IBM

# Integrated Management Module II
# Guide d'utilisation

Integrated Management Module II

# Guide d'utilisation

**Troisième édition - Juillet 2013**



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 processeur de service du module de gestion intégré II (Integrated Management Module II, IMM2) est la deuxième génération du processeur de service du module de gestion intégré (IMM) qui consolide les fonctionnalités de processeur de service, Super I/O, contrôleur vidéo et intervention à distance en une seule puce située sur la carte mère du serveur. Comme IMM, IMM2 offre plusieurs améliorations par rapport aux fonctionnalités combinées du contrôleur de gestion de la carte mère (BMC) et du Remote Supervisor Adapter II, y compris ces fonctions :

- Choix entre une connexion Ethernet dédiée ou partagée pour la gestion des systèmes.
- 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 IBM® BladeCenter.
- Analyse système dynamique (DSA) intégrée.
- Configuration distante à l'aide de l'utilitaire Advanced Settings Utility (ASU). Cette fonctionnalité ne s'applique pas aux serveurs lame IBM BladeCenter.
- Possibilité pour les applications et les outils d'accéder au module IMM2 via communication intrabande ou hors bande. Seule la connexion intrabande IMM2 est prise en charge sur les serveurs lame IBM BladeCenter.
- Fonctions d'intervention à distance améliorées. Cette fonctionnalité ne s'applique pas aux serveurs lame IBM BladeCenter.

**Remarques :**

- Aucun port réseau de gestion de système dédié n'est disponible sur les serveurs lame IBM BladeCenter et certains serveurs System x ; pour ces serveurs, seul le paramètre *partagé* est disponible.
- Pour les serveurs lame IBM BladeCenter, le module de gestion évolué IBM BladeCenter est le module de gestion primaire pour les fonctions de gestion de système et le multiplexage clavier/vidéo/souris (KVM).

Le microprogramme de serveur IBM System x® constitue l'implémentation IBM de l'interface UEFI (Unified Extensible Firmware Interface). Il remplace le système de base entrée/sortie (BIOS) dans les serveurs IBM System x et les serveurs lame IBM BladeCenter. 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 non disponibles dans BIOS, y compris la conformité UEFI 2.3, la compatibilité iSCSI, la technologie Active Energy Manager et des fonctions de fiabilité et de service avancées. 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 IBM.

Ce document explique comment utiliser les fonctions du module IMM2 dans un serveur IBM. Le module IMM2 opère avec le microprogramme IBM System x Server Firmware pour fournir une capacité de gestion de systèmes aux serveurs System x, BladeCenter et IBM Flex System.

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 de produit, la famille de produit et les numéros de modèle de vos sous-systèmes de stockage. 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 de base, standard et avancées du module IMM2

Le module IMM2 est proposé avec trois niveaux de fonctionnalités : le niveau de base, le niveau standard et le niveau avancé. Pour plus d'information sur le niveau IMM2 installé sur votre serveur IBM, consultez la documentation de votre serveur. Tous les niveaux offrent les fonctionnalités 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

En outre, les niveaux standard et avancé prennent en charge la gestion basée sur le Web avec des navigateurs Web standard.

**Remarque :** Certaines fonctions peuvent ne pas s'appliquer aux serveurs lame IBM BladeCenter.

Les fonctions du niveau de base IMM2 sont répertoriées ci-après.

### Fonctions du niveau de base IMM2

Les fonctions du niveau de base du module IMM2 sont les suivantes :

- Interface IPMI 2.0
- Contrôle de température

- Contrôle de ventilateur
- Gestion des voyants
- Contrôle d'alimentation/de réinitialisation du serveur
- Contrôle de détecteur
- Alerte des événements de la plateforme IPMI
- IPMI série sur LAN

## Fonctionnalités de niveau standard du module IMM2

Les fonctionnalités de niveau standard du module IMM2 sont les suivantes :

