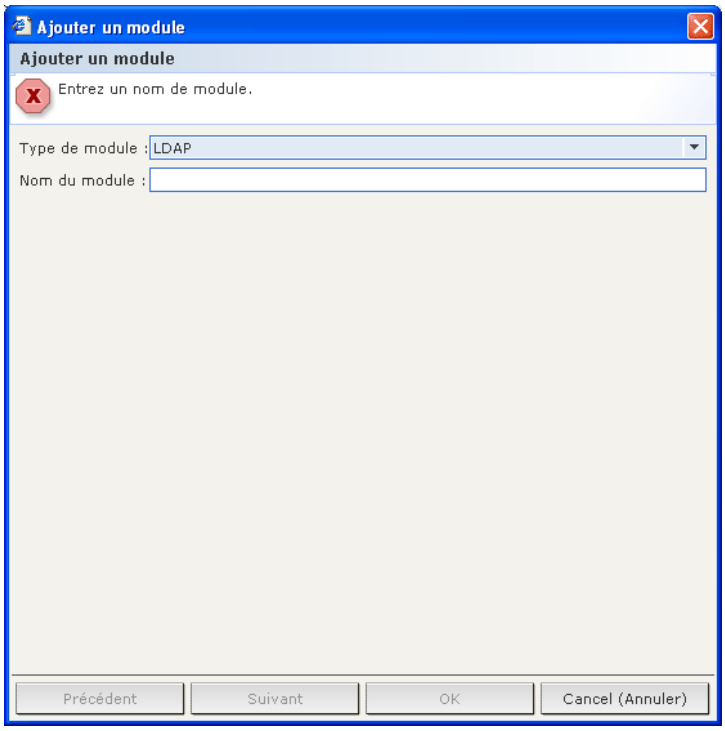

Figure 102 Ajouter un module LDAP

3. Cliquez sur le menu déroulant **Type de module** et sélectionnez LDAP dans la liste.
4. Entrez le nom du serveur LDAP dans le champ **Nom du module**.
5. Cliquez sur **Suivant** pour continuer. L'onglet **Généralités** s'ouvre.

Paramètres généraux LDAP

1. Cliquez sur l'onglet **Généralités**.

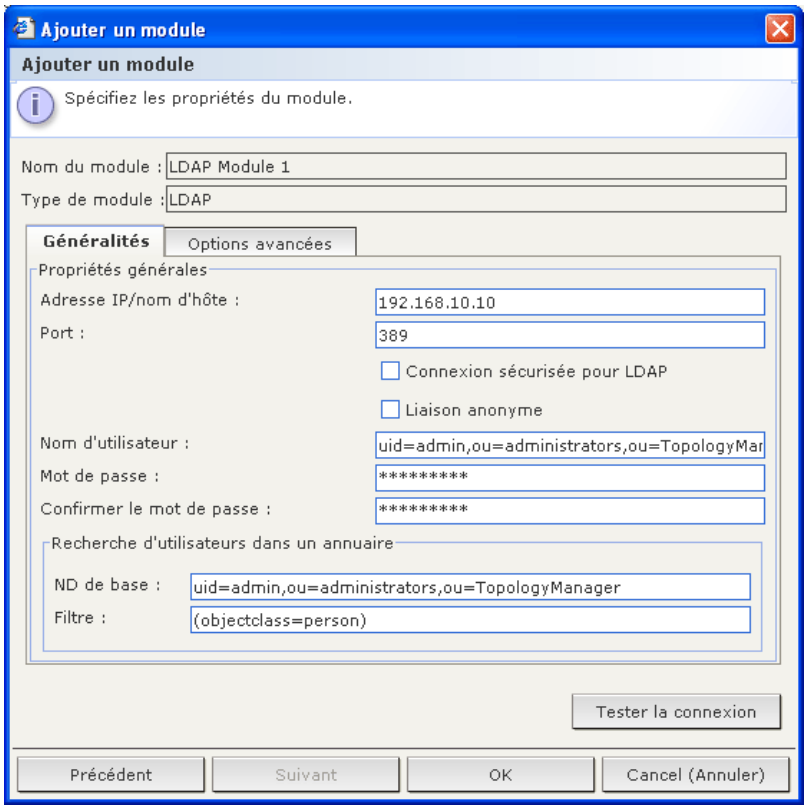

Figure 103 Paramètres généraux LDAP

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 et sigles** dans le **Chapitre 1 : Introduction**.
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 même 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**.

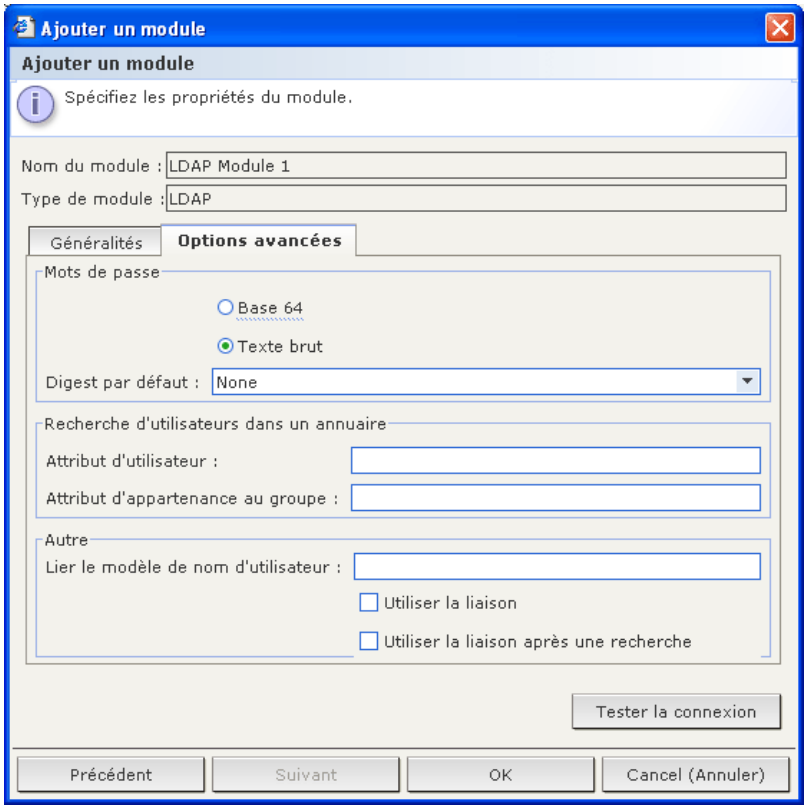

Figure 104 Paramètres avancés LDAP

2. Cliquez sur la case d'option **Base 64** pour envoyer le mot de passe au serveur LDAP avec chiffrement. Cliquez sur la case d'option **Texte brut** pour envoyer le mot de passe au serveur LDAP sous forme de texte brut.
3. Cliquez sur le menu déroulant **Digest par défaut** et sélectionnez le mode de 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**.
6. 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.
7. 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.
8. Cliquez sur **OK** pour enregistrer les 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**

Paramètres de certificat LDAP

Les paramètres de certificat LDAP permettent de télécharger un certificat LDAP. Vous pouvez également accepter ou refuser des certificats téléchargés.

1. Cliquez sur l'onglet **Options avancées**.
2. Cliquez sur **Parcourir**, accédez au fichier du certificat que vous souhaitez télécharger et cliquez sur **Ouvrir**.
3. Cliquez sur **Accepter** pour accepter le certificat comme approuvé par CC-SG. Cliquez sur **Refuser** pour retirer le certificat.
4. Si vous souhaitez supprimer un certificat, sélectionnez-le, puis cliquez sur **Supprimer**.
5. Cliquez sur **OK** pour enregistrer les modifications.

Ajout d'un module TACACS+

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. Pour plus d'informations sur l'ajout d'utilisateurs à authentifier à distance, reportez-vous au **Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs**.

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** apparaît, qui affiche l'onglet **Généralités**.
2. Cliquez sur **Ajouter…** pour ouvrir la fenêtre **Ajouter un module**.

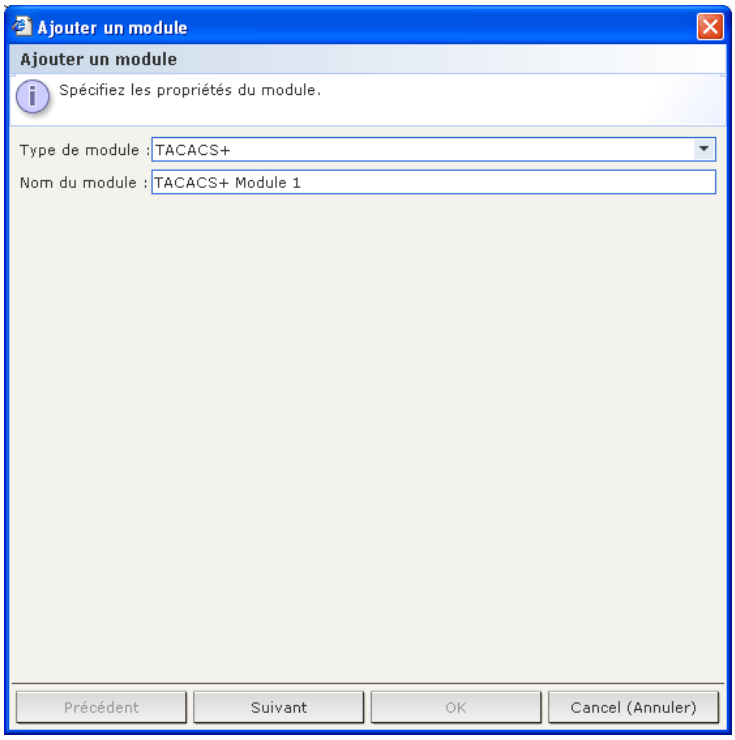

Figure 105 Ajouter un module TACACS+

3. Cliquez sur le menu déroulant **Type de module** et sélectionnez TACACS+ dans la liste.
4. Entrez le nom du serveur TACACS+ dans le champ **Nom du module**.
5. Cliquez sur **Suivant** pour continuer. 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 et sigles dans le Chapitre 1 : Introduction.

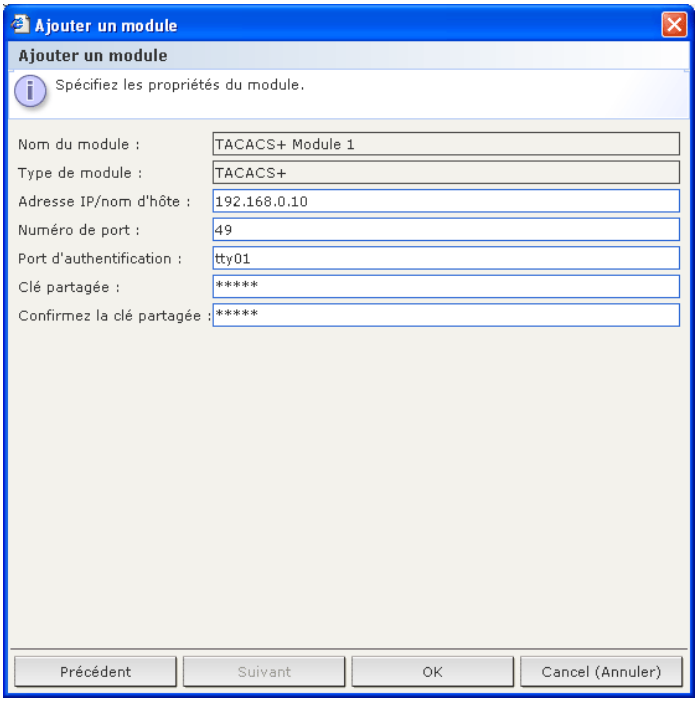

Figure 106 Paramètres généraux TACACS+

2. Entrez le numéro du port d'écoute du serveur TACACS+ dans le champ **Numéro de port**. Le numéro de port par défaut est **49**.
3. Entrez le port d'authentification dans le champ **Port d'authentification**.
4. Renseignez les champs **Clé partagée** et **Confirmez la clé partagée**.
5. Cliquez sur **OK** pour enregistrer les modifications.

Ajout d'un module RADIUS

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. Pour plus d'informations sur l'ajout d'utilisateurs à authentifier à distance, reportez-vous au **Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs**.

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** apparaît, qui affiche l'onglet **Généralités**.
2. Cliquez sur **Ajouter…** pour ouvrir la fenêtre **Ajouter un module**.

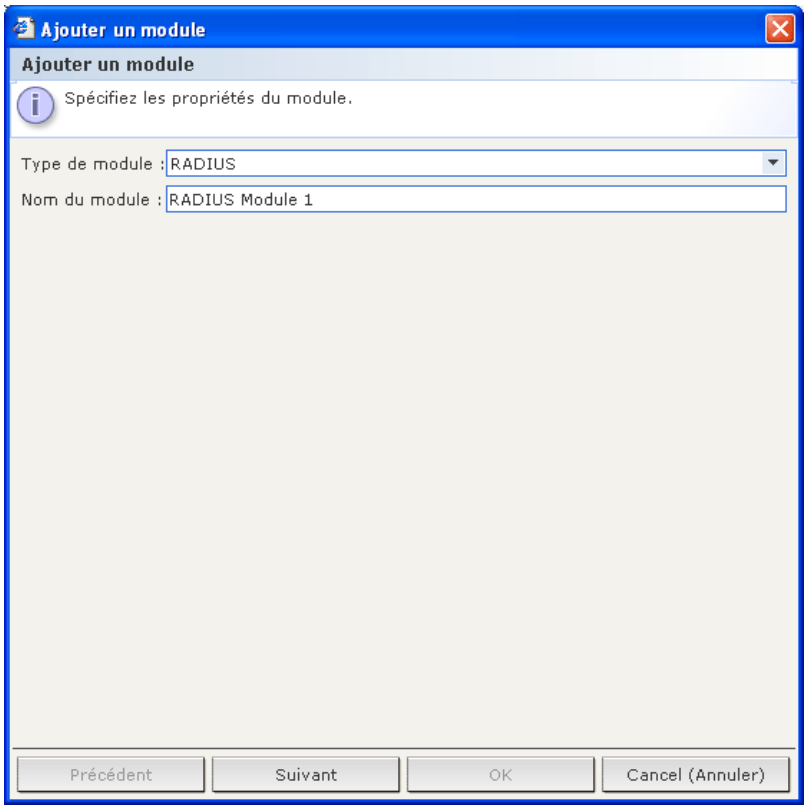

Figure 107 Ecran Ajouter un module du Gestionnaire de sécurité

3. Cliquez sur le menu déroulant **Type de module** et sélectionnez RADIUS dans la liste.
4. Entrez le nom du serveur RADIUS dans le champ **Nom du module**.
5. Cliquez sur **Suivant** pour continuer. L'onglet **Généralités** s'ouvre.

Paramètres généraux RADIUS

1. Cliquez sur l'onglet **Généralités**.

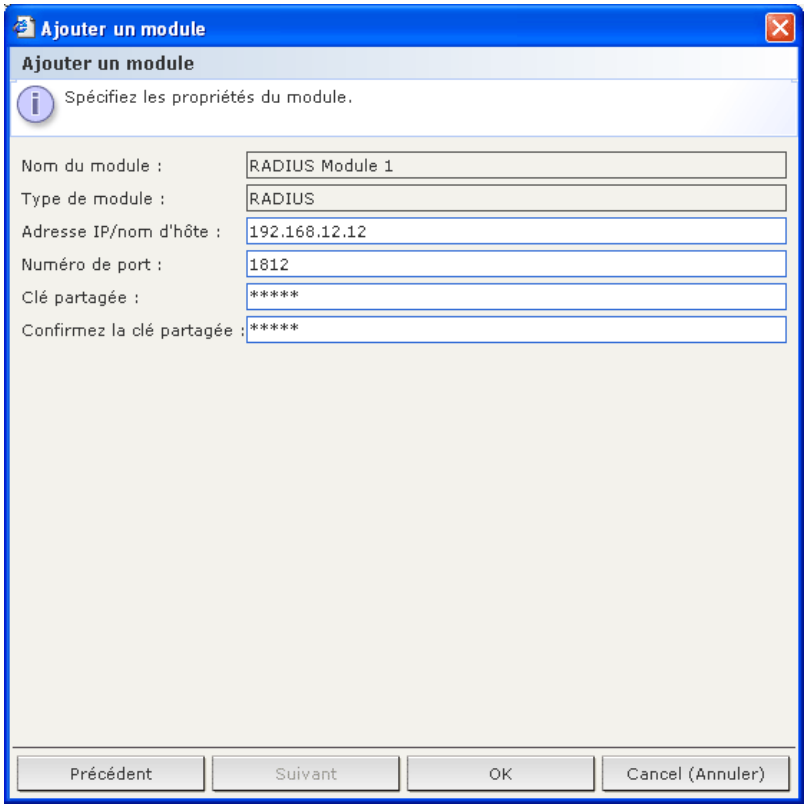

Figure 108 Définition d'un serveur RADIUS

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 et sigles** dans le **Chapitre 1 : Introduction**.
3. Entrez le numéro de port dans le champ **Numéro de port**. Le numéro de port par défaut est **1812**.
4. Entrez le port d'authentification dans le champ **Port d'authentification**.
5. Renseignez les champs **Clé partagée** et **Confirmez la clé partagée**.
6. Cliquez sur **OK** pour enregistrer les modifications.

Authentification à deux facteurs à l'aide de RADIUS

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

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

La configuration du serveur RADIUS et du gestionnaire d'authentification permettant cette opération ne fait pas partie de l'objectif de ce document. La configuration de CC-SG est identique à l'authentification distante RADIUS standard décrite plus haut. CC-SG doit être configuré de manière à pointer vers le serveur RADIUS. Reportez-vous à l'**annexe G : Authentification à deux facteurs** pour plus d'informations.

Définition des modules pour l'authentification et l'autorisation

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

1. Dans le menu **Administration**, cliquez sur **Sécurité**. Lorsque l'écran **Gestionnaire de sécurité** s'affiche, cliquez sur l'onglet **Généralités**. Tous les serveurs externes d'authentification et d'autorisation configurés s'affichent dans la section **Serveurs AA externes**.
2. Pour chaque serveur, cochez la case **Authentification** si vous souhaitez que CC-SG utilise le serveur pour l'authentification des utilisateurs.
3. Pour chaque serveur, 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

Dans l'onglet **Généralités**, vous pouvez définir l'ordre dans lequel CC-SG interroge les serveurs AA externes configurés. 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.

1. Dans le menu **Administration**, cliquez sur **Sécurité**. Lorsque l'écran **Gestionnaire de sécurité** s'affiche, cliquez sur l'onglet **Généralités**.

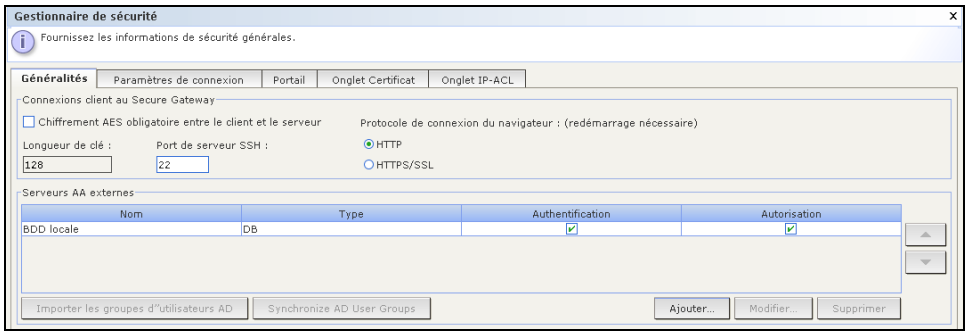

Figure 109 Onglet Généralités de l'écran Gestionnaire de sécurité

2. La section **Serveurs AA externes** répertorie toutes les options d'authentification et d'autorisation disponibles dans CC-SG. Sélectionnez un nom dans cette liste, puis cliquez sur les flèches haut et bas pour définir la priorité de la séquence d'engagement.
3. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Chapitre 10 : Génération de rapports

Les rapports peuvent être triés en cliquant sur les en-têtes de colonne. 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.

Vous pouvez redimensionner la largeur des colonnes dans tous les rapports. 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. Cliquez et faites glisser la flèche vers la gauche ou la droite pour changer la largeur des colonnes.

Le paramètre de tri et la largeur des colonnes utilisés constituent la vue par défaut du rapport que vous afficherez la prochaine fois que vous vous connecterez et exécuterez des rapports CC-SG. Pour afficher des détails supplémentaires sur un rapport, vous pouvez double-cliquer sur une ligne.

***Remarque** : dans tous les rapports, utilisez CTRL+clic pour désélectionner une ligne mise en surbrillance.*

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

1. Dans le menu **Rapports**, cliquez sur **Journal d'audit**. L'écran **Journal d'audit** s'affiche.

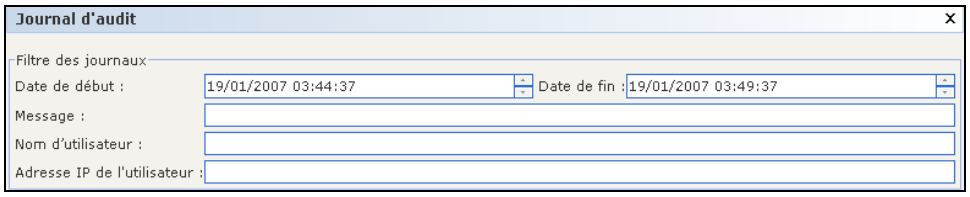

Figure 110 Ecran Journal d'audit

2. Définissez la période couverte par le rapport dans les champs **Date de début** et **Date de fin**. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
3. Vous pouvez limiter les données contenues dans le rapport en renseignant les champs **Message**, **Nom d'utilisateur** et **Adresse IP de l'utilisateur**.

- Pour limiter le rapport en fonction du texte du message associé à une activité, renseignez le champ **Message**.
- Pour limiter le rapport aux activités d'un utilisateur particulier, entrez le nom de ce dernier dans le champ **Nom d'utilisateur**.
- Pour limiter le rapport aux activités d'une adresse IP particulière, entrez l'adresse IP de l'utilisateur dans le champ **Adresse IP de l'utilisateur**.

4. Cliquez sur **OK** pour créer le rapport. Celui-ci est généré. Les données relatives aux activités de la période indiquée et répondant aux paramètres supplémentaires spécifiés s'affichent.

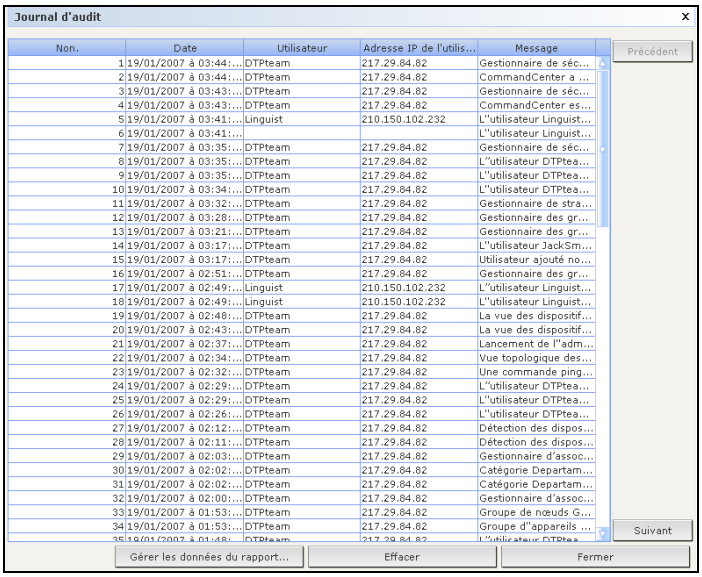

Figure 111 Rapport Journal d'audit

- Cliquez sur **Suivant** ou **Précédent** pour parcourir les pages du rapport.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Effacer** pour effacer les fichiers journaux utilisés dans le rapport.
- Cliquez sur **Fermer** pour fermer le rapport.

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.

1. Dans le menu **Rapports**, cliquez sur **Journal d'erreurs**. L'écran **Journal d'erreurs** s'affiche.

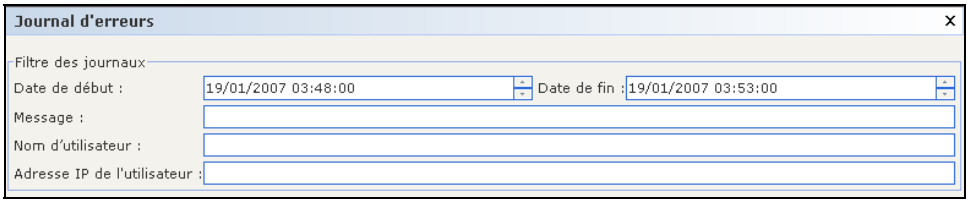

Figure 112 Ecran Journal d'erreurs

2. Définissez la période couverte par le rapport dans les champs **Date de début** et **Date de fin**. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
3. Vous pouvez limiter les données contenues dans le rapport en renseignant les champs **Message**, **Nom d'utilisateur** et **Adresse IP de l'utilisateur**.

- Pour limiter le rapport en fonction du texte du message associé à une activité, renseignez le champ **Message**.

- Pour limiter le rapport aux activités d'un utilisateur particulier, entrez le nom de ce dernier dans le champ **Nom d'utilisateur**.
- Pour limiter le rapport aux activités d'une adresse IP particulière, entrez l'adresse IP de l'utilisateur dans le champ **Adresse IP de l'utilisateur**.

4. Cliquez sur **OK** pour créer le rapport. Celui-ci est généré. Les données relatives aux activités de la période indiquée et répondant aux paramètres supplémentaires spécifiés s'affichent.

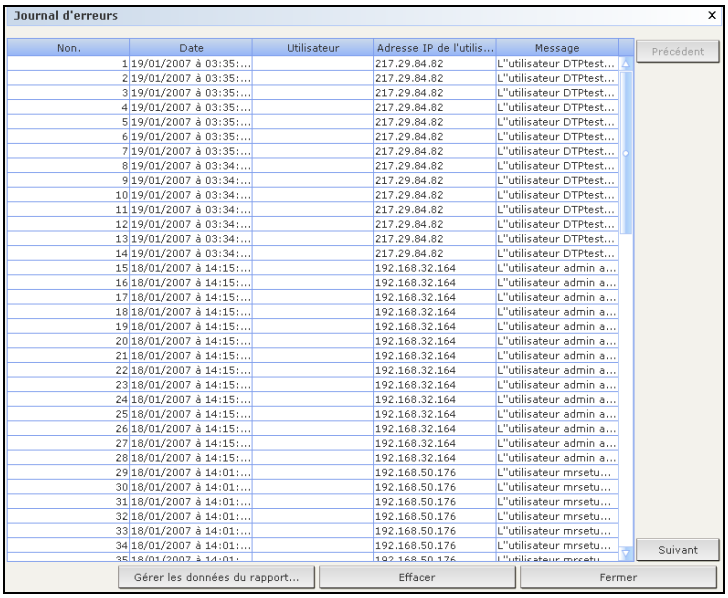

Figure 113 Rapport Journal d'erreurs

- Cliquez sur **Suivant** ou **Précédent** pour parcourir les pages du rapport.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Effacer** pour effacer les fichiers journaux utilisés dans le rapport.
- Cliquez sur **Fermer** pour fermer le rapport.

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).

1. Dans le menu **Rapports**, cliquez sur **Rapport d'accès**. L'écran **Rapport d'accès** s'affiche.

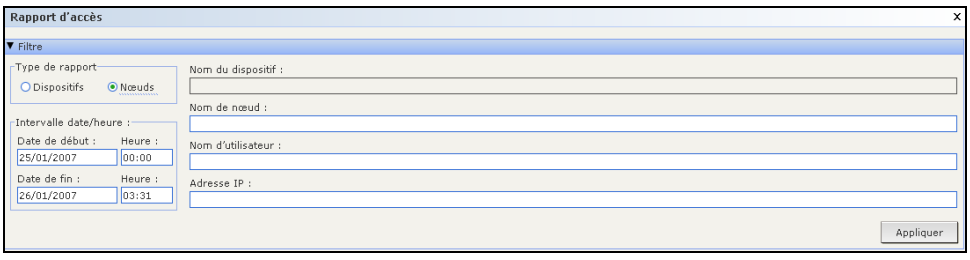

Figure 114 Ecran Rapport d'accès

2. Définissez la période couverte par le rapport dans les champs **Date de début** et **Date de fin**. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.

3. Vous pouvez limiter les données contenues dans le rapport en renseignant les champs **Message**, **Nom du dispositif**, **Nom du port**, **Nom d'utilisateur** et **Adresse IP de l'utilisateur**.

- Pour limiter le rapport en fonction du texte du message associé à une activité, renseignez le champ **Message**.
- Pour limiter le rapport à un dispositif particulier, renseignez le champ **Nom du dispositif**.
- Pour limiter le rapport à un port particulier, renseignez le champ **Nom du port**.
- Pour limiter le rapport aux activités d'un utilisateur particulier, entrez le nom de ce dernier dans le champ **Nom d'utilisateur**.
- Pour limiter le rapport aux activités d'une adresse IP particulière, entrez l'adresse IP de l'utilisateur dans le champ **Adresse IP de l'utilisateur**.

4. Cliquez sur **OK** pour créer le rapport. Celui-ci est généré. Les données relatives aux accès effectués pendant la période indiquée et répondant aux paramètres supplémentaires spécifiés s'affichent.

Nœud	Dispositif	Date/Heure	Interface	Type	Nom d"utilisateur	Adresse IP de l'utilisateur
Admin	Kenny-KSX440	26/01/2007 à 03:28:14 ...	Admin	Out-of-Band - Serial	DTPteam	217.29.84.82
Admin	Kenny-KSX440	26/01/2007 à 03:27:08 ...	Admin	Out-of-Band - Serial	DTPteam	217.29.84.82
Admin	Kenny-KSX440	26/01/2007 à 03:25:44 ...	Admin	Out-of-Band - Serial	DTPteam	217.29.84.82
Admin	Kenny-KSX440	26/01/2007 à 03:16:20 ...	Admin	Out-of-Band - Serial	DTPteam	217.29.84.82
Admin	Kenny-KSX440	26/01/2007 à 03:15:54 ...	Admin	Out-of-Band - Serial	DTPteam	217.29.84.82
Admin	Kenny-KSX440	26/01/2007 à 03:15:13 ...	Admin	Out-of-Band - Serial	DTPteam	217.29.84.82
Admin	Kenny-KSX440	26/01/2007 à 03:13:01 ...	Admin	Out-of-Band - Serial	DTPteam	217.29.84.82
Admin	Kenny-KSX440	26/01/2007 à 03:12:19 ...	Admin	Out-of-Band - Serial	DTPteam	217.29.84.82
Admin	Kenny-KSX440	26/01/2007 à 02:38:52 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	26/01/2007 à 02:38:52 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	26/01/2007 à 02:32:43 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 20:14:10 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 20:12:21 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 20:07:50 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
HP Server 364	Kenny-KSX440	25/01/2007 à 16:18:32 ...	KVM Target 1	Out-of-Band - KVM	admin	192.168.50.130
HP Server 364	Kenny-KSX440	25/01/2007 à 16:18:31 ...	KVM Target 1	Out-of-Band - KVM	admin	192.168.50.130
HP Server 364	Kenny-KSX440	25/01/2007 à 16:18:28 ...	KVM Target 1	Out-of-Band - KVM	admin	192.168.50.130
RemoKSX440C	P2SC-3260	25/01/2007 à 13:45:46 ...	RemoKSX440C	Out-of-Band - KVM	admin	192.168.51.161
RemoKSX440C	P2SC-3260	25/01/2007 à 13:45:31 ...	RemoKSX440C	Out-of-Band - KVM	admin	192.168.51.161
RemoKSX440C	P2SC-3260	25/01/2007 à 13:45:27 ...	RemoKSX440C	Out-of-Band - KVM	admin	192.168.51.161
Admin	Kenny-KSX440	25/01/2007 à 06:54:14 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 06:54:14 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 06:46:42 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 06:14:11 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 06:06:49 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 06:03:49 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 05:49:38 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KSX440	25/01/2007 à 05:48:25 ...	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
HP Server 364	Kenny-KSX440	25/01/2007 à 05:44:14 ...	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112
HP Server 364	Kenny-KSX440	25/01/2007 à 05:44:14 ...	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112

Gérer les données du rapport... Cancel (Annuler)

Figure 115 Rapport d'accès

- Cliquez sur **Suivant** ou **Précédent** pour parcourir les pages du rapport.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Effacer** pour effacer les fichiers journaux utilisés dans le rapport.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport de disponibilité

Le rapport de disponibilité affiche l'état de toutes les connexions, en répertoriant les dispositifs par nom et adresse IP. Ce rapport permet de visualiser, sur une vue unique, tous les dispositifs de votre système et vous fournit des informations qui peuvent être utiles en cas de dépannage.

1. Dans le menu **Rapports**, cliquez sur **Rapport de disponibilité**. Le **rapport de disponibilité** est généré.

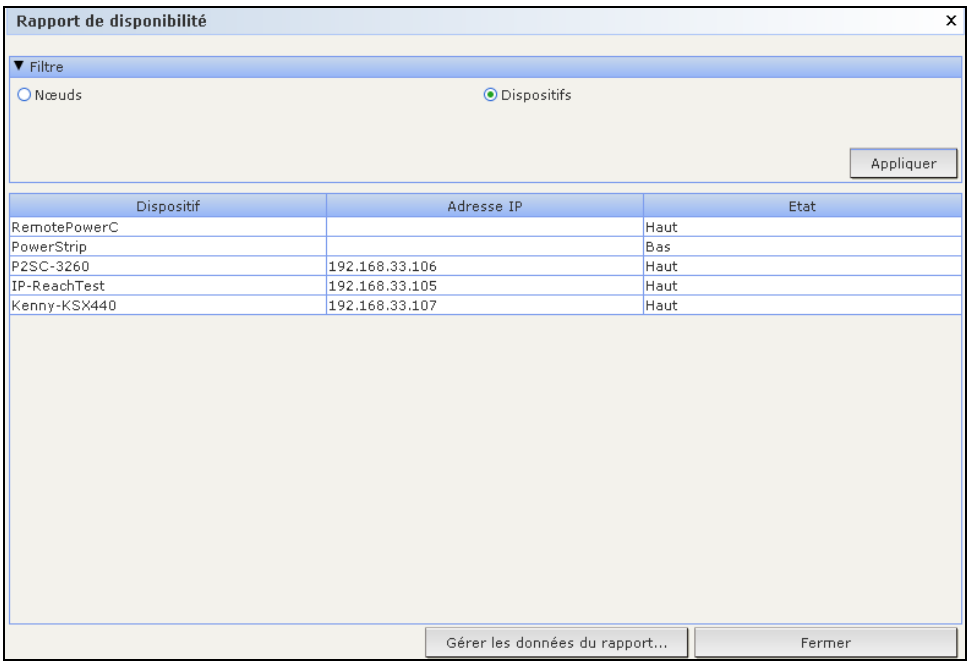

Figure 116 Rapport de disponibilité

- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport Utilisateurs actifs

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

1. Dans le menu **Rapports**, cliquez sur **Utilisateurs**, puis sur **Utilisateurs actifs**. Le rapport **Utilisateurs actifs** est généré.

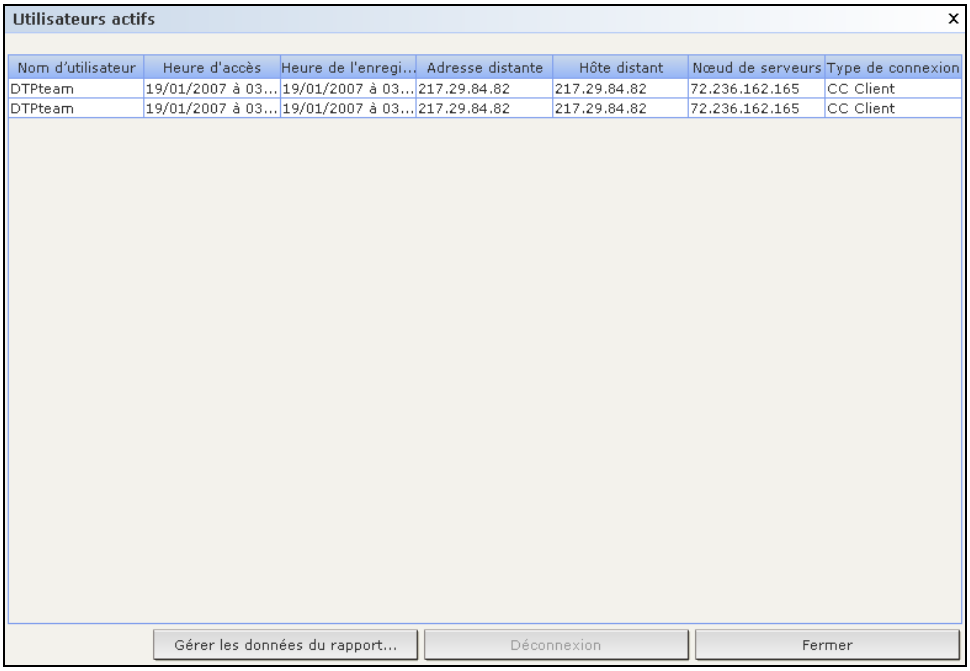

Figure 117 Rapport Utilisateurs actifs

- Pour déconnecter un utilisateur d'une session active de CC-SG, sélectionnez son nom, puis cliquez sur **Déconnexion**.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

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 **Chapitre 12 : Administration avancée, Paramètres de verrouillage** pour plus d'informations sur les paramètres de verrouillage.

1. Dans le menu **Rapports**, cliquez sur **Utilisateurs**, puis sur **Utilisateurs verrouillés**.

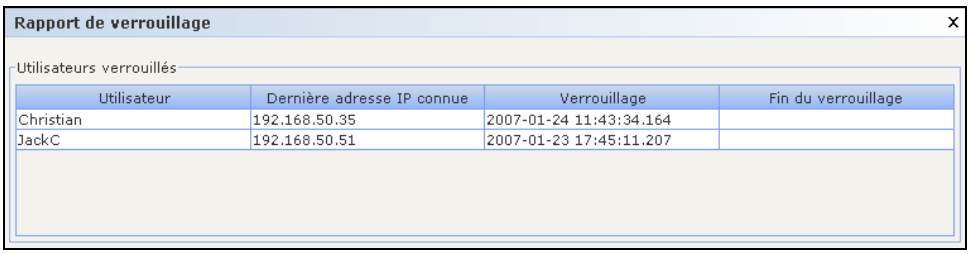

Figure 118 Rapport Utilisateurs verrouillés

- Pour déverrouiller un utilisateur, sélectionnez son nom, puis cliquez sur **Déverrouiller l'utilisateur**.
- Cliquez sur **Cancel** (Annuler) pour fermer le rapport.

Rapport Données de tous les utilisateurs

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

1. Dans le menu **Rapports**, cliquez sur **Utilisateurs**, puis sur **Données d'utilisateurs**. Le rapport **Données de tous les utilisateurs** est généré.

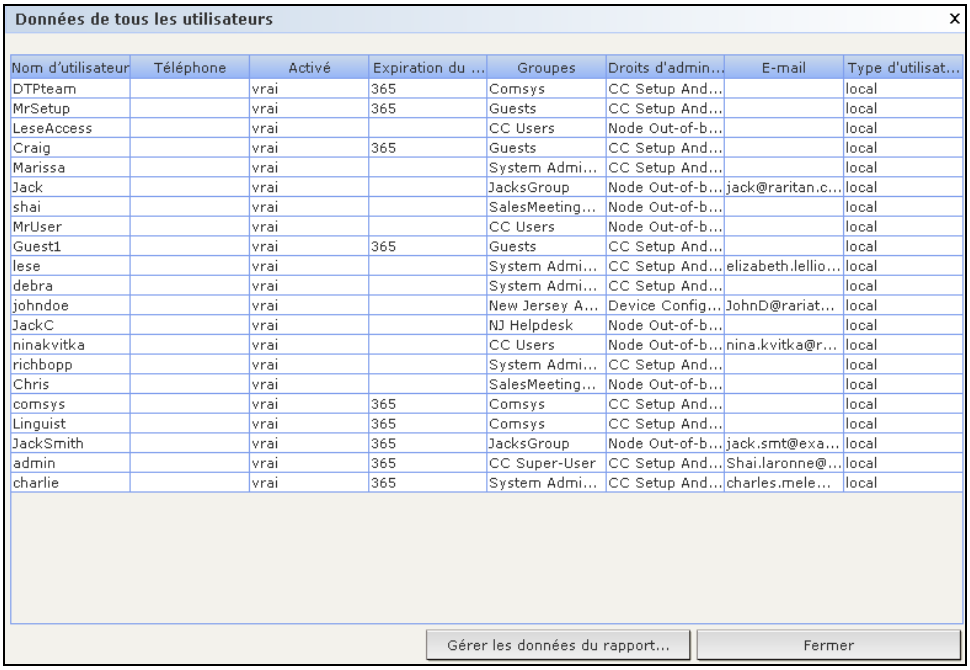

Figure 119 Rapport Données de tous les utilisateurs

- Le champ **Nom d'utilisateur** affiche le nom d'utilisateur de tous les utilisateurs de CC-SG.
- Le champ **Téléphone** affiche le numéro de rappel automatique de l'utilisateur. Cette option est disponible uniquement pour les utilisateurs de systèmes CC-SG G1 avec modem.
- Le champ **Activé** affiche **vrai** si l'utilisateur peut se connecter à CC-SG, **faux** dans le cas contraire, suivant que la case **Connexion activée** est cochée ou non dans le profil utilisateur. Reportez-vous à **Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs, Ajout d'un utilisateur** pour plus d'informations.
- 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 **Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs, Ajout d'un utilisateur** pour plus d'informations.
- Le champ **Groupes** affiche les groupes auxquels l'utilisateur appartient.
- Le champ **Droits d'administrateur** affiche les droits d'administrateur CC-SG attribués à l'utilisateur. Reportez-vous à l'**Annexe C : Privilèges de groupe d'utilisateurs** pour plus d'informations.
- Le champ **E-mail** affiche l'adresse électronique de l'utilisateur définie dans le profil utilisateur.
- Le champ **Type d'utilisateur** indique **local** ou **distant**, suivant la méthode d'accès de l'utilisateur.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport Utilisateurs dans les groupes

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

1. Dans le menu **Rapports**, cliquez sur **Utilisateurs**, puis sur **Utilisateurs dans groupes**. Le rapport **Utilisateurs dans les groupes** est généré.

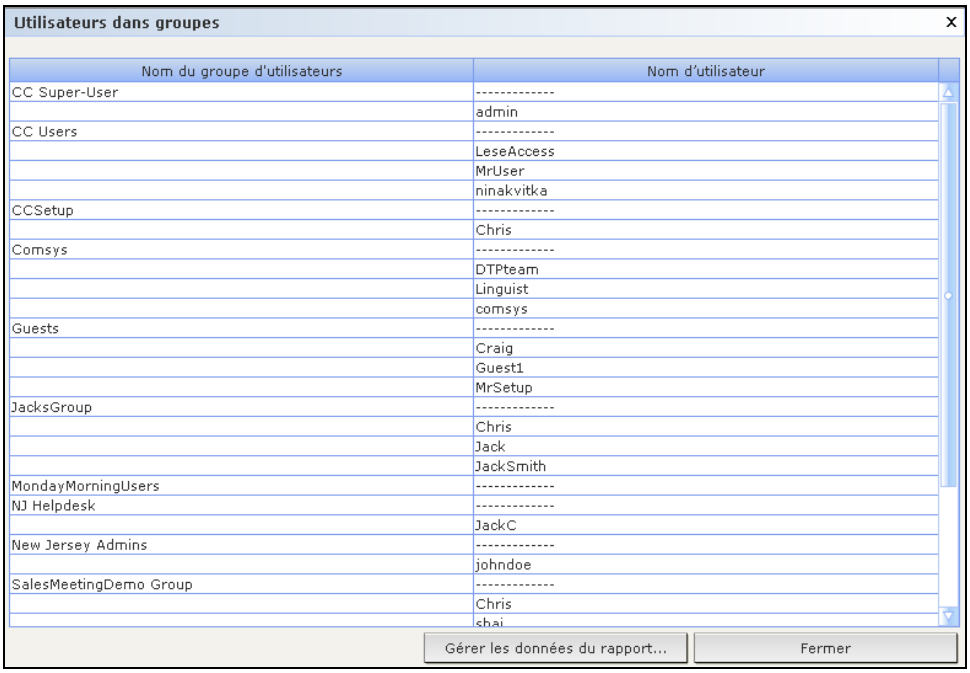

Figure 120 Rapport Utilisateurs dans les groupes

- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport Groupes

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

1. Dans le menu **Rapports**, cliquez sur **Utilisateurs**, puis sur **Données de groupes**. Le rapport **Groupes** est généré.

