IBM

Integrated Management Module I
Guide d'utilisation

Integrated Management Module I

Guide d'utilisation

Septième Edition (Novembre 2013)

Réf. US : 00FH192

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Tableaux

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Chapitre 1. Introduction

Le module de gestion intégré (Integrated Management Module, IMM) consolide les fonctionnalités de processeur de service, de Super I/O, de contrôleur vidéo et de téléprésence sur une seule puce sur la carte mère du serveur. Le module de gestion intégré remplace le contrôleur de gestion de la carte mère et Remote Supervisor Adapter II sur les serveurs IBM System x.

Avant l'utilisation d'IMM, le contrôleur de gestion de la carte mère (BMC) et le BIOS (Basic Input/Output System) constituaient le matériel et le microprogramme standard de gestion des systèmes. Les serveurs System x utilisaient des processeurs de service BMC pour gérer l'interface entre le logiciel de gestion des systèmes et le matériel de la plateforme. Remote Supervisor Adapter II et Remote Supervisor Adapter II Slimline constituaient des contrôleurs facultatifs pour gestion de serveur hors bande.

Important : Bien que le module IMM soit installé en standard sur certains produits IBM BladeCenter et serveurs lame IBM, le module de gestion évolué BladeCenter représente le module de gestion principal pour les fonctions de gestion des systèmes et multiplexage clavier/vidéo/souris (KVM) pour les serveurs BladeCenter et les serveurs lame. Les contenus relatifs à l'interface Web IMM et à l'interface de ligne de commande ne s'appliquent pas à IBM BladeCenter et aux serveurs Blade. Les utilisateurs qui souhaitent configurer les paramètres du module de gestion intégré sur les serveurs blade doivent utiliser Advanced Settings Utility (ASU) sur le serveur blade pour effectuer ces actions.

Le module IMM offre plusieurs améliorations par rapport aux fonctionnalités combinées du contrôleur de gestion de la carte mère (BMC) et de la carte Remote Supervisor Adapter :

- Choix entre connexion Ethernet dédiée ou partagée. La connexion Ethernet dédiée n'est pas disponible sur les serveurs lame ou sur certains serveurs System x.

  Remarque : Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur votre serveur. Si votre matériel ne dispose pas d'un port réseau dédié, l'option *partagée* est la seule option IMM disponible.
- Une seule adresse IP pour l'interface de gestion de plateforme intelligente (IPMI) et de l'interface de processeur de service. Cette fonctionnalité ne s'applique pas aux serveurs lame.
- Analyse système dynamique (DSA) intégrée.
- Possibilité de mise à jour en local ou à distance d'autres entités sans nécessité de redémarrer le serveur pour lancer le processus de mise à jour.
- Configuration distante à l'aide de l'utilitaire Advanced Settings Utility (ASU). Cette fonctionnalité ne s'applique pas aux serveurs lame.
- Possibilité pour les applications et les outils d'accéder au module IMM via communication intrabande ou hors bande. Seule la connexion IMM intrabande est prise en charge sur les serveurs lame.
- Fonctions d'intervention à distance améliorées. Cette fonctionnalité ne s'applique pas aux serveurs lame.

Le microprogramme de serveur IBM System x® constitue l'implémentation IBM de l'interface UEFI (Unified Extensible Firmware Interface). Il remplace le BIOS sur les serveurs System x et les serveurs lame IBM. Le BIOS était auparavant le code de microprogramme standard contrôlant les opérations de base du matériel, telles que les interactions avec les unités de disquette, les unités de disque dur et le clavier Le microprogramme de serveur IBM System x offre plusieurs fonctions absentes du BIOS, notamment la conformité avec UEFI 2.1, la compatibilité iSCSI, la technologie Active Energy Manager, ainsi qu'une fiabilité accrue et des fonctionnalités de service. L'utilitaire Setup fournit des informations sur le serveur, permet de configurer le serveur, de le personnaliser, et établit l'ordre des périphériques d'amorçage.

Remarques :

- Dans ce document, le microprogramme de serveur IBM System x est fréquemment dénommé microprogramme de serveur, et parfois UEFI.
- Le microprogramme de serveur IBM System x est entièrement compatible avec les systèmes d'exploitation non UEFI.
- Pour plus d'informations sur l'utilisation du programme IBM System x Server Firmware, reportez-vous à la documentation fournie avec votre serveur.

Ce document explique comment utiliser les fonctions du module IMM dans un serveur IBM. Le module IMM opère avec le microprogramme IBM System x Server Firmware pour fournir une capacité de gestion de systèmes pour les serveurs System x et BladeCenter.

Ce document ne contient pas d'explications des erreurs ou des messages. Les erreurs et messages d'IMM sont décrits dans le manuel *Problem Determination and Service Guide* livré avec votre serveur. Pour obtenir la dernière version de ce document ou du livre blanc IBM *Transitioning to UEFI and IMM* sur le portail du support IBM®, procédez comme suit.

Remarque : La première fois que vous accédez au portail du support IBM, vous devez choisir la catégorie du produit, la famille du produit, et les numéros de modèle de votre serveur. La prochaine fois que vous accédez au portail du support IBM, les produits sélectionnés initialement sont préchargés par le site Web et seuls les liens correspondant à vos produits sont affichés. Pour modifier ou ajouter des éléments à votre liste de produits, cliquez sur le lien **Manage my product lists**.

Des modifications sont apportées périodiquement au site Web d'IBM. La procédure de recherche des microprogrammes et de la documentation peut être légèrement différente de celle décrite dans le présent document.

1. Rendez-vous à l'adresse http://www.ibm.com/support/entry/portal.
2. Sous **Choose your products**, sélectionnez **Browse for a product** et développez la catégorie **Hardware**.
3. Selon le type de votre serveur, cliquez sur **Systems** > **System x** ou sur **Systems** > **BladeCenter**, et cochez la case correspondant à votre serveur ou à vos serveurs.
4. Sous **Choose your task**, cliquez sur **Documentation**.
5. Sous **See your results**, cliquez sur **View your page**.
6. Dans la zone Documentation, cliquez sur **More results**.
7. Dans la zone Catégorie, cochez la case **Integrated Management Module (IMM)**. Des liens vers la documentation IMM et UEFI apparaissent.

Si des mises à jour du microprogramme sont disponibles, vous pouvez les télécharger depuis le site Web d'IBM. Le module IMM peut comporter des fonctions non décrites dans la documentation. La documentation elle-même peut faire l'objet de mises à jour afin d'intégrer les informations relatives à ces fonctions ou des informations de dernière minute peuvent également être publiées pour fournir des informations supplémentaires non incluses dans la documentation IMM.

Pour vérifier la disponibilité de mises à jour du microprogramme, procédez comme suit.

Remarque : La première fois que vous accédez au portail du support IBM, vous devez choisir la catégorie du produit, la famille du produit, et les numéros de modèle de votre serveur. La prochaine fois que vous accédez au portail du support IBM, les produits sélectionnés initialement sont préchargés par le site Web et seuls les liens correspondant à vos produits sont affichés. Pour modifier ou ajouter des éléments à votre liste de produits, cliquez sur le lien **Manage my product lists**.

Des modifications sont apportées périodiquement au site Web d'IBM. La procédure de recherche des microprogrammes et de la documentation peut être légèrement différente de celle décrite dans le présent document.

1. Rendez-vous à l'adresse http://www.ibm.com/support/entry/portal.
2. Sous **Choose your products**, sélectionnez **Browse for a product** et développez la catégorie **Hardware**.
3. Selon le type de votre serveur, cliquez sur **Systems** > **System x** ou sur **Systems** > **BladeCenter**, et cochez la case correspondant à votre serveur ou à vos serveurs.
4. Sous **Choose your task**, cliquez sur **Downloads**.
5. Sous **See your results**, cliquez sur **View your page**.
6. Dans la zone Flashes & alerts, cliquez sur le lien de téléchargement approprié ou cliquez sur **More results** pour afficher des liens supplémentaires.

Fonctions du module IMM

Le module IMM dispose des fonctions suivantes :

- Accès à distance et gestion en continu de votre serveur
- Gestion à distance indépendante du statut du serveur géré
- Contrôle à distance du matériel et des systèmes d'exploitation
- Gestion depuis le Web avec des navigateurs Web standard

IMM fournit deux types de fonctionnalités IMM : fonctions IMM Standard et fonctions IMM Premium. Pour plus d'informations sur le type de matériel IMM sur votre serveur, consultez la documentation accompagnant votre serveur.

Fonctions du module IMM Standard

Remarque : Certaines de ces fonctions ne s'appliquent pas aux serveurs lame.

- Accès aux paramètres cruciaux du serveur
- Accès aux données techniques essentielles (VPD)
- Prise en charge de l'analyse prédictive de panne (PFA) avancée
- Notification automatique et alertes
- Surveillance et contrôle permanents de l'état du serveur

- Choix d'une connexion Ethernet dédiée ou partagée (si applicable).

  Remarque : Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur votre serveur.
- Prise en charge de serveur de noms de domaine (DNS)
- Prise en charge du protocole DHCP (Dynamic Host Configuration Protocol)
- Alertes par courrier électronique
- Fonctionnalité d'analyse système dynamique (DSA) intégrée
- Niveaux d'autorisations utilisateur améliorés
- Fonction LAN over USB pour communications intrabande avec le module IMM
- Journaux d'événements horodatés, enregistrés sur le module IMM, et pouvant être attachés à des alertes par courrier électronique
- Interfaces et protocoles aux normes du secteur
- Programmes de surveillance du système d'exploitation
- Configuration à distance via l'utilitaire Advanced Settings Utility (ASU)
- Mise à jour à distance du microprogramme
- Contrôle à distance de l'alimentation
- Accélération graphique à distance et transparente
- Interface utilisateur sécurisée au serveur Web
- Serial over LAN
- Redirection de la console du serveur
- Prise en charge du protocole SNMP (Simple Network Management Protocol)
- Authentification utilisateur via une connexion sécurisée à un serveur LDAP (Lightweight Directory Access Protocol)

Fonctions du module IMM Premium

Remarque : Certaines de ces fonctions ne s'appliquent pas aux serveurs lame.

- Accès aux paramètres cruciaux du serveur
- Accès aux données techniques essentielles (VPD)
- Prise en charge de l'analyse prédictive de panne (PFA) avancée
- Notification automatique et alertes
- Surveillance et contrôle permanents de l'état du serveur
- Choix d'une connexion Ethernet dédiée ou partagée (si applicable).

  Remarque : Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur votre serveur.
- Prise en charge de serveur de noms de domaine (DNS)
- Prise en charge du protocole DHCP (Dynamic Host Configuration Protocol)
- Alertes par courrier électronique
- Fonctionnalité d'analyse système dynamique (DSA) intégrée
- Niveaux d'autorisations utilisateur améliorés
- Fonction LAN over USB pour communications intrabande avec le module IMM
- Journaux d'événements horodatés, enregistrés sur le module IMM, et pouvant être attachés à des alertes par courrier électronique
- Interfaces et protocoles aux normes du secteur
- Programmes de surveillance du système d'exploitation

- Configuration à distance via l'utilitaire Advanced Settings Utility (ASU)
- Mise à jour à distance du microprogramme
- Contrôle à distance de l'alimentation
- Accélération graphique à distance et transparente
- Interface utilisateur sécurisée au serveur Web
- Serial over LAN
- Redirection de la console du serveur
- Prise en charge du protocole SNMP (Simple Network Management Protocol)
- Authentification utilisateur via une connexion sécurisée à un serveur LDAP (Lightweight Directory Access Protocol)
- Intervention à distance, y compris contrôle à distance d'un serveur
- Capture d'écran d'un échec du système d'exploitation et affichage via l'interface Web
- Disque distant, qui permet l'association d'une unité de disquette, d'une unité de CD/DVD, d'une unité USB Flash ou d'une image disque à un serveur

Remarque : Les fonctions suivantes de l'adaptateur Remote Supervisor Adapter II ne sont pas disponibles sur le module IMM :

- Affichage des adresses MAC de serveur
- Entrées multiples de serveur NTP

Mise à niveau depuis IMM Standard vers IMM Premium

Si votre serveur est doté de fonctions IMM Standard, vous pouvez procéder à une mise à niveau vers IMM Premium en faisant l'acquisition et en installant une clé de support virtuel sur la carte mère de votre serveur. Aucun nouveau microprogramme n'est requis.

Pour commander une clé de support virtuel, accédez au site http://www.ibm.com/systems/x/newgeneration.

Remarque : Pour plus d'informations sur l'installation de la clé de support virtuel, consultez la documentation accompagnant votre serveur.

Si vous avez besoin d'aide pour effectuer votre commande, appelez le numéro sans frais figurant sur la page des pièces détachées, ou contactez votre représentant IBM local pour une assistance en direct.

Comparaison du module IMM avec d'autres dispositifs de gestion des systèmes sur les serveurs System x

Le tableau suivant compare les fonctions IMM aux fonctions BMC et Remote Supervisor Adapter II sur les serveurs System x.

Remarque : De même que le contrôleur BMC, IMM utilise la spécification IPMI standard.

Tableau 1. Comparaison des fonctions IMM et des fonctions combinées de BMC et de Remote Supervisor Adapter II sur les serveurs System x

Description	BMC avec Remote Supervisor Adapter II	Module de gestion intégré
Connexions réseau	BMC utilise une connexion réseau partagée avec un serveur et une adresse IP différente de celle de la carte Remote Supervisor Adapter II. Remote Supervisor Adapter II utilise une connexion réseau dédiée à la gestion des systèmes et une adresse IP différente de celle du contrôleur BMC.	IMM assure les mêmes fonctions que le contrôleur BMC et l'adaptateur Remote Supervisor Adapter II via la même connexion réseau. Une seule adresse IP est utilisée pour les deux. Si votre serveur dispose d'un port dédié à la gestion des systèmes, vous pouvez sélectionner une connexion réseau dédiée ou bien partagée. **Remarque :** Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur votre serveur. Si votre matériel ne dispose pas d'un port réseau dédié, l'option *partagée* est la seule option IMM disponible.
Fonctions de mise à jour	Chaque serveur requiert une mise à jour unique pour BMC et Remote Supervisor Adapter II. BIOS et les outils de diagnostic peuvent être mis à jour via une communication intrabande.	Une image du microprogramme IMM peut être utilisée pour tous les serveurs auxquels elle s'applique. Le microprogramme IMM, le microprogramme du serveur System x, et le microprogramme DSA (Dynamic System Analysis) peuvent être mis à jour via une communication intrabande ou hors bande. Le module IMM peut se mettre à jour lui-même, ainsi que les microprogrammes du serveur et de DSA, localement ou à distance, sans nécessiter le redémarrage du serveur pour lancer le processus de mise à jour.

Tableau 1. Comparaison des fonctions IMM et des fonctions combinées de BMC et de Remote Supervisor Adapter II sur les serveurs System x (suite)

Description	BMC avec Remote Supervisor Adapter II	Module de gestion intégré
Fonctions de configuration	Les modifications de configuration à l'aide de l'utilitaire ASU ne sont disponibles que via une communication intrabande. Le système requiert des configurations distinctes pour le contrôleur BMC, l'adaptateur Remote Supervisor Adapter II, et le BIOS.	L'utilitaire ASU peut s'exécuter intrabande ou hors bande et peut configurer à la fois le microprogramme d'IMM et celui du serveur. A l'aide de l'utilitaire ASU, vous pouvez également modifier l'ordre d'amorçage, iSCSI, et les données techniques essentielles (type de machine, numéro de série, UUID et ID de l'actif). Les paramètres de configuration du microprogramme de serveur sont conservés par le module IMM. Par conséquent, vous pouvez les modifier alors que le serveur est hors tension ou alors que le système d'exploitation est en cours d'exécution, et ces modifications entrent en vigueur au démarrage suivant du serveur. Les paramètres de configuration du module IMM peuvent être configurés intrabande ou hors bande via les interfaces utilisateur IMM suivantes : • Interface Web • Interface de ligne de commande • Interface IBM Systems Director • SNMP
Capture d'écran du système d'exploitation	Des captures d'écran sont effectuées par l'adaptateur Remote Supervisor Adapter II en cas d'échecs du système d'exploitation. L'affichage de l'écran Capture requiert une applet Java.	Cette fonction est disponible uniquement avec le produit IMM Premium. Pour plus d'informations sur la mise à niveau de module standard vers IMM Premium, voir «Mise à niveau depuis IMM Standard vers IMM Premium», à la page 5. Les captures d'écran sont affichées directement par le navigateur Web, sans besoin d'applet Java.
Consignation d'erreurs au journal	Le contrôleur BMC fournit un journal des événements système BMC (journal d'événements IPMI). L'adaptateur Remote Supervisor Adapter II fournit un journal au format texte contenant des descriptions des événements signalés par le contrôleur BMC. Ce journal contient également des informations sur les événements détectés par l'adaptateur Remote Supervisor Adapter II lui-même.	Le module IMM dispose de deux journaux d'événements : 1. Le journal des événements système est accessible via l'interface IPMI. 2. Le journal des événements de châssis est accessible via les autres interfaces IMM. Ce journal affiche des messages texte générés d'après les spécifications DTMF (Distributed Management Task Force specifications) DSP0244 et DSP8007. **Remarque :** Pour une explication d'événement ou de message spécifique, reportez-vous au manuel *Problem Determination and Service Guide* fourni avec votre serveur.

Tableau 1. Comparaison des fonctions IMM et des fonctions combinées de BMC et de Remote Supervisor Adapter II sur les serveurs System x (suite)

Description	BMC avec Remote Supervisor Adapter II	Module de gestion intégré
Surveillance	Le contrôleur BMC avec adaptateur Remote Supervisor Adapter II dispose des fonctions de surveillance suivantes : • Surveillance du serveur et du voltage de la batterie, de la température du serveur, des ventilateurs, des alimentations électriques et du statut du processeur et des barrettes DIMM • Contrôle de la vitesse du ventilateur • Prise en charge de l'analyse prédictive de pannes • Contrôle des voyants de diagnostic système (alimentation, disque dur, activité, alertes, signaux de présence) • Redémarrage automatique du serveur • Reprise automatique du BIOS (ABR)	Le module IMM dispose des mêmes capacités de surveillance que le contrôleur BMC et l'adaptateur Remote Supervisor Adapter II. Lorsqu'il est utilisé dans une configuration RAID, le statut étendu d'unité de disque dur, y-compris l'analyse prédictive de panne d'unité de disque, est pris en charge par le module IMM.

Tableau 1. Comparaison des fonctions IMM et des fonctions combinées de BMC et de Remote Supervisor Adapter II sur les serveurs System x (suite)

Description	BMC avec Remote Supervisor Adapter II	Module de gestion intégré
Intervention à distance	Le contrôleur BMC avec adaptateur Remote Supervisor Adapter II dispose des capacités d'intervention à distance suivantes : • Redirection de console graphique sur le réseau local • Disquette et CD-ROM virtuels distants • Redirection haute vitesse de vidéo PCI, clavier et souris • Prise en charge de résolution vidéo jusqu'à 1024 x 768, à 70 Hz • Chiffrement des données	Cette fonction est disponible uniquement avec le produit IMM Premium. Pour plus d'informations sur la mise à niveau de module standard vers IMM Premium, voir «Mise à niveau depuis IMM Standard vers IMM Premium», à la page 5. Outre les fonctions d'intervention à distance de l'adaptateur Remote Supervisor Adapter II, le module IMM dispose également des capacités suivantes. **Remarque :** Le module IMM requiert Java Runtime Environment 1.5 (ou version ultérieure), ou ActiveX si Internet Explorer est utilisé avec Windows. • Prise en charge de résolution vidéo jusqu'à 1280 x 1024, à 75 Hz • Prise en charge de USB 2.0 pour clavier, souris et dispositifs de stockage de masse virtuels • Profondeur de couleur sur 15 bits • Choix de mode souris absolu ou relatif • Prise en charge de clé USB Flash • Contrôle de l'alimentation et de la réinitialisation du serveur depuis la fenêtre de contrôle à distance • Possibilité d'enregistrer dans un fichier la vidéo de la fenêtre de contrôle à distance Le module IMM fournit deux fenêtres distinctes. L'une est destinée à l'interaction vidéo, clavier et souris, l'autre aux supports virtuels. L'interface Web d'IMM comporte un élément de menu permettant un ajustement de la profondeur de couleur afin de réduire la quantité de données transmise en cas de bande passante étroite. L'interface de l'adaptateur Remote Supervisor Adapter II comporte un curseur de bande passante.
Sécurité	Remote Supervisor Adapter II dispose de fonctions de sécurité avancées, notamment la possibilité d'utilisation de SSL (Secure Sockets Layer) et du chiffrement des données.	Le module IMM dispose des mêmes fonctions de sécurité que l'adaptateur Remote Supervisor Adapter II.

Tableau 1. Comparaison des fonctions IMM et des fonctions combinées de BMC et de Remote Supervisor Adapter II sur les serveurs System x (suite)

Description	BMC avec Remote Supervisor Adapter II	Module de gestion intégré
Redirection série	La fonction IPMI Serial over LAN (SOL) est une fonctionnalité standard du contrôleur BMC. L'adaptateur Remote Supervisor Adapter II permet de rediriger les données série du serveur vers une session Telnet ou SSH. **Remarque :** Cette fonction n'est pas disponible sur certains serveurs.	Le port COM1 est utilisé pour SOL sur les serveurs System x. COM1 ne peut être configuré que via l'interface IPMI. Le port COM2 est utilisé pour redirection série via Telnet ou SSH. COM2 est configurable via toutes les interfaces IMM, excepté l'interface IPMI. Le port COM2 est utilisé pour SOL sur les serveurs lame. La configuration des deux ports COM est limitée à 8 bits de données, parité nulle, 1 bit d'arrêt et l'un des débits suivants : 9600, 19200, 38400, 57600, 115200 ou 230400. Sur les serveurs lame, COM2 est un port COM interne sans accès externe. Le partage de port série IPMI n'est pas possible sur les serveurs lame. Sur les serveurs montés en armoire ou tour, le port IMM COM2 est un port COM interne sans accès externe.
SNMP	La prise en charge de SNMP est limitée à SNMPv1.	Le module IMM prend en charge SNMPv1 et SNMPv3.

Utilisation d'IMM avec un module de gestion évolué BladeCenter

Le module de gestion évolué BladeCenter représente l'interface standard de gestion des systèmes sur les serveurs IBM BladeCenter et sur les serveurs lame IBM. Bien que le module IMM soit dorénavant inclus avec certains serveurs IBM BladeCenter et serveurs lame IBM, le module de gestion évolué demeure le module de gestion pour les fonctions de gestion de systèmes et de multiplexage du clavier, de la vidéo et de la souris (KVM) pour les serveurs BladeCenter et lame. Les interfaces réseau externes au module IMM ne sont pas disponibles sur serveur BladeCenter.

Aucun accès réseau externe au module IMM n'est disponible sur les serveurs. Le module de gestion évolué doit être utilisé pour la gestion à distance de serveurs lame. Le module IMM remplace la fonctionnalité assurée par le contrôleur BMC et la carte facultative cKVM (contrôle simultané du clavier, de la vidéo et de la souris) présents sur des produits de serveur lame antérieurs.

Exigences relatives au navigateur Web et au système d'exploitation

L'interface Web d'IMM requiert le plug-in Java™ 1.5 ou ultérieur (pour la fonction d'intervention à distance) et l'un des navigateurs Web suivants :

- Microsoft Internet Explorer version 6.0, 7.0, ou 8.0 avec le Service Pack le plus récent. Versions ultérieures à 8.0 non prises en charge.
- Mozilla Firefox version 1.5, (ou version ultérieure)

Les systèmes d'exploitation de serveur ci-après prennent en charge la connexion USB requise par la fonction d'intervention à distance.

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux, versions 4.0 et 5.0
- SUSE Linux, version 10.0
- Novell NetWare 6.5

Remarque : L'interface Web d'IMM ne prend pas en charge les langues codées sur deux octets (DBCS).

Mentions utilisées dans ce manuel

Les mentions suivantes sont utilisées dans la documentation :

- **Remarque :** Ces mentions contiennent des conseils, des instructions ou des recommandations importants.
- **Important :** Ces consignes de sécurité fournissent des informations ou des conseils qui peuvent vous aider à éviter des problèmes.
- **Avertissement :** Indique la présence d'un risque pouvant occasionner des dommages aux programmes, aux périphériques ou aux données. Ce type de consigne est placé avant l'instruction ou la situation à laquelle elle se rapporte.

Chapitre 2. Ouverture et utilisation de l'interface Web d'IMM

Le module IMM réunit sur une seule puce les fonctions de processeur de maintenance, de contrôleur vidéo et d'intervention à distance (lorsqu'une clé de support virtuel facultative est installée). Pour accéder à distance au module IMM à l'aide de son interface Web, vous devez d'abord vous connecter. Ce chapitre décrit les procédures de connexion et les actions que vous pouvez effectuer à partir de l'interface Web d'IMM.

Accès à l'interface Web d'IMM

IMM prend en charge l'adressage IPv4 statique et DHCP (Dynamic Host Configuration Protocol). L'adresse statique par défaut IPv4 affectée au module IMM est 192.168.70.125. Le module IMM est configuré initialement pour tenter d'obtenir une adresse depuis un serveur DHCP, et s'il n'y parvient pas, utilise alors l'adresse IPv4 statique.

IMM prend également en charge IPv6, mais ne dispose pas d'une adresse IPv6 statique fixe par défaut. Pour l'accès initial au module IMM dans un environnement IPv6, vous pouvez utiliser soit l'adresse IP IPv4 IP, soit l'adresse lien-local IPv6. Le module IMM génère une adresse lien-local IPv6 unique, laquelle est indiquée dans l'interface Web d'IMM sur la page Network Interfaces. L'adresse lien-local IPv6 suit le format présenté dans l'exemple ci-après :

```
fe80::21a:64ff:fee6:4d5
```

Lorsque vous accédez au module IMM, les conditions IPv6 suivantes sont définies par défaut :

- La configuration d'adresse IPv6 automatique est activée.
- La configuration d'adresse IP IPv6 statique est désactivée.
- DHCPv6 est activé.
- L'autoconfiguration sans état est activée.

IMM permet de choisir entre l'utilisation d'une connexion réseau de gestion des systèmes dédiée (si applicable) ou partagée avec le serveur. La connexion par défaut pour les serveurs montés en armoire et en tour utilise le connecteur réseau de gestion des systèmes dédié.

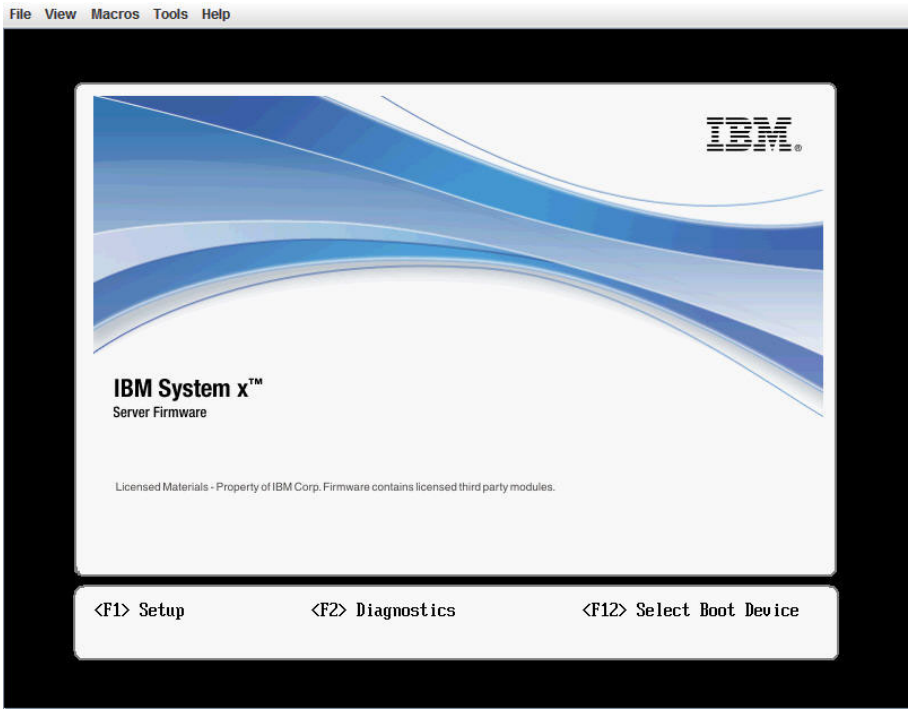
Remarque : Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur votre serveur. Si votre matériel ne dispose pas d'un port réseau dédié, l'option *partagée* est la seule option IMM disponible.

Configuration de la configuration réseau IMM via l'utilitaire IBM System x Server Firmware

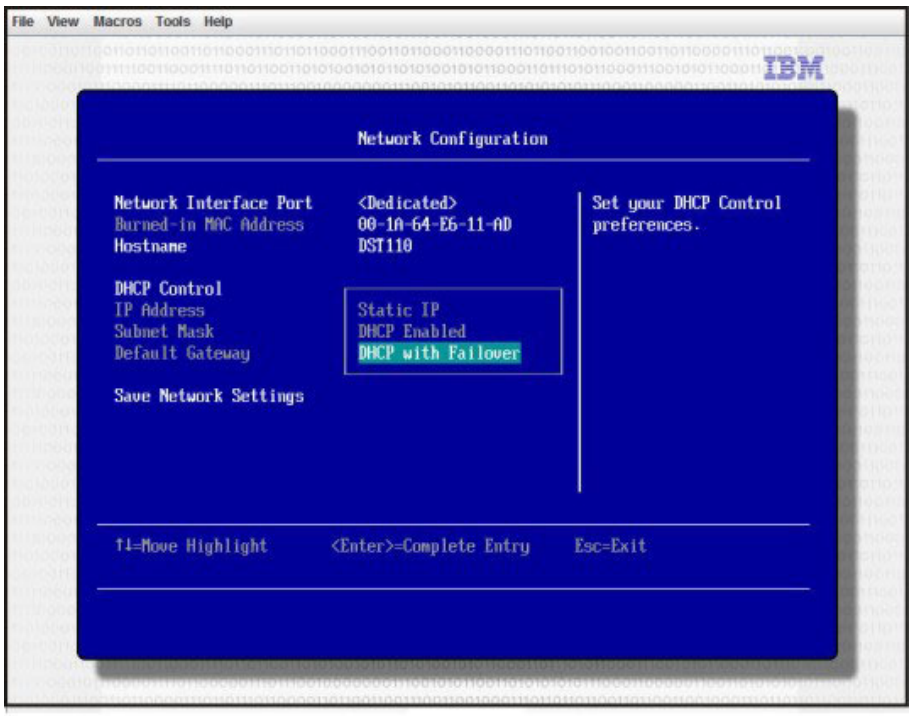
Après avoir démarré le serveur, vous pouvez utiliser l'utilitaire Setup pour sélectionner une connexion réseau IMM. Le serveur hébergeant le matériel IMM doit être connecté à un serveur DHCP (Dynamic Host Configuration Protocol) ou le réseau du serveur doit être configuré afin d'utiliser l'adresse IP statique d'IMM. Pour configurer la connexion réseau IMM via l'utilitaire Setup, procédez comme suit.

1. Mettez le serveur sous tension. L'écran d'accueil d'IBM System x Server Firmware s'affiche.

Remarque : Environ 2 minutes après la connexion du serveur au courant alternatif, le bouton de contrôle de l'alimentation devient actif.



2. A l'invite `<F1> Setup`, appuyez sur la touche F1. Si vous avez défini un mot de passe à la mise sous tension et un mot de passe administrateur, vous devez entrer le mot de passe administrateur pour accéder au menu complet de l'utilitaire de configuration.
3. Dans le menu principal de l'utilitaire de configuration, sélectionnez **System Settings**.
4. Sur l'écran suivant, sélectionnez **Integrated Management Module**.
5. Sur l'écran suivant, sélectionnez **Network Configuration Module**.
6. Mettez en évidence l'entrée **DHCP Control**. Trois options de connexion réseau IMM sont présentées dans la zone **DHCP Control** :
   - Static IP
   - DHCP Enabled
   - DHCP with Failover, laquelle est l'option par défaut



7. Sélectionnez l'une des options de connexion réseau suivantes.
8. Si vous choisissez d'utiliser une adresse IP statique, vous devez spécifier l'adresse IP, le masque de sous-réseau, et la passerelle par défaut.
9. Vous pouvez également utiliser l'utilitaire Setup pour sélectionner une connexion réseau dédiée (si votre serveur dispose d'un port réseau dédié) ou une connexion réseau IMM partagée.

   Remarques :

   - Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur votre serveur. Si votre matériel ne dispose pas d'un port réseau dédié, l'option *shared* est la seule option IMM disponible. Depuis l'écran **Network Configuration**, sélectionnez **Dedicated**, le cas échéant, ou **Shared** dans la zone **Network Interface Port**.
   - Pour identifier l'emplacement des connecteurs Ethernet utilisés par IMM sur votre serveur IMM, reportez-vous à la documentation accompagnant votre serveur.
10. Sélectionnez **Save Network Settings**.
11. Quittez l'utilitaire de configuration.

Remarques :

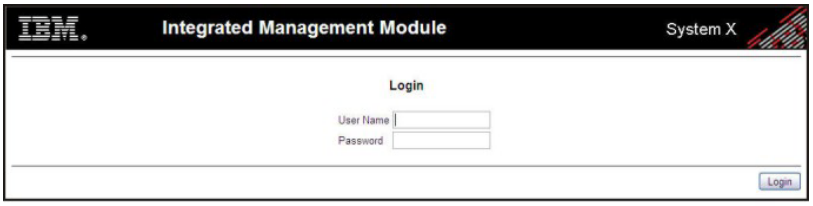
- Vous devez patienter environ 1 minute pour que les modifications prennent effet avant que le microprogramme du serveur ne soit à nouveau fonctionnel.
- Vous pouvez également configurer la connexion réseau IMM via l'interface Web d'IMM. Pour plus d'informations, voir «Configuration des interfaces réseau», à la page 40.

Connexion à IMM

Important : IMM est configuré initialement avec le nom d'utilisateur `USERID` et le mot de passe `PASSW0RD` (le chiffre 0 et non pas la lettre O). Cet utilisateur par défaut dispose d'un accès Superviseur. Modifiez ce mot de passe par défaut lors de votre configuration initiale pour une sécurité accrue.

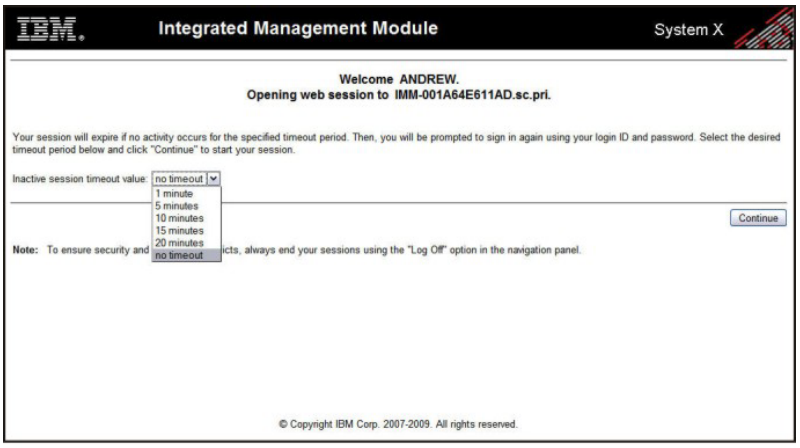
Pour accéder à IMM depuis l'interface Web d'IMM, procédez comme suit.

1. Ouvrez un navigateur Web. Dans la zone d'adresse ou d'URL, entrez l'adresse IP ou le nom d'hôte du serveur IMM auquel vous désirez vous connecter.

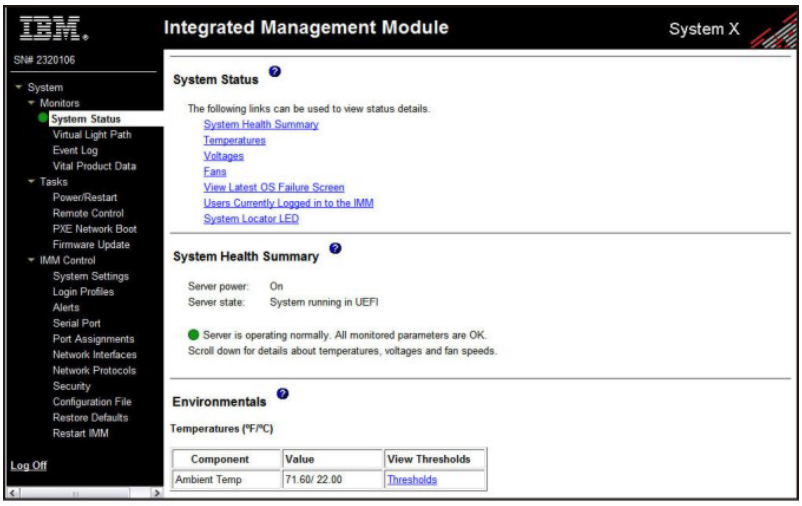


2. Entrez votre nom d'utilisateur et votre mot de passe dans la fenêtre IMM Login. Si vous utilisez IMM pour la première fois, vous pouvez vous procurer votre nom d'utilisateur et votre mot de passe auprès de votre administrateur système. Toutes les tentatives de connexion sont consignées dans le journal des événements. Selon la façon dont votre administrateur a configuré l'ID utilisateur, vous devrez éventuellement entrer un nouveau mot de passe.
3. Sur la page d'accueil, sélectionnez une valeur de délai d'attente dans la liste déroulante dans la zone à cet effet. Si votre navigateur reste inactif durant le nombre de minutes spécifié, IMM vous déconnecte alors de l'interface Web.

   Remarque : Selon la façon dont votre administrateur a configuré les paramètres de connexion globaux, le délai d'attente peut être une valeur fixe.



4. Cliquez sur **Continue** pour démarrer la session. Le navigateur ouvre la page System Status qui offre un aperçu rapide de l'état du serveur et un récapitulatif de son état de fonctionnement.



Pour les descriptions des actions que vous pouvez effectuer à partir des liens dans le panneau de navigation de gauche de l'interface Web d'IMM, voir «Descriptions des actions du module IMM». Consultez ensuite le Chapitre 3, «Configuration du module IMM», à la page 21.

Descriptions des actions du module IMM

Le tableau 2 répertorie les actions disponibles lorsque vous êtes connecté au module IMM.

Tableau 2. Actions du module IMM

Lien	Action	Description
System Status	Affiche l'état de santé système d'un serveur, la capture d'écran d'échec du système d'exploitation et les utilisateurs connectés au module IMM	Vous pouvez surveiller l'état d'alimentation et de santé du serveur, la température, le voltage et le statut des ventilateurs de votre serveur sur la page System Health. Vous pouvez également afficher l'image de la capture d'écran du dernier échec du système d'exploitation et les utilisateurs connectés au module IMM.
Virtual Light Path	Affiche le nom, la couleur et le statut de chaque voyant sur le témoin lumineux du serveur	La page Virtual Light Path affiche le statut actuel des voyants lumineux sur le serveur.
Event log	Affiche les journaux d'événements des serveurs distants	La page Event Log contient des entrées qui sont actuellement stockées dans le journal des événements du châssis. Le journal contient une description texte des événements signalés par le contrôleur BMC, ainsi que des informations sur toutes les tentatives d'accès distant et sur les modifications de configuration. Tous les événements recensés dans le journal sont accompagnés d'un horodatage, lequel utilise les paramètres de date et heure d'IMM. Certains événements génèrent également des alertes s'ils sont configurés en conséquence sur la page Alerts. Vous pouvez trier et filtrer les événements dans le journal des événements.
Vital Product Data	Affiche les données techniques essentielles du produit (VPD)	Le module IMM collecte des informations sur le serveur, sur le microprogramme du serveur et sur les données techniques essentielles de ses composants. Ces données sont disponibles sur la page Vital Product Data.

Tableau 2. Actions du module IMM (suite)

Lien	Action	Description
Power/Restart	Met sous tension ou redémarre un serveur à distance	Le module IMM permet un contrôle à distance complet de l'alimentation de votre serveur avec des actions de mise sous tension, de mise hors tension et de redémarrage. De plus, des statistiques sur l'alimentation et le redémarrage sont collectées et affichées pour indiquer l'état de disponibilité du matériel du serveur.
Remote Control	Permet de rediriger la console vidéo du serveur et d'utiliser une unité de disque ou une image de disque sur votre ordinateur comme une unité sur le serveur	Vous pouvez lancer la fonction de contrôle à distance depuis la page Remote Control. A l'aide de la fonction Remote Control, vous pouvez visualiser la console du serveur depuis votre ordinateur et monter l'une des unités de disque de votre ordinateur, par exemple l'unité CD-ROM ou de disquette, sur le serveur. Vous pouvez utiliser votre souris et clavier pour interagir et contrôler le serveur. Lorsque vous avez monté un disque, vous pouvez l'utiliser pour redémarrer le serveur et pour mettre à jour le microprogramme sur celui-ci. Il apparaît comme une unité de disque USB reliée au serveur.
PXE Network Boot	Permet de modifier la séquence de démarrage (amorçage) du serveur hôte pour le prochain redémarrage afin de tenter un démarrage réseau PXE (Preboot Execution Environment)/DHCP (Dynamic Host Configuration Protocol)	Si le microprogramme du serveur et l'utilitaire d'agent d'amorçage PXE sont correctement configurés, vous pouvez modifier depuis la page PXE Network Boot la séquence de démarrage (amorçage) du serveur hôte pour le prochain redémarrage afin de tenter un démarrage réseau PXE/DHCP. La séquence de démarrage du serveur hôte sera modifiée uniquement si celui-ci n'est pas sous protection PAP (Privileged Access Protection). Après le prochain redémarrage, la case sur la page PXE Network Boot sera décochée.
Firmware Update	Permet de mettre à jour le microprogramme sur le module IMM	Utilisez les options sur la page Firmware Update pour mettre à jour le microprogramme d'IMM, du serveur et de DSA.
System Settings	Permet d'afficher et de modifier les paramètres du serveur IMM	Vous pouvez configurer depuis la page System Settings l'emplacement du serveur et des informations générales, telles que le nom du module IMM, les paramètres de délai d'attente du serveur, et les informations de contact pour le module IMM.
	Configuration de l'horloge IMM	Vous pouvez configurer l'horloge IMM utilisée pour l'horodatage des entrées dans le journal des événements.
	Activation ou désactivation de l'interface USB intrabande	Vous pouvez activer ou désactiver l'interface USB intrabande (ou LAN over USB).
Login Profiles	Permet de configurer les profils de connexion à IMM et les paramètres de connexion globaux	Vous pouvez définir jusqu'à 12 profils de connexion permettant un accès au module IMM. Vous pouvez également définir des paramètres de connexion globaux qui s'appliquent à tous les profils de connexion, y compris l'activation de l'authentification serveur LDAP (Lightweight Directory Access Protocol) et la personnalisation des niveau de sécurité de compte.

Tableau 2. Actions du module IMM (suite)

Lien	Action	Description
Alerts	Configuration à distance d'alertes et de destinataires distants	Vous pouvez configurer le module IMM pour générer et transmettre des alertes pour différents événements. Sur la page Alerts, vous pouvez configurer les alertes à surveiller et les destinataires à notifier.
	Configuration d'événements SNMP (Simple Network Management Protocol)	Vous pouvez définir les catégories d'événements pour lesquels des alertes SNMP sont envoyées.
	Configuration de paramètres d'alerte	Vous pouvez établir des paramètres globaux s'appliquant à tous les destinataires d'alertes distants, comme le nombre de nouvelles tentatives d'alerte et le délai entre les tentatives.
Serial Port	Configuration des paramètres de port série IMM	Dans la page Serial Port, vous pouvez configurer le débit en bauds du port série utilisé par la fonction de redirection série. Vous pouvez également configurer la séquence de touches utilisée pour basculer entre le mode de redirection série et d'interface de ligne de commande (CLI).
Port assignments	Permet de modifier les numéros de port des protocoles IMM	Depuis la page Port Assignments, vous pouvez afficher et modifier les numéros de port affectés aux protocoles IMM (par exemple, HTTP, HTTPS, Telnet et SNMP).
Network Interfaces	Permet de configurer les interfaces réseau du module IMM	Depuis la page Network Interfaces, vous pouvez configurer les paramètres d'accès réseau pour la connexion Ethernet sur le module IMM.
Network Protocols	Permet de configurer les protocoles réseau du module IMM	Vous pouvez configurer depuis la page Network Protocols les paramètres SNMP (Simple Network Management Protocol), DNS (Domain Name System) et SMTP (Simple Mail Transfer Protocol) utilisés par le module IMM. Vous pouvez également configurer les paramètres LDAP.
Security	Permet de configurer la couche SSL (Secure Sockets Layer)	Vous pouvez également activer ou désactiver la connexion SSL et gérer les certificats SSSL utilisés. Vous pouvez aussi spécifier si une connexion SSL doit être utilisée pour la connexion à un serveur LDAP.
	Activation de l'accès SSH (Secure Shell)	Vous pouvez activer l'accès SSH au module IMM.
Configuration File	Permet de sauvegarder et de restaurer la configuration IMM	Vous pouvez sauvegarder, modifier, et restaurer la configuration du module IMM et afficher un résumé de la configuration depuis la page Configuration File.
Restore Default Settings	Permet de restaurer les paramètres IMM par défaut	**Avertissement :** Lorsque vous cliquez sur **Restore Defaults**, toutes les modifications apportées au module IMM sont perdues. Vous pouvez réinitialiser la configuration du module IMM d'après ses paramètres usine par défaut.
Restart IMM	Redémarre le module IMM	Vous pouvez redémarrer le module IMM.
Scalable Partitioning	Permet de configurer le serveur en tant que partition dans un complexe évolutif.	Si le serveur est configuré dans un complexe évolutif, le module IMM vous permet de contrôler le système dans un complexe. En cas de problème d'évolutivité du serveur, le module IMM signalera une erreur.

Tableau 2. Actions du module IMM (suite)

Lien	Action	Description
Service Advisor	Transmet les codes d'événements réparables au support IBM	Lorsque cette option est activée, Service Advisor permet au module IMM de transférer les codes d'événements réparables au support IBM pour dépannage complémentaire. **Remarque :** Consultez la documentation de votre serveur pour déterminer si votre serveur prend en charge cette fonction.
Log off	Déconnecte le module IMM	Vous pouvez clôturer votre connexion au module IMM.

Vous pouvez cliquer sur le lien **View Configuration Summary**, situé à l'angle supérieur droit de la plupart des pages, pour afficher rapidement la configuration du module IMM.

Chapitre 3. Configuration du module IMM

Utilisez les liens sous **IMM Control** dans le panneau de navigation pour configurer le module IMM.

Depuis la page System Settings, vous pouvez :

- Définir les informations du serveur
- Définir les délais d'attente serveur
- Régler la date et l'heure du module IMM
- Activer ou désactiver des commandes sur l'interface USB

Depuis la page Login Profiles, vous pouvez :

- Définir des profils de connexion pour contrôler l'accès au module IMM
- Configurer des paramètres de connexion globaux, comme la période de verrouillage après des tentatives de connexion infructueuses
- Configurer le niveau de sécurité du compte

Depuis la page Alerts, vous pouvez :

- Configurer des destinataires d'alerte distantes
- Définir le nombre de tentatives d'alerte distantes
- Sélectionner le délai entre alertes
- Sélectionner les alertes à envoyer et leur mode d'acheminement

Depuis la page Serial Port, vous pouvez :

- Configurer le débit en bauds du port série 2 (COM2) pour redirection série
- Spécifier la séquence de touches à utiliser pour basculer entre la redirection série et l'interface de ligne de commande (CLI)

Depuis la page Port Assignments, vous pouvez changer les numéros de port des services IMM.

Depuis la page Network Interfaces, vous pouvez configurer la connexion Ethernet pour le module IMM.

Depuis la page Network Protocols, vous pouvez configurer les éléments suivants :

- Configuration SNMP
- Configuration DNS
- Telnet
- Configuration SMTP
- Configuration LDAP
- Protocole SLP

Depuis la page Security, vous pouvez installer et configurer les paramètres SSL (Secure Sockets Layer).

Depuis la page Configuration File, vous pouvez créer une sauvegarde, modifier et restaurer la configuration du module IMM.

Depuis la page Restore Defaults, vous pouvez restaurer la configuration IMM à ses paramètres usine par défaut.

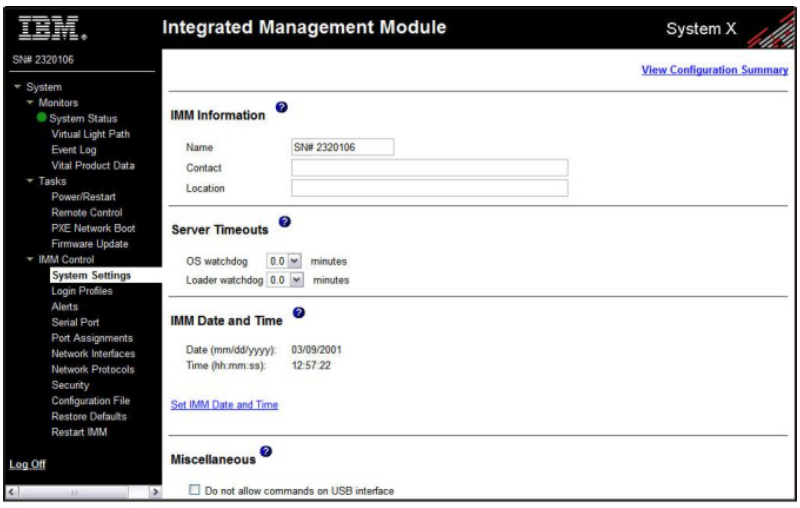
Depuis la page Restart IMM, vous pouvez redémarrer le module IMM.

Définition des informations système

Pour définir les informations système d'IMM, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez définir les informations système. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **System Settings**. Une page comparable à celle présentée dans la figure ci-après s'affiche.

   Remarque : Les zones disponibles sur la page System Settings sont déterminées par le serveur auquel vous accédez.



3. Dans la zone **Name** de la section **IMM Information**, entrez le nom du module IMM. Utilisez la zone **Name** pour spécifier un nom pour le module IMM sur ce serveur. Ce nom est inclus avec les notifications d'notification d'alerte électronique et SNMP pour identifier leur origine.

   Remarque : Le nom de votre module IMM (dans la zone **Name**) et le nom d'hôte IP du module IMM (dans la zone **Hostname** de la page Network Interfaces) ne sont pas forcément identiques vu que la zone **Name** est limitée à 16 caractères. La zone **Hostname**, par contre, peut héberger jusqu'à 63 caractères. Pour limiter la possibilité de confusion, définissez la zone **Name** d'après la partie non qualifiée du nom d'hôte IP. Cette partie est celle précédant le premier point dans le nom d'hôte IP qualifié complet. Par exemple, pour le nom d'hôte IP qualifié complet imm1.us.company.com, le nom d'hôte non qualifié est imm1. Pour plus d'informations sur les noms d'hôte, voir «Configuration des interfaces réseau», à la page 40.
4. Dans la zone **Contact**, entrez les informations de contact. Vous pouvez, par exemple, spécifier le nom et le numéro de téléphone de la personne à contacter en cas de problème avec ce serveur. Vous pouvez entrer un maximum de 47 caractères dans cette zone.

5. Dans la zone **Location**, entrez l'emplacement du serveur. Entrez dans cette zone suffisamment d'informations pour localiser rapidement le serveur pour maintenance ou à d'autres fins. Vous pouvez entrer un maximum de 47 caractères dans cette zone.
6. Faites défiler la page jusqu'en bas et cliquez sur **Save**.

Configuration des délais d'attente du serveur

Remarque : Les délais d'attente du serveur requièrent que l'interface USB intrabande (or LAN over USB) soit activée afin d'autoriser des commandes. Pour plus d'informations sur l'activation et la désactivation des commandes de l'interface USB, voir «Désactivation de l'interface USB intrabande», à la page 26. Pour plus d'informations sur l'installation des pilotes de périphérique requis, voir «Installation de pilotes de périphérique», à la page 134.

Pour définir les valeurs de délai d'attente du serveur, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez configurer les délais d'attente du serveur. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **System Settings** et accédez à la zone **Server Timeouts**.