- Toutes les fonctionnalités de niveau de base du module IMM2
- Gestion basée sur le Web avec navigateurs Web standard
- Interfaces SNMPv1 et SNMPv3
- Interfaces de ligne de commande Telnet et SSH
- Contrôle d'alimentation/de réinitialisation serveur planifié
- Journalisation des audits et événements lisible à l'oeil
- Indication de l'état du santé du système
- Chargeur et programmes de surveillance du système d'exploitation
- Authentification et autorisation LDAP
- Alerte SNMP, alerte par indication CIM, Syslog et courrier électronique
- Synchronisation de l'horloge NTP
- Réacheminement de la console en série via Telnet/SSH

## Fonctions du niveau avancé IMM2

Les fonctions de niveau avancé du module IMM2 sont les suivantes :

- Toutes les fonctions du niveau de base et du niveau standard IMM2
- Intervention à distance clients Java et ActivX :
  - Prise en charge clavier, vidéo et souris à distance
  - Support distant
  - Disque distant sur carte
- Capture d'écran d'échec en cas de blocage du système d'exploitation

## Améliorations des fonctionnalités IMM2

Les fonctionnalités IMM2 suivantes ont été améliorées par rapport au module IMM :

- Sécurité (processeur de service approuvé) :
  - Démarrage sécurisé
  - Mises à jour signées
  - Core Root for Trust Measurement (CRTM) IMM2
  - Module de plateforme sécurisé
- Nouvelle conception Web cohérente à travers le système x IBM
- Amélioration de la résolution vidéo et de la profondeur de couleur de l'intervention distante
- Client d'intervention distante ActiveX
- Interface Ethernet-via-USB mise à niveau à USB 2.0
- Alerte syslog

- Aucune réinitialisation du IMM2 requise après les modifications de configuration

### Mise à niveau du module IMM2

Si votre serveur IBM vous a été fourni avec la fonctionnalité de microprogramme IMM2 de base ou standard, vous pouvez mettre à niveau la fonctionnalité IMM2 sur votre serveur. Pour plus d'informations sur les mises à niveau disponibles et les modalités de commande, voir Chapitre 7, «Features on Demand», à la page 137.

## Utilisation du module IMM2 avec le module de gestion évolué BladeCenter

Le module de gestion évolué BladeCenter représente l'interface standard de gestion des systèmes des produits IBM BladeCenter. Bien que le module IMM2 soit maintenant inclus sur certains serveurs lame IBM BladeCenter, le module de gestion évolué demeure le module de gestion utilisé pour les fonctions de gestion des systèmes et le multiplexage KVM des produits IBM BladeCenter, y compris les serveurs lame IBM.

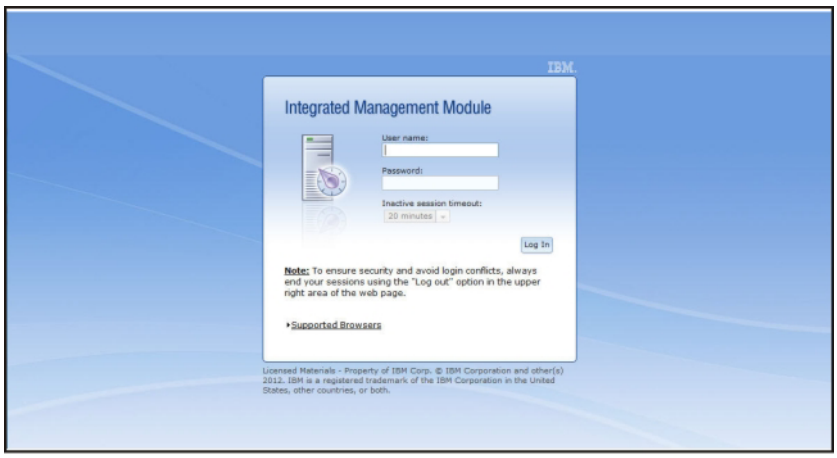
Il n'existe pas d'accès réseau externe au module IMM2 sur les serveurs lame IBM BladeCenter et le module de gestion évolué doit être utilisé pour la gestion à distance des serveurs lame IBM BladeCenter. Le module IMM2 remplace la fonctionnalité assurée par le contrôleur BMC et la carte facultative cKVM (contrôle simultané du clavier, de la vidéo et de la souris) présents sur des produits de serveur lame IBM antérieurs.