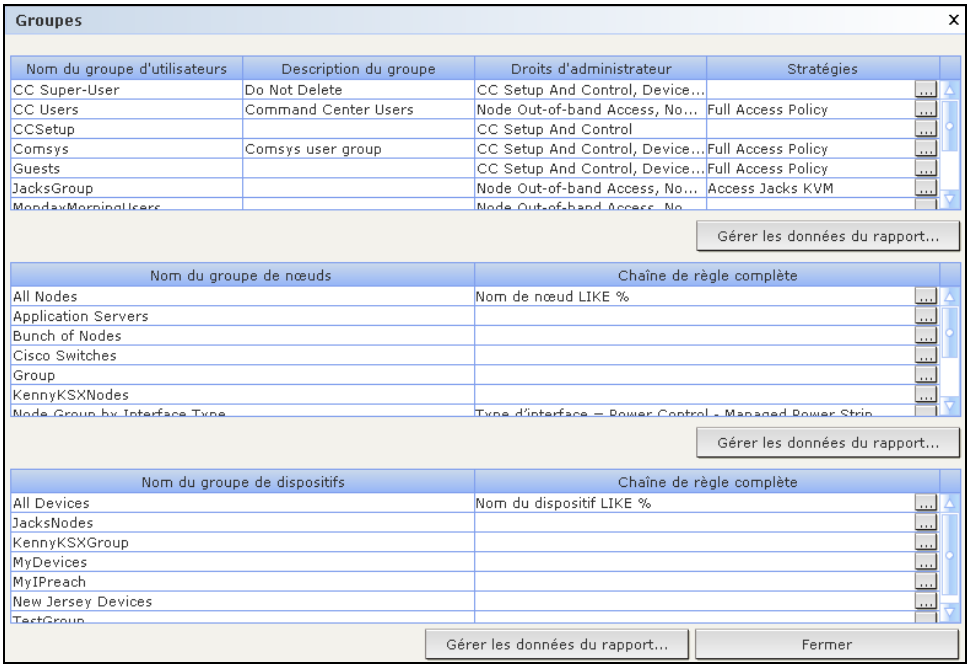

Figure 121 Rapport Groupes

- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer la section de rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.
- Cliquez sur le bouton **…** en regard d'une ligne pour afficher les stratégies associées au groupe d'utilisateurs, la liste des nœuds répondant à la règle de groupe de nœuds ou la liste de dispositifs répondant à la règle de groupe de dispositifs.

Rapport sur le groupe d'utilisateurs AD

Le rapport sur les groupes d'utilisateurs AD présente tous les utilisateurs des groupes importés dans CC-SG à partir de serveurs Active Directory configurés pour l'authentification et pour l'autorisation. Il ne répertorie pas les utilisateurs ajoutés localement, via CC-SG, aux groupes d'utilisateurs AD.

1. Dans le menu **Rapports**, cliquez sur **Utilisateurs**, puis sur **Rapport sur le groupe d'utilisateurs AD**. L'écran **Rapport sur le groupe d'utilisateurs AD** s'affiche.
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**. Le rapport sur les groupes d'utilisateurs AD est généré.

- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer la section de rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport Gestion du parc

Le rapport **Gestion du parc** affiche des données relatives aux dispositifs gérés actuellement par CC-SG.

1. Dans le menu **Rapports**, cliquez sur **Dispositifs**, puis sur **Rapport de gestion du parc**. Le rapport **Gestion du parc** est généré pour tous les dispositifs.
2. Pour filtrer les données du rapport par type de dispositif, cliquez sur la flèche déroulante **Type de dispositif**, sélectionnez un type dans la liste, puis cliquez sur **Appliquer**. Le rapport est généré à nouveau à l'aide du filtre sélectionné.

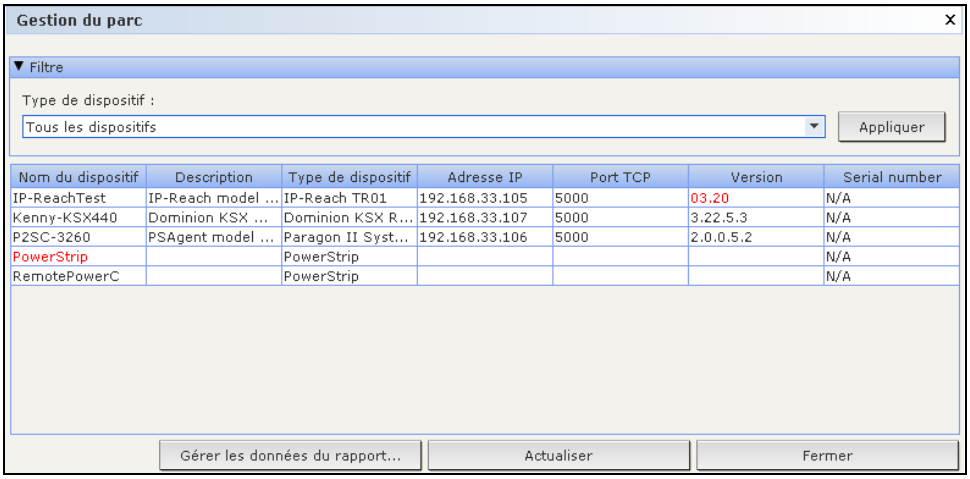

Figure 122 Rapport Gestion du parc

- Les dispositifs dont la version ne correspond pas à la matrice de compatibilité sont affichés en rouge dans le champ **Nom du dispositif**.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer la section de rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Actualiser** pour générer un nouveau rapport. La génération du rapport peut demander plusieurs minutes, en fonction de la taille de la configuration de votre système.
- Cliquez sur **Fermer** pour fermer 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 également filtrer le rapport afin de n'inclure que les données relatives aux nœuds associés à un groupe, type d'interface, type de dispositif ou dispositif particulier.

1. Dans le menu **Rapports**, cliquez sur **Nœuds**, puis sur **Rapport sur le parc du nœud**. L'écran **Rapport sur le parc du nœud** s'affiche.

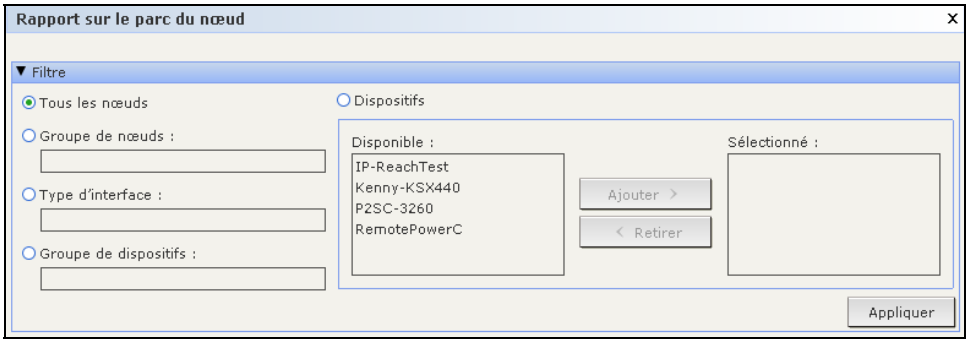

Figure 123 Ecran Rapport sur le parc du nœud

2. Cliquez sur la case d'option correspondant aux critères de filtrage que vous souhaitez appliquer au rapport : **Tous les nœuds**, **Groupe de nœuds**, **Groupe de dispositifs** ou **Dispositifs**.
   - Si vous sélectionnez **Groupe de nœuds**, **Type d'interface** ou **Groupe de dispositifs**, cliquez sur la flèche déroulante correspondante, puis choisissez un paramètre dans la liste.
   - Si vous sélectionnez **Dispositifs**, choisissez dans la liste **Disponible** les dispositifs dont vous souhaitez inclure le parc de nœud dans le rapport, puis cliquez sur **Ajouter** pour les déplacer vers la liste **Sélectionné**.
3. Cliquez sur **Appliquer** pour générer le rapport. Le rapport sur le parc du nœud est généré.

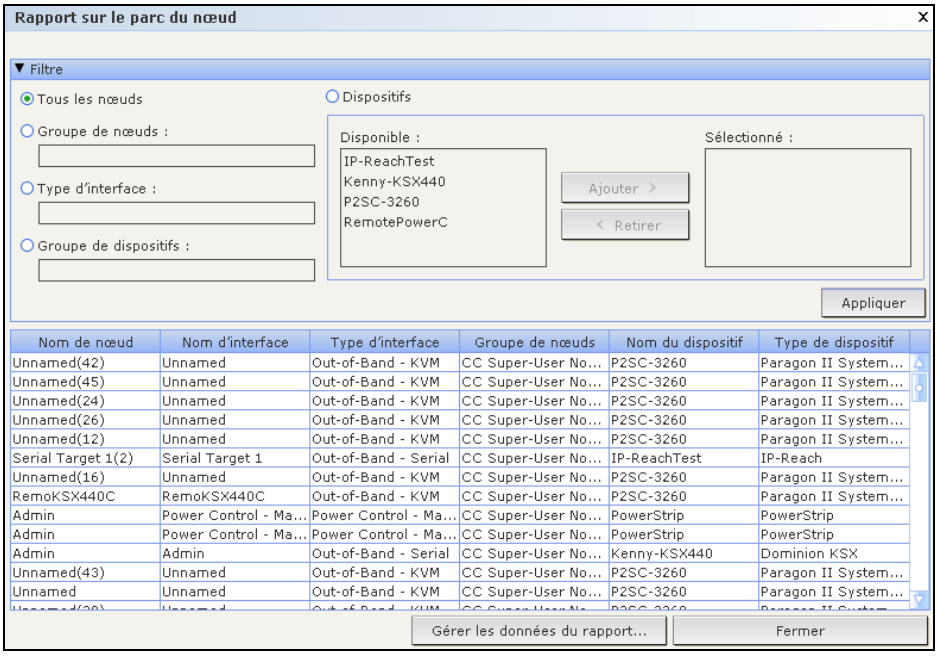

Figure 124 Rapport sur le parc du nœud

- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport sur les nœuds actifs

Le rapport sur les nœuds actifs indique les nom et type de chaque interface active, l'utilisateur actuel, un horodateur et l'adresse IP de l'utilisateur pour chaque nœud à connexion active. Vous pouvez consulter la liste des nœuds actifs et déconnecter des nœuds à partir de ce rapport.

1. Dans le menu **Rapports**, cliquez sur **Nœuds**, puis sur **Nœuds actifs**. Le rapport est généré si des nœuds sont actifs.

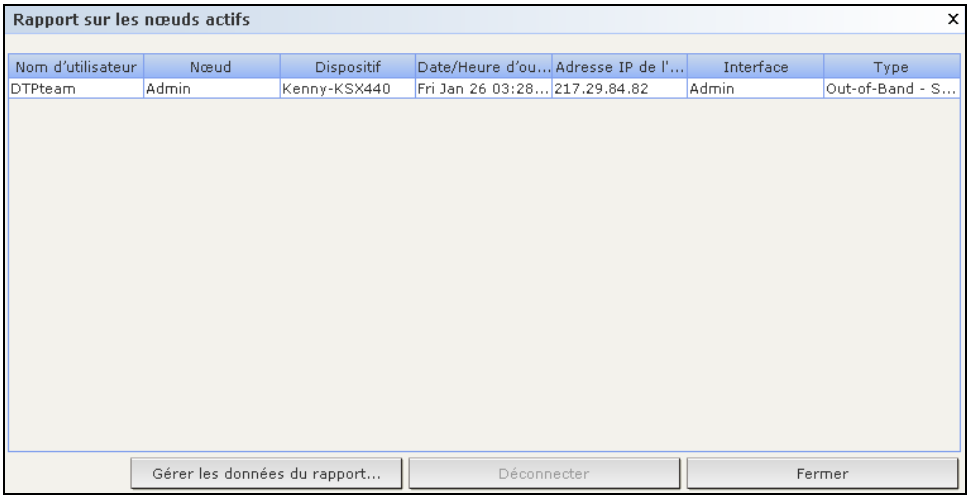

Figure 125 Rapport sur les nœuds actifs

- Pour déconnecter un nœud à partir d'une session en cours, sélectionnez-le, puis cliquez sur **Déconnecter**.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport sur la création de nœuds

Le rapport sur la création de nœuds répertorie toutes les tentatives de création de nœuds, réussies ou non, pendant une période donnée. Vous pouvez décider d'afficher toutes les tentatives de création de nœuds ou simplement les doublons potentiels.

1. Dans le menu **Rapports**, cliquez sur **Nœuds**, puis sur **Création du nœud**. L'écran **Rapport sur la création de nœuds** s'affiche.

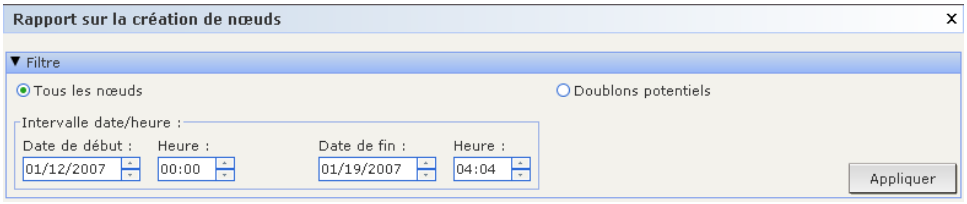

Figure 126 Ecran Rapport sur la création de nœuds

2. Définissez la période couverte par le rapport dans les champs **Date de début** et **Date de fin**. Cliquez sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité.
3. Cochez la case **Doublons potentiels** afin de limiter le rapport aux nœuds marqués comme doublons potentiels.
4. Cliquez sur **Appliquer**. Le rapport sur la création de nœuds est généré.

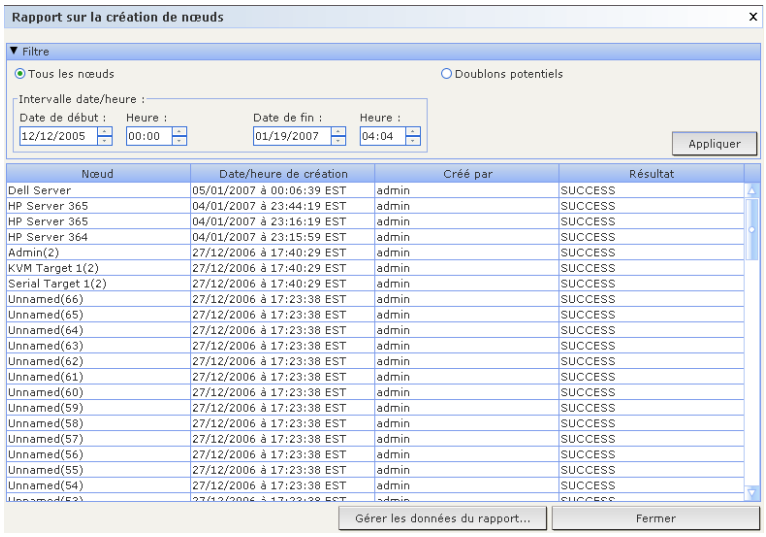

Figure 127 Rapport sur la création de nœuds

- Le champ Résultat indique **Success** (réussite), **Failed** (échec) ou **Potential Duplicate** (doublon potentiel) pour décrire l'issue de la tentative de création de nœud.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer la section de rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport Interrogation des ports

Le rapport **Interrogation des ports** affiche tous les ports en fonction de leur état.

1. Dans le menu **Rapports**, cliquez sur **Ports**, puis sur **Interrogation des ports**. L'écran **Interrogation des ports** s'affiche.

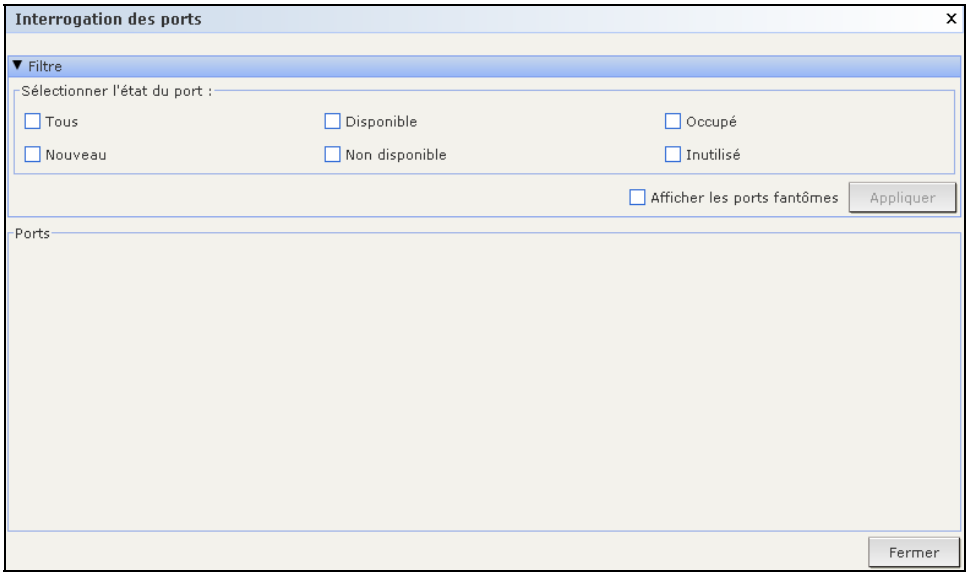

Figure 128 Ecran Interrogation des ports

2. Dans la section **Sélectionner l'état du port**, cochez les cases correspondant aux états que vous souhaitez voir figurer dans le rapport. L'activation de plusieurs cases à cocher et de l'option **Appliquer** affiche les ports associés à tous les états sélectionnés.

ETAT DU PORT	DÉFINITION
Tous	Tous les états de port.
Nouveau	Le port est disponible (connexion physique au serveur cible établie), mais il n'est pas configuré.
Inutilisé	Le port n'est pas disponible (connexion physique au serveur cible non établie) et il n'est pas configuré.
Disponible	Le port a été configuré et la connexion au port est possible.
Non disponible	La connexion au port n'est pas possible car le dispositif est arrêté et non disponible.
Occupé	Un utilisateur est connecté à ce port.

3. Cochez la case **Afficher les ports fantômes** conjointement à un ou plusieurs états de port pour afficher les ports dotés de l'état sélectionné et doublés. Un port fantôme peut survenir lorsqu'un CIM ou un serveur cible est retiré du système Paragon ou mis hors tension (manuellement ou par mégarde). Reportez-vous au **manuel d'utilisation de Paragon II** pour plus d'informations.

4. Cliquez sur **Appliquer** pour générer le rapport.

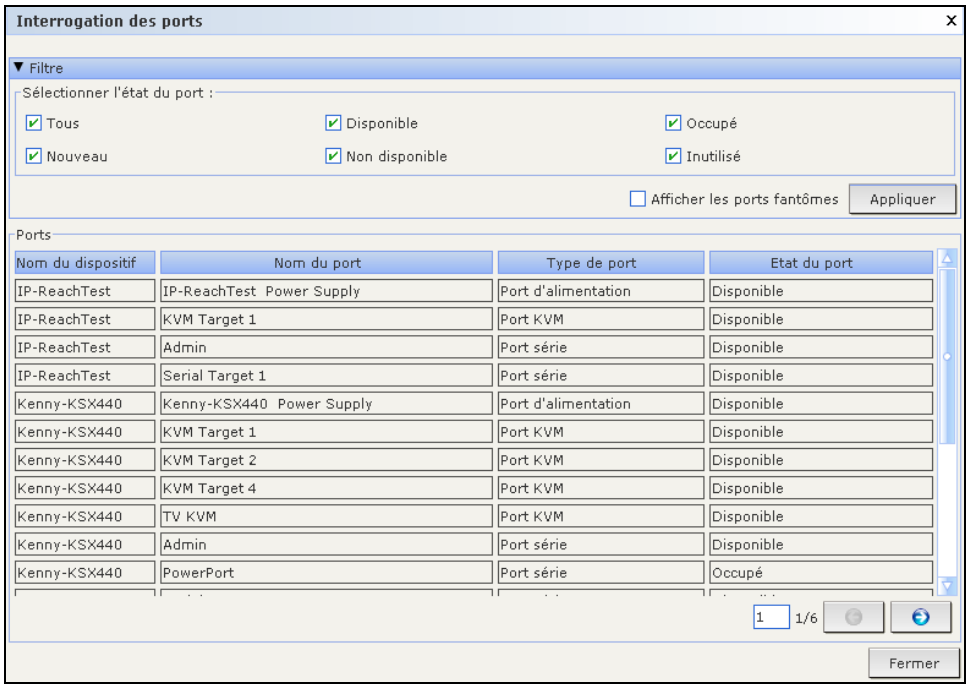

Figure 129 Rapport Interrogation des ports

- Cliquez sur les icônes de flèche dans le coin inférieur droit du rapport pour parcourir, le cas échéant, les pages du rapport.
- Cliquez sur **Configurer** en regard des ports marqués Nouveau ou Inutilisé dans le rapport afin de les paramétrer.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapport Ports actifs

Le rapport Ports actifs affiche les ports hors bande actuellement utilisés. Vous pouvez consulter la liste des ports actifs et déconnecter des ports à partir de ce rapport.

1. Dans le menu **Rapports**, cliquez sur **Ports**, puis sur **Ports actifs**. Le rapport **Ports actifs** est généré.

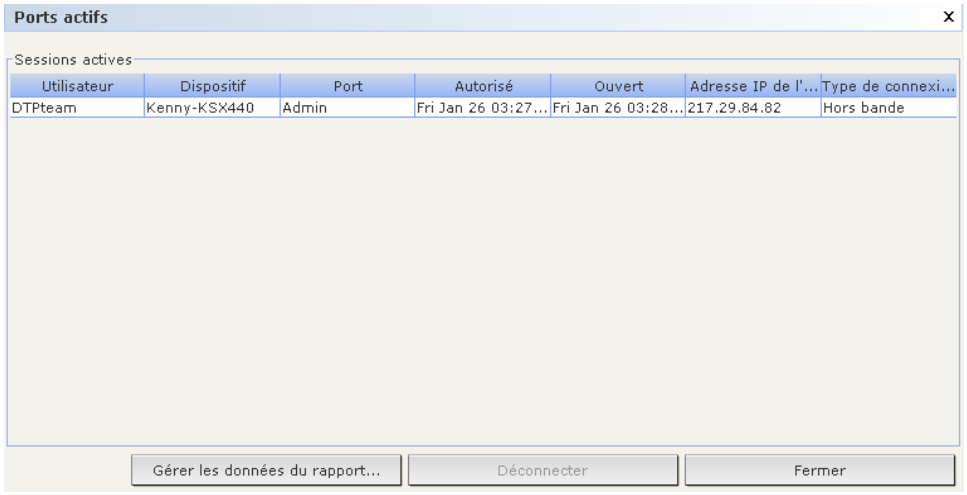

Figure 130 Rapport Ports actifs

- Pour déconnecter un port à partir d'une session en cours, sélectionnez-le, puis cliquez sur **Déconnecter**.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.
- Cliquez sur **Fermer** pour fermer le rapport.

Rapports programmés

L'écran Rapports programmés affiche les rapports programmés dans le Gestionnaire des tâches. Tous les rapports programmés peuvent être consultés au format HTML. Reportez-vous au **Chapitre 12 : Administration avancée** pour plus d'informations.

1. Dans le menu **Rapports**, cliquez sur **Rapports programmés**.
2. Cliquez sur **Obtenir les rapports** pour afficher la liste complète de tous les rapports programmés créés par tous les propriétaires. Par défaut, tous les rapports programmés dans l'heure précédente sont affichés.
3. Pour filtrer les rapports affichés, vous pouvez sélectionner un **type de rapport** particulier, tel que Rapport Ports actifs, ou **Propriétaire du rapport**, ou modifier les dates de début et de fin dans les champs **Rapports générés entre** en cliquant sur chaque composant de la date par défaut (mois, jour, année, heure, minute, seconde) pour le sélectionner, puis sur les flèches haut et bas pour afficher le nombre souhaité. Vous pouvez également renseigner le champ **Nom du rapport** pour filtrer sur le nom : entrez le nom complet ou une partie du nom ; les correspondances ne tiennent pas compte de la casse et les caractères joker ne sont pas autorisés.
4. Cliquez sur **Obtenir les rapports** pour visualiser la liste filtrée.
5. Pour visualiser un rapport, mettez-le en surbrillance dans la liste et cliquez sur **Afficher le rapport**.
6. Cliquez sur **Fermer** pour fermer le 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 un CC-NOC** dans le **Chapitre 12 : Administration avancée** pour plus d'informations. Vous pouvez également purger des cibles de la base de données CC-SG à partir de ce rapport.

1. Dans le menu **Rapports**, cliquez sur **Synchronisation CC-NOC**.
2. Sélectionnez une **dernière date détectée** et cliquez sur **Obtenir des cibles**. Les cibles découvertes à la dernière date de détection ou avant cette date sont affichées sous **Cibles détectées**.

- Pour purger une cible de la base de données CC-SG, sélectionnez-la, puis cliquez sur **Purger**.
- Pour purger la liste entière de cibles de la base de données CC-SG, cliquez sur **Effacer tout**.
- Cliquez sur **Gérer les données du rapport…** pour enregistrer ou imprimer le rapport. Cliquez sur **Enregistrer** pour sauvegarder les enregistrements affichés dans la page de rapport active dans un fichier CSV ou sur **Enregistrer tout** pour sauvegarder tous les enregistrements. Cliquez sur **Imprimer** pour imprimer les enregistrements affichés dans la page de rapport active ou sur **Imprimer tout** pour imprimer tous les enregistrements. Cliquez sur **Fermer** pour fermer la fenêtre.

Chapitre 11 : Maintenance du système

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. Ces opérations sont réalisables à partir de l'interface utilisateur ou d'une interface de ligne de commande SSH par l'intermédiaire de clients, tels que Putty, OpenSSH Client, etc. Pour plus d'informations, reportez-vous au **Chapitre 12 : Administration avancée, Accès SSH à CC-SG**.

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 au **Chapitre 12 : Administration avancée, Gestionnaire des tâches** pour plus d'informations sur les tâches programmées. Lorsque l'unité CC-SG quitte le mode de maintenance, les tâches programmées sont exécutées dès que possible.

Entrer en mode de maintenance

Pour entrer en mode de maintenance :

1. Dans le menu Maintenance du système, cliquez sur Mode de maintenance, puis sur Entrer en mode de maintenance.

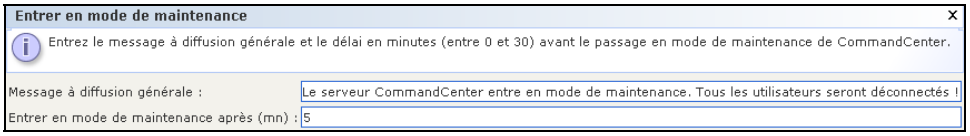

Figure 131 Entrer en mode de maintenance

2. Tapez un **message à diffusion générale** ou acceptez le message par défaut fourni. Ce message sera envoyé à tous les utilisateurs connectés pour les prévenir qu'ils seront déconnectés lorsque CC-SG entrera en mode de maintenance.
3. Tapez une durée (en minutes) dans le champ **Entrer en mode de maintenance après (mn)**. Il s'agit de la durée qui s'écoulera avant que CC-SG n'entre en mode de maintenance. Le temps indiqué peut se situer entre **0** et **30** minutes, **0** indiquant l'entrée immédiate en mode de maintenance.
4. Cliquez sur **OK**.

Quitter le mode de maintenance

Pour quitter le mode de maintenance :

1. Dans le menu **Maintenance du système**, cliquez sur **Mode de maintenance**.
2. Cliquez sur **Quitter le mode de maintenance**. L'écran **Quitter le mode de maintenance** apparaît.
3. Cliquez sur **OK** pour quitter le mode de maintenance.

Un message s'affiche pour indiquer que 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.

1. Dans le menu **Maintenance du système**, cliquez sur **Sauvegarde**. L'écran **Sauvegarder CommandCenter** s'affiche.

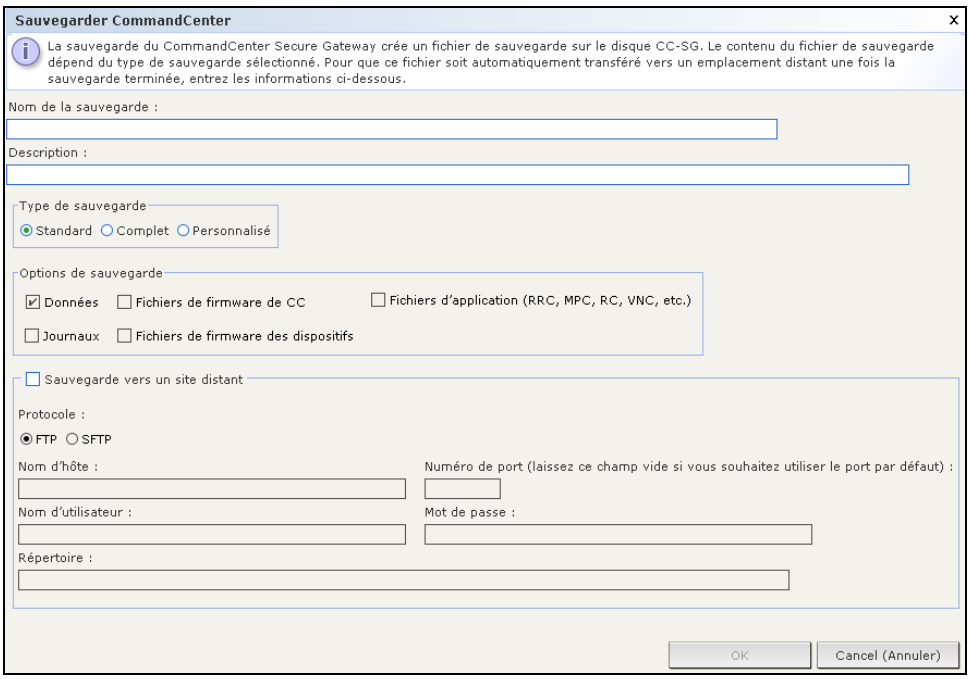

Figure 132 Ecran Sauvegarder CommandCenter

2. Renseignez le champ **Nom de la sauvegarde**.
3. Si vous le souhaitez, entrez une brève description de la sauvegarde dans le champ **Description**.
4. Sélectionnez un **type de sauvegarde**.
   - **Personnalisé** : permet de définir les composants à ajouter à la sauvegarde en les cochant dans la zone **Options de sauvegarde** en dessous. Cochez les options que vous souhaitez inclure dans la sauvegarde.
     - **Données** : configuration de CC-SG, configuration des dispositifs et des nœuds, et données utilisateur. (Standard)
     - **Journaux** : journaux d'erreur et rapports d'événement stockés dans CC-SG.
     - **Fichiers de firmware de CC** : fichiers de firmware stockés utilisés pour la mise à jour du serveur CC-SG.
     - **Fichiers de firmware des dispositifs** : fichiers de firmware stockés utilisés pour la mise à jour des dispositifs Raritan gérés par CC-SG.
     - **Fichiers d'application** : applications stockées utilisées par CC-SG pour connecter les utilisateurs aux nœuds.
   - **Complet** : crée une sauvegarde de la totalité des **données**, **journaux**, fichiers de firmware et **fichiers d'application** stockés dans CC-SG. Ceci produit les fichiers de sauvegarde les plus volumineux.
   - **Standard** : crée uniquement une sauvegarde des **données** critiques dans CC-SG. Cette sauvegarde inclut des données sur la configuration de CC-SG, la configuration des dispositifs et des nœuds et la configuration des utilisateurs. Ceci produit les fichiers de sauvegarde les plus petits.
5. Si vous souhaitez enregistrer une copie de ce fichier de sauvegarde sur un serveur externe, cochez la case **Sauvegarde vers un site distant**.
   a. Sélectionnez le **protocole** à utiliser pour la connexion à un serveur distant, **FTP** ou **SFTP**
   b. Entrez l'adresse IP ou le nom d'hôte du serveur dans le champ **Nom d'hôte**.

c. 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**.
d. Entrez un **nom d'utilisateur** pour le serveur distant dans le champ correspondant.
e. Entrez un **mot de passe** pour le serveur distant dans le champ correspondant.
f. Dans le champ **Répertoire**, indiquez le répertoire utilisé pour stocker la sauvegarde sur le serveur distant.

6. Cliquez sur **OK**.

Un message confirmant la sauvegarde de CC-SG s'affiche. 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.

Restauration de CC-SG

1. Dans le menu **Maintenance du système**, cliquez sur **Restaurer**. L'écran **Restaurer CommandCenter** affiche une table de sessions de sauvegarde disponibles pour CC-SG. Cette table répertorie également le type de la sauvegarde, sa date, une description, la version de CC-SG utilisée et la taille du fichier de sauvegarde.

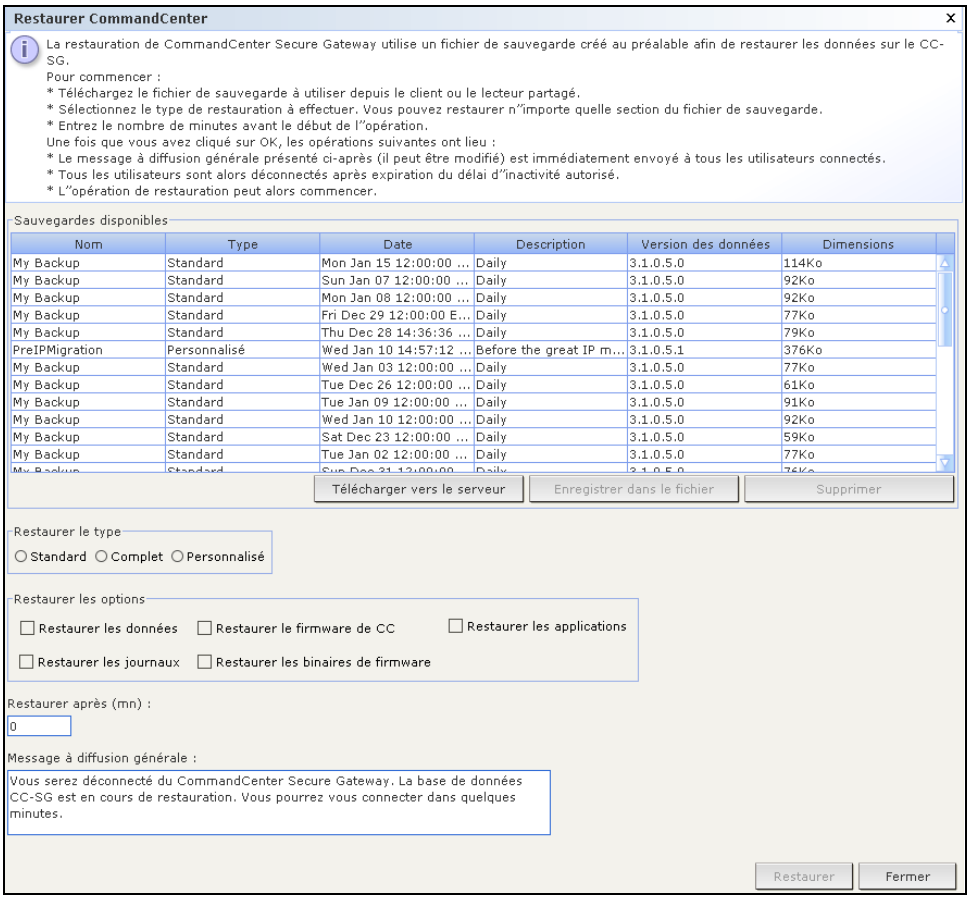

Figure 133 Ecran Restaurer CommandCenter

2. Pour restaurer une sauvegarde stockée hors du système CC-SG, vous devez la télécharger pour la rendre disponible. Cliquez sur **Télécharger vers le serveur**. Un écran de dialogue **Ouvrir** apparaît. Vous pouvez extraire le fichier de n'importe quel emplacement du réseau du client.
   a. Recherchez le fichier de sauvegarde et sélectionnez-le dans la fenêtre de dialogue.
   b. Cliquez sur **Ouvrir** pour télécharger ce fichier sur CC-SG.
   c. Cette opération terminée, le fichier de sauvegarde apparaît dans la table **Sauvegardes disponibles**.
3. Sélectionnez la sauvegarde à restaurer dans la table **Sauvegardes disponibles**.

4. Le cas échéant, sélectionnez le type de restauration que vous souhaitez effectuer à partir de cette sauvegarde :

- **Standard** : restaure uniquement les **données** critiques dans CC-SG. Ceci inclut des données sur la configuration de CC-SG, la configuration des dispositifs et des nœuds et la configuration des utilisateurs.
- **Complet** : restaure la totalité des **données**, **journaux**, fichiers de firmware et **fichiers d'application** stockés dans le fichier de sauvegarde. Une sauvegarde complète doit avoir été effectuée pour ce fichier.
- **Personnalisé** : permet de définir les composants de la sauvegarde à restaurer dans CC-SG en les cochant dans la zone **Restaurer les options** en dessous. Cochez les options que vous souhaitez inclure dans la restauration.
    a. **Données** : configuration de CC-SG, configuration des dispositifs et des nœuds, et données utilisateur.
    b. **Journaux** : journaux d'erreur et rapports d'événement stockés dans CC-SG.
    c. **Fichiers de firmware de CC** : fichiers de firmware stockés utilisés pour la mise à jour du serveur CC-SG.
    d. **Fichiers de firmware des dispositifs** : fichiers de firmware stockés utilisés pour la mise à jour des dispositifs Raritan gérés par CC-SG.
    e. **Fichiers d'application** : applications stockées utilisées par CC-SG pour connecter les utilisateurs aux nœuds.

5. Entrez le nombre de minutes, de 0 à 60, qui doivent s'écouler avant que CC-SG n'exécute l'opération de restauration dans le champ **Restaurer après**. Ceci permet aux utilisateurs de terminer leur travail et de se déconnecter.
6. Dans le champ **Message à diffusion générale**, entrez un message pour prévenir les autres utilisateurs de CC-SG qu'une restauration va avoir lieu.
7. Cliquez sur **Restaurer**.

Après cela, CC-SG attendra le temps indiqué dans le champ **Restaurer après** avant de récupérer la configuration issue de la sauvegarde sélectionnée. Lorsque la restauration se produit, tous les autres utilisateurs sont déconnectés.

Enregistrer et supprimer des fichiers de sauvegarde

Vous pouvez également enregistrer et supprimer des sauvegardes stockées sur le système CC-SG à partir de l'écran **Restaurer CommandCenter**. L'enregistrement de sauvegardes vous permet de conserver une copie du fichier de sauvegarde sur un autre PC, alors que la suppression de sauvegardes inutiles permet de gagner de l'espace sur CC-SG.

Pour enregistrer une sauvegarde

1. Dans la table **Sauvegardes disponibles**, sélectionnez la sauvegarde à enregistrer sur votre PC.
2. Cliquez sur **Enregistrer dans le fichier**. Une boîte de dialogue **Enregistrer** apparaît.

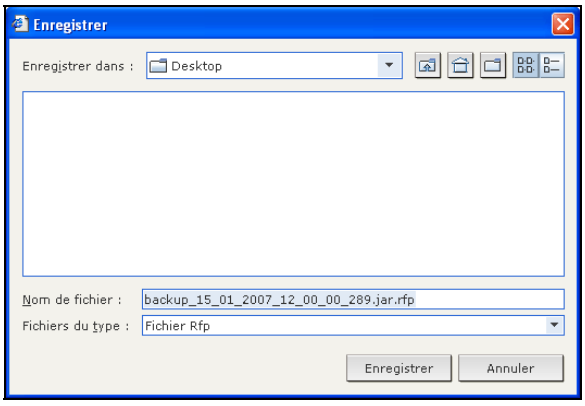

Figure 134 Enregistrer un fichier de sauvegarde

3. Spécifiez un emplacement d'enregistrement du fichier de sauvegarde de CC-SG, puis cliquez sur **Enregistrer**. Le fichier de sauvegarde est copié sur votre PC client.

Pour supprimer une 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 ou sur **Cancel** (Annuler) pour quitter sans rien supprimer. Une fois supprimé, le fichier de sauvegarde sera retiré de CC-SG.

***Remarque** : la sauvegarde et la restauration peuvent être utilisées pour déplacer une sauvegarde d'une unité CC-SG à une autre. La sauvegarde et la suppression peuvent être utilisées pour conserver une archive sécurisée des sauvegardes CC-SG sans stocker l'archive entière dans le système.*

Réinitialisation de CC-SG

Utilisez la commande Réinitialiser CommandCenter pour purger la base de données CC-SG. Cette opération ne réinitialisera pas les données de configuration système, telles que l'adresse IP de CC-SG. Les actions ci-après se produiront : réinitialisation de la base de données CC-SG, de la configuration SNMP, rétablissement du firmware par défaut, chargement du firmware par défaut dans la base de données CC-SG et récupération des valeurs par défaut de la console de diagnostic.

1. Dans le menu **Maintenance du système**, cliquez sur **Réinitialiser**.

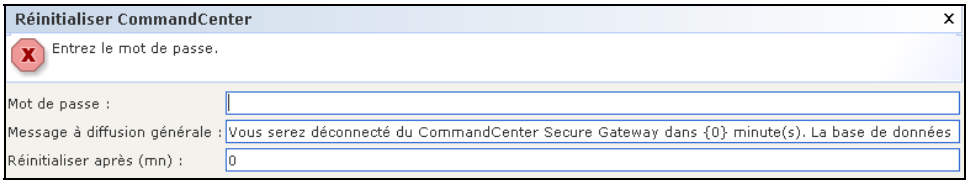

Figure 135 Ecran Réinitialiser CommandCenter

2. Tapez votre **mot de passe** CC-SG.
3. Acceptez le **message à diffusion générale** actuel ou modifiez-le pour créer le vôtre.
4. Dans le champ **Réinitialiser après (mn)**, entrez le nombre de minutes, de 0 à 60, qui doivent s'écouler avant que CC-SG n'exécute la réinitialisation. La valeur par défaut est 0 ; elle permet de réinitialiser l'unité CC-SG immédiatement.
5. Cliquez sur **OK** pour réinitialiser votre unité CC-SG. Un message de confirmation s'affiche à l'écran, indiquant que la réinitialisation a été effectuée.

Important : l'utilisation de la commande Réinitialiser a pour effet de purger la base de données de CC-SG. Tous les dispositifs, nœuds, ports et utilisateurs existants seront retirés. L'authentification est également réinitialisée sur l'utilisation de la BDD locale. Il est recommandé d'effectuer une copie de sauvegarde de CC-SG avant d'utiliser la commande Réinitialiser.

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.

***Remarque** : le redémarrage n'entraîne pas une alimentation cyclique de l'unité CC-SG. Pour un réamorçage complet, il vous faut accéder à la console de diagnostic ou à l'interrupteur d'alimentation de l'unité.*

1. Dans le menu **Maintenance du système**, cliquez sur **Redémarrer**. L'écran **Redémarrer CommandCenter** s'affiche.

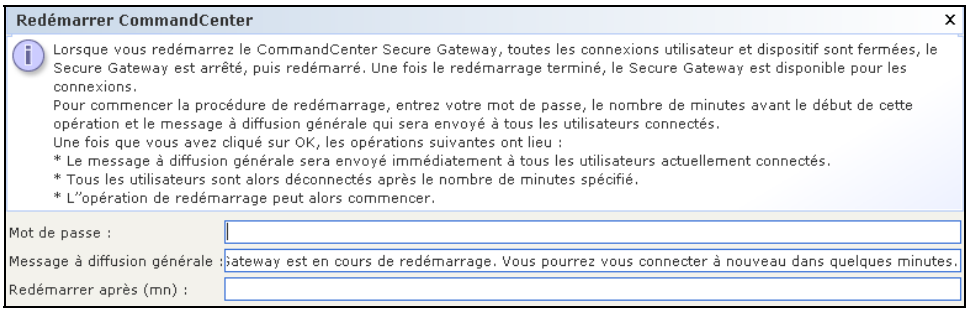

Figure 136 Ecran Redémarrer CommandCenter

2. Entrez votre mot de passe dans le champ **Mot de passe**.
3. Dans le champ **Message à diffusion générale**, acceptez le message par défaut ou entrez le message d'avertissement 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 la raison pour laquelle vous redémarrez le système). Tous les utilisateurs seront déconnectés lors du redémarrage de CC-SG.
4. Dans le champ **Redémarrer après (mn)**, entrez le nombre de minutes, de 0 à 60, qui doivent s'écouler avant que CC-SG ne redémarre.
5. Cliquez sur **OK** pour redémarrer CC-SG ou sur **Cancel** (Annuler) pour quitter l'écran sans procéder au redémarrage. Une fois CC-SG redémarré, le message à diffusion générale que vous avez saisi s'affiche.
6. Cliquez sur **OK** pour redémarrer CC-SG. CC-SG redémarre et peut de nouveau être utilisé.