   Vous pouvez configurer IMM afin de répondre automatiquement aux événements suivants :

   - Blocage du système d'exploitation
   - Echec du chargement du système d'exploitation
3. Activation des délais d'attente du serveur correspondant aux événements pour lesquels vous désirez qu'IMM réponde automatiquement.

   OS watchdog

   Utilisez la zone **OS watchdog** pour spécifier le nombre de minutes entre vérifications du système d'exploitation par IMM. Si le système d'exploitation ne répond pas à l'une de ces vérifications, IMM génère alors une alerte de délai d'attente du système d'exploitation et redémarre le serveur. Une fois que le serveur est redémarré, le programme de surveillance du système d'exploitation est désactivé jusqu'à ce que le système d'exploitation soit fermé et le serveur arrêté, puis redémarré.

   Pour définir une valeur pour le programme de surveillance du système d'exploitation, sélectionnez un intervalle de temps dans le menu. Pour désactiver ce programme de surveillance, sélectionnez **0.0** dans le menu. Pour pouvoir effectuer des captures d'écran des échecs du système d'exploitation, vous devez activer le programme de surveillance dans la zone **OS watchdog**.

   Loader watchdog

   Utilisez la zone **Loader watchdog** pour spécifier le nombre de minutes pendant lequel IMM doit patienter entre l'achèvement des vérifications POST et le lancement du système d'exploitation. Si ce délai est dépassé, IMM génère une alerte de délai d'attente du programme de chargement et redémarre alors automatiquement le serveur. Une fois que le serveur est redémarré, le délai d'attente du chargeur du chargeur est automatiquement désactivé jusqu'à la fermeture du système d'exploitation et l'arrêt et le redémarrage du serveur (ou après le démarrage du système d'exploitation et le chargement du logiciel).

Pour définir la valeur du délai d'attente du chargeur, sélectionnez le délai pendant lequel IMM doit attendre l'achèvement du chargement du système d'exploitation. Pour désactiver ce programme de surveillance, sélectionnez **0.0** dans le menu.

Power off delay

Utilisez la zone **Power off delay** pour spécifier le nombre de minutes pendant lequel IMM doit attendre l'arrêt du système d'exploitation avant de mettre hors tension le serveur (s'il n'a pas été mis hors tension par le système d'exploitation lui-même). En définissant ce délai, vous pouvez vous assurer que le système d'exploitation dispose de suffisamment de temps pour un arrêt ordonné avant que l'alimentation du serveur ne soit coupée. Pour déterminer le délai de mise hors tension pour votre serveur, arrêtez-celui-ci en chronométrant le temps requis jusqu'à son arrêt. Ajoutez une marge de sécurité à cette valeur et utilisez cette durée comme délai de mise hors tension.

Pour définir le délai de mise hors tension, sélectionnez la valeur voulue dans le menu. La valeur X'0' signifie que le système d'exploitation, et non pas IMM, se charge de mettre hors tension le serveur.

4. Accédez au bas de la page et cliquez sur **Save**.

Définition de la date et de l'heure d'IMM

IMM utilise sa propre horloge temps réel pour horodater tous les événements consignés dans le journal des événements.

Remarque : Le paramètre de date et heure IMM affecte uniquement l'horloge d'IMM et non pas celle du serveur. L'horloge temps réel d'IMM et celle du serveur sont des horloges distinctes et indépendantes qui peuvent être réglées différemment. Pour synchroniser l'horloge IMM avec celle du serveur, accédez à la section **Network Time Protocol** de la page et sélectionnez pour le nom d'hôte ou l'adresse IP du serveur NTP le même nom d'hôte ou adresse IP que celui utilisé pour définir l'heure du serveur. Pour plus d'informations, voir «Synchronisation des horloges dans un réseau», à la page 25.

Les alertes envoyées par courrier électronique et par SNMP utilisent le paramètre d'horloge temps réel pour horodater les alertes. Les paramètres d'horloge prennent en charge les décalages par rapport à l'heure GMT (Greenwich Mean Time), ainsi que l'observation de l'heure d'été, pour faciliter la gestion à distance par les administrateurs entre des fuseaux horaires différents. Vous pouvez accéder à distance au journal des événements même si le serveur est hors tension ou désactivé.

Pour vérifier les paramètres de date et d'heure du module IMM, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez configurer les valeurs de date et heure. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **System Settings** et accédez à la section **IMM Date and Time**, laquelle indique la date et heure de génération de la page Web.
3. Pour remplacer les paramètres de date et d'heure et activer l'heure d'été et les décalages avec l'heure de Greenwich (GMT), cliquez sur **Set IMM Date and Time**. Une page comparable à celle présentée dans la figure ci-après s'affiche.

4. Dans la zone **Date**, entrez les chiffres correspondant au mois, au jour et à l'année en cours.
5. Dans la zone **Time**, entrez les chiffres correspondant à l'heure, aux minutes et aux secondes dans les zones d'entrée applicables. L'heure (hh) doit être un nombre compris entre 00 et 23 tel que représenté sur une horloge au format 24 heures. Les minutes (mm) et les secondes (ss) doivent être des chiffres compris entre 00 et 59.
6. Dans la zone **GMT offset**, sélectionnez le chiffre indiquant le décalage, en heures, par rapport à l'heure GMT (Greenwich Mean Time) du fuseau horaire sur lequel le serveur est situé.
7. Sélectionnez ou décochez la case **Automatically adjust for daylight saving changes** pour spécifier si l'horloge IMM doit être automatiquement corrigée lors du passage de l'heure standard à l'heure d'été.
8. Cliquez sur **Save**.

Synchronisation des horloges dans un réseau

Le protocole NTP (Network Time Protocol) permet de synchroniser les horloges à travers un réseau informatique en permettant à un client NTP d'obtenir l'heure correcte auprès d'un serveur NTP.

La fonction NTP d'IMM permet de synchroniser l'horloge temps réel d'IMM avec l'heure indiquée par un serveur NTP. Vous pouvez spécifier le serveur NTP à utiliser, la fréquence de synchronisation du module IMM, activer ou désactiver la fonction NTP et demander une synchronisation immédiate des horloges.

Cette fonction NTP ne permet pas la sécurité et l'authentification étendues assurées par les algorithmes de chiffrement de NTP Version 3 et de NTP Version 4. La fonction NTP d'IMM ne prend en charge que le protocole SNTP (Simple Network Time Protocol) sans authentification.

Pour configurer les paramètres de la fonction NTP d'IMM, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez synchroniser les horloges du réseau. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **System Settings** et accédez à la section **IMM Date and Time**.
3. Cliquez sur **Set IMM Date and Time**. Une page comparable à celle présentée dans la figure ci-après s'affiche.

4. Sous **Network Time Protocol (NTP)**, vous pouvez sélectionner l'un des paramètres suivants :

   NTP auto-synchronization service
   Utilisez cette sélection pour activer ou désactiver la synchronisation automatique de l'horloge IMM avec un serveur NTP.

   NTP server host name or IP address
   Utilisez cette zone pour spécifier le nom du serveur NTP à utiliser pour la synchronisation de l'horloge.

   NTP update frequency
   Utilisez cette zone pour spécifier l'intervalle approximatif (en minutes) entre les demandes de synchronisation. Entrez une valeur comprise entre 3 et 1440 minutes.

   Synchronize Clock Now
   Cliquez sur ce bouton pour demander une synchronisation immédiate au lieu d'attendre l'écoulement du délai spécifié.

5. Cliquez sur **Save**.

Désactivation de l'interface USB intrabande

Important : Si vous désactivez l'interface USB intrabande, vous ne pouvez plus effectuer une mise à jour intrabande du microprogramme IMM, du microprogramme du serveur ou DSA à l'aide des utilitaires de flashage de Linux ou Windows. Si cette interface est désactivée, utilisez l'option Firmware Update de l'interface Web d'IMM pour mettre à jour le microprogramme. Pour plus d'informations, voir «Mise à niveau du microprogramme», à la page 128.

Si vous désactivez l'interface USB intrabande, désactivez également les délais d'attente du programme de surveillance pour éviter des redémarrages intempestifs du serveur. Pour plus d'informations, voir «Configuration des délais d'attente du serveur», à la page 23.

L'interface USB intrabande, ou LAN over USB, est utilisée pour les communications intrabande avec IMM. Pour empêcher une application s'exécutant sur le serveur de demander à IMM de réaliser des tâches, vous devez désactiver l'interface USB intrabande. Pour plus d'informations sur l'interface LAN over USB, voir Chapitre 6, «LAN over USB», à la page 133.

Pour désactiver l'interface USB intrabande, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez désactiver l'interface de pilote de périphérique USB. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **System Settings** et accédez à la section **Miscellaneous**. Une page comparable à celle présentée dans la figure ci-après s'affiche.

3. Pour désactiver l'interface USB intrabande, sélectionnez **Disabled** dans la liste **Allow commands on the USB interface**. La sélection de cette option n'affecte pas les fonctions d'opération à distance USB (par exemple, de la souris, du clavier et de stockage de masse). Si vous désactivez cette interface, il se peut que les applications de gestion intrabande des systèmes, telles que ASU (Advanced Settings Utility) et les utilitaires de package de mise à jour du microprogramme ne fonctionnent plus.

   Remarque : L'utilitaire ASU fonctionne avec une interface USB intrabande désactivée si un pilote de périphérique IPMI est installé.
   Si vous tentez d'utiliser des applications de gestion des systèmes alors que cette interface est désactivée, il se peut que ces applications ne fonctionnent pas.
4. Cliquez sur **Save**.

Pour activer l'interface de pilote de périphérique USB après sa désactivation, décochez la case **Do not allow commands on USB interface** et cliquez sur **Save**.

Remarque :

1. L'interface USB intrabande, également dénommée "LAN over USB", est décrite plus en détail dans le Chapitre 6, «LAN over USB», à la page 133.
2. Lorsque vous tenter d'effectuer une installation réseau de certaines distributions Linux, l'installation peut échouer si l'interface USB intrabande IMM est activée. Pour plus d'informations, voir http://rhn.redhat.com/errata/RHBA-2009-0127.html.
3. Si vous effectuez une installation réseau dépourvue de la mise à jour sur le site Web Red Hat décrite dans la remarque 2 précédente, vous devez désactiver l'interface USB intrabande avant de procéder à l'installation et l'activer au terme de l'installation.
4. Pour plus d'informations sur la configuration de l'interface LAN over USB, voir «Configuration manuelle de l'interface LAN over USB», à la page 134.

Création d'un profil de connexion

Utilisez le tableau Login Profiles pour afficher, configurer ou modifier des profils de connexion spécifiques. Utilisez les liens de la colonne Login ID pour configurer des profils de connexion individuels. Vous pouvez définir jusqu'à 12 profils uniques. Chaque lien dans la colonne Login ID est identifié par l'ID de connexion configuré du profil associé.

Certains profils de connexion sont partagés avec les ID utilisateur IPMI, permettant ainsi d'utiliser un seul jeu de comptes utilisateurs locaux (nom_d'utilisateur/mot de passe) avec toutes les interfaces utilisateur IMM, y-compris IPMI. Les règles régissant ces profils de connexion partagés sont décrites dans la liste ci-après.

- L'ID 1 d'utilisateur IPMI est toujours l'utilisateur Null.
- L'ID 2 d'utilisateur IPMI est mappé à l'ID de connexion 1, l'ID 3 d'utilisateur IPMI est mappé à l'ID de connexion 2, et ainsi de suite.

- L'utilisateur par défaut IMM est défini à `USERID` et `PASSW0RD` (le chiffre zéro et non pas la lettre O) pour l'ID 2 d'utilisateur IPMI et l'ID de connexion 1.

Par exemple, si un utilisateur est ajouté via des commandes IPMI, les informations sur l'utilisateur sont également disponible pour une authentification via les interfaces Web, Telnet, SSH, et autres. Réciproquement, si un utilisateur est ajouté via l'interface Web ou une autre interface, ces informations utilisateur sont disponibles pour le lancement d'une session IPMI.

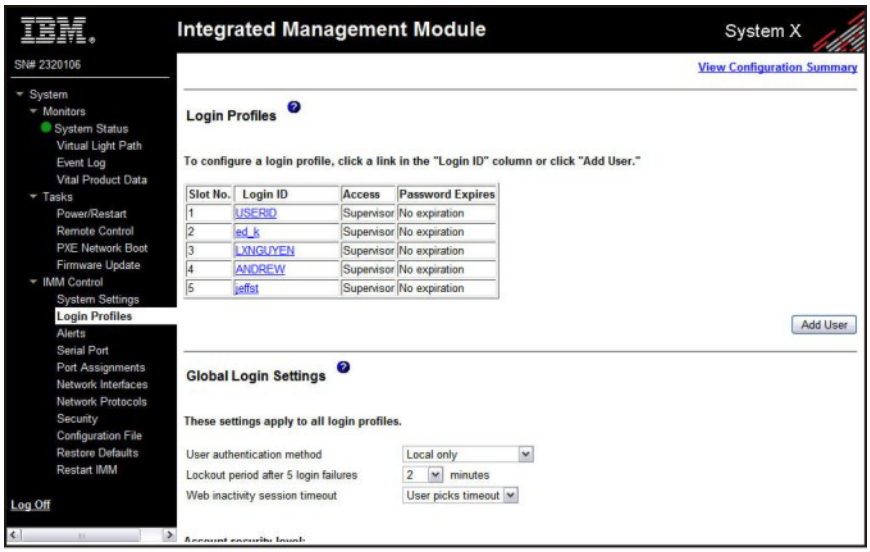
Etant donné que les comptes utilisateur sont partagés avec IPMI, certaines restrictions sont imposées pour établir une base commune entre les différentes interfaces qui utilisent ces comptes. La liste ci-après décrit les restrictions affectant le profils de connexion IMM et IPMI :

- IPMI permet un maximum de 64 ID utilisateur. L'implémentation IPMI d'IMM n'autorise que 12 comptes utilisateur.
- IPMI permet les connexions anonymes (nom d'utilisateur et mot de passe NULL), mais IMM ne l'autorise pas.
- IPMI permet plusieurs ID utilisateur avec le même nom d'utilisateur, mais IMM ne l'autorise pas.
- Les requêtes IPMI visant à modifier le nom actuel de l'utilisateur en lui attribuant à nouveau le même nom renvoient un code d'achèvement `invalid parameter` (paramètre non valide) vu que le nom d'utilisateur demandé est déjà utilisé.
- La longueur maximale du mot de passe IPMI pour IMM est de 16 octets.
- Les termes suivants sont réservés et ne peuvent pas être utilisés comme noms d'utilisateur locaux IMM :
  - immroot
  - nobody
  - ldap
  - lighttpd
  - sshd
  - daemon
  - immftp

Pour configurer un profil de connexion, procédez comme suit.

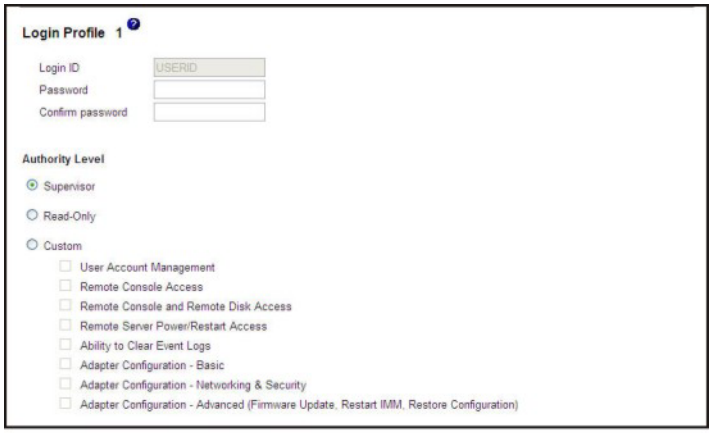
1. Connectez-vous au module IMM sur lequel vous désirez configurer un profil de connexion. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Login Profiles**.

   Remarque : Si vous n'avez pas configuré un profil, il n'apparaît pas dans le tableau Login Profiles.
   La page Login Profiles affiche chaque ID de connexion, son niveau d'accès et les informations d'expiration du mot de passe, comme indiqué dans l'illustration ci-après.



Important : Par défaut, IMM est configuré avec un profil de connexion permettant un accès à distance avec l'ID utilisateur `USERID` et le mot de passe `PASSW0RD` (0 correspond au chiffre zéro et non pas à la lettre O). Pour éviter un risque de sécurité potentiel, modifiez ce profil de connexion par défaut lors de la configuration initiale d'IMM

3. Cliquez sur **Add User**. Une page de profil individuel comparable à celle présentée dans la figure ci-après s'affiche.



4. Dans la zone **Login ID**, entrez le nom du profil. Vous pouvez entrer jusqu'à 16 caractères dans la zone **Login ID**. Caractères valides : lettres en majuscules et minuscules, chiffres, points et traits de soulignement.

   Remarque : Cet ID de connexion est utilisé pour accorder un accès à distance au module IMM.

5. Dans la zone **Password**, affectez un mot de passe à l'ID de connexion. Le mot de passe doit comporter au moins 5 caractères, dont un caractère non alphabétique. Les mots de passe Null ou vides sont acceptés.

   Remarque : Ce mot de passe est utilisé avec l'ID de connexion pour accorder l'accès à distance au module IMM.

6. Dans la zone **Confirm password**, entrez à nouveau le mot de passe.

7. Dans la zone **Authority Level**, sélectionnez l'une des options suivantes pour définir les droits d'accès de cet ID de connexion :

   Supervisor
   Aucune restriction n'affecte l'utilisateur.

   Read Only
   L'utilisateur dispose d'un accès en lecture seule et ne peut pas effectuer des actions telles que de transfert de fichier, d'alimentation ou de redémarrage, ou des fonctions d'intervention à distance.

   Custom
   Si vous sélectionnez cette option, vous devez sélectionner au moins l'un des niveaux d'autorisation personnalisés suivants :

   - **User Account Management :** Un utilisateur peut ajouter, modifier ou supprimer des utilisateurs et modifier les paramètres de connexion locaux sur la page Login Profiles.
   - **Remote Console Access :** Un utilisateur peut accéder à la console distante.
   - **Remote Console and Virtual Media Access :** Un utilisateur peut accéder à la console distante et à la fonction de média virtuel.
   - **Remote Server Power/Restart Access :** Un utilisateur peut accéder aux fonctions de contrôle de l'alimentation et de redémarrage du serveur distant. Ces fonctions sont accessibles sur la page Power/Restart.
   - **Ability to Clear Event Logs :** Un utilisateur peut effacer les journaux d'événements. Tout le monde peut consulter les journaux d'événements mais cette permission spécifique est requise pour pouvoir les effacer.
   - **Adapter Configuration - Basic :** Un utilisateur peut modifier les paramètres de configuration sur les pages System Settings et Alerts.
   - **Adapter Configuration - Networking & Security :** Un utilisateur peut modifier les paramètres de configuration sur les pages Security, Network Protocols, Network Interface, Port Assignments et Serial Port.
   - **Adapter Configuration - Advanced :** Un utilisateur n'est pas soumis à des restrictions lorsqu'il configure le module IMM. De plus, l'utilisateur dispose d'un accès en administration au module IMM, c'est-à-dire qu'il peut exécuter les fonctions avancées suivantes : mises à jour de microprogramme, amorçage réseau PXE, restauration des paramètres usine IMM par défaut, modification et restauration de la configuration IMM depuis un fichier de configuration, redémarrage et réinitialisation du module IMM.

   Lorsqu'un utilisateur définit le niveau d'autorisation d'un ID de connexion IMM, le niveau d'autorisations IPMI de l'ID utilisateur IPMI correspondant est défini conformément aux priorités suivantes :

   - Si l'utilisateur définit le niveau d'autorisation IMM à Supervisor (superviseur), le niveau d'autorisation IPMI est défini à Administrator (administrateur).
   - Si l'utilisateur définit le niveau d'autorisation IMM à Read Only (lecture seule), le niveau d'autorisation IPMI est défini à User (utilisateur).

- Si l'utilisateur définit le niveau d'autorisation IMM d'après l'un des types d'accès suivants, le niveau d'autorisation IPMI est défini à Administrator (administrateur) :
  - User Account Management Access
  - Remote Console Access
  - Remote Console and Remote Disk Access
  - Adapter Configuration - Networking & Security
  - Adapter Configuration - Advanced
- Si l'utilisateur définit le niveau d'autorisation IMM à Remote Server Power/Restart Access ou à Ability to Clear Event Logs, le niveau d'autorisation IPMI est défini à Operator.
- Si l'utilisateur définit le niveau d'autorisation IMM à Adapter Configuration (Basic), le niveau d'autorisation IPMI est défini à User.

Remarque : Pour rétablir les profils de connexion à leurs paramètres usine par défaut, cliquez sur **Clear Login Profiles**.

8. Dans la zone **Configure SNMPv3 User**, cochez la case si l'utilisateur doit avoir accès à IMM via le protocole SNMPv3. Une fois que vous cliquez sur la case à cocher, une zone de la page similaire à celle de la figure ci-après apparaît.

Utilisez les zones suivantes pour configurer les paramètres SNMPv3 du profil utilisateur :

Authentication Protocol
Utilisez cette zone pour spécifier comme protocole d'authentification **HMAC-MD5** ou **HMAC-SHA**. Il s'agit des algorithmes de hachage utilisés par le modèle de sécurité SNMPv3 pour l'authentification. Le mot de passe du compte Linux sera utilisé pour l'authentification. Si vous sélectionnez **None**, aucun protocole d'authentification n'est utilisé.

Privacy Protocol
Le transfert de données entre le client SNMP et l'agent peut être protégé à l'aide de leur chiffrement. Les méthodes prises en charge sont **DES** et **AES**. Le protocole de confidentialité n'est valide que si le protocole d'authentification est défini à HMAC-MD5 ou à HMAC-SHA.

Privacy Password
Utilisez cette zone pour spécifier le mot de passe de chiffrement.

Confirm Privacy Password
Utilisez cette zone pour confirmer le mot de passe de chiffrement.

Access Type
Utilisez cette zone pour spécifier comme type d'accès **Get** ou **Set**. Les utilisateurs SNMPv3 avec type d'accès Get ne peuvent effectuer que des interrogations. Les utilisateurs SNMPv3 avec type d'accès Set peuvent

effectuer des interrogations tout comme modifier des paramètres (par exemple, définir le mot de passe d'un utilisateur).

Hostname/IP address for traps
Utilisez cette zone pour spécifier la destination des alertes pour l'utilisateur. Il peut s'agir d'une adresse IP ou d'un nom d'hôte. En utilisant des alertes, l'agent SNMP avise la station de gestion des événements survenus (par exemple, lorsque la température d'un processeur dépasse la limite prescrite).

9. Cliquez sur **Save** pour enregistrer vos paramètres d'ID de connexion.

Suppression d'un profil de connexion

Pour supprimer un profil de connexion, procédez comme suit.

1. Connectez-vous au module IMM pour lequel vous désirez créer un profil de connexion. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Login Profiles**. La page Login Profiles affiche chaque ID de connexion, le niveau d'accès de la connexion, et les informations d'expiration du mot de passe.
3. Cliquez sur le profil de connexion que vous désires supprimer. La page Login Profile de cet utilisateur s'affiche.
4. Cliquez sur **Clear Login Profile**.

Configuration des paramètres de connexion globaux

Procédez comme suit pour définir les conditions qui s'appliquent à tous les profils de connexion pour le module IMM :

1. Connectez-vous au module IMM pour lequel vous désirez définir les paramètres de connexion globaux. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Login Profiles**.
3. Accédez à la zone **Global Login Settings**. Une page comparable à celle présentée dans la figure ci-après s'affiche.

4. Dans la zone **User authentication method**, spécifiez comment authentifier les utilisateurs qui tentent de se connecter. Sélectionnez l'une des méthodes d'authentification suivantes :
   - **Local uniquement:** les utilisateurs sont authentifiés par une recherche d'une table locale au module IMM. Si l'ID et le mot de passe de l'utilisateur ne

correspondent pas, l'accès est refusé. Les utilisateurs dont l'authentification aboutit se voient affecter le niveau d'autorisation configuré dans «Création d'un profil de connexion», à la page 27.

- **LDAP only:** IMM tente d'authentifier l'utilisateur par le biais du serveur LDAP. Les tables d'utilisateur locales sur le module IMM ne sont jamais explorées si vous utilisez cette méthode d'authentification.
- **Local first, then LDAP:** L'authentification locale est tentée en premier. Si l'authentification locale échoue, l'authentification LDAP est tentée.
- **LDAP first, then Local:** L'authentification LDAP est tentée en premier. Si l'authentification LDAP échoue, l'authentification locale est tentée.

Remarque :

a. Seuls les comptes administrés au niveau local sont partagés avec l'interface IPMI vu qu'IPMI ne prend pas en charge l'authentification LDAP.
b. Même si la zone **User authentication method** est définie à **LDAP only**, les utilisateurs peuvent se connecter à l'interface IPMI à l'aide des comptes administrés au niveau local.

5. Dans la zone **Lockout period after 5 login failures**, spécifiez la durée, en minutes, pendant lequel IMM interdit les tentatives de connexion à distance si plus de cinq tentatives de connexion à distance infructueuses sont détectées. Le blocage d'un utilisateur n'empêche pas les autres utilisateurs de se connecter.
6. Dans la zone **Web inactivity session timeout**, spécifiez le délai, en minutes, avant qu'IMM ne déconnecte une session Web inactive. Sélectionnez **No timeout** pour désactiver cette fonction. Sélectionnez **User picks timeout** si l'utilisateur sélectionnera lui-même le délai d'expiration lors du processus de connexion.
7. (Facultatif) Dans la zone **Account security level**, sélectionnez le niveau de sécurité du mot de passe. Les paramètres **Legacy security settings** et **High security settings** appliquent les valeurs par défaut telles qu'indiquées dans la liste des exigences.
8. Pour personnaliser les paramètres de sécurité, sélectionnez **Custom security settings** pour afficher et modifier la configuration de gestion de la sécurité du compte.

   User login password required
   Utilisez cette zone pour indiquer si un ID utilisateur sans mot de passe est autorisé.

   Number of previous passwords that cannot be used
   Utilisez cette zone pour indiquer le nombre de mots de passe antérieurs qui ne peuvent pas être réutilisés. Vous pouvez comparer jusqu'à cinq mots de passe antérieurs. Sélectionnez **0** pour permettre la réutilisation de tous les mots de passe antérieurs.

   Maximum Password Age
   Utilisez cette zone pour indiquer l'âge maximal de mot de passe autorisé avant qu'il ne doive être changé. Les valeurs 0 à 365 sont prises en charge. Sélectionnez **0** pour désactiver la vérification de l'expiration du mot de passe.
9. Cliquez sur **Save**.

Configuration des paramètres d'alertes distantes

Vous pouvez configurer depuis le lien **Alerts** sur le panneau de navigation les destinataires d'alertes à distance, le nombre de tentatives d'alerte, les incidents qui déclenchent des alertes distantes et des alertes locales.

Après avoir configuré un destinataire d'alerte à distance, IMM envoie à ce destinataire une alerte via une connexion réseau lorsque survient un événement sélectionné dans le groupe Monitored Alerts. L'alerte contient des informations sur la nature de l'événement, sa date et heure, et le nom du système qui a généré l'alerte.

Remarque : Si les zones **SNMP Agent** ou **SNMP Traps** n'ont pas été définies à **Enabled**, aucune alerte SNMP n'est envoyée. Pour plus d'informations sur ces zones, voir «Configuration SNMP», à la page 46.

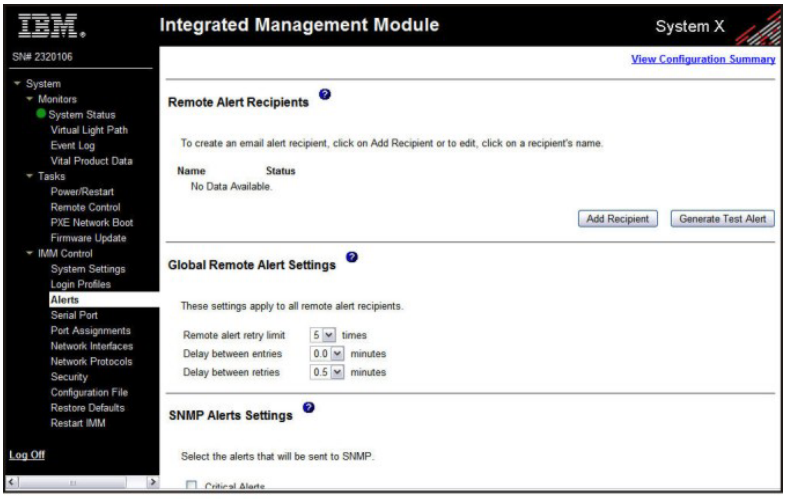
Configuration de destinataires d'alerte distante

Vous pouvez définir jusqu'à 12 destinataires d'alerte distante uniques. Chaque lien vers un destinataire d'alerte indique le nom du destinataire et le statut de l'alerte.

Remarque : Si vous n'avez pas configuré un profil de destinataire d'alerte, le profil n'apparaît pas dans la liste des destinataires d'alerte distante.

Pour configurer un destinataire d'alerte distante, procédez comme suit.

1. Connectez-vous au module IMM pour lequel vous désirez configurer des paramètres d'alerte distante. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Alerts**. La page Remote Alert Recipients s'affiche. Elle mentionne la méthode de notification et le statut d'alerte pour chaque destinataire, s'ils ont été configurés.



3. Cliquez sur l'un des liens de destinataires d'alerte distante ou sur **Add Recipient**. Une fenêtre de destinataire individuel similaire à celle de cette illustration s'ouvre.

4. Dans la zone **Status**, cliquez sur **Enabled** pour activer le destinataire d'alerte distante.
5. Dans la zone **Name**, entrez le nom du destinataire ou un autre identifiant. Le nom saisi figurera en tant que lien vers le destinataire sur la page Alerts.
6. Dans la zone **E-mail address**, entrez l'adresse électronique du destinataire de l'alerte.
7. Utiliser la case à cocher pour inclure les journaux d'événements avec des alertes par courrier électronique.
8. Dans la zone **Monitored Alerts**, sélectionnez le type d'alerte à envoyer au destinataire des alertes. Les alertes distantes sont classées d'après les niveaux de gravité suivants :

   Critical alerts
   Alertes critiques générées pour les événements signalant qu'un composant du serveur ne fonctionne plus.

   Warning alerts
   Les alertes de niveau avertissement sont générées pour les événements qui peuvent progresser vers un niveau critique.

   System alerts
   Les alertes système sont générées pour des événements survenant à la suite d'erreurs système ou de modifications de la configuration.

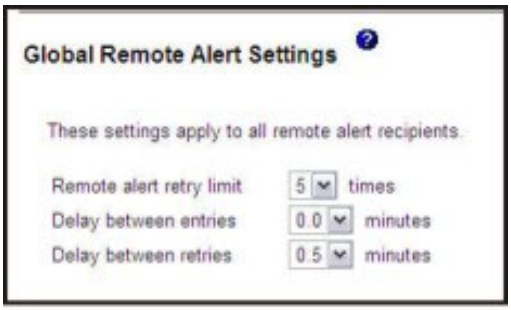
   Toutes les alertes sont consignées dans le journal des événements et envoyées aux destinataires d'alertes distantes configurés.
9. Cliquez sur **Save**.

Configuration des paramètres globaux d'alerte distante

Les paramètres globaux d'alerte distante s'appliquent uniquement aux alertes transmises.

Procédez comme suit pour définir le nombre de tentatives d'envoi d'une alerte par IMM :

1. Connectez-vous au module IMM sur lequel vous désirez définir les tentatives d'alerte distante. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Alerts** et accédez à la section **Global Remote Alert Settings**.



Utilisez ces paramètres pour définir le nombre de tentatives d'alerte distante et le délai entre les tentatives. Les paramètres s'appliquent à tous les destinataires d'alerte distante configurés.

Remote alert retry limit
Utilisez la zone **Remote alert retry limit** pour spécifier le nombre de tentatives supplémentaires d'envoi d'une alerte à un destinataire par IMM. IMM n'envoie pas plusieurs alertes ; les tentatives supplémentaires n'ont lieu qu'en cas d'échec lorsque IMM tente d'envoyer l'alerte initiale.

Remarque : Ce paramètre d'alerte ne s'applique pas aux alertes SNMP.

Delay between entries
Utilisez la zone **Delay between entries** pour spécifier l'intervalle (en minutes) pendant lequel IMM patiente avant d'envoyer une alerte au destinataire suivant dans la liste.

Delay between retries
Utilisez la zone **Delay between retries** pour spécifier l'intervalle (en minutes) pendant lequel IMM patiente avant d'effectuer une nouvelle tentative d'envoi d'une alerte à un destinataire.

3. Faites défiler la page jusqu'en bas et cliquez sur **Save**.

Configuration des paramètres d'alerte SNMP

L'agent SNMP avise le module IMM des événements via des alertes SNMP. Vous pouvez configurer le protocole SNMP pour filtrer les événements en fonction du type d'événement. Les catégories d'événement disponibles pour le filtrage sont Critical, Warning and System (critique, avertissement et système). Les paramètres d'alerte SNMP sont globaux à toutes les alertes SNMP.

Remarque :

1. IMM fournit deux fichiers MIB (Management Information Base) pour leur utilisation avec des applications SNMP. Les fichiers MIB sont inclus dans les packages de mise à jour du microprogramme IMM.
2. IMM prend en charge les normes SNMPv1 et SNMPv3.

Procédez comme suit pour sélectionner le type ou les types d'alertes envoyées à SNMP :

1. Connectez-vous au module IMM sur lequel vous désirez définir les tentatives d'alerte distante. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Alerts** et accédez à la section **SNMP Alerts Alert Settings**.

3. Sélectionnez le type ou les types d'alerte. Les alertes distantes sont classées d'après les niveaux de gravité suivants :
   - Critical (Critique)
   - Warning (Avertissement)
   - System (Système)
4. Faites défiler la page jusqu'en bas et cliquez sur **Save**.

Configuration des paramètres de port série

IMM comporte deux ports série qui sont utilisés pour la redirection série.

Le port série 1 (COM1) sur les serveurs System x est utilisé pour SOL (Serial over LAN) IPMI. COM1 est configurable uniquement via l'interface IPMI.

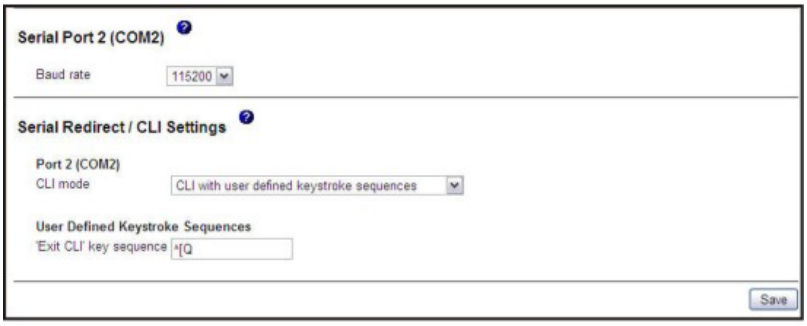
Sur les serveurs lame, le port série 2 (COM2) est utilisé pour SOL. Sur les serveurs System x, COM2 est utilisé pour la redirection série via Telnet ou SSH. COM2 n'est pas configurable via l'interface IPMI. Sur les serveurs montés en armoire ou tour, COM2 est un port COM interne sans accès externe.

Les deux ports série utilisent 8 bits de données, une parité nulle et 1 bit d'arrêt. Vous pouvez choisir l'un des débits en bauds suivants : 9600, 19200, 38400, 57600, 115200 et 230400.

Vous pouvez configurer la redirection série et l'interface de ligne de commande pour le port COM2 dans le module IMM.

Pour configurer le débit de transfert de données et la redirection série, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez configurer le port série. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Serial Port**. Une page semblable à celle de la figure suivante s'affiche.



3. Dans la zone **Baud rate**, sélectionnez le débit de transfert de données correspondant au débit du port COM du serveur que vous désirez utiliser pour la redirection série. Utilisez la zone **Baud rate** pour spécifier le débit de transfert de données de votre connexion de port série. Pour définir le débit en bauds, sélectionnez le débit de transfert des données, en bits par seconde, correspondant à votre connexion de port série.
4. Dans la zone **CLI mode** de la section **Serial Redirect/CLI Settings**, sélectionnez **CLI with EMS compatible keystroke sequences** si vous désirez utiliser la séquence de touches compatible Microsoft Windows Server 2003 Emergency

Management Services (EMS) pour quitter l'opération de redirection série ou sélectionnez **CLI with user defined keystroke sequences** si vous désirez utiliser votre propre séquence de touches.

Remarque : Si vous sélectionnez **CLI with user defined keystroke sequences**, vous devez définir la séquence de touches.

Après la lancement de la redirection série, celle-ci se poursuit tant que l'utilisateur n'a pas saisi la séquence de touches de sortie. Lorsque la séquence de touches de sortie est saisie, la redirection série s'arrête et l'utilisateur est ramené au mode de commande dans la session Telnet ou SSH. Utilisez cette zone pour spécifier la séquence de touches de sortie.

5. Cliquez sur **Save**.

Configuration de la redirection série à Telnet ou SSH

La redirection série à Telnet ou à SSH permet à un administrateur d'utiliser le module IMM comme un serveur de terminal série. Un port série serveur peut être joint depuis une connexion Telnet ou SSH lorsque la redirection série est activée.

Remarques :

1. IMM permet d'avoir au maximum deux sessions Telnet ouvertes. Les sessions Telnet peuvent accéder indépendamment aux ports série de sorte que plusieurs utilisateurs peuvent avoir une vue simultanée d'un port série redirigé.
2. La commande d'interface de ligne de commande **console 1** permet de lancer une session de redirection série avec le port COM .

Exemple de session

```
telnet 192.168.70.125 (Appuyez sur la touche Entrée)
Connecting to 192.168.70.125...
username: USERID (Appuyez sur la touche Entrée)
password: ******** (Appuyez sur la touche Entrée)
system> console 1 (Appuyez sur la touche Entrée)
```

Tout le trafic en provenance de COM2 est dorénavant acheminé à la session Telnet. Tout le trafic en provenance de la session Telnet ou SSH est acheminé à COM2.

```
ESC Q
```

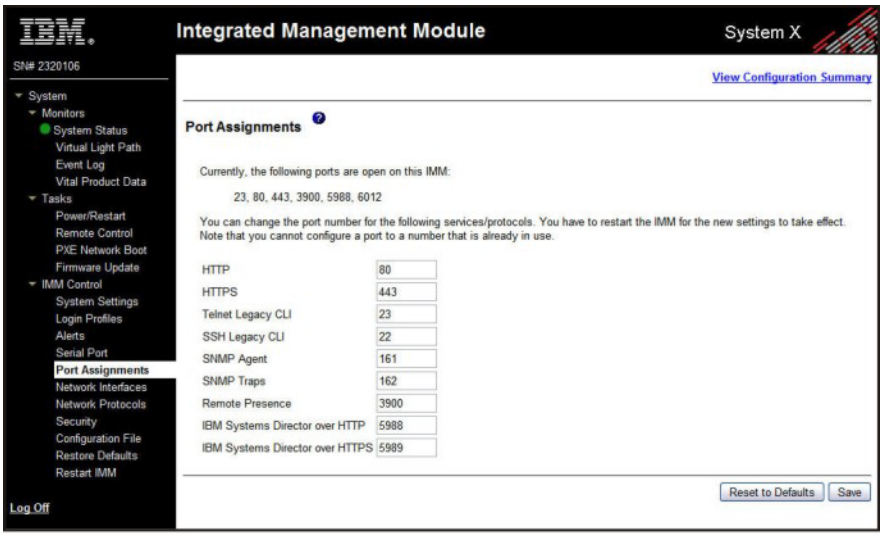
Entrez la séquence de touches de sortie pour revenir à l'interface de ligne de commande. Dans cet exemple, appuyez sur la touche Echap, puis entrez `Q` .

```
Back to LegacyCLI console....
```

Configuration des affectations de ports

Pour changer les numéros de port des services IMM, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez configurer les affectations de ports. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Port Assignments**. Une page comparable à celle présentée dans la figure ci-après s'affiche.



3. Utilisez les informations suivantes pour affecter des valeurs aux zones :

   HTTP Il s'agit du numéro de port pour le serveur HTTP du module IMM. Numéro de port par défaut : 80. Les valeurs valides sont situées sur la plage 1 à 65535. Si vous changez ce numéro de port, vous devez ajouter ce numéro de port, précédé par un signe deux-points, à la fin de l'adresse Web. Par exemple, si le port HTTP est à présent le port 8500, entrez `http://hostname:8500/` pour ouvrir l'interface Web d'IMM. Notez que vous devez saisir le préfixe `http://` avant l'adresse IP et le numéro de port.

   HTTPS
   Il s'agit du numéro de port utilisé pour le trafic HTTPS (SSL) de l'interface Web. Valeur par défaut : 443. Les valeurs valides sont situées sur la plage 1 à 65535.

   Telnet Legacy CLI
   Il s'agit du numéro de port sur lequel l'interface CLI antérieure se connecte au service Telnet. Valeur par défaut : 23. Les valeurs valides sont situées sur la plage 1 à 65535.

   SSH Legacy CLI
   Il s'agit du numéro de port sur lequel l'interface CLI antérieure se connecte via SSH. Valeur par défaut : 22.

   SNMP Agent
   Il s'agit du numéro de port pour l'agent SNMP qui s'exécute sur le module IMM. Valeur par défaut : 161. Les valeurs valides sont situées sur la plage 1 à 65535.

   SNMP Traps
   Il s'agit du numéro de port qui est utilisé pour les alertes SNMP. Valeur par défaut : 162. Les valeurs valides sont situées sur la plage 1 à 65535.

   Remote Presence
   Il s'agit du numéro de port que la fonction de contrôle à distance utilise pour afficher et interagir avec la console du serveur. La valeur par défaut est 3900 pour les serveurs montés en armoire et en tour.

Remarque : La fonction cKVM (Concurrent Keyboard, Video, and Mouse) sur BladeCenter requiert d'utiliser le numéro de port 2068. Ne modifiez pas ce numéro de port sur un serveur lame.

IBM Systems Director over HTTP
Il s'agit du numéro de port utilisé par IBM Systems Director pour interagir avec la console du serveur. Valeur par défaut : 5988.

IBM Systems Director over HTTPS
Il s'agit du numéro de port utilisé par IBM Systems Director pour interagir avec la console du serveur via SSL. Valeur par défaut : 5989.

Les numéros de ports suivants sont réservés et ne peuvent être utilisées que pour les services correspondants.

Tableau 3. Numéros de ports réservés

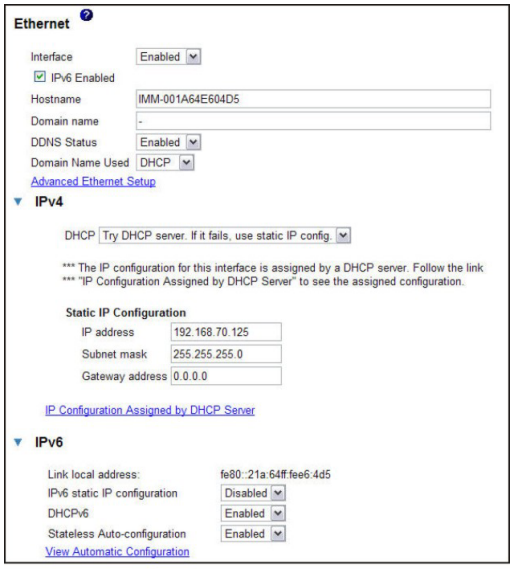
Numéro de port	Services qui l'utilisent
427	SLP
7070 à 7077	Gestion de partition

4. Cliquez sur **Save**.

Configuration des interfaces réseau

Sur la page Network Interfaces, vous pouvez définir l'accès au module IMM en configurant une connexion Ethernet au module. Pour configurer les paramètres Ethernet pour le module IMM, modifiez les paramètres dans les zones Ethernet, IPv4 ou IPv6 sur la page Network Interfaces comme il convient. Les paramètres de chaque zone sont décrits dans les sections ci-après.

Remarque : Les valeurs présentées dans cette image ne sont que des exemples. Vos propres paramètres seront différents.



Pour afficher un récapitulatif de tous les paramètres de configuration actuels, cliquez dans la page Network Interfaces sur **View Configuration Summary**. Avant de configurer les paramètres sur la page Network Interfaces, consultez les informations des sections ci-après.

Remarque : Vous pouvez également configurer la connexion réseau IMM via l'utilitaire Setup. Pour plus d'informations, voir «Configuration de la configuration réseau IMM via l'utilitaire IBM System x Server Firmware», à la page 13.

Configuration des paramètres Ethernet

Les paramètres suivants peuvent être modifiés dans la zone Ethernet de la page Network Interfaces.

Interface
Utilisez cette zone pour activer ou désactiver cette interface réseau. Pour autoriser les connexions réseau via cette interface réseau, sélectionnez **Enabled**.

IPv6 Enabled
Utilisez cette case à cocher pour activer ou désactiver la prise en charge d'IPv6 sur le module IMM.

Remarque : Si vous décochez la case **IPv6 Enabled**, la case **Hide all IPv6 configuration fields when IPv6 is disabled** est affichée. Si la nouvelle case à cocher est sélectionnée, la zone IPv6 est masquée sur la page Network Interfaces de l'interface Web.

Hostname
Utilisez cette zone pour définir un nom d'hôte unique pour le sous-système IMM. Vous pouvez entrer un maximum de 63 caractères dans cette zone. Le nom d'hôte ne peut être composé que de caractères alphanumériques, de tirets et de traits de soulignement.

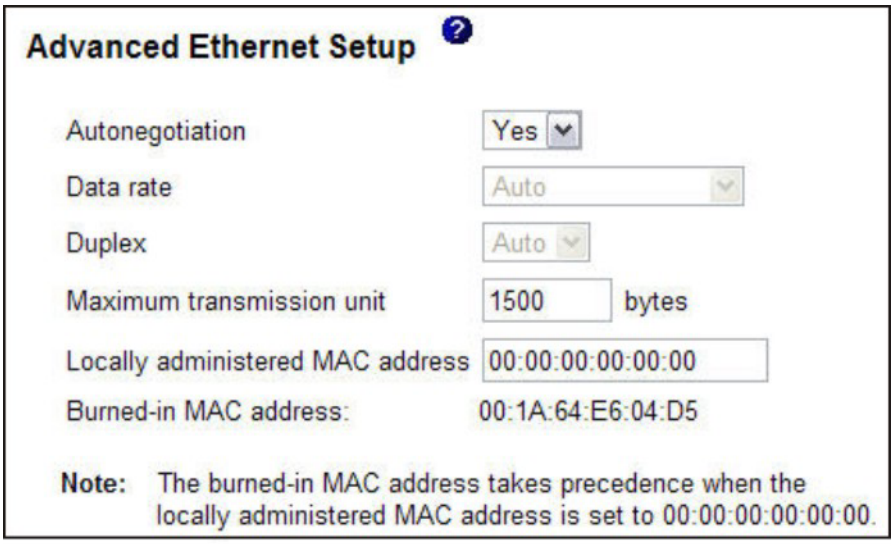
Remarque : Le nom d'hôte par défaut est `IMM-`, suivi par l'adresse MAC gravée.

Domain name
Utilisez cette zone pour définir un nom de domaine DNS.

DDNS Status
Utilisez cette zone pour activer ou désactiver la configuration DNS dynamique (DDNS). DDNS permet à IMM d'indiquer à un serveur DNS de modifier, en temps réel, la configuration DNS active de ses noms d'hôte configurés, des adresses ou d'autres informations stockées sur le DNS. Lorsque DDNS est activé, IMM notifie le serveur DNS de l'adresse IP reçue soit depuis un serveur DHCP, soit via la configuration automatique.

Domain Name Used
Utilisez cette zone pour indiquer si le nom de domaine DHCP ou affecté manuellement doit être envoyé au DNS lorsque DDNS est activé. La valeur sera définie sur DHCP ou sur Manual.

Advanced Interface Setup
Cliquez sur ce lien pour ouvrir la page Advanced Interface Setup, laquelle ressemble à l'image ci-après.



Depuis cette page, vous pouvez visualiser et modifier des paramètres supplémentaires pour l'interface. Le tableau suivant décrit les paramètres affichés sur la page Advanced Ethernet Setup.

Tableau 4. Paramètres de la page Advanced Ethernet Setup

Paramètre	Fonction
Autonegotiate	Utilisez ce paramètre pour spécifier si les paramètres de débit de données et de réseau duplex sont configurables ou non. Si Autonegotiate est défini à **Yes**, les paramètres Data rate et Duplex sont définis à **Auto** et ne sont pas configurables. Si Autonegotiate est défini à **No**, l'utilisateur peut configurer les paramètres Data rate et Duplex.
Data rate	Utilisez cette zone pour spécifier le volume de données à transférer par seconde à travers votre connexion de réseau local. Pour définir le débit réseau, sélectionnez le débit de transfert de données en mégaoctets (Mo) correspondant à votre capacité réseau. Pour détecter automatiquement la vitesse de transfert de données, sélectionnez **Auto**.
Duplex	Utilisez cette zone pour spécifier le type de canal de communication utilisé sur votre réseau. Pour définir le mode duplex, sélectionnez **Full** ou **Half**. Le duplex intégral permet de transférer simultanément des données dans les deux directions. Un canal semi-duplex permet de transférer des données dans une direction ou dans l'autre, mais pas les deux en même temps. Pour détecter automatiquement le mode duplex, sélectionnez **Auto**.

Tableau 4. Paramètres de la page Advanced Ethernet Setup (suite)

Paramètre	Fonction
Maximum transmission unit (MTU)	Utilisez cette zone pour définir la taille maximale d'un paquet (en octets) pour l'interface réseau. Pour définir la valeur MTU, entrez le nombre souhaité dans la zone de texte. Pour Ethernet, la plage MTU valide est 68 à 1500.
Locally administered MAC address	Cette zone permet de spécifier une adresse physique pour ce sous-système IMM. Si une valeur est spécifiée, l'adresse administrée localement remplace l'adresse MAC gravée. L'adresse administrée localement doit être une valeur hexadécimale comprise entre 000000000000 et FFFFFFFFFFFF. Cette valeur doit se conformer au format *XX:XX:XX:XX:XX:XX*, où *X* est un nombre compris entre 0 et 9 et A à F. Le module IMM n'admet pas l'utilisation d'une adresse de multidiffusion. Dans une adresse de multidiffusion, le bit le moins significatif du premier octet est défini à 1. Par conséquent, le premier octet doit être un nombre pair.
Burned-in MAC address	L'adresse MAC gravée est une adresse physique unique attribuée au module IMM par le fabricant.

Configuration des paramètres IPv4

Les paramètres suivants peuvent être modifiés dans la zone IPv4 de la page Network Interfaces.

DHCP Utilisez cette zone pour spécifier si les paramètres TCP/IP du port Ethernet du sous-système IMM doivent être configurés via un serveur DHCP (Dynamic Host Configuration Protocol) sur votre réseau. Pour utiliser la configuration DHCP, sélectionnez **Enabled - Obtain IP config. from DHCP server**. Pour configurer manuellement vos paramètres TCP/IP, sélectionnez **Disabled - Use static IP configuration**. Si vous désirez tenter d'utiliser un serveur DHCP et revenir à la configuration IP statique si un serveur DHCP n'est pas accessible, sélectionnez **Try DHCP server. If it fails, use static IP config**.

Si la configuration IP est affectée par un serveur DHCP, cliquez sur le lien **IP Configuration Assigned by DHCP server** pour afficher les détails de la configuration.

Remarque :

1. Si vous sélectionnez l'option **Enabled - Obtain IP config. from DHCP server**, un serveur DHCP accessible, actif et configuré doit être présent sur votre réseau.
2. La configuration affectée par un serveur DHCP supplantera les paramètres IP statiques.
3. L'option **Try DHCP server. If it fails, use static IP config.** n'est pas prise en charge sur certains modules IMM.

Static IP Configuration

Les zones suivantes contiennent la configuration IP statique pour cette interface. Ces paramètres ne seront utilisés que si DHCP est désactivé. Si DHCP est activé, la configuration IP dynamique attribuée par le serveur DHCP prévaut sur ces paramètress statiques.