## Exigences relatives au navigateur Web et au système d'exploitation

L'interface Web d'IMM2 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 7 ou 8
- Mozilla Firefox version 3.5 ou ultérieure

Si vous utilisez des versions plus récentes de Microsoft Internet Explorer, il est conseillé d'utiliser l'affichage de compatibilité dans Internet Explorer pour pouvoir afficher les pages Web IMM2. Les navigateurs précédemment indiqués sont ceux qui sont actuellement pris en charge par le microprogramme IMM2. Le microprogramme IMM2 peut faire l'objet d'améliorations régulières pour inclure la prise en charge d'autres navigateurs. Consultez la liste "Supported Browsers" sur la page de connexion IMM2 pour savoir quels sont les navigateurs pris en charge par la version du microprogramme IMM2 actuellement installée sur le système. La figure ci-après représente l'écran de connexion IMM2.




Les systèmes d'exploitation de serveur suivants prennent en charge la connexion USB requise par la fonction d'intervention à distance :

- 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

Le cache de votre navigateur Internet stocke les informations relatives aux pages Web que vous visitez afin qu'elles se chargent plus rapidement plus tard. Après une mise à jour flash du microprogramme IMM2, il se peut que votre navigateur continue à utiliser les informations du cache au lieu de les extraire du module IMM2. Il est donc recommandé après une telle mise à jour de vider le cache afin de garantir un affichage correct des pages Web issues du module IMM2.

## 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 IMM2

**Important :** Cette section ne s'applique pas aux serveurs lame IBM et IBM BladeCenter. Bien que le module IMM2 soit installé en standard sur certains produits IBM BladeCenter et serveurs lame IBM, le module de gestion évolué IBM BladeCenter constitue le module de gestion principal pour les fonctions de gestion des systèmes et multiplexage KVM des produits IBM BladeCenter, y compris les serveurs lame IBM. Les utilisateurs qui souhaitent configurer les paramètres IMM2 sur les serveurs blade doivent utiliser Advanced Settings Utility (ASU) sur le serveur blade pour effectuer ces actions.

Le module IMM2 réunit sur une seule puce les fonctions de processeur de service, de contrôleur vidéo et d'intervention à distance (lorsqu'une clé de support virtuel facultative est installée). Pour accéder à distance au module IMM2 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'IMM2.

## Accès à l'interface Web IMM2

Le module IMM2 prend en charge l'adressage IPv4 statique et DHCP (Dynamic Host Configuration Protocol). L'adresse IPv4 statique par défaut affectée au module IMM2 est 192.168.70.125. Le module IMM2 est configuré initialement pour tenter d'obtenir une adresse depuis un serveur DHCP, et s'il n'y parvient pas, il utilise alors l'adresse IPv4 statique.

Le module IMM2 prend également en charge IPv6, mais il ne dispose pas d'une adresse IP IPv6 statique fixe par défaut. Pour l'accès initial au module IMM2 dans un environnement IPv6, vous pouvez utiliser l'adresse IP IPv4 ou l'adresse lien-local IPv6. Le module IMM2 génère une adresse lien-local IPv6 unique qui est indiquée dans l'interface Web d'IMM2 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 IMM2, 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.

Le module IMM2 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.