Mise à niveau de CC-SG

La commande de mise à niveau permet de passer à une version plus récente du firmware de CC-SG. Pour mettre à niveau CC-SG, vous devez en premier lieu enregistrer le dernier fichier de firmware sur votre PC client. Les fichiers de firmware se trouvent dans la section Support du site Web de Raritan à l'adresse : **http://www.raritan.com/support/sup_upgrades.aspx**

Il est recommandé d'effectuer une sauvegarde de CC-SG avant la mise à niveau.

Remarque : *si vous utilisez un cluster CC-SG, vous devez d'abord supprimer le cluster et mettre chaque nœud à niveau individuellement.*

1. Dans le menu **Maintenance du système**, cliquez sur **Mode de maintenance**, puis sur **Entrer en mode de maintenance** pour passer à ce mode. Vous ne pouvez pas effectuer la mise à niveau de CC-SG sans cette action. Reportez-vous à la section **Mode de maintenance** de ce chapitre pour plus d'informations.
2. Lorsque CC-SG est en mode de maintenance, dans le menu **Maintenance du système**, cliquez sur **Mettre à niveau**. L'écran **Mettre à jour CommandCenter** s'affiche.

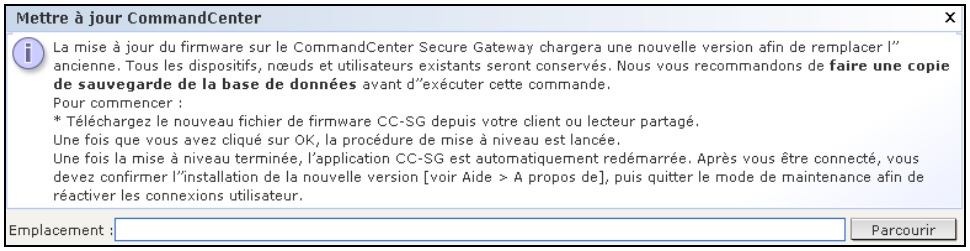

Figure 137 Ecran Mettre à jour CommandCenter

3. Cliquez sur **Parcourir**, puis recherchez et sélectionnez le fichier de firmware de CC-SG ; cliquez ensuite sur **Ouvrir**.
4. Cliquez sur **OK** pour télécharger ce fichier sur CC-SG.
5. Une fois le fichier de firmware téléchargé sur CC-SG, vous recevez un message de confirmation. Il indique que CC-SG a reçu le fichier et entamé le processus de mise à niveau. Tous les utilisateurs sont alors déconnectés de CC-SG. Cliquez sur **OK** pour quitter CC-SG et lui permettre de redémarrer.
6. Vous devez attendre environ 8 minutes que CC-SG redémarre. Fermez la fenêtre de votre navigateur, puis videz la mémoire cache de ce dernier.
7. Après 8 minutes, ouvrez une nouvelle fenêtre du navigateur et lancez CC-SG. Dans le menu **Aide**, cliquez sur **A propos de Raritan Secure Gateway**. Dans la fenêtre qui s'affiche, vérifiez que le numéro de version correspond à celui de la mise à niveau. 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.
8. CC-SG est toujours en **mode de maintenance**, ce qui signifie que la plupart des utilisateurs ne peuvent pas se connecter. Pour quitter le mode de maintenance, dans le menu **Maintenance du système**, cliquez sur **Mode de maintenance**, puis sur **Quitter le mode de maintenance**. Cliquez sur **OK**.

Arrêt de CC-SG

Voici les méthodes d'arrêt de CC-SG recommandées pour les administrateurs. Cette opération permet de fermer le logiciel CC-SG, mais elle n'entraîne pas la mise sous tension de l'unité CC-SG.

1. Dans le menu **Maintenance du système**, sélectionnez **Arrêter**. L'écran **Arrêter CommandCenter** s'affiche.

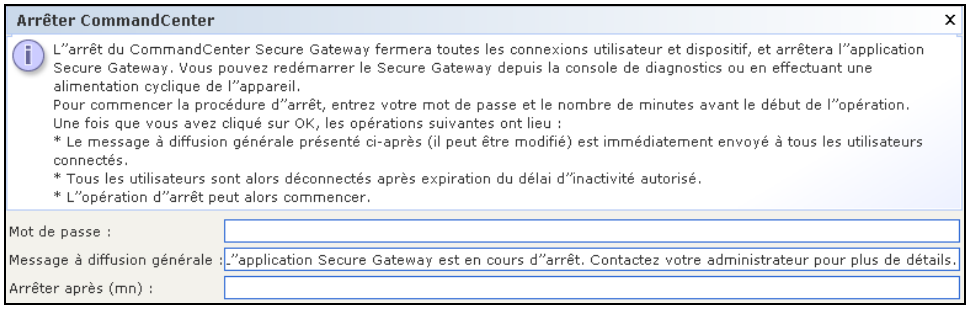

Figure 138 Ecran Arrêter CommandCenter

2. Entrez votre mot de passe dans le champ **Mot de passe**.
3. Dans le champ **Message à diffusion générale**, acceptez le message par défaut ou entrez le message à afficher sur l'écran de tous les utilisateurs actuellement connectés (vous pouvez, par exemple, accorder quelques minutes aux utilisateurs pour terminer les tâches en cours dans CC-SG et leur indiquer quand le système sera à nouveau disponible). Tous les utilisateurs seront déconnectés lors de l'arrêt de CC-SG.
4. Dans le champ **Arrêter après (mn)**, entrez le nombre de minutes, de 0 à 60, qui doivent s'écouler avant l'arrêt de CC-SG.
5. Cliquez sur **OK** pour arrêter CC-SG ou sur **Cancel** (Annuler) pour quitter l'écran sans procéder à l'arrêt. Une fois l'unité arrêtée, la fenêtre de connexion de CC-SG s'affiche.

***Remarque** : après l'arrêt de CC-SG, tous les utilisateurs sont déconnectés et redirigés vers l'écran de connexion. Les utilisateurs ne peuvent pas se reconnecter tant que vous n'avez pas redémarré CC-SG de la façon décrite dans la section suivante.*

Redémarrage de CC-SG après un arrêt

Après avoir arrêté CC-SG, redémarrez l'unité de l'une des deux façons suivantes :

1. Par le biais de la console de diagnostic : reportez-vous à la section **Console de diagnostic** du **Chapitre 12 : Administration avancée** pour plus d'informations.
2. Réinitialisez l'alimentation de l'unité CC-SG.

Fermeture d'une session CC-SG

Fermer une session

Pour quitter CC-SG à l'issue d'une session ou pour actualiser la base de données lorsque vous, ou un autre utilisateur, avez effectué des modifications, déconnectez-vous complètement de CC-SG et ouvrez une nouvelle session.

1. Dans le menu **Passerelle sécurisée**, cliquez sur **Déconnexion**. La fenêtre **Déconnexion** s'affiche.
2. Cliquez sur **Oui** pour vous déconnecter de CC-SG ou sur **Non** pour fermer la fenêtre. Une fois la déconnexion effectuée, la fenêtre de connexion de CC-SG s'affiche.
3. Connectez-vous à nouveau à CC-SG ou cliquez sur **Quitter** pour fermer complètement CC-SG.

Quitter CC-SG

Vous pouvez quitter CC-SG à tout moment.

1. Dans le menu **Passerelle sécurisée**, cliquez sur **Quitter**. La fenêtre **Quitter** s'affiche.
2. Cliquez sur **Oui** pour quitter CC-SG ou sur **Non** pour fermer la fenêtre et poursuivre votre travail.

Chapitre 12 : Administration avancée

Paramétrage guidé

Le **paramétrage guidé** guide l'administrateur à travers certaines tâches courantes sur CC-SG : création d'associations, paramétrage des dispositifs Raritan, création de groupes d'utilisateurs et d'utilisateurs. Pour plus d'informations sur l'exécution du **paramétrage guidé**, reportez-vous au **Chapitre 3 : Configuration de CC-SG par paramétrage guidé**.

Paramétrage du Message du jour

La fonction Message du jour permet aux administrateurs Secure Gateway de créer un message qui apparaît à tous les utilisateurs à la connexion. Pour configurer le message du jour, les administrateurs doivent disposer du privilège **CC Setup and Control** (paramétrage et contrôle de CC).

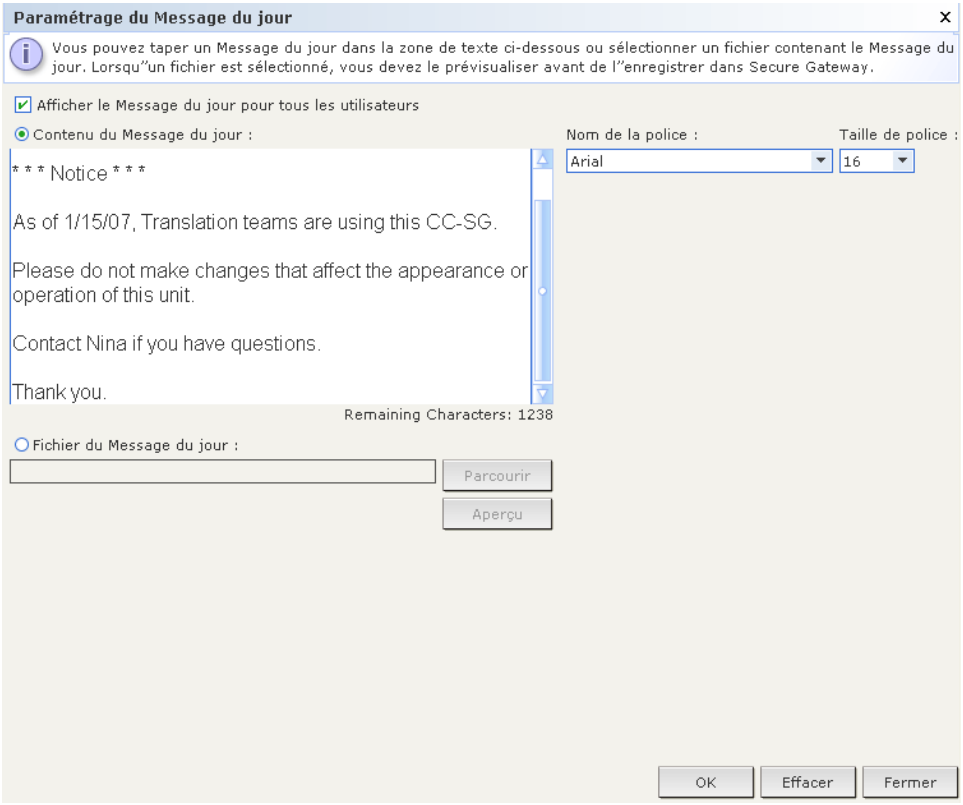

Figure 139 Configurer le message du jour

1. Dans le menu **Administration**, cliquez sur **Paramétrage du Message du jour**. L'écran de paramétrage du message du jour apparaît.
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.
3. Sélectionnez **Contenu du Message du jour** si vous souhaitez entrer un message dans CC-SG, ou **Fichier du Message du jour** pour le charger depuis un fichier existant.
   Si vous sélectionnez **Contenu du Message du jour** :
   a. Entrez un message dans la boîte de dialogue fournie.
   b. Cliquez sur le menu déroulant **Nom de la police** et sélectionnez la police d'affichage du message.
   c. Cliquez sur le menu déroulant **Taille de police** et sélectionnez la taille d'affichage du message.

   Si vous sélectionnez **Fichier du Message du jour** :

a. Cliquez sur **Parcourir** pour rechercher le fichier de message.
b. Sélectionnez le fichier dans la fenêtre de dialogue qui apparaît, puis cliquez sur **Ouvrir**.
c. Cliquez sur **Aperçu** pour vérifier le contenu du fichier.

4. Cliquez sur **Effacer** pour supprimer le contenu de la boîte de dialogue **Contenu du Message du jour**, ou le chemin d'accès au **fichier du Message du jour**.
5. Cliquez sur **OK** pour enregistrer vos paramètres dans CC-SG.

Gestionnaire des applications

Le gestionnaire des applications fournit aux administrateurs une interface permettant d'ajouter des applications d'accès à CC-SG, de modifier des applications existantes et de définir l'application par défaut d'accès aux nœuds sur les dispositifs Raritan.

Dans le menu **Administration**, cliquez sur **Applications**. L'écran **Gestionnaire des applications** s'affiche.

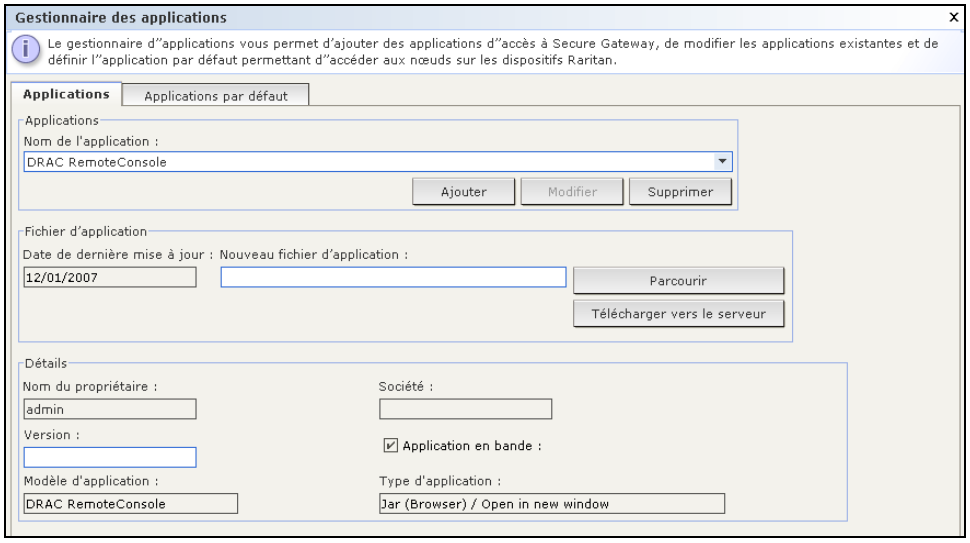

Figure 140 Onglet Applications du gestionnaire des applications

Ajouter, modifier et supprimer des applications

Cliquez sur l'onglet **Applications** du Gestionnaire des applications pour ajouter, modifier ou supprimer une application.

Ajouter une application :

1. Cliquez sur **Ajouter** dans la section **Applications** de l'onglet **Applications**. La fenêtre de dialogue **Ajouter une application** s'affiche.

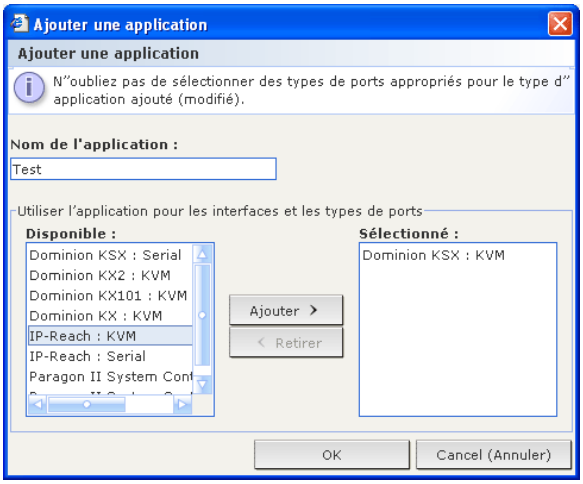

Figure 141 Ajouter une application

2. Renseignez le champ **Nom de l'application**.
3. Dans la liste **Disponible**, sélectionnez les dispositifs Raritan avec lesquels l'application fonctionnera, puis cliquez sur **Ajouter** pour les déplacer vers la liste **Sélectionné**. Une fois l'application ajoutée, les dispositifs de la liste **Sélectionné** pourront la choisir pour l'accès. Si un dispositif fournit l'accès KVM et série, il figure deux fois dans la liste, une pour chaque méthode.
4. 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** lorsque les dispositifs nécessaires ont été sélectionnés pour fonctionner avec l'application. Une fenêtre de dialogue **Ouvrir** s'affiche.
6. Dans cette fenêtre, accédez à l'emplacement du fichier d'application (fichier .jar ou .cab généralement), sélectionnez le fichier, puis cliquez sur **Ouvrir**.

L'application sélectionnée est alors chargée sur CC-SG.

Modifier une application :

1. Faites une sélection dans le menu déroulant **Nom de l'application** de la section **Applications** de l'onglet Applications. Des informations sur l'application sélectionnée apparaissent dans la zone **Détails** de l'onglet.
2. Selon l'application, certains détails peuvent être configurables. Le cas échéant, configurez les paramètres de la zone **Détails**.
3. Cliquez sur **Modifier**. La fenêtre **Modifier une application** s'affiche.
4. Dans la liste **Disponible**, sélectionnez le cas échéant des dispositifs Raritan supplémentaires avec lesquels l'application fonctionnera, puis cliquez sur **Ajouter** pour les déplacer vers la liste **Sélectionné**.
5. Le cas échéant, pour ne plus autoriser l'utilisation d'un dispositif avec l'application, choisissez-le dans la liste **Sélectionné**, puis cliquez sur **Retirer**.
6. Cliquez sur **OK** lorsque les dispositifs nécessaires ont été sélectionnés pour fonctionner avec l'application.

Supprimer une application :

1. Faites une sélection dans le menu déroulant **Nom de l'application** de la section **Applications** de l'onglet Applications. Des informations sur l'application sélectionnée apparaissent dans la zone **Détails** de l'onglet.
2. Cliquez sur **Supprimer** pour supprimer l'application sélectionnée. Une boîte de dialogue de confirmation s'affiche.
3. Cliquez sur **Oui** pour confirmer ou sur **Non** pour annuler sans supprimer l'application.

Applications par défaut

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.

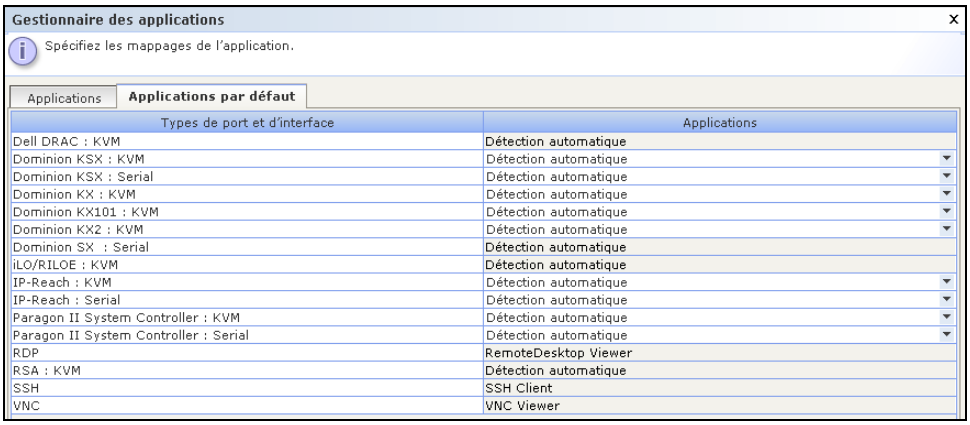

Figure 142 Liste des applications par défaut

Pour modifier l'application par défaut d'une interface ou d'un type de port :

1. Sélectionnez la ligne de l'interface ou du type de port.
2. Double-cliquez sur l'**application** indiquée sur cette ligne. La valeur devient un menu déroulant. Notez que les valeurs grisées ne sont pas modifiables.
3. Dans le menu déroulant, sélectionnez une application par défaut à utiliser lors de la connexion à l'interface ou au type de port en surbrillance. Si vous sélectionnez **Détection automatique**, CC-SG détectera automatiquement l'application en fonction du navigateur client.
4. Une fois toutes les applications par défaut configurées, cliquez sur **Mettre à jour** pour enregistrer votre sélection dans CC-SG.

Vous pouvez cliquer sur **Fermer** à tout moment pour quitter tous les écrans du **Gestionnaire des applications**.

Gestionnaire des firmware

CC-SG stocke le firmware des dispositifs Raritan pour mettre à jour les dispositifs qu'il contrôle. Le gestionnaire des firmware permet de télécharger et de supprimer les fichiers de firmware des dispositifs dans CC-SG.

Télécharger un firmware

Cette commande permet de télécharger différentes versions de firmware sur votre système. Lorsqu'une nouvelle version est disponible, elle est postée sur le site Web de Raritan.

1. Dans le menu **Administration**, cliquez sur **Firmware**. L'écran **Gestionnaire des firmware** s'affiche.

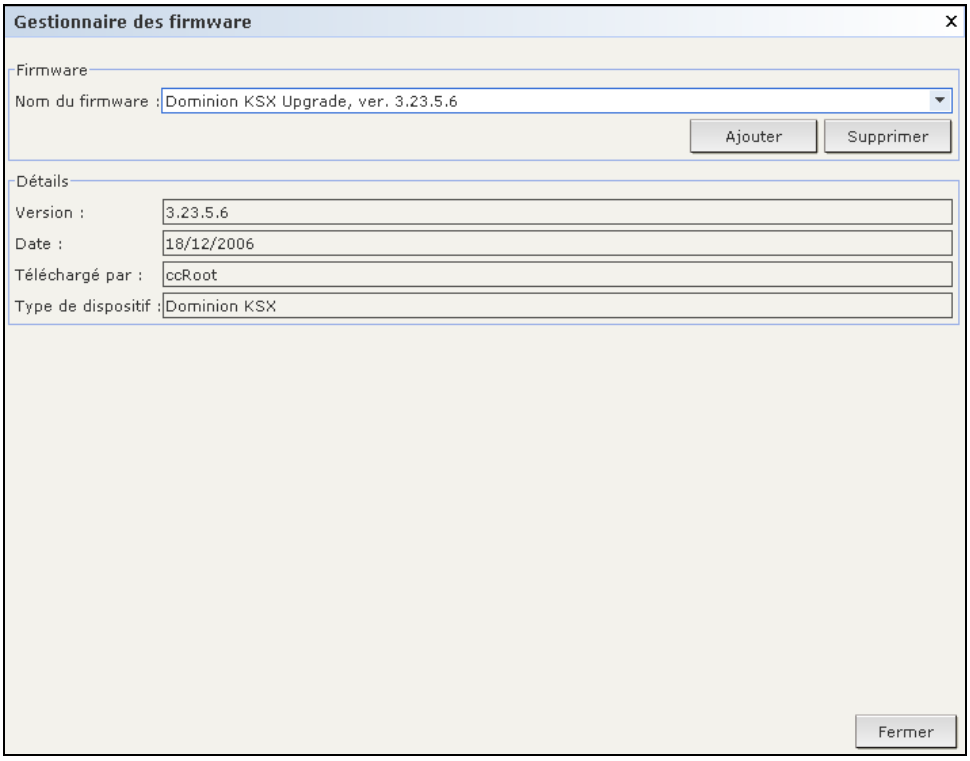

Figure 143 Ecran Gestionnaire des firmware

2. Cliquez sur **Ajouter** pour ajouter le fichier d'un nouveau firmware. Une fenêtre de recherche s'affiche.

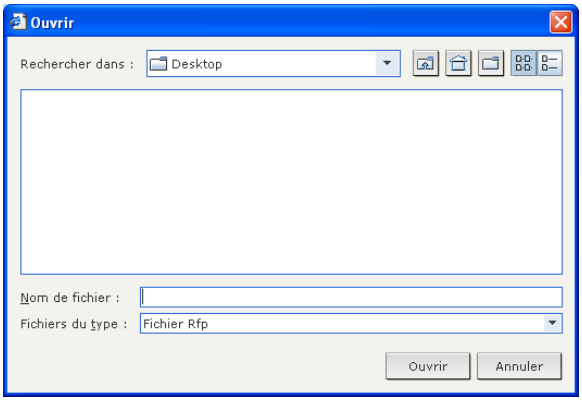

Figure 144 Fenêtre de recherche de firmware

3. Cliquez sur la flèche déroulante **Rechercher dans** et localisez le fichier du firmware. Une fois le firmware localisé, sélectionnez-le et cliquez sur **Ouvrir**. Une fois le firmware ajouté, son nom apparaît dans le champ **Nom du firmware** du gestionnaire des firmware.

Supprimer un firmware

1. Dans le menu **Administration**, cliquez sur **Firmware**. L'écran **Gestionnaire des firmware** s'affiche.
2. Cliquez sur la flèche déroulante **Nom du firmware** et sélectionnez le firmware à supprimer.
3. Cliquez sur **Supprimer**. La fenêtre **Supprimer un firmware** s'affiche.

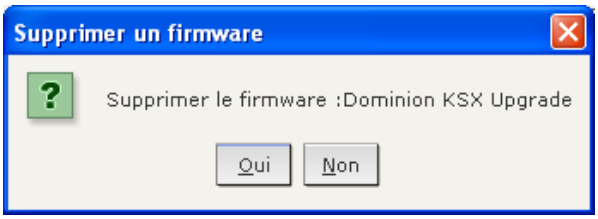

Figure 145 Fenêtre Supprimer un firmware

4. Cliquez sur **Oui** pour supprimer le firmware ou sur **Non** pour fermer la fenêtre.
5. Cliquez sur **Fermer** pour fermer l'écran **Gestionnaire des firmware**.

Gestionnaire de configuration

Le Gestionnaire de configuration permet d'administrer plusieurs paramètres CC-SG de base, tels que la configuration réseau.

Configuration réseau

1. Dans le menu **Administration**, cliquez sur **Configuration**. L'écran **Gestionnaire de configuration** s'affiche.
2. Cliquez sur l'onglet **Configuration réseau**.

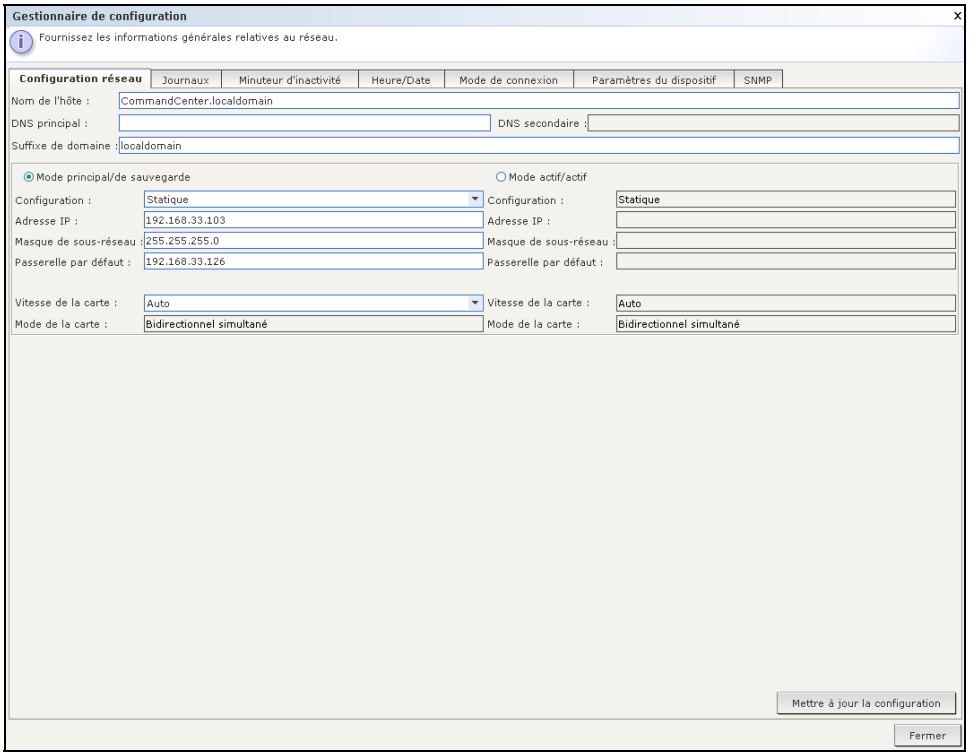

Figure 146 Ecran Gestionnaire de configuration – Configuration réseau

3. Tapez le nom de l'hôte CC-SG dans le champ **Nom de l'hôte**. Reportez-vous au chapitre 1 du présent manuel pour consulter les règles relatives aux noms d'hôte. Lorsque l'option **Mettre à jour la configuration** sera sélectionnée, le champ sera actualisé pour refléter le nom de domaine complet si un serveur et un suffixe de domaine ont été configurés.

4. Cliquez sur **Mode principal/de sauvegarde** ou sur **Mode actif/actif**. Une unité CC-SG fournit deux contrôleurs d'interface réseau. Les contrôleurs d'une unité G1 ou V1 sont libellés de gauche à droite, à l'arrière de l'unité, comme suit :

MODÈLE	CONTRÔLEUR D'INTERFACE RÉSEAU À L'EXTRÊME GAUCHE (INTERFACE PRINCIPALE)	CONTRÔLEUR D'INTERFACE RÉSEAU À L'EXTRÊME DROITE
G1	LAN1	LAN0
V1	LAN1	LAN2

Les contrôleurs d'une unité E1 sont différents, comme suit :

MODÈLE	CONTRÔLEUR D'INTERFACE RÉSEAU (INTERFACE PRINCIPALE)	CONTRÔLEUR D'INTERFACE RÉSEAU INFÉRIEUR
E1	LAN1	LAN2

Vous pouvez utiliser une interface seule ou les deux simultanément. Pour simplifier, l'explication ci-dessous utilise LAN1 comme contrôleur d'interface réseau gauche et LAN2 comme contrôleur d'interface réseau droit. Certains diagnostics et messages internes peuvent utiliser « eth0 » et « eth1 » pour faire référence à ces interfaces.

***Remarque** : si les deux interfaces sont déconnectées, CC-SG redémarre.*

A. Choisissez **Mode principal/de sauvegarde** pour implémenter le basculement et la redondance réseau. Dans ce mode, seul un contrôleur d'interface réseau est actif à la fois et une seule affectation d'adresse IP est possible.

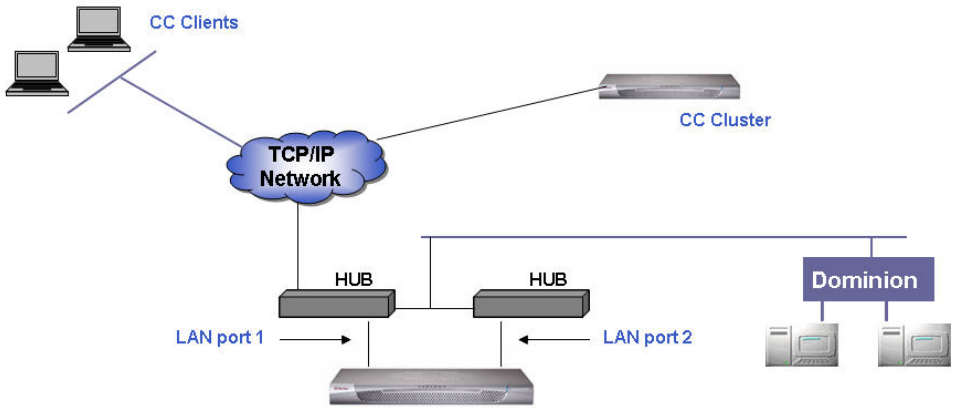

Figure 147 Réseau principal/de sauvegarde

En règle générale, les deux contrôleurs d'interface réseau sont connectés au même sous-réseau local, mais des commutateurs (ou concentrateurs) différents peuvent être utilisés à des fins de fiabilité. Lorsque les deux contrôleurs sont utilisés, un niveau de redondance réseau est fourni. Par exemple, si LAN1 est connecté et reçoit un signal d'intégrité de liens, CC-SG utilise ce contrôleur pour toutes les communications. En cas de défaillance de LAN1, et si LAN2 est connecté, CC-SG migre l'adresse IP affectée (éventuellement par DHCP) vers LAN2. LAN2 est utilisé jusqu'à la réparation et la remise en service de LAN1. CC-SG reprend l'utilisation de LAN1.

Si une interface est viable, un client PC ne doit remarquer aucune interruption de service au cours d'une défaillance. CC-SG demeure à la même adresse IP logique, mais tente de maintenir les canaux de communication et les sessions existantes dans l'éventualité de défaillances réseau. La communication (par exemple, client PC, gestion des dispositifs Raritan, pair sur cluster, etc.) est établie via ce canal de communication unique géré par les deux contrôleurs d'interface réseau.

B. Choisissez **Mode actif/actif** dans les situations de réseau spéciales ; en particulier si vous disposez de deux réseaux où l'acheminement peut être absent. Si la sécurité réseau est un point important et que vous utilisez des déploiements de type Proxy, sélectionnez également ce mode.

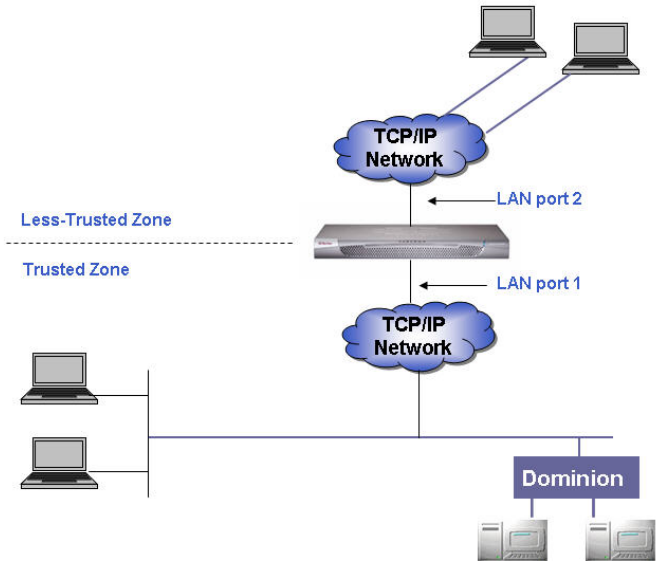

Figure 148 Réseau actif/actif

Dans ce mode, CC-SG fait office de « routeur » ou d'« agent de la circulation » entre deux domaines IP distincts, en particulier lorsque le mode **Proxy** est utilisé. (Reportez-vous à **Mode de connexion** plus loin dans ce chapitre pour plus d'informations.) En mode Proxy, le mode **actif/actif** est nécessaire pour permettre à CC-SG d'acheminer les sessions de clients PC mandatées jusqu'à leurs nœuds respectifs. Il est recommandé de connecter les dispositifs contrôlés par Raritan à LAN1, et les connexions de clients PC mandatées à LAN2. Les deux contrôleurs d'interface réseau doivent figurer sur des sous-réseaux distincts ; toutefois, si vous utilisez DHCP, cela n'est pas toujours possible et la configuration ne serait pas prise en charge. Lors de la configuration des deux contrôleurs d'interface réseau, indiquez une adresse de passerelle par défaut pour un seul d'entre eux et laissez l'autre vide.

En cas de défaillance d'un contrôleur, CC-SG tente d'acheminer le paquet à partir de l'autre contrôleur en fonction du tableau d'acheminement IP actuel. Cet acheminement risque d'échouer, surtout en la présence de pare-feu. Si des routes supplémentaires sont nécessaires, elles peuvent être ajoutées à la console de diagnostic. Reportez-vous à **Modification des routes statiques (interfaces réseau)** plus loin dans ce chapitre pour plus d'informations.

***Remarque** : le clustering ne peut pas être configuré en mode **actif/actif**.*

5. Cliquez sur la flèche déroulante **Configuration** et sélectionnez **DHCP** ou **Statique** dans la liste. Si vous choisissez **DHCP**, assurez-vous que le serveur DHCP a été configuré correctement, puis entrez le nom d'hôte. Les informations DNS, le suffixe de domaine, l'adresse IP, la passerelle par défaut et le masque de sous-réseau sont automatiquement indiqués lorsque l'option Mettre à jour la configuration est sélectionnée. A l'aide de ces données, CC-SG s'enregistre de manière dynamique auprès du serveur DNS si les mises à jour dynamiques sont autorisées. Après l'enregistrement, CC-SG est accessible à partir du nom d'hôte si l'adresse IP est inconnue lors de l'utilisation de DHCP.

   Si vous choisissez **Statique**, entrez une **adresse IP**, un **masque de sous-réseau**, une **passerelle par défaut**, des serveurs **DNS principal** et **DNS secondaire** dans les champs appropriés. Entrez également une chaîne pour la configuration du domaine dans le champ **Suffixe de domaine**.
6. Cliquez sur la flèche déroulante **Vitesse de la carte** et sélectionnez une vitesse de ligne dans la liste.
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. Si vous avez choisi le mode **Actif/Actif**, suivez les étapes 5 à 7 pour configurer la seconde interface réseau.
9. Cliquez sur **Mettre à jour la configuration** pour actualiser la configuration du réseau de votre système.
10. Cliquez sur **Fermer** pour fermer l'écran **Gestionnaire de configuration**.

Configuration des journaux

L'onglet **Journaux** vous permet de configurer CC-SG afin d'envoyer des rapports à des serveurs d'enregistrement externes. Vous pouvez configurer le niveau des messages consignés dans chacun des journaux.

Configurer l'activité d'enregistrement

1. Dans le menu **Administration**, cliquez sur **Configuration**. L'écran **Gestionnaire de configuration** s'affiche.
2. Cliquez sur l'onglet **Journaux**.

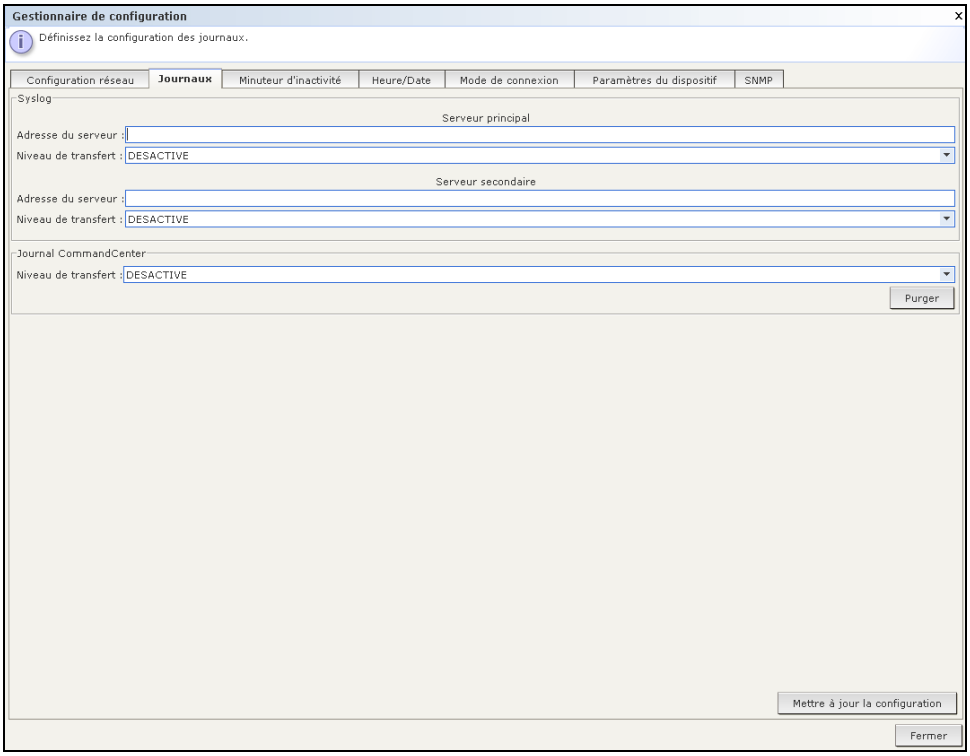

Figure 149 Ecran Gestionnaire de configuration – Journaux

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. Lorsque les journaux sont configurés, cliquez sur **Mettre à jour la configuration** pour enregistrer les paramètres dans CC-SG.
8. Cliquez sur **Fermer** pour fermer l'écran **Gestionnaire de configuration**.

Purger le journal interne de CC-SG

L'onglet **Journaux** permet également d'effacer le journal d'événements de CC-SG. Cette commande ne permet de vider que le journal d'événements de CC-SG, elle ne purge pas les événements consignés par des serveurs d'enregistrement externes.

1. Dans le menu **Administration**, cliquez sur **Configuration**. L'écran **Gestionnaire de configuration** s'affiche.
2. Cliquez sur l'onglet **Journaux**.
3. Cliquez sur **Purger** au bas de l'écran. Une fenêtre de dialogue apparaît vous demandant de confirmer.
4. Cliquez sur **Oui** pour effacer le journal d'événements de CC-SG.

***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 purgeront également leurs données.*

Configuration du minuteur d'inactivité

Cet écran vous permet de configurer combien de temps une session peut rester active avant d'être stoppée.

1. Dans le menu **Administration**, cliquez sur **Configuration**. L'écran **Gestionnaire de configuration** s'affiche.
2. Cliquez sur l'onglet **Minuteur d'inactivité**.

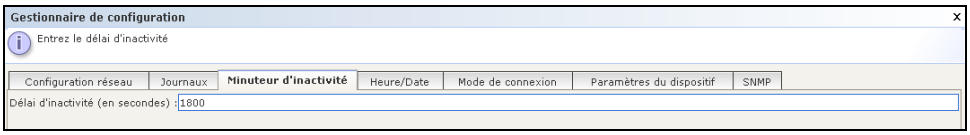

Figure 150 Onglet Minuteur d'inactivité

3. Entrez le délai d'inactivité souhaité (en secondes) dans le champ **Délai d'inactivité**.
4. Cliquez sur **Mettre à jour la configuration** pour enregistrer vos paramètres dans CC-SG.

Configuration de l'heure et de la date

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 au **Chapitre 12 : Administration avancée, Gestionnaire des tâches** pour plus d'informations. Il peut y avoir un décalage entre l'heure réglée sur le client et celle réglée dans CC-SG.

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

1. Dans le menu **Administration**, cliquez sur **Configuration** pour ouvrir l'écran **Gestionnaire de configuration**.
2. Cliquez sur l'onglet **Heure/Date**.

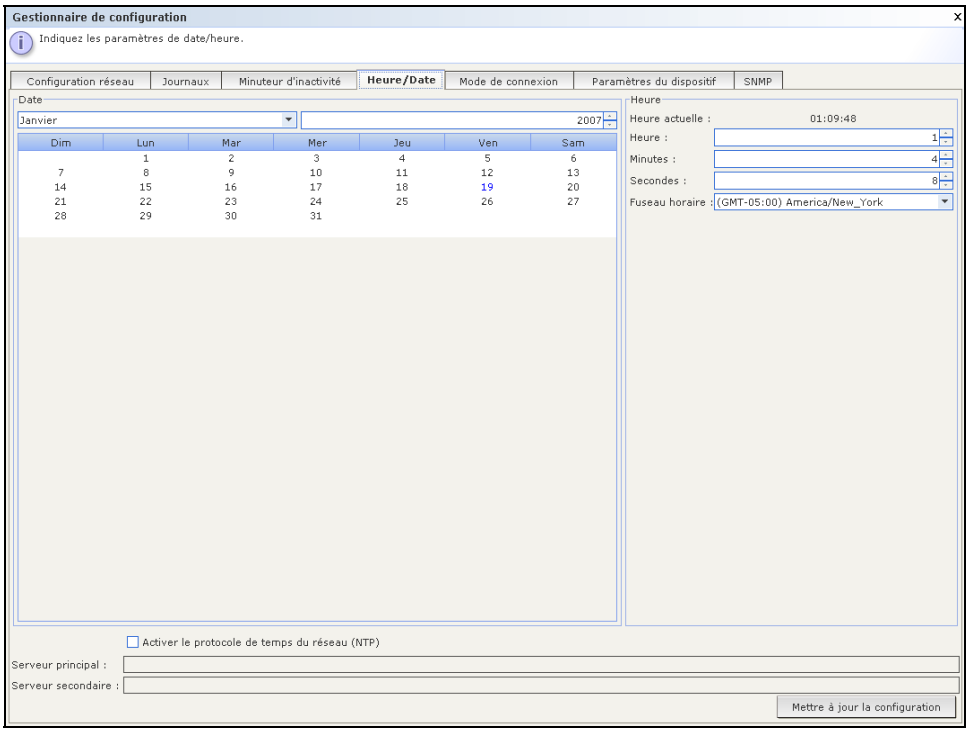

Figure 151 Ecran Gestionnaire de configuration – Heure/Date

a. **Si vous souhaitez définir la date et l'heure manuellement** : **Date** – cliquez sur la flèche déroulante afin de sélectionner le **mois**, utilisez les flèches haut et bas pour sélectionner l'**année** et cliquez sur le **jour** dans la zone du calendrier. **Heure** – utilisez les flèches haut et bas afin de sélectionner les paramètres **Heure**, **Minutes** et **Secondes**, puis cliquez sur la flèche déroulante **Fuseau horaire** pour sélectionner le fuseau horaire applicable à CC-SG.

b. **Si vous souhaitez définir la date et l'heure à l'aide du protocole NTP** : cochez la case **Activer le protocole de temps du réseau** au bas de la fenêtre et indiquez les adresses IP des **serveur principal (NTP)** et **serveur secondaire (NTP)** dans les champs correspondants.