- **IP address :** Utilisez cette zone pour définir l'adresse IP du sous-système IMM auquel accède cette interface réseau. Pour définir l'adresse IP, entrez cette adresse dans la zone de texte. L'adresse IP doit contenir quatre entiers (compris entre 0 et 255) séparés par des points, sans espace.

  Remarque : La valeur par défaut de cette zone est `192.168.70.125`.
- **Subnet mask :** Utilisez cette zone pour définir le masque de sous-réseau qui sera utilisé par le sous-système IMM. Pour définir le masque de sous-réseau, entrez le masque de bits dans la zone de texte. Le masque de sous-réseau doit être composé de quatre entiers (compris entre 0 et 255) séparés par des points, sans espace. Les bits sont définis en contigu à partir du bit le plus à gauche. Par exemple, `0.255.0.0` n'est pas un masque de sous-réseau valide. Cette zone ne peut pas être définie à `0.0.0.0` ou à `255.255.255.255`.

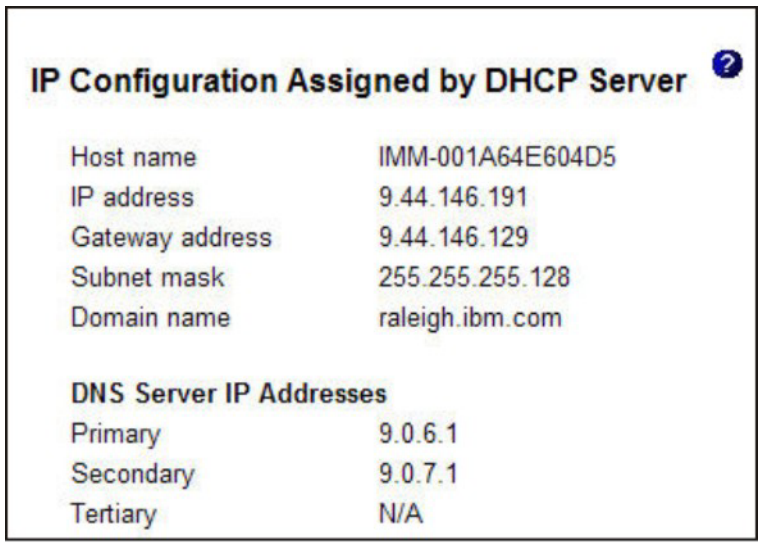
  Remarque : La valeur par défaut de cette zone est `255.255.255.0`.
- **Gateway address :** Utilisez cette zone pour identifier l'adresse IP de votre passerelle par défaut. Pour définir l'adresse de la passerelle, entrez cette adresse dans la zone de texte. L'adresse de passerelle doit être composée de quatre entiers (compris entre 0 et 255) séparés par des points, sans espaces et sans points consécutifs.

  Remarque : La valeur par défaut de cette zone est `0.0.0.0`.

IP Configuration Assigned by DHCP Server

Cliquez sur ce lien pour visualiser la configuration IP affectée par le serveur DHCP. La page IP Configuration Assigned by DHCP Server, similaire à l'image ci-après, s'affiche.

Remarque : Cette option n'est disponible que si DHCP est activé.



Configuration des paramètres IPv6

Les paramètres suivants peuvent être modifiés dans la zone IPv6 de la page Network Interfaces.

Remarque : Au moins une des options de configuration IPv6 décrites dans cette section (IPv6 Static Configuration, DHCPv6, ou Stateless Auto-configuration) doit être activée.

Link local address
Il s'agit de l'adresse IPv6 affectée au module IMM. Son format est similaire à l'exemple suivant :

```
fe80::21a:64ff:fee6:4d5
```

IPv6 Static Configuration
Utilisez cette zone pour activer ou désactiver les paramètres de configuration statique pour IPv6. Lorsque la case **IPv6 Static Configuration** est cochée, les options suivantes sont disponibles :

- **IP address :** Utilisez cette zone pour définir l'adresse IPv6 du sous-système IMM auquel accède cette interface réseau. Pour définir l'adresse IP, entrez l'adresse IPv6 dans la zone de texte. La valeur de cette zone doit correspondre à une adresse IPv6 valide.

  Remarque : La valeur par défaut de cette zone est `0::0`.
- **Address prefix length (1 - 128) :** Utilisez cette zone pour définir la longueur du préfixe pour l'adresse IPv6 statique.
- **Default route :** Utilisez cette zone pour définir l'adresse IPv6 de votre route par défaut. Pour définir la route par défaut, entrez l'adresse IPv6 dans la zone correspondante. La valeur de cette zone doit correspondre à une adresse IPv6 valide.

  Remarque : La valeur par défaut de cette zone est `0::0`.
  .

DHCPv6
Utilisez cette zone pour activer ou désactiver la configuration DHCPv6 affectée sur le module IMM.

Stateless Auto-configuration
Utilisez cette zone pour activer ou désactiver la configuration automatique sans état sur le module IMM.

View Automatic Configuration (lien)
Cliquez sur ce lien pour afficher la configuration IPv6 affectée par le serveur DHCP. La page IPv6 Automatic Configuration s'affiche.

Configuration des protocoles réseau

Sur la page Network Protocols, vous pouvez réaliser les opérations suivantes :

- Configuration SNMP (Simple Network Management Protocol)
- Configuration DNS (Domain Name System)
- Configuration du protocole Telnet
- Configuration SMTP (Simple Mail Transfer Protocol)
- Configuration LDAP (Lightweight Directory Access Protocol)
- Configuration SLP (Service Location Protocol)

Les modifications des paramètres de protocole réseau requièrent un redémarrage d'IMM pour entrer en vigueur. Si vous modifiez plusieurs protocoles, vous devez attendre d'avoir apporté toutes vos modifications et de les avoir enregistrées avant de redémarrer IMM.

Configuration SNMP

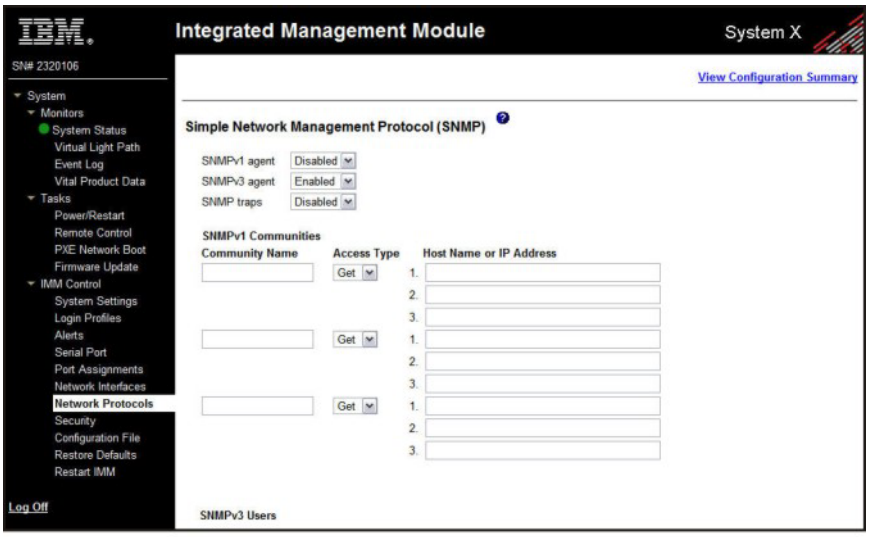
Vous pouvez utiliser l'agent SNMP pour collecter des informations et contrôler le serveur. IMM peut également être configuré pour envoyer des alertes SNMP aux noms d'hôte ou aux adresses IP configurés.

Remarque :

1. IMM fournit deux fichiers MIB (Management Information Base) pour leur utilisation avec des applications SNMP. Les fichiers MIB sont inclus dans les packages de mise à jour du microprogramme IMM.
2. IMM prend en charge les normes SNMPv1 et SNMPv3.

Pour configurer SNMP, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez configurer SNMP. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Network Protocols**. Une page comparable à celle présentée dans la figure ci-après s'affiche.



3. Sélectionnez **Enabled** dans la zone **SNMPv1 agent** ou **SNMPv3 agent**.

   Remarque : Si vous avez activé l'agent SNMPv3, vous devez configurer les paramètres SNMPv3 pour les profils de connexion actifs afin que l'interaction entre le gestionnaire SNMPv3 et l'agent SNMPv3 fonctionne correctement. Vous pouvez configurer ces paramètres au bas de chaque profil de connexion sur la page Login Profiles (voir «Création d'un profil de connexion», à la page 27 pour plus d'informations). Cliquez sur le lien du profil de connexion à configurer, accédez au bas de la page, puis cochez la case **Configure SNMPv3 User**.
4. Sélectionnez **Enabled** dans la zone **SNMP traps** pour acheminer les alertes aux communautés SNMP sur votre réseau. Pour activer l'agent SNMP, les critères ci-après doivent être remplis.

- Un contact système doit être spécifié sur la page System Settings. Pour plus d'informations sur les paramètres de la page System Settings, voir «Définition des informations système», à la page 22.
- L'emplacement du système doit être spécifié sur la page System Settings.
- Au moins un nom de communauté doit être spécifié.
- Au moins une adresse IP ou un nom d'hôte valide (si DNS est activé) doit être spécifié pour cette communauté.

Remarque : Les destinataires d'alertes dont la méthode de notification est SNMP ne peuvent pas recevoir d'alertes à moins que les zones **SNMPv1 agent** ou **SNMPv3 agent** et **SNMP traps** n'aient été définies à **Enabled**.

5. Configurez une communauté pour définir la relation d'administration entre les agents SNMP et les gestionnaires SNMP. Vous devez définir au moins une communauté. Chaque définition de communauté comprend les paramètres suivants :
   - Community Name (Nom de communauté)
   - Access Type (Type d'accès)
   - IP Address (Adresse IP)

   Si l'un de ces paramètres n'est pas correct, l'accès à la gestion SNMP n'est pas accordé.

   Remarque : Si un message d'erreur apparaît, modifiez les zones mentionnées en conséquence. Accédez ensuite au bas de la page et cliquez sur **Save** pour enregistrer les informations corrigées. Vous devez configurer au moins une communauté pour activer cet agent SNMP.
6. Dans la zone **Community Name**, entrez un nom ou une chaîne d'authentification pour indiquer une communauté.
7. Dans la zone **Access Type**, sélectionnez un type d'accès. Sélectionnez **Trap** pour permettre à tous les hôtes de la communauté de recevoir des alertes. Sélectionnez **Get** pour permettre à tous les hôtes de la communauté de recevoir des alertes et d'extraire des objets MIB. Sélectionnez **Set** pour permettre à tous les hôtes de la communauté de recevoir des alertes, d'extraire et de définir des objets MIB.
8. Dans la zone **Host Name or IP Address**, entrez le nom d'hôte ou l'adresse IP de chaque gestionnaire de communauté.
9. Faites défiler la page jusqu'en bas et cliquez sur **Save**.
10. Dans le panneau de navigation, cliquez sur **Restart IMM** pour activer vos modifications.

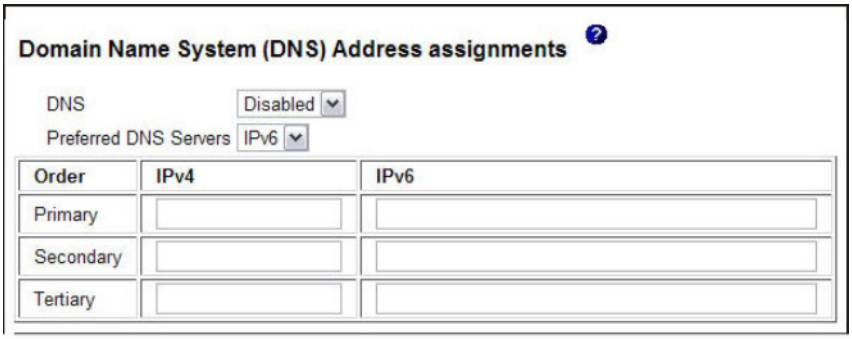
Configuration DNS

Vous pouvez configurer les paramètres DNS (Domain Name System) afin de spécifier si des adresses de serveur DNS supplémentaires doivent être incluses dans l'ordre de recherche pour la résolution de nom d'hôte en adresse IP. La recherche DNS est toujours activée et d'autres adresses DNS peuvent être automatiquement affectées par le serveur DHCP lorsque la fonctionnalité DHCP est activée.

Pour que les adresses DNS supplémentaires puissent être activées, au moins une de ces adresses doit avoir une valeur différente de zéro. Les serveurs DNS supplémentaires sont ajoutés en tête de la liste de recherche ; par conséquent, la recherche de nom d'hôte est effectuée sur ces serveurs avant d'être effectuée sur un serveur DNS affecté automatiquement par un serveur DHCP.

Pour configurer le système DNS, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez configurer le système DNS. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Network Protocols**, défilez jusqu'à la zone **Domain Name System (DNS) Address assignments** sur cette page. Une section de la page similaire à l'illustration ci-après s'affiche.



3. Si un ou plusieurs serveurs DNS sont disponibles sur le réseau, sélectionnez **Enabled** dans la zone **DNS**. La zone **DNS** indique si vous utilisez un serveur DNS sur le réseau pour convertir les noms d'hôte en adresses IP.
4. Si vous disposez d'adresses de serveur DNS IPv4 et IPv6, sélectionnez soit **IPv4**, soit **IPv6**, dans la liste **Preferred DNS Servers** pour spécifier les adresses serveur préférées.
5. Si vous avez activé le système d'adressage DNS, utilisez les zones Primary, Secondary et Tertiary pour spécifier les adresses de jusqu'à six serveurs DNS sur votre réseau. Pour définir les trois adresses de serveurs DNS IPv4 ou IPv6, entrez ces adresses dans les zones de texte correspondantes. Veillez à ce que les adresses IPv4 ou IPv6 aient un format valide.
6. Faites défiler la page jusqu'en bas et cliquez sur **Save**.
7. Dans le panneau de navigation, cliquez sur **Restart IMM** pour activer vos modifications.

Configuration de Telnet

Pour configurer Telnet, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez configurer Telnet. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Network Protocols** et accédez à la section **Telnet Protocol** sur la page. Vous pouvez définir le nombre maximum d'utilisateurs simultanés de Telnet, ou vous pouvez désactiver l'accès Telnet.
3. Faites défiler la page jusqu'en bas et cliquez sur **Save**.
4. Dans le panneau de navigation, cliquez sur **Restart IMM** pour activer vos modifications.

Configuration de SMTP

Pour indiquer l'adresse IP ou le nom d'hôte du serveur SMTP (Simple Mail Transfer Protocol), procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez configurer SMTP. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.

2. Dans le panneau de navigation, cliquez sur **Network Protocols** et accédez à la section **SMTP** sur la page.
3. Dans la zone **SMTP Server Host Name or IP address**, entrez le nom d'hôte du serveur SMTP. Utilisez cette zone pour indiquer l'adresse IP ou, si DNS est activé et configuré, le nom d'hôte du serveur SMTP.
4. Faites défiler la page jusqu'en bas et cliquez sur **Save**.
5. Dans le panneau de navigation, cliquez sur **Restart IMM** pour activer vos modifications.

Configuration de LDAP

Si vous utilisez un serveur LDAP (Lightweight Directory Access Protocol), IMM peut authentifier un utilisateur en interrogeant ou en effectuant une recherche dans un annuaire LDAP sur un serveur LDAP au lieu de passer par une base de données utilisateurs locale. Ensuite, IMM peut authentifier à distance les accès utilisateur vi un serveur LDAP central. Ceci nécessite la prise en charge de client LDAP sur le module IMM. Vous pouvez également affecter des niveaux d'autorisation selon les informations résidant sur le serveur LDAP.

Vous pouvez également utiliser LDAP pour affecter des utilisateurs et des modules IMM à des groupes et procéder à une authentification de groupe, en plus de l'authentification usuelle d'utilisateur (vérification du mot de passe). Par exemple, un IMM peut être associé à un ou plusieurs groupes et un utilisateur ne passerait l'authentification de groupe que s'il appartient au moins à un groupe associé à l'IMM.

Des informations sur la configuration des deux serveurs LDAP suivants sont fournies dans cette section :

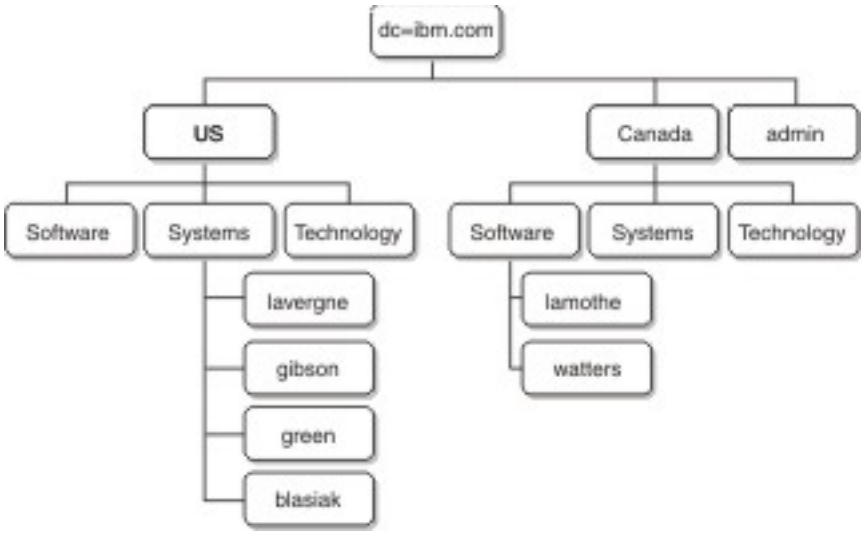
- Novell eDirectory version 8.7.1
- Microsoft Windows Server 2003 Active Directory

Exemple de schéma d'utilisateurs

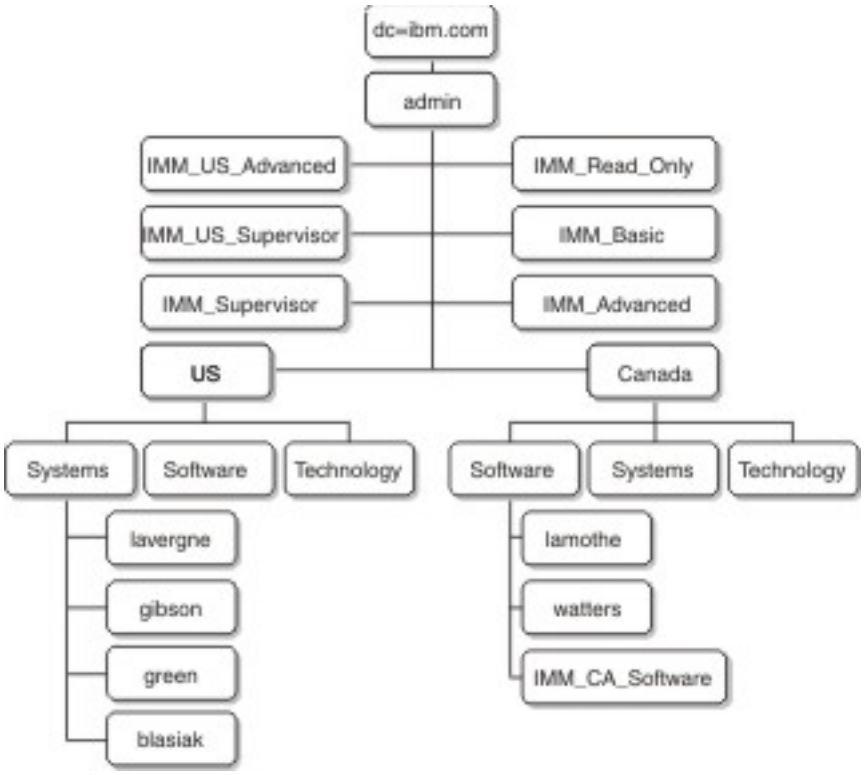
Cette section décrit un exemple de schéma d'utilisateurs simple. Cet exemple est utilisé à travers le document pour illustrer la configuration tant sur le client LDAP que sur le serveur LDAP.

L'exemple de schéma d'utilisateurs a pour racine un composant de domaine intitulé ibm.com. En d'autres termes, chaque objet dans cette arborescence a un nom racine distinctif égal à dc=ibm,dc=com. Supposons maintenant que cette arborescence représente une société désirant classer les utilisateurs et les groupes d'utilisateurs en fonction de leur pays et de leur organisation. La hiérarchie est la suivante racine → pays → organisation → personnes.

La figure ci-après présente une vue simplifiée du schéma utilisée dans ce document. Notez l'utilisation d'un compte utilisateur (userid=admin) directement sous la racine. Il s'agit de l'administrateur.



La figure ci-après illustre l'ajout de groupes d'utilisateurs. Six groupes d'utilisateurs sont définis et ajoutés au premier niveau, et un autre groupe d'utilisateurs est ajouté dans l'organisation Software dans le pays Canada.



Les utilisateurs et les groupes d'utilisateurs associés dans la tableau 5 sont utilisés pour compléter le schéma.

Tableau 5. Mappage d'utilisateur à un groupe

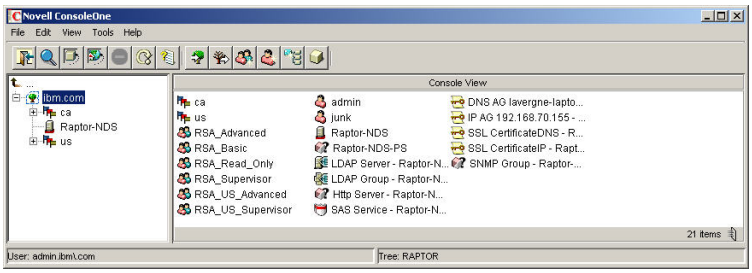
Nom distinctif de l'utilisateur	**Appartenance au groupe**
cn=lavergne, o=Systems, c=us, dc=ibm.com	cn=IMM_Supervisor, dc=ibm.com cn=IMM_US_Supervisor, dc=ibm.com

Tableau 5. Mappage d'utilisateur à un groupe (suite)

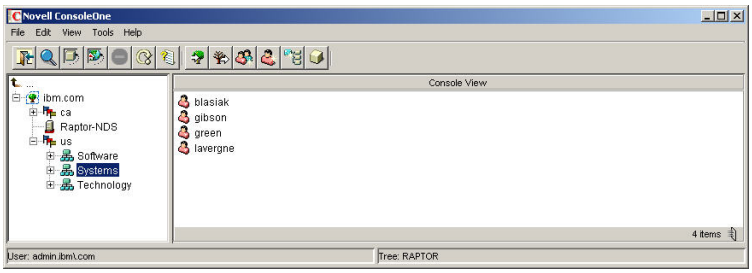
Nom distinctif de l'utilisateur	Appartenance au groupe
cn=blasiak, o=Systems, c=us, dc=ibm.com	cn=IMM_US_Advanced, dc=ibm.com
cn=gibson, o=Systems, c=us, dc=ibm.com	cn=IMM_Basic, dc=ibm.com
cn=green, o=Systems, c=us, dc=ibm.com	cn=IMM_Read_Only, dc=ibm.com
cn=watters, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com
cn=lamothe, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com

Vue de schéma Novell eDirectory

A l'aide de l'outil Novell ConsoleOne, le schéma décrit dans l'«Exemple de schéma d'utilisateurs», à la page 49 a été intégré dans un annuaire Novell eDirectory. La figure suivante illustre la vue de premier niveau du schéma, telle qu'affichée par l'outil ConsoleOne.



La figure ci-après capture les utilisateurs sous o=Systems, c=us, dc=ibm.com.



Appartenance à un groupe

Novell eDirectory utilise un attribut intitulé **groupmembership** pour identifier les groupes dont un utilisateur est membre. La classe d'objet User utilise spécifiquement cet attribut. Le client LDAP utilise une valeur par défaut **memberOf** dans sa demande de recherche au serveur LDAP afin d'extraire les groupes dont est membre un utilisateur.

Vous pouvez configurer le client LDAP pour déterminer l'appartenance à des groupes à l'aide d'une des méthodes suivantes :

- Configurez la valeur **GroupMembership** dans la zone **Group Search Attribute** sur le client LDAP.
- Créez un mappage d'attribut entre **GroupMembership** et **memberOf** sur le serveur LDAP Novell eDirectory.

Procédez comme suit pour configurer l'attribut par défaut sur le client LDAP.

1. Dans le volet de navigation de gauche sur l'interface Web d'IMM, cliquez sur **Network Protocols**.
2. Faites défiler la page jusqu'à la section **LDAP Search Attributes**.
3. Dans la zone **Group Search Attribute**, entrez l'attribut par défaut voulu.

Si la zone **Group Search Attribute** est vide, elle reçoit par défaut la valeur **memberOf** et vous devrez alors configurer le serveur Novell eDirectory en mappant l'attribut **GroupMembership** à **memberOf**. Procédez comme suit pour configurer le serveur Novell eDirectory en mappant l'attribut **GroupMembership** à **memberOf**.

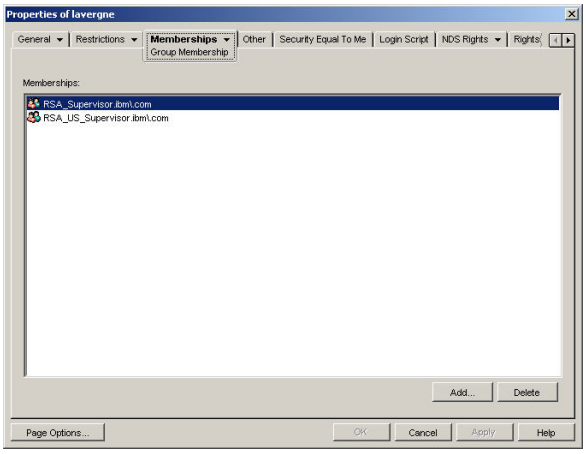
1. A l'aide de l'outil ConsoleOne, cliquez avec le bouton droit de la souris sur l'icône **LDAP Group**, puis cliquez sur **Properties**. La fenêtre Properties of LDAP Group s'affiche.
2. Cliquez sur l'onglet **Attribute Mappings**.
3. Cliquez sur **Add**, puis créez un mappage entre **Group Membership** et **memberOf**.
4. Cliquez sur **OK**. Une page affichant les propriétés du groupe LDAP s'ouvre.

Ajout d'utilisateurs à des groupes d'utilisateurs

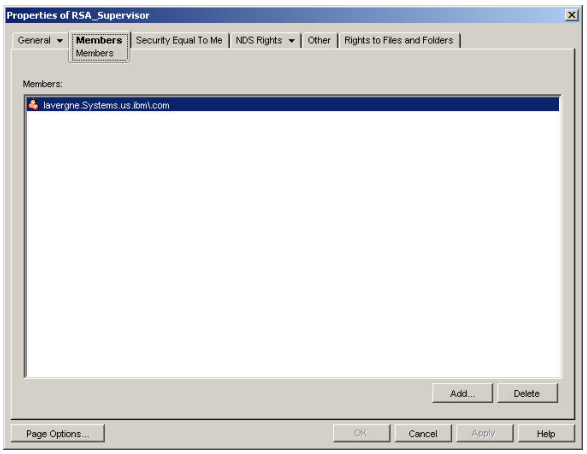
Vous pouvez ajouter des utilisateurs aux groupes d'utilisateurs appropriés en ajoutant les groupes au profil d'un utilisateur, ou en ajoutant des utilisateurs au profil d'un groupe. Le résultat final est identique.

Par exemple, dans l'exemple de schéma utilisateur précédent, l'utilisateur lavergne est membre à la fois d'IMM_US_Supervisor et d'IMM_Supervisor. A l'aide d'un outil de navigateur tel que Novell ConsoleOne, vous pouvez vérifier le schéma (effectuez un double clic sur **user lavergne** et sélectionnez l'onglet **Memberships**).

Une page semblable à celle de la figure suivante s'affiche.



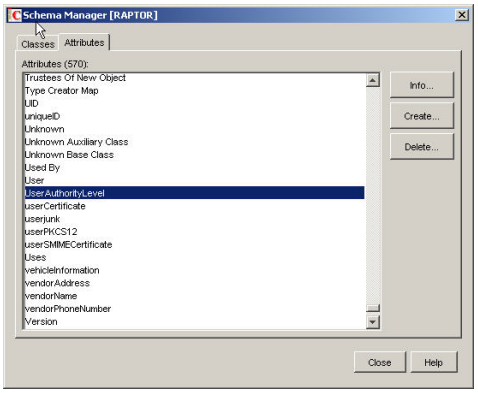
De même, si les propriétés du groupe IMM_Supervisor sont affichées et que vous sélectionnez l'onglet **Members**, une page semblable à celle de la figure ci-après s'affiche.



Niveaux d'autorisation

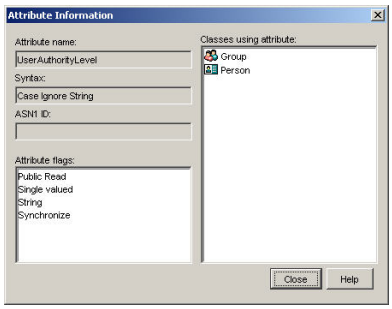
Pour utiliser cette fonctionnalité, utilisez ConsoleOne afin de créer un nouvel attribut intitulé `UserAuthorityLevel` dans l'annuaire Novell eDirectory. Ce nouvel attribut sera utilisé pour prendre en charge les niveaux d'autorisation.

1. Dans l'outil Novell ConsoleOne, cliquez sur **Tools** > **Schema Manager**.
2. Cliquez sur l'onglet **Attributes**, puis sur **Create**.
3. Intitulez l'attribut **UserAuthorityLevel**. Laissez la zone **ID ASN1** vide ou contactez votre administrateur LDAP pour déterminer la valeur à utiliser. Cliquez sur **Next**.
4. Définissez la syntaxe à **Case Ignore String**. Cliquez sur **Next**.
5. Définissez les indicateurs le cas échéant. Contactez votre administrateur LDAP pour vérifier qu'ils sont définis correctement. Cochez la case **Public Read**, puis cliquez sur **Next**.
6. Cliquez sur **Finish**. Une page semblable à celle de la figure suivante s'affiche.



7. Revenez à la fenêtre Schema Manager et cliquez sur l'onglet **Classes**.
8. Cliquez sur la classe **Person**, puis sur **Add**. Notez que vous pouvez utiliser à la place la classe d'objets User.
9. Accédez à l'attribut **UserAuthorityLevel**, sélectionnez-le et ajoutez-le aux attributs de cette classe. Cliquez sur **OK**.
10. Cliquez sur la classe **Group**, puis sur **Add**.
11. Accédez à l'attribut **UserAuthorityLevel**, sélectionnez-le et ajoutez-le aux attributs de cette classe. Cliquez sur **OK**.
12. Pour vérifier que l'attribut a bien été ajouté à la classe, dans la fenêtre Schema Manager, sélectionnez la classe **Attributes**.

13. Accédez à l'attribut **UserAuthorityLevel**, puis cliquez sur **Info**. Une page semblable à celle de la figure suivante s'affiche.



Définition des niveaux d'autorisation

Cette section explique comment interpréter et à utiliser l'attribut UserAuthorityLevel. La valeur affectée à l'attribut UserAuthorityLevel détermine les permissions (ou niveaux d'autorisation) affectés à un utilisateur après une authentification réussie.

L'attribut UserAuthorityLevel est lu comme une chaîne de bits (bits 0 et 1). Les bits sont numérotés de gauche à droite. Le premier bit est un bit de position 0, Le second un bit de position 1, etc.

Le tableau suivant fournit une explication de chaque position de bit.

Tableau 6. Bits d'autorisation

Position de bit	Fonction	Explication
0	Refuser toujours	S'il est utilisé, l'authentification de l'utilisateur échoue toujours. Cette fonction peut être utilisée pour bloquer un ou plusieurs utilisateurs associés à un groupe spécifique.
1	Accès superviseur	S'il est utilisé, les privilèges administrateur sont octroyés à l'utilisateur. L'utilisateur dispose d'un accès en lecture et écriture à chaque fonction. Si vous définissez ce bit, vous n'avez pas à définir individuellement les autres.
2	Accès en lecture seule	S'il est défini, l'utilisateur dispose d'un accès en lecture seule et ne peut pas exécuter de procédures de maintenance (par exemple, un redémarrage, des actions à distance ou des mises à jour de microprogramme). Il ne peut rien modifier à l'aide des fonctions d'enregistrement, d'effacement ou de restauration. La position de bit 2 et tous les autres bits s'excluent mutuellement, la position de bit 2 étant celle avec la plus faible priorité. Si un autre bit est défini, ce bit sera ignoré.

Tableau 6. Bits d'autorisation (suite)

Position de bit	Fonction	Explication
3	Réseau et sécurité	S'il est défini, un utilisateur peut modifier la configuration dans les panneaux Security, Network Protocols, Network Interface, Port Assignments et Serial Port.
4	Gestion des comptes utilisateur	S'il est défini, un utilisateur peut ajouter, modifier ou supprimer des utilisateurs et changer les paramètres de connexion globaux dans le panneau Login Profiles.
5	Accès à la console distante	S'il est défini, un utilisateur peut accéder à la console du serveur distant et modifier la configuration dans le panneau Serial Port.
6	Accès à la console distante et au disque distant	S'il est défini, un utilisateur peut accéder à la console du serveur distant et aux fonctions de disque distant pour le serveur distant . L'utilisateur peut également modifier la configuration dans le panneau Serial Port.
7	Accès aux fonctions d'alimentation/de redémarrage du serveur distant	S'il est défini, un utilisateur peut accéder aux fonctions d'alimentation, de redémarrage et de délai d'attente du serveur distant.
8	Configuration de base de l'adaptateur	S'il est défini, un utilisateur peut modifier les paramètres de configuration dans les panneaux System Settings et Alerts (à l'exception des paramètres Contact, Location et Server Timeout).
9	Possibilité d'effacer les journaux d'événements	S'il est défini, un utilisateur peut effacer les journaux d'événements. **Remarque :** Tous les utilisateurs peuvent afficher les journaux des événements mais ce niveau d'autorisation est requis pour pouvoir effacer leur contenu.

Tableau 6. Bits d'autorisation (suite)

Position de bit	Fonction	Explication
10	Configuration avancée d'adaptateur	S'il est défini, l'utilisateur n'est pas soumis à des restrictions lors de la configuration de l'adaptateur et dispose de droits d'administration sur le module IMM. L'utilisateur peut exécuter les fonctions avancées suivantes : mises à jour de microprogramme, amorçage réseau PXE, restauration des paramètres usine par défaut de l'adaptateur, modification et restauration de la configuration de l'adaptateur depuis un fichier de configuration et redémarrage/réinitialisation de l'adaptateur. Ceci exclut les fonctions de contrôle/redémarrage et de délai d'attente du serveur.
11	Réservé	Cette position de bit est réservée pour un usage ultérieur (actuellement ignorée).

Remarques :

- Si des bits ne sont pas utilisés, leur valeur par défaut pour l'utilisateur sera définie pour lecture seule.
- Les autorisations de connexion extraites directement de l'enregistrement utilisateur sont prioritaires. Si l'enregistrement utilisateur ne contient pas de nom dans la zone **Login Permission Attribute**, le système tente d'extraire les autorisations du groupe auquel appartient l'utilisateur et qui correspondent au filtre de groupe. Dans ce cas, l'utilisateur reçoit l'opérateur inclusif OR de tous les bits pour tous les groupes.
- Si le bit de position 0 (Refuser toujours) est défini pour l'un des groupes, l'accès est refusé à l'utilisateur. Ce bit prévaut toujours sur les autres.
- Si un utilisateur a la possibilité de modifier les paramètres de configuration de base, de réseau ou de sécurité de l'adaptateur, vous devriez envisager de l'autoriser à redémarrer le module IMM (bit de position 10). Sans cette possibilité, l'utilisateur pourra modifier un paramètre mais sans que cette modification n'entre en vigueur.

Le tableau suivant contient des exemples et leurs descriptions :

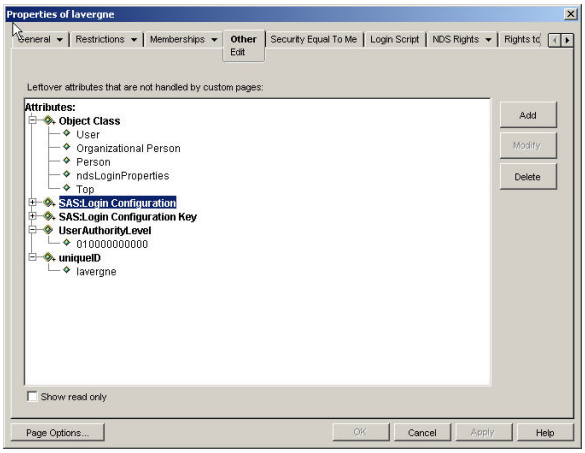
Tableau 7. Exemples et descriptions d'attributs UserLevelAuthority

Exemple d'attribut UserLevelAuthority	Description
IBMRBSPermissions=010000000000	Accès superviseur (bit de position 1 défini)
IBMRBSPermissions=001000000000	Accès en lecture seule (bit de position 2 défini)
IBMRBSPermissions=100000000000	Pas d'accès (bit de position 0 défini)
IBMRBSPermissions=000011111100	Toutes les autorisations excepté de configuration avancée de l'adaptateur
IBMRBSPermissions=000011011110	Toutes les autorisations excepté l'accès au média virtuel

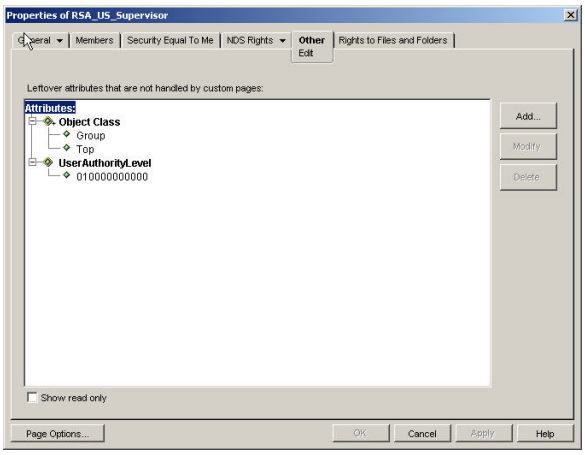
Procédez comme suit pour ajouter l'attribut UserAuthorityLevel à l'utilisateur *lavergne* et à chacun des groupes d'utilisateurs.

1. Cliquez avec le bouton droit sur l'utilisateur **lavergne** et cliquez sur **Properties**.
2. Cliquez sur l'onglet **Other**. Cliquez sur **Add**.
3. Accédez à **UserAuthorityAttribute** et cliquez sur **OK**.
4. Affectez la valeur voulue à l'attribut. Par exemple, si vous désirez accorder un accès de niveau Superviseur, définissez l'attribut à **IBMRBSPermissions=010000000000**. Cliquez sur **OK**.
5. Répétez les étapes 1 à 4 pour chaque groupe d'utilisateurs et attribuez à **UserAuthorityLevel** la valeur appropriée.

   La figure suivante présente les propriétés de l'utilisateur *lavergne*.



   La figure suivante présente les propriétés du groupe IMM_US_Supervisor.



   Le tableau suivant présente les autorisations **UserAuthorityLevel** affectées à chaque groupe d'utilisateurs dans l'exemple de schéma utilisateur.

Tableau 8. Affectations UserAuthorityLevel aux groupes d'utilisateurs

Groupe d'utilisateurs	UserAuthorityLevel	Signification
IMM_Basic	IBMRBSPermissions=000100000000	Réseau et sécurité

Tableau 8. Affectations UserAuthorityLevel aux groupes d'utilisateurs (suite)

Groupe d'utilisateurs	UserAuthorityLevel	Signification
IMM_CA_Software	IBMRBSPermissions=000101111010	Réseau et sécurité Accès à la console distante et au média virtuel Accès aux fonctions d'alimentation et de redémarrage du serveur distant Configuration de base de l'adaptateur Configuration avancée de l'adaptateur
IMM_Advanced	IBMRBSPermissions=000110111100	Réseau et sécurité Accès à la console distante et au média virtuel Accès aux fonctions d'alimentation et de redémarrage du serveur distant Configuration de base de l'adaptateur Configuration avancée de l'adaptateur Possibilité d'effacer les journaux d'événements
IMM_Supervisor	IBMRBSPermissions=010000000000	Accès superviseur
IMM_Read_Only	IBMRBSPermissions=001000000000	Accès en lecture seule
IMM_US_Advanced	IBMRBSPermissions=000110111100	Réseau et sécurité Gestion des comptes utilisateurs Accès à la console distante et au média virtuel Accès aux fonctions d'alimentation et de redémarrage du serveur distant Configuration de base de l'adaptateur Possibilité d'effacer les journaux d'événements
IMM_US_Supervisor	IBMRBSPermissions=010000000000	Accès superviseur

Exploration du serveur LDAP

Avant de tenter de vous connecter à votre serveur LDAP depuis le client LDAP sur le module IMM, vous connecter à votre serveur LDAP à l'aide d'un navigateur LDAP tiers de votre choix. Vous pouvez, par exemple, télécharger un outil d'exploration d'annuaire depuis le site http://www.ldapbrowser.com.

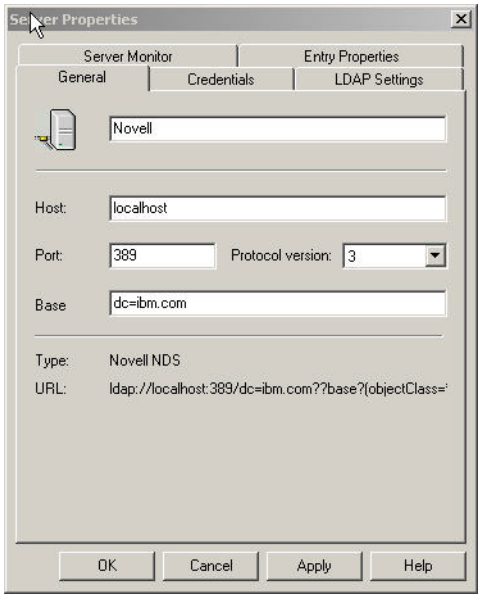
L'utilisation du navigateur LDAP avant de tenter d'utiliser le client LDAP IMM présente les avantages suivants :

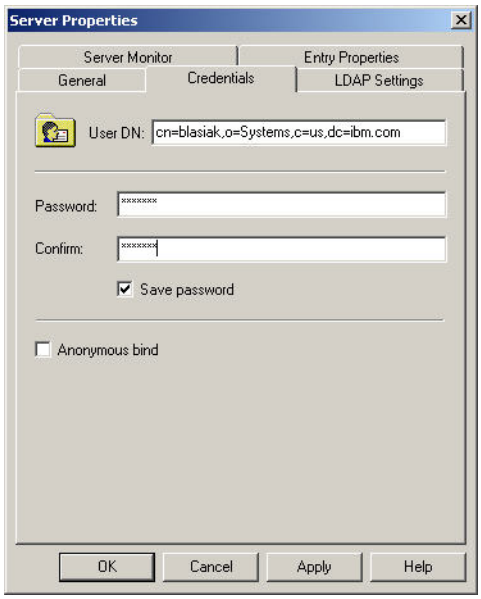
- Capacité de liaison à un serveur à l'aide de données d'identification variées. Ceci indiquera si les comptes utilisateurs sur le serveur LDAP sont configurés correctement. Si vous pouvez créer une liaison au serveur à l'aide du navigateur, mais non pas à l'aide du client LDAP d'IMM, ce client n'est pas configuré

correctement. Si vous ne parvenez pas à créer une liaison au serveur à l'aide du navigateur, vous ne pourrez pas créer une liaison avec le client LDAP sur le module IMM.

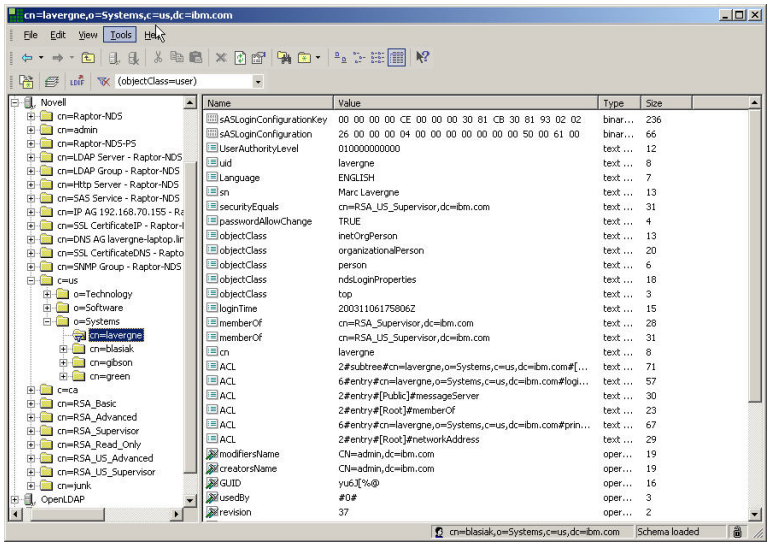
- Après que vous soyez parvenu à créer la liaison au serveur, vous pourrez naviguer à travers la base de données du serveur LDAP et émettre rapidement des requêtes de recherche. Ceci confirmera si le serveur LDAP est configuré comme voulu pour l'accès aux divers objets. Par exemple, vous pourriez constater que vous ne parvenez pas à afficher un attribut spécifique ou à visualiser tous les objets attendus sous une requête de recherche spécifique. Ceci indiquerait que les permissions affectées aux objets (par exemple, les éléments visibles par le public ou ceux masqués) ne sont pas configurés correctement. Contactez l'administrateur du serveur LDAP pour corriger le problème. Notez que les données d'identification utilisées pour la liaison déterminent vos autorisations sur le serveur.
- Vérifiez l'appartenance aux groupes pour tous les utilisateurs. Vérifiez l'attribut **UserAuthorityLevel** affecté aux utilisateurs et aux groupes d'utilisateurs.

Les figures suivantes illustrent diverses requêtes et les résultats de recherche effectuées sur un serveur Novell eDirectory configuré d'après l'«Exemple de schéma d'utilisateurs», à la page 49. En l'occurrence, l'outil de navigateur Softerra a été utilisé. La liaison initiale au serveur a été effectuée avec les propriétés et les données d'identification présentées dans l'illustration.

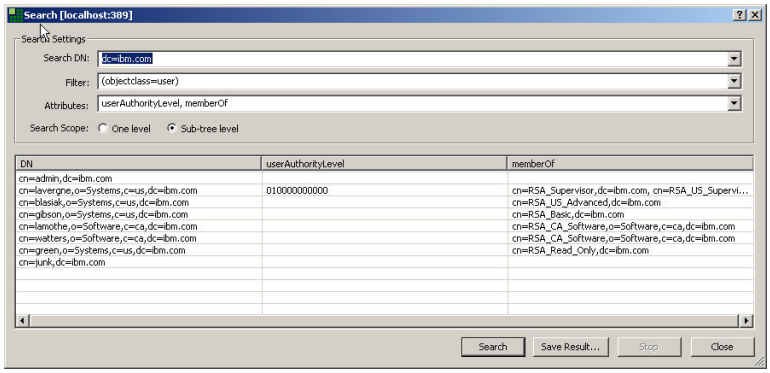




Après la réussite de la liaison initiale, la vue suivante du schéma sur l'annuaire Novell eDirectory est affichée.



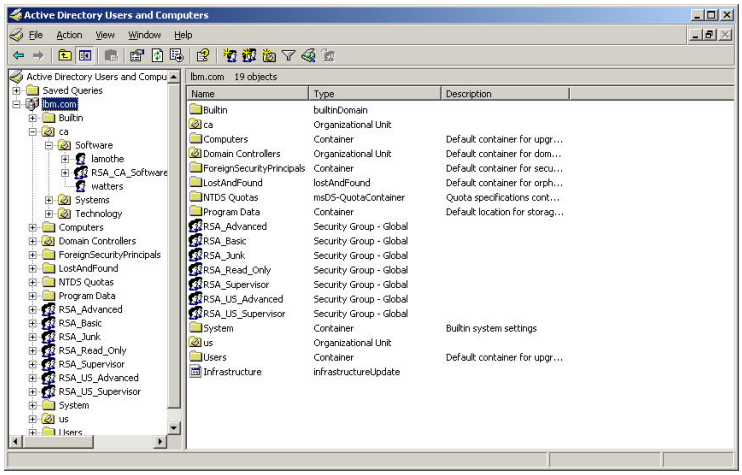
L'illustration suivante présente une requête portant sur tous les utilisateurs et visant à extraire les attributs **userAuthorityLevel** et **memberOf**.



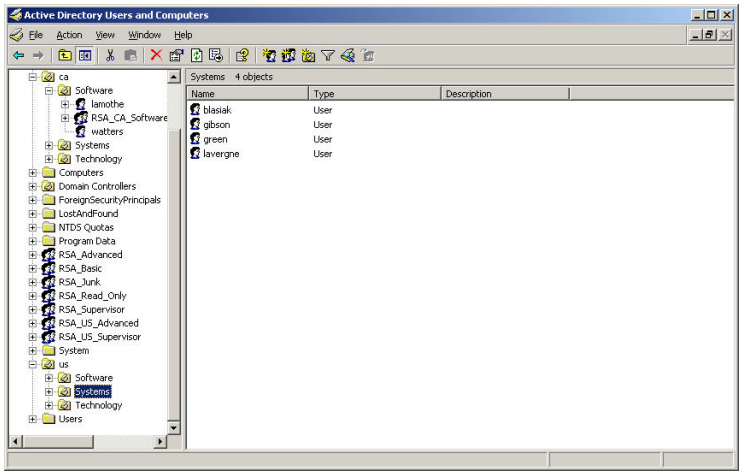
Vue de schéma Microsoft Windows Server 2003 Active Directory

Cette section décrit certains aspects de configuration concernant la capture d'informations dans l'«Exemple de schéma d'utilisateurs», à la page 49 sous Microsoft Windows Server 2003 Active Directory.

La figure suivante illustre la vue de premier niveau du schéma, telle qu'affichée par l'outil de gestion Active Directory Users and Computers.



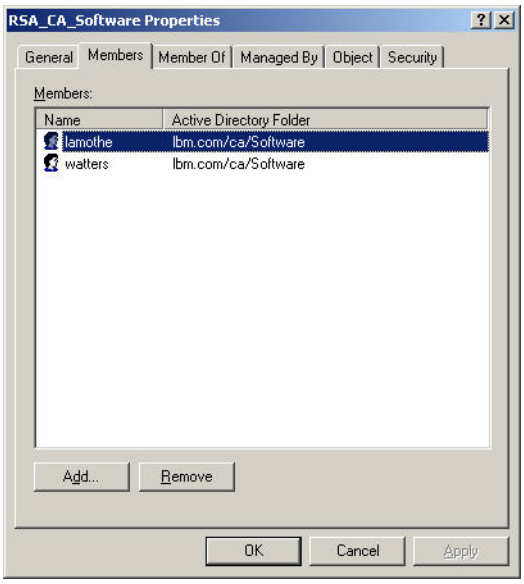
La figure suivante présente les utilisateurs sous ou=Systems, ou=us, dc=ibm, dc=com.



Ajout d'utilisateurs à des groupes d'utilisateurs

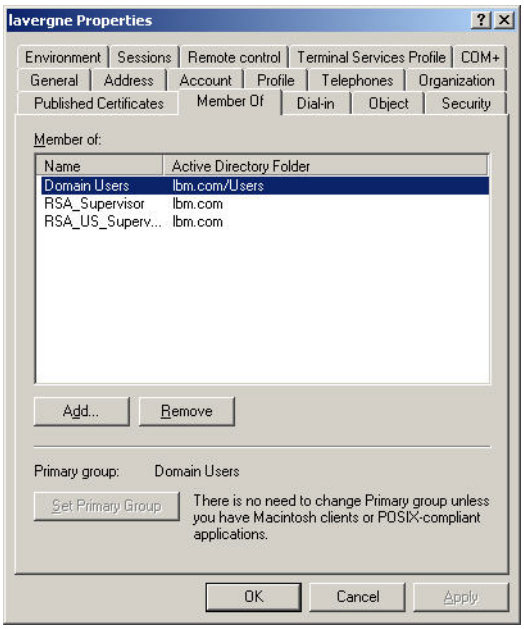
Dans Active Directory, vous pouvez soit ajouter des groupes à un utilisateur spécifique, soit ajouter des utilisateurs à un groupe spécifique. Cliquez avec le bouton droit de la souris sur l'objet utilisateur ou groupe d'utilisateurs, puis cliquez sur **Properties**.