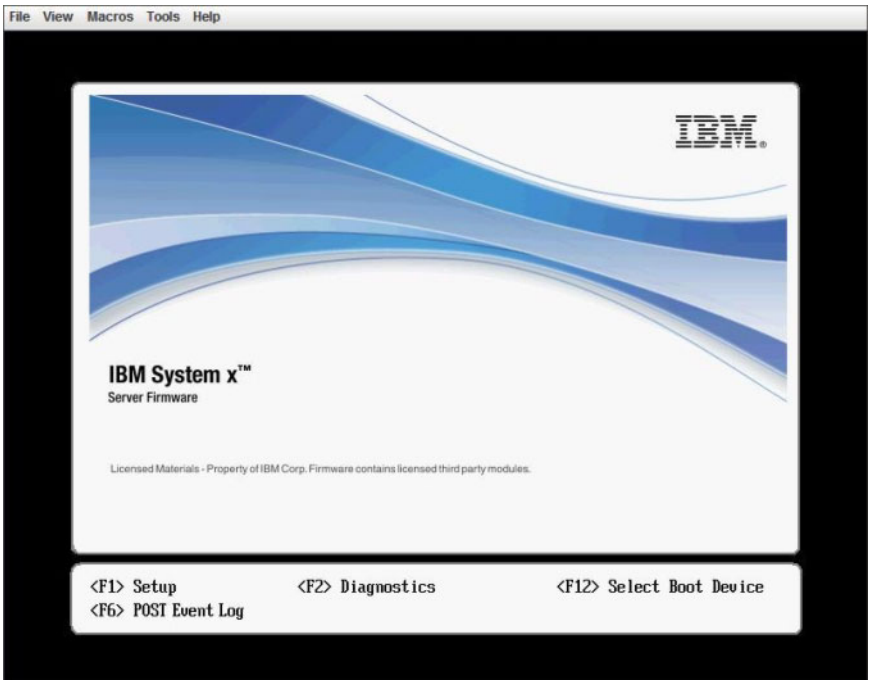
**Remarque :** Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur votre serveur. Si votre matériel ne dispose pas d'un port réseau dédié, l'option *shared* est la seule option IMM2 disponible.

## Configuration de la configuration réseau IMM2 via l'utilitaire Setup du IBM System x Server Firmware

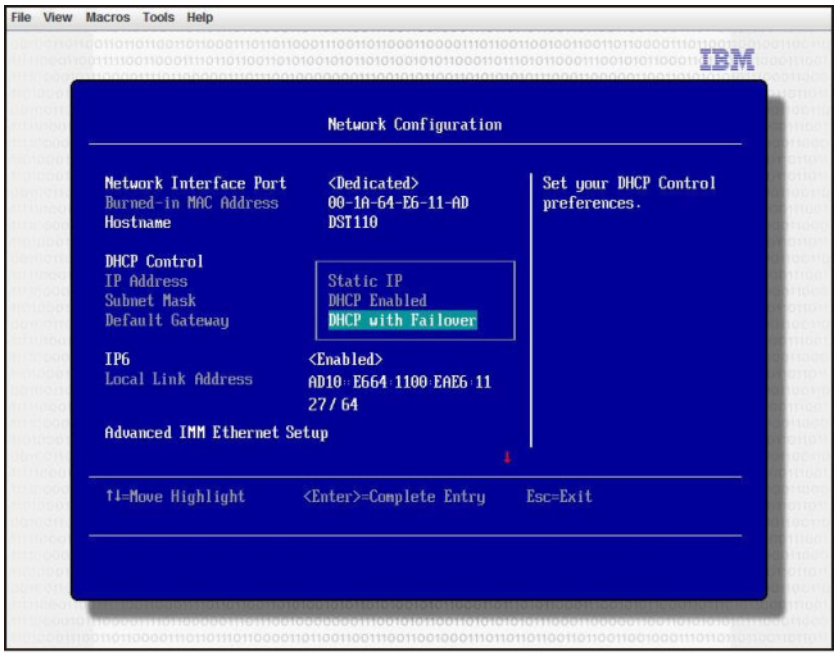
Après avoir démarré le serveur, vous pouvez utiliser l'utilitaire Setup pour sélectionner une connexion réseau IMM2. Le serveur hébergeant le matériel IMM2 doit être connecté à un serveur DHCP ou le réseau du serveur doit être configuré afin d'utiliser l'adresse IP statique d'IMM2. Pour configurer la connexion réseau du module IMM2 à l'aide de 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 90 secondes 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 IMM2 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 IMM2 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 IMM2 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 le module IMM2 sur votre serveur, reportez-vous à la documentation accompagnant votre serveur.
10. Faites défiler vers le bas et 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 opérationnel.
- Vous pouvez également configurer la connexion réseau IMM2 à travers l'interface Web ou l'interface de ligne de commande(CLI) du module IMM2. Dans l'interface Web du module IMM2, les connexions réseau sont configurées sur la page **Network Protocol Properties** (sélectionnez **Network** dans le menu **IMM Management**). Dans l'interface de ligne de commande du module IMM2, les connexions réseau sont configurées au moyen de plusieurs commandes qui dépendent de la configuration de votre installation.