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

3. Cliquez sur **Mettre à jour la configuration** pour appliquer les modifications relatives à l'heure et à la date à l'unité CC-SG.
4. Cliquez sur **Rafraîchir** pour recharger le nouveau temps serveur dans le champ **Heure actuelle**.
5. Dans le menu **Maintenance du système**, cliquez sur **Redémarrer** pour relancer CC-SG.

***Remarque** : le changement de fuseau horaire est désactivé dans une configuration de clusters.*

Configuration du modem

Cet écran vous permet d'accéder à une unité G1 CC-SG depuis une machine cliente via une connexion par ligne commutée. Cette méthode d'accès à CC-SG peut être utilisée dans les cas d'urgence.

***Remarque** : les plates-formes V1 et E1 ne disposent pas de modem et n'en permettent pas la configuration.*

Configurer CC-SG

1. Dans le menu **Administration**, cliquez sur **Configuration**. Lorsque l'écran **Gestionnaire de configuration** s'affiche, cliquez sur l'onglet **Modem**.

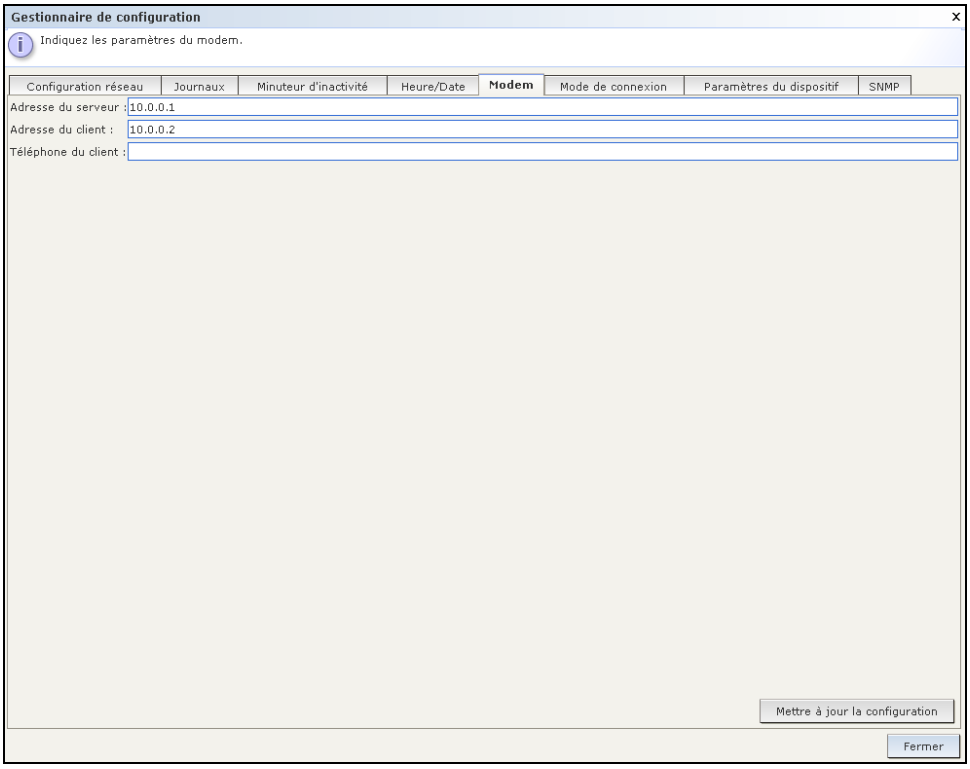

Figure 152 Ecran Gestionnaire de configuration – Modem

2. Entrez l'adresse IP de l'unité CC-SG dans le champ **Adresse du serveur**.
3. Dans le champ **Adresse du client**, entrez l'adresse IP du client qui doit se connecter par ligne commutée à l'unité CC-SG.
4. Dans le champ **Téléphone du client**, entrez le numéro de rappel composé par l'unité CC-SG pour se connecter au client, en cas de numérotation de rappel.
5. Cliquez sur **Mettre à jour la configuration** pour enregistrer les informations concernant le modem.

Configurer le modem du PC client

Branchez une ligne téléphonique sur l'unité G1 CC-SG, qui contient un modem intégré. Vous pouvez retirer les câbles de réseau local.

Sur le client de numérotation, connectez un modem à la machine cliente, un ordinateur Windows XP par exemple. Branchez une ligne téléphonique au modem client. Redémarrez la machine cliente ; le modem connecté est détecté en tant que nouveau matériel. Installez le modem sur le client comme suit (en supposant qu'il s'agit d'une machine cliente Windows XP) :

1. Sélectionnez **Panneau de configuration → Options de modems et téléphonie**.
2. Cliquez sur l'onglet **Modems**.

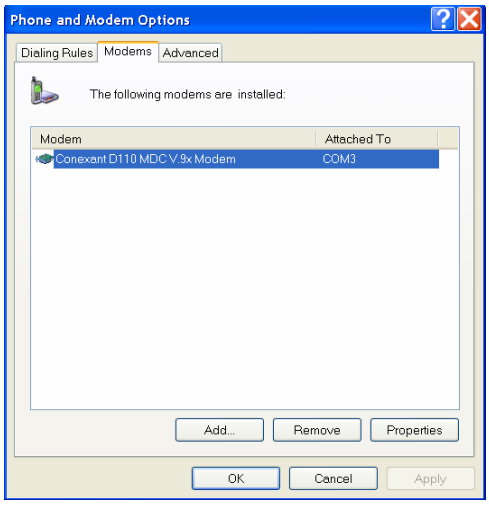

Figure 153 Onglet Modems

3. Cliquez sur **Propriétés**.
4. Cliquez sur l'onglet **Paramètres avancés**.

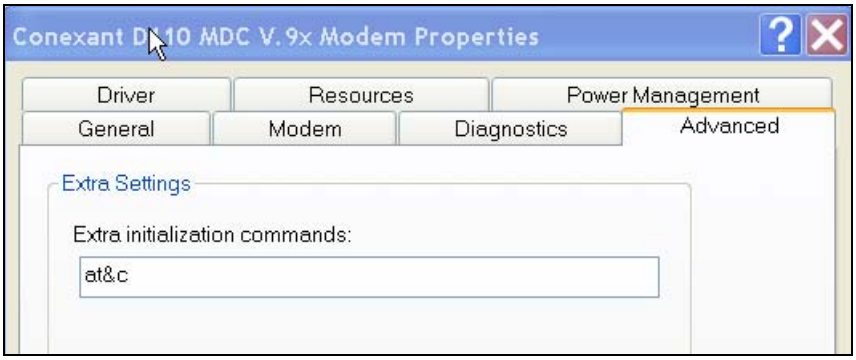

Figure 154 Commandes d'initialisation supplémentaires

5. Dans le champ **Commandes d'initialisation supplémentaires**, tapez une commande d'initialisation qui sera utilisée par votre modem pour définir l'indicateur « Carrier detection » (Ecoute de porteuse). Par exemple, tapez **at&c** pour un modem télécopieur SoftK56. Il est nécessaire d'indiquer à Windows de ne pas fermer le processus de connexion de modem démarré lorsque la connexion est interrompue par la partie appelante (accès entrant). Cliquez sur **OK** pour enregistrer les paramètres.

Configurer la connexion à distance

La procédure suivante illustre la création d'une connexion entrante à distance à CC-SG depuis un ordinateur client Windows XP :

1. Dans le menu **Démarrer**, cliquez sur **Favoris réseau**.
2. Cliquez avec le bouton droit de la souris dans la fenêtre et sélectionnez **Propriétés**.

3. Sous **Gestion du réseau** dans la fenêtre **Connexions réseau**, cliquez sur **Créer une nouvelle connexion**.

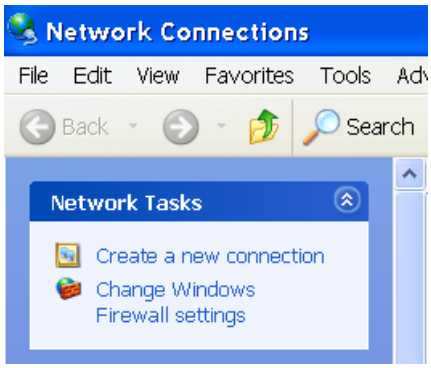

Figure 155 Créer une nouvelle connexion

4. Cliquez sur **Suivant**, **Connexion au réseau d'entreprise**, **Connexion d'accès à distance**.
5. Tapez un nom pour CC-SG, **CommandCenter** par exemple.

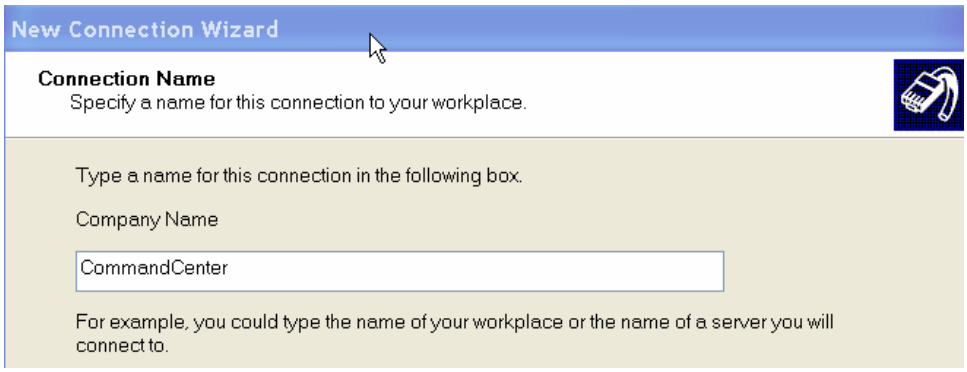

Figure 156 Nom de la connexion

6. Tapez le numéro de téléphone utilisé pour la connexion à CC-SG et cliquez sur **Suivant**. Il NE S'AGIT PAS du numéro de rappel configuré dans le champ **Téléphone du client** de l'onglet **Modem** du **Gestionnaire de configuration** sur CC-SG.

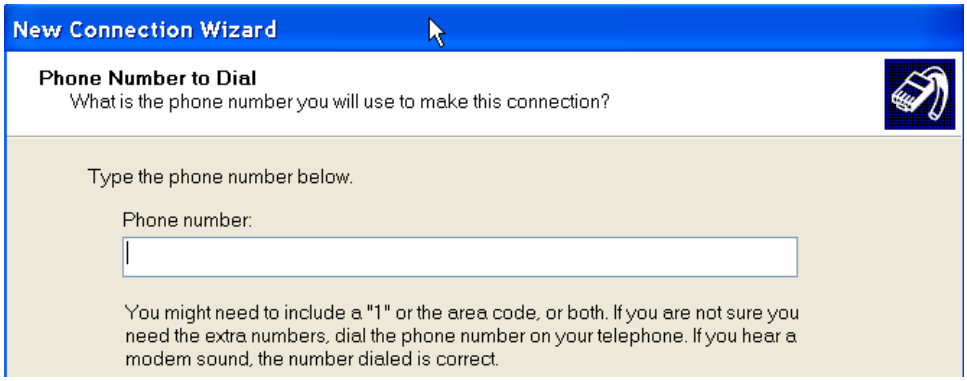

Figure 157 Numéro de téléphone à composer

7. La connexion à CC-SG ne requiert pas de carte à puce. Si vous n'en utilisez pas, cliquez sur **Ne pas utiliser ma carte à puce** pour cette connexion, puis sur **Suivant**.
8. Dans l'écran suivant, il est conseillé de cliquer sur **Mon utilisation uniquement** pour rendre la connexion disponible à vous seul.
9. Cliquez sur **Terminer** dans le dernier écran pour enregistrer les paramètres de connexion.

Configurer la connexion de rappel

Si l'unité CC-SG utilise une connexion de rappel, vous devez utiliser un fichier de script décrit ci-dessous. Pour définir un fichier de script de rappel :

1. Dans le menu **Démarrer**, cliquez sur **Favoris réseau**.
2. Cliquez sur **Afficher les connexions** réseau sous **Gestion du réseau**.
3. Cliquez avec le bouton droit sur la connexion **CommandCenter**, puis sur **Propriétés**.
4. Cliquez sur l'onglet **Sécurité**.

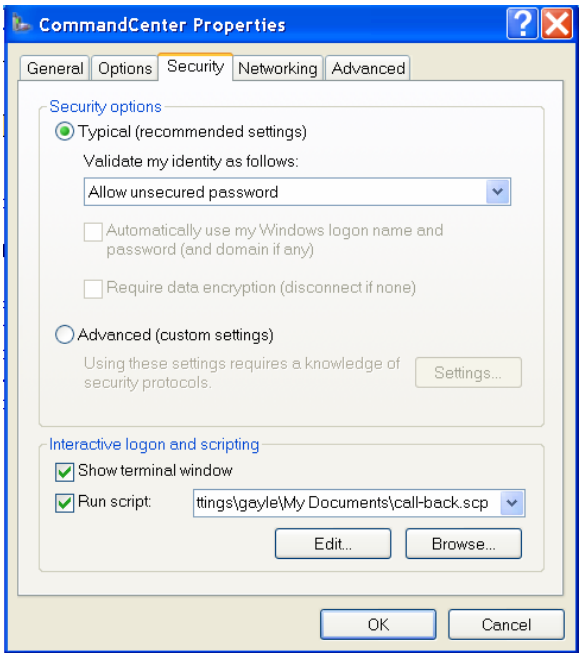

Figure 158 Définition du script de connexion à distance

5. Cliquez sur **Afficher une fenêtre de terminal**.
6. Cliquez sur **Exécuter le script**, puis sur **Parcourir** pour entrer le script de connexion à distance, **call-back.scp** par exemple.
7. Cliquez sur **OK**.

Exemple de fichier de script de rappel :

```
proc main
delay 1
waitfor "ogin:"
transmit "ccclient^M"
waitfor "client:"
transmit "dest^M"
waitfor "callback."
transmit "ATH^M"
waitfor "RING"
transmit "ATA^M"
waitfor "CONNECT"
waitfor "ogin:"
transmit "ccclient^M"
endproc
```

Se connecter à CC-SG par modem

Pour se connecter à CC-SG :

1. Dans le menu **Démarrer**, cliquez sur **Favoris réseau**.
2. Cliquez sur **Afficher les connexions réseau** sous **Gestion du réseau**.
3. Double-cliquez sur la connexion **CommandCenter**.

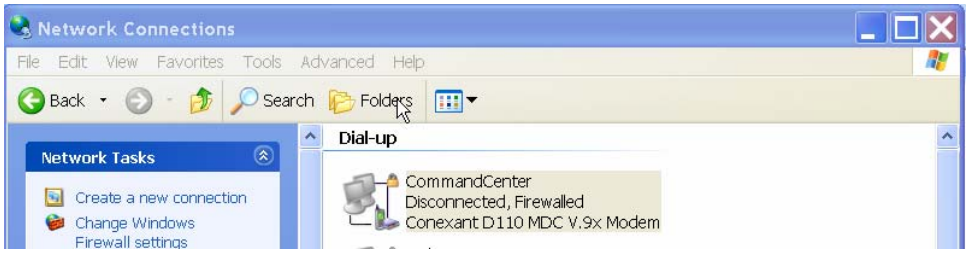

Figure 159 Connexion à CC-SG

4. Tapez le nom d'utilisateur **ccclient** et le mot de passe **cbupass**.

Figure 160 Saisie du nom d'utilisateur et du mot de passe

5. Si le champ n'est pas encore renseigné, entrez le numéro de téléphone de connexion à CC-SG. Il NE S'AGIT PAS du numéro de rappel.
6. Cliquez sur **Composer**. Si vous utilisez la fonction de rappel, le modem compose le numéro de l'unité CC-SG, qui compose à son tour celui du PC client.

7. Si l'option **Afficher une fenêtre de terminal** a été cochée, comme décrit dans la section **Configurer la connexion de rappel** plus haut dans ce chapitre, une fenêtre semblable à celle de la figure ci-dessous s'affiche :

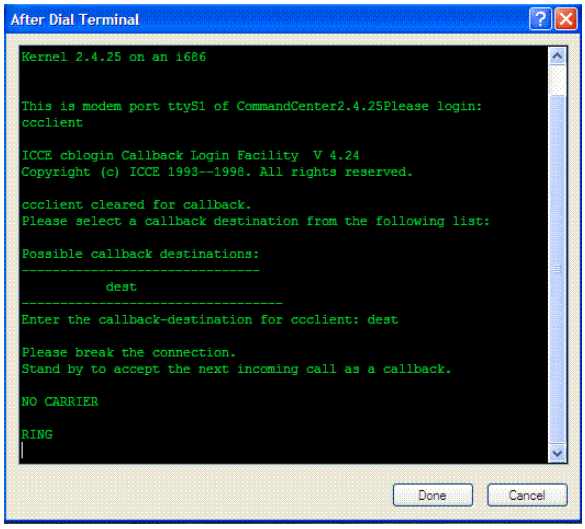

Figure 161 Terminal après numérotation

8. Patientez 1 à 2 minutes puis, dans un navigateur pris en charge, entrez l'adresse IP de CC-SG configurée dans le champ **Adresse du serveur** de l'onglet **Modem** du **Gestionnaire de configuration** sur CC-SG, et connectez-vous à CC-SG.

Mode de connexion

Lors de la connexion à un nœud, vous pouvez soit faire passer des données directement via ce nœud (**Mode direct**), soit acheminer toutes les données via l'unité CC-SG (**Mode Proxy**). Bien que le **mode Proxy** augmente la charge de la bande passante sur le serveur CC-SG, seuls les ports TCP de CC-SG (80, 443 et 2400) doivent être maintenus ouverts au niveau du pare-feu. Pour plus d'informations, reportez-vous au **guide de déploiement des solutions numériques** Raritan.

1. Dans le menu **Administration**, cliquez sur **Configuration**. L'écran **Gestionnaire de configuration** s'affiche.

2. Cliquez sur l'onglet **Mode de connexion**.

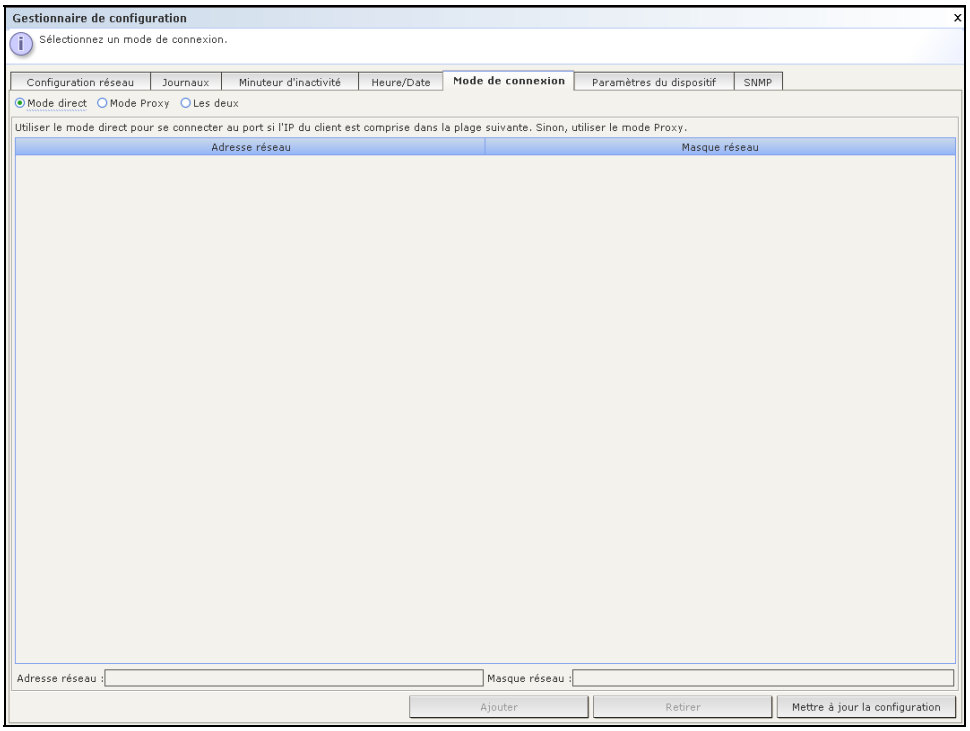

Figure 162 Ecran Gestionnaire de configuration – Mode de connexion, Mode direct

3. Activez la case d'option située en regard du mode de connexion que vous préférez.
   a. Activez la case d'option **Mode direct** pour une connexion directe au dispositif.
   b. Activez la case d'option **Mode Proxy** pour une connexion au dispositif via l'unité CC-SG.
   c. Activez la case d'option **Les deux** pour une connexion directe à certains dispositifs et une connexion via le **mode Proxy** à d'autres. Spécifiez les paramètres des dispositifs pour lesquels vous souhaitez une connexion directe :
      i. Entrez l'adresse IP du client dans le champ **Adresse réseau** qui se trouve en bas de l'écran.
      ii. Dans le champ **Masque réseau**, entrez le masque réseau de votre client.
      iii. Cliquez sur le bouton **Ajouter** pour ajouter l'adresse réseau et le masque réseau dans l'écran. Il est possible que vous deviez utiliser les barres de défilement situées dans la partie droite de l'écran pour visualiser les boutons **Ajouter/Supprimer/Mettre à jour la configuration**.

Paramètres du dispositif

1. Dans le menu **Administration**, cliquez sur **Configuration**. L'écran **Gestionnaire de configuration** s'affiche.
2. Cliquez sur l'onglet **Paramètres du dispositif**.

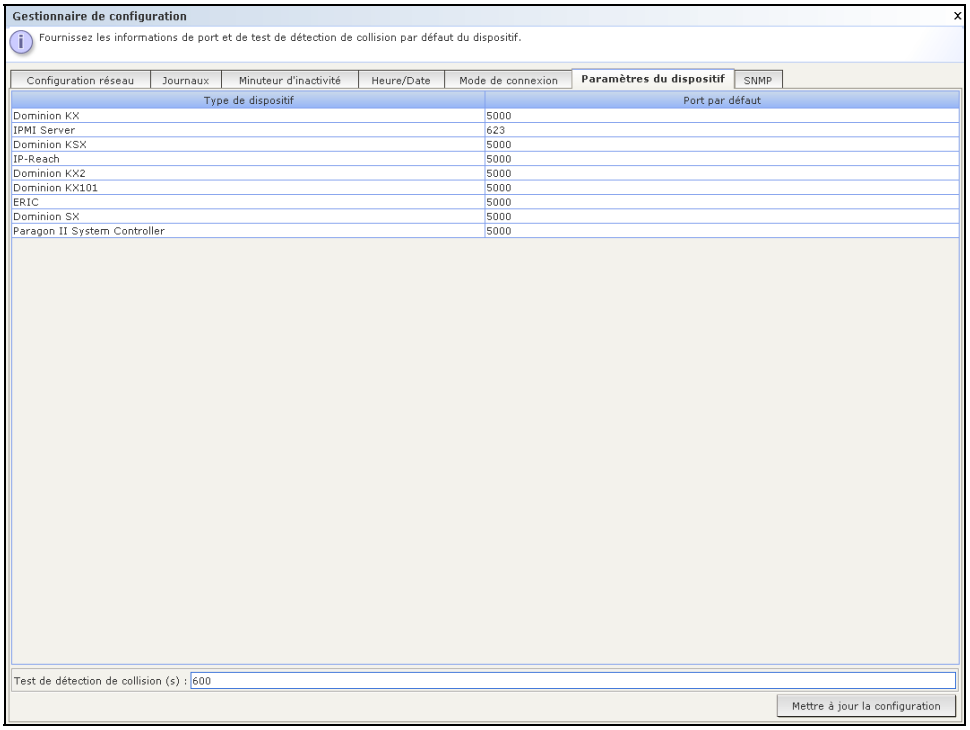

Figure 163 Ecran de configuration des paramètres du dispositif

3. Pour mettre à jour le port par défaut du dispositif, sélectionnez un type de dispositif dans le tableau et double-cliquez sur la valeur du paramètre **Port par défaut**. Tapez la nouvelle valeur du port par défaut et appuyez sur la touche **Entrée**.
4. Pour mettre à jour le délai d'attente du test de détection de collision du dispositif, double-cliquez sur la valeur du paramètre **Test de détection de collision(s)** situé en bas de l'écran. Entrez la nouvelle valeur du délai d'attente du test de détection de collision pour ce dispositif.
5. Cliquez sur **Mettre à jour la configuration** pour enregistrer les nouvelles valeurs du dispositif. Un message de confirmation s'affichera à l'écran, indiquant la mise à jour de tous les paramètres du dispositif associé.

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. Seul un administrateur de CC-SG formé à la gestion d'une infrastructure SNMP est autorisé à configurer CC-SG pour qu'il fonctionne avec le protocole SNMP.

CC-SG prend également en charge les opérations GET/SET SNMP avec les solutions de gestion d'entreprise 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. Pour plus d'informations, reportez-vous à la norme RFC 1213. Ces identifiants fournissent des informations de contact, d'administration et d'emplacement concernant le nœud géré.

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 l'**Annexe D : Traps SNMP**. Ce fichier MIB personnalisé figure sur le CD fourni avec votre unité CC-SG et sous **Mises Firmware Upgrades** (mises à niveau de firmware) sur le site **http://www.raritan.com/support**.

Configurer SNMP dans CC-SG

1. Dans le menu **Administration**, cliquez sur **Configuration**. L'écran **Gestionnaire de configuration** s'affiche.
2. Cliquez sur l'onglet **SNMP**.

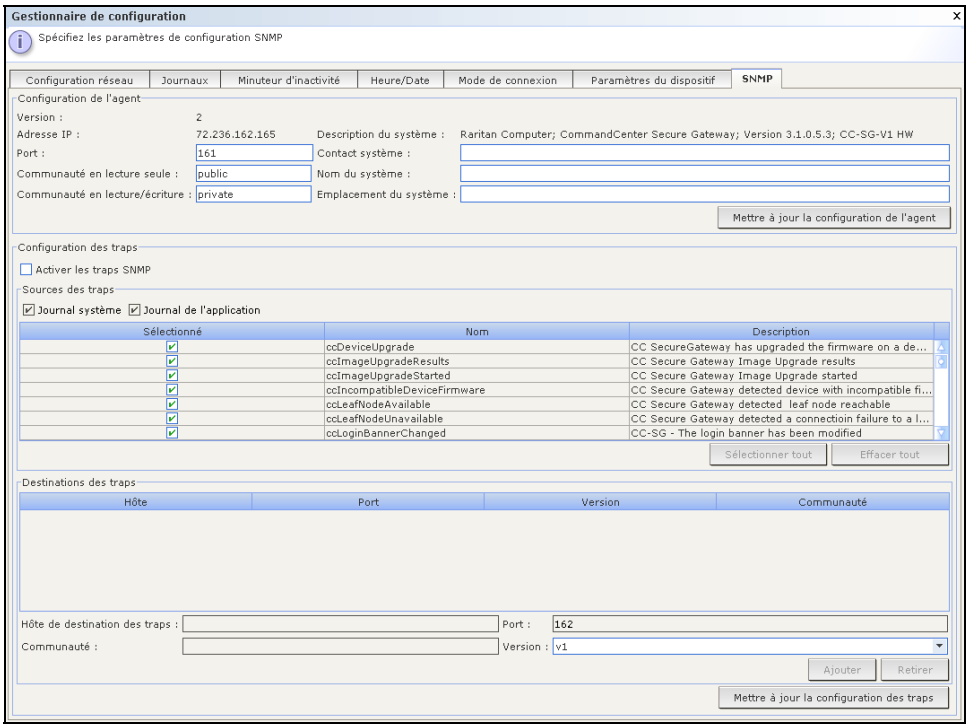

Figure 164 Ecran de configuration des paramètres du dispositif

3. Pour identifier l'agent SNMP exécuté sur CC-SG auprès des solutions de gestion d'entreprise tierces, renseignez les champs de la section **Configuration de l'agent**. Tapez le **port** de l'agent (**161** étant la valeur par défaut). Tapez une chaîne **Communauté en lecture seule** (**public** par défaut) et une chaîne **Communauté en lecture/écriture** (**private** par défaut). Vous pouvez entrer plusieurs chaînes de communauté ; séparez-les par une virgule. Entrez un **contact système**, un **nom du système** et un **emplacement du système** pour fournir des informations sur le nœud géré.
4. Cliquez sur **Mettre à jour la configuration de l'agent** pour enregistrer les informations d'identifiant d'agents SNMP.
5. Sous **Configuration des traps**, cochez la case **Activer les traps SNMP** pour activer l'envoi de traps SNMP de CC-SG vers un hôte SNMP.
6. Cochez les cases en regard des traps que CC-SG doit envoyer à vos hôtes SNMP.
   Dans le panneau **Sources des traps**, les traps SNMP sont classés en deux catégories différentes : **Journal système**, contenant les notifications sur l'état de l'unité CC elle-même, par exemple une défaillance du disque dur ; et **Journal de l'application**, contenant les notifications générées par les événements de l'application CC, par exemple les modifications apportées à un compte utilisateur. Pour activer les traps par type, cochez les cases **Journal système** et **Journal de l'application**. Chaque trap peut être activé ou désactivé en cochant la case correspondante. Les boutons **Sélectionner tout** et **Effacer tout** permettent d'activer tous les traps ou de désactiver toutes les cases. Consultez les fichiers MIB pour obtenir la liste des traps SNMP fournis. Reportez-vous à **Fichiers MIB** pour plus d'informations.
7. Dans le panneau **Destinations des traps**, entrez l'adresse IP de l'hôte et le numéro de port utilisés par les hôtes SNMP. Le port par défaut est **162**.
8. Dans le panneau **Destinations des traps**, tapez la chaîne **Communauté** et la **version** (**v1** ou **v2**) utilisées par les hôtes SNMP.
9. Cliquez sur **Ajouter** pour ajouter cet hôte de destination à la liste des hôtes configurés. Pour supprimer un hôte de la liste, sélectionnez-le et cliquez sur **Supprimer**. Vous pouvez inclure dans cette liste autant de gestionnaires que vous le souhaitez.
10. Une fois les traps SNMP et leurs destinations configurés, cliquez sur **Mettre à jour la configuration des traps**.

Configuration des clusters

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 aux utilisateurs actifs et connexions actives, et toutes les données relatives à l'état sont répliquées entre ces deux nœuds. Les nœuds primaire et secondaire d'un cluster doivent exécuter la même version du logiciel. A moins que cela ne soit défini par l'utilisateur, CC-SG attribue un nom par défaut à chaque nœud de cluster.

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 du nœud primaire. 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 à l'unité principale CC-SG détecteront que le nœud primaire ne répond pas et répondront alors aux requêtes émanant du nœud secondaire.

***Remarque** : dans une configuration de cluster, seule l'unité CC-SG principale communique avec CC-NOC. Lorsqu'une unité CC-SG devient primaire, elle envoie son adresse IP, en plus de celle de l'unité CC-SG secondaire, à CC-NOC.*

Créer un cluster

En cas de basculement, l'administrateur doit envoyer un e-mail à tous les utilisateurs CC-SG pour les prévenir d'utiliser l'adresse IP du nouveau nœud CC-SG primaire.

Important : il est recommandé de sauvegarder votre configuration sur les deux nœuds avant de configurer un cluster.

***Remarque** : une unité CC-SG doit exécuter ses ports réseau en mode **Principal/Sauvegarde** pour être utilisée pour la mise en cluster. Cette opération ne fonctionne pas avec une configuration Actif/Actif. Reportez-vous à **Configuration réseau** dans ce chapitre pour plus d'informations.*

Définir un nœud CC-SG primaire

1. Dans le menu **Administration**, cliquez sur **Configuration des clusters**. L'écran **Configuration des clusters** s'affiche.

2. Cliquez sur **Découvrir les appareils CommandCenter** pour analyser et afficher tous les appareils CC-SG dans le sous-ensemble que vous utilisez actuellement. Vous pouvez ajouter un CC-SG, d'un sous-réseau différent par exemple, en spécifiant une adresse IP dans **Adresse de CommandCenter** au bas de la fenêtre, puis en cliquant sur **Ajouter un appareil CommandCenter**.

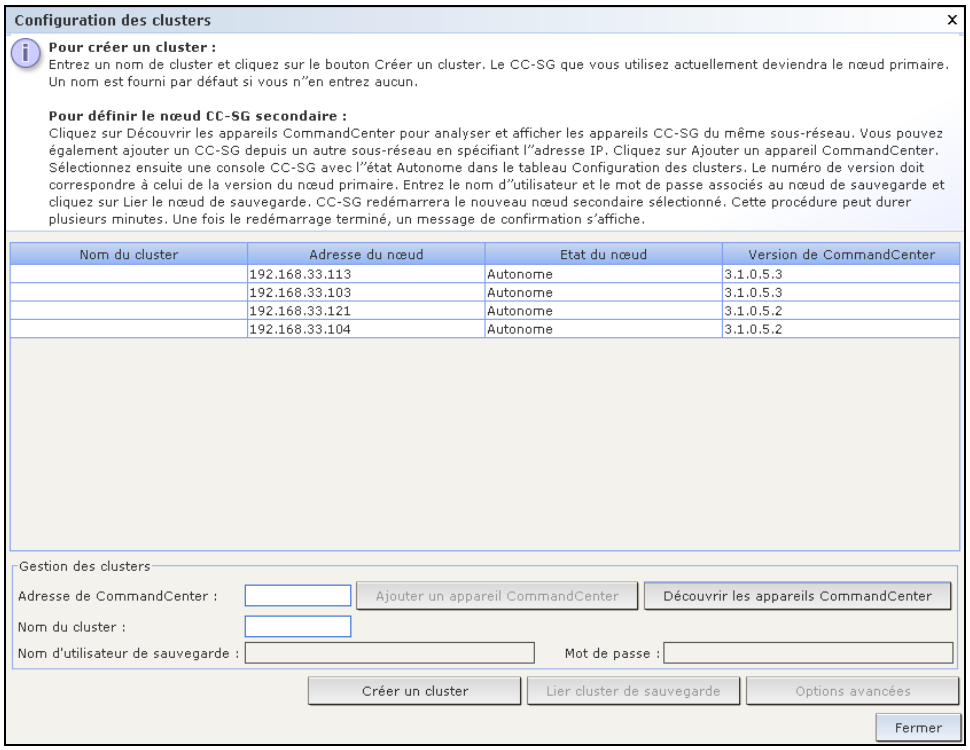

Figure 165 Ecran Configuration des clusters

3. Renseignez le champ **Nom du cluster**. Si vous n'entrez pas de nom maintenant, un nom par défaut sera fourni, tel que **cluster192.168.51.124**, à la création du cluster.
4. Cliquez sur **Créer un cluster**.

5. Cliquez sur **Oui** à l'invite si vous souhaitez poursuivre. L'unité CC-SG que vous utilisez actuellement devient nœud primaire et un nom par défaut est fourni si vous n'avez rien entré dans le champ **Nom du cluster**.

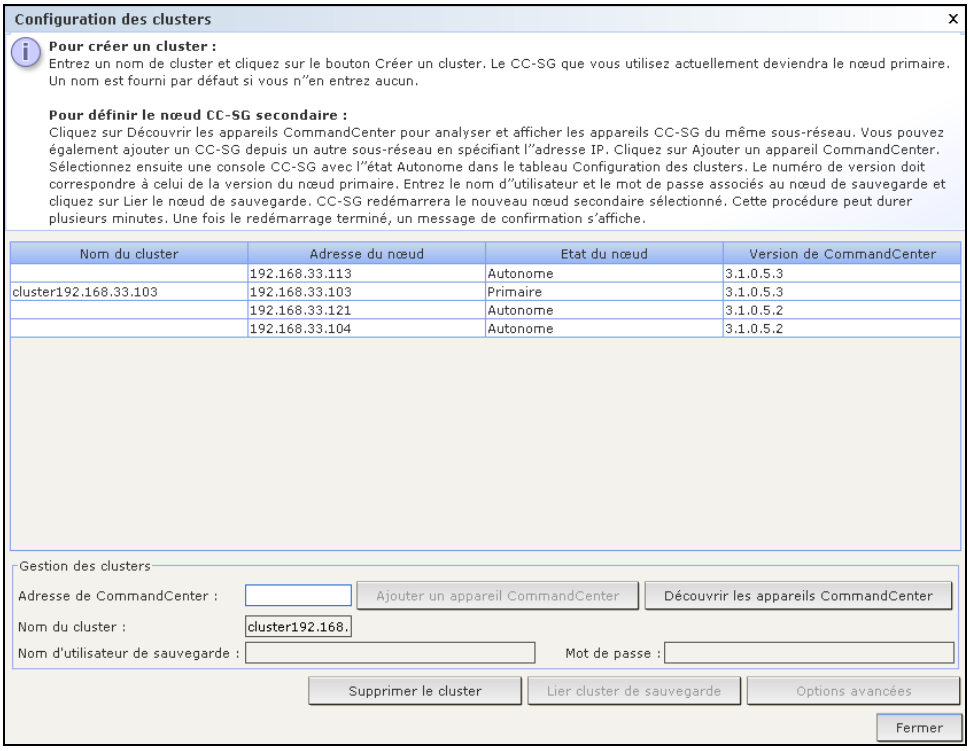

Figure 166 Configuration d'un cluster – Définition du nœud primaire

Définir un nœud CC-SG secondaire

1. Cliquez sur **Découvrir les appareils CommandCenter** pour analyser et afficher tous les appareils CC-SG dans le sous-ensemble que vous utilisez actuellement. Vous pouvez ajouter un CC-SG, d'un sous-réseau différent par exemple, en spécifiant une adresse IP dans **Adresse de CommandCenter** au bas de la fenêtre. Cliquez sur **Ajouter un appareil CommandCenter**.

***Remarque** : l'ajout d'un CC-SG de sauvegarde à partir d'un sous-réseau ou réseau différent permet d'éviter les problèmes affectant un réseau ou un emplacement physique unique.*

2. Pour ajouter un nœud secondaire, ou nœud CC-SG de sauvegarde, sélectionnez une unité CC-SG à l'état **Autonome** dans le tableau Configuration des clusters. Le numéro de version doit correspondre à celui du nœud primaire.
3. Entrez un nom d'utilisateur et un mot de passe valides pour le nœud de sauvegarde dans les champs **Nom d'utilisateur de sauvegarde** et **Mot de passe**.
4. Cliquez sur **Lier cluster de sauvegarde**.
5. Un message de confirmation s'affiche. Cliquez sur **Oui** pour attribuer l'état Secondaire au nœud sélectionné ou sur **Non** pour annuler.

Important : une fois le processus de liaison entamé, n'exécutez aucune autre fonction dans CC-SG avant la fin, comme indiqué à l'étape 6, ci-dessous.

6. Lorsque vous cliquez sur **Oui**, CC-SG redémarre le nouveau nœud secondaire sélectionné. Cette procédure peut durer plusieurs minutes. Une fois le redémarrage effectué, un message de confirmation s'affiche à l'écran.

7. Dans le menu **Administration**, cliquez sur l'option **Configuration des clusters** pour afficher le tableau mis à jour Configuration des clusters.

***Remarque** : si la communication est interrompue entre les nœuds primaire et secondaire, le nœud secondaire prend le rôle du nœud primaire. Lorsque la connectivité sera rétablie, vous aurez parfois deux nœuds primaires. Le cas échéant, retirez l'un d'entre eux et réinitialisez-le comme nœud secondaire.*

Supprimer un nœud CC-SG secondaire

1. Pour annuler le statut Nœud secondaire d'une unité CC-SG et réaffecter ce statut à une autre unité de votre configuration, sélectionnez le nœud CC-SG secondaire dans le tableau Configuration des clusters et cliquez sur **Supprimer le cluster de sauvegarde**.
2. Lorsque le message de confirmation s'affiche, cliquez sur **Oui** pour supprimer le statut Nœud secondaire ou sur **Non** pour annuler.

***Remarque** : en cliquant sur l'option **Supprimer le cluster de sauvegarde**, vous supprimez la désignation Nœud secondaire. L'unité secondaire CC-SG n'est pas effacée de votre configuration.*

Supprimer un nœud CC-SG primaire

1. Pour annuler le statut Nœud primaire d'une unité CC-SG et réaffecter ce statut à une autre unité de votre configuration, sélectionnez le nœud CC-SG primaire dans le tableau Configuration des clusters, puis cliquez sur **Supprimer le cluster**.
2. Lorsque le message de confirmation s'affiche, cliquez sur **Oui** pour supprimer le statut Nœud primaire ou sur **Non** pour annuler.

***Remarque** : en cliquant sur l'option **Supprimer le cluster**, vous ne supprimez pas l'unité primaire CC-SG de votre configuration ; cette action supprime simplement la désignation Nœud primaire. **Supprimer le cluster** est disponible uniquement en l'absence de nœuds de sauvegarde.*

Récupérer un nœud CC-SG défaillant

Si un nœud est défaillant et qu'un basculement se produit, l'état **En attente** du nœud indique sa récupération.

1. Sélectionnez le nœud En attente dans le tableau Configuration des clusters.
2. Ajoutez-le en tant que nœud de sauvegarde en cliquant sur **Lier nœud en attente**.
3. Un message de confirmation s'affiche. Cliquez sur **Oui** pour attribuer l'état Secondaire au nœud sélectionné ou sur **Non** pour annuler. Si vous cliquez sur **Oui**, vous devrez attendre que le nœud secondaire redémarre, de la même manière qu'avec **Lier cluster de sauvegarde**.

***Remarque** : lorsqu'un nœud passe au mode **En attente**, il peut être démarré en mode **Autonome** ou en mode **Sauvegarde**.*

Définir des paramètres avancés

Pour définir les paramètres avancés d'une configuration de clusters :

1. Sélectionnez le nœud primaire que vous venez de créer.
2. Cliquez sur **Options avancées**. La fenêtre **Paramètres avancés** s'affiche.

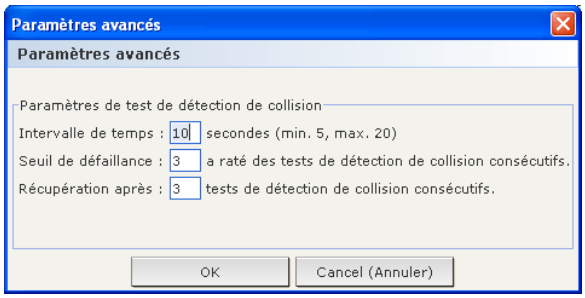

Figure 167 Paramètres avancés de la configuration des clusters

3. Dans le champ **Intervalle de temps**, entrez la fréquence à laquelle vous souhaitez que CC-SG vérifie sa connexion avec l'autre nœud.

***Remarque** : un intervalle de temps court augmente le trafic réseau généré par les tests de détection de collision consécutifs. Les clusters dont les nœuds sont très éloignés l'un de l'autre peuvent nécessiter des intervalles plus longs.*

4. Dans le champ **Seuil de défaillance**, entrez le nombre de tests de détection de collision consécutifs qui doivent être exécutés sans réponse avant qu'un nœud CC-SG ne soit considéré comme défaillant.
5. Dans le champ **Récupération après**, entrez le nombre de tests de détection de collision consécutifs qui doivent être renvoyés avec succès avant qu'une connexion défaillante ne soit considérée comme étant récupérée.
6. Cliquez sur **OK** pour enregistrer les paramètres.

***Remarque** : le changement de fuseau horaire est désactivé dans une configuration de clusters.*

Configuration de la 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, 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 au **Chapitre 9 : Configuration de l'authentification à distance** pour obtenir des instructions détaillées sur le paramétrage des serveurs d'authentification à distance.

Connexions client sécurisées

Dans le Gestionnaire de sécurité, vous pouvez configurer des paramètres de sécurité pour les connexions client vers CC-SG.

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** s'affiche.
2. Cliquez sur l'onglet **Généralités**.

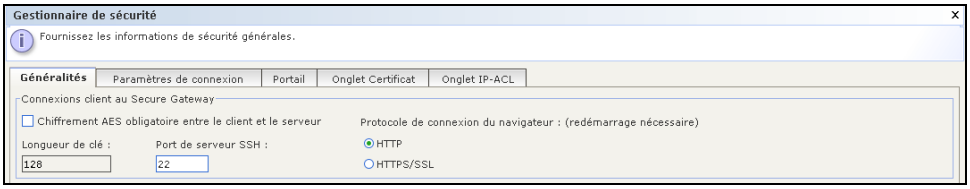

Figure 168 Connexions client sécurisées

3. Cochez la case **Chiffrement AES obligatoire entre le client et le serveur** pour établir des connexions AES chiffrées à CC-SG. Entrez la longueur de la clé de chiffrement souhaitée dans le champ **Longueur de clé**. La longueur de clé par défaut est **128**.
4. Entrez le numéro du port d'accès à CC-SG via SSH dans le champ **Port de serveur SSH**. Pour plus d'informations, reportez-vous à **Accès SSH à CC-SG**, plus loin dans ce chapitre.
5. Cliquez sur la case d'option **HTTP** ou **HTTP/SSL** pour sélectionner le protocole de connexion du navigateur que le client doit utiliser afin de se connecter à CC-SG. Vous devez redémarrer CC-SG pour que les modifications apportées à ce paramètre entrent en vigueur.
6. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

Paramètres de connexion

Les paramètres de connexion vous permettent de configurer les paramètres de mot de passe fort et de verrouillage.