Si vous sélectionnez un groupe d'utilisateurs, puis cliquez sur l'onglet **Members**, une page similaire à celle de la figure ci-après s'ouvre.



Pour ajouter ou supprimer des utilisateurs dans le groupe d'utilisateurs, cliquez respectivement sur **Add** ou sur **Remove**.

Si vous sélectionnez un utilisateur, puis cliquez sur l'onglet **MembersOf**, une page similaire à celle de la figure ci-après s'ouvre.

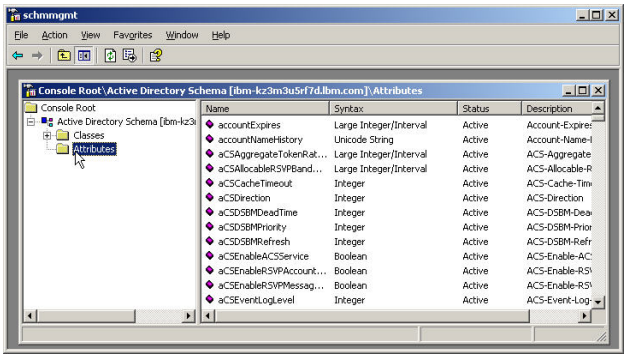


Pour ajouter ou supprimer des utilisateurs dans le groupe d'utilisateurs, cliquez respectivement sur **Add** ou sur **Remove**.

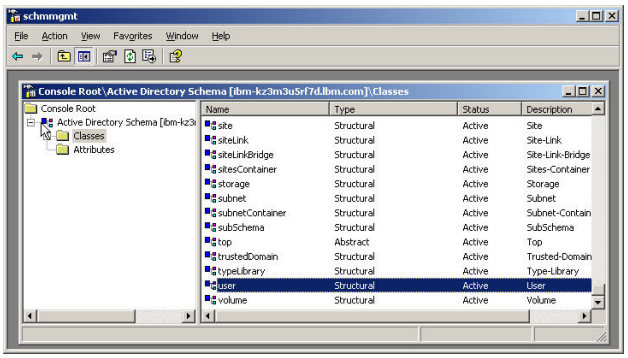
Niveaux d'autorisation

La section «Niveaux d'autorisation», à la page 53 explique comment créer un nouvel attribut avec le serveur Novell eDirectory afin de prendre en charge le concept de niveaux d'autorisations et comment ces niveaux sont affectés aux utilisateurs qui s'authentifient auprès d'un serveur LDAP depuis IMM. L'attribut créé a été intitulé **UserAuthorityLevel**. Dans cette section, vous allez créer cet attribut dans Active Directory.

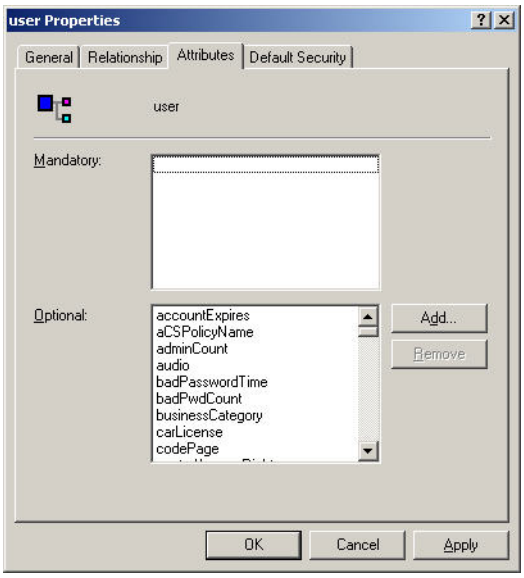
1. Installez l'outil Active Directory Schema Snap-In. Pour plus d'informations, consultez la documentation accompagnant Active Directory.
2. Lancez le schéma Active Directory.
3. Cliquez sur **Action** > **Create Attribute**. Renseignez les zones suivantes :
   a. Définissez Common à **UserAuthorityLevel**
   b. Définissez Syntax à **Case Insensitive String**
   c. Définissez Minimum et Maximum à **12**
4. Contactez votre administrateur système pour affecter un nouvel ID objet X.500. Si vous ne désirez pas définir un nouvel ID objet X.500, utilisez un attribut existant au lieu d'en créer un nouveau pour le niveau d'autorisation.



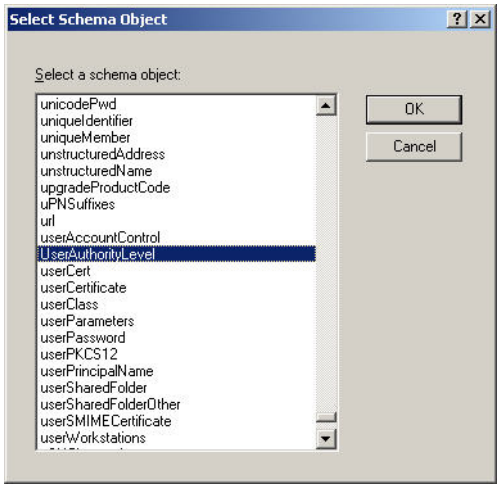
5. Après avoir enregistré l'attribut, sélectionnez le dossier **Classes**.



6. Effectuez un double-clic sur la classe **user**. La fenêtre user Properties s'ouvre.

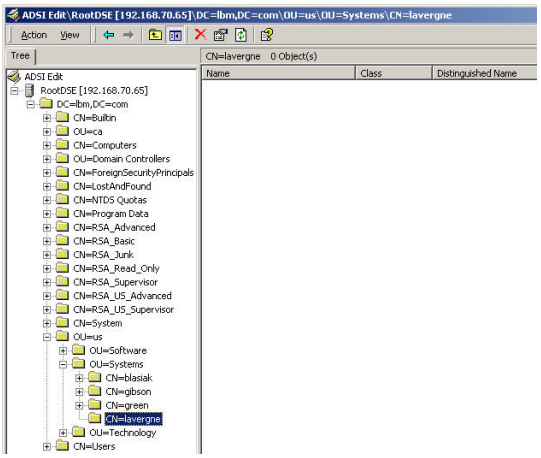


7. Sélectionnez l'onglet **Attributes** et cliquez sur **Add**. La fenêtre Select Schema Object s'ouvre.

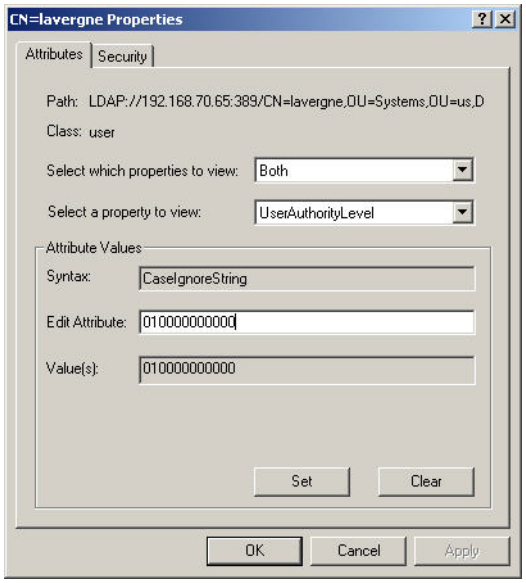


8. Accédez à **UserAuthorityLevel** et cliquez sur **OK**. Cet attribut apparaît dorénavant dans la liste des attributs facultatifs de la classe d'objet user.
9. Répétez les étapes 6, à la page 63 à 8 pour la classe groups. Ceci permet d'affecter l'attribut **UserAuthorityLevel** à un utilisateur ou à un groupe d'utilisateurs. Ce sont les deux seules classes d'objets qui ont besoin d'utiliser ce nouvel attribut.
10. Affectez l'attribut **UserAuthorityLevel** aux utilisateurs et aux groupes d'utilisateurs appropriés. Pour vous conformer au schéma défini sous le serveur Novell eDirectory, utilisez les mêmes valeurs que dans «Définition des niveaux d'autorisation», à la page 54. Pour ce faire, vous pouvez utiliser l'outil ADSI Edit. L'outil Microsoft ADSI Edit est un composant logiciel enfichable MMC (Microsoft Management Console) permettant de visualiser tous les objets de l'annuaire (y-compris le schéma et les informations de configuration), de modifier des objets et de définir des listes de contrôle d'accès pour ces objets.
11. Pour cet exemple, supposons que vous désirez ajouter l'attribut **UserAuthorityLevel** pour l'utilisateur lavergne. Pour ce faire, utilisez ADSI Edit. Vous devez soumettre les données d'identification appropriées pour vous

connecter à Active Directory, faute de quoi vous risquez de ne pas disposer des autorisations utilisateur adéquates pour modifier des objets sur le serveur. La figure suivante présente le schéma, tel qu'identifié par ADSI, après la connexion au serveur.



12. Cliquez avec le bouton droit de la souris sur **lavergne**, puis cliquez sur **Properties**. Une fenêtre similaire à celle de la figure suivante s'ouvre.



13. Dans la zone **Select which properties to view**, sélectionnez **UserAuthorityLevel**.
14. Dans la zone **Edit Attribute**, entrez `IBMRBSPermissions=010000000000`, ce qui correspond à un accès Superviseur. Cliquez sur **Set**.
15. Cliquez sur **OK**.
16. Vous pouvez ajouter cet attribut à des groupes d'utilisateurs en suivant la même procédure pour l'objet groupe d'utilisateurs que vous désirez modifier.

Vérification de la configuration Active Directory

Avant de tenter de connecter le client LDAP au serveur Active Directory (pour l'authentification des utilisateurs), explorez le schéma Active Directory avec un navigateur LDAP. Emettez au minimum les requêtes répertoriées dans le tableau suivant pour vérifier les niveaux d'autorisation et l'appartenance aux groupes.

Tableau 9. Vérification des niveaux d'autorisation et de l'appartenance aux groupes

Nom distinctif de recherche	Filtre	Attributs
DC=ibm, DC=com	(objectclass=user)	memberOf, userAuthorityLevel
DC=ibm, DC=com	(objectclass=group)	member, userAuthorityLevel

Configuration du client LDAP

Vous pouvez configurer LDAP afin d'authentifier les utilisateurs du module de gestion. Le module IMM prend en charge l'authentification d'utilisateur locale et distante. L'authentification locale utilise les informations fournies sur la page Login Profiles pour authentifier les utilisateurs. Si vous utilisez un serveur LDAP, un module de gestion peut authentifier un utilisateur en lançant des requêtes ou des recherches dans un annuaire LDAP sur un serveur LDAP distant au lieu d'utiliser une base de données d'utilisateurs locale.

Lorsque l'un des types d'authentification distante est utilisé, vous pouvez demander que les droits de chaque utilisateur authentifié soient autorisés en local ou en fonction des informations stockées sur le serveur LDAP utilisé pour l'authentification distante. Les autorisations octroyées à chaque utilisateur spécifient les actions qu'il peut effectuer alors qu'il est connecté au module the IMM. Les méthodes d'authentification distantes sont décrites dans les rubriques suivantes :

- Authentification Active Directory avec autorisation locale
- Authentification et autorisation Active Directory basée rôle
- Modèle d'authentification et d'autorisation LDAP existant

Authentification Active Directory avec autorisation locale

Vous pouvez configurer une authentification LDAP à distance, avec une autorisation locale de l'utilisateur, par le biais de l'authentification Active Directory.

Remarque : L'authentification Active Directory avec une autorisation locale s'applique uniquement à un serveur utilisé en environnement Active Directory.

En cas d'utilisation de l'authentification Active Directory avec autorisation locale, les serveurs Active Directory ne sont utilisés que pour authentifier des utilisateurs en vérifiant leurs données d'identification. Aucune information d'autorisation n'est stockée sur le serveur Active Directory pour un utilisateur ; les profils de groupes stockés sur IMM doivent être configurés avec les informations d'autorisation. Les informations d'autorisation utilisées pour configurer les profils des groupes peuvent être obtenues en extrayant les informations d'appartenance d'un utilisateur sur le serveur Active Directory. Ces informations d'appartenance répertorient les groupes auxquels appartient un utilisateur (les groupes imbriqués sont pris en charge). Les groupes spécifiés sur le serveur Active Directory sont ensuite comparés aux noms de groupe configurés localement sur le module IMM. Pour chaque groupe dont il est membre, l'utilisateur se voit affecter les autorisations attribuées à ce groupe. Pour chaque nom de groupe configuré localement sur le module IMM existe un profil d'autorisation correspondant également configuré pour ce groupe.

IMM prend en charge jusqu'à 16 noms de groupes configurés localement. Chaque nom de groupe est limité à 63 caractères. L'un des attributs ci-après doit être configuré comme nom de groupe pour correspondre aux informations d'appartenance au groupe extraites des serveurs Active Directory.

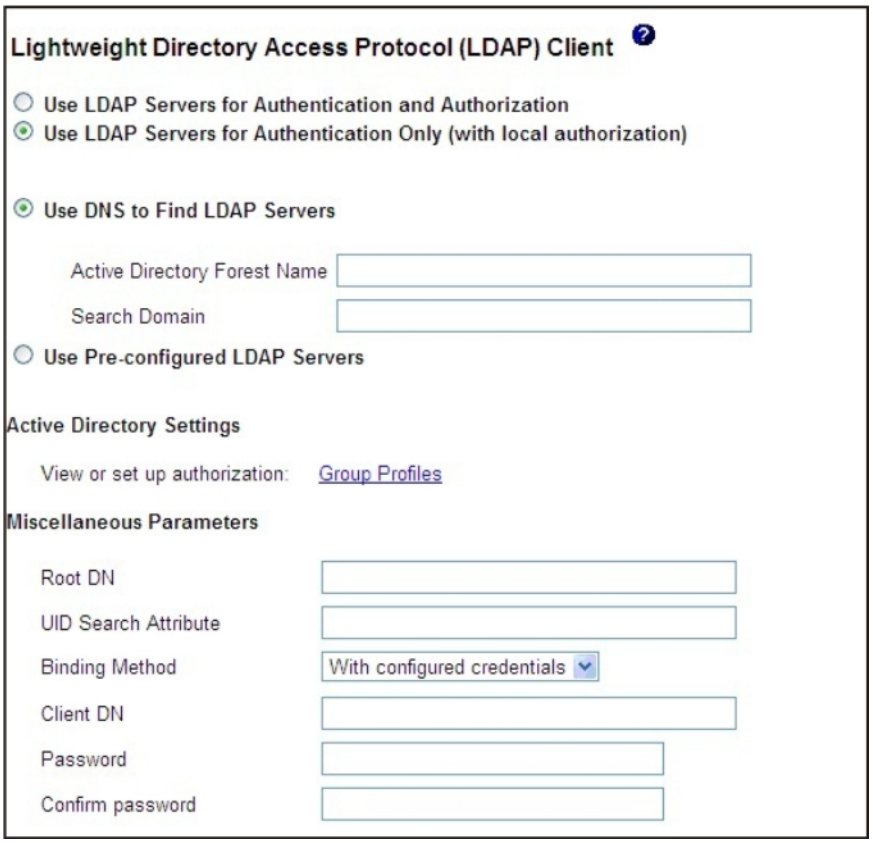
- Distinguished name (DN) (Nom distinctif)
- Attribut "cn"
- Attribut "name"
- Attribut "sAMAccountName"

Pour configurer l'authentification Active Directory avec une autorisation locale pour IMM, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Network Protocols**.
2. Accédez à la section **Lightweight Directory Access Protocol (LDAP) Client**.
3. Sélectionnez **Use LDAP Servers for Authentication Only (with local authorization)**.
4. Sélectionnez l'une des options suivantes pour configurer manuellement ou reconnaître dynamiquement les contrôleurs de domaine :
   - Sélectionnez **Use DNS to find LDAP Servers** pour détecter dynamiquement les contrôleurs de domaine d'après les enregistrements SVR DNS.
   - Sélectionnez **Use Pre-Configured LDAP Servers** (sélection par défaut) pour configurer manuellement les contrôleurs de domaine.
5. Si vous utilisez DNS pour détecter les contrôleurs de domaine de manière dynamique, configurez les paramètres suivants, puis passez à l'étape 7, à la page 68.

   Remarque : Si vous utilisez DNS pour détecter les contrôleurs de domaine de manière dynamique, vous devez spécifier le nom de domaine complet du contrôleur de domaine.
   - Search Domain
     - Entrez le nom de domaine du contrôleur de domaine dans la zone **Search Domain**.
   - Active Directory Forest Name
     - Cette zone facultative permet d'identifier les catalogues globaux. Les catalogues globaux sont nécessaires pour les utilisateurs qui sont membres de groupes universels communs à plusieurs domaines. Dans des environnements où l'appartenance à un groupe commun à plusieurs domaines ne s'applique pas, cette zone peut rester vide.

La figure suivante présente la fenêtre LDAP Client lorsque DNS est utilisé pour détection dynamique des contrôleurs de domaine.



6. Si vous configurez manuellement les contrôleurs de domaine et les catalogues globaux, sélectionnez **Use Pre-Configured LDAP Servers** (sélection par défaut), puis configurez les zones **LDAP Server Host Name or IP Address** et **Port**.

   Vous pouvez configurer jusqu'à quatre contrôleurs de domaine en utilisant une adresse IP ou un nom d'hôte complet. Les serveurs de catalogue global sont identifiés à l'aide des numéros de port 3268 ou 3269. L'utilisation d'un autre numéro de port indique qu'un contrôleur de domaine est en cours de configuration.
7. Si vous utilisez des profils d'autorisation de groupe, cliquez sur **Group Profiles** dans la section Active Directory Settings pour les afficher ou les configurer (voir «Profils de groupe pour utilisateurs Active Directory», à la page 70 pour plus d'informations).
8. Revenez à la page Network Protocols. Cliquez sur le lien **LDAP Client section of the Network Protocols page** situé sur la page Group Profiles for Active Directory Users, puis accédez à la section **Lightweight Directory Access Protocol (LDAP) Client**.
9. Configurez les zones de la section Miscellaneous Parameters pour le module IMM. Reportez-vous au tableau suivant pour plus d'informations sur les paramètres.

Tableau 10. Paramètres divers

Zone	Description	Option
Root DN	IMM utilise la zone **Root DN** au format DN comme entrée racine de l'arborescence. Cette valeur DN sera utilisée comme objet de base pour toutes les recherches. Exemple : `dc=mycompany,dc=com`.	
Binding method	La zone **Binding Method** (Méthode de liaison) est utilisée pour les liaisons initiales au serveur du contrôleur de domaine. Sélectionnez une option.	• With configured credentials (Avec données d'identification configurées) : Entrez le nom distinctif et le mot de passe de l'utilisateur à utiliser pour la liaison initiale. Si cette liaison échoue, la procédure d'authentification échoue également. Si la liaison aboutit, une recherche tente d'identifier un enregistrement utilisateur correspondant au nom distinctif (DN) du client saisi dans la zone **Client DN**. La procédure recherche normalement des attributs communs correspondant à l'ID utilisateur indiqué pendant la procédure de connexion. Il s'agit des attributs suivants : displayName, sAMAccountName et userPrincipalName. Si la zone **UID search attribute** est configurée, la recherche inclut également cet attribut. Si la recherche aboutit, le système tente d'effectuer une seconde liaison, cette fois avec le nom distinctif de l'utilisateur (extrait par la recherche) et le mot de passe indiqué pendant la procédure de connexion. Si la seconde tentative de liaison aboutit, la partie authentification est validée et les informations d'appartenance de l'utilisateur à des groupes sont extraites et comparées aux groupes configurés localement sur IMM. Les groupes concordants définissent les droits affectés à l'utilisateur. • With login credentials (Avec données d'identification de connexion) : La liaison initiale avec le serveur du contrôleur de domaine est effectuée à l'aide des données d'identification soumises lors de la procédure de connexion. Si cette liaison échoue, la procédure d'authentification échoue également. Si la liaison aboutit, une recherche tente de trouver un enregistrement d'utilisateur. Une fois localisées, les informations d'appartenance de l'utilisateur à des groupes sont extraites et comparées aux groupes configurés localement sur IMM. Les groupes concordants définissent les droits affectés à l'utilisateur. • Anonymously (anonyme): La liaison initiale avec le serveur du contrôleur de domaine est effectuée sans nom distinctif (DN), ni mot de passe. Cette option est déconseillée car la plupart des serveurs sont configurés pour interdire des demandes de recherche sur des enregistrements d'utilisateur spécifiques.

Profils de groupe pour utilisateurs Active Directory

Les profils de groupe sont configurés afin de fournir des spécifications d'autorisation locale pour des groupes d'utilisateurs. Chaque profil de groupe inclut des autorisations exprimées sous forme de Niveau d'autorisation (Rôles), exactement comme dans les profils de connexion. Pour configurer des profils de groupe, les utilisateurs doivent disposer de l'autorisation de gestion de comptes utilisateurs. Pour associer des utilisateurs aux profils de groupe, des serveurs d'authentification LDAP sont requis.

Liste des profils de groupe

Vous pouvez accéder à cette liste en cliquant sur **IMM Control** > **Login Profiles**. L'ID du groupe et le récapitulatif de ses rôles est affiché pour chaque profil de groupe (comme pour les profils de connexion). Depuis cette liste, vous pouvez ajouter de nouveaux groupes et sélectionner des groupes existants pour les modifier ou les supprimer.

La figure suivante présente la fenêtre Group Profiles for Active Directory Users.

Pour modifier un profil de groupe, cliquez sur **Edit**. Une page Group Profile s'affiche pour ce groupe. Pour supprimer un profil de groupe, cliquez sur **Delete**. Vous êtes invité à confirmer la suppression du profil de groupe. Pour ajouter un nouveau profil de groupe, cliquez sur le lien **Add a group**. Une page Group Profile s'ouvre pour y entrer les informations sur le nouveau profil de groupe. Vous pouvez ajouter au maximum 16 profils de groupe. les noms des profils de groupe n'ont pas besoin d'être uniques.

Le tableau suivant décrit les zones de la page Group Profile.

Tableau 11. Informations sur les profils de groupe

Zone	Option	Description
Group ID		Cette zone permet de spécifier l'ID de groupe du profil de groupe. Cette zone peut contenir au maximum 63 caractères. L'ID du groupe doit être identique à celui de ses homologues sur les serveurs LDAP. Exemples de noms de groupe : IMM Admin Group and IMM/Robert.
Role		Sélectionnez les rôles (Niveaux d'autorisation) associés à cet ID de connexion et transférez-les vers le cadre **Assigned roles**. Vous pouvez utiliser la touche Entrée ou un clic sur la souris pour transférer les éléments sélectionnés d'un cadre à l'autre.
	Supervisor	Aucune restriction n'affecte l'utilisateur hormis la portée qui lui est affectée.

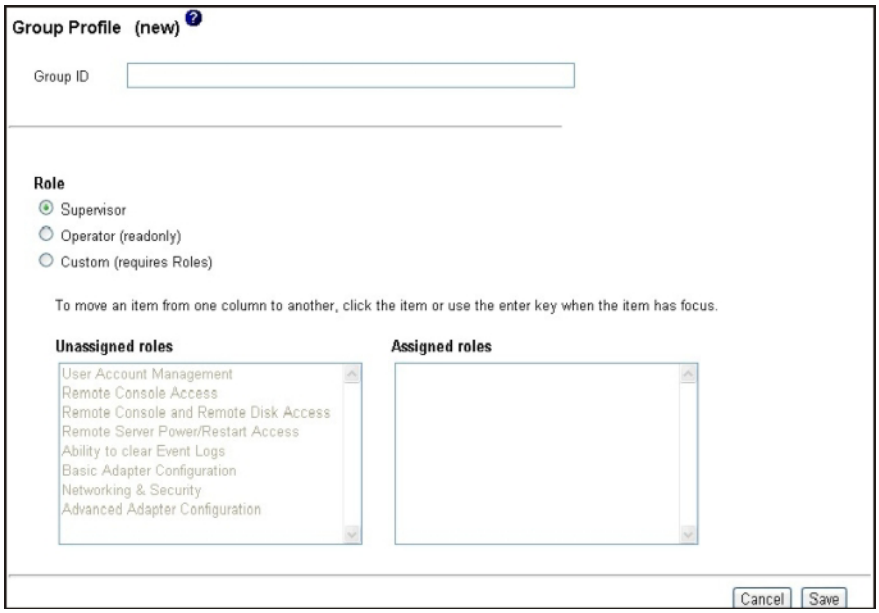
Tableau 11. Informations sur les profils de groupe (suite)

Zone	Option	Description
	Operator	L'utilisateur ne dispose que d'une autorisation d'accès en lecture seule et ne peut effectuer aucune modification (par exemple, enregistrement, édition ou effacement). Ces restrictions concernent également les opérations débouchant sur un changement d'état comme le redémarrage d'IMM, la restauration des paramètres par défaut ou la mise à niveau du microprogramme.
Role	Custom	Des restrictions peuvent affecter, ou non, l'utilisateur selon le niveau d'autorisation personnalisé qui lui a été octroyé. Si vous optez pour Custom, vous devez sélectionner un ou plusieurs des niveaux d'autorisation suivants : • Networking and Security – L'utilisateur est habilité à modifier la configuration dans les panneaux Security, Network Protocols, Network Interface, Port Assignments et Serial Port. • User account management – L'utilisateur peut ajouter, modifier ou supprimer des utilisateurs, tout comme modifier les paramètres de connexion globaux (Global Login) dans le panneau Login Profiles. • Remote Console Access – Les utilisateurs peuvent accéder à la console du serveur distant. • Remote Console and Remote Disk Access – L'utilisateur peut accéder à la console du serveur distant et aux fonctions de disque distant pour le serveur distant. • Remote Server Power/Restart Access – L'utilisateur peut accéder aux fonctions d'alimentation, de redémarrage et de délai d'attente du serveur distant. • Basic Adapter Configuration – L'utilisateur peut modifier les paramètres de configuration sur les panneaux System Settings (hormis les paramètres Contact, Location et Server Timeouts) et Alerts. • Ability to Clear Event Logs – L'utilisateur peut effacer les journaux d'événements. **Remarque :** Tous les utilisateurs peuvent consulter les journaux d'événements, mais cette autorisation est requise pour pouvoir les effacer.

Tableau 11. Informations sur les profils de groupe (suite)

Zone	Option	Description
		• Advanced Adapter Configuration – L'utilisateur n'est pas soumis à des restrictions lors de la configuration de l'adaptateur et dispose de droits d'administration sur le module IMM. L'utilisateur peut exécuter les fonctions avancées suivantes : mises à jour de microprogramme, amorçage réseau PXE, restauration des paramètres usine par défaut de l'adaptateur, modification et restauration de la configuration de l'adaptateur depuis un fichier de configuration et redémarrage/réinitialisation de l'adaptateur. **Remarque :** Ce niveau d'autorisation exclut les fonctions de contrôle de l'alimentation, du redémarrage et du délai d'attente du serveur.
Remarque : Pour éviter une situation où aucun utilisateur n'aurait d'accès en lecture/écriture, le profil de connexion numéro 1 devrait être défini avec au moins la capacité de modifier les profils de connexion. Cet utilisateur doit bénéficier d'un accès de type Superviseur ou Gestion de comptes utilisateur. Ceci garantit qu'au moins u utilisateur puisse effectuer des actions, apporter des modifications à la configuration et ajouter des utilisateurs aux profils de connexion pouvant eux-aussi effectuer des actions et modifier la configuration.		

La figure suivante présente la fenêtre Group Profile.



Authentification et autorisation Active Directory basée rôle

Vous pouvez configurer l'authentification et l'autorisation distante LDAP d'utilisateurs à l'aide d'Active Directory.

Remarques :

- L'authentification et l'autorisation Active Directory basée rôle ne s'applique qu'à un serveur utilisé dans un environnement Active Directory.
- L'outil optimisé Security Snap-in basé rôle est requis pour l'authentification et l'autorisation Active Directory basée rôle.

L'authentification et l'autorisation Active Directory basée rôle utilise les informations de configuration stockées sur un serveur Active Directory pour authentifier un utilisateur, puis lui associer des permissions. Avant d'utiliser l'authentification et l'autorisation Active Directory basée rôle, utilisez l'outil optimisé Security Snap-in basé rôle pour stocker les informations de configuration sur le serveur Active Directory devant associer des permissions aux utilisateurs. Cet outil opère sur n'importe quel client Microsoft Windows et peut être téléchargé depuis le site http://www.ibm.com/systems/support/.

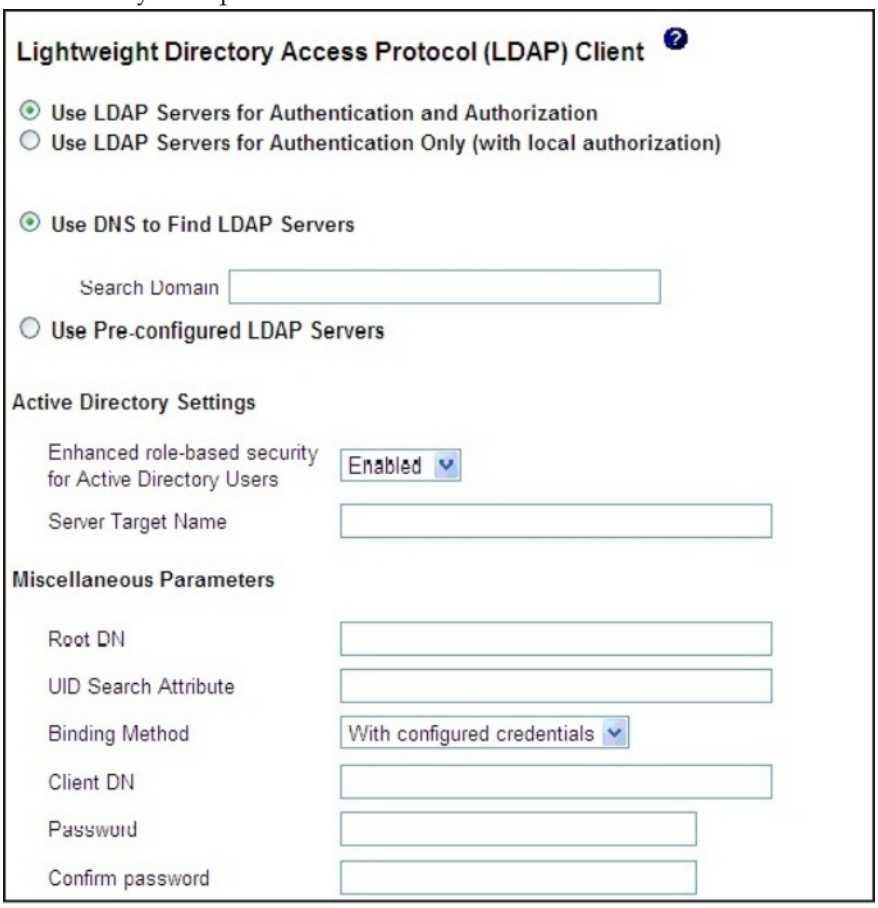
L'outil optimisé Security Snap-in basé rôle vous permet de configurer des rôles sur un serveur Active Directory et d'associer le module IMM, des utilisateurs et des groupes à ces rôles. Pour obtenir des informations et des instructions, reportez-vous à la documentation de l'outil Enhanced role-based Based Security Snap-in. Les rôles identifient les permissions octroyées aux utilisateurs et aux groupes, ainsi que les cibles de commandes, comme IMM ou un serveur lame, auxquelles un rôle est rattaché. Avant d'activer l'authentification et l'autorisation par rôle d'Active Directory, vous devez configurer des rôles sur le serveur Active Directory.

Le nom facultatif défini dans la zone **Server Target Name** identifie un module IMM spécifique et peut être associé à un ou plusieurs rôles sur le serveur Active Directory via l'outil Security Snap-In basé rôle. Ceci est réalisé en créant des cibles gérées, en affectant à ces cibles des noms spécifiques et en associant ces cibles aux rôles appropriés. Si un nom de serveur cible (Server Target Name) est configuré, il peut définir des rôles spécifiques pour les utilisateurs et les cibles IMM membres du même rôle. Lorsqu'un utilisateur se connecte à IMM et est authentifié via Active Directory, les rôles de cet utilisateur sont extraits de l'annuaire. Les autorisations attribuées à l'utilisateur sont extraites des rôles avec une cible membre dont le nom correspond à ce module IMM, ou avec une cible correspondant à un module IMM quelconque. Le module IMM peut avoir un nom unique ou plusieurs modules IMM peuvent partager le même nom de cible. Le fait d'affecter plusieurs modules IMM au même nom de cible permet de les regrouper et de les affecter au même rôle.

Pour configurer l'authentification et l'autorisation Active Directory basée rôle pour le module IMM, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Network Protocols**.
2. Accédez à la section **Lightweight Directory Access Protocol (LDAP) Client**.
3. Sélectionnez **Use LDAP Servers for Authentication and Authorization**.
4. Sélectionnez **Enabled** pour la zone **Enhanced role-based security for Active Directory Users**.
5. Sélectionnez l'une des options suivantes pour configurer manuellement ou reconnaître dynamiquement les contrôleurs de domaine :
   - Sélectionnez **Use DNS to find LDAP Servers** pour détecter dynamiquement les contrôleurs de domaine d'après les enregistrements SVR DNS.
   - Sélectionnez **Use Pre-Configured LDAP Servers** (sélection par défaut) pour configurer manuellement les contrôleurs de domaine.
6. Si vous utilisez DNS pour détecter les contrôleurs de domaine de manière dynamique, configurez le nom de domaine du contrôleur, puis passez à l'étape 8, à la page 75. Vous devez spécifier le nom de domaine complet du contrôleur de domaine. Entrez le nom de domaine du contrôleur de domaine dans la zone **Search Domain**.

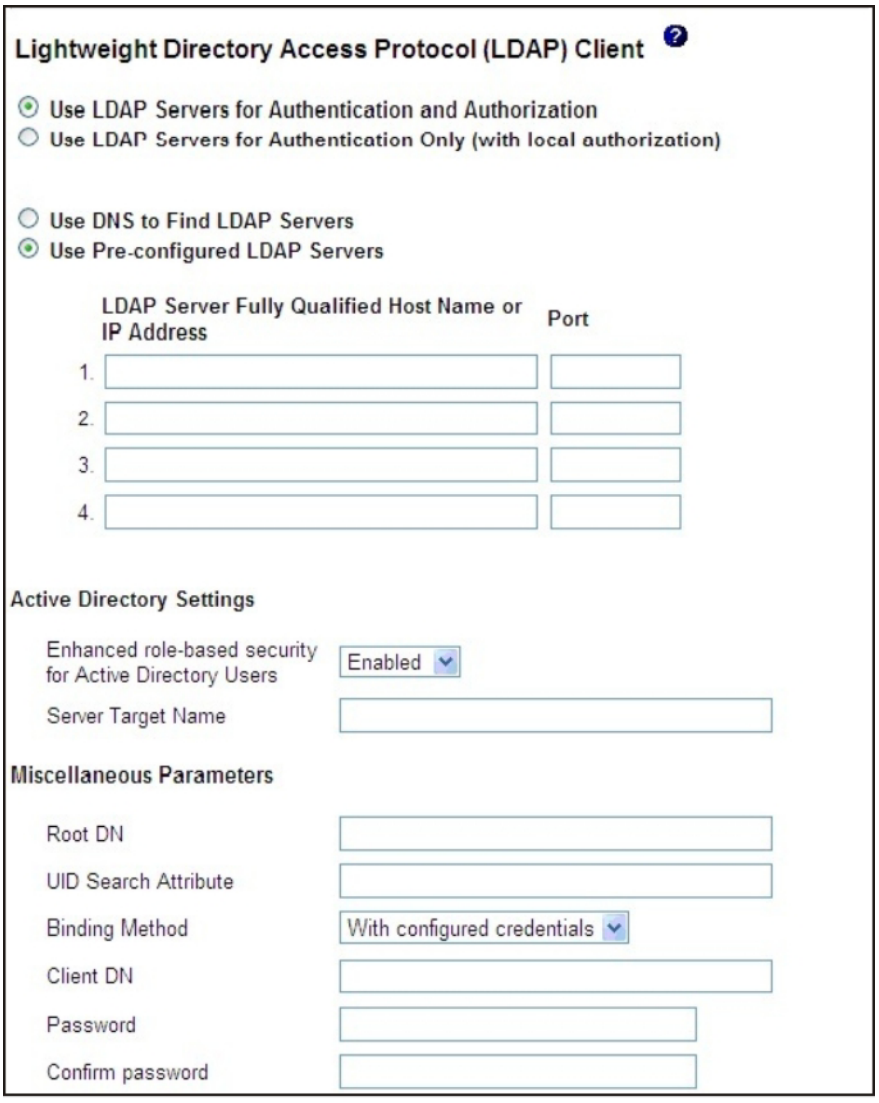
La figure suivante présente la fenêtre LDAP Client lorsque DNS est utilisé pour détection dynamique des contrôleurs de domaine.



7. Si vous configurez manuellement les contrôleurs de domaine, configurez les zones **LDAP Server Host Name or IP Address** and **Port**.

   Remarque : Vous pouvez configurer jusqu'à quatre contrôleurs de domaine en utilisant une adresse IP ou un nom d'hôte complet.

La figure suivante présente la fenêtre LDAP Client lorsque vous configurez manuellement les contrôleurs de domaine.



8. Configurez les paramètres Active Directory Settings en sélectionnant **Enabled** dans le menu **Enhanced role-based security for Active Directory Users**.
9. Configurez la section Miscellaneous Parameters. Reportez-vous au tableau suivant pour plus d'informations sur ces paramètres.

Tableau 12. Paramètres divers

Zone	Description	Option
Root DN	IMM utilise la zone **Root DN** au format DN comme entrée racine de l'arborescence. Cette valeur DN sera utilisée comme objet de base pour toutes les recherches. Exemple : `dc=mycompany,dc=com`.	

Tableau 12. Paramètres divers (suite)

Zone	Description	Option
Binding method	La zone **Binding Method** (Méthode de liaison) est utilisée pour les liaisons initiales au serveur du contrôleur de domaine. Sélectionnez une option.	• Anonymously (anonyme): La liaison initiale avec le serveur du contrôleur de domaine est effectuée sans nom distinctif (DN), ni mot de passe. Cette option est déconseillée car la plupart des serveurs sont configurés pour interdire des demandes de recherche sur des enregistrements d'utilisateur spécifiques. • With configured credentials (Avec données d'identification configurées) : Entrez le nom distinctif et le mot de passe de l'utilisateur à utiliser pour la liaison initiale. • With login credentials (Avec données d'identification de connexion) : La liaison initiale avec le serveur du contrôleur de domaine est effectuée à l'aide des données d'identification soumises lors de la procédure de connexion. L'ID utilisateur peut être fourni en indiquant une valeur DN (nom distinctif), une valeur DN partielle, un nom de domaine complet, ou un ID utilisateur correspondant à la zone **UID Search Attribute** configurée sur le module IMM. Si les données d'identification ressemblent à un nom distinctif partiel (par exemple, `cn=joe`), celui-ci sera apposé en préfixe au nom distinctif racine configuré afin de tenter de créer un nom distinctif correspondant à l'enregistrement de l'utilisateur. Si la tentative de liaison échoue, une tentative finale sera effectuée en ajoutant le préfixe `cn=` aux données d'identification de connexion, puis en ajoutant la chaîne résultante au nom distinctif racine configuré.

Modèle d'authentification et d'autorisation LDAP existant

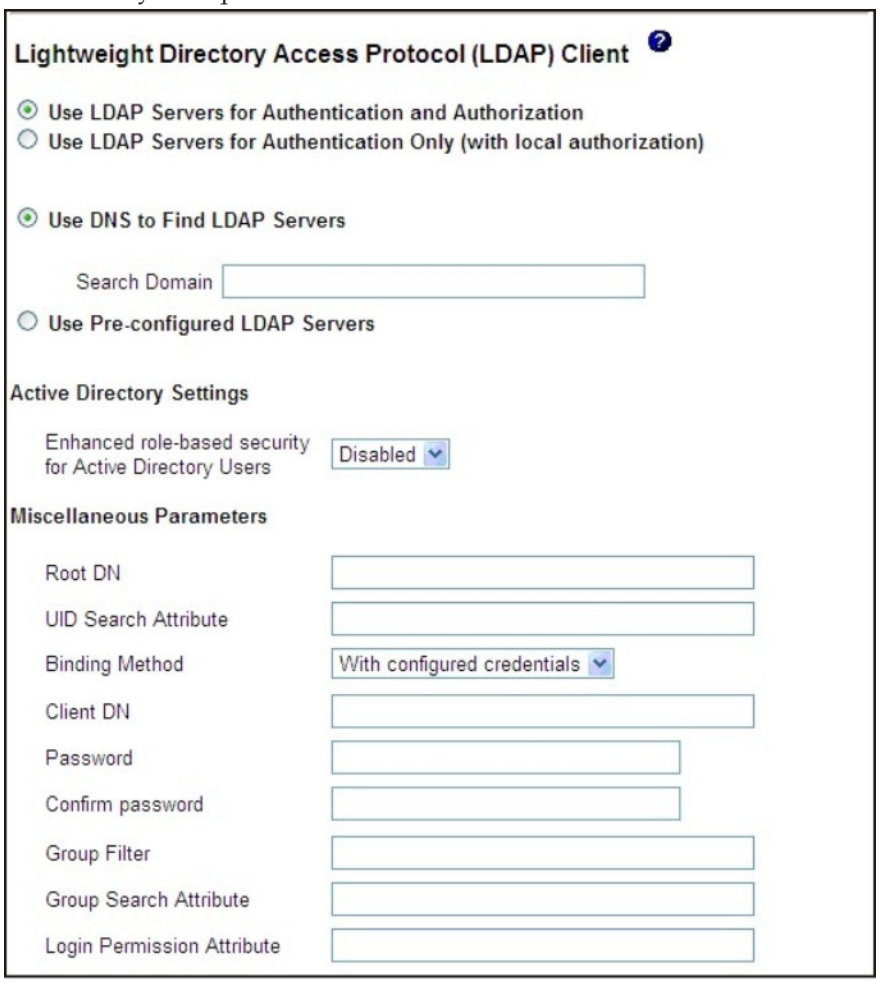
L'authentification et autorisation LDAP héritée constitue le modèle original utilisé avec le module IMM. L'authentification et autorisation LDAP héritée prend en charge les environnements Active Directory, Novell eDirectory, OpenLDAP, et s'appuie sur les informations de configuration stockées sur un serveur LDAP pour associer des autorisations à un utilisateur. L'authentification et autorisation LDAP héritée est utilisée pour authentifier et autoriser des utilisateurs via un serveur LDAP. Si l'option Enhanced Role-based Security for Active Directory Users est désactivée sur un module IMM, il vous est permis de configurer les attributs de recherche LDAP pour le module IMM.

Pour configurer l'authentification et autorisation LDAP héritée pour le module IMM, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Network Protocols**.
2. Accédez à la section **Lightweight Directory Access Protocol (LDAP) Client**.
3. Sélectionnez **Use LDAP Servers for Authentication and Authorization**.
4. Sélectionnez **Disabled** pour la zone **Enhanced role-based security for Active Directory Users**.
5. Sélectionnez l'une des options suivantes pour configurer manuellement ou reconnaître dynamiquement les serveurs LDAP à utiliser pour l'authentification :
   - Sélectionnez **Use DNS to find LDAP Servers** pour détecter dynamiquement les serveurs LDAP d'après les enregistrements SVR DNS.
   - Sélectionnez **Use Pre-Configured LDAP Servers** (sélection par défaut) pour configurer manuellement les serveurs LDAP.
6. Si vous utilisez DNS pour détecter dynamiquement les serveurs LDAP, configurez le nom de domaine du serveur LDAP, puis passez à l'étape 8, à la page 78

page 78. Vous devez spécifier le nom de domaine complet du serveur LDAP. Entrez le nom de domaine du serveur LDAP dans la zone **Search Domain**.

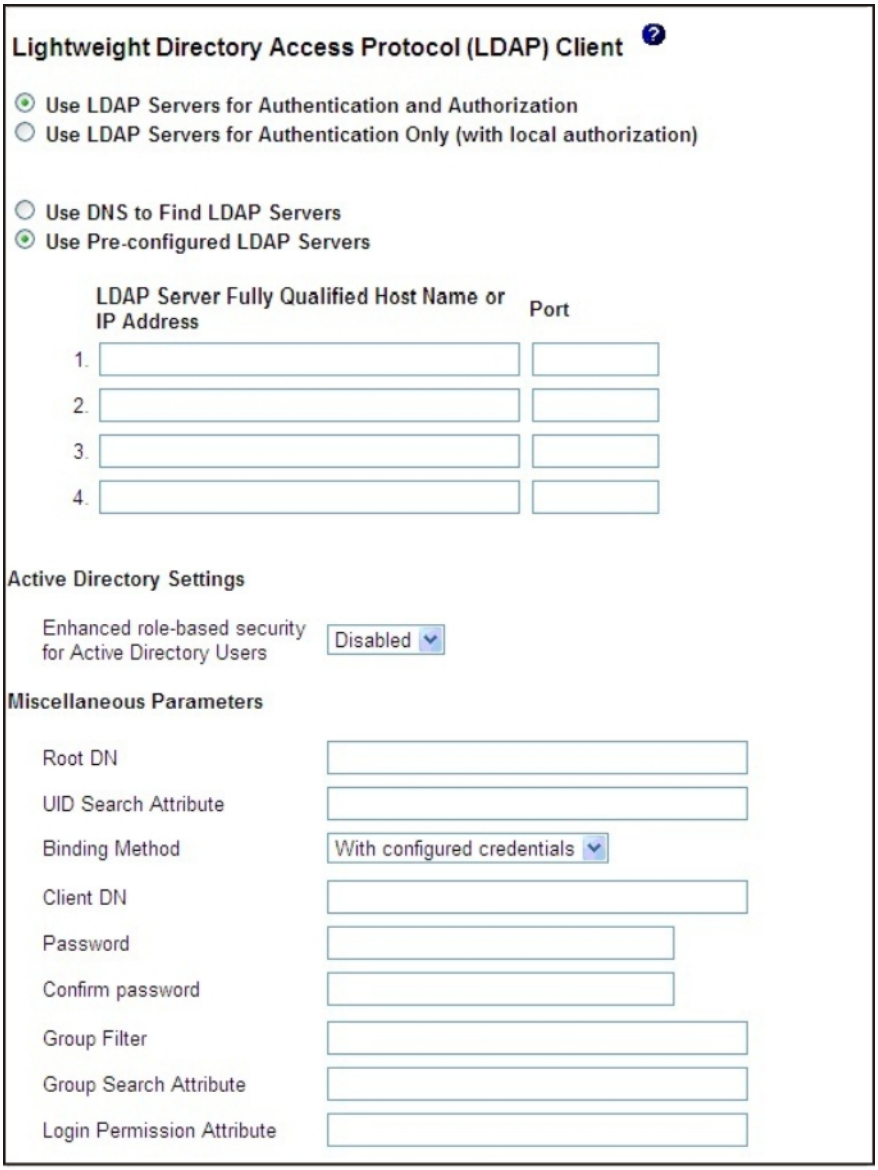
La figure suivante présente la fenêtre LDAP Client lorsque DNS est utilisé pour détection dynamique des serveurs LDAP.



7. Si vous configurez manuellement les serveurs LDAP, configurez les zones **LDAP Server Host Name or IP Address** et **Port**, puis passez à l'étape 8, à la page 78.

   Remarque : Vous pouvez configurer jusqu'à quatre serveurs LDAP en utilisant une adresse IP ou un nom d'hôte complet.

La figure suivante présente la fenêtre LDAP Client lorsque vous configurez manuellement les serveurs LDAP.



8. Configurez les paramètres Active Directory Settings en sélectionnant **Disabled** dans le menu **Enhanced role-based security for Active Directory Users**.
9. Configurez la section Miscellaneous Parameters. Reportez-vous à la liste suivante pour obtenir une description des zones de paramètres requis.
   - IMM utilise la zone **Root DN** au format DN comme entrée racine de l'arborescence. Cette valeur DN sera utilisée comme objet de base pour toutes les recherches. Exemple : `dc=mycompany,dc=com`.
   - La zone **Binding Method** (Méthode de liaison) est utilisée pour les liaisons initiales au serveur du contrôleur de domaine. Sélectionnez l'une des options de liaison suivantes :
     - Anonymously (anonyme):

       La liaison initiale avec le serveur du contrôleur de domaine est effectuée sans nom distinctif (DN), ni mot de passe. Cette option est déconseillée car la plupart des serveurs sont configurés pour interdire des demandes de recherche sur des enregistrements d'utilisateur spécifiques.

– With configured credentials (Avec données d'identification configurées) :

  Entrez le nom distinctif et le mot de passe de l'utilisateur à utiliser pour la liaison initiale.

– With login credentials (Avec données d'identification de connexion) :

  Liaison avec les données d'identification fournies pendant le processus de connexion. L'ID utilisateur peut être fourni en indiquant une valeur DN (nom distinctif), une valeur DN partielle, un nom de domaine complet, ou un ID utilisateur correspondant aux informations de la zone **UID Search Attribute** configurée sur le module IMM. Si les données d'identification ressemblent à un nom distinctif partiel (par exemple, `cn=joe`), celui-ci sera apposé en préfixe au nom distinctif racine configuré afin de tenter de créer un nom distinctif correspondant à l'enregistrement de l'utilisateur. Si la tentative de liaison échoue, une tentative finale sera effectuée en ajoutant le préfixe `cn=` aux données d'identification de connexion, puis en ajoutant la chaîne résultante au nom distinctif racine configuré.

- La zone **Group Filter** est utilisée pour l'authentification des groupes. Elle spécifie le groupe auquel appartient le module IMM. Si le filtre de groupe est laissé vide, l'authentification de groupe réussit automatiquement. L'authentification de groupe, si elle est activée, est effectuée après l'authentification de l'utilisateur. Le système tente de déterminer si au moins un groupe dans le filtre de groupes correspond à un groupe dont l'utilisateur fait partie. S'il n'y a pas de groupe concordant, l'authentification de l'utilisateur échoue et l'accès est refusé. Si au moins une concordance est trouvée, l'authentification de groupe aboutit. Les comparaisons sont sensibles à la casse.

  Lorsque l'authentification de groupe est désactivée, l'enregistrement personnel de l'utilisateur doit contenir l'attribut d'autorisation, faute de quoi l'accès sera refusé. Pour chaque groupe correspondant au filtre, les permissions associées à ce groupe sont attribuées à l'utilisateur. Les permissions associées à un groupe sont obtenues en extrayant les informations de la zone **Login Permission Attribute**.

  Le filtre est limité à 511 caractères, et se compose d'un ou plusieurs noms de groupe. Le signe deux-points (:) doit être utilisé pour spécifier plusieurs noms de groupes. Les espaces de début et de fin sont ignorés. Tous les autres espaces sont traités comme faisant partie du nom du groupe. Un nom de groupe peut être spécifié en utilisant un nom distinctif complet ou seulement la portion *cn*. Par exemple, un groupe dont le nom distinctif est `cn=adminGroup,dc=mycompany,dc=com` peut être spécifié en utilisant ce nom distinctif ou seulement adminGroup.

  Remarque : L'astérisque (*) utilisé auparavant n'est plus traité comme un caractère générique. Le concept de caractère générique a été supprimé pour des raisons de sécurité.

- La zone **Group Search Attribute** est utilisée par l'algorithme de recherche pour rechercher les informations d'appartenance d'un utilisateur spécifique à un groupe. Lorsque le nom du filtre de groupe est configuré, la liste des groupes auxquels l'utilisateur appartient doit être extraite du serveur LDAP. Cette liste est requise pour effectuer l'authentification de groupe. Pour extraire cette liste, le filtre de recherche envoyé au serveur LDAP doit spécifier le nom d'attribut associé aux groupes. La zone **Group Search Attribute** spécifie le nom d'attribut.

  Dans un environnement Active Directory ou Novell eDirectory, la zone **Group Search Attribute** spécifie le nom d'attribut qui identifie les groupes auxquels appartient un utilisateur. Dans Active Directory, l'attribut

memberOf est utilisé et dans Novell eDirectory, l'attribut **groupMembership**. Dans un environnement de serveur OpenLDAP, les utilisateurs sont généralement affectés aux groupes pour lesquels objectClass correspond à PosixGroup. Dans ce contexte, le paramètre Group Search Attribute spécifie le nom d'attribut qui identifie les membres d'un PosixGroup spécifique. Il s'agit généralement de l'attribut **memberUid**. Si la zone **Group Search Attribute** est laissée vide, le nom d'attribut dans le filtre reçoit par défaut la valeur **memberOf**.