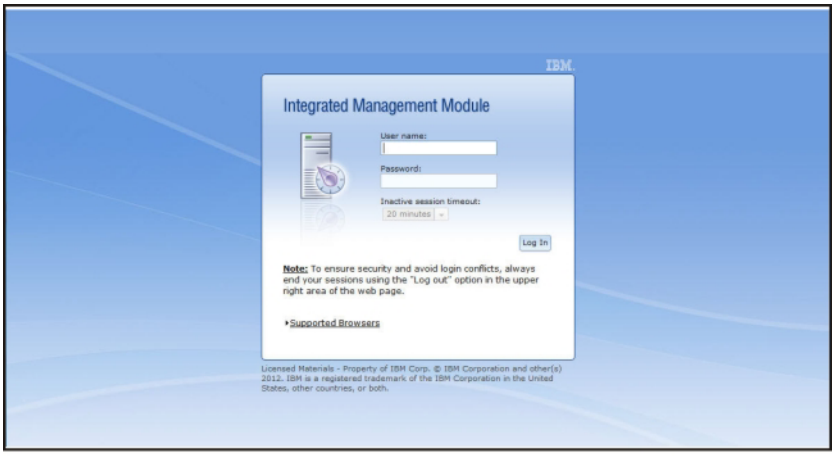
## Connexion au module IMM2

**Important :** Le module IMM2 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. Pour une sécurité accrue, modifiez ce nom d'utilisateur et ce mot de passe lors de votre configuration initiale.

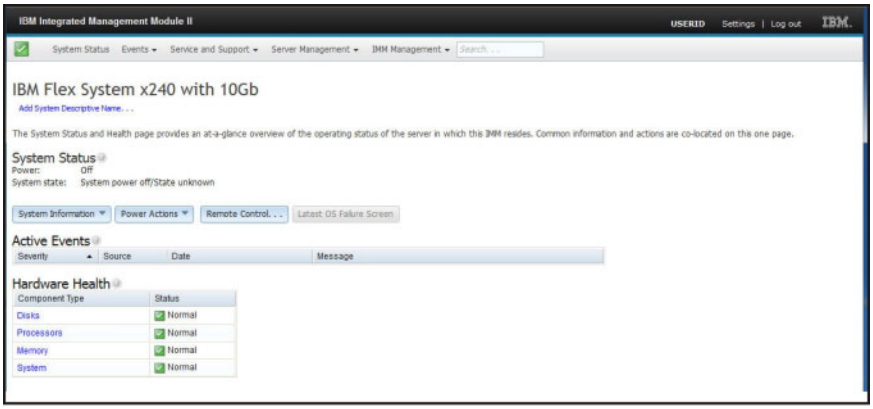
Pour accéder au module IMM2 depuis l'interface Web IMM2, procédez comme suit.

1. Ouvrez un navigateur Web. Dans la zone d'adresse ou d'URL, entrez l'adresse IP ou le nom d'hôte du module IMM2 auquel vous souhaitez vous connecter.
2. Entrez votre nom d'utilisateur et votre mot de passe dans la fenêtre IMM2 Login. Si vous utilisez le module IMM2 pour la première fois, vous pouvez obtenir le nom d'hôte et le 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.

   La figure suivante représente la fenêtre Login.




3. Cliquez sur **Log In** pour ouvrir une session. Le navigateur ouvre la page System Status, comme représentée dans la figure suivante. Cette page offre un aperçu rapide de l'état du serveur et un récapitulatif de son état de fonctionnement.



Pour obtenir une description des actions pouvant être réalisées depuis les onglets situés dans la partie supérieure de l'interface Web IMM2, voir «Descriptions des actions IMM2».

## Descriptions des actions IMM2

Naviguez dans la partie supérieure de la fenêtre IMM2 pour réaliser des activités avec IMM2. La barre de titre indique le nom d'utilisateur avec lequel vous êtes connecté. Elle vous permet de configurer les **paramètres** de fréquence de rafraîchissement de l'écran d'état et un message d'accueil personnalisé, et de vous **déconnecter** de l'interface Web IMM2. Sous la barre de titre se trouvent des onglets qui vous permettent d'accéder aux différentes fonctions du module IMM2, comme indiqué dans le tableau 1.