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** s'affiche.
2. Cliquez sur l'onglet **Paramètres de connexion**.

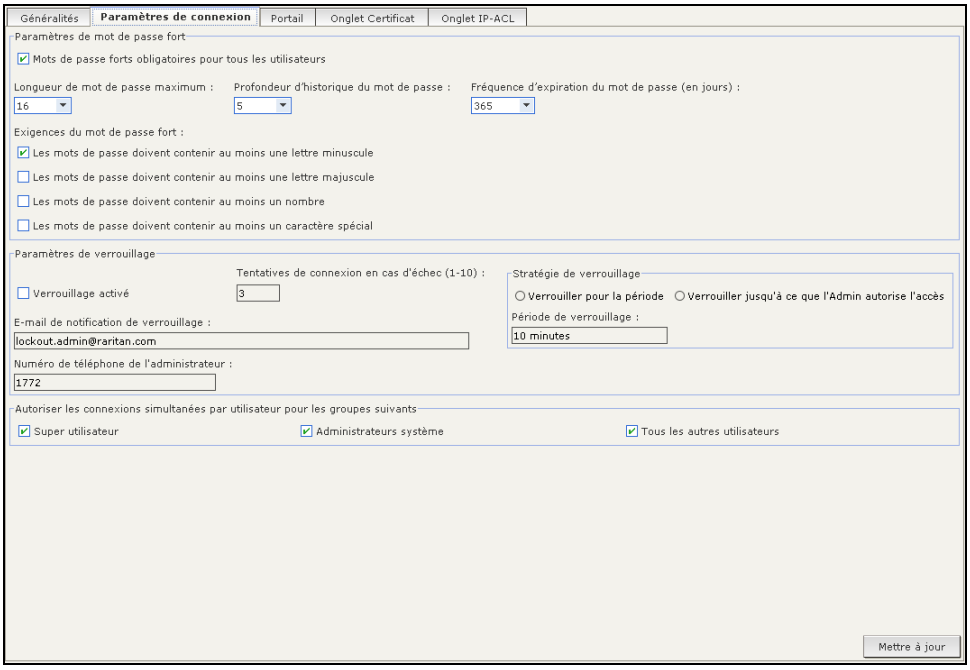

Figure 169 Paramètres de connexion

Paramètres de mot de passe fort

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, du moins en théorie. Les mots de passe forts ne sont pas activés par défaut dans CC-SG. Pour les utiliser, les administrateurs doivent d'abord cocher **Mots de passe forts obligatoires pour tous les utilisateurs**.

Remarque : *un mot de passe respectant toutes les exigences en matière de mot de passe fort est toujours obligatoire pour le super utilisateur CC.*

Une fois l'option activée, les administrateurs peuvent modifier les champs de la zone Paramètres de mot de passe fort afin de personnaliser leurs règles de mot de passe. La configuration de tous les mots de passe forts doit au moins répondre aux critères suivants :

- **Longueur de mot de passe maximum** – les mots de passe ne doivent pas dépasser un certain nombre de caractères. Cliquez sur le menu déroulant et sélectionnez la longueur maximum des mots de passe.
- **Profondeur d'historique du mot de passe** – cliquez sur le menu déroulant et sélectionnez le nombre de mots de passe précédents conservés dans l'historique. Les utilisateurs ne peuvent pas réutiliser un mot de passe de l'historique lorsqu'il leur est demandé d'en choisir un nouveau. Par exemple, si le champ d'**historique du mot de passe** indique 5, les utilisateurs ne peuvent pas réutiliser leurs 5 derniers mots de passe.
- **Fréquence d'expiration du mot de passe** – tous les mots de passe doivent expirer après un nombre défini de jours. Cliquez sur le menu déroulant et sélectionnez le nombre de jours de validité du mot de passe. Après l'expiration du mot de passe, les utilisateurs devront en choisir un nouveau à la connexion suivante.

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.

Sous **Exigences du mot de passe fort**, l'administrateur peut configurer des règles de mot de passe entraînant des exigences supplémentaires :

- 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).

Lorsque la configuration des règles de mot de passe fort est terminée, cliquez sur **Mettre à jour** pour enregistrer les paramètres. Toutes les règles sélectionnées sont cumulatives : les mots de passe doivent répondre à tous les critères configurés par l'administrateur. Une fois les règles de mot de passe fort configurées, tous les mots de passe suivants doivent répondre à ces critères et tous les utilisateurs doivent modifier leur mot de passe à la connexion suivante si les nouveaux critères sont plus exigeants 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 lui-même.

Raritan vous suggère d'utiliser la fonction **Message du jour** pour prévenir les utilisateurs que les règles de mot de passe fort vont changer et indiquer les nouveaux critères.

Paramètres de verrouillage

Les administrateurs peuvent verrouiller les utilisateurs de CC-SG, de CC-NOC et de SSH après un nombre donné d'échecs de tentative de connexion. Cette fonction s'applique aux utilisateurs authentifiés et autorisés localement par CC-SG et ne concerne pas ceux authentifiés à distance par des serveurs externes. Reportez-vous au Chapitre 9 : Configuration de l'authentification à istance pour plus d'informations. Les échecs de connexion dus à un nombre insuffisant de licences utilisateur ne sont pas non plus concernés.

***Remarque** : par défaut, le compte **admin** est verrouillé pendant cinq minutes après trois tentatives de connexion ayant échoué. Pour **admin**, le nombre d'échecs de connexion avant et après verrouillage n'est pas configurable.*

Pour configurer le verrouillage de l'utilisateur :

1. Cochez la case **Verrouillage activé**.
2. Par défaut, **3** échecs de connexion sont autorisés avant le verrouillage d'un utilisateur. Vous pouvez remplacer cette valeur par un chiffre compris entre **1** et **10**.
3. Choisissez une stratégie de verrouillage :
   a. Si vous choisissez **Verrouiller pour la période**, indiquez un délai (en minutes) pendant lequel l'utilisateur est verrouillé avant de pouvoir se connecter à nouveau. Par défaut, ce délai est de **5** minutes, mais vous pouvez indiquer une valeur comprise entre **1** minute et **1 440** 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.
   b. Si vous choisissez **Verrouiller jusqu'à ce que l'Admin autorise l'accès**, les utilisateurs sont verrouillés jusqu'à ce qu'un administrateur les autorise à se reconnecter. Pour apprendre comment déverrouiller un utilisateur, reportez-vous au **Chapitre 10 : Génération de rapports**.
4. Renseignez le champ **E-mail de notification de verrouillage** pour informer le destinataire qu'un verrouillage s'est produit. Si le champ est vide, aucune notification n'est envoyée.
5. Renseignez le champ **Numéro de téléphone de l'administrateur** au cas où l'administrateur devrait être contacté.
6. Cliquez sur **Mettre à jour** pour enregistrer les paramètres de configuration.

Autoriser les connexions simultanées par utilisateur

Ces paramètres permettent d'autoriser plusieurs sessions simultanées sur CC-SG avec un même nom d'utilisateur.

1. Cochez **Super utilisateur** pour autoriser plusieurs connexions simultanées à CC-SG avec le compte **admin**.
2. Cochez **Administrateurs système** pour autoriser plusieurs connexions simultanées des comptes du groupe d'utilisateurs **System Administrators**.
3. Cochez **Tous les autres utilisateurs** pour autoriser des connexions simultanées à tous les autres comptes.

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 un client. Pour accéder aux paramètres de portail :

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** s'affiche.
2. Cliquez sur l'onglet **Portail**.

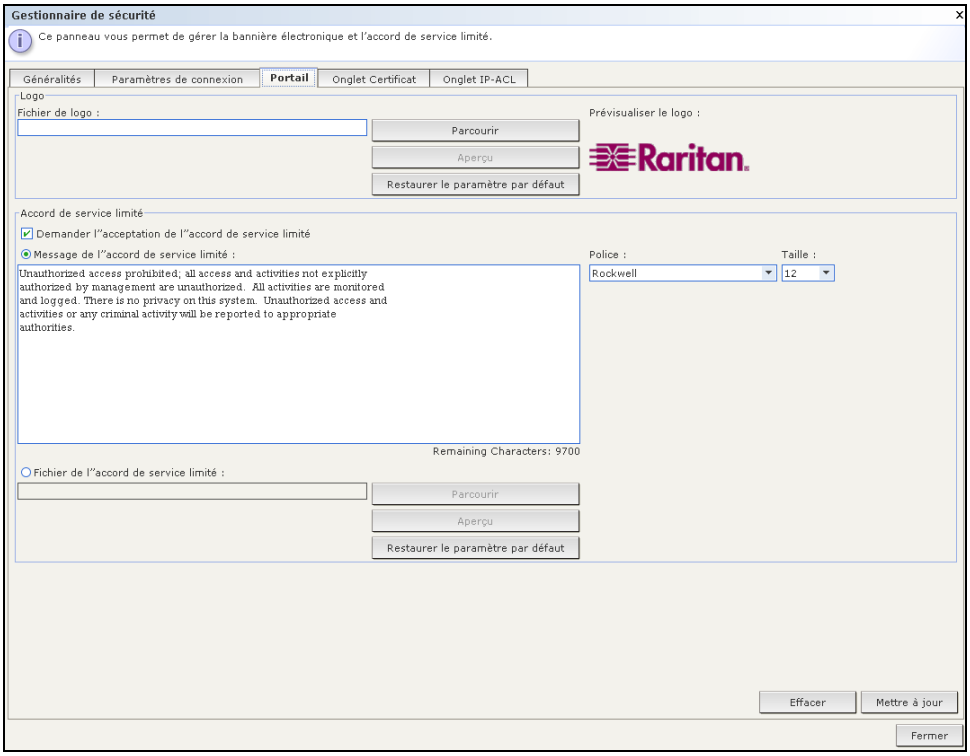

Figure 170 Paramètres de portail

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. Si vous le souhaitez, cliquez sur **Aperçu** pour prévisualiser le logo. Le fichier graphique sélectionné apparaît sur la droite.
4. Cliquez sur **Mettre à jour** pour enregistrer le changement de logo sur CC-SG.

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.

1. Cochez **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. Sélectionnez **Message de l'accord de service limité** si vous souhaitez entrer directement le texte de la bannière.
   a. Tapez le texte de l'accord dans le champ prévu à cet effet. La longueur maximum du message est de 10 000 caractères.
   b. Cliquez sur le menu déroulant **Police** et sélectionnez la police d'affichage du message.
   c. Cliquez sur le menu déroulant **Taille** et sélectionnez la taille d'affichage du message.

   Sélectionnez **Fichier de l'accord de service limité** pour charger un message à partir d'un fichier texte (.TXT).
   a. Cliquez sur **Parcourir**. Une fenêtre de dialogue s'affiche.
   b. 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.
   c. Cliquez sur **Aperçu** pour prévisualiser le texte du fichier. Il apparaît dans le champ de message de la bannière au-dessus.
3. Cliquez sur **Mettre à jour** pour enregistrer les modifications apportées à l'accord de service limité dans CC-SG.

Une fois les paramètres de logo et d'accord de service limité mis à jour, ils apparaissent sur l'écran de connexion lorsque l'utilisateur accède à un client.

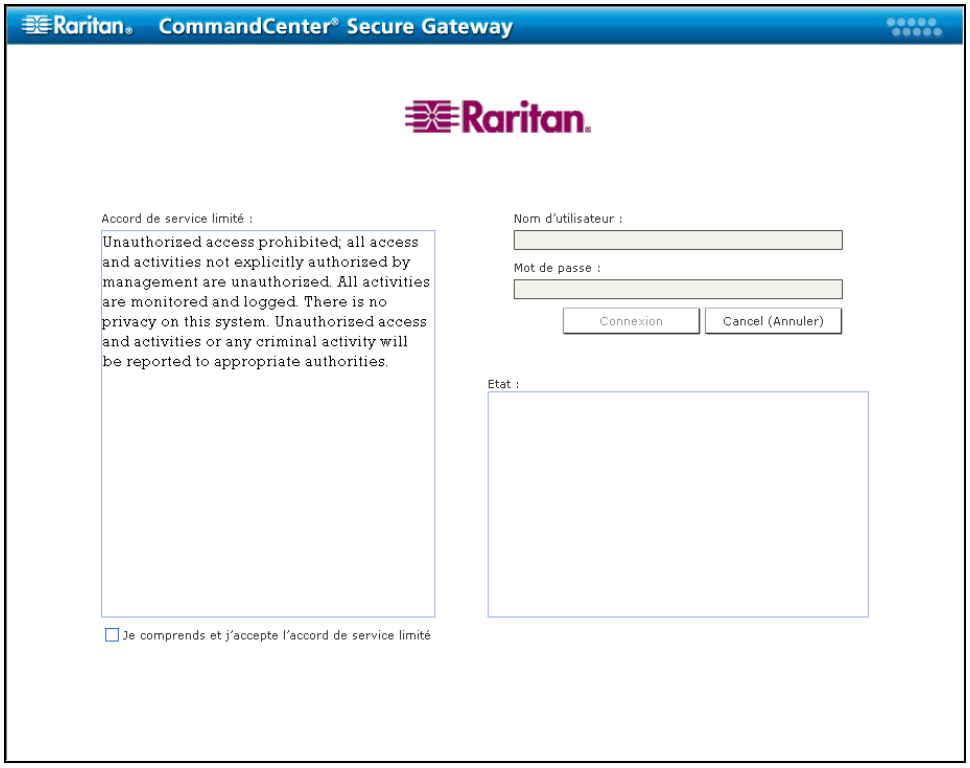

Figure 171 Portail de connexion avec accord de service limité

Certificat

Les options de cette fenêtre permettent de générer une demande de signature de certificat (ou demande de certification). Ce message est envoyé par un candidat à une autorité de certification pour demander un certificat d'identité numérique. Avant de créer la demande, le candidat génère une paire de clés, en gardant la clé privée secrète. La demande de certification contient des informations identifiant le candidat (par exemple, un nom de répertoire dans le cas d'un certificat X.509), et la clé publique choisie par le candidat.

***Remarque** : le bouton **Exporter** au bas de l'écran devient **Importer** ou **Générer**, selon l'option de certificat sélectionnée.*

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** s'affiche.
2. Cliquez sur l'onglet **Certificat**.

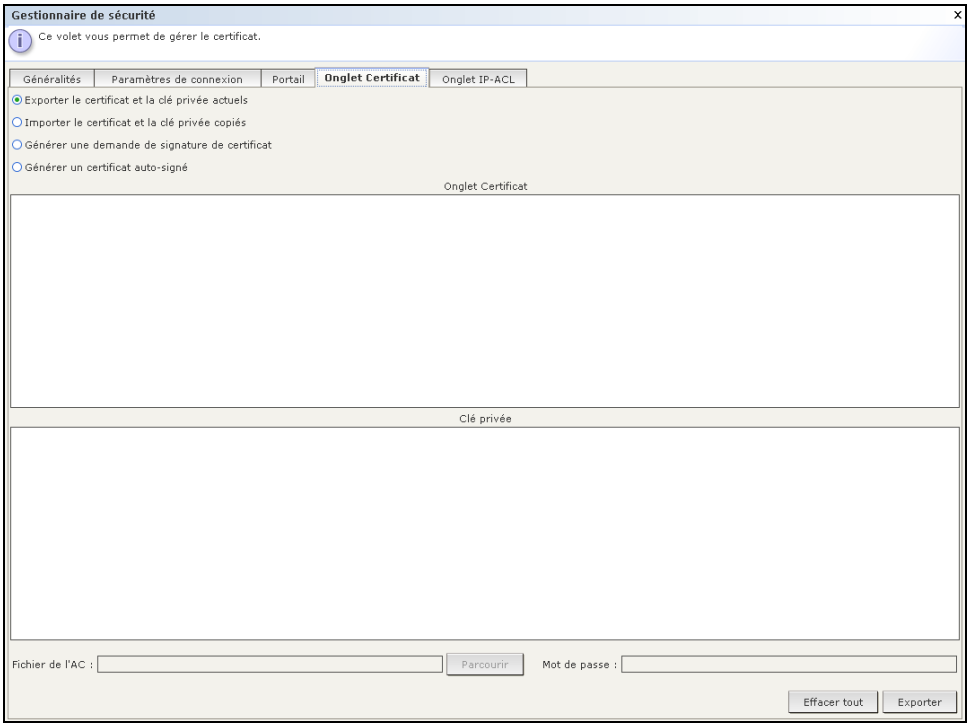

Figure 172 Ecran Gestionnaire de sécurité – Certificat

Exporter le certificat et la clé privée actuels

Cliquez sur **Exporter le certificat et la clé privée actuels**. Le certificat s'affiche dans le panneau **Certificat** et la clé privée s'affiche dans le panneau **Clé privée**. Copiez le texte des panneaux **Certificat** et **Clé privée** et validez-le en cliquant sur **Exporter**.

Générer une demande de signature de certificat

La section suivante explique comment générer une demande de signature de certificat et une clé privée sur l'unité CC-SG. Cette demande est soumise au serveur approprié qui émet un certificat signé. Un certificat racine est également exporté du serveur et enregistré dans un fichier. Le certificat signé, le certificat racine et la clé privée sont alors importés.

1. Cliquez sur **Générer une demande de signature de certificat**, puis sur **Générer**. La fenêtre **Générer une demande de signature de certificat** s'affiche.

2. Entrez les données requises pour la demande de signature de certificat dans les champs prévus à cet effet.

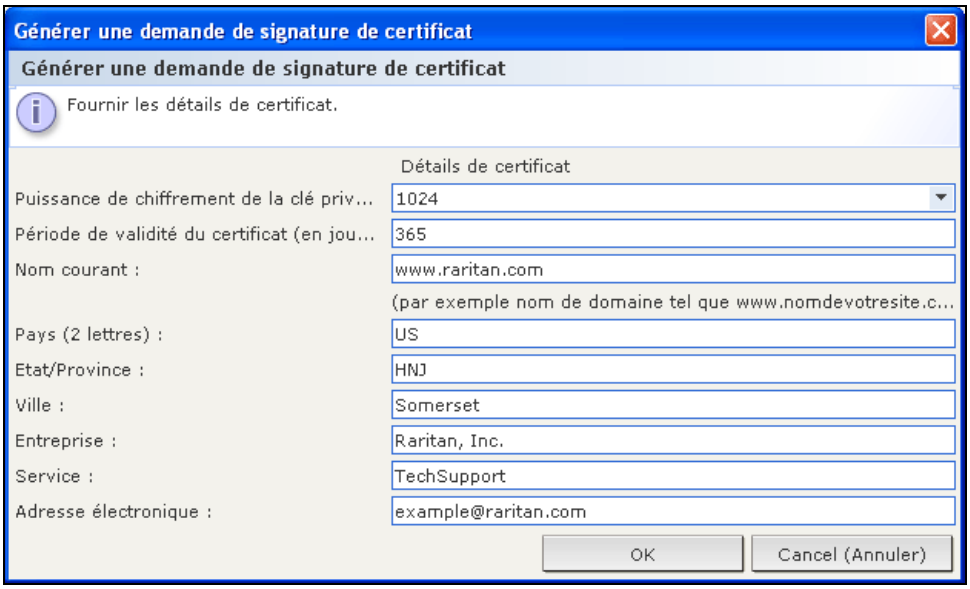

Figure 173 Ecran Générer une demande de signature de certificat

3. Cliquez sur **OK** pour générer la demande de signature de certificat ou sur **Cancel** (Annuler) pour fermer la fenêtre. La demande de signature de certificat et la clé privée apparaissent dans les champs correspondants de l'écran **Certificat**.

Figure 174 Demande de certificat générée

4. 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**.
5. Dans un éditeur ASCII, tel que le Bloc-notes, copiez et collez la clé privée dans un fichier de texte.
6. Soumettez le fichier CSR (**.cer**) enregistré à l'étape 4 au serveur approprié pour obtenir un certificat signé.
7. 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.
8. Lorsque vous avez reçu le certificat signé du serveur, cliquez sur **Importer le certificat et la clé privée copiés**.

9. Copiez et collez le certificat signé dans le champ **Demande de certificat**. Collez la clé privée enregistrée précédemment dans le champ **Clé privée**.
10. Cliquez sur **Parcourir** en regard du champ **Fichier de l'AC :** et sélectionnez le fichier de certificat racine enregistré à l'étape 6.
11. Tapez **raritan** dans le champ **Mot de passe** si la demande de signature de certificat a été générée par CC-SG. Si une application différente a généré la demande, utilisez le mot de passe associé à cette application.

***Remarque** : si le certificat importé est signé par une autorité de certification (AC) racine et sous-racine, l'utilisation d'un certificat racine ou sous-racine uniquement échouera. Pour résoudre ce problème, copiez et collez les certificats racine et sous-racine dans un fichier, puis importez ce dernier.*

Générer un certificat auto-signé

Activez la case d'option **Générer un certificat auto-signé**, puis cliquez sur **Générer**. La fenêtre **Générer un certificat auto-signé** s'affiche. Entrez les données requises pour le certificat auto-signé dans les champs prévus à cet effet. Cliquez sur **OK** pour générer le certificat ou sur **Cancel** (Annuler) pour fermer la fenêtre. Le certificat et la clé privée s'affichent sous forme cryptée dans les champs correspondants de l'écran **Certificat**.

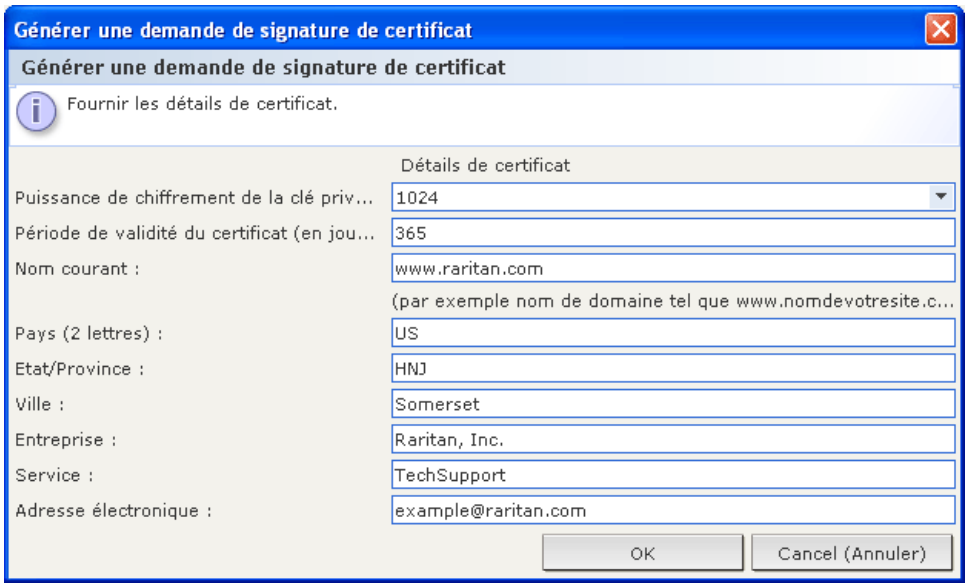

Figure 175 Fenêtre Générer un certificat auto-signé

IP-ACL

Cette fonctionnalité limite l'accès à l'unité CC-SG en fonction des adresses IP. Pour spécifier une liste de contrôle d'accès IP (IP-ACL), entrez une plage d'adresses IP, le groupe auquel elle s'applique et un privilège Autoriser/Refuser.

1. Dans le menu **Administration**, cliquez sur **Sécurité**. L'écran **Gestionnaire de sécurité** s'affiche.

2. Cliquez sur l'onglet **IP-ACL**.

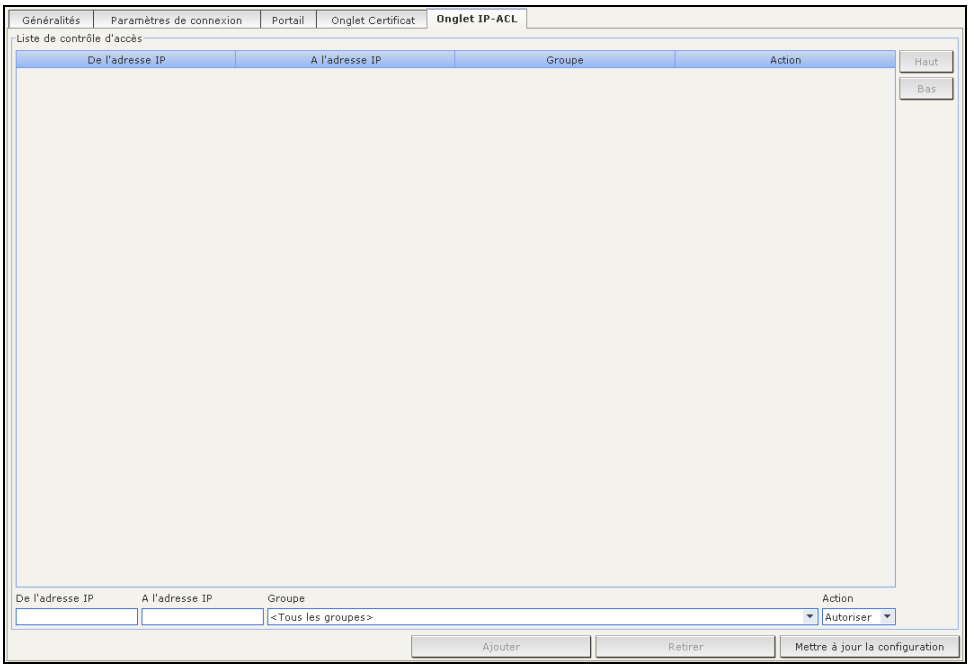

Figure 176 Ecran Gestionnaire de sécurité – IP-ACL

3. Pour modifier l'ordre des éléments de ligne de la **liste de contrôle d'accès**, sélectionnez l'élément de ligne et cliquez sur **Haut** ou **Bas**. La connexion des utilisateurs sera autorisée ou refusée, conformément à la première règle appliquée (de haut en bas).
4. Pour ajouter un élément à la liste, définissez une plage d'application de la règle en saisissant la valeur IP de départ dans le champ **De l'adresse IP**, et la valeur IP de fin dans le champ **A l'adresse IP**.
5. Cliquez sur la flèche déroulante **Groupe** pour sélectionner le groupe auquel la règle doit être appliquée.
6. Cliquez sur la flèche déroulante **Action** et indiquez si l'accès du groupe à la plage IP doit être autorisé ou refusé.
7. Cliquez sur **Ajouter** pour ajouter la règle à la liste de contrôle d'accès.
8. Pour effacer un élément de ligne, sélectionnez-le et cliquez sur **Supprimer**.
9. Cliquez sur **Mettre à jour la configuration** pour actualiser votre système avec les nouvelles règles de contrôle d'accès.

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**, plus loin dans ce chapitre pour plus d'informations. Après avoir configuré le serveur SMTP, vous pouvez choisir d'envoyer un e-mail de test au destinataire désigné et de prévenir celui-ci du résultat du test.

Pour configurer un serveur SMTP externe :

1. Dans le menu **Administration**, cliquez sur **Notifications**. L'écran **Gestionnaire des notifications** s'affiche.

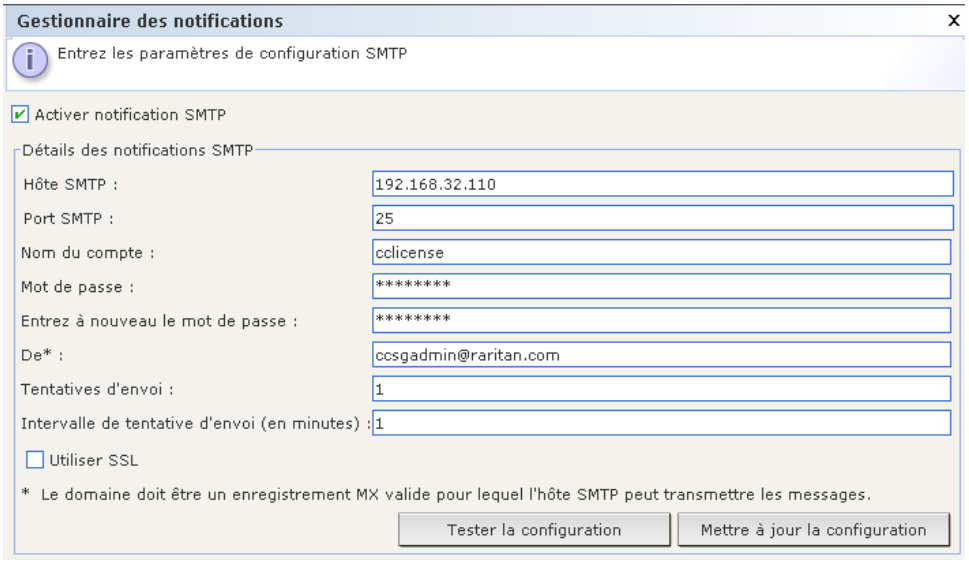

Figure 177 Gestionnaire des notifications

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** dans le **Chapitre 1 : Introduction**.
4. Entrez un numéro de port SMTP valide dans le champ **Port SMTP**.
5. Entrez un nom de compte valide permettant la connexion au serveur SMTP dans le champ **Nom du compte**.
6. Entrez le mot de passe du nom de compte dans les champs **Mot de passe** et **Entrez à nouveau le mot de passe**.
7. Entrez une adresse e-mail dans le champ **De** afin d'indiquer que les messages proviennent de CC-SG.
8. Dans le champ **Tentatives d'envoi**, entrez le nombre de fois où les messages électroniques doivent être renvoyés en cas d'échec.
9. Dans le champ **Intervalle de tentative d'envoi (en minutes)**, entrez le nombre de minutes, entre 1 et 60, qui doivent s'écouler entre les tentatives d'envoi.
10. Cochez **Utiliser SSL** si vous souhaitez un envoi sécurisé des messages via Secure Sockets Layer (SSL).
11. Cliquez sur **Tester la configuration** pour envoyer un message de test au compte SMTP spécifié. Assurez-vous que le message est bien arrivé.
12. Cliquez sur **Mettre à jour la configuration** pour enregistrer vos modifications.

Gestionnaire des tâches

Utilisez le gestionnaire des tâches pour programmer des tâches CC-SG quotidiennes, hebdomadaires, mensuelles ou annuelles. Une tâche peut être programmée pour une exécution unique ou périodique un jour particulier de la semaine et à un intervalle défini. Par exemple, il est possible de programmer des sauvegardes de dispositifs toutes les trois semaines le vendredi ou d'envoyer un rapport particulier tous les lundis à un ou plusieurs destinataires.

***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 :

- Sauvegarde de la configuration du dispositif (dispositif individuel ou groupe de dispositifs)
- Restauration de la configuration du dispositif (ne s'applique pas aux groupes de dispositifs)
- Copie de la configuration du dispositif (dispositif individuel ou groupe de dispositifs)
- Mise à niveau du firmware du dispositif (dispositif individuel ou groupe de dispositifs). Notez que le firmware doit être rendu accessible avant de programmer cette tâche.
- Sauvegarde de CC-SG
- Redémarrage du dispositif (ne s'applique pas aux groupes de dispositifs)
- Gestion de l'alimentation des ports de prise (Mise sous tension/hors tension/réactivation de ports de prise)
- Génération de tous les rapports (formats HTML ou CSV)
- Purge des journaux

Programmation 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.

Notifications par courrier électronique

Une fois la tâche effectuée, un e-mail peut être envoyé à un destinataire particulier. Dans le Gestionnaire des notifications, vous pouvez spécifier la destination et le mode d'envoi du message, par exemple s'il est envoyé de manière sécurisée via SSL. Reportez-vous à **Gestionnaire des notifications**, plus haut dans ce chapitre, pour plus d'informations.

Rapports programmés

Les rapports programmés sont envoyés par courrier électronique aux destinataires définis.

Tous les rapports associés à un état **Terminé** sont stockés sur CC-SG pendant 30 jours et peuvent être consultés au format HTML en sélectionnant **Rapports programmés** sous le menu **Rapports**. Reportez-vous au **Chapitre 10 : Génération de rapports, Rapports programmés** pour plus d'informations.

Créer une tâche

Pour programmer une nouvelle tâche :

1. Dans le menu **Administration**, cliquez sur **Tâches**. L'écran **Gestionnaire des tâches** s'affiche.

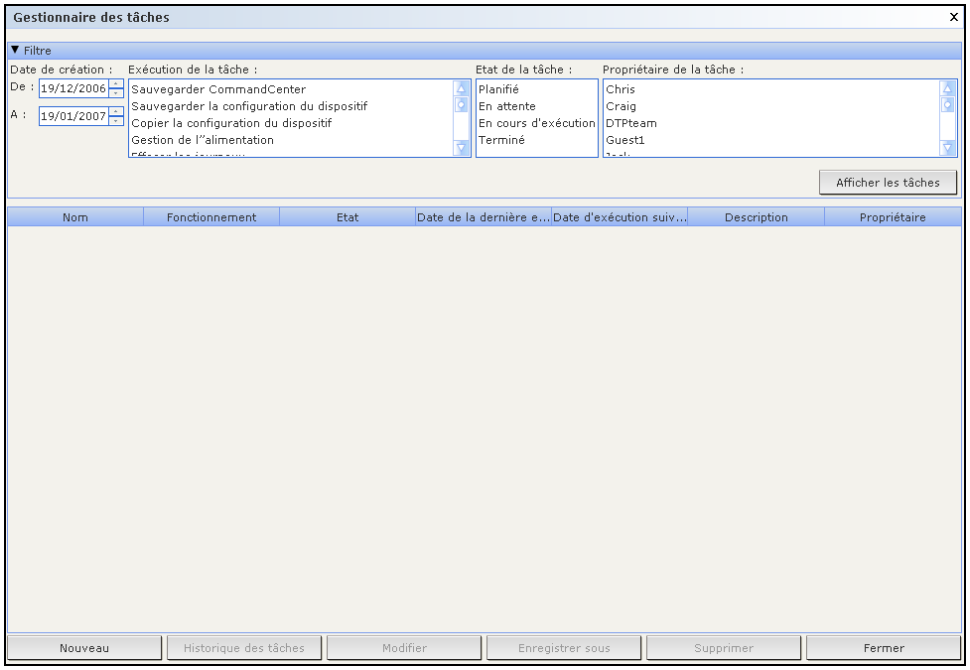

Figure 178 Gestionnaire des tâches

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**, puis sélectionnez dans la liste la tâche à programmer, par exemple **Mettre à niveau le firmware du dispositif**. Notez que les champs obligatoires varient suivant la tâche sélectionnée.
6. Cliquez sur l'onglet **Périodicité**.
7. Dans le champ **Période**, cliquez sur la case d'option correspondant à la fréquence souhaitée de la tâche programmée.
   - **Une fois** : utilisez les flèches haut et bas pour sélectionner l'**heure de début** de la tâche.
   - **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.
   - **Quotidienne** : cliquez sur la case d'option en regard de **Chaque jour** si vous souhaitez que la tâche se répète 7 jours par semaine. Cliquez sur la case d'option en regard de **Chaque jour de la semaine** si vous souhaitez que la tâche se répète chaque jour, du lundi au vendredi.
   - **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.
   - **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.
   - **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. Vous pouvez indiquer 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. Reportez-vous au **Chapitre 7 : Ajout et gestion des utilisateurs et des groupes d'utilisateurs** pour plus d'informations. Pour ajouter une autre adresse, cliquez sur **Ajouter**, entrez l'adresse électronique dans la fenêtre qui apparaît, puis cliquez sur **OK**. Par défaut, un e-mail est envoyé si l'exécution de la tâche aboutit. Pour prévenir les destinataires de l'échec des tâches, cochez la case **En cas d'échec**.
13. Cliquez sur **OK** pour enregistrer la tâche.

Afficher une tâche, les détails d'une tâche et l'historique des tâches

Pour afficher une tâche :

1. Dans le menu **Administration**, cliquez sur **Tâches**. L'écran **Gestionnaire des tâches** s'affiche.
2. Pour rechercher des tâches, utilisez les boutons haut et bas pour sélectionner la période qui doit être couverte par la recherche. Vous pouvez filtrer la liste davantage en sélectionnant une ou plusieurs tâches, un ou plusieurs états ou un ou plusieurs propriétaires (**Ctrl+clic**). Cliquez sur **Afficher les tâches** pour visualiser la liste de tâches.

- Pour effacer une tâche, sélectionnez-la, puis cliquez sur **Supprimer**.

Remarque : *vous ne pouvez pas supprimer une tâche en cours d'exécution.*

- Pour afficher l'historique d'une tâche, sélectionnez-la et cliquez sur **Historique des tâches**.
- Pour afficher les détails d'une tâche, double-cliquez dessus.
- Pour changer une tâche programmée, sélectionnez-la, puis cliquez sur **Modifier** pour ouvrir la fenêtre **Modifier la tâche**. Modifiez les spécifications de la tâche selon vos besoins, puis cliquez sur **Mettre à jour**. Reportez-vous à **Créer une tâche**, plus haut dans ce chapitre, pour obtenir la description des onglets.
- Pour créer une tâche en fonction d'une tâche configurée précédemment, sélectionnez la tâche à copier, puis cliquez sur **Enregistrer sous** pour ouvrir la fenêtre **Enregistrer la tâche sous**. Les informations de la tâche configurée précédemment sont indiquées dans les onglets. Modifiez les spécifications de la tâche selon vos besoins, puis cliquez sur **Mettre à jour**. Reportez-vous à **Créer une tâche**, plus haut dans ce chapitre, pour obtenir la description des onglets.

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.*

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.

Important : au cours de la procédure suivante, des codes de passe sont générés. Vous devez fournir ceux-ci à l'administrateur qui doit les intégrer à CC-NOC dans les cinq minutes. Evitez de transmettre ces codes par e-mail ou tout autre moyen électronique pour empêcher une interception éventuelle par des systèmes automatisés. Il est recommandé de les transmettre par téléphone ou par écrit à des intervenants de confiance.

Ajouter un CC-NOC

***Remarque** : pour créer une connexion valide, les paramètres d'heure définis sur le CC-NOC et CC-SG doivent être synchronisées. Pour effectuer cette synchronisation, il est recommandé d'utiliser un serveur NTP (Network Time Protocol). Aussi, le CC-NOC et CC-SG doivent être configurés pour utiliser un serveur NTP.*

1. Dans le menu **Accès**, cliquez sur **Configuration CC-NOC**. L'écran **Configuration CC-NOC** s'affiche.
2. Cliquez sur Ajouter. L'écran Ajouter une configuration CC-NOC s'affiche.
3. Sélectionnez la version de logiciel CC-NOC à ajouter et cliquez sur **Suivant**. La version 5.1 comporte moins de fonctionnalités d'intégration que la version 5.2 et les versions ultérieures et ne nécessite qu'un nom et une adresse IP. Pour plus d'informations sur CC-NOC 5.1, consultez le site **www.raritan.fr/support**. Cliquez sur **Manuels de produits**, puis sur **CommandCenter NOC**.

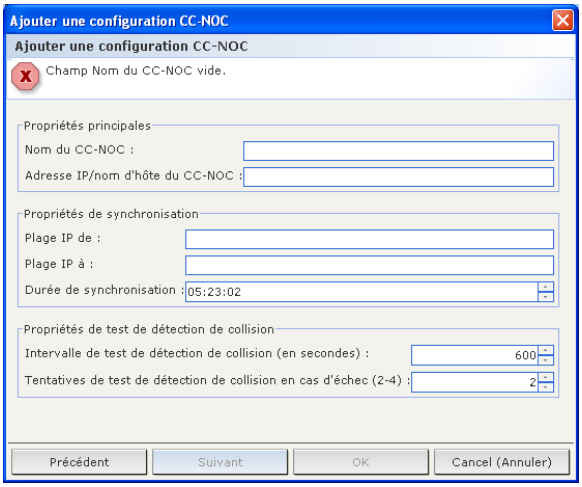

Figure 179 Ecran Ajouter une configuration CC-NOC

4. Entrez un nom descriptif de la console CC-NOC dans le champ **Nom du CC-NOC**. La longueur maximum est de 50 caractères alphanumériques.
5. Entrez l'adresse IP ou le nom d'hôte de la console CC-NOC dans le champ **Adresse IP/nom d'hôte du CC-NOC**. Ce champ est obligatoire. Pour connaître les règles des noms d'hôte, reportez-vous à **Terminologie et sigles** dans le **Chapitre 1 : Introduction**.

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**. Elle représente la plage d'adresses intéressant CC-SG et indique à la console CC-NOC d'envoyer des événements sur ces dispositifs à CC-SG. Elle est associée à la plage de détection configurée dans la console CC-NOC. Pour plus de détails, reportez-vous au **manuel de l'administrateur de CommandCenter NOC**. 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.

Pour arrêter la surveillance d'un dispositif par CC-NOC, vous pouvez lui affecter le statut *non géré*. Reportez-vous au **manuel de l'administrateur de CommandCenter NOC** pour plus d'informations.

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. Pour plus d'informations, reportez-vous à la section* ***Rapport Synchronisation CC-NOC*** *du* ***Chapitre 10 : Génération de rapports****.*

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 minutes) 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. En général, il n'est pas nécessaire de modifier cette valeur.
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. En général, il n'est pas nécessaire de modifier cette valeur.
10. Cliquez sur **Suivant**.

11. Copiez et collez les codes de passe dans les champs CC-NOC si vous êtes l'administrateur concerné, ou soumettez les deux codes à l'administrateur. Comme indiqué dans le **manuel de l'administrateur de CommandCenter NOC**, l'administrateur de CC-NOC entre alors ces codes de passe dans la console, ce qui déclenche un échange de certificats de sécurité.

Important : pour améliorer la sécurité, vous devez entrer les codes de passe dans la console CC-NOC dans les cinq minutes suivant leur génération sur CC-SG. Ceci réduit la possibilité pour les intrus de pénétrer dans le système par une attaque de force. Evitez de transmettre ces codes par e-mail ou tout autre moyen électronique pour empêcher une interception éventuelle par des systèmes automatisés. Il est recommandé de les transmettre par téléphone ou par écrit à des intervenants de confiance.

12. Une fois l'échange de certificats terminé, un canal sécurisé est établi entre le CC-NOC et l'unité CC-SG. Les données du CC-NOC sont copiées sur l'unité CC-SG. Cliquez sur **OK** pour terminer la procédure. Si celle-ci ne prend pas fin dans les **5** minutes, le délai expire, les données ne sont pas enregistrées sur l'unité CC-SG et les certificats stockés sont supprimés. Effectuez à nouveau la procédure ; allez à l'étape 1 de la section **Ajouter un CC-NOC** à la page 183.

Remarque : *CommandCenter NOC ne peut être ajouté que sur des serveurs CC-SG à nœud autonome ou primaire.*

Modifier un CC-NOC

1. Dans le menu **Accès**, cliquez sur **Configuration CC-NOC**. L'écran **Configuration CC-NOC** s'affiche.
2. Mettez en surbrillance un CC-NOC dans la liste et cliquez sur **Modifier**. L'écran **Modifier la configuration CC-NOC** s'affiche.
3. Modifiez la configuration selon vos besoins. Reportez-vous à la section précédente, **Ajouter un CC-NOC**, pour plus d'informations sur les champs.

Lancer un CC-NOC

Pour lancer un CC-NOC à partir de l'unité CC-SG :

1. Dans le menu **Accès**, cliquez sur **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

Pour retirer et désenregistrer un CC-NOC dans CC-SG, procédez comme suit.

1. Dans le menu **Accès**, cliquez sur **Configuration CC-NOC**. L'écran **Configuration CC-NOC** s'affiche.
2. Sélectionnez le CC-NOC à retirer de CC-SG, puis cliquez sur **Supprimer**. Vous êtes invité à confirmer la suppression.
3. Cliquez sur **Oui** pour supprimer le CC-NOC. Un message de suppression de CC-NOC confirme que l'unité a bien été supprimée.

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 sont accessibles via SSH pour administrer des dispositifs et CC-SG lui-même.

L'utilisateur du client SSH est authentifié par l'unité CC-SG dans laquelle des stratégies d'authentification et d'autorisation sont appliquées au client SSH. Les commandes disponibles pour le client SSH sont déterminées par les autorisations des groupes d'utilisateurs auxquels l'utilisateur du client SSH appartient.

