Dominion KX II

Manuel d'utilisation

Version 2.2

Copyright © 2009 Raritan, Inc.

DKX2-v2.2.0-0L-F

Janvier 2010

255-62-4023-00

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

© Copyright 2009 Raritan, Inc., CommandCenter®, Dominion®, Paragon® et le logo de la société Raritan sont des marques ou des marques déposées de Raritan, Inc. Tous droits réservés. Java® est une marque déposée de Sun Microsystems, Inc. Internet Explorer® est une marque déposée de Microsoft Corporation. Netscape® et Netscape Navigator® sont des marques déposées de Netscape Communication Corporation. Toutes les autres marques ou marques déposées sont la propriété de leurs détenteurs respectifs.

Informations FCC (Etats-Unis seulement)

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

Informations VCCI (Japon)

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

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

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

Table des matières

Chapitre 1 Introduction 1

Aide Dominion KX II 1
Documentation connexe 1
Nouveautés de l'aide 2
Dominion KX II - Présentation 3
Applications clients utilisables avec Dominion KX II 5
Support virtuel 6
Photos du produit 7
Caractéristiques du produit 9
Matériel 9
Logiciel 10
Terminologie 10
Contenu de l'emballage 12

Chapitre 2 Installation et configuration 13

Présentation 13
Données de connexion par défaut 13
Mise en route 14
Etape 1 : Configuration des serveurs cible KVM 14
Etape 2 : Configuration des paramètres du pare-feu de réseau 28
Etape 3 : Connexion de l'équipement 29
Etape 4 : Configuration de Dominion KX II 32
Caractères spéciaux valides pour les noms de cibles 37
Etape 5 (facultative) : Configuration de la langue du clavier 40

Chapitre 3 Utilisation des serveurs cible 42

Interfaces 42
Interface de la console locale de Dominion KX II 43
Interface de la console distante de Dominion KX II 43
Interface Multi-Platform Client 56
Virtual KVM Client 57
Présentation 57
Connexion à un serveur cible KVM 57
Barre d'outils VKC 58
Commutation entre les serveurs cible KVM 60
Gestion de l'alimentation d'un serveur cible 60
Déconnexion des serveurs cible KVM 61
Sélection des profils USB 62
Connection Properties (Propriétés de connexion) 63
Informations sur la connexion 65

Options de clavier 66
Propriétés vidéo 70
Options de souris 75
Supports virtuels VKC 80
Cartes à puce (VKC et MPC) 81
Options d'outils 84
Options d'affichage 87
Options d'aide 87
Active KVM Client (AKC) 89
Présentation 89
Conditions préalables à l'utilisation d'AKC 90
Systèmes d'exploitation et navigateurs pris en charge par AKC 91

Chapitre 4 Support virtuel 92

Présentation 93
Conditions requises pour l'utilisation des supports virtuels 96
Utilisation du support virtuel via VKC et AKC dans un environnement Windows 97
Utilisation des supports virtuels 98
Configuration du serveur de fichiers (Images ISO du serveur de fichiers uniquement) 99
Connexion aux supports virtuels 101
Local Drives (Lecteurs locaux) 101
Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible 102
CD-ROM/DVD-ROM/ISO Images (Images ISO/CD-ROM/DVD-ROM) 103
Déconnexion des supports virtuels 105

Chapitre 5 Profils USB 106

Présentation 106
Compatibilité CIM 107
Profils USB disponibles 107
Sélection des profils pour un port KVM 114
Modes de souris lors de l'utilisation du profil USB Mac OS X avec DCIM-VUSB 114

Chapitre 6 User Management (Gestion des utilisateurs) 115

Groupes d'utilisateurs 115
Liste des groupes d'utilisateurs 116
Relation entre les utilisateurs et les groupes 116
Ajout d'un nouveau groupe d'utilisateurs 117
Modification d'un groupe d'utilisateurs existant 124
Utilisateurs 125
Liste des utilisateurs 125
Ajout d'un nouvel utilisateur 126
Modification d'un utilisateur existant 127
Déconnexion d'un utilisateur (Déconnexion forcée) 127
Paramètres d'authentification 128
Implémentation de l'authentification à distance LDAP/LDAPS 129
Renvoi des informations relatives aux groupes d'utilisateurs à partir d'Active Directory 133
Implémentation de l'authentification à distance RADIUS 134

Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS 137
Spécifications des échanges de communication RADIUS 137
Processus d'authentification de l'utilisateur 139
Modification d'un mot de passe 141

Chapitre 7 Gestion des dispositifs 142

Network Settings (Paramètres réseau) 142
Paramètres réseau de base 143
Paramètres de l'interface LAN 146
Services du dispositif 147
Présentation de l'accès direct aux ports 149
Présentation de la fonction Activer la validation du certificat du serveur de téléchargement AKC 150
Paramètres de modem 151
Configuration des paramètres de date et heure 153
Gestion des événements 154
Configuration de la gestion des événements - Paramètres 155
Gestion des événements - Destinations 157
Configuration de l'alimentation 162
Configuration des ports 164
Configuration des serveurs cible standard 165
Configuration des cibles des barrettes d'alimentation (PDU de rack) 166
Configuration des châssis de lames 172
Configuration des profils USB (page Port) 197
Configuration des paramètres du port local de Dominion KX II 200

Chapitre 8 Gestion des prises de barrettes d'alimentation (PDU de rack) 205

Présentation 205
Mise sous/hors tension des prises et alimentation cyclique 206

Chapitre 9 Gestion de la sécurité 209

Security Settings (Paramètres de sécurité) 209
Limitations de connexion 210
Mots de passe sécurisés 212
User Blocking (Blocage des utilisateurs) 213
Encryption & Share (Chiffrement & partage) 215
Activation de FIPS 140-2 219

Configuration du contrôle d'accès IP 221
Certificats SSL 224

Chapitre 10 Maintenance 227

Journal d'audit 227
Device Information (Informations sur le dispositif) 228
Backup and Restore (Sauvegarde et restauration) 229
USB Profile Management (Gestion des profils USB) 232
Gestion des conflits dans les noms de profil 233
Mise à niveau des CIM 233
Mise à niveau du firmware 234
Historique des mises à niveau 237
Redémarrage 237
Arrêt de la gestion par CC-SG 239

Chapitre 11 Diagnostics 241

Page d'interface réseau 241
Page Network Statistics (Statistiques réseau) 241
Page Ping Host (Envoi de commande Ping à l'hôte) 244
Page Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte) 245
Page Device Diagnostics (Diagnostics du dispositif) 246

Chapitre 12 Interface de ligne de commande (CLI) 248

Présentation 248
Accès à Dominion KX II à l'aide de la CLI 249
Connexion SSH à Dominion KX II 249
Accès SSH depuis un PC Windows 249
Accès SSH depuis un poste de travail UNIX/Linux 250
Connexion via Telnet à Dominion KX II 250
Activation de Telnet 250
Accès à Telnet depuis un PC Windows 250
Connexion 251
Navigation de la CLI 252
Saisie automatique des commandes 253
Syntaxe CLI - Conseils et raccourcis 253
Commandes courantes pour tous les niveaux de la CLI 253
Configuration initiale à l'aide de la CLI 254
Définition des paramètres 254
Définition des paramètres réseau 255
Invites CLI 255
Commandes CLI 255
Problèmes de sécurité 256
Administration des commandes de configuration du serveur de console de Dominion KX II ... 257
Configuration du réseau 257
Commande interface 258
Commande name 258
Commande IPv6 259

Chapitre 13 Console locale de Dominion KX II 260

Présentation 260
Utilisation de la console locale de Dominion KX II 260
Utilisateurs simultanés 260
Interface de la console locale de Dominion KX II 261
Sécurité et authentification 261
Accès par carte à puce à la console locale 262
Accès par carte à puce pour les dispositifs KX2 8 263
Résolutions disponibles 263
Page d'accès aux ports (affichage de serveur de la console locale) 264
Raccourcis-clavier et touches de connexion 266
Exemples de touches de connexion 266
Combinaisons de touches Sun spéciales 267
Accès à un serveur cible 268
Retour à l'interface de la console locale de Dominion KX II 268
Administration du port local 269
Configuration des paramètres du port local de la console locale de Dominion KX II 269
Réinitialisation des paramètres d'usine de la console locale de Dominion KX II 273
Réinitialisation de Dominion KX II à l'aide du bouton de réinitialisation 274

Annexe A Spécifications 276

Spécifications physiques 276
Impératifs d'environnement 279
Modules d'interface pour ordinateur (CIM) 279
Systèmes d'exploitation et CIM pris en charge (serveurs cible) 281
Systèmes d'exploitation pris en charge (Clients) 287
Navigateurs pris en charge 288
Modems certifiés 289
Dispositifs pris en charge par le port local étendu de KX2-832 et de KX2-864 289
Distance de connexion et résolution vidéo du serveur cible 289
Distances maximales recommandées pour le port local étendu de KX2-832 et de KX2-864 290
Connexion à distance 290
Résolutions vidéo prises en charge 291
Langues de clavier prises en charge 292
Lecteurs de cartes à puce 293
Lecteurs de cartes à puce pris en charge ou non 293
Configuration système minimale requise 295
Ports TCP et UDP utilisés 297
Paramètres de vitesse réseau 299

Annexe B Mise à jour du schéma LDAP 301

Renvoi des informations relatives aux groupes d'utilisateurs 301
A partir de LDAP 301
A partir de Active Directory (AD) de Microsoft 301

Définition du Registre pour autoriser les opérations d'écriture sur le schéma 302
Création d'un attribut..... 302
Ajout d'attributs à la classe 303
Mise à jour du cache de schéma 305
Modification des attributs rciusergroup pour les membres utilisateurs..... 305

Annexe C Remarques d'informations 309

Présentation..... 309
Java Runtime Environment (JRE) 309
Remarques sur la prise en charge d'IPv6..... 310
Claviers 311
Claviers non américains 311
Claviers Macintosh 314
Synchronisation des pointeurs de souris (Fedora) 315
Longueurs de câbles et résolutions vidéo pour châssis Dell..... 315
Fedora..... 316
Résolution du focus de Fedora Core..... 316
Connexions par carte à puce VKC et MPC aux serveurs Fedora..... 316
Dépannage des problèmes de blocage de Firefox lors de l'utilisation de Fedora..... 316
Modes et résolutions vidéo 317
Modes vidéo SUSE/VESA..... 317
Résolutions vidéo prises en charge non affichées 317
Ports et profils USB..... 318
Ports USB VM-CIM et DL360 318
Aide pour la sélection des profils USB 318
Modification d'un profil USB lors de l'utilisation d'un lecteur de cartes à puce..... 320
CIM..... 320
Souris à 3 boutons Windows sur les cibles Linux 320
Comportement des dispositifs USB composites Windows 2000 pour la fonction Support virtuel 321
Support virtuel..... 322
Support virtuel non rafraîchi après l'ajout de fichiers 322
Durée d'amorçage du BIOS cible avec les supports virtuels 322
Echec de connexion des supports virtuels lors de l'utilisation du haut débit..... 322
CC-SG 322
Version de Virtual KVM Client non reconnue par le mode proxy CC-SG 322
Mode souris simple - Connexion à une cible Dominion KX II contrôlée par CC-SG via VKC utilisant Firefox 323
Mode proxy et MPC..... 323
Déplacement entre ports de Dominion KX II 323

Annexe D FAQ **324**

Questions générales 325
Accès à distance 327
Support virtuel universel 329
Profils USB 330
Ethernet et mise en réseau IP 332
Gestion de réseau IPv6 339
Windows 341
Serveurs lames 342
Installation 345
Port local 347
Port local étendu (modèles KX2-832 et KX2-864 Dominion uniquement) 349
Gestion de l'alimentation 350
Evolutivité 351
Modules d'interface pour ordinateur (CIM) 352
Sécurité 353
Authentification par cartes à puce et CAC 355
Capacités de gestion 356
Divers 357

Index **359**

Chapitre 1 Introduction

Dans ce chapitre

Aide Dominion KX II 1
Nouveautés de l'aide 2
Dominion KX II - Présentation 3
Applications clients utilisables avec Dominion KX II 5
Support virtuel 6
Photos du produit 7
Caractéristiques du produit.....9
Terminologie 10
Contenu de l'emballage 12

Aide Dominion KX II

L'aide Dominion KX II explique comment installer, paramétrer et configurer Dominion KX II. Elle comprend également des informations sur l'accès aux serveurs cible et aux barrettes d'alimentation, à l'aide des supports virtuels, sur la gestion des utilisateurs et de la sécurité, ainsi que sur la maintenance et les diagnostics du produit Dominion KX II.

Une version PDF de l'aide peut être téléchargée de la ***page Firmware and Documentation*** http://www.raritan.com/support/firmware-and-documentation/ du site Web de Raritan. Raritan vous recommande de consulter son site Web pour obtenir les derniers manuels d'utilisation disponibles.

Remarque : Pour utiliser l'aide en ligne, Active Content (Contenu actif) doit être activé dans votre navigateur. Consultez l'aide de votre navigateur pour en savoir plus sur l'activation du contenu actif.

Documentation connexe

L'aide Dominion KX II est accompagnée du manuel de configuration rapide Dominion KX II, qui se trouve sur la ***page Firmware and Documentation*** http://www.raritan.com/support/firmware-and-documentation/ du site Web de Raritan. Les exigences et les instructions d'installation des applications clientes utilisées avec Dominion KX II se trouvent dans le **manuel des clients d'accès KVM et série**, également présent sur le site Web de Raritan. Le cas échéant, des fonctions clientes particulières utilisées avec Dominion KX II sont incluses dans l'aide.

Nouveautés de l'aide

Les informations suivantes ont été ajoutées à cause d'améliorations et de modifications apportées à l'équipement et/ou à la documentation utilisateur.

- Active KVM Client (AKC) est un nouveau client spécifique aux environnements Windows et pris en charge par Dominion KX II. Reportez-vous au **manuel des clients KVM et série** pour en savoir plus et à ***Active KVM Client (AKC)*** (à la page 89) pour une présentation.
- Dominion KX II contient maintenant un module cryptographique validé FIPS 140-2 imbriqué. Reportez-vous à ***Cryptage et partage*** (voir "Encryption & Share (Chiffrement & partage)" à la page 215).
- Une fonction Direct Port Access (Accès direct aux ports) permettant de se connecter directement aux cibles à partir du navigateur a été ajoutée à Dominion KX II. Reportez-vous à ***Services du dispositif*** (à la page 147).
- Une fonction permettant un accès à distance facultatif aux dispositifs sous la gestion de CC-SG a été ajoutée à Dominion KX II. Reportez-vous à ***Définition des autorisations*** (voir "Configuration des autorisations" à la page 119).
- La prise en charge de résolutions vidéo grand écran supplémentaires a été ajoutée à Dominion KX II. Reportez-vous à ***Résolutions vidéo prises en charge*** (à la page 291).
- Dominion KX II prend maintenant en charge le système d'exploitation Window 7 de Microsoft. Reportez-vous à ***CIM et systèmes d'exploitation pris en charge (serveurs cible)*** (voir "Systèmes d'exploitation et CIM pris en charge (serveurs cible)" à la page 281) et ***Systèmes d'exploitation pris en charge (clients)*** (à la page 287).

Reportez-vous aux notes de versions pour obtenir une explication plus détaillée des modifications apportées à cette version de l'aide.

Dominion KX II - Présentation

Dominion KX II est un commutateur KVM (écran-clavier-souris) numérique sécurisé conçu pour l'entreprise, qui offre un accès au niveau du BIOS (et au-dessus) et permet de gérer des serveurs, où que vous vous trouviez dans le monde, par l'intermédiaire d'un navigateur Web. 64 serveurs au plus peuvent être contrôlés avec une unité Dominion KX II standard. Pour le modèle Dominion KX II pour huit utilisateurs, 32 serveurs au plus peuvent être contrôlés avec KX2-832 et jusqu'à 64 serveurs avec KX2-864.

Dominion KX II prend en charge jusqu'à huit canaux vidéo, et permet à tout moment à huit utilisateurs de se connecter simultanément à huit cibles vidéo différentes. Sur le rack, Dominion KX II permet de contrôler au niveau du BIOS jusqu'à 64 serveurs et autres dispositifs informatiques depuis un ensemble clavier, écran et souris unique. Les fonctions d'accès à distance intégrées à Dominion KX II procurent le même niveau de contrôle des serveurs via un navigateur Web.

L'installation de Dominion KX II est facilitée par l'utilisation d'un câblage UTP (Cat5/5e/6) standard. Ses caractéristiques clés sont les suivantes : support virtuel, chiffrement 128 bits, double alimentation, gestion de l'alimentation à distance, Ethernet double, LDAP, RADIUS, Active Directory, intégration de Syslog, capacités de modem externe et gestion Web. Le modèle Dominion KX II pour huit utilisateurs dispose également d'un port local étendu à l'arrière du dispositif. Ces fonctions permettent d'améliorer les temps d'exploitation, la productivité et la sécurité, n'importe où, n'importe quand.

Les produits Dominion KX II peuvent fonctionner de manière autonome et ne dépendent pas d'un dispositif de gestion central. Pour les centres de données et les entreprises de plus grande envergure, plusieurs dispositifs Dominion KX II (associés à des dispositifs Dominion SX pour l'accès à distance à une console série, et Dominion KSX pour la gestion des bureaux distants et des filiales) peuvent être intégrés dans une solution logique unique à l'aide de la console de gestion CommandCenter Secure Gateway (CC-SG) de Raritan.

1
2
3
4
5
A
B
6
7
8
9

Légende			
1	Câble Cat5	7	Lecteur(s) USB de support virtuel à distance
2	Module d'interface pour ordinateur (CIM)	8	Barrette d'alimentation
3	Dominion KX II	9	Accès local *Remarque : KX2-832 et KX2-864 utilisent également un port local étendu.*
4	Dispositifs KVM et série distants	A	Réseau IP local/étendu
5	Modem	B	RTPC
6	Accès distant (réseau)		

Applications clients utilisables avec Dominion KX II

Les applications clientes suivantes peuvent être utilisées dans Dominion KX II :

Produit	Fonctionne avec...				
	MPC	RRC	VKC	RSC	AKC
KX II (deuxième génération)	✓		✓		
KX II 2.2 (ou supérieur)	✓		✓		✓

Reportez-vous au **manuel des clients KVM et série** pour en savoir plus sur les applications clientes. Reportez-vous également à la section ***Utilisation des serveurs cible*** (à la page 42) du présent manuel, qui contient des informations sur l'utilisation des clients avec Dominion KX II.

Remarque : MPC et VKC requièrent Java Runtime Environment (JRE). AKC est basé .NET.

Support virtuel

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

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

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

Les nouveaux modules d'interface pour ordinateur D2CIM-VUSB et D2CIM-DVUSB prennent en charge les sessions sur support virtuel pour les serveurs cible KVM disposant de l'interface USB 2.0. Ces CIM prennent également en charge Absolute Mouse Synchronization™ ainsi que la mise à jour du firmware à distance.

Le connecteur noir du CIM DVUSB est utilisé pour le clavier et la souris. Le connecteur gris est utilisé pour le support virtuel. Laissez les deux prises du CIM branchées sur le dispositif. Le dispositif risque de ne pas fonctionner correctement si les deux prises ne sont pas branchées sur le serveur cible.

Photos du produit

Dominion KX II

KX2-832

KX2-864

Caractéristiques du produit

Matériel

- Accès distant KVM sur IP intégré
- Montage en rack 1U ou 2U (supports de fixation fournis)
- Double alimentation avec fonction de basculement automatique, alimentation à commutation automatique avec avertissement de panne de courant
- 8, 16, 32 ou 64 (sur KX2-464) ports de serveur
- 32 (KX2-832) ou 64 (KX2-864) ports de serveur
- Jusqu'à huit canaux vidéo, suivant le modèle du dispositif, permettant à huit utilisateurs au plus de se connecter à Dominion KX II en même temps
- Fonction pour utilisateurs multiples (1/2/4/8 utilisateurs distants, 1 utilisateur local)
- Câblage de serveur UTP (Cat5/5e/6)
- Ports Ethernet doubles (10/100/1000 LAN) à protection par basculement
- Améliorable en clientèle
- Port utilisateur local pour accès en rack
  - Ports de souris/clavier PS/2. KX2-832 et KX2-864 sont USB uniquement.
  - Un port USB 2.0 sur le panneau avant et trois sur le panneau arrière pour les dispositifs USB pris en charge
  - Simultanéité complète avec l'accès utilisateur à distance
  - Interface graphique utilisateur (GUI) locale pour l'administration
- Un port local étendu offre une portée étendue pour un accès en rack aux dispositifs KX2.
- Sécurité de l'accès centralisé
- Gestion de l'alimentation intégrée
- Voyants indiquant le statut de la double alimentation, l'activité du réseau et le statut des utilisateurs distants
- Bouton de réinitialisation matérielle
- Port série pour la connexion à un modem externe.

Logiciel

- Support virtuel avec les CIM D2CIM-VUSB et D2CIM-DVUSB
- Synchronisation absolue de la souris avec les CIM D2CIM-VUSB et D2CIM-DVUSB
- Plug and Play
- Gestion et accès Web
- Interface utilisateur graphique intuitive
- Chiffrement 128 bits de l'ensemble du signal KVM, signal vidéo et support virtuel inclus
- LDAP, Active Directory, RADIUS ou authentification et autorisation internes
- Adressage DHCP ou IP fixe
- Authentification par carte à puce/CAC
- Gestion Syslog et SNMP
- Prise en charge d'IPv4 et d'IPv6
- Gestion de l'alimentation associée directement aux serveurs pour éviter les erreurs
- Intégration avec l'unité de gestion CommandCenter Secure Gateway (CC-SG) de Raritan
- Fonction CC Unmanage pour suspendre la gestion d'un dispositif par CC-SG.

Terminologie

Ce manuel utilise la terminologie ci-après pour désigner les composants d'une configuration Dominion KX II type :

Légende du schéma	
1	TCP/IP IPv4 et/ou IPv6
2	KVM (clavier/vidéo/souris)
3	Câble UTP (Cat5/5e/6)
A	Dominion KX II
B	Console d'accès local (Local Access Console) Utilisateur local - Console utilisateur facultative (constituée d'un clavier, d'une souris et d'un écran VGA Multisync) directement reliée à Dominion KX II pour gérer des serveurs cible KVM (directement au niveau du rack et non par l'intermédiaire du réseau). Un lecteur de cartes à puce USB peut également être branché au port local pour être monté sur un serveur cible. Un port local étendu est également fourni sur les modèles DKX2-832 et DKX2-864.
C	Ordinateur distant (Remote PC) Ordinateurs mis en réseau utilisés pour accéder aux serveurs cible connectés à Dominion KX II et les gérer. Un lecteur de cartes à puce USB peut également être branché au PC distant et relié à un serveur cible via Dominion KX II.
D	CIM Clés connectées sur chacun des serveurs cible ou chacune des barrettes d'alimentation. Disponibles pour tous les systèmes d'exploitation pris en charge.
E	Serveurs cible (Target Servers) Serveurs cibles KVM - Serveurs disposant de cartes vidéo et d'interfaces utilisateur (par exemple, Windows, Linux, Solaris, etc.) et accessibles à distance via Dominion KX II.
F	Barrettes d'alimentation Dominion PX Barrettes d'alimentation Raritan accessibles à distance via Dominion KX II.

Reportez-vous à ***CIM et systèmes d'exploitation pris en charge (serveurs cible)*** (voir "Systèmes d'exploitation et CIM pris en charge (serveurs cible)" à la page 281) pour obtenir la liste des systèmes d'exploitation et CIM pris en charge, et reportez-vous à ***Systèmes d'exploitation pris en charge (clients)*** (à la page 287) pour obtenir la liste des systèmes d'exploitation pris en charge par Dominion KX II à distance.

Contenu de l'emballage

Chaque Dominion KX II est un produit autonome entièrement configuré, dans un châssis de montage en rack 1U (2U pour DKX2-864) 19 pouces standard. Chaque dispositif Dominion KX II est livré avec les éléments suivants :

Quantité	Elément
1	Dispositif Dominion KX II
1	Manuel de configuration rapide Dominion KX II
1	Kit de montage en rack
1	Cordon d'alimentation secteur
1	Câble réseau Cat5
1	Câble réseau croisé Cat5
1	Ensemble de 4 pieds en caoutchouc (pour utilisation sur un bureau)
1	Note d'application
1	Carte de garantie

Chapitre 2 Installation et configuration

Dans ce chapitre

Présentation 13
Données de connexion par défaut 13
Mise en route.....14

Présentation

Cette section propose un bref aperçu du processus d'installation. Chaque étape est décrite en détails dans les autres sections de ce chapitre.

Pour installer et configurer Dominion KX II :

- ***Etape 1 : Configuration des serveurs cible KVM*** (à la page 14)
- ***Etape 2 : Configuration des paramètres du pare-feu de réseau*** (à la page 28)
- ***Etape 3 : Connexion de l'équipement*** (à la page 29)
- ***Etape 4 : Configuration de Dominion KX II*** (à la page 32)
- ***Etape 5 (facultative) : Configuration de la langue du clavier*** (à la page 40)

Vous trouverez également dans cette section les données de connexion par défaut dont vous aurez besoin. Particulièrement, l'adresse IP, le nom d'utilisateur et le mot de passe par défaut. Reportez-vous à ***Données de connexion par défaut*** (à la page 13).

Données de connexion par défaut

Valeur par défaut	Valeur
Nom d'utilisateur	Le nom d'utilisateur par défaut est admin. Cet utilisateur dispose de droits d'administrateur.
Mot de passe	Le mot de passe par défaut est raritan. Les mots de passe respectent la casse, doivent être saisis exactement de la même manière que lors de leur création. Par exemple, le mot de passe par défaut raritan doit être saisi uniquement en lettres minuscules. La première fois que vous démarrez Dominion KX II, il vous est demandé de changer le mot de passe par défaut.

Valeur par défaut	Valeur
IP address (Adresse IP)	Dominion KX II est fourni avec l'adresse IP par défaut 192.168.0.192.

Important : à des fins de sauvegarde et de continuité des opérations, il est fortement recommandé de créer un nom d'utilisateur et un mot de passe de secours pour l'administrateur, et de conserver ces données dans un endroit sûr.

Mise en route

Etape 1 : Configuration des serveurs cible KVM

Les serveurs cible KVM sont des ordinateurs qui seront accessibles et contrôlés via Dominion KX II. Avant d'installer Dominion KX II, configurez tous les serveurs cible KVM afin d'obtenir des performances optimales. Cette configuration s'applique aux serveurs cible KVM uniquement, non aux postes de travail clients (ordinateurs distants) utilisés pour accéder à distance à Dominion KX II. Reportez-vous à ***Terminologie*** (à la page 10) pour plus d'informations.

Papier peint du Bureau

Pour une utilisation de bande passante et une qualité vidéo optimales, les serveurs cible KVM qui exécutent des interfaces utilisateur graphiques telles que Windows, Linux, X-Windows, Solaris et KDE doivent être configurés. Il n'est pas nécessaire que le papier peint du Bureau soit complètement uni. Evitez cependant les papiers peints de Bureau ornés de photos ou de dégradés complexes qui peuvent nuire aux performances.

Paramètres de souris

Plusieurs modes souris sont disponibles pour l'unité Dominion KX II :

- Absolute Mouse Mode™ (mode souris absolue) (D2CIM-VUSB uniquement)
- Mode souris intelligente (n'utilisez pas de souris animée)
- Mode souris standard

Les paramètres de souris n'ont pas besoin d'être modifiés pour la synchronisation absolue de la souris mais le module D2CIM-VUSB ou D2CIM-DVUSB est requis pour ce mode. Quel que soit le mode souris suivant : standard ou intelligente, les paramètres de la souris doivent être configurés sur des valeurs spécifiques décrites plus loin dans ce manuel. Les configurations de souris varient sur différents systèmes d'exploitation cible. Reportez-vous à la documentation de votre système d'exploitation pour de plus amples informations.

Le mode Souris intelligente fonctionne généralement de façon satisfaisante sur la plupart des plates-formes Windows. Il peut cependant donner des résultats imprévisibles lorsque Active Desktop est activé sur le serveur cible. Pour plus d'informations sur les paramètres du mode Souris intelligente, reportez-vous à ***Mode Souris intelligente*** (à la page 78).

Les serveurs disposant de commutateurs KVM internes dans un châssis à lame ne prennent habituellement pas en charge la technologie de souris absolue.

Paramètres Windows XP, Windows 2003 et Windows 2008

▶ Pour configurer les serveurs cible KVM exécutant Microsoft Windows® XP®, Windows 2003® et Windows 2008® :

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Panneau de configuration > Souris.
   b. Cliquez sur l'onglet Options du pointeur.
   c. Dans la partie Mouvement du pointeur :

- Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
- Désactivez l'option Améliorer la précision du pointeur.
- Désactivez l'option Alignement.
- Cliquez sur OK.

Remarque : lorsque vous exécutez Windows 2003 sur votre serveur cible et que vous accédez au serveur via KVM et effectuez l'une des actions répertoriées ci-dessous, la synchronisation de la souris peut être perdue si elle était déjà activée. Il vous faudra sélectionner la commande Synchronize Mouse (Synchroniser la souris) dans le menu Mouse (Souris) du client pour la réactiver. Les actions ci-après peuvent provoquer ce problème :

- Ouvrir un éditeur de texte.

- Accéder aux propriétés de la souris, du clavier et options de modem et de téléphonie à partir du Panneau de configuration Windows.

---

2. Désactivez les effets de transition :
   a. Sélectionnez l'option Affichage du Panneau de configuration.
   b. Cliquez sur l'onglet Apparence.
   c. Cliquez sur le bouton Effets.
   d. Désélectionnez la case Utiliser l'effet de transition suivant pour les menus et les info-bulles.
   e. Cliquez sur OK.
3. Fermez le Panneau de configuration.

Remarque : pour les serveurs cible KVM exécutant Windows XP, Windows 2000 ou Windows 2008, vous pouvez créer un nom d'utilisateur qui servira uniquement pour les connexions à distance via Dominion KX II. Vous pourrez ainsi réserver aux connexions Dominion KX II les paramètres d'accélération/de mouvement lent du pointeur de la souris définis pour le serveur cible.

Les pages de connexion de Windows XP, 2000 et 2008 rétablissent les paramètres prédéfinis de la souris qui diffèrent de ceux suggérés pour des performances optimales de l'unité Dominion KX II. En conséquence, il est possible que la synchronisation de la souris ne soit pas optimale pour ces écrans.

AVERTISSEMENT ! Effectuez cette opération uniquement si vous êtes capable de manipuler le Registre des serveurs cible KVM Windows. Vous pouvez obtenir une meilleure synchronisation de la souris Dominion KX II aux pages de connexion en utilisant l'éditeur du Registre Windows pour modifier les paramètres suivants : HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Paramètres Windows 2000

Pour configurer les serveurs cible KVM exécutant Microsoft Windows® 2000® :

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Panneau de configuration > Souris.
   b. Cliquez sur l'onglet Motion (Mouvement).
      - Définissez l'accélération du pointeur sur Aucune.
      - Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
      - Cliquez sur OK.
2. Désactivez les effets de transition :
   a. Sélectionnez l'option Affichage du Panneau de configuration.
   b. Cliquez sur l'onglet Effets.
      - Désélectionnez la case Utiliser l'effet de transition suivant pour les menus et les info-bulles.
3. Cliquez sur OK et fermez le Panneau de configuration.

Remarque : pour les serveurs cible KVM exécutant Windows XP, Windows 2000 ou Windows 2008, vous pouvez créer un nom d'utilisateur qui servira uniquement pour les connexions à distance via Dominion KX II. Vous pourrez ainsi réserver aux connexions Dominion KX II les paramètres d'accélération/de mouvement lent du pointeur de la souris définis pour le serveur cible.

Les pages de connexion de Windows XP, 2000 et 2008 rétablissent les paramètres prédéfinis de la souris qui diffèrent de ceux suggérés pour des performances optimales de l'unité Dominion KX II. En conséquence, il est possible que la synchronisation de la souris ne soit pas optimale pour ces écrans.

AVERTISSEMENT ! Effectuez cette opération uniquement si vous êtes capable de manipuler le Registre des serveurs cible KVM Windows. Vous pouvez obtenir une meilleure synchronisation de la souris Dominion KX II aux pages de connexion en utilisant l'éditeur du Registre Windows pour modifier les paramètres suivants : HKey_USERS\.DEFAULT\Control Panel\Mouse: > MouseSpeed = 0;MouseThreshold 1=0;MouseThreshold 2=0.

Paramètres Windows Vista

Pour configurer les serveurs cible KVM exécutant Microsoft Windows Vista® :

1. Définissez les paramètres de la souris :
   a. Sélectionnez Démarrer > Paramètres > Panneau de configuration > Souris.
   b. Cliquez sur l'onglet Options du pointeur.
   c. Dans la partie Mouvement du pointeur :
      - Réglez la vitesse de déplacement du pointeur de la souris exactement au milieu.
      - Désactivez l'option Améliorer la précision du pointeur.
      - Cliquez sur OK.
2. Désactivez les effets de fondu et d'animation :
   a. Sélectionnez l'option Système à partir du Panneau de configuration.
   b. Sélectionnez Informations sur les performances et Outils > Outils avancés > Ajuster pour régler l'apparence et les performances de Windows.
   c. Cliquez sur l'onglet Avancé.
   d. Cliquez sur le bouton Paramètres du groupe Performances pour ouvrir la boîte de dialogue Options de performances.

e. Sous les options Personnalisation, désélectionnez les cases à cocher suivantes :

- Options d'animation :
  - Animer les commandes et les éléments à l'intérieur des fenêtres
  - Animer les fenêtres lors de la réduction et de l'agrandissement
- Options de fondu :
  - Fondre ou faire glisser les menus dans la zone de visualisation
  - Fondre ou faire glisser les info-bulles dans la zone de visualisation
  - Fermer en fondu les commandes de menu après le clic de souris

3. Cliquez sur OK et fermez le Panneau de configuration.

Paramètres Linux (Red Hat 9)

Remarque : les paramètres suivants sont optimisés uniquement pour le mode souris standard.

Pour configurer les serveurs cible KVM exécutant Linux® (interface utilisateur graphique) :

1. Définissez les paramètres de la souris :
   a. Choisissez Main Menu (Menu principal) > Preferences > Mouse (Souris). La boîte de dialogue des préférences de la souris s'affiche.
   b. Cliquez sur l'onglet Motion (Mouvement).
   c. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
   d. Dans la même section, définissez également une faible sensibilité.
   e. Dans la section du glisser-déposer, définissez un seuil faible.
   f. Fermez la boîte de dialogue des préférences de la souris.

   Remarque : si ces étapes ne fonctionnent pas, saisissez la commande xset mouse 1 1, comme décrit dans les instructions de ligne de commande Linux.

2. Définissez la résolution d'écran :
   a. Choisissez Main Menu (Menu principal) > System Settings (Paramètres système) > Display (Affichage). La boîte de dialogue des paramètres d'affichage apparaît.

b. Dans l'onglet Display (Affichage), sélectionnez une résolution prise en charge par Dominion KX II.

c. Dans l'onglet Advanced (Avancé), vérifiez que le taux de rafraîchissement est pris en charge par Dominion KX II.

Remarque : dans la plupart des environnement graphiques Linux, une fois que la connexion au serveur cible est établie, la commande <Ctrl> <Alt> <+> change la résolution vidéo en faisant défiler toutes les résolutions disponibles activées dans le fichier XF86Config ou /etc/X11/xorg.conf, suivant la distribution de votre serveur X.

Pour configurer les serveurs cible KVM exécutant Linux (ligne de commande) :

1. Définissez l'accélération du pointeur de la souris et le seuil exactement sur 1. Entrez la commande suivante : *xset mouse 1 1*. Ce paramètre doit est réglé pour être exécuté lorsque vous vous connectez.
2. Assurez-vous que tous les serveurs cible exécutant Linux utilisent une résolution VESA standard et un taux de rafraîchissement pris en charge par Dominion KX II.
3. Les serveurs cible Linux doivent également être configurés de manière à ce que les temps de passage en blanc correspondent aux valeurs VESA standard +/- 40 % :

   a. Localisez le fichier de configuration Xfree86 (XF86Config).

   b. Désactivez toutes les résolutions qui ne sont pas prises en charge par Dominion KX II à l'aide d'un éditeur de texte.

   c. Désactivez la fonctionnalité de bureau virtuel (non prise en charge par Dominion KX II).

   d. Vérifiez les temps de passage en blanc (valeurs VESA standard +/- 40 %).

   e. Redémarrez l'ordinateur.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Remarque concernant les serveurs cible KVM Red Hat 9

Si vous exécutez Red Hat 9 sur le serveur cible à l'aide d'un CIM USB, et que vous rencontrez des problèmes avec le clavier et/ou la souris, vous pouvez essayer un autre paramètre de configuration.

Conseil : ces étapes peuvent se révéler nécessaires même après une installation propre du SE.

Pour configurer les serveurs Red Hat 9 à l'aide de CIM USB :

1. Recherchez le fichier de configuration (généralement /etc/modules.conf) sur le système.
2. Ouvrez l'éditeur de votre choix et assurez-vous que la ligne alias usb-controller du fichier modules.conf est comme suit :

   alias usb-controller usb-uhci

   Remarque : si une autre ligne fait apparaître usb-uhci dans le fichier /etc/modules.conf, elle doit être supprimée ou mise en commentaire.
3. Enregistrez le fichier.
4. Redémarrez le système pour que les modifications soient appliquées.

Paramètres Linux (Red Hat 4)

Remarque : les paramètres suivants sont optimisés uniquement pour le mode souris standard.

Pour configurer les serveurs cible KVM exécutant Linux (interface utilisateur graphique) :

1. Définissez les paramètres de la souris :
   a. Choisissez Main Menu (Menu principal) > Preferences > Mouse (Souris). La boîte de dialogue des préférences de la souris s'affiche.
   b. Ouvrez l'onglet Motion (Mouvement).
   c. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
   d. Dans la même section, définissez également une faible sensibilité.
   e. Dans la section du glisser-déposer, définissez un seuil faible.
   f. Fermez la boîte de dialogue des préférences de la souris.

Remarque : si ces étapes ne fonctionnent pas, saisissez la commande xset mouse 1 1, comme décrit dans les instructions de ligne de commande Linux.

2. Définissez la résolution d'écran :
   a. Choisissez Main Menu (Menu principal) > System Settings (Paramètres système) > Display (Affichage). La boîte de dialogue des paramètres d'affichage apparaît.
   b. Dans l'onglet Settings (Paramètres), sélectionnez une résolution prise en charge par Dominion KX II.
   c. Cliquez sur OK.

Remarque : dans la plupart des environnement graphiques Linux, une fois que la connexion au serveur cible est établie, la commande <Ctrl> <Alt> <+> change la résolution vidéo en faisant défiler toutes les résolutions disponibles activées dans le fichier XF86Config ou /etc/X11/xorg.conf, suivant la distribution de votre serveur X.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Paramètres SUSE Linux 10.1

Remarque : n'essayez pas de synchroniser la souris à l'invite de connexion SUSE Linux®. Vous devez être connecté au serveur cible pour synchroniser les curseurs de souris.

Pour configurer les paramètres de la souris :

1. Choisissez Desktop (Bureau) > Control Center (Centre de contrôle). La boîte de dialogue des préférences du bureau s'affiche.
2. Cliquez sur Mouse (Souris). La boîte de dialogue des préférences de la souris s'affiche.
3. Ouvrez l'onglet Motion (Mouvement).
4. Dans la section permettant de définir la vitesse, définissez l'accélération du pointeur exactement au centre.
5. Dans la même section, définissez également une faible sensibilité.
6. Dans la section du glisser-déposer, définissez un seuil faible.
7. Cliquez sur Close (Fermer).

Pour configurer la vidéo :

1. Choisissez Desktop Preferences (Préférences du bureau) > Graphics Card and Monitor (Carte graphique et moniteur). La boîte de dialogue des propriétés de la carte et du moniteur s'affiche.

2. Vérifiez que la résolution et le taux de rafraîchissement utilisés sont pris en charge par Dominion KX II. Reportez-vous à ***Résolutions vidéo prises en charge*** (à la page 291) pour plus d'informations.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Rendre les paramètres Linux permanents

Remarque : ces étapes peuvent varier légèrement selon la version de Linux utilisée.

Pour rendre vos paramètres dans Linux permanents (invite) :

1. Choisissez System Menu (Menu système) > Preferences > Personal (Personnel) > Sessions.
2. Cliquez sur l'onglet Session Options (Options de session).
3. Activez l'option Prompt on log off (Invite à la déconnexion), puis cliquez sur OK. Cette option vous invite à enregistrer la session en cours lorsque vous vous déconnectez.
4. Au moment de la déconnexion, activez l'option Save current setup (Enregister la configuration actuelle) dans la boîte de dialogue.
5. Cliquez sur OK.

Conseil : pour empêcher que cette invite ne s'affiche lorsque vous vous déconnectez, exécutez la procédure suivante.

Pour rendre vos paramètres dans Linux permanents (sans invite) :

1. Choisissez Desktop (Bureau) > Control Center (Centre de contrôle) > System (Système) > Sessions.
2. Cliquez sur l'onglet Session Options (Options de session).
3. Désactivez la case à cocher Prompt on the log off (Invite à la déconnexion).
4. Activez l'option Automatically save changes to the session (Enregistrer automatiquement les modifications de la session), puis cliquez sur OK. Cette option enregistre automatiquement votre session actuelle au moment de la déconnexion.

Paramètres Sun Solaris

Pour configurer les serveurs cible KVM exécutant Sun® Solaris™ :

1. Définissez la valeur d'accélération du pointeur de la souris et le seuil exactement sur 1. Cela peut être effectué :

- à partir de l'interface utilisateur graphique ;

- à partir de la ligne de commande *xset mouse a t* où *a* représente l'accélération et *t*, le seuil.

2. Tous les serveurs cible KVM doivent être configurés en utilisant l'une des résolutions d'affichage prises en charge par Dominion KX II. Les résolutions les plus courantes sur les ordinateurs Sun sont :

Résolution d'affichage	Taux de rafraîchissement vertical	Rapport hauteur/largeur
1600 x 1200	60 Hz	4:3
1280 x 1024	60, 75, 85 Hz	5:4
1152 x 864	75 Hz	4:3
1024 x 768	60, 70, 75, 85 Hz	4:3
800 x 600	56, 60, 72, 75, 85 Hz	4:3
720 x 400	85 Hz	9:5
640 x 480	60, 72, 75, 85 Hz	4:3

3. Les serveurs cible KVM exécutant le système d'exploitation Solaris doivent utiliser une sortie vidéo VGA (signaux H-Sync et V-Sync, pas à synchronisation composite).

Pour passer d'une sortie de carte graphique Sun synchronisée de manière composite à une sortie VGA non standard :

1. Lancez la commande Stop+A pour afficher le mode bootprom.
2. Lancez la commande suivante pour modifier la résolution de sortie : *setenv output-device screen:r1024x768x70*
3. Lancez la commande `boot` pour redémarrer le serveur.

Vous pouvez également vous procurer un adaptateur de sortie vidéo auprès de votre revendeur Raritan.

Si vous avez	Utilisez cet adaptateur de sortie vidéo
Sun 13W3 avec une sortie synchronisée de manière composite	convertisseur APSSUN II Guardian.
Sun HD15 avec une sortie synchronisée de manière composite	convertisseur 1396C pour convertir de HD15 à 13W3 et un convertisseur APSSUN II Guardian pour prendre en charge la synchronisation composite.
Sun HD15 avec une sortie synchronisée de manière séparée	convertisseur APKMSUN Guardian.

Remarque : certains écrans d'arrière-plan Sun ne se centrent pas toujours précisément sur les serveurs Sun ayant des bordures sombres. Utilisez un autre arrière-plan ou une icône de couleur claire dans le coin supérieur gauche.

Paramètres de souris

Pour configurer les paramètres de la souris (Sun Solaris 10.1) :

1. Choisissez Launcher (Lancement). Application Manager - Desktop Controls (Gestionnaire d'applications - Contrôles de bureau) apparaît.
2. Sélectionnez Mouse Style Manager (Gestionnaire du style de souris). La boîte de dialogue Style Manager - Mouse (Gestionnaire de style - Souris) apparaît.
3. Définissez Acceleration sur 1.0.
4. Définissez Threshold (Seuil) sur 1.0.
5. Cliquez sur OK.

Accès à la ligne de commande

1. Cliquez avec le bouton droit de la souris.
2. Sélectionnez Tools (Outils) > Terminal. Une fenêtre de terminal s'ouvre. (Il est préférable de se trouver à la racine pour lancer des commandes.)

Paramètres vidéo (POST)

Les systèmes Sun ont deux paramètres de résolution différents : une résolution POST et une résolution GUI. Exécutez ces commandes depuis la ligne de commande.

Remarque : les valeurs 1024x768x75 sont utilisées ici à titre d'exemple. Remplacez ces paramètres par la résolution et le taux de rafraîchissement que vous utilisez.

Pour vérifier la résolution POST actuelle :

- Exécutez la commande suivante à la racine : `# eeprom output-device`

Pour modifier la résolution POST :

1. Exécutez `# eeprom output-device=screen:r1024x768x75`.
2. Déconnectez-vous ou redémarrez l'ordinateur.

Paramètres vidéo (GUI)

La résolution GUI peut être vérifiée et définie à l'aide de différentes commandes selon la carte vidéo utilisée. Exécutez ces commandes depuis la ligne de commande.

Remarque : les valeurs 1024x768x75 sont utilisées ici à titre d'exemple. Remplacez ces paramètres par la résolution et le taux de rafraîchissement que vous utilisez.

Carte	Pour vérifier la résolution :	Pour modifier la résolution :
32 bits	# /usr/sbin/pgxconfig -prconf	1. # /usr/sbin/pgxconfig -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.
64 bits	# /usr/sbin/m64config -prconf	1. # /usr/sbin/m64config -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.
32 bits et 64 bits	# /usr/sbin/fbconfig -prconf	1. # /usr/sbin/fbconfig -res 1024x768x75 2. Déconnectez-vous ou redémarrez l'ordinateur.

Paramètres IBM AIX 5.3

Suivez la procédure ci-après pour configurer les serveurs cible KVM exécutant IBM AIX® 5.3.

Pour configurer la souris :

1. Démarrez le lanceur.
2. Sélectionnez Style Manager (Gestionnaire de style).
3. Cliquez sur Mouse (Souris). La boîte de dialogue Style Manager - Mouse (Gestionnaire de style - Souris) apparaît.
4. Définissez Mouse acceleration (Accélération de la souris) sur 1.0 et Threshold (Seuil) sur 1.0.
5. Cliquez sur OK.

Pour configurer la vidéo :

1. Depuis le lanceur, sélectionnez Application Manager (Gestionnaire d'applications).
2. Sélectionnez System_Admin.
3. Sélectionnez Smit > Devices > Graphic Displays > Select the Display Resolution and Refresh Rate (Smit > Dispositifs > Affichages graphiques > Sélectionner la résolution d'affichage et le taux de rafraîchissement).
4. Sélectionnez la carte vidéo utilisée.
5. Cliquez sur List. Une liste de modes d'affichage apparaît.
6. Sélectionnez une résolution et un taux de rafraîchissement pris en charge par Dominion KX II. Reportez-vous à ***Résolutions vidéo prises en charge*** (à la page 291) pour plus d'informations.

Remarque : si vous modifiez la résolution vidéo, vous devez vous déconnecter du serveur cible, puis vous reconnecter pour appliquer les nouveaux paramètres vidéo.

Rendre les paramètres UNIX permanents

Remarque : ces étapes peuvent varier légèrement selon le type d'UNIX® (par exemple, Solaris, IBM AIX) et la version utilisée.

1. Sélectionnez Style Manager (Gestionnaire de style) > Startup (Démarrage). La boîte de dialogue Style Manager - Startup(Gestionnaire de style - Démarrage) apparaît.
2. Dans la fenêtre Logout Confirmation (Confirmation de connexion), sélectionnez l'option On (Activé). Cette option vous invite à enregistrer la session en cours lorsque vous vous déconnectez.

Paramètres Apple Macintosh

Sur les serveurs cible KVM exécutant le système d'exploitation Apple Macintosh®, la meilleure solution est d'utiliser la technologie D2CIM-VUSB et la synchronisation absolue de la souris.

Remarque : L'option USB Profile Mac OS-X, version 10.4.9 and later (Profil USB Mac OS X, versions 10.4.9 et supérieure) doit être sélectionnée dans le menu USB Profile (Profil USB) ou sur la page Port Configuration (Configuration des ports).

Etape 2 : Configuration des paramètres du pare-feu de réseau

Pour accéder à Dominion KX II à travers un pare-feu de réseau par l'intermédiaire de Multi-Platform Client ou de la page Port Access (Accès aux ports), le pare-feu doit autoriser la communication sur TCP Port 5000 ou sur un autre port de votre choix.

Pour tirer parti de Dominion KX II :	le pare-feu doit permettre la communication en amont sur :
Fonctionnalités d'accès Web	Port 443 : port TCP standard pour la communication HTTPS
Redirection automatique des requêtes HTTP vers HTTPS (l'adresse plus courante http://xxx.xxx.xxx.xxx peut être utilisée à la place de https://xxx.xxx.xxx.xxx.)	Port 80 : port TCP standard pour la communication HTTP

Reportez-vous à ***Paramètres réseau*** (voir "Network Settings (Paramètres réseau)" à la page 142) pour plus d'informations sur la désignation d'un autre port de détection.

Etape 3 : Connexion de l'équipement

Branchez Dominion KX II sur l'alimentation, le réseau, le PC local et les serveurs cible. Les lettres du schéma correspondent aux rubriques de description de la connexion dans cette section.

A. Alimentation CA

Pour connecter l'alimentation :

1. Raccordez le cordon d'alimentation CA fourni avec Dominion KX II et branchez-le sur une prise électrique.
2. Pour une alimentation à double protection par basculement, raccordez le second cordon d'alimentation fourni et branchez-le à une source d'alimentation différente de celle auquel le premier cordon est raccordé.

Remarque : si vous ne connectez qu'un cordon, le voyant d'alimentation sur le panneau avant de Dominion KX II est rouge car le système n'est pas configuré pour détecter les deux sources automatiquement. Reportez-vous à **Configuration de l'alimentation** *(à la page 162) pour obtenir des informations sur la désactivation de la fonction de détection automatique de la source d'alimentation non utilisée.*

B. Port du modem (facultatif)

Dominion KX II dispose d'un port modem dédié qui permet l'accès à distance même lorsque le réseau local/réseau étendu n'est pas disponible. Utilisez un câble série à brochage direct (RS-232) pour relier un modem série externe au port libellé MODEM à l'arrière de l'unité Dominion KX II (reportez-vous à ***Spécifications*** (à la page 276) pour obtenir la liste des modems agréés et ***Paramètres de modem*** (à la page 151) pour plus d'informations sur la configuration du modem).

Remarque : Raritan recommande de configurer le modem en activant le paramètre CD (Carrier Detect).

C. Port réseau

Dominion KX II dispose de deux ports Ethernet pour les basculements (et non pour l'équilibrage des charges). Par défaut, seul LAN1 est actif et le basculement automatique est désactivé. S'il est activé et que l'interface réseau interne de l'unité Dominion KX II ou le commutateur réseau auquel elle est connectée n'est plus disponible, LAN2 est activé avec la même adresse IP.

Remarque : les ports de basculement n'étant pas activés avant un basculement effectif, Raritan recommande de ne pas surveiller ces ports ou de le faire après un basculement.

Pour connecter le réseau :

1. Reliez un câble Ethernet standard (fourni) du port réseau LAN1 à un commutateur, concentrateur ou routeur Ethernet.
2. Pour utiliser les capacités de basculement Ethernet facultatives de Dominion KX II :
   - Reliez un câble Ethernet standard du port réseau libellé LAN2 à un commutateur, concentrateur ou routeur Ethernet.
   - Activez Automatic Failover (Basculement automatique) sur l'écran Network Configuration (Configuration réseau).

Remarque : n'utilisez les deux ports réseau que si l'un doit servir de port de basculement.

D. Port pour accès local (PC local)

Pour accéder facilement aux serveurs cible sur le rack, utilisez le port d'accès local de Dominion KX II. Si le port d'accès local est obligatoire pour l'installation et le paramétrage, il est facultatif par la suite. Le port d'accès local fournit également une interface utilisateur graphique depuis la console locale de Dominion KX II pour l'administration et l'accès au serveur cible.

KX2-832 KX2-864 fournissent également un port Extended Local, libellé EXT LOCAL à l'arrière du dispositif, pour accéder aux serveurs cible sur le rack. Ce port n'est pas requis pour l'installation et le paramétrage initiaux. Il est configuré depuis les consoles locale et distante. Reportez-vous à ***Configuration des paramètres du port local Dominion KX II*** (voir "Configuration des paramètres du port local de Dominion KX II" à la page 200) pour plus d'informations.

Pour connecter le port local :

- Reliez un écran MultiSync VGA, une souris et un clavier aux ports libellés Local User (Utilisateur local) respectifs. Utilisez un clavier et une souris PS/2 ou USB (DKX2-832 et DKX2-864 offrent l'USB uniquement). Les connexions physiques des ports Local User (Utilisateur local) et Extended Local (Local étendu) se trouvent sur le panneau arrière de Dominion KX II.

Connexion	Description
Ecran	Branchez un écran VGA Multisync standard sur le port vidéo HD15 (femelle).
Clavier	Branchez un clavier PS/2 standard sur un port clavier Mini-DIN6 (femelle) ou un clavier USB standard sur un des ports USB de type A (femelle).
Souris	Branchez une souris PS/2 standard sur un port souris Mini-DIN6 (femelle) ou une souris USB standard sur un des ports USB de type A (femelle).

E. Ports de serveur cible

Dominion KX II utilise un câblage UTP standard (Cat5/5e/6) pour sa connexion à chaque serveur cible.

Pour connecter un serveur cible à Dominion KX II :

1. Utilisez le module CIM (Computer Interface Module) approprié. Reportez-vous à ***CIM et systèmes d'exploitation pris en charge (serveurs cible)*** (voir "Systèmes d'exploitation et CIM pris en charge (serveurs cible)" à la page 281) pour plus d'informations sur les CIM à utiliser avec chaque système d'exploitation.
2. Raccordez le connecteur vidéo HD15 de votre CIM au port vidéo du serveur cible. Vérifiez que la vidéo du serveur cible est déjà configurée sur une résolution et un taux de rafraîchissement pris en charge. Pour les serveurs Sun, assurez-vous également que la carte vidéo du serveur cible est paramétrée sur une sortie VGA standard (Sync H-et-V) et non Sync Composite.
3. Reliez le connecteur clavier/souris de votre CIM aux ports correspondants du serveur cible. A l'aide d'un câble UTP à brochage direct standard (Cat5/5e/6), raccordez le CIM à un port serveur disponible à l'arrière du dispositif Dominion KX II.

Remarque : DCIM-USB G2 présente un petit commutateur à l'arrière du CIM. Placez ce commutateur sur P pour les serveurs cible USB PC. Placez ce commutateur sur S pour les serveurs cible USB Sun.

Une nouvelle position de commutateur ne prend effet qu'après l'alimentation cyclique du CIM. Pour effectuer l'alimentation cyclique du CIM, retirez le connecteur USB du serveur cible, puis rebranchez-le quelques secondes plus tard.

Etape 4 : Configuration de Dominion KX II

A la première mise sous tension du dispositif Dominion KX II, vous devez effectuer des opérations de configuration initiale via la console locale de Dominion KX II :

- Modifier le mot de passe par défaut
- Affecter l'adresse IP
- Désigner les serveurs cible KVM.

Modification du mot de passe par défaut

Dominion KX II est livré avec un mot de passe par défaut. La première fois que vous démarrez l'unité, il vous est demandé de changer ce mot de passe.

Pour changer le mot de passe par défaut :

1. Mettez Dominion KX II sous tension à l'aide des commutateurs d'alimentation situés à l'arrière. Patientez pendant le démarrage de l'unité Dominion KX II. (Un signal sonore indique la fin du démarrage.)
2. Une fois l'unité démarrée, la console locale de Dominion KX II est visible sur le moniteur relié au port local de Dominion KX II. Entrez les nom d'utilisateur (admin) et mot de passe (raritan) par défaut, puis cliquez sur Login (Connexion). L'écran Change Password (Modifier le mot de passe) s'affiche.
3. Tapez votre ancien mot de passe (raritan) dans le champ Old Password (Ancien mot de passe).
4. Tapez un nouveau mot de passe dans le champ New Password ; retapez-le dans le champ Confirm New Password (Confirmer le nouveau mot de passe). Les mots de passe peuvent contenir un maximum de 64 caractères alphanumériques et spéciaux.
5. Cliquez sur Apply (Appliquer).
6. Vous recevrez confirmation que le mot de passe a bien été changé. Cliquez sur OK. La page Port Access (Accès aux ports) apparaît.

Remarque : le mot de passe par défaut peut également être modifié à partir de Multi-Platform Client (MPC) de Raritan.

Affectation d'une adresse IP

Ces procédures décrivent comment affecter une adresse IP sur la page Network Settings (Paramètres réseau). Pour obtenir des informations complètes sur tous les champs ainsi que sur le fonctionnement de cette page, reportez-vous à ***Paramètres réseau*** (voir "Network Settings (Paramètres réseau)" à la page 142).

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Indiquez un nom de dispositif significatif pour votre unité Dominion KX II. 32 caractères alphanumériques au plus, avec des caractères spéciaux valides et aucun espace.
3. Dans la section IPv4, entrez ou sélectionnez les paramètres réseau spécifiques à IPv4 appropriés :
   a. Le cas échéant, entrez l'adresse IP. L'adresse IP par défaut est 192.168.0.192.

b. Renseignez le champ Subnet Mask (Masque de sous-réseau). Le masque de sous-réseau par défaut est 255.255.255.0.

c. Renseignez le champ Default Gateway (Passerelle par défaut) si l'option None (Néant) est sélectionnée dans la liste déroulante IP Auto Configuration (Configuration automatique IP).

d. Renseignez le champ Preferred DHCP Host Name (Nom de l'hôte DHCP privilégié) si l'option DHCP est sélectionnée dans la liste déroulante IP Auto Configuration (Configuration automatique IP).

e. Sélectionnez une option dans le champ IP Auto Configuration (Configuration automatique IP). Les options suivantes sont disponibles :

- None (Static IP) (Néant (IP statique)) - Cette option requiert une saisie manuelle des paramètres réseau.

  Il s'agit de l'option recommandée car Dominion KX II est un dispositif d'infrastructure et son adresse IP ne devrait pas changer.

- DHCP - Le protocole de configuration d'hôte dynamique est utilisé par les ordinateurs mis en réseau (clients) pour obtenir des adresses IP uniques et d'autres paramètres du serveur DHCP.

  Avec cette option, les paramètres réseau sont affectés par le serveur DHCP. Si DHCP est utilisé, entrez le nom d'hôte privilégié (DHCP uniquement). 63 caractères au plus.

4. Si IPv6 doit être utilisé, entrez ou sélectionnez les paramètres réseau spécifiques à IPv6 appropriés dans la section IPv6 :

   a. Cochez la case IPv6 pour activer les champs de la section.

   b. Renseignez le champ Global/Unique IP Address (Adresse IP globale/unique). Il s'agit de l'adresse IP affectée à Dominion KX II.

   c. Renseignez le champ Prefix Length (Longueur de préfixe). Il s'agit du nombre de bits utilisés dans l'adresse IPv6.

   d. Renseignez le champ Gateway IP Address (Adresse IP de la passerelle).

   e. Link-Local IP Address (Adresse IP Lien-local). Cette adresse est attribuée automatiquement au dispositif. Elle est utilisée pour la détection de voisins ou en l'absence de routeurs. **Read-Only (Lecture seule)**

   f. Zone ID. Ce champ identifie le dispositif auquel l'adresse est associée. **Read-Only (Lecture seule)**

   g. Sélectionnez une option dans le champ IP Auto Configuration (Configuration automatique IP). Les options suivantes sont disponibles :

- None (Néant) - Utilisez cette option si vous ne souhaitez pas de configuration IP automatique et préférez définir l'adresse IP vous-même (IP statique). Cette option par défaut est recommandée.

  Lorsqu'elle est sélectionnée pour la configuration IP automatique, les champs Network Basic Settings (Paramètres réseau de base) sont activés : Global/Unique IP Address (Adresse IP globale/unique), Prefix Length (Longueur de préfixe) et Gateway IP Address (Adresse IP de la passerelle). Vous pouvez paramétrer manuellement la configuration IP.

- Router Discovery (Détection de routeur) - Utilisez cette option pour affecter automatiquement des adresses IPv6 ayant une portée « Global » ou « Unique Local » au-delà des adresses « Link Local » qui ne s'appliquent qu'à un sous-réseau connecté directement.

5. Si l'option DHCP est activée et que le champ Obtain DNS Server Address Automatically (Obtenir l'adresse du serveur DNS automatiquement) est accessible, sélectionnez-le. Les données DNS fournies par le serveur DHCP seront alors utilisées.
6. Si l'option Use the Following DNS Server Addresses (Utiliser les adresses de serveurs DNS suivantes) est activée, que DHCP soit sélectionné ou non, les adresses saisies dans cette section seront utilisées pour la connexion au serveur DNS.

   Entrez les données suivantes si l'option Following DNS Server Addresses (Utiliser les adresses de serveurs DNS suivantes) est activée. Il s'agit des adresses DNS primaire et secondaire qui seront utilisées si la connexion au serveur DNS primaire est perdue lors d'une panne.

   a. Adresse IP du serveur DNS primaire
   b. Adresse IP du serveur DNS secondaire.
7. Lorsque vous avez terminé, cliquez sur OK. Le dispositif Dominion KX II est maintenant accessible depuis le réseau.

Reportez-vous à ***Paramètres de l'interface LAN*** (à la page 146) pour plus d'informations sur la configuration de cette section de la page Network Settings (Paramètres réseau).

Remarque : dans certains environnements, le paramètre par défaut du champ LAN Interface Speed & Duplex (Vitesse d'interface LAN & Duplex), Autodetect (auto-détection), ne définit pas correctement les paramètres réseau, ce qui entraîne des problèmes sur le réseau. Dans ce cas, paramétrez le champ LAN Interface Speed & Duplex (Vitesse & Duplex de l'interface LAN) de Dominion KX II sur 100 Mbps/Full Duplex (Bidirectionnel simultané) (ou toute option appropriée à votre réseau) pour résoudre le problème. Reportez-vous à la page **Paramètres réseau** *(voir "Network Settings (Paramètres réseau)" à la page 142) pour plus d'informations.*

Désignation des serveurs cible

Pour nommer les serveurs cible :

1. Connectez tous les serveurs cible si vous ne l'avez pas encore fait. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 29) pour obtenir une description de la connexion de l'équipement.
2. Depuis la console locale de l'unité Dominion KX II, sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports). La page Port Configuration s'ouvre.
3. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
4. Attribuez un nom au serveur connecté à ce port. Ce nom peut contenir jusqu'à 32 caractères alphanumériques et spéciaux.
5. Cliquez sur OK.

Caractères spéciaux valides pour les noms de cibles

Caractère	Description	Caractère	Description
!	Point d'exclamation	;	Point-virgule
"	Guillemet	=	Signe égal
#	Dièse	>	Signe supérieur à
$	Symbole du dollar	?	Point d'interrogation
%	Symbole du pourcentage	@	Arobas
&	« Et » commercial	[	Crochet ouvrant
(	Parenthèse ouvrante	\	Trait oblique inversé
)	Parenthèse fermante	]	Crochet fermant
*	Astérisque	^	Accent circonflexe
+	Signe plus	_	Trait de soulignement
,	Virgule	`	Accent grave
-	Tiret	{	Accolade gauche
.	Point	|	Barre
/	Trait oblique	}	Accolade droite

Caractère	Description	Caractère	Description
<	Signe inférieur à	~	Tilde
:	Deux-points		

Spécification de la détection automatique de l'alimentation

Dominion KX II offre une double alimentation. Par ailleurs, elle peut détecter et notifier automatiquement l'état de ces alimentations. Une configuration appropriée garantit l'envoi de notifications adéquates par Dominion KX II en cas de panne de courant.

La page Power Supply Setup (Configuration de l'alimentation) est configurée de manière à détecter automatiquement les deux sources d'alimentation lorsque deux sources sont utilisées. Si une seule source d'alimentation est utilisée dans votre configuration, vous pouvez désactiver la détection automatique sur la page de configuration de l'alimentation.

Pour activer la détection automatique des alimentations utilisées :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Power Supply Setup (Configuration de l'alimentation). La page Power Supply Setup s'ouvre.
2. Si vous branchez une arrivée électrique dans l'alimentation numéro un (alimentation la plus à gauche à l'arrière du dispositif), cochez la case Powerln1 Auto Detect (Détection automatique Powerln1).
3. Si vous branchez une arrivée électrique dans l'alimentation numéro deux (alimentation la plus à droite à l'arrière du dispositif), cochez la case Powerln2 Auto Detect (Détection automatique Powerln2).
4. Cliquez sur OK.

Remarque : si l'une de ces cases est cochée et que l'arrivée électrique n'est pas branchée, le voyant d'alimentation sur la partie avant de l'unité s'affiche en rouge.

Pour désactiver la détection automatique d'alimentation non utilisée :

1. Depuis la console locale de Dominion KX II, sélectionnez Device Settings (Paramètres du dispositif) > Power Supply Setup (Configuration de l'alimentation). La page Power Supply Setup s'ouvre.
2. Désactivez la détection automatique de l'alimentation que vous n'utilisez pas.

Pour plus d'informations, reportez-vous à ***Configuration de l'alimentation*** (à la page 162).