*Tableau 1. Actions du module IMM2*

| Onglet | Sélection | Description |
|---|---|---|
| System Status | | La page System Status vous permet d'afficher l'état du système, les événements système actifs et des informations sur la santé du matériel. Elle fournit des liens rapides vers les pages System Information, Server Power Actions, et Remote Control de l'onglet Server Management, et vous permet d'afficher une image de la dernière capture d'écran relative à une panne du système d'exploitation. Pour plus d'informations, voir «Onglet System Status», à la page 18 et «Affichage de l'état du système», à la page 93. |
| Events | Event Log | La page Event Log affiche les entrées qui sont actuellement stockées dans le journal des événements du module IMM2. Le journal contient une description des événements système qui sont signalés, notamment des informations sur toutes les tentatives d'accès à distance et les modifications de configuration. Tous les événements recensés dans le journal sont accompagnés d'un horodatage qui utilise les paramètres de date et d'heure du module IMM2. Certains événements génèrent également des alertes, s'ils ont été configurés pour cela. Vous pouvez trier et filtrer les événements du journal des événements et les exporter dans un fichier texte. Pour plus d'informations, voir «Onglet Events», à la page 24 et «Gestion du journal des événements», à la page 121. |
| | Event Recipients | La page Event Recipients vous permet de gérer les destinataires des événements système. Elle vous permet de configurer chaque destinataire et de gérer les paramètres qui s'appliquent à tous les destinataires d'événement. Vous pouvez également générer un événement test afin de vérifier le fonctionnement du dispositif de notification. Pour plus d'informations, voir «Destinataires des événements», à la page 26 et «Notification des événements système», à la page 123. |
| Service and Support | Download Service Data | La page Download Service Data permet de créer un fichier compressé contenant des informations qui peuvent être utilisées par le support IBM pour vous aider. Pour plus d'informations, voir «Téléchargement des données de service», à la page 29 et «Collecte des informations de service et de support», à la page 128. |

*Tableau 1. Actions du module IMM2 (suite)*

| Onglet | Sélection | Description |
|---|---|---|
| Server Management | Server Firmware | La page Server Firmware affiche des niveaux de microprogramme et vous permet de mettre à jour le microprogramme de module IMM2, le microprogramme de serveur et le microprogramme DSA. Pour plus d'informations, voir «Microprogramme de serveur», à la page 31 et «Mise à jour du microprogramme de serveur», à la page 116. |
| | Remote Control | La page Remote Control vous permet de contrôler le serveur au niveau du système d'exploitation. Elle permet d'accéder aux fonctionnalités de disque distant et de console distante. Vous pouvez afficher et utiliser la console serveur à partir de votre ordinateur, et vous pouvez monter l'une de vos unités de disque, telles que l'unité de CD-ROM ou l'unité de disquette, sur le serveur. Lorsque vous avez monté un disque, vous pouvez l'utiliser pour redémarrer le serveur et pour mettre à jour le microprogramme sur le serveur. Il apparaît comme une unité de disque USB reliée au serveur. Pour plus d'informations, voir «Contrôle à distance», à la page 36 et «Fonctions d'intervention et de contrôle à distance», à la page 103. |
| | Server Properties | La page Server Properties permet d'accéder aux différentes propriétés, conditions d'états et paramètres du serveur. Elle comprend les options suivantes :<br>• L'onglet General Settings contient des informations qui identifient le système auprès du support technique et des opérations.<br>• L'onglet des voyants affiche l'état de tous les voyants du système. Il vous permet également de modifier l'état du voyant d'emplacement.<br>• L'onglet Hardware Information affiche les données techniques essentielles du serveur. Le module IMM2 collecte des informations sur le serveur, des informations sur le composant serveur et des informations sur le matériel de réseau.<br>• L'onglet Environmentals affiche les informations de tension et de température relatives au serveur et à ses composants.<br>• L'onglet Hardware Activity affiche un historique des composants d'unité remplaçable sur site ayant été ajoutés ou retirés du système.<br><br>Pour plus d'informations, voir «Propriétés serveur», à la page 41. |
| | Server Power Actions | La page Server Power Actions permet un contrôle d'alimentation à distance total sur le serveur via des actions de mise sous tension, de mise hors tension et de redémarrage. Pour plus d'informations, voir «Actions de contrôle de l'alimentation serveur», à la page 44 et «Contrôle de l'état d'alimentation du serveur», à la page 102. |
| | Disks | La page Hard Disks affiche l'état des unités de disque dur présentes dans le serveur. Vous pouvez cliquer sur le nom d'une unité de disque dur pour afficher les événements actifs correspondants. Pour plus d'informations, voir «Disques», à la page 45. |
| | Memory | La page Memory affiche les modules de mémoire disponibles dans le système, ainsi que leur état, type et capacité. Vous pouvez cliquer sur le nom d'un module pour afficher un événement et d'autres informations matérielles pour le module de mémoire. Si vous retirez ou remplacez une barrette DIMM, le serveur doit être mis sous tension au moins une fois après le retrait ou le remplacement pour afficher les informations de mémoire correctes. Pour plus d'informations, voir «Mémoire», à la page 45. |