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

Pour accéder à CC-SG via SSH :

1. Lancez un client SSH, tel que Putty.
2. Entrez l'adresse IP de CC-SG et **22** pour le port, puis ouvrez la connexion. La configuration du port pour l'accès SSH s'effectue dans le Gestionnaire de sécurité. Reportez-vous à Gestionnaire de sécurité plus haut dans ce chapitre pour plus d'informations.
3. A l'invite, connectez-vous avec vos nom d'utilisateur et mot de passe CC-SG.
4. Une invite de commande apparaît. Tapez **ls** pour afficher toutes les commandes disponibles. Vous pouvez taper **?** ou **help** pour afficher la description et le format de saisie de toutes les commandes.

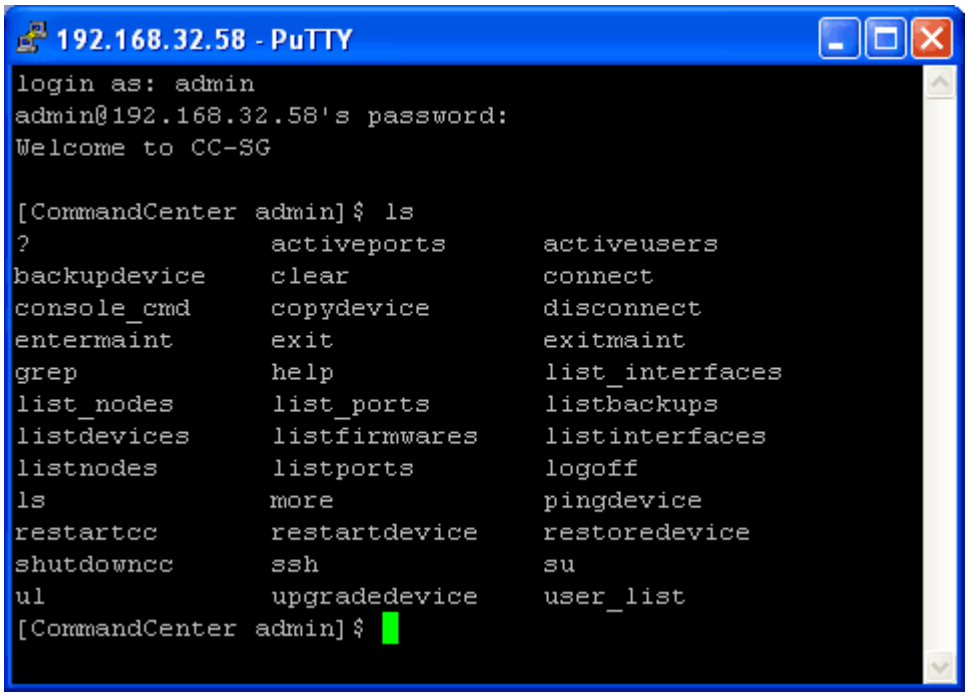

Figure 180 Commandes CC-SG via SSH

Commandes SSH

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

DESCRIPTION DE LA COMMANDE
activeports Répertorie les ports actifs.
activeusers Répertorie les utilisateurs actifs.
backup device <[-host <hôte>] | [-id <id_dispositif>]> nom_sauvegarde [description] Sauvegarde la configuration du dispositif.
clear Efface l'écran.
connect [-d <nom_dispositif>] [-e <car_echap>] <[-i <id_interface>] | [-n <nom_port>] | [id_port]> Etablit la connexion à un port série. Si <nom_port> ou <nom_dispositif> contient des espaces, il doit être entouré de guillemets.
copydevice <[-b <id_sauvegarde>] | [hôte_dispositif_source]> hôte_dispositif_cible Copie la configuration du dispositif.
disconnect <[-u <nomutilisateur>] [-p <id_port>] [-id <id_connexion>]> Ferme la connexion du port.
entermaint minutes [message] Place CC-SG en mode de maintenance.
exitmaint Sort CommandCenter du mode de maintenance.
grep terme_recherche Recherche du texte dans le flux de sortie redirigé.
help Affiche l'écran d'aide.
listbackups <[-id <id_dispositif>] | [hôte]> Répertorie les sauvegardes de configuration du dispositif disponibles.
listdevices Répertorie les dispositifs disponibles.
listfirmwares [[-id <id_dispositif>] | [hôte]] Répertorie les versions de firmware disponibles pour la mise à niveau.
listinterfaces [-id <id_nœud>] Répertorie toutes les interfaces.
listnodes Répertorie tous les nœuds.
listports [[-id <id_dispositif>] | [hôte]] Répertorie tous les ports.
logoff [-u <nomutilisateur>] message Déconnecte l'utilisateur.
ls Répertorie les commandes.

more [-p <taille_page>] Effectue la pagination.
pingdevice <[-id <id_dispositif>] | [hôte]> Envoie une commande ping au dispositif.
restartcc minutes [message] Redémarre CC-SG.
restartdevice <[-id <id_dispositif>] | [hôte]> Redémarre le dispositif.
restoredevice <[-host <hôte>] | [-id <id_dispositif>]> [id_sauvegarde] Restaure la configuration du dispositif.
shutdowncc minutes [message] Arrête CC-SG.
ssh [-e <car_échap>] <[-id <id_dispositif>] | [hôte]> Ouvre une connexion SSH à un dispositif SX.
su [-u <nom_utilisateur>] Modifie un utilisateur.
upgradedevice <[-id <id_dispositif>] | [hôte]> Met à niveau le firmware du dispositif.
exit Ferme une session SSH.

Tapez la commande suivie du commutateur **-h** pour afficher l'aide de cette commande, par exemple **listfirmwares -h**.

Astuces sur les commandes

La section suivante décrit différentes nuances des commandes SSH :

- 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 dans le **Chapitre 1 : Introduction**.
- Les commandes copydevice et restartdevice s'appliquent seulement à quelques dispositifs Raritan, par exemple Dominion SX. Les serveurs IPMI, les dispositifs génériques ne sont pas pris en charge par ces commandes.

Créer une connexion SSH à un dispositif SX

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

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

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

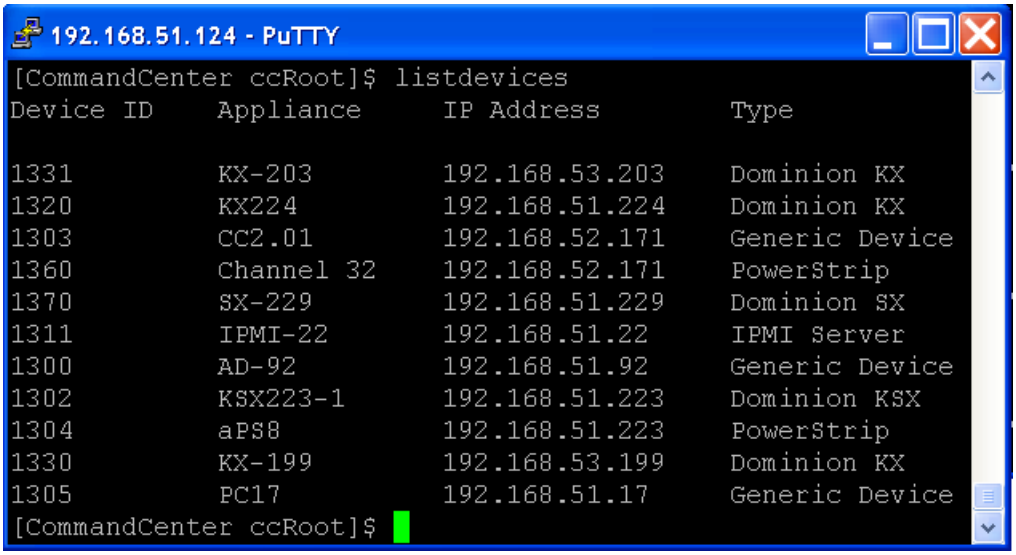

Figure 181 Liste des dispositifs sur CC-SG

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

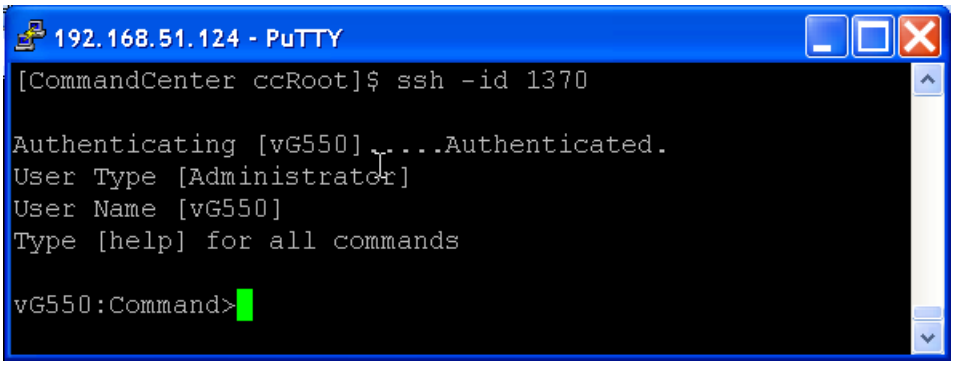

Figure 182 Accès à un dispositif SX via SSH

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.

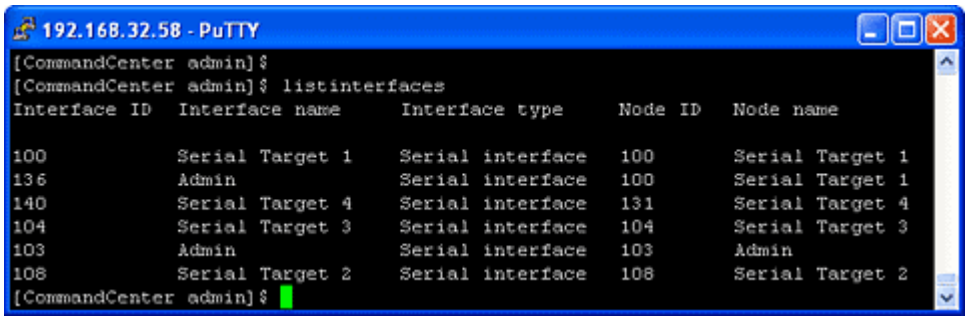

Figure 183 Listinterfaces dans SSH

2. Tapez **`connect –i <id_interface>`** pour vous connecter au nœud associé à l'interface.

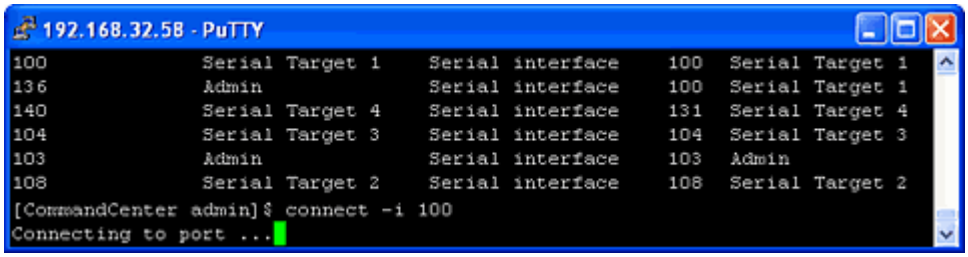

Figure 184 Se connecter à un nœud via une interface série hors bande

3. Une fois connecté au nœud, appuyez sur les touches d'échappement par défaut « ~ » suivi d'un point « **.** ». Vous pouvez alors entrer des commandes ou alias spécifiques comme décrit ci-après :

COMMANDE	ALIAS	DESCRIPTION
quit	**q**	Met fin à la connexion et retourne à l'invite SSH.
get_write	**gw**	Obtient un accès en écriture. Permet à l'utilisateur SSH d'exécuter des commandes sur le serveur alors que l'utilisateur du navigateur peut uniquement observer les procédures.
get_history	**gh**	Extrait l'historique. Affiche les dernières commandes et résultats du serveur cible.
send_break	**sb**	Envoie une rupture. Interrompt la boucle dans le serveur cible émanant de l'utilisateur du navigateur.
help	**?,h**	Imprime l'écran d'aide.

Quitter une session

Pour mettre fin entièrement à la connexion SSH à CC-SG, tapez **`exit`**.

Console de diagnostic

La console de diagnostic est une interface standard, non graphique, qui fournit un accès local à CC-SG. Elle est accessible à partir d'un port série ou KVM, ou de clients Secure Shell (SSH), par exemple Putty ou OpenSSH Client.

Deux noms de connexion sont fournis : **status**, qui donne accès à la console d'état et **admin**, qui donne accès à la console d'administrateur. Tous les noms d'utilisateur et mots de passe de connexion sont sensibles à la casse.

A propos de la console d'état

Dans la configuration par défaut, la console d'état ne requiert pas de mot de passe. Tapez **status** à l'invite **login** pour afficher les données système actuelles et déterminer l'état de CC-SG, des divers services utilisés par CC-SG et du réseau connecté.

A propos de la console d'administrateur

Les nom d'utilisateur/mot de passe par défaut de la console d'administrateur sont **admin/raritan**. Le compte admin vous permet de définir certains paramètres initiaux, d'établir la configuration réseau initiale, de déboguer des fichiers journaux et d'effectuer des diagnostics limités, comme redémarrer CC-SG. Le compte **admin** de la console de diagnostic est différent et distinct du compte et du mot de passe **admin** utilisés dans le Director Client de l'administrateur CC-SG et du client d'accès html. Vous pouvez utiliser le même mot de passe ou des mots de passe différents pour les deux comptes. La modification d'un de ces mots de passe n'affecte pas l'autre.

Remarque : *si vous accédez à la console de diagnostic via SSH, les consoles d'état et d'administrateur héritent des paramètres d'apparence configurés dans votre client SSH et des associations de clavier, qui pourraient différer de la présente documentation.*

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. Le moniteur doit détecter un signal, et la saisie de <Retour> au clavier doit appeler une invite de connexion à l'écran.

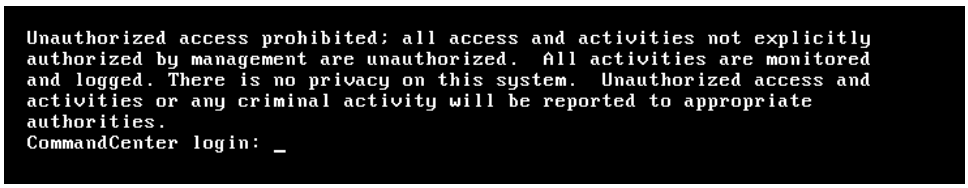

Figure 185 Connexion à la console de diagnostic

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, et spécifiez **23** pour le port.
3. Cliquez sur le bouton permettant la connexion. Une fenêtre s'ouvre pour vous demander vos identifiants de connexion.

Accéder à la console d'état

L'accès à la console d'état ne nécessite pas de mot de passe, mais il est possible d'en imposer l'usage.

1. A l'invite de connexion, tapez **status**. La console d'état en lecture seule apparaît.

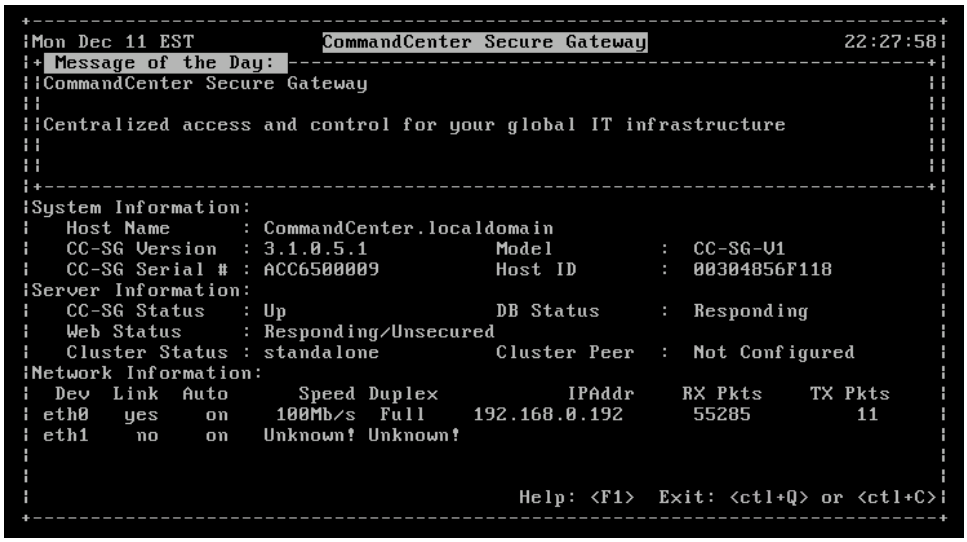

Figure 186 Console d'état

- Cet écran affiche de manière dynamique des informations sur l'état du système et indique si la console CC-SG et ses sous-composants fonctionnent.
- L'heure affichée dans le coin supérieur droit de l'écran indique la dernière interrogation des données sur l'unité CC-SG.
- Les informations de cet écran sont actualisées toutes les 5 secondes environ.
- Appuyez sur les touches **Ctrl-L** pour effacer l'écran actuel et recharger des informations à jour. Vous pouvez actualiser l'écran une fois par seconde au maximum.
- Appuyez sur les touches **Ctrl-Q** ou **Ctrl-C** pour quitter l'écran.
- La console d'état n'accepte aucune autre saisie ni navigation d'écran. Toutes les autres saisies sont ignorées.

Le tableau suivant décrit les états de CC-SG et de sa base de données :

ETAT	DESCRIPTION
Etat de CC-SG : Up (actif)	CC-SG est disponible.
Etat de CC-SG : Down (inactif)	CC-SG peut être en cours de réamorçage. Si l'état **Down** se poursuit, essayez de redémarrer CC-SG.
Etat de CC-SG : Restarting (redémarrage)	CC-SG est en cours de redémarrage.
Etat de la BD : Responding (réponse)	La base de données de CC-SG est disponible.
Etat de la BD : Down (inactif)	CC-SG peut être en cours de réamorçage.

Accéder à la console d'administrateur

***Remarque** : toutes les informations affichées dans la console d'administrateur sont statiques. Si des changements sont apportés à la configuration via l'interface graphique CC-SG ou la console de diagnostic, vous devez vous reconnecter à la console d'administrateur pour voir apparaître ces modifications.*

1. A l'invite de connexion, tapez **admin**.

2. Tapez le mot de passe CC-SG. Le mot de passe par défaut est **raritan**. A la première connexion, ce mot de passe expire et vous devez en choisir un nouveau. Entrez ce mot de passe et, à l'invite, tapez un nouveau mot de passe. Reportez-vous à **Mots de passe de la console de diagnostic (Admin)** plus loin dans ce chapitre pour plus d'informations sur la définition de la force du mot de passe.
3. L'écran principal de la console d'administrateur apparaît. Vous pouvez effectuer une configuration initiale de l'interface réseau système, modifier le message du jour dans la fenêtre Status et afficher des fichiers journaux. Le menu File (fichier) vous permet de quitter la console d'administrateur.

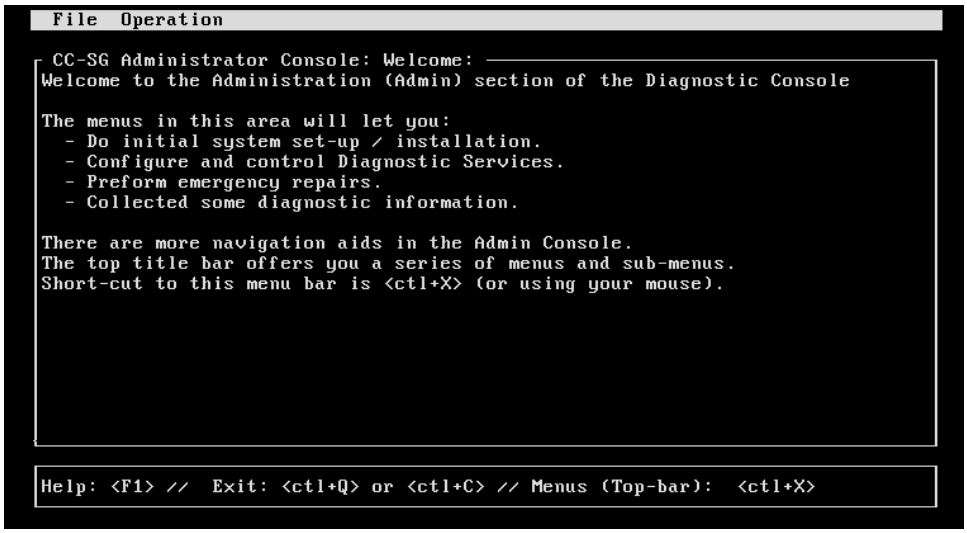

Figure 187 Console d'administrateur

Naviguer dans la console d'administrateur

Le tableau suivant vous indique les diverses méthodes de navigation au sein des menus de la console de diagnostic. Pour certaines sessions (SSH en particulier), la souris peut également être utilisée pour naviguer dans les différents écrans. Toutefois, ces manipulations ne sont peut-être pas possibles sur certains clients SSH ou sur la console KVM.

APPUYEZ SUR	POUR
CTRL+C ou CTRL+Q	Quitter la console de diagnostic.
CTRL+L	Effacer l'écran et retracer les informations (qui ne sont pas mises à jour ni rafraîchies).
TAB	Passer à l'option disponible suivante.
ESPACE	Sélectionner l'option en cours.
les touches de direction	Vous déplacer entre les champs dans une option.
la souris	Pointer sur une option et la sélectionner, le cas échéant.

Modifier l'accord de service limité et le message du jour dans la console de diagnostic

Le message Accord de service limité apparaît dans la console d'administrateur après la saisie d'un nom d'utilisateur et avant celle du mot de passe. Le message du jour (MOTD) s'affiche en haut de la console d'état.

1. Pour modifier l'accord de service limité (appelé message de préconnexion dans la console de diagnostic) ou le message du jour, cliquez sur **Operation**, **Diagnostic Console Config** (configuration de la console de diagnostic), puis sur **Edit Pre-Login Message** (modifier le message de préconnexion) ou **Edit MOTD** (modifier le message du jour).

2. A l'aide des touches **Supprimer** et **Retour arrière**, entrez un nouveau message dans la case prévue à cet effet. Pour le message du jour, vous pouvez entrer jusqu'à 76 caractères.

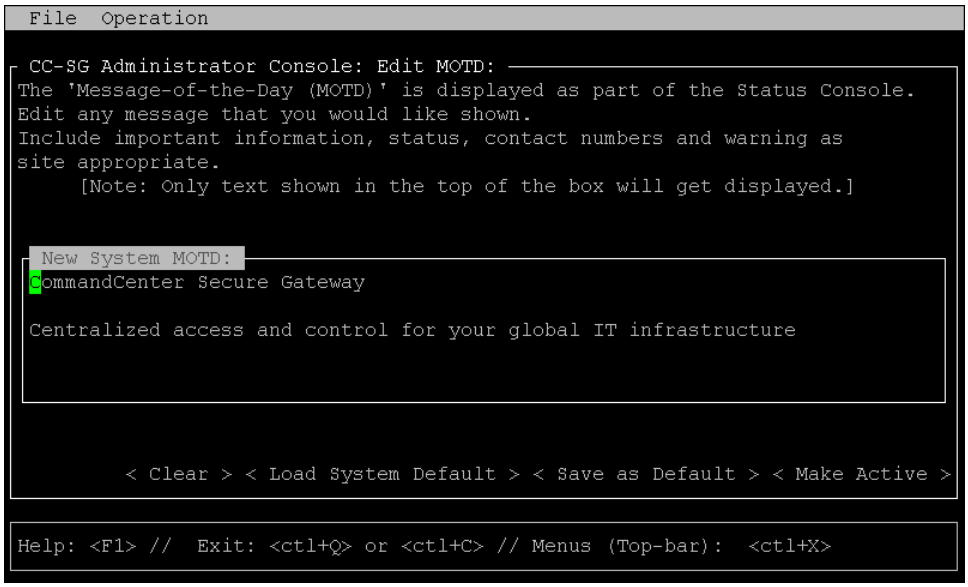

Figure 188 Modification du message du jour pour la console d'état

3. Cliquez sur **Make Active** (activer) au bas de l'écran, ou appuyez sur la touche **TAB** jusqu'à ce que **Make Active** soit sélectionné, et appuyez une fois sur la **BARRE D'ESPACEMENT**.
4. Les messages de préconnexion et du jour disposent de trois mémoires tampon ou zones distinctes :

- Ecran Admin Console – commence par une copie du tampon de message actif et peut être modifié par cet utilisateur / cette session.
- Une mémoire tampon système qui contient un prototype ou un modèle de message et est conservée pendant les réinitialisations du système.
- La mémoire tampon Active Message (telle que la voit l'utilisateur lorsqu'il interagit avec le système). Elle est conservée pendant les redémarrages et réamorçages du système.

BOUTON	DESCRIPTION
Clear	Retire tout le texte de l'écran de la console d'administrateur affiché. N'a aucun effet sur la valeur utilisée par le système.
Load System Default	Remplace l'écran de la console d'administrateur par le contenu de la mémoire tampon système.
Save as Default	Place l'écran de la console d'administrateur actif dans la mémoire tampon système. N'a aucun effet sur l'affichage du message actif.
Make Active	Remplace le message actif actuel par le contenu de l'écran de la console d'administrateur. Tous les nouveaux utilisateurs verront le nouveau message.

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 Secure Shell (SSH). Pour chaque type de port, vous pouvez décider si des connexions **status** ou **admin** sont autorisées et si le personnel d'assistance sur site peut également accéder à la console de diagnostic depuis le port. Pour les SSH, vous pouvez également configurer le numéro de port à utiliser, s'il n'est pas encore employé par un autre service CC-SG.

Pour modifier la configuration de la console de diagnostic :

1. Cliquez sur **Operation**, **Diagnostic Console Config**, puis sur **Diagnostic Console Service**.

2. Cliquez ou utilisez les touches **TAB**, ↓↑ et **Entrée** pour déterminer comment vous souhaitez configurer la console de diagnostic et y accéder. Il existe trois mécanismes d'accès à la console de diagnostic : port série (COM1), console KVM, SSH (réseau IP). La console de diagnostic offre trois services : Affichage d'état (Status Display), Console d'administration (Admin Console), Assistance sur site Raritan (Raritan Field Support). Cet écran permet de sélectionner les services disponibles via les différents mécanismes d'accès.
3. Entrez le numéro de port que vous souhaitez définir pour l'accès SSH à la console de diagnostic dans le champ **Port**. Le port par défaut est **23**.

Important : veillez à ne pas verrouiller complètement tous les accès Administrateur ou Assistance sur site.

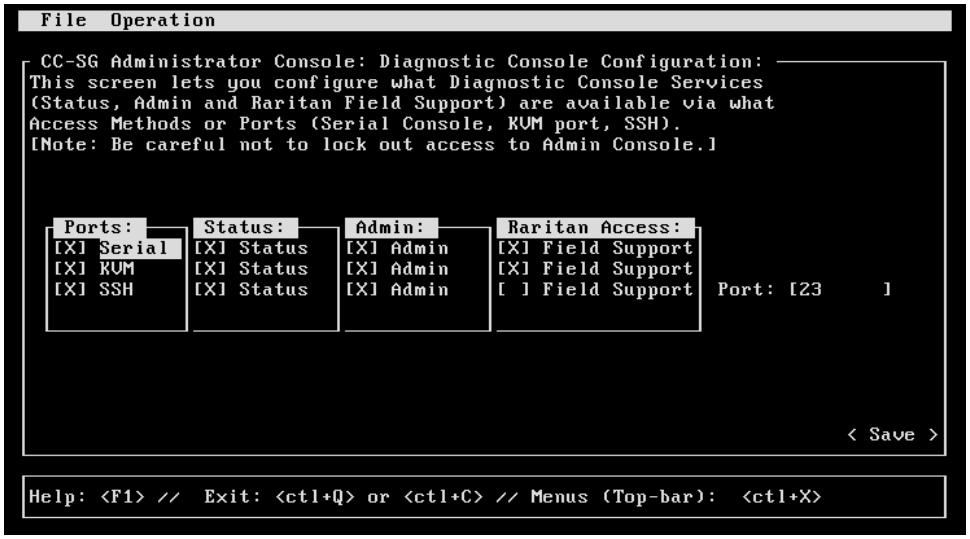

Figure 189 Modifier la configuration de la console de diagnostic

4. Cliquez sur **Save** (enregistrer) au bas de l'écran ou appuyez sur la touche **TAB** jusqu'à ce que **Save** soit sélectionné, puis sur **Entrée**.

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. Cliquez ou utilisez les touches **TAB** et de direction pour naviguer. Appuyez sur la touche **Entrée** pour sélectionner une valeur.

1. Pour modifier les données d'interface réseau, cliquez sur **Operation**, **Network Interfaces** (interfaces réseau), puis sur **Network Interface Config** (configuration des interfaces réseau).

2. Si les interfaces réseau sont déjà configurées, vous verrez un message d'**avertissement** indiquant que vous devez utiliser l'interface graphique CC-SG (Director Client de l'administrateur) pour les paramétrer. Si vous souhaitez poursuivre, cliquez sur **YES**. L'écran par défaut de configuration des interfaces réseau est présenté ici :

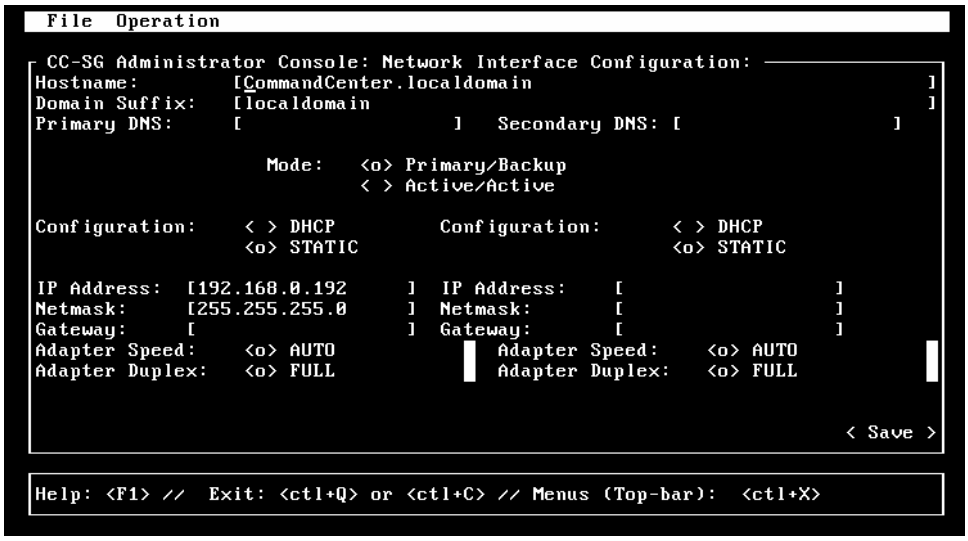

Figure 190 Modifier les interfaces réseau

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, le cas échéant. Pour connaître les règles des noms d'hôte, reportez-vous à **Terminologie et sigles** dans le **Chapitre 1 : Introduction**.
4. Dans le champ Mode, sélectionnez **Primary/Backup Mode** (mode principal/sauvegarde) ou **Active/Active Mode**. Reportez-vous à **Configuration réseau** plus haut dans ce chapitre pour plus d'informations. Appuyez sur la touche **TAB** pour sélectionner le champ, puis sur les flèches de direction pour choisir un des deux modes. Pour sélectionner un mode, appuyez sur la **BARRE D'ESPACEMENT**.
5. Cliquez ou appuyez sur la touche **TAB** jusqu'à **Configuration Field** (champ de configuration), et sélectionnez **DHCP** ou **Static** dans la liste.
   - 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 que vous vous reconnectez à la console d'administrateur.
   - Si vous choisissez **Static**, renseignez les champs **IP Address** (obligatoire), **Netmask** (obligatoire), **Default Gateway** (facultatif), **Primary DNS** (facultatif) et **Secondary DNS** (facultatif), et entrez un nom de domaine dans le champ **Domain Suffix** (facultatif).
   - Même si DHCP est utilisé pour déterminer la configuration IP d'une interface, une **adresse IP** et un **masque réseau** formatés correctement doivent être fournis.
6. A l'aide de la touche **TAB**, accédez à **Adapter Speed** ou cliquez dessus, et utilisez les touches ↓↑ pour sélectionner une vitesse de ligne dans la liste. Les autres valeurs 10, 100 et 1000 Mbps figurent dans une liste déroulante (où une seule valeur est visible à la fois) ; les touches ↓↑ permettent d'y accéder, et <**ESPACE**> permet de sélectionner une autre valeur (le cas échéant).
7. Si vous n'avez pas choisi **AUTO** pour **Adapter Speed**, cliquez sur **Adapter Duplex** et utilisez les touches ↓↑ pour sélectionner un mode duplex (**FULL** ou **HALF**) dans la liste, le cas échéant. Même s'il est toujours possible de sélectionner un mode duplex, il ne prend effet que si la valeur du champ **Adapter Speed** n'est pas **AUTO**.
8. Si vous avez sélectionné l'option **Active/Active Mode**, répétez ces étapes pour la seconde interface réseau.

9. Sélectionnez **Save** pour enregistrer les modifications. L'unité CC-SG est redémarrée, 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. Sélectionnez <**YES**> pour continuer.
10. La progression du système peut être surveillée dans l'écran d'état de la console de diagnostic. Sur le port KVM, une autre session de terminal peut être sélectionnée par la saisie de <**ALT**>+<**F2**> et la connexion sous le nom **status**. Pour retourner à la session de terminal d'origine, tapez <**ALT**>+<**F1**>. Six sessions de terminal sont disponibles de <**F1**> à <**F6**>. Pour un accès SSH, le lancement d'une autre session SSH à partir du client et la connexion sous le nom **status** fonctionnent tant que la reconfiguration du réseau permet la connectivité.

Envoyer une commande ping à une adresse IP (Interfaces réseau)

Utilisez la commande ping pour vérifier si la connexion entre l'ordinateur CC-SG et une adresse IP particulière fonctionne correctement.

***Remarque** : certains sites bloquent explicitement les requêtes ping. Assurez-vous que la cible et le réseau concerné autorisent les commandes ping avant de penser à un éventuel problème.*

1. Cliquez sur **Operation**, **Network Interfaces**, puis sur **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. Si vous le souhaitez, sélectionnez :

OPTION	DESCRIPTION
Show other received ICMP packets	Sortie détaillée, qui répertorie d'autres paquets ICMP reçus en plus des paquets ECHO_RESPONSE. Survient rarement.
No DNS Resolution	Ne résout pas les adresses des noms d'hôte.
Record Route	Enregistre la route. Définit l'option de route de l'enregistrement IP, qui stockera la route du paquet dans l'en-tête IP.
Use Broadcast Address	Autorise l'envoi d'une commande ping à un message à diffusion générale.
Adaptive Timing	Commande ping adaptable. L'intervalle interpaquets s'adapte à la durée aller-retour, afin qu'il n'existe pas plus d'une inspection sans réponse sur le réseau. L'intervalle minimum est de 200 millisecondes.

4. Vous pouvez également entrer des valeurs pour le nombre de secondes d'exécution de la commande ping, le nombre de requêtes ping envoyées et la taille des paquets ping (la valeur par défaut est 56, qui donne 64 octets de données ICMP lorsqu'elle est combinée aux 8 octets des données d'en-tête ICMP). Si les champs restent vides, les valeurs par défaut sont utilisées.
5. Cliquez sur **Ping** dans le coin inférieur droit de la fenêtre. 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, une panne s'est produite quelque part entre votre ordinateur et le domaine. Dans ce cas, la prochaine étape consiste à effectuer une détermination d'itinéraire. Reportez-vous à la section suivante pour plus d'informations.
6. Appuyez sur **CTRL+C** pour mettre fin à la session ping. Le système présente l'invite **Return?** avant de retourner à la console de diagnostic (les sorties peuvent ainsi être visualisées et analysées comme il convient).

***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 (Interfaces réseau)

La détermination d'itinéraire est souvent utilisée pour le dépannage du réseau. En affichant une liste des routeurs traversés, elle vous permet d'identifier le chemin emprunté par votre ordinateur pour atteindre une destination particulière sur le réseau. Elle répertorie tous les routeurs traversés jusqu'à sa destination ou son échec et son rejet. De plus, elle vous indique la durée du « saut » d'un routeur à un autre. Vous pouvez ainsi identifier les problèmes d'acheminement ou les pare-feu qui peuvent bloquer l'accès à un site.

Pour exécuter une détermination d'itinéraire sur une adresse IP ou un nom d'hôte :

1. Cliquez sur **Operation**, **Network Interfaces**, puis sur **Traceroute**.
2. Entrez l'adresse IP ou le nom d'hôte de la cible que vous souhaitez vérifier dans le champ **Traceroute Target**.
3. Si vous le souhaitez, sélectionnez :

OPTION	DESCRIPTION
Verbose	Sortie détaillée, qui répertorie les paquets ICMP reçus, autres que TIME_EXCEEDED et UNREACHABLE.
No DNS Resolution	Ne résout pas les adresses des noms d'hôte.
Use ICMP (vs. normal UDP)	Utilisez ICMP ECHO au lieu des datagrammes UDP.

4. Le cas échéant, entrez des valeurs pour le nombre de sauts que la commande de détermination d'itinéraire utilisera dans les paquets d'inspection sortants (la valeur par défaut est 30), le port de destination UDP à utiliser dans les inspections (la valeur par défaut est 33434) et la taille des paquets de détermination d'itinéraire. Si les champs restent vides, les valeurs par défaut sont utilisées.
5. Cliquez sur **Traceroute** dans le coin inférieur droit de la fenêtre.
6. Appuyez sur **Ctrl+C** ou **Ctrl+Q** pour mettre fin à la session de détermination d'itinéraire. Une invite **Return?** apparaît ; appuyez sur **Entrée** 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 des routes statiques (Interfaces réseau)

Dans Static Routes, vous pouvez consulter le tableau de l'acheminement IP actuel et modifier, ajouter ou supprimer des routes. L'utilisation et le placement précis des routes statiques peuvent réellement améliorer les performances de votre réseau, vous permettant ainsi de conserver de la bande passante pour des applications de gestion importantes. Ils peuvent également être utiles pour les paramètres Réseau actif/actif où chaque interface est reliée à un domaine IP distinct. Reportez-vous à la section Configuration réseau du Chapitre 12 : Administration avancée pour plus d'informations. Cliquez avec la souris ou utilisez les touches **TAB**, ↓↑ pour naviguer et appuyez sur la touche **Entrée** pour sélectionner une valeur.

Pour visualiser ou modifier des routes statiques :

1. Cliquez sur **Operation**, **Network Interfaces**, puis sur **Static Routes**.

2. Le tableau d'acheminement IP actuel s'affiche. Vous pouvez ajouter une route hôte ou réseau, ou supprimer une route. Le bouton <**Refresh**> met à jour les informations d'acheminement du tableau ci-dessus.

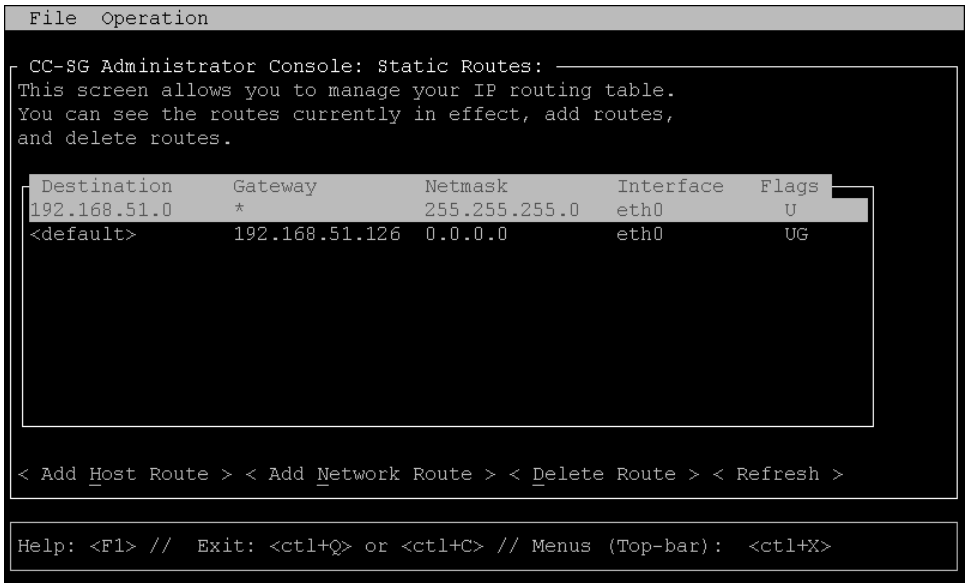

Figure 191 Modification des routes statiques

Afficher les fichiers journaux (Admin)

Vous pouvez visualiser un fichier journal ou en consulter plusieurs simultanément via LogViewer, qui permet la consultation de plusieurs fichiers à la fois, pour examiner l'activité du système.

Pour afficher les fichiers journaux :

1. Cliquez sur **Operation**, **Admin**, puis **System Logfile Viewer**.
2. L'écran Logviewer se divise en 4 zones principales (voir l'écran ci-dessous) :
   - 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 (détails ci-dessous).
   - Sélecteur Export/View (exporter/afficher).

3. Cliquez ou utilisez les touches de direction pour vous déplacer, et appuyez sur la **BARRE D'ESPACEMENT** pour sélectionner un fichier journal en le signalant par un **X**. Vous pouvez visualiser plusieurs fichiers journaux à la fois.

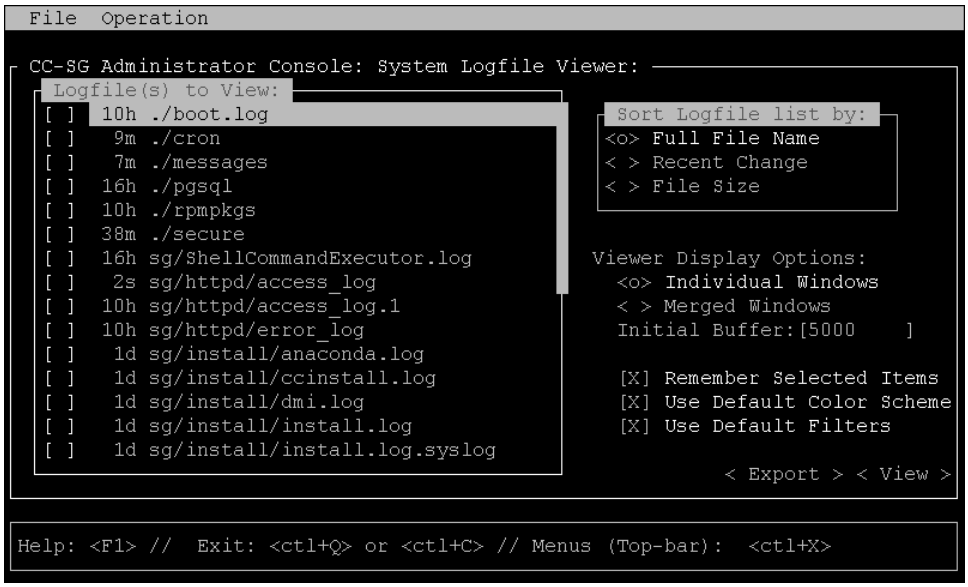

Figure 192 Sélection des fichiers journaux à afficher

La liste des fichiers journaux n'est mise à jour qu'à l'activation de la liste associée (par exemple, l'utilisateur entre dans la zone de liste des fichiers journaux) ou à la sélection d'une nouvelle option de tri. Les noms de fichier sont précédés d'un cachet indiquant la dernière réception de données par le fichier journal ou sa taille. Les cachets indiquent s → secondes, m → minutes, h → heures et d → jours. La taille de fichier indique B → Octets, K → Kilo (1000) octets, M → Méga (1 000 000) octets et G → Gigaoctets. Les cachets sont utilisés avec les options de tri Full Name ou Recent Change, et les tailles de fichier avec File Sizes.

La fenêtre Sort Logfile list by: se compose d'un ensemble de cases d'option (s'excluant mutuellement) et contrôle l'ordre d'affichage des fichiers journaux dans la fenêtre Logfile to View.

OPTION	DESCRIPTION
Individual Windows	Affiche les journaux sélectionnés dans des sous-fenêtres distinctes.
Merged Windows	Fusionne les journaux sélectionnés dans une fenêtre d'affichage.
Initial Buffer	Paramètre la mémoire tampon ou la taille de l'historique initiales. **5000** est la valeur par défaut. Ce système est configuré pour mettre en mémoire tampon toutes les nouvelles informations qui se présentent.
Remember Selected Items	Si cette case est cochée, les sélections de fichier journal actuelles (le cas échéant) seront conservées. Sinon, la sélection est réinitialisée chaque fois qu'une nouvelle liste de fichiers journaux est générée. Ceci est utile si vous souhaitez parcourir les fichiers.
Use Default Color Scheme	Si cette case est cochée, certains fichiers journaux seront affichés avec un jeu de couleurs standard. Remarque : des commandes multitail peuvent être utilisées pour modifier le jeu de couleurs lorsque les fichiers journaux sont ouverts.