Remarque aux utilisateurs de CC-SG

Si vous utilisez Dominion KX II dans une configuration CC-SG, suivez la procédure d'installation. Celle-ci terminée, consultez le **manuel d'utilisation**, **manuel de l'administrateur** ou **guide de déploiement** de CommandCenter Secure Gateway pour poursuivre (tous se trouvent sur le site Web de Raritan, www.raritan.com, sous Support).

Remarque : la suite de cette aide s'applique essentiellement au déploiement des dispositifs Dominion KX II sans utiliser les fonctions d'intégration de CC-SG.

Authentification à distance

Remarque aux utilisateurs de CC-SG

Lorsque Dominion KX II est géré par CommandCenter Secure Gateway, CC-SG authentifie les utilisateurs et les groupes, à l'exception des utilisateurs locaux requérant l'accès au port local. Lorsque CC-SG assure la gestion de Dominion KX II, les utilisateurs du port local sont authentifiés par rapport à la base de données des utilisateurs locaux ou au serveur d'authentification à distance (LDAP/LDAPS ou RADIUS) configurés sur Dominion KX II. Ils ne sont pas authentifiés par rapport à la base de données des utilisateurs de CC-SG.

Pour plus d'informations sur l'authentification de CC-SG, consultez le manuel d'utilisation, le manuel de l'administrateur ou le guide de déploiement de CommandCenter Secure Gateway, disponibles par téléchargement dans la section Support du ***site Web de Raritan*** http://www.raritan.com.

Protocoles pris en charge

Afin de simplifier la gestion des noms d'utilisateur et des mots de passe, Dominion KX II offre la possibilité de transférer les requêtes d'authentification vers un serveur d'authentification externe. Deux protocoles d'authentification externes sont pris en charge : LDAP/LDAPS et RADIUS.

Remarque relative à Microsoft Active Directory

Microsoft Active Directory utilise le protocole LDAP/LDAPS de manière native et peut servir de source d'authentification et serveur LDAP/LDAPS avec Dominion KX II. Si le serveur Microsoft Active Directory dispose d'un composant IAS (serveur d'autorisation Internet), il peut également être utilisé comme source d'authentification RADIUS.

Création de groupes d'utilisateurs et d'utilisateurs

Pendant la configuration initiale, vous devez définir des groupes d'utilisateurs et des utilisateurs pour permettre à ceux-ci d'accéder à Dominion KX II.

Dominion KX II utilise des groupes par défaut fournis par le système, mais vous pouvez aussi créer des groupes et spécifier les autorisations adéquates pour répondre à vos besoins.

Un nom d'utilisateur et un mot de passe sont nécessaires pour accéder à Dominion KX II. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre unité Dominion KX II.

Reportez-vous à Gestion des utilisateurs pour plus d'informations sur l'ajout et la modification des groupes d'utilisateurs et des utilisateurs.

Etape 5 (facultative) : Configuration de la langue du clavier

Remarque : cette étape n'est pas obligatoire si vous utilisez un clavier américain/international.

Si vous utilisez une langue autre que l'anglais américain, le clavier doit être configuré pour celle-ci. De plus, la langue du clavier de l'ordinateur client et des serveurs cible KVM doit être la même.

Consultez la documentation de votre système d'exploitation pour plus d'informations sur la modification de la disposition du clavier.

Modification du code de disposition de clavier (cibles Sun)

Suivez cette procédure si vous disposez d'un DCIM-SUSB et souhaitez utiliser une disposition de clavier dans une autre langue.

Pour modifier le code de disposition du clavier (DCIM-SUSB uniquement) :

1. Ouvrez une fenêtre de l'éditeur de texte sur le poste de travail Sun.
2. Assurez-vous que la touche Verr num est active, et appuyez sur la touche Ctrl située à gauche et sur la touche Suppr du clavier. Le voyant du verrouillage des majuscules clignote pour indiquer que le CIM est en mode de modification du code de disposition. La fenêtre de texte affiche les informations suivantes : `Raritan Computer, Inc. Current keyboard layout code = 22h (US5 UNIX)`.
3. Saisissez le code de disposition souhaité (par exemple, *31* pour le clavier japonais).
4. Appuyez sur Entrée.
5. Mettez le dispositif hors tension, puis à nouveau sous tension. Le DCIM-SUSB procède à une réinitialisation (alimentation cyclique).

6. Vérifiez que les caractères sont corrects.

Chapitre 3 Utilisation des serveurs cible

Dans ce chapitre

Interfaces 42
Virtual KVM Client 57
Active KVM Client (AKC) 89

Interfaces

Dominion KX II dispose de plusieurs interfaces utilisateur qui fournissent un accès aisé à tout moment, où que vous soyez. Ces interfaces incluent la console locale de Dominion KX II, la console distante de Dominion KX II et Multi-Platform Client (MPC). Le tableau ci-après décrit les interfaces et leur utilisation pour l'accès aux serveurs cible et la gestion de ces derniers localement et à distance :

Interface utilisateur	Accès local	Admin	Accès distant	Admin
Console locale de Dominion KX II	✓	✓		
Console distante de Dominion KX II			✓	✓
Virtual KVM Client			✓	
Multi-Platform Client (MPC)			✓	✓
Active KVM Client (AKC)			✓	✓

Les sections suivantes de l'aide contiennent des informations sur l'utilisation d'interfaces particulières pour accéder à Dominion KX II et gérer les cibles :

- Console locale
- Console distante
- Virtual KVM Client
- Multi-Platform Client

Interface de la console locale de Dominion KX II

Lorsque vous êtes situé au niveau du rack du serveur, Dominion KX II permet une gestion KVM standard via la console locale de Dominion KX II. La console locale de Dominion KX II offre une connexion (analogique) KVM directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur.

Les interfaces graphiques utilisateur de la console locale de Dominion KX II et de la console distante de Dominion KX II présentent de nombreuses ressemblances. Les éventuelles différences sont indiquées dans l'aide.

L'option Factory Reset (Rétablir les valeurs usine) est disponible sur la console locale de Dominion KX II et non sur la console distante de Dominion KX II.

Interface de la console distante de Dominion KX II

La console distante de Dominion KX II est une interface graphique utilisateur navigateur qui vous permet de vous connecter aux serveurs cible KVM et aux cibles série connectés à Dominion KX II, et de gérer Dominion KX II à distance.

Elle offre une connexion numérique à vos serveurs cible KVM connectés. Lorsque vous accédez à un serveur cible KVM à l'aide de la console distante de Dominion KX II, une fenêtre Virtual KVM Client s'ouvre.

Il existe de nombreuses ressemblances entre les interfaces utilisateur graphiques de la console locale de Dominion KX II et de la console distante de Dominion KX II. Les éventuelles différences sont indiquées dans le manuel d'utilisation. Les options suivantes sont disponibles sur la console distante de Dominion KX II mais non sur la console locale de Dominion KX II :

- Support virtuel
- Favorites (Favoris)
- Backup/Restore (Sauvegarde/Restauration)
- Firmware Upgrade (Mise à niveau du firmware)
- Upgrade Report (Rapport de mise à niveau)
- Diagnostics
- USB Profile Selection (Sélection de profils USB)
- USB Profile Management (Gestion des profils USB)
- Certificats SSL

Lancement de la console distante de Dominion KX II

Important : quel que soit le navigateur utilisé, vous devez autoriser les fenêtres contextuelles provenant de l'adresse IP du dispositif Dominion pour lancer la console distante de Dominion KX II.

Selon le navigateur utilisé et les paramètres de sécurité, il est possible que plusieurs avertissements relatifs aux certificats et à la sécurité s'affichent. Il vous faudra accepter ces avertissements pour lancer la console distante de Dominion KX II.

Vous pouvez réduire le nombre de messages d'avertissement lors des connexions suivantes en cochant les options suivantes dans les messages d'avertissement relatifs aux certificats et à la sécurité :

- In the future, do not show this warning (A l'avenir, ne plus afficher ce message d'avertissement)
- Always trust content from this publisher (Toujours faire confiance au contenu provenant de cet éditeur)

Pour démarrer la console distante de Dominion KX II :

1. Connectez-vous à un poste de travail doté d'une connectivité réseau à votre unité Dominion KX II et de Java Runtime Environment (JRE est disponible sur le ***site Web de Java*** http://java.sun.com/).
2. Démarrez un navigateur Web pris en charge, tel qu'Internet Explorer (IE) ou Firefox.
3. Saisissez l'URL suivante : *http://ADRESSE-IP*, où ADRESSE-IP correspond à l'adresse IP que vous avez affectée au dispositif Dominion KX II. Vous pouvez aussi utiliser https, le nom DNS de Dominion KX II attribué par l'administrateur (à condition qu'un serveur DNS ait été configuré), ou simplement saisir l'adresse IP dans le navigateur (Dominion KX II redirige toujours l'adresse IP de HTTP vers HTTPS). La page de connexion s'ouvre.

4. Tapez votre nom d'utilisateur et votre mot de passe. S'il s'agit de la première connexion, utilisez le nom d'utilisateur (admin) et le mot de passe (raritan, en minuscules) par défaut usine. Il vous est alors demandé de modifier le mot de passe par défaut. Reportez-vous à ***Modification du mot de passe par défaut*** (à la page 33) pour plus d'informations.
5. Cliquez sur Login (Se connecter).
6. Reportez-vous à ***Virtual KVM Client*** (à la page 57) pour plus d'informations sur les fonctions Dominion KX II disponibles via la console distante.

Disposition de la console Dominion KX II

Les interfaces de la console distante de Dominion KX II et celle de la console locale de Dominion KX II présentent toutes les deux une interface HTML (Web) pour la configuration et l'administration, ainsi qu'une liste et des fonctions de sélection des serveurs cible. Les options sont organisées dans différents onglets.

Une fois la connexion réussie, la page d'accès aux ports s'affiche avec la liste de tous les ports ainsi que leur état et leur disponibilité. Deux onglets sont présents et permettent un affichage par port ou par groupe. Vous pouvez effectuer un tri par numéro de port, nom de port, état (activé ou non) et disponibilité (inactif, connecté, occupé, indisponible ou en cours de connexion) en cliquant sur un en-tête de colonne. Reportez-vous à ***Page d'accès aux ports*** (voir "Page Port Access" à la page 46) pour plus d'informations.

Navigation dans la console Dominion KX II

Les interfaces de la console Dominion KX II offrent plusieurs méthodes de navigation et de sélection.

Pour sélectionner une option (utilisez n'importe laquelle des méthodes suivantes) :

- Cliquez sur un onglet. Une page d'options disponibles apparaît.
- Placez le curseur sur un onglet puis sélectionnez l'option souhaitée dans le menu.
- Cliquez sur l'option directement dans la hiérarchie de menu affichée (fils d'Ariane).

Pour faire défiler les pages plus longues que l'écran :

- Utilisez les touches PageSup et PageInf sur votre clavier ;
- utilisez la barre de défilement à droite de l'écran.

Page Port Access

Une fois connecté à la console distante de Dominion KX II, la page Port Access (Accès aux ports) s'ouvre. Elle répertorie tous les ports de Dominion KX II, les serveurs cible KVM connectés ainsi que leur état et leur disponibilité. Elle indique le chemin permettant d'accéder aux serveurs cible KVM connectés à Dominion KX II. Ces serveurs cible KVM sont des serveurs que vous souhaitez gérer via le dispositif Dominion KX II. Ils sont connectés aux ports de Dominion KX II placés à l'arrière du dispositif.

Remarque : une nouvelle page de Virtual KVM Client s'ouvre pour chaque connexion à un serveur cible KVM.

La page Port Acces (Accès aux ports) présente également les châssis de lames configurés dans Dominion KX II. Le châssis de lames s'affiche dans une liste hiérarchique extensible sur la page Port Access ; le châssis de lames est placé à la racine de la hiérarchie et chaque lame est libellée et affichée sous la racine.

Remarque : pour afficher le châssis de lames dans l'ordre hiérarchique, ses sous-types doivent être configurés.

Par défaut, l'onglet View by Port (Afficher par port) apparaît sur la page Port Access. L'onglet View by Group (Afficher par groupe) affiche les mêmes informations que l'onglet View by Ports, toutefois, les ports sont classés suivant les affectations de groupes de ports existants.

Pour utiliser la page Port Access :

1. Dans la console distante de Dominion KX II, cliquez sur l'onglet Port Access (Accès aux ports). La page Port Access s'affiche.

   Les serveurs cible KVM sont triés initialement par numéro de port. Vous pouvez modifier l'affichage en effectuant le tri sur n'importe quelle colonne.

   - Port Number (Numéro de port) - Les ports sont numérotés de 1 au nombre total de ports disponibles pour le dispositif Dominion KX II. Notez que les ports connectés aux barrettes d'alimentation ne figurent pas sur la liste, ce qui génère des blancs dans la séquence des numéros de port.
   - Port Name (Nom de port) - Nom du port de Dominion KX II. Initialement, ce champ est paramétré sur Dominion-KX2-Port# mais vous pouvez remplacer ce nom par un autre plus parlant. Lorsque vous cliquez sur un lien Port Name (Nom du port), le menu d'action des ports (Port Action Menu) s'affiche.

   Remarque : n'utilisez pas d'apostrophe pour le nom de port (CIM).

- Status (Statut) - Le statut des serveurs cible standard est activé ou désactivé.
- Type - Type de serveur ou CIM. Pour les châssis de lames, ce type peut être Blade Chassis, Blade, BladeChassisAdmin et BladeChassisURL.
- Availability (Disponibilité) - La disponibilité peut être Idle (Inactif), Connected (Connecté), Busy (Occupé) ou Unavailable (Indisponible). Les serveurs lames peuvent être associés à une disponibilité partagée ou exclusive lorsqu'une connexion à cette lame est établie.

2. Cliquez sur View by Port (Afficher par port) ou View by Group (Afficher par groupe) pour passer d'une vue à l'autre.
3. Cliquez sur le nom du port du serveur cible auquel vous souhaitez accéder. Le menu d'action des ports (Port Action Menu) apparaît. Reportez-vous à **Port Action Menu (Menu d'action de ports)** (à la page 48) pour plus d'informations sur les options de menu disponibles.
4. Sélectionnez la commande souhaitée dans le menu d'action des ports.

Pour modifier l'ordre de tri d'affichage :

- Cliquez sur l'en-tête de la colonne par laquelle vous souhaitez effectuer un tri. La liste des serveurs cible KVM est triée par cette colonne.

Port Action Menu (Menu d'action de ports)

Lorsque vous cliquez sur un nom de port dans la liste Port Access, le menu d'action des ports s'affiche. Choisissez l'option de menu souhaitée pour ce port afin de l'exécuter. Notez que seules les options actuellement disponibles, suivant l'état et la disponibilité du port, seront répertoriées dans le menu d'actions des ports :

- Connect (Connecter) - Crée une nouvelle connexion au serveur cible. Pour la console distante de Dominion KX II, une nouvelle page ***Virtual KVM Client*** (à la page 57) apparaît. Pour la console locale de Dominion KX II, l'affichage passe de l'interface utilisateur locale au serveur cible. Sur le port local, l'interface de la console locale de Dominion KX II doit être visible pour pouvoir procéder à la commutation. La commutation par raccourci-clavier est également disponible à partir du port local.

  Remarque : cette option ne fonctionne pas pour un port disponible à partir de la console distante de Dominion KX II si toutes les connexions sont occupées.

- Switch From (Basculer depuis) : permet de basculer d'une connexion existante au port sélectionné (serveur cible KVM). Cette option de menu est disponible uniquement pour les cibles KVM et n'est visible que lorsqu'un client KVM virtuel est ouvert.

  Remarque : cette option de menu n'est pas disponible sur la console locale de Dominion KX II.

- Disconnect (Déconnecter) : permet de déconnecter ce port et de fermer la page du client KVM virtuel pour ce serveur cible. Cette option de menu est disponible uniquement lorsque l'état du port est actif et connecté, ou actif et occupé.

  Remarque : cette option de menu n'est pas disponible sur la console locale de Dominion KX II. La seule façon de se déconnecter de la cible activée dans la console locale est d'utiliser le raccourci clavier.

- Power On (Mettre sous tension) : permet de mettre le serveur cible sous tension par l'intermédiaire de la prise associée. Cette option est visible uniquement lorsqu'il existe au moins une association d'alimentation à la cible.
- Power Off (Mettre hors tension) : permet de mettre le serveur cible hors tension par l'intermédiaire des prises associées. Cette option est visible uniquement lorsqu'il existe au moins une association d'alimentation à la cible, lorsque la cible est activée (état du port actif) et lorsque l'utilisateur dispose de l'autorisation nécessaire pour opérer ce service.
- Power Cycle (Alimentation cyclique) : permet d'éteindre puis de rallumer le serveur cible par l'intermédiaire des prises associées. Cette option est visible uniquement lorsqu'il existe au moins une association d'alimentation à la cible et lorsque l'utilisateur dispose de l'autorisation nécessaire pour opérer ce service.

Gestion des favoris

Une fonction Favorites (Favoris) intégrée permet d'organiser les dispositifs que vous utilisez fréquemment et d'y accéder rapidement. La section Favorite Devices (Dispositifs favoris) se trouve dans la partie inférieure gauche (cadre) de la page Port Access et permet les opérations suivantes :

- créer et gérer une liste de dispositifs favoris ;
- accéder rapidement aux dispositifs fréquemment utilisés ;
- répertorier vos favoris par nom de dispositif, adresse IP ou nom d'hôte DNS ;
- détecter les dispositifs Dominion KX II sur le sous-réseau (avant et après la connexion) ;
- récupérer les dispositifs Dominion KX II détectés à partir du dispositif KX connecté (après la connexion).

Remarque : cette option est disponible uniquement sur la console distante de Dominion KX II (non sur la console locale de Dominion KX IIou l'AKC).

Pour accéder à un dispositif Dominion KX II favori :

- Cliquez sur le nom du dispositif (liste figurant sous Favorite Devices). Un nouveau navigateur s'ouvre pour le dispositif en question.

Pour afficher les favoris en fonction de leur nom :

- Cliquez sur Display by Name (Afficher par nom).

Pour afficher les favoris en fonction de leur adresse IP :

- Cliquez sur Display by IP (Afficher par adresse IP).

Pour afficher les favoris en fonction du nom d'hôte :

- Cliquez sur Display by Host Name (Afficher par nom d'hôte).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Page Manage Favorites (Gérer les favoris)

Pour ouvrir la page Manage Favorites :

- Cliquez sur le bouton Manage (Gérer) dans le panneau de gauche. La page Manage Favorites (Gérer les favoris) qui s'ouvre contient les éléments suivants :

Utilisez :	Pour :
Liste des favoris (Favorites List)	Gérer la liste de vos dispositifs favoris.
Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local)	Détecter les dispositifs Raritan sur le sous-réseau local du PC client.
Discover Devices - Dominion KX II Subnet (Détecter les dispositifs - Sous-réseau de Dominion KX II)	Détecter les dispositifs Raritan sur le sous-réseau du dispositif Dominion KX II.
Add New Device to Favorites (Ajouter un nouveau dispositif aux favoris)	Ajouter, modifier et supprimer des dispositifs dans votre liste de favoris.

Page Favorites List (Liste des favoris)

A partir de la page Favorites List, vous pouvez ajouter, modifier et supprimer des dispositifs dans votre liste de favoris.

Pour ouvrir la page Favorites List :

- Sélectionnez Manage (Gérer) > Favorites List (Liste des favoris). La page Favorites List s'ouvre.

Détection des dispositifs sur le sous-réseau local

Cette option détecte les dispositifs sur votre sous-réseau local, c'est-à-dire le sous-réseau sur lequel la console distante de Dominion KX II est exécutée. Ces dispositifs sont accessibles directement à partir de cette page ou vous pouvez les ajouter à votre liste de favoris. Reportez-vous à ***Page Favorites List (Liste des favoris)*** (à la page 52).

Pour détecter des dispositifs sur le sous-réseau local :

1. Sélectionnez Manage (Gérer) > Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local). La page Discover Devices - Local Subnet (Détecter les dispositifs - Sous-réseau local) apparaît.
2. Choisissez le port de détection approprié :
   - Pour utiliser le port de détection par défaut, sélectionnez la case Use Default Port 5000 (Utiliser le port 5000 par défaut).
   - Pour utiliser un port de détection différent :
     a. Désélectionnez la case Use Default Port 5000 (Utiliser le port 5000 par défaut).
     b. Entrez le numéro de port dans le champ Discover on Port (Détecter sur le port).
     c. Cliquez sur Save (Enregistrer).
3. Cliquez sur Refresh (Actualiser). La liste des dispositifs du sous-réseau KX est actualisée.

Pour ajouter des dispositifs à votre liste de favoris :

1. Cochez la case située en regard du nom du dispositif/de l'adresse IP.
2. Cliquez sur Add (Ajouter).

Conseil : utilisez les boutons Select All (Sélectionner tout) et Deselect All (Désélectionner tout) pour sélectionner (ou désélectionner) rapidement l'ensemble des dispositifs sur le sous-réseau de la console distante.

Pour accéder à un dispositif détecté :

- Cliquez sur le nom du dispositif ou sur son adresse IP. Un nouveau navigateur s'ouvre pour le dispositif en question.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Détection des dispositifs sur le sous-réseau de Dominion KX II

Cette option détecte les dispositifs sur le sous-réseau du dispositif, c'est-à-dire le sous-réseau de l'adresse IP du dispositif Dominion KX II même. Vous pouvez accéder à ces dispositifs directement à partir de la page Subnet (Sous-réseau) ou les ajouter à votre liste de favoris. Reportez-vous à ***Page Favorites List (Liste des favoris)*** (à la page 52).

Cette fonction permet à plusieurs dispositifs Dominion KX II d'interagir et de se mettre en corrélation automatiquement. La console distante de Dominion KX II détecte automatiquement les dispositifs Dominion KX II, et n'importe quel autre dispositif Raritan, sur le sous-réseau de Dominion KX II.

Pour détecter des dispositifs sur le sous-réseau du dispositif :

1. Choisissez Manage (Gérer) > Discover Devices - Dominion KX II Subnet (Détecter les dispositifs - Sous-réseau de Dominion KX II). La page Discover Devices - Dominion KX II Subnet (Détecter les dispositifs - Sous-réseau de Dominion KX II) apparaît.
2. Cliquez sur Refresh (Actualiser). La liste des dispositifs du sous-réseau KX est actualisée.

Pour ajouter des dispositifs à votre liste de favoris :

1. Cochez la case située en regard du nom du dispositif/de l'adresse IP.
2. Cliquez sur Add (Ajouter).

Conseil : utilisez les boutons Select All (Sélectionner tout) et Deselect All (Désélectionner tout) pour sélectionner (ou désélectionner) rapidement l'ensemble des dispositifs du sous-réseau du dispositif Dominion KX II.

Pour accéder à un dispositif détecté :

- Cliquez sur le nom du dispositif ou sur son adresse IP. Un nouveau navigateur s'ouvre pour le dispositif en question.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Ajout, suppression et modification des favoris

Pour ajouter un dispositif dans votre liste de favoris :

1. Sélectionnez Manage Favorites (Gérer les favoris) > Add New Device to Favorites (Ajouter un nouveau dispositif aux favoris). La page Add New Favorite (Ajouter un nouveau favori) apparaît.
2. Saisissez une description significative.
3. Entrez l'adresse IP ou le nom d'hôte du dispositif.
4. Modifiez le port de détection (le cas échéant).
5. Sélectionnez le type de produit.

6. Cliquez sur OK. Le dispositif est ajouté à votre liste de favoris.

Pour modifier un favori :

1. Dans la page Favorites List (Liste des favoris), cochez la case située en regard du dispositif Dominion KX II approprié.
2. Cliquez sur le bouton Edit (Modifier). La page Edit (Modifier) apparaît.
3. Mettez à jour les champs, le cas échéant :
   - Description
   - IP Address/Host Name (Adresse IP/Nom d'hôte) - Entrez l'adresse IP du dispositif Dominion KX II.
   - Port (si nécessaire)
   - Product Type (Type de produit).
4. Cliquez sur OK.

Pour supprimer un favori :

Important : Soyez prudent lorsque vous supprimez des favoris. Vous êtes invité à en confirmer la suppression.

1. Cochez la case en regard du dispositif Dominion KX II approprié.
2. Cliquez sur le bouton Delete (Supprimer). Le favori est supprimé de la liste.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Se déconnecter

Pour quitter la console distante de Dominion KX II :

- Cliquez sur Logout (Se déconnecter) dans le coin supérieur droit de la page.

Remarque : la déconnexion ferme également toutes les sessions ouvertes de Virtual KVM Client, ainsi que les sessions clientes série.

Interface Multi-Platform Client

Multi-Platform Client (MPC) de Raritan est une interface graphique utilisateur pour les lignes de produits Raritan qui permet un accès à distance aux serveurs cible connectés à Raritan KVM via des dispostifs IP. Pour plus d'informations sur l'utilisation de MPC, reportez-vous au **manuel des clients d'accès KVM et série** disponible sur le site Web de Raritan à la même page que le manuel d'utilisation. Des instructions sur le lancement de MPC sont fournies ici.

Lancement de MPC à partir d'un navigateur Web

Important : quel que soit le navigateur utilisé, vous devez autoriser l'affichage des fenêtres contextuelles à partir de l'adresse IP du dispositif Dominion pour lancer MPC.

1. Pour ouvrir MPC à partir d'un client exécutant n'importe quel type de navigateur pris en charge, tapez http://ADRESSE-IP/mpc dans la ligne d'adresse, où ADRESSE-IP correspond à l'adresse IP de votre dispositif Raritan. MPC s'ouvre dans une nouvelle fenêtre.

   Remarque : la commande Alt+Tab permet de basculer entre des fenêtres sur le système local uniquement.

   Lorsque MPC s'ouvre, les dispositifs Raritan détectés automatiquement qui se trouvent sur votre sous-réseau s'affichent en arborescence dans le navigateur.

2. Si le nom de votre dispositif n'apparaît pas dans le navigateur, ajoutez-le manuellement :

   a. Choisissez Connection (Connexion) > New Profile (Nouveau profil). La fenêtre Add Connection (Ajouter une connexion) s'affiche.

   b. Entrez-y la description d'un dispositif, indiquez un type de connexion, ajoutez l'adresse IP du dispositif, puis cliquez sur OK. Vous pouvez modifier ces spécifications ultérieurement.

3. Dans le panneau de navigation situé à gauche de la page, double-cliquez sur l'icône qui correspond à votre dispositif Raritan pour vous y connecter.

Remarque : selon le navigateur utilisé et ses paramètres de sécurité, plusieurs vérifications de sécurité et de certificats, ainsi que des messages d'avertissement peuvent s'afficher. Vous devez accepter les options pour ouvrir MPC.

Remarque : si vous utilisez Firefox 3.0.3, vous pouvez rencontrer des problèmes de lancement de l'application. Si cela se produit, effacez la mémoire cache du navigateur et lancez l'application à nouveau.

Virtual KVM Client

Présentation

Chaque fois que vous accédez à un serveur cible à l'aide de la console distante, une fenêtre Virtual KVM Client (VKC) s'ouvre. A chaque serveur cible connecté correspond une fenêtre Virtual KVM Client. Ces fenêtres sont accessibles via la barre de tâches Windows.

Elles peuvent être réduites, agrandies et déplacées sur le bureau de votre ordinateur.

Remarque : le rafraîchissement de votre navigateur HTML entraîne la fermeture de la connexion de Virtual KVM Client ; faites donc attention.

Remarque : si vous utilisez Firefox 3.0.3, vous pouvez rencontrer des problèmes de lancement de l'application. Si cela se produit, effacez la mémoire cache du navigateur et lancez l'application à nouveau.

Connexion à un serveur cible KVM

Pour se connecter à un serveur cible KVM :

1. Dans la console distante de Dominion KX II, cliquez sur l'onglet Port Access (Accès aux ports) pour l'ouvrir. La page Port Access s'affiche.
2. Cliquez sur le nom de port de la cible à laquelle vous souhaitez accéder. Le menu Port Action (Action des ports) apparaît.
3. Cliquez sur Connect (Connecter). Une fenêtre ***Virtual KVM Client*** (à la page 57) s'ouvre sur le serveur cible connecté à ce port.

Barre d'outils VKC

Remarque : l'interface VKC de KX II-101 est différente de celles des produits Dominion KX. Reportez-vous à Barre d'outils VKC pour KX II-101.

Bouton	Nom du bouton	Description
	Connection Properties (Propriétés de connexion)	Ouvre la boîte de dialogue Modify Connection Properties (Modifier les propriétés de connexion) à partir de laquelle vous pouvez manuellement définir les options de bande passante (telles que la vitesse de connexion, le nombre de couleurs, etc.).
	Video Settings (Paramètres vidéo)	Ouvre la boîte de dialogue Video Settings (Paramètres vidéo) qui permet de définir manuellement les paramètres de conversion des signaux vidéo.
	Color Calibration (Calibrage des couleurs)	Ajuste les paramètres de couleur de manière à réduire le bruit de couleur superflu. Revient à choisir Video > Color Calibrate (Calibrage des couleurs).
	Target Screenshot (Capture d'écran de la cible)	Cliquez pour effectuer une capture d'écran du serveur cible et l'enregistrer dans un fichier de votre choix.
	Synchronize Mouse (Synchronise r la souris)	En mode souris double, force le réalignement du pointeur de la souris du serveur cible sur le pointeur de la souris.
	Refresh Screen (Actualiser l'écran)	Force le rafraîchissement de l'écran vidéo.
	Auto-sense Video Settings (Détection automatique des paramètres vidéo)	Force le rafraîchissement des paramètres vidéo (résolution, taux de rafraîchissement).

Bouton	Nom du bouton	Description
	Smart Card (Carte à puce)	Ouvre une boîte de dialogue qui permet d'effectuer une sélection dans une liste de lecteurs de cartes à puce reliés à un PC client. *Remarque : cette fonction est disponible uniquement sur KX II 2.1.10 ou supérieur.* *Remarque : AKC ne prend pas en charge les cartes à puce.*
	Send Ctrl+Alt+Del (Envoyer Ctrl+Alt+Suppr)	Envoie la combinaison de touches de raccourci Ctrl+Alt+Suppr au serveur cible.
	Single Cursor Mode (Mode curseur simple)	Démarre le mode curseur simple par lequel le pointeur de souris locale n'apparaît plus à l'écran. Pour quitter ce mode, appuyez sur CTRL+ALT+O. Vous pouvez également choisir Single/Double Cursor (Curseur simple/double) dans le menu de raccourcis, qui s'ouvre à l'aide des touches Ctrl+Alt gauche+M.
	Mode Full Screen (Mode Plein écran)	Agrandit la zone de l'écran afin d'afficher le Bureau du serveur cible. *Remarque : AKC utilise une icône Exit Full Screen Mode (Quitter le mode Plein écran)* *pour sortir du mode Plein écran lorsque vous vous y trouvez.*
	Scaling (Mise à l'échelle)	Augmente ou réduit la taille de la vidéo cible de manière à afficher la totalité du contenu de la fenêtre du serveur cible sans l'aide de la barre de défilement.

Commutation entre les serveurs cible KVM

Grâce à Dominion KX II, vous pouvez accéder à plusieurs serveurs cible KVM. Dominion KX II permet de basculer d'un serveur cible à l'autre.

Remarque : cette fonction est disponible pour la console distante de Dominion KX II uniquement.

Pour commuter entre des serveurs cible KVM :

1. Si vous utilisez déjà un serveur cible, accédez à la page Port Access de Dominion KX II.
2. Cliquez sur le nom du port associé à la cible à laquelle vous souhaitez accéder. Le menu Port Action (Action des ports) apparaît.
3. Sélectionnez Switch From (Commuter depuis) dans le menu d'action des ports. La fenêtre Virtual KVM Client (Client KVM virtuel) bascule sur le nouveau serveur cible que vous avez sélectionné.

Gestion de l'alimentation d'un serveur cible

Remarque : ces fonctions sont disponibles uniquement si vous avez effectué des associations d'alimentation.

Pour effectuer l'alimentation cyclique d'un serveur cible KVM :

1. Dans la console distante de Dominion KX II, cliquez sur l'onglet Port Access (Accès aux ports). La page Port Access s'affiche.
2. Cliquez sur le nom du port du serveur cible souhaité. Le menu Port Action (Action des ports) apparaît.
3. Choisissez Power Cycle (Alimentation cyclique). Un message de confirmation apparaît.

Pour mettre sous tension un serveur cible :

1. Dans la console distante de Dominion KX II, cliquez sur l'onglet Port Access (Accès aux ports). La page Port Access s'affiche.
2. Cliquez sur le nom du port du serveur cible souhaité. Le menu Port Action (Action des ports) apparaît.
3. Choisissez Power On (Mettre sous tension). Un message de confirmation apparaît.

Pour mettre un serveur cible hors tension :

1. Dans la console distante de Dominion KX II, cliquez sur l'onglet Port Access (Accès aux ports) pour l'ouvrir. La page Port Access s'affiche.

2. Cliquez sur le nom du port du serveur cible souhaité. Le menu Port Action (Action des ports) apparaît.
3. Choisissez Power Off (Mettre hors tension). Un message de confirmation apparaît.

Déconnexion des serveurs cible KVM

Remarque : cette option n'est pas disponible sur la console locale de Dominion KX II. La seule façon de se déconnecter de la cible activée dans la console locale est d'utiliser le raccourci clavier.

Pour déconnecter un serveur cible :

1. Cliquez sur le nom de port de la cible que vous souhaitez déconnecter. Le menu Port Action (Action des ports) apparaît.
2. Choisissez Disconnect (Déconnecter).

Conseil : vous pouvez également fermer la fenêtre du client KVM virtuel en sélectionnant Connection (Connexion) > Exit (Quitter) à partir du menu Virtual KVM.

Sélection des profils USB

Lorsque vous vous connectez à un serveur cible KVM pour la première fois, comme décrit dans ***Connexion à un serveur cible KVM*** (à la page 57), le profil USB privilégié pour ce port est utilisé automatiquement. Si vous vous êtes déjà connecté au serveur cible à l'aide d'un profil différent, le profil USB de la dernière connexion est utilisé. Vous êtes averti de l'utilisation d'un profil autre que le profil privilégié par un avertissement semblable au suivant :

Après vous être connecté au serveur cible, vous pouvez modifier le profil USB, le cas échéant. Par défaut, les profils qui apparaissent sous le menu USB Profile (Profil USB) de VKC sont ceux que vous êtes le plus susceptible d'utiliser. Ces profils ont été présélectionnés par l'administrateur pour être utilisés avec le serveur cible connecté, selon les conditions de fonctionnement. Cependant, tous les profils sont disponibles pour être sélectionnés via l'option Other Profiles (Autres profils) dans le menu USB Profile (Profil USB).

Pour choisir un profil USB :

1. Connectez à un serveur cible KVM comme décrit dans ***Connexion à un serveur cible KVM*** (à la page 57).
2. Dans VKC, choisissez un profil USB dans le menu USB Profile.

   Le nom du profil indique le système d'exploitation ou le serveur avec lequel il doit être utilisé. Reportez-vous à ***Profils USB*** (à la page 106) pour plus d'informations sur les profils USB.

Connection Properties (Propriétés de connexion)

Les algorithmes de compression vidéo dynamique maintiennent le caractère convivial des consoles KVM avec différents types de bande passante. Les dispositifs optimisent la sortie KVM pour l'utilisation dans un réseau local, mais également pour l'utilisation dans un réseau étendu. Ces dispositifs peuvent également contrôler le nombre de couleurs et limiter la sortie vidéo permettant ainsi un équilibre optimal entre qualité vidéo et réactivité du système pour n'importe quelle bande passante.

Les paramètres de la boîte de dialogue Properties (Propriétés) peuvent être optimisés pour répondre à vos critères spécifiques selon les différents environnements d'exploitation. Les propriétés de connexion sont enregistrées pour les connexions suivantes sur des dispositifs de deuxième génération une fois paramétrées et enregistrées.

Remarque : VKC pour KX II-101 utilise un ensemble d'icônes différent de celui utilisé dans VKC pour d'autres produits Dominion KX. Reportez-vous à Barre d'outils VKC pour KX II-101 pour en savoir plus.

Pour définir les propriétés de connexion :

1. Choisissez Connection (Connexion) > Properties (Propriétés) ou cliquez sur le bouton Connection Properties (Propriétés de connexion) de la barre d'outils. La boîte de dialogue Properties (Propriétés) s'ouvre.

Remarque : KX II-101 ne prend pas en charge Ethernet 1 G.

Remarque : VKC pour KX II-101 utilise un ensemble d'icônes différent de celui utilisé dans VKC pour d'autres produits Dominion KX. Reportez-vous à Barre d'outils VKC pour KX II-101 pour en savoir plus.

2. Sélectionnez une valeur dans la liste déroulante Connection Speed (Vitesse de connexion). Le dispositif peut détecter automatiquement la basse passante disponible et ne pas en restreindre l'utilisation. Cependant, vous pouvez également en régler l'utilisation en fonction des limitations de bande passante.
   - Auto
   - Ethernet 1 G
   - Ethernet 100 Mo
   - Ethernet 10 Mo
   - 1,5 Mo (MAX DSL/T1)
   - 1 Mo (DSL/T1 rapide)
   - 512 Ko (DSL/T1 moyen)
   - 384 Ko (DSL/T1 lent)
   - 256 Ko (Câble)
   - 128 Ko (ISDN double)
   - 56 Ko (Modem ISP)
   - 33 Ko (Modem rapide)
   - 24 Ko (Modem lent)

   Notez que ces paramètres représentent des valeurs optimales dans des conditions spécifiques plutôt que le débit exact. Le client et le serveur s'efforcent de transmettre les données vidéo aussi rapidement que possible sur le réseau quels que soient la vitesse réseau et le paramètre d'encodage. Le système sera cependant plus réactif si les paramètres coïncident avec l'environnement réel.
3. Sélectionnez une valeur dans la liste déroulante Color Depth (Nombre de couleurs). Le dispositif peut adapter de manière dynamique le nombre de couleurs transmis aux utilisateurs distants afin d'optimiser la convivialité pour toutes les bandes passantes.
   - Couleurs RVB 15 bits
   - Couleurs RVB 8 bits
   - Couleurs 4 bits
   - Gris 4 bits
   - Gris 3 bits
   - Gris 2 bits
   - Noir et blanc

Important : pour la plupart des tâches d'administration (surveillance de serveur, reconfiguration, etc.), l'ensemble du spectre de couleurs 24 bits ou 32 bits disponible avec la plupart des cartes graphiques modernes n'est pas nécessaire. Les tentatives de transmission d'un nombre de couleurs aussi élevé entraîne une perte de bande passante du réseau.

4. Utilisez le curseur pour sélectionner le niveau de lissage souhaité (mode couleurs 15 bits uniquement). Le niveau de lissage détermine le degré de fusion des zones de l'écran aux variations de couleurs faibles en une couleur unique et uniforme. Le lissage améliore l'apparence des vidéos cible en réduisant les bruits vidéo affichés.
5. Cliquez sur OK pour conserver ces propriétés.

Informations sur la connexion

Pour obtenir des informations sur votre connexion à Virtual KVM Client :

- Sélectionnez Connection (Connexion) > Connection Info (Informations sur la connexion). La fenêtre Connection Info (Informations sur la connexion) s'ouvre.

Les informations suivantes relatives à la connexion en cours s'affichent :

- Device Name (Nom de dispositif) - Nom du dispositif.
- IP Address (Adresse IP) - Adresse IP du dispositif.
- Port - Port TCP/IP de communication KVM utilisé pour l'accès au dispositif cible.
- Data In/Second (Entrée de données/seconde) - Débit en entrée.
- Data Out/Second (Sortie de données/seconde) - Débit en sortie.
- Connect Time (Temps de connexion) - Durée de connexion.
- FPS - Images par seconde transmises pour la vidéo.
- Horizontal Resolution - Résolution d'écran horizontale.
- Vertical Resolution - Résolution d'écran verticale.
- Refresh Rate (Taux de rafraîchissement) - Fréquence à laquelle l'écran est actualisé.
- Protocol Version (Version du protocole) - Version du protocole RFB.

Pour copier ces informations :

- Cliquez sur Copy to Clipboard (Copier dans le Presse-papiers). Ces informations peuvent maintenant être collées dans le programme de votre choix.

Options de clavier

Macros de clavier

Les macros de clavier garantissent l'envoi des combinaisons de touches destinées au serveur cible et leur interprétation par celui-ci uniquement. Sinon, elles risquent d'être interprétées par l'ordinateur sur lequel est exécuté Virtual KVM Client (votre PC client).

Les macros sont stockées sur le PC client et sont spécifiques au PC. Aussi, si vous en utilisez un autre, vous ne verrez pas vos macros. Par ailleurs, si une autre personne utilise votre PC et se connecte sous un nom différent, elle verra vos macros puisqu'elles appartiennent à l'ordinateur.

Les macros de clavier créées dans Virtual KVM Client sont disponibles dans MPC et inversement. Cependant, les macros de clavier créées dans AKC ne peuvent pas être utilisées dans VKC ou MPC, et vice versa.

Définition d'une macro de clavier

Pour définir une macro :

1. Sélectionnez Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Cliquez sur Add (Ajouter). La boîte de dialogue Add Keyboard Macro (Ajouter une macro de clavier) s'affiche.
3. Saisissez un nom dans le champ Keyboard Macro Name (Nom de la macro de clavier). Ce nom apparaîtra dans le menu Keyboard (Clavier) après sa création.
4. Dans la liste déroulante du champ Hot-Key Combination (Raccourci-clavier), sélectionnez un raccourci-clavier. Ceci vous permet d'exécuter la macro avec une touche prédéfinie. **Facultatif**
5. Dans la liste déroulante Keys to Press (Touches à enfoncer), sélectionnez les touches que vous souhaitez utiliser pour émuler les touches qui seront utilisées pour effectuer la commande. Sélectionnez les touches dans l'ordre où elles devront être enfoncées. Après chaque sélection, sélectionnez Add Key (Ajouter la touche). Chaque touche sélectionnée apparaît dans le champ Macro Sequence (Séquence de la macro) et une commande Release Key (Relâcher la touche) est automatiquement ajoutée après chaque sélection.
6. Pour utiliser la fonction Send Text to Target (Envoyer un texte à la cible) pour la macro, cliquez sur le bouton Construct Macro from Text (Créer la macro à partir du texte).

7. Par exemple, créez une macro pour fermer une fenêtre en sélectionnant Ctrl de gauche+Echap. Ceci apparaît dans la case Macro Sequence (Séquence de la macro) comme suit :

   Press Left Ctrl (Appuyer sur Ctrl de gauche)

   Release Left Ctrl (Relâcher Ctrl de gauche)

   Press Esc (Appuyer sur Echap)

   Release Esc (Relâcher Echap).

8. Relisez le champ Macro Sequence pour vous assurer que la séquence de la macro est définie correctement.

   a. Pour supprimer une étape de la séquence, sélectionnez-la et cliquez sur Remove (Supprimer).

   b. Pour changer l'ordre des étapes de la séquence, cliquez sur l'étape, puis sur les boutons fléchés haut et bas pour réorganiser les étapes comme vous le souhaitez.

9. Cliquez sur OK pour enregistrer la macro. Cliquez sur Clear (Effacer) pour effacer le contenu du champ et recommencer. Si vous cliquez sur OK, la fenêtre Keyboard Macros (Macros de clavier) s'affiche et présente la nouvelle macro de clavier.

10. Cliquez sur Close (Fermer) pour fermer la boîte de dialogue Keyboard Macros. La macro apparaît maintenant dans le menu Keyboard (Clavier) de l'application. Sélectionnez la nouvelle macro dans le menu pour l'exécuter ou utilisez les touches affectées à la macro.

Lancement d'une macro de clavier

Une fois que vous avez créé une macro de clavier, exécutez-la à l'aide de la macro de clavier que vous lui avez affectée ou en la choisissant dans le menu Keyboard (Clavier).

Exécution d'une macro à partir de la barre de menus

Lorsque vous créez une macro, elle s'affiche dans le menu Keyboard (Clavier). Exécutez la macro du clavier en cliquant sur son nom dans le menu Keyboard (Clavier).

Exécution d'une macro avec une combinaison de touches

Si vous avez attribué une combinaison de touches à une macro lors de sa création, vous pouvez exécuter la macro en appuyant sur les touches correspondantes. Par exemple, appuyez simultanément sur les touches Ctrl+Alt+0 pour réduire toutes les fenêtres sur un serveur cible Windows.

Modification et suppression des macros de clavier

Pour modifier une macro :

1. Choisissez Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Choisissez la macro parmi celles qui figurent dans la liste.
3. Cliquez sur Modify (Modifier). La fenêtre d’ajout/de modification de la macro apparaît.
4. Effectuez vos modifications.
5. Cliquez sur OK.

Pour supprimer une macro :

1. Choisissez Keyboard (Clavier) > Keyboard Macros (Macros de clavier). La boîte de dialogue Keyboard Macros (Macros de clavier) s'affiche.
2. Choisissez la macro parmi celles qui figurent dans la liste.
3. Cliquez sur Remove (Supprimer). La macro est supprimée.

Les combinaisons de touches qui coïncident avec les séquences de touches de commutation de châssis de lames ne sont pas envoyées aux lames hébergées par ces châssis.

Paramétrage des options clavier/souris CIM

Pour accéder au menu de configuration de DCIM-USBG2 :

1. Mettez en surbrillance à l'aide de la souris une fenêtre telle que Notepad (Windows) ou son équivalent.
2. Appuyez sur la touche Ctrl de gauche et Verr num simultanément. Le menu de configuration CIM apparaît dans la fenêtre active.
3. Définissez la langue et les paramètres de souris.
4. Quittez le menu pour retourner à la fonctionnalité CIM normale.

Propriétés vidéo

Refresh Screen (Actualiser l'écran)

La commande Refresh Screen (Actualiser l'écran) force le rafraîchissement de l'écran vidéo. Les paramètres vidéo peuvent être actualisés automatiquement de plusieurs manières :

- La commande Refresh Screen (Actualiser l'écran) force le rafraîchissement de l'écran vidéo.
- La commande Auto-sense Video Settings (Détection automatique des paramètres vidéo) permet de détecter automatiquement les paramètres vidéo du serveur cible.
- La commande Calibrate Color (Calibrer les couleurs) permet de procéder au calibrage de la vidéo afin d'optimiser les couleurs affichées.

Vous pouvez également régler les paramètres manuellement à l'aide de la commande Video Settings (Paramètres vidéo).

Remarque : VKC pour KX II-101 utilise un ensemble d'icônes différent de celui utilisé dans VKC pour d'autres produits Dominion KX. Reportez-vous à Barre d'outils VKC pour KX II-101 pour en savoir plus.

Pour actualiser les paramètres vidéo, effectuez l'une des opérations suivantes :

- Choisissez Video > Refresh Screen (Actualiser l'écran) ou cliquez sur le bouton Refresh Screen de la barre d'outils.

Auto-Sense Video Settings (Détection automatique des paramètres vidéo)

La commande Auto-sense Video Settings force une nouvelle détection des paramètres vidéo (résolution, taux de rafraîchissement) et redessine l'écran vidéo.

Remarque : VKC pour KX II-101 utilise un ensemble d'icônes différent de celui utilisé dans VKC pour d'autres produits Dominion KX. Reportez-vous à Barre d'outils VKC pour KX II-101 pour en savoir plus.

Pour détecter automatiquement les paramètres vidéo :

- Choisissez Video > Auto-sense Video Settings (Détection automatique des paramètres vidéo) ou cliquez sur le bouton Auto-Sense Video Settings de la barre d'outils. Un message s'affiche pour indiquer que le réglage automatique est en cours.

Calibrage de la couleur

Utilisez la commande Calibrate Color pour optimiser les niveaux de couleur (teinte, luminosité, saturation) des images vidéo transmises. Les paramètres couleur concernent le serveur cible.

Remarque : la commande Calibrate Color (Calibrer les couleurs) s'applique à la connexion en cours uniquement.

Remarque : KX II-101 ne prend pas en charge le calibrage des couleurs.

Pour calibrer la couleur :

- Choisissez Video > Calibrate Color (Calibrer les couleurs) ou cliquez sur le bouton Calibrate Color de la barre d'outils. Le calibrage des couleurs de l'écran du dispositif cible est mis à jour.

Réglage des paramètres vidéo

Utilisez la commande Video Settings (Paramètres vidéo) pour ajuster manuellement les paramètres vidéo.

Pour modifier les paramètres vidéo :

1. Choisissez Video > Video Settings ou cliquez sur le bouton Video Settings de la barre d'outils pour ouvrir la boîte de dialogue du même nom.
2. Définissez les paramètres ci-après, le cas échéant. Les effets sont visibles dès que vous définissez les paramètres :
   a. Noise Filter (Filtre antiparasite)

      Le dispositif ProductName peut supprimer les interférences électriques de la sortie vidéo des cartes graphiques. Cette fonction optimise la qualité des images et réduit la bande passante. Les paramètres plus élevés transmettent des pixels de variante uniquement s'il existe une importante variation de couleurs par rapport aux pixels voisins. Néanmoins, si vous définissez un seuil trop élevé, des modifications souhaitées au niveau de l'écran peuvent être filtrées de manière non intentionnelle.
      Un seuil plus bas permet de transmettre le plus de changements de pixels. Si ce seuil est défini de manière trop faible, l'utilisation de la bande passante risque d'être plus importante.

   b. Brightness : utilisez cette option pour ajuster la luminosité de l'écran du serveur cible.

   c. Brightness Red : contrôle la luminosité de l'écran du serveur cible pour le signal rouge.

   d. Brightness Green : contrôle la luminosité du signal vert.

e. Brightness Blue : contrôle la luminosité du signal bleu.

f. Contrast Red : contrôle le contraste du signal rouge.

g. Contrast Green : contrôle le signal vert.

h. Contrast Blue : contrôle le signal bleu.

Si l'image vidéo semble très floue ou que sa mise au point ne semble pas correcte, les paramètres d'horloge et de phase peuvent être ajustés jusqu'à ce qu'une image de meilleure qualité s'affiche sur le serveur cible actif.

Avertissement : soyez prudent lorsque vous modifiez les paramètres Clock and Phase (Horloge et phase) ; en effet ces modifications peuvent entraîner des pertes ou des distorsions vidéo et vous risquez de ne plus pouvoir rétablir l'état précédent. Contactez l'assistance technique Raritan avant d'effectuer tout changement.

---

i. Clock (Horloge) : contrôle la vitesse d'affichage des pixels vidéo sur l'écran vidéo. Les modifications apportées aux paramètres d'horloge entraînent l'étirement ou la réduction de l'image vidéo sur le plan horizontal. Nous vous recommandons d'utiliser des nombres impairs. Dans la majorité des cas, ce paramètre ne doit pas être modifié car la détection automatique est en général très précise.

j. Phase : les valeurs de phase sont comprises entre 0 et 31 et s'affichent en boucle. Arrêtez-vous à la valeur de phase qui produit la meilleure image vidéo pour le serveur cible actif.

k. Horizontal Offset (Décalage horizontal) : contrôle le positionnement horizontal de l'affichage du serveur cible sur votre écran.

l. Vertical Offset (Décalage vertical) : contrôle le positionnement vertical de l'affichage du serveur cible sur votre écran.

3. Sélectionnez Auto Color Calibration (Calibrage automatique des couleurs) pour activer cette fonction.

4. Sélectionnez le mode de détection vidéo :

   - Best possible video mode (Mode vidéo optimal) :

   le dispositif effectue la totalité du processus de détection automatique lorsque vous changez de cibles ou de résolutions cible. La sélection de cette option calibre la vidéo pour obtenir la qualité d'image optimale.

   - Quick sense video mode (Détection rapide du mode vidéo) :

   avec cette option, le dispositif utilise la détection rapide automatique du mode vidéo pour afficher au plus vite le signal vidéo de la cible. Cette option est particulièrement utile lors de la saisie de la configuration BIOS d'un serveur cible immédiatement après un redémarrage.

5. Cliquez sur OK pour appliquer les paramètres et fermer la boîte de dialogue. Cliquez sur Apply pour appliquer les paramètres sans fermer la boîte de dialogue.

Remarque : certains écrans d'arrière-plan Sun, tels que les écrans à bord très sombres, risquent de ne pas se centrer de façon précise sur certains serveurs Sun. Utilisez un arrière-plan différent ou une icône de couleur plus claire dans le coin supérieur gauche de l'écran.

Remarque : VKC pour KX II-101 utilise un ensemble d'icônes différent de celui utilisé dans VKC pour d'autres produits Dominion KX. Reportez-vous à Barre d'outils VKC pour KX II-101 pour en savoir plus.

Utilisation de la fonction Screenshot from Target (Capture d'écran de la cible)

Vous pouvez effectuer une capture d'écran d'un serveur cible à l'aide de la commande serveur Screenshot from Target (Capture d'écran de la cible). Vous enregistrez ensuite cette capture d'écran à l'emplacement de votre choix dans un fichier bitmap, JPEG ou PNG.

Remarque : la fonction Screenshot from Target n'est pas disponible pour KX II-101.

Pour effectuer une capture d'écran du serveur cible :

1. Sélectionnez Video > Screenshot from Target (Capture d'écran de la cible) ou cliquez sur le bouton Screenshot from Target de la barre d'outils.
2. Dans la boîte de dialogue Save (Enregistrer), choisissez l'emplacement d'enregistrement du fichier, nommez le fichier et sélectionnez un format dans la liste déroulante Types de fichiers.
3. Cliquez sur Save (Enregistrer) pour sauvegarder la capture d'écran.

Modification du taux de rafraîchissement maximum

Si la carte vidéo dont vous disposez utilise un logiciel personnalisé et que vous accédez à la cible par l'intermédiaire de MPC ou de VKC, il vous faudra sans doute modifier le taux maximum de rafraîchissement de l'écran pour que celui-ci prenne effet sur la cible.

Pour régler le taux de rafraîchissement de l'écran :

1. Sous Windows, sélectionnez Propriétés d'affichage > Paramètres > Avancé pour ouvrir la boîte de dialogue Plug-and-Play.
2. Cliquez sur l'onglet Moniteur.
3. Définissez l'option Fréquence de rafraîchissement du moniteur/Fréquence d'actualisation du moniteur au-dessus de 100 Hz.
4. Cliquez sur OK, puis à nouveau sur OK pour appliquer le paramètre.

Options de souris

Lors de la gestion d'un serveur cible, la console distante affiche deux curseurs de souris : un curseur correspond à votre poste de travail client et l'autre au serveur cible.

Vous avez la possibilité d'opérer en mode souris simple ou en mode souris double. En mode souris double et si l'option est configurée correctement, les curseurs de la souris sont synchronisés.

En présence de deux curseurs de souris, le dispositif propose plusieurs modes souris :

- Absolue (Synchronisation de la souris)
- Intelligente (Mode souris)
- Standard (Mode souris)

Synchronisation des pointeurs de souris

Lorsque vous affichez à distance un serveur cible utilisant une souris, vous verrez apparaître deux curseurs de souris : un curseur correspond à votre poste de travail client distant et l'autre au serveur cible. Lorsque le pointeur de votre souris se trouve dans la zone de la fenêtre du serveur cible de Virtual KVM Client, les mouvements et les clics de souris sont directement transmis au serveur cible connecté. Lorsqu'il est en mouvement, le pointeur de la souris du client est légèrement en avance sur celui de la souris de la cible en raison des paramètres d'accélération de souris.

Avec des connexions de réseau local rapides, il vaut mieux désactiver le pointeur de la souris de Virtual KVM Client et afficher uniquement le pointeur de la souris du serveur cible. Vous pouvez basculer entre ces deux modes souris (simple et double).

Remarque : VKC pour KX II-101 utilise un ensemble d'icônes différent de celui utilisé dans VKC pour d'autres produits Dominion KX. Reportez-vous à Barre d'outils VKC pour KX II-101 pour en savoir plus.

Conseils de synchronisation de la souris

Veillez à suivre ces étapes lorsque vous configurez la synchronisation des souris :

1. Vérifiez que la résolution vidéo et le taux de rafraîchissement sélectionnés sont pris en charge par le dispositif. La boîte de dialogue Virtual KVM Client Connection Info (Informations sur la connexion de Virtual KVM Client) affiche les valeurs réellement observées par le dispositif.
2. Assurez-vous que la longueur de câble se trouve dans les limites spécifiées pour la résolution vidéo sélectionnée.
3. Vérifiez que la souris et la vidéo ont été configurées correctement au cours de l'installation.
4. Forcez la détection automatique en cliquant sur le bouton de détection automatique de Virtual KVM Client.
5. Si cela n'améliore pas la synchronisation de la souris (pour des serveurs cible KVM Linux, UNIX et Solaris) :
   a. Ouvrez une fenêtre de terminal.
   b. Entrez la commande `xset mouse 1 1`.
   c. Fermez la fenêtre de terminal.
6. Cliquez sur le bouton de synchronisation de la souris de Virtual KVM Client .

Remarques supplémentaires sur le mode souris intelligente

- Aucune icône ou application ne doit se trouver dans la partie supérieure gauche de l'écran dans la mesure où la routine de synchronisation a lieu à cet emplacement.
- N'utilisez pas de souris animée.
- Désactivez le bureau actif sur les serveurs cible KVM.

Synchronize Mouse (Synchroniser la souris)

En mode souris double, la commande Synchronize Mouse (Synchroniser la souris) force un nouvel alignement du pointeur de la souris du serveur cible avec le pointeur de la souris de Virtual KVM Client.

Pour synchroniser la souris, effectuez l'une des opérations suivantes :

- Choisissez Mouse (Souris) > Synchronize Mouse (Synchroniser la souris) ou cliquez sur le bouton Synchronize Mouse de la barre d'outils.

Mode souris standard

Le mode souris standard utilise un algorithme de synchronisation de souris standard reprenant les positions de souris relatives. Le mode souris standard requiert la désactivation de l'accélération de la souris et que les autres paramètres de souris soient configurés correctement afin que la souris du client et celle du serveur restent synchronisées. Le mode souris standard est le mode par défaut.

Pour entrer en mode souris standard :

- Choisissez Mouse (Souris) > Standard.

Mode souris intelligente

En mode souris intelligente, le dispositif peut détecter les paramètres de la souris cible et synchroniser les curseurs de souris en conséquence, permettant une accélération de la souris au niveau de la cible. Dans ce mode, le curseur de souris effectue une « danse » dans le coin supérieur gauche de l'écran et calcule l'accélération. Pour que ce mode fonctionne correctement, certaines conditions doivent être remplies.

Pour entrer en mode souris intelligente :

- Sélectionnez Mouse (Souris) > Intelligent (Intelligente).

Conditions de synchronisation d'une souris intelligente

La commande Intelligent Mouse Synchronization (Synchronisation de souris intelligente), disponible dans le menu Mouse (Souris) synchronise automatiquement les curseurs de souris lors des moments d'inactivité. Cependant, pour que cette option fonctionne correctement, les conditions suivantes doivent être remplies :

- Le bureau actif doit être désactivé sur le serveur cible.
- Aucune fenêtre ne doit apparaître dans le coin supérieur gauche de la page cible.
- Le coin supérieur gauche de la page cible ne doit pas comporter d'arrière-plan animé.
- La forme du pointeur de la souris cible doit être normale et non animée.
- La vitesse de déplacement du pointeur de souris du serveur cible ne doit pas être réglée sur une valeur très basse ou très élevée.
- Les propriétés de souris avancées, telles que Enhanced pointer precision (Améliorer la précision du pointeur) ou Snap mouse to default button in dialogs (Déplacer automatiquement le pointeur sur le bouton par défaut dans les boîtes de dialogue) doivent être désactivées.
- Les utilisateurs doivent sélectionner l'option Best Possible Video Mode (Mode vidéo optimal) dans la fenêtre Video Settings (Paramètres vidéo).
- Les bords de l'affichage vidéo du serveur cible doivent être clairement visibles (une bordure noire doit être visible entre le bureau de la cible et la fenêtre de la console KVM distante lorsque vous affichez un bord de l'image vidéo de la cible).
- La fonction de synchronisation de la souris intelligente risque de ne pas fonctionner correctement si vous avez une icône de fichier ou de dossier dans le coin supérieur gauche du bureau. Pour éviter tout problème avec cette fonction, Raritan vous recommande de ne pas avoir d'icônes de fichier ou de dossier dans le coin supérieur gauche de votre bureau.

Après avoir exécuté la fonction de détection automatique des paramètres vidéo, exécutez manuellement la synchronisation de la souris en cliquant sur le bouton Synchronize Mouse (Synchroniser la souris) dans la barre d'outils. Cette recommandation est également valable si la résolution du serveur cible est modifiée, entraînant une désynchronisation des pointeurs de souris.

Si la synchronisation de souris intelligente échoue, la souris reprend son comportement standard.

Notez que les configurations de souris varient selon le système d'exploitation cible. Reportez-vous aux instructions de votre système d'exploitation pour de plus amples informations. Notez également que la synchronisation intelligente de la souris ne fonctionne pas avec les cibles UNIX.

Mode souris absolue

Dans ce mode, des coordonnées absolues sont utilisées pour maintenir la synchronisation des curseurs client et cible, même si l'accélération ou la vitesse de la souris cible est configurée sur une valeur différente. Ce mode est pris en charge sur des serveurs avec ports USB.

Pour entrer en mode souris absolue :

- Sélectionnez Mouse (Souris) > Absolute (Absolue).

Remarque : le paramètre de souris absolue nécessite un système cible USB. Il est recommandé pour KX II-101.

Remarque : la synchronisation absolue de la souris est disponible uniquement pour les CIM USB pour lesquels le support virtuel est activé (D2CIM-VUSB et D2CIM-DVUSB).

Curseur de souris simple

Le mode souris simple utilise uniquement le curseur de la souris du serveur cible ; le pointeur de souris locale n'apparaît plus à l'écran. Si vous êtes en mode souris simple, la commande Synchronize Mouse n'est pas disponible (il n'est pas nécessaire de synchroniser un curseur de souris simple).

Remarque : VKC pour KX II-101 utilise un ensemble d'icônes différent de celui utilisé dans VKC pour d'autres produits Dominion KX. Reportez-vous à Barre d'outils VKC pour KX II-101 pour en savoir plus.

Pour passer en mode souris simple, procédez comme suit :

1. Sélectionnez Mouse (Souris) > Single Mouse Cursor (Curseur de souris simple).

2. Cliquez sur le bouton Single/Double Mouse Cursor (Curseur de souris simple/double) dans la barre d'outils.

Pour quitter le mode souris simple :

1. Appuyez sur Ctrl+Alt+O sur le clavier pour quitter le mode souris simple.

Supports virtuels VKC

Reportez-vous au chapitre sur les supports virtuels pour obtenir des informations complètes sur la configuration et l'utilisation des supports virtuels.

Cartes à puce (VKC et MPC)

Avec KX II 2.1.10 ou supérieur, vous pouvez monter un lecteur de cartes à puce sur le serveur cible pour prendre en charge l'authentification par carte à puce et les applications annexes. Pour obtenir la liste des cartes à puce et des lecteurs de cartes à puce pris en charge, ainsi que des exigences système supplémentaires, reportez-vous à ***Lecteurs de cartes à puce pris en charge et non pris en charge*** (voir "Lecteurs de cartes à puce pris en charge ou non" à la page 293) et Configuration système minimale requise.

Remarque : AKC ne prend pas en charge les cartes à puce.

Lorsque vous accédez à un serveur à distance, vous avez la possibilité de sélectionner un lecteur de cartes à puce branché et de le monter sur le serveur. L'authentification par carte à puce est utilisée avec le serveur cible, et non pour se connecter au dispositif. Aussi, les modifications apportées aux codes PIN et aux informations d'authentification ne nécessitent pas de mises à jour des comptes de dispositifs. Une fois montés sur le serveur cible, le lecteur de cartes et la carte à puce forceront le serveur à se comporter comme s'ils étaient directement connectés. Le retrait de la carte à puce ou du lecteur de cartes entraînera le verrouillage de la session utilisateur ou vous serez déconnecté suivant la stratégie de retrait de la carte définie dans le système d'exploitation du serveur cible. Lorsque la session KVM est arrêtée, parce qu'elle a été fermée ou parce que vous êtes passé sur une autre cible, le lecteur de cartes à puce est automatiquement démonté du serveur cible.

Lorsque le mode PC-Share est activé sur le dispositif, plusieurs utilisateurs peuvent partager l'accès à un serveur cible. Cependant, lorsqu'un lecteur de cartes à puce est connecté à une cible, le dispositif imposera la confidentialité quel que soit le paramètre du mode PC-Share. De plus, si vous rejoignez une session partagée sur un serveur cible, le montage du lecteur de cartes à puce sera désactivé jusqu'à ce qu'un accès exclusif au serveur cible soit disponible.

Une fois qu'une session KVM est établie vers le serveur cible, un menu et un bouton Smart Card (Carte à puce) sont disponibles sur Virtual KVM Client et Multi-Platform Client. Lorsque le menu est ouvert ou que le bouton Smart Card est sélectionné, les lecteurs de cartes à puce détectés comme branchés au client distant s'affichent. A partir de cette boîte de dialogue, vous pouvez relier des lecteurs de cartes à puce supplémentaires, actualiser la liste de lecteurs de cartes à puce reliés à la cible et déconnecter ces derniers. Vous pouvez également retirer ou réinsérer une carte à puce. Cette fonction permet d'envoyer une notification au système d'exploitation d'un serveur cible qui nécessite le retrait ou la réinsertion afin d'afficher la boîte de dialogue de connexion qui convient. L'utilisation de cette fonction permet l'envoi de la notification vers une cible unique sans affecter les autres sessions KVM actives.

Pour monter un lecteur de cartes à puce :

1. Cliquez sur le menu Smart Card, puis sélectionnez Smart Card Reader (Lecteur de cartes à puce). Vous pouvez également cliquer sur le bouton Smart Card de la barre d'outils.
2. Sélectionnez le lecteur de cartes à puce dans la boîte de dialogue Select Smart Card Reader (Sélectionner un lecteur de cartes à puce).
3. Cliquez sur Mount (Monter).
4. Une boîte de dialogue de progression s'ouvre. Cochez la case Mount selected card reader automatically on connection to targets (Monter le lecteur de cartes à puce sélectionné automatiquement lors de la connexion aux cibles) pour monter le lecteur automatiquement la prochaine fois que vous vous connectez à une cible. Cliquez sur OK pour démarrer le montage.