- La zone **Login Permission Attribute** spécifie le nom d'attribut associé aux autorisations de connexion de l'utilisateur. Lorsque l'authentification d'un utilisateur aboutit avec un serveur LDAP, il est nécessaire d'extraire les autorisations de connexion de l'utilisateur.

  Remarque : La zone **Login Permission Attribute** ne doit pas être laissée vide, sans quoi il est impossible d'extraire les autorisations de l'utilisateur. Sans droits vérifiés, la tentative de connexion échoue.

  La valeur d'attribut renvoyée par le serveur LDAP est recherchée via la chaîne de mot clé `IBMRBSPermissions=`. Ce mot clé doit être immédiatement suivi par une chaîne de bits (jusqu'à 12 occurrences consécutives de 0 ou de 1). Chaque bit correspond à un ensemble spécifique de fonctions. Les bits sont numérotés selon leur position. Le bit le plus à gauche correspond à la position 0 et celui le plus à droite, à la position 11. Une valeur 1 à une position donnée active la fonction correspondante. Une valeur 0 désactive cette fonction. La chaîne `IBMRBSPermissions=010000000000` est un exemple.

  Le mot clé `IBMRBSPermissions=` peut être placé n'importe où dans la zone **Login Permission Attribute**. Ceci permet à l'administrateur LDAP de réutiliser un attribut existant, évitant ainsi une extension du schéma LDAP et permettant d'utiliser l'attribut pour sa fonction initiale. L'utilisateur peut maintenant ajouter la chaîne de mot clé au début, à la fin, ou à n'importe quel emplacement dans cette zone. L'attribut utilisé permet une chaîne au format libre.

  Le tableau suivant fournit une explication de chaque position de bit.

Tableau 13. Bits d'autorisation

Position de bit	Fonction	Explication
0	Refuser toujours	S'il est utilisé, l'authentification de l'utilisateur échoue toujours. Cette fonction peut être utilisée pour bloquer un ou plusieurs utilisateurs associés à un groupe spécifique.
1	Accès superviseur	S'il est utilisé, les privilèges administrateur sont octroyés à l'utilisateur. L'utilisateur dispose d'un accès en lecture et écriture à chaque fonction. Si vous définissez ce bit, vous n'avez pas à définir individuellement les autres.

Tableau 13. Bits d'autorisation (suite)

Position de bit	Fonction	Explication
2	Accès en lecture seule	S'il est défini, l'utilisateur dispose d'un accès en lecture seule et ne peut pas exécuter de procédures de maintenance (par exemple, un redémarrage, des actions à distance ou des mises à jour de microprogramme). Il ne peut rien modifier à l'aide des fonctions d'enregistrement, d'effacement ou de restauration. La position de bit 2 et tous les autres bits s'excluent mutuellement, la position de bit 2 étant celle avec la plus faible priorité. Si un autre bit est défini, ce bit sera ignoré.
3	Réseau et sécurité	S'il est défini, un utilisateur peut modifier la configuration dans les panneaux Security, Network Protocols, Network Interface, Port Assignments et Serial Port.
4	Gestion des comptes utilisateur	S'il est défini, un utilisateur peut ajouter, modifier ou supprimer des utilisateurs et changer les paramètres connexion globaux dans le panneau Login Profiles.
5	Accès à la console distante	S'il est défini, un utilisateur peut accéder à la console du serveur distant et modifier la configuration dans le panneau Serial Port.
6	Accès à la console distante et au disque distant	S'il est défini, un utilisateur peut accéder à la console du serveur distant et aux fonctions de disque distant pour le serveur distant . L'utilisateur peut également modifier la configuration dans le panneau Serial Port.
7	Accès aux fonctions d'alimentation/de redémarrage du serveur distant	S'il est défini, un utilisateur peut accéder aux fonctions d'alimentation, de redémarrage et de délai d'attente du serveur distant.
8	Configuration de base de l'adaptateur	S'il est défini, un utilisateur peut modifier les paramètres de configuration dans les panneaux System Settings et Alerts (à l'exception des paramètres Contact, Location et Server Timeout).
9	Possibilité d'effacer les journaux d'événements	S'il est défini, un utilisateur peut effacer les journaux d'événements. **Remarque :** Tous les utilisateurs peuvent afficher les journaux des événements mais ce niveau d'autorisation est requis pour pouvoir effacer leur contenu.

Tableau 13. Bits d'autorisation (suite)

Position de bit	Fonction	Explication
10	Configuration avancée d'adaptateur	S'il est défini, l'utilisateur n'est pas soumis à des restrictions lors de la configuration de l'adaptateur et dispose de droits d'administration sur le module IMM. L'utilisateur peut exécuter les fonctions avancées suivantes : mises à jour de microprogramme, amorçage réseau PXE, restauration des paramètres usine par défaut de l'adaptateur, modification et restauration de la configuration de l'adaptateur depuis un fichier de configuration et redémarrage/réinitialisation de l'adaptateur. Ceci exclut les fonctions de contrôle/redémarrage et de délai d'attente du serveur.
11	Réservé	Cette position de bit est réservée pour un usage ultérieur (actuellement ignorée).

Remarques :

- Si des bits ne sont pas utilisés, leur valeur par défaut pour l'utilisateur sera définie pour lecture seule.
- Les autorisations de connexion extraites directement de l'enregistrement utilisateur sont prioritaires. Si l'enregistrement utilisateur ne contient pas de nom dans la zone **Login Permission Attribute**, le système tente d'extraire les autorisations du groupe auquel appartient l'utilisateur et qui correspondent au filtre de groupe. Dans ce cas, l'utilisateur reçoit l'opérateur inclusif OR de tous les bits pour tous les groupes.
- Si le bit de position 0 (Refuser toujours) est défini pour l'un des groupes, l'accès est refusé à l'utilisateur. Ce bit prévaut toujours sur les autres.
- Si un utilisateur a la possibilité de modifier les paramètres de configuration de base, de réseau ou de sécurité de l'adaptateur, vous devriez envisager de l'autoriser à redémarrer le module IMM (bit de position 10). Sans cette possibilité, l'utilisateur pourra modifier un paramètre mais sans que cette modification n'entre en vigueur.

Configuration de la sécurité

Vous pouvez utiliser la procédure générale de cette section pour configurer la sécurité du chiffrement de données sensibles, le serveur Web d'IMM, la connexion entre le module IMM et IBM Systems Director, la connexion entre le module IMM et un serveur LDAP et la gestion cryptographique. Si vous ne savez pas comment utiliser les certificats SSL, lisez les informations de la rubrique «Certificat SSL», à la page 85.

Pour configurer la sécurité du module IMM, procédez comme suit.

1. Configuration du chiffrement de données sensibles :
   a. Dans le panneau de navigation, cliquez sur **Security**. Faites défiler jusqu'à la section **Enable Data Encryption** et sélectionnez **Enable** pour activer le chiffrement de données. Pour désactiver le chiffrement de données, sélectionnez **Disable**.

2. Configuration du serveur Web sécurisé :
   a. Dans le panneau de navigation, cliquez sur **Security**. Faites défiler jusqu'à la section **HTTPS Server Configuration for Web Server** et sélectionnez **Disable** pour désactiver le serveur SSL.
   b. Pour générer ou importer un certificat, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **HTTPS Server Certificate Management**. Pour plus d'informations sur la gestion des certificats, voir «Gestion du certificat du serveur SSL», à la page 85.
   c. Pour activer le serveur SSL, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **HTTPS Server Configuration for Web Server**. Pour plus d'informations sur l'activation SSL, voir «Activation de SSL pour le serveur Web sécurisé ou pour IBM Systems Director over HTTPS», à la page 89.
3. Configuration de la connexion IBM Systems Director :
   a. Pour désactiver le paramètre **Systems Director over HTTPS**, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **IBM Systems Director over HTTPS Server Configuration**.
   b. Pour générer ou importer un certificat, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **IBM Systems Director over HTTPS Server Certificate Management**. Pour plus d'informations, voir «Gestion du certificat du serveur SSL», à la page 85.
   c. Pour activer le serveur SSL, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **IBM Systems Director over HTTPS Server Configuration**. Pour plus d'informations sur l'activation SSL, voir «Activation de SSL pour le serveur Web sécurisé ou pour IBM Systems Director over HTTPS», à la page 89.
4. Configurez la sécurité SSL pour les connexions LDAP :
   a. Pour désactiver le client SSL, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **SSL Client Configuration for LDAP Client**.
   b. Pour générer ou importer un certificat, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **SSL Client Certificate Management**. Pour plus d'informations, voir «Gestion du certificat du serveur SSL», à la page 85.
   c. Pour importer un ou plusieurs certificats de confiance, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **SSL Client Trusted Certificate Management**. Pour plus d'informations, voir SSL client trusted certificate management.
   d. Pour activer le client SSL, cliquez sur **Security** dans le panneau de navigation et faites défiler jusqu'à la section **SSL Client Configuration for LDAP Client**. Pour plus d'informations, voir «Activation de SSL pour le serveur Web sécurisé ou pour IBM Systems Director over HTTPS», à la page 89.
5. Configuration de la gestion cryptographique :
   a. Dans le panneau de navigation, cliquez sur **Security** et faites défiler jusqu'à la section **Cryptography Management**. Sélectionnez **Basic Compatible Mode**.
   b. Dans le panneau de navigation, cliquez sur **Security** et faites défiler jusqu'à la section **Cryptography Management**. Sélectionnez **High Security Mode**.
6. Redémarrez le module IMM pour que les modifications de la configuration du serveur SSL entrent en vigueur. Pour plus d'informations, voir «Redémarrage d'IMM», à la page 96.

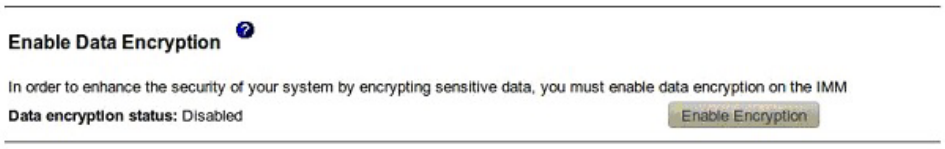
Remarque : Les modifications concernant le chiffrement de données et la configuration du client SSL prennent effet immédiatement et ne nécessitent pas un redémarrage d'IMM.

Activation du chiffrement de données

Par défaut, les données sensibles sont enregistrées sans chiffrement pour rester compatible avec la version précédente. Pour accoître la sécurité de votre système, vous devez activer le chiffrement de données sur IMM.

Pour activer le chiffrement de données, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Security**.



2. Cliquez sur **Enable Encryption** pour activer le chiffrement de données.

   Remarque :

   - Si vous devez rétromigrer le microprogramme IMM version 1.42 à une version précédente, qui ne fournit de chiffrement de données, vous devez désactiver d'abord le chiffrement de données. Si vous ne le désactivez pas, les informations relatives au compte seront perdues.
   - Si vous souhaitez désactivez le chiffrement de données ultérieurement, sélectionnez **Disable Encryption**.

Sécuriser le serveur Web, IBM Systems Director et LDAP

SSL (Secure Sockets Layer) est un protocole de sécurité assurant la confidentialité des communications. SSL permet aux applications serveur client de communiquer en empêchant les écoutes, la contrefaçon et la falsification des messages.

Vous pouvez configurer IMM afin d'utiliser la prise en charge SSL sur deux types de connexions : le serveur Web sécurisé (HTTPS) et la connexion LDAP sécurisée (LDAPS). Selon le type de connexion, le module IMM remplit le rôle de client SSL ou de serveur SSL.

Le tableau suivant indique les fonctions du module IMM pour les connexions de serveur Web et LDAP sécurisées.

Tableau 14. Prise en charge de connexion SSL par IMM

Type de connexion	Client SSL	Serveur SSL
Serveur Web sécurisé (HTTPS)	Navigateur Web (Exemple : Microsoft Internet Explorer)	Serveur Web IMM
Connexion IBM Systems Director sécurisée	IBM Systems Director	Serveur IMM Systems Director
Connexion LDAP sécurisée (LDAPS)	Client LDAP IMM	Serveur LDAP

Vous pouvez afficher ou modifier les paramètres SSL depuis la page Security, y compris activer ou désactiver SSL et gérer les certificats requis pour SSL.

Certificat SSL

Vous pouvez utiliser SSL avec un certificat autosigné ou un certificat signé par une autorité de certification tierce.

Le certificat d'auto-signature représente la méthode la plus simple pour utiliser SSL mais il soulève un risque de sécurité. Lorsque vous l'utilisez, le client SSL n'a aucun moyen de valider l'identité du serveur SSL lors de la première tentative de connexion entre le client et le serveur. En effet, un tiers peut usurper l'identité du serveur pour intercepter les données échangées entre IMM et le navigateur web. Si le certificat autosigné est importé dans le magasin de certificats du navigateur lors de la première connexion entre le navigateur et IMM, toutes les communications futures avec le navigateur seront sécurisées ; sous réserve que la première connexion n'a pas été compromise par une attaque.

Pour une sécurité accrue, vous pouvez utiliser un certificat signé par une autorité de certification. Pour obtenir un certificat signé, utilisez la page SSL Certificate Management afin de générer une demande de signature de certificat. Vous devez envoyer cette demande à une autorité de certification et convenir avec celle-ci de sa délivrance. Après réception du certificat, vous pouvez l'importer dans IMM en cliquant sur le lien **Import a Signed Certificate** puis activer la connexion SSL.

La fonction de l'autorité de certification est de vérifier l'identité du module IMM. Le certificat contient les signatures numériques de l'autorité de certification et du module IMM. Si une autorité de certification connue émet le certificat ou si le certificat de l'autorité de certification a déjà été importé dans le navigateur Web, le navigateur peut valider le certificat et identifier de manière catégorique le serveur Web IMM.

IMM requiert un certificat pour le serveur Web sécurisé et un autre pour le client LDAP sécurisé. De même, le client LDAP sécurisé requiert un ou plusieurs certificats de confiance. Le certificat de confiance est utilisé par le client LDAP sécurisé pour identifier de manière catégorique le serveur LDAP. Le certificat de confiance est le certificat de l'autorité de certification qui a signé le certificat du serveur LDAP. Si le serveur LDAP utilise des certificats autosignés, le certificat de confiance peut être le certificat du serveur LDAP lui-même. Des certificats de confiance supplémentaires doivent être importés si vous utilisez plusieurs serveurs LDAP dans votre configuration.

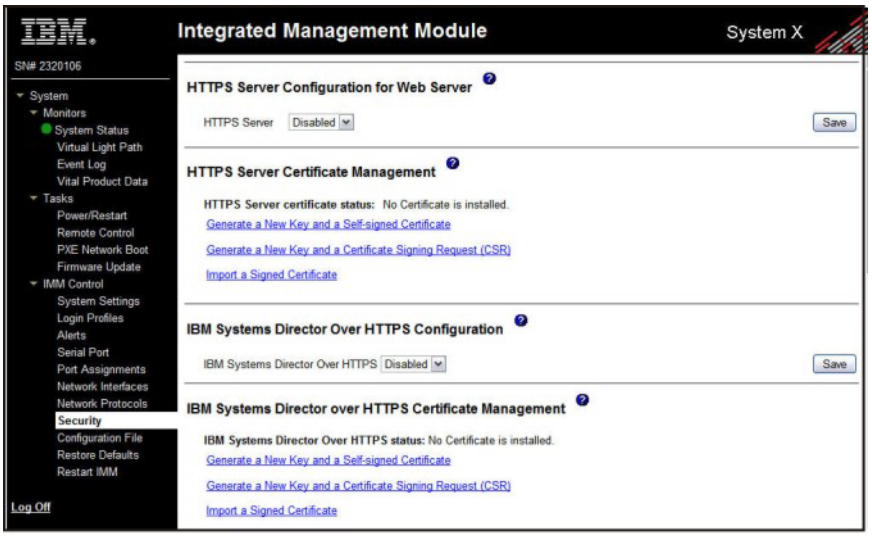
Gestion du certificat du serveur SSL

Le serveur SSL requiert l'installation d'un certificat valide et de la clé de chiffrement privée correspondante avant l'activation de SSL. Deux méthodes sont disponibles pour générer la clé privée et le certificat requis : l'utilisation d'un certificat autosigné et l'utilisation d'un certificat signé par une autorité de certification. Si vous souhaitez utiliser un certificat d'auto-signature avec le serveur SSL, voir «Génération d'un certificat autosigné» pour plus d'informations. Sinon, voir «Génération d'une demande de signature de certificat», à la page 87.

Génération d'un certificat autosigné

Pour générer une nouvelle clé de chiffrement privée et un nouveau certificat d'auto-signature, procédez comme suit.

1. Cliquez sur **Security** depuis le panneau de navigation pour afficher la page ci-après.



2. Vérifiez dans la zone **SSL Server Configuration for Web Server** ou **IBM Systems Director Over HTTPS Configuration** que **Disabled** est sélectionné. Dans le cas contraire, sélectionnez **Disabled** puis cliquez sur **Save**.

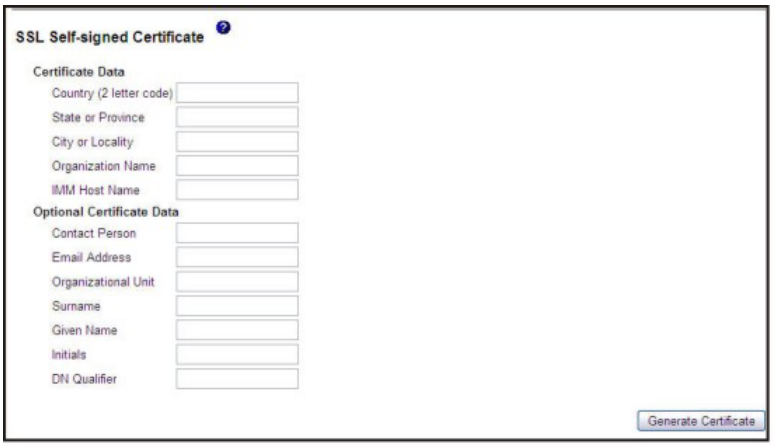
   Remarque :

   a. IMM doit être redémarré avant que la valeur sélectionnée (**Enabled** ou **Disabled**) n'entre en vigueur.

   b. Avant de pouvoir activer SSL, un certificat SSL valide doit être en place.

   c. Pour utiliser SSL, vous devez configurer un navigateur client Web pour utiliser SSL3 ou TLS. Les navigateurs plus anciens ne prenant en charge que SSL2 ne peuvent pas être utilisés.

3. Dans la zone **SSL Server Certificate Management**, sélectionnez **Generate a New Key and a Self-signed Certificate**. Une page similaire à celle de la figure suivante s'affiche.

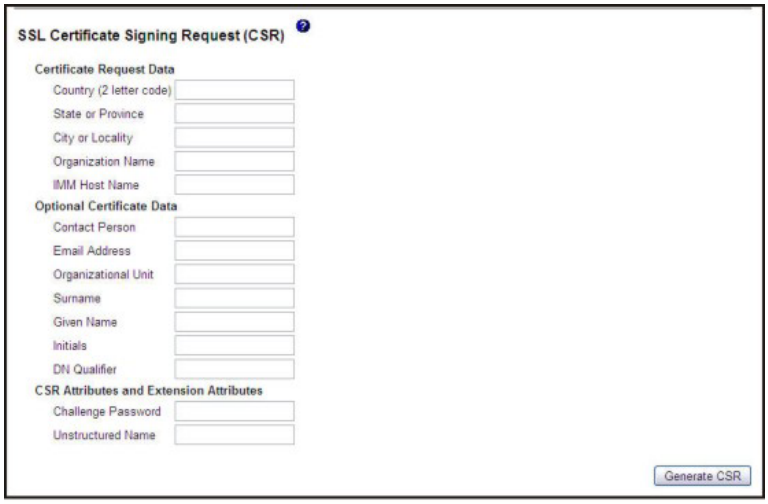


4. Entrez les informations dans les zones obligatoires et dans les zones facultatives qui s'appliquent à votre configuration. Pour obtenir une description des zones, voir “Required certificate data”. 87. Avant d'entrer ces informations, cliquez sur **Generate Certificate**. Vos nouvelles clés de chiffrement et votre certificat sont générés. Cette procédure peut prendre plusieurs minutes. Une confirmation est affichée si un certificat autosigné est installé.

Génération d'une demande de signature de certificat

Pour générer une clé de chiffrement privée et une demande de signature de certificat, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Security**.
2. Vérifiez dans la zone **SSL Server Configuration for Web Server** que le serveur SSL est désactivé. Dans le cas contraire, sélectionnez **Disabled** et cliquez sur **Save** dans la zone **SSL Server**.
3. Dans la zone **SSL Server Certificate Management**, sélectionnez **Generate a New Key and a Certificate-Signing Request**. Une page similaire à celle de la figure suivante s'affiche.



4. Complétez les zones obligatoires et les zones facultatives concernant votre configuration. Les zones sont les mêmes que pour le certificat autosigné, avec quelques zones supplémentaires.

   Consultez les informations des sections suivantes pour une description de chacune des zones communes.

   Required certificate data Les zones de saisie utilisateur suivantes sont obligatoires pour générer un certificat autosigné ou une demande de signature de certificat :

   Country
   Utilisez cette zone pour spécifier le pays où est situé physiquement le module IMM. Cette zone doit contenir le code pays formé de 2 caractères.

   State or Province
   Utilisez cette zone pour spécifier la région où est situé physiquement le module IMM. Cette zone peut contenir au maximum 30 caractères.

   City or Locality
   Utilisez cette zone pour spécifier la ville ou la localité où est situé physiquement le module IMM. Vous devez indiquer un nom de 50 caractères maximum.

   Organization Name
   Utilisez cette zone pour indiquer l'entreprise ou l'organisation propriétaire du module IMM. Lorsque cette zone est utilisée pour générer un demande de signature de certificat, l'autorité de certification émettrice peut vérifier que l'organisme demandant le certificat est habilitée à revendiquer la propriété de l'entreprise ou de l'organisation mentionnée. Cette zone peut contenir au maximum 60 caractères.

IMM Host Name
Utilisez cette zone pour indiquer le nom d'hôte IMM figurant actuellement dans la barre d'adresse du navigateur Web.

Prenez soin d'entrer un nom d'hôte correspondant exactement à celui connu du navigateur Web. Le navigateur Web compare le nom d'hôte figurant dans l'adresse Web résolue au nom mentionné dans le certificat. Pour éviter que le navigateur Web n'affiche des avertissements relatifs au certificat, la valeur utilisée dans cette zone doit être identique au nom d'hôte que le navigateur Web utilise pour se connecter à IMM. Par exemple, si l'adresse dans la barre d'adresse Web est http://mm11.xyz.com/private/main.ssi, la valeur utilisée pour la zone IMM Host Name doit être mm11.xyz.com. Si l'adresse Web est http://mm11/private/main.ssi, la valeur utilisée doit être mm11. Si l'adresse Web est http://192.168.70.2/private/main.ssi, la valeur utilisée doit être 192.168.70.2.

Cet attribut de certificat est généralement dénommé "nom commun".

La zone peut contenir 60 caractères maximum.

Contact Person
Utilisez cette zone pour indiquer le nom d'un contact responsable du module IMM. La zone peut contenir 60 caractères maximum.

Email Address
Utilisez cette zone pour indiquer l'adresse électronique du contact responsable du module IMM. La zone peut contenir 60 caractères maximum.

Optional certificate data Les zones de saisie utilisateur suivantes sont facultatives pour générer un certificat autosigné ou une demande de signature de certificat :

Organizational Unit
Utilisez cette zone pour indiquer le nom de l'unité propriétaire du module IMM au sein de l'entreprise ou de l'organisation. La zone peut contenir 60 caractères maximum.

Surname
Utiliser cette zone pour fournir des informations complémentaires, comme le nom du responsable du module IMM. La zone peut contenir 60 caractères maximum.

Given Name
Utiliser cette zone pour fournir des informations complémentaires, comme le prénom du responsable du module IMM. La zone peut contenir 60 caractères maximum.

Initials
Utiliser cette zone pour fournir des informations complémentaires, comme les initiales du responsable du module IMM. Cette zone peut contenir au maximum 20 caractères.

DN Qualifier
Utiliser cette zone pour fournir des informations complémentaires, comme le nom distinctif du module IMM. Vous devez indiquer un nom de 60 caractères maximum.

Certificate-Signing request attributes Les zones suivantes sont facultatives sauf si elles sont requises par l'autorité de certification sélectionnée :

Challenge Password
Mot de passe de la requête de certificat serveur. Cette zone peut contenir au maximum 30 caractères.

Unstructured Name
Utiliser cette zone pour fournir des informations complémentaires,

comme le nom non structuré affecté au module IMM. Vous devez indiquer un nom de 60 caractères maximum.

5. Après avoir indiqué les informations, cliquez sur **Generate CSR**. Le système génère les nouvelles clés de chiffrement et le nouveau certificat. L'opération peut prendre un certain temps.
6. Cliquez sur **Download CSR**, puis sur **Save** pour enregistrer le fichier sur votre poste de travail. Le fichier généré lors de la création d'une demande de signature de certificat est au format DER. Si l'autorité de certification attend un autre format de données comme PEM, vous pouvez convertir le fichier en utilisant un outil de type OpenSSL (accessible à l'adresse http://www.openssl.org). Si l'autorité de certification vous demande de copier le contenu du fichier de demande de signature de certificat dans une fenêtre de navigateur Web, le format PEM est généralement le format prévu.

   La commande de conversion d'une demande de signature de certificat du format DER au format PEM à l'aide de OpenSSL est similaire à l'exemple suivant :

   ```
   openssl req -in csr.der -inform DER -out csr.pem -outform PEM
   ```
7. Envoyez la demande de signature de certificat à l'autorité de certification. Si elle renvoie le certificat signé, vous devrez peut-être le convertir au format DER. Si vous avez reçu le certificat au format texte dans un message électronique ou une page Web, il est probablement au format PEM. Vous pouvez le convertir en utilisant un outil délivré par l'autorité de certification ou un outil de type OpenSSL (accessible à l'adresse http://www.openssl.org). La commande de conversion d'un certificat du format PEM au format DER est similaire à l'exemple suivant :

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   Passez à l'étape 8 une fois que le certificat signé a été renvoyé par l'autorité de certification.
8. Dans le panneau de navigation, cliquez sur **Security**. Accédez à la zone **SSL Server Certificate Management** ou à la zone **IBM Systems Director Over HTTPS Certificate Management**.
9. Cliquez sur **Import a Signed Certificate**.
10. Cliquez sur **Browse**.
11. Cliquez sur le fichier de certification approprié, puis sur **Open**. Le système affiche le nom et le chemin complet du fichier dans la zone figurant en regard du bouton **Browse**.
12. Cliquez sur **Import Server Certificate** pour lancer la procédure. Un indicateur de progression apparaît lors du transfert du fichier pour son stockage sur IMM. Gardez cette page affichée jusqu'à ce que le transfert soit terminé.

Activation de SSL pour le serveur Web sécurisé ou pour IBM Systems Director over HTTPS

Procédez comme suit pour activer le serveur Web sécurisé.

Remarque : Pour activer SSL, vous devez installer un certificat SSL valide.

1. Dans le panneau de navigation, cliquez sur **Security**. La page qui est affichée indique qu'un certificat serveur SSL valide a été installé. Si le statut du certificat serveur SSL ne confirme pas qu'un certificat SSL valide a été installé, consultez la section «Gestion du certificat du serveur SSL», à la page 85.

2. Accédez à la section **SSL Server Configuration for web Server** ou à la section **IBM Systems Director Over HTTPS Configuration**, sélectionnez **Enabled** dans la zone **SSL Client**, puis cliquez sur **Save**. La valeur sélectionnée prend effet au redémarrage suivant d'IMM.

Gestion du certificat du client SSL

Le client SSL requiert l'installation d'un certificat valide et de la clé de chiffrement privée correspondante avant l'activation de SSL. Deux méthodes sont disponibles pour générer la clé privée et le certificat requis : l'utilisation d'un certificat autosigné ou l'utilisation d'un certificat signé par une autorité de certification.

Pour générer la clé de chiffrement privée et le certificat client SSL, vous devez exécuter la même procédure que pour le serveur SSL, si ce n'est que vous devez compléter complétez la section **SSL Client Certificate Management** au lieu de la section **SSL Server Certificate Management** de la page Web Security. Si vous souhaitez utiliser un certificat d'auto-signature avec le client SSL, voir «Génération d'un certificat autosigné», à la page 85. Sinon, voir «Génération d'une demande de signature de certificat», à la page 87.

Gestion des certificats de confiance du client SSL

Le client SSL sécurisé (client LDAP) utilise des certificats de confiance pour identifier le serveur LDAP. Le certificat sécurisé correspond au certificat délivré par l'autorité de certification qui a signé le certificat du serveur LDAP ou au certificat du serveur LDAP lui-même. Avant d'activer le client SSL, vous devez importer au moins un certificat dans IMM. Vous pouvez importer jusqu'à trois certificats de confiance.

Pour importer un certificat sécurisé, procédez comme suit.

1. Dans le panneau de navigation, sélectionnez **Security**.
2. Vérifiez que le client SSL est désactivé dans la zone **SSL Client Configuration for LDAP Client**. Dans le cas contraire, sélectionnez **Disabled** et cliquez sur **Save** dans la zone **SSL Client**.
3. Accédez à la zone **SSL Client Trusted Certificate Management**.
4. Cliquez sur le bouton **Import** figurant en regard de l'une des zones **Trusted CA Certificate 1**.
5. Cliquez sur **Browse**.
6. Sélectionnez le fichier certificat et cliquez sur **Open**. Le système affiche le nom et le chemin complet du fichier dans la zone figurant en regard du bouton **Browse**.
7. Pour lancer la procédure d'importation, cliquez sur **Import Certificate**. Un indicateur de progression apparaît lors du transfert du fichier pour son stockage sur IMM. Laissez la page affichée jusqu'à la fin du transfert.

   Le système a ajouté le bouton **Remove** en regard de l'option Trusted CA Certificate 1. Pour supprimer un certificat sécurisé, cliquez sur le bouton **Remove** correspondant.

   Pour importer d'autres certificats sécurisés, cliquez sur le bouton **Import** des zones Trusted CA Certificate 2 et Trusted CA Certificate 3.

Activation de SSL pour le client LDAP

Utilisez la section **SSL Client Configuration for LDAP Client** de la page Security pour activer ou désactiver SSL pour le client LDAP. Pour activer SSL, un certificat client SSL valide et au moins un certificat de confiance doivent d'abord être installés.

Pour activer SSL pour le client, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Security**.

   La page Security présente un certificat client SSL installé et le certificat de confiance 1 de l'autorité de certification.
2. Sur la page SSL Client Configuration for LDAP Client, sélectionnez **Enabled** dans la zone **SSL Client**.

   Remarque :

   a. La valeur sélectionnée (Enabled ou Disabled) prend effet immédiatement.
   b. Avant de pouvoir activer SSL, un certificat SSL valide doit être en place.
   c. Votre serveur LDAP doit prendre en charge SSL3 ou TLS pour être compatible avec l'implémentation SSL utilisée par le client LDAP.
3. Cliquez sur **Save**. La valeur sélectionnée est immédiatement appliquée.

Gestion cryptographique

Vous pouvez utiliser la zone **Cryptography Management** sur la page Security pour configurer la puissance de la suite de chiffrement des serveurs SSL dans IMM, y compris le serveur HTTPS et IBM System Director via HTTPS.

Les modes de gestion cryptographique possèdent différentes puissances de sécurité. Le mode Basic Compatible est le mode par défaut et est compatible avec des versions plus anciennes de microprogramme et avec des navigateurs et autres clients réseaux qui n'utilisent pas le mode stricter security requirements. Le mode High Security permet de restreindre l'utilisation d'une clé symétrique SSL supérieure à 128 bits par IMM.

Pour configurer le mode, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Security**.
2. Localisez la zone **Cryptography Management**, et sélectionnez **Basic Compatible Mode** ou **High Security Mode**.
3. Cliquez sur **Save** et le mode sélectionné prendra effet après redémmarrage d'IMM.

Configuration du serveur Secure Shell

La fonctionnalité Secure Shell (SSH) permet un accès sécurisé à l'interface de ligne de commande et aux fonctions de redirection série (console texte) du module IMM.

Le système authentifie les utilisateurs SSH en envoyant leur ID et mots de passe utilisateur. Il les transmet après avoir établi le canal de chiffrement. La paire ID-mot de passe peut correspondre à l'une des 12 combinaisons ID utilisateur/mot de passe enregistrées en local, mais elles peuvent également résider sur un serveur LDAP. Le système ne prend pas en charge l'authentification par clé publique.

Génération d'une clé de serveur SSH

Une clé de serveur Secure Shell est utilisée pour authentifier l'identité du serveur Secure Shell auprès du client. Avant de créer une nouvelle clé privée de serveur SSH, vous devez désactiver SSH. En effet, vous devez créer la clé avant d'activer le serveur SSH.

Lorsque vous demandez une nouvelle clé de serveur, une clé Rivest, Shamir et Adelman et une clé DSA sont créées pour permettre l'accès à IMM depuis un client SSH version 2. Par souci de sécurité, le système ne sauvegarde pas la clé privée du serveur SSH pendant la sauvegarde ou la restauration de la configuration.

Pour créer une nouvelle clé de serveur SSH, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Security**.
2. Accédez à la zone **Secure Shell (SSH) Server** et vérifiez que le serveur Secure Shell est désactivé. Dans le cas contraire, sélectionnez **Disabled** et cliquez sur **Save** dans la zone **SSH Server**.
3. Accédez à la zone **SSH Server Key Management**.
4. Cliquez sur **Generate SSH Server Private Key**. Une fenêtre de progression s'affiche. Attendez la fin de l'opération.

Activation du serveur SSH

Vous pouvez activer ou désactiver le serveur SSH depuis la page Security. Votre sélection ne prend effet qu'après le redémarrage d'IMM. La valeur affichée à l'écran (Enabled ou Disabled) est la dernière valeur sélectionnée et celle utilisée au redémarrage d'IMM.

Remarque : Vous pouvez activer le serveur SSH uniquement si vous avez installé une clé privée de serveur SSH valide au préalable.

Pour activer le serveur SSH, procédez comme suit.

1. Dans le panneau de navigation, cliquez sur **Security**.
2. Accédez à la zone **Secure Shell (SSH) Server**.
3. Cliquez sur **Enabled** dans la zone **SSH Server**.
4. Dans le panneau de navigation, cliquez sur **Restart IMM** pour redémarrer IMM.

Utilisation du serveur SSH

Si vous utilisez le client SSH fourni avec Red Hat Linux version 7.3, pour lancer une session Secure Shell sur un module IMM avec l'adresse réseau 192.168.70.132, entrez une commande similaire à celle de l'exemple suivant :

```
ssh -x -l ID_utilisateur 192.168.70.132
```

où -x indique de ne pas utiliser l'acheminement X Window System et -l indique que la session doit utiliser l'ID *ID_utilisateur*.

Restauration et modification de votre configuration IMM

Vous pouvez restaurer intégralement une configuration sauvegardée ou modifier certaines zones clés de cette configuration avant de la restaurer dans IMM. En modifiant le fichier de configuration avant de la restaurer, vous pouvez implanter plusieurs modules IMM dotés de configurations similaires. Vous pouvez spécifier

rapidement des paramètres requérant des valeurs uniques, comme les noms et les adresses IP, sans besoin de renseigner à nouveau des informations communes partagées.

Pour restaurer ou modifier la configuration, procédez comme suit.

1. Connectez-vous au module IMM dont vous désirez restaurer la configuration. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Configuration File**.
3. Dans la zone **Restore IMM Configuration**, cliquez sur **Browse**.
4. Cliquez sur le fichier de configuration de votre choix, puis sur **Open**. Le système affiche le nom et le chemin complet du fichier dans la zone figurant en regard du bouton **Browse**.
5. Si vous ne souhaitez pas modifier le fichier de configuration, cliquez sur **Restore**. Une nouvelle fenêtre s'ouvre en affichant les informations de configuration IMM. Vérifiez qu'il s'agit bien de la configuration que vous désirez restaurer. Si ce n'est pas le cas, cliquez sur **Cancel**.

   Si vous désirez apporter des modifications au fichier de configuration avant de la restaurer, cliquez sur **Modify and Restore** afin d'ouvrir une fenêtre de configuration récapitulative modifiable. Initialement, seules les zones autorisant des modifications sont affichées. Pour passer de la vue courante à la vue récapitulative (et inversement), cliquez sur le bouton **Toggle View** figurant en haut ou en bas de la fenêtre. Pour modifier le contenu d'une zone, cliquez sur la zone de texte correspondante et entrez les informations appropriées.

   Remarque : Lorsque vous cliquez sur le bouton **Restore** ou **Modify and Restore**, le système peut afficher un message d'alerte si le fichier de configuration que vous tentez de restaurer a été créé par un type différent de processeur de service ou par le même type mais avec un microprogramme plus ancien (et doté par conséquent de moins de fonctionnalités). Ce message d'alerte inclut une liste des fonctions de liste à configurer une fois la restauration terminée. Certaines fonctions impliquent la configuration de plusieurs fenêtres.
6. Pour poursuivre la restauration du fichier sur le module IMM, cliquez sur **Restore Configuration**. Un indicateur signale la progression de la mise à jour du microprogramme sur IMM. Une fenêtre confirme enfin l'aboutissement de la mise à niveau.

   Remarque : Les paramètres de sécurité de la page Security ne sont pas restaurés. Pour modifier ces paramètres, voir «Sécuriser le serveur Web, IBM Systems Director et LDAP», à la page 84.
7. Après confirmation de l'achèvement du processus de restauration, cliquez dans le panneau de navigation sur **Restart IMM**, puis cliquez sur **Restart**.
8. Cliquez sur **OK** pour confirmer votre intention de redémarrer IMM.
9. Cliquez sur **OK** pour fermer la fenêtre de navigateur en cours.
10. Pour vous connecter à nouveau à IMM, lancez le navigateur et suivez votre procédure de connexion habituelle.

Utilisation du fichier de configuration

Sélectionnez dans le panneau de navigation **Configuration File** pour créer une sauvegarde et restaurer la configuration IMM.

Important: Les paramètres de la page Security ne sont pas enregistrés lors de l'opération de sauvegarde et ne peuvent pas être par l'opération de restauration.

Sauvegarde de votre configuration actuelle

Vous pouvez télécharger une copie de votre configuration IMM actuelle vers l'ordinateur client sur lequel s'exécute l'interface Web d'IMM. Utilisez cette copie de sauvegarde pour restaurer votre configuration IMM si celle-ci a été modifiée ou endommagée par inadvertance. Utilisez-la comme base que vous pourrez modifier pour configurer plusieurs modules IMMs avec des configurations similaires.

Les informations de configuration sauvegardées sous cette procédure n'incluent pas les paramètres de configuration de microprogramme de serveur System x ou des paramètres IPMI qui ne seraient pas communs avec des interfaces utilisateur non IMPI.

Pour effectuer une copie de sauvegarde de la configuration en cours, procédez comme suit.

1. Connectez-vous au module IMM dont vous désirez sauvegarder la configuration actuelle. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Configuration File**.
3. Dans la zone **Backup IMM Configuration**, cliquez sur **View the current configuration summary**.
4. Vérifiez les paramètres, puis cliquez sur **Close**.
5. Pour sauvegarder cette configuration, cliquez sur **Backup**.
6. Affectez un nom à la sauvegarde, sélectionnez le répertoire dans lequel vous souhaitez enregistrer le fichier et cliquez sur **Save**.

   Sous Mozilla Firefox, cliquez sur **Enregistrer le fichier**, puis sur **OK**.

   Sous Microsoft Internet Explorer, cliquez sur **Enregistrer ce fichier sur disque**, puis sur **OK**.

Restauration et modification de votre configuration IMM

Vous pouvez restaurer intégralement une configuration sauvegardée ou modifier certaines zones clés de cette configuration avant de la restaurer dans IMM. En modifiant le fichier de configuration avant de la restaurer, vous pouvez implanter plusieurs modules IMM dotés de configurations similaires. Vous pouvez spécifier rapidement des paramètres requérant des valeurs uniques, comme les noms et les adresses IP, sans besoin de renseigner à nouveau des informations communes partagées.

Pour restaurer ou modifier la configuration, procédez comme suit.

1. Connectez-vous au module IMM dont vous désirez restaurer la configuration. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Configuration File**.
3. Dans la zone **Restore IMM Configuration**, cliquez sur **Browse**.
4. Cliquez sur le fichier de configuration de votre choix, puis sur **Open**. Le système affiche le nom et le chemin complet du fichier dans la zone figurant en regard du bouton **Browse**.
5. Si vous ne souhaitez pas modifier le fichier de configuration, cliquez sur **Restore**. Une nouvelle fenêtre s'ouvre en affichant les informations de

configuration IMM. Vérifiez qu'il s'agit bien de la configuration que vous désirez restaurer. Si ce n'est pas le cas, cliquez sur **Cancel**.

Si vous désirez apporter des modifications au fichier de configuration avant de la restaurer, cliquez sur **Modify and Restore** afin d'ouvrir une fenêtre de configuration récapitulative modifiable. Initialement, seules les zones autorisant des modifications sont affichées. Pour passer de la vue courante à la vue récapitulative (et inversement), cliquez sur le bouton **Toggle View** figurant en haut ou en bas de la fenêtre. Pour modifier le contenu d'une zone, cliquez sur la zone de texte correspondante et entrez les informations appropriées.

Remarque : Lorsque vous cliquez sur le bouton **Restore** ou **Modify and Restore**, le système peut afficher un message d'alerte si le fichier de configuration que vous tentez de restaurer a été créé par un type différent de processeur de service ou par le même type mais avec un microprogramme plus ancien (et doté par conséquent de moins de fonctionnalités). Ce message d'alerte inclut une liste des fonctions de liste à configurer une fois la restauration terminée. Certaines fonctions impliquent la configuration de plusieurs fenêtres.

6. Pour poursuivre la restauration du fichier sur le module IMM, cliquez sur **Restore Configuration**. Un indicateur signale la progression de la mise à jour du microprogramme sur IMM. Une fenêtre confirme enfin l'aboutissement de la mise à niveau.

   Remarque : Les paramètres de sécurité de la page Security ne sont pas restaurés. Pour modifier ces paramètres, voir «Sécuriser le serveur Web, IBM Systems Director et LDAP», à la page 84.
7. Après confirmation de l'achèvement du processus de restauration, cliquez dans le panneau de navigation sur **Restart IMM**, puis cliquez sur **Restart**.
8. Cliquez sur **OK** pour confirmer votre intention de redémarrer IMM.
9. Cliquez sur **OK** pour fermer la fenêtre de navigateur en cours.
10. Pour vous connecter à nouveau à IMM, lancez le navigateur et suivez votre procédure de connexion habituelle.

Restauration des paramètres par défaut

Si vous disposez d'un accès Superviseur, utilisez le lien **Restore Defaults** pour restaurer la configuration IMM par défaut.

Avertissement : Si vous cliquez sur **Restore Defaults**, toutes les modifications apportées à IMM seront perdues.

Pour restaurer les paramètres IMM par défaut, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Restore Defaults** pour restaurer les paramètres par défaut d'IMM. S'il s'agit d'un serveur local, votre connexion TCP/IP sera coupée et vous devrez reconfigurer l'interface réseau pour restaurer la connectivité.
3. Connectez-vous à nouveau pour utiliser l'interface Web d'IMM.
4. Reconfigurez l'interface réseau pour restaurer la connectivité. Pour plus d'informations sur l'interface réseau, voir «Configuration des interfaces réseau», à la page 40.

Redémarrage d'IMM

Utilisez le lien **Restart IMM** pour redémarrer IMM. Vous ne pouvez exécuter cette fonction que si vous disposez d'un accès Superviseur. Les connexions Ethernet éventuelles sont momentanément coupées. Vous devez vous reconnecter pour utiliser l'interface IMM.

Pour redémarrer IMM, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Restart IMM** pour redémarrer IMM. Vos connexions TCP/IP ou modem sont coupées.
3. Connectez-vous à nouveau pour utiliser l'interface Web d'IMM.

Partitionnement évolutif

Le module IMM vous permet de configurer et de contrôler le système dans un complexe évolutif.

Le module IMM vous permet de configurer et de contrôler le système dans un complexe évolutif. Si une erreur affecte le serveur, IMM consigne un code d'événement dans les journaux d'événements (voir «Affichage des journaux d'événements», à la page 108).

1. Connectez-vous au module IMM dont vous désirez restaurer la configuration. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Scalable Partitioning**, puis sur **Manage Partitions**.

fonction Service Advisor

La fonction Service Advisor détecte et collecte les événements d'erreur matérielle système et transmet automatiquement les données au service d'assistance IBM pour l'identification du problème. Elle peut également collecter des données sur les erreurs système et transmettre ces données au service d'assistance IBM. Consultez la documentation de votre serveur pour déterminer s'il prend en charge cette fonction. Les instructions de configuration, de test et de maintenance de Service Advisor figurent dans les rubriques suivantes.

- Configuration de Service Advisor
- Utilisation de Service Advisor

Configuration de Service Advisor

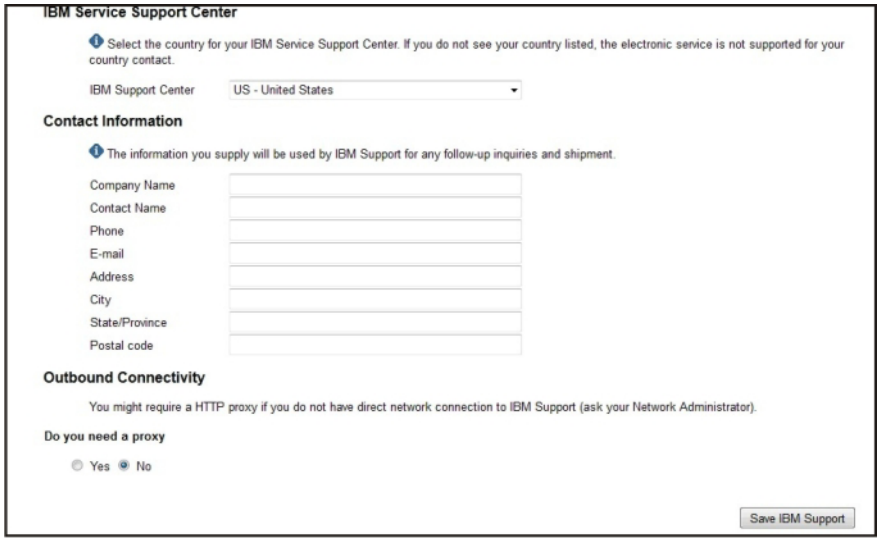
Pour configurer Service Advisor, procédez comme suit.

1. Connectez-vous au module IMM sur lequel vous désirez activer Service Advisor. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Service Advisor**.
3. Si vous utilisez cette option pour la première fois ou si IMM a été réinitialisé à ses valeurs par défaut, vous devez lire et accepter le contrat de licence.
   a. Cliquez sur **View Terms and Conditions** pour afficher le contrat d'utilisation de Service Advisor.

b. Cliquez sur **I accept the agreement** sur la page Terms and Conditions pour activer Service Advisor.

4. Cliquez sur l'onglet **Service Advisor Settings**.

   Une page comparable à celle présentée dans la figure ci-après s'affiche.



5. Entrez les informations de contact de l'administrateur du serveur. Reportez-vous au tableau suivant pour une explication des zones **Contact Information**.

Tableau 15. Informations de contact

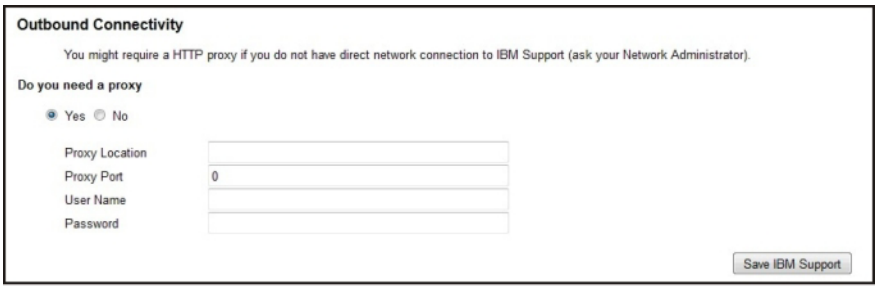
Zone	Description
IBM Service Support Center	Indiquez dans cette zone le code pays du centre de support IBM. Il s'agit d'un code pays ISO composé de deux caractères et qui ne s'applique qu'aux clients ayant accès au centre de support IBM.
Company Name	Indiquez dans cette zone le nom de l'organisation ou de la société de la personne à contacter. Cette zone peut contenir de 1 à 30 caractères.
Contact Name	Indiquez dans cette zone le nom de l'organisation ou de la société de la personne à contacter. Cette zone peut contenir de 1 à 30 caractères.
Phone	Indiquez dans cette zone le numéro de téléphone de la personne à contacter. Cette zone peut contenir de 5 à 30 caractères.
Email	Indiquez dans cette zone l'adresse électronique de la personne à contacter. Cette zone peut comporter au maximum 30 caractères.
Address	Indiquez dans cette zone la rue où le module IMM est physiquement installé. Cette zone peut contenir de 1 à 30 caractères.
City	Indiquez dans cette zone la ville ou la localité où le module IMM est physiquement installé.
Etat/province	Indiquez dans cette zone l'état ou la province où le module IMM est physiquement installé. Cette zone peut contenir de 2 à 3 caractères.

Tableau 15. Informations de contact (suite)

Zone	Description
Postal Code	Indiquez dans cette zone le code postal de l'emplacement du serveur. Cette zone peut contenir de 1 à 9 caractères, (seuls les caractères alphanumériques sont valides).

6. Créez un proxy HTTP si le module IMM ne dispose pas d'une connexion réseau directe avec l'assistance IBM. Procédez comme suit pour configurer les informations de connectivité sortante.
   a. Dans la zone **Do you need a proxy**, cliquez sur **Yes**. Reportez-vous à l'illustration précédente.

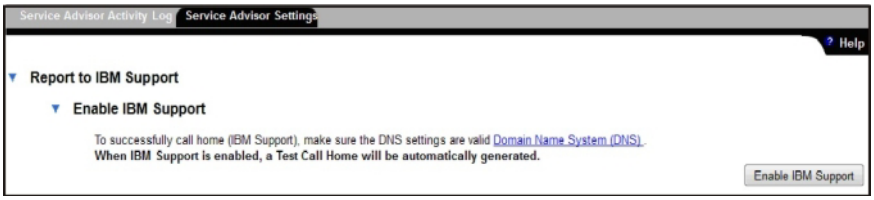
      Une page comparable à celle présentée dans la figure ci-après s'affiche.



   b. Renseignez les zones **Proxy Location** (emplacement du proxy), **Proxy Port** (port proxy), **User Name** (nom d'utilisateur) et **Password** (mot de passe).
7. Cliquez sur **Save IBM Support** pour enregistrer vos modifications.
8. Cliquez sur **Enable IBM Support** (cette zone est située vers le sommet de la page) pour permettre à Service Advisor de contacter le support IBM lorsqu'un code d'événement pris en charge est généré.

   Remarque : Après l'activation du support IBM, un code de test est envoyé au site du support IBM.
9. Cliquez sur l'onglet **Service Advisor Activity Log** pour afficher le statut du code de test.

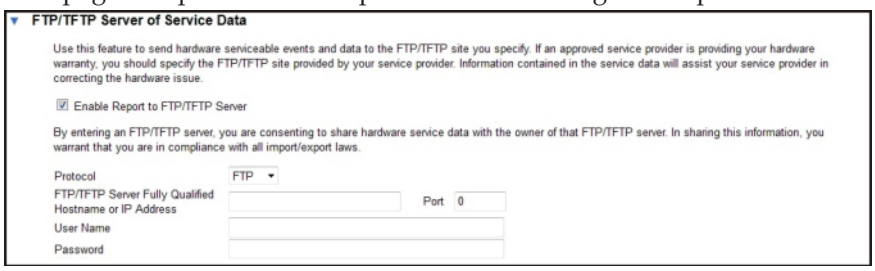
   Une page comparable à celle présentée dans la figure ci-après s'affiche.