Use Default Filters	Si cette case est cochée, des filtres automatiques 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 :

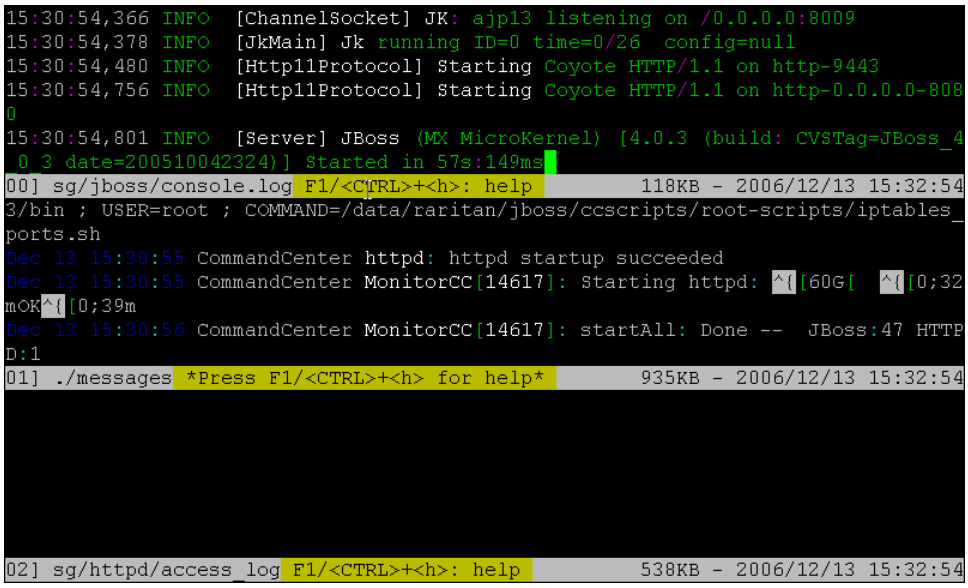

Figure 193 Sélection des fichiers journaux à afficher

4. Lorsque vous visualisez les fichiers journaux, tapez **q, Ctrl-Q** ou **Ctrl+C** pour retourner à l'écran précédent.
5. 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 si vous avez décidé d'en consulter plusieurs.

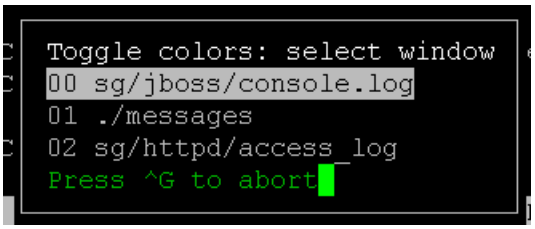

Figure 194 Modification des couleurs des fichiers journaux

6. 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.*

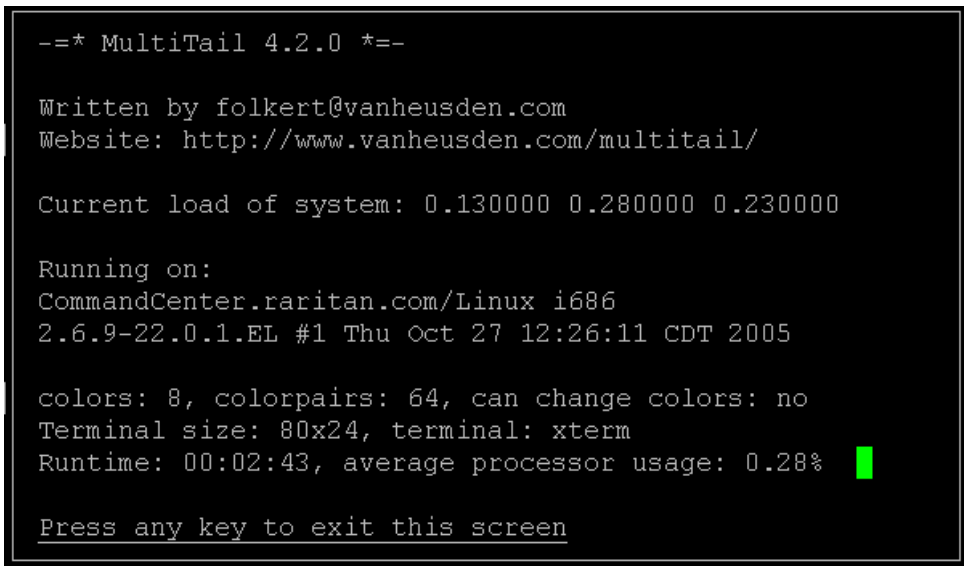

Figure 195 Affichage des informations

7. Le cas échéant, vous pouvez filtrer le fichier journal à l'aide d'une expression standard. Entrez **e** pour ajouter ou modifier une expression standard et sélectionnez un journal dans la liste si vous avez décidé d'en consulter plusieurs.

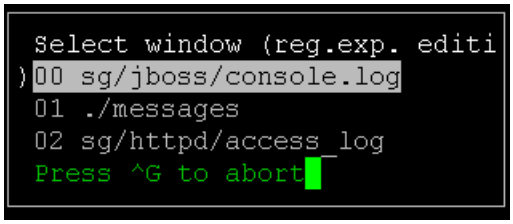

Figure 196 Modification des expressions dans les fichiers journaux

8. Entrez **a** pour ajouter une expression standard. Par exemple, si vous souhaitez 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.*

Figure 197 Définition d'une expression standard pour un fichier journal

9. Sélectionnez **F1** pour obtenir de l'aide sur toutes les options LogViewer. Appuyez sur les touches **Ctrl+C** et **Ctrl+Q** pour mettre fin à la session de LogViewer.

Redémarrer l'unité CC-SG (Admin)

Vous pouvez redémarrer CC-SG, qui déconnectera tous ses utilisateurs actuels et mettra fin à leurs sessions sur les serveurs cible distants.

Important : il est FORTEMENT recommandé de redémarrer l'unité CC-SG dans l'interface utilisateur graphique CC-SG, à moins qu'il ne soit absolument indispensable de la redémarrer ici. Reportez-vous à **Redémarrage de CC-SG** dans le **Chapitre 11 : Maintenance du système** pour plus d'informations. Le redémarrage de CC-SG dans la console de diagnostic NE PREVIENDRA PAS les utilisateurs de l'interface utilisateur graphique CC-SG du redémarrage.

Pour redémarrer CC-SG :

1. Cliquez sur **Operation**, **Admin**, puis sur **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.

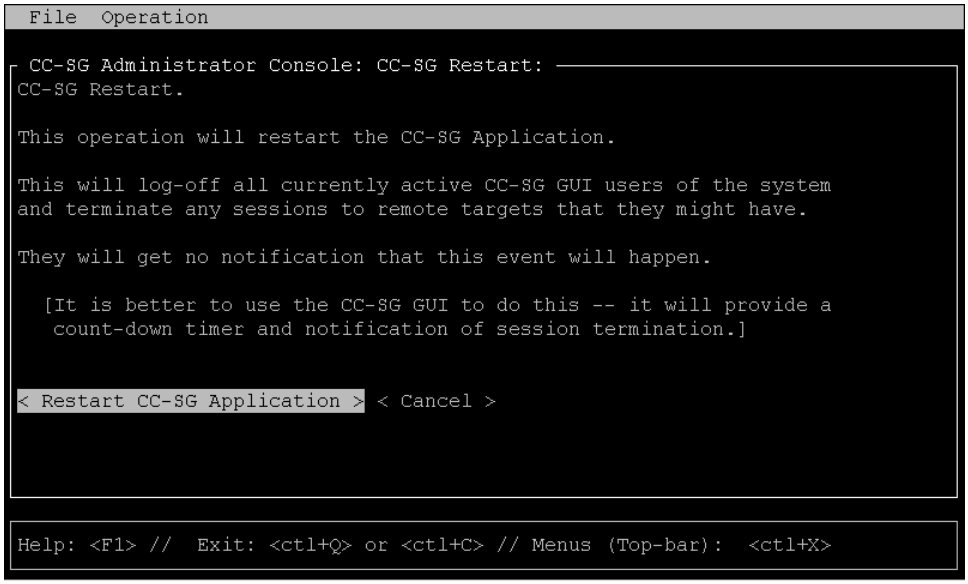

Figure 198 Redémarrage de CC-SG dans la console de diagnostic

Réamorcer l'unité CC-SG (Admin)

Cette option entraîne un réamorçage complet de CC-SG, qui simule un cycle d'alimentation. Les utilisateurs ne recevront aucune notification. Les utilisateurs de CC-SG, SSH et la console de diagnostic (cette session comprise) seront déconnectés. Toutes les connexions aux serveurs cible distants seront également interrompues.

Pour réamorcer CC-SG :

1. Cliquez sur **Operation**, **Admin**, puis sur **CC-SG System Reboot**.
2. Cliquez sur **REBOOT System** ou appuyez sur la touche **ENTRÉE** pour réinitialiser CC-SG. Confirmez le réamorçage dans l'écran suivant pour continuer.

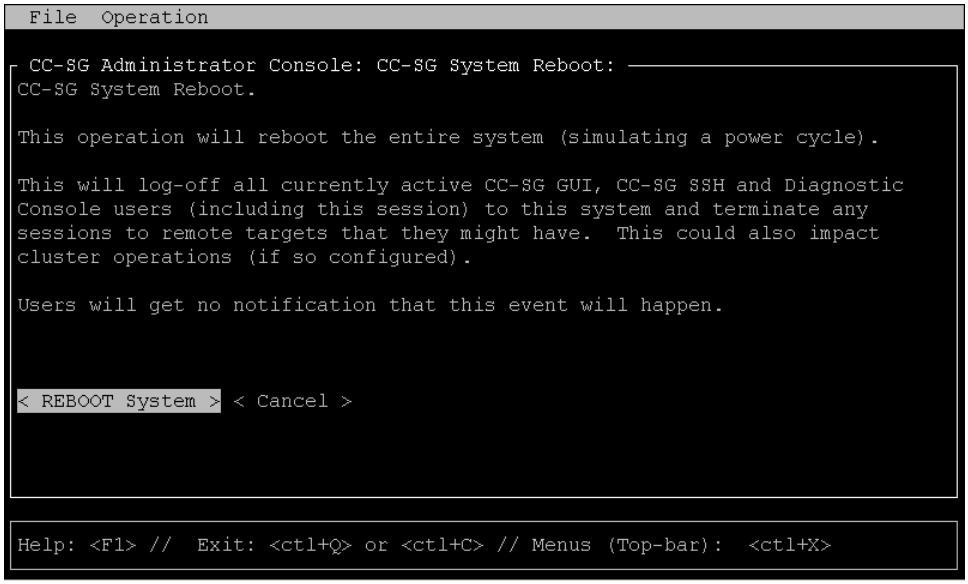

Figure 199 Réamorçage de CC-SG dans la console de diagnostic

Mettre le système CC-SG hors tension (Admin)

Cette option entraîne la mise hors tension complète de CC-SG. Les utilisateurs ne recevront aucune notification. Les utilisateurs de CC-SG, SSH et la console de diagnostic (cette session comprise) seront déconnectés. Toutes les connexions aux serveurs cible distants seront également interrompues. 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. Cliquez sur **Operation**, **Admin**, puis sur **CC-SG System Power OFF**.
2. Cliquez sur **Power OFF the CC-SG** ou appuyez sur **ENTREE** pour couper l'alimentation de l'unité CC-SG. Confirmez la mise hors tension dans l'écran suivant pour continuer.

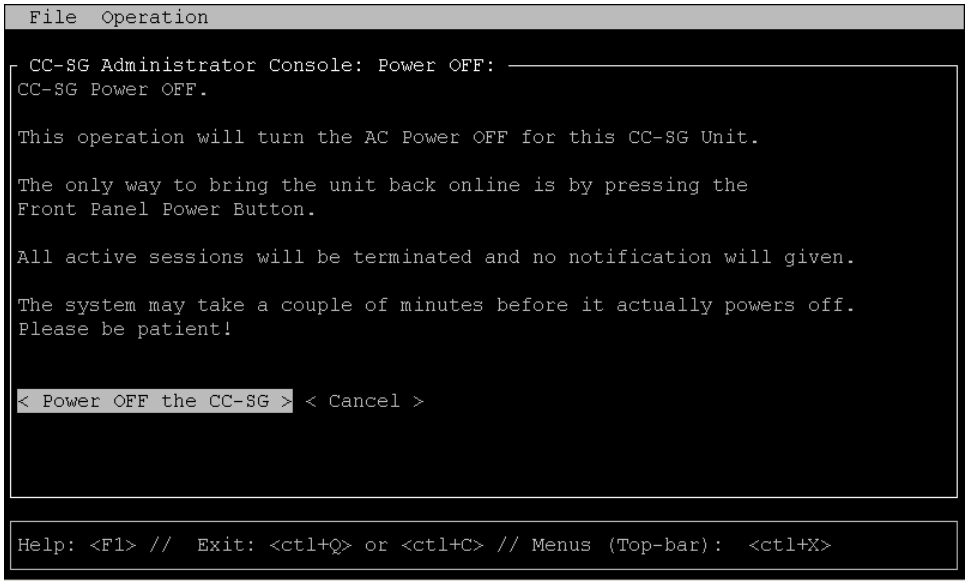

Figure 200 Mise hors tension de CC-SG dans la console de diagnostic

Réinitialiser le mot de passe admin de l'interface CC-SG

Cette option permet de réinitialiser le mot de passe de l'interface CC-SG pour le compte admin à la valeur par défaut usine.

***Remarque** : il ne s'agit pas du mot de passe de l'utilisateur admin de la console de diagnostic. Reportez-vous à Mots de passe de la console de diagnostic ci-dessous pour plus d'informations sur la modification du mot de passe de ce compte.*

Pour réinitialiser le mot de passe admin de l'interface CC-SG :

1. Cliquez sur **Operation**, **Admin**, puis sur **CC-SG ADMIN Password Reset**.
2. Cliquez sur **Reset CC-SG GUI Admin Password** ou appuyez sur **ENTREE** pour rétablir le mot de passe admin par défaut usine. Confirmez la réinitialisation du mot de passe dans l'écran suivant pour continuer.

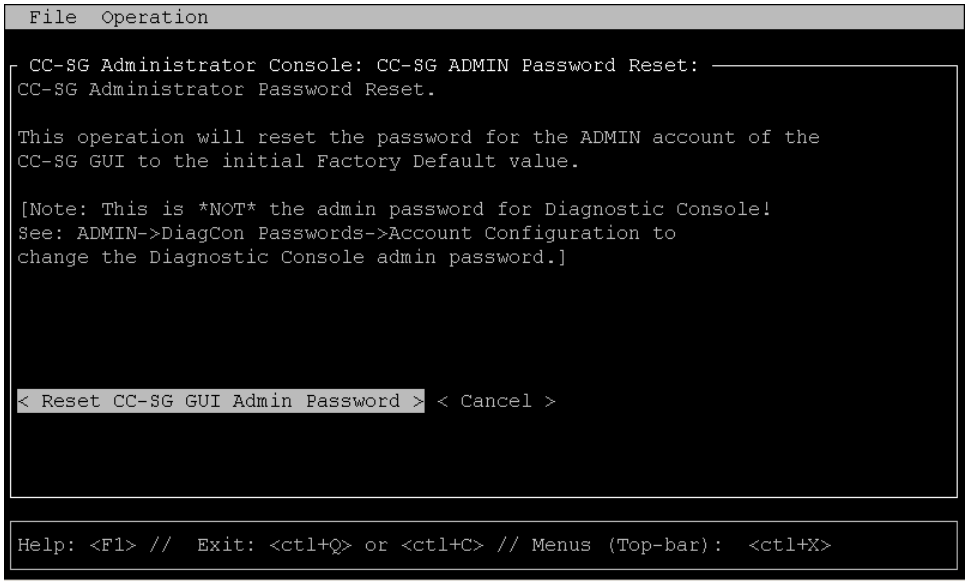

Figure 201 Réinitialisation du mot de passe Admin pour l'interface CC-SG dans la console de diagnostic

Réinitialiser la configuration usine de CC-SG (Admin)

Cette option réinitialisera la totalité ou une partie du système CC-SG à ses valeurs par défaut usine. Tous les utilisateurs de CC-SG actifs seront déconnectés sans notification et le traitement SNMP sera interrompu. Il est fortement recommandé de faire passer CC-SG en **mode de maintenance** avant de commencer cette opération. Si possible, réinitialisez CC-SG depuis le Director Client de l'administrateur, plutôt qu'avec la console de diagnostic. L'option de réinitialisation du Director Client peut exécuter toutes les fonctions répertoriées ici, sauf la réinitialisation des valeurs de réseau.

1. Dans le menu **Operation**, cliquez sur **Admin**, puis sur **Factory Reset**. L'écran suivant présentant 7 options de réinitialisation (**Reset Options**) apparaît.

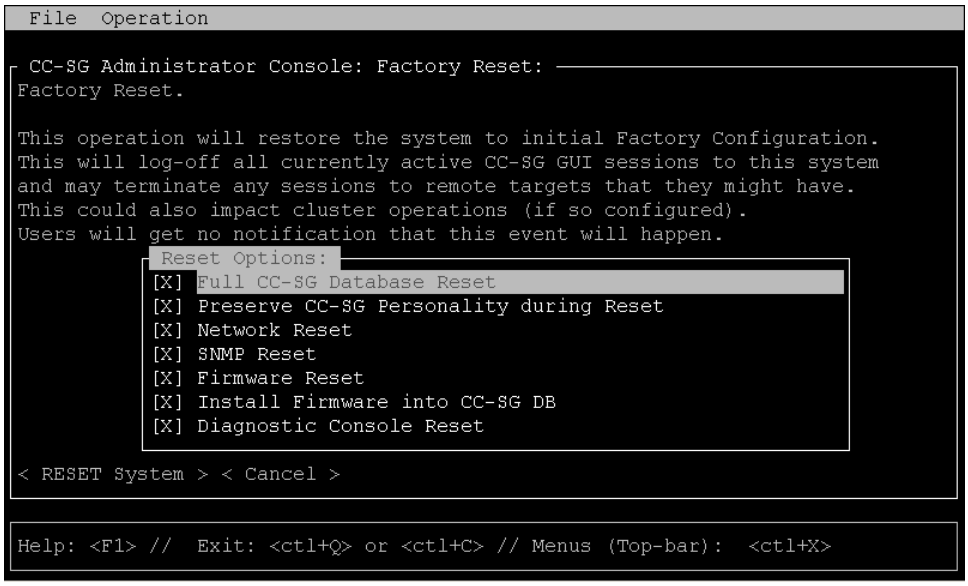

Figure 202 Réinitialiser la configuration usine de CC-SG

OPTION	DESCRIPTION
Full CC-SG Database Reset	La sélection de cette option supprime entièrement la base de données CC-SG existante et crée une version nouvelle en la chargeant avec les valeurs par défaut usine.
Preserve CC-SG Personality during Reset	Cette option n'est valide et active que si l'option précédente est également sélectionnée. Lors de la reconstitution de la base de données CC-SG (dans l'option précédente), les valeurs suivantes seront migrées vers la nouvelle version de la base de données (si elles sont lisibles et disponibles ; sinon, les valeurs par défaut seront utilisées). Le système tente de conserver les informations suivantes : La valeur par défaut apparaît entre crochets. ▪ Communication sécurisée [non sécurisée] entre les clients PC et CC-SG. ▪ Vérification des mots de passe forts [désactivée] : sélectionne si l'application du mot de passe fort est activée. ▪ Connexions directe et Proxy [Directe] indique si des connexions directe ou Proxy sont utilisées par les clients PC vers les nœuds hors bande. ▪ Minuteur d'inactivité [1800] : délai après lequel les sessions inactives sont déconnectées. ▪ Paramètres du modem [10.0.0.1/10.0.0.2/<none>] : paramètre d'adresse IP du serveur, d'adresse IP du client et numéro de téléphone de rappel du modem.
Network Reset	Cette option rétablit les paramètres réseau par défaut usine : ▪ Nom d'hôte = CommandCenter ▪ Nom de domaine = localdomain ▪ Mode = Principal / Sauvegarde ▪ Configuration = Statique ▪ Adresse IP = 192.168.0.192 ▪ Masque réseau = 255.255.255.0 ▪ Passerelle = <none> ▪ DNS principal = <none> ▪ DNS secondaire = <none> Vitesse de carte = Auto
SNMP Reset	Réinitialise la configuration SNMP aux valeurs par défaut usine. ▪ Port : 161 ▪ Communauté en lecture seule : public ▪ Communauté en lecture/écriture : private ▪ Contact système, Nom, Emplacement : <empty> ▪ Configuration des traps SNMP Destinations des traps SNMP
Firmware Reset	Retire les fichiers de firmware téléchargés et restaure les versions par défaut dans le référentiel de système de fichiers, mais ne modifie pas la BD CC-SG.
Install Firmware into CC-SG DB	Charge les fichiers de firmware trouvés dans le référentiel de système de fichiers dans la BD CC-SG.
Diagnostic Console Reset	Restaure la configuration, les paramètres de compte et les valeurs par défaut usine d'origine de la console de diagnostic.

Mots de passe de la console de diagnostic (Admin)

Cette option permet de configurer la force des mots de passe (status et admin), ainsi que leurs attributs, tels que le paramétrage du nombre maximum de jours devant s'écouler avant la modification du mot de passe (effectuée via le menu de configuration de compte). L'opération de ces menus s'applique uniquement aux comptes (status et admin) et aux mots de passe de la console de diagnostic. Elle n'a aucun effet sur les comptes ou mots de passe habituels de l'interface utilisateur graphique de CC-SG.

Configuration des mots de passe

1. Cliquez sur **Operation**, **Admin**, **DiagCon Passwords**, puis sur **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**.

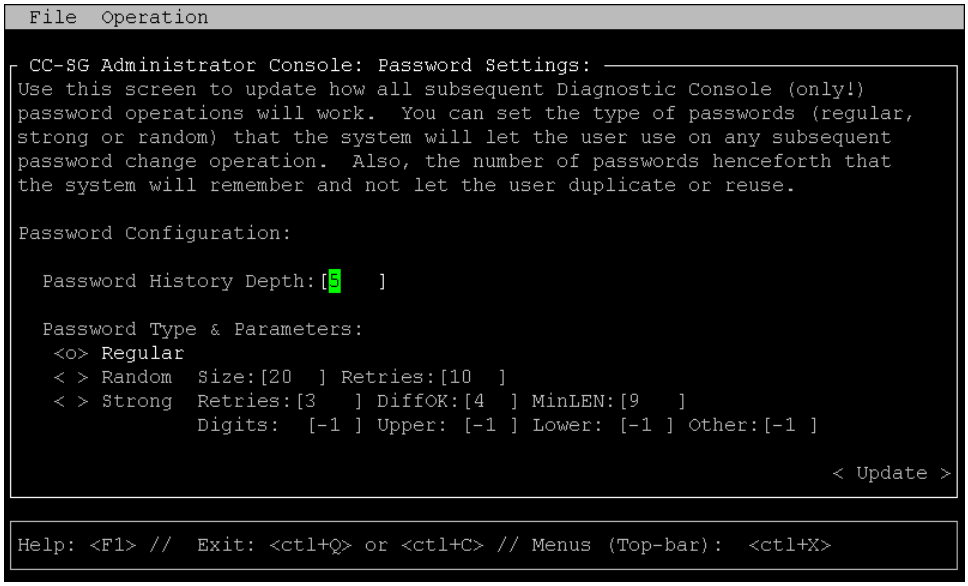

Figure 203 Configuration des paramètres de mot de passe

3. Sélectionnez **Regular**, **Random** ou **Strong** pour les mots de passe **admin** et **status** (s'ils sont activés).

PARAMÈTRE DE MOT DE PASSE	DESCRIPTION
Regular	Il s'agit de mots de passe standard. Les mots de passe doivent contenir plus de quatre caractères avec peu de restrictions. Il s'agit de la configuration de mot de passe par défaut du système.
Random	Fournit des mots de passe générés de manière aléatoire. Configure la taille (size) maximum de mots de passe en bits (le minimum est 14, le maximum, 70 ; la valeur par défaut est 20) et le nombre de tentatives (retries) (la valeur par défaut est 10), c'est-à-dire le nombre de fois que le système vous demandera si vous acceptez le nouveau mot de passe. Vous pouvez accepter (en tapant le nouveau de passe deux fois) ou rejeter le mot de passe aléatoire. Vous ne pouvez pas choisir votre propre mot de passe.
Strong	Impose des mots de passe forts. **Retries** représente le nombre d'invites que vous recevez avant l'affichage d'un message d'erreur. **DiffOK** indique le nombre de caractères pouvant être identiques dans le nouveau mot de passe et l'ancien. **MinLEN** est la longueur minimum de caractères requise dans le mot de passe. Indiquez dans les champs Digits (chiffres), Upper (majuscules), Lower (minuscules) et Other (spéciaux), les caractères nécessaires dans le mot de passe. Les nombres positifs représentent le « crédit » maximum de cette classe de caractères pouvant être pris en compte dans l'évaluation de la « simplicité ». Les nombres négatifs impliquent que le mot de passe DOIT comporter un nombre minimum de caractères d'une classe donnée. Ainsi, -1 indique que chaque mot de passe doit comporter au moins un chiffre.

Configuration des comptes

Par défaut, le compte **status** ne nécessite pas de mot de passe, mais vous pouvez le configurer pour qu'il en nécessite un. D'autres aspects du mot de passe **admin** peuvent être configurés et les comptes d'assistance sur site, activés ou désactivés.

1. Pour configurer des comptes, cliquez sur **Operation**, **Admin**, **DiagCon Passwords**, puis sur **Account Configuration**.
2. Dans l'écran qui apparaît, vous pouvez consulter les paramètres de chaque compte, **Status**, **Admin**, **FS1** et **FS2**.

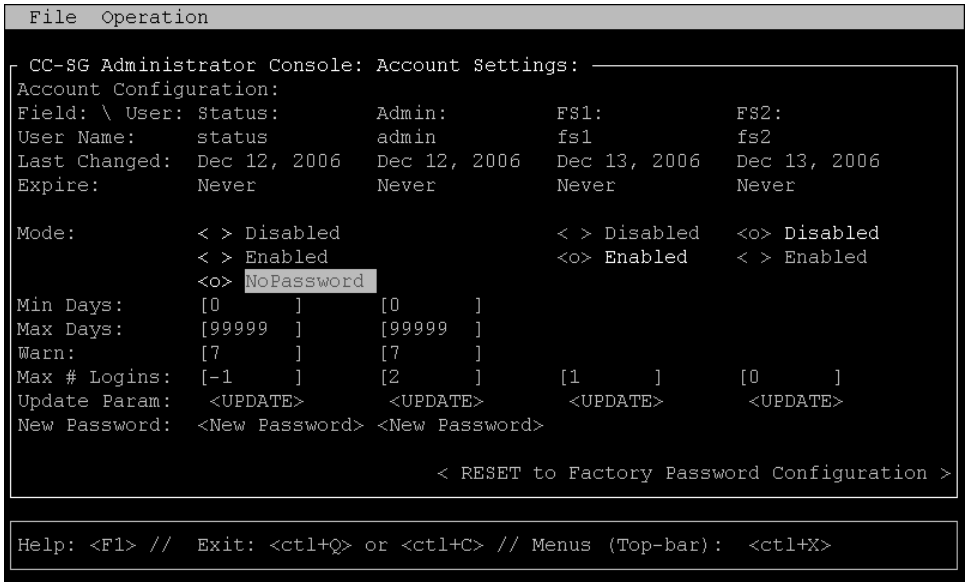

Figure 204 Configuration des comptes

Cet écran est divisé en trois zones principales :

- Celle du haut affiche des informations en lecture seule sur les comptes du système.
- La section du milieu présente les différents paramètres pertinents pour chaque ID, ainsi qu'un jeu de boutons, afin de permettre la mise à jour de ces paramètres ou la définition de nouveaux mots de passe pour les comptes.
- La dernière zone sert à restaurer les paramètres usine pour la configuration du mot de passe (c'est-à-dire les paramètres du système au moment de son expédition).

3. Si vous souhaitez rendre le mot de passe obligatoire pour le compte **Status**, sélectionnez **Enabled** sous ce dernier.
4. Pour les comptes **Admin** et **Status**, vous pouvez configurer :

PARAMÈTRE	DESCRIPTION
User \ User Name	(Lecture seule). Il s'agit du nom d'utilisateur ou de l'ID actuel du compte.
Last Changed	(Lecture seule). Il s'agit de la date de dernière modification du mot de passe pour ce compte.
Expire	(Lecture seule). Indique le jour où ce compte doit changer de mot de passe.
Mode	Option configurable si le compte est désactivé (aucune connexion autorisée) ou activé (jeton d'authentification obligatoire), ou si l'accès est autorisé et qu'aucun mot de passe n'est requis. (Ne verrouillez pas les comptes Admin et FS1 en même temps ; sinon, vous ne pourrez plus utiliser la console de diagnostic.)
Min Days	Nombre minimum de jours après lesquels un mot de passe peut être à nouveau changé. La valeur par défaut est **0**.
Max Days	Nombre maximum de jours pendant lesquels le mot de passe sera effectif. La valeur par défaut est **99999**.
Avertissement	Nombre de jours pendant lesquels des messages d'avertissement sont affichés avant expiration du mot de passe.
Max # of Logins	Nombre maximum de connexions simultanées autorisées par le compte. Les chiffres négatifs indiquent qu'il n'existe aucune restriction (**-1** est la valeur par défaut pour la connexion status). **0** signifie que personne ne peut se connecter. Un chiffre positif définit le nombre d'utilisateurs pouvant se connecter simultanément (**2** est la valeur par défaut pour la connexion admin).
UPDATE	Enregistre les modifications effectuées pour cet ID.
New Password	Entrez un nouveau mot de passe pour ce compte.

Afficher l'état du disque (Utilitaires)

Cette option affiche l'état des disques CC-SG, par exemple leur taille, s'ils sont actifs, l'état de RAID-1 et la quantité d'espace actuellement utilisée par différents systèmes de fichiers.

Pour afficher l'état du disque du CC-SG :

1. Cliquez sur **Operation**, **Utilities**, puis sur **Disk Status**.

2. Cliquez sur **Refresh** ou appuyez sur **Entrée** pour actualiser l'affichage. Le rafraîchissement de l'écran est particulièrement utile lors de la mise à niveau ou de l'installation, et lorsque vous souhaitez voir la progression des disques RAID au fur et à mesure de leurs reconstruction et synchronisation.

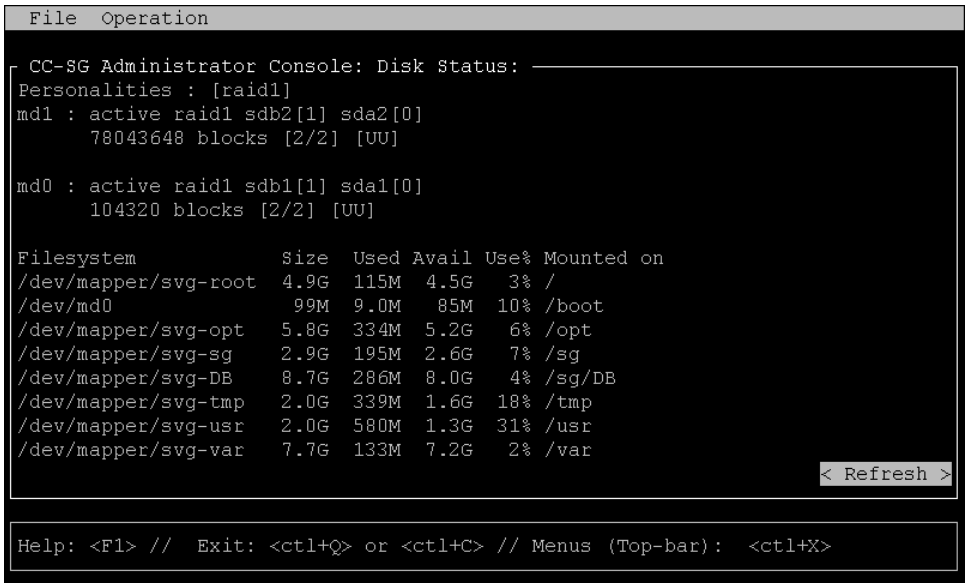

Figure 205 Affichage de l'état du disque de CC-SG dans la console de diagnostic

***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. Le statut des tableaux **md0** et **md1** est [**UU**].*

Afficher les processus exécutés sur CC-SG (Utilitaires)

Cette option présente la liste des processus actuellement exécutés sur CC-SG, les attributs de ces processus, ainsi que l'état général du système.

1. Pour afficher les processus exécutés sur CC-SG, cliquez sur **Operation**, **Utilities**, puis **Top Display**.
2. Affichez le nombre des processus exécutés, en veille, le total des processus et ceux qui sont arrêtés.

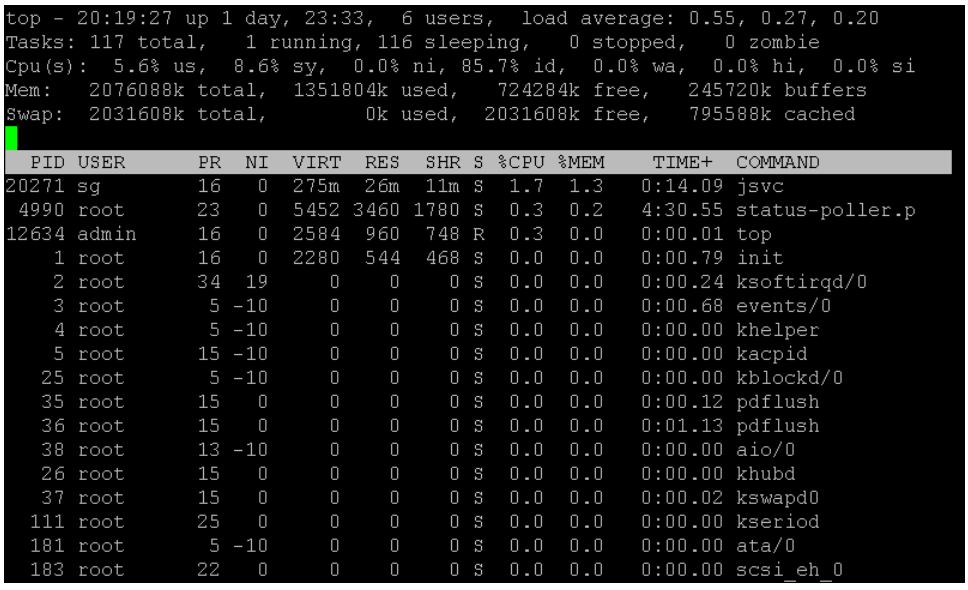

Figure 206 Affichage des processus CC-SG dans la console de diagnostic

3. Tapez **h** afin d'afficher un écran d'aide exhaustif pour la commande supérieure. La touche d'aide **F1** n'est pas opérationnelle ici. Pour retourner à la console d'administrateur, utilisez **Ctrl+Q** ou **Ctrl+C**.

Afficher l'état NTP (Network Time Protocol) (Utilitaires)

Cette option affiche l'état du démon de temps NTP s'il est configuré et exécuté sur CC-SG.

Pour afficher l'état du démon NTP sur CC-SG :

1. Cliquez sur **Operation**, **Utilities**, puis sur **NTP Status Display**.
2. Le démon NTP peut être configuré uniquement dans le Director Client de l'administrateur de CC-SG. Si NTP n'est pas activé et configuré correctement, l'écran ci-après s'affiche :

Figure 207 NTP non configuré dans l'interface utilisateur graphique de CC-SG

3. Si NTP est correctement configuré et exécuté sur CC-SG, un écran semblable à celui ci-après doit être généré :

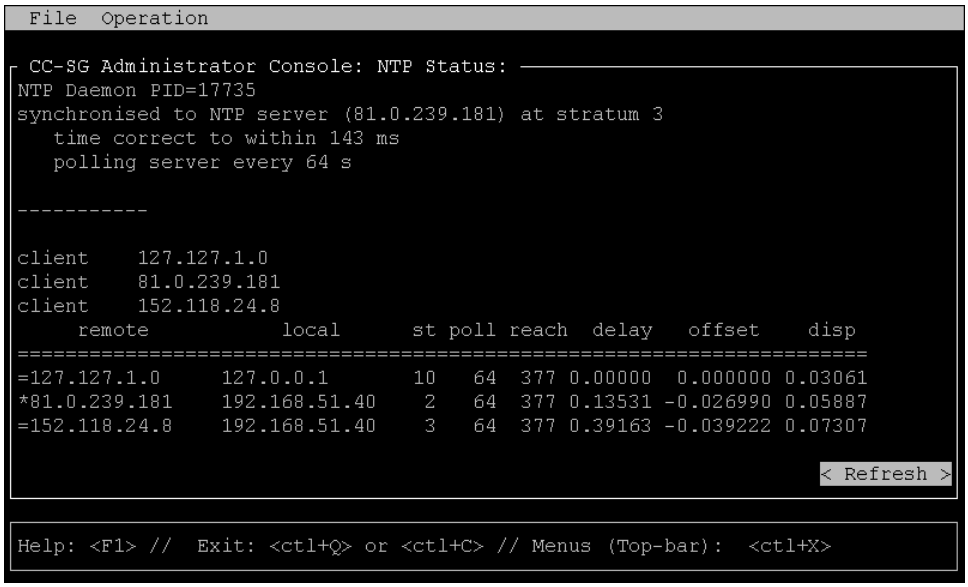

Figure 208 NTP exécuté dans l'interface utilisateur graphique de CC-SG

4. Sélectionnez **Refresh** pour mettre à jour les informations de cette page.

Annexe A : Spécifications (G1, V1 et E1)

Plate-forme G1

Spécifications générales

Facteur de forme	1U
Dimensions (PxLxH)	563 mm x 440 mm x 44 mm
Poids	10,92 kg
Alimentation	Détection automatique des alimentations redondantes permutables à chaud, 110/220 V, 2,0 A
Temps moyen entre défaillances (MTBF)	38 269 heures
Port d'administration KVM	(Clavier/souris DB15 + PS2)
Port d'administration série	DB9
Port de console	S/O

Spécifications matérielles

Processeur	Intel® Pentium® III 1 GHz
Mémoire	512 Mo
Interfaces réseau	(2) 10/100 Ethernet (RJ45)
Disque dur et contrôleur	RAID 1 avec (2) IDE de 40 Go à 7 200 tr/min
Lecteur CD/ROM	CD/ROM 40x lecture seule

Impératifs d'environnement

EN FONCTIONNEMENT	
Humidité résiduelle	20 à 85 %
Altitude	Fonctionne correctement aux altitudes comprises entre 0 et 10 000 pieds (0 à 3 000 m), stockage à 40 000 pieds (12 000 m) (estimation)
Vibrations	5-55-5 Hz, 0,38 mm, 1 minute par cycle, 30 minutes par axe (X, Y, Z)
Chocs	S/O
A L'ARRÊT	
Température	0 à 30 degrés C ; 32 à 104 degrés F
Humidité résiduelle	10 à 90 %
Altitude	Fonctionne correctement aux altitudes comprises entre 0 et 10 000 pieds (0 à 3 000 m), stockage à 40 000 pieds (12 000 m) (estimation)
Vibrations	5-55-5 Hz, 0,38 mm, 1 minute par cycle, 30 minutes par axe (X, Y, Z)
Chocs	S/O

Plate-forme V1

Spécifications générales

Facteur de forme	1U
Dimensions (PxLxH)	615 mm x 485 mm x 44 mm
Poids	10,80 kg
Alimentation	Alimentation simple (1 x 300 watts)
Température de fonctionnement	10 à 35 degrés C ; 50 à 95 degrés F
Temps moyen entre défaillances (MTBF)	36 354 heures
Port d'administration KVM	(Clavier/souris DB15 + PS2 ou USB)
Port d'administration série	DB9
Port de console	(2) ports USB 2.0

Spécifications matérielles

Processeur	AMD Opteron 146
Mémoire	2 Go
Interfaces réseau	(2) 10/100/1000 Ethernet (RJ45)
Disque dur et contrôleur	RAID 1 avec (2) SATA de 80 Go à 7 200 tr/min
Lecteur CD/ROM	DVD-ROM

Impératifs d'environnement

EN FONCTIONNEMENT	
Humidité résiduelle	8 à 90 %
Altitude	Fonctionne correctement aux altitudes comprises entre 0 et 3 048 m, stockage à 12 192 m (estimation)
Vibrations	5-55-5 HZ, 0,38 mm,1 minute par cycle ; 30 minutes par axe (X,Y,Z)
Chocs	S/O
A L'ARRÊT	
Température	-40 à 60 degrés C ; -40 à 140 degrés F
Humidité résiduelle	5 à 95 %
Altitude	Fonctionne correctement aux altitudes comprises entre 0 et 3 048 m, stockage à 12 192 m (estimation)
Vibrations	5-55-5 HZ, 0,38 mm,1 minute par cycle ; 30 minutes par axe (X,Y,Z)
Chocs	S/O

Plate-forme 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	0~50 °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

Spécifications matérielles

Processeur	(2) processeurs AMD Opteron 250 2,4 GHz 1 Mo
Mémoire	4 Go
Interfaces réseau	Adaptateur serveur double port Intel PRO/1000 PT
Disque dur et contrôleur	Cache 16 Mo avec (2) WD740ADFD SATA de 74 Go à 10K tr/min
Lecteur CD/ROM	DVD-ROM

Impératifs d'environnement

EN FONCTIONNEMENT	
Humidité résiduelle	5 à 90 %, sans condensation
Altitude	Niveau de la mer à 213 360,00 cm
Vibrations	Balayage de 10 à 500 Hz à une accélération constante de 0,5 g pendant une heure, sur chaque axe perpendiculaire X, Y et Z
Chocs	5 g pendant 11 ms avec demi-onde sinusoïdale pour chaque axe perpendiculaire X, Y et Z
A L'ARRÊT	
Température	-40 à 70 °C
Humidité résiduelle	5 à 90 %, sans condensation
Altitude	Niveau de la mer à 1 219 200,00 cm
Vibrations	Balayage de 10 à 300 Hz à une accélération constante de 2 g pendant une heure, sur chaque axe perpendiculaire X, Y et Z
Chocs	30 g pendant 11 ms avec demi-onde sinusoïdale pour chaque axe perpendiculaire X, Y et Z

Cette page est laissée intentionnellement blanche.

Annexe B : Configuration de CC-SG et du réseau

Introduction

Cette annexe indique la configuration réseau requise (adresses, protocoles et ports) d'un déploiement CC-SG standard. Elle comporte des informations relatives au mode de configuration de votre réseau pour l'accès externe (le cas échéant), ainsi que pour la mise en application de la sécurité interne et de la stratégie d'acheminement (le cas échéant). Ces données sont destinées à l'administrateur d'un réseau TCP/IP, dont le rôle et les responsabilités peuvent s'étendre au-delà de ceux d'un administrateur CC-SG, et qui souhaite intégrer CC-SG et ses composants aux stratégies d'accès de sécurité et d'acheminement d'un site.

Comme décrit dans le schéma ci-après, un déploiement CC-SG standard peut utiliser aucune fonction, certaines des fonctions ou toutes les fonctions, par exemple, un pare-feu ou un réseau VPN (Virtual Private Network). Les tableaux qui suivent présentent les protocoles et ports utilisés par CC-SG et ses composants associés qu'il vous faut connaître et comprendre, particulièrement si des pare-feu ou réseaux VPN se trouvent sur votre réseau, et si des stratégies d'accès et de sécurité seront mises en application par le réseau.

Synthèse

Les sections ci-après fournissent une analyse très complète et détaillée des communications et des ports utilisés par CC-SG et ses composants associés. Pour les clients qui souhaitent simplement savoir quels ports ouvrir sur un pare-feu pour autoriser l'accès à CC-SG et aux cibles qu'il contrôle, les ports ci-après doivent être ouverts :

Numéro de port	Protocole	Usage
80	TCP	Accès HTTP à CC-SG
443	TCP	Accès HTTPS (SSL) à CC-SG
8080	TCP	CC-SG <-> PC Client
2400	TCP	Accès au nœud (mode Proxy et accès en bande)
5000[1]	TCP	Accès au nœud (mode direct)
51000[1]	TCP	Accès cible SX (mode direct)

Cette liste peut être affinée davantage :

- le port 80 peut être abandonné si l'accès à CC-SG est toujours effectué via des adresses HTTPS ;
- les ports 5000 et 51000 peuvent être abandonnés si le mode Proxy de CC-SG est utilisé pour toutes les connexions depuis les pare-feu.

Ainsi, une configuration minimum nécessite l'ouverture de trois (3) ports uniquement [443, 8080 et 2400] pour permettre un accès externe à CC-SG.