Pour mettre à jour la carte à puce dans la boîte de dialogue Select Smart Card Reader :

- Cliquez sur Refresh List (Actualiser la liste) si un lecteur de cartes à puce a été branché sur le PC client.

Pour envoyer des notifications de retrait et de réinsertion de la carte à puce à la cible :

- Sélectionnez le lecteur de cartes à puce monté actuellement et cliquez sur le bouton Remove/Reinsert (Retirer/Réinsérer).

Pour démonter un lecteur de cartes à puce :

- Sélectionnez le lecteur de cartes à puce à démonter et cliquez sur le bouton Unmount (Démonter).

Le montage des lecteurs de cartes à puce est également pris en charge depuis la console locale. Reportez-vous à ***Accès des cartes à puce à la console locale*** (voir "Accès par carte à puce à la console locale" à la page 262).

Options d'outils

A partir du menu Tools (Outils), vous pouvez définir certaines options à utiliser avec Virtual KVM Client, pour la connexion, la configuration du type de clavier et la définition de raccourcis-clavier pour quitter le mode de plein écran et de curseur simple.

Pour définir les options d'outils :

1. Sélectionnez Tools (Outils) > Options. La boîte de dialogue Options s'affiche.
2. Cochez la case Enable Logging (Activer la journalisation) uniquement si le support technique vous y invite. Cette option permet de créer un fichier journal dans votre répertoire personnel.
3. Sélectionnez le type de clavier (Keyboard Type) dans la liste déroulante (le cas échéant). Les options incluent :
   - US/International (Anglais Etats-Unis/international)
   - Français (France)
   - Allemand (Allemagne)
   - Japonais
   - United Kingdom
   - Coréen (Corée)
   - Belge (Belgique)
   - Norvégien (Norvège)
   - Portugais (Portugal)
   - Danois (Danemark)
   - Suédois (Suède)
   - Allemand (Suisse)
   - Hongrois (Hongrie)
   - Espagnol (Espagne)
   - Italien (Italie)
   - Slovène
   - Traduction : Français - US
   - Traduction : Français - US International

Remarque : dans AKC, le type de clavier provient par défaut du client local, cette option ne s'applique donc pas.

4. Exit Full Screen Mode (Quitter le mode Plein écran) - Raccourci-clavier. Lorsque vous entrez en mode Plein écran, l'affichage du serveur cible entre en mode Plein écran et acquiert la même résolution que le serveur cible. Il s'agit du raccourci-clavier utilisé pour quitter ce mode.

   Remarque : la fonction Exit Full Screen Hotkey (Quitter le mode Plein écran - Raccourci-clavier) ne s'applique pas à AKC. Dans AKC, une icône Exit Full Screen Mode *s'affiche à la place lorsque vous déplacez la souris vers le haut de l'écran.*

5. Exit Single Cursor Mode - Hotkey (Quitter le mode de curseur simple - Raccourci-clavier). Lorsque vous entrez en mode de curseur simple, seul le curseur de souris du serveur cible est visible. Il s'agit du raccourci-clavier utilisé pour quitter le mode de curseur simple et rétablir le curseur de souris du client. Cliquez sur OK.

Restrictions concernant les claviers

Claviers slovènes

La touche < ne fonctionne pas sur les claviers slovènes à cause d'une restriction JRE.

Configuration des langues étrangères sous Linux

Comme Sun JRE sous Linux a des difficultés à générer les événements clés corrects pour les claviers étrangers configurés à l'aide des préférences du système, Raritan recommande de configurer ces claviers étrangers à l'aide des méthodes utilisées dans le tableau suivant.

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Français	Indicateur de clavier
Allemand	Paramètres système (centre de contrôle)
Japonais	Paramètres système (centre de contrôle)
Anglais britannique	Paramètres système (centre de contrôle)
Coréen	Paramètres système (centre de contrôle)
Belge	Indicateur de clavier
Norvégien	Indicateur de clavier
Danois	Indicateur de clavier
Suédois	Indicateur de clavier
Hongrois	Paramètres système (centre de contrôle)

Langue/clavier	Méthode de configuration
Espagnol	Paramètres système (centre de contrôle)
Italien	Paramètres système (centre de contrôle)
Slovène	Paramètres système (centre de contrôle)
Portugais	Paramètres système (centre de contrôle)

Remarque : l'indicateur de clavier doit être utilisé sur les systèmes Linux utilisant l'environnement de bureau Gnome.

Options d'affichage

View Toolbar (Affichage de la barre d'outils)

Vous pouvez utiliser le Virtual KVM Client avec ou sans l'affichage de la barre d'outils.

Pour afficher et masquer la barre d'outils :

- Choisissez View > View Toolbar (Affichage > Afficher la barre d'outils).

Scaling (Mise à l'échelle)

La mise à l'échelle de votre fenêtre cible permet d'afficher la totalité de l'écran du serveur cible. Cette fonction augmente ou réduit la taille de la vidéo cible pour qu'elle tienne dans la fenêtre du Virtual KVM Client et conserve le rapport hauteur/largeur de manière à permettre l'affichage de la totalité du bureau du serveur cible sans utiliser la barre de défilement.

Pour activer et désactiver la mise à l'échelle :

- Choisissez View > Scaling (Affichage > Mise à l'échelle).

Target Screen Resolution (Résolution d'écran de la cible)

Lorsque vous entrez en mode Plein écran, l'affichage du serveur cible entre en mode Plein écran et acquiert la même résolution que le serveur cible. Le raccourci-clavier utilisé pour quitter ce mode est spécifié dans la boîte de dialogue Options (par défaut, il s'agit de Ctrl+Alt+M).

Pour entrer en mode Plein écran :

- Choisissez View > Full Screen (Affichage > Plein écran).

Pour quitter le mode Plein écran :

- Appuyez sur le raccourci clavier configuré dans la boîte de dialogue Options du menu Tools (Outils). Il s'agit par défaut de Ctrl+Alt+M. AKC cliquez sur l'icône Exit Full Screen Mode (Quitter le mode Plein écran).

Options d'aide

About Raritan Virtual KVM Client (A propos de Virtual KVM Client de Raritan)

Cette option de menu fournit les informations relatives à la version de Virtual KVM Client dans le cas où vous avez besoin de l'assistance technique de Raritan.

Pour obtenir les informations sur la version :

1. Sélectionnez Help > About Raritan Virtual KVM Client (Aide > A propos de Virtual KVM Client de Raritan).

2. Utilisez le bouton Copy to Clipboard (Copier dans le Presse-papiers) pour copier les informations contenues dans la boîte de dialogue dans un fichier de presse-papiers afin qu'elles soient accessibles ultérieurement lorsque vous communiquez avec le support (le cas échéant).

Active KVM Client (AKC)

Présentation

Le client KVM actif Microsoft Windows .NET (AKC) est disponible avec KX II 2.2 (ou supérieur) et prend en charge tous les modèles KX II, même si les modèles KX2-101 et KSX2 ne sont pas pris en charge actuellement. AKC est basé sur la technologie Microsoft Windows .NET et permet aux utilisateurs d'exécuter le client dans des environnements Windows sans utiliser Java Runtime Environment (JRE), qui est obligatoire pour exécuter les clients Virtual KVM et Multi-Platform de Raritan. AKC fonctionne également avec CC-SG.

AKC et VKC offrent des fonctions similaires à l'exception des suivantes :

- Configuration système minimale requise
- Systèmes d'exploitation et navigateurs pris en charge
- Les cartes à puce ne sont pas prises en charge dans AKC.
- La gestion des favoris n'est pas prise en charge dans AKC.
- Les macros de clavier créées dans AKC ne peuvent pas être utilisées dans VKC.

Reportez-vous à la section ***Virtual KVM Client*** (à la page 57) pour plus d'informations sur l'utilisation des fonctions disponibles de l'application. Les différences de fonctionnement entre AKC et VKC sont notées dans la rubrique.

Reportez-vous également à ***Présentation de l'accès direct aux ports*** (à la page 149) et à ***Présentation de la fonction Enable AKC Download Server Certificate Validation (Activer la validation du certificat du serveur de téléchargement AKC)*** (voir "Présentation de la fonction Activer la validation du certificat du serveur de téléchargement AKC" à la page 150) pour des informations de configuration pour l'utilisation d'AKC.

Remarque : si vous utilisez l'accès direct aux ports avec AKC, vous devez ouvrir une nouvelle fenêtre de navigateur ou un autre onglet de navigateur pour chaque cible à laquelle vous souhaitez accéder. Si vous tentez d'accéder à une autre cible en entrant l'URL de DPA dans la même fenêtre de navigateur ou le même onglet à partir desquels vous accédez actuellement à une cible, vous ne pourrez pas vous connecter et risquez d'obtenir une erreur.

Conditions préalables à l'utilisation d'AKC

Pour utiliser AKC :

- Vérifiez que les cookies de l'adresse IP du dispositif auquel vous accédez ne sont pas bloqués.
- Les utilisateurs de serveurs Windows Vista, Windows 7 et Windows 2008 doivent s'assurer que l'adresse IP du dispositif auquel ils accèdent est incluse dans la zone Sites approuvés de leur navigateur et que le mode protégé n'est pas activé lors de l'accès au dispositif.

De même, si l'administrateur KX II (ou CC-SG) a activé l'option Activer la validation du certificat du serveur de téléchargement AKC :

- Les administrateurs doivent téléverser un certificat auto-signé sur KX II ou en générer un sur KX II. Le certificat auto-signé doit désigner un hôte valide.
- Chaque utilisateur doit ajouter ce certificat dans la liste des autorités de certification de confiance de son navigateur.

Lorsque vous lancez AKC depuis le client Admin de CC-SG, vous devez disposer de JRE 1.6.0_10 ou supérieur.

Systèmes d'exploitation et navigateurs pris en charge par AKC

.NET Framework

AKC requiert la version 3.5 de .NET, et fonctionne si les versions 3.5 et 4.0 sont installées.

Systèmes d'exploitation

Lorsqu'il est lancé depuis Internet Explorer ou comme application autonome, AKC permet d'atteindre les serveurs cible via KX II 2.2 (ou supérieur). AKC est compatible avec les plates-formes suivantes exécutant Microsoft .NET Framework 3.5 :

- Windows XP
- Windows Vista
- Windows 7

.NET est requis pour exécuter AKC. S'il n'est pas installé ou si la version installée n'est pas prise en charge, vous recevrez un message vous demandant de vérifier la version de .NET.

Navigateur

- Internet Explorer 6 ou supérieur

Si vous tentez d'ouvrir AKC à partir d'un navigateur autre qu'IE 6 ou supérieur, vous recevrez un message d'erreur vous demandant de vérifier votre navigateur et d'utiliser Internet Explorer.

Chapitre 4 Support virtuel

Dans ce chapitre

Présentation 93
Conditions requises pour l'utilisation des supports virtuels.....96
Utilisation du support virtuel via VKC et AKC dans un environnement Windows 97
Utilisation des supports virtuels.....98
Configuration du serveur de fichiers (Images ISO du serveur de fichiers uniquement).....99
Connexion aux supports virtuels 101
Déconnexion des supports virtuels 105

Présentation

La fonction Support virtuel prolonge les capacités KVM en permettant aux serveurs cible KVM d'accéder à distance aux supports des serveurs de fichiers de PC clients et réseau. Grâce à cette fonction, les supports montés sur les serveurs de fichiers de PC clients et réseau sont intégrés virtuellement au serveur cible. Le serveur cible peut ensuite lire et écrire sur ce support comme si ce dernier lui était physiquement connecté. Outre la prise en charge des fichiers de données via support virtuel, les fichiers sont supportés par support virtuel via une connexion USB.

Les supports virtuels possibles sont les suivants : lecteurs de CD et de DVD internes et USB, mémoires de stockage de grande capacité USB, disques durs de PC et images ISO (images disque).

Remarque : ISO9660 est la norme prise en charge par Raritan. D'autres normes ISO peuvent cependant être utilisées.

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

- le transfert de fichiers ;
- la réalisation de diagnostics ;
- l'installation ou la correction d'applications ;
- l'installation complète du système d'exploitation.

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

B
C
A
D
4
3
KVM
2
IP
1
A
D
B
C

Légende			
1	Ordinateur de bureau	A	Lecteur CD/DVD
2	Dominion KX II	B	Dispositif de stockage de masse USB
3	CIM	C	Disque dur de l'ordinateur
4	Serveur cible	D	Serveur de fichiers à distance (images ISO)

Conditions requises pour l'utilisation des supports virtuels

Avec la fonction Support virtuel, vous pouvez monter jusqu'à deux lecteurs (de types différents) pris en charge par le profil USB actuellement appliqué à la cible. Ces lecteurs sont accessibles pendant toute la durée de la session KVM.

Par exemple, vous pouvez monter un CD-ROM spécifique, l'utiliser, puis le déconnecter lorsque vous avez terminé. Néanmoins, le « canal » de supports virtuels du CD-ROM demeure ouvert afin que vous puissiez monter un autre CD-ROM virtuellement. Ces « canaux » de supports virtuels restent ouverts jusqu'à la fermeture de la session KVM tant que le profil USB la prend en charge.

Pour utiliser le support virtuel, connectez/reliez-le au serveur de fichiers réseau ou client auquel vous souhaitez accéder à partir du serveur cible. Ceci n'est pas nécessairement la première étape mais elle doit être effectuée avant de tenter d'accéder au support.

Les conditions suivantes doivent être remplies pour pouvoir utiliser les supports virtuels :

Dispositif Dominion

- Pour les utilisateurs ayant besoin d'accéder aux supports virtuels, des autorisations de dispositif doivent être définies pour permettre l'accès aux ports concernés, ainsi que l'accès aux supports virtuels pour ces ports (Autorisations des ports d'accès aux supports virtuels). Les permissions des ports sont définies au niveau du groupe.
- Il doit exister une connexion USB entre le dispositif et le serveur cible.
- Pour utiliser PC-Share, des paramètres de sécurité doivent également être activés sur la page Security Settings. **Facultatif**
- Vous devez choisir le profil USB correct pour le serveur cible KVM auquel vous vous connectez.

Ordinateur client

- Certaines options de supports virtuels nécessitent des droits d'administrateur sur le PC client (par exemple, redirection de la totalité des lecteurs).

Remarque : Si vous utilisez Microsoft Vista ou Windows 7, désactivez Contrôle de compte d'utilisateur ou sélectionnez Exécuter en tant qu'administrateur lorsque vous démarrez Internet Explorer. Pour cela, cliquez sur le menu Démarrer, recherchez Internet Explorer, cliquez dessus avec le bouton droit de la souris et sélectionnez Exécuter en tant qu'administrateur.

Serveur cible

- Les serveurs cible KVM doivent prendre en charge les lecteurs connectés USB.
- Tous les patchs récents doivent être installés sur les serveurs cible KVM qui exécutent Windows 2000.
- Les ports USB 2.0 sont rapides et plus appropriés.

Utilisation du support virtuel via VKC et AKC dans un environnement Windows

Les droits Administrateur et utilisateur standard de Windows XP sont différents de ceux de Windows Vista et Windows 7.

Lorsqu'elle est activée dans Vista ou dans Windows 7, la fonction Contrôle d'accès d'utilisateur fournit le niveau de droits le plus bas dont un utilisateur a besoin pour une application. Par exemple, l'option Exécuter en tant qu'administrateur est fournie dans Internet Explorer pour autoriser explicitement les utilisateurs à effectuer des tâches de niveau Administrateur, sinon celles-ci ne seraient pas accessibles même si l'utilisateur dispose d'une connexion administrateur. La fonction Exécuter en tant qu'administrateur est fournie dans Internet Explorer. Elle permet aux utilisateurs d'effectuer des tâches de niveau Administrateur dans un environnement Windows.

Ces deux fonctions affectent le type de supports virtuels accessibles aux utilisateurs via Virtual KVM Client (VKC) et Active KVM Client (AKC). Consultez l'aide Microsoft pour en savoir plus sur ces fonctions et comment les utiliser.

La liste suivante répertorie des types de supports virtuels accessibles via VKC et AKC dans un environnement Windows. Ces fonctions sont classées par client, puis par rôle utilisateur Windows.

Windows XP

- Si vous utilisez VKC et AKC dans un environnement Windows XP, les utilisateurs doivent disposer de droits Administrateur pour accéder à n'importe quel type de support virtuel autre que les ISO et les images ISO.

Windows Vista et Windows 7

- Si vous utilisez VKC et AKC dans un environnement Windows Vista ou Windows 7 et que la fonction Contrôle d'accès d'utilisateur est activée, les types de supports virtuels suivants sont accessibles suivant le rôle Windows de l'utilisateur :

Client	Administrateur	Utilisateur standard
VKC	Accès : • Lecteurs fixes et partitions de lecteurs fixes • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes	Accès : • Lecteurs amovibles • Images ISO • Images ISO distantes
AKC	Accès : • Lecteurs fixes et partitions de lecteurs fixes • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes	Accès : • Lecteurs amovibles • Lecteurs CD/DVD • Images ISO • Images ISO distantes

Utilisation des supports virtuels

Reportez-vous à Conditions requises pour l'utilisation des supports virtuels avant d'utiliser le support virtuel.

Pour utiliser les supports virtuels :

1. Si vous souhaitez accéder à des images ISO de serveur de fichiers, identifiez ces images et ces serveurs de fichiers par le biais de la page Remote Console File Server Setup (Configuration des serveurs de fichiers de la console distante). Reportez-vous à Configuration du serveur de fichiers (Images ISO du serveur de fichiers uniquement).

   Remarque : le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

2. Ouvrez une session KVM avec le serveur cible adéquat.
   a. Ouvrez la page Port Access (Accès aux ports) depuis la console distante.

b. Connectez-vous au serveur cible à partir de la page Port Access (Accès aux ports) :

- Cliquez sur le nom du port (Port Name) du serveur approprié.
- Choisissez la commande Connect (Connecter) dans le menu d'action des ports. Le serveur cible s'ouvre dans une fenêtre Virtual KVM Client.

3. Connectez-vous au support virtuel.

Pour :	Sélectionnez cette option VM :
Lecteurs locaux	Local Drives (Lecteurs locaux)
Lecteurs de CD/DVD locaux	CD-ROM/DVD-ROM/ISO Images (Images ISO/CD-ROM/DVD-ROM)
Images ISO	Connect CD-ROM/ISO Image (Connecter l'image ISO/CD-ROM)
Images ISO de serveur de fichiers	Connect CD-ROM/ISO Image (Connecter l'image ISO/CD-ROM)

Une fois vos tâches terminées, déconnectez le support virtuel. Reportez-vous à ***Déconnexion des supports virtuels*** (à la page 105).

Configuration du serveur de fichiers (Images ISO du serveur de fichiers uniquement)

Remarque : cette fonction est requise uniquement lors de l'utilisation de supports virtuels pour accéder aux images ISO du serveur de fichiers.

le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

Utilisez la page File Server Setup (Configuration des serveurs de fichiers) de la console distante pour spécifier les serveurs de fichiers et les chemins d'accès aux images auxquelles vous souhaitez accéder à l'aide de la fonction Support virtuel. Les images ISO de serveurs de fichiers spécifiées sur cette page seront alors disponibles dans les listes déroulantes Remote Server ISO Image Hostname (Nom d'hôte des images ISO de serveur distant) et Image de la boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image CD/ISO des supports virtuels). Reportez-vous à **Images ISO/CD-ROM/DVD-ROM** (voir "CD-ROM/DVD-ROM/ISO Images (Images ISO/CD-ROM/DVD-ROM)" à la page 103).

Pour désigner les images ISO de serveur de fichiers pour l'accès aux supports virtuels :

1. Sélectionnez Virtual Media (Supports virtuels) dans la console distante. La page File Server Setup (Configuration des serveurs de fichiers) s'ouvre.

2. Cochez la case Selected (Sélectionné) pour tous les supports qui seront accessibles comme supports virtuels.
3. Entrez les informations relatives aux images ISO de serveur de fichiers auxquelles vous souhaitez accéder :
   - IP Address/Host Name - Nom d'hôte ou adresse IP du serveur de fichiers.
   - Image Path - Nom complet du chemin d'accès à l'emplacement de l'image ISO.

   Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.
4. Cliquez sur Save (Enregistrer). Tous les supports que vous avez spécifiés peuvent désormais être sélectionnés dans la boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image CD/ISO des supports virtuels).

Remarque : vous ne pouvez pas accéder à une image ISO distante via les supports virtuels à l'aide d'une adresse IPv6 à cause des limites techniques du logiciel tiers utilisé par KX2.

Remarque : si vous vous connectez à un serveur Windows 2003 et tentez de charger une image ISO à partir de ce serveur, vous risquez de recevoir un message d'erreur indiquant : « Virtual Media mounting on port failed. Unable to connect to the file server or incorrect File Server username and password » (Echec du montage du support virtuel. Impossible de connecter le serveur de fichiers ou nom d'utilisateur et mot de passe du serveur de fichiers erroné). Dans ce cas, désactivez l'option Serveur réseau Microsoft : communications signées numériquement sur le serveur sous les stratégies Contrôleurs de domaine.

Connexion aux supports virtuels

Local Drives (Lecteurs locaux)

Cette option permet de monter un lecteur entier, ce qui signifie que le lecteur de disque entier est monté virtuellement sur le serveur cible. Utilisez-la uniquement pour les disques durs et les lecteurs externes. Ceux-ci ne comprennent pas les lecteurs réseau, CD-ROM ou DVD-ROM. Il s'agit de la seule option pour laquelle la fonction Read-Write (Lecture/écriture) est disponible.

Remarque : les serveurs cible KVM exécutant certaines versions du système d'exploitation Windows risquent de ne pas accepter les nouvelles connexions de stockage en masse après la redirection vers eux d'une partition de format NTFS (par exemple, le disque C local).

Dans ce cas, fermez la console distante, puis reconnectez-vous avant de rediriger un autre dispositif de support virtuel. Si d'autres utilisateurs sont connectés au même serveur cible, ils doivent également fermer leurs connexions au serveur cible.

Remarque : dans Dominion KX II 2.1.0 et supérieur, lorsque vous montez un lecteur externe, tel qu'un lecteur de disquettes, le voyant reste allumé parce que le dispositif vérifie le lecteur toutes les 500 millisecondes afin de s'assurer qu'il est toujours monté.

Pour accéder à un lecteur de l'ordinateur client :

1. Dans Virtual KVM Client, sélectionnez Virtual Media (Supports virtuels) > Connect Drive (Connecter le lecteur). La boîte de dialogue Map Virtual Media Drive (Mapper le lecteur de support virtuel) s'affiche.

2. Sélectionnez le lecteur dans la liste déroulante Local Drive (Lecteur local).

3. Pour disposer d'un accès en lecture et en écriture, cochez la case Read-Write (Lecture-écriture). Cette option est désactivée pour les lecteurs non amovibles. Reportez-vous à ***Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible*** (à la page 102) pour plus d'informations. Lorsque cette case est cochée, vous aurez accès en lecture et en écriture au disque USB connecté.

   AVERTISSEMENT : l'activation de la fonction Lecture-écriture peut être dangereuse. L'accès simultané à un même lecteur à partir de plusieurs entités peut altérer les données. Si vous n'avez pas besoin d'un accès en écriture, ne sélectionnez pas cette option.

4. Cliquez sur Connect (Connecter). Le support est monté sur le serveur cible virtuellement. Vous pouvez y accéder de la même manière que pour tous les autres lecteurs.

Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible

La fonction Lecture-écriture du support virtuel n'est pas disponible dans les situations suivantes :

- pour tous les disques durs
- lorsque le lecteur est protégé en écriture
- lorsque l'utilisateur ne dispose pas de l'autorisation de lecture-écriture :
  - l'accès aux autorisations d'accès aux ports est défini sur None (Néant) ou View (Afficher)
  - l'accès des supports virtuels aux autorisations d'accès aux ports est défini sur Read-Only (Lecture seule) ou Deny (Refuser).

CD-ROM/DVD-ROM/ISO Images (Images ISO/CD-ROM/DVD-ROM)

Cette option permet de monter des images ISO, CD-ROM et DVD-ROM.

Remarque : le format ISO9660 est la norme prise en charge par Raritan. Cependant, les autres extensions de CD-ROM peuvent également fonctionner.

Pour accéder à une image ISO, CD-ROM ou DVD-ROM :

1. Dans Virtual KVM Client, sélectionnez Virtual Media > Connect CD-ROM/ISO Image (Supports virtuels > Connecter l'image ISO/CD-ROM). La boîte de dialogue Map Virtual Media CD/ISO Image (Mapper l'image ISO/CD de support virtuel) s'affiche.

2. Pour les lecteurs de CD-ROM ou DVD-ROM internes et externes :
   a. Sélectionnez l'option Local CD/DVD Drive (Lecteur CD/DVD local).
   b. Sélectionnez le lecteur dans la liste déroulante Local CD/DVD Drive (Lecteur CD/DVD local). Tous les noms de lecteurs CD/DVD internes et externes sont générés dans la liste déroulante.
   c. Cliquez sur Connect (Connecter).
3. Pour les images ISO :
   a. Sélectionnez l'option ISO Image (Image ISO). Utilisez cette option lorsque vous souhaitez accéder à une image disque de CD, de DVD ou de disque dur. Le format ISO est le seul format pris en charge.
   b. Cliquez sur le bouton Browse (Parcourir).

c. Localisez l'image disque que vous souhaitez utiliser, puis cliquez sur Open (Ouvrir). Le chemin d'accès est généré dans le champ Image Path (Chemin d'accès à l'image).

d. Cliquez sur Connect (Connecter).

4. Pour les images ISO distantes d'un serveur de fichiers :

a. Sélectionnez l'option Remote Server ISO Image (Image ISO de serveur à distance).

b. Sélectionnez un nom d'hôte et une image dans la liste déroulante. Les chemins d'accès aux images et les serveurs de fichiers disponibles sont ceux que vous avez configurés via la page File Server Setup (Configuration des serveurs de fichiers). Seuls les éléments que vous avez configurés à l'aide de cette page figurent dans la liste déroulante.

c. File Server Username - Nom d'utilisateur requis pour l'accès au serveur de fichiers.

d. File Server Password - Mot de passe requis pour l'accès au serveur de fichiers (le champ est masqué lorsque vous tapez).

e. Cliquez sur Connect (Connecter).

Le support est monté sur le serveur cible virtuellement. Vous pouvez y accéder de la même manière que pour tous les autres lecteurs.

Remarque : si vous travaillez sur des fichiers sur une cible Linux, utilisez la commande Sync de Linux après la copie des fichiers à l'aide des supports virtuels afin d'afficher les fichiers copiés. Les fichiers risquent de ne pas apparaître si la synchronisation n'est pas effectuée.

Remarque : si vous utilisez Windows 7, Disque amovible n'apparaît pas par défaut dans le dossier Poste de travail de Windows lorsque vous montez un lecteur de CD/DVD local, ou une image ISO locale ou distante. Pour afficher le lecteur de CD/DVD local, ou l'image ISO locale ou distante dans ce dossier, sélectionnez Outils > Options des dossiers > Affichage et désélectionnez Masquer les dossiers vides dans le dossier Ordinateur.

Remarque : vous ne pouvez pas accéder à une image ISO distante via les supports virtuels à l'aide d'une adresse IPv6 à cause des limites techniques du logiciel tiers utilisé par KX2.

Déconnexion des supports virtuels

Pour déconnecter les lecteurs de supports virtuels :

- Pour les lecteurs locaux, sélectionnez Virtual Media (Supports virtuels) > Disconnect Drive (Déconnecter le lecteur).
- Pour les images ISO, CD et DVD, sélectionnez Virtual Media (Supports Virtuels) > Disconnect CD-ROM/ISO Image (Déconnecter l'image ISO/CD-ROM)

Remarque : outre la commande Disconnect (Déconnecter), la simple fermeture de la connexion KVM entraîne la déconnexion du support virtuel.

Chapitre 5 Profils USB

Dans ce chapitre

Présentation 106
Compatibilité CIM 107
Profils USB disponibles 107
Sélection des profils pour un port KVM 114

Présentation

Pour élargir la compatibilité de Dominion KX II avec différents serveurs cible KVM, Raritan fournit une sélection standard de profils de configuration USB pour des implémentations de serveurs sur une grande variété de systèmes d'exploitation et de niveaux de BIOS.

Le profil USB générique (défaut) répond aux besoins de la grande majorité des configurations de serveurs cible KVM déployées. Des profils supplémentaires sont fournis pour répondre aux besoins spécifiques d'autres configurations de serveurs déployées courantes (par exemple, Linux et MAC OS X). Un certain nombre de profils (désignés par nom de plate-forme et révision de BIOS) permet également d'améliorer la compatibilité de la fonction Support virtuel avec le serveur cible ; par exemple, lors d'un fonctionnement au niveau du BIOS.

Les profils USB sont configurés sur la page Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) > Port des consoles distantes et locales de Dominion KX II. Un administrateur de dispositifs peut configurer le port avec les profils répondant le mieux aux besoins de l'utilisateur et de la configuration des serveurs cible.

Un utilisateur qui se connecte à un serveur cible KVM choisit parmi les profils présélectionnés dans ***Virtual KVM Client*** (à la page 57), suivant l'état de fonctionnement du serveur cible KVM. Par exemple, si le serveur est lancé et que l'utilisateur souhaite se servir du système d'exploitation Windows, il est recommandé d'utiliser le profil générique. Mais si l'utilisateur souhaite modifier les paramètres du menu du BIOS ou effectuer le démarrage à partir d'un lecteur de support virtuel, suivant le modèle du serveur cible, un profil BIOS est sans doute plus adéquat.

Si aucun des profils USB standard fournis par Raritan ne fonctionne avec une cible KVM précise, veuillez contactez l'assistance technique de Raritan.

Compatibilité CIM

Pour utiliser les profils USB, vous devez disposer d'un D2CIM-VUSB ou D2CIM-DVUSB dont le firmware est mis à jour. Un VM-CIM dont le firmware n'est pas mis à niveau prendra en charge une large gamme de configurations (clavier, souris, CD-ROM et lecteur amovible) mais ne pourra pas utiliser les profils optimisés pour des configurations cible particulières. Les VM-CIM existants doivent donc être mis à niveau avec le dernier firmware pour accéder aux profils USB. Tant qu'ils ne le seront pas, ils fourniront des fonctionnalités équivalentes à celles du profil générique.

Le firmware VM-CIM est automatiquement mis à niveau lors de la mise à niveau du firmware de Dominion KX II, mais les VM-CIM dont le firmware n'est pas actualisé peuvent l'être tel que décrit dans ***Mise à niveau des CIM*** (à la page 233).

Reportez-vous à ***Modules d'interface pour ordinateur (CIM)*** (à la page 279) pour plus d'informations.

Profils USB disponibles

La version actuelle de Dominion KX II comporte une sélection de profils USB décrits dans le tableau ci-après. Les nouveaux profils sont inclus avec chaque mise à niveau de firmware fournie par Raritan. Lorsque des nouveaux profils sont ajoutés, ils sont décrits dans l'aide.

Profil USB	Description
BIOS Dell PowerEdge 1950/2950/2970/6950/R200	BIOS Dell PowerEdge 1950/2950/2970/6950/R200 Utilisez ce profil ou le profil générique pour le BIOS Dell PowerEdge 1950/2950/2970/6950/R200. Restrictions : • Néant
BIOS DellOptiplex Keyboard Only	Accès BIOS Dell Optiplex (clavier uniquement) Utilisez ce profil pour disposer de la fonctionnalité de clavier pour le BIOS Dell Optiplex lors de l'utilisation de D2CIM-VUSB. Avec le nouveau D2CIM-DVUSB, utilisez le profil générique. Avis : • Optiplex 210L/280/745/GX620 nécessite D2CIM-DVUSB avec le

Profil USB	Description
	profil générique pour prendre en charge les supports virtuels. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Fonction Supports virtuels non prise en charge
BIOS DellPowerEdge Keyboard Only	Accès BIOS Dell PowerEdge (clavier uniquement) Utilisez ce profil pour disposer de la fonctionnalité de clavier pour le BIOS Dell PowerEdge lors de l'utilisation de D2CIM-VUSB. Avec le nouveau D2CIM-DVUSB, utilisez le profil générique. Avis : • PowerEdge 650/1650/1750/2600/2650 BIOS ne prend pas en charge les lecteurs USB CD-ROM et les disques durs comme service armorçable • PowerEdge 750/850/860/1850/2850/SC1425 BIOS nécessite D2CIM-DVUSB avec le profil générique pour prendre en charge les supports virtuels. • Utilisez BIOS Dell PowerEdge 1950/2950/2970/6950/R200 ou le profil générique pour PowerEdge 1950/2950/2970/6950/R200 lors d'un fonctionnement dans le BIOS. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge • Fonction Supports virtuels non prise en charge
BIOS Generic	BIOS Generic

Profil USB	Description
	Utilisez ce profil lorsque le profil générique du système d'exploitation ne fonctionne pas sur le BIOS. AVERTISSEMENT : l'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS HP Proliant DL145	HP Proliant DL145 PhoenixBIOS Utilisez ce profil pour HP Proliant DL145 PhoenixBIOS pendant l'installation du système d'exploitation. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps)
BIOS HPCompaq DC7100/DC7600	BIOS HP Compaq DC7100/DC7600 Utilisez ce profil pour démarrer les ordinateurs de la série HP Compaq DC7100/DC7600 à partir du support virtuel. Restrictions : • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS IBM ThinkCentre Lenovo	BIOS IBM Thinkcentre Lenovo Utilisez le profil pour la carte principale IBM Thinkcentre Lenovo (modèle 828841U) pendant les opérations du BIOS. Restrictions : • Vitesse du bus USB limitée à plein

Profil USB	Description
	régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
BIOS Lenovo ThinkPad T61 & X61	BIOS Lenovo ThinkPad T61 et X61 (démarrage à partir du support virtuel) Utilisez ce profil pour démarrer les ordinateurs portables des séries T61 et X61 à partir du support virtuel. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps)
BIOS Mac	BIOS Mac Utilisez ce profil pour le BIOS Mac. Restrictions : • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Générique	Le profil USB générique se comporte comme dans la version du KX2 original. Utilisez-le pour Windows 2000, XP, Vista et ultérieur. Restrictions : • Néant
HP Proliant DL360/DL380 G4 (HP SmartStart CD)	HP Proliant DL360/DL380 G4 (HP SmartStart CD) Utilisez ce profil pour le serveur HP Proliant DL360/DL380 série G4 lors de l'installation du système d'exploitation à l'aide de HP SmartStart CD. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge

Profil USB	Description
HP Proliant DL360/DL380 G4 (Installation Windows 2003 Server)	HP Proliant DL360/DL380 G4 (Installation Windows 2003 Server) Utilisez ce profil pour le serveur HP Proliant DL360/DL380 série G4 lors de l'installation de Windows 2003 Server sans HP SmartStart CD. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps)
Linux	Profil Linux générique Il s'agit du profil Linux générique ; utilisez-le pour Redhat Enterprise Linux, SuSE Linux Enterprise Desktop et distributions semblables. Restrictions : • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge
MAC OS X (10.4.9 et supérieur)	MAC OS X, versions 10.4.9 et supérieure Ce profil compense la mise à l'échelle des coordonnées de la souris présente dans les versions récentes de Mac OS X. Sélectionnez-le si les positions de la souris distante et locale sont désynchronisées près des bordures du bureau. Restrictions : • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Carte-mère industrielle RUBY (AwardBIOS)	Carte-mère industrielle RUBY (AwardBIOS) Utilisez ce profil pour les cartes mères industrielles de la série RUBY-9715VG2A avec Phoenix/AwardBIOS v6.00PG. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et

Profil USB	Description
	disques durs virtuels ne peuvent pas être utilisés simultanément.
Supermicro Mainboard Phoenix (AwardBIOS)	Carte-mère Supermicro Phoenix (AwardBIOS) Utilisez ce profil pour les cartes-mères de la série Supermicro avec Phoenix AwardBIOS. Restrictions : • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément.
Suse 9.2	SuSE Linux 9.2 Utilisez-le pour la distribution SuSE Linux 9.2. Restrictions : • Absolute mouse synchronization™ (Synchronisation absolue de la souris) non prise en charge • Vitesse du bus USB limitée à plein régime (12 Mbps)
Troubleshooting 1	Dépannage de profil 1 • Stockage en masse en premier • Clavier et souris (Type 1) • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : l'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté.
Troubleshooting 2	Dépannage de profil 2 • Clavier et souris (Type 2) en premier • Stockage en masse • Vitesse du bus USB limitée à plein régime (12 Mbps)

Profil USB	Description
	• Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : l'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté.
Troubleshooting 3	Dépannage de profil 3 • Stockage en masse en premier • Clavier et souris (Type 2) • Vitesse du bus USB limitée à plein régime (12 Mbps) • Les lecteurs de CD-ROM et disques durs virtuels ne peuvent pas être utilisés simultanément. AVERTISSEMENT : l'énumération USB se déclenche dès que le support virtuel est connecté ou déconnecté.
Utiliser le plein régime pour le CIM de support virtuel	Utiliser le plein régime pour le CIM de support virtuel Ce profil se comporte comme dans la version du KX2 original lorsque l'option Full Speed for Virtual Media CIM (Plein régime pour le CIM de support virtuel) est activée. Utile pour le BIOS qui ne peut pas traiter les dispositifs USB High Speed. Restrictions : • Vitesse du bus USB limitée à plein régime (12 Mbps)

Sélection des profils pour un port KVM

Dominion KX II est fourni avec un ensemble des profils USB que vous pouvez affecter à un port KVM suivant les caractéristiques du serveur cible KVM auquel il se connecte. Vous attribuez des profils USB à un port KVM sur la page Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) > Port de la console distante ou locale de Dominion KX II.

L'administrateur désigne les profils les plus susceptibles d'être utilisés pour une cible spécifique. Ces profils peuvent alors être sélectionnés via MPC/VKC. Si un profil n'est pas disponible, vous pouvez accéder à n'importe quel profil disponible en sélectionnant USB Profile (Profil USB) > Other Profiles (Autres profils).

L'affectation de profils USB à un port KVM met ceux-ci à la disposition d'un utilisateur connecté à un serveur cible KVM. Le cas échéant, l'utilisateur peut sélectionner un profil USB dans le menu USB Profile de VKC ou de MPC.

Pour plus d'informations sur l'affectation de profils USB à un port KVM, reportez-vous à ***Configuration des profils USB (page Port)*** (à la page 197).

Modes de souris lors de l'utilisation du profil USB Mac OS X avec DCIM-VUSB

Si vous utilisez DCIM-VUSB, avec un profil USB Mac OS X, en exécutant Mac OS X 10.4.9 (ou supérieur), vous devez passer en mode de souris unique lors du redémarrage pour utiliser la souris dans le menu Boot (Amorçage).

Pour configurer la souris pour qu'elle fonctionne dans le menu Boot :

1. Redémarrez le Mac et appuyez sur la touche Option pendant le redémarrage pour ouvrir le menu Boot. La souris ne répond pas à ce moment.
2. Sélectionnez le mode de souris intelligente, puis le mode de souris unique. La souris répond.

   Remarque : la souris peut être lente en mode de souris unique.

3. Une fois que vous avez quitté le menu Boot et avez amorcé le système d'exploitation, quittez le mode de souris unique et repassez en mode de souris absolue pour obtenir de meilleures performances de la souris.

Chapitre 6 User Management (Gestion des utilisateurs)

Dans ce chapitre

Groupes d'utilisateurs 115
Utilisateurs 125
Paramètres d'authentification 128
Modification d'un mot de passe 141

Groupes d'utilisateurs

Dominion KX II stocke une liste interne de tous les noms des utilisateurs et des groupes pour déterminer les autorisations et permissions d'accès. Ces informations sont stockées de manière interne dans un format chiffré. Il existe plusieurs formes d'authentification et celle-ci est connue sous le nom d'authentification locale. Tous les utilisateurs doivent être authentifiés. Si Dominion KX II est configuré pour LDAP/LDAPS ou RADIUS, cette authentification est traitée en premier, suivie par l'authentification locale.

Tous les dispositifs Dominion KX II sont livrés avec trois groupes d'utilisateurs par défaut. Ces groupes ne peuvent être supprimés :

Utilisateur	Description
Admin	Les membres de ce groupe disposent de droits d'administrateur complets. L'utilisateur par défaut usine est membre de ce groupe et dispose de la totalité des droits de système. De plus, l'utilisateur Admin doit être membre du groupe Admin.
Unknown (Inconnu)	Il s'agit du groupe par défaut pour les utilisateurs authentifiés en externe à l'aide de LDAP/LDAPS ou RADIUS, ou que le système ne connaît pas. Si le serveur externe LDAP/LDAPS ou RADIUS ne peut pas identifier un groupe d'utilisateurs valide, le groupe Unknown est alors utilisé. De plus, tout utilisateur qui vient d'être créé est automatiquement affecté à ce groupe en attendant d'être transféré dans un autre.
Individual Group (Groupe individuel)	Un groupe individuel ne comporte en fait qu'un seul membre. Cet utilisateur spécifique est donc dans son propre groupe et non affilié à d'autres groupes réels. Les groupes individuels sont repérables par leur nom qui comporte le signe @. Le groupe individuel permet à un compte d'utilisateur de bénéficier des mêmes droits qu'un groupe.

Liste des groupes d'utilisateurs

Les groupes d'utilisateurs sont utilisés avec une authentification à distance et locale (par l'intermédiaire de RADIUS ou de LDAP/LDAPS). Il est recommandé de définir les groupes avant de créer les différents utilisateurs car lorsque vous ajoutez un utilisateur, vous devez l'affecter à un groupe d'utilisateurs existant.

La page User Group List (Liste des groupes d'utilisateurs) affiche une liste de tous les groupes d'utilisateurs. Ceux-ci peuvent être triés dans l'ordre croissant ou décroissant en cliquant sur l'en-tête de colonne Group Name. A partir de la page User Group List, vous pouvez ajouter, modifier ou supprimer des groupes d'utilisateurs.

Pour répertorier les groupes d'utilisateurs :

- Sélectionnez User Management (Gestion des utilisateurs) > User Group List (Liste des groupes d'utilisateurs). La page User Group List s'ouvre.

Relation entre les utilisateurs et les groupes

Les utilisateurs appartiennent à un groupe et les groupes disposent de droits. La répartition en groupes des utilisateurs de votre unité Dominion KX II offre un gain de temps, puisqu'elle permet de gérer les autorisations de l'ensemble des utilisateurs d'un groupe donné en une seule fois au lieu de les gérer individuellement.

Vous pouvez également choisir de ne pas associer des utilisateurs particuliers à des groupes. Vous avez alors la possibilité de classer l'utilisateur comme « individuel ».

Lorsqu'un utilisateur est authentifié, le dispositif utilise les informations relatives au groupe auquel il appartient pour déterminer ses autorisations : ports de serveur accessibles, autorisation éventuelle de redémarrer l'unité, etc.

Ajout d'un nouveau groupe d'utilisateurs

Pour ajouter un nouveau groupe d'utilisateurs :

1. Ouvrez la page Group (Groupe) en sélectionnant User Management (Gestion des utilisateurs) > Add New User Group (Ajouter un nouveau groupe d'utilisateurs), ou en cliquant sur le bouton Add (Ajouter) de la page User Group List (Liste des groupes d'utilisateurs).

   La page Group est organisée en plusieurs catégories : Group (Groupe), Permissions (Autorisations), Port Permissions (Autorisations d'accès aux ports) et IP ACL (LCA IP).

2. Entrez un nom descriptif pour le nouveau groupe d'utilisateurs dans le champ Group Name (64 caractères au plus).
3. Définissez les permissions (autorisations) pour le groupe. Cochez les cases situées en regard des permissions que vous souhaitez attribuer à tous les utilisateurs appartenant à ce groupe. Reportez-vous à ***Définition des autorisations*** (voir "Configuration des autorisations" à la page 119).
4. Définissez les autorisations d'accès aux ports. Spécifiez les ports de serveur auxquels peuvent accéder les utilisateurs appartenant à ce groupe (et le type d'accès). Reportez-vous à ***Configuration des autorisations d'accès aux ports*** (à la page 121).
5. Configurez la liste de contrôle d'accès IP (IP ACL). Cette fonction limite l'accès au dispositif Dominion KX II par le biais de la spécification d'adresses IP. Cette fonction s'applique uniquement aux utilisateurs appartenant à un groupe spécifique, contrairement à la fonction de liste de contrôle d'accès IP qui s'applique à toutes les tentatives d'accès au dispositif (et est prioritaire). **Facultatif**. Reportez-vous à ***LCA (liste de contrôle d'accès) IP de groupes*** (à la page 122).
6. Cliquez sur OK.

Remarque : plusieurs fonctions d'administration sont disponibles dans MPC et à partir de la console locale de Dominion KX II. Elles sont disponibles uniquement pour les membres du groupe par défaut Admin.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Configuration des autorisations

Important : la sélection de la case User Management (Gestion des

utilisateurs) permet aux membres du groupe de modifier les autorisations de tous les utilisateurs, y compris les leurs. Accordez ces autorisations avec prudence.

Autorisation	Description
Device Access While Under CC-SG Management (Accès au dispositif sous la gestion de CC-SG)	Permet aux utilisateurs et aux groupes d'utilisateurs ayant cette autorisation d'accéder directement à Dominion KX II à l'aide d'une adresse IP lorsque l'accès local est activé pour le dispositif dans CC-SG. Le dispositif est accessible à partir de la console locale, de la console distante, de MPC, de VKC et de AKC. Lorsque vous accédez à un dispositif directement alors qu'il est géré par CC-SG, l'activité d'accès et de connexion est consignée dans Dominion KX II. L'authentification de l'utilisateur est effectuée suivant les paramètres d'authentification de Dominion KX II. *Remarque : le groupe d'utilisateurs Admin dispose de cette autorisation par défaut.*
Device Settings (Paramètres du dispositif)	Paramètres réseau, paramètres date/heure, configuration des ports (nom de canal, association d'alimentation), gestion des événements (SNMP, Syslog), configuration du serveur de fichiers du support virtuel
Diagnostics	Etat d'interface réseau, statistiques de réseau, envoi d'une commande Ping à un hôte, tracer l'itinéraire jusqu'à un hôte, diagnostics de l'unité Dominion KX II
Maintenance	Sauvegarde et restauration de base des données, mise à niveau du firmware, réinitialisation des paramètres usine, redémarrage
Modem Access (Accès par modem)	Autorisation d'utiliser le modem pour la connexion au dispositif Dominion KX II
PC-Share	Accès simultané à la même cible par plusieurs utilisateurs
Sécurité	Certificat SSL, paramètres de sécurité (VM Share, PC-Share), LCA IP
User Management (Gestion des utilisateurs)	Gestion des utilisateurs et des groupes, authentification à distance (LDAP/LDAPS/RADIUS), paramètres de connexion

Configuration des autorisations d'accès aux ports

Pour chaque port de serveur, vous pouvez spécifier le type d'accès du groupe, ainsi que le type d'accès aux ports du support virtuel et la gestion de l'alimentation. Veuillez noter que le paramètre par défaut de toutes les autorisations est Deny (Refuser).

Port Access (Accès aux ports)	
Option	**Description**
Deny (Refuser)	Accès refusé complètement
View (Afficher)	Afficher (mais non interagir avec) le serveur cible connecté
Control (Contrôler)	Contrôle le serveur cible connecté. Le contrôle doit être affecté au groupe si l'accès du support virtuel et de gestion d'alimentation est également accordé.

VM access (Accès au support virtuel)	
Option	**Description**
Deny (Refuser)	L'autorisation d'accès au support virtuel est entièrement refusée pour le port.
Read-Only (Lecture seule)	L'accès au support virtuel est limité à l'accès en lecture uniquement.
Read-Write (Lecture-écriture)	Accès total (en lecture, en écriture) au support virtuel

Power control access (Accès à la gestion d'alimentation)	
Option	**Description**
Deny (Refuser)	Refuser la gestion d'alimentation au serveur cible
Access (Accès)	Autorisation totale de gestion d'alimentation sur un serveur cible

Dans le cas d'un châssis de lames, les autorisations d'accès aux ports contrôleront l'accès aux URL configurées pour ce châssis. Les options sont Deny (Refuser) ou Control (Contrôler). De plus, chaque lame hébergée par le châssis utilise son propre paramètre Port Permissions indépendant.

Définition des autorisation pour un groupe individuel

Pour configurer des autorisations pour un groupe d'utilisateurs individuel :

1. Localisez le groupe parmi ceux de la liste. Les groupes individuels peuvent être identifiés par le signe @ dans leur nom.
2. Cliquez sur le nom du groupe. La page Group s'ouvre.
3. Sélectionnez les autorisations appropriées.
4. Cliquez sur OK.

Remarque : reportez-vous à Paramètres de l'autre authentification RADIUS pour en savoir plus sur les paramètres supplémentaires si vous utilisez une autre authentification RADIUS.

LCA (liste de contrôle d'accès) IP de groupes

Important : soyez prudent lorsque vous utilisez le contrôle d'accès IP applicable à des groupes. L'accès à Dominion KX II risque d'être verrouillé si votre adresse IP se trouve dans la plage des adresses à laquelle l'accès a été refusé.

Cette fonction limite à certaines adresses IP l'accès au dispositif Dominion KX II pour les utilisateurs appartenant au groupe sélectionné. Elle s'applique uniquement aux utilisateurs appartenant à un groupe spécifique, contrairement à la fonction de liste de contrôle d'accès IP qui s'applique à toutes les tentatives d'accès au dispositif, est traitée en premier, et est donc prioritaire).

Important : l'adresse IP 127.0.0.1 est utilisée par le port local de Dominion KX II et ne peut pas être verrouillée.

Utilisez la section IP ACL (LCA IP) de la page Group pour ajouter, insérer, remplacer et supprimer les règles de contrôle d'accès au niveau des groupes.

Pour ajouter des règles :

1. Saisissez la première adresse IP dans le champ Starting IP (Adresse IP de départ).
2. Entrez la dernière adresse IP dans le champ Ending IP (Adresse IP de fin).
3. Choisissez l'action à effectuer dans la liste des options disponibles :
   - Accept - Les adresses IP paramétrées sur Accept sont autorisées à accéder au dispositif Dominion KX II.
   - Drop - Les adresses IP paramétrées sur Drop ne sont pas autorisées à accéder au dispositif Dominion KX II.
4. Cliquez sur Append (Ajouter). La règle est ajoutée au bas de la liste des règles. Répétez les étapes 1 à 4 pour chacune des règles à entrer.

Pour insérer une règle :

1. Entrez un numéro de règle (#). Ce numéro est requis lorsque vous utilisez la commande Insert (Insérer).
2. Renseignez les champs Starting IP et Ending IP.
3. Choisissez une option dans la liste déroulante Action.
4. Cliquez sur Insert (Insérer). Si le numéro de règle que vous venez d'entrer est le même que celui d'une règle existante, la nouvelle règle est placée avant la règle existante et toutes les règles sont descendues d'un rang.

Pour remplacer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez remplacer.
2. Renseignez les champs Starting IP et Ending IP.
3. Choisissez une option dans la liste déroulante Action.

4. Cliquez sur Replace (Remplacer). Votre nouvelle règle remplace la règle d'origine dont elle conserve le numéro.

Pour supprimer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez supprimer.
2. Cliquez sur Delete (Supprimer).
3. Lorsque vous êtes invité à confirmer la suppression, cliquez sur OK.

Important : les règles LCA sont évaluées selon l'ordre dans lequel elles sont répertoriées. Par exemple si, dans l'exemple présenté ici, les deux règles LCA étaient inversées, Dominion n'accepterait aucune communication.

Conseil : les numéros de règle vous permettent de mieux contrôler l'ordre de création des règles.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Modification d'un groupe d'utilisateurs existant

Remarque : toutes les autorisations relatives au groupe Admin sont activées (et ne peuvent pas être modifiées).

Pour modifier un groupe d'utilisateurs existant :

1. A partir de la page Group, modifiez les champs appropriés et définissez les autorisations adéquates.
2. Définissez les permissions pour le groupe. Cochez les cases situées en regard des permissions que vous souhaitez attribuer à tous les utilisateurs appartenant à ce groupe. Reportez-vous à Définition des autorisations.
3. Définissez les autorisations d'accès aux ports. Spécifiez les ports de serveur auxquels peuvent accéder les utilisateurs appartenant à ce groupe (et le type d'accès). Reportez-vous à **Définition des autorisations d'accès aux ports** (voir "Configuration des autorisations d'accès aux ports" à la page 121).
4. Configurez la liste de contrôle d'accès IP (IP ACL) (facultatif). Cette fonction limite l'accès au dispositif Dominion KX II par le biais de la spécification d'adresses IP. Reportez-vous à **LCA (liste de contrôle d'accès) IP de groupes** (à la page 122).
5. Cliquez sur OK.

Pour supprimer un groupe d'utilisateurs :

Important : si vous supprimez un groupe contenant des utilisateurs, ces derniers sont automatiquement affectés au groupe d'utilisateurs <unknown (inconnu)>.

Conseil : pour déterminer quels utilisateurs appartiennent à un groupe particulier, triez la User List (Liste des utilisateurs) par User Group (Groupe d'utilisateurs).

1. Sélectionnez un groupe parmi ceux qui figurent dans la liste en cochant la case située à gauche du nom de groupe.
2. Cliquez sur Delete (Supprimer).
3. Lorsque vous êtes invité à confirmer la suppression, cliquez sur OK.

Utilisateurs

Les utilisateurs doivent disposer de noms d'utilisateur et de mots de passe pour accéder à Dominion KX II. Ces informations sont utilisées pour authentifier les utilisateurs qui tentent d'accéder à votre unité Dominion KX II.

Liste des utilisateurs

La page User List (Liste des utilisateurs) affiche une liste de tous les utilisateurs, avec leur nom d'utilisateur, leur nom complet et le groupe d'utilisateurs auquel ils appartiennent. Pour trier cette liste en fonction d'une colonne, cliquez sur le nom de celle-ci. A partir de la page User List, vous pouvez également ajouter, modifier ou supprimer des utilisateurs.

Pour afficher la liste des utilisateurs :

- Sélectionnez User Management (Gestion des utilisateurs) > User List (Liste des utilisateurs). La page User List (Liste des utilisateurs) s'ouvre.

Ajout d'un nouvel utilisateur

Il est recommandé de définir les groupes d'utilisateurs avant de créer des utilisateurs Dominion KX II, car lorsque vous ajoutez un utilisateur, vous devez l'affecter à un groupe d'utilisateurs existant. Reportez-vous à **Ajout d'un nouveau groupe d'utilisateurs** (à la page 117).

Vous pouvez ajouter de nouveaux utilisateurs, modifier leurs informations et réactiver des utilisateurs sur la page User.

Remarque : un nom d'utilisateur peut être désactivé lorsque le nombre de tentatives de connexion qui ont échoué a atteint la limite définie dans la page Security Settings (Paramètres de sécurité). Reportez-vous à ***Paramètres de sécurité****.*

Pour ajouter un nouvel utilisateur :

1. Ouvrez la page User (Utilisateur) en sélectionnant User Management (Gestion des utilisateurs) > Add New User (Ajouter un nouvel utilisateur), ou en cliquant sur le bouton Add (Ajouter) de la page User List (Liste des utilisateurs).
2. Tapez un nom unique dans le champ Username (Nom d'utilisateur) (16 caractères au maximum).
3. Tapez le nom complet de la personne dans le champ Full Name (Nom complet) (64 caractères au maximum).
4. Tapez un mot de passe dans le champ Password, puis entrez-le à nouveau dans le champ Confirm Password (Confirmer le mot de passe) (64 caractères au maximum).
5. Choisissez un groupe dans la liste déroulante User Group (Groupe d'utilisateurs). La liste contient tous les groupes que vous avez créés en plus des groupes par défaut fournis par le système, <Unknown> (Inconnu), paramètre par défaut, Admin, Individual Group (Groupe individuel).

   Si vous ne souhaitez pas affecter cet utilisateur à un groupe d'utilisateurs existant, sélectionnez Individual Group (Groupe individuel) dans la liste déroulante. Pour plus d'informations sur les autorisations associées à un groupe individuel, reportez-vous à ***Définition des autorisations pour un groupe individuel*** (voir "Définition des autorisation pour un groupe individuel" à la page 122).
6. Pour activer le nouvel utilisateur, cochez la case Active. L'utilisateur est activé par défaut.
7. Cliquez sur OK.

Modification d'un utilisateur existant

Pour modifier un utilisateur existant :

1. Ouvrez la page User List (Liste des utilisateurs) en choisissant User Management (Gestion des utilisateurs) > User List.
2. Localisez l'utilisateur parmi ceux répertoriés sur la page User List.
3. Cliquez sur le nom d'utilisateur. La page User (Utilisateur) s'ouvre.
4. Sur la page User (Utilisateur), modifiez les champs appropriés. Reportez-vous à ***Ajout d'un nouvel utilisateur*** (à la page 126) pour plus d'informations sur les méthodes d'accès à la page User.
5. Pour supprimer un utilisateur, cliquez sur Delete. Vous êtes invité à confirmer la suppression.
6. Cliquez sur OK.

Déconnexion d'un utilisateur (Déconnexion forcée)

Si vous êtes administrateur, vous pouvez déconnecter un autre utilisateur authentifié localement qui est connecté à Dominion KX II.

Pour déconnecter un utilisateur :

1. Ouvrez la page User List en choisissant User Management > User List ou cliquez sur le lien Connected User (Utilisateur connecté) dans le panneau gauche de la page.
2. Recherchez l'utilisateur parmi ceux répertoriés sur la page User List et cochez la case en regard de son nom.
3. Cliquez sur le bouton Force User Logoff (Forcer la déconnexion de l'utilisateur).
4. Cliquez sur OK dans la boîte de dialogue Logoff User (Déconnecter l'utilisateur) pour forcer la déconnexion.

5. Un message de confirmation indique alors que l'utilisateur est déconnecté. Ce message contient les date et heure de la déconnexion. Cliquez sur OK pour fermer ce message.

Paramètres d'authentification

L'authentification est un processus qui consiste à vérifier l'identité d'un utilisateur. Une fois l'utilisateur authentifié, son groupe permet de déterminer ses autorisations d'accès aux ports et au système. Les droits accordés à l'utilisateur déterminent le type d'accès autorisé. Cela s'appelle l'autorisation.

Lorsque Dominion KX II est configuré pour l'authentification à distance, le serveur d'authentification externe est utilisé principalement à des fins d'authentification et non d'autorisation.

Sur la page Authentication Settings (Paramètres d'authentification), vous pouvez configurer le type d'authentification utilisé pour l'accès à Dominion KX II.

Remarque : lorsque l'authentification à distance (LDAP/LDAPS ou RADIUS) est sélectionnée, si l'utilisateur est introuvable, la base de données d'authentification locale est également vérifiée.

Pour configurer l'authentification :

1. Choisissez User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification). La page Authentication Settings s'ouvre :
2. Choisissez le protocole d'authentification que vous souhaitez utiliser (Local Authentication [Authentification locale], LDAP/LDAPS ou RADIUS). L'option LDAP active les champs LDAP restants ; l'option RADIUS active les champs RADIUS restants.
3. Si vous sélectionnez Local Authentication (Authentification locale), passez à l'étape 6.
4. Si vous sélectionnez LDAP/LDAPS, lisez la section intitulée Implémentation de l'authentification à distance LDAP pour obtenir des informations sur la façon de renseigner les champs dans la section LDAP de la page Authentication Settings (Paramètres d'authentification).
5. Si vous sélectionnez RADIUS, lisez la section intitulée Implémentation de l'authentification à distance RADIUS pour obtenir des informations sur la façon de renseigner les champs dans la section RADIUS de la page Authentication Settings (Paramètres d'authentification).
6. Cliquez sur OK pour enregistrer.

Pour réinitialiser les paramètres par défaut usine :

1. Cliquez sur le bouton Reset to Defaults (Restaurer les paramètres par défaut).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Implémentation de l'authentification à distance LDAP/LDAPS

LDAP (Lightweight Directory Access Protocol, protocole allégé d'accès à un annuaire) est un protocole de mise en réseau pour la recherche et la modification de services d'annuaires fonctionnant sur TCP/IP. Un client démarre une session LDAP en se connectant à un serveur LDAP/LDAPS (le port TCP par défaut est 389). Le client envoie ensuite les demandes de fonctionnement au serveur, et le serveur envoie les réponses en retour.

Rappel : Microsoft Active Directory fonctionne de manière native comme serveur d'authentification LDAP/LDAPS.

Pour utiliser le protocole d'authentification LDAP :

1. Cliquez sur User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification) pour ouvrir la page Authentication Settings.
2. Sélectionnez le bouton radio LDAP pour activer la section LDAP de la page.
3. Cliquez sur l'icône ▸ LDAP pour développer la section LDAP de la page.

Configuration du serveur

4. Dans le champ Primary LDAP Server (Serveur LDAP principal), entrez l'adresse IP ou le nom DNS de votre serveur d'authentification à distance LDAP/LDAPS (256 caractères au plus). Lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) est sélectionnée avec l'option Enable LDAPS Server Certificate Validation (Activer la validation du certificat du serveur LDAPS), le nom DNS doit être utilisé pour vérifier le certificat du serveur LDAP du CN.
5. Dans le champ Secondary LDAP Server (Serveur LDAP secondaire), entrez l'adresse IP ou le nom DNS de votre serveur de sauvegarde LDAP/LDAPS (256 caractères au plus). Lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) sélectionnée, le nom DNS doit être utilisé. Notez que les champs restants comportent les mêmes paramètres que le champ Primary LDAP Server. **Facultatif**
6. Type de serveur LDAP externe.
7. Entrez le nom du domaine Active Directory. Par exemple, *testradius.com*. Consultez l'administrateur Active Directory pour obtenir un nom de domaine spécifique.

8. Dans le champ User Search DN (ND de recherche d'utilisateur), entrez le ND de l'emplacement dans la base de données LDAP où la recherche d'informations d'utilisateur doit commencer. Vous pouvez entrer jusqu'à 64 caractères. Exemple de valeur de recherche de base : `cn=Users,dc=raritan,dc=com`. Consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ces champs.
9. Entrez le Distinguished Name de l'utilisateur administratif dans le champ DN of Administrative User (64 caractères au plus). Renseignez ce champ si votre serveur LDAP autorise uniquement les administrateurs à rechercher des informations d'utilisateur à l'aide du rôle Administrative User. Consultez l'administrateur de votre serveur d'authentification pour obtenir les valeurs à saisir dans ce champ. Exemple de valeur de ND d'utilisateur administratif : `cn=Administrator,cn=Users,dc=testradius,dc=com`. **Facultatif**

10. Si vous avez entré un Distinguished Name pour l'utilisateur administratif, vous devez entrer le mot de passe qui sera utilisé pour authentifier le ND de l'utilisateur administratif par comparaison avec le serveur d'authentification à distance. Entrez le mot de passe dans le champ Secret Phrase (Expression secrète) et à nouveau dans le champ Confirm Secret Phrase (Confirmer l'expression secrète) (128 caractères au plus).

LDAP/LDAP sécurisé

11. Cochez la case Enable Secure LDAP (Activer le LDAP sécurisé) si vous souhaitez utiliser SSL. Ceci coche la case Enable LDAPS Server Certificate Validation (Activer la validation du certificat du serveur LDAPS). SSL (Secure Sockets Layer) est un protocole cryptographique qui permet à Dominion KX II de communiquer en toute sécurité avec le serveur LDAP/LDAPS.
12. Le port par défaut est 389. Utilisez le port LDAP TCP standard ou spécifiez un autre port.

13. Le port LDAP sécurisé par défaut est 636. Utilisez le port par défaut ou spécifiez un autre port. Ce champ est utilisé uniquement lorsque la case Enable Secure LDAP (Activer le LDAP sécurisé) est cochée.
14. Cochez la case Enable LDAPS Server Certificate Validation afin d'utiliser le fichier de certificat de l'autorité de certification (AC) racine téléversé précédemment pour valider le certificat fourni par le serveur. Si vous ne souhaitez pas utiliser le fichier de certificat, désactivez la case à cocher. Désactiver cette fonction revient à accepter un certificat signé par une autorité de certification inconnue. Cette case à cocher est uniquement disponible lorsque la case Enable Secure LDAP est cochée.

Remarque : lorsque l'option Enable LDAPS Server Certificate Validation est sélectionnée, outre l'utilisation du certificat de l'AC racine pour la validation, le nom d'hôte du serveur doit correspondre au nom commun fourni dans le certificat du serveur.

15. Le cas échéant, téléversez le fichier de certificat de l'AC racine. Ce champ est activé lorsque l'option Enable Secure LDAP (Activer le LDAP sécurisé) est sélectionnée. Consultez l'administrateur de votre serveur d'authentification pour obtenir le fichier de certificat de l'AC au format Base64 codé X-509 pour le serveur LDAP/LDAPS. Utilisez le bouton Browse (Parcourir) pour localiser le fichier du certificat. Si vous remplacez un certificat pour un serveur LDAP/LDAPS par un nouveau, vous devez redémarrer Dominion KX II pour que ce nouveau certificat prenne effet.

Test de l'accès à un serveur LDAP

16. Dominion KX II permet de tester la configuration LDAP dans la page Authentication Settings (Paramètres d'authentification) à cause de la difficulté à configurer correctement le serveur LDAP et Dominion KX II pour l'authentification à distance. Pour tester la configuration LDAP, entrez le nom et le mot de passe de connexion dans les champs Login for testing (Nom de connexion pour le test) et Password for testing (Mot de passe pour le test) respectivement. Il s'agit des nom d'utilisateur et de mot de passe entrés pour accéder à Dominion KX II et que le serveur LDAP utilisera pour vous authentifier. Cliquez sur Test.