*Tableau 1. Actions du module IMM2 (suite)*

| Onglet | Sélection | Description |
|---|---|---|
| Server Management<br><br>*(suite)* | Processors | La page CPUs affiche les modules de mémoire disponibles dans le système, ainsi que leur état, type et capacité. Vous pouvez cliquer sur le nom d'un microprocesseur pour afficher les événements et d'autres informations sur le matériel relatifs à ce microprocesseur. Pour plus d'informations, voir «Processeurs», à la page 47. |
| | Server Timeouts | La page Server Timeouts vous permet de gérer des dépassements de délai d'attente de démarrage de serveur afin de détecter des occurrences de blocage de serveur et d'effectuer les reprises correspondantes. Pour plus d'informations, voir «Délais d'attente serveur», à la page 48 et «Configuration des délais d'attente du serveur», à la page 54. |
| | PXE Network Boot | La page PXE Network Boot vous permet de modifier la phase de démarrage (amorçage) du serveur hôte pour le redémarrage suivant afin de tenter un démarrage réseau PXE (Preboot Execution Environment)/DHCP (Dynamic Host Configuration Protocol). La séquence de démarrage du serveur hôte sera modifiée uniquement si celui-ci n'est pas sous protection PAP (Privileged Access Protection). Pour plus d'informations, voir «Amorçage réseau PXE», à la page 48 et «Configuration de l'amorçage réseau PXE», à la page 115. |
| | Latest OS Failure Screen | La page Latest OS Failure Screen affiche une image écran (si disponible) du dernier échec du système d'exploitation sur le serveur. Pour que votre module IMM2 puisse capturer les écrans d'échec du système d'exploitation, le programme de surveillance de système d'exploitation doit être activé. Pour plus d'informations, voir «Derniers échecs du système d'exploitation», à la page 48 et «Capture des données d'écran du dernier échec du système d'exploitation», à la page 130. |
| | Power Management | La page Server Power Management vous permet de gérer les règles et le matériel relatifs à l'alimentation et elle contient l'historique de la quantité d'énergie utilisée par le serveur. Pour plus d'informations, voir «Gestion de l'alimentation serveur», à la page 131. |
| IMM Management<br><br>*(suite à la page suivante)* | IMM Properties | La page IMM Properties permet d'accéder aux différentes propriétés et paramètres de votre module IMM2. Elle comprend les options suivantes :<br>• L'onglet Firmware fournit un lien vers la section Server Firmware de l'onglet Server Management.<br>• L'onglet IMM Date and Time Settings vous permet d'afficher et de configurer les paramètres de date et d'heure du module IMM2.<br>• L'onglet Serial Port permet de configurer les paramètres de port série du module IMM2. Ces paramètres incluent notamment le débit en bauds de port série utilisé par la fonction de réacheminement de port et la séquence de touches à utiliser pour passer du mode de réacheminement série au mode d'interface de ligne de commande.<br><br>Pour plus d'informations, voir Chapitre 4, «Configuration du module IMM2», à la page 51. |
| | Users | La page Users permet de configurer les profils de connexion au module IMM2 et les paramètres de connexion globaux. Elle permet également d'afficher les utilisateurs actuellement connectés au module IMM2. Les paramètres de connexion globaux incluent l'activation de l'authentification LDAP (Lightweight Directory Access Protocol), la définition du délai d'attente d'inactivité Web et la personnalisation des paramètres de sécurité de compte. Pour plus d'informations, voir «Configuration des comptes utilisateurs», à la page 58. |