Les sections ci-après présentent des données relatives à ces méthodes et ports d'accès, ainsi que les contrôles et options de configuration.

[1] 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.

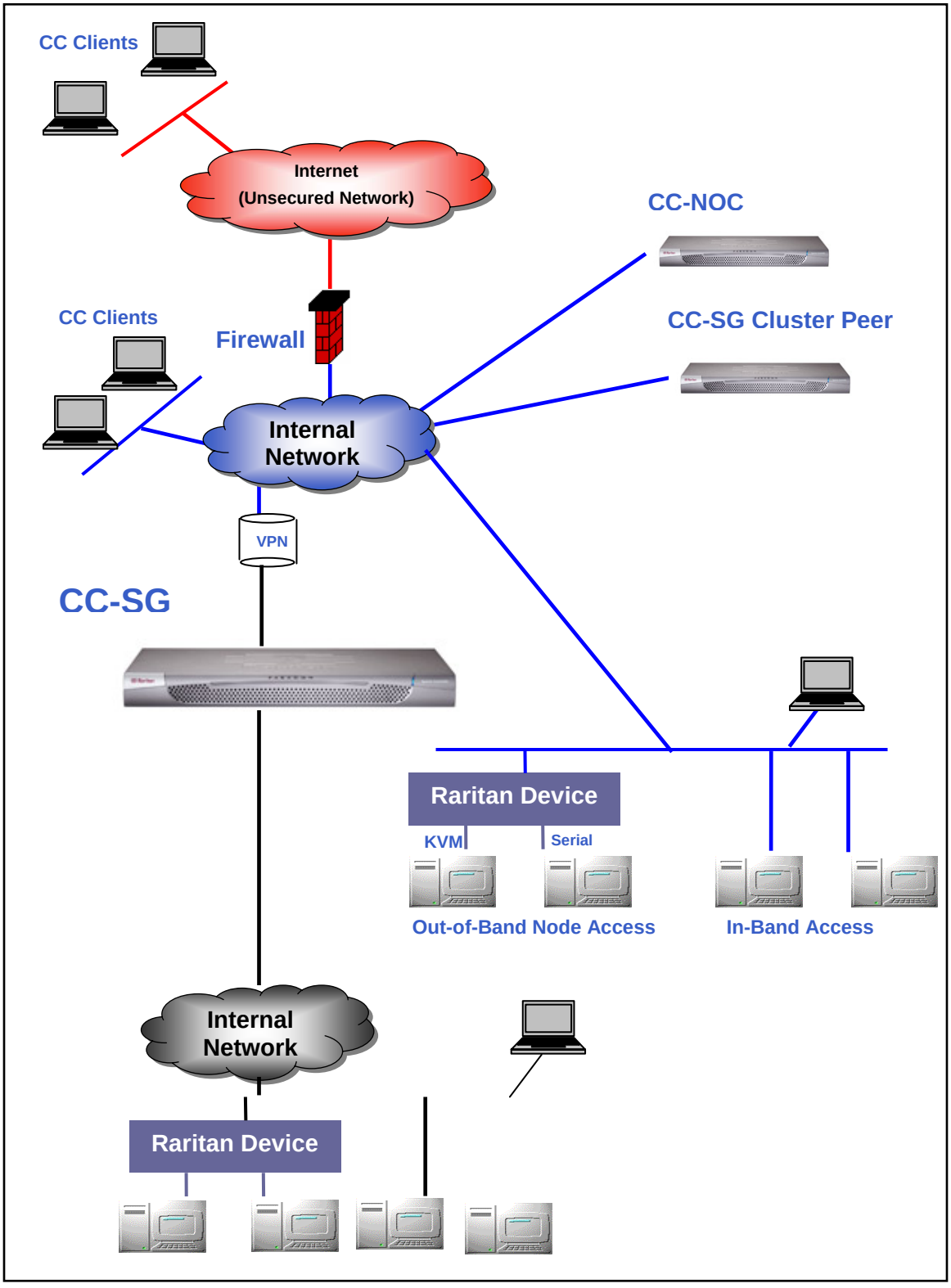

Figure 209 Eléments de déploiement de CC-SG

Canaux de communication CC-SG

Les canaux de communication sont partitionnés comme suit :

- CC-SG ↔ Dispositifs Raritan
- CC-SG ↔ Cluster CC-SG (facultatif)
- CC-SG ↔ Services d'infrastructure
- Clients ↔ CC-SG
- Clients ↔ Cibles (mode direct)
- Clients ↔ Cibles (mode Proxy)
- Clients ↔ Cibles (en bande)
- CC-SG ↔ CC-NOC

Pour chaque canal de communication, les tableaux des sections suivantes :

- Représentent les **adresses IP** symboliques utilisées par les parties en communication. Ces adresses doivent être autorisées sur tous les chemins de communication entre les entités.
- Indiquent la **direction** de la communication. Ceci peut être important pour les stratégies particulières à votre site. Pour un rôle CC-SG donné, le chemin entre les parties en communication correspondantes doit être disponible, ainsi que pour les autres chemins de réacheminement qui pourraient être utilisés dans le cas d'une défaillance de réseau.
- Fournissent les **numéro de port** et **protocole** utilisés par CC-SG.
- Indiquent si le port est **configurable**, ce qui signifie que l'interface utilisateur graphique ou la console de diagnostic fournit un champ dans lequel vous pouvez remplacer le numéro de port par défaut indiqué a cause de conflits avec d'autres applications du réseau ou pour des raisons de sécurité.

CC-SG et dispositifs Raritan

Un des rôles principaux de CC-SG consiste à gérer et à contrôler des dispositifs Raritan (par exemple, Dominion KX, KSX, etc.). Généralement, CC-SG communique avec ces dispositifs sur un réseau TCP/IP (local, étendu ou VPN) et les protocoles TCP et UDP sont utilisés comme suit :

Direction de la communication	Numéro de port	Protocole	Configurable ?
CC-SG → Diffusion locale	5000	UDP	oui
CC-SG → IP LAN distant	5000	UDP	oui
CC-SG ↔ Dispositif Raritan	5000	TCP	oui
Dispositif Raritan ↔ CC-SG	5001	UDP	non

Cluster CC-SG

Lorsque la fonction facultative de cluster CC-SG est utilisée (c'est-à-dire lorsque deux unités CC-SG sont interconnectées et fonctionnent comme une seule unité), les ports ci-après doivent être disponibles pour les sous-réseaux en interconnexion. {Si la fonction de cluster n'est pas utilisée, aucun de ces ports n'a besoin d'être disponible sur le réseau.}

Chaque CC-SG du cluster peut être sur un LAN distinct. Toutefois, l'interconnexion entre les unités doit être fiable et non soumise à des périodes d'encombrement.

Direction de la communication	Numéro de port	Protocole	Configurable ?
CC-SG → Diffusion locale	10000	UDP	non
CC-SG → IP LAN distant	10000	UDP	non
CC-SG ↔ CC-SG	5432	TCP	non
CC-SG ↔ CC-SG	8732	TCP	non
CC-SG ↔ CC-SG	3232	TCP	non

Accès aux services d'infrastructure

CC-SG peut être configuré pour utiliser plusieurs services conformes aux normes de l'industrie comme DHCP, DNS et NTP. Pour que CC-SG communique avec ces serveurs facultatifs, les ports et protocoles suivants sont utilisés :

Direction de la communication	Numéro de port	Protocole	Configurable ?
Serveur DHCP → CC-SG	68	UDP	non
CC-SG → Serveur DHCP	67	UDP	non
Serveur d'horloge NTP ↔ CC-SG	123	UDP	non
CC-SG → DNS	53	UDP	non

Clients PC vers CC-SG

Les clients PC se connectent à CC-SG via un de ces trois modes :

- Interface utilisateur graphique CC-SG Web/applet Java
- Interface de ligne de commande CC-SG via SSH
- Console de diagnostic CC-SG

Le premier mode est la méthode principale utilisée par les utilisateurs et administrateurs pour se connecter à CC-SG. Les deux autres modes sont moins fréquents. Ces modes requièrent la configuration réseau suivante :

Direction de la communication	Numéro de port	Protocole	Configurable ?
Client → Interface utilisateur graphique CC-SG	443	TCP	non
Client → Interface utilisateur graphique CC-SG	80	TCP	non
Client → Interface utilisateur graphique CC-SG	8080	TCP	non
Client → CC-CLI SSH	22	TCP	oui
Client → Console de diagnostic CC	23	TCP	oui

Clients PC vers nœuds

L'autre rôle important de CC-SG consiste à connecter des clients PC à différentes cibles (ou nœuds). Ces cibles peuvent être des connexions de console en série ou KVM aux dispositifs Raritan (appelées connexions hors bande). Un autre mode consiste à utiliser les méthodes d'accès en bande (IBA), par exemple, Virtual Network Computer (VNC), Windows Remote Desktop (RDP) ou Secure Shell (SSH).

Un autre aspect de la communication entre client PC et cible implique que :

- le client PC est connecté directement à la cible (via un dispositif Raritan ou un accès en bande) ; il s'agit du **mode direct** ;
- ou, le client PC est connecté à la cible via CC-SG qui sert de pare-feu d'application ; il s'agit du **mode Proxy**.

Direction de la communication	Numéro de port	Protocole	Configurable ?
Client → CC-SG via Proxy → Cible	2400 (sur CC-SG)	TCP	non
Client → Cible Raritan (mode direct)	5000 (sur dispositif)	TCP	oui
Client → Dominion SX → (mode direct)	51000	TCP	oui

CC-SG et Client pour IPMI, iLO/RILOE, DRAC, RSA

Un autre rôle important de CC-SG est de gérer des dispositifs tiers, tels que des dispositifs iLO/RILOE ou des serveurs Integrated Lights Out/Remote Insight Lights Out de Hewlett Packard. Les cibles d'un dispositif iLO/RILOE sont mises sous/hors tension et réactivées directement. Les serveurs IPMI (Intelligent Platform Management Interface) peuvent également être contrôlés par CC-SG. Les cibles DRAC et RSA Dell peuvent aussi être gérées par CC-SG.

Direction de la communication	Numéro de port	Protocole	Configurable ?
CC-SG → IPMI	623	UDP	non
CC-SG → iLO/RILOE (utilise des ports HTTP)	80 ou 443	UDP	non
CC-SG → DRAC	80 ou 443	UDP	non
CC-SG → RSA	80 ou 443	UDP	non

CC-SG et SNMP

Le protocole SNMP (Simple Network Management Protocol) permet à CC-SG d'envoyer des traps SNMP (notifications d'événements) à un gestionnaire SNMP du réseau. CC-SG prend également en charge les opérations GET/SET SNMP avec les solutions de gestion d'entreprise tierces, comme HP OpenView.

Direction de la communication	Numéro de port	Protocole	Configurable ?
Gestionnaire SNMP → CC-SG	161	UDP	oui
CC-SG → Gestionnaire SNMP	162	UDP	oui

CC-SG et CC-NOC

L'appareil facultatif CC-NOC peut être déployé conjointement à CC-SG. CC-NOC est une console de surveillance réseau Raritan qui permet l'audit et la surveillance du statut des serveurs, de l'équipement et des dispositifs Raritan gérés par CC-SG.

Direction de la communication	Numéro de port	Protocole	Configurable ?
CC-SG ↔ CC-NOC	9443	TCP	non

Ports internes CC-SG

CC-SG utilise plusieurs ports pour les fonctions internes. Sa fonction de pare-feu local bloque l'accès à ces derniers. Cependant, certains analyseurs externes peuvent détecter ceux-ci comme « bloqués » ou « filtrés ». L'accès externe à ces ports n'est pas obligatoire et peut être bloqué davantage. Les ports actuellement utilisés sont :

1088, 1098, 2222, 4444, 4445, 8009, 8083 et 8093

En plus de ces ports, CC-SG peut disposer de quelques ports TCP et UDP ouverts dans 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), par exemple, alors le mode Proxy doit être activé pour toutes les connexions utilisant ce pare-feu. De plus, ce pare-feu doit être configuré pour des connexions externes aux ports 80 (non-SSL)/443 (SSL)[2], 8080 et 2400 pour être transmis à CC-SG (puisque le client PC initialise les sessions sur ces ports).

Toutes les connexions à accès en bande (IBA) utilisent CC-SG comme connexion Proxy et aucune configuration supplémentaire n'est nécessaire. Les connexions à accès hors bande (OBA) qui utilisent le pare-feu doivent être configurées à l'aide du menu **Configuration ➔ Gestionnaire de configuration ➔ Mode de connexion** pour faire appel au mode Proxy. Ainsi, CC-SG se connecte aux différentes cibles (IBA ou OBA) pour répondre aux demandes du client PC. Toutefois, CC-SG mettra fin à la connexion TCP/IP entre le client PC et la cible qui passe par le pare-feu.

[2] Il n'est pas recommandé d'exécuter du trafic non-SSL via un pare-feu.

Securité et analyses des ports ouverts

Dans le cadre du processus d'assurance-qualité de CC-SG, plusieurs analyseurs de ports ouverts sont appliqués au produit et Raritan vérifie que son produit n'est pas vulnérable à ces attaques connues. Tous les ports ouverts ou filtrés/bloqués sont répertoriés dans les sections précédentes. Parmi les menaces les plus fréquentes, on compte :

ID du problème [3]	Synopsis	Commentaire
CVE-1999-0517 CVE-1999-0186 CVE-1999-0254 CVE-1999-0516	snmp (161/UDP) – le nom de communauté du serveur SNMP distant peut être deviné.	Le nom de communauté SNMP CC-SG par défaut est « public ». Les utilisateurs sont encouragés à le remplacer par une valeur spécifique au site (**Configuration ➔ Gestionnaire de configuration ➔** menu **SNMP**). Reportez-vous au **manuel de l'administrateur de CC-SG** pour plus d'informations.
CVE-2000-0843	Le serveur telnet distant a brusquement fermé la connexion après la saisie d'un long nom d'utilisateur suivi d'un mot de passe.	Le port 23 est généralement utilisé pour les services telnet. Cependant, CC-SG utilise ce port pour les sessions de la console de diagnostic SSH V2. Les utilisateurs peuvent modifier le port et/ou interdire complètement la méthode d'accès SSH à la console de diagnostic. Reportez-vous au **manuel de l'administrateur de CC-SG** pour plus d'informations.
CVE-2004-0230	L'hôte distant peut être vulnérable à un bogue d'approximation des numéros de séquence, ce qui peut permettre à un attaquant de lui envoyer des paquets RST de diversion et de fermer les connexions établies.	La pile de protocole TCP/IP sous-jacente utilisée par CC-SG ne semble pas sensible à cette menace.
CVE-2004-0079 CVE-2004-0081 CVE-2004-0112	L'hôte distant utilise une version d'OpenSSL antérieure à 0.9.6m ou 0.9.7d.	Les correctifs ci-après ayant été appliqués à OpenSSL, cette menace est écartée : • RHSA-2004:120 • RHSA-2005:830 • RHSA-2003:101-01

[3] Les bases de données CVE se trouvent sur le site **http://cve.mitre.org**.

Annexe C : Privilèges de groupe d'utilisateurs

MENU > SOUS-MENU	OPTION DE MENU	PRIVILEGE REQUIS	DESCRIPTION
Passerelle sécurisée	**Ce menu est disponible pour tous les utilisateurs.**		
	Mon profil	Aucun*	
	Message du jour	Aucun*	
	Imprimer	Aucun*	
	Déconnexion	Aucun*	
	Quitter	Aucun*	
Utilisateurs	**Ce menu et l'arborescence Utilisateurs sont disponibles uniquement pour les utilisateurs disposant du privilège User Management (gestions des utilisateurs).**		
> Gestionnaire des utilisateurs	> Ajouter un utilisateur	Gestion des utilisateurs	
	(Modification des utilisateurs)	Gestion des utilisateurs	Via Profil utilisateur
	> Supprimer un utilisateur	Gestion des utilisateurs	
	> Supprimer un utilisateur du groupe	Gestion des utilisateurs	
	> Déconnecter le ou les utilisateur(s)	Gestion des utilisateurs	
	> Copier en bloc	Gestion des utilisateurs	
> Gestionnaire des groupes d'utilisateurs	> Ajouter un groupe d'utilisateurs	Gestion des utilisateurs	
	(Modification des groupes d'utilisateurs)	Gestion des utilisateurs	Via Profil du groupe d'utilisateurs
	> Supprimer un groupe d'utilisateurs	Gestion des utilisateurs	
	> Affecter des utilisateurs à un groupe	Gestion des utilisateurs	
	> Déconnecter les utilisateurs	Gestion des utilisateurs	
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	Gestion des dispositifs, des ports et des nœuds	
> Gestionnaire des dispositifs	> Ajouter un dispositif	Gestion des dispositifs, des ports et des nœuds	

MENU > SOUS-MENU	OPTION DE MENU	PRIVILEGE REQUIS	DESCRIPTION
	(Modification des dispositifs)	Gestion des dispositifs, des ports et des nœuds	Via Profil du dispositif
	> Supprimer un dispositif	Gestion des dispositifs, des ports et des nœuds	
	> Copier en bloc	Gestion des dispositifs, des ports et des nœuds	
	> Mettre le dispositif à jour	Gestion de la configuration et de la mise à niveau des dispositifs	
>> Configuration	>> Sauvegarde	Gestion de la configuration et de la mise à niveau des dispositifs	
	>> Restaurer	Gestion de la configuration et de la mise à niveau des dispositifs	
	>> Copier la configuration	Gestion de la configuration et de la mise à niveau des dispositifs	
	> Redémarrer le dispositif	Gestion des dispositifs, des ports et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
	> Envoyer une commande ping au dispositif	Gestion des dispositifs, des ports et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
	> Suspendre la gestion	Gestion des dispositifs, des ports et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
	> Gestionnaire d'alimentation des dispositifs	Gestion des dispositifs, des ports et des nœuds	
	> Démarrer Admin	Gestion des dispositifs, des ports	

MENU > SOUS-MENU	OPTION DE MENU	PRIVILEGE REQUIS	DESCRIPTION
		et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
	> Lancer l'Admin de station utilisateur		
	> Déconnecter utilisateurs	Gestion des dispositifs, des ports et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
	> Vue topologique	Gestion des dispositifs, des ports et des nœuds	
> Modifier la vue	> Créer une vue personnalisée	Gestion des dispositifs, des ports et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
	> Tree View (Arborescence)	Gestion des dispositifs, des ports et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
> Gestionnaire des ports	> Connecter	Gestion des dispositifs, des ports et des nœuds	
	> Configurer les ports	Gestion des dispositifs, des ports et des nœuds	
	> Ajouter le port aux signets	Gestion des dispositifs, des ports et des nœuds	
	> Se déconnecter du port	Gestion des dispositifs, des ports et des nœuds	
	> Copier en bloc	Gestion des dispositifs, des ports et des nœuds	
	> Supprimer des ports	Gestion des dispositifs, des ports et des nœuds	
> Options de tri des ports	> Par nom de port	Gestion des dispositifs, des ports	

MENU > SOUS-MENU	OPTION DE MENU	PRIVILEGE REQUIS	DESCRIPTION
		et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
	> Par état de port	Gestion des dispositifs, des ports et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
Nœuds	**Ce menu et l'arborescence Nœuds 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)** **Node In-Band Access (accès en bande au nœud)** **Node Out-of-Band Access (accès hord bande au nœud)** **Node Power Control (gestion de l'alimentation des nœuds)**		
	Ajouter un nœud	Gestion des dispositifs, des ports et des nœuds	
	(Modification des nœuds)	Gestion des dispositifs, des ports et des nœuds	Via Profil du nœud
	Supprimer un nœud	Gestion des dispositifs, des ports et des nœuds	
	<nomInterface>	Accès en bande ou Accès hors bande	
	Déconnecter	Accès en bande ou Accès hors bande	
	Gestion de l'alimentation	Gestion de l'alimentation	
	Regrouper la gestion de l'alimentation	Gestion de l'alimentation	
> Options de tri du nœud	> Par nom de nœud	L'un des suivants : Gestion des dispositifs, des ports et des nœuds ou Accès en bande ou Accès hors bande ou Gestion de l'alimentation	
	> Par état de nœud	L'un des suivants : Gestion des dispositifs, des ports et des nœuds ou	

MENU > SOUS-MENU	OPTION DE MENU	PRIVILEGE REQUIS	DESCRIPTION
		Accès en bande ou Accès hors bande ou Gestion de l'alimentation	
> Conversation	> Démarrer la session de conversation	Accès en bande ou Accès hors bande ou Gestion de l'alimentation	
	> Afficher la session de conversation	Accès en bande ou Accès hors bande ou Gestion de l'alimentation	
	> Terminer la session de conversation	Accès en bande ou Accès hors bande ou Gestion de l'alimentation	
> Modifier la vue	> Créer une vue personnalisée	L'un des suivants : Gestion des dispositifs, des ports et des nœuds ou Accès en bande ou Accès hors bande ou Gestion de l'alimentation	
	> Tree View (Arborescence)	L'un des suivants : Gestion des dispositifs, des ports et des nœuds ou Accès en bande ou Accès hors bande ou Gestion de l'alimentation	
Associations	**Ce menu est disponible uniquement pour les utilisateurs disposant du privilège User Security Management (gestion de la sécurité des utilisateurs).**		
	> Associations	Gestion de la sécurité des utilisateurs	Comporte la capacité d'ajouter, de modifier et de supprimer.
	> Groupes de dispositifs	Gestion de la sécurité des utilisateurs	Comporte la capacité d'ajouter, de modifier et de supprimer.
	> Groupes de nœuds	Gestion de la sécurité des utilisateurs	Comporte la capacité d'ajouter, de modifier et de supprimer.
	> Stratégies	Gestion de la sécurité des utilisateurs	Comporte la capacité d'ajouter, de modifier et de supprimer.

MENU > SOUS-MENU	OPTION DE MENU	PRIVILEGE REQUIS	DESCRIPTION
Rapports	**Ce menu est disponible pour tous les utilisateurs.**		
	Journal d'audit	Paramétrage et contrôle de CC	
	Journal d'erreurs	Paramétrage et contrôle de CC	
	Rapport d'accès	Disponible uniquement pour les utilisateurs du groupe System Administrators	
	Rapport de disponibilité	Gestion des dispositifs, des ports et des nœuds ou Gestion de la configuration et de la mise à niveau des dispositifs	
> Utilisateurs	> Utilisateurs actifs	Gestion des utilisateurs	
	> Utilisateurs verrouillés	Paramétrage et contrôle de CC	
	> Données d'utilisateurs	Pour consulter les données de tous les utilisateurs : Gestion des utilisateurs Pour consulter vos propres données utilisateur : Aucun	
	> Utilisateurs dans groupes	Gestion des utilisateurs	
	> Données de groupes	Gestion de la sécurité des utilisateurs	
	> Rapport sur le groupe d'utilisateurs AD	Paramétrage et contrôle de CC ou Gestion des utilisateurs	
> Dispositifs	Gestion du parc	Gestion des dispositifs, des ports et des nœuds	
> Nœuds	> Rapport sur le parc du nœud	Gestion des dispositifs, des ports et des nœuds	
	> Nœuds actifs	Gestion des dispositifs, des ports et des nœuds	
	> Création du nœud	Gestion des dispositifs, des ports et des nœuds	
> Ports	> Interrogation des ports	Gestion des dispositifs, des ports et des nœuds	

MENU > SOUS-MENU	OPTION DE MENU	PRIVILEGE REQUIS	DESCRIPTION
	> Ports actifs	Gestion des dispositifs, des ports et des nœuds	
	Rapports programmés	Paramétrage et contrôle de CC	
	Synchronisation CC-NOC	Paramétrage et contrôle de CC	
Accès			
	Configuration CC-NOC	Paramétrage et contrôle de CC	
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 : Gestion des dispositifs, des ports et des nœuds, Gestion des utilisateurs et Gestion de la sécurité des utilisateurs	
	Paramétrage du Message du jour	Paramétrage et contrôle de CC	
	Applications	Paramétrage et contrôle de CC	
	Firmware	Paramétrage et contrôle de CC	
	Configuration	Paramétrage et contrôle de CC	
	Sécurité	Paramétrage et contrôle de CC	
	Notifications	Paramétrage et contrôle de CC	
	Tâches	Paramétrage et contrôle de CC	
	Matrice de compatibilité	Gestion de la configuration et de la mise à niveau des dispositifs	
Maintenance du système			
	Sauvegarde	Paramétrage et contrôle de CC	
	Restaurer	Paramétrage et contrôle de CC	
	Réinitialiser	Paramétrage et contrôle de CC	
	Redémarrer	Paramétrage et	

MENU > SOUS-MENU	OPTION DE MENU	PRIVILEGE REQUIS	DESCRIPTION
		contrôle de CC	
	Mettre à niveau	Paramétrage et contrôle de CC	
	Arrêter	Paramétrage et contrôle de CC	
> Mode de maintenance	> Entrer en mode de maintenance	Paramétrage et contrôle de CC	
	> Quitter le mode de maintenance	Paramétrage et contrôle de CC	
Afficher		Aucun*	
Fenêtre		Aucun*	
Aide		Aucun*	

*Aucun indique qu'aucun privilège particulier n'est requis. Tous les utilisateurs ayant accès à CC-SG peuvent accéder à ces menus et commandes.

Annexe D : Traps SNMP

CC-SG fournit les traps 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	Raison de l'échec de l'exécution d'une tâche programmée.
ccDiagnosticConsoleLogin	Un utilisateur s'est connecté à la console de diagnostic CC-SG.
ccDiagnosticConsoleLogout	Un utilisateur s'est déconnecté de la console de diagnostic CC-SG.
ccNOCAvailable	CC-SG a détecté que CC-NOC est disponible.
ccNOCUnavailable	CC-SG a détecté que CC-NOC n'est pas disponible.
ccUserGroupAdded	Un nouveau groupe d'utilisateurs a été ajouté à CC-SG.
ccUserGroupDeleted	Un groupe d'utilisateurs CC-SG a été supprimé.
ccUserGroupModified	Un groupe d'utilisateurs CC-SG a été modifié.
ccSuperuserNameChanged	Le mot de passe super utilisateur CC-SG a changé.
ccSuperuserPasswordChanged	Le mot de passe super utilisateur CC-SG a changé.
ccLoginBannerChanged	La bannière de connexion CC-SG a changé.
ccMOTDChanged	Le message du jour CC-SG (MOTD) a changé.

Annexe E : Guide de dépannage

- Pour lancer CC-SG à partir de votre navigateur Web, il vous faut un plug-in Java. Si votre machine ne dispose pas de la bonne version, CC-SG vous guidera dans la procédure d'installation. Si votre machine ne dispose de plug-in Java, CC-SG ne peut pas être lancé automatiquement. Dans ce cas, vous devez désinstaller ou désactiver votre ancienne version de Java et fournir une connectivité de port série à CC-SG pour assurer un fonctionnement optimal.
- Si l'applet CC-SG ne se charge pas, vérifiez les paramètres de votre navigateur Web.
  - Dans Internet Explorer : vérifiez que Java (Sun) est activé.
  - Ouvrez le plug-in Java dans le Panneau de configuration et réglez les paramètres dans votre navigateur.
- Si vous rencontrez des problèmes pour ajouter des dispositifs, vérifiez que les versions des firmware des dispositifs sont correctes.
- Si le câble de l'interface réseau reliant le dispositif et CC-SG est déconnecté, patientez pendant le test de détection de collision défini, puis rebranchez le câble d'interface réseau. Pendant la période de détection de collision configurée, le dispositif fonctionne en mode autonome et est accessible via RRC, MPC ou RC.
- Si vous recevez un message d'erreur indiquant que la version de votre client est différente de la version du serveur et que le comportement peut être imprévisible, vous devez redémarrer et vider la mémoire cache de votre navigateur.

Configuration requise pour le navigateur client

Pour obtenir une liste complète des navigateurs et plates-formes pris en charge, reportez-vous à la **matrice de compatibilité** sur **http://www.raritan.com/support**. Dans la page **Support** (Assistance), cliquez sur **Firmware Upgrades** (Mises à niveau de firmware), puis sur **CommandCenter Secure Gateway**.

Annexe F : Authentification à deux facteurs

Dans le cadre de l'authentification à distance RADIUS, CC-SG peut être configuré afin de pointer vers un serveur RSA RADIUS prenant en charge l'authentification à deux facteurs via un gestionnaire d'authentification RSA associé. 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.

Environnements pris en charge

Les composants d'authentification à deux facteurs RSA 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.

Configuration requise

La configuration correcte d'un serveur RSA RADIUS et d'un gestionnaire d'authentification RSA ne fait pas partie de l'objectif de ce guide. Reportez-vous à la documentation RSA pour plus d'informations.

Notez, toutefois, que les procédures ci-après doivent être effectuées :

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.

Problèmes répertoriés

Le mode RSA RADIUS « New PIN » nécessitant un mot de passe ou un numéro d'identification personnel de vérification ne fonctionnera pas. Aussi, tous les utilisateurs de ce schéma doivent recevoir des mots de passe fixes.

Annexe G : FAQ

QUESTION	RÉPONSE
Généralités	
Qu'est-ce que CC-SG ?	CC-SG est un dispositif de gestion réseau permettant d'ajouter et d'intégrer des serveurs et des équipements réseau généralement déployés dans un centre de données et connectés à un produit Raritan qui prend en charge le protocole IP.
A quoi sert CC-SG ?	La gestion de vos centres de données devient de plus en plus complexe à mesure que vous y déployez d'autres serveurs et dispositifs. CC-SG permet aux administrateurs ou aux responsables système d'accéder à l'ensemble des serveurs, équipements et utilisateurs, et de les gérer à partir d'un seul dispositif.
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 ?	CC-SG prend en charge tous les produits Dominion - les produits KVM sur IP de Raritan - Dominion KX ; - les produits de serveurs de consoles sécurisées de Raritan - Dominion SX ; - les produits de gestion des bureaux distants de Raritan - Dominion KSX. CC-SG prend également en charge Paragon II associé à des stations utilisateur à accès par IP facultatives.
Comment CC-SG s'intègre-t-il avec les autres produits Raritan ?	CC-SG utilise une technologie de recherche et de détection propriétaire unique qui identifie les dispositifs Raritan et s'y connecte à l'aide d'une adresse réseau connue. Une fois CC-SG connecté et configuré, les dispositifs qui lui sont reliés sont transparents et le fonctionnement et la gestion deviennent extrêmement simples.
L'accès par assistant numérique personnel est-il possible ?	Réponse générique : Oui, dans la mesure où l'assistant numérique personnel dispose d'un navigateur Java et prend en charge le cryptage SSL 128 bits (ou de puissance inférieure dans certaines régions). Pour plus d'informations, prenez contact avec le support technique de Raritan. Aucun essai n'a été effectué dans ce domaine.
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 est situé 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 autorisé 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 ?	Il n'existe pas de limite spécifique au nombre de nœuds et/ou d'unités Dominion et/ou d'unités IP-Reach qui peuvent être connectés. Mais il n'est cependant pas illimité : les performances du processeur et la quantité de mémoire sur le serveur hôte déterminent le nombre de ports auxquels il est réellement possible de se connecter.

QUESTION	RÉPONSE
Existe-t-il une manière d'optimiser les performances de Microsoft Internet Explorer si celui-ci est mon navigateur Web préféré ?	Pour améliorer les performances de Microsoft Internet Explorer lors de l'accès à la console, désactivez les options « Compilateur Java JIT activé », « Journalisation Java activée » et « Console Java activée ». Dans la barre de menus principale, sélectionnez **Outils > Options Internet > Avancées**. Faites défiler la liste des options jusqu'à ce que vous voyiez les éléments ci-dessus et assurez-vous qu'ils **ne sont pas** cochés.
Que faire si je ne parviens pas à ajouter un port série/de console à CC-SG ?	Si le dispositif de console/série est un produit Dominion, vérifiez que les conditions suivantes sont remplies : - l'unité Dominion est active ; - l'unité Dominion n'a pas atteint le nombre maximum de comptes utilisateur configurés.
Quelles sont les versions de Java prises en charge par CC-SG de Raritan ?	Pour en savoir plus sur la configuration Java minimum requise côtés serveur et client, consultez la matrice de compatibilité sur **http://www.raritan.fr/support**. Cliquez sur **Mises à niveau de firmware**, puis sur **CommandCenter Secure Gateway**.
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 par l'intermédiaire d'un navigateur Web 443 : pour l'accès HTTPS par l'intermédiaire d'un navigateur Web 8080 : pour les fonctions serveur de CC-SG 2400 : pour les connexions en Mode Proxy 5001 : pour la notification d'événements IPR/DKSX/DKX/P2-SC Si un pare-feu se trouve entre deux nœuds de cluster, les ports suivants doivent être ouverts pour que le cluster fonctionne correctement : 8732 : pour le test de détection de collision des nœuds du cluster 5432 : pour la réplication BD des nœuds du cluster
Quelles sont les instructions de conception pour les systèmes à grande échelle ? Contraintes ou hypothèses ?	Raritan propose deux modèles pour l'évolutivité du serveur : le modèle centre de données et le modèle réseau. Le modèle centre de données utilise Paragon pour gérer des milliers de systèmes dans un seul centre de données. Il s'agit de la méthode la plus efficace et la plus rentable pour gérer un emplacement unique. Il prend également en charge le modèle réseau avec IP-Reach et la station utilisateur à accès par IP (UST-IP). Le modèle réseau est géré par le biais du réseau TCP/IP et regroupe l'accès par l'intermédiaire de CC-SG. Les utilisateurs n'ont donc pas besoin de connaître les adresses IP ou la topologie des dispositifs d'accès. Il propose également une connexion unique pratique.

QUESTION	RÉPONSE
Authentification	
Combien de comptes utilisateur peuvent-ils être créés pour CC-SG ?	Vérifiez les limites associées à votre licence. Il n'existe pas de limite spécifique au nombre de comptes utilisateur que vous pouvez créer. Ce nombre n'est cependant pas illimité. La taille de la base de données, les performances du processeur et la quantité de mémoire sur le serveur qui héberge CC-SG déterminent le nombre de comptes utilisateur pouvant réellement être créés.
Puis-je attribuer une adresse de nœud spécifique à un utilisateur spécifique ?	Oui, si vous disposez de droits d'administrateur. Les administrateurs ont la possibilité d'affecter des nœuds spécifiques à chaque utilisateur.
Si nous disposons de plus de 1 000 utilisateurs, comment la gestion peut-elle être effectuée ? Active Directory est-il pris en charge ?	CC-SG fonctionne avec Microsoft Active Directory, Sun iPlanet ou Novell eDirectory. Si un compte utilisateur existe déjà sur un serveur d'authentification, CC-SG prend en charge l'authentification à distance à l'aide d'**AD/TACACS+ /RADIUS/LDAP**.
Quelles sont les options disponibles pour l'authentification avec des services d'annuaires et des outils de sécurité tels que LDAP, AD, RADIUS, etc. ?	CC-SG autorise l'authentification locale, ainsi que l'authentification à distance. Les serveurs d'authentification à distance pris en charge sont les suivants : AD, TACACS+, RADIUS et LDAP.
Sécurité	
Parfois, lorsque j'essaie de me connecter, j'obtiens un message m'indiquant que mon nom d'utilisateur est incorrect, même si je suis certain d'avoir saisi le nom d'utilisateur et le mot de passe exacts. Pourquoi ?	Un identifiant de session spécifique est transmis chaque fois que vous vous connectez à CC-SG. Cet identifiant possède une fonction d'expiration et, en conséquence, si vous ne vous connectez pas à l'unité avant que le délai d'expiration soit atteint, 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 m'indiquant que je ne suis plus connecté lorsque je clique sur un menu de CC-SG. Pourquoi ?	CC-SG surveille la durée de chaque session utilisateur. En cas d'inactivité pendant une période prédéfinie, CC-SG déconnecte l'utilisateur. La durée de la période est prédéfinie sur 60 minutes, mais peut être reconfigurée. Il est recommandé aux utilisateurs de **quitter** CC-SG lorsqu'ils terminent une session.
Raritan accède au serveur en tant qu'agent root. Il est donc possible que cela	Non, les utilisateurs n'ont pas accès au serveur en tant qu'agents root une fois que l'unité est livrée par Raritan, Inc.

QUESTION	RÉPONSE
occasionne 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 ?	
Le chiffrement SSL est-il interne et externe (pas seulement réseau étendu mais également réseau local) ?	Les deux. La session est chiffrée sans tenir compte de l'origine, réseau local ou réseau étendu.
CC-SG prend-il en charge la liste CRL, c'est-à-dire la liste LDAP des certificats invalides ?	Non.
CC-SG prend-il en charge la demande de certificat client ?	Non.
Comptabilité	
L'heure des événements dans le rapport Journal d'audit semble incorrecte. Pourquoi ?	L'heure des événements est consignée selon les paramètres de date et d'heure de l'ordinateur client. Vous pouvez modifier ces derniers.
Les fonctions d'audit/ enregistrement permettent-elles de savoir quel utilisateur a effectué une mise sous/hors tension ?	La mise hors tension directe n'est pas enregistrée, mais la gestion de l'alimentation par le biais de CC-SG peut être consignée dans des journaux d'audit.
Performances	
En tant qu'administrateur de CC-SG, j'ai ajouté plus de 500 nœuds que je me suis affectés. A présent, la connexion à CC-SG prend beaucoup de temps.	En tant qu'administrateur, lorsqu'un grand nombre de nœuds vous est affecté, CC-SG télécharge les informations pour tous les nœuds lors de la connexion, ce qui ralentit considérablement cette dernière. Nous vous recommandons de ne pas affecter un trop grand nombre de nœuds aux comptes administrateur utilisés essentiellement pour gérer la configuration/les paramètres de CC-SG.
Quelle est la bande passante utilisée par le client ?	Le niveau d'activité réseau d'un accès à distance à une console série sur TCP/IP est pratiquement le même que celui d'une session Telnet. Cependant, il existe une limite de la bande passante RS232 du port de console proprement dit, plus le temps système SSL/TCP/IP. Raritan Remote Client (RRC) gère l'accès à distance à une console KVM. Cette application permet de disposer d'une bande passante ajustable des réseaux locaux jusqu'aux utilisateurs connectés à distance.

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 ».
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 qui est 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 qui se produisent au niveau du système et du réseau.
Quelles sont les recommandations au sujet du déplacement/changement des modules d'interface pour ordinateur (Computer Interface Module, CIM) au niveau physique avec des modifications apportées à la base de données logique ?	Chaque CIM a un numéro de série et un nom système cible. Nos systèmes considèrent qu'un CIM reste connecté à la cible correspondant à son nom en cas de déplacement de la connexion d'un commutateur à un autre. Ce mouvement se reflète automatiquement sur la configuration système et est répercuté dans CC-SG. En revanche, si le CIM est déplacé sur un autre serveur, un administrateur doit le renommer.
Interopérabilité	
Comment CC-SG s'intègre-t-il aux produits à châssis à lame ?	CC-SG peut prendre en charge tout dispositif 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.

QUESTION	RÉPONSE
Autorisation	
L'autorisation est-elle possible avec RADIUS/TACACS/ LDAP ?	LDAP et TACACS sont utilisés uniquement pour l'authentification à distance, pas pour l'autorisation.
Expérience utilisateur	
En ce qui concerne la gestion de la console par l'intermédiaire d'un port réseau ou d'un port série local (COM2, par exemple) : la connexion est-elle gérée en local par CC-SG, ou perdue ?	La connexion à CC-SG par l'intermédiaire de la console CC-SG elle-même équivaut à obtenir le privilège racine du système d'exploitation (Linux) sur lequel CC-SG est exécuté. Syslog enregistre ce genre d'événements, mais ce que les utilisateurs saisissent au niveau de la console CC-SG est perdu.

Annexe H : Raccourcis clavier

Les raccourcis clavier ci-après peuvent être utilisés dans Director Client.

OPÉRATION	RACCOURCI CLAVIER
Actualiser	F5
Panneau d'impression	Ctrl + P
Aide	F1
Insérer une ligne dans le tableau Associations	Ctrl + I

Bureaux en Amérique du Nord

Raritan
400 Cottontail Lane
Somerset, NJ 08873
Etats-Unis d'Amérique
Tél. (732) 764-8886
ou (800) 724 -8090
Fax (732) 764 -8887
E-mail : **sales@raritan.com**
Site Web : Raritan.com

Raritan NC
4901 Waters Edge Dr.
Suite 101
Raleigh, NC 27606
Tél. (919) 277-0642
E-mail : **sales.nc@raritan.com**
Site Web : Raritan.com

Raritan Canada
4 Robert Speck Pkwy, Suite 1500
Mississauga, ON L4Z 1S1 Canada
Tél. (905) 949-3650
Fax (905) 949-3651
E-mail : **sales.canada@raritan.com**
Site Web : Raritan.ca

Bureaux européens

Raritan Pays-Bas
Eglantierbaan 16
2908 LV Capelle aan den IJssel
Pays-Bas
Tél. (31) 10-284-4040
Fax (31) 10-284-4049
E-mail : **sales.europe@raritan.com**
Site Web : Raritan.info

Raritan Allemagne
Lichtstraße 2
D-45127 Essen, Allemagne
Tél. (49) 201-747-98-0
Fax (49) 201-747-98-50
E-mail : **sales.germany@raritan.com**
Site Web : Raritan.de

Raritan France
120 Rue Jean Jaurès
92300 Levallois-Perret, France
Tél. (33) 14-756-2039
Fax (33) 14-756-2061
E-mail : **sales.france@raritan.com**
Site Web : Raritan.fr

Raritan Royaume-Uni
36 Great St. Helen's
London EC3A 6AP, Royaume-Uni
Tél. (44) 20-7614-7700
Fax (44) 20-7614-7701
E-mail : **sales.uk@raritan.com**
Site Web : Raritan.co.uk

Raritan Italie
Via dei Piatti 4
20123 Milan, Italie
Tél. (39) 02-454-76813
Fax (39) 02-861-749
E-mail : **sales.italy@raritan.com**
Site Web : Raritan.it

Bureaux au Japon

Raritan Japon
4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-Ku
Tokyo 104-0033, Japon
Tél. (81) 03-3523-5991
Fax (81) 03-3523-5992
E-mail : **sales@raritan.co.jp**
Site Web : Raritan.co.jp

Raritan Osaka
1-15-8 Nishihonmachi, Nishi-ku
Osaka 550-0005, Japon
Tél. (81) (6) 4391-7752
Fax (81) (6) 4391-7761
E-mail : **sales@raritan.co.jp**
Site Web : Raritan.co.jp

Bureaux dans la région Asie Pacifique

Raritan Taïwan
5F, 121, Lane 235, Pao-Chiao Road
Hsin Tien City
Taipei Hsien, Taïwan, ROC
Tél. (886) 2 8919-1333
Fax (886) 2 8919-1338
E-mail : **sales.taiwan@raritan.com**
Site Web en chinois : Raritan.com.tw
Site Web en anglais : Raritan-ap.com

Raritan Shanghaï
Rm 17E Cross Region Plaza
No. 899 Lingling Road
Shanghaï, Chine 200030
Tél. (86) 21 5425-2499
Fax (86) 21 5425-3992
E-mail : **sales.china@raritan.com**
Site Web : Raritan.com.cn

Raritan Beijing
Unit 1310, Air China Plaza
No.36 XiaoYun Road
Chaoyang District
Beijing 100027, Chine
Tél. (86) 10 8447-5706
Fax (86) 10 8447-5700
E-mail : **sales.china@raritan.com**
Site Web : Raritan.com.cn

Raritan Guangzhou
Room 1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou 510075 Chine
Tél. (86-20)8755 5581
Fax (86-20)8755 5571
E-mail : **sales.china@raritan.com**
Site Web : Raritan.com.cn

Raritan Corée
#3602, Trade Tower,
World Trade Center
Samsung-dong, Kangnam-gu
Séoul, Corée
Tél. : (82) 2 557-8730
Fax (82) 2 557-8733
E-mail : **sales.korea@raritan.com**
Site Web : Raritan.co.kr

Raritan Australie
Level 2, 448 St Kilda Road,
Melbourne, VIC 3004, Australie
Tél. (61) 3 9866-6887
Fax (61) 3 9866-7706
E-mail : **sales.au@raritan.com**
Site Web : Raritan.co.au

Raritan Inde
210 2nd Floor Orchid Square Sushant Lok 1,
Block B, Gurgaon 122 002 Haryana Inde
Tél. (91) 124 510 7881
Fax (91) 124 510 7880
E-mail : **sales.india@raritan.com**
Site Web : Raritan.co.in

Division OEM de Raritan

Peppercon AG, Raritan OEM Division
Scheringerstrasse 1
08056 Zwickau Allemagne
Tél. : (49) 375-27-13-49-0
E-mail : **info@peppercon.com**
Site Web : www.peppercon.de