    Une fois le test terminé, un message s'affiche pour indiquer si le test a réussi ou s'il a échoué, un message d'erreur détaillé apparaît. Un message de réussite ou détaillé d'erreur, en cas d'échec, apparaît. Il donne également des informations de groupe extraites du serveur LDAP distant pour l'utilisateur du test en cas de réussite.

Renvoi des informations relatives aux groupes d'utilisateurs à partir d'Active Directory

Dominion KX II prend en charge l'authentification des utilisateurs auprès d'Active Directory (AD) sans qu'il soit nécessaire de définir les utilisateurs localement au niveau de Dominion KX II. Les comptes et mots de passe des utilisateurs Active Directory peuvent ainsi être gérés exclusivement sur le serveur AD. L'autorisation et les droits des utilisateurs AD sont contrôlés et administrés par le biais de stratégies classiques dans Dominion KX II et de droits appliqués localement à des groupes d'utilisateurs AD.

IMPORTANT : si vous êtes déjà client de Raritan, Inc. et que vous avez configuré le serveur Active Directory en modifiant le schéma AD, Dominion KX II continue de prendre en charge cette configuration et il ne vous est pas nécessaire d'effectuer les opérations suivantes. Pour obtenir des informations sur la mise à jour du schéma AD LDAP/LDAPS, reportez-vous à Mise à jour du schéma LDAP.

Pour activer le serveur AD sur Dominion KX II :

1. A l'aide de Dominion KX II, créez des groupes spéciaux et attribuez-leur les autorisations et privilèges appropriés. Par exemple, créez des groupes tels que KVM_Admin et KVM_Operator.
2. Sur le serveur Active Directory, créez des groupes portant le même nom qu'à l'étape précédente.
3. Sur votre serveur AD, affectez les utilisateurs de l'unité Dominion KX II aux groupes créés au cours de l'étape 2.
4. A partir de Dominion KX II, activez et configurez le serveur AD comme il se doit. Reportez-vous à Implémentation de l'authentification à distance LDAP/LDAPS.

Remarques importantes :

- Le nom de groupe est sensible à la casse.
- Dominion KX II fournit les groupes par défaut suivants qui ne peuvent pas être modifiés ni supprimés : Admin et <Unknown (Inconnu)>. Vérifiez que le serveur Active Directory n'utilise pas les mêmes noms de groupe.
- Si les informations de groupe renvoyées par le serveur Active Directory ne correspondent pas à une configuration de groupe Dominion KX II, ce dernier attribue automatiquement le groupe <Unknown> (Inconnu) aux utilisateurs qui ont réussi à s'authentifier.
- Si vous utilisez un numéro de rappel, vous devez entrer la chaîne sensible à la casse suivante : *msRADIUSCallbackNumber.*
- D'après les recommandations de Microsoft, il vaut mieux utiliser les groupes globaux avec les comptes d'utilisateurs, non les groupes locaux de domaines.

Implémentation de l'authentification à distance RADIUS

RADIUS (Remote Authentication Dial-in User Service) est un protocole d'authentification, d'autorisation et de gestion destiné aux applications d'accès aux réseaux.

Pour utiliser le protocole d'authentification RADIUS :

1. Cliquez sur User Management (Gestion des utilisateurs) > Authentication Settings (Paramètres d'authentification) pour ouvrir la page Authentication Settings.
2. Cliquez sur le bouton radio RADIUS pour activer la section RADIUS de la page.
3. Cliquez sur l'icône RADIUS pour développer la section RADIUS de la page.

4. Dans les champs Primary Radius Server (Serveur Radius principal) et Secondary Radius Server (Serveur Radius secondaire), entrez l'adresse IP des serveurs d'authentification à distance principal et secondaire facultatif, respectivement (256 caractères au plus).
5. Dans les champs Shared Secret (Secret partagé), entrez le secret du serveur utilisé pour l'authentification (128 caractères au plus).

   Le secret partagé est constitué d'une chaîne de caractères devant être connus à la fois par Dominion KX II et le serveur RADIUS afin de leur permettre de communiquer en toute sécurité. C'est en fait un mot de passe.
6. La valeur par défaut Authentication Port (Port d'authentification) est 1812 mais peut être modifiée si nécessaire.
7. La valeur par défaut Accounting Port (Port de gestion) est 1813 mais peut être modifiée si nécessaire.
8. La valeur Timeout (Délai d'attente) est enregistrée en secondes et le délai d'attente par défaut est 1 seconde, mais peut être modifiée si nécessaire.

   Le délai d'attente correspond au laps de temps utilisé par Dominion KX II pour obtenir une réponse du serveur RADIUS avant d'envoyer une autre requête d'authentification.
9. Le nombre de tentatives par défaut est 3.

   Il s'agit du nombre de tentatives accordées à Dominion KX II pour envoyer une requête d'authentification au serveur RADIUS.
10. Sélectionnez une option dans la liste déroulante Global Authentication Type (Type d'authentification globale) :
    - PAP - Avec le protocole PAP, les mots de passe sont envoyés en texte brut. Le protocole PAP n'est pas interactif. Le nom d'utilisateur et le mot de passe sont envoyés en un ensemble unique de données une fois la connexion établie, et non sous la forme d'une invite de connexion suivie de l'attente d'une réponse.

- CHAP - Avec le protocole CHAP, l'authentification peut être demandée par le serveur à tout moment. Le protocole CHAP est plus sûr que le protocole PAP.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS

Lorsqu'une demande d'authentification RADIUS est acceptée, Dominion KX II détermine les autorisations accordées à un utilisateur donné en fonction des autorisations du groupe auquel il appartient.

Votre serveur RADIUS distant peut fournir ces noms de groupes d'utilisateurs en retournant un attribut, implémenté comme FILTER-ID (ID FILTRE) RADIUS. Le format du FILTER-ID (ID FILTRE) doit être le suivant : Raritan:G{*NOM_GROUPE*} où *NOM_GROUPE* est une chaîne indiquant le nom du groupe auquel l'utilisateur appartient.

Raritan:G{NOM_GROUPE}:D{Numéro de rappel}

ou NOM_GROUPE est une chaîne indiquant le nom du groupe auquel appartient l'utilisateur et Numéro de rappel est le numéro associé au compte de l'utilisateur dont le modem Dominion KX II se servira pour rappeler le compte de l'utilisateur.

Spécifications des échanges de communication RADIUS

Dominion KX II envoie les attributs RADIUS suivants à votre serveur RADIUS :

Attribut	Données
Connexion	
Access-Request (1)	
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-IP-Address (4)	Adresse IP de Dominion KX II.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.
User-Password(2)	Mot de passe chiffré.
Accounting-Request(4)	
Acct-Status (40)	Start(1) - Démarre la gestion.
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-Port (5)	Toujours 0.
NAS-IP-Address (4)	Adresse IP de Dominion KX II.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion

Attribut	Données
Connexion	
Acct-Session-ID (44)	ID de session pour la gestion.
Déconnexion	
Accounting-Request(4)	
Acct-Status (40)	Stop(2) - Met fin à la gestion.
NAS-Port-Type (61)	VIRTUAL (5) pour les connexions réseau.
NAS-Port (5)	Toujours 0.
NAS-IP-Address (4)	Adresse IP de Dominion KX II.
User-Name (1)	Nom d'utilisateur entré dans l'écran de connexion
Acct-Session-ID (44)	ID de session pour la gestion.

Processus d'authentification de l'utilisateur

Lorsque le dispositif est configuré pour authentifier et autoriser des utilisateurs locaux de CC, l'ordre dans lequel les informations d'identification de l'utilisateur sont validées suit le processus ci-après :

L'authentification à distance suit le processus défini dans le diagramme ci-dessous :

Modification d'un mot de passe

Pour modifier votre mot de passe :

1. Sélectionnez User Management (Gestion des utilisateurs) > Change Password (Modifier le mot de passe). La page Change Password (Modifier le mot de passe) s'ouvre.
2. Entrez votre mot de passe actuel dans le champ Old Password (Ancien mot de passe).
3. Entrez un nouveau mot de passe dans le champ New Password. Retapez-le dans le champ Confirm New Password (Confirmer le nouveau mot de passe). Les mots de passe peuvent contenir un maximum de 64 caractères alphanumériques et caractères spéciaux (présents sur un clavier anglais).
4. Cliquez sur OK.
5. Vous recevrez confirmation que le mot de passe a bien été changé. Cliquez sur OK.

Remarque : si des mots de passe sécurisés sont utilisés, cette page affiche des informations sur le format requis pour ces mots de passe. Pour plus d'informations sur les mots de passe et les mots de passe sécurisés, reportez-vous à **Mots de passe sécurisés** *(à la page 212).*

Chapitre 7 Gestion des dispositifs

Dans ce chapitre

Network Settings (Paramètres réseau) 142
Services du dispositif.....147
Paramètres de modem.....151
Configuration des paramètres de date et heure.....153
Gestion des événements.....154
Configuration de l'alimentation 162
Configuration des ports 164

Network Settings (Paramètres réseau)

Utilisez la page Network Settings (Paramètres réseau) pour personnaliser la configuration du réseau (par exemple, adresse IP, port de détection et paramètres de l'interface LAN) de votre unité Dominion KX II.

Deux options permettent de paramétrer votre configuration IP :

- None (Néant) (valeur par défaut) : il s'agit de l'option recommandée (IP statique). Comme Dominion KX II fait partie intégrante de l'infrastructure de votre réseau, vous ne voulez probablement pas que son adresse IP change fréquemment. Cette option vous permet de définir les paramètres de réseau.
- DHCP : avec cette option, l'adresse IP est automatiquement attribuée par un serveur DHCP.

Pour modifier la configuration de réseau :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Mettez à jour les paramètres réseau de base. Reportez-vous à Paramètres réseau de base.
3. Mettez à jour les paramètres relatifs à l'interface LAN. Reportez-vous à Paramètres de l'interface LAN.
4. Cliquez sur OK pour confirmer ces configurations. Si vos modifications nécessitent le redémarrage du dispositif, un message de redémarrage apparaît.

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Rétablir les paramètres par défaut).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Paramètres réseau de base

Ces procédures décrivent comment affecter une adresse IP sur la page Network Settings (Paramètres réseau). Pour obtenir des informations complètes sur tous les champs ainsi que sur le fonctionnement de cette page, reportez-vous à ***Paramètres réseau*** (voir "Network Settings (Paramètres réseau)" à la page 142).

1. Sélectionnez Device Settings (Paramètres du dispositif) > Network (Réseau). La page Network Settings (Paramètres réseau) s'ouvre.
2. Indiquez un nom de dispositif significatif pour votre unité Dominion KX II. 32 caractères alphanumériques au plus, avec des caractères spéciaux valides et aucun espace.
3. Dans la section IPv4, entrez ou sélectionnez les paramètres réseau spécifiques à IPv4 appropriés :
   a. Le cas échéant, entrez l'adresse IP. L'adresse IP par défaut est 192.168.0.192.
   b. Renseignez le champ Subnet Mask (Masque de sous-réseau). Le masque de sous-réseau par défaut est 255.255.255.0.
   c. Renseignez le champ Default Gateway (Passerelle par défaut) si l'option None (Néant) est sélectionnée dans la liste déroulante IP Auto Configuration (Configuration automatique IP).
   d. Renseignez le champ Preferred DHCP Host Name (Nom de l'hôte DHCP privilégié) si l'option DHCP est sélectionnée dans la liste déroulante IP Auto Configuration (Configuration automatique IP).
   e. Sélectionnez une option dans le champ IP Auto Configuration (Configuration automatique IP). Les options suivantes sont disponibles :
   - None (Static IP) (Néant (IP statique)) - Cette option requiert une saisie manuelle des paramètres réseau.

     Il s'agit de l'option recommandée car Dominion KX II est un dispositif d'infrastructure et son adresse IP ne devrait pas changer.
   - DHCP - Le protocole de configuration d'hôte dynamique est utilisé par les ordinateurs mis en réseau (clients) pour obtenir des adresses IP uniques et d'autres paramètres du serveur DHCP.

     Avec cette option, les paramètres réseau sont affectés par le serveur DHCP. Si DHCP est utilisé, entrez le nom d'hôte privilégié (DHCP uniquement). 63 caractères au plus.
4. Si IPv6 doit être utilisé, entrez ou sélectionnez les paramètres réseau spécifiques à IPv6 appropriés dans la section IPv6 :
   a. Cochez la case IPv6 pour activer les champs de la section.

b. Renseignez le champ Global/Unique IP Address (Adresse IP globale/unique). Il s'agit de l'adresse IP affectée à Dominion KX II.

c. Renseignez le champ Prefix Length (Longueur de préfixe). Il s'agit du nombre de bits utilisés dans l'adresse IPv6.

d. Renseignez le champ Gateway IP Address (Adresse IP de la passerelle).

e. Link-Local IP Address (Adresse IP Lien-local). Cette adresse est attribuée automatiquement au dispositif. Elle est utilisée pour la détection de voisins ou en l'absence de routeurs. **Read-Only (Lecture seule)**

f. Zone ID. Ce champ identifie le dispositif auquel l'adresse est associée. **Read-Only (Lecture seule)**

g. Sélectionnez une option dans le champ IP Auto Configuration (Configuration automatique IP). Les options suivantes sont disponibles :

- None (Néant) - Utilisez cette option si vous ne souhaitez pas de configuration IP automatique et préférez définir l'adresse IP vous-même (IP statique). Cette option par défaut est recommandée.

  Lorsqu'elle est sélectionnée pour la configuration IP automatique, les champs Network Basic Settings (Paramètres réseau de base) sont activés : Global/Unique IP Address (Adresse IP globale/unique), Prefix Length (Longueur de préfixe) et Gateway IP Address (Adresse IP de la passerelle). Vous pouvez paramétrer manuellement la configuration IP.

- Router Discovery (Détection de routeur) - Utilisez cette option pour affecter automatiquement des adresses IPv6 ayant une portée « Global » ou « Unique Local » au-delà des adresses « Link Local » qui ne s'appliquent qu'à un sous-réseau connecté directement.

5. Si l'option DHCP est activée et que le champ Obtain DNS Server Address Automatically (Obtenir l'adresse du serveur DNS automatiquement) est accessible, sélectionnez-le. Les données DNS fournies par le serveur DHCP seront alors utilisées.

6. Si l'option Use the Following DNS Server Addresses (Utiliser les adresses de serveurs DNS suivantes) est activée, que DHCP soit sélectionné ou non, les adresses saisies dans cette section seront utilisées pour la connexion au serveur DNS.

   Entrez les données suivantes si l'option Following DNS Server Addresses (Utiliser les adresses de serveurs DNS suivantes) est activée. Il s'agit des adresses DNS primaire et secondaire qui seront utilisées si la connexion au serveur DNS primaire est perdue lors d'une panne.

a. Adresse IP du serveur DNS primaire

b. Adresse IP du serveur DNS secondaire.

7. Lorsque vous avez terminé, cliquez sur OK. Le dispositif Dominion KX II est maintenant accessible depuis le réseau.

Reportez-vous à ***Paramètres de l'interface LAN*** (à la page 146) pour plus d'informations sur la configuration de cette section de la page Network Settings (Paramètres réseau).

Remarque : dans certains environnements, le paramètre par défaut du champ LAN Interface Speed & Duplex (Vitesse d'interface LAN & Duplex), Autodetect (auto-détection), ne définit pas correctement les paramètres réseau, ce qui entraîne des problèmes sur le réseau. Dans ce cas, paramétrez le champ LAN Interface Speed & Duplex (Vitesse & Duplex de l'interface LAN) de Dominion KX II sur 100 Mbps/Full Duplex (Bidirectionnel simultané) (ou toute option appropriée à votre réseau) pour résoudre le problème. Reportez-vous à la page **Paramètres réseau** *(voir "Network Settings (Paramètres réseau)" à la page 142) pour plus d'informations.*

Paramètres de l'interface LAN

1. Les paramètres actuels sont identifiés dans le champ Current LAN interface parameters (Paramètres actuels de l'interface LAN).
2. Renseignez le champ LAN Interface Speed & Duplex (Vitesse et duplex de l'interface LAN) en sélectionnant une des options suivantes :
   - Autodetect (Détection automatique) (option par défaut)
   - 10 Mbps/Half - Les deux témoins clignotent.
   - 10 Mbps/Full - Les deux témoins clignotent.
   - 100 Mbps/Half - Le témoin jaune clignote.
   - 100 Mbps/Full - Le témoin jaune clignote.
   - 1000 Mbps/Full (gigabit) - Le témoin vert clignote.
   - Half-duplex permet la communication dans les deux directions, mais seulement une direction à la fois (non simultanément).
   - Full-duplex permet la communication dans les deux directions simultanément.

   Remarque : des problèmes surviennent parfois lors de l'exécution à 10 Mbps en half duplex ou en full duplex. Dans ce cas, essayez un autre paramètre de vitesse et de duplex.

   Reportez-vous à ***Paramètres de vitesse réseau*** (à la page 299) pour plus d'informations.
3. Cochez la case Enable Automatic Failover (Activer le basculement automatique) pour permettre à Dominion KX II de récupérer automatiquement sa connexion réseau via un second port réseau en cas de panne du port réseau actif.

   Remarque : les ports de basculement n'étant pas activés avant un basculement effectif, Raritan recommande de ne pas surveiller ces ports ou de le faire après un basculement.

   Lorsque cette option est activée, les deux champs ci-après sont utilisés :
   - Ping Interval (seconds) - L'intervalle ping détermine la fréquence à laquelle Dominion KX II vérifie l'état du chemin réseau d'accès à la passerelle désignée. L'intervalle ping par défaut est de 30 secondes.
   - Timeout (seconds) - La temporisation détermine la durée pendant laquelle une passerelle désignée reste injoignable via la connexion réseau avant qu'un basculement ne se produise.

Remarque : l'intervalle ping et la temporisation peuvent être configurés pour répondre au mieux aux conditions du réseau local. La temporisation doit être définie pour permettre la transmission de deux demandes ping au moins et le retour des réponses. Par exemple, si une fréquence élevée de basculement est observée en raison d'une utilisation importante du réseau, la temporisation doit être prolongée pour atteindre trois ou quatre fois l'intervalle ping.

4. Sélectionnez la bande passante parmi les options suivantes :
   - 100 Megabit
   - 10 Megabit
   - 5 Megabit
   - 2 Megabit
   - 512 Kilobit
   - 256 Kilobit
   - 128 Kilobit
5. Cliquez sur OK pour appliquer les paramètres LAN.

Services du dispositif

1. Sélectionnez Device Settings (Paramètres du dispositif) > Device Services (Services du dispositif). La page de paramétrage Device Services (Services du dispositif) apparaît.
2. Renseignez le champ Discovery Port (Port de détection).

   La détection de Dominion KX II s'effectue sur un port TCP unique et configurable. Le port par défaut est le port 5000 mais vous pouvez configurer ce paramètre de manière à utiliser le port TCP de votre choix à l'exception des ports 80 et 443. Pour accéder à Dominion KX II par-delà un pare-feu, les paramètres du pare-feu doivent permettre la communication bidirectionnelle par l'intermédiaire du port 5000 par défaut ou d'un autre port configuré ici.
3. Cochez la case Enable SSH Access (Activer l'accès SSH) pour permettre aux administrateurs d'accéder à Dominion KX II via l'application SSH v2.
4. Renseignez le champ SSH Port. Le numéro de port TCP SSH standard est 22 mais ce numéro peut être changé pour offrir un niveau supérieur d'opérations de sécurité.

5. Sélectionnez Enable Direct Port Access via URL (Autoriser l'accès direct aux ports via URL) pour permettre aux utilisateurs d'accéder directement à une cible via Dominion KX II en indiquant les paramètres nécessaires dans l'URL. Ceci permet aux utilisateurs d'éviter les pages de connexion et d'accès aux ports du dispositif. Cette fonction permet également d'entrer un nom d'utilisateur et un mot de passe directement, et d'accéder à la cible si le nom d'utilisateur et le mot de passe ne sont pas contenus dans l'URL. Reportez-vous à ***Présentation de l'accès direct aux ports*** (à la page 149) pour en savoir plus sur les informations d'URL nécessaires.
6. Si vous utilisez le client AKC, vous pouvez activer la fonction Enable AKC Download Server Certificate Validation (Activer la validation du certificat du serveur de téléchargement AKC) en cochant la case ou vous pouvez laisser cette fonction désactivée (par défaut). Reportez-vous à ***Présentation de la fonction Enable AKC Download Server Certificate Validation (Activer la validation du certificat du serveur de téléchargement AKC)*** (voir "Présentation de la fonction Activer la validation du certificat du serveur de téléchargement AKC" à la page 150) pour en savoir plus sur chacune de ces options et sur la procédure à suivre selon l'option choisie.
7. Cliquez sur OK.

Présentation de l'accès direct aux ports

Si vous utilisez VKC et l'accès direct aux ports :

- https://IPaddress/dpa.asp?username=nom d'utilisateur&password=mot de passe&port=numéro de port

Si vous utilisez AKC et l'accès direct aux ports :

- https://IPaddress/dpa.asp?username=nom d'utilisateur&password=mot de passe&port=numéro de port

Où :

- Nom d'utilisateur et mot de passe sont facultatifs. S'ils ne sont pas fournis, une boîte de dialogue de connexion apparaît et, après avoir été authentifié, l'utilisateur est connecté directement à la cible.
- Le port peut être un numéro ou un nom de port. Si vous utilisez un nom de port, il doit être unique ou une erreur est signalée. Si le port est totalement omis, une erreur est signalée.
- Pour les châssis de lames, le port est désigné par <numéro de port>'-'<numéro de connecteur>. Par exemple, 1-2 pour un châssis de lames connecté au port 1, connecteur 2.
- Client=akc est facultatif sauf si vous utilisez un client AKC. Si client=akc n'est pas inclus, VKC est utilisé comme client.

Présentation de la fonction Activer la validation du certificat du serveur de téléchargement AKC

Si vous utilisez le client AKC, vous pouvez décider d'utiliser ou non la fonction Activer la validation du certificat du serveur de téléchargement AKC.

Option 1 : vous n'activez pas la validation du certificat du serveur de téléchargement AKC (paramètre par défaut)

Si vous n'activez pas la fonction Activer la validation du certificat du serveur de téléchargement AKC, tous les utilisateurs de KX II et du client de signets et d'accès CC-SG doivent :

- Vérifiez que les cookies de l'adresse IP du dispositif auquel vous accédez ne sont pas bloqués.
- Les utilisateurs de serveurs Windows Vista, Windows 7 et Windows 2008 doivent s'assurer que l'adresse IP du dispositif auquel ils accèdent est incluse dans la zone Sites approuvés de leur navigateur et que le mode protégé n'est pas activé lors de l'accès au dispositif.

Option 2 : vous activez la validation du certificat du serveur de téléchargement AKC

Si vous n'activez pas cette fonction :

- Les administrateurs doivent téléverser un certificat auto-signé sur Dominion KX II ou en générer un sur Dominion KX II. Le certificat auto-signé doit désigner un hôte valide.
- Chaque utilisateur doit ajouter ce certificat dans la liste des autorités de certification de confiance de son navigateur.

Pour installer le certificat auto-signé lorsque vous utilisez Windows Vista et Windows 7 :

1. Incluez l'adresse IP de Dominion KX II dans la zone des sites de confiance et désactivez le mode protégé.
2. Lancez Internet Explorer en utilisant l'adresse IP de Dominion KX II comme URL. Un message d'erreur de certificat s'affiche.
3. Sélectionnez Afficher les certificats.
4. Dans l'onglet Général, cliquez sur Installer le certificat. Le certificat est alors installé dans la liste Autorités de certification racines de confiance.
5. Après l'installation du certificat, l'adresse IP de Dominion KX II peut être retirée de la zone des sites de confiance.

Paramètres de modem

Pour configurer les paramètres de modem :

1. Cliquez sur Device Settings (Paramètres du dispositif) > Modem Settings (Paramètres de modem) pour ouvrir la page Modem Settings.
2. Cochez la case Enable Modem (Activer le modem). Les champs Serial Line Speed (Vitesse de la ligne série) et Modem Init String (Chaîne initiale du modem) sont activés.
3. Le champ Serial Line Speed du modem est paramétré sur 115200. **Lecture seule**
4. Renseignez le champ Modem Init String. Si la chaîne du modem est laissée vide, la chaîne suivante est envoyée par défaut au modem : ATZ OK AT OK.

   Cette information est utilisée pour configurer les paramètres du modem. Comme chaque modem paramètre ces valeurs à sa manière, ce document n'indique pas comme définir ces valeurs. L'utilisateur doit se référer au modem pour créer la chaîne appropriée.

   - Paramètres de modem :
   - Activation du contrôle de flux RTS/CTS (demande pour émettre/prêt à émettre)
   - Envoi de données à l'ordinateur dès la réception de RTS
   - CTS devrait être configuré de manière à abandonner uniquement lorsque le contrôle de flux le demande.
   - DTR devrait être configuré pour les réinitialisations de modem avec basculement DTR.
   - DSR devrait toujours être activé.
   - DCD devrait être configuré comme étant activé après la détection d'un signal porteur. (DCD ne devrait être activé que lorsque la connexion du modem est établie avec le côté distant.)
5. Renseignez le champ Modem Server IPv4 Address (Adresse IPv4 du serveur de modem) et le champ Modem Client IPv4 Address (Adresse IPv4 du client de modem).

   Remarque : les adresses IP des client et serveur du modem doivent provenir du même sous-réseau et ne peuvent pas chevaucher le sous-réseau LAN KX.

6. Cliquez sur OK pour appliquer vos changements ou sur Reset to Defaults (Restaurer les paramètres par défaut) pour rétablir les valeurs par défaut des paramètres.

Reportez-vous à ***Modems certifiés*** (à la page 289) pour plus d'informations sur les modems certifiés qui fonctionnent avec Dominion KX II. Pour plus d'informations sur les paramètres qui permettront les meilleures performances lors de la connexion à Dominion KX II par modem, reportez-vous à Création, modification et suppression des profils dans MPC - Dispositifs de la deuxième génération dans le **manuel des clients d'accès KVM et série**.

Remarque : l'accès direct par modem à l'interface HTML de Dominion KX II n'est pas prise en charge. Vous devez utiliser le MPC autonome pour accéder à Dominion KX II par modem.

Configuration des paramètres de date et heure

La page Date/Time Settings (Paramètres de date/heure) permet d'indiquer la date et l'heure de Dominion KX II. Il existe deux méthodes pour ce faire :

- Définir la date et l'heure manuellement ou
- les synchroniser avec un serveur NTP.

Pour définir la date et l'heure :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Date/Time (Date/heure). La page Date/Time Settings (Paramètres de date/heure) s'ouvre.
2. Sélectionnez votre fuseau horaire dans la liste déroulante Time Zone (Fuseau horaire).
3. Pour prendre en compte l'heure d'été, cochez la case Adjust for daylight savings time (Régler selon les changements d'heure).
4. Choisissez la méthode que vous souhaitez utiliser pour définir la date et l'heure :
   - User Specified Time - Sélectionnez cette option pour saisir la date et l'heure manuellement.

     Pour l'option User Specified Time (Heure spécifiée par l'utilisateur), entrez la date et l'heure. Pour l'heure, utilisez le format hh:mm (système de 24 heures).
   - Synchronize with NTP Server - Sélectionnez cette option pour synchroniser la date et l'heure avec le serveur NTP.
5. Pour l'option Synchronize with NTP Server (Synchroniser avec le serveur NTP) :
   a. Entrez une adresse IP dans le champ Primary Time server (Serveur d'horloge principal).
   b. Renseignez le champ Secondary Time server (Serveur d'horloge secondaire). **Facultatif**

6. Cliquez sur OK.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Gestion des événements

La fonction de gestion des événements de Dominion KX II propose un ensemble d'écrans permettant d'activer et de désactiver l'envoi d'informations sur les événements système vers des gestionnaires SNMP, Syslog et le journal d'audit. Ces événements sont regroupés dans différentes catégories et vous pouvez décider d'envoyer chacun vers une ou plusieurs destinations.

Configuration de la gestion des événements - Paramètres

Configuration SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole qui gouverne la gestion du réseau et la surveillance des dispositifs réseau ainsi que leurs fonctions. Dominion KX II offre la prise en charge de l'agent SNMP via la fonction Event Management (Gestion des événements).

Pour configurer SNMP (permettre la journalisation de SNMP) :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Event Management - Settings (Gestion des événements - Paramètres). La page Event Management - Settings (Gestion des événements - Paramètres) s'ouvre :
2. Sélectionnez SNMP Logging Enabled (Journalisation SNMP activée). Les champs SNMP sont alors activés.
3. Dans les champs Name (Nom), Contact et Location (Emplacement), entrez respectivement le nom de l'agent SNMP (nom du dispositif) tel qu'il apparaît dans l'interface de la console Dominion KX II, un contact pour cette unité et l'emplacement physique de l'unité Dominion.
4. Renseignez le champ Agent Community String (Chaîne de communauté de l'agent) (la chaîne du dispositif). Une communauté SNMP est le groupe auquel les dispositifs et les postes de gestion exécutant SNMP appartiennent. Elle aide à définir le destinataire des informations. Le nom de la communauté permet d'identifier le groupe. Le dispositif ou agent SNMP peut appartenir à plusieurs communautés SNMP.
5. Spécifiez si la communauté est en lecture seule ou en lecture-écriture à l'aide de la liste déroulante Type.
6. Configurez jusqu'à cinq gestionnaires SNMP en renseignant les champs Destination IP/Host Name, Port # et Community.
7. Cliquez sur le lien « Click here to view the Dominion SNMP MIB » (Cliquez ici pour afficher le MIB SNMP de Dominion) pour accéder à la base des informations de gestion SNMP.
8. Cliquez sur OK.

Pour configurer Syslog (activer le transfert Syslog) :

1. Sélectionnez Enable Syslog Forwarding (Activer le transfert Syslog) pour consigner les messages du dispositif sur un serveur Syslog distant.
2. Entrez l'adresse IP-nom d'hôte de votre serveur Syslog dans le champ IP Address.

3. Cliquez sur OK.

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Remarque : les adresses IPv6 ne peuvent pas comporter plus de 80 caractères pour le nom d'hôte.

Gestion des événements - Destinations

Les événements système, si l'option System events est activée, peuvent générer des événements de notification SNMP (traps) ou être consignés dans Syslog ou dans le journal d'audit. Utilisez la page Event Management - Destinations (Gestion des événements - Destinations) pour sélectionner les événements système à suivre et l'emplacement vers lequel envoyer les informations.

Remarque : des traps SNMP seront générés uniquement si l'option SNMP Logging Enabled (Journalisation SNMP activée) est sélectionnée. Des événements Syslog seront générés uniquement si l'option Enable Syslog Forwarding (Activer le transfert Syslog) est sélectionnée. Ces deux options se trouvent sur la page Event Management - Settings (Gestion des événements - Paramètres). Reportez-vous à Configuration de la gestion des événements - Paramètres).

Pour sélectionner des événements et leurs destinations :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Event Management - Destinations (Gestion des événements - Destinations). La page correspondante s'ouvre.

   Les événements système sont regroupés en plusieurs catégories : Device Operation (Opération sur les dispositifs), Device Management (Gestion des dispositifs), Security, User Activity et User Group Administration.

2. Cochez les cases en regard des éléments de la ligne d'événement pour indiquer ceux que vous souhaitez activer ou désactiver, et pour préciser l'emplacement où vous souhaitez envoyer les informations.

   Conseil : activez ou désactivez des catégories entières en sélectionnant ou désélectionnant les cases Category (Catégorie).

3. Cliquez sur OK.

Home > Device Settings > Event Management - Destinations Logout

Event Management - Destinations

Note: SNMP traps will only be generated if the "SNMP Logging Enabled" option is checked. Similarly, Syslog events will only be generated if the "Enable Syslog Forwarding" option is checked. These options can be found on the "Event Management - Settings" page on the Device Settings menu.

Category	Event	SNMP	Syslog	Audit Log
Device Operation		☑	☑	☑
	System Startup	☑	☑	☑
	System Shutdown	☑	☑	☑
	Power Supply Status Changed	☑	☑	☑
	Powerstrip Outlet Status Changed	☑	☑	☑
	Network Parameter Changed	☑	☑	☑
	Port Status Changed	☑	☑	☑
	Network Failure			☑
	Ethernet Failover	☑	☑	☑
Device Management		☑	☑	☑
	FactoryReset	☑	☑	☑
	Begin CC Control	☑	☑	☑
	End CC Control	☑	☑	☑
	Device Update Started	☑	☑	☑
	Device Update Completed	☑	☑	☑
	Device Update Failed	☑	☑	☑
	Firmware Update Failed	☑	☑	☑
	Firmware File Discarded	☑	☑	☑
	Firmware Validation Failed	☑	☑	☑
	Configuration Backed Up	☑	☑	☑
	Configuration Restored	☑	☑	☑
	Port Connection Denied	☑	☑	☑
Security		☑	☑	☑
	Password Settings Changed	☑	☑	☑
	Login Failed	☑	☑	☑
	Password Changed	☑	☑	☑
	User Blocked		☑	☑
User Activity		☑	☑	☑
	Port Connected	☑	☑	☑
	Port Disconnected	☑	☑	☑

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur Reset to Defaults (Réinitialiser les valeurs par défaut).

Avertissement : lorsque vous utilisez les traps SNMP via UDP, il est possible que Dominion KX II et le routeur auquel elle est reliée se désynchronisent au moment où Dominion KX II redémarre, ce qui empêche le trap SNMP du redémarrage terminé d'être enregistré.

Configuration des agents SNMP

Les dispositifs conformes à SNMP, appelés agents, stockent les données qui les concernent dans des bases de données MIB et renvoient ces données aux gestionnaires SNMP. La page Event Logging (Journalisation des événements) permet de configurer la connexion SNMP entre Dominion KX II (agent SNMP) et un gestionnaire SNMP.

Configuration des traps SNMP

SNMP permet d'envoyer des traps, ou notifications, pour prévenir un administrateur qu'une ou plusieurs conditions ont été remplies. Le tableau suivant répertorie les traps SNMP de Dominion KX II :

Nom de trap	Description
bladeChassisCommError	Une erreur de communication avec le dispositif avec châssis de lames connecté à ce port a été détectée. *Remarque : pas de prise en charge par KX II-101.*
configBackup	La configuration du dispositif a été sauvegardée.
configRestore	La configuration du dispositif a été restaurée.
deviceUpdateFailed	La mise à jour du dispositif a échoué.
deviceUpgradeCompleted	Dominion KX II a effectué la mise à jour via un fichier RFP.
deviceUpgradeStarted	Dominion KX II a commencé la mise à jour via un fichier RFP.
factoryReset	Les valeurs par défaut usine du dispositif ont été rétablies.
firmwareFileDiscarded	Le fichier du firmware a été rejeté.
firmwareUpdateFailed	La mise à jour du firmware a échoué.
firmwareValidationFailed	La validation du firmware a échoué.
groupAdded	Un groupe a été ajouté au système Dominion KX II.
groupDeleted	Un groupe a été supprimé du système.

Nom de trap	Description
groupModified	Un groupe a été modifié.
ipConflictDetected	Un conflit d'adresse IP a été détecté.
ipConflictResolved	Un conflit d'adresse IP a été résolu.
networkFailure	Une interface Ethernet du produit ne peut plus communiquer via le réseau.
networkParameterChanged	Une modification a été appliquée aux paramètres réseau.
passwordSettingsChanged	Les paramètres des mots de passe sécurisés ont été modifiés.
portConnect	Un utilisateur authentifié au préalable a démarré une session KVM.
portConnectionDenied	Une connexion au port cible a été refusée.
portDisconnect	Un utilisateur engagé dans une session KVM ferme la session correctement.
portStatusChange	Le port n'est plus disponible.
powerNotification	Notification de l'état de la prise d'alimentation : 1=Active, 0=Inactive.
powerOutletNotification	Notification de l'état d'une prise de barrette d'alimentation.
rebootCompleted	Le redémarrage de Dominion KX II est terminé.
rebootStarted	Dominion KX II a commencé à redémarrer lors de l'alimentation cyclique du système ou lors d'un redémarrage à chaud à partir du système d'exploitation.
securityViolation	Violation de sécurité.
startCCManagement	Le dispositif a été placé sous la gestion de CommandCenter.
stopCCManagement	Le dispositif a été retiré de la gestion de CommandCenter.
userAdded	Un utilisateur a été ajouté au système.
userAuthenticationFailure	Un utilisateur a essayé de se connecter sans nom d'utilisateur et/ou mot de passe corrects.
userConnectionLost	Un utilisateur avec une session active a subi une interruption anormale de session.
userDeleted	Un compte d'utilisateur a été supprimé.
userForcedLogout	Un utilisateur a été déconnecté de force par

Nom de trap	Description
	Admin.
userLogin	Un utilisateur s'est connecté à Dominion KX II et a été authentifié.
userLogout	Un utilisateur s'est déconnecté correctement de Dominion KX II.
userModified	Un compte d'utilisateur a été modifié.
userPasswordChanged	Cet événement est déclenché lorsque le mot de passe de n'importe quel utilisateur du dispositif est modifié.
userSessionTimeout	Un utilisateur avec une session active a subi une interruption de session en raison du délai d'attente.
userUploadedCertificate	Un utilisateur a téléversé un certificat SSL.
vmImageConnected	Un utilisateur a tenté de monter un dispositif ou une image sur la cible à l'aide de la fonction Support virtuel. Pour chaque tentative de mappage (montage) de dispositif/image, cet événement est généré.
vmImageDisconnected	Un utilisateur a tenté de démonter un dispositif ou une image sur la cible à l'aide de la fonction Support virtuel.

Configuration de l'alimentation

L'unité Dominion KX II offre une double alimentation. Elle peut détecter et indiquer automatiquement l'état de ces alimentations. Utilisez la page Power Supply Setup (Configuration de l'alimentation) pour préciser si vous utilisez une source d'alimentation ou deux. Une configuration appropriée garantit l'envoi de notifications adéquates par Dominion KX II en cas de panne de courant. Par exemple, si l'alimentation numéro un tombe en panne, le voyant d'alimentation situé à l'avant de l'unité devient rouge.

Pour activer la détection automatique des alimentations utilisées :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Power Supply Setup (Configuration de l'alimentation). La page Power Supply Setup s'ouvre.

2. Si vous branchez une arrivée électrique dans l'alimentation numéro un (la plus à gauche à l'arrière de l'unité), sélectionnez l'option PowerIn1 Auto Detect (Détection automatique PowerIn1).
3. Si vous branchez une arrivée électrique dans l'alimentation numéro deux (la plus à droite à l'arrière de l'unité), sélectionnez l'option PowerIn2 Auto Detect (Détection automatique PowerIn2).
4. Cliquez sur OK.

Remarque : si l'une de ces cases est cochée et l'arrivée électrique n'est pas branchée, le voyant d'alimentation sur la partie avant de l'unité devient rouge.

Pour désactiver la détection automatique :

- Désélectionnez la case correspondant à la source d'alimentation appropriée.

Pour réinitialiser les valeurs par défaut usine :

- Cliquez sur le bouton Reset to Defaults (Rétablir les valeurs par défaut).

Remarque : Dominion KX II NE génère PAS de rapport sur l'état de l'alimentation pour CommandCenter. Dominion I (génération 1), en revanche, établit des rapports sur l'état d'alimentation pour CommandCenter.

Configuration des ports

La page Port Configuration (Configuration des ports) affiche la liste des ports de l'unité Dominion KX II. Les ports connectés aux serveurs cible KVM (serveurs lames et standard) et aux barrettes d'alimentation sont affichés en bleu et peuvent être modifiés. Pour les ports sans CIM connecté ou pour lesquels le nom de CIM est vide, un nom de port par défaut Dominion-KX2_Port# est attribué, où Port# est le numéro du port physique de Dominion KX II.

Pour accéder à la configuration d'un port :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports). La page Port Configuration s'ouvre.

Port Number	Port Name	Port Type
1	Dominion-KX2_Port1	Not Available
2	Dominion-KX2_Port2	Not Available
3	Dominion-KX2_Port3	Not Available
4	Dominion-KX2_Port4	Not Available
5	JLtestPC	DCIM
6	Dominion-KX2_Port6	Not Available
7	Dominion-KX2_Port7	Not Available
8	Dominion-KX2_Port8	Not Available
9	Local Port	VM
10	Dominion-KX2_Port10	Not Available
11	Dominion-KX2_Port11	Not Available
12	Dominion-KX2_Port12	Not Available
13	Dominion-KX2_Port13	Not Available
14	Dominion-KX2_Port14	Not Available
15	Dominion-KX2_Port15	Not Available
16	PowerStrip	PowerStrip

Cette page est affichée initialement par ordre de numéros de port, mais elle peut être triée sur n'importe quel champ en cliquant sur son en-tête de colonne.

- Port Number (Numéro de port) - Les ports sont numérotés de 1 au nombre total de ports disponibles pour le dispositif Dominion KX II.

- Port Name - Nom attribué au port. Un nom de port affiché en noir indique que ce nom ou ce port ne peut pas être modifié. Les noms de port affichés en bleu sont modifiables.

Remarque : n'utilisez pas d'apostrophe pour le nom de port (CIM).

- Port Type (Type de port)

Type de port	Description
DCIM	CIM Dominion
Non disponible	Aucun CIM connecté
PCIM	CIM Paragon
PowerStrip	CIM d'alimentation
VM	CIM de support virtuel (D2CIM-VUSB et D2CIM-DVUSB)
Châssis de lames	Châssis de lames et les lames qui lui sont associées (affichés dans un ordre hiérarchique).

2. Cliquez sur le nom du port que vous souhaitez modifier.
   - Pour les ports KVM, la page Port s'ouvre. A partir de cette page, vous pouvez nommer les ports et créer des associations d'alimentation.
   - Pour les barrettes d'alimentation, la page Port relative aux barrettes d'alimentation s'ouvre. Sur cette page, vous pouvez nommer les barrettes d'alimentation et leurs prises.

Configuration des serveurs cible standard

Pour nommer les serveurs cible :

1. Connectez tous les serveurs cible si vous ne l'avez pas encore fait. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 29) pour obtenir une description de la connexion de l'équipement.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports). La page Port Configuration s'ouvre.
3. Cliquez sur le nom du port du serveur cible que vous souhaitez renommer. La page Port s'ouvre.
4. Attribuez un nom au serveur connecté à ce port. Ce nom peut contenir jusqu'à 32 caractères alphanumériques et spéciaux.
5. Cliquez sur OK.

Configuration des cibles des barrettes d'alimentation (PDU de rack)

KX II vous permet de connecter des barrettes d'alimentation (PDU de rack) aux ports KX II. La configuration des barrettes d'alimentation KX II s'effectue sur la page KX II Port Configuration.

Branchement d'une barrette d'alimentation

Les barrettes d'alimentation des séries PX et RPC de Raritan sont connectées à KX II à l'aide du CIM D2CIM-PWR. Le diagramme de la présente section utilise une unité PX comme exemple.

Pour brancher la barrette d'alimentation :

1. Branchez la fiche RJ-45 mâle du D2CIM-PWR au connecteur RJ-45 femelle du port série de la barrette d'alimentation.
2. Branchez la fiche RJ-45 femelle du D2CIM-PWR à l'un des connecteurs de port système femelle disponible sur l'unité KX II à l'aide d'un câble Cat5 à brochage direct.
3. Reliez un cordon d'alimentation CA au serveur cible et à une prise de barrette d'alimentation disponible.
4. Branchez la barrette à une source d'alimentation CA.

5. Mettez le dispositif sous tension.

Appellation des barrettes d'alimentation de KX II (page Port pour les barrettes d'alimentation)

Remarque : Les barrettes d'alimentation PX peuvent être nommées dans l'unité PX, ainsi que dans l'unité KX II.

La page Port s'ouvre lorsque vous sélectionnez un port dans la page Port Configuration (Configuration des ports), ce port étant connecté à une barrette d'alimentation distante Raritan. Les champs Type et Name (Nom) sont déjà renseignés.

Remarque : Le champ Type (CIM) ne peut pas être modifié.

Les informations suivantes s'affichent pour chaque prise de la barrette d'alimentation : numéro, nom et association de port de la prise.

Utilisez cette page pour nommer la barrette d'alimentation et ses prises. Tous les noms peuvent contenir jusqu'à 32 caractères alphanumériques maximum et inclure des caractères spéciaux.

Remarque : lorsqu'une barrette d'alimentation est associée à un serveur cible (port), le nom de la prise est remplacé par le nom du serveur cible (même si vous attribuez un autre nom à la prise).

Pour nommer la barrette d'alimentation (et les prises) :

Remarque : CommandCenter Service Gateway ne reconnaît pas les noms de barrette d'alimentation contenant des espaces.

1. Entrez le nom de la barrette d'alimentation (le cas échéant).
2. Modifiez le nom (de la prise) si vous le souhaitez. (Le nom par défaut d'une prise est son numéro.)

3. Cliquez sur OK.

Association de prises aux serveurs cible sur KX II

La page Port s'ouvre lorsque vous cliquez sur un port sur la page Port Configuration (Configuration des ports). A partir de cette page, vous pouvez créer des associations d'alimentation, remplacer le nom du port par un nom plus évocateur et mettre à jour les paramètres de serveur cible si vous utilisez le CIM D2CIM-VUSB. Les champs (CIM) Type et (Port) Name sont déjà renseignés ; notez que le type de CIM ne peut pas être modifié.

Un serveur peut disposer de quatre prises d'alimentation au plus et vous pouvez associer une barrette d'alimentation différente à chacune d'elle. A partir cette page, définissez les associations de façon à effectuer la mise sous tension, hors tension et l'alimentation cyclique du serveur sur la page Port Access.

Pour utiliser cette fonction, vous avez besoin :

- de barrettes d'alimentation Raritan
- de CIM d'alimentation (D2CIM-PWR).

Pour créer des associations d'alimentation (associer les prises des barrettes d'alimentation aux serveurs cible KVM) :

Remarque : lorsqu'une barrette d'alimentation est associée à un serveur cible (port), le nom de la prise est remplacé par le nom du serveur cible (même si vous avez attribué un autre nom à la prise).

1. Sélectionnez la barrette d'alimentation dans la liste déroulante Power Strip Name (Nom de barrette d'alimentation).
2. Pour cette barrette d'alimentation, sélectionnez la prise dans la liste déroulante Outlet Name.
3. Répétez les étapes 1 et 2 pour chaque association d'alimentation voulue.
4. Cliquez sur OK. Un message de confirmation s'affiche.

Pour modifier le nom du port :

1. Tapez un nom évocateur dans le champ Name. Par exemple, vous pouvez utiliser le nom du serveur cible. Ce nom peut comporter 32 caractères alphanumériques au plus et inclure des caractères spéciaux.
2. Cliquez sur OK.

Suppression des associations d'alimentation

Si vous déconnectez des serveurs cible et/ou des barrettes d'alimentation de l'unité KX II, toutes les associations d'alimentation doivent être au préalable supprimées. Lorsqu'une cible a été associée à une barrette d'alimentation et que la première est retirée de KX II, l'association d'alimentation demeure. Lorsque cela se produit, vous ne pouvez pas accéder à la configuration des ports de ce serveur cible déconnecté dans Device Settings (Paramètres du dispositif) pour supprimer correctement l'association d'alimentation.

Pour supprimer l'association d'une barrette d'alimentation :

1. Sélectionnez la barrette d'alimentation appropriée dans la liste déroulante Power Strip Name.
2. Pour cette barrette d'alimentation, sélectionnez la prise appropriée dans la liste déroulante Outlet Name.
3. Sélectionnez None dans la liste déroulante Outlet Name.
4. Cliquez sur OK. Cette association barrette d'alimentation-prise est supprimée et un message de confirmation s'affiche.

Pour supprimer une association de barrette d'alimentation lorsque cette dernière a été retirée de la cible :

1. Cliquez sur Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports), puis sur la cible active.
2. Associez la cible active au port d'alimentation déconnecté. Cette action rompt l'association d'alimentation de la cible déconnectée.
3. Associez ensuite la cible active au port d'alimentation correct.

Configuration des châssis de lames

Outre les serveurs standard et les barrettes d'alimentation, Dominion KX II permet de gérer les châssis de lames branchés sur un port de Dominion KX II. Huit châssis de lames au plus peuvent être gérés via Dominion KX II à un moment donné.

Comme avec les serveurs standard, les châssis de lames sont détectés automatiquement par Dominion KX II lorsqu'ils sont connectés. Lorsqu'un châssis de serveurs lames est détecté par Dominion KX II, un nom par défaut lui est attribué et il s'affiche sur la page Port Access avec les serveurs cible standard et les barrettes d'alimentation (reportez-vous à ***Page Port Access*** (à la page 46)). Le châssis de lames s'affiche dans une liste hiérarchique extensible sur la page Port Access ; le châssis de lames est placé à la racine de la hiérarchie et chaque lame est libellée et affichée sous la racine.

Remarque : pour afficher le châssis de lames dans l'ordre hiérarchique, ses sous-types doivent être configurés.

A l'exception des châssis de lames HP, les châssis de lames génériques, IBM et Dell sont configurés sur la page Port. Le port connecté au châssis de lames doit être configuré avec le modèle du châssis. Les informations spécifiques que vous pouvez configurer dépendent de sa marque du serveur lames que vous utilisez. Pour obtenir des informations particulières concernant chaque châssis de lame pris en charge, reportez-vous à la rubrique correspondante dans cette section de l'aide.

Les châssis de lames ci-après sont pris en charge :

- IBM BladeCenter modèles E et H
- Dell PowerEdge 1855, 1955 et M1000e

Une option Generic permet de configurer un châssis de lame qui ne figure pas dans la liste qui précède. HP BladeSystem c3000 et c7000 sont pris en charge via des connexions individuelles de Dominion KX II pour chaque lame. Les ports sont regroupés dans une représentation de châssis à l'aide de la fonction Port Group Management (Gestion des groupes de ports).

Remarque : les lames Dell PowerEdge 1855/1955 permettent également une connexion de chaque lame à un port de Dominion KX II. Dans ce cas, les lames peuvent également être rassemblées pour créer des groupes de serveurs lames.

Deux modes d'opération sont possibles pour les châssis de lames : la configuration manuelle et la détection automatique, selon les capacités du châssis de lames. Lorsqu'un châssis de lames est configuré pour la détection automatique, Dominion KX II effectue un suivi et une mise à jour les actions suivantes :

- lorsqu'un nouveau serveur lame est ajouté au châssis ;
- lorsqu'un serveur lame existant est retiré du châssis.

Remarque : Dans le cas des modèles E et H d'IBM Blade Center, Dominion KX II prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

Dominion KX II prend également en charge l'utilisation des séquences de raccourcis-clavier pour commuter l'accès KVM sur un châssis de lames. Lorsqu'un châssis de lames permet aux utilisateurs de sélectionner une séquence de raccourcis-clavier, ces options seront fournies sur la page Port Configuration. Lorsqu'un châssis de lames est fourni avec des séquences de raccourcis-clavier prédéfinies, ces séquences seront entrées sur la page Port Configuration lorsque le châssis sera sélectionné. Par exemple, la séquence de raccourcis-clavier pour commuter l'accès KVM sur une unité IBM BladeCenter H est Verr num+ Verr num + Numéro de connecteur, cette séquence est donc appliquée par défaut lorsqu'une unité IBM BladeCenter H est sélectionnée pendant la configuration. Consultez la documentation de votre châssis de lames pour plus d'informations sur les séquences de raccourcis-clavier.

Vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Au niveau du châssis, quatre liens au plus peuvent être définis. Le premier est réservé à la connexion à l'interface utilisateur graphique du module d'administration du châssis de lames. Par exemple, ce lien peut être utilisé par l'assistance technique pour vérifier rapidement la configuration d'un châssis.

Les châssis de lames peuvent être gérés à partir du Virtual KVM Client (VKC) Dominion KX II, Multi-Platform Client (MPC) de Raritan et CC-SG. La gestion des serveurs lames via VKC et MPC est identique à la gestion des serveurs cible standard. Reportez-vous à ***Utilisation des serveurs cible*** (à la page 42) et au **manuel de l'administrateur de CC-SG** pour en savoir plus. Les changements apportés à la configuration du châssis de lames dans Dominion KX II seront reportés dans ces applications clientes.

Important : lorsque le CIM reliant le châssis de lames à Dominion KX II est mis hors tension ou déconnecté de Dominion KX II, toutes les connexions au châssis de lame établies seront abandonnées. Lorsque le CIM est reconnecté ou mis sous tension, vous devrez établir à nouveau les connexions.

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

Configuration des châssis de lames génériques

La sélection de Generic Blade Chassis (Châssis de lames génériques) ne permet qu'une configuration manuelle. Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 190), ***CIM pris en charge pour les châssis de lames*** (à la page 190) et ***Configurations requises et recommandées de châssis de lames*** (à la page 193) pour des informations supplémentaires importantes concernant la configuration des châssis de lames.

1. Connectez le châssis de lames à Dominion KX II. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 29) pour plus d'informations.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez Generic dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames).
6. Configurez le châssis de lames, le cas échéant.
   a. Switch Hot Key Sequence - Définissez la séquence de raccourcis-clavier qui permettra de commuter de KVM au châssis de lames. La séquence de raccourcis-clavier de commutation doit correspondre à celle utilisée par le module KVM dans le châssis de lames.
   b. Administrative Module Primary IP Address/Host Name - Sans objet.
   c. Maximum Number of Slots - Entrez le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames.
   d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.
   e. Username - Sans objet.
   f. Password - Sans objet.
7. Modifiez le nom du châssis de lames, le cas échéant.
8. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.

9. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links ▸ Blade Chassis Managed Links pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

   b. URL - Entrez l'URL de l'interface. **Obligatoire**

   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface. **Facultatif**

   d. Password - Entrez le mot de passe utilisé à accéder à l'interface. **Facultatif**

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

   e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 185) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web. **Facultatif**

10. Les informations de profil USB ne s'appliquent pas à une configuration générique.

11. Cliquez sur OK pour enregistrer la configuration.

Configuration des châssis de lames Dell®

Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 190), ***CIM pris en charge pour les châssis de lames*** (à la page 190) et ***Configurations requises et recommandées de châssis de lames*** (à la page 193) pour des informations supplémentaires importantes concernant la configuration des châssis de lames. Reportez-vous à ***Longueurs de câbles et résolutions vidéo pour châssis Dell*** (à la page 315) pour plus d'informations sur les longueurs de câbles et résolutions vidéo lors de l'utilisation des châssis Dell avec Dominion KX II.

1. Connectez le châssis de lames à Dominion KX II. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 29) pour plus d'informations.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez le modèle de châssis de lames Dell dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames).

Pour configurer un Dell PowerEdge M1000e :

1. Si vous avez sélectionné Dell PowerEdge M1000e, la détection automatique est disponible. Configurez le châssis de lames, le cas échéant. Avant de configurer un châssis de lames pouvant être détecté automatiquement, celui-ci doit accepter les connexions SSH sur le numéro de port désigné (reportez-vous à ***Services du dispositif*** (à la page 147)). De plus, il faut créer au préalable un compte d'utilisateur disposant d'informations d'authentification sur le châssis de lames.
   a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames. La séquence de raccourcis-clavier de commutation doit correspondre à celle utilisée par le module KVM dans le châssis de lames.
   b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.
   c. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames. **Obligatoire pour le mode de détection automatique**

d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Changez ce numéro, le cas échéant. **Obligatoire pour le mode de détection automatique**

e. Username - Entrez le nom d'utilisateur servant à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**

f. Password - Entrez le mot de passe utilisé à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**

2. Si vous souhaitez que Dominion KX II détecte automatique les lames du châssis, cochez la case Blade Auto-Discovery (Détection automatique des lames), puis cliquez sur Discover Blades on Chassis Now (Détecter les lames sur le châssis maintenant). Lorsque les lames sont détectées, elles s'affichent sur la page.

3. Modifiez le nom du châssis de lames, le cas échéant. Si le châssis porte déjà un nom, ce champ est automatiquement renseigné. Sinon, Dominion KX II attribue un nom au châssis. La convention d'appellation apr défaut pour les châssis de lames par Dominion KX II est # Blade_Chassis_Port#.

4. En mode manuel, indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.

   En mode de détection automatique, la case Installed affiche les connecteurs contenant des lames pendant la détection.

5. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links ▸ Blade Chassis Managed Links pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

---

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 195) pour obtenir des exemples de configuration pour le Dell M1000e.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

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

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 185) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

6. Les profils USB ne s'appliquent pas aux châssis Dell.

7. Cliquez sur OK pour enregistrer la configuration.

Pour configurer un Dell PowerEdge 1855/1955 :

1. Si vous avez sélectionné Dell 1855/1955, la détection automatique *n'est pas disponible*. Configurez le châssis de lames, le cas échéant.

   a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames.

   b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.

   c. Administrative Module Primary IP Address/Host Name - Sans objet.

   d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.

   e. Username - Sans objet.

f. Password - Sans objet.

2. Modifiez le nom du châssis de lames, le cas échéant.
3. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.
4. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links ► Blade Chassis Managed Links pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

   a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

   b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 195) pour obtenir des exemples de configuration pour le Dell PowerEdge 1855/1955.

   c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

   d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

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

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 185) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

5. Les profils USB ne s'appliquent pas aux châssis Dell.
6. Cliquez sur OK pour enregistrer la configuration.

Configuration des châssis de lames IBM®

Reportez-vous à ***Modèles de châssis de lames pris en charge*** (à la page 190), ***CIM pris en charge pour les châssis de lames*** (à la page 190) et ***Configurations requises et recommandées de châssis de lames*** (à la page 193) pour des informations supplémentaires importantes concernant la configuration des châssis de lames.

1. Connectez le châssis de lames à Dominion KX II. Reportez-vous à ***Etape 3 : Connexion de l'équipement*** (à la page 29) pour plus d'informations.
2. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports) pour ouvrir la page Port Configuration.
3. Sur cette page, cliquez sur le nom du châssis de lames que vous souhaitez configurer. La page Port s'ouvre.
4. Sélectionnez le bouton radio Blade Chassis. La page affiche alors les champs nécessaires pour configurer un châssis de lames.
5. Sélectionnez le modèle de châssis de lames IBM dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames).

Pour configurer un IBM BladeCenter H et E :

1. Si vous avez sélectionné IBM BladeCenter H ou E, la détection automatique est disponible. Configurez le châssis de lames, le cas échéant. Avant de configurer un châssis de lames pouvant être détecté automatiquement, celui-ci doit accepter les connexions SSH sur le numéro de port désigné (reportez-vous à ***Services du dispositif*** (à la page 147)). De plus, il faut créer au préalable un compte d'utilisateur disposant d'informations d'authentification sur le châssis de lames. Dominion KX II ne prend en charge la détection automatique que pour AMM[1].

   a. Switch Hot Key Sequence - Prédéfinie.

b. Maximum Number of Slots - Le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames est entré automatiquement.

c. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames. **Obligatoire pour le mode de détection automatique**

d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Changez ce numéro, le cas échéant. **Obligatoire pour le mode de détection automatique**

e. Username - Entrez le nom d'utilisateur servant à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**

f. Password - Entrez le mot de passe utilisé à accéder au châssis de lames. **Obligatoire pour le mode de détection automatique**

2. Si vous souhaitez que Dominion KX II détecte automatique les lames du châssis, cochez la case Blade Auto-Discovery (Détection automatique des lames), puis cliquez sur Discover Blades on Chassis Now (Détecter les lames sur le châssis maintenant). Lorsque les lames sont détectées, elles s'affichent sur la page.

3. Modifiez le nom du châssis de lames, le cas échéant. Si le châssis porte déjà un nom, ce champ est automatiquement renseigné. Sinon, Dominion KX II attribue un nom au châssis. La convention d'appellation apr défaut pour les châssis de lames par Dominion KX II est # Blade_Chassis_Port#.

4. En mode manuel, indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames.

   En mode de détection automatique, la case Installed affiche les connecteurs contenant des lames pendant la détection.

5. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links ► Blade Chassis Managed Links pour développer la section sur la page.

   Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

   Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 195) pour obtenir des exemples de configuration pour l'IBM BladeCenter.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

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

---

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 185) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

6. Le cas échéant, définissez le profil USB pour le châssis de lames ou sélectionnez un profil USB existant. Cliquez sur l'icône USB Profiles for Port (Profils USB pour le port) ▸ Select USB Profiles for Port ou sur l'icône Apply Select Profiles to Other Ports (Appliquer les profils sélectionnés aux autres ports) ▸ Apply Selected Profiles to Other Ports pour développer ces sections de la page. Reportez-vous à ***Configuration des profils USB (page Port)*** (à la page 197).

7. Cliquez sur OK pour enregistrer la configuration.

▸ Pour configurer un IBM BladeCenter (autre) :

1. Si vous avez sélectionné IBM BladeCenter (Other), la détection automatique *n'est pas* disponible. Configurez le châssis de lames, le cas échéant.

   a. Switch Hot Key Sequence - Sélectionnez la séquence de raccourcis-clavier qui permettra de commuter de KVM au serveur lames.

b. Administrative Module Primary IP Address/Host Name - Entrez l'adresse IP principale du châssis de lames.Sans objet.

c. Maximum Number of Slots - Entrez le nombre maximum par défaut de connecteurs disponibles sur le châssis de lames.

d. Port Number - Le numéro de port par défaut pour le châssis de lames est 22. Sans objet.

e. Username - Sans objet.

f. Password - Sans objet.

2. Modifiez le nom du châssis de lames, le cas échéant.

3. Indiquez les lames installées dans le châssis en cochant la case Installed pour chaque connecteur contenant une lame. Vous pouvez également utiliser la case à cocher Select All (Tout sélectionner). Le cas échéant, modifiez le nom des serveurs lames. S'ils ne sont pas nommés, Dominion KX II leur attribue un nom. La convention d'appellation par défaut des serveurs lames est # Blade_Chassis_Port#_Slot#.

4. Dans la section Blade Chassis Managed Links (Liens gérés des châssis de lames) de la page, vous pouvez configurer la connexion à l'interface de navigateur Web d'un châssis de lames si elle est disponible. Cliquez sur l'icône Blade Chassis Managed Links

pour développer la section sur la page.

Le premier lien URL sert à la connexion à l'interface graphique utilisateur du module d'administration des châssis de lames.

Remarque : l'accès aux liens URL entrés dans cette section de la page est gouverné par les autorisations d'accès aux ports des châssis de lames.

---

a. Active - Pour activer le lien lorsqu'il est configuré, cochez la case Active. Laissez la case à cocher vide pour que le lien reste inactif. Il est possible de renseigner les champs de lien et d'enregistrer même lorsque l'option Active n'est pas sélectionnée. Lorsque l'option Active est sélectionnée, le champ URL est obligatoire. Les champs de nom d'utilisateur et de mot de passe sont facultatifs suivant qu'une connexion unique est souhaitée ou non.

b. URL - Entrez l'URL de l'interface. Reportez-vous à ***Exemples de formats d'URL de châssis de lames*** (à la page 195) pour obtenir des exemples de configuration pour l'IBM BladeCenter.

c. Username - Entrez le nom d'utilisateur servant à accéder à l'interface.

d. Password - Entrez le mot de passe utilisé à accéder à l'interface.

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

e. Les champs Username et Password, tous les deux facultatifs, contiennent des libellés qui doivent être associés avec les entrées de nom d'utilisateur et de mot de passe. C'est dans ces champs que vous devez entrer des noms pour les champs de nom d'utilisateur et de mot de passe utilisés sur l'écran de connexion pour l'application Web. Vous pouvez visualiser la source HTML de l'écran de connexion pour trouver le *nom* des champs, et non leur libellé. Reportez-vous à ***Astuces pour ajouter une interface Navigateur Web*** (à la page 185) pour obtenir des conseils pour l'ajout d'une interface de navigateur Web.

5. Les profils USB ne sont pas utilisés par les configurations IBM (Other).
6. Cliquez sur OK pour enregistrer la configuration.

Astuces pour ajouter une interface Navigateur Web

Vous pouvez ajouter une interface navigateur Web pour créer une connexion à un dispositif intégrant un serveur Web. Une interface navigateur Web permet également la connexion à une application Web quelconque, telle que celle associée à une carte de processeur RSA, DRAC ou ILO.

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

Pour ajouter une interface navigateur Web :

1. Le nom par défaut d'une interface navigateur Web est fourni. Les cas échéant, vous pouvez modifier le nom dans le champ Name.
2. Entrez l'URL ou le nom du domaine de l'application Web dans le champ URL. Vous devez entrer l'URL à laquelle l'application Web doit lire le nom d'utilisateur et le mot de passe.

   Suivez les exemples ci-après pour entrer des formats corrects :

   - http(s)://192.168.1.1/login.asp
   - http(s)://www.example.com/cgi/login
   - http(s)://example.com/home.html
3. Entrez les nom d'utilisateur et mot de passe autorisant l'accès à cette interface. **Facultatif**

4. Si un nom d'utilisateur et un mot de passe ont été entrés, dans Username Field et Password Field, tapez le nom des champs de nom d'utilisateur et de mot de passe utilisés dans l'écran de connexion de l'application Web. Vous devez visualiser la source HTML de l'écran de connexion pour trouver le nom des champs, et non leur libellé.

Astuce pour repérer le nom des champs :

- Dans le code source HTML de la page de connexion de l'application Web, recherchez le libellé du champ, tel que Username et Password.
- Examinez ensuite le code adjacent pour trouver une balise ressemblant à : name="user". Le mot entre guillemets est le nom du champ.

Configuration des châssis de lames HP® (Gestion des groupes de ports)

Dominion KX II prend en charge l'agrégation des ports connectés à certains types de lames dans un groupe représentant le châssis de lames ; particulièrement, les lames HP BladeServer et Dell PowerEdge 1855/1955 lorsque le DellPowerEdge 1855/1955 est connecté de chaque lame au port sur Dominion KX II.