*Tableau 1. Actions du module IMM2 (suite)*

| Onglet | Sélection | Description |
|---|---|---|
| IMM Management<br><br>*(suite)* | Network | La page Network Protocol Properties permet d'accéder aux propriétés, aux états et aux paramètres de mise en réseau pour le module IMM2 :<br>• L'onglet Ethernet permet de gérer la communication du module IMM2 à l'aide d'Ethernet.<br>• L'onglet SNMP permet de configurer les agents SNMPv1 et SNMPv3.<br>• L'onglet DNS permet de configurer les serveurs DNS avec lesquels le module IMM2 interagit.<br>• L'onglet DDNS permet d'activer ou de désactiver et de configurer DDNS (Dynamic Domain Name System) pour le module IMM2.<br>• L'onglet SMTP permet de configurer les informations sur le serveur SMTP utilisées pour les alertes envoyées par courrier électronique.<br>• L'onglet LDAP permet de configurer l'authentification d'utilisateur qui sera utilisée avec un ou plusieurs serveurs LDAP.<br>• L'onglet Telnet permet de gérer l'accès Telnet au module IMM2.<br>• L'onglet USB permet de contrôler l'interface USB utilisée pour la communication par voie interne entre le serveur et le module IMM2. Ces paramètres n'ont aucun impact sur les fonctions de contrôle à distance USB (clavier, souris et mémoire de masse).<br>• L'onglet Port Assignments vous permet de modifier les numéros de port utilisés par certains services sur le module IMM2.<br><br>Pour plus d'informations, voir «Configuration des protocoles réseau», à la page 68. |
| | Security | La page IMM Security permet d'accéder aux propriétés, à l'état et aux paramètres de sécurité du module IMM2 :<br>• L'onglet HTTPS Server vous permet d'activer ou de désactiver le serveur HTTPS et de gérer ses certificats.<br>• L'onglet CIM Over HTTPS vous permet d'activer ou de désactiver CIM over HTTPS et de gérer ses certificats.<br>• L'onglet LDAP vous permet d'activer ou de désactiver la sécurité LDAP et de gérer ses certificats.<br>• L'onglet SSH Server vous permet d'activer ou de désactiver le serveur SSH et de gérer ses certificats.<br><br>Pour plus d'informations, voir «Configuration des paramètres de sécurité», à la page 82. |
| | IMM Configuration | La page IMM Configuration affiche un récapitulatif des paramètres de configuration du module IMM2. Pour plus d'informations, voir «Restauration et modification de votre configuration IMM», à la page 89. |
| | Restart IMM | La page Restart IMM vous permet de réinitialiser le module IMM2. Pour plus d'informations, voir «Redémarrage du module IMM2», à la page 89. |
| | Reset IMM to factory defaults... | La page Reset IMM to factory defaults... vous permet de réinitialiser la configuration du module IMM2 avec les paramètres par défaut d'usine. Pour plus d'informations, voir «Réinitialisation du module IMM2 aux paramètres usine par défaut», à la page 90.<br><br>**Avertissement :** Lorsque vous cliquez sur **Reset IMM to factory defaults...**, toutes les modifications que vous avez effectuées sur le module IMM2 sont perdues. |
| | Activation Key Management | La page Activation Key Management page vous permet de gérer les clés d'activation des dispositifs en option Features on Demand (FoD) du serveur ou du module IMM2. Pour plus d'informations, voir «Clé de gestion de l'activation», à la page 91. |

# Chapitre 3. Présentation de l'interface utilisateur Web IMM2