10. Si vous désirez autoriser un autre fournisseur de service à recevoir les codes d'événements avant de contacter le support IBM, cliquez sur **Enable Report to FTP/TFTP Server**.

    Attention : En entrant un serveur FTP/TFTP, vous consentez à partager les données de maintenance du matériel avec le propriétaire de ce serveur. En partageant ces informations, vous garantissez que vous êtes en conformité avec toutes les lois régissant l'importation/l'exportation.

Une page comparable à celle présentée dans la figure ci-après s'affiche.



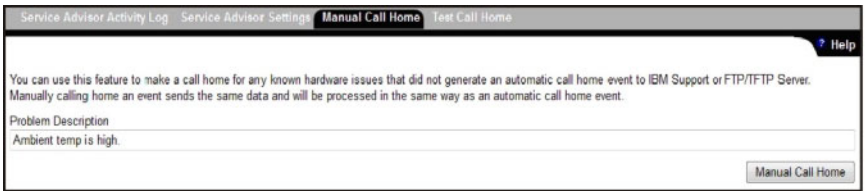
Utilisation de Service Advisor

Une fois Service Advisor configuré, vous pouvez afficher le journal d'activité ou générer un message de test.

Procédez comme suit pour créer un rapport d'incident matériel pour votre serveur :

1. Connectez-vous au module IMM sur lequel vous désirez utiliser Service Advisor. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Service Advisor**.
3. Cliquez sur l'onglet **Manual Call Home**.

   Une page comparable à celle présentée dans la figure ci-après s'affiche.

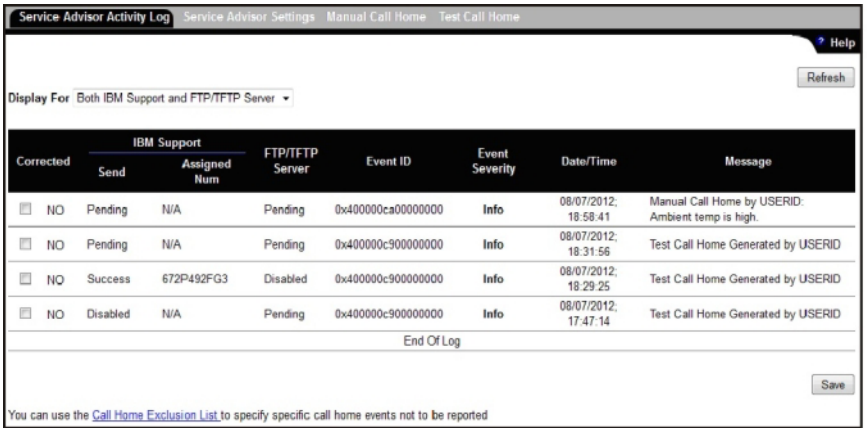


4. Procédez comme suit pour générer manuellement un événement d'appel vers IBM.
   a. Entrez la description du problème dans la zone **Problem Description**.
   b. Cliquez sur le bouton **Manual Call Home**.
5. Pour générer un message de test, cliquez sur l'onglet **Test Call Home**, puis cliquez sur le bouton **Test Call Home**.

   Remarques :

   - Cette option de menu valide le chemin de communication entre IMM et IBM ou le serveur FTP/TFTP d'après les paramètres actuels.
   - Si le test échoue, vérifiez la configuration réseau.
   - Pour envoyer des rapports au support IBM, Service Advisor requiert que l'adresse du serveur DNS soit correctement configurée sur le module IMM.
   - Si l'appel aboutit, un numéro de service ou de ticket lui sera affecté. Le ticket ouvert auprès du support IBM sera identifié comme se rapportant à un ticket de test. Aucune action n'est requise du support IBM pour un tel ticket et l'appel sera clôturé.
6. Cliquez sur l'onglet **Service Advisor Activity Log** pour afficher le statut du journal d'activité.

Une page comparable à celle présentée dans la figure ci-après s'affiche.



Remarques :

- Le journal d'activité affiche les cinq derniers événements d'appel vers IBM, y compris les événements de test d'appel et d'appel manuel.
- Les résultats dans la zone **Send** peuvent être l'un des suivants :

  Success
  L'appel a été reçu par IBM ou le serveur FTP/TFTP. La zone **Assigned Service Number** inclut le numéro de ticket du problème.

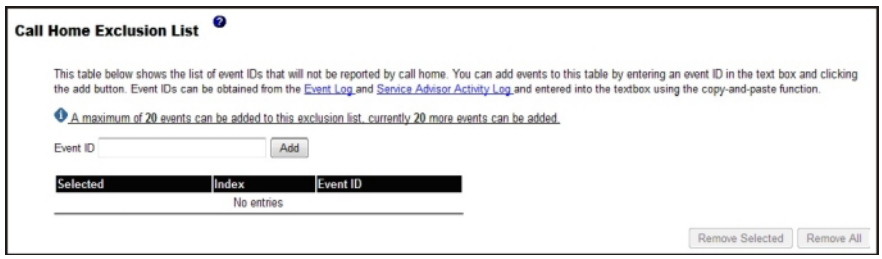
  Pending
  L'événement d'appel vers IBM est en cours.

  Echec L'événement d'appel vers IBM a échoué. Dans ce cas, contactez le support IBM pour signaler l'événement de service matériel. Aucune nouvelle tentative n'est effectuée pour les appels vers IBM ayant échoué.

7. Après avoir résolu un événement, cochez la case **Corrected** pour cet événement afin de faciliter la recherche des événements non résolus.

   Remarque : Si la case **Corrected** n'est pas cochée pour un événement, l'occurrence suivante du même événement ne *fera pas l'objet d'un appel vers IBM* tant que cinq jours ne se seront pas écoulés depuis la première occurrence.
8. Cliquez sur **Refresh** pour afficher les informations les plus récentes.

   Remarque : Le numéro **Assigned Service Number** peut être utilisé pour référencer l'appel vers IBM lors de la communication avec le support IBM.
9. Pour supprimer un événement spécifié dans le rapport au support IBM, procédez comme suit.
   a. Cliquez sur le lien **Call Home Exclusion List**. Une page comparable à celle présentée dans la figure ci-après s'affiche.



   b. Entrez l'ID événement hexadécimal dans la zone **Event ID**.

c. Cliquez sur **Add**.

Déconnexion

Pour vous déconnecter d'IMM ou d'un autre serveur distant, cliquez sur **Log Off** dans le panneau de navigation.

Chapitre 4. Surveillance du statut du serveur

Utilisez les liens sous l'en-tête **Monitors** du panneau de navigation pour afficher le statut du serveur auquel vous accédez.

Depuis la page System Status, vous pouvez :

- Surveiller le statut de l'alimentation du serveur et afficher l'état du système d'exploitation
- Afficher les relevés de température, les seuils de tension et la vitesse des ventilateurs du serveur
- Visualiser la dernière capture d'écran d'échec du système d'exploitation du serveur
- Afficher la liste des utilisateurs qui sont connectés au module IMM

Depuis la page Virtual Light Path, vous pouvez afficher le nom, la couleur et le statut des voyants allumés sur un serveur.

Depuis la page Event Log, vous pouvez :

- Afficher certains événements qui ont été consignés dans le journal des événements du module IMM
- Visualiser la gravité des événements

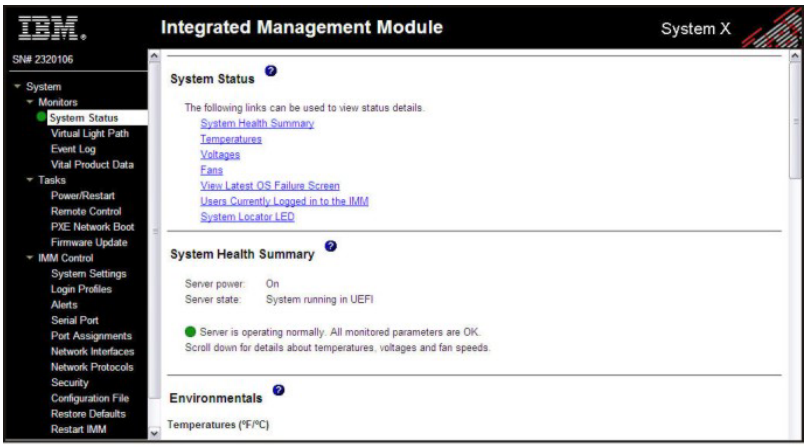
Depuis la page Vital Product Data (VPD), vous pouvez examiner les données techniques essentielles.

Affichage de l'état du système

Sur la page System Status, vous pouvez surveiller les relevés de température, les seuils de voltage et l'état des ventilateurs de votre serveur. Vous pouvez également afficher la capture d'écran du dernier échec du système d'exploitation, les utilisateurs connectés au module IMM, et le voyant de localisation système.

Pour afficher les informations sur l'état de santé et sur l'environnement du serveur, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **System Status** pour afficher une mise à jour dynamique de l'état de santé global du serveur. Une page similaire à celle de la figure ci-après s'affiche.



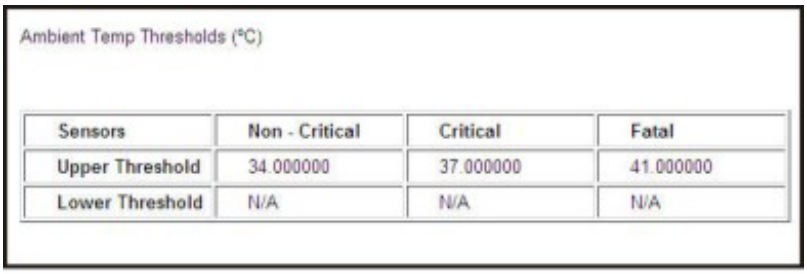
L'état de votre serveur détermine le message affiché en haut de la page System Health Summary. L'un des symboles suivants est affiché :

- Un cercle vert plein et la phrase `Server is operating normally` (le serveur fonctionne normalement)
- Un cercle rouge contenant un x ou un triangle jaune contenant un point d'exclamation et la phrase `One or more monitored parameters are abnormal` (un ou plusieurs paramètres surveillés sont anormaux)

Si les paramètres surveillés dévient des plages d'exploitation normales, une liste des paramètres concernés est affichée sur la page System Health Summary.

3. Accédez à la zone **Temperature** dans la section **Environmentals**, laquelle contient des informations sur la température, le voltage et la vitesse des ventilateurs.

   IMM effectue le suivi des relevés de température actuels et des niveaux de seuil de composants système tels que les microprocesseurs, la carte mère et le fond de panier d'unités de disque dur. Lorsque vous cliquez sur un relevé de température, une nouvelle fenêtre s'ouvre.



La page Temperature Thresholds affiche les niveaux de température auxquels IMM réagit. Les valeurs de seuil de température sont prédéfinies sur le serveur distant et ne sont pas modifiables.

Les températures signalées sont mesurées par rapport aux plages de seuil suivantes :

Non-Critical

Lorsque la température atteint une valeur spécifiée, une alerte correspondante est envoyée aux destinataires d'alerte à distance configurés. Vous devez cocher la case **Warning Alerts** de la zone **SNMP Alerts Settings** sur la page Alerts ou la case **Warning Alerts** sur la page Remote Alert Recipient pour que l'alerte soit envoyée.

Pour plus d'informations sur la sélection d'options d'alerte, voir «Configuration des paramètres d'alerte SNMP», à la page 36 ou «Configuration de destinataires d'alerte distante», à la page 34.

Critical

Lorsque la température atteint une valeur spécifiée au-dessus de la valeur d'avertissement (le seuil d'arrêt graduel), une seconde alerte de température est envoyée aux destinataires d'alertes spécifiés et le serveur déclenche le processus d'arrêt avec un arrêt ordonné du système d'exploitation. Le serveur se met ensuite hors tension. Vous devez cocher la case **Critical Alerts** de la zone **SNMP Alerts Settings** sur la page Alerts ou la case **Critical Alerts** sur la page Remote Alert Recipient pour que l'alerte soit envoyée.

Pour plus d'informations sur la sélection d'options d'alerte, voir «Configuration des paramètres d'alerte SNMP», à la page 36 ou «Configuration de destinataires d'alerte distante», à la page 34.

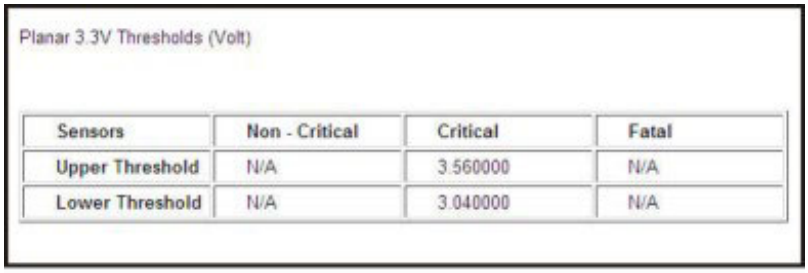
Fatal Lorsque la température atteint une valeur spécifiée au-dessus de la valeur d'arrêt graduel (le seuil d'arrêt immédiat), le serveur s'arrête immédiatement et envoie une alerte aux destinataires d'alerte distante configurés. Vous devez cocher la case **Critical Alerts** de la zone **SNMP Alerts Settings** sur la page Alerts ou la case **Critical Alerts** sur la page Remote Alert Recipient pour que l'alerte soit envoyée.

Pour plus d'informations sur la sélection d'options d'alerte, voir «Configuration des paramètres d'alerte SNMP», à la page 36 ou «Configuration de destinataires d'alerte distante», à la page 34.

IMM génère un événement non critique, ou critique, lorsque le seuil est atteint et déclenche des actions d'arrêt si elles sont requises.

4. Accédez à la zone **Voltages**. IMM enverra une alerte si un voltage de la source d'alimentation sous surveillance s'écarte des plages d'opération spécifiées.

   Si vous cliquez sur un relevé de voltage, une nouvelle fenêtre s'ouvre.



La page Voltage Thresholds affiche les niveaux de voltage auxquels IMM réagit. Ces valeurs sont prédéfinies sur le serveur distant et ne sont pas modifiables.

L'interface Web d'IMM affiche les relevés de voltages de la carte système et des régulateurs de tension. Le système définit une plage de voltage à laquelle les actions suivantes sont exécutées :

Non-Critical

Lorsque le voltage tombe au-dessous ou dépasse une plage spécifiée, une alerte sur le voltage est envoyée aux destinataires d'alerte distante configurés. Vous devez cocher la case **Warning Alerts** de la zone **SNMP Alerts Settings** sur la page Alerts pour que l'alerte soit envoyée.

Pour plus d'informations sur la sélection d'options d'alerte, voir «Configuration des paramètres d'alerte SNMP», à la page 36.

Critical

Lorsque le voltage tombe au-dessous ou dépasse une plage spécifiée, une alerte sur le voltage est envoyée aux destinataires d'alerte distante configurés et le serveur déclenche le processus d'arrêt avec un arrêt ordonné du système d'exploitation. Le serveur se met ensuite hors tension. Vous devez cocher la case **Critical Alerts** de la zone **SNMP Alerts Settings** sur la page Alerts pour que l'alerte soit envoyée.

Pour plus d'informations sur la sélection d'options d'alerte, voir «Configuration des paramètres d'alerte SNMP», à la page 36.

Fatal Lorsque le voltage tombe au-dessous ou dépasse une plage spécifiée, le serveur s'arrête immédiatement et envoie une alerte aux destinataires d'alerte distante configurés. Vous devez cocher la case **Critical Alerts** de la zone **SNMP Alerts Settings** sur la page Alerts pour que l'alerte soit envoyée.

Remarque : L'alerte d'arrêt immédiat n'est envoyée que si une alerte d'arrêt graduel n'a pas encore été envoyée.

Pour plus d'informations sur la sélection d'options d'alerte, voir «Configuration des paramètres d'alerte SNMP», à la page 36.

IMM génère un événement non critique, ou critique, lorsque le seuil est atteint et génère des actions d'arrêt, si celles-ci sont requises.

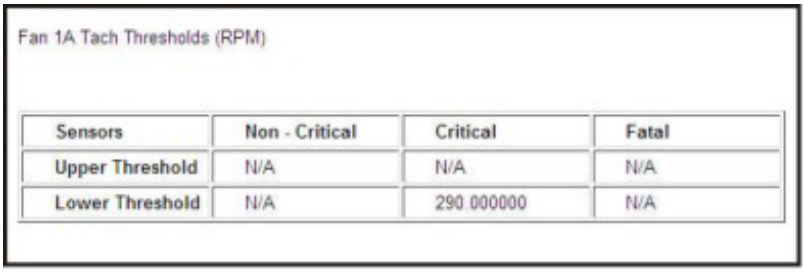
Non Critique

Si IMM indique que ce seuil a été atteint, un événement d'avertissement est généré.

Critical

Si IMM indique que ce seuil a été atteint, un événement critique est généré.

5. Accédez à la zone **Fan Speeds (% of max)**. L'interface Web d'IMM affiche la vitesse de fonctionnement des ventilateurs du serveur (exprimée en pourcentage de la vitesse maximale). Si vous cliquez sur un relevé de ventilateur, une nouvelle fenêtre s'ouvre.



Vous recevez une alerte de ventilateur lorsque sa vitesse tombe à un niveau inacceptable ou qu'il s'arrête. Vous devez cocher la case **Critical Alerts** de la zone **SNMP Alerts Settings** sur la page Alerts pour que l'alerte soit envoyée.

Pour plus d'informations sur la sélection d'options d'alerte, voir «Configuration des paramètres d'alerte SNMP», à la page 36.

6. Accédez à la zone **View Latest OS Failure Screen**. Cliquez sur **View OS Failure Screen** pour accéder à une image de l'écran d'échec du système d'exploitation capturée lorsque le serveur a cessé de fonctionner.

Remarque :

La fonction de capture d'écran d'échec du système d'exploitation n'est disponible qu'avec IMM Premium. Pour plus d'informations sur la mise à niveau de module standard vers IMM Premium, voir «Mise à niveau depuis IMM Standard vers IMM Premium», à la page 5.

Si un événement provoquant l'arrêt du fonctionnement du système d'exploitation se produit, le programme de surveillance du système d'exploitation est déclenché, ce qui entraîne la capture par IMM des données de l'écran d'échec du système d'exploitation et son stockage. IMM ne stocke que les informations de l'événement d'erreur le plus récent, en écrasant les données d'écran d'échec du système d'exploitation plus anciennes lorsqu'un nouvel événement d'erreur survient.

Pour accéder à distance à une image d'écran d'échec du système d'exploitation du serveur, procédez comme suit.

a. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
b. Dans le panneau de navigation, cliquez sur **System Health**, puis accédez à la zone **View Latest OS Failure Screen**.
c. Cliquez sur **View OS Failure Screen**. L'image de l'écran d'échec du système d'exploitation s'affiche sur votre écran.

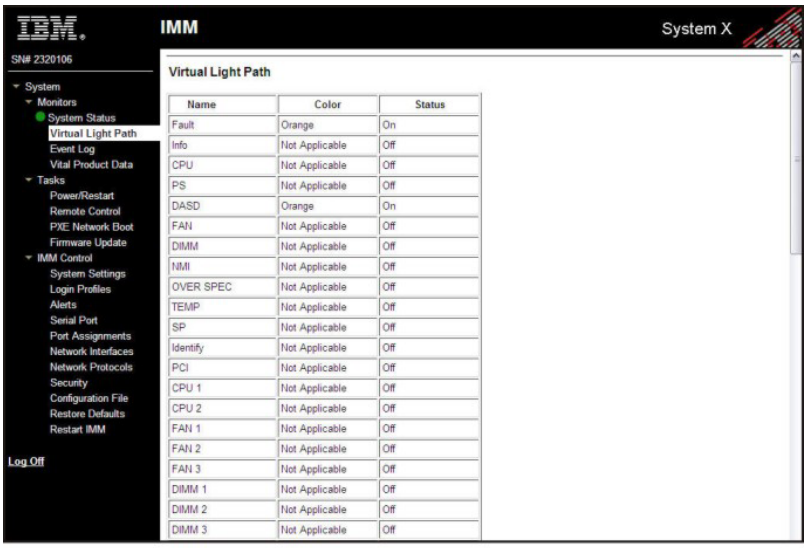
7. Accédez à la zone **Users Currently Logged in**. L'interface Web d'IMM affiche l'ID de connexion et la méthode d'accès de chaque utilisateur connecté à IMM.
8. Accédez à la zone **System Locator LED**. L'interface Web d'IMM affiche l'état du voyant de localisation système. Elle fournit également des boutons permettant de modifier l'état du voyant. Pour la signification des graphiques affichés dans cette zone, reportez-vous à l'aide en ligne.

Affichage du témoin lumineux virtuel

L'écran Virtual Light Path affiche le nom, la couleur et l'état des voyants allumés sur le serveur.

Pour accéder à l'écran Virtual Light Path, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Virtual Light** pour afficher l'historique récent des événements sur le serveur. Une page similaire à celle de la figure ci-après s'affiche.



3. Déplacez-vous vers le bas de l'écran pour visualiser le contenu complet de l'écran Virtual Light Path.

   Remarque : Si un voyant n'est pas allumé sur le serveur, la colonne Color du tableau Virtual Light Path indique que le paramètre Color du voyant ne s'applique pas.

Affichage des journaux d'événements

Remarque : Pour une explication de message ou d'événement spécifique, consultez la documentation de votre serveur.
Les codes et messages d'erreur sont affichés dans les types suivants de journaux d'événements :

- **Journal des événements système** : Ce journal contient des événements POST et SMI (system management interrupt), ainsi que tous les événements générés par le contrôleur BMC intégré dans le module IMM. Vous pouvez afficher ce journal via l'utilitaire Setup et le programme DSA (Dynamic System Analysis), comme le journal d'événements IPMI.

  La taille du journal des événements du système est limitée. Lorsque le journal est saturé, les nouvelles entrées n'écrasent pas les entrées existantes. Par conséquent, vous devez régulièrement , sauvegarder, puis effacer le contenu du journal des événements système via l'utilitaire Setup. Lors de l'identification et de la résolution des problèmes, il se peut que vous deviez sauvegarder puis effacer le journal des événements système pour rendre disponibles pour leur analyse les événements les plus récents.

  Les messages sont répertoriés sur le côté gauche de l'écran, et les détails concernant le message sélectionné s'affichent sur le côté droit de l'écran. Pour passer d'une entrée à l'autre, utilisez les touches flèche vers le haut (↑) et flèche vers le bas (↓).

  Le journal des événements système consigne un événement d'assertion lorsqu'un événement se produit. Il consigne un événement d'annulation d'assertion une fois que l'événement ne se produit plus.

  Certains détecteurs d'Integrated Management Module provoquent la consignation d'événements d'assertion lorsque leur valeur de consigne est

atteinte. Lorsqu'une condition de valeur de consigne n'existe plus, un événement de désassertion correspondant est consigné. Toutefois, tous les événements ne sont pas du type assertion.

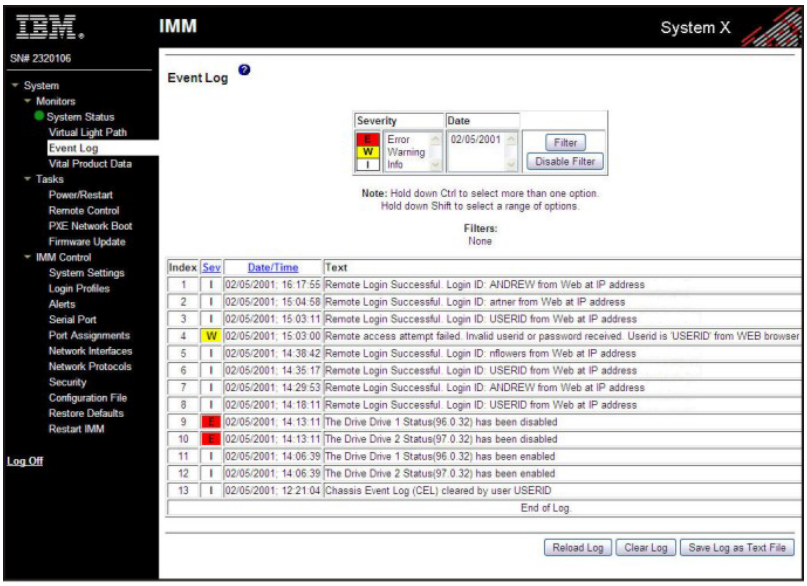
- **Journal des événements du module IMM** : Ce journal contient un sous-ensemble filtré de tous les événements IMM, POST et SMI (System Management Interrupt). Vous pouvez consulter ce journal depuis l'interface Web d'IMM et via le programme DSA (Dynamic System Analysis), comme le journal des événements ASM.
- **Journal DSA** : Ce journal est généré par le programme DSA et fusionne chronologiquement le journal d'événements système (comme le journal d'événements IPMI), le journal d'événements de châssis IMM (comme le journal d'événements ASM) et les journaux d'événements du système d'exploitation. Vous pouvez visualiser le journal DSA via programme DSA.
- **Journal des événements de châssis** : le module IMM génère des messages texte pour les événements d'assertion et d'annulation d'assertion IPMI et crée des entrées pour celles-ci dans le journal des événements de châssis. Le texte est généré pour ces événements via les spécifications DMTF (Distributed Management Task Force) DSP0244 et DSP8007. Ce journal contient également des entrées pour des événements autres que des assertions et annulations d'assertion du capteur IPMI. Il comprend, par exemple, des entrées lorsqu'un utilisateur modifie un paramètre réseau ou lorsqu'un utilisateur se connecte à l'interface Web. Ce journal peut être consulté à partir de l'interface Web d'IMM.

Affichage du journal des événements système depuis l'interface Web

Remarque : La taille du journal des événements système est limitée. Lorsque cette limite est atteinte, les événements les plus anciens sont supprimés sur la base du premier entré, premier sorti.

Pour accéder et consulter le journal des événements, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Event Log** pour afficher l'historique récent des événements sur le serveur. Une page similaire à celle de la figure ci-après s'affiche.



3. Déplacez-vous vers le bas de l'écran pour visualiser le contenu complet du journal d'événements. Les niveaux de gravité suivants sont attribués aux événements :

   Informational
   Ce niveau de gravité est affecté à un événement dont vous devez prendre note.

   Warning
   Ce niveau de gravité est affecté à un événement susceptible d'affecter les performances du serveur.

   Error Ce niveau de gravité est affecté à un événement qui nécessite votre attention immédiate.

   L'interface Web d'IMM différencie les événements d'avertissement en leur affectant dans la colonne de gravité la lettre W sur arrière-plan jaune et les événements d'erreur identifiés par la lettre E sur arrière-plan rouge.
4. Cliquez sur **Save Log as Text File** pour enregistrer le contenu du journal d'événements sous forme de fichier texte. Cliquez sur **Reload Log** pour actualiser l'affichage du journal d'événements. Cliquez sur **Clear Log** pour effacer le contenu du journal d'événements.

Affichage des journaux d'événements depuis l'utilitaire Setup

Pour des informations complètes sur l'utilisation de l'utilitaire Setup, voir la documentation fournie avec votre serveur.

Pour consulter le journal des événements de l'autotest à la mise sous tension, procédez comme suit.

1. Mettez le serveur sous tension.

   Remarque : Environ 2 minutes après la connexion du serveur au courant alternatif, le bouton de contrôle de l'alimentation devient actif.
2. A l'invite `<F1> Setup`, appuyez sur la touche F1. Si vous avez défini un mot de passe administrateur et un mot de passe à la mise sous tension, vous devez taper le mot de passe administrateur pour afficher les journaux des événements.

3. Sélectionnez **System Event Logs** et utilisez l'une des procédures suivantes :
   - Pour afficher le journal des événements de l'autotest à la mise sous tension, sélectionnez **POST Event Viewer**.
   - Pour afficher le journal des événements système, sélectionnez **System Event Log**.

Affichage des journaux des événements sans redémarrer le serveur

Si le serveur n'est pas bloqué, plusieurs méthodes vous permettent de visualiser des journaux d'événements sans avoir à redémarrer le serveur.

Si vous avez installé la version portable ou installable de Dynamic System Analysis (DSA), vous pouvez utiliser ce programme pour afficher le journal des événements système (comme le journal des événements IPMI), le journal des événements IMM (comme le journal des événements ASM), les journaux d'événements du système d'exploitation ou le journal DSA fusionné. Vous pouvez également utiliser le programme DSA Preboot pour consulter ces journaux, bien que pour ce faire vous deviez redémarrer le serveur. Pour installer Portable DSA, Installable DSA ou DSA Preboot, ou pour télécharger une image CD de DSA Preboot, accédez à l'adresse http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-DSA&brandind=5000008 ou procédez comme suit.

Remarque : Des modifications sont apportées périodiquement au site Web d'IBM. Il se peut que la procédure réelle soit légèrement différente de celle qui est décrite dans le présent document.

1. Accédez au site http://www.ibm.com/systems/support/.
2. Sous **Product support**, cliquez sur **System x**.
3. Sous **Popular links**, cliquez sur **Software and device drivers**.
4. Sous **Related downloads**, cliquez sur **Dynamic System Analysis (DSA)** pour afficher la liste des fichiers DSA téléchargeables.

Si IPMItool est installé sur le serveur, vous pouvez l'utiliser pour afficher le journal des événements du système. Les versions les plus récentes du système d'exploitation Linux disposent d'une version d'IPMItool. Pour plus d'informations sur IPMItool, visitez le site http://sourceforge.net/.

Remarque : Des modifications sont apportées périodiquement au site Web d'IBM. Il se peut que la procédure réelle soit légèrement différente de celle qui est décrite dans le présent document.

1. Accédez au site http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp.
2. Dans le panneau de navigation, cliquez sur **IBM System x and BladeCenter Tools Center**.
3. Développez successivement **Tools reference**, **Configuration tools**, **IPMI tools**, puis cliquez sur **IPMItool**.

Pour une présentation d'IPMI, accédez au site http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/liaai/ipmi/liaaiipmi.htm ou procédez comme suit.

1. Accédez au site http://publib.boulder.ibm.com/infocenter/systems/index.jsp.
2. Dans le panneau de navigation, cliquez sur **IBM Systems Information Center**.

3. Développez successivement **Operating systems**, **Linux information**, **Blueprints for Linux on IBM systems**, puis cliquez sur **Using Intelligent Platform Management Interface (IPMI) on IBM Linux platforms**.

Vous pouvez afficher le journal d'événements IMM à l'aide du lien **Event Log** dans l'interface Web d'IMM.

Le tableau suivant décrit les méthodes vous permettant d'afficher les journaux des événements, en fonction de la condition du serveur. Les deux premières conditions ne requièrent généralement pas le redémarrage du serveur.

Tableau 16. Méthodes d'affichage des journaux des événements

Condition	Action
Le serveur n'est pas bloqué et il est connecté à un réseau.	Utilisez l'une des méthodes suivantes : • Exécutez Portable ou Installable DSA pour afficher les journaux d'événements ou créez un fichier de sortie que vous pourrez envoyer au service d'assistance IBM. • Entrez l'adresse IP d'IMM et accédez à la page Event Log. • Utilisez IPMItool pour afficher le journal des événements système.
Si le serveur n'est pas bloqué et n'est pas connecté à un réseau.	Utilisez localement IPMItool pour consulter le journal des événements système.
Le serveur est bloqué.	• Si DSA Preboot est installé, redémarrez le serveur et appuyez sur la touche F2 pour lancer DSA Preboot et afficher les journaux d'événements. • Si DSA Preboot n'est pas installé, insérez le CD DSA Preboot CD et redémarrez le serveur pour lancer DSA Preboot et afficher les journaux d'événements. • Vous pouvez également redémarrer le serveur et appuyer sur F1 pour lancer l'utilitaire de configuration et afficher le journal des événements de l'autotest à la mise sous tension. Pour plus d'informations, voir «Affichage des journaux d'événements depuis l'utilitaire Setup», à la page 110.

Affichage des données techniques essentielles

Au démarrage du serveur, IMM collecte des informations sur le serveur, sur son microprogramme et des données techniques essentielles sur ses composants et stocke celles-ci en mémoire non volatile. Vous pouvez accéder à ces informations à tout moment depuis presque n'importe quel ordinateur. La page Vital Product Data contient des informations clés sur le serveur distant géré sous suivi par IMM.

Pour afficher les données techniques essentielles des composants du serveur, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.

2. Dans le panneau de navigation, cliquez sur **Vital Product Data** pour visualiser le statut des composants matériels et logiciels sur le serveur.
3. Faites défiler la page vers le bas pour examiner les relevés suivants des données techniques essentielles :

Machine level VPD

Les données techniques essentielles du serveur sont présentées dans cette zone. Pour l'affichage des données techniques essentielles, celles au niveau machine incluent un identificateur unique universel (UUID).

Remarque : Les données techniques essentielles au niveau machine, au niveau composant et le journal d'activité des composants ne fournissent des informations que lorsque le serveur est sous tension.

Tableau 17. Données techniques essentielles au niveau machine

Zone	Fonction
Machine type and model	Identifie le type de serveur et le numéro de modèle surveillé par IMM.
Serial Number	Identifie le numéro de série du serveur surveillé par IMM.
UUID	Identifie l'identificateur unique universel (UUID), représenté par un nombre hexadécimal à 32 chiffres, du serveur surveillé par IMM.

Component Level VPD

Les données techniques essentielles des composants du serveur distant géré sont affichées dans cette zone.

Tableau 18. Données techniques essentielles au niveau composant

Zone	Fonction
FRU name	Identifie l'unité remplaçable sur site (FRU) pour chaque composant.
Serial Number	Identifie le numéro de série de chaque composant.
Mfg ID	Identifie l'ID fabricant pour chaque composant.

Component Activity Log

Vous pouvez visualiser dans cette zone un enregistrement de l'activité du composant.

Tableau 19. Journal d'activité du composant

Zone	Fonction
FRU name	Identifie l'unité remplaçable sur site (FRU) du composant.
Serial Number	Identifie le numéro de série du composant.
Mfg ID	Identifie le fabricant du composant.
Action	Identifie l'action entreprise pour chaque composant.
Timestamp	Identifie la date et l'heure de l'action du composant. La date est affichée au format *mm/jj/aa*. L'heure est affichée au format *hh:mm:ss*.

IMM VPD

Les données techniques essentielles du microprogramme IMM, du microprogramme du serveur System x et du microprogramme DSA (Dynamic System Analysis) pour le serveur distant géré sont affichées dans cette zone.

Tableau 20. Données techniques essentielles IMM, UEFI et DSA

Zone	Fonction
Firmware type	Indique le type de code de microprogramme.
Version string	Indique la version du code de microprogramme.
Release date	Indique quand le microprogramme a été publié.

Chapitre 5. Exécution de tâches IMM

Utilisez les fonctions sous l'en-tête **Tasks** dans le panneau de navigation pour contrôler directement les actions du module IMM et de votre serveur. Les tâches que vous pouvez effectuer dépendent du serveur sur lequel le module IMM est installé.

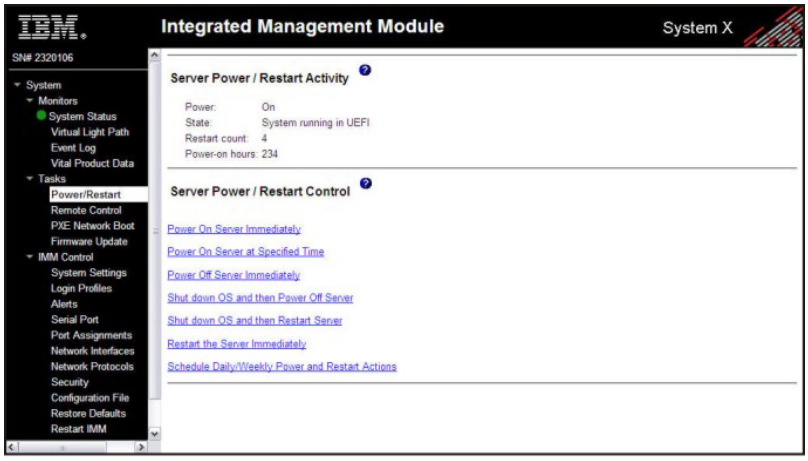
Vous pouvez effectuer les tâches suivantes :

- Afficher l'activité de mise sous tension et de redémarrage du serveur
- Contrôler à distance le statut d'alimentation du serveur
- Accéder à distance à la console du serveur
- Rattacher à distance un disque ou une image disque au serveur
- Mettre à jour le microprogramme IMM

Remarque : Certaines fonctions ne sont disponibles que sur les serveurs exécutant un système d'exploitation Microsoft Windows pris en charge.

Affichage de l'état d'alimentation et de l'activité de redémarrage du serveur

La zone **Server Power/Restart Activity** affiche l'état d'alimentation du serveur au moment où la page Web a été générée.



Alimentation
Cette zone affiche l'état d'alimentation du serveur lorsque la page Web actuelle a été générée.

Etat Cette zone affiche l'état du serveur lorsque la page Web actuelle a été générée. Les états possibles sont les suivants :

- System power off/State unknown (Système hors tension/Etat inconnu)
- System on/starting UEFI (Système sous tension/démarrage UEFI)
- System stopped in UEFI (Error detected) (Système arrêté dans UEFI - Erreur détectée)
- System running in UEFI (Système en cours d'exécution dans UEFI)

- Booting OS or in unsupported OS (Amorçage du système OS ou système d'exploitation non pris en charge - Peut être dans le système d'exploitation si le système d'exploitation n'est pas configuré pour prendre en charge l'interface intrabande à l'IMM)
- OS booted (Système d'exploitation démarré))

Restart count
Cette zone indique le nombre de redémarrages du serveur.

Remarque : Le compteur est remis à zéro chaque fois que le sous-système IMM est restauré à ses paramètres usine par défaut.

Power-on hours
Cette zone indique le nombre d'heures total pendant lesquelles le serveur a été sous alimentation.

Contrôle du statut d'alimentation d'un serveur

Le module IMM permet un contrôle complet de l'alimentation de votre serveur avec des actions de mise sous tension, de mise hors tension et de redémarrage. De plus, des statistiques sur l'alimentation et le redémarrage sont collectées et affichées pour indiquer l'état de disponibilité du matériel du serveur. Pour exécuter les actions de la zone **Server Power/Restart Control**, vous devez disposer d'un accès Superviseur à IMM.

Pour effectuer les actions relatives à l'alimentation et au redémarrage du serveur, procédez comme suit.

Remarque : Sélectionnez les options suivantes uniquement en cas d'urgence, ou si vous êtes hors site et que le serveur ne répond.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Power/Restart**. Accédez à la zone **Server Power/Restart Control**.
3. Sélectionnez l'une des options suivantes :

Power on server immediately
Met sous tension le serveur et lance le système d'exploitation.

Power on server at specified time
Met sous tension le serveur à l'heure spécifiée et lance le système d'exploitation.

Power off server immediately
Met hors tension le serveur sans arrêter le système d'exploitation.

Shut down OS and then power off server
Arrête le système d'exploitation, puis met hors tension le serveur.

Remarque : Si le système d'exploitation est en mode écran de veille ou verrouillé lorsqu'une demande "Shut down OS and then power off server" est traitée, il se peut qu'IMM ne puisse pas déclencher un arrêt ordonné. IMM exécutera une réinitialisation ou un arrêt immédiat à l'expiration du délai de mise hors tension même si le système d'exploitation est toujours en opération.

Shut down OS and then restart server
Redémarre le système d'exploitation.

Remarque : Si le système d'exploitation est en mode écran de veille ou verrouillé lorsqu'une demande "Shut down OS and then restart server" est traitée, il se peut qu'IMM ne puisse pas déclencher un arrêt ordonné. IMM exécutera une réinitialisation ou un arrêt immédiat à l'expiration du délai de mise hors tension même si le système d'exploitation est toujours en opération.

Restart the server immediately
Met sous tension le serveur et le remet sous tension immédiatement sans arrêter tout d'abord le système d'exploitation.

Schedule daily/weekly power and restart actions
Arrête le système d'exploitation et met hors tension le serveur sur la base quotidienne ou hebdomadaire spécifiée (en redémarrant ou non le serveur), et met sous tension le serveur à une heure quotidienne ou hebdomadaire spécifiée.

Un message de confirmation s'affiche si vous sélectionnez l'une de ces options, et vous pouvez annuler l'opération si elle a été sélectionnée par inadvertance.

Intervention à distance

Remarque :

1. La fonction IMM d'intervention à distance est disponible uniquement dans le module IMM Premium. Pour plus d'informations sur la mise à niveau de module standard vers IMM Premium, voir «Mise à niveau depuis IMM Standard vers IMM Premium», à la page 5.
2. La fonction de contrôle à distance est disponible uniquement dans l'interface Web d'IMM. Pour utiliser les fonctions de contrôle à distance, vous devez vous connecter à IMM avec un ID disposant d'un accès Superviseur.

Vous pouvez utiliser la fonction d'intervention à distance, ou la fonction de contrôle à distance dans l'interface Web d'IMM, pour afficher et interagir avec la console du serveur. Vous pouvez également affecter au serveur une unité de CD ou de DVD, une unité de disquette, une unité USB Flash ou une image de disque sur votre ordinateur.

La fonction de contrôle à distance fournit les fonctionnalités suivantes :

- Visualisation de vidéo à distance avec des résolutions graphiques allant jusqu'à 1280 x 1024 à 75 Hz, quel que soit l'état du système
- Accès à distance au serveur, à l'aide du clavier et de la souris à partir d'un client distant
- Mappage de l'unité de CD/DVD, de l'unité de disquette et de l'unité flash USB sur un client distant ; mappage ISO et fichiers image de disquette en tant qu'unités virtuelles accessibles via le serveur.
- Téléchargement d'une image de disquette vers la mémoire du module IMM et mappage de cette dernière sur le serveur en tant qu'unité virtuelle.

Mise à jour du microprogramme IMM et d'applet Java ou ActiveX

Important : IMM utilise une applet Java ou ActiveX pour exécuter la fonction d'intervention à distance. Lorsqu'IMM est mis à jour vers le dernier niveau du microprogramme, l'applet Java et l'applet ActiveX sont elles aussi mises à jour vers le niveau le plus récent. Par défaut, Java met en cache (stocke localement) les

applets utilisées auparavant. Après une mise à jour flash du microprogramme IMM, il se peut que l'applet Java utilisée par le serveur ne soit pas au niveau le plus récent.

Pour corriger ce problème, procédez comme suit.

1. Cliquez sur **Démarrer → Paramètres → Panneau de configuration**.
2. Double-cliquez sur **plug-in Java 1,5**. La fenêtre de plug-in Java du panneau de configuration s'ouvre.
3. Cliquez sur l'onglet **Cache**.
4. Sélectionnez l'une des options suivantes :
   - Décochez la case **Activer la mise en cache** de sorte que la mise en cache Java soit toujours désactivée.
   - Cliquez sur **Vider le cache**. Si vous choisissez cette option, vous devez cliquer sur **Clear Caching** après chaque mise à jour du microprogramme IMM.

Pour plus d'informations sur la mise à jour du microprogramme IMM, voir «Mise à niveau du microprogramme», à la page 128.

Activation de la fonction d'intervention à distance

Remarque : La fonction IMM d'intervention à distance est disponible uniquement dans le module IMM Premium. Pour plus d'informations sur la mise à niveau de module standard vers IMM Premium, voir «Mise à niveau depuis IMM Standard vers IMM Premium», à la page 5.

Pour activer la fonction d'intervention à distance, procédez comme suit.

1. Coupez l'alimentation du serveur en débranchant le cordon d'alimentation.
2. Installez la clé de média virtuel dans l'emplacement dédié sur la carte mère.
3. Rétablissez l'alimentation du serveur.

   Remarque : Environ 2 minutes après la connexion du serveur au courant alternatif, le bouton de contrôle de l'alimentation devient actif.
4. Mettez le serveur sous tension.

Contrôle à distance

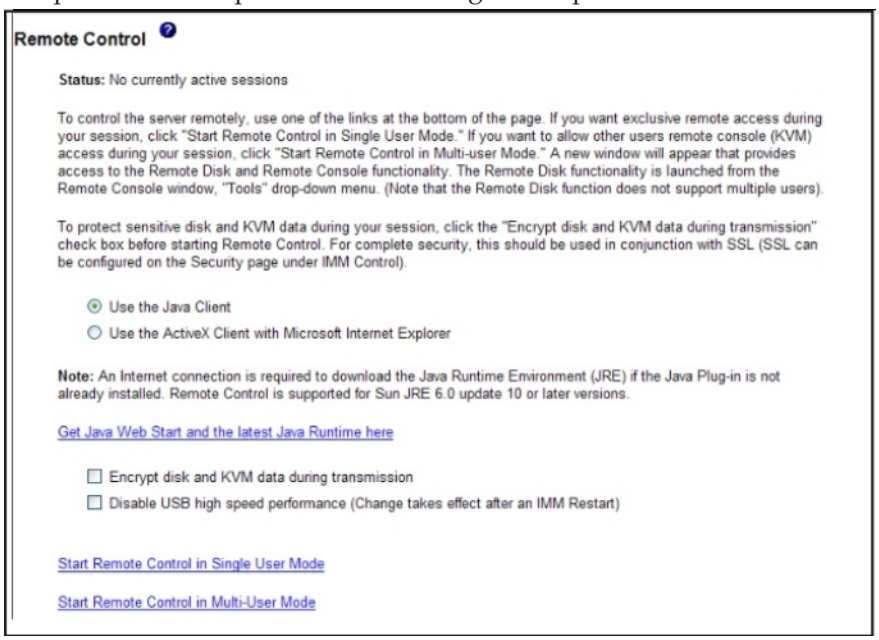
La fonction de contrôle à distance du module IMM est constituée de deux applications Java dans deux fenêtres distinctes :

Video Viewer
Video Viewer utilise une console distante pour gestion des systèmes distants. Une console distante est un affichage d'interface graphique interactive du serveur , visible sur votre ordinateur. Votre écran affiche exactement ce qui figure sur la console du serveur et vous pouvez contrôler la console via le clavier et la souris.

Virtual Media Session
La fenêtre Virtual répertorie toutes les unités sur le client qui peuvent être mappées en tant qu'unités distantes. Elle vous permet de mapper des fichiers ISO et d'images de disquette en tant qu'unités virtuelles. Chaque unité mappée peut être marquée comme étant en lecture seule. Les unités de CD et de DVD et les images ISO sont toujours en lecture seule.

Pour accéder à distance à une console serveur, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Remote Control**. Une page comparable à celle présentée dans la figure ci-après s'affiche.



3. Sélectionnez l'une des options suivantes :
   - Cliquez sur **Use the Java Client** pour utiliser l'applet Java pour les interventions à distance.
   - Cliquez sur **Use the ActiveX Client with Microsoft Internet Explorer** pour utiliser Internet Explorer sous les systèmes d'exploitation Windows si vous désirez utiliser l'applet ActiveX pour les interventions à distance.

     Remarque : Le client d'intervention à distance ActiveX 32 bits est disponible avec le microprogramme IMM version 1.28 (ou version ultérieure). le client ActiveX 64 bits est disponible avec le microprogramme IMM version 1.30 ou ultérieure.
4. Pour contrôler à distance le serveur, utilisez l'un des liens au bas de la page Remote Control. Si vous désirez un accès à distance exclusif lors de votre session, cliquez sur **Start Remote Control in Single User Mode**. Si vous désirez autoriser d'autres utilisateurs à disposer d'un accès de console distante (KVM) au cours de votre session, cliquez sur **Start Remote Control in Multi-user Mode**. De nouvelles fenêtres fournissant un accès aux fonctionnalités Remote Disk et Remote Console s'ouvrent.

   Si la case **Encrypt disk and KVM data during transmission** a été cochée avant l'ouverture de la fenêtre Remote Control, les données du disque sont chiffrées avec le chiffrement ADES.

Fermez la fenêtre Video Viewer, ainsi que la fenêtre Virtual Media Session, lorsque vous avez fini d'utiliser la fonction Remote Control.

Remarques :

1. Ne fermez pas la fenêtre Virtual si un disque distant est actuellement mappé. Voir «Disque distant», à la page 125 pour les instructions de fermeture et d'annulation du mappage d'un disque distant.

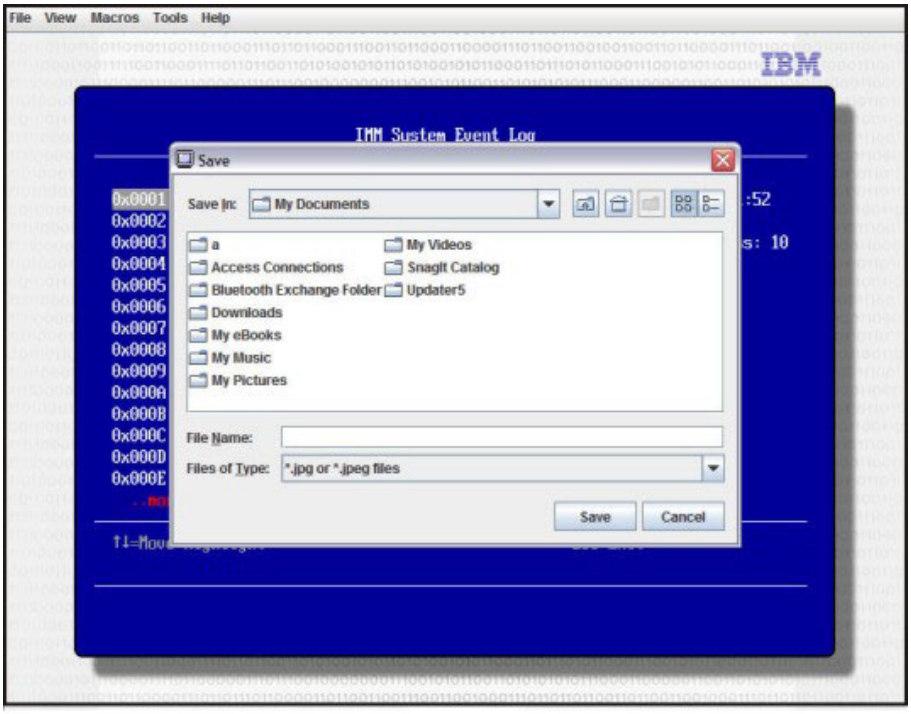
2. Si vous rencontrez des problèmes avec le clavier ou la souris lorsque vous utilisez la fonction Remote Control, consultez l'aide accessible depuis la page Remote Control dans l'interface Web.
3. Si vous utilisez la console distante pour modifier des paramètres IMM dans l'utilitaire Setup, il se peut que le serveur redémarre le module IMM. Vous perdrez dans ce cas la console distante et la session de connexion. Après un bref délai, vous pourrez vous reconnecter à IMM en ouvrant une nouvelle session, redémarrer la console distante et quitter l'utilitaire Setup.

Capture d'écran par la fonction de contrôle à distance

La fonction de capture d'écran dans la fenêtre Video Viewer capture le contenu de l'affichage vidéo sur le serveur. Pour capturer et enregistrer une image écran, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **File**.
2. Sélectionnez l'option **Capture to File** dans le menu.
3. A l'invite, attribuez un nom au fichier image et enregistrez-le à l'emplacement de votre choix sur le client local.

Remarque : Les images des captures d'écran sont enregistrées sous le type de fichier JPG ou JPEG.



Modes d'affichage de contrôle à distance Video Viewer

Pour modifier l'affichage de la fenêtre Video Viewer, cliquez sur **View**. Les options de menu disponibles sont les suivantes :

Refresh

La visionneuse vidéo retrace l'affichage vidéo avec les données vidéo du serveur.

Full Screen
L'afficheur Video Viewer remplit le bureau du client avec l'affichage vidéo. Cette option n'est disponible que lorsque Video Viewer n'est pas en mode plein écran.

Windowed
Video Viewer bascule du mode plein écran au mode fenêtre. Cette option n'est disponible que lorsque Video Viewer est en mode plein écran.

Fit Video Viewer redimensionne l'affichage afin de couvrir le bureau du client sans bordure supplémentaire ou barres de défilement. Ceci requiert que le bureau du client soit suffisamment spacieux pour afficher la fenêtre redimensionnée.