Le châssis est identifié par un nom de groupe de ports et ce groupe est désigné comme Blade Server Group (Groupe de serveurs lames) sur la page Port Group Management (Gestion des groupes de ports). Les groupes de ports comprennent uniquement des ports configurés comme ports KVM standard, non des ports configurés comme châssis de lames. Un port ne peut être membre que d'un seul groupe.

Les ports connectés aux modules KVM intégrés dans un châssis de lames sont configurés comme sous-types de châssis de lames. Ces ports peuvent être inclus dans des groupes de ports.

Lorsque les ports Dominion KX II sont connectés à des modules KVM intégrés dans un châssis de lames et à des lames individuelles, ils sont configurés comme sous-types de châssis de lames. Ces ports ne peuvent pas être inclus dans des groupes de ports et n'apparaissent pas dans la liste Available (Disponibles) de la section Select Ports for Group (Sélectionner des ports pour le groupe).

Lorsqu'un port KVM standard a été inclus dans un groupe de ports, puis réorienté pour être utilisé comme sous-type de châssis de lames, il doit d'abord être supprimé du groupe de ports.

Les groupes de ports sont restaurés à l'aide de l'option Backup and Restore (Sauvegarde et restauration) (reportez-vous à ***Sauvegarde et restauration*** (voir "Backup and Restore (Sauvegarde et restauration)" à la page 229)).

Pour ajouter un groupe de ports :

1. Cliquez sur Device Settings (Paramètres du dispositif) > Port Group Management (Gestion des groupes de ports) pour ouvrir la page Port Group Management.
2. Cliquez sur le bouton Add (Ajouter) pour ouvrir la page Port Group (Groupe de ports).
3. Entrez un nom de groupe de ports. Les noms de groupes de ports ne sont pas sensibles à la casse et peuvent contenir jusqu'à 32 caractères.
4. Cochez la case Blade Server Group (Groupe de serveurs lames).

   Si vous souhaitez indiquer que ces ports sont reliés à des lames hébergées dans un châssis de lames (par exemple, HP c3000 ou Dell PowerEdge 1855), sélectionnez la case à cocher Blade Server Group.

   Remarque : ceci est particulièrement important pour les utilisateurs de CC-SG qui souhaitent organiser les lames HP par châssis, même si chaque lame a sa propre connexion à un port de Dominion KX II.

5. Cliquez sur un port dans le champ Available (Disponibles) de la section Select Ports for Group (Sélectionner des ports pour le groupe). Cliquez sur Add pour ajouter le port au groupe. Le port est placé dans le champ Selected (Sélectionnés).

6. Cliquez sur OK pour ajouter le groupe de ports.

Pour modifier les informations relatives à un groupe de ports :

1. Sur la page Port Group Management (Gestion des groupes de ports), cliquez sur le lien du groupe de ports que vous souhaitez modifier. La page Port Group (Groupe de ports) s'ouvre.
2. Modifiez les informations selon les besoins.
3. Cliquez sur OK pour enregistrer les modifications.

Pour supprimer un groupe de ports :

1. Cliquez sur la page Port Group Management (Gestion des groupes de ports), cochez la case du groupe de ports que vous souhaitez supprimer.
2. Cliquez sur le bouton Delete (Supprimer).
3. Cliquez sur OK dans le message d'avertissement.

Modèles de châssis de lames pris en charge

Ce tableau présente des modèles de châssis de lames pris en charge par Dominion KX II et les profils correspondant qui devraient être sélectionnés selon le modèle de châssis lors de leur configuration dans l'application Dominion KX II. Une liste de ces modèles peut être sélectionnée sur la page Port Configuration (Configuration des ports) dans la liste déroulante Blade Server Chassis Model (Modèle de châssis de serveurs lames), qui apparaît lorsque le bouton radio Blade Chassis est sélectionné. Pour obtenir des informations concernant la configuration de chaque châssis de lames, reportez-vous à la rubrique correspondante dans cette section de l'aide.

Modèle de châssis de lames	Profil de Dominion KX II
Dell PowerEdge 1855/1955	Dell PowerEdge 1855/1955
Dell PowerEdge M1000e	Dell PowerEdge M1000e
IBM BladeCenter S	IBM (autre)
IBM BladeCenter H	IBM BladeCenter H
IBM BladeCenter T	IBM (autre)
IBM BladeCenter HT	IBM (autre)
IBM BladeCenter E	IBM BladeCenter E
HP	Configurez à l'aide des fonctions de gestion des groupes de ports. Reportez-vous à ***Configuration des châssis de lames HP® (Gestion des groupes de ports)*** (à la page 187).

CIM pris en charge pour les châssis de lames

Les CIM suivants sont pris en charge pour les châssis de lames gérés via Dominion KX II:

- DCIM-PS2
- DCIM-USBG2
- D2CIM-VUSB
- D2CIM-DVUSB

Le tableau suivant contient les CIM pris en charge pour chaque modèle de châssis de lames supporté par Dominion KX II.

Châssis de lames	Méthode de connexion	CIM recommandés
Générique	Si un D2CIM-VUSB ou D2CIM-DVUSB est utilisé lors de la connexion à un châssis de lames configuré en tant que Générique, vous pouvez sélectionner les profils USB sur la page Port Configuration (Configuration des ports) et le menu USB Profile du client. Toutefois, la fonction Support virtuel n'est pas prise en charge pour les châssis de lames génériques et le menu Virtual Media est désactivé sur le client.	• DCIM-PS2 • DCIM-USBG2
Dell PowerEdge 1855	Inclut un des trois modules KVM : • Module de commutateur Ethernet KVM analogique (standard) • Module de commutateur KVM à accès numérique (facultatif) • Module de commutateur KVM (standard sur les systèmes antérieurs à avril 2005) Ces commutateurs présentent un connecteur personnalisé autorisant la connexion de deux dispositifs PS/2 et d'un dispositif vidéo au système. Source : *Manuel d'utilisation de Dell PowerEdge 1855*	• DCIM-PS2
Dell PowerEdge 1955	Un des deux types de modules KVM peut être installé : • Module de commutateur KVM analogique • Module de commutateur KVM à accès numérique Ces deux modules autorisent la connexion d'un clavier, d'une souris et d'un écran PS/2 compatibles au système (à l'aide d'un câble personnalisé fourni avec le système). Source : *Manuel d'utilisation de Dell PowerEdge 1955*	• DCIM-PS2
Dell PowerEdge M1000e	Le module commutateur KVM (iKVM) est intégré à ce châssis. L'iKVM est compatible avec les périphériques suivants : • claviers USB, dispositifs de pointage USB • écrans VGA avec prise en charge DDC Source : *Guide d'utilisation du contrôleur de gestion de châssis Dell, version de*	• DCIM-USBG2

Châssis de lames	Méthode de connexion	CIM recommandés
	firmware 1.0	
HP BladeSystem c3000	Le câble HP c-Class Blade SUV vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des châssis de lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. Source : *Guide de maintenance et de service du serveur lame HP ProLiant BL480c*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (pour un fonctionnement de port KVM standard sans option KVM)
HP BladeSystem c7000	Le câble HP c-Class Blade SUV vous permet d'assurer l'administration, la configuration et les procédures de diagnostic des serveurs lames en reliant des dispositifs vidéo et USB directement à la lame de serveur. Source : *Guide de maintenance et de service du serveur lame HP ProLiant BL480c*	• DCIM-USBG2 • D2CIM-VUSB • D2CIM-DVUSB (pour un fonctionnement de port KVM standard)
IBM BladeCenter S	Le module AMM (de gestion avancée) offre des fonctions de gestion du système et de multiplexage de clavier/vidéo/souris (KVM) pour tous les châssis de lames. Les connexions AMM incluent : un port série, une connexion vidéo, un port de gestion à distance (Ethernet) et deux ports USB v2.0 pour un clavier et une souris. Source : *Mise en œuvre du châssis IBM BladeCenter S*	• DCIM-USBG2
IBM BladeCenter H	Le châssis BladeCenter H est livré en standard avec un module AMM. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter E	Le modèle de châssis actuel BladeCenter E (8677-3Rx) est livré en standard avec un module AMM. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2 • D2CIM-DVUSB
IBM BladeCenter T	Le châssis BladeCenter T est livré en standard avec un module AMM. Contrairement au châssis BladeCenter standard, le module KVM et le module de gestion du châssis BladeCenter T sont des composants distincts. L'avant du module de gestion ne comporte des voyants que pour	• DCIM-PS2

Châssis de lames	Méthode de connexion	CIM recommandés
	l'affichage de l'état. Toutes les connexions Ethernet et KVM sont alimentées par l'arrière aux modules LAN et KVM. Le module KVM est un module à remplacement à chaud à l'arrière du châssis, fournissant deux connecteurs PS/2 pour un clavier et une souris, un panneau d'état du système et un connecteur vidéo HD-15. Source : *Produits et technologie IBM BladeCenter*	
IBM BladeCenter HT	Le châssis BladeCenter HT est livré en standard avec un module AMM. Ce module permet de gérer le châssis et offre la fonction KVM locale. Source : *Produits et technologie IBM BladeCenter*	• DCIM-USBG2

Remarque : Pour prendre en charge la détection automatique, les modèles H et E d'IBM BladeCenter doivent utiliser AMM avec la version de firmware BPET36K ou supérieure.

Remarque : Dans le cas des modèles E et H d'IBM Blade Center, Dominion KX II prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

Configurations requises et recommandées de châssis de lames

Ce tableau contient des informations sur les limitations et les contraintes qui s'appliquent à la configuration des châssis de lames pour qu'ils fonctionnent avec le dispositif Dominion KX II. Raritan vous recommande de suivre toutes les informations suivantes.

Châssis de lames	Action requise/recommandée
Dell PowerEdge M1000e	• Désactivez l'écran de veille de l'interface utilisateur d'iKVM. Sinon, une boîte de dialogue d'autorisation s'affiche et empêche le fonctionnement correct d'iKVM. • Quittez le menu de l'interface utilisateur d'iKVM avant de connecter le châssis Dell à un CIM Raritan. Sinon, iKVM risque de ne pas fonctionner correctement. • Configurez le menu principal de l'interface utilisateur d'iKVM pour sélectionner les lames cible par connecteur, et non par nom. Sinon, iKVM risque de ne pas fonctionner correctement. • *Ne désignez aucun* connecteur pour les opérations d'analyse dans le menu Setup Sans (Paramétrage de l'analyse) de

Châssis de lames	Action requise/recommandée
	l'interface utilisateur d'iKVM. Sinon, iKVM risque de ne pas fonctionner correctement. • *Ne désignez aucun* connecteur pour les opérations de clavier/souris de diffusion dans le menu Setup Broadcast (Paramétrage de la diffusion) de l'interface utilisateur d'iKVM. Sinon, iKVM risque de ne pas fonctionner correctement. • Désignez une seule séquence de touches pour appeler l'interface utilisateur d'iKVM. Cette séquence doit également être identifiée au cours de la configuration des ports de Dominion KX II. Sinon, iKVM risque de fonctionner de manière erratique après une saisie sur le client. • Assurez-vous que l'option Front Panel USB/Video Enabled (USB/Vidéo du panneau avant activés) *n'est pas* sélectionnée au cours de la configuration d'iKVM via l'interface utilisateur de Dell CMC. Sinon, les connexions effectuées à l'avant du châssis auront priorité sur la connexion de Dominion KX II à l'arrière, ce qui empêcherait un fonctionnement correct d'iKVM. Un message s'affichera indiquant User has been disabled as front panel is currently active. (L'utilisateur a été désactivé car le panneau avant est actif.). • Assurez-vous que l'option Allow access to CMC CLI from iKVM (Autoriser l'accès à la CLI CMC depuis iKVM) *n'est pas* sélectionnée au cours de la configuration d'iKVM via l'interface utilisateur de Dell CMC. • Pour empêcher l'affichage de l'interface utilisateur iKVM lors de la connexion au châssis de lames, définissez l'option Screen Delay Time (Délai d'écran) sur 8 secondes. • La sélection de Timed (Différé) et Displayed (Affiché) est recommandé au cours du paramétrage de l'indicateur (Flag Setup) dans l'interface utilisateur d'iKVM. Vous pouvez ainsi confirmer visuellement la connexion au connecteur de lame souhaité.
Dell PowerEdge 1855/1955	• Désactivez l'écran de veille de l'interface utilisateur d'iKVM. Sinon, une boîte de dialogue d'autorisation s'affiche et empêche le fonctionnement correct d'iKVM. • Quittez le menu de l'interface utilisateur d'iKVM avant de connecter le châssis Dell à un CIM Raritan. Sinon, iKVM risque de ne pas fonctionner correctement. • Configurez le menu principal de l'interface utilisateur d'iKVM pour sélectionner les lames cible par connecteur, et non par nom. Sinon, iKVM risque de ne pas fonctionner correctement. • *Ne désignez aucun* connecteur pour les opérations d'analyse dans le menu Setup Scan (Paramétrage de l'analyse) de l'interface utilisateur d'iKVM. Sinon, iKVM risque de ne pas

Châssis de lames	Action requise/recommandée
	fonctionner correctement. • Pour empêcher l'affichage de l'interface utilisateur iKVM lors de la connexion au châssis de lames, définissez l'option Screen Delay Time (Délai d'écran) sur 8 secondes. • La sélection de Timed (Différé) et Displayed (Affiché) est recommandé au cours du paramétrage de l'indicateur (Flag Setup) dans l'interface utilisateur d'iKVM. Vous pouvez ainsi confirmer visuellement la connexion au connecteur de lame souhaité.
Détection automatique IBM/Dell	• Il est recommandé d'activer l'option Auto-Discovery (Détection automatique) lors de l'application des autorisations d'accès au niveau des lames. Sinon, définissez des autorisations d'accès au niveau du châssis de lames. • Secure Shell (SSH) doit être activé sur le module de gestion des châssis de lames. • Le port SSH configuré dans le module de gestion des châssis de lames doit correspondre au numéro de port saisi sur la page Port Configuration (Configuration des ports).
Support virtuel IBM KX2	• La fonction Support virtuel de Dominion KX II de Raritan n'est prise en charge que sur les modèles H et E d'IBM BladeCenter. Elle requiert l'utilisation de D2CIM-DVUSB. Le connecteur USB à faible vitesse D2CIM-DVUSB noir est relié au module AMM (Administrative Management Module) à l'arrière de l'unité. Le connecteur USB à haute vitesse D2CIM-DVUSB gris est relié au tiroir de support (MT) à l'avant de l'unité. Un câble d'extension USB est nécessaire.

Remarque : tous les IBM BladeCenters utilisant AMM doivent utiliser la version de firmware BPET36K ou supérieure pour fonctionner avec Dominion KX II.

Remarque : Dans le cas des modèles E et H d'IBM Blade Center, Dominion KX II prend uniquement en charge la détection automatique lorsqu'AMM[1] est le module de gestion principal.

Exemples de formats d'URL de châssis de lames

Ce tableau contient des exemples de formats d'URL de châssis de lames configurés dans Dominion KX II.

Châssis de lames	Exemple de format d'URL
Dell M1000e	• URL : https://192.168.60.44/cgi-bin/webcgi/login • Username (Nom d'utilisateur) : root

	• Username Field (Champ du nom d'utilisateur) : user • Password (Mot de passe) : calvin • Password Field (Champ du mot de passe) : password
Dell 1855	• URL : https://192.168.60.33/Forms/f_login • Username (Nom d'utilisateur) : root • Username Field (Champ du nom d'utilisateur) : TEXT_USER_NAME • Password (Mot de passe) : calvin • Password Field (Champ du mot de passe) : TEXT_PASSWORD
IBM BladeCenter E ou H	• http://192.168.84.217/private/welcome.ssi

Configuration des profils USB (page Port)

La sélection des profils USB disponibles pour un port s'effectue dans la section Select USB Profiles for Port de la page Port. Les profils USB choisis dans la page Port deviennent les profils disponibles à l'utilisateur dans VKC lors de la connexion à un serveur cible KVM depuis le port. Le profil par défaut est le profil Windows 2000/XP/Vista. Pour plus d'informations sur les profils USB, reportez-vous à ***Profils USB*** (à la page 106).

Remarque : pour définir les profils USB d'un port, un VM-CIM doit être connecté avec un firmware compatible avec la version de firmware courante de Dominion KX II. Reportez-vous à **Mise à niveau des CIM** *(à la page 233).*

Les profils disponibles à affecter à un port apparaissent dans la liste Available (Disponibles) à gauche. Les profils sélectionnés pour une utilisation avec un port apparaissent dans la liste Selected à droite. Lorsque vous sélectionnez un profil dans une des listes, sa description et son utilisation apparaissent dans le champ Profile Description (Description du profil).

Outre la sélection d'un ensemble de profils pour les mettre à la disposition d'un port KVM, vous pouvez également spécifier le profil privilégié pour le port et appliquer les paramètres définis pour un port à d'autres ports KVM.

Remarque : Reportez-vous à pour en savoir plus sur l'utilisation du profil USB Mac OS-X si vous utilisez un DCIM-VUSB ou DCIM-DVUSB.

Pour ouvrir la page Port :

1. Sélectionnez Device Settings (Paramètres du dispositif) > Port Configuration (Configuration des ports). La page Port Configuration s'ouvre.
2. Cliquez sur le nom du port KVM que vous souhaitez modifier. La page Port s'ouvre.

Pour sélectionner les profils USB d'un port KVM :

1. Dans la section Select USB Profiles for Port (Sélectionner les profils USB du port), choisissez un ou plusieurs profils USB dans la liste Available (Disponibles).
   - Appuyez sur la touche Maj+cliquez, et faites glisser pour sélectionner plusieurs profils contigus.

- Appuyez sur la touche Ctrl+cliquez pour sélectionner plusieurs profils non contigus.

2. Cliquez sur Add (Ajouter). Les profils sélectionnés apparaissent dans la liste Selected. Ces profils peuvent être utilisés pour le serveur cible KVM connecté au port.

Pour spécifier un profil USB privilégié :

1. Après avoir sélectionné les profils disponibles pour un port, choisissez-en un dans le menu Preferred Profile for Port (Profil privilégié pour le port). La valeur par défaut est Generic (Générique). Le profil sélectionné est utilisé lors de la connexion au serveur cible KVM. Le cas échéant, vous pouvez le remplacer par n'importe quel autre profil USB.

Pour retirer les profils USB sélectionnés :

1. Dans la section Select USB Profiles for Port (Sélectionner les profils USB du port), choisissez un ou plusieurs profils USB dans la liste Selected (Sélectionnés).

- Appuyez sur la touche Maj+cliquez, et faites glisser pour sélectionner plusieurs profils contigus.
- Appuyez sur la touche Ctrl+cliquez pour sélectionner plusieurs profils non contigus.

2. Cliquez sur Remove (Supprimer). Les profils sélectionnés apparaissent dans la liste Available (Disponibles). Ils ne sont plus disponibles pour un serveur cible KVM connecté à ce port.

Pour appliquer une sélection de profils à plusieurs ports :

1. Dans la section Apply Selected Profiles to Other Ports (Appliquer les profils sélectionnés à d'autres ports), cochez la case Apply (Appliquer) pour chaque port KVM auquel vous souhaitez appliquer l'ensemble en cours de profils USB sélectionnés.

- Pour sélectionner tous les ports KVM, cliquez sur Select All (Tout sélectionner).
- Pour désélectionner tous les ports KVM, cliquez sur Deselect All (Tout désélectionner).

Configuration des paramètres du port local de Dominion KX II

A partir de la page de paramétrage du port local, vous avez la possibilité de personnaliser de nombreux paramètres de la console locale de Dominion KX II, notamment le clavier, les raccourcis-clavier, le délai de commutation de l'écran, le mode d'économie d'alimentation, les paramètres de résolution de l'interface utilisateur locale et l'authentification d'utilisateur locale.

Pour KX2-832 et KX2-864, vous pouvez également configurer le port local étendu sur la page Local Port Settings (Paramètres du port local). Le port local étendu peut être connecté à un commutateur ou à une station utilisateur Paragon pour prolonger le port local. Comme pour le port local standard, vous pouvez configurer les paramètres suivants : clavier, raccourcis-clavier, délai de commutation de l'écran, mode d'économie d'alimentation, résolution de l'interface utilisateur locale et authentification d'utilisateur locale. Le port local étendu peut être configuré depuis la console distante et la console locale. Reportez-vous à ***Paramètres des ports locaux standard et étendu KX2-832 et KX2-864*** (voir "Paramètres des ports locaux standard et étendu de KX2-832 et KX2-864" à la page 204) pour en savoir plus sur le port local standard et sur le port local étendu.

Remarque : si le port local étendu est activé sur KX2-832 et KX2-864, et que rien n'est connecté au port, un délai de deux ou trois secondes se produira lors du passage à une cible via le port local.

▶ Pour configurer les paramètres du port local :

Remarque : certaines modifications apportées aux paramètres de la page Local Port Settings (Paramètres du port local) redémarrent le navigateur dans lequel vous travaillez. Si un redémarrage doit se produire lorsqu'un paramètre est modifié, il est indiqué dans la procédure fournie ici.

1. Sélectionnez Device Settings (Paramètres du dispositif) > Local Port Configuration (Configuration du port local). La page des paramètres du port local s'ouvre.
2. Cochez la case en regard du port local standard pour l'activer. Désélectionnez la case à cocher pour le désactiver. Par défaut, le port local standard est activé, mais peut être désactivé selon les besoins. Le navigateur redémarrera lorsque cette modification sera effectuée.
3. Si vous utilisez un dispositif KX2-832 ou KX2-864, cochez la case en regard du port local étendu pour l'activer. Désélectionnez les cases à cocher pour le désactiver. Si vous utilisez la fonction Carte à puce, le port local étendu doit être désactivé. Le navigateur redémarrera lorsque cette modification sera effectuée.

Si le port local standard et le port local étendu sont désactivés, les ports locaux ne sont pas accessibles. Si vous tentez d'accéder à un dispositif KX2-832 ou KX2-864 via un port local désactivé, un message apparaît indiquant que le dispositif est géré à distance et que la connexion est désactivée.

Remarque : KX2-832 et KX2-864 ne prennent pas en charge la connexion de Dominion KX II au port local étendu. Reportez-vous à **Dispositifs pris en charge par le port local étendu de KX2-832 et de KX2-864** *(à la page 289) pour en savoir plus sur les connexions prises en charge.*

Remarque : si vous connectez un dispositif Paragon au port local étendu de KX2-832 et KX2-864, vous devez utiliser le client distant pour modifier le profil USB.

4. Sélectionnez le type de clavier approprié parmi les options de la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - US
   - US/International (Anglais Etats-Unis/international)
   - United Kingdom
   - Français (France)
   - Allemand (Allemagne)
   - Japonais (JIS)
   - Chinois simplifié
   - Chinois traditionnel
   - Dubeolsik Hangul (Coréen)
   - Allemand (Suisse)
   - Portugais (Portugal)
   - Norvégien (Norvège)
   - Suédois (Suède)
   - Danois (Danemark)
   - Belge (Belgique)

Remarque : l'utilisation du clavier pour le chinois, le japonais et le coréen ne concerne que l'affichage. La saisie dans la langue locale n'est pas prise en charge pour le moment pour les fonctions de la console locale de Dominion KX II.

5. Sélectionnez le raccourci-clavier du port local. Le raccourci-clavier du port local vous permet de retourner à l'interface de la console locale de Dominion KX II lorsque l'interface d'un serveur cible est affichée. Le paramètre par défaut est Double Click Scroll Lock (Double-clic sur Arrêt défil), mais vous pouvez également sélectionner n'importe quelle combinaison de touches dans la liste déroulante :

Raccourci-clavier :	Appuyez sur :
Double-clic sur Arrêt défil	La touche Arrêt défil deux fois sans interruption
Double-clic sur Verr num	La touche Verr num deux fois sans interruption
Double-clic sur Verr. maj.	La touche Verr. maj. deux fois sans interruption
Double-clic sur Alt	La touche Alt deux fois sans interruption
Double-clic sur Maj gauche	La touche Maj gauche deux fois sans interruption
Double-clic sur la touche Ctrl gauche	La touche Ctrl gauche deux fois sans interruption

6. Sélectionnez la touche de connexion du port local. Utilisez une séquence de touches pour la connexion à une cible et la permutation vers une autre. Vous pouvez alors utiliser le raccourci-clavier pour la déconnexion de la cible et le retour à l'interface utilisateur du port local. La touche de connexion fonctionne pour les serveurs standard et les châssis de lames. Une fois la touche de connexion du port local créée, elle apparaît dans le panneau de navigation de l'interface utilisateur. Vous pouvez alors l'employer comme référence. Reportez-vous à ***Exemples de touches de connexion*** (à la page 266) pour obtenir des exemples de séquences de touches de connexion.
7. Réglez Video Switching Delay (Délai de commutation écran) entre 0 et 5 secondes, le cas échéant. En général, la valeur 0 est utilisée à moins que vous n'ayez besoin de plus de temps (certains écrans nécessitent plus de temps pour commuter la vidéo).
8. Si vous souhaitez utiliser la fonction d'économie d'alimentation électrique.
   a. Cochez la case Power Save Mode (Mode d'économie d'alimentation).
   b. Définissez le laps de temps (en minutes) à l'issue duquel le mode d'économie d'alimentation est lancé.

9. Sélectionnez la résolution de la console locale de Dominion KX II dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - 800 x 600
   - 1024 x 768
   - 1280 x 1024
10. Sélectionnez le taux de rafraîchissement dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
    - 60 Hz
    - 75 Hz
11. Sélectionnez le type d'authentification d'utilisateur locale.
    - Local/LDAP/RADIUS. Il s'agit de l'option recommandée. Pour plus d'informations sur l'authentification, reportez-vous à ***Authentification à distance*** (à la page 39).
    - Aucun. Aucun processus d'authentification n'a lieu pour l'accès à la console locale. Cette option est recommandée pour les environnements sécurisés uniquement.
    - Cochez la case Ignore CC managed mode on local port (Ignorer le mode géré par CC sur le port local) si vous souhaitez un accès utilisateur local à Dominion KX II même si le dispositif est géré par CC-SG.

    Remarque : si vous choisissez au départ d'ignorer le mode CC Manage (Gestion par CC) sur le port local, mais souhaitez par la suite un accès au port local, vous devez désactiver la gestion par CC-SG (depuis CC-SG) du dispositif. Vous pourrez alors cocher cette case.

    Remarque : pour utiliser le port local standard et le port local étendu alors que Dominion KX II est géré par CC-SG, l'option Ignore CC managed mode on local port (Ignorer le mode géré par CC sur le port local) doit être sélectionnée. Cochez la case Ignore CC managed mode on local port si vous souhaitez un accès utilisateur local, via le port local standard ou étendu, à Dominion KX II même si le dispositif est géré par CC-SG.

12. Cliquez sur OK.

Paramètres des ports locaux standard et étendu de KX2-832 et KX2-864

KX2-832 et KX2-864 vous offrent deux options pour le port local : le port local standard et le port local étendu. Chacune de ces options de port est activée et désactivée depuis la console distante sur la page Port Configuration ou depuis la console locale sur la page Local Port Settings (Paramètres du port local). Pour en savoir plus, reportez-vous à ***Configuration des paramètres du port local de Dominion KX II*** (à la page 200).

Par défaut, le port local standard est activé et le port local étendu est désactivé. Si vous souhaitez prolonger le port local, activez le port local étendu et utilisez un câble Cat5/5e/6 pour effectuer la connexion à DKX2-832 ou DKX2-864 depuis une unité Paragon II UMT, EUST, UST ou URKVMG.

Remarque : si le port local étendu est activé sur KX2-832 et KX2-864, et que rien n'est connecté au port, un délai de deux ou trois secondes se produira lors du passage à une cible via le port local.

Vous devez disposer des droits d'administrateur pour configurer ces options. Pour accéder à un port, vous ne devez entrer vos nom d'utilisateur et mot de passe qu'une seule fois. Vous n'avez pas à les entrer pour chaque port auquel vous accédez.

Reportez-vous à la section ***Spécifications*** (à la page 276) pour en savoir plus sur les dispositifs pris en charge par le port local étendu, les spécifications de distance et les CIM pris en charge.

Limitations de connexion des KX2-832 et KX2-864

Les ports locaux standard et étendu partagent l'accès à une cible. Lorsqu'ils sont tous les deux activés, ils se partagent le clavier, le moniteur et la souris. Ils seront tous les deux connectés à la cible ou déconnectés.

Lorsque le port local standard ou le port local étendu est désactivé, le clavier, le moniteur et la souris de ces ports sont désactivés et un message vous indique que les ports locaux sont désactivés.

Chapitre 8 Gestion des prises de barrettes d'alimentation (PDU de rack)

Dans ce chapitre

Présentation 205
Mise sous/hors tension des prises et alimentation cyclique.....206

Présentation

Dominion KX II vous permet de contrôler les prises de barrettes d'alimentation des séries PX et RPC de Raritan connectées à Dominion KX II via un D2CIM-PWR.

*Remarque : pour plus d'informations sur le paramétrage d'une unité PX, reportez-vous au **manuel d'utilisation de Dominion PX**.*

Une fois l'unité de la série PX ou RPC paramétrée puis connectée à Dominion KX II, la barrette d'alimentation et ses prises peuvent être contrôlées depuis la page Powerstrip (Barrette d'alimentation) de l'interface de Dominion KX II. Pour accéder à cette page, cliquez sur le menu Power (Alimentation) en haut de la page.

Sur la page Powerstrip, vous pouvez mettre les prises sous et hors tension, et effectuer leur alimentation cyclique. Vous pouvez également visualiser les informations suivantes relatives à la barrette d'alimentation et aux prises :

- Informations sur le dispositif de barrette d'alimentation :
  - Nom
  - Modèle
  - Température
  - Current Amps (Courant en ampères)
  - Maximum Amps (Courant maximal en ampères)
  - Voltage (Tension)
  - Power in Watts (Puissance en watts)
  - Power in Volts Ampere (Puissance en voltampère)
- Informations sur l'affichage des prises :
  - Name (Nom) - Il s'agit du nom affecté à la prise lors de sa configuration.
  - State (Etat) - Etat sous ou hors tension de la prise.

- Control (Contrôle) - Permet de mettre les prises sous ou hors tension, ou d'effectuer leur alimentation cyclique.
- Association - Il s'agit des ports associés à la prise.

Initialement, lorsque vous ouvrez la page Powerstrip, les barrettes d'alimentation actuellement connectées à Dominion KX II s'affichent dans la liste déroulante Powerstrip. En outre, les informations relatives à la barrette d'alimentation sélectionnée s'affichent. Le nom, l'état et les associations de ports de la barrette d'alimentation n'apparaissent pas, ni les contrôles de mise sous et hors tension, et d'alimentation cyclique. Cliquez sur le bouton Refresh (Actualiser) pour afficher ces informations et les contrôles de prise. Si aucune barrette d'alimentation n'est connectée à Dominion KX II, un message indiquant « No powerstrips found » (Aucune barrette d'alimentation détectée) s'affiche dans la section Powerstrip Device (Dispositif de barrette d'alimentation) de la page.

Mise sous/hors tension des prises et alimentation cyclique

Pour mettre une prise sous tension :

1. Cliquez sur le menu Power (Alimentation) pour accéder à la page Powerstrip (Barrette d'alimentation).
2. Dans la liste déroulante Powerstrip, sélectionnez la barrette d'alimentation PX que vous souhaitez mettre sous tension.

3. Cliquez sur Refresh (Actualiser) pour afficher les contrôles d'alimentation.
4. Cliquez sur On (Sous tension).

5. Cliquez sur OK pour fermer la boîte de dialogue de confirmation Power On (Sous tension). La prise est mise sous tension et son état indique on.

Pour mettre une prise hors tension :

1. Cliquez sur Off (Hors tension).
2. Cliquez sur OK dans la boîte de dialogue Power Off (Hors tension).

3. Cliquez sur OK dans la boîte de dialogue de confirmation Power Off (Hors tension). La prise est mise hors tension et son état indique off.

Pour effectuer l'alimentation cyclique d'une prise :

1. Cliquez sur le bouton Cycle (Alimentation cyclique). La boîte de dialogue Power Cycle Port (Port d'alimentation cyclique) s'ouvre.

2. Cliquez sur OK. L'alimentation cyclique de la prise débute alors (notez qu'elle peut prendre plusieurs secondes).

3. Une fois l'alimentation cyclique terminée, la boîte de dialogue s'ouvre. Cliquez sur OK pour fermer la boîte de dialogue.

Chapitre 9 Gestion de la sécurité

Dans ce chapitre

Security Settings (Paramètres de sécurité).....209
Configuration du contrôle d'accès IP.....221
Certificats SSL.....224

Security Settings (Paramètres de sécurité)

A partir de la page **Security Settings**, spécifiez les limitations de connexion, le blocage des utilisateurs, les règles de mot de passe, ainsi que les paramètres de chiffrement et de partage.

Les certificats SSL Raritan sont utilisés pour des échanges de clés publiques et privées. Ils fournissent un niveau de sécurité supplémentaire. Les certificats de serveur Web Raritan sont auto-signés. Les certificats d'applet Java sont signés par VeriSign. Le chiffrement garantit la sécurité de vos informations en les protégeant contre l'interception frauduleuse. Ces certificats garantissent que l'entité est bien Raritan, Inc.

Pour configurer les paramètres de sécurité :

1. Sélectionnez Security (Sécurité) > Security Settings (Paramètres de sécurité). La page Security Settings s'ouvre.
2. Mettez à jour les paramètres de ***limitations de connexion*** (à la page 210) en fonction de vos besoins.
3. Mettez à jour les paramètres de ***mots de passe sécurisés*** (à la page 212) en fonction de vos besoins.
4. Mettez à jour les paramètres de ***blocage des utilisateurs*** (voir "User Blocking (Blocage des utilisateurs)" à la page 213) en fonction de vos besoins.
5. Mettez à jour les paramètres de chiffrement & partage en fonction de vos besoins.
6. Cliquez sur OK.

Pour rétablir les paramètres par défaut :

- Cliquez sur Reset to Defaults (Rétablir les paramètres par défaut).

Limitations de connexion

A l'aide des limitations de connexion, spécifiez les restrictions en matière de connexion unique, de vieillissement de mot de passe et de déconnexion des utilisateurs inactifs.

Limitation	Description
Enable Single Login Limitation (Activer la limitation de connexion unique)	Si vous sélectionnez cette option, seule une connexion par nom d'utilisateur est autorisée à n'importe quel moment. En revanche, si elle est désélectionnée, une combinaison nom d'utilisateur/mot de passe donnée peut être connectée au dispositif à partir de plusieurs postes de travail clients simultanément.
Enable Password Aging (Activer le	Si vous sélectionnez cette option, tous les utilisateurs sont obligés de modifier leur mot de

Limitation	Description
vieillissement du mot de passe)	passe régulièrement en fonction du nombre de jours spécifiés dans le champ Password Aging Interval (Intervalle de vieillissement du mot de passe). Ce champ est activé et obligatoire lorsque la case Enable Password Aging (Activer le vieillissement du mot de passe) est cochée. Entrez le nombre de jours après lequel une modification de mot de passe est requise. Le nombre par défaut est 60 jours.
Log off idle users, After (1-365 minutes) (Déconnecter les utilisateurs inactifs, Après)	Cochez la case Log off idle users pour déconnecter automatiquement les utilisateurs après le délai spécifié dans le champ After (1-365 minutes). En l'absence d'activité du clavier ou de la souris, toutes les sessions et toutes les ressources sont déconnectées. En revanche, si une session de support virtuel est en cours, elle n'expire pas. Le champ After (Après) permet de définir le délai (en minutes) après lequel un utilisateur inactif est déconnecté. Ce champ est activé lorsque l'option Log Out Idle Users (Déconnecter les utilisateurs inactifs) est sélectionnée. La valeur saisie dans le champ peut aller jusqu'à 365 minutes.

Mots de passe sécurisés

Les mots de passe sécurisés fournissent une authentification locale du système accrue. Utilisez les mots de passe sécurisés pour spécifier le format des mots de passe locaux valides de Dominion KX II, tel que la longueur minimum et maximum, les caractères obligatoires et la conservation de l'historique des mots de passe.

Les mots de passe sécurisés créés par les utilisateurs doivent compter un minimum de 8 caractères avec au moins un caractère alphabétique et un caractère non alphabétique (signe de ponctuation ou chiffre). De plus, les quatre premiers caractères du mot de passe et du nom d'utilisateur ne peuvent pas être identiques.

Si cette option est sélectionnée, les règles des mots de passe sécurisés sont appliquées. Les utilisateurs dont les mots de passe ne répondent pas aux critères de mot de passe sécurisé sont automatiquement invités à modifier leur mot de passe lors de la connexion suivante. Si l'option est désélectionnée, seule la validation du format standard est appliquée. Lorsqu'elle est sélectionnée, les champs suivants sont activés et obligatoires :

Champ	Description
Minimum length of strong password (Longueur minimale du mot de passe sécurisé)	Le mot de passe doit compter au moins 8 caractères. La valeur par défaut est 8, mais vous pouvez entrer jusqu'à 63 caractères.
Maximum length of strong password (Longueur maximale du mot de passe sécurisé)	La valeur par défaut est 16, mais vous pouvez entrer jusqu'à 64 caractères.
Enforce at least one lower case character (Imposer au moins un caractère minuscule)	Lorsqu'elle est cochée, cette option impose au moins un caractère minuscule dans le mot de passe.
Enforce at least one upper case character (Imposer au moins un caractère majuscule)	Lorsqu'elle est cochée, cette option impose au moins un caractère majuscule dans le mot de passe.
Enforce at least one numeric character (Imposer au moins un caractère numérique)	Lorsqu'elle est cochée, cette option impose au moins un caractère numérique dans le mot de passe.
Enforce at least one printable special character (Imposer au moins un caractère spécial	Lorsqu'elle est cochée, cette option impose au moins un caractère spécial (imprimable) dans le mot de passe.

Champ	Description
imprimable)	
Number of restricted passwords based on history (Nombre de mots de passe restreints en fonction de l'historique)	Ce champ représente la profondeur de l'historique des mots de passe ; c'est-à-dire le nombre de mots de passe précédents ne pouvant pas être répétés. La plage va de 1 à 12, la valeur par défaut étant 5.

User Blocking (Blocage des utilisateurs)

Les options de blocage d'utilisateurs spécifient les critères selon lesquels les utilisateurs se voient refuser l'accès au système après un nombre spécifique d'échecs de connexion.

Les trois options s'excluent les unes les autres :

Option	Description
Disabled (Désactivé)	Il s'agit de l'option par défaut. Les utilisateurs ne sont pas bloqués quel que soit le nombre d'échecs d'authentification.

Option	Description
Timer Lockout (Période de verrouillage)	Les utilisateurs se voient refuser l'accès au système après avoir dépassé le nombre d'échecs de connexion autorisé. Lorsque cette option est sélectionnée, les champs suivants sont activés : ▪ Attempts (Tentatives) - Il s'agit du nombre d'échecs de connexion après lequel l'utilisateur est bloqué. La plage autorisée va de 1 à 10, la valeur par défaut étant 3 tentatives. ▪ Lockout Time (Durée de verrouillage) - Il s'agit du laps de temps pendant lequel l'utilisateur est bloqué. La plage autorisée va de 1 à 1 440 minutes, la valeur par défaut étant 5 minutes. *Remarque : les utilisateurs dotés du rôle Administrateur ne sont pas concernés par les paramètres de période de verrouillage.*
Deactivate User-ID (Désactiver l'ID de l'utilisateur)	Sélectionnée, cette option indique que l'utilisateur ne peut plus accéder au système après un nombre spécifique de tentatives de connexion échouées, défini dans le champ Failed Attempts (Tentatives échouées) : ▪ Failed Attempts (Tentatives échouées) - Il s'agit du nombre d'échecs de connexion après lequel l'ID de l'utilisateur est désactivé. Le champ est activé lorsque l'option Deactivate User-ID (Désactiver l'ID de l'utilisateur) est sélectionnée. Les valeurs autorisées sont comprises entre 1 et 10.

Lorsque l'ID d'un utilisateur est désactivé suite à un nombre spécifique d'échecs de connexion, l'administrateur doit modifier le mot de passe de l'utilisateur et activer le compte de celui-ci en cochant la case Active (Actif) dans la page User (Utilisateur).

Encryption & Share (Chiffrement & partage)

A l'aide des paramètres de chiffrement et de partage, vous pouvez spécifier le type de chiffrement utilisé, les modes de partage PC et VM, ainsi que le type de réinitialisation effectuée lorsque le bouton Reset de Dominion KX II est enfoncé.

AVERTISSEMENT : si vous sélectionnez un mode de chiffrement non pris en charge par votre navigateur, vous ne pourrez pas utiliser ce dernier pour accéder à Dominion KX II.

1. Sélectionnez une option dans la liste déroulante Encryption Mode (Mode de chiffrement). Lorsqu'un mode de chiffrement est sélectionné, un avertissement s'affiche si votre navigateur ne prend pas en charge ce mode. Dans ce cas, vous ne serez pas en mesure de vous connecter à Dominion KX II. L'avertissement indique « When the Encryption Mode is specified please ensure that your browser supports this encryption mode; otherwise you will not be able to connect to the Dominion KX II. » (Lorsque le mode de chiffrement est spécifié, assurez-vous que votre navigateur le prend en charge ; sinon, vous ne pourrez pas vous connecter à Dominion KX II.).

Mode de chiffrement	Description
Auto	Il s'agit de l'option recommandée. Dominion KX II négocie automatiquement au niveau le plus élevé de chiffrement possible. Vous *devez* sélectionner Auto pour que le dispositif et le client négocient avec succès l'utilisation des algorithmes compatibles FIPS.
RC4	Permet de sécuriser les noms d'utilisateur, les mots de passe et les données KVM, notamment les transmissions vidéo, à l'aide de la méthode de chiffrement RSA RC4. Le protocole Secure Socket Layer (SSL) à 128 bits fournit un canal de communication privé entre le dispositif Dominion KX II et l'ordinateur distant lors de l'authentification de la connexion initiale. Si vous activez le mode FIPS 140-2 et que RC4 est sélectionné, vous recevrez un message d'erreur. RC4 n'est pas disponible en mode FIPS 140-2.
AES-128	La norme de chiffrement avancée (AES - Advanced Encryption Standard) est une norme approuvée par l'Institut National des

Mode de chiffrement	Description
	Normes et de la Technologie (NIST - National Institute of Standards and Technology) pour le chiffrement des données électroniques (la longueur de clé est de 128). Si l'option AES-128 est sélectionnée, assurez-vous que votre navigateur la prend en charge. Sinon, vous ne pourrez pas vous connecter. Reportez-vous à ***Vérification de la prise en charge du chiffrement AES par votre navigateur*** (à la page 218) pour plus d'informations.
AES-256	La norme de chiffrement avancée (AES - Advanced Encryption Standard) est une norme approuvée par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) pour le chiffrement des données électroniques (la longueur de clé est de 256). Si l'option AES-256 est sélectionnée, assurez-vous que votre navigateur la prend en charge. Sinon, vous ne pourrez pas vous connecter. Reportez-vous à ***Vérification de la prise en charge du chiffrement AES par votre navigateur*** (à la page 218) pour plus d'informations.

Remarque : MPC négocie systématiquement au niveau le plus élevé de chiffrement et s'adapte au mode de chiffrement paramétré s'il n'est pas défini sur Auto.

Remarque : si vous exécutez Windows XP avec Service Pack 2, Internet Explorer 7 ne peut pas se connecter à distance à Dominion KX II à l'aide du chiffrement AES-128.

2. Apply Encryption Mode to KVM and Virtual Media (Appliquer le mode de chiffrement à KVM et aux supports virtuels). Lorsqu'elle est sélectionnée, cette option applique le mode de chiffrement sélectionné à la fois à KVM et aux supports virtuels. Après authentification, les données KVM et MV sont également transférées avec un chiffrement de 128 bits.
3. Pour les organismes gouvernementaux et autres environnements de haute sécurité, activez le mode FIPS 140-2 en cochant la case Enable FIPS 140-2 (Activer FIPS 140-2). Reportez-vous à ***Activation de FIPS 140-2*** (à la page 219) pour en savoir plus à ce sujet.

4. PC share mode (Mode PC-Share). Détermine l'accès KVM à distance simultané global, permettant ainsi à huit utilisateurs distants au maximum de se connecter simultanément à une unité Dominion KX II et d'afficher et gérer, en même temps, le même serveur cible par l'intermédiaire du dispositif. Cliquez sur la liste déroulante pour sélectionner une des options suivantes :
   - Private - No PC share (Privé - Pas de PC-Share). Il s'agit du mode par défaut. Seul un utilisateur à la fois peut accéder au serveur cible.
   - PC-Share - Huit utilisateurs maximum (administrateurs ou non) peuvent accéder simultanément aux serveurs cible KVM. Chaque utilisateur distant dispose du même contrôle au niveau du clavier et de la souris. Notez toutefois que le contrôle n'est pas homogène si un utilisateur n'arrête pas de taper ou de déplacer la souris.
5. En cas de besoin, sélectionnez VM Share Mode (Mode de partage du support virtuel). Cette option est activée uniquement si le mode PC-Share est activé. Lorsqu'elle est sélectionnée, cette option permet le partage des supports virtuels entre plusieurs utilisateurs ; cela signifie que de multiples utilisateurs peuvent accéder à la même session de supports virtuels. Par défaut, ce mode est désactivé.
6. Le cas échéant, cochez la case Disable Local Port Output (Désactiver la sortie du port local). Si cette option est sélectionnée, aucune sortie vidéo ne se produit sur le port local. Ce paramètre s'applique uniquement à KX2 832 et à KX2 864. Si vous utilisez des lecteurs de cartes à puce, le port local *doit* être désactivé.
7. Le cas échéant, sélectionnez Local Device Reset Mode (Mode Réinitialisation du dispositif local). Cette option spécifie les actions entreprises lorsque le bouton Reset (situé à l'arrière du dispositif) est enfoncé. Pour plus d'informations, reportez-vous à Réinitialisation de Dominion KX II à l'aide du bouton de réinitialisation. Sélectionnez une des options suivantes :

Mode Réinitialisation du dispositif local	**Description**
Enable Local Factory Reset (Activer la réinitialisation locale des paramètres d'usine) (valeur par défaut).	Le dispositif Dominion KX II retrouve les paramètres d'usine par défaut.
Enable Local Admin Password Reset (Activer la réinitialisation locale du mot de passe	Permet de réinitialiser le mot de passe d'administrateur local uniquement. Le mot de passe raritan est rétabli.

Mode Réinitialisation du dispositif local	Description
administrateur)	
Disable All Local Resets (Désactiver toutes les réinitialisations locales)	Aucune action de réinitialisation n'est entreprise.

Vérification de la prise en charge du chiffrement AES par votre navigateur

Dominion KX II prend en charge AES-256. Pour savoir si votre navigateur utilise le chiffrement AES, vérifiez auprès de l'éditeur du navigateur ou consultez le site Web https://www.fortify.net/sslcheck.html à l'aide du navigateur avec la méthode de chiffrement que vous souhaitez vérifier. Ce site Web détecte la méthode de chiffrement de votre navigateur et fournit un rapport.

Remarque : IE6 ne prend pas en charge le chiffrement AES 128 bits, ni le chiffrement AES 256 bits.

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

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

- Firefox 2.0.0.x et 3
- Mozilla 1.7.13
- Internet Explorer 7 et 8

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

Selon la version de JRE utilisée, ces fichiers peuvent être téléchargés à la rubrique « other downloads » des pages suivantes dont voici les liens :

- JRE1.5 - http://java.sun.com/javase/downloads/index_jdk5.jsp

Activation de FIPS 140-2

Pour les organismes gouvernementaux et autres environnements de haute sécurité, l'activation du mode FIPS 140-2 est souhaitable. Dominion KX II utilise un module cryptographique validé FIPS 140-2 s'exécutant sur une plate-forme Linux selon la section G.5 des directives de mise en œuvre de FIPS 140-2. Une fois ce mode activé, la clé privée utilisée pour produire les certificats SSL doit être générée en interne ; elle ne peut être ni téléchargée ni exportée.

Pour activer FIPS 140-2 :

1. Accédez à la page Encryption & Share page (reportez-vous à ***Cryptage & partage*** (voir "Encryption & Share (Chiffrement & partage)" à la page 215)).
2. Pour activer le mode FIPS 140-2, cochez la case Enable FIPS 140-2 dans la section Encryption & Share (Cryptage & partage) de la page Security Settings (Paramètres de sécurité). Vous utiliserez alors les algorithmes approuvés FIPS 140-2 pour les communications externes. Le module cryptographique FIPS sert au cryptage du trafic de session KVM constitué de données vidéo, de clavier, de souris, de support virtuel et de carte à puce.
3. Redémarrez Dominion KX II **Obligatoire**

   Une fois le mode FIPS activé, la mention FIPS Mode: Enabled apparaît dans la section Device Information (Informations sur le dispositif) du panneau gauche de l'écran.

   Pour plus de sécurité, vous pouvez également créer une demande de signature de certificat une fois le mode FIPS activé. Elle sera créée à l'aide des chiffres de clé requis. Téléversez le certificat après sa signature ou créez un certificat auto-signé. Le statut du certificat SSL passe de Not FIPS Mode Compliant (Non compatible au mode FIPS) à FIPS Mode Compliant (Compatible au mode FIPS).

   Lorsque le mode FIPS est activé, les fichiers de clé ne peuvent être ni téléchargés ni téléversés. La demande de signature de certificat la plus récente sera associée en interne au fichier de clé. En outre, le certificat SSL émanant de l'autorité de certification et la clé privée de celui-ci ne sont pas inclus dans la restauration totale du fichier sauvegardé. La clé ne peut pas être exportée de Dominion KX II.

Exigences en matière de prise en charge de FIPS 140-2

Dominion KX II prend en charge l'utilisation des algorithmes de chiffrement approuvés FIPS 140-20. Ceci permet à un serveur et à un client SSL de négocier la suite de chiffrement utilisée pour la session chiffrée lorsqu'un client est configuré pour le mode FIPS 140-2 seul.

Les recommandations relatives à l'utilisation de FIPS 140-2 avec Dominion KX II figurent ci-après :

Dominion KX II

- Paramétrez Encryption & Share (Chiffrement & Partager) sur Auto sur la page Security Settings (Paramètres de sécurité). Reportez-vous à Cryptage et partage.

Microsoft Client

- FIPS 140-2 doit être activé sur l'ordinateur client et dans Internet Explorer.

Pour activer FIPS 140-2 sur un client Windows :

1. Sélectionnez Panneau de configuration > Outils d'administration > Stratégie de sécurité locale pour ouvrir la boîte de dialogue Paramètres de sécurité locaux.
2. Dans l'arborescence de navigation, sélectionnez Stratégies locales > Options de sécurité.
3. Activez l'option Cryptographie système : utilisez des algorithmes compatibles FIPS pour le cryptage, le hachage et la signature.
4. Redémarrez l'ordinateur client.

Pour activer FIPS 140-2 dans Internet Explorer :

1. Dans Internet Explorer, sélectionnez Outils > Options Internet et cliquez sur l'onglet Avancé.
2. Cochez la case Utiliser TLS 1.0.
3. Redémarrez le navigateur.

Configuration du contrôle d'accès IP

A l'aide du contrôle d'accès IP, vous pouvez réguler l'accès à votre Dominion KX II. Le fait de configurer une liste de contrôle d'accès (LCA) globale permet de garantir que votre dispositif ne répondra pas aux paquets envoyés à partir d'adresses IP non autorisées. Le contrôle d'accès IP est global et affecte l'ensemble du dispositif Dominion KX II. Cependant, vous pouvez également contrôler l'accès à votre dispositif au niveau du groupe. Reportez-vous à ***LCA (liste de contrôle d'accès) IP de groupes*** (à la page 122) pour plus d'informations sur le contrôle au niveau du groupe.

Important : l'adresse IP 127.0.0.1 est utilisée par le port local de Dominion KX II. Lorsque vous créez une liste de contrôle d'accès IP, 127.0.0.1 ne doit pas figurer dans la plage des adresses IP bloquées ou vous n'aurez plus accès au port local de Dominion KX II.

Pour utiliser le contrôle d'accès IP :

1. Ouvrez la page IP Access Control (Contrôle d'accès IP) en sélectionnant Security (Sécurité) > IP Access Control. La page IP Access Control s'ouvre.
2. Cochez la case Enable IP Access Control (Activer le contrôle de l'accès par IP) pour activer le contrôle de l'accès par IP, ainsi que les autres champs de la page.
3. Sélectionnez la stratégie par défaut (Default Policy). Cette action concerne les adresses IP qui ne figurent pas dans les plages spécifiées.
   - Accept (Accepter) - Les adresses IP sont autorisées à accéder au dispositif Dominion KX II.
   - Drop (Abandonner) - Les adresses IP ne sont pas autorisées à accéder au dispositif Dominion KX II.

   Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Pour ajouter des règles :

1. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).

   Remarque : l'adresse IP doit être saisie à l'aide de la notation CIDR (Classless Inter-Domain Routing, dans laquelle les 24 premiers bits sont utilisés comme adresse réseau).
2. Sélectionnez la stratégie dans la liste déroulante Policy.
3. Cliquez sur Append (Ajouter). La règle est ajoutée au bas de la liste des règles.

Pour insérer une règle :

1. Tapez un numéro de règle (Rule #). Un numéro de règle est requis lorsque vous utilisez la commande Insert (Insérer).
2. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).
3. Sélectionnez la stratégie dans la liste déroulante Policy.
4. Cliquez sur Insert (Insérer). Si le numéro de règle que vous venez d'entrer est le même que celui d'une règle existante, la nouvelle règle est placée avant la règle existante et toutes les règles sont descendues d'un rang.

Conseil : les numéros de règle vous permettent de mieux contrôler l'ordre de création des règles.

Pour remplacer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez remplacer.
2. Tapez l'adresse IP et le masque de sous-réseau dans le champ IPv4/Mask (IPv4/Masque) ou IPv6/Prefix Length (IPv6/Longueur de préfixe).
3. Sélectionnez la stratégie dans la liste déroulante Policy.
4. Cliquez sur Replace (Remplacer). Votre nouvelle règle remplace la règle d'origine portant le même numéro.

Pour supprimer une règle :

1. Spécifiez le numéro de la règle que vous souhaitez supprimer.
2. Cliquez sur Delete (Supprimer).

3. Vous êtes invité à confirmer la suppression. Cliquez sur OK.

Certificats SSL

Dominion KX II utilise le protocole SSL (Secure Socket Layer) pour le trafic réseau chiffré entre lui-même et un client connecté. A l'établissement d'une connexion, Dominion KX II doit s'identifier à un client à l'aide d'un certificat de cryptage.

Il est possible de générer une demande de signature de certificat (CSR) et d'installer un certificat signé par l'autorité de certification (CA) sur Dominion KX II. L'autorité vérifie l'identité de l'auteur de la demande. Elle retourne alors un certificat contenant sa signature à l'auteur. Le certificat, portant la signature de l'autorité de certification reconnue, est utilisé pour confirmer l'identité du détenteur du certificat.

Pour créer et installer un certificat SSL :

1. Sélectionnez Security (Sécurité) > SSL Certificate (Certificat SSL).

2. Remplissez les champs suivants :
   a. Common name (Nom courant) - Il s'agit du nom réseau de Dominion KX II une fois qu'il est installé dans le réseau de l'utilisateur (en règle générale, le nom de domaine complet qualifié). Il est identique au nom utilisé pour accéder à Dominion KX II avec un navigateur Web, mais sans le préfixe http://. Si le nom indiqué ici diffère du nom de réseau, le navigateur affiche un avertissement de sécurité lors de l'accès à Dominion KX II par le biais du protocole HTTPS.
   b. Organizational unit (Unité organisationnelle) - Ce champ permet de spécifier le service, au sein d'une organisation, auquel Dominion KX II appartient.
   c. Organization (Organisation) - Il s'agit du nom de l'organisation à laquelle Dominion KX II appartient.
   d. Locality/City (Localité/Ville) - Il s'agit de la ville où se situe l'organisation.
   e. State/Province (Etat/Province) - Il s'agit de l'Etat ou de la province où se situe l'organisation.
   f. Country (ISO code) (Pays (code ISO)) - Il s'agit du pays où se situe l'organisation. Il s'agit du code ISO de deux lettres ; par exemple, DE pour l'Allemagne ou US pour les Etats-Unis.
   g. Challenge Password (Mot de passe challenge) - Certaines autorités de certification requièrent un mot de passe challenge pour autoriser des modifications ultérieures au certificat (par exemple, la révocation du certificat). La longueur minimale de ce mot de passe est de quatre caractères.
   h. Confirm Challenge Password (Confirmer le mot de passe challenge) - Il s'agit de la confirmation du mot de passe challenge.
   i. Email (Courriel) - Il s'agit de l'adresse électronique d'un contact responsable du dispositif Dominion KX II et de sa sécurité.
   j. Key length (Longueur de la clé) - Il s'agit de la longueur de la clé générée en bits. 1024 est la valeur par défaut.
3. Cliquez sur Create (Créer) pour générer la demande de signature de certificat (CSR).

Pour télécharger un certificat CSR :

1. La demande et le fichier contenant la clé privée utilisée lors de sa génération peuvent être téléchargés en cliquant sur le bouton Download.

Remarque : la demande de signature de certificat et le fichier de clé privée forment un ensemble et doivent être traités en conséquence. Si le certificat signé n'est pas associé à la clé privée utilisée pour le générer à l'origine, le certificat est inutile. Ceci s'applique au téléversement et au téléchargement de la demande de signature de certificat et de ses fichiers de clé privée.

2. Envoyez la demande enregistrée à une autorité de certification pour confirmation. Vous recevrez le nouveau certificat de l'autorité de certification.

Pour téléverser une demande CSR :

1. Téléversez le certificat dans Dominion KX II en cliquant sur le bouton Upload.

Remarque : la demande de signature de certificat et le fichier de clé privée forment un ensemble et doivent être traités en conséquence. Si le certificat signé n'est pas associé à la clé privée utilisée pour le générer à l'origine, le certificat est inutile. Ceci s'applique au téléversement et au téléchargement de la demande de signature de certificat et de ses fichiers de clé privée.

Une fois ces étapes effectuées, Dominion KX II dispose de son propre certificat permettant d'identifier la carte auprès de ses clients.

Important : si vous détruisez la demande de signature de certificat sur Dominion KX II, il n'existe aucun moyen de la récupérer ! Si vous l'avez supprimée par mégarde, vous devez répéter les trois étapes décrites ci-dessus. Pour éviter ceci, utilisez la fonction de téléchargement pour disposer d'une copie de la demande et de sa clé privée.

Chapitre 10 Maintenance

Dans ce chapitre

Journal d'audit 227
Device Information (Informations sur le dispositif) 228
Backup and Restore (Sauvegarde et restauration) 229
USB Profile Management (Gestion des profils USB) 232
Mise à niveau des CIM 233
Mise à niveau du firmware.....234
Historique des mises à niveau 237
Redémarrage.....237
Arrêt de la gestion par CC-SG 239

Journal d'audit

Un journal des événements du système Dominion KX II est créé.

Pour consulter le journal d'audit de votre unité Dominion KX II :

1. Sélectionnez Maintenance > Audit Log (Journal d'audit). La page Audit Log s'ouvre :

   La page du journal d'audit affiche les événements par date et heure (les événements les plus récents étant répertoriés en premier). Le journal d'audit fournit les informations suivantes :

   - Date : date et heure auxquelles l'événement s'est produit (système de 24 heures).
   - Event : nom de l'événement tel que répertorié dans la page Event Management (Gestion des événements).
   - Description : description détaillée de l'événement.

Pour enregistrer le journal d'audit :

Remarque : l'option d'enregistrement du journal d'audit est disponible uniquement sur la console distante de Dominion KX II et non sur la console locale.

1. Cliquez sur Save to File (Enregistrer dans le fichier). Une boîte de dialogue Save File (Enregistrer le fichier) apparaît.
2. Choisissez le nom et l'emplacement du fichier, puis cliquez sur Save (Enregistrer). Le journal d'audit est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.

Pour naviguer dans le journal d'audit :

- Utilisez les liens [Older] (Plus ancien) et [Newer] (Plus récent).

Device Information (Informations sur le dispositif)

La page Device Information fournit des informations détaillées sur votre dispositif Dominion KX II et sur les CIM en cours d'utilisation. Ces informations sont utiles si vous avez besoin de contacter l'assistance technique Raritan.

Pour afficher les informations sur votre Dominion KX II et ses CIM :

- Sélectionnez Maintenance > Device Information (Informations sur le dispositif). La page des informations relatives au dispositif s'ouvre.

Les informations suivantes relatives à Dominion KX II sont fournies :

- Modèle
- Numéro de version du matériel
- Version de firmware
- Numéro de série
- Adresse MAC

Les informations suivantes relatives aux CIM en cours d'utilisation sont fournies :

- (Numéro de) port
- Nom
- Type de CIM - DCIM, PCIM, Barrette d'alimentation ou VM
- Version de firmware
- Numéro de série

Backup and Restore (Sauvegarde et restauration)

La page Backup/Restore (Sauvegarder/Restaurer) vous permet de sauvegarder et de restaurer les paramètres et la configuration de votre Dominion KX II.

Outre l'utilisation de la sauvegarde et de la restauration pour la continuité des opérations, vous pouvez utiliser cette fonction pour gagner du temps. Par exemple, vous pouvez donner rapidement un accès à votre équipe à partir d'un autre Dominion KX II en sauvegardant les paramètres de configuration utilisateur du dispositif Dominion KX II en cours d'utilisation et en restaurant ces paramètres sur le nouveau Dominion KX II. Vous pouvez également configurer un Dominion KX II et copier sa configuration dans plusieurs dispositifs Dominion KX II.

Pour accéder à la page de sauvegarde/restauration :

- Sélectionnez Maintenance > Backup/Restore (Sauvegarder/Restaurer). La page Backup/Restore (Sauvegarder/Restaurer) s'ouvre.

Remarque : les sauvegardes sont toujours des sauvegardes complètes du système. Les restaurations, en revanche, peuvent être totales ou partielles selon votre sélection.

Pour effectuer une copie de sauvegarde de Dominion KX II, si vous utilisez Firefox ou Internet Explorer 5 ou précédent :

1. Cliquez sur Backup (Sauvegarder). La boîte de dialogue File Download (Téléchargement de fichiers) s'ouvre.
2. Cliquez sur Save (Enregistrer). La boîte de dialogue Save As (Enregistrer sous) s'affiche.

3. Sélectionnez l'emplacement, spécifiez un nom de fichier, puis cliquez sur Save (Enregistrer). La boîte de dialogue Download Complete (Téléchargement terminé) s'affiche.
4. Cliquez sur Close (Fermer). Le fichier de sauvegarde est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.

Pour effectuer une copie de sauvegarde de Dominion KX II, si vous utilisez Firefox ou Internet Explorer 6 ou supérieur :

1. Cliquez sur Backup (Sauvegarder). Une boîte de dialogue File Download (Téléchargement de fichier) contenant un bouton Open (Ouvrir) apparaît. Ne cliquez pas sur Open.

   Dans IE 6 et supérieur, IE est utilisé comme application par défaut pour ouvrir les fichiers ; vous êtes donc invité à ouvrir le fichier au lieu de l'enregistrer. Pour éviter ce problème, vous devez remplacer l'application utilisée par défaut pour ouvrir les fichiers par Wordpad.
2. Pour ce faire :
   a. Enregistrez le fichier de sauvegarde. Le fichier de sauvegarde est enregistré localement sur l'ordinateur client avec le nom et l'emplacement spécifiés.
   b. Une fois le fichier enregistré, localisez-le et cliquez dessus avec le bouton droit. Sélectionnez Propriétés.
   c. Dans l'onglet Général, cliquez sur Modifier et sélectionnez Wordpad.

Pour restaurer votre Dominion KX II :

AVERTISSEMENT : soyez prudent lorsque vous restaurez une version antérieure de votre Dominion KX II. Les noms d'utilisateur et mots de passe spécifiés au moment de la sauvegarde sont restaurés. En cas d'oubli des anciens noms d'utilisateur et mots de passe administratifs, vous n'aurez plus accès à Dominion KX II.

Par ailleurs, si vous utilisiez une adresse IP différente au moment de la sauvegarde, cette adresse IP est également restaurée. Si la configuration utilise DHCP, procédez à cette opération uniquement lorsque vous avez accès au port local pour vérifier l'adresse IP après la mise à jour.

1. Sélectionnez le type de restauration que vous souhaitez exécuter :

- Full Restore (Restauration totale) - Restauration complète de l'intégralité du système. Généralement utilisée à des fins de sauvegarde et de restauration traditionnelles.
- Protected Restore (Restauration protégée) - Tout est restauré, hormis les informations spécifiques au dispositif : adresse IP, nom, etc. Cette option vous permet également de configurer un Dominion KX II et de copier sa configuration dans plusieurs dispositifs Dominion KX II.
- Custom Restore (Restauration personnalisée) - Avec cette option, vous pouvez sélectionner User and Group Restore (Restauration des utilisateurs et des groupes) et/ou Device Settings Restore (Restauration des paramètres du dispositif).
    - User and Group Restore (Restauration des utilisateurs et des groupes) - Cette option inclut uniquement les informations relatives aux utilisateurs et aux groupes. Cette option *ne restaure pas* le certificat et les fichiers de clé privée. Utilisez cette option pour configurer rapidement des utilisateurs sur un autre Dominion KX II.
    - Device Settings Restore (Restauration des paramètres du dispositif) - Cette option n'inclut que les paramètres du dispositif : associations d'alimentation, profils USB, paramètres de configuration relatifs au châssis de lames et les affectations de groupes de ports. Utilisez cette option pour copier rapidement les informations relatives au dispositif.

1. Cliquez sur Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
2. Localisez et sélectionnez le fichier de sauvegarde approprié puis cliquez sur Open (Ouvrir). Le fichier sélectionné apparaît dans le champ Restore File (Restaurer le fichier).
3. Cliquez sur Restore (Restaurer). La configuration (en fonction du type de restauration sélectionnée) est restaurée.

USB Profile Management (Gestion des profils USB)

Depuis la page USB Profile Management, vous pouvez téléverser les profils personnalisés fournis par l'assistance technique Raritan. Ces profils sont conçus pour répondre aux besoins de la configuration du serveur cible, si l'ensemble de profils standard ne suffisait pas. L'assistance technique Raritan vous fournira le profil personnalisé et travaillera avec vous pour vérifier si les besoins spécifiques du serveur cible sont couverts.

Pour accéder à la page USB Profile Management :

- Sélectionnez Maintenance > USB Profile Management (Gestion des profils USB). La page USB Profile Management s'ouvre.

Pour téléverser un profil personnalisé dans Dominion KX II :

1. Cliquez sur le bouton Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
2. Localisez et sélectionnez le fichier de profil personnalisé approprié puis cliquez sur Open (Ouvrir). Le fichier sélectionné apparaît dans le champ USB Profile File (Fichier de profil USB).
3. Cliquez sur Upload (Téléverser). Le profil personnalisé sera téléversé et affiché dans le tableau Profile (Profil).

Remarque : si une erreur ou un avertissement apparaît pendant le téléversement (par exemple, écrasement d'un profil personnalisé existant), vous pouvez poursuivre l'opération en cliquant sur Upload ou l'annuler en cliquant sur Cancel.

Pour supprimer un profil personnalisé de Dominion KX II :

1. Cochez la case correspondant à la rangée du tableau contenant le profil personnalisé à supprimer.

2. Cliquez sur Delete (Supprimer). Le profil personnalisé est supprimé et retiré du tableau Profile (Profil).

Comme indiqué, vous pouvez supprimer un profil personnalisé du système, alors qu'il est toujours désigné comme étant actif. Les éventuelles sessions Support virtuel en place seront alors interrompues.

Gestion des conflits dans les noms de profil

Un conflit d'appellation entre les profils USB personnalisés et standard peut se produire au cours d'une mise à niveau de firmware. Cela peut se produire si un profil personnalisé créé et incorporé à la liste des profils standard porte le nom d'un nouveau profil USB téléchargé dans le cadre de la mise à niveau du firmware.

Dans ce cas, le profil personnalisé préexistant sera marqué old_. Par exemple, si un profil personnalisé appelé GenericUSBProfile5 a été créé et un profil du même nom est téléchargé au cours d'une mise à niveau de firmware, le fichier existant sera alors appelé old_GenericUSBProfile5.

Le cas échéant, vous pouvez supprimer le profil existant. Reportez-vous à ***USB Profile Management (Gestion des profils USB)*** (à la page 232) pour plus d'informations.

Mise à niveau des CIM

Utilisez cette procédure pour mettre à niveau les CIM à l'aide des versions de firmware stockées dans la mémoire de votre dispositif Dominion KX II. En général, tous les CIM sont mis à niveau lorsque vous mettez à niveau le firmware du dispositif via la page Firmware Upgrade (Mise à niveau du firmware).

Pour utiliser les profils USB, vous devez disposer d'un D2CIM-VUSB ou D2CIM-DVUSB dont le firmware est mis à jour. Un VM-CIM dont le firmware n'est pas mis à niveau prendra en charge une large gamme de configurations (Windows, clavier, souris, CD-ROM et lecteur amovible) mais ne pourra pas utiliser les profils optimisés pour des configurations cible particulières. Les VM-CIM existants doivent donc être mis à niveau avec le firmware le plus récent pour accéder aux profils USB. Tant qu'ils ne le seront pas, ils fourniront des fonctionnalités équivalentes à celles du profil générique.

Remarque : seul D2CIM-VUSB peut être mis à niveau à partir de cette page.

Pour mettre à niveau les CIM à l'aide de la mémoire de Dominion KX II :

1. Sélectionnez Maintenance > CIM Firmware Upgrade (Mise à niveau du firmware du CIM). La page CIM Upgrade from (Mise à niveau du CIM à partir de) s'ouvre.

Le (numéro de) port, le nom, le type, la version actuelle du CIM et la mise à niveau de la version du CIM sont affichés pour faciliter l'identification des CIM.

2. Cochez la case Selected (Sélectionné) pour chacun des CIM que vous voulez mettre à niveau.

Conseil : utilisez les boutons Select All (Tout sélectionner) et Deselect All (Tout désélectionner) pour sélectionner (ou désélectionner) rapidement tous les CIM.

3. Cliquez sur le bouton Upgrade (Mettre à niveau). Vous êtes invité à confirmer la mise à niveau.
4. Cliquez sur OK pour continuer la mise à niveau. Des barres de progression s'affichent lors de la mise à niveau. La mise à niveau prend environ 2 minutes (ou moins) par CIM.

Mise à niveau du firmware

La page Firmware Upgrade (Mise à niveau du firmware) permet de mettre à niveau le firmware de votre Dominion KX II et de tous les CIM reliés. Cette page est disponible sur la console distante de Dominion KX II uniquement.

Important : ne mettez pas votre Dominion KX II hors tension et ne déconnectez pas les CIM pendant la mise à niveau ; cela risque fortement d'endommager l'unité ou les CIM.

Pour mettre à niveau votre unité Dominion KX II :

1. Localisez le fichier de distribution du firmware Raritan (*.RFP) sur la page des mises à niveau du firmware du ***site Web de Raritan*** http://www.raritan.com :
2. Décompressez le fichier. Lisez attentivement l'ensemble des instructions incluses dans les fichiers ZIP du firmware avant de procéder à la mise à niveau.

Remarque : copiez le fichier de mise à jour du firmware sur un PC local avant de procéder au téléversement. Ne chargez pas le fichier depuis un lecteur connecté en réseau.

3. Sélectionnez Maintenance > Firmware Upgrade (Mise à niveau du firmware). La page Firmware Upgrade (Mise à niveau du firmware) s'ouvre :

4. Cliquez sur le bouton Browse (Parcourir) pour accéder au répertoire où vous avez décompressé le fichier de mise à niveau.
5. Cochez la case Review CIM Version Information? (Vérifier les informations relatives à la version du CIM) pour afficher les informations relatives aux versions des CIM utilisés.
6. Cliquez sur Upload (Téléverser) dans la page de mise à niveau du firmware. Les informations concernant les numéros de mise à niveau et de version sont affichées pour votre confirmation (si vous avez opté pour la vérification des informations relatives au CIM, ces informations sont également affichées) :

Remarque : à ce stade, les utilisateurs connectés sont déconnectés et toute nouvelle tentative de connexion est bloquée.

7. Cliquez sur Upgrade (Mettre à niveau). Patientez jusqu'à la fin de la mise à niveau. Des informations sur l'état et des barres de progression s'affichent pendant la mise à niveau. Une fois la mise à niveau terminée, l'unité redémarre (1 bip est émis pour signaler la fin du redémarrage).

8. A l'invite, fermez le navigateur et attendez environ 5 minutes avant de vous connecter de nouveau à Dominion KX II.

Pour plus d'informations sur la mise à niveau du firmware du dispositif à l'aide de Multi-Platform Client, reportez-vous à **Mise à niveau du firmware du dispositif**.

Remarque : les mises à niveau de firmware ne sont pas prises en charge via modem.

Historique des mises à niveau

Dominion KX II fournit des informations sur les mises à niveau effectuées sur Dominion KX II et les CIM reliés.

Pour afficher l'historique des mises à niveau :

- Sélectionnez Maintenance > Upgrade History (Historique des mises à niveau). La page Upgrade History (Historique des mises à niveau) s'ouvre.

Les informations fournies concernent les mises à niveau de Dominion KX II exécutées, l'état final de la mise à niveau, les heures de début et de fin, et les versions de firmware précédente et courante. Des informations relatives aux CIM sont également fournies ; pour les obtenir, cliquez sur le lien show (afficher) correspondant à une mise à niveau. Les informations relatives aux CIM fournies sont les suivantes :

- Type - Indique le type de CIM.
- Port - Indique le port sur lequel est connecté le CIM.
- User - Indique l'utilisateur qui a effectué la mise à niveau.
- IP - Indiquez l'adresse IP de l'emplacement du firmware.
- Start Time - Indique l'heure de début de la mise à niveau.
- End Time - Indique l'heure de fin de la mise à niveau.
- Previous Version - Indique la version précédente du firmware de CIM.
- Upgrade Version - Indique la version courante du firmware de CIM.
- CIMs - Indique les CIM mis à niveau.
- Result - Indique le résultat de la mise à niveau (réussite ou échec).

Redémarrage

La page Reboot (Redémarrer) offre une manière sûre et contrôlée de redémarrer votre Dominion KX II. Il s'agit de la méthode recommandée pour le redémarrage.

Important : toutes les connexions KVM et série sont fermées et tous les utilisateurs déconnectés.

Pour redémarrer votre Dominion KX II :

1. Sélectionnez Maintenance > Reboot (Redémarrer). La page Reboot (Redémarrer) s'ouvre.

2. Cliquez sur Reboot. Vous êtes invité à confirmer l'action. Cliquez sur Yes (Oui) pour procéder au redémarrage.

Arrêt de la gestion par CC-SG

Pendant que Dominion KX II est géré par CC-SG, si vous tentez d'accéder au dispositif directement, vous êtes averti que CC-SG assure son contrôle.

Si vous gérez Dominion KX II via CC-SG et que la connectivité entre CC-SG et Dominion KX II est perdue après un délai spécifié (10 minutes en général), vous pouvez mettre fin à la session de gestion par CC-SG depuis la console de Dominion KX II.

Remarque : vous devez disposer des autorisations appropriées pour mettre fin à la gestion par CC-SG de Dominion KX II. En outre, l'option Stop CC-SG Management (Arrêter la gestion par CC-SG) n'est accessible que si vous utilisez actuellement CC-SG pour gérer Dominion KX II.

Pour arrêter la gestion d'un dispositif Dominion KX II par CC-SG :

1. Cliquez Maintenance > Stop CC-SG Management (Arrêter la gestion par CC-SG). Un message indiquant que le dispositif est géré par CC-SG s'affiche. Une option permettant de retirer le dispositif de la gestion par CC-SG apparaît également.

2. Cliquez sur Yes (Oui) pour débuter le traitement de retrait du dispositif de la gestion par CC-SG. Un message apparaît alors vous demandant de confirmer le retrait du dispositif de la gestion par CC-SG.

3. Cliquez sur Yes (Oui) pour retirer le dispositif de la gestion par CC-SG. Une fois la gestion par CC-SG terminée, une confirmation apparaît.

Chapitre 11 Diagnostics

Dans ce chapitre

Page d'interface réseau.....241
Page Network Statistics (Statistiques réseau) 241
Page Ping Host (Envoi de commande Ping à l'hôte) 244
Page Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte) 245
Page Device Diagnostics (Diagnostics du dispositif) 246

Page d'interface réseau

Dominion KX II fournit des informations sur l'état de votre interface réseau.

Pour afficher les informations relatives à votre interface réseau :

- Sélectionnez Diagnostics > Network Interface (Interface réseau). La page d'interface réseau s'ouvre.

Les informations suivantes s'affichent :

- l'état de l'interface Ethernet (active ou non) ;
- si la commande ping peut être émise sur la passerelle ;
- le port LAN actif.

Pour actualiser ces informations :

- Cliquez sur le bouton Refresh (Actualiser).

Page Network Statistics (Statistiques réseau)

Dominion KX II fournit des statistiques sur votre interface réseau.

Pour afficher les statistiques relatives à votre interface réseau :

1. Sélectionnez Diagnostics > Network Statistics (Statistiques réseau). La page des statistiques réseau s'ouvre.
2. Sélectionnez l'option appropriée parmi celles de la liste déroulante Options :

- Statistics - Génère une page similaire à celle affichée ici.

- Interfaces - Génère une page similaire à celle affichée ici.

- Route - Génère une page similaire à celle affichée ici.

3. Cliquez sur Refresh (Actualiser). Les informations concernées sont affichées dans le champ Result (Résultat).

Page Ping Host (Envoi de commande Ping à l'hôte)

La commande Ping est un outil réseau qui permet de vérifier si un hôte ou une adresse IP spécifique est accessible via un réseau IP. Grâce à la page Ping Host (Envoyer une commande Ping à l'hôte), vous pouvez déterminer si un serveur cible ou un autre Dominion KX II est accessible.

Pour envoyer une commande Ping à l'hôte :

1. Sélectionnez Diagnostics > Ping Host (Envoyer une commande Ping à l'hôte). La page Ping Host (Envoyer une commande Ping à l'hôte) apparaît.

2. Tapez le nom de l'hôte ou l'adresse IP dans le champ IP Address/Host Name.

Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

3. Cliquez sur Ping. Les résultats de la commande Ping sont affichés dans le champ Result (Résultat).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Page Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte)

Cette page est un outil réseau permettant de tracer l'itinéraire emprunté jusqu'au nom d'hôte ou jusqu'à l'adresse IP fournis.

Pour déterminer l'itinéraire jusqu'à l'hôte :

1. Sélectionnez Diagnostics > Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte). La page Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte) s'ouvre.
2. Tapez l'adresse IP ou le nom de l'hôte dans le champ IP Address/Host Name.

   Remarque : le nom d'hôte ne peut pas dépasser 232 caractères.

3. Sélectionnez une valeur dans la liste déroulante Maximum Hops (Sauts maximum) (de 5 à 50 par incréments de 5).
4. Cliquez sur Trace Route. La commande de détermination d'itinéraire est exécutée pour le nom d'hôte ou l'adresse IP, et le nombre de sauts maximum donnés. Les données de détermination d'itinéraire sont affichées dans le champ Result (Résultat).

Page Device Diagnostics (Diagnostics du dispositif)

Remarque : cette page est en principe destinée aux techniciens de l'assistance. Vous pouvez l'utiliser lorsque l'assistance technique Raritan vous y invite directement.

La page Device Diagnostics (Diagnostics du dispositif) télécharge les informations de diagnostic de Dominion KX II vers l'ordinateur client. Deux opérations peuvent être effectuées sur cette page :

- Exécutez un script de diagnostics spécial fourni par le support technique Raritan lors d'une session de débogage d'erreurs critiques. Le script est téléversé sur le dispositif et exécuté. Une fois le script exécuté, vous pouvez télécharger les messages de diagnostics via le bouton Save to File (Enregistrer dans un fichier).
- Téléchargez le journal de diagnostic du dispositif pour obtenir un instantané des messages de diagnostics de Dominion KX II vers le client. Ce fichier chiffré est ensuite envoyé à l'assistance technique Raritan. Seul Raritan peut interpréter ce fichier.

Remarque : cette page n'est accessible que par les utilisateurs disposant des droits d'administration.

Pour exécuter les diagnostics du système Dominion KX II :

1. Sélectionnez Diagnostics > Dominion KX II Diagnostics (Diagnostics de Dominion KX II). La page de diagnostics de Dominion KX II s'ouvre.
2. Pour exécuter un fichier de script de diagnostics qui vous a été envoyé par courrier électronique par l'assistance technique Raritan :
   a. Récupérez le fichier de diagnostics fourni par Raritan et décompressez-le si nécessaire.
   b. Utilisez le bouton Browse (Parcourir). La boîte de dialogue Choose File (Choisir un fichier) s'ouvre.
   c. Localisez et sélectionnez le fichier de diagnostics.
   d. Cliquez sur Open (Ouvrir). Le fichier s'affiche dans le champ Script File (Fichier de script).

   e. Cliquez sur Run Script (Exécuter le script). Envoyez ce fichier à l'assistance technique Raritan.

3. Pour créer un fichier de diagnostics à envoyer à l'assistance technique Raritan :

   a. Cliquez sur le bouton Save to File (Enregistrer dans le fichier). La boîte de dialogue File Download (Téléchargement de fichier) s'ouvre.

   b. Cliquez sur Save (Enregistrer). La boîte de dialogue Save As (Enregistrer sous) s'affiche.

   c. Localisez le répertoire voulu puis cliquez sur Save (Enregistrer).

   d. Envoyez ce fichier par courrier électronique à l'assistance technique Raritan.

Chapitre 12 Interface de ligne de commande (CLI)

Dans ce chapitre

Présentation 248
Accès à Dominion KX II à l'aide de la CLI 249
Connexion SSH à Dominion KX II 249
Connexion via Telnet à Dominion KX II.....250
Connexion 251
Navigation de la CLI 252
Configuration initiale à l'aide de la CLI 254
Invites CLI.....255
Commandes CLI.....255
Administration des commandes de configuration du serveur de console de Dominion KX II.....257
Configuration du réseau 257

Présentation

L'interface de ligne de commande (CLI) permet de configurer l'interface réseau de Dominion KX II et d'effectuer des fonctions de diagnostic si vous disposez des autorisations appropriées pour cela.

Les figures suivantes présentent les commandes CLI. Reportez-vous à ***Commandes CLI*** (voir "Commandes CLI" à la page 255) pour consulter une liste de commandes, de définitions et de liens vers les sections de ce chapitre comportant des exemples de ces commandes.

Les commandes courantes suivantes peuvent être utilisées depuis tous les niveaux du CLI : top (haut), history (historique), log off (déconnecter), quit (quitter), show (afficher) et help (aide).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Accès à Dominion KX II à l'aide de la CLI

Pour accéder à Dominion KX II, choisissez l'une des méthodes suivantes :

- Telnet via connexion IP
- SSH via connexion IP
- Interface série de port local via RS-232

Un certain nombre de clients SSH/Telnet sont disponibles et peuvent être obtenus sur les sites suivants :

- Putty - ***http://www.chiark.greenend.org.uk/~sgtatham/putty/*** http://www.chiark.greenend.org.uk/~sgtatham/putty/
- SSH Client depuis ssh.com - ***www.ssh.com*** http://www.ssh.com
- Applet SSH Client - ***www.netspace.org/ssh*** http://www.netspace.org/ssh
- OpenSSH Client - ***www.openssh.org*** http://www.openssh.org

Connexion SSH à Dominion KX II

Utilisez un client SSH prenant en charge SSHv2 pour effectuer la connexion à Dominion KX II. Vous devez activer l'accès SSH dans la page Device Services (Services du dispositif).

Remarque : pour des raisons de sécurité, les connexions SSH V1 ne sont pas prises en charge par le dispositif Dominion KX II.

Accès SSH depuis un PC Windows

Pour ouvrir une session SSH depuis un PC Windows :

1. Lancez le logiciel client SSH.
2. Entrez l'adresse IP du serveur de Dominion KX II. Par exemple, 192.168.0.192.
3. Choisissez SSH, qui utilise le port de configuration 22 par défaut.
4. Cliquez sur Ouvrir.

L'invite `login as:` apparaît.

Reportez-vous à ***Connexion*** (à la page 251).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Accès SSH depuis un poste de travail UNIX/Linux

▶ **Pour ouvrir une session SSH depuis un poste de travail UNIX/Linux et vous connecter comme administrateur, entrez la commande suivante :**

```
ssh -l admin 192.168.30.222
```

L'invite Password (Mot de passe) s'affiche.

Reportez-vous à ***Connexion*** (à la page 251).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Connexion via Telnet à Dominion KX II

En raison d'un manque de sécurité, le nom d'utilisateur, le mot de passe et tout le trafic apparaissent en texte clair sur le fil. L'accès via Telnet est désactivé par défaut.

Activation de Telnet

Si vous souhaitez utiliser Telnet pour accéder à Dominion KX II, accédez-y d'abord depuis la CLI ou un navigateur.

▶ **Pour activer Telnet :**

- Activez l'accès Telnet dans le menu Device Settings (Paramètres du dispositif) > Device Services (Services du dispositif).

Une fois l'accès Telnet activé, vous pouvez l'utiliser pour accéder à Dominion KX II et configurer les paramètres restants.

Accès à Telnet depuis un PC Windows

▶ **Pour ouvrir une session Telnet depuis un PC Windows :**

1. Choisissez Démarrer > Exécuter.
2. Tapez *Telnet* dans la zone de texte Ouvrir.
3. Cliquez sur OK. La page Telnet s'ouvre.
4. A l'invite, entrez la commande suivante : `Microsoft Telnet> open <adresse IP>` où <adresse IP> est l'adresse IP de Dominion KX II.

5. Appuyez sur la touche Entrée. Le message suivant apparaît : `Connecting To <adresse IP>... (Connexion à)` L'invite `login as:` apparaît.

Reportez-vous à ***Connexion*** (à la page 251).

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Connexion

Pour vous connecter, entrez le nom d'utilisateur admin, comme indiqué ci-après :

1. Connectez-vous sous `admin`.
2. L'invite Password (Mot de passe) s'affiche. Entrez le mot de passe par défaut : *raritan*

   Le message de bienvenue s'affiche. Vous êtes maintenant connecté en tant qu'administrateur.

Après avoir pris connaissance de la section ***Navigation de la CLI*** (à la page 252), effectuez les tâches de configuration initiale.

```
192.168.59.173 - PuTTY
login as: admin
admin@192.168.59.173's password:

--------------------------------------------------------------------------------
Device Type:   Dominion KX2        Model: DKX2-232
Device Name:   Dennis_KX2          FW Version: 2.0.20.5.6926      SN: HKB7500230
IP Address:    192.168.59.173      Idle Timeout: 0min
--------------------------------------------------------------------------------

Port Port                                Port           Port    Port
No.  Name                                Type           Status  Availability
2  - Dominion-KX2_Port2                  Not Available  down    idle
3  - Dominion_KX2_Port3                  Not Available  down    idle
4  - Dominion_KX2_Port4                  Not Available  down    idle
5  - Dominion_KX2_Port5                  Not Available  down    idle
6  - Dominion_KX2_Port6                  Not Available  down    idle
7  - Dominion_KX2_Port7                  Not Available  down    idle
8  - P2CIM-AUSB012345678901 2345678901   Not Available  down    idle
9  - Dominion_KX2_Port9                  Not Available  down    idle
10 - Dominion_KX2_Port10                 Not Available  down    idle
11 - Dominion_KX2_Port11                 Not Available  down    idle
12 - Dominion_KX2_Port12                 Not Available  down    idle
13 - Dominion_KX2_Port13                 Not Available  down    idle
14 - Dominion_KX2_Port14                 Not Available  down    idle
15 - Dominion_KX2_Port15                 Not Available  down    idle
16 - Dominion_KX2_Port16                 Not Available  down    idle
17 - Dominion_KX2_Port17                 Not Available  down    idle
18 - Dominion_KX2_Port18                 Not Available  down    idle
19 - Dominion_KX2_Port19                 Not Available  down    idle
20 - Dominion_KX2_Port20                 Not Available  down    idle
21 - Dominion_KX2_Port21                 Not Available  down    idle
22 - Dominion_KX2_Port22                 Not Available  down    idle
23 - Dominion_KX2_Port23                 Not Available  down    idle
24 - Dominion_KX2_Port24                 Not Available  down    idle
25 - Dominion_KX2_Port25                 Not Available  down    idle
26 - Dominion_KX2_Port26                 Not Available  down    idle
27 - Dominion_KX2_Port27                 Not Available  down    idle
28 - Dominion_KX2_Port28                 Not Available  down    idle
29 - Dominion_KX2_Port29                 Not Available  down    idle
30 - Dominion_KX2_Port30                 Not Available  down    idle
31 - Dominion_KX2_Port31                 Not Available  down    idle
32 - Dominion_KX2_Port32                 Not Available  down    idle

Current Time: Tue Jun 17 16:27:30 2008
```

Navigation de la CLI

Pour utiliser la CLI, il est essentiel d'en comprendre la navigation et la syntaxe. Certaines combinaisons de touches simplifient également l'utilisation de la CLI.

Saisie automatique des commandes

La CLI complète les commandes partiellement entrées. Entrez les premiers caractères d'une entrée et appuyez sur la touche Tab. Si les caractères forment une correspondance unique, la CLI complétera la saisie.

- Si aucune correspondance n'est trouvée, la CLI affiche les entrées valides pour ce niveau.
- S'il existe plusieurs correspondances, la CLI affiche toutes les entrées valides.

Entrez des caractères supplémentaires jusqu'à ce que l'entrée soit unique et appuyez sur la touche Tab pour compléter la saisie.

Syntaxe CLI - Conseils et raccourcis

Conseils

- Les commandes sont répertoriées par ordre alphabétique.
- Les commandes ne sont pas sensibles à la casse.
- Les noms de paramètre sont composés d'un seul mot, sans trait de soulignement.
- Les commandes sans arguments affichent par défaut les paramètres actuels de la commande.
- Si vous entrez un point d'interrogation (?) après une commande, l'aide correspondant à celle-ci s'affiche.
- Une ligne verticale (|) indique un choix parmi un ensemble de mots-clés ou d'arguments facultatifs ou obligatoires.

Raccourcis

- Appuyez sur la flèche Haut pour afficher la dernière entrée.
- Appuyez sur la touche Retour arrière pour supprimer le dernier caractère tapé.
- Utilisez Ctrl + C pour interrompre une commande ou l'annuler si vous avez saisi des paramètres erronés.
- Utilisez la touche Entrée pour exécuter la commande.
- Appuyez sur la touche Tab pour compléter automatiquement une commande. Par exemple, `Admin Port > Conf` Le système affiche ensuite l'invite `Admin Port > Config >`.

Commandes courantes pour tous les niveaux de la CLI

Les commandes disponibles à tous les niveaux du CLI sont indiquées ci-après. Ces commandes permettent également de parcourir la CLI.

Commandes	Description
top	Revient au niveau supérieur de la hiérarchie CLI, ou

Commandes	Description
	à l'invite username.
history	Affiche les 200 dernières commandes entrées par l'utilisateur dans la CLI de Dominion KX II.
help	Affiche une présentation de la syntaxe CLI.
quit	Fait revenir l'utilisateur au niveau précédent.
logout	Déconnecte la session utilisateur.

Configuration initiale à l'aide de la CLI

Remarque : Ces étapes, qui utilisent la CLI, sont facultatives car cette même configuration peut être effectuée via KVM. Reportez-vous à **Mise en route** *(à la page 14) pour plus d'informations.*

Les dispositifs Dominion KX II sont livrés avec les paramètres usine par défaut. Lorsque vous mettez sous tension le dispositif et vous y connectez pour la première fois, vous devez définir les paramètres de base suivants, pour permettre un accès sécurisé au dispositif depuis le réseau :

1. Réinitialisez le mot de passe administrateur. Tous les dispositifs Dominion KX II sont livrés avec le même mot de passe par défaut. Pour éviter toute intrusion, il est donc impératif de remplacer le mot de passe admin raritan par un mot de passe personnalisé pour les administrateurs qui assureront la gestion du dispositif Dominion KX II.
2. Affectez l'adresse IP, le masque de sous-réseau et l'adresse IP de passerelle pour autoriser l'accès à distance.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Définition des paramètres

Pour définir les paramètres, vous devez être connecté avec des privilèges d'administration. Au niveau supérieur, vous verrez l'invite `Username>`, qui pour la configuration initiale est `admin`. Entrez la commande top pour retourner au niveau de menu supérieur.

Remarque : si vous êtes connecté sous un nom d'utilisateur différent, ce nom apparaîtra au lieu d'admin.

Définition des paramètres réseau

Les paramètres réseau sont configurés à l'aide de la commande d'interface.

```
admin > Config > Network > interface enable true if lan1
ip 192.16.151.12 mask 255.255.255 gw 192.168.51.12
```

Lorsque la commande est acceptée, le dispositif abandonne automatiquement la connexion. Vous devez vous reconnecter au dispositif à l'aide de la nouvelle adresse IP, et du nom d'utilisateur et du mot de passe que vous avez créés dans la section de réinitialisation de mot de passe usine par défaut.

Important : en cas d'oubli du mot de passe, Dominion KX II doit être réinitialisé à la valeur par défaut usine à l'aide du bouton Reset à l'arrière de Dominion KX II. Les tâches de configuration initiale doivent être alors exécutées à nouveau.

Dominion KX II est maintenant doté d'une configuration de base et est accessible à distance via SSH, l'interface utilisateur ou localement à l'aide du port série local. L'administrateur doit configurer les utilisateurs et groupes, les services, la sécurité et les ports série par lesquels les cibles série sont connectées au Dominion KX II.

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Invites CLI

L'invite CLI indique le niveau de commande actuel. La partie racine de l'invite est le nom de connexion. Pour une connexion de port série admin directe avec une application d'émulation de terminal, Admin Port est la partie racine d'une commande.

```
admin >
```

Pour TELNET/SSH, admin est la partie racine de la commande :

```
admin > config > network >
```

0

Commandes CLI

- Entrez `admin > help`.

Commande	Description
config	Passe au sous-menu config.
diagnostics	Passe au sous-menu diag.

Commande	Description
help	Affiche une présentation des commandes.
history	Affiche l'historique des lignes de commande de la session actuelle.
listports	Répertorie les ports accessibles.
logout	Déconnecte de la session CLI actuelle.
top	Revient au menu racine.
userlist	Répertorie les sessions utilisateur actives.

- Entrez admin > config > network.

Commande	Description
help	Affiche une présentation des commandes.
history	Affiche l'historique des lignes de commande de la session actuelle.
interface	Définit/Extrait les paramètres réseau.
ipv6_interface	Définit/Extrait les paramètres réseau IPv6.
logout	Déconnecte de la session CLI actuelle.
name	Configuration du nom de dispositif.
quit	Revient au menu précédent.
stop	Revient au menu racine.

Problèmes de sécurité

Eléments à considérer en matière de sécurité pour les serveurs de console :

- Chiffrement le trafic des données envoyées entre la console de l'opérateur et le dispositif Dominion KX II.
- Authentification et autorisation des utilisateurs.
- Profil de sécurité.

Dominion KX II prend en charge chacun de ces éléments ; toutefois, ils doivent être configurés avant l'utilisation générale.

Administration des commandes de configuration du serveur de console de Dominion KX II

Remarque : les commandes CLI sont les mêmes pour les sessions SSH, Telnet et Port local.

La commande Network est accessible depuis le menu Configuration de Dominion KX II.

Configuration du réseau

Les commandes du menu Network permettent de configurer l'adaptateur réseau de Dominion KX II.

Commandes	Description
interface	Configure l'interface réseau du dispositif Dominion KX II.
name	Configuration du nom du réseau.
ipv6	Définit/Extrait les paramètres réseau IPv6.

Commande interface

La commande interface permet de configurer l'interface réseau de Dominion KX II. La syntaxe de la commande interface est la suivante :

```
interface [ipauto <none|dhcp>] [ip <ipaddress>] [mask
<subnetmask>] [gw <ipaddress>] [mode <mode>]

Set/Get ethernet parameters

ipauto <none|dhcp> IP auto configuration (none/dhcp)

ip <ipaddress> Adresse IP

mask <subnetmask> Masque de sous-réseau

gw <ipaddress> Adresse IP de passerelle

mode <mode> Set Ethernet Mode
(auto/10hdx/10fdx/100hdx/100fdx/1000fdx)
```

Exemple d'utilisation de la commande interface

La commande suivante activer l'interface numéro 1, définit l'adresse IP, le masque et les adresses de passerelle. Elle définit également le mode sur détection automatique.

```
Admin > Config > Network > interface ipauto none ip
192.16.151.12 mask 255.255.255.0 gw 192.168.51.12 mode
auto
```

Remarque : les adresses IPv4 et IPv6 sont prises en charge.

Commande name

La commande name permet de configurer le nom de réseau. La syntaxe de la commande name est la suivante :

```
name [devicename <nomDispositif>] [hostname <nomHôte>]
```

Configuration du nom de dispositif.

```
devicename <devicename>   Nom du dispositif

hostname   <hostname>    Nom d'hôte privilégié (DHCP
uniquement)
```

Exemple d'utilisation de la commande name

La commande suivante définit le nom de réseau :

```
Admin > Config > Network > name devicename My-KSX2
```

Commande IPv6

Utilisez la commande IPv6 pour définir les paramètres réseau IPv6 et extraire les paramètres IPv6 existants.

Chapitre 13 Console locale de Dominion KX II

Dans ce chapitre

Présentation 260
Utilisation de la console locale de Dominion KX II 260
Interface de la console locale de Dominion KX II.....261
Sécurité et authentification 261
Accès par carte à puce à la console locale.....262
Résolutions disponibles.....263
Page d'accès aux ports (affichage de serveur de la console locale) 264
Raccourcis-clavier et touches de connexion.....266
Combinaisons de touches Sun spéciales.....267
Accès à un serveur cible 268
Retour à l'interface de la console locale de Dominion KX II.....268
Administration du port local 269
Réinitialisation de Dominion KX II à l'aide du bouton de réinitialisation 274

Présentation

Dominion KX II fournit un accès et une administration sur le rack via son port local qui intègre une interface utilisateur graphique par navigateur pour commuter rapidement et aisément entre différents serveurs. La console locale de Dominion KX II offre une connexion analogique directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur. La console locale de Dominion KX II fournit les mêmes fonctionnalités d'administration que la console distante Dominion KX II.

Utilisation de la console locale de Dominion KX II

Utilisateurs simultanés

La console locale Dominion KX II offre un chemin d'accès indépendant aux serveurs cible KVM connectés. L'utilisation de la console locale n'empêche pas les autres utilisateurs de se connecter en même temps sur le réseau. Même lorsque des utilisateurs sont connectés à distance à Dominion KX II, vous pouvez toujours accéder à vos serveurs simultanément à partir du rack via la console locale.

Interface de la console locale de Dominion KX II

Lorsque vous êtes situé au niveau du rack du serveur, Dominion KX II permet une gestion KVM standard via la console locale de Dominion KX II. La console locale de Dominion KX II offre une connexion (analogique) KVM directe aux serveurs connectés. Vous obtenez les mêmes performances que si vous étiez directement connecté aux ports clavier, souris et vidéo du serveur.

Les interfaces graphiques utilisateur de la console locale de Dominion KX II et de la console distante de Dominion KX II présentent de nombreuses ressemblances. Les éventuelles différences sont indiquées dans l'aide.

L'option Factory Reset (Rétablir les valeurs usine) est disponible sur la console locale de Dominion KX II et non sur la console distante de Dominion KX II.

Sécurité et authentification

Pour utiliser la console locale de Dominion KX II, vous devez d'abord vous authentifier à l'aide d'un nom d'utilisateur et d'un mot de passe valides. Dominion KX II dispose d'un schéma d'authentification et de sécurité entièrement intégré que votre accès passe par le réseau ou le port local. Dans ces deux cas, Dominion KX II ne permet l'accès qu'aux serveurs pour lesquels un utilisateur dispose de permissions. Reportez-vous à ***Gestion des utilisateurs*** (voir "User Management (Gestion des utilisateurs)" à la page 115) pour plus d'informations sur la définition des paramètres d'accès et de sécurité des serveurs.

Si votre Dominion KX II a été configuré pour des services d'authentification externe (LDAP/LDAPS, RADIUS ou Active Directory), les tentatives d'authentification au niveau de la console locale sont également authentifiées à l'aide du service d'authentification externe.

Remarque : vous pouvez également ne spécifier aucune authentification pour l'accès à la console locale ; cette option est recommandée uniquement dans les environnements sécurisés.

Pour utiliser la console locale de Dominion KX II :

1. Branchez un clavier, une souris et un affichage vidéo sur les ports locaux situés à l'arrière de Dominion KX II.
2. Démarrez Dominion KX II L'interface de la console locale de Dominion KX II s'affiche.

Accès par carte à puce à la console locale

Pour accéder à un serveur au niveau de la console locale à l'aide d'une carte à puce, connectez un lecteur USB à Dominion KX II par un des ports USB situés sur le dispositif. Lorsqu'un lecteur de cartes à puce est branché sur ou débranché de Dominion KX II, Dominion KX II le détecte automatiquement. Pour obtenir la liste des cartes à puce prises en charge et des informations supplémentaires sur la configuration système requise, reportez-vous à ***Lecteurs de cartes à puce pris en charge ou non*** (à la page 293) et ***Configuration système minimale requise*** (à la page 295).

Une fois montés sur le serveur cible, le lecteur de cartes et la carte à puce forceront le serveur à se comporter comme s'ils étaient directement connectés. Le retrait de la carte à puce ou du lecteur de cartes entraînera le verrouillage de la session utilisateur ou vous serez déconnecté suivant la stratégie de retrait de la carte définie dans le système d'exploitation du serveur cible. Lorsque la session KVM est arrêtée, parce qu'elle a été fermée ou parce que vous êtes passé sur une autre cible, le lecteur de cartes à puce est automatiquement démonté du serveur cible.

Pour monter un lecteur de cartes à puce sur une cible via la console locale Dominion KX II :

1. Connectez un lecteur de cartes à puce USB à Dominion KX II à l'aide d'un des ports USB situés sur le dispositif. Une fois branché, le lecteur sera détecté par Dominion KX II.
2. Depuis la console locale, cliquez sur Tools (Outils).
3. Sélectionnez le lecteur dans la liste Card Readers Detected (Lecteurs de cartes détectés). Sélectionnez None (Aucun) dans la liste si vous ne souhaitez pas monter de lecteur de cartes à puce.
4. Cliquez sur OK. Une fois le lecteur de cartes à puce ajouté, un message apparaît sur la page pour indiquer que l'opération a abouti. Le statut Selected (Sélectionné) ou Not Selected (Non sélectionné) apparaît dans le panneau gauche de la page sous Card Reader (Lecteur de cartes).

Pour mettre à jour la liste des lecteurs de cartes détectés :

- Cliquez sur Refresh (Actualiser) si un nouveau lecteur de cartes à puce a été monté. La liste Card Readers Detected est rafraîchie pour inclure le lecteur de cartes à puce ajouté.

Accès par carte à puce pour les dispositifs KX2 8

Si vous utilisez un lecteur de cartes à puce pour accéder à un serveur depuis la console locale via un dispositif KX2-832 ou KX2-864, le port local étendu (page Local Port Settings (Paramètres du port local)) doit être désactivé. Le port local étendu ne prend pas en charge l'authentification par carte à puce.

Résolutions disponibles

La console locale de Dominion KX II offre les résolutions suivantes pour prendre en charge divers écrans :

- 800 x 600
- 1024 x 768
- 1280 x 1024

Chacune de ces résolutions prend en charge un taux de rafraîchissement de 60 Hz et 75 Hz.

Page d'accès aux ports (affichage de serveur de la console locale)

Une fois que vous êtes connecté à la console locale de Dominion KX II, la page d'accès aux ports s'ouvre. Elle répertorie tous les ports de Dominion KX II, les serveurs cible KVM connectés ainsi que leur état et leur disponibilité.

La page Port Acces (Accès aux ports) présente également les châssis de lames configurés dans Dominion KX II. Le châssis de lames s'affiche dans une liste hiérarchique extensible sur la page Port Access ; le châssis de lames est placé à la racine de la hiérarchie et chaque lame est libellée et affichée sous la racine.

Remarque : pour afficher le châssis de lames dans l'ordre hiérarchique, ses sous-types doivent être configurés.

Par défaut, l'onglet View by Port (Afficher par port) apparaît sur la page Port Access. L'onglet View by Group (Afficher par groupe) affiche les mêmes informations que l'onglet View by Ports, toutefois, les ports sont classés suivant les affectations de groupes de ports existants.

No.	Name	Type	Status	Availability
1	BC_Port1_KXName_r2	BladeChassis	up	connected
1-1	BC_Port1_Slot1_To_Local_Port	Blade	-	shared
1-2	Blade_Chassis_Port1_Slot2	Blade	-	-
1-3	Blade_Chassis_Port1_Slot3	Blade	-	-
1-4	Blade_Chassis_Port1_Slot4	Blade	-	-
1-5	Blade_Chassis_Port1_Slot5	Blade	-	-
1-6	Blade_Chassis_Port1_Slot6	Blade	-	-
1-7	Blade_Chassis_Port1_Slot7	Blade	-	-
1-8	Blade_Chassis_Port1_Slot8	Blade	-	-
1-9	Blade_Chassis_Port1_Slot9	Blade	-	-
1-10	Blade_Chassis_Port1_Slot10	Blade	-	-
1-11	Blade_Chassis_Port1_Slot11	Blade	-	-
1-12	Blade_Chassis_Port1_Slot12	Blade	-	-
1-13	Blade_Chassis_Port1_Slot13	Blade	-	-
1-14	Blade_Chassis_Port1_Slot14	Blade	-	-
1-15	Blade_Chassis_Port1_Slot15	Blade	-	-
1-16	Blade_Chassis_Port1_Slot16	Blade	-	-
2	KX2_Port2_CCName_r2	DCIM	up	idle

Pour utiliser la page Port Access :

1. Connectez-vous à la console locale.

Les serveurs cible KVM sont triés initialement par numéro de port. Vous pouvez modifier l'affichage en effectuant le tri sur n'importe quelle colonne.

- Port Number (Numéro de port) - Les ports sont numérotés de 1 au nombre total de ports disponibles pour le dispositif Dominion KX II. Notez que les ports connectés aux barrettes d'alimentation ne figurent pas sur la liste, ce qui génère des blancs dans la séquence des numéros de port.
- Port Name (Nom de port) - Nom du port de Dominion KX II. Initialement, ce champ est paramétré sur Dominion-KX2-Port# mais vous pouvez remplacer ce nom par un autre plus parlant. Lorsque vous cliquez sur un lien Port Name (Nom du port), le menu d'action des ports (Port Action Menu) s'affiche.

Remarque : n'utilisez pas d'apostrophe pour le nom de port (CIM).

- Status (Statut) - Le statut des serveurs cible standard est activé ou désactivé.
- Type - Type de serveur ou CIM. Pour les châssis de lames, ce type peut être Blade Chassis, Blade, BladeChassisAdmin et BladeChassisURL.
- Availability (Disponibilité) - La disponibilité peut être Idle (Inactif), Connected (Connecté), Busy (Occupé) ou Unavailable (Indisponible). Les serveurs lames peuvent être associés à une disponibilité partagée ou exclusive lorsqu'une connexion à cette lame est établie.

2. Cliquez sur View by Port (Afficher par port) ou View by Group (Afficher par groupe) pour passer d'une vue à l'autre.
   - Outre Port Number (Numéro de port), Port Name (Nom de port), Status (Etat), Type et Availability (Disponibilité), une colonne Group apparaît également dans l'onglet View by Group (Afficher par groupe). Cette colonne contient les groupes de ports disponibles.
3. Cliquez sur le nom du port du serveur cible auquel vous souhaitez accéder. Le menu d'action des ports (Port Action Menu) apparaît. Reportez-vous à **Port Action Menu (Menu d'action de ports)** (à la page 48) pour plus d'informations sur les options de menu disponibles.
4. Sélectionnez la commande souhaitée dans le menu d'action des ports.

Pour modifier l'ordre de tri d'affichage :

- Cliquez sur l'en-tête de la colonne par laquelle vous souhaitez effectuer un tri. La liste des serveurs cible KVM est triée par cette colonne.

Raccourcis-clavier et touches de connexion

Comme l'interface de la console locale de Dominion KX II est entièrement remplacée par l'interface du serveur cible auquel vous accédez, un raccourci-clavier est utilisé pour vous déconnecter d'une cible et retourner à l'interface utilisateur du port local. Une touche de connexion permet de se connecter à une cible ou de basculer entre plusieurs cibles.

Le raccourci-clavier du port local vous permet d'accéder rapidement à l'interface utilisateur de la console locale de Dominion KX II lorsqu'un serveur cible est en cours d'affichage. L'opération définie par défaut est d'appuyer deux fois rapidement sur la touche Arrêt défil, mais vous pouvez aussi spécifier une autre combinaison de touches (reportez-vous à la page de paramétrage des ports locaux) comme raccourci-clavier. Reportez-vous à Paramètres du port local de la console locale de Dominion KX II pour plus d'informations.

Exemples de touches de connexion

Serveurs standard	
Action de la touche de connexion	**Exemple de séquence de touches**
Accès à un port depuis l'interface utilisateur du port local	Accès au port 5 depuis l'interface utilisateur du port local : • Appuyez sur la touche Alt > Appuyez sur la touche 5 et relâchez-la > Relâchez la touche Alt
Permutation entre les ports	Passer du port cible 5 au port 11 : • Appuyez sur la touche Alt > Appuyez sur la touche 1 et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Relâchez la touche Alt
Déconnexion d'une cible et retour à l'interface utilisateur du port local	Se déconnecter du port cible 11 et retourner à l'interface utilisateur du port local (la page à partir de laquelle vous vous êtes connecté à la cible) : • Double-clic sur Arrêt défil

Châssis de lames	
Action de la touche de connexion	**Exemple de séquence de touches**
Accès à un port depuis l'interface utilisateur du port local	Accéder au port 5, connecteur 2 : • Appuyez sur la touche Alt > Appuyez sur la touche 5 et relâchez-la > Appuyez sur la touche - et relâchez-la > Appuyez sur la touche 2 et relâchez-la > Relâchez la touche Alt
Permutation entre les ports	Passer du port cible 5, commutateur 2 au port 5, connecteur 11 : • Appuyez sur la touche Alt > Appuyez sur la touche 5 et relâchez-la > Appuyez sur la touche - et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Appuyez sur la touche 1 et relâchez-la > Relâchez la touche Alt
Déconnexion d'une cible et retour à l'interface utilisateur du port local	Se déconnecter du port cible 5, connecteur 11 et retourner à l'interface utilisateur du port local (la page à partir de laquelle vous vous êtes connecté à la cible) : • Double-clic sur Arrêt défil

Combinaisons de touches Sun spéciales

Les combinaisons de touches suivantes pour les touches spéciales du serveur Sun Microsystems fonctionnent sur le port local. Ces touches spéciales sont disponibles dans le menu Clavier lorsque vous vous connectez à un serveur cible Sun :

Touche Sun	Combinaison de touches de port local
Again	Ctrl + Alt + F2
Props	Ctrl + Alt + F3
Undo	Ctrl + Alt + F4
Stop A	Break a
Front	Ctrl + Alt + F5
Copy	Ctrl + Alt + F6

Touche Sun	Combinaison de touches de port local
Open	Ctrl + Alt + F7
Find	Ctrl + Alt + F9
Cut	Ctrl + Alt + F10
Paste	Ctrl + Alt + F8
Muet	Ctrl + Alt + F12
Compose	Ctrl+ Alt + KPAD *
Vol +	Ctrl + Alt + KPAD +
Vol -	Ctrl + Alt + KPAD -
Stop	Aucune combinaison de touches
Alimentation	Aucune combinaison de touches

Accès à un serveur cible

Pour accéder à un serveur cible :

1. Cliquez sur le nom de port de la cible à laquelle vous souhaitez accéder. Le menu d'action des ports apparaît.
2. Sélectionnez Connect (Connecter) dans le menu d'action des ports. L'affichage vidéo bascule sur l'interface du serveur cible.

Retour à l'interface de la console locale de Dominion KX II

Important : le raccourci-clavier par défaut de la console locale de Dominion KX II consiste à appuyer deux fois sans interruption sur la touche Arrêt défil. Cette combinaison de touches peut être modifiée dans la page Local Port Settings (Paramètres du port local). Reportez-vous à Paramètres du port local de la console locale de Dominion KX II.

Pour revenir à la console locale de Dominion KX II à partir du serveur cible :

- Appuyez deux fois rapidement sur le raccourci-clavier (par défaut, la touche Arrêt défil). L'affichage écran passe de l'interface du serveur cible à celle de la console locale de Dominion KX II.

Administration du port local

Dominion KX II peut être géré par la console locale ou par la console distante. Notez que la console locale de Dominion KX II donne également accès à :

- Factory Reset (Réinitialisation des paramètres d'usine)
- Paramètres du port local(disponible également dans la console distante)

Remarque : seuls les utilisateurs disposant des droits d'administrateur peuvent accéder à ces fonctions.

Configuration des paramètres du port local de la console locale de Dominion KX II

A partir de la page de paramétrage du port local, vous avez la possibilité de personnaliser de nombreux paramètres de la console locale de Dominion KX II, notamment le clavier, les raccourcis-clavier, le délai de commutation de l'écran, le mode d'économie d'alimentation, les paramètres de résolution de l'interface utilisateur locale et l'authentification d'utilisateur locale.

Remarque : seuls les utilisateurs disposant des droits d'administrateur peuvent accéder à ces fonctions.

Pour configurer les paramètres du port local :

Remarque : certaines modifications apportées aux paramètres de la page Local Port Settings (Paramètres du port local) redémarrent le navigateur dans lequel vous travaillez. Si un redémarrage doit se produire lorsqu'un paramètre est modifié, il est indiqué dans la procédure fournie ici.

1. Sélectionnez Device Settings (Paramètres du dispositif) > Local Port Configuration (Configuration du port local). La page des paramètres du port local s'ouvre.
2. Sélectionnez le type de clavier approprié parmi les options de la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - US
   - US/International (Anglais Etats-Unis/international)
   - United Kingdom
   - Français (France)
   - Allemand (Allemagne)

- Japonais (JIS)
- Chinois simplifié
- Chinois traditionnel
- Dubeolsik Hangul (Coréen)
- Allemand (Suisse)
- Portugais (Portugal)
- Norvégien (Norvège)
- Suédois (Suède)
- Danois (Danemark)
- Belge (Belgique)

Remarque : l'utilisation du clavier pour le chinois, le japonais et le coréen ne concerne que l'affichage. La saisie dans la langue locale n'est pas prise en charge pour le moment pour les fonctions de la console locale de Dominion KX II.

3. Sélectionnez le raccourci-clavier du port local. Le raccourci-clavier du port local vous permet de retourner à l'interface de la console locale de Dominion KX II lorsque l'interface d'un serveur cible est affichée. Le paramètre par défaut est Double Click Scroll Lock (Double-clic sur Arrêt défil), mais vous pouvez également sélectionner n'importe quelle combinaison de touches dans la liste déroulante :

Raccourci-clavier :	Appuyez sur :
Double-clic sur Arrêt défil	La touche Arrêt défil deux fois sans interruption
Double-clic sur Verr num	La touche Verr num deux fois sans interruption
Double-clic sur Verr. maj.	La touche Verr. maj. deux fois sans interruption
Double-clic sur Alt	La touche Alt deux fois sans interruption
Double-clic sur Maj gauche	La touche Maj gauche deux fois sans interruption
Double-clic sur la touche Ctrl gauche	La touche Ctrl gauche deux fois sans interruption

4. Sélectionnez la touche de connexion du port local. Utilisez une séquence de touches pour la connexion à une cible et la permutation vers une autre. Vous pouvez alors utiliser le raccourci-clavier pour la déconnexion de la cible et le retour à l'interface utilisateur du port local. La touche de connexion fonctionne pour les serveurs standard et les châssis de lames. Une fois la touche de connexion du port local créée, elle apparaît dans le panneau de navigation de l'interface utilisateur. Vous pouvez alors l'employer comme référence. Reportez-vous à ***Exemples de touches de connexion*** (à la page 266) pour obtenir des exemples de séquences de touches de connexion.
5. Réglez Video Switching Delay (Délai de commutation écran) entre 0 et 5 secondes, le cas échéant. En général, la valeur 0 est utilisée à moins que vous n'ayez besoin de plus de temps (certains écrans nécessitent plus de temps pour commuter la vidéo).
6. Si vous souhaitez utiliser la fonction d'économie d'alimentation électrique.
   a. Cochez la case Power Save Mode (Mode d'économie d'alimentation).
   b. Définissez le laps de temps (en minutes) à l'issue duquel le mode d'économie d'alimentation est lancé.
7. Sélectionnez la résolution de la console locale de Dominion KX II dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - 800 x 600
   - 1024 x 768
   - 1280 x 1024
8. Sélectionnez le taux de rafraîchissement dans la liste déroulante. Le navigateur redémarrera lorsque cette modification sera effectuée.
   - 60 Hz
   - 75 Hz
9. Sélectionnez le type d'authentification d'utilisateur locale.
   - Local/LDAP/RADIUS. Il s'agit de l'option recommandée. Pour plus d'informations sur l'authentification, reportez-vous à ***Authentification à distance*** (à la page 39).
   - Aucun. Aucun processus d'authentification n'a lieu pour l'accès à la console locale. Cette option est recommandée pour les environnements sécurisés uniquement.
   - Cochez la case Ignore CC managed mode on local port (Ignorer le mode géré par CC sur le port local) si vous souhaitez un accès utilisateur local à Dominion KX II même si le dispositif est géré par CC-SG.

Remarque : si vous choisissez au départ d'ignorer le mode CC Manage (Gestion par CC) sur le port local, mais souhaitez par la suite un accès au port local, vous devez désactiver la gestion par CC-SG (depuis CC-SG) du dispositif. Vous pourrez alors cocher cette case.

10. Cliquez sur OK.

Configuration des paramètres du port local de Dominion KX II depuis la console locale

Les ports locaux standard et étendu peuvent être configurés depuis la console distante sur la page Port Configuration ou depuis la console locale sur la page Local Port Settings (Paramètres du port local). Reportez-vous à ***Configuration des paramètres du port local de Dominion KX II*** (à la page 200) pour en savoir plus sur la configuration de ces ports.

Réinitialisation des paramètres d'usine de la console locale de Dominion KX II

Remarque : cette fonction est disponible sur la console locale de Dominion KX II uniquement.

Dominion KX II offre plusieurs types de modes de réinitialisation à partir de l'interface utilisateur de la console locale.

*Remarque : il est recommandé d'enregistrer le journal d'audit avant de procéder à la réinitialisation des paramètres d'usine. Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de réinitialisation n'est pas consigné dans le journal d'audit. Pour plus d'informations sur l'enregistrement du journal d'audit, reportez-vous à **Journal d'audit** (à la page 227).*

Pour procéder à une réinitialisation des paramètres d'usine :

1. Choisissez Maintenance > Factory Reset (Maintenance > Réinitialisation des paramètres usine). La page de réinitialisation des paramètres d'usine s'ouvre.
2. Choisissez l'option de réinitialisation appropriée parmi les suivantes :

- Full Factory Reset (Réinitialisation intégrale des paramètres d'usine) : supprime la totalité de la configuration et rétablit complètement les paramètres d'usine du dispositif. Notez que toute association de gestion avec CommandCenter est interrompue. En raison du caractère intégral de cette réinitialisation, vous êtes invité à confirmer la réinitialisation des paramètres d'usine.
- Network Parameter Reset (Réinitialisation des paramètres réseau) : rétablit les paramètres réseau du dispositif aux valeurs par défaut (cliquez sur Device Settings (Paramètres du dispositif) > Network Settings (Paramètres réseau) pour accéder à ces informations) :
  - IP auto configuration (Configuration IP automatique)
  - IP address (Adresse IP)
  - Subnet mask (masque de sous-réseau)
  - Gateway IP address (Adresse IP de passerelle)

- Primary DNS server IP address (Adresse IP du serveur DNS primaire)
- Adresse IP du serveur DNS secondaire (Adresse IP du serveur DNS secondaire)
- Discovery port (Port de détection)
- Bandwidth limit (Limite de bande passante)
- LAN interface speed & duplex (Vitesse & duplex de l'interface LAN).
- Enable automatic failover (Activer le basculement automatique)
- Ping interval (seconds) (Intervalle Ping (secondes))
- Timeout (seconds) (Temporisation (secondes))

1. Cliquez sur Reset (Réinitialiser) pour continuer. Vous êtes invité à confirmer la réinitialisation des paramètres d'usine car tous les paramètres réseau seront effacés définitivement.
2. Cliquez sur OK pour continuer. Quand vous avez terminé, le dispositif Dominion KX II est automatiquement redémarré.

Réinitialisation de Dominion KX II à l'aide du bouton de réinitialisation

Sur le panneau arrière du dispositif figure un bouton Reset (Réinitialiser). Il est encastré pour éviter les réinitialisations accidentelles (vous aurez besoin d'un objet pointu pour utiliser ce bouton).

Les opérations effectuées lorsque le bouton de réinitialisation est enfoncé sont définies dans l'interface utilisateur graphique. Reportez-vous à Cryptage et partage.

Remarque : il est recommandé d'enregistrer le journal d'audit avant de procéder à la réinitialisation des paramètres d'usine. Le journal d'audit est effacé lorsqu'une réinitialisation des paramètres d'usine est effectuée et l'événement de réinitialisation n'est pas consigné dans le journal d'audit. Pour plus d'informations sur l'enregistrement du journal d'audit, reportez-vous à **Journal d'audit** *(à la page 227).*

Pour réinitialiser le dispositif :

1. Mettez Dominion KX II hors tension.
2. Utilisez un objet pointu pour appuyer sur le bouton Reset (Réinitialiser) et pour le maintenir.
3. Tout en continuant à maintenir enfoncé le bouton Reset, mettez à nouveau sous tension le dispositif Dominion KX II.

4. Continuez de maintenir le bouton enfoncé pendant 10 secondes. Une fois l'unité réinitialisée, deux bips courts signalent la fin de l'opération.

Annexe A Spécifications

Dans ce chapitre

Spécifications physiques 276
Impératifs d'environnement 279
Modules d'interface pour ordinateur (CIM) 279
Systèmes d'exploitation et CIM pris en charge (serveurs cible) 281
Systèmes d'exploitation pris en charge (Clients) 287
Navigateurs pris en charge.....288
Modems certifiés 289
Dispositifs pris en charge par le port local étendu de KX2-832 et de KX2-864.....289
Distance de connexion et résolution vidéo du serveur cible 289
Distances maximales recommandées pour le port local étendu de KX2-832 et de KX2-864.....290
Connexion à distance 290
Résolutions vidéo prises en charge 291
Langues de clavier prises en charge.....292
Lecteurs de cartes à puce 293
Ports TCP et UDP utilisés 297
Paramètres de vitesse réseau.....299

Spécifications physiques

Spécifications de Dominion KX II

Numéro de référence	Description de l'élément de ligne	Code UPC	Alimentation	Poids	Dimensions du produit (LxPxH)	Poids à l'expédition	Dimensions à l'expédition (LxPxH)
DKX2-108	Dominion KX II à 8 ports avec accès réseau et port local 1 utilisateur ; support virtuel, double alimentation	785813624109	Double alimentation 100/240 V 50/60 Hz 0,6A 25 watts	8,58 lb	1,75" x 17,32" x 11,4"	14,3 lb	22" x 16,6" x 6,5"
				3,9 kg	44 mm x 439 mm x 290 mm	6,5 kg	559 mm x 422 mm x 165 mm
DKX2-116	Dominion KX II à 16 ports avec accès réseau et port local 1 utilisateur ; support virtuel, double	785813624055	Double alimentation 100/240 V 50/60 Hz 0,6A 25,4 watts	8,65 lb	1,75" x 17,3" x 11,4"	14,85 lb	22" x 16,6" x 6,5"
				3,9 kg	44 mm x 439 mm x 290 mm	6,7 kg	559 mm x 422 mm x 165 mm

Numéro de référence	Description de l'élément de ligne	Code UPC	Alimentation	Poids	Dimensions du produit (LxPxH)	Poids à l'expédition	Dimensions à l'expédition (LxPxH)
	alimentation						
DKX2-132	Dominion KX II à 32 ports avec accès réseau et port local 1 utilisateur ; support virtuel, double alimentation	785813624079	Double alimentation 100/240 V 50/60 Hz 0,6A 26 watts	9 lb	1,75" x 17,3" x 11,4"	14,9 lb	22" x 16,6" x 6,5"
				4,1 kg	44 mm x 439 mm x 290 mm	6,8 kg	559 mm x 422 mm x 165 mm
DKX2-216	Dominion KX II à 16 ports avec accès réseau et port local 2 utilisateurs ; support virtuel, double alimentation	785813624086	Double alimentation 100/240 V 50/60 Hz 0,6A 26,3 watts	8,65 lb	1,75" x 17,3" x 11,4"	14,49 lb	22" x 16,6" x 6,5"
				3,9 kg	44 mm x 439 mm x 290 mm	6,6 kg	559 mm x 422 mm x 165 mm
DKX2-232	Dominion KX II à 32 ports avec accès réseau et port local 2 utilisateurs ; support virtuel, double alimentation	785813625021	Double alimentation 100/240 V 50/60 Hz (optimal 47 - 63 Hz) 0,6 A 27 watts	9,0 lb	1,75" x 17,3" x 11,4"	14,9 lb	22" x 16,6" x 6,5"
				4,1 kg	44 mm x 439 mm x 290 mm	6,8 kg	559 mm x 422 mm x 165 mm
DKX2-416	Dominion KX II à 16 ports avec accès réseau et port local 4 utilisateurs ; support virtuel, double alimentation	785813625359	Double alimentation 100/240 V 50/60 Hz 1A 62 watts	9,04 lb	17,3” x 11,6” x 1,75”	14,94 lb	22” x 16,5” x 6,5”
				4,1 kg	440 mm x 295 mm x 44 mm	6,8 kg	560 mm x 420 mm x 165 mm
DKX2-432	Dominion KX II à 32 ports avec accès réseau et port local	785813625380	Double alimentation 100/240 V 50/60 Hz	9,48 lb	17,3” x 11,6” x 1,75”	15,38 lb	22” x 16,5” x 6,5”
				4,3 kg	440 mm x 295 mm x 44	7,0 kg	560 mm x 420 mm x 165 mm

Numéro de référence	Description de l'élément de ligne	Code UPC	Alimentation	Poids	Dimensions du produit (LxPxH)	Poids à l'expédition	Dimensions à l'expédition (LxPxH)
	4 utilisateurs ; support virtuel, double alimentation		1A 64 watts		mm		
DKX2-464	Dominion KX II à 64 ports avec accès réseau et port local 4 utilisateurs ; support virtuel, double alimentation	785813625298	Double alimentation 100/240 V 50/60 Hz 1A 64 watts	11,29 lb	17,3” x 11,6” x 3,5”	19,8 lb	22” x 16,5” x 6,5”
				5,12 kg	440 mm x 295 mm x 88 mm	9 kg	560 mm x 420 mm x 165 mm

Spécifications de KX2-8

Numéro de référence	Description de l'élément de ligne	Code UPC	Alimentation	Poids	Dimensions du produit (LxPxH)	Poids à l'expédition	Dimensions à l'expédition (LxPxH)
DKX2-832	Dominion KX II à 32 ports avec accès réseau 8 utilisateurs, port local standard, port local étendu, support virtuel, double alimentation	0785813620019	Double alimentation 100/240 V 50/60 Hz 1A (0,5A) 64 watts	10,57 lb	17,3” x 14,2” x 1,73”	35,90 lb	22” x 18,5” x 11”
				4,8 kg	440 mm x 360 mm x 44 mm	16,3 kg	560 mm x 470 mm x 280 mm
DKX2-864	Dominion KX II à 64 ports avec accès réseau 8 utilisateurs, port local standard, port local étendu, support virtuel, double alimentation	0785813620026	Double alimentation 100/240 V 50/60 Hz 1,2A 64 watts	13,22 lb	17,3” x 14,6” x 3,5”	22,47 lb	21,7” x 20,1” x 7,5”
				6,0 kg	440 mm x 370 mm x 88 mm	10,2 kg	550 mm x 510 mm x 190 mm

Impératifs d'environnement

En fonctionnement	
Température	0°C- 40°C
Humidité	20 à 85 % HR
Altitude	S/O
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°C- 50°C
Humidité	10 à 90 % HR
Altitude	S/O
Vibrations	5-55-5 Hz, 0,38 mm, 1 minute par cycle ; 30 minutes par axe (X,Y,Z)
Chocs	S/O

Modules d'interface pour ordinateur (CIM)

Numéro de référence	Description de l'élément de ligne	Poids du produit	Dimensions du produit (LxPxH)	Poids à l'expédition	Dimensions à l'expédition (LxPxH)	Code UPC
D2CIM-VUSB	Module d'interface pour ordinateurs Dominion KX II [Port USB avec support virtuel]	91 g	33 mm x 76 mm x 15 mm	91 g	183 mm x 229 mm x 15 mm	785813332004
DCIM-PS2	Module d'interface pour ordinateur Dominion KX I & II [Port PS/2]	91 g	33 mm x 76 mm x 15 mm	91 g	183 mm x 229 mm x 15 mm	785813338532
DCIM-USB	Module d'interface pour ordinateur	91 g	33 mm x 76 mm x 15 mm	91 g	183 mm x 229 mm x 15 mm	785813338518

Numéro de référence	Description de l'élément de ligne	Poids du produit	Dimensions du produit (LxPxH)	Poids à l'expédition	Dimensions à l'expédition (LxPxH)	Code UPC
	Dominion KX I & II [Port USB]					
DCIM-SUSB	Module d'interface pour ordinateur Dominion KX I & II [Port USB pour Sun]	91 g	33 mm x 76 mm x 15 mm	91 g	183 mm x 229 mm x 15 mm	785813338556
DCIM-USBG2	Module d'interface pour ordinateur CIM G2 Dominion KX I & II [Port USB et Sun USB]	91 g	33 mm x 76 mm x 15 mm	91 g	183 mm x 229 mm x 15 mm	785813338884
DCIM-SUN	Module d'interface pour ordinateurs Dominion KX I & II [Port Sun, vidéo HD15]	91 g	33 mm x 76 mm x 15 mm	91 g	183 mm x 229 mm x 15 mm	785813338549
D2CIM-PWR	Module d'interface pour ordinateur Dominion KX II pour barrettes d'alimentation à distance	91 g	33 mm x 76 mm x 15 mm	91 g	183 mm x 229 mm x 15 mm	785813332011
D2CIM-VUSB-32PAC	Lot de 32 D2CIM-VUSB	2,90 kg	(33 mm x 76 mm x 15 mm)*32	3,63 kg	550 mm x 310 mm x 110 mm	785813332028
D2CIM-VUSB -64PAC	Lot de 64 D2CIM-VUSB	5,81 kg	(33 mm x 76 mm x 15 mm)*64	18,13 lb	22,64"x9,45" x12,99"	785813332035
D2CIM-DVUSB	Module d'interface pour ordinateur Dominion KX II [Port double USB avec support virtuel]	105 g	3,53”x1,68”x0,76” 89,7 x 42,7 x 19,3 mm	112,5 g	3,9”x 5,7”x 1,0” 100*145*27 mm	785813339508

Numéro de référence	Description de l'élément de ligne	Poids du produit	Dimensions du produit (LxPxH)	Poids à l'expédition	Dimensions à l'expédition (LxPxH)	Code UPC
D2CIM-DVUSB-32PAC	Lot de 32 D2CIM-DVUSB	4,6 kg	21,9”x12,2”x4,3” 555 x 310 x 110 mm	4,6 kg	21,9”x12,2”x4,3” 555 x 310 x 110 mm	785813332080
D2CIM-DVUSB -64PAC	Lot de 64 D2CIM-DVUSB	10,2 kg	9,4”x22,6”x13,0” 240 x 575 x 330 mm	10,2 kg	9,4”x22,6”x13,0” 240*575*330 mm	785813332097

Systèmes d'exploitation et CIM pris en charge (serveurs cible)

Outre les nouveaux D2CIM Dominion KX II, la plupart des CIM Paragon® et CIM Dominion KX I sont pris en charge. Le tableau suivant indique les systèmes d'exploitation des serveurs cible, les CIM, les supports virtuels et les modes souris pris en charge :

Remarque : seuls les systèmes d'exploitation 32 bits pour les serveurs cible Windows et Linux sont pris en charge pour les dispositifs de première génération.