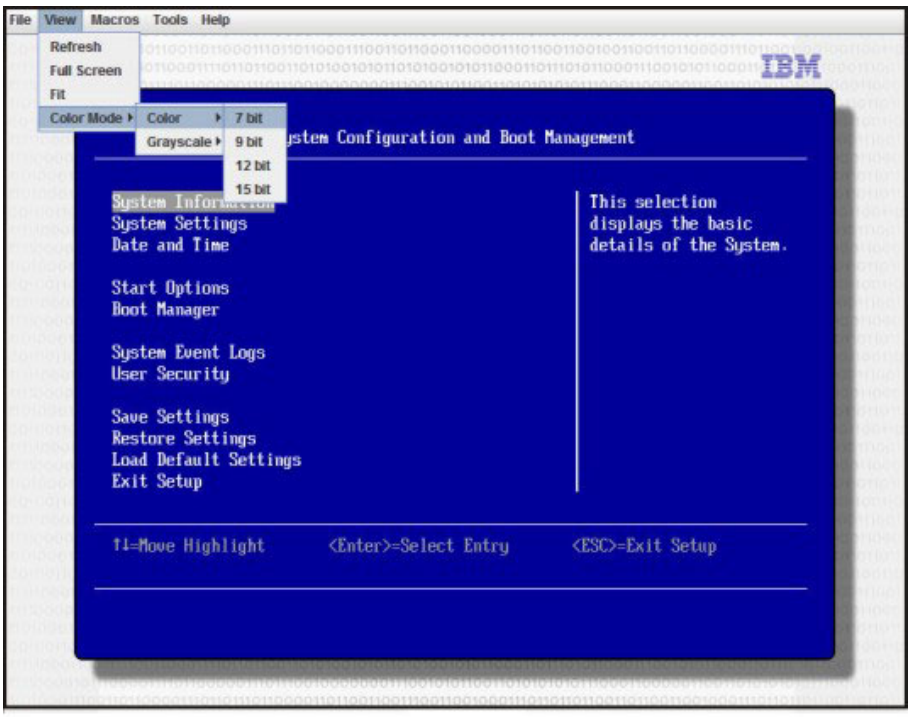
Mode couleur vidéo de la fonction de contrôle à distance

Si votre connexion au serveur distant dispose d'une bande passante limitée, vous pouvez réduire la demande de bande passante de Video Viewer en ajustant les paramètres de couleur dans la fenêtre Video Viewer.

Remarque : Au lieu du curseur de bande passante de l'interface Remote Supervisor Adapter II, IMM dispose d'un élément de menu permettant l'ajustement de la profondeur de couleur afin de réduire la quantité de données transmise dans les situations de bande passante limitée.

Pour changer le mode couleur vidéo, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **View**.
2. Lorsque vous positionnez le pointeur de la souris sur **Color Mode** dans le menu, deux options de mode couleur sont affichées :
   - Color: 7, 9, 12 et 15 bits
   - Grayscale: 16, 32, 64, 128 teintes

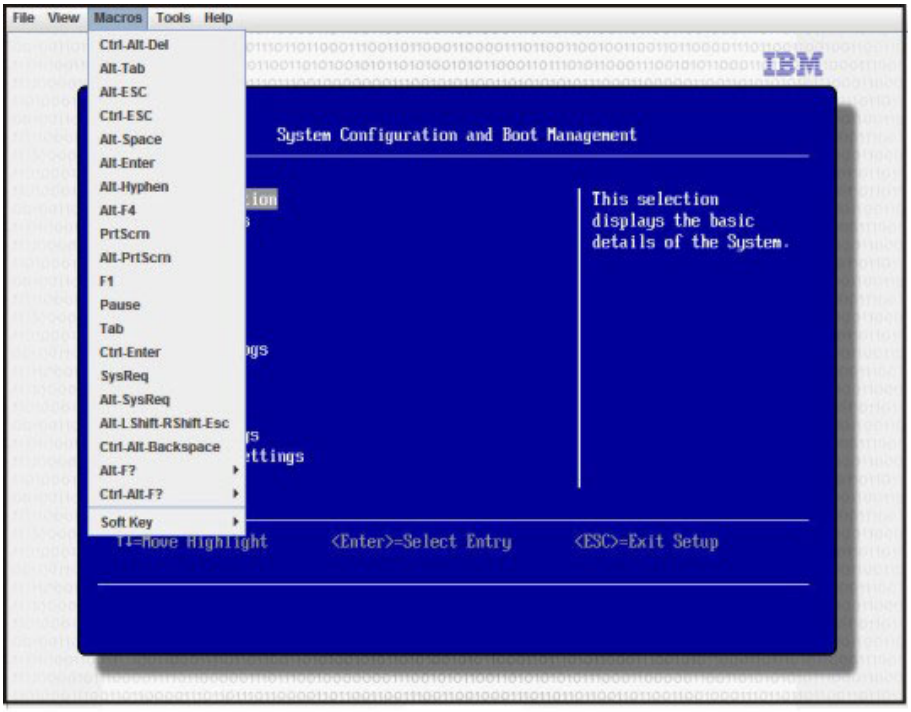


3. Sélectionnez le paramètre color (couleur) ou le paramètre grayscale (nuances de gris).

Prise en charge du clavier par la fonction de contrôle à distance

Le système d'exploitation sur le serveur client que vous utilisez intercepte certaines combinaisons de touches, telles que Ctrl+Alt+Suppr dans Microsoft Windows, au lieu de les transmettre au serveur. D'autres touches, telles que F1, peuvent provoquer une action sur votre ordinateur de même que sur le serveur. Pour utiliser des combinaisons de touches affectant le serveur distant et non pas le client local, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **Macros**.
2. Sélectionnez dans le menu l'une des combinaisons de touches prédéfinies ou sélectionnez **Soft Key** pour choisir ou ajouter une combinaison de touches définie par l'utilisateur.



Utilisez l'élément de menu **Macros** de Video Viewer pour créer et éditer des boutons personnalisés que vous pourrez utiliser pour envoyer des séquences de touches au serveur.

Pour créer et éditer des boutons personnalisés, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **Macros**.
2. Sélectionnez **Soft Key**, puis **Add**. Une nouvelle fenêtre s'ouvre.
3. Cliquez sur **New** pour ajouter une nouvelle combinaison de touches ou sélectionnez-en une et cliquez sur **Delete** pour supprimer une combinaison de touches existante.
4. Si vous ajoutez une nouvelle combinaison, entrez la combinaison que vous désirez définir dans la fenêtre en incrustation et cliquez sur **OK**.

5. Lorsque vous avez fini de définir ou de supprimer des combinaisons de touches, cliquez sur **OK**.

Prise en charge de clavier international

Video Viewer utilise un code natif spécifique à la plateforme pour intercepter les événements de touches afin d'accéder directement aux informations de touche physique. Le client détecte les événements de touche physique et les transmet au serveur. Le serveur détecte les mêmes frappes que celles identifiées par le client et prend en charge toutes les dispositions de clavier standard, l'unique limitation étant que le serveur et le client utilisent la même disposition de clavier. Si un utilisateur distant utilise une disposition de clavier différente de celle du serveur, l'utilisateur peut changer celle du serveur lors de son accès à distance, puis la rétablir.

Clavier en mode pass-through (mode de transfert direct)

Cette fonction désactive le traitement de la plupart des combinaisons de touches spéciales de sorte à pouvoir transmettre ces frappes directement au serveur. Ceci fournit une alternative à l'utilisation de macros.

Certains systèmes d'exploitation définissent certaines frappes comme n'étant pas sous le contrôle d'une application, par conséquent le comportement du mécanisme de transfert direct opère indépendamment du serveur. Par exemple, dans une session Linux X, la combinaison de touches Ctrl+Alt+F2 bascule vers la console virtuelle 2. Aucun mécanisme ne permet d'intercepter cette séquence de touches et, par conséquent, le client ne peut pas transmettre directement ces touches à la cible. La seule option dans ce cas consiste à utiliser les macros clavier définies à cet effet.

Pour activer ou désactiver le mode clavier pass-through, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **Tools**.
2. Sélectionnez **Session Options** dans le menu.
3. Lorsque la fenêtre Session Options s'affiche, cliquez sur l'onglet **General**.
4. Cochez ou décochez la case **Pass all keystrokes to target** pour activer ou désactiver cette fonction.
5. Cliquez sur **OK** pour enregistrer votre sélection.

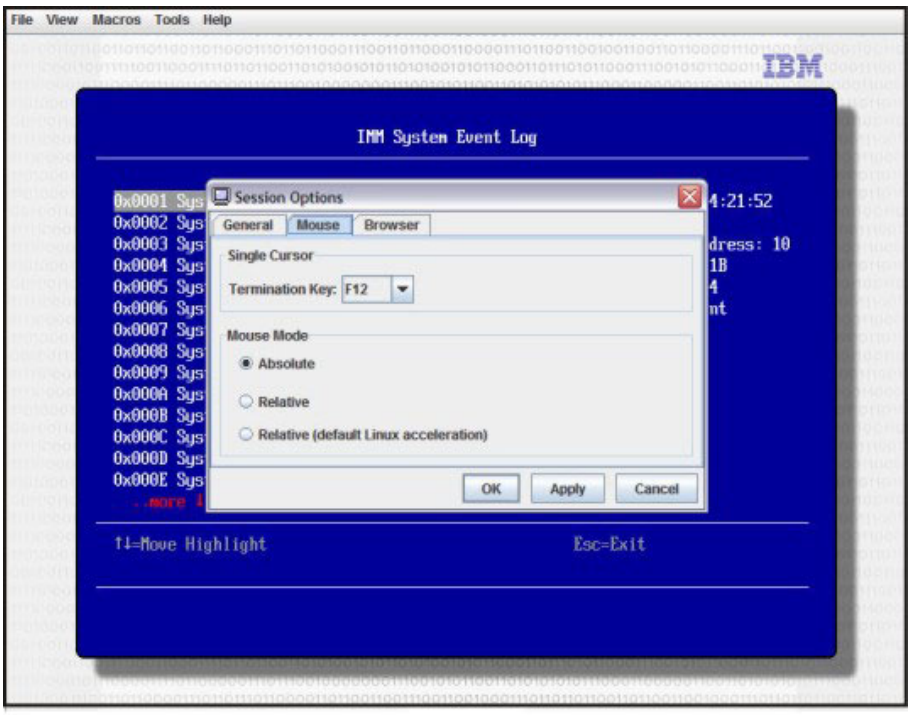
Prise en charge de la souris par la fonction de contrôle à distance

La fenêtre Video Viewer propose plusieurs options pour le contrôle de la souris, y compris le contrôle absolu de la souris, le contrôle relatif de la souris, et le mode curseur simple.

Contrôle absolu et relatif de la souris

Pour accéder aux options de contrôle absolu et relatif de la souris, procédez comme suit.

1. Dans la fenêtre Remote Control, cliquez sur **Tools**.
2. Sélectionnez **Session Options** dans le menu.
3. Lorsque la fenêtre Session Options s'affiche, cliquez sur l'onglet **Mouse**.



4. Sélectionnez l'un des modes suivants pour la souris :

   Absolute
   Le client envoie au serveur des messages d'emplacement de la souris relatifs à l'origine (angle supérieur gauche) de la zone d'affichage.

   Relative
   Le client envoie l'emplacement de la souris en tant que décalage par rapport à la position précédente.

   Relative (default Linux acceleration)
   Le client applique un facteur d'accélération pour mieux aligner la souris sur les cibles Linux. Les paramètres d'accélération ont été sélectionnés pour optimiser la compatibilité avec les distributions Linux.

Mode de curseur unique

Certains systèmes d'exploitation ne synchronisent pas le curseur local et le curseur distant, ce qui entraîne des décalages entre-eux. Le mode de curseur unique masque le curseur du client local lorsque la souris est positionnée dans la fenêtre Video Viewer. Lorsque ce mode est activé, seul le curseur distant est visible.

Pour activer le mode de curseur unique, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **Tools**.
2. Sélectionnez **Single Cursor**.

Lorsque Video Viewer opère en mode de curseur unique, vous ne pouvez pas basculer vers une autre fenêtre ou cliquer hors de la fenêtre du client KVM, vu qu'un curseur local n'est pas disponible. Pour désactiver le mode de curseur unique, appuyez sur la touche définie pour y mettre fin. Pour afficher cette touche ou la modifier, cliquez sur **Tools > Session Options > Mouse**.

Contrôle à distance de l'alimentation

Vous pouvez envoyer des commandes de contrôle de l'alimentation et de redémarrage du serveur depuis la fenêtre Video Viewer sans besoin de revenir au navigateur Web. Pour contrôler l'alimentation du serveur à l'aide de Video Viewer, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **Tools**.
2. Lorsque vous positionnez le pointeur de la souris sur **Power** dans le menu, les options suivantes sont affichées :

   On Met sous tension le serveur.

   Off Met hors tension le serveur.

   Reboot
   Redémarre le serveur.

   Cycle Met le serveur hors tension, puis le remet sous tension.

Affichage des statistiques de performances

Pour afficher les statistiques de performances de Video Viewer, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **Tools**.
2. Cliquez sur **Stats**. La page contient les options suivantes :

   Frame Rate
   Moyenne mobile du nombre de cadres, décodé par seconde par le client.

   Bandwidth
   Moyenne mobile du nombre total de kilooctets par seconde reçu par le client.

   Compression
   Moyenne mobile de la réduction de la bande passante due à la compression vidéo. Cette valeur est souvent affiché comme 100,0 %. Elle est arrondie au dixième de pour cent.

   Packet Rate
   Moyenne mobile du nombre de paquets vidéo reçu par seconde.

Lancement du protocole RDP (Remote Desktop Protocol)

Si un client RDP (Remote Desktop Protocol) Windows est installé, vous pouvez basculer vers le client RDP au lieu d'utiliser le client KVM. Le serveur distant doit être configuré pour recevoir les connexions RDP.

Disque distant

Depuis la fenêtre Virtual Media Session, vous pouvez affecter au serveur une unité de CD ou de DVD, une unité de disquette, ou une unité USB Flash sur votre ordinateur ou spécifier une image de disque sur votre ordinateur afin que le serveur l'utilise. Vous pouvez utiliser l'unité pour des fonctions telles que le redémarrage (amorçage) du serveur, la mise à jour du code, l'installation de nouveaux logiciels sur le serveur et l'installation ou la mise à jour du système d'exploitation sur le serveur. Vous pouvez utiliser la fonction de contrôle à distance pour accéder au disque distant. Les unités et les images de disque sont affichées en tant qu'unités USB sur le serveur.

Remarques :

1. Les systèmes d'exploitation de serveur suivants prennent en charge la connexion USB, laquelle est requise pour la fonction de contrôle à distance :
   - Microsoft Windows Server 2008
   - Microsoft Windows Server 2003
   - Red Hat Linux versions 4.0 et 5.0
   - SUSE Linux version 10.0
   - Novell NetWare 6.5
2. Le serveur du client requiert le plug-in Java 1.5, ou ultérieur.
3. Le serveur du client doit disposer d'un microprocesseur Intel Pentium III, ou plus avancé, avec une vitesse d'horloge de 700 MHz, ou plus rapide, ou de leur équivalent.

Accès à la fonction Remote Control (accès à distance)

Pour lancer une session de contrôle à distance et accéder au disque distant, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **Remote Control**.
3. Sur la page Remote Control, cliquez sur l'une des options **Start Remote Control** :
   - Si vous désirez un accès distant exclusif au cours de votre session, cliquez sur **Start Remote Control in Single User Mode**.
   - Si vous désirez autoriser d'autres utilisateurs à disposer d'un accès de console distante (KVM) lors de votre session, cliquez sur **Start Remote Control in Multi-user Mode**.

   La fenêtre Video Viewer s'ouvre.
4. Pour ouvrir une fenêtre Virtual Media Session, cliquez sur **Tools** > **Launch Virtual Media** dans la fenêtre Video Viewer.

Remarque : Si la case **Encrypt disk and KVM data during transmission** a été cochée avant l'ouverture de la fenêtre Remote Control, les données du disque sont chiffrées avec le chiffrement ADES.
La fenêtre Virtual Media Session est distincte de la fenêtre Video Viewer. La fenêtre Virtual Media répertorie toutes les unités sur le client qui peuvent être mappées en tant qu'unités distantes. La fenêtre Virtual Media Session vous permet également de mapper des fichiers d'images ISO et de disquettes en tant qu'unités virtuelles. Chaque unité mappée peut être marquée comme étant en lecture seule. Les unités de CD et de DVD et les images ISO sont toujours en lecture seule.

Mappage et annulation du mappage d'unités avec le microprogramme IMM version 1.03 et versions ultérieures

Pour mapper une unité, cochez la case **Select** en regard de l'unité concernée.

Remarque : Un lecteur de CD ou de DVD doit contenir le média avant d'être mappé. Si le lecteur est vide, vous êtes invité à insérer un CD ou un DVD dans le lecteur.

Cliquez sur le bouton **Mount Selected** pour monter et mapper l'unité ou les unités sélectionnées.

Si vous cliquez sur **Add Image**, des fichiers image de disquette et ISO peuvent être ajoutés à la liste des unités disponibles. Une fois que le fichier image de disquette ou ISO est répertorié dans la fenêtre Virtual Media Session, il peut être mappé comme n'importe quelle autre unité.

Pour annuler le mappage des unités, cliquez sur le bouton **Unmount All**. Avant l'annulation du mappage des unités, vous devez confirmer cette annulation.

Remarque : Après que vous ayez confirmé l'opération, toutes les unités sont démontées. Vous ne pouvez pas démonter des unités individuellement.

Vous pouvez sélectionner un fichier image de disquette et enregistrer cette image dans la mémoire IMM. Ceci permet de maintenir le disque monté sur le serveur pour pouvoir y accéder ultérieurement, même après la clôture de la session d'interface Web d'IMM. Une seule image d'unité peut être stockée sur la carte IMM. Le contenu de l'unité ou de l'image ne doit pas dépasser 1,44 Mo. Pour télécharger sur la carte un fichier image de disquette, procédez comme suit.

1. Cliquez sur **RDOC**.
2. Lorsque la nouvelle fenêtre s'ouvre, cliquez sur **Upload**.
3. Cliquez sur **Browse** pour sélectionner le fichier image à utiliser.
4. Dans la zone **Name**, entrez un nom pour l'image et cliquez sur **OK** pour télécharger le fichier.

   Remarque : Pour décharger le fichier image de la mémoire, sélectionnez son nom dans la fenêtre RDOC Setup et cliquez sur **Delete**.

Mappage et annulation du mappage d'unités avec le microprogramme IMM version 1.02 et versions antérieures

Pour mapper une unité, cochez la case **Mapped** en regard de l'unité concernée.

Remarque : Un lecteur de CD ou de DVD doit contenir le média avant d'être mappé. Si le lecteur est vide, vous êtes invité à insérer un CD ou un DVD dans le lecteur.

Si vous cliquez sur **Add Image**, des fichiers image de disquette et ISO peuvent être ajoutés à la liste des unités disponibles. Une fois que le fichier image de disquette ou ISO est répertorié dans la fenêtre Virtual Media Session, il peut être mappé comme n'importe quelle autre unité.

Pour annuler le mappage d'une unité, décochez la case **Mapped** de l'unité concernée. Avant l'annulation du mappage de l'unité, vous devez confirmer cette annulation.

Vous pouvez sélectionner un fichier image de disquette et enregistrer cette image dans la mémoire IMM. Ceci permet de maintenir le disque monté sur le serveur pour pouvoir y accéder ultérieurement, même après la clôture de la session d'interface Web d'IMM. Une seule image d'unité peut être stockée sur la carte IMM. Le contenu de l'unité ou de l'image ne doit pas dépasser 1,44 Mo. Pour télécharger sur la carte un fichier image de disquette, procédez comme suit.

1. Cliquez sur **RDOC**.
2. Lorsque la nouvelle fenêtre s'ouvre, cliquez sur **Upload**.
3. Cliquez sur **Browse** pour sélectionner le fichier image à utiliser.
4. Dans la zone **Name**, entrez un nom pour l'image et cliquez sur **OK** pour télécharger le fichier.

Remarque : Pour décharger le fichier image de la mémoire, sélectionnez son nom dans la fenêtre RDOC Setup et cliquez sur **Delete**.

Sortie de la fonction Remote Control (Contrôle à distance)

Fermez la fenêtre Video Viewer, ainsi que la fenêtre Virtual Media Session, quand vous avez fini d'utiliser la fonction Remote Control.

Configuration de l'amorçage réseau PXE

Pour configurer votre serveur pour tenter un amorçage réseau PXE (Preboot Execution Environment) au prochain redémarrage du serveur, procédez comme suit.

1. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
2. Dans le panneau de navigation, cliquez sur **PXE Network Boot**.
3. Cochez la case **Attempt PXE network boot at next server restart**.
4. Cliquez sur **Save**.

Mise à niveau du microprogramme

Utilisez l'option Firmware Update sur le panneau de navigation pour mettre à jour le microprogramme d'IMM, du serveur System x et de DSA (Dynamic System Analysis).

Pour mettre à jour le microprogramme, procédez comme suit.

Remarque : Des modifications sont apportées périodiquement au site Web d'IBM. Il se peut que la procédure réelle soit légèrement différente de celle qui est décrite dans le présent document.

1. Téléchargez la dernière mise à jour du microprogramme applicable pour le serveur sur lequel IMM est installé :
   a. Accédez au site http://www.ibm.com/systems/support/.
   b. Sous **Product support**, cliquez sur **System x** ou sur **BladeCenter**.
   c. Sous **Popular links**, cliquez sur **Software and device drivers**.
   d. Cliquez sur le lien correspondant à votre serveur pour afficher la liste des fichiers téléchargeables.
   e. Accédez au module IMM, au microprogramme de serveur ou à la zone DSA, sélectionnez le lien vers la mise à jour du microprogramme et enregistrez le fichier de mise à jour.
2. Connectez-vous au module IMM. Pour plus d'informations, voir Chapitre 2, «Ouverture et utilisation de l'interface Web d'IMM», à la page 13.
3. Dans le panneau de navigation, cliquez sur **Firmware Update**.
4. Cliquez sur **Browse**.
5. Accédez au package de mise à jour que vous désirez appliquer.

   Remarque :
   a. Le microprogramme de serveur System x ne peut pas être mis à jour alors que le serveur est hors tension ou en cours de démarrage.
   b. Pour déterminer le type de fichier de microprogramme à utiliser, voir le fichier Readme du package de mise à jour. Dans la plupart des cas, IMM intégré peut utiliser le fichier EXE ou le fichier BIN pour effectuer la mise à jour.

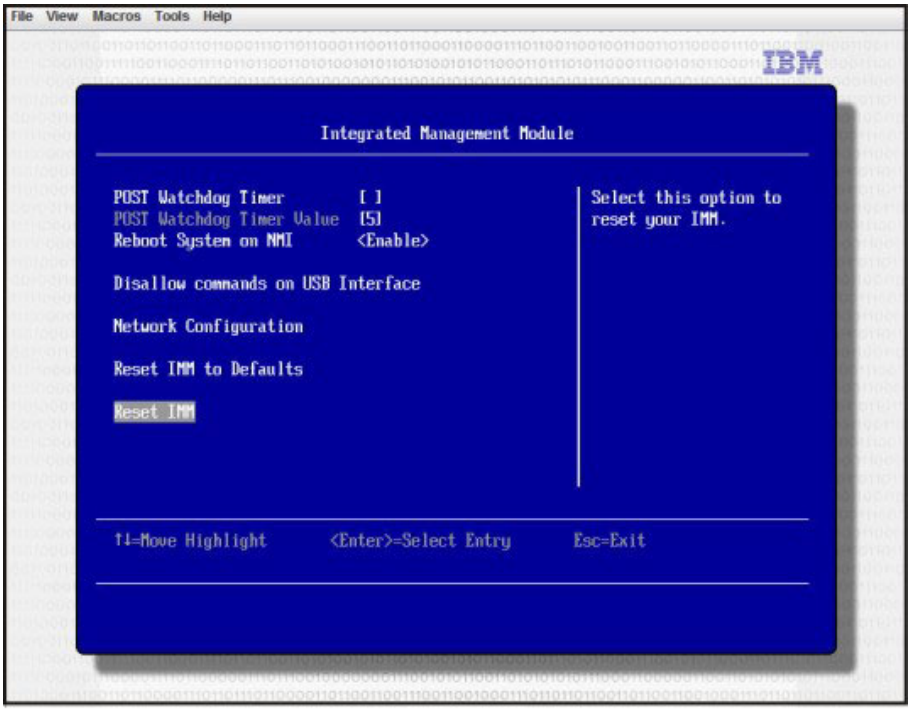
6. Cliquez sur **Open**. Le fichier et son chemin d'accès complet sont affichés dans la zone en regard de **Browse**.
7. Pour lancer la procédure de mise à jour, cliquez sur **Update**. Un indicateur signale la progression du transfert du fichier vers le stockage temporaire sur le module IMM. Une fenêtre de confirmation s'ouvre lorsque le transfert de fichier est terminé.
8. Vérifiez que le fichier indiqué dans la fenêtre Confirm Firmware Update est bien celui à mettre à jour. Si ce n'est pas le cas, cliquez sur **Cancel**.
9. Pour terminer la procédure de mise à jour, cliquez sur **Continue**. Un indicateur signale la progression de la mise à jour du microprogramme. Une fenêtre confirme enfin l'aboutissement de la mise à niveau.
10. Si vous mettez à jour le microprogramme d'IMM, cliquez sur **Restart IMM** dans le panneau de navigation, puis cliquez sur **Restart**. Les mises à jour du microprogramme du serveur System x et de DSA ne requièrent pas un redémarrage d'IMM. Ces mises à jour prennent effet au démarrage suivant du serveur.
11. Cliquez sur **OK** pour confirmer votre intention de redémarrer IMM.
12. Cliquez sur **OK** pour fermer la fenêtre de navigateur en cours.
13. Après le redémarrage d'IMM, connectez-vous à nouveau à IMM pour accéder à l'interface Web.

Réinitialisation d'IMM à l'aide de l'utilitaire Setup

Pour réinitialiser IMM via l'utilitaire Setup, procédez comme suit.

1. Mettez le serveur sous tension.

   Remarque : Environ 2 minutes après la connexion du serveur au courant alternatif, le bouton de contrôle de l'alimentation devient actif.
2. Lorsque l'invite `F1 Setup` s'affiche, appuyez sur F1. Si vous avez défini un mot de passe à la mise sous tension et un mot de passe administrateur, vous devez entrer le mot de passe administrateur pour accéder au menu complet de l'utilitaire de configuration.
3. Dans le menu principal de l'utilitaire de configuration, sélectionnez **System Settings**.
4. Sur l'écran ci-après, sélectionnez **Integrated Management Module**.
5. Sélectionnez **Reset IMM**.



Remarque : Après la réinitialisation d'IMM, ce message de confirmation s'affiche immédiatement :

```
IMM reset command has been sent successfully!! Press ENTER to continue.
```

Le processus de réinitialisation d'IMM n'est pas encore terminé. Vous devez patienter environ 4 minutes pour que la réinitialisation s'achève et qu'IMM soit à nouveau fonctionnel. Si vous tentez d'accéder aux informations du microprogramme du serveur alors qu'il est encore en cours de réinitialisation, la mention `Unknown` est affichée dans les zones, accompagnée de le description `Error retrieving information from IMM` (Erreur lors de l'extraction d'informations depuis IMM).

Gestion des outils et des utilitaires avec IMM et IBM System x Server Firmware

Cette section décrit les outils et utilitaires pris en charge par IMM et IBM System x Server Firmware. Les outils IBM que vous utilisez pour gérer le module IMM intrabande ne requièrent pas l'installation de pilotes de périphériques. Toutefois, si vous choisissez d'utiliser certains outils tels que IPMItool intrabande, vous devez installer les pilotes OpenIPMI.

Les mises à jour et les téléchargements des outils et utilitaires IBM de gestion de systèmes sont disponibles sur le site Web d'IBM. Pour vérifier la disponibilité de mises à jours d'outils et d'utilitaires, procédez comme suit.

Remarque : Des modifications sont apportées périodiquement au site Web d'IBM. La procédure de recherche des microprogrammes et de la documentation peut être légèrement différente de celle décrite dans le présent document.

1. Accédez au site http://www.ibm.com/systems/support/.
2. Sous **Product support**, cliquez sur **System x**.

3. Sous **Popular links**, cliquez sur **Utilities**.

Utilisation d'IPMItool

IPMItool fournit différents outils qui vous permettent de gérer et de configurer un système IPMI. Vous pouvez utiliser IPMItool en mode intrabande ou hors bande pour gérer et configurer IMM.

Pour plus d'informations sur IPMItool ou pour le télécharger, visitez le site http://sourceforge.net/.

Utilisation d'OSA System Management Bridge

OSA System Management Bridge (SMBridge) est un outil qui permet de gérer des serveurs à distance. Vous pouvez l'utiliser pour gérer des serveurs utilisant les protocoles IPMI 1.5 et SOL (Serial over LAN).

Pour plus d'informations sur SMBridge, visitez le site http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-62198&brandind=5000008 ou procédez comme suit.

1. Accédez au site http://www.ibm.com/systems/support/.
2. Cliquez sur **System x**.
3. Sous **Support & downloads**, cliquez sur **Search**.
4. Dans la zone de recherche, entrez `smbridge`, puis cliquez sur **Search**.
5. Dans la liste de résultats, cliquez sur le lien **SMBridge Tool Help - Servers**.

Utilisation d'IBM Advanced Settings Utility

Le programme IBM ASU (Advanced Settings Utility) version 3.0.0, (ou version ultérieure), est requis pour gérer IMM. ASU est un outil que vous pouvez utiliser pour modifier depuis l'interface de ligne de commande les paramètres de microprogramme sur plusieurs plateformes de système d'exploitation. Il vous permet également d'émettre certaines commandes de configuration d'IMM. Vous pouvez utiliser ASU en mode intrabande ou hors bande pour gérer et configurer IMM.

Remarque : Si l'interface USB intrabande (LAN over USB) est désactivée, ASU requiert l'installation de pilotes de périphériques IPMI.

Pour plus d'informations sur l'utilitaire ASU, voir http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-55021&brandind=5000008, ou procédez comme suit.

1. Accédez au site http://www.ibm.com/systems/support/.
2. Cliquez sur **System x**, sélectionnez votre serveur dans le menu **Product family** puis cliquez sur **Go**.
3. Dans le menu **Refine results**, sélectionnez **Advanced Settings Utility** et cliquez sur **Go**.
4. Cliquez sur le lien vers la dernière version de l'utilitaire ASU.

Utilisation des utilitaires Flash d'IBM

Un utilitaire flash vous permet de mettre à jour le matériel et le microprogramme du serveur tout en ne nécessitant aucune installation manuelle de nouveaux microprogrammes ou mises à jour de microprogramme depuis une disquette physique ou un autre support. Vous pouvez utiliser les utilitaires flash d'IBM pour

IMM, le microprogramme de serveur et DSA, en mode intrabande ou hors bande. Pour rechercher un utilitaire flash, procédez comme suit.

1. Accédez au site http://www.ibm.com/systems/support/.
2. Sous **Product support**, cliquez sur **System x**.
3. Dans la zone de recherche, entrez `flash utility`, puis cliquez sur **Search**.
4. Cliquez sur le lien vers l'utilitaire flash approprié

Autres méthodes de gestion du module IMM

Vous pouvez utiliser les interfaces utilisateur suivantes pour gérer et configurer le module IMM :

- Interface Web IMM
- SNMPv1
- SNMPv3
- CLI Telnet
- CLI SSH

Chapitre 6. LAN over USB

Contrairement au contrôleur BMC et à l'adaptateur Remote Supervisor Adapter II, IMM n'a pas besoin de pilotes d'unité IPMI ou de démons USB pour la communication IMM intrabande. A la place, une interface LAN over USB permet les communications intrabande avec le module IMM ; le matériel IMM sur la carte mère comporte une carte d'interface réseau interne depuis IMM vers le système d'exploitation.

Remarque : LAN over USB est également appelé «interface USB intrabande» dans l'interface Web d'IMM.

L'adresse IP IMM pour l'interface LAN over USB reçoit l'adresse statique 169.254.95.118 et le masque de sous-réseau 255.255.0.0. La seule exception concerne le module de gestion intégré dans le noeud secondaire d'un système multi-noeud (par exemple, x3850 X5 ou x3950 X5) où l'adresse IP du module de l'interface LAN over USB est 169.254.96.118.

Conflits possibles avec l'interface LAN over USB

Dans certaines situations, l'interface IMM LAN over USB peut entrer en conflit avec certaines configurations réseau, avec des applications, ou les deux. Par exemple, Open MPI tente d'utiliser toutes les interfaces réseau disponibles sur un serveur. Open MPI détecte l'interface IMM LAN over USB et tente de l'utiliser pour communiquer avec d'autres systèmes dans un environnement en cluster. L'interface LAN over USB est une interface interne et ne fonctionne donc pas pour les communications externes avec d'autres systèmes dans le cluster.

Résolution de conflits affectant l'interface LAN over USB d'IMM

Plusieurs actions peuvent permettre de résoudre des conflits LAN over USB liés à des applications et à des configurations réseau :

- Dans le cas de conflits avec Open MPI, configurez l'application afin qu'elle ne tente pas d'utiliser l'interface.
- Arrêtez l'interface (exécutez la commande `ifdown` sous Linux).
- Supprimez le pilote de périphérique (exécutez la commande `rmmod` sous Linux).
- Désactivez l'interface USB intrabande sur le module IMM via l'une des méthodes suivantes.

  Important : Si vous désactivez l'interface USB intrabande, vous ne pouvez pas effectuer une mise à jour intrabande du microprogramme IMM à l'aide des utilitaires de flashage Linux ou Windows. Si l'interface USB intrabande est désactivée, utilisez l'option Firmware Update depuis l'interface Web d'IMM pour mettre à jour le microprogramme. Pour plus d'informations, voir «Mise à niveau du microprogramme», à la page 128.

  Si vous désactivez l'interface USB intrabande, désactivez également les délais d'attente du programme de surveillance pour empêcher des redémarrages intempestifs du serveur. Pour plus d'informations sur la désactivation des programmes de surveillance, voir «Configuration des délais d'attente du serveur», à la page 23.

– Pour désactiver l'interface LAN over USB depuis l'interface Web d'IMM, voir «Désactivation de l'interface USB intrabande», à la page 26.
– Pour désactiver l'interface LAN over USB depuis l'interface Web du module de gestion évolué, procédez comme suit.
  1. Accédez à l'interface Web du module de gestion évolué.
  2. Dans le panneau de navigation, cliquez sur **Blade Configuration** sous l'en-tête **Blade Tasks**.
  3. Accédez à l'interface LAN over USB du processeur de service sur la page Web Blade Configuration. Cette section répertorie tous les serveurs lame sur le châssis capables d'activer et de désactiver l'interface LAN over USB.
  4. Cochez les cases en regard des serveurs lame que vous désirez activer ou désactiver.
  5. Cliquez sur **Disable** pour désactiver l'interface LAN over USB sur les serveurs lame sélectionnés.

Configuration manuelle de l'interface LAN over USB

Pour que le module IMM utilise l'interface LAN over USB, vous devrez peut-être réaliser d'autres tâches de configuration si la configuration automatique échoue ou si vous préférez configurer manuellement cette interface. Le package de mise à jour du microprogramme ou l'utilitaire ASU (Advanced Settings Utility) tente d'effectuer automatiquement la configuration. Pour plus d'informations sur la configuration LAN over USB sur différents systèmes d'exploitation, consultez le livre blanc IBM *Transitioning to UEFI and IMM* sur le site Web d'IBM.

Installation de pilotes de périphérique

Pour que le module IMM utilise l'interface LAN over USB, vous devrez peut-être installer des pilotes pour votre système d'exploitation. Si la configuration automatique échoue ou si vous préférez configurer manuellement l'interface LAN over USB, utilisez l'une des procédures ci-après. Pour plus d'informations sur la configuration LAN over USB sur différents systèmes d'exploitation, consultez le livre blanc IBM *Transitioning to UEFI and IMM* sur le site Web d'IBM.

Installation du pilote de périphérique IPMI sous Windows

Le pilote de périphérique IPMI Microsoft n'est pas installé par défaut sur les systèmes d'exploitation Microsoft Windows Server 2003 R2. Pour l'installer, procédez comme suit.

1. Depuis le bureau Windows, cliquez sur **Démarrer > Panneau de configuration > Ajout ou suppression de programmes**.
2. Cliquez sur **Ajouter ou Supprimer des composants Windows**.
3. Dans la liste des composants, sélectionnez **Outils de gestion et d'analyse**, puis cliquez sur **Détails**.
4. Sélectionnez **Gestion du matériel**.
5. Cliquez sur **Suivant**. L'assistant d'installation s'ouvre et vous guide tout au long de l'installation.

   Remarque : Le CD d'installation de Windows peut vous être réclamé.

Installation du pilote de périphérique LAN over USB sous Windows

Lorsque vous installez Windows, un périphérique RNDIS inconnu est affiché dans le gestionnaire de périphériques. Vous devez installer un fichier INF Windows qui identifie ce périphérique et qui est exigé par le système d'exploitation Windows pour détecter et utiliser la fonctionnalité LAN over USB. La version signée du fichier INF est incluse dans toutes les versions Windows des packages de mise à jour d'IMM, d'UEFI et de DSA. Ce fichier n'a besoin d'être installé qu'une seule fois. Pour installer le fichier INF Windows, procédez comme suit.

1. Procurez-vous une version Windows du module de mise à jour d'IMM, du microprogramme du serveur ou de DSA (voir «Mise à niveau du microprogramme», à la page 128 pour plus d'informations).
2. Décompressez les fichiers `ibm_rndis_server_os.inf` et `device.cat` depuis le package de mise à jour de microprogramme et copiez-les dans le sous-répertoire `\WINDOWS\inf`.
3. **Sous Windows 2003** : Installez le fichier `ibm_rndis_server_os.inf` en cliquant avec le bouton droit de la souris sur le fichier et sélectionnez **Install**. Cette opération génère un fichier PNF du même nom dans `\WINDOWS\inf`. **Sous Windows 2008** : Sélectionnez **Gestion de l'ordinateur**, puis **Gestionnaire de périphériques** et localisez le périphérique RNDIS. Sélectionnez **Propriétés > Pilote > Réinstaller le pilote**. Désignez au serveur le répertoire `\Windows\inf` contenant le fichier `ibm_rndis_server_os.inf` pour qu'il puisse installer le périphérique.
4. Sélectionnez **Gestion de l'ordinateur**, puis **Gestionnaire de périphériques**. Cliquez avec le bouton droit de la souris sur **Cartes réseau** et sélectionnez **Rechercher les modifications du matériel**. Un message confirme que le périphérique Ethernet a été trouvé et installé. L'assistant Nouveau matériel démarre automatiquement.
5. A l'invite `Autorisez-vous Windows à se connecter à Windows Update pour rechercher les mises à jour ?`, cliquez sur **Non, pas cette fois**. Cliquez sur **Suivant** pour continuer.
6. A l'invite `Que souhaitez-vous que l'assistant fasse ?`, cliquez sur **Installer à partir d'une liste ou d'un emplacement spécifié (utilisateurs expérimentés)**. Cliquez sur **Suivant** pour continuer.
7. A l'invite `Choisissez vos options de recherche et d'installation`, cliquez sur **Ne pas rechercher. je vais choisir le pilote à installer**. Cliquez sur **Suivant** pour continuer.
8. A l'invite `Sélectionnez un type de matériel, puis cliquez sur Suivant`, cliquez sur **Cartes réseau**. Cliquez sur **Suivant** pour continuer.
9. A l'invite `Fin de l'Assistant Nouveau matériel détecté`, cliquez sur **Terminer**.

   Remarque : Une nouvelle connexion de zone locale est affichée et peut indiquer `Cette connexion a une connectivité limitée ou inexistante`. Ignorez ce message.
10. Revenez au gestionnaire de périphériques. Vérifiez que l'entrée **Périphérique réseau NDIS distant USB IBM** figure sous **Cartes réseau**.
11. Ouvrez une invite de commande, entrez `ipconfig` et appuyez sur la touche Entrée. La connexion de zone locale pour le périphérique RNDIS USB IBM est affichée avec une adresse sur la plage 169.254.*xxx.xxx* avec le masque de sous-réseau 255.255.0.0.

Installation du pilote de périphérique LAN over USB sous Linux

Les versions actuelles de Linux, telles que RHEL5 Update 2 et SLES10 Service Pack 2, prennent en charge l'interface LAN over USB par défaut. Cette interface est détectée et affichée pendant l'installation de ces systèmes d'exploitation. Lorsque vous configurez le périphérique, utilisez l'adresse IP statique 169.254.95.130 avec le masque de sous-réseau 255.255.0.0.

Remarque : Les distributions Linux plus anciennes risquent de ne pas détecter l'interface LAN over USB et peuvent exiger une configuration manuelle. Pour plus d'informations sur la configuration LAN over USB sur des distributions Linux spécifiques, consultez le livre blanc *Transitioning to UEFI and IMM* sur le site Web d'IBM.

L'interface IMM LAN over USB interface requiert le chargement des pilotes de périphérique `usbnet` et `cdc_ether`. Si ces pilotes de périphérique n'ont pas été installés, utilisez la commande modprobe pour les installer. Lorsque ces pilotes sont installés, l'interface LAN over USB du module d'IMM est présentée en tant que périphérique réseau dans le système d'exploitation. Pour identifier le nom affecté à l'interface réseau USB d'IMM, entrez la commande :

```
dmesg | grep -i cdc ether
```

Utilisez la commande ifconfig pour configurer l'interface avec une adresse IP située sur la plage 169.254.*xxx.xxx*. Par exemple :

```
ifconfig IMM_device_name 169.254.1.102 netmask 255.255.0.0
```

Cette est configurée pour utiliser une adresse IP sur la plage 169.254.*xxx.xxx* chaque fois que le système d'exploitation est démarré.

Chapitre 7. Interface de ligne de commande

Vous pouvez utiliser l'interface de ligne de commande (CLI) d'IMM pour accéder au module IMM sans avoir à utiliser l'interface Web. Cette interface fournit un sous-ensemble des fonctions de gestion disponibles dans l'interface Web.

Vous pouvez accéder à l'interface CLI via une session Telnet ou SSH. Vous devez être authentifié par le module IMM avant de pouvoir lancer des commandes dans l'interface CLI.

Gestion d'IMM avec IPMI

IMM est livré avec l'ID utilisateur 2 défini initialement avec le nom d'utilisateur USERID et le mot de passe PASSW0RD (le chiffre 0 et non pas la lettre O). Cet utilisateur dispose d'un accès Superviseur.

Important : Modifiez ce mot de passe par défaut lors de votre configuration initiale pour une sécurité accrue.

IMM fournit également les fonctions IPMI de gestion de serveur distant suivantes :

Interfaces de ligne de commande
L'interface de ligne de commande fournit un accès direct aux fonctions de gestion du serveur via le protocole IPMI 2.0. Vous pouvez utiliser SMBridge ou IPMItool pour émettre des commandes de contrôle de l'alimentation du serveur, afficher des informations sur le serveur et identifier celui-ci. A l'aide de SMBridge, vous pouvez également enregistrer une ou plusieurs commandes dans un fichier texte et exécuter ce fichier en tant que script. Pour plus d'informations sur IPMItool, voir «Utilisation d'IPMItool», à la page 131. Pour plus d'informations sur SMBridge, voir «Utilisation d'OSA System Management Bridge», à la page 131.

Serial over LAN
Pour gérer des serveurs depuis un site distant, utilisez SMBridge ou IPMItool afin d'établir une connexion SOL (Serial over LAN). Pour plus d'informations sur IPMItool, voir «Utilisation d'IPMItool», à la page 131. Pour plus d'informations sur SMBridge, voir «Utilisation d'OSA System Management Bridge», à la page 131.

Accès à la ligne de commande

Pour accéder à la ligne de commande, ouvrez une session Telnet ou SSH sur l'adresse IP d'IMM (voir «Configuration de la redirection série à Telnet ou SSH», à la page 38 pour plus d'informations).

Connexion à la session de ligne de commande

Pour vous connecter à l'interface de ligne de commande, procédez comme suit.

1. Etablissez une connexion avec le module IMM.
2. A l'invite du nom d'utilisateur, entrez l'ID utilisateur.
3. A l'invite de mot de passe, entrez le mot de passe que vous utilisez pour vous connecter à IMM.

Vous êtes connecté à la ligne de commande. L'invite de ligne de commande est la suivante : `system>`. La session de ligne de commande se poursuit jusqu'à ce que vous saisissiez `exit` depuis la ligne de commande. Vous êtes alors déconnecté et la session de ligne de commande prend fin.

syntaxe de commande

Consultez les directives suivantes avant d'utiliser les commandes :

- Le format de toutes les commandes est le suivant :

  `commande [arguments] [-options]`
- La syntaxe de commande est sensible à la casse.
- Le nom de la commande doit figurer en minuscules.
- Tous les arguments doit suivre immédiatement la commande. Les options suivent immédiatement les arguments.
- Chaque option est toujours précédée par un tiret (-). Une option peut figurer au format court (lettre unique) ou long (plusieurs lettres).
- Si une option comporte un argument, l'argument est obligatoire, par exemple :

  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`

  où **ifconfig** est la commande, eth0 est un argument, et -i, -g, -s sont des options. Dans cet exemple, les trois options ont des arguments.
- Des crochets indiquent que l'argument ou l'option est facultatif. Les crochets ne font pas partie de la commande que vous saisissez.

Fonctionnalités et limitations

Le module CLI se caractérise par les fonctionnalités et limitations suivantes :

- Possibilité de pPlusieurs sessions CLI simultanées avec différentes méthodes d'accès (Telnet ou SSH). Au plus, deux sessions de ligne de commande Telnet peut être actives simultanément.

  Remarque : Le nombre de sessions Telnet est configurable. Les valeurs valides sont 0, 1, et 2. La valeur 0 signifie que l'interface Telnet est désactivée.
- Une seule commande est autorisée par ligne (limitée à 160 caractères, y-compris les espaces).
- Aucun caractère de continuation n'est disponible pour les commandes longues. La seule fonction d'édition est la touche Retour arrière qui efface le caractère que vous venez de saisir.
- Les touches de direction Flèche vers le haut et Flèche vers le bas peuvent être utilisées pour parcourir les huit dernières commandes. La commande **history** affiche la liste des huit dernières commandes, que vous pouvez alors utiliser comme raccourci pour exécuter une commande, comme dans l'exemple suivant :

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
```

```
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

- Dans l'interface de ligne de commande, la mémoire tampon de sortie est limitée à 2 Ko. Aucune mise en mémoire tampon n'a lieu. La sortie d'une commande ne peut pas dépasser 2048 caractères. Cette limite ne s'applique pas en mode de redirection série (les données sont mises en mémoire tampon lors de la redirection série).
- Le résultat d'une commande est affiché à l'écran une fois son exécution terminée. De ce fait, il n'est pas possible de rendre compte en temps réel du statut d'exécution. Par exemple, sous le mode prolixe de la commande **flashing**, la progression de l'opération n'est pas affichée en temps réel. Elle est présentée à l'issue de l'exécution de la commande.
- Des messages texte simples sont utilisés pour indiquer le statut d'exécution de la commande, comme dans l'exemple suivant :

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```

- La syntaxe de commande est sensible à la casse.
- Au moins un espace doit figurer entre une option et son argument. Par exemple, la syntaxe `ifconfig eth0 -i192.168.70.133` est incorrecte. La syntaxe correcte est la suivante : `ifconfig eth0 -i 192.168.70.133`.
- Toutes les commandes admettent les options `-h`, `-help` et `?` , lesquelles fournissent une aide sur la syntaxe. Tous les exemples suivants débouchent sur le même résultat :

```
system> power -h
system> power -help
system> power ?
```

- Certaines des commandes décrites dans les sections ci-après peuvent ne pas être disponibles. Pour afficher la liste des commandes prises en charge, utilisez l'option help ou l'option ?, comme illustré dans les exemples ci-après.

```
system> help
system> ?
```

Commandes d'utilitaire

Les commandes d'utilitaire sont les suivantes :

- exit
- aide
- history

Commande exit

Utilisez la commande **exit** pour vous déconnecter et mettre fin à la session d'interface de ligne de commande.

Commande help

Utilisez la commande **help** pour afficher la liste et une brève description de chacune des commandes. Vous pouvez également entrer **?** à l'invite de commande.

Commande history

Utilisez la commande **history** pour afficher une liste historique indexée des huit dernières commandes émises. Les index peuvent être utilisés en tant que raccourcis (en les précédant du signe !) pour réexécuter des commandes figurant dans cette liste.

Exemple :

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Commandes de surveillance

Les commandes de surveillance sont les suivantes :

- clearlog
- fans
- readlog
- syshealth
- temps
- volts
- vpd

Commande clearlog

Utilisez la commande **clearlog** pour effacer le journal des événements IMM. Vous devez être habilité à effacer les journaux d'événements pour émettre cette commande.

Commande fans

Utilisez la commande **fans** pour afficher la vitesse de chacun des ventilateurs du serveur.

Exemple :

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

Commande readlog

Utilisez la commande **readlog** pour afficher les entrées du journal des événements IMM, cinq à la fois. Les entrées sont affichées à partir de la plus récente jusqu'à la plus ancienne.

readlog affiche les cinq premières entrées dans le journal des événements, en commençant par la plus récente, à sa première exécution, et les cinq suivantes à chaque appel ultérieur.

readlog -f réinitialise le compteur et affiche les 5 premières entrées dans le journal des événements, en commençant par la plus récente.