CIM Paragon pris en charge	Système d'exploitation et dispositifs série (le cas échéant)	Support virtuel	Mode Souris absolue	Mode Souris intelligente	Mode Souris standard
• P2CIM-PS2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • IBM AIX • HP UX			✓	✓
• P2CIM-AUSB • UUSBPD	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • IBM AIX • HP UX • Mac OS			✓	✓

CIM Paragon pris en charge	Système d'exploitation et dispositifs série (le cas échéant)	Support virtuel	Mode Souris absolue	Mode Souris intelligente	Mode Souris standard
• UKVMPD	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11			✓	✓
• P2CIM-SUN • P2CIM-SUSB	• Tous les systèmes d'exploitation Solaris pris en charge dans Dominion KX I				✓
• P2CIM-SER	• Dispositifs série				

DCIM Dominion KX I pris en charge	Serveur cible	Support virtuel	Mode Souris absolue	Mode Souris intelligente	Mode Souris standard
• DCIM-PS2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora Core 3 et supérieur • IBM AIX • HP UX			✓	✓
• DCIM-USB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS • IBM AIX • HP UX			✓	✓

DCIM Dominion KX I pris en charge	Serveur cible	Support virtuel	Mode Souris absolue	Mode Souris intelligente	Mode Souris standard
• DCIM-USBG2	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS • Tous les systèmes d'exploitation Solaris pris en charge dans Dominion KX I • IBM AIX • HP UX			✓	✓
Remarque : DCIM-USBG2 présente un petit commutateur à l'arrière du CIM. Placez le commutateur sur P pour les serveurs cible USB PC ; placez-le sur S pour les serveurs cible USB Sun. Une nouvelle position de commutateur ne prend effet qu'après l'alimentation cyclique du CIM. Pour effectuer l'alimentation cyclique du CIM, retirez le connecteur USB du serveur cible, puis rebranchez-le quelques secondes plus tard.					
• DCIM-SUN • DCIM-SUSB	• Tous les systèmes d'exploitation Solaris pris en charge dans Dominion KX I			✓	✓

D2CIM Dominion KX II pris en charge	Serveur cible et barrettes d'alimentation à distance (le cas échéant)	Support virtuel	Mode Souris absolue	Mode Souris intelligente	Mode Souris standard
• D2CIM-VUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora Core 3 et supérieur • Red Hat Enterprise Linux 4 ES • Red Hat Enterprise Linux 5 • Mac OS	✓	✓	✓	✓
Remarque : D2CIM-VUSB n'est pas pris en charge sur les serveurs cible Sun (Solaris).					
• D2CIM-DVUSB	• Windows XP • Windows 2000 • Windows 2000 Server • Windows 2003 Server • Windows Vista • Windows 7 • Windows 2008 • Open SUSE 10, 11 • Fedora 8 - 11 • Mac OS	✓	✓	✓	✓
• D2CIM-PWR	• Barrettes d'alimentation à distance				

Systèmes d'exploitation pris en charge (Clients)

Les systèmes d'exploitation suivants sont pris en charge sur Virtual KVM Client et Multi-Platform Client (MPC) :

Système d'exploitation client	Prise en charge des supports virtuels (VM) sur client
Windows 7®	Oui
Windows XP®	Oui
Windows 2008®	Oui
Windows Vista®	Oui
Windows 2000 SP4® Server	Oui
Windows 2003® Server	Oui
Windows 2008® Server	Oui
Red Hat® Desktop 5.0	Oui. Image ISO conservée localement, montage du serveur de fichiers distant directement à partir de Dominion KX II.
Red Hat Desktop 4.0	Oui. Image ISO conservée localement, montage du serveur de fichiers distant directement à partir de Dominion KX II.
Open SUSE 10, 11	Oui. Image ISO conservée localement, montage du serveur de fichiers distant directement à partir de Dominion KX II.
Fedora™ 8 - 11	Oui. Image ISO conservée localement, montage du serveur de fichiers distant directement à partir de Dominion KX II.
Mac OS	Non
Solaris	Non

Le plug-in JRE est disponible pour les systèmes d'exploitation Windows 32 bits et 64 bits. MPC et VKC peuvent être lancés uniquement à partir d'un navigateur 32 bits, ou d'un navigateur 64 bits IE7 ou IE8.

Les prérequis des systèmes d'exploitation Windows Java 32 bits et 64 bits sont donnés ci-après.

Mode	Système d'exploitation	Navigateur
Windows x64 mode 32 bits	Windows XP	• IE 6.0 SP1+ ou 7.0, IE 8 • Mozilla 1.4.X ou 1.7+ • Netscape 7.X • Firefox 1.06 - 3
	Windows Server 2003	• IE 6.0 SP1++, IE 7, IE 8 • Mozilla 1.4.X ou 1.7+ • Netscape 7.X • Firefox 1.06 - 3
	Windows Vista	• IE 7.0 ou 8.0
Windows x64 mode 64 bits	Windows XP	SE 64 bits, navigateurs 32 bits : • IE 6.0 SP1+, 7.0 ou 8.0 • Mozilla 1.4.X ou 1.7+ • Netscape 7.X • Firefox 1.06 - 3 Mode 64 bits, navigateurs 64 bits : • IE 7.0 ou 8.0
	Windows XP Professionnel	
	Windows XP Edition Tablet PC	
	Windows Vista	
	Windows Server 2003	
	Windows Server 2008	

Navigateurs pris en charge

Dominion KX II prend en charge les navigateurs suivants :

- Internet Explorer 6, 7 et 8
- Firefox 1.5, 2.0 et 3.0 (jusqu'à la version 3.0.10)
- Mozilla 1.7
- Safari 2.0

Modems certifiés

- US Robotics 56K 5686E
- ZOOM v90
- ZOOM v92
- US Robotics Sportster 56K
- US Robotics Courier 56K

Dispositifs pris en charge par le port local étendu de KX2-832 et de KX2-864

Le port local étendu prend en charge la connexion des dispositifs suivants :

- Station utilisateur Paragon II (P2-UST) connectée directement au port local étendu.
- Station utilisateur optimisée Paragon II (P2-EUST) connectée directement au port local étendu.
- Récepteur URKVMG Cat5Reach connecté directement au port local étendu.
- Port cible de commutateur KVM analogique Paragon II (UMT) connecté directement au port local étendu. Permet un accès supplémentaire au port local étendu, lorsqu'il est utilisé avec la station utilisateur optimisée Paragon II.

Distance de connexion et résolution vidéo du serveur cible

La distance maximale prise en charge dépend de plusieurs facteurs, notamment le type/la qualité du câble Cat5, le type et le fabricant du serveur, le pilote et l'écran vidéo, les conditions de l'environnement et les attentes de l'utilisateur. Le tableau suivant indique la distance maximale du serveur cible pour différentes résolutions vidéo et taux de rafraîchissement :

Résolution vidéo	Taux de rafraîchissement	Distance maximale
1600 x 1200	60	15 m
1280 x 1024	60	30 cm
1024 x 768	60	45 m

Remarque : en raison de la diversité des types et fabricants de serveurs, des versions de systèmes d'exploitation, des pilotes vidéo, etc. et de la nature subjective de la qualité vidéo, Raritan ne peut pas garantir les performances sur toutes les distances et dans tous les environnements.

Reportez-vous à ***Résolutions vidéo prises en charge*** (à la page 291) pour connaître les résolutions vidéo prises en charge par Dominion KX II.

Distances maximales recommandées pour le port local étendu de KX2-832 et de KX2-864

Dispositif étendu	1 024 x 768 à 60 Hz	1280 x 1024 à 60 Hz
Paragon II UMT avec EUST	1000	900
Paragon EUST	500	400
URKVM	650	250
Paragon UST	500	200

Connexion à distance

Connexion à distance	Détails
Réseau	Ethernet 10BASE-T, 100BASE-T et 1000BASE-T (Gigabit)
Protocoles	TCP/IP, UDP, SNTP, HTTP, HTTPS, RADIUS, LDAP/LDAPS

Résolutions vidéo prises en charge

Assurez-vous que la résolution vidéo et le taux de rafraîchissement de chaque serveur cible sont pris en charge par l'unité Dominion KX II, et que le signal est non entrelacé.

La résolution vidéo et la longueur de câble sont des facteurs importants dans la réalisation de la synchronisation de la souris. Reportez-vous à ***Distance de connexion et résolution vidéo du serveur cible*** (à la page 289).

L'unité Dominion KX II prend en charge ces résolutions :

Résolutions	
640 x 350 à 70Hz	1024 x 768 à 75Hz
640 x 350 à 85Hz	1024 x 768 à 90Hz
640 x 400 à 56Hz	1024 x 768 à 100Hz
640 x 400 à 84Hz	1152 x 864 à 60Hz
640 x 400 à 85Hz	1152 x 864 à 70Hz
640 x 480 à 60Hz	1152 x 864 à 75Hz
640 x 480 à 66,6Hz	1152 x 864 à 85Hz
640 x 480 à 72Hz	1152 x 870 à 75,1Hz
640 x 480 à 75Hz	1152 x 900 à 66Hz
640 x 480 à 85Hz	1152 x 900 à 76Hz
720 x 400 à 70Hz	1280 x 720 à 60Hz
720 x 400 à 84Hz	1280 x 960 à 60Hz
720 x 400 à 85Hz	1280 x 960 à 85Hz
800 x 600 à 56Hz	1280 x 1024 à 60Hz
800 x 600 à 60Hz	1280 x 1024 à 75Hz
800 x 600 à 70Hz	1280 x 1024 à 85Hz
800 x 600 à 72Hz	1360 x 768 à 60Hz
800 x 600 à 75Hz	1366 x 768 à 60Hz
800 x 600 à 85Hz	1368 x 768 à 60Hz
800 x 600 à 90Hz	1400 x 1050 à 60Hz
800 x 600 à 100Hz	1440 x 900 à 60Hz
832 x 624 à	1600 x 1200 à 60Hz

Résolutions	
75,1Hz	
1024 x 768 à 60Hz	1680 x 1050 à 60Hz

Remarque : la synchronisation composite et la vidéo Sync-on-Green nécessitent un adaptateur supplémentaire.

Remarque : certaines résolutions ne sont peut-être pas disponibles par défaut. Si une résolution n'apparaît pas, branchez d'abord le moniteur, débranchez-le, puis branchez le CIM.

Remarque : si les résolutions 1440x900 et 1680x1050 ne s'affichent pas, mais sont prises en charge par la carte graphique du serveur cible, un adaptateur DDC-1440 ou DDC-1680 peut être nécessaire.

Langues de clavier prises en charge

L'unité Dominion KX II fournit un support clavier pour les langues indiquées dans le tableau suivant.

Remarque : vous pouvez utiliser le clavier pour le chinois, le japonais et le coréen à des fins d'affichage uniquement ; l'entrée de données dans la langue locale n'est pas prise en charge pour le moment en ce qui concerne les fonctions de la console locale de Dominion KX II. Pour plus d'informations sur les claviers non US, reportez-vous à **Remarques d'informations** *(à la page 309).*

Remarque : Raritan recommande d'utiliser systèm-config-clavier pour modifier les langues si vous travaillez dans un environnement Linux.

Langue/clavier	Régions	Disposition du clavier
Anglais américain	Etats-Unis d'Amérique et la plupart des pays anglophones : par exemple, Canada, Australie et Nouvelle-Zélande.	Disposition du clavier américain
Anglais américain international	Etats-Unis d'Amérique et pays dont les langues n'utilisent pas de caractères spéciaux : par exemple, les Pays-Bas.	Disposition du clavier américain
Anglais britannique	United Kingdom	Disposition du clavier britannique
Chinois traditionnel	Hong Kong RAS, République de Chine (Taïwan)	Chinois traditionnel
Chinois	République populaire de Chine	Chinois simplifié

Langue/clavier	Régions	Disposition du clavier
simplifié		
Coréen	Corée du Sud	Hangeul mode Dubeolsik
Japonais	Japon	Clavier JIS
Français	France	Disposition du clavier français (AZERTY)
Allemand	Allemagne et Autriche	Clavier allemand (disposition QWERTZ)
Belge	Belgique	Belge
Norvégien	Norvège	Norvégien
Danois	Danemark	Danois
Suédois	Suède	Suédois
Hongrois	Hongrie	Hongrois
Slovène	Slovénie	Slovène
Italien	Italie	Italien
Espagnol	Espagne et la plupart des pays hispanophones	Espagnol
Portugais	Portugal	Portugais

Lecteurs de cartes à puce

Lecteurs de cartes à puce pris en charge ou non

Seuls les lecteurs de cartes à puce externes de type USB sont pris en charge par Dominion KX II.

Lecteurs de cartes à puce pris en charge

Type	Fabricant	Modèle	Vérifié
USB	SCM Microsystems	SCR331	Vérifié en local et à distance
USB	ActivIdentity	Lecteur USB v2.0 ActivIdentity	Vérifié en local et à distance
USB	ActivIdentity	Lecteur USB v3.0 ActivIdentity	Vérifié en local et à distance

Type	Fabricant	Modèle	Vérifié
USB	SCM Microsystems	SCR331	Vérifié en local et à distance
USB	Gemalto	GemPC USB-SW	Vérifié en local et à distance
Clavier avec lecteur de cartes USB	Dell	Clavier/Lecteur de cartes à puce USB	Vérifié en local et à distance
Clavier avec lecteur de cartes USB	Cherry GmbH	G83-6744 SmartBoard	Vérifié en local et à distance
Lecteur USB de cartes SIM	Omnikey	6121	Vérifié en local et à distance
Intégré (Dell Latitude D620)	O2Micro	OZ776	En local uniquement
PCMCIA	ActivIdentity	Lecteur PCMCIA ActivIdentity	En local uniquement
PCMCIA	SCM Microsystems	SCR243	En local uniquement

Remarque : les lecteurs de cartes à puce SCR331 SCM Microsystems doivent utiliser le firmware SCM Microsystems v5.25.

Lecteurs de cartes à puce non pris en charge

Ce tableau contient la liste des lecteurs testés par Raritan qui, à notre connaissance, ne fonctionnent pas avec Dominion KX II et ne sont donc pas pris en charge. Si un lecteur de cartes à puce n'apparaît ni dans le tableau des lecteurs pris en charge ni dans celui des lecteurs non pris en charge, Raritan ne peut pas garantir qu'il fonctionne avec Dominion KX II.

Type	Fabricant	Modèle	Remarques
Clavier avec lecteur de cartes USB	HP	ED707A	Point de terminaison sans interruption => non compatible avec pilote Microsoft
Clavier avec lecteur de cartes USB	SCM Microsystems	SCR338	Mise en œuvre de lecteur de cartes propriétaire (non compatible CCID)
Jeton USB	Aladdin	eToken PRO	Mise en œuvre propriétaire

Configuration système minimale requise

Exigences en matière de port local

L'exigence en matière d'interopérabilité de base pour la connexion du port local au Dominion KX II est la suivante :

- Tous les dispositifs (lecteur de cartes à puce ou jeton) connectés localement doivent être compatibles USB CCID.

Exigences en matière de serveur cible

Pour l'utilisation de lecteurs de cartes à puce, les exigences de base en matière d'interopérabilité au niveau du serveur cible sont les suivantes :

- Le gestionnaire IFD (lecteur de cartes à puce) doit être un pilote de périphérique CCID USB standard (comparable au pilote CCID USB Microsoft générique).
- Un D2CIM-DVUSB (CIM double VM) est nécessaire et doit utiliser la version de firmware 3A6E ou supérieure.
- Les connexions de serveurs avec châssis de lames, où un CIM par lame est utilisé, sont prises en charge.
- Ce type de connexions, où un CIM par châssis est utilisé, n'est pris en charge que pour les modèles E et H d'IBM BladeCenter où la détection automatique est activée.

Cibles Windows XP

Les cibles Windows XP doivent exécuter Windows XP SP3 afin d'utiliser des cartes à puce avec Dominion KX II.

Cibles Linux

Si vous utilisez une cible Linux, les exigences suivantes doivent être respectées pour permettre l'utilisation de lecteurs de cartes à puce avec Dominion KX II.

- Exigences CCID

  Si D2CIM-DVUSB VM/CCID Raritan n'est pas reconnu en tant que lecteur de cartes à puce par votre cible Linux, il vous faudra peut-être mettre à jour la version du pilote CCID à 1.3.8 ou supérieure, et le fichier de configuration du pilote (Info.plist).

Système d'exploitation	Exigences CCID
RHEL 5	ccid-1.3.8-1.el5
SuSE 11	pcsc-ccid-1.3.8-3.12

Fedora Core 10	ccid-1.3.8-1.fc10.i386

Exigences en matière de client distant

Les exigences de base en matière d'interopérabilité au niveau du client distant sont les suivantes :

- Le gestionnaire IFD (lecteur de cartes à puce) doit être un pilote de périphérique compatible PC/SC.
- Le gestionnaire de ressources ICC (carte à puce) doit être disponible et compatible PC/SC.
- Le programme JRE 1.6.x avec interface API pour carte à puce doit être disponible pour être utilisé par l'application cliente Raritan.

Clients Linux

Si vous utilisez un client Linux, les exigences suivantes doivent être respectées pour permettre l'utilisation de lecteurs de cartes à puce avec Dominion KX II.

Remarque : la connexion de l'utilisateur au client, à l'insertion d'une carte à puce, peut durer plus longtemps si une ou plusieurs sessions KVM sont actives vers les cibles. Le processus de connexion à ces cibles est en effet en cours.

- Exigences PC/SC

Système d'exploitation	PC/SC requis
RHEL 5	pcsc-lite-1.4.4-0.1.el5
SuSE 11	pcsc-lite-1.4.102-1.24
Fedora Core 10	pcsc-lite-1.4.102.3.fc10.i386

- Créer un lien vers la bibliothèque Java

  Un lien symbolique doit être créé vers libpcsclite.so après la mise à niveau de RHEL 4, RHEL 5 et FC 10. Par exemple, ln –s /usr/lib/libpcsclite.so.1 /usr/lib/libpcsclite.so, en supposant que l'installation du progiciel ait placé les bibliothèques dans /usr/lib ou /user/local/lib.

- Démon PC/SC

  Lorsque le démon pcsc (gestionnaire de ressources dans framework) est redémarré, relancez le navigateur et MPC.

Ports TCP et UDP utilisés

Port	Description
HTTP, Port 80	Toutes les requêtes reçues par Dominion KX II via HTTP (port 80) sont automatiquement transmises à HTTPS pour garantir une sécurité complète. Pour plus de facilité, Dominion KX II répond au port 80 (les utilisateurs n'ont ainsi pas à taper explicitement dans le champ URL pour accéder à Dominion KX II) tout en préservant un niveau complet de sécurité.
HTTP, Port 443	Ce port est utilisé à diverses fins, notamment pour le serveur Web du client HTML, le téléchargement du logiciel client (MPC/VKC) sur l'hôte du client et le transfert de flux de données KVM et de support virtuel vers le client.
Protocole Dominion KX II (Raritan KVM sur IP), Port 5000 configurable	Ce port est utilisé pour détecter d'autres dispositifs Dominion et pour la communication entre les dispositifs et les systèmes Raritan, CC-SG inclus. Le port défini par défaut est le port 5000. Vous pouvez néanmoins configurer ce paramètre pour utiliser tout port TCP libre. Pour plus de détails sur la façon de configurer ce paramètre, reportez-vous à Paramètres réseau.
SNTP (serveur d'horloge) sur le port UDP configurable 123	Dominion KX II offre la fonction facultative de synchroniser son horloge interne sur un serveur d'horloge central. Cette fonction nécessite l'utilisation du port UDP 123 (le port standard pour SNTP). Elle peut également être configurée sur le port de votre choix. **Facultatif**
LDAP/LDAPS sur les ports configurables 389 ou 636	Si Dominion KX II est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole LDAP, les ports 386 ou 636 sont utilisés. Le système peut également être configuré pour utiliser le port de votre choix. **Facultatif**
RADIUS sur le port configurable 1812	Si Dominion KX II est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole RADIUS, le port 1812 est utilisé. Le système peut également être configuré pour utiliser le port de votre choix. **Facultatif**
Gestion RADIUS sur le port configurable 1813	Si Dominion KX II est configuré de manière à authentifier à distance les connexions des utilisateurs via le protocole RADIUS et qu'il utilise également Gestion RADIUS pour la consignation des événements, le port 1813 ou un port supplémentaire de votre choix est utilisé pour transmettre les notifications du journal.
SYSLOG sur le port UDP configurable 514	Si Dominion KX II est configuré pour envoyer des messages à un serveur Syslog, les ports indiqués sont utilisés pour la communication (utilise le port UDP 514).
Ports UDP par défaut SNMP	Le port 161 est utilisé pour l'accès SNMP entrant/sortant, en lecture/écriture, et le port 162 est utilisé pour le trafic sortant des traps SNMP. **Facultatif**
Port TCP 21	Le port 21 est utilisé pour l'interface de ligne de commande de Dominion KX II (lorsque vous travaillez avec l'assistance technique

	Raritan).

Paramètres de vitesse réseau

Paramètre de vitesse réseau Dominion KX II

Paramètre de port de commutateur réseau		**Auto**	**1000/Full**	**100/Full**	**100/Half**	**10/Full**	**10/Half**
	Auto	Vitesse disponible maximale	1000/Full	Dominion KX II : 100/Full Commutateur : 100/Half	100/Half	Dominion KX II : 10/Full Commutateur : 10/Half	10/Half
	1000/Full	1000/Full	1000/Full	Aucune communication	Aucune communication	Aucune communication	Aucune communication
	100/Full	Dominion KX II : 100/Half Commutateur : 100/Full	Dominion KX II : 100/Half Commutateur : 100/Full	100/Full	Dominion KX II : 100/Half Commutateur : 100/Full	Aucune communication	Aucune communication
	100/Half	100/Half	100/Half	Dominion KX II : 100/Full Commutateur : 100/Half	100/Half	Aucune communication	Aucune communication
	10/Full	Dominion KX II : 10/Half Commutateur : 10/Full	Aucune communication	Aucune communication	Aucune communication	10/Full	Dominion KX II : 10/Half Commutateur : 10/Full
	10/Half	10/Half	Aucune communication	Aucune communication	Aucune communication	Dominion KX II : 10/Full Commutateur : 10/Half	10/Half

Légende :

	Ne fonctionne pas comme prévu

Pris en charge

Fonctionne ; non recommandé

NON pris en charge par la spécification Ethernet ; le produit peut communiquer mais des collisions se produisent.

Selon la spécification Ethernet, « aucune communication » ne devrait se produire ; notez toutefois que le comportement Dominion KX II diffère du comportement attendu.

Remarque : pour assurer une communication réseau fiable, configurez Dominion KX II et le commutateur LAN sur les mêmes valeurs de vitesse d'interface de réseau local et duplex. Par exemple, configurez Dominion KX II et le commutateur LAN sur Autodetect (détection automatique) (recommandé) ou sur une vitesse fixe/duplex, comme 100Mo/s/Full.

Annexe B Mise à jour du schéma LDAP

Remarque : les procédures de ce chapitre ne doivent être effectuées que par des utilisateurs confirmés.

Dans ce chapitre

Renvoi des informations relatives aux groupes d'utilisateurs 301
Définition du Registre pour autoriser les opérations d'écriture sur le schéma 302
Création d'un attribut 302
Ajout d'attributs à la classe.....303
Mise à jour du cache de schéma.....305
Modification des attributs rciusergroup pour les membres utilisateurs .305

Renvoi des informations relatives aux groupes d'utilisateurs

Utilisez les informations de cette section pour renvoyer les informations relatives aux groupes d'utilisateurs (et faciliter le processus d'autorisation), une fois l'authentification réussie.

A partir de LDAP

Lorsqu'une demande d'authentification LDAP/LDAPS aboutit, >ProductName< détermine les autorisations accordées à un utilisateur donné selon les autorisations du groupe auquel il appartient. Votre serveur LDAP distant peut fournir ces noms de groupes d'utilisateurs en renvoyant un attribut désigné de la manière suivante :

rciusergroup attribute type: chaîne

Il est possible que cette opération nécessite une extension de schéma sur votre serveur LDAP/LDAPS. Consultez l'administrateur de votre serveur d'authentification pour activer cet attribut.

A partir de Active Directory (AD) de Microsoft

Remarque : seul un administrateur Active Directory confirmé doit tenter cette opération.

Le renvoi des informations relatives aux groupes d'utilisateurs à partir de Microsoft Active Directory pour Windows 2000 Server nécessite la mise à jour du schéma LDAP/LDAPS. Reportez-vous à la documentation Microsoft pour plus d'informations.

1. Installez le plug-in de schéma pour Active Directory. Reportez-vous à la documentation de Microsoft Active Directory pour obtenir des instructions.

2. Lancez la console Active Directory et sélectionnez Active Directory Schema (Schéma Active Directory).

Définition du Registre pour autoriser les opérations d'écriture sur le schéma

Pour autoriser un contrôleur de domaine à écrire sur le schéma, vous devez définir une entrée de Registre permettant les mises à jour du schéma.

Pour permettre les opérations d'écriture sur le schéma :

1. Cliquez avec le bouton droit de la souris sur le nœud racine Schéma Active Directory dans le volet de gauche de la fenêtre, puis cliquez sur Maître d'opérations. La boîte de dialogue Changer le contrôleur de schéma s'affiche.

2. Cochez la case Le schéma peut être modifié sur ce contrôleur de domaine. **Facultatif**
3. Cliquez sur OK.

Création d'un attribut

Pour créer des attributs pour la classe rciusergroup :

1. Cliquez sur le symbole + en regard de Schéma Active Directory dans le volet de gauche de la fenêtre.
2. Cliquez avec le bouton droit de la souris sur Attributs dans le volet de gauche.

3. Cliquez sur Nouveau, puis sélectionnez Attribut. Lorsque le message d'avertissement apparaît, cliquez sur Continuer ; la boîte de dialogue Créer un nouvel attribut s'affiche.

4. Tapez *rciusergroup* dans le champ Nom commun.
5. Tapez *rciusergroup* dans le champ Nom LDAP affiché.
6. Tapez *1.3.6.1.4.1.13742.50* dans le champ ID d'objet X.500 unique.
7. Entrez une description significative dans le champ Description.
8. Cliquez sur la flèche de la liste déroulante Syntaxe et sélectionnez Chaîne insensible à la casse dans la liste.
9. Tapez *1* dans le champ Minimum.
10. Tapez *24* dans le champ Maximum.
11. Cliquez sur OK pour créer l'attribut.

Ajout d'attributs à la classe

Pour ajouter des attributs à la classe :

1. Cliquez sur Classes dans le volet de gauche de la fenêtre.

2. Faites défiler le volet droit jusqu'à la classe user et cliquez dessus avec le bouton droit de la souris.

3. Sélectionnez Propriétés dans le menu. La fenêtre Propriétés de user s'affiche.
4. Cliquez sur l'onglet Attributs pour l'ouvrir.
5. Cliquez sur Add (Ajouter).

6. Sélectionnez rciusergroup dans la liste Sélectionnez l'objet Schéma.

7. Cliquez sur OK dans la boîte de dialogue Sélectionnez l'objet Schéma.
8. Cliquez sur OK dans la boîte de dialogue Propriétés de user.

Mise à jour du cache de schéma

Pour mettre à jour le cache du schéma :

1. Cliquez avec le bouton droit de la souris sur Schéma Active Directory dans le volet de gauche de la fenêtre et sélectionnez Recharger le schéma.
2. Réduisez la console Active Directory Schema MMC (Microsoft Management Console).

Modification des attributs rciusergroup pour les membres utilisateurs

Pour exécuter un script Active Directory sur un serveur Windows 2003, utilisez le script fourni par Microsoft (disponible sur le CD d'installation de Windows Server 2003). Ces scripts sont chargés sur votre système lors de l'installation de Microsoft Windows 2003. ADSI (ou Active Directory Service Interface) sert d'éditeur de bas niveau pour Active Directory. Il vous permet d'effectuer des tâches d'administration courantes, telles que l'ajout, la suppression et le déplacement d'objets avec un service d'annuaire.

Pour modifier les attributs d'un utilisateur individuel au sein du groupe rciusergroup, procédez comme suit :

1. Sur le CD d'installation, sélectionnez Support > Tools (Outils).

2. Cliquez deux fois sur SUPTOOLS.MSI pour installer les outils de support.
3. Ouvrez le répertoire dans lequel les outils de support sont installés. Exécutez adsiedit.msc. La fenêtre Editeur ADSI s'ouvre.

4. Ouvrez le domaine.

5. Dans le volet gauche de la fenêtre, sélectionnez le dossier CN=Users.

6. Recherchez le nom d'utilisateur dont vous souhaitez régler les propriétés dans le volet de droite. Cliquez avec le bouton droit sur le nom d'utilisateur et sélectionnez Propriétés.

7. Cliquez sur l'onglet Editeur d'attribut s'il n'est pas déjà ouvert. Sélectionnez rciusergroup dans la liste Attributs.

8. Cliquez sur Modifier. La boîte de dialogue Editeur d'attribut de chaîne apparaît.

9. Tapez le groupe d'utilisateurs (créé dans Dominion KX II) dans le champ Modifier l'attribut. Cliquez sur OK.

Annexe C Remarques d'informations

Dans ce chapitre

Présentation 309
Java Runtime Environment (JRE) 309
Remarques sur la prise en charge d'IPv6 310
Claviers.....311
Synchronisation des pointeurs de souris (Fedora).....315
Longueurs de câbles et résolutions vidéo pour châssis Dell 315
Fedora 316
Modes et résolutions vidéo.....317
Ports et profils USB 318
CIM 320
Support virtuel 322
CC-SG 322

Présentation

Cette section comporte des remarques importantes sur l'utilisation de Dominion KX II. Les mises à jour à venir seront rapportées et disponibles en ligne via le lien d'aide de l'interface de la console distante de Dominion KX II.

Java Runtime Environment (JRE)

Important : il est recommandé de désactiver la mise en mémoire cache de Java et d'effacer le cache de Java. Reportez-vous à la documentation Java ou au manuel des clients d'accès KVM et série pour plus d'informations.

La console distante de Dominion KX II et le client MPC requièrent l'environnement JRE pour fonctionner. La console distante de Dominion KX II vérifie la version de Java. Si la version est incorrecte ou obsolète, vous êtes invité à télécharger une version compatible.

Raritan vous recommande d'utiliser la version 1.5 du programme Java Runtime Environment (JRE) pour garantir des performances optimales. La console distante Dominion KX II et MPC fonctionnent cependant avec la version 1.6.x du programme JRE ou une version supérieure (à l'exception de la version 1.6.2).

Remarque : pour que les claviers multilingues fonctionnent dans la console distante de Dominion KX II (Virtual KVM Client), installez la version multilingue de Java Runtime Environment (JRE).

Remarques sur la prise en charge d'IPv6

Java

Java 1.5 prend en charge IPv6 pour :

- Solaris 8 et supérieur
- Linux kernel 2.1.2 et supérieur (RedHat 6.1 et supérieur)

Java 5.0 et supérieur prend en charge IPv6 pour :

- Solaris 8 et supérieur
- Linux kernel 2.1.2 et supérieur (kernel 2.4.0 et supérieur recommandés pour une meilleure prise en charge d'IPv6)
- Windows XP SP1 et Windows 2003, Windows Vista

Les configurations IPv6 suivantes *ne sont pas* prises en charge par Java :

- J2SE 1.4 ne prend pas en charge IPv6 sous Microsoft Windows.

Serveurs

- Linux kernel 2.4.0 ou supérieur est recommandé pour l'utilisation d'IPv6.
- Un noyau compatible IPv6 doit être installé ou le noyau doit être reconstruit avec les options IPv6 activées.
- Plusieurs utilitaires réseau doivent également être installés pour Linux si IPv6 est utilisé. Pour plus d'informations, reportez-vous à http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/IPv6-HOWTO.html

Serveurs

- Les utilisateurs de Windows XP et Windows 2003 doivent installer le service pack Microsoft IPV6 pour activer IPV6.

Mac Leopard

- IPv6 n'est pas pris en charge dans la version 2.0.20 de Dominion KX II pour Mac Leopard.

Samba

- IPv6 n'est pas pris en charge pour une utilisation avec les supports virtuels sous Samba.

Claviers

Claviers non américains

Clavier français

Caret (clients Linux uniquement)

Virtual KVM Client et Multi-Platform Client (MPC) ne traitent pas la combinaison de touches Alt Gr + 9 comme le caret (^) lorsqu'un clavier français est utilisé avec des clients Linux.

Pour obtenir le caret :

Sur un clavier français, appuyez sur la touche ^ (à droite de la touche P), puis immédiatement sur la barre d'espacement.

Ou, créez une macro constituée des commandes suivantes :

1. Appuyez sur la touche Alt Gr.
2. Appuyez sur la touche 9.
3. Relâchez la touche 9.
4. Relâchez la touche Alt Gr.

Remarque : ces procédures ne s'appliquent pas à l'accent circonflexe (au-dessus des voyelles). Dans tous les cas, la touche ^ (à droite de la touche P) fonctionne sur les claviers français pour créer l'accent circonflexe, lorsqu'elle est utilisée en combinaison avec un autre caractère.

Accent (clients Windows XP seulement)

Depuis Virtual KVM Client et Multi-Platform Client, la combinaison de touches Alt Gr + 7 entraîne l'affichage en double du caractère accentué lors de l'utilisation d'un clavier français avec les clients Windows XP.

Remarque : ceci ne se produit pas avec les clients Linux.

Pavé numérique

Depuis Virtual KVM Client et Multi-Platform Client, les symboles du pavé numérique s'affichent comme suit lors de l'utilisation d'un clavier français :

Symbole du pavé numérique	Affiche
/	;

.	;

Tilde

Depuis Virtual KVM Client et Multi-Platform Client, la combinaison de touches Alt Gr + 2 ne produit pas le tilde (~) lors de l'utilisation d'un clavier français.

Pour obtenir le tilde :

Créez une macro constituée des commandes suivantes :

- Appuyez sur la touche Alt Gr.
- Appuyez sur la touche 2.
- Relâchez la touche 2.
- Relâchez la touche Alt Gr.

Combinaisons de touches et Java Runtime Environment (JRE)

En raison d'une limitation de Java Runtime Environment (JRE), les clients Fedora, Linux et Solaris reçoivent une réponse non valide lorsque la touche Alt Gr est utilisée sur des claviers paramétrés sur la langue Anglais (Royaume-Uni) et US International. Fedora, Linux et Solaris ne renvoient pas de réponse lorsqu'une combinaison incluant la touche Alt Gr est utilisée avec Java 1.5. Java 1.6 semble apporter des améliorations, cependant les événements associés à keyPressed et keyReleased indique toujours que le code de touche est inconnu lorsque la touche Alt Gr est utilisée.

Par ailleurs, une touche utilisée en combinaison avec Alt Gr (comme par exemple Alt Gr-4, qui, sur un clavier du Royaume-Uni, permet de saisir le symbole euro), va seulement générer un événement keyTyped suivi d'un événement keyReleased pour cette valeur, sans événement keyPressed. Java 1.6 apporte une amélioration à ce problème, l'événement keyPressed n'est plus vide.

Préférence de la langue du clavier (clients Fedora Linux)

Etant donné que Sun JRE sous Linux a des difficultés à générer les événements KeyEvents corrects pour les claviers dans d'autres langues configurés à l'aide des préférences système, Raritan recommande de configurer ces claviers à l'aide des méthodes décrites dans le tableau suivant.

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Anglais britannique	Paramètres système (centre de contrôle)

Langue/clavier	Méthode de configuration
US Intl	Valeur par défaut
Français	Indicateur de clavier
Allemand	Indicateur de clavier
Hongrois	Paramètres système (centre de contrôle)
Espagnol	Paramètres système (centre de contrôle)
Allemand (Suisse)	Paramètres système (centre de contrôle)
Norvégien	Indicateur de clavier
Suédois	Indicateur de clavier
Danois	Indicateur de clavier
Japonais	Paramètres système (centre de contrôle)
Coréen	Paramètres système (centre de contrôle)
Slovène	Paramètres système (centre de contrôle)
Italien	Paramètres système (centre de contrôle)
Portugais	Paramètres système (centre de contrôle)

Remarque : l'indicateur de clavier doit être utilisé sur les systèmes Linux utilisant l'environnement de bureau Gnome.

Sur un clavier hongrois depuis un client Linux, les lettres U et O avec deux accents aigus ne fonctionnent qu'avec JRE 1.6.

Plusieurs méthodes permettent de définir les préférences de langue de clavier sur les clients Fedora Linux. La méthode suivante est obligatoire pour le mappage correct des touches des Virtual KVM Client et Multi-Platform Client (MPC).

Pour définir la langue du clavier à l'aide des paramètres système :

1. Depuis la barre d'outils, choisissez Système > Préférences > Clavier.
2. Ouvrez l'onglet Agencements.
3. Ajoutez ou sélectionnez la langue appropriée.
4. Cliquez sur Fermer.

Pour définir la langue du clavier à l'aide de l'indicateur de clavier :

1. Cliquez avec le bouton droit sur la barre de tâches et choisissez Ajouter au tableau de bord.

2. Dans la boîte de dialogue Ajouter au tableau de bord, cliquez avec le bouton sur Indicateur de clavier, et dans le menu, choisissez Ouvrir les préférences clavier.
3. Dans la boîte de dialogue Préférences clavier, cliquez sur l'onglet Agencements.
4. Ajoutez et enlevez des langues selon les besoins.

Claviers Macintosh

Clavier Macintosh

Lorsqu'un Macintosh est utilisé comme client, les touches suivantes du clavier ne sont pas capturées par Java Runtime Environment (JRE) :

- F9
- F10
- F11
- F14
- F15
- Monter le volume
- Descendre le volume
- Muet
- Ejection

En conséquence, Virtual KVM Client et Multi-Platform Client (MPC) ne sont pas en mesure de traiter ces touches d'un clavier de client Mac.

Combinaisons de touches Macintosh non prises en charge

Les combinaisons de touches Mac suivantes ne sont pas prises en charge dans certains navigateurs lorsque vous utilisez Dominion KX II afin de gérer une configuration client Mac à serveur cible Mac.

Remarque : des macros peuvent être créées pour remplacer ces combinaisons de touches.

Safari avec JRE 1.5

Par défaut, les combinaisons de touches suivantes ne sont pas prises en charge. Toutefois, des combinaisons de touches sont configurables dans Safari. Aussi, pour contourner le problème, elles peuvent le cas échéant être configurées pour effectuer une action différente.

Combinaison de touches Mac	Description	Prise en charge ?
Commande + O	Ouvre l'application	Non

	sélectionnée.	
Option + Commande + M	Réduit toutes les fenêtres.	Non

Firefox avec JRE 1.5

Combinaison de touches Mac	Description	Prise en charge ?
Commande + O	Ouvre l'application sélectionnée.	Non
Commande + D	Duplique l'élément sélectionné.	Non

Synchronisation des pointeurs de souris (Fedora)

Lors d'une connexion en mode souris double à un serveur cible exécutant Fedora 7, les pointeurs de souris cible et locale risquent de perdre leur synchronisation après quelque temps.

Pour resynchroniser les curseurs de souris :

- Utiliser l'option Synchronize Mouse (Synchroniser la souris) de Virtual KVM Client.

Le tableau suivant récapitule les modes souris de Dominion KX II et indique si ces modes restent synchronisés lors de l'accès aux serveurs cible KVM exécutant Fedora :

Mode souris	Fedora Core 5	Fedora Core 6
Synchronisation absolue de la souris	Non	Non
Mode Souris intelligente	Non	Oui
Mode Souris standard	Oui	Non

Longueurs de câbles et résolutions vidéo pour châssis Dell

Afin de maintenir la qualité vidéo, Raritan recommande l'utilisation des longueurs de câbles et les résolutions vidéo suivantes lorsque vous êtes connecté à un châssis de lames Dell depuis Dominion KX II :

Longueur de câble	Résolution vidéo
1 524,00 cm	1024 x 768 x 60
1 524,00 cm	1280 x 1024 x 60
914,40 cm	1600 x 1200 x 60

Fedora

Résolution du focus de Fedora Core

Lors de l'utilisation de Multi-Platform Client (MPC), il est parfois impossible de se connecter à un dispositif Dominion KX II ou d'accéder aux serveurs cible KVM (Windows, SUSE, etc.). En outre, la combinaison de touches Ctrl+Alt+M n'affiche peut-être pas le menu des raccourcis-clavier. Cette situation se produit avec la configuration client suivante : Fedora Core 6 et Firefox 1.5 ou 2.0.

Des tests ont permis de déterminer que l'installation de libXp résolvait les problèmes de focus de fenêtre avec Fedora Core 6. Raritan a effectué les tests avec libXp-1.0.0.8.i386.rpm ; tous les problèmes de focus de clavier et de menus contextuels.

Remarque : libXp est également requis pour permettre le fonctionnement du navigateur SeaMonkey (précédemment Mozilla) avec le plug-in Java.

Connexions par carte à puce VKC et MPC aux serveurs Fedora

Si vous utilisez une carte à puce pour la connexion à un serveur Fedora via MPC ou VKC, et que vous retirez la carte une fois connecté, la bibliothèque pcsc-lite sur les serveurs FC7 et FC8 n'est pas libérée. Pour cela, vous devez redémarrer le démon pcscd. Pour éviter ce problème, mettez à niveau la bibliothèque pcsc-lite à 1.4.102-3 ou supérieur.

Dépannage des problèmes de blocage de Firefox lors de l'utilisation de Fedora

Si vous accédez à Firefox et que vous utilisez un serveur Fedora, Firefox risque de se bloquer à l'ouverture. Pour résoudre ce problème, installez le plug-in libnpjp2.so Java sur le serveur.

Modes et résolutions vidéo

Modes vidéo SUSE/VESA

L'outil de configuration SaX2 de SuSE X.org génère des modes vidéo à l'aide des entrées ModeLine du fichier de configuration X.org. Ces modes vidéo ne correspondent pas exactement au minutage du mode vidéo VESA (même si un écran VESA est sélectionné). Dominion KX II, en revanche, s'appuie sur le minutage du monde VESA exact pour une synchronisation parfaite. Cette disparité peut entraîner des bordures noires, des sections d'image absentes et des parasites.

Pour configurer l'affichage vidéo SUSE :

1. Le fichier de configuration généré /etc/X11/xorg.conf inclut une section Monitor comportant une option appelée UseModes. Par exemple,
   UseModes "Modes[0]"
2. Mettez cette ligne en commentaire (à l'aide de #) ou supprimez-la complètement.
3. Redémarrez le serveur X.

Grâce à cette modification, le minutage du mode vidéo interne du serveur X sera utilisé et correspondra exactement au minutage du mode vidéo VESA, entraînant un affichage vidéo correct sur Dominion KX II.

Résolutions vidéo prises en charge non affichées

Lorsque vous utilisez un CIM, certaines résolutions vidéo, indiquées dans ***Résolutions vidéo prises en charge*** (à la page 291), peuvent ne pas être disponibles à la sélection par défaut.

Pour afficher toutes les résolutions vidéo disponibles si elles n'apparaissent pas :

1. Branchez le moniteur.
2. Débranchez ensuite le moniteur et branchez le CIM. Toutes les résolutions vidéo sont à présent disponibles et peuvent être utilisées.

Ports et profils USB

Ports USB VM-CIM et DL360

Les serveurs HP DL360 sont dotés d'un port USB à l'arrière et d'un autre à l'avant. Avec DL360, les deux ports ne peuvent pas être utilisés simultanément. Aussi, un VM-CIM double ne peut pas être utilisé sur les serveurs DL360.

Toutefois, pour contourner ce problème, un concentrateur USB2 peut être connecté au port USB à l'arrière du dispositif et un VM-CIM double peut être connecté au concentrateur.

Aide pour la sélection des profils USB

Lorsque vous êtes connecté à un serveur cible KVM dans VKC, vous pouvez afficher des informations relatives aux profils USB via l'aide sur la commande USB Profiles (Profils USB) du menu USB Profile (Profil USB).

L'aide relative aux profils USB apparaît dans la fenêtre USB Profile Help. Pour plus d'informations sur des profils USB spécifiques, reportez-vous à ***Profils USB disponibles*** (à la page 107).

Raritan propose une sélection standard de profils de configuration USB pour des implémentations de serveurs sur une grande variété de systèmes d'exploitation et de niveaux de BIOS. Ces profils sont conçus pour offrir une adéquation optimale entre les configurations des dispositifs USB distants et des serveurs cible.

Le profil Generic (Générique) répond aux besoins des configurations de serveurs cible déployées les plus fréquentes.

Des profils supplémentaires sont disponibles pour répondre aux besoins spécifiques d'autres configurations de serveurs déployées courantes (par exemple, Linux, MAC OS-X).

Un certain nombre de profils (désignés par nom de plate-forme et révision de BIOS) ont également été adaptés pour améliorer la compatibilité de la fonction Support virtuel avec le serveur cible ; par exemple, lors d'un fonctionnement au niveau du BIOS.

L'option Add Other Profiles (Ajouter d'autres profils) permet d'accéder aux autres profils disponibles sur le système. Les profils sélectionnés dans cette liste sont ajoutés au menu USB Profile (Profil USB). Sont inclus des profils de dépannage (Troubleshooting) conçus pour identifier les limites des configurations.

Les options du menu USB Profile sont configurables via la page Console Device Settings > Port Configuration (Paramètres du dispositif de console > Configuration des ports).

Si les profils USB standard fournis par Raritan ne répondent pas aux conditions requises de votre serveur cible, l'assistance technique Raritan peut vous aider à trouver une solution adaptée à cette cible. Raritan vous recommande d'effectuer les opérations suivantes :

1. Consultez les notes de publication les plus récentes sur le site Web de Raritan (www.raritan.com) sur la page des mises à jour de firmware pour vérifier s'il n'existe pas de solution pour votre configuration.
2. Dans le cas contraire, fournissez les informations lorsque vous contactez l'assistance technique Raritan :
   a. Informations sur le serveur cible : fabricant, modèle, BIOS, fabricant et version.
   b. Usage envisagé (par exemple, redirection d'une image pour recharger le système d'exploitation d'un serveur depuis le CD).

Modification d'un profil USB lors de l'utilisation d'un lecteur de cartes à puce

Dans certains cas, vous serez amené à modifier le profil USB d'un serveur cible. Vous aurez par exemple à remplacer la vitesse de connexion par Use Full Speed for Virtual Media CIM (Utiliser le haut débit pour le CIM du support virtuel) lorsque la cible rencontre des difficultés avec la vitesse de connexion High Speed USB (USB à haut débit).

A la modification d'un profil, vous recevrez, le cas échéant, un message Nouveau matériel détecté et devrez vous connecter à la cible avec des droits d'administrateur afin de réinstaller le pilote USB. Ceci ne se produira probablement que les premières fois où la cible détectera les nouveaux paramètres du périphérique USB. Elle sélectionnera correctement le pilote par la suite.

CIM

Souris à 3 boutons Windows sur les cibles Linux

Lorsque vous utilisez une souris à 3 boutons sur un client Windows connecté à une cible Linux, le bouton gauche peut être mappé sur le bouton central de la souris à 3 boutons du client Windows.

Comportement des dispositifs USB composites Windows 2000 pour la fonction Support virtuel

Le système d'exploitation Windows 2000 ne prend pas en charge les dispositifs USB composites, comme D2CIM-VUSB de Raritan, de la même façon que les dispositifs USB non composites.

En conséquence, l'icône de la barre d'état Supprimer le périphérique en toute sécurité n'apparaît pas pour les lecteurs mappés par D2CIM-VUSB et un message d'avertissement peut s'afficher lors de la déconnexion du dispositif. Raritan n'a toutefois constaté aucun problème à la suite de message.

Le service technique de Raritan aux Etats-Unis a mis au point une configuration prenant en charge l'icône Supprimer le périphérique en toute sécurité et évitant ce message Windows. Cette configuration requiert l'utilisation de l'adaptateur de supports virtuels D2CIM-DVUSB et le profil USB Troubleshooting 3, qui configure D2CIM-DVUSB en tant que dispositif USB non composite prenant en charge une connexion de supports virtuels unique. Raritan a testé cette configuration avec succès aux Etats-Unis et au Japon.

Support virtuel

Support virtuel non rafraîchi après l'ajout de fichiers

Après le montage d'un lecteur de support virtuel, si vous ajoutez des fichiers à ce lecteur, ces fichiers peuvent ne pas apparaître immédiatement sur le serveur cible. Supprimez, puis rétablissez la connexion de support virtuel.

Durée d'amorçage du BIOS cible avec les supports virtuels

L'amorçage du BIOS de certaines cibles peut durer plus longtemps sur le support est monté virtuellement à la cible.

Pour raccourcir la durée d'amorçage :

1. Fermez Virtual KVM Client pour libérer complètement les lecteurs de supports virtuels.
2. Redémarrez la cible.

Echec de connexion des supports virtuels lors de l'utilisation du haut débit

Dans certains cas, il peut être nécessaire de sélectionner l'option Use Full Speed for Virtual Media CIM ((Utiliser le haut débit pour le CIM du support virtuel) lorsque la cible rencontre des difficultés avec la vitesse de connexion High Speed USB (USB à haut débit) ou qu'elle connaît des erreurs de protocole USB en raison d'une dégradation du signal due à la présence de connecteurs et de câbles supplémentaires (par exemple, une connexion à un serveur lame via une clé électronique).

CC-SG

Version de Virtual KVM Client non reconnue par le mode proxy CC-SG

Lorsque Virtual KVM Client est démarré depuis CommandCenter Secure Gateway (CC-SG) en mode proxy, la version de Virtual KVM Client est inconnue. Dans la boîte de dialogue About Raritan Virtual KVM Client (A propos de Virtual KVM Client de Raritan), la version est indiquée comme inconnue.

Mode souris simple - Connexion à une cible Dominion KX II contrôlée par CC-SG via VKC utilisant Firefox

Si vous utilisez Firefox pour vous connecter à une cible Dominion KX II contrôlée par CC-SG à l'aide de DCIM-PS2 ou DCIM-USBG2, et que vous passez au mode souris simple dans Virtual KVM Client, le focus ne sera plus sur la fenêtre VKC et la souris ne répondra pas. Dans ce cas, cliquez ou appuyez sur Alt+Tab pour rétablir le focus sur la fenêtre VKC.

Mode proxy et MPC

Si vous utilisez Dominion KX II dans une configuration CC-SG, ne vous servez pas du mode proxy CC-SG si vous avez l'intention d'utiliser Multi-Platform Client (MPC).

Déplacement entre ports de Dominion KX II

Si vous effectuez un déplacement entre ports du même dispositif Dominion KX II et reprenez la gestion au bout d'une minute, CC-SG peut afficher un message d'erreur. Si vous reprenez la gestion, l'affichage est mis à jour.

Annexe D FAQ

Dans ce chapitre

Questions générales.....325
Accès à distance 327
Support virtuel universel.....329
Profils USB 330
Ethernet et mise en réseau IP 332
Gestion de réseau IPv6 339
Windows 341
Serveurs lames.....342
Installation 345
Port local.....347
Port local étendu (modèles KX2-832 et KX2-864 Dominion uniquement)349
Gestion de l'alimentation 350
Evolutivité 351
Modules d'interface pour ordinateur (CIM).....352
Sécurité.....353
Authentification par cartes à puce et CAC 355
Capacités de gestion 356
Divers.....357

Questions générales

Qu'est-ce que Dominion KX II ?

Dominion KX II est un commutateur KVM (clavier/vidéo/souris) numérique de la seconde génération qui permet à un, deux, quatre ou huit administrateurs informatiques d'accéder à et de gérer 8, 16, 32 ou 64 serveurs sur le réseau grâce à des fonctionnalités au niveau BIOS. Dominion KX II est entièrement indépendant du matériel et du système d'exploitation. Les utilisateurs peuvent dépanner et reconfigurer les serveurs même lorsqu'ils sont éteints.

Pour le rack, Dominion KX II offre les mêmes fonctionnalités, facilités, économies d'espace et de coût que les commutateurs KVM traditionnels. Toutefois, Dominion KX II intègre également la technologie KVM sur réseau IP la plus performante du secteur, permettant ainsi à plusieurs administrateurs d'accéder aux consoles des serveurs KVM de n'importe quel poste de travail mis en réseau.

En quoi le dispositif Dominion KX II diffère-t-il d'un logiciel de gestion à distance ?

Lors d'une utilisation de Dominion KX II à distance, au premier abord, l'interface peut sembler similaire aux logiciels de gestion à distance pcAnywhere, Windows Terminal Services/Bure distant, VNC, etc. Toutefois, étant donné que Dominion KX II n'est pas une solution logicielle, mais matérielle, il est beaucoup plus puissant. Spécifiquement :

- Ne dépend ni du système d'exploitation ni du matériel - Dominion KX II peut être utilisé pour gérer des serveurs exécutant nombre de systèmes d'exploitation courants, notamment Intel®, Sun™, PowerPC exécutant Windows, Linux®, Solaris™, etc.
- Ne dépend pas de l'état ou d'un serveur sans agent - Dominion KX II n'a pas besoin que le système d'exploitation du serveur géré soit actif, ni qu'un logiciel spécial soit installé sur le serveur géré.
- Hors-bande – Même s'il n'existe pas de connexion disponible sur le réseau même du serveur géré, celui-ci peut quand même être géré par Dominion KX II.
- Accès au niveau du BIOS – Même si le serveur est bloqué lors du démarrage, il requiert un redémarrage en mode sans échec ou une modification des paramètres BIOS du système, Dominion KX II fonctionne toujours sans faille pour permettre de procéder à ces configurations.

Quelles sont les nouveautés de Dominion KX II par rapport à KX I ?

Dominion KX II offre de nombreuses fonctions inédites et remarquables, telles que support virtuel, Absolute Mouse Synchronization™ (synchronisation absolue de la souris), double alimentation, Ethernet double d'un gigabit, interfaces utilisateur Web courantes, port local de nouvelle génération, etc.

Comment dois-je effectuer la migration de Dominion KX I à Dominion KX II ?

De manière générale, les clients peuvent continuer à utiliser leurs commutateurs existants pendant de nombreuses années. À mesure que leurs centres de données se développent, les clients peuvent acheter et utiliser les nouveaux modèles Dominion KX II. L'unité de gestion centralisée de Raritan, CommandCenter® Secure Gateway, ainsi que le client MPC (Multi-Platform Client) prennent tous les deux en charge les commutateurs KX I et Dominion KX II de manière transparente.

Mes CIM KX I existants vont-ils fonctionner avec le commutateur Dominion KX II ?

Oui, les CIM KX I existants fonctionnent avec le commutateur Dominion Dominion KX II. De plus, certains CIM Paragon fonctionnent avec Dominion KX II. Cela permet aux utilisateurs désireux de passer au KVM sur IP de migrer en toute facilité vers Dominion KX II à partir de Paragon I. Toutefois, vous pouvez également utiliser les CIM D2CIM-VUSB et D2CIM-DVUSB qui prennent en charge le support virtuel et la synchronisation absolue de la souris.

Le dispositif Dominion KX II peut-il être monté en rack ?

Oui. Dominion KX II est livré en standard avec des fixations de montage en rack 19". Il peut également être monté en rack par l'arrière de façon à ce que les ports du serveur soient dirigés vers l'avant.

Quelles sont les dimensions de Dominion KX II ?

Dominion KX II ne mesure que 1U de hauteur (à l'exception de KX2-464 qui mesure 2U), s'adapte dans un rack standard de 19 pouces et ne mesure que 29 cm de profondeur. Dominion KX2-832 et KX2-864 mesurent 44 cm de profondeur.

Accès à distance

Combien d'utilisateurs peuvent accéder à distance aux serveurs sur chaque Dominion KX II ?

Les modèles Dominion KX II permettent la connexion distante de huit utilisateurs au maximum par canal d'utilisateur pour l'accès et la gestion simultanés d'un serveur cible unique. Pour les dispositifs à un canal tels que DKX2-116, un seul serveur cible peut être utilisé et géré par huit utilisateurs distants maximum. Pour les dispositifs à deux canaux tels que DKX2-216, huit utilisateurs distants au maximum peuvent utiliser et gérer le serveur sur le canal un et huit autres utilisateurs au maximum sur le canal deux. En ce qui concerne les dispositifs à quatre canaux, huit utilisateurs au maximum par canal, pour un total de 32 (8 x 4) utilisateurs, peuvent accéder à quatre serveurs et les gérer. De même, pour les dispositifs à huit canaux, huit utilisateurs au maximum peuvent accéder à un seul serveur, jusqu'à un total maximum de 32 utilisateurs sur huit canaux.

Deux utilisateurs peuvent-ils visualiser le même serveur simultanément ?

Oui, huit personnes au maximum peuvent utiliser et gérer n'importe quel serveur unique en même temps.

Deux utilisateurs, l'un à distance et l'autre à partir du port local, peuvent-ils accéder au même serveur ?

Oui, le port local est totalement indépendant des « ports » à distance. Le port local peut accéder au même serveur grâce à la fonctionnalité PC-Share.

Quelle configuration matérielle, logicielle ou réseau dois-je utiliser pour accéder à Dominion KX II à partir d'un ordinateur client ?

Dominion KX II étant entièrement accessible par le Web, il ne requiert l'installation d'aucun logiciel propriétaire sur les ordinateurs clients utilisés pour y accéder. Un client installé facultatif est disponible sur Raritan.com. Il est obligatoire pour l'accès par modem externe.

Dominion KX II est accessible par le biais des principaux navigateurs Web, notamment : Internet Explorer, Mozilla et Firefox. Dominion KX II est maintenant accessible sur les ordinateurs Windows, Linux et Macintosh, par l'intermédiaire du nouveau client Windows de Raritan, et des clients Java Multiplatform et Virtual KVM.

Les administrateurs Dominion KX II peuvent également effectuer des fonctions de gestion à distance, telles que définir des mots de passe et la sécurité, renommer les serveurs, modifier les adresses IP, etc., grâce à une interface navigateur pratique.

Quelle est la taille de fichier de l'applet Virtual KVM Client (Client KVM virtuel) utilisé pour accéder à Dominion KX II ? Combien de temps faut-il pour l'extraire ?

La taille de l'applet Virtual KVM Client utilisé pour accéder à Dominion KX II est d'environ 500 Ko. Le tableau suivant indique le temps nécessaire pour extraire l'applet de Dominion KX II à différentes vitesses réseau :

Vitesse	Description	Durée
100 Mbps	Vitesse réseau théorique 100 mégabits	0,05 seconde
60 Mbps	Vitesse réseau pratique probable 100 mégabits	0,08 seconde
10 Mbps	Vitesse réseau théorique 10 mégabits	0,4 seconde
6 Mbps	Vitesse réseau pratique probable 10 mégabits	0,8 seconde
512 Kbps	Vitesse de téléchargement (type) d'un modem câblé	8 secondes

Comment puis-je accéder aux serveurs connectés à Dominion KX II en cas d'indisponibilité du réseau ?

Vous pouvez accéder aux serveurs sur rack ou par modem. Dominion KX II offre un port de modem dédié pour connecter un modem externe.

Disposez-vous d'un client Windows ?

Oui, dans la version 2.2, nous disposons d'un client Windows .NET natif, appelé Raritan Active KVM Client.

Disposez-vous d'un client non Windows ?

Oui. Les clients Virtual KVM Client et Multi-Platform Client (MPC) permettent tous les deux aux utilisateurs exécutant des systèmes non-Windows de se connecter aux serveurs cible KVM via les commutateurs Dominion KX I et Dominion KX II. Le client MPC peut être exécuté à l'aide d'un navigateur Web ou en mode autonome. Reportez-vous à **Virtual KVM Client** et **Systèmes d'exploitation pris en charge par Multi-Platform Client (MPC) de Raritan** pour plus d'informations.

Au cours d'une session Virtual KVM Client, la touche Alt semble parfois bloquée. Que dois-je faire ?

Ceci se produit généralement dans des situations où la touche Alt est enfoncée et n'est pas relâchée. Par exemple, si vous maintenez la touche Alt en appuyant sur la barre d'espacement, la mise en évidence peut passer du serveur cible au PC client. Le système d'exploitation local interprète ensuite cette combinaison de touches et déclenche l'action correspondante dans la fenêtre active (PC client).

Support virtuel universel

Quels modèles Dominion KX II prennent en charge la fonction Support virtuel ?

Tous les modèles Dominion KX II prennent en charge la fonction Support virtuel. Elle est disponible en version autonome et via CommandCenter Secure Gateway, l'unité de gestion centralisée de Raritan.

Quels types de supports virtuels Dominion KX II prend-il en charge ?

Dominion KX II prend en charge les types de supports suivants : lecteurs CD/DVD internes et connectés USB, dispositifs de stockage de masse USB, lecteurs de disque dur PC et images ISO.

Le support virtuel est-il fiable ?

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

Quelles sont les conditions requises pour l'utilisation du support virtuel ?

Un CIM de support virtuel Dominion KX II est requis. Il existe deux CIM de ce type : D2CIM-VUSB et le nouveau D2CIM-DVUSB.

D2CIM-DVUSB est doté de connecteurs USB double et est destiné aux clients souhaitant utiliser le support virtuel au niveau du BIOS. D2CIM-DVUSB est également requis pour l'authentification par carte à puce.

D2CIM-VUSB est doté d'un connecteur USB simple et est destiné aux clients souhaitant utiliser le support virtuel au niveau du système d'exploitation.

Ces deux CIM prennent en charge des sessions de support virtuel sur les serveurs cible supportant l'interface USB 2.0.

Disponible en coffrets économiques de 32 et 64 CIM, ces CIM prennent en charge la synchronisation absolue de la souris, ainsi que la mise à jour du firmware à distance.

Profils USB

Qu'est-ce qu'un profil USB ?

Certains serveurs requièrent une interface USB configurée de manière spécifique pour les services USB, tels que les supports virtuels. Le profil USB adapte l'interface USB de Dominion KX II au serveur pour prendre en compte les caractéristiques spécifiques de ce dernier.

En quoi un profil USB peut-il m'être utile ?

Les profils USB sont le plus souvent exigés au niveau du BIOS, où la spécification USB n'est peut-être pas totalement prise en charge lors de l'accès aux lecteurs de support virtuel.

Toutefois, les profils sont parfois utilisés au niveau du système d'exploitation, par exemple, pour la synchronisation de la souris des serveurs Max et Linux.

Comment un profil USB est-il utilisé ?

Les ports peuvent être configurés individuellement ou par groupe par l'administrateur pour utiliser un profil USB spécifique sur la page de configuration des ports de Dominion KX II.

Un profil USB peut également être sélectionné dans le client Dominion KX II en cas de besoin.

Que se passe-t-il si je ne choisis pas le profil USB correct ?

La sélection d'un profil USB incorrect pour un serveur cible KVM peut empêcher complètement ou partiellement le fonctionnement d'un dispositif de stockage de masse, d'une souris ou d'un clavier.

Dois-je systématiquement définir un profil USB si j'utilise la fonction Support virtuel ?

Non, dans de nombreux cas, le profil USB par défaut est suffisant pour l'utilisation de la fonction Support virtuel au niveau du système d'exploitation, ou pour le fonctionnement au niveau du BIOS sans accès aux supports virtuels.

Quels profils sont disponibles ?

Reportez-vous à ***Profils USB disponibles*** (à la page 107).

Comment puis-je déterminer le meilleur profil USB pour un serveur cible donné ?

Le profil générique convient le mieux à une grande majorité de serveurs cible. Si ce profil ne fonctionne pas avec un serveur cible KVM donné, vous pouvez choisir le profil USB approprié dans ***Profils USB disponibles*** (à la page 107). Sélectionnez le profil correspondant le mieux à votre serveur cible.

Quel est l'objet d'un profil BIOS ?

Un profil BIOS a été conçu pour répondre aux exigences du BIOS d'un serveur particulier qui ne met pas en œuvre la spécification USB complète. Le profil permet l'utilisation de clavier, souris et supports virtuels au niveau du BIOS, surmontant les restrictions ou les limitations du BIOS.

Ai-je besoin d'un CIM spécial pour utiliser les profils USB ?

Vous devez utiliser un D2CIM-VUSB ou D2CIM-DVUSB avec firmware mis à jour.

Raritan fournira-t-il des profils USB pour d'autres configurations de serveur cible ?

Raritan fournira de nouveaux profils USB pour répondre aux besoins des clients. Au fur et à mesure de la disponibilité de ces profils, ils seront inclus dans les mises à niveau de firmware.

Ethernet et mise en réseau IP

Dominion KX II offre-t-il des ports Ethernet doubles d'un gigabit pour fournir un basculement redondant ?

Oui. Dominion KX II est doté de ports Ethernet doubles d'un gigabit pour fournir des fonctionnalités de basculement redondant. En cas de panne du port Ethernet primaire (ou du commutateur/routeur auquel il est connecté), Dominion KX II bascule sur le port réseau secondaire avec la même adresse IP, empêchant ainsi toute interruption de fonctionnement de votre serveur. Notez que la protection par basculement automatique doit être activée par l'administrateur.