Syntaxe :

```
readlog [options]
option :
-f
```

Exemple :

```
system> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
Login ID:''USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
Login ID: ''USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

Commande syshealth

Utilisez la commande **syshealth** pour afficher un récapitulatif de l'état de santé du serveur. L'état d'alimentation, l'état du serveur, le nombre de redémarrages et le statut du logiciel IMM sont affichés.

Exemple :

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

Commande temps

Utilisez la commande **temps** pour afficher toutes les températures et les seuils de température. Le groupe de températures affiché est le même que dans l'interface Web.

Exemple :

```
system> temps
Les températures s'affichent en degrés Fahrenheit et Celsius
        WR      W      T     SS     HS
---------------------------------------
CPU1   65/18  72/22  80/27  85/29  90/32
```

```
CPU2   58/14  72/22  80/27  85/29  9/320
DASD1  66/19  73/23  82/28  88/31  9/332
Amb    59/15  70/21  83/28  90/32  9/355
system>
```

Remarques :

1. La sortie comporte les en-têtes de colonnes suivants :
   - WR : avertissement de réinitialisation
   - W : avertissement
   - T : température (valeur actuelle)
   - SS : arrêt graduel
   - HS : arrêt immédiat
2. Toutes les valeurs de température sont affichées en degrés Fahrenheit et Celsius.

Commande volts

Utilisez la commande **volts** pour afficher tous les voltages et leurs seuils. Le groupe de voltages affiché est le même que dans l'interface Web.

Exemple :

```
system> volts
      HSL   SSL   WL    WRL   V     WRH   WH   SSH    HSH
-------------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                        3.45
VRM2                        5.45
system>
```

Remarque : La sortie comporte les en-têtes de colonnes suivants :

- HSL : arrêt immédiat - seuil inférieur
- SSL : arrêt graduel - seuil inférieur
- WL : avertissement - seuil inférieur
- WRL : avertissement de réinitialisation - seuil inférieur
- V : voltage (valeur actuelle)
- WRH : avertissement de réinitialisation - seuil supérieur
- WH : avertissement -seuil supérieur
- SSH : arrêt graduel - seuil supérieur
- HSH : arrêt immédiat - seuil supérieur

Commande vpd

Utilisez la commande **vpd** pour afficher les données techniques essentielles pour le système (sys), pour IMM, pour le microprogramme du serveur (bios) et pour le programme Dynamic System Analysis Preboot (dsa). Les informations qui s'affichent sont les mêmes que dans l'interface Web.

Syntaxe :

```
vpd sys
vpd IMM
vpd biosvpd dsa
```

Exemple :

```
system> vpd dsa
Type     Version      ReleaseDate
----     -------      -----------
dsa      D6YT19AUS    02/27/2009
system>
```

Commande de contrôle de l'alimentation et du redémarrage du serveur

Les commandes d'alimentation et de redémarrage du serveur sont les suivantes :

- power
- reset

Commande power

Utilisez la commande **power** pour contrôler l'alimentation du serveur. Pour émettre des commandes **power**, vous devez être habilité à contrôler l'alimentation et le redémarrage du serveur.

power on met le serveur sous tension.

power off met le serveur hors tension. L'option **-s** arrête le système d'exploitation avant la mise hors tension du serveur.

power state affiche l'état d'alimentation du serveur (on ou off) et l'état actuel du serveur.

power cycle met hors tension le serveur, puis sous tension. L'option **-s** arrête le système d'exploitation avant la mise hors tension du serveur.

Syntaxe :

```
power on
power off [-s]
power state
power cycle [-s]
```

Commande reset

Utilisez la commande **reset** pour redémarrer le serveur. Pour utiliser cette commande, vous devez être habilité à contrôler l'alimentation et le redémarrage du serveur. L'option **-s** arrête le système d'exploitation avant le redémarrage du serveur.

Syntaxe :

```
reset [option]
option :
-s
```

Commande de redirection série

Une seule commande de redirection série est disponible : console.

Commande console

Utilisez la commande **console** pour lancer un session console de redirection série vers le port série IMM désigné.

Syntaxe :

```
console 1
```

Commandes de configuration

Les commandes de configuration sont les suivantes :

- dhcpinfo
- dns
- gprofile
- ifconfig
- ldap
- ntp
- passwordcfg
- portcfg
- slp
- srcfg
- ssl
- tcpcmdmode
- timeouts
- usbeth
- users

Commande dhcpinfo

Utilisez la commande **dhcpinfo** pour afficher la configuration IP affectée par le serveur DHCP pour eth0 si l'interface est configurée automatiquement par un serveur DHCP. Vous pouvez utiliser la commande **ifconfig** pour activer ou désactiver DHCP.

Syntaxe :

```
dhcpinfo eth0
```

Exemple :

```
system> dhcpinfo eth0

-server : 192.168.70.29
-n     : IMMA-00096B9E003A
-i     : 192.168.70.202
-g     : 192.168.70.29
-s     : 255.255.255.0
-d     : linux-sp.raleigh.ibm.com
-dns1   : 192.168.70.29
-dns2   : 0.0.0.0
-dns3   : 0.0.0.0
-i6    : 0::0
-d6    : *
-dns61  : 0::0
-dns62  : 0::0
-dns63  : 0::0
system>
```

La tableau suivant décrit la sortie de cet exemple.

Option	Description
-server	Serveur DHCP ayant affecté la configuration
-n	Nom d'hôte affecté
-i	Adresse IPv4 affectée

Option	Description
-g	Adresse de passerelle affectée
-s	Masque de sous-réseau affecté
-d	Nom de domaine affecté
-dns1	Adresse IP du serveur DNS IPv4 principal
-dns2	Adresse IP du serveur DNS IPv4 secondaire
-dns3	Adresse IP du serveur DNS IPv4 tertiaire
-i6	Adresse IPv6
-d6	Nom de domaine IPv6
-dns61	Adresse IP du serveur DNS IPv6 principal
-dns62	Adresse IP du serveur DNS IPv6 secondaire
-dns63	Adresse IP du serveur DNS IPv6 tertiaire

Commande dns

Utilisez la commande **dns** pour afficher la configuration DNS du module IMM.

Syntaxe :

```
dns
```

Remarque : L'exemple suivant présente une configuration IMM où DNS est activé.

Exemple :

```
system> dns
-state  : enabled
-i1     : 192.168.70.202
-i2     : 192.168.70.208
-i3     : 192.168.70.212
-i61    : fe80::21a:64ff:fee6:4d5
-i62    : fe80::21a:64ff:fee6:4d6
-i63    : fe80::21a:64ff:fee6:4d7
-ddns   : enabled
-dnsrc  : dhcp
-p     : ipv6

system>
```

La tableau suivant décrit la sortie de cet exemple.

Option	Description
-state	Etat du DNS (`enabled` ou `disabled`)
-i1	Adresse IP du serveur DNS IPv4 principal
-i2	Adresse IP du serveur DNS IPv4 secondaire
-i3	Adresse IP du serveur DNS IPv4 tertiaire
-i61	Adresse IP du serveur DNS IPv6 principal
-i62	Adresse IP du serveur DNS IPv6 secondaire
-i63	Adresse IP du serveur DNS IPv6 tertiaire
-ddns	Etat du DDNS (`enabled` ou `disabled`)
-dnsrc	Nom de domaine DDNS préféré (`dhcp` ou `manual`)
-p	Serveurs DNS préférés (`ipv4` or `ipv6`)

Commande gprofile

Utilisez la commande **gprofile** pour afficher et configurer les profils de groupe pour le module IMM.

Le tableau suivant présente les arguments pour les options.

Option	Description	Valeurs
-clear	Supprime un groupe	Enabled, disabled
-n	Nom du groupe	Chaîne pouvant comprendre jusqu'à 63 caractères pour *nom_groupe*. *nom_groupe* doit être unique.
-a	Niveau de sécurité (d'autorisation) basé rôle	Supervisor, operator, rbs <liste_rôles>: ns | uam | rca | rcrda | rpr | bac | ce | aac Les valeurs de la liste de rôles doivent être spécifiées en les séparant par une barre verticale.
-h	Affiche la syntaxe et les options de la commande	

Syntaxe :

```
gprofile [1 - 16] [options]
options :
-clear état
-n  nom_groupe
-a  niveau_sécurité:
    -ns réseau et sécurité
    -uam gestion de comptes utilisateur
    -rca accès à la console distante
    -rcrda accès à la console distante et au disque distant
    -rpr accès aux fonctions d'alimentation/de redémarrage du serveur
    -bac configuration de base de l'adaptateur
    -ce possibilité d'effacer les journaux d'événements
    -aac configuration avancée de l'adaptateur
-h
```

Commande ifconfig

Utilisez la commande **ifconfig** pour configurer l'interface Ethernet. Entrez `ifconfig eth0` pour afficher la configuration actuelle de l'interface Ethernet. Pour modifier la configuration de l'interface Ethernet, entrez les options voulues, suivies par leurs valeurs. Pour modifier la configuration de l'interface, vous devez disposer au moins de l'autorisation Adapter Networking and Security Configuration.

Le tableau suivant présente les arguments pour les options.

Option	Description	Valeurs
-state	Etat de l'interface	disabled, enabled
-c	Méthode de configuration	dhcp, static, dthens (dthens correspond à **essayer le serveur dhcp, en cas d'échec utiliser l'option static config** sur l'interface Web)
-i	Adresse IP statique	Adresse avec format valide
-g	Adresse de la passerelle	Adresse avec format valide

Option	Description	Valeurs
-s	Masque de sous-réseau	Adresse avec format valide
-n	Nom d'hôte	Chaîne pouvant comprendre jusqu'à 63 caractères. La chaîne peut inclure des lettres, des chiffres, des points, des traits de soulignement et des tirets.
-dn	Nom de domaine	Nom de domaine avec format valide
-ipv6	Etat IPv6	disabled, enabled
-lla	Adresse lien-local **Remarque :** L'adresse lien-local n'apparaît que si IPv6 est activé.	L'adresse lien-local est déterminée par IMM. Cette valeur est en lecture seule et n'est pas configurable.
-ipv6static	Etat IPv6 statique	disabled, enabled
-i6	Adresse IP statique	Adresse IP statique pour canal Ethernet 0 au format IPv6
-p6	Longueur de préfixe d'adresse	Valeur numérique comprise entre 1 et 128
-g6	Passerelle ou route par défaut	Adresse IP pour la passerelle ou la route par défaut pour le canal Ethernet 0 dans IPv6
-dhcp6	Etat DHCPv6	disabled, enabled
-sa6	Etat de configuration automatique IPv6 sans état	disabled, enabled
-address_table	Table des adresses IPv6 générées automatiquement et de leurs longueurs de préfixes **Remarque :** Cette option n'est visible que si IPv6 et la configuration automatique sans état sont activés.	Cette valeur est en lecture seule et n'est pas configurable.
-auto	Paramètre de négociation automatique qui détermine si les paramètres réseau Data rate et Duplex sont configurables	true, false
-r	Débit de données	10, 100, auto
-d	Mode duplex	full, half, auto
-m	MTU	Valeur numérique comprise entre 60 et 1500
-l	LAA	Format d'adresse MAC. Les adresses de multidiffusion ne sont pas autorisés (le premier octet doit être pair).

Syntaxe :

```
ifconfig eth0 [options]
options :
-state état_interface
-c méthode_config
-i adresse_IP_statique
-g adresse_passerelle
-s masque_sous-réseau
```

```
-n nom_hôte
-r débit_données
-d mode_duplex
-m max_unité_transmission
-l MAC_administrée_localement
```

Exemple :

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
Ces modifications de configuration prendront effet à la réinitialisation
suivante du module IMM.
system>
```

Remarque : L'option **-b** dans l'affichage de ifconfig est destinée à l'adresse MAC gravée. Cette adresse est en lecture seule et n'est pas configurable.

Commande ldap

Utilisez la commande **LDAP** pour afficher et configurer les paramètres de configuration du protocole LDAP.

Le tableau suivant présente les arguments pour les options.

Option	Description	Valeurs
-aom	Mode d'authentification uniquement	Enabled, disabled
-a	Méthode d'authentification d'utilisateur	Local only, LDAP only, local first then LDAP, LDAP first then local
-b	Méthode de liaison	Bind with Anonymous, bind with ClientDN and password et bind with Login Credential
-c	Nom distinctif du client	Chaîne pouvant comprendre jusqu'à 63 caractères pour *nom_distinctif_client*
-fn	Nom de la forêt	Environnements Active Directory, chaîne de 127 caractères pour *nom_forêt*
-d	Domaine de recherche	Chaîne pouvant comprendre jusqu'à 31 caractères pour *domaine_recherche*
-f	Filtre de groupe	Chaîne pouvant comprendre jusqu'à 63 caractères pour *filtre_groupe*
-g	Attribut de recherche de groupe	Chaîne pouvant comprendre jusqu'à 63 caractères pour *attribut_recherche_groupe*
-l	Attribut de permission de connexion	Chaîne pouvant comprendre jusqu'à 63 caractères pour *chaîne*
-p	Mot de passe du client	Chaîne pouvant comprendre jusqu'à 15 caractères pour *mot_de_passe_client*

Option	Description	Valeurs
-pc	Confirme le mot de passe du client	Chaîne pouvant comprendre jusqu'à 15 caractères pour *confirmation_mot_de_passe* Syntaxe de la commande : ldap -p *mot_de_passe_client* -pc *confirmation_mot_de_passe* Cette option est requise lorsque vous modifiez le mot de passe du client. Elle compare l'argument *confirmation_mot_de_passe* à l'argument *mot_de_passe_client* et la commande échoue s'ils ne concordent pas.
-r	Nom distinctif d'entrée racine (DN)	Chaîne pouvant comprendre jusqu'à 63 caractères pour *nom_distinctif_racine*
-rbs	Sécurité étendue basée rôles pour les utilisateurs d'Active Directory	Enabled, disabled
s1ip	Nom d'hôte/adresse IP de Server 1	Chaîne pouvant comporter jusqu'à 63 caractères ou adresse IP pour *nom_d'hôte/adresse_IP*
s2ip	Nom d'hôte/adresse IP de Server 2	Chaîne pouvant comporter jusqu'à 63 caractères ou adresse IP pour *nom_d'hôte/adresse_IP*
s3ip	Nom d'hôte/adresse IP de Server 3	Chaîne pouvant comporter jusqu'à 63 caractères ou adresse IP pour *nom_d'hôte/adresse_IP*
-s4ip	Nom d'hôte/adresse IP de Server 4	Chaîne pouvant comporter jusqu'à 63 caractères ou adresse IP pour *nom_d'hôte/adresse_IP*
s1pn	Numéro de port de Server 1	Numéro de port pouvant comporter jusqu'à 5 chiffres pour *numéro_port*
s2pn	Numéro de port de Server 2	Numéro de port pouvant comporter jusqu'à 5 chiffres pour *numéro_port*
s3pn	Numéro de port de Server 3	Numéro de port pouvant comporter jusqu'à 5 chiffres pour *numéro_port*
s4pn	Numéro de port de Server 4	Numéro de port pouvant comporter jusqu'à 5 chiffres pour *numéro_port*
-t	Nom de cible serveur	Lorsque l'option -rbs est activée, cette zone spécifie un nom de cible qui peut être associé à un ou plusieurs rôles sur le serveur Active Directory via le composant logiciel enfichable Role Based Security.
-u	Attribut de recherche d'UID	Chaîne pouvant comprendre jusqu'à 23 caractères pour *attribut_recherche*
-v	Obtention de l'adresse du serveur LDAP via DNS	Off, on
-h	Affiche la syntaxe et les options de la commande	

Syntaxe :

```
ldap [options]
options :
   -aom enabled|disabled|
   -a loc|ldap|locId|ldloc
   -b anon|client|login
```

```
-c nom_distinctif_client
-d domaine_de_recherche
-fn nom_forêt
-f filtre_groupe
-g attribut_recherche_groupe
-l chaîne
-p mot_de_passe_client
-pc confirmation_mot_de_passe
-r nom_distinctif_racine
-rbs enabled|disabled
-s1ip nom_d'hôte/adresse_IP
-s2ip nom_d'hôte/adresse_IP
-s3ip nom_d'hôte/adresse_IP
-s4ip nom_d'hôte/adresse_IP
-s1pn numéro_port
-s2pn numéro_port
-s3pn numéro_port
-s4pn numéro_port
-t nom
-u attribut_recherche
-v off|on
-h
```

Commande ntp

Utilisez la commande **ntp** pour afficher et configurer le protocole NTP (Network Time Protocol).

Le tableau suivant présente les arguments pour les options.

Option	Description	Valeurs
-en	Active ou désactive le protocole NTP (Network Time Protocol)	Enabled, disabled
-i	Nom ou adresse IP du serveur Network Time Protocol	Nom du serveur NTP à utiliser pour la synchronisation d'horloge.
-f	Fréquence (en minutes) de synchronisation de l'horloge IMM avec le serveur Network Time Protocol	3 à 1440 minutes
-synch	Demande une synchronisation immédiate avec le serveur Network Time Protocol	Aucune valeur n'est spécifiée avec ce paramètre.

Syntaxe :

```
ntp [options]
options :
-en état
-i  nom_d'hôte
-f  fréquence
-synch
```

Exemple :

```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

Commande passwordcfg

Utilisez la commande **passwordcfg** pour afficher et configurer les paramètres de mot de passe.

Option	Description
-legacy	Définit la sécurité du compte d'après un ensemble de valeurs prédéfinies héritées
-high	Définit la sécurité du compte d'après un ensemble de valeurs prédéfinies de niveau élevé
-exp	Age maximal du mot de passe (0 à 365 jours). Sélectionnez la valeur 0 si vous désirez qu'il n'expire jamais.
-cnt	Nombre de mots de passe antérieurs ne pouvant pas être réutilisés (0 à 5)
-nul	Autorise des comptes dépourvus de mot de passe (yes | no)
-h	Affiche la syntaxe et les options de la commande

Syntaxe :

```
passwordcfg [options]
options : {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

Exemple :

```
system> passwordcfg
Niveau de sécurité : existant
system> passwordcfg -exp 365
ok
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
ok
system> passwordcfg
Niveau de sécurité : personnalisé
-exp: 365
-cnt: 5
-nul: allowed
```

Commande portcfg

Utilisez la commande **portcfg** pour configurer le port série. Pour modifier la configuration du port série, entrez les options voulues, suivies par leurs valeurs. Pour modifier la configuration du port série, vous devez disposer au moins de l'autorisation Adapter Networking and Security Configuration.

Les paramètres sont définis dans le matériel et ne peuvent pas être modifiés :

- 8 bits de données
- pas de parité
- 1 bit d'arrêt

Le tableau ci-après présente les arguments pour les options.

Option	Description	Valeurs
-b	Débit en bauds	9600, 19200, 38400, 57600, 115200, 230400
-climode	Mode CLI	none, cliems, cliuser • none : L'interface de ligne de commande est désactivée • cliems : L'interface de ligne de commande est activée avec séquences de touches compatibles EMS • cliuser : L'interface de ligne de commande est activée avec séquences de touches définies par l'utilisateur

Syntaxe :

```
portcfg [options]
portcfg [options]
options :
-b débit en bauds
-climode mode_cli
-cliauth auth_cli
```

Exemple :

```
system> portcfg
-b       : 115200
-climode : 2 (CLI avec séquences de touches définies par l'utilisateur) system>
system>
```

Commande portcontrol

Utilisez la commande **portcontrol** pour configurer l'état de port du service IMM. Pour modifier l'état de port, entrez les options suivies des valeurs. Pour modifier l'état de contrôle de port, vous devez au moins disposer de l'autorisation Adapter Networking et Security Configuration.

Le tableau ci-après présente les arguments pour les options.

Option	Description	Valeurs
-ipmi	port IPMI	On, Off (activé/désactivé)

Syntaxe :

```
portcontrol [options]
options :
-ipmi status
```

Exemple :

```
system> portcontrol
-ipmi : on
```

Commande srcfg

Utilisez la commande **srcfg** pour configurer la redirection série. Entrez `srcfg` pour afficher la configuration actuelle. Pour modifier la configuration de la redirection série, entrez les options voulues, suivies par leurs valeurs. Pour modifier la configuration de la redirection série, vous devez disposer au moins de l'autorisation Adapter Networking and Security Configuration.

Le tableau ci-après présente les arguments pour l'option `-exitcliseq`.

Option	Description	Valeurs
-exitcliseq	Séquence de touches pour quitter l'interface de ligne de commande	Séquence de touches définie par l'utilisateur pour quitter l'interface CLI. Pour plus de détails, voir les valeurs pour l'option -entercliseq dans ce tableau.

Syntaxe :

```
srcfg [options]
options :
-exitcliseq séquence_de_touches_sortie_cli
```

Exemple :

```
system> srcfg
-exitcliseq ^[Q
system>
```

Commande ssl

Utilisez la commande **ssl** pour afficher et configurer les paramètres SSL (Secure Sockets Layer).

Remarque : Avant de pouvoir activer un client SSL, un certificat client doit être installé.

Option	Description
-ce	Active ou désactive un client SSL
-se	Active ou désactive un serveur SSL
-h	Affiche la syntaxe et les options de la commande

Syntaxe :

```
ssl [options]
options :
-ce on | off
-se on | off
-h
```

Paramètres : les paramètres suivants sont présentés avec l'affichage du statut de la commande **SSL** et sont extraits uniquement à partir de l'interface de ligne de commande :

Server secure transport enable
Ce statut est en lecture seule et ne peut pas être défini directement.

Server Web/CMD key status
Ce statut est en lecture seule et ne peut pas être défini directement. Les valeurs en sortie possibles de la ligne de commande sont les suivantes :

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL server CSR key status

Ce statut est en lecture seule et ne peut pas être défini directement. Les valeurs en sortie possibles de la ligne de commande sont les suivantes :

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client LDAP key status

Ce statut est en lecture seule et ne peut pas être défini directement. Les valeurs en sortie possibles de la ligne de commande sont les suivantes :

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client CSR key status

Ce statut est en lecture seule et ne peut pas être défini directement. Les valeurs en sortie possibles de la ligne de commande sont les suivantes :

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

Commande timeouts

Utilisez la commande **délais** pour afficher les valeurs de délai d'attente ou les modifier. Pour afficher les délais d'attente, entrez `timeouts`. Pour modifier les valeurs de délai d'attente, entrez les options voulues, suivies par leurs valeurs. Pour modifier les valeurs de délai d'attente, vous devez disposer au moins de l'autorisation Adapter Configuration.

Le tableau ci-après présente les arguments pour les valeurs de délai d'attente. Ces valeurs correspondent aux options des graduations du menu déroulant pour les délais d'attente du serveur dans l'interface Web.

Option	Délai d'attente	Unités	Valeurs
-o	Délai d'attente du système d'exploitation	minutes	disabled, 2.5, 3, 3.5, 4
-l	Délai d'attente du programme de chargement	minutes	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120

Syntaxe :

```
timeouts [options]
options :
-o option_du_programme_de_surveillance_du_système_d'exploitation
-l option_du_programme_de_surveillance_du_chargeur
```

Exemple :

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

Commande usbeth

Utilisez la commande **usbeth** pour activer l'interface LAN over USB intrabande. Pour plus d'informations sur l'activation ou la désactivation de cette interface, voir «Désactivation de l'interface USB intrabande», à la page 26.

Syntaxe :

```
usbeth [options]
options :
-en <enabled|disabled>
```

Exemple :

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

Commande users

Utilisez la commande **users** pour accéder à tous les comptes utilisateur et à leurs niveaux d'autorisations, pour créer de nouveaux comptes et modifier des comptes existants.

Examinez les directives suivantes pour l'utilisation de la commande **users** :

- Les numéros d'utilisateur doivent être compris entre 1 et 12 (inclus).
- Les noms d'utilisateur doivent comprendre moins de 16 caractères et ne peuvent contenir que certains chiffres, des lettres, des points et des traits de soulignement.
- Les mots de passe doivent comporter plus de 5 caractères et moins de 16 caractères et doivent comporter au moins un caractère alphabétique et un caractère non alphabétique.
- Le niveau d'autorisation peut être l'un des suivants :
  - super (superviseur)
  - ro (lecture seule)
  - N'importe quelle combinaison des valeurs suivantes, séparées par |:

    am (accès à la gestion de compte utilisateur)

    rca (accès à distance à la console)

    rcvma (accès à distance à la console et aux médias virtuels)

    pr (accès à distance à l'alimentation/au redémarrage du serveur)

    cel (possibilité d'effacement des journaux d'événements)

    bc (configuration [de base] de l'adaptateur)

    nsc (configuration de l'adaptateur [réseau et sécurité])

    ac (configuration de l'adaptateur [avancée])

Syntaxe :

```
users [options]
options :
-numéro_utilisateur
-n nom_utilisateur
-p mot_de_passe
-a niveau_d'autorisation
```

Exemple :

```
system> users
1. USERID Read/Write
Expiration du mot de passe : pas d'expiration
2. manu Read Only
Expiration du mot de passe : pas d'expiration
3. eliflippen Read Only
Expiration du mot de passe : pas d'expiration
4.  <non utilisé>
5. jacobyackenovic custom:cel|ac
Expiration du mot de passe : pas d'expiration
system> users -7 -n sptest -p PASSW0RD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID Read/Write
Expiration du mot de passe : pas d'expiration
2. test    Read/Write
Expiration du mot de passe : pas d'expiration
3. test2   Read/Write
Expiration du mot de passe : pas d'expiration
4. <non utilisé>
5. jacobyackenovic custom:cel|ac
Expiration du mot de passe : pas d'expiration
6. <non utilisé>
7. sptest  custom:am|rca|cel|nsc|ac
Expiration du mot de passe : pas d'expiration
8. <non utilisé>
9. <non utilisé>
10. <non utilisé>
11. <non utilisé>
12. <non utilisé>
system>
```

Commandes de contrôle du module IMM

Les commandes de contrôle du module IMM sont les suivantes :

- clearcfg
- clock
- identify
- resetsp
- update

Commande clearcfg

Utilisez la commande **clearcfg** pour rétablir la configuration IMM à ses paramètres usine par défaut. Vous devez disposer au moins des droits Advanced Adapter Configuration pour émettre cette commande. Après l'effacement de la configuration IMM, le module IMM est redémarré.

Commande clock

Utilisez la commande **clock** pour afficher la date et heure actuelle d'après l'horloge IMM et le décalage par rapport au fuseau GMT. Vous pouvez définir la date, l'heure, le décalage GMT, les paramètres d'heure d'été.

Prenez en compte les informations suivantes :

- Pour un décalage GMT de +2 ou +10, des paramètres d'heure d'été spéciaux sont requis.
- Pour +2, les options d'observation de l'heure d'été sont les suivantes : off (désactivation), ee (Europe de l'est), gtb (Grande-Bretagne), egt (Egypte), fle (Finlande).
- Pour +10, les options d'observation de l'heure d'été sont les suivantes : off (désactivation), ea (Est de l'Australie), tas (Tasmanie), vlad (Vladivostok).
- L'année doit être comprise entre 2000 et 2089 (inclus).
- Le mois, la date, l'heure, les minutes, et les secondes peuvent être des valeurs représentées par un seul chiffre (par exemple, 9:50:25 au lieu de 09:50:25).
- Le décalage GMT peut suivre le format +2:00, +2, ou 2 pour les décalages positifs et -5:00 ou -5 pour les négatifs.

Syntaxe:

```
clock [options]
options :
-d mm/jj/aaaa
-t hh:mm:ss
-g décalage gmt
-dst on/off/cas spécial
```

Exemple :

```
system> clock
12/12/2003 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2004
ok
system> clock
12/31/2004 13:15:30 GMT-5:00 dst on
```

Commande identify

Utilisez la commande **identify** pour activer ou désactiver le voyant d'identification du châssis ou pour le faire clignoter. L'option -d peut être utilisée de pair avec -s pour activer uniquement le voyant pendant le nombre de secondes spécifié par le paramètre -d. Une fois ce délai écoulé, le voyant est désactivé.

Syntaxe :

```
identify [options]
options :
-s on/off/blink
-d secondes
```

Exemple :

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

Commande resetsp

Utilisez la commande **resetsp** pour redémarrer le module IMM. Vous devez disposer au moins des droits Advanced Adapter Configuration pour émettre cette commande.

Commande update

Utilisez la commande **update** pour mettre à jour le microprogramme du module IMM ou IMM. Pour utiliser cette commande, vous devez disposer au moins de l'autorisation Advanced Adapter Configuration. Le fichier du microprogramme (spécifié par *nom_fichier*) est d'abord transféré depuis le serveur TFTP (spécifié par son adresse IP) vers le module IMM, puis flashé. L'option **-v** spécifie d'utiliser le mode prolixe.

Remarque : Assurez-vous que le serveur TFTP est en cours d'exécution sur le serveur depuis lequel le fichier sera téléchargé.

Option	Description
-i	Adresse IP du serveur TFTP
-l	Nom du fichier (à flasher)
-v	Mode prolixe

Syntaxe :

```
update -i Adresse_IP_serveur_TFTP -l nom_fichier
```

Exemple : en mode prolixe, la progression de l'opération de flashage est signalée en temps réel par le pourcentage d'achèvement.

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Downloading image - 66%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flashing image - 45%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flash operation completed.
system>
```

Si le flashage n'est pas configuré en mode prolixe, la progression est signalée par des caractères # consécutifs.

```
system>update -i 192.168.70.200 -l dsa_d6yt28a_68608_2.upd
Firmware update is in progress. Please wait..
Downloading image: ################################################
Flashing image: ################################################
Flash operation completed.
```

Commandes de Service Advisor

Les commandes de Service Advisor sont les suivantes :

- autoftp
- chconfig
- chlog
- chmanual
- events
- sdemail

Commande autoftp

Utilisez la commande **autoftp** pour afficher et configurer les paramètres du serveur FTP/TFTP pour Service Advisor.

Remarque : Vous devez accepter les dispositions de licence de Service Advisor avant d'utiliser cette commande.

Le tableau ci-après présente les arguments pour les options.

Option	Description	Valeurs
-m	Mode de notification automatisée des problèmes	*ftp, tftp, disabled*
-i	Adresse IP ou nom d'hôte du serveur ftp/tftp pour notification automatisée des problèmes	Adresse IP ou nom d'hôte
-p	Port de transmission FTP/TFTP	Valeur numérique comprise entre 1 et 65535 pour *numéro_port*
-u	Nom d'utilisateur ftp délimité par des apostrophes pour notification des problèmes	Chaîne pouvant comprendre jusqu'à 63 caractères pour *nom_utilisateur*
-pw	Mot de passe ftp délimité par des apostrophes pour notification des problèmes	Chaîne pouvant comprendre jusqu'à 63 caractères pour *mot_de_passe*
Remarque : Pour la valeur *ftp*, toutes les options (zones -i, -p, -u, and -pw) doivent être renseignées. Pour la valeur *tftp*, seules les options -i et -p sont requises.		

Syntaxe :

```
autoftp [options]
options :
-m ftp|tftp|disable
-i nom_d'hôte|adresse_ip
-p numéro_port
-u nom_utilisateur
-pw mot_de_passe
```

Commande chconfig

Utilisez la commande **chconfig** pour afficher et configurer les paramètres de Service Advisor pour le module IMM.

Le tableau ci-après présente les arguments pour les options.

Option	Description	Valeurs
-li	Affichage ou acceptation des dispositions de licence de Service Advisor. Ces dispositions doivent être acceptées via cette option avant de configurer d'autres options.	view, accept
-sa	Statut d'assistance IBM pour Service Advisor	enabled, disabled
-sc	Code pays pour le centre d'assistance IBM	Code pays ISO à deux caractères
-ca	Adresse délimitée par des apostrophes de l'emplacement de la machine	Chaîne pouvant comprendre jusqu'à 30 caractères pour *adresse*
-cci	Ville délimitée par des apostrophes de l'emplacement de la machine	Chaîne pouvant comprendre jusqu'à 30 caractères pour *ville*
-ce	Adresse électronique de la personne à contacter sous la forme *ID_utilisateur@nom_d'hôte*	Chaîne pouvant comprendre jusqu'à 30 caractères pour *courrier_électronique*
-cn	Nom délimité par des apostrophes de la personne à contacter	Chaîne pouvant comprendre jusqu'à 30 caractères pour *nom_contact*
-co	Nom délimité par des apostrophes de l'organisation/de l'entreprise de la personne à contacter	Chaîne pouvant comprendre jusqu'à 30 caractères pour *nom_entreprise*
-cph	Numéro de téléphone délimité par des apostrophes de la personne à contacter	Chaîne comprenant de 5 à 30 caractères pour *numéro_téléphone*
-cs	Etat de l'emplacement de la machine	Chaîne comprenant de 2 à 3 caractères pour *état/province*
-cz	Code postal délimité par des apostrophes de l'emplacement de la machine	Chaîne pouvant comprendre jusqu'à 9 caractères pour *code_postal*
-loc	Nom d'hôte qualifié complet ou l'adresse IP pour le proxy HTTP	Chaîne pouvant comporter jusqu'à 63 caractères ou adresse IP pour *nom_d'hôte/adresse_IP*
-po	Port du proxy HTTP	chiffre compris entre 1 et 65535 pour *numéro_port*
-ps	Statut du proxy HTTP	enabled, disabled
-pw	Mot de passe délimité par des apostrophes pour le proxy HTTP	Chaîne pouvant comprendre jusqu'à 15 caractères pour *mot_de_passe*
-u	Nom d'utilisateur délimité par des apostrophes pour le proxy HTTP	Chaîne pouvant comprendre jusqu'à 30 caractères pour *nom_utilisateur*

Option	Description	Valeurs
1. Les dispositions de licence de Service Advisor doivent être acceptées via l'option -li avant de configurer d'autres options. 2. Toutes les zones d'informations de contact et de centre de support IBM sont requises avant de pouvoir activer l'assistance IBM pour Service Advisor. Si un proxy est requis, les zones de proxy HTTP doivent être renseignées.		

Syntaxe :

```
chconfig [options]
options :
-li view|accept
-sa statut Service Advisor
-sc code_pays
-ca adresse
-cci ville
-ce courrier_électronique
-cn nom_contact
-co nom_société
-cph numéro_téléphone
-cs état/province
-cz code_postal
-loc nom_d'hôte/adresse_IP
-po numéro_port
-ps statut
-pw mot_de_passe
-u nom_utilisateur
```

Commande chlog

Utilisez la commande **chlog** pour afficher les cinq derniers événements d'appel vers IBM émis par le système ou par l'utilisateur. L'appel le plus récent est répertorié en premier.

Le tableau ci-après présente les arguments pour les options.

Remarque : Vous devez accepter les dispositions de licence de Service Advisor avant d'utiliser cette commande.

Option	Description	Valeurs
-event_index	Spécifiez une entrée d'appel vers IBM à l'aide de son index dans le journal d'activité	Valeur numérique comprise entre 1 et 5
-ack	Avec/sans accusé de réception, un événement d'appel vers IBM a été corrigé	yes, no
-s	N'afficher que le résultat du support IBM	
-f	N'afficher que le résultat du serveur FTP/TFTP	

Syntaxe :

```
chlog [options]
options :
-event_index
-ack yes|no
-s
-f
```

Commande chmanual

Utilisez la commande **chmanual** pour générer un événement d'appel manuel vers IBM ou de test d'appel.

Remarque : Vous devez accepter les dispositions de licence de Service Advisor avant d'utiliser cette commande.

Le tableau ci-après présente les arguments pour les options.

Option	Description	Valeurs
-test	Générer un événement de test d'appel vers IBM	
-desc	Description, délimitée par des apostrophes, du problème	Chaîne pouvant comporter jusqu'à 100 caractères pour *description*

Syntaxe :

```
chmanual [options]
options :
-test
-desc description
```

Commande events

Utiliser la commande **events** pour afficher et éditer des événements d'exclusion.

Remarque : Vous devez accepter les dispositions de licence de Service Advisor avant d'utiliser cette commande.

Le tableau ci-après présente les arguments pour les options.

Option	Description	Valeurs
-che	Affichage et édition d'événements d'exclusion	
-add	Ajoute un événement d'appel vers IBM dans la liste d'exclusions d'appels	*ID_événement* sous le format `0xhhhhhhhhhhhhhhhh`
-rm	Supprime un événement d'appel vers IBM de la liste des d'exclusions d'appels	*ID_événement*|*all* sous le format `0xhhhhhhhhhhhhhhhh`, ou all

Syntaxe :

```
events [options]
options : -che {-add}|{-rm}
-add ID_événement
-rm ID_événement|all
```

Commande sdemail

Utilisez la commande **sdemail** pour configurer les informations de service de messagerie pour les destinataires spécifiés.

Le tableau ci-après présente les arguments pour les options.

Option	Description	Valeurs
-subj	Objet, délimité par des apostrophes, du courrier électronique	Chaîne pouvant comprendre jusqu'à 119 caractères pour *objet_du_courrier_électronique*
-to	Adresse électronique du destinataire. Cette option peut héberger plusieurs adresses en les séparant par une virgule.	Chaîne pouvant comprendre jusqu'à 119 caractères pour *adresse_électronique*

Syntaxe :

```
sdemail [options]
options :
-subj objet_du_courrier_électronique
-to adresse_électronique
```

Annexe A. Service d'aide et d'assistance

IBM met à votre disposition un grand nombre de services que vous pouvez contacter pour obtenir de l'aide, une assistance technique ou tout simplement pour en savoir plus sur les produits IBM.

La présente annexe explique comment obtenir des informations complémentaires sur IBM et les produits IBM, comment procéder et où vous adresser en cas de problème avec votre système.

Avant d'appeler

Avant d'appeler, vérifiez que vous avez effectué les étapes nécessaires pour essayer de résoudre le problème seul.

Si vous pensez qu'IBM doit faire jouer le service prévu par la garantie vis-à-vis de votre produit IBM, les techniciens de maintenance IBM peuvent vous aider à préparer plus efficacement votre appel.

- Vérifiez que tous les câbles sont bien connectés.
- Observez les interrupteurs d'alimentation pour vérifier que le système et les périphériques en option éventuels sont sous tension.
- Vérifiez si des mises à jour des logiciels, du microprogramme et des pilotes de périphériques du système d'exploitation sont disponibles pour votre produit IBM. La Déclaration de garantie IBM souligne que le propriétaire du produit IBM (autrement dit vous) est responsable de la maintenance et de la mise à jour de tous les logiciels et microprogrammes du produit (sauf si lesdites activités sont couvertes par un autre contrat de maintenance). Votre technicien de maintenance IBM vous demandera de mettre à niveau vos logiciels et microprogrammes si ladite mise à niveau inclut une solution documentée permettant de résoudre le problème.
- Si vous avez installé un nouveau matériel ou de nouveaux logiciels dans votre environnement, consultez la page http://www.ibm.com/systems/info/x86servers/serverproven/compat/us pour vérifier que votre produit IBM les prend en charge.
- Accédez au site http://www.ibm.com/supportportal pour rechercher des informations utiles à la résolution de votre problème.
- Rassemblez les informations suivantes pour les transmettre au support IBM. Ces données aideront le support IBM à trouver rapidement une solution à votre problème et permettent de garantir que vous recevrez le niveau de service prévu par le contrat auquel vous avez éventuellement souscrit.
  - Numéros des contrats de maintenance souscrits au titre du matériel et des logiciels, le cas échéant
  - Numéro de type de machine (identificateur IBM à quatre chiffres de la machine)
  - Numéro de modèle
  - Numéro de série
  - Niveaux du code UEFI et du microprogramme actuels du système
  - Toute autre information pertinente (messages d'erreur, journaux)

- Pour soumettre une demande de service électronique, accédez au site http://www.ibm.com/support/entry/portal/Open_service_request. En déposant une demande de service électronique, vous engagez le processus de recherche de solution à votre problème en mettant rapidement et efficacement les informations pertinentes à la disposition du support IBM. Les techniciens de maintenance IBM peuvent commencer à travailler sur votre solution dès que vous avez complété et déposé une demande de service électronique.

Bon nombre d'incidents peuvent être résolus sans aide extérieure. Pour cela, suivez les procédures indiquées par IBM dans l'aide en ligne ou dans la documentation fournie avec votre produit IBM. Les documents livrés avec les systèmes IBM décrivent également les tests de diagnostic que vous pouvez exécuter. La plupart des systèmes, systèmes d'exploitation et programmes sont fournis avec des documents présentant les procédures d'identification et de résolution des incidents, ainsi que des explications sur les messages et les codes d'erreur. Si vous pensez que l'incident est d'origine logicielle, consultez la documentation qui accompagne le système d'exploitation ou le programme.

Utilisation de la documentation

Les informations concernant votre système IBM et les logiciels préinstallés (et les dispositifs en option éventuels) figurent dans la documentation fournie avec le produit. Cette documentation est constituée de manuels imprimés, de livres électroniques, de fichiers README et de fichiers d'aide.

Pour en savoir plus, consultez les informations d'identification et de résolution des incidents dans la documentation de votre système. Les informations d'identification et de résolution des incidents et les programmes de diagnostic peuvent vous signaler la nécessité d'installer des pilotes de périphérique supplémentaires ou mis à niveau, voire d'autres logiciels. IBM gère des pages Web à partir desquelles vous pouvez vous procurer les dernières informations techniques, des pilotes de périphérique ou des mises à jour. Pour accéder à ces pages, accédez au site http://www.ibm.com/supportportal.

Service d'aide et d'information sur le Web

Des informations à jour sur les produits IBM et leur support sont disponibles sur le Web.

Sur le Web, vous trouverez des informations à jour relatives aux systèmes, aux périphériques en option, aux services et au support IBM sur la page http://www.ibm.com/supportportal. Les informations relatives à IBM System x sont disponibles sur http://www.ibm.com/systems/x. Les informations relatives à IBM BladeCenter sont disponibles sur http://www.ibm.com/systems/bladecenter. Les informations relatives à IBM IntelliStation sont disponibles sur http://www.ibm.com/systems/intellistation.

Procédure d'envoi de données DSA à IBM

Utilisez IBM Enhanced Customer Data Repository pour envoyer des données de diagnostic à IBM.

Avant d'envoyer des données de diagnostic à IBM, voir les conditions d'utilisation à l'adresse http://www.ibm.com/de/support/ecurep/terms.html.

Utilisez l'une des méthodes suivantes pour envoyer des données de diagnostic à IBM :

- **Téléchargement standard :** http://www.ibm.com/de/support/ecurep/send_http.html
- **Téléchargement standard avec le numéro de série du système :** http://www.ecurep.ibm.com/app/upload_hw
- **Téléchargement sécurisé :** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Téléchargement sécurisé avec le numéro de série du système :** https://www.ecurep.ibm.com/app/upload_hw

Création d'une page Web de support personnalisée

Vous pouvez créer une page de support personnalisée en identifiant les produits IBM qui vous intéressent.

Pour créer une page Web de support personnalisée, accédez à la page http://www.ibm.com/support/mynotifications. A partir de cette page personnalisée, vous pouvez vous inscrire pour recevoir des notifications hebdomadaires par courrier électronique sur les nouveaux documents techniques, pour rechercher des informations et des produits téléchargeables, et accéder à divers services d'administration.

Service et support logiciel

Grâce à IBM Support Line, vous pouvez bénéficier d'une assistance téléphonique payante sur l'utilisation, la configuration et les problèmes logiciels relatifs à vos produits IBM.

Pour savoir quels produits sont pris en charge par Support Line dans votre pays ou dans votre région, consultez la page http://www.ibm.com/services/supline/products.

Pour plus d'informations sur Support Line et les autres services IBM, visitez le site Web à l'adresse http://www.ibm.com/services ou http://www.ibm.com/planetwide pour obtenir la liste des numéros de téléphone d'assistanc. Au Canada, appelez le 1-800-IBM-SERV (1-800-426-7378) ; en France, appelez le 0810 TEL IBM (0810 835 426).

Service et support matériel

Vous pouvez bénéficier du service matériel auprès de votre revendeur IBM ou d'IBM Services.

Pour trouver un revendeur autorisé par IBM à fournir un service de garantie, accédez au site http://www.ibm.com/partnerworld et cliquez sur **Rechercher des partenaires commerciaux**. Pour obtenir les numéros de téléphone du support IBM, consultez la page http://www.ibm.com/planetwide. Au Canada, appelez le 1-800-IBM-SERV (1-800-426-7378) ; en France, appelez le 0801 TEL IBM (0801 835 426).

Aux Etats-Unis et au Canada, le service et le support matériel sont disponibles 24 heures sur 24, 7 jours sur 7. Au Royaume-Uni, ces services sont disponibles du lundi au vendredi, de 9 heures à 18 heures.

Service produits d'IBM Taïwan

Utilisez les informations suivantes pour contacter le service produits d'IBM Taïwan.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

Coordonnées du service produits d'IBM Taïwan :

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Téléphone : 0800-016-888

Annexe B. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service IBM puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Etats-Unis

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7 Canada

LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT» SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non-IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de services peuvent appartenir à des tiers.

La liste actualisée de toutes les marques d'IBM est disponible sur le Web à l'adresse http://www.ibm.com/legal/us/en/copytrade.shtml.

Adobe et PostScript sont des marques d'Adobe Systems Incorporated aux Etats-Unis et/ou dans certains autres pays.

Cell Broadband Engine est une marque de Sony Computer Entertainment, Inc., aux Etats-Unis et/ou dans certains autres pays, et est utilisée sous licence.

Intel, Intel Xeon, Itanium et Pentium sont des marques d'Intel Corporation ou de ses filiales aux Etats-Unis et/ou dans certains autres pays.

Java ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Microsoft, Windows et Windows NT sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

UNIX est une marque enregistrée de The Open Group aux Etats-Unis et/ou dans certains autres pays.

Remarques importantes

La vitesse du processeur correspond à la vitesse de l'horloge interne du microprocesseur. D'autres facteurs peuvent également influer sur les performances d'une application.

Les vitesses de l'unité de CD ou de DVD recensent les débits de lecture variable. La vitesse réelle varie et est souvent inférieure aux vitesses maximales possibles.

Lorsqu'il est fait référence à la mémoire principale, à la mémoire réelle et virtuelle ou au volume des voies de transmission, 1 ko correspond à 1024 octets, 1 Mo correspond à 1 048 576048 576 octets et 1 073 741 824 Go correspond à 1 073 741 824 octets.

En matière de taille de disque dur ou de volume de communications, 1 Mo correspond à 1 000 000 octets, 1 Go correspond à 1 000 000 000 octets. La capacité totale à laquelle l'utilisateur a accès peut varier en fonction de l'environnement d'exploitation.

La capacité maximale de disques durs internes suppose que toutes les unités de disque dur standard ont été remplacées et que toutes les baies d'unité sont occupées par des unités IBM. La capacité de ces unités doit être la plus importante disponible à ce jour.

La mémoire maximale peut nécessiter le remplacement de la mémoire standard par un module de mémoire en option.

Chaque cellule de mémoire SSD doit avoir un nombre de cycles d'écriture intrinsèque déterminé pouvant être pris en charge par la cellule. Par conséquent, une unité SSD peut faire l'objet d'un nombre maximal de cycles d'écriture, exprimé en `nombre d'octets écrits total`. Toute unité ayant dépassé cette limite peut ne pas pouvoir répondre aux commandes émises par le système ou ne pas être disponible pour des opérations d'écriture. IBM n'est pas responsable du remplacement d'une unité ayant dépassé son nombre maximal garanti de cycles de programmation/d'effacement, documenté dans les spécifications officielles publiées pour l'unité.

IBM ne prend aucun engagement et n'accorde aucune garantie concernant les produits et les services non IBM liés à ServerProven, y compris en ce qui concerne les garanties d'aptitude à l'exécution d'un travail donné. Seuls les tiers proposent et assurent la garantie de ces produits.

IBM ne prend aucun engagement et n'accorde aucune garantie concernant les produits non IBM. Seuls les tiers sont chargés d'assurer directement le support des produits non IBM.

Les applications fournies avec les produits IBM peuvent être différentes des versions mises à la vente et ne pas être fournies avec la documentation complète ou toutes les fonctions.

Contamination particulaire

Attention : les particules aériennes (notamment les écailles ou particules de métal) et les gaz réactifs agissant seuls ou en combinaison avec d'autres facteurs environnementaux, tels que l'humidité ou la température, peuvent représenter un risque pour le périphérique décrit dans le présent document.

Les risques liés à la présence de niveaux de particules ou de concentration de gaz nocifs excessifs incluent les dégâts pouvant provoquer le dysfonctionnement du périphérique, voire l'arrêt total de celui-ci. Cette spécification présente les limites relatives aux particules et aux gaz permettant d'éviter de tels dégâts. Ces limites ne doivent pas être considérées comme définitives, car de nombreux autres facteurs, tels que la température ou le niveau d'humidité de l'air, peuvent influencer l'effet des particules ou du transfert environnemental des contaminants gazeux ou corrosifs. En l'absence de limites spécifiques exposées dans le présent document, vous devez mettre en oeuvre des pratiques permettant de maintenir des niveaux de particules et de gaz protégeant la santé et la sécurité humaines. Si IBM détermine que les niveaux de particules ou de gaz de votre environnement ont provoqué l'endommagement du périphérique, IBM peut, sous certaines conditions, mettre à disposition la réparation ou le remplacement des périphériques ou des composants lors de la mise en oeuvre de mesures correctives appropriées, afin de réduire cette contamination environnementale. La mise en oeuvre de ces mesures correctives est de la responsabilité du client.

Tableau 21. Limites relatives aux particules et aux gaz

Contaminant	Limites
Particule	• L'air de la pièce doit être filtré en continu selon un rendement à la tache atmosphérique de 40 % (MERV 9), conformément à la norme ASHRAE 52.2[1]. • L'air pénétrant dans un centre de données doit être filtré selon une efficacité minimale de 99,97 % à l'aide de filtres HEPA (high-efficiency particulate air) conformes à la spécification MIL-STD-282. • L'humidité relative déliquescente de la contamination particulaire doit être supérieure à 60 %[2]. • La pièce doit être exempte de contamination par conducteurs tels que les trichites de zinc.
Gaz	• Cuivre : classe G1, conformément à la norme ANSI/ISA 71.04-1985[3] • Argent : taux de corrosion inférieur à 300 Å en 30 jours

[1] ASHRAE 52.2-2008 - *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] L'humidité relative déliquescente de la contamination par particules correspond à l'humidité relative à partir de laquelle la poussière absorbe suffisamment d'eau pour devenir humide et favoriser une conduction ionique.

[3] ANSI/ISA-71.04-1985. *Environmental conditions for process measurement and control systems: Airborne contaminants*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Format de la documentation

Les publications relatives à ce produit sont au format Adobe PDF (Portable Document Format) et doivent respecter des normes d'accessibilité. Si vous rencontrez des difficultés lors de l'utilisation des fichiers PDF et souhaitez obtenir une publication au format basé sur le Web ou accessible au format PDF, envoyez votre e-mail à l'adresse suivante :

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
Etats-Unis

Dans votre demande, veuillez inclure le numéro de référence ainsi que le titre de la publication.

Lors de l'envoi d'informations à IBM, vous accordez à IBM le droit non exclusif d'utiliser ou de diffuser ces informations de toute manière qu'elle jugera appropriée et sans obligation de sa part.

Déclaration réglementaire relative aux télécommunications

Ce produit n'est peut-être pas certifié dans votre pays pour la connexion, par quelque moyen que ce soit, à des interfaces de réseaux de télécommunications publiques. Des certifications supplémentaires peuvent être requises pas la loi avant d'effectuer toute connexion. Contactez un représentant IBM ou votre revendeur pour toute question.

Bruits radioélectriques

Lorsque vous connectez un moniteur à l'équipement, vous devez utiliser le câble du moniteur dédié et tous les dispositifs de suppression des interférences qui sont fournis avec le moniteur.

Recommandation de la Federal Communications Commission (FCC) [Etats Unis]

Remarque : cet appareil respecte les limites des caractéristiques d'immunité des appareils numériques définies par la classe A, conformément au chapitre 15 de la réglementation de la FCC. La conformité aux spécifications de cette classe offre une garantie acceptable contre les perturbations électromagnétiques dans les zones commerciales. Ce matériel génère, utilise et peut émettre de l'énergie radiofréquence. Il risque de parasiter les communications radio s'il n'est pas installé conformément aux instructions du constructeur. L'exploitation faite en zone résidentielle peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire à prendre les dispositions nécessaires pour en éliminer les causes.

Utilisez des câbles et connecteurs correctement blindés et mis à la terre afin de respecter les limites de rayonnement définies par la réglementation de la FCC. IBM ne peut pas être tenue pour responsable du brouillage des réceptions radio ou télévision résultant de l'utilisation de câbles ou connecteurs inadaptés ou de modifications non autorisées apportées à cet appareil. Toute modification non autorisée pourra annuler le droit d'utilisation de cet appareil.

Cet appareil est conforme aux restrictions définies dans le chapitre 15 de la réglementation de la FCC. Son utilisation est soumise aux deux conditions suivantes : (1) il ne peut pas causer de perturbations électromagnétiques gênantes et (2) il doit accepter toutes les perturbations reçues, y compris celles susceptibles d'occasionner un fonctionnement indésirable.

Avis de conformité à la réglementation d'Industrie Canada pour la classe A

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Recommandation relative à la classe A (Australie et Nouvelle-Zélande)

Avertissement : Ce matériel appartient à la classe A. Il est susceptible d'émettre des ondes radioélectriques risquant de perturber les réceptions radio. Son emploi dans une zone résidentielle peut créer des interférences. L'utilisateur devra alors prendre les mesures nécessaires pour les supprimer.

Avis de conformité à la directive de l'Union Européenne

Le présent produit satisfait aux exigences de protection énoncées dans la directive 2004/108/CE du Conseil concernant le rapprochement des législations des Etats membres relatives à la compatibilité électromagnétique. IBM décline toute responsabilité en cas de non-respect de cette directive résultant d'une modification non recommandée du produit, y compris l'ajout de cartes en option non IBM.

Avertissement : Ce matériel appartient à la classe A EN 55022. Il est susceptible d'émettre des ondes radioélectriques risquant de perturber les réceptions radio. Son emploi dans une zone résidentielle peut créer des interférences. L'utilisateur devra alors prendre les mesures nécessaires pour les supprimer.

Fabricant compétent :

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Contact pour l'Union Européenne :

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Téléphone : +49 7032 15 2941
Adresse électronique : lugi@de.ibm.com

Avis de conformité à la classe A (Allemagne)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:
Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Avis de conformité à la classe A (VCCI japonais)

この装置は、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。 VCCI-A

Ce produit de la classe A respecte les limites des caractéristiques d'immunité définies par le Voluntary Control Council for Interference (VCCI) japonais. Si ce produit est utilisé dans une zone résidentielle, il peut créer des perturbations électromagnétiques. L'utilisateur devra alors prendre les mesures nécessaires pour en éliminer les causes.

Recommandation de la Korea Communications Commission (KCC)

이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Cet équipement est un équipement professionnel à compatibilité électromagnétique (type A). Les vendeurs et les utilisateurs doivent en prendre soin. Cet équipement n'est pas destiné à un usage domestique.

Recommandation relative aux interférences électromagnétiques pour la classe A (Russie)

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

Recommandation pour la classe A (République populaire de Chine)

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Avis de conformité pour la classe A à Taïwan

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Index

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

Référence : 00FH265

(1P) P/N: 00FH265