Comment la bande passante est-elle utilisée dans les systèmes KVM sur IP ?

Dominion KX II offre la technologie KVM par IP nouvelle génération : la compression vidéo la plus performante qui soit. Raritan a reçu de nombreuses récompenses techniques confirmant la haute qualité de ses transmissions vidéo et l'utilisation limitée de la bande passante.

Dominion KX II numérise, compresse et chiffre les signaux du clavier, de l'écran et de la souris provenant du serveur cible et transmet des paquets IP via le réseau IP au client distant afin de créer une session distante pour l'utilisateur. Dominion KX II offre une expérience sur le rack basée sur ses algorithmes de traitement vidéo de pointe.

Les changements d'écran, notamment vidéo, représentent la majorité de la bande passante utilisée ; l'activité du clavier et de la souris est considérablement inférieure.

Il est important de noter que la bande passante n'est employée que lorsque l'utilisateur est actif. La quantité de bande passante utilisée est basée sur le volume de changements se produisant à l'écran vidéo du serveur.

En l'absence de changement à l'écran vidéo, l'utilisateur n'interagit pas avec le serveur, la bande passante n'est pas utilisée. Si l'utilisateur déplace la souris ou tape un caractère, la quantité de bande passante utilisée est réduite. Si l'affichage exécute un écran de veille complexe ou lit une vidéo, la bande passante utilisée peut être plus conséquente.

Comment la bande passante affecte-t-elle les performances KVM sur IP ?

En général, il existe un compromis entre bande passante et performances. Plus la bande passante disponible est importante, plus les performances sont bonnes. Dans les environnements à bande passante réduite, les performances peuvent se dégrader. Dominion KX II a été optimisé pour fournir des performances solides dans une grande variété d'environnements.

Quels facteurs affectent la bande passante ?

De nombreux facteurs déterminent la quantité de bande passante utilisée. Le facteur principal, comme indiqué précédemment, est la quantité de changements se produisant dans l'affichage vidéo du serveur cible. Il dépend des tâches et actions de l'utilisateur.

Parmi les autres facteurs figurent la résolution vidéo du serveur, la vitesse et les caractéristiques du réseau, les ressources du client PC et le bruit de la carte vidéo.

Dominion KX II dispose d'algorithmes de traitement vidéo très élaborés qui optimisent la bande passante et les performances pour des environnements divers. En outre, ils sont hautement configurables car de nombreux paramètres permettent d'optimiser l'usage de la bande passante. Le paramètre Connection Speed (Vitesse de connexion) des clients distants (VKC, MPC) en particulier peut être défini pour réduire la bande passante utilisée.

Contrairement à KX I, le paramètre Noise Filter (Filtre antiparasite) ne joue généralement pas un rôle important dans la réduction de la bande passante ou l'amélioration des performances.

Quelle est la quantité de bande passante utilisée par Dominion KX II pour les tâches courantes ?

La bande passante dépend principalement des tâches et actions de l'utilisateur. Plus l'écran vidéo du serveur change, plus le débit de bande passante utilisée est important.

Le tableau ci-dessous résume des cas d'utilisation standard avec les paramètres de bande passante par défaut de Dominion KX II et deux paramètres de bande passante réduite (paramètre Connection Speed d'1 Mo avec couleur 15 et 8 bits) sur un serveur cible Windows XP (résolution de 1024 x 768) sur un réseau local de 100 Mbits/s :

Tâche utilisateur	Valeur par défaut	Vitesse d'1Mo et couleur 15 bits	Vitesse d'1Mo et couleur 8 bits
Bureau de Windows inactif	0 Ko/s	0 Ko/s	0 Ko/s
Déplacement du curseur de la souris	5 à 15 Ko/s	2 à 6 Ko/s	2 à 3 Ko/s
Glissement d'icône	40 à 70 Ko/s	10 à 25 Ko/s	5 à 15 Ko/s
Glissement de dossier	10 à 40 Ko/s	5 à 20 Ko/s	5 à 10 Ko/s
Ouverture d'une fenêtre de texte	50 à 100 Ko/s	25 à 50 Ko/s	10 à 15 Ko/s
Frappe en continu	1 Ko/s	0,5 à 1 Ko/s	0,2 à 5 Ko/s
Défilement d'une	10 à 50 Ko/s	5 à 25 Ko/s	2 à 10 Ko/s

Tâche utilisateur	Valeur par défaut	Vitesse d'1Mo et couleur 15 bits	Vitesse d'1Mo et couleur 8 bits
fenêtre de texte			
Fermeture d'une fenêtre de texte	50 à 100 Ko/s	20 à 40 Ko/s	10 à 15 Ko/s
Ouverture d'un panneau	50 à 100 Ko/s	60 à 70 Ko/s	20 à 30 Ko/s
Changement d'onglet dans un panneau	40 à 50 Ko/s	20 à 50 Ko/s	10 à 20 Ko/s
Fermeture d'un panneau	50 à 100 Ko/s	40 à 60 Ko/s	20 à 30 Ko/s
Changement d'option du panneau	2 à 10 Ko/s	1 à 5 Ko/s	1 à 3 Ko/s
Ouverture d'une page de navigateur	100 à 300 Ko/s	50 à 200 Ko/s	40 à 80 Ko/s
Défilement du navigateur	75 à 200 Ko/s	50 à 200 Ko/s	30 à 100 Ko/s
Fermeture du navigateur	100 à 150 Ko/s	75 à 100 Ko/s	30 à 60 Ko/s
Ouverture du menu Démarrer	75 à 100 Ko/s	50 à 75 Ko/s	20 à 30 Ko/s
Fermeture du menu Démarrer	75 à 100 Ko/s	25 à 50 Ko/s	10 à 15 Ko/s
Ecran de veille Champ d'étoiles	25 à 50 Ko/s	10 à 15 Ko/s	7 à 10 Ko/s
Ecran de veille d'écran Canalisations 3D	10 à 100 Ko/s	5 à 20 Ko/s	2 à 10 Ko/s
Vidéo Windows Media	500 à 1200 Ko/s	300 à 500 Ko/s	150 à 300 Ko/s
Vidéo QuickTime nº1	700 à 2500 Ko/s	400 à 500 Ko/s	150 à 350 Ko/s
Vidéo QuickTime nº2	1500 à 2500 Ko/s	400 à 550 Ko/s	200 à 350 Ko/s

Avec les paramètres de bande passante réduite, celle-ci est considérablement diminuée pour pratiquement toutes les tâches. Avec le paramètre de couleur 15 bits, les performances perçues sont similaires à celles des paramètres par défaut. En outre, les réductions de bande passante sont possibles par des modifications supplémentaires des paramètres.

Notez que ces chiffres de bande passante ne sont que des exemples et peuvent varier de ceux constatés dans votre environnement en raison de nombreux facteurs.

Comment puis-je réduire la bande passante ?

Dominion KX II offre divers paramètres dans vos clients distants pour optimiser la bande passante et les performances. Les paramètres par défaut fournissent un niveau de performances sur le rack dans les environnements de réseau local/étendu avec une utilisation économique de la bande passante.

Les paramètres de gestion de la bande passante incluent la vitesse de connexion (Connection Speed) et le nombre de couleurs (Color Depth). Pour réduire la bande passante :

Réduction de la vitesse de connexion

La réduction de la vitesse de connexion peut considérablement diminuer la bande passante utilisée. Dans les environnements de réseau local/étendu, la définition de la vitesse de connexion sur 1,5 ou 1 Mbits par seconde réduit la bande passante en maintenant des performances correctes. Les paramètres au-dessous réduiront davantage la bande passante et conviennent aux connexions par bande passante à faible débit.

Réduction du nombre des couleurs

La réduction du nombre de couleurs diminue la bande passante et augmente les performances considérablement. Toutefois, étant donné qu'un nombre inférieur de couleurs est utilisé, la vidéo s'en trouve dégradée. Ceci peut être acceptable pour certaines tâches d'administration système.

Pour les connexions Internet lentes, l'utilisation de la couleur 8 bits ou d'un nombre inférieur de bits peut réduire la bande passante et améliorer les performances.

Autres astuces pour réduire la bande passante :

- Utilisez un papier peint uni pour le Bureau au lieu d'une image complexe.
- Désactivez les écrans de veille.
- Utilisez une résolution plus basse sur le serveur cible.

- Désactivez l'option Afficher le contenu des fenêtres pendant leur déplacement dans Windows.
- Utilisez des images, thèmes et bureaux simples (par exemple, Windows Classique).

Que dois-je faire sur les connexions par bande passante à faible débit ?

Les paramètres de vitesse de connexion et de nombre de couleurs peuvent être peaufinés pour optimiser les performances des connexions par bande passante à faible débit. Par exemple, dans le client MPC ou KVM virtuel, définissez la vitesse de connexion sur 1,5 Mb ou 1 Mb, et le nombre de couleurs sur 8 bits. Des paramètres de vitesse de connexion et de nombre de couleurs plus bas encore peuvent être utilisés en cas de bande passante à très faible débit.

Je souhaite me connecter via Internet. A quel type de performance dois-je m'attendre ?

Ceci dépend de la bande passante et de la latence de la connexion Internet entre votre client distant et Dominion KX II. Avec une connexion par modem câble ou ADSL à haut débit, vos performances peuvent être très similaires à une connexion par réseau local/étendu. Pour les connexions plus lentes, utilisez les suggestions ci-dessus pour améliorer les performances.

Mon environnement dispose d'une bande passante à haut débit. Comment puis-je optimiser les performances ?

Les paramètres par défaut fournissent des performances solides dans un environnement à bande passante à haut débit. Assurez-vous que la vitesse de connexion est définie sur 100 Mb ou 1 Gb, et le nombre de couleurs sur Couleur RVB 15 bits.

Quelle est la vitesse des interfaces Ethernet de Dominion KX II ?

Dominion KX II prend en charge Gigabit et 10/100 Ethernet. Dominion KX II prend en charge deux interfaces Ethernet de vitesse 10/100/1000, avec possibilité de configurer la vitesse et les paramètres duplex (détectés automatiquement ou définis manuellement).

Est-il possible d'accéder à Dominion KX II via une connexion sans fil ?

Oui. Dominion KX II utilise non seulement l'Ethernet standard, mais également une bande passante très modérée de très haute qualité vidéo. Par conséquent, si vous disposez avez d'un client sans fil équipé d'une connectivité réseau à Dominion KX II, vous pouvez configurer et gérer vos serveurs au niveau du BIOS sans fil.

Est-il possible d'utiliser Dominion KX II sur un réseau étendu (Internet) ou uniquement sur le réseau local de l'entreprise ?

Que ce soit par un réseau local d'entreprise rapide, par un réseau étendu moins prévisible (Internet), par un modem câble ou par un modem d'accès à distance, la technologie KVM sur IP de Dominion KX II s'adapte à votre type de connexion.

Puis-je utiliser Dominion KX II avec un réseau VPN ?

Oui, Dominion KX II utilise les technologies IP (protocole Internet) standard de la couche 1 à 4. L'encombrement peut être facilement canalisé par des réseaux VPN standard.

Combien de ports TCP doivent être ouverts sur mon pare-feu pour autoriser l'accès réseau à Dominion KX II ? Ces ports sont-ils configurables ?

Un seul. Dominion KX II n'ayant besoin d'accéder qu'à un seul port TCP pour fonctionner, la sécurité de votre réseau est assurée. Pour plus de sécurité, ce port est entièrement configurable.

Notez que pour pouvoir utiliser la fonction de navigateur Web facultative de Dominion KX II, le port 443 HTTPS standard doit, bien évidemment, aussi être ouvert.

Dominion KX II requiert-il un serveur d'authentification externe pour fonctionner ?

Non. Dominion KX II est entièrement autonome. Une fois qu'une adresse IP a été affectée à Dominion KX II, il est prêt à l'emploi. Ses fonctionnalités de navigateur Web et d'authentification sont complètement intégrées.

Dominion KX II permet l'utilisation d'un serveur d'authentification externe (tel que LDAP, Active Directory, RADIUS, etc.) et, en cas d'indisponibilité de votre serveur d'authentification externe, basculera même sur son propre réseau d'authentification interne. La philosophie de conception de Dominion KX II est ainsi optimisée pour offrir une facilité d'installation, une indépendance totale vis-à-vis d'un serveur externe et un maximum de flexibilité.

Dominion KX II peut-il être utilisé avec CITRIX ?

Dominion KX II peut fonctionner avec des produits d'accès à distance tels que CITRIX si la configuration est effectuée correctement. Raritan ne peut cependant pas garantir que les performances de fonctionnement soient acceptables. Les produits tels que CITRIX utilisent des technologies de réacheminement vidéo dont le concept est similaire à celui des commutateurs KVM, si bien que deux technologies KVM par IP sont utilisées simultanément.

Dominion KX II peut-il utiliser DHCP ?

L'adressage DHCP peut être utilisé, mais Raritan recommande l'utilisation d'un adressage fixe. En effet, Dominion KX II est un dispositif d'infrastructure, et l'accès et l'administration sont réalisés plus efficacement au moyen d'une adresse IP fixe.

J'ai des problèmes à me connecter à Dominion KX II via mon réseau IP. Quel pourrait être le problème ?

Dominion KX II s'appuie sur votre réseau local/étendu. Les éventuels problèmes incluent :

- Négociation automatique d'Ethernet - Sur certains réseaux, la négociation automatique 10/100 ne fonctionne pas correctement et l'unité Dominion KX II doit alors être réglée sur 100 Mo/full duplex, ou sur une option adaptée au réseau.
- Adresse IP en double - Si l'adresse IP de Dominion KX II est la même que celle d'un autre dispositif, il est possible que la connectivité du réseau soit erratique.
- Conflits au niveau du port 5000 - Si un autre dispositif utilise le port 5000, le port par défaut de Dominion KX II (ou celui de l'autre dispositif) doit être modifié.

Lors de la modification de l'adresse IP de Dominion KX II ou du passage à un nouveau Dominion KX II, vous devez attendre suffisamment longtemps pour que ses adresses MAC et IP soient reconnues par les réseaux des couches 2 et 3.

Gestion de réseau IPv6

Qu'est-ce qu'IPv6 ?

IPv6 est l'acronyme d'Internet Protocol Version 6. Il s'agit du protocole IP nouvelle génération qui remplacera la version 4 (IPv4) actuelle du protocole IP.

IPv6 corrige certains problèmes constatés dans IPv4, comme le nombre limité d'adresses IPv4. Il améliore également IPv4 dans des domaines, tels que le routage et la configuration automatique du réseau. IPv6 devrait remplacer IPv4 graduellement, les deux coexistant pendant quelques années.

IPv6 aide à résoudre l'un des problèmes les plus épineux rencontrés par l'administrateur : la configuration et la gestion d'un réseau IP.

Pourquoi Dominion KX II prend-il en charge la gestion de réseau IPv6 ?

Les organismes publics et le ministère de la Défense américains sont maintenant dans l'obligation d'acheter des produits compatibles IPv6. En outre, de nombreuses entreprises et de nombreux pays, tels que la Chine, effectueront la transition à IPv6 au cours des prochaines années.

Qu'est-ce que la « double pile » et pourquoi est-elle nécessaire ?

La double pile consiste à prendre en charge simultanément les protocoles IPv4 et IPv6. Etant donné la transition graduelle d'IPv4 à IPv6, la double pile est un prérequis fondamental pour la prise en charge d'IPv6.

Comment puis-je activer IPv6 sur Dominion KX II ?

Utilisez la page Network Settings (Paramètres réseau), disponible depuis le menu Device Settings (Paramètres du dispositif) dans Dominion KX II. Activez l'adressage IPv6 et choisissez la configuration manuelle ou automatique. Vous devez également l'activer dans MPC.

Et si je dispose d'un serveur externe avec une adresse IPv6 address que je souhaite utiliser avec mon dispositif Dominion KX II ?

Dominion KX II peut accéder aux serveurs externes via leurs adresses IPv6 ; par exemple, un gestionnaire SNMP, un serveur Syslog ou un serveur LDAP.

Grâce à l'architecture à double pile de Dominion KX II, ces serveurs externes sont accessibles via (1) une adresse IPv4, (2) une adresse IPv6 ou (3) un nom d'hôte. Dominion KX II prend donc en charge l'environnement mixte IPv4/IPv6 dont de nombreux clients disposent.

Dominion KX I prend-il en charge IPv6 ?

Non, Dominion KX I ne prend pas en charge les adresses IPv6.

Et si mon réseau ne prend pas en charge IPv6 ?

La gestion de réseau par défaut de Dominion KX II est définie en usine pour IPv4 uniquement. Dès que vous êtes prêt à utiliser IPv6, suivez les instructions ci-dessous pour activer le fonctionnement à double pile IPv6/IPv4.

Où puis-je obtenir des informations supplémentaires sur IPv6 ?

Consultez www.ipv6.org pour obtenir des informations générales sur IPv6. Le manuel d'utilisation de Dominion KX II décrit la prise en charge de IPv6 par Dominion KX II.

Windows

Dominion KX II dépend-il d'un serveur Windows pour fonctionner ?

Absolument pas. Etant donné que les utilisateurs comptent sur l'infrastructure KVM pour être toujours disponible dans n'importe quelle situation (et qu'ils auront probablement à employer cette infrastructure pour résoudre les problèmes éventuels), Dominion KX II est conçu pour être entièrement indépendant de tout serveur externe. Par exemple, si le centre de données est attaqué par un ver ou un virus Windows, les administrateurs devront utiliser la solution KVM pour résoudre le problème. Par conséquent, il est essentiel que cette solution KVM ne dépende d'aucun de ces serveurs Windows (ou de tout autre serveur d'ailleurs) pour être opérationnelle afin que la solution KVM fonctionne.

Pour cette raison, Dominion KX II est entièrement indépendant. Même si un utilisateur choisit de configurer Dominion KX II pour permettre l'authentification par un serveur Active Directory, en cas d'indisponibilité de ce dernier, l'authentification propre à Dominion KX II sera activée et entièrement opérationnelle.

Dois-je installer un serveur Web tel que Microsoft Internet Information Services (IIS) pour utiliser la fonction de navigateur Web de Dominion KX II ?

Non. Dominion KX II est un dispositif entièrement autonome. Une fois une adresse IP affectée à Dominion KX II, ce dernier est prêt à l'emploi avec un navigateur Web et des fonctions d'authentification entièrement intégrés.

Quel logiciel dois-je installer pour accéder à Dominion KX II depuis un poste de travail donné ?

Aucun. Dominion KX II est entièrement accessible via un navigateur Web Il existe toutefois un client installé facultatif fourni sur le site Web de Raritan (www.raritan.com), qui est requis pour les connexions par modem. Un client Java est maintenant disponible pour les utilisateurs non-Windows.

Que dois-je faire pour préparer la connexion d'un serveur à Dominion KX II ?

Réglez simplement les paramètres souris de manière à fournir aux utilisateurs la meilleure synchronisation de souris lors des connexions à distance et désactivez les fonctions de gestion d'alimentation qui affectent l'affichage de l'écran. Toutefois, si vous utilisez le nouvel adaptateur D2CIM-VUSB (prenant en charge Absolute Mouse Synchronization™), vous n'avez pas besoin de régler manuellement les paramètres de souris.

Serveurs lames

Puis-je connecter des serveurs lames à Dominion KX II ?

Oui. Dominion KX II prend en charge les modèles courants de serveurs lames des principaux fabricants : HP, IBM et Dell.

Quels serveurs lames sont pris en charge ?

Les modèles suivants sont pris en charge :

- Dell PowerEdge 1855, 1955 et M1000e
- HP BladeSystem c3000 et c7000
- IBM BladeCenter H et E

Remarque : les modèles S, T et HT IBM BladeCenter sont gérés à l'aide de la sélection IBM (Other) (IBM (Autre)).

Les CIM lames Paragon sont-ils utilisés ?

Non, le CIM lame Paragon II ne fonctionnera pas avec Dominion KX II.

Quel CIM dois-je utiliser ?

Tout dépend du type de ports KVM figurant sur la marque et le modèle spécifiques du serveur lame que vous utilisez. Les CIM suivants sont pris en charge : DCIM-PS2, DCIM-USBG2, D2CIM-VUSB et D2CIM-DVUSB.

Quels types d'accès et de contrôle sont disponibles ?

Dominion KX II offre un accès KVM automatisé et sécurisé : (1) sur le rack, (2) à distance sur IP, (3) via CommandCenter et (4) par modem.

Dois-je utiliser des raccourcis-clavier pour permuter entre les lames ?

Certains serveurs lames requièrent l'utilisation de raccourcis-clavier pour permuter entre les lames. Avec Dominion KX II, ces raccourcis-clavier sont inutiles. Il vous suffit de cliquer sur le nom du serveur lame pour que Dominion KX II passe automatiquement sur cette lame sans l'utilisation explicite du raccourci-clavier.

Puis-je accéder au module de gestion du serveur lame ?

Oui, vous pouvez définir l'URL du module de gestion et y accéder depuis Dominion KX II ou CC-SG. S'il est configuré, l'accès en un clic est disponible.

Combien de serveurs lames puis-je connecter à un dispositif Dominion KX II ?

Aux fins de performances et de fiabilité, vous pouvez connecter jusqu'à 8 châssis de lames à un dispositif Dominion KX II, indépendamment du modèle. Raritan recommande de connecter jusqu'à deux fois le nombre de connexions à distance prises en charge par le dispositif. Par exemple, avec un KX2-216 doté de deux canaux à distance, nous vous recommandons de connecter jusqu'à quatre châssis de serveurs lames. Vous pouvez bien entendu connecter des serveurs individuels aux ports de serveur restants.

Je suis un client SMB possédant quelques Dominion KX II. Dois-je utiliser votre station de gestion CC-SG ?

Non, vous n'y êtes pas obligé. Les clients SMB n'ont pas à utiliser CC-SG pour exploiter les nouvelles fonctions de lames.

Je suis un client professionnel utilisant CC-SG. Puis-je accéder aux serveurs lames via CC-SG ?

Oui. Une fois les serveurs lames configurés sur Dominion KX II, l'utilisateur CC-SG peut y accéder via des connexions KVM. En outre, les serveurs lames sont organisés par châssis, ainsi que par vues personnalisées CC-SG.

Et si je souhaite un accès KVM en bande ou intégré ?

Oui, l'accès en bande et intégré aux serveurs lames peut être configuré au sein de CC-SG.

J'exécute VMware sur certains serveurs lames. Est-ce pris en charge ?

Oui, avec CC-SG, vous pouvez afficher les machines virtuelles exécutées sur les lames serveurs, et y accéder.

Le support virtuel est-il pris en charge ?

Nous prenons en charge cette fonction sur les modèles H et E IBM BladeCenter, avec D2CIM - DVUSB.

La synchronisation absolue de la souris est-elle prise en charge ?

Les serveurs disposant de commutateurs KVM internes dans un châssis à lame ne prennent habituellement pas en charge la technologie de souris absolue. Pour HP Blade et certains serveurs lames Dell, le CIM est connecté à chaque lame. La synchronisation absolue de la souris est donc prise en charge si le système d'exploitation sous-jacent exécuté sur la lame la supporte.

L'accès aux lames est-il sécurisé ?

Oui, l'accès aux lames utilisent toutes les fonctions de sécurité standard de Dominion KX II, telles que le chiffrement 128 bits ou 256 bits. En outre, il existe des fonctions de sécurité spécifiques aux lames, telles que les autorisations d'accès par lame et le blocage des raccourcis-clavier qui interdit l'accès non autorisé.

Les dispositifs Dominion KSX II ou KX II-101 prennent-ils en charge les serveurs lames ?

Pour le moment, ces produits ne disposent pas de ces nouvelles fonctionnalités de serveurs lames.

Installation

Hormis le dispositif lui-même, que dois-je commander à Raritan pour installer Dominion KX II ?

Chaque serveur connecté à Dominion KX II requiert un module d'interface pour ordinateur (CIM) Dominion ou Paragon, et un adaptateur qui se branche directement sur les ports clavier, écran et souris du serveur.

Quel type de câble Cat5 dois-je utiliser pour mon installation ?

Dominion KX II peut utiliser n'importe quel câble UTP (à paire torsadée) standard : Cat5, Cat5e ou Cat6. Dans ses manuels et brochures publicitaires, Raritan ne mentionne bien souvent que le câble « Cat5 ». En réalité, n'importe quel câble marqué UTP convient pour Dominion KX II.

Quels types de serveurs peuvent être connectés à Dominion KX II ?

Dominion KX II n'est lié à aucun fabricant. N'importe quel serveur avec ports clavier, vidéo et souris normalisés peut être connecté.

Comment puis-je connecter des serveurs à Dominion KX II ?

Les serveurs connectés à Dominion KX II requièrent un module d'interface pour ordinateur (CIM) Dominion ou Paragon qui se branche directement sur les ports clavier, écran et souris du serveur. Connectez ensuite chaque CIM à Dominion KX II au moyen d'un câble UTP (à paire torsadée) standard : Cat5, Cat5e ou Cat6.

Quelle est la distance maximale autorisée entre mes serveurs et Dominion KX II ?

En règle générale, les serveurs peuvent se trouver jusqu'à 45 m de Dominion KX II, selon le type de serveur. Reportez-vous au site Web de Raritan (www.raritan.com) ou à ***Distance de connexion et résolution vidéo du serveur cible*** (à la page 289) pour plus d'informations. Pour les nouveaux CIM D2CIM-VUSB et D2CIM-DVUSB qui prennent en charge les fonctions Support virtuel et Synchronisation absolue de la souris, une distance de 30 m est recommandée.

Certains systèmes d'exploitation se bloquent lorsque je déconnecte un clavier ou une souris pendant le fonctionnement. Que faut-il faire pour éviter aux serveurs connectés à Dominion KX II de se bloquer lorsque je passe à un autre ?

Chaque clé électronique de module d'interface pour ordinateur Dominion (DCIM) se comporte comme un clavier et une souris virtuels vis-à-vis du serveur auquel elle est connectée. Cette technologie est appelée KME (émulation clavier/souris). La technologie KME de Raritan est adaptée aux centres de données, a fait ses preuves sur le terrain et est d'une fiabilité nettement supérieure à celle des commutateurs KVM bas de gamme : fruit de plus de 15 années d'expérience, elle a été déployée sur des millions de serveurs dans le monde entier.

Ne faut-il pas installer des agents sur les serveurs connectés à Dominion KX II ?

Dominion KX II étant directement connecté par voie matérielle aux ports clavier, vidéo et souris des serveurs, les serveurs connectés à Dominion KX II ne nécessitent l'installation d'aucun agent logiciel.

Combien de serveurs peuvent être connectés à chaque dispositif Dominion KX II ?

La gamme des modèles Dominion KX II offre de 8, 16 ou 32 ports dans un châssis 1U, à 64 ports dans un châssis 2U. C'est le commutateur KVM numérique offrant la densité de ports la plus élevée du secteur.

Que se passe-t-il si je déconnecte un serveur de Dominion KX II, le connecte à un autre dispositif Dominion KX II, ou le connecte à un port différent sur le même dispositif Dominion KX II ?

Dominion KX II met automatiquement à jour les noms de ports de serveurs lorsque les serveurs sont déplacés d'un port à l'autre. De plus, cette mise à jour automatique n'affecte pas seulement le port d'accès local, mais également tous les clients distants et l'appareil de gestion CommandCenter Secure Gateway en option.

Comment dois-je connecter un dispositif contrôlé en série (RS-232) à Dominion KX II, tel qu'un routeur/commutateur Cisco ou un serveur Sun headless (sans tête) ?

Si le nombre de dispositifs contrôlés en série est réduit, ils peuvent être connectés à Dominion KX II via le nouveau convertisseur série P2CIM-SER de Raritan.

Toutefois, si vous disposez d'au moins quatre dispositifs contrôlés en série, nous vous recommandons d'utiliser la gamme KSX II ou SX de Raritan des serveurs de console sécurisée. Ces dispositifs sont simples à utiliser, à configurer et à gérer et peuvent être entièrement intégrés au déploiement d'une série Dominion. En particulier, de nombreux administrateurs UNIX et de réseau apprécient l'utilisation du protocole SSH pour établir une connexion directe avec un dispositif.

Port local

Est-il possible d'accéder à mes serveurs directement depuis le rack ?

Oui. Sur le rack, Dominion KX II se comporte exactement comme un commutateur KVM traditionnel, vous permettant de contrôler jusqu'à 64 serveurs au moyen d'un seul clavier, écran et souris.

L'accès à distance aux serveurs d'autres utilisateurs est-il bloqué lorsque j'utilise le port local ?

Non. Le port local de Dominion KX II dispose d'un chemin d'accès aux serveurs entièrement indépendant. Cela signifie qu'un utilisateur peut accéder localement aux serveurs sur le rack, sans affecter le nombre d'utilisateurs qui accèdent simultanément au rack à distance.

Est-il possible d'utiliser un clavier ou une souris USB sur le port local ?

Oui. Dominion KX II offre à la fois des ports clavier et souris PS/2 et USB sur le port local. Notez que les ports USB sont des ports USB v1.1 et ne supportent que les claviers et souris, et non des dispositifs USB tels que des scanneurs ou des imprimantes.

Existe-t-il un affichage à l'écran pour l'accès local sur le rack ?

Oui, mais l'accès sur le rack de Dominion KX II dépasse largement les affichages écran classiques. Doté de l'interface navigateur la plus aboutie du secteur en matière d'accès sur le rack, le port local de Dominion KX II utilise la même interface pour l'accès local et distant. Par ailleurs, la plupart des fonctions d'administration sont disponibles sur le rack.

Comment sélectionner les serveurs tout en utilisant le port local ?

Le port local affiche les serveurs connectés à l'aide de la même interface utilisateur que celle du client distant. Connectez-vous à un serveur d'un simple clic de souris.

Comment s'assurer que seuls les utilisateurs autorisés peuvent accéder aux serveurs depuis le port local ?

Les utilisateurs essayant d'utiliser le port local doivent subir le même niveau d'authentification que les utilisateurs à distance. En d'autres termes :

- Si votre Dominion KX II est configuré pour interagir avec un serveur RADIUS, LDAP ou Active Directory externe, les utilisateurs essayant d'accéder au port local seront authentifiés par le même serveur.
- Si les serveurs d'authentification externe ne sont pas disponibles, Dominion KX II passe sur sa base de données d'authentification interne.

- Dominion KX II possède sa propre authentification autonome, offrant une installation instantanée, prête à l'emploi.

En cas d'utilisation du port local pour renommer un serveur connecté, est-ce que cela affecte également les clients d'accès distant ? L'unité CommandCenter en option est-elle affectée ?

Oui. La présentation du port local est identique et entièrement synchronisée avec les clients d'accès distant et la console de gestion CommandCenter Secure Gateway en option de Raritan. Plus simplement, si vous renommer un serveur sur l'affichage à l'écran Dominion KX II, cela met à jour en temps réel tous les clients à distance et les serveurs de gestion externes.

En cas d'utilisation des outils d'administration à distance de Dominion KX II pour renommer un serveur connecté, est-ce que cela affecte également l'affichage à l'écran du port local ?

Oui. Si vous renommez un serveur à distance ou au moyen de la console de gestion CommandCenter Secure Gateway en option de Raritan, cette mise à jour affecte immédiatement l'affichage à l'écran de Dominion KX II.

Parfois je vois des « ombres » sur l'interface utilisateur du port local. Quelle en est l'origine ?

Ces ombres/effets de réplication peuvent apparaître sur les écrans LCD qui sont restés allumés longtemps. Les propriétés LCD et la charge électrique/statique peuvent générer ces effets lorsque l'écran est sous tension sur une longue période.

Port local étendu (modèles KX2-832 et KX2-864 Dominion uniquement)

Qu'est-ce que le port local étendu ?

Dominion KX2-832 et KX2-864 comportent un port local étendu. Les modèles huit utilisateurs de Dominion KX II sont dotés d'un port local standard, et d'un nouveau port local étendu qui prolonge le port local, via un câble Cat5, au-delà du rack vers une salle de contrôle, un autre point du centre de données ou un commutateur Paragon II.

Le port local étendu requiert-il une station utilisateur ?

Oui, les dispositifs suivants peuvent servir de « station utilisateur » pour le port local étendu. Paragon II EUST, Paragon II UST et le dispositif URKVMG Cat5 Reach. En outre, le port local étendu peut être connecté via un câble Cat5 à un port serveur sur un commutateur Paragon II. Cette configuration peut être utilisée pour consolider les ports locaux de nombreux dispositifs KX2-8xxx sur un seul commutateur.

Quelle est la distance maximale autorisée entre la station utilisateur et Dominion KX II ?

La distance est de 61 m à 305, mais varie selon le type de station utilisateur, la résolution vidéo, le type et la qualité du câble.

Un CIM est-il nécessaire ?

Un CIM n'est pas nécessaire. Il vous suffit de connecter un câble Cat5.

Dois-je utiliser le port local étendu ?

Non, le port local étendu est une fonction facultative et est désactivé par défaut. Utilisez la page Local Port Settings (Paramètres du port local). Pour plus de sécurité, vous pouvez également désactiver le port local standard si vous ne l'utilisez pas.

Gestion de l'alimentation

Dominion KX II propose-t-il l'option de double alimentation ?

Tous les modèles Dominion KX II sont équipés d'arrivées CA et d'alimentations en double avec basculement automatique. En cas de défaillance au niveau d'une arrivée électrique ou de l'alimentation électrique, Dominion KX II commute automatiquement sur l'autre système.

Les paramètres de tension sont-ils automatiquement détectés par l'alimentation de Dominion KX II ?

Oui. L'alimentation de Dominion KX II peut être utilisée sur une tension alternative comprise entre 100 et 240 volts, à 50-60 Hz.

Suis-je informé en cas de coupure de courant ou de défaillance au niveau d'une arrivée électrique ?

Le voyant DEL situé sur le panneau avant de Dominion KX II avertit l'utilisateur d'une panne de courant. Une entrée est également envoyée dans le journal d'audit et affichée dans l'interface utilisateur Remote Client de Dominion KX II. Des événements SNMP ou Syslog sont également générés, si les options correspondantes ont été configurées par l'administrateur.

Quelles sont les fonctions de gestion de l'alimentation offertes par Dominion KX II ?

Les barrettes de gestion d'alimentation à distance de Raritan peuvent être branchées sur Dominion KX II pour contrôler l'alimentation des serveurs cible. Après une simple opération de configuration unique, il vous suffit de cliquer avec le bouton droit de la souris sur le nom du serveur pour mettre sous tension, hors tension ou réactiver un serveur bloqué. Notez que redémarrer physiquement équivaut à débrancher le serveur de la prise de courant, puis à le rebrancher.

Dominion KX II prend-il en charge les serveurs à alimentations multiples ? Que se passe-t-il si chaque alimentation est branchée sur une barrette d'alimentation différente ?

Oui. Dominion KX II peut être facilement configuré pour prendre en charge des alimentations multiples branchées sur plusieurs barrettes d'alimentation. Jusqu'à huit (8) barrettes d'alimentation peuvent être connectées au dispositif Dominion KX II. Quatre alimentations peuvent être connectées par serveur cible sur plusieurs barrettes d'alimentation.

La gestion de l'alimentation à distance nécessite-t-elle une configuration spéciale du serveur ?

Certains serveurs sont livrés avec des paramètres BIOS par défaut qui rendent impossible le redémarrage automatique du serveur après une coupure de l'alimentation et son rétablissement. Consultez la documentation du serveur pour modifier ce paramètre.

Quel type de barrettes d'alimentation Dominion KX II prend-il en charge ?

Pour tirer parti de l'interface utilisateur de gestion de l'alimentation intégrée de Dominion KX II et encore plus de la sécurité intégrée, utilisez les barrettes d'alimentation Remote Power Control (RPC) de Raritan. Elles sont livrées avec de nombreuses variations de prises, connecteurs et tensions. Vous devez vous procurer le module D2CIM-PWR pour connecter les barrettes RPC à Dominion KX II.

Evolutivité

Comment puis-je interconnecter plusieurs dispositifs Dominion KX II pour obtenir une solution unique ?

Il n'est pas nécessaire de connecter physiquement entre eux plusieurs dispositifs Dominion KX II. Chaque Dominion KX II est plutôt connecté au réseau. Ils fonctionnent automatiquement ensemble en tant que solution unique s'ils sont déployés avec la console de gestion en option CommandCenter Secure Gateway (CC-SG) de Raritan. CC-SG sert de point d'accès et de gestion à distance unique. CC-SG offre tout un ensemble d'outils pratiques, tels que le regroupement de la configuration et de la mise à jour des firmware, ainsi qu'une base de données d'authentification et d'autorisation unique.

De plus, CC-SG permet des fonctions de tri, de définition d'autorisations et d'accès avancées pour les serveurs. Si le déploiement de la console de gestion CC-SG de Raritan n'est pas envisageable, les dispositifs Dominion KX II multiples continuent d'interagir et d'évoluer automatiquement : L'interface utilisateur distante de Dominion KX II et le Client MPC détecteront automatiquement les unités Dominion KX II. Vous pouvez accéder aux dispositifs Dominion KX II qui n'ont pas été détectés au moyen d'un profil défini par l'utilisateur.

Est-il possible de connecter un commutateur KVM analogique existant à Dominion KX II ?

Oui. Les commutateurs KVM analogiques peuvent être connectés à l'un des ports de serveur de Dominion KX II. Il vous suffit d'utiliser un module d'interface pour ordinateur (CIM) PS/2 et de le connecter aux ports utilisateur du commutateur KVM analogique existant. Notez que les spécifications des commutateurs KVM varient, et que Raritan ne peut pas garantir l'interopérabilité d'un commutateur KVM analogique tiers particulier. Contactez le support technique Raritan pour obtenir de plus amples informations.

Modules d'interface pour ordinateur (CIM)

Est-il possible d'utiliser des modules d'interface pour ordinateur (CIM) venant du commutateur analogique matriciel KVM de Raritan, Paragon, avec Dominion KX II ?

Oui. Certains modules d'interface pour ordinateur (CIM) Paragon peuvent être compatibles avec Dominion KX II (consultez les notes de version de Dominion KX II sur le site Web de Raritan pour obtenir la dernière liste de ces modules certifiés).

Toutefois, les modules d'interface pour ordinateur (CIM) Paragon étant plus chers que les modules de Dominion KX II (en raison de leur technologie de transmission vidéo intégrée sur une distance allant jusqu'à 300 mètres), il n'est généralement pas conseillé d'acheter les modules Paragon pour les utiliser avec Dominion KX II. Notez également que lorsque les modules d'interface pour ordinateur Paragon sont connectés à Dominion KX II, leur transmission vidéo est limitée à 45 mètres, égalant les performances de transmission des modules Dominion KX II, et n'est plus de 300 mètres comme lorsqu'ils sont connectés à Paragon.

Est-il possible d'utiliser des modules d'interface pour ordinateur (CIM) venant de Dominion KX II avec le commutateur analogique matriciel KVM de Raritan, Paragon ?

Non. Les modules d'interface pour ordinateur Dominion KX II offrent une transmission vidéo sur une distance de 15 à 45 mètres et par conséquent, ne sont pas compatibles avec Paragon, qui nécessite des modules avec transmission vidéo sur une distance de 300 mètres. Pour que tous les clients de Raritan bénéficient de la qualité vidéo la plus performante qui soit du secteur, une caractéristique constante de Raritan, il n'existe pas d'interopérabilité entre les modules d'interface pour ordinateur (CIM) de série Dominion ne sont pas compatibles et Paragon.

Sécurité

Dominion KX II est-il certifié FIPS 140-2 ?

Depuis la version 2.2.0, Dominion KX II offre aux utilisateurs la possibilité d'employer un module cryptographique validé FIPS 140-2 s'exécutant sur une plate-forme Linux selon les directives de mise en œuvre de FIPS 140-2. Ce module cryptographique sert au cryptage du trafic de session KVM constitué de données vidéo, de clavier, de souris, de support virtuel et de carte à puce.

Quel type de chiffrement Dominion KX II utilise-t-il ?

Dominion KX II utilise un système de chiffrement RC4 ou AES standard (extrêmement sûr) pour ses communications SSL et son propre flux de données. Littéralement, aucune donnée n'est transmise entre les clients distants et Dominion KX II si elle n'est pas complètement sécurisée par chiffrement.

Dominion KX II prend-il en charge le chiffrement AES comme recommandé par les normes NIST et FIPS 140-2 du gouvernement américain ?

Dominion KX II utilise le chiffrement AES (Advanced Encryption Standard) pour une sécurité accrue.

AES est un algorithme de cryptage approuvé par le gouvernement américain et recommandé par l'Institut National des Normes et de la Technologie (NIST - National Institute of Standards and Technology) dans la norme FIPS 197.

Dominion KX II permet-il le chiffrement de données vidéo ? Ou effectue-t-il uniquement le chiffrement des données de clavier et de souris ?

Contrairement aux solutions concurrentes, qui ne chiffrent que les données de clavier et de souris, Dominion KX II ne met pas votre sécurité en danger. Il permet de chiffrer les données de clavier, souris et vidéo.

Comment Dominion KX II intègre-t-il les serveurs d'authentification externes tels qu'Active Directory, RADIUS ou LDAP ?

Grâce à une configuration très simple, il est possible de programmer Dominion KX II pour renvoyer toutes les demandes d'authentification vers un serveur externe tel que LDAP, Active Directory ou RADIUS. Pour chaque utilisateur authentifié, le serveur d'authentification transmet à Dominion KX II le groupe auquel appartient l'utilisateur concerné. Dominion KX II détermine ensuite les autorisations d'accès de l'utilisateur en fonction du groupe auquel il appartient.

Comment sont stockés les noms d'utilisateur et mots de passe ?

En cas d'utilisation des fonctions d'authentification interne de Dominion KX II, toutes les informations critiques, telles que les noms d'utilisateur et mots de passe, sont stockées sous une forme cryptée. En d'autres termes, personne, pas même le support technique ni les services d'ingénierie de produits Raritan, ne peut récupérer ces noms d'utilisateur et mots de passe.

Dominion KX II prend-il en charge les mots de passe sécurisés ?

Oui, Dominion KX II dispose de la fonction de vérification stricte du mot de passe, configurable par l'administrateur, afin de garantir que les mots de passe créés par les utilisateurs répondent aux normes gouvernementales et/ou d'entreprise et résistent au piratage de force.

Si le mode de chiffrement de Dominion KX II est défini sur Auto, quel est le niveau de chiffre obtenu ?

Le niveau de chiffrement qui est négocié automatiquement est tributaire du navigateur utilisé.

Authentification par cartes à puce et CAC

Dominion KX II prend-il en charge l'authentification par carte à puce et CAC ?

Oui, l'authentification par cartes à puce et DoD Common Access Card (CAC) sur les serveurs cible est prise en charge depuis la version 2.1.10.

Quels modèles de Dominion KX II prennent en charge les cartes à puce/CAC ?

Tous les modèles Dominion KX II. Dominion KSX2 et KX2-101 ne prennent pas pour le moment en charge les cartes à puce et CAC.

Quels CIM prennent en charge les cartes à puce/CAC ?

D2CIM-DVUSB est nécessaire. Ce CIM doit être mis à niveau avec la version 2.1.10 du firmware.

Quelle version de firmware est nécessaire ?

La version 2.1.10 de Dominion KX II au minimum est requise.

Quels lecteurs de cartes à puce sont pris en charge ?

Les normes de lecteur requises sont CCID USB et PC/SC. Consultez ***Lecteurs de cartes à puce pris en charge ou non*** (à la page 293) par Dominion KX II 2.1.10 ou les les notes de publication pour obtenir la liste des lecteurs certifiés et des informations supplémentaires.

L'authentification par carte à puce/CAC fonctionne-t-elle sur le port local et via Command Center ?

Oui. Pour le port local, connectez un lecteur de cartes à puce compatible au port USB de Dominion KX II.

Les UST et CIM Paragon habilités carte à puce sont-ils utilisés ?

Non, P2-EUST/C et P2CIM-AUSB-C ne sont pas intégrés à la solution Dominion KX II.

Capacités de gestion

Est-il possible de gérer et de configurer à distance Dominion KX II via un navigateur Web ?

Oui, Dominion KX II peut être complètement configuré via un navigateur Web. Pour cela, votre poste de travail doit disposer d'une version de Java Runtime Environment (JRE) appropriée.

Il est possible de configurer entièrement la solution sur le réseau à l'exception du paramètre initial de l'adresse IP de Dominion KX II. (En fait, vous pouvez même configurer les paramètres initiaux au moyen d'un câble Ethernet croisé et de l'adresse IP par défaut de Dominion KX II via un navigateur Web.)

Est-il possible de sauvegarder et de restaurer la configuration de Dominion KX II ?

Oui, il est possible de sauvegarder entièrement les configurations de l'utilisateur et du dispositif Dominion KX II pour une restauration ultérieure en cas de catastrophe.

Les fonctionnalités de sauvegarde et de restaurer de Dominion KX II peuvent être utilisées à distance sur le réseau ou via la console distante.

Quelles fonctions d'audit ou de consignation Dominion KX II offre-t-il ?

Pour assurer toutes les responsabilités, Dominion KX II consigne tous les principaux événements utilisateur et système avec la date et l'heure exactes. Par exemple, les événements rapportés comprennent (liste non exhaustive) : connexion de l'utilisateur, déconnexion de l'utilisateur, accès utilisateur à un serveur particulier, échec de connexion, modifications de configuration, etc.

Dominion KX II peut-il s'intégrer à Syslog ?

Oui. Dominion KX II peut également, en plus de ses propres fonctions de consignation interne, envoyer tous les événements enregistrés vers un serveur Syslog centralisé.

Dominion KX II peut-il s'intégrer à SNMP ?

Oui. Dominion KX II peut également, en plus de ses propres fonctions de consignation interne, envoyer des traps SNMP vers les systèmes de gestion SNMP comme HP Openview et CC-NOC de Raritan.

Est-il possible de synchroniser l'horloge interne de Dominion KX II avec un serveur de temps ?

Oui, Dominion KX II prend en charge le protocole NTP standard pour se synchroniser avec le serveur de temps de votre entreprise ou avec n'importe quel serveur de temps public (en partant du principe que le pare-feu de votre entreprise autorise les demandes NTP sortantes).

Divers

Quelle est l'adresse IP par défaut de Dominion KX II ?

192.168.0.192

Quels sont les nom d'utilisateur et mot de passe par défaut de Dominion KX II ?

Le nom d'utilisateur par défaut de Dominion KX II est admin et le mot de passe raritan [tout en minuscules]. Cependant, au niveau de sécurité le plus élevé, Dominion KX II force l'administrateur à changer les nom d'utilisateur et le mot de passe administratifs par défaut lorsque l'unité est lancée pour la première fois.

En cas de modification et d'oubli du mot de passe administratif de Dominion KX II, vous est-il possible de le récupérer ?

Dominion KX II comporte un bouton de réinitialisation matérielle qui peut être utilisé pour rétablir les paramètres usine du dispositif et par la même occasion le mot de passe administratif sur le dispositif.

Je suis connecté à Dominion KX II via Firefox et j'ai ouvert un autre navigateur Firefox. Je suis automatiquement connecté au même dispositif Dominion KX II avec le second navigateur Firefox. Est-ce normal ?

Oui. C'est le résultat direct des modes de fonctionnement des navigateurs et des cookies.

Je suis connecté à Dominion KX II via Firefox et j'essaie de me connecter à un autre via une autre session du navigateur Firefox à partir du même client. Je suis déconnecté des deux Dominion KX II. Ce comportement est-il correct ?

Oui, pour accéder à deux dispositifs Dominion KX II distincts, vous devez fermer la première session ou utiliser un autre PC client.

Lorsque j'exécute une session KVM à l'aide de mon navigateur Firefox et que certaines boîtes de dialogue sont ouvertes dans Virtual KVM Client (par exemple, Connection Properties, Video Settings), cela semble bloquer le navigateur (même d'autres sessions Firefox). Que puis-je faire ?

Ce comportement est normal car toutes les sessions Firefox sont associées. Dès que vous fermez la boîte de dialogue Virtual KVM Client, Firefox n'est plus bloqué.

Index

A

A partir de Active Directory (AD) de Microsoft - 301
A partir de LDAP - 301
A. Alimentation CA - 29
Accès à distance - 327
Accès à Dominion KX II à l'aide de la CLI - 249
Accès à Telnet depuis un PC Windows - 250
Accès à un serveur cible - 268
Accès par carte à puce à la console locale - 83, 262
Accès par carte à puce pour les dispositifs KX2 8 - 263
Accès SSH depuis un PC Windows - 249
Accès SSH depuis un poste de travail UNIX/Linux - 250
Activation de FIPS 140-2 - 216, 219
Activation de Telnet - 250
Active KVM Client (AKC) - 2, 89
Administration des commandes de configuration du serveur de console de Dominion KX II - 257
Administration du port local - 269
Affectation d'une adresse IP - 33
Aide Dominion KX II - 1
Aide pour la sélection des profils USB - 318
Ajout d'attributs à la classe - 303
Ajout d'un nouveau groupe d'utilisateurs - 117, 126
Ajout d'un nouvel utilisateur - 126, 127
Ajout, suppression et modification des favoris - 54
Appellation des barrettes d'alimentation de KX II (page Port pour les barrettes d'alimentation) - 168
Applications clients utilisables avec Dominion KX II - 5
Arrêt de la gestion par CC-SG - 239
Association de prises aux serveurs cible sur KX II - 170
Astuces pour ajouter une interface Navigateur Web - 176, 179, 181, 183, 185
Authentification à distance - 39, 203, 271
Authentification par cartes à puce et CAC - 355
Auto-Sense Video Settings (Détection automatique des paramètres vidéo) - 70

B

B. Port du modem (facultatif) - 30
Backup and Restore (Sauvegarde et restauration) - 187, 229
Barre d'outils VKC - 58
Branchement d'une barrette d'alimentation - 166

C

C. Port réseau - 30
Calibrage de la couleur - 71
Capacités de gestion - 356
Caractéristiques du produit - 9
Cartes à puce (VKC et MPC) - 81
CC-SG - 322
CD-ROM/DVD-ROM/ISO Images (Images ISO/CD-ROM/DVD-ROM) - 99, 103
Certificats SSL - 224
CIM - 320
CIM pris en charge pour les châssis de lames - 175, 177, 181, 190
Clavier français - 311
Clavier Macintosh - 314
Claviers - 311
Claviers Macintosh - 314
Claviers non américains - 311
Combinaisons de touches et Java Runtime Environment (JRE) - 312
Combinaisons de touches Macintosh non prises en charge - 314
Combinaisons de touches Sun spéciales - 267
Commande interface - 258
Commande IPv6 - 259
Commande name - 258
Commandes CLI - 248, 255
Commandes courantes pour tous les niveaux de la CLI - 253
Commutation entre les serveurs cible KVM - 60
Compatibilité CIM - 107
Comportement des dispositifs USB composites Windows 2000 pour la fonction Support virtuel - 321
Conditions dans lesquelles la fonction Lecture-écriture n'est pas disponible - 102

Conditions préalables à l'utilisation d'AKC - 90
Conditions requises pour l'utilisation des supports virtuels - 96
Configuration de la gestion des événements - Paramètres - 155
Configuration de l'alimentation - 30, 39, 162
Configuration des autorisations - 2, 117, 119
Configuration des autorisations d'accès aux ports - 117, 121, 124
Configuration des châssis de lames - 172
Configuration des châssis de lames Dell® - 177
Configuration des châssis de lames génériques - 175
Configuration des châssis de lames HP® (Gestion des groupes de ports) - 187, 190
Configuration des châssis de lames IBM® - 181
Configuration des cibles des barrettes d'alimentation (PDU de rack) - 166
Configuration des paramètres de date et heure - 153
Configuration des paramètres du port local de Dominion KX II - 31, 200, 204, 273
Configuration des paramètres du port local de Dominion KX II depuis la console locale - 273
Configuration des paramètres du port local de la console locale de Dominion KX II - 269
Configuration des ports - 164
Configuration des profils USB (page Port) - 114, 183, 197
Configuration des serveurs cible standard - 165
Configuration du contrôle d'accès IP - 221
Configuration du réseau - 257
Configuration du serveur de fichiers (Images ISO du serveur de fichiers uniquement) - 99
Configuration initiale à l'aide de la CLI - 254
Configuration système minimale requise - 262, 295
Configurations requises et recommandées de châssis de lames - 175, 177, 181, 193
Connection Properties (Propriétés de connexion) - 63
Connexion - 250, 251
Connexion à distance - 290
Connexion à un serveur cible KVM - 57, 62
Connexion aux supports virtuels - 101
Connexion SSH à Dominion KX II - 249
Connexion via Telnet à Dominion KX II - 250
Connexions par carte à puce VKC et MPC aux serveurs Fedora - 316
Console locale de Dominion KX II - 260
Contenu de l'emballage - 12
Création de groupes d'utilisateurs et d'utilisateurs - 40
Création d'un attribut - 302
Curseur de souris simple - 79

D

D. Port pour accès local (PC local) - 31
Déconnexion des serveurs cible KVM - 61
Déconnexion des supports virtuels - 99, 105
Déconnexion d'un utilisateur (Déconnexion forcée) - 127
Définition des autorisation pour un groupe individuel - 122, 126
Définition des paramètres - 254
Définition des paramètres réseau - 255
Définition du Registre pour autoriser les opérations d'écriture sur le schéma - 302
Définition d'une macro de clavier - 66
Dépannage des problèmes de blocage de Firefox lors de l'utilisation de Fedora - 316
Déplacement entre ports de Dominion KX II - 323
Désignation des serveurs cible - 37
Détection des dispositifs sur le sous-réseau de Dominion KX II - 53
Détection des dispositifs sur le sous-réseau local - 52
Device Information (Informations sur le dispositif) - 228
Diagnostics - 241
Dispositifs pris en charge par le port local étendu de KX2-832 et de KX2-864 - 201, 289
Disposition de la console Dominion KX II - 45
Distance de connexion et résolution vidéo du serveur cible - 289, 291, 345
Distances maximales recommandées pour le port local étendu de KX2-832 et de KX2-864 - 290
Divers - 357
Documentation connexe - 1
Dominion KX II - Présentation - 3
Données de connexion par défaut - 13
Durée d'amorçage du BIOS cible avec les supports virtuels - 322

E

E. Ports de serveur cible - 32
Echec de connexion des supports virtuels lors de l'utilisation du haut débit - 322
Encryption & Share (Chiffrement & partage) - 2, 215, 219
Etape 1
Configuration des serveurs cible KVM - 13, 14
Etape 2
Configuration des paramètres du pare-feu de réseau - 13, 28
Etape 3
Connexion de l'équipement - 13, 29, 37, 165, 175, 177, 181
Etape 4
Configuration de Dominion KX II - 13, 32
Etape 5 (facultative)
Configuration de la langue du clavier - 13, 40
Ethernet et mise en réseau IP - 332
Evolutivité - 351
Exemples de formats d'URL de châssis de lames - 179, 180, 183, 184, 195
Exemples de touches de connexion - 202, 266, 271
Exigences en matière de client distant - 296
Exigences en matière de port local - 295
Exigences en matière de prise en charge de FIPS 140-2 - 220
Exigences en matière de serveur cible - 295

F

FAQ - 324
Fedora - 316

G

Gestion de la sécurité - 209
Gestion de l'alimentation - 350
Gestion de l'alimentation d'un serveur cible - 60
Gestion de réseau IPv6 - 339
Gestion des conflits dans les noms de profil - 233
Gestion des dispositifs - 142
Gestion des événements - 154
Gestion des événements - Destinations - 157
Gestion des favoris - 50
Gestion des prises de barrettes d'alimentation (PDU de rack) - 205
Groupes d'utilisateurs - 115

H

Historique des mises à niveau - 237

I

Impératifs d'environnement - 279
Implémentation de l'authentification à distance LDAP/LDAPS - 129
Implémentation de l'authentification à distance RADIUS - 134
Informations sur la connexion - 65
Installation - 345
Installation et configuration - 13
Interface de la console distante de Dominion KX II - 43
Interface de la console locale de Dominion KX II - 43, 261
Interface de ligne de commande (CLI) - 248
Interface Multi-Platform Client - 56
Interfaces - 42
Introduction - 1
Invites CLI - 255

J

Java Runtime Environment (JRE) - 309
Journal d'audit - 227, 273, 274

L

Lancement de la console distante de Dominion KX II - 44
Lancement de MPC à partir d'un navigateur Web - 56
Lancement d'une macro de clavier - 68
Langues de clavier prises en charge - 292
LCA (liste de contrôle d'accès) IP de groupes - 117, 122, 124, 221
Lecteurs de cartes à puce - 293
Lecteurs de cartes à puce pris en charge ou non - 81, 262, 293, 355
Limitations de connexion - 209, 210
Liste des groupes d'utilisateurs - 116
Liste des utilisateurs - 125
Local Drives (Lecteurs locaux) - 101
Logiciel - 10
Longueurs de câbles et résolutions vidéo pour châssis Dell - 177, 315

M

Macros de clavier - 66
Maintenance - 227

Matériel - 9
Mise à jour du cache de schéma - 305
Mise à jour du schéma LDAP - 301
Mise à niveau des CIM - 107, 197, 233
Mise à niveau du firmware - 234
Mise en route - 14, 254
Mise sous/hors tension des prises et alimentation cyclique - 206
Mode proxy et MPC - 323
Mode souris absolue - 79
Mode souris intelligente - 15, 78
Mode souris simple - Connexion à une cible Dominion KX II contrôlée par CC-SG via VKC utilisant Firefox - 323
Mode souris standard - 77
Modèles de châssis de lames pris en charge - 175, 177, 181, 190
Modems certifiés - 152, 289
Modes de souris lors de l'utilisation du profil USB Mac OS X avec DCIM-VUSB - 114
Modes et résolutions vidéo - 317
Modes vidéo SUSE/VESA - 317
Modification des attributs rciusergroup pour les membres utilisateurs - 305
Modification du code de disposition de clavier (cibles Sun) - 40
Modification du mot de passe par défaut - 33, 45
Modification du taux de rafraîchissement maximum - 75
Modification d'un groupe d'utilisateurs existant - 124
Modification d'un mot de passe - 141
Modification d'un profil USB lors de l'utilisation d'un lecteur de cartes à puce - 320
Modification d'un utilisateur existant - 127
Modification et suppression des macros de clavier - 68
Modules d'interface pour ordinateur (CIM) - 107, 279, 352
Mots de passe sécurisés - 141, 209, 212

N

Navigateurs pris en charge - 288
Navigation dans la console Dominion KX II - 45
Navigation de la CLI - 252
Network Settings (Paramètres réseau) - 28, 33, 36, 142, 143, 145
Nouveautés de l'aide - 2

O

Options d'affichage - 87
Options d'aide - 87
Options de clavier - 66
Options de souris - 75
Options d'outils - 84

P

Page d'accès aux ports (affichage de serveur de la console locale) - 264
Page Device Diagnostics (Diagnostics du dispositif) - 246
Page d'interface réseau - 241
Page Favorites List (Liste des favoris) - 52, 53
Page Manage Favorites (Gérer les favoris) - 51
Page Network Statistics (Statistiques réseau) - 241
Page Ping Host (Envoi de commande Ping à l'hôte) - 244
Page Port Access - 45, 46, 172
Page Trace Route to Host (Déterminer l'itinéraire jusqu'à l'hôte) - 245
Papier peint du Bureau - 14
Paramétrage des options clavier/souris CIM - 69
Paramètres Apple Macintosh - 28
Paramètres d'authentification - 128
Paramètres de l'interface LAN - 36, 145, 146
Paramètres de modem - 30, 151
Paramètres de souris - 15
Paramètres de vitesse réseau - 146, 299
Paramètres des ports locaux standard et étendu de KX2-832 et KX2-864 - 200, 204
Paramètres IBM AIX 5.3 - 27
Paramètres Linux (Red Hat 4) - 21
Paramètres Linux (Red Hat 9) - 19
Paramètres réseau de base - 143
Paramètres Sun Solaris - 23
Paramètres SUSE Linux 10.1 - 22
Paramètres Windows 2000 - 17
Paramètres Windows Vista - 18
Paramètres Windows XP, Windows 2003 et Windows 2008 - 15
Photos du produit - 7
Port Action Menu (Menu d'action de ports) - 47, 48, 265
Port local - 347

Port local étendu (modèles KX2-832 et KX2-864 Dominion uniquement) - 349
Ports et profils USB - 318
Ports TCP et UDP utilisés - 297
Ports USB VM-CIM et DL360 - 318
Préférence de la langue du clavier (clients Fedora Linux) - 312
Présentation - 13, 57, 89, 93, 106, 205, 248, 260, 309
Présentation de la fonction Activer la validation du certificat du serveur de téléchargement AKC - 89, 148, 150
Présentation de l'accès direct aux ports - 89, 148, 149
Problèmes de sécurité - 256
Processus d'authentification de l'utilisateur - 139
Profils USB - 62, 106, 197, 330
Profils USB disponibles - 107, 319, 330
Propriétés vidéo - 70
Protocoles pris en charge - 39

Q

Questions générales - 325

R

Raccourcis-clavier et touches de connexion - 266
Redémarrage - 237
Refresh Screen (Actualiser l'écran) - 70
Réglage des paramètres vidéo - 71
Réinitialisation de Dominion KX II à l'aide du bouton de réinitialisation - 274
Réinitialisation des paramètres d'usine de la console locale de Dominion KX II - 273
Relation entre les utilisateurs et les groupes - 116
Remarque aux utilisateurs de CC-SG - 39
Remarque relative à Microsoft Active Directory - 39
Remarques d'informations - 292, 309
Remarques sur la prise en charge d'IPv6 - 310
Rendre les paramètres Linux permanents - 23
Rendre les paramètres UNIX permanents - 27
Renvoi des informations relatives aux groupes d'utilisateurs - 301
Renvoi des informations relatives aux groupes d'utilisateurs à partir d'Active Directory - 133
Renvoi des informations relatives aux groupes d'utilisateurs via RADIUS - 137
Résolution du focus de Fedora Core - 316
Résolutions disponibles - 263
Résolutions vidéo prises en charge - 2, 23, 27, 290, 291, 317
Résolutions vidéo prises en charge non affichées - 317
Retour à l'interface de la console locale de Dominion KX II - 268

S

Saisie automatique des commandes - 253
Se déconnecter - 56
Sécurité - 353
Sécurité et authentification - 261
Security Settings (Paramètres de sécurité) - 209
Sélection des profils pour un port KVM - 114
Sélection des profils USB - 62
Serveurs lames - 342
Services du dispositif - 2, 147, 177, 181
Souris à 3 boutons Windows sur les cibles Linux - 320
Spécification de la détection automatique de l'alimentation - 38
Spécifications - 30, 204, 276
Spécifications des échanges de communication RADIUS - 137
Spécifications physiques - 276
Support virtuel - 6, 92, 322
Support virtuel non rafraîchi après l'ajout de fichiers - 322
Support virtuel universel - 329
Supports virtuels VKC - 80
Synchronisation des pointeurs de souris - 76
Synchronisation des pointeurs de souris (Fedora) - 315
Syntaxe CLI - Conseils et raccourcis - 253
Systèmes d'exploitation et CIM pris en charge (serveurs cible) - 2, 12, 32, 281
Systèmes d'exploitation et navigateurs pris en charge par AKC - 91
Systèmes d'exploitation pris en charge (Clients) - 2, 12, 287

T

Terminologie - 10, 14

U

USB Profile Management (Gestion des profils USB) - 232, 233
User Blocking (Blocage des utilisateurs) - 209, 213

User Management (Gestion des utilisateurs) - 115, 261
Utilisateurs - 125
Utilisateurs simultanés - 260
Utilisation de la console locale de Dominion KX II - 260
Utilisation de la fonction Screenshot from Target (Capture d'écran de la cible) - 74
Utilisation des serveurs cible - 5, 42, 173
Utilisation des supports virtuels - 98
Utilisation du support virtuel via VKC et AKC dans un environnement Windows - 97

V

Vérification de la prise en charge du chiffrement AES par votre navigateur - 215, 216, 218
Version de Virtual KVM Client non reconnue par le mode proxy CC-SG - 322
Virtual KVM Client - 45, 48, 57, 89, 106

W

Windows - 341

Etats-Unis/Canada/Amérique latine

Lundi - Vendredi
8h00 - 20h00, heure de la côte Est des Etats-Unis
Tél. : 800-724-8090 ou 732-764-8886
Pour CommandCenter NOC : appuyez sur 6, puis sur 1.
Pour CommandCenter Secure Gateway : appuyez sur 6, puis sur 2.
Fax : 732-764-8887
E-mail pour CommandCenter NOC : tech-ccnoc@raritan.com
E-mail pour tous les autres produits : tech@raritan.com

Chine

Beijing
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-10-88091890

Shanghai
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-21-5425-2499

Guangzhou
Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +86-20-8755-5561

Inde

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +91-124-410-7881

Japon

Lundi - Vendredi
9h30 - 17h30, heure locale
Tél. : +81-3-3523-5991
E-mail : support.japan@raritan.com

Europe

Europe
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +31-10-2844040
E-mail : tech.europe@raritan.com

Royaume-Uni
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +44-20-7614-77-00

France
Lundi - Vendredi
8h30 - 17h00, CET (UTC/GMT+1)
Tél. : +33-1-47-56-20-39

Allemagne
Lundi - Vendredi
8h30 - 17h30, CET (UTC/GMT+1)
Tél. : +49-20-17-47-98-0
E-mail : rg-support@raritan.com

Melbourne, Australie

Lundi - Vendredi
9h00 - 18h00, heure locale
Tél. : +61-3-9866-6887

Taiwan

Lundi - Vendredi
9h00 - 18h00, UTC/GMT - Heure normale 5 - Heure avancée 4
Tél. : +886-2-8919-1333
E-mail : support.apac@raritan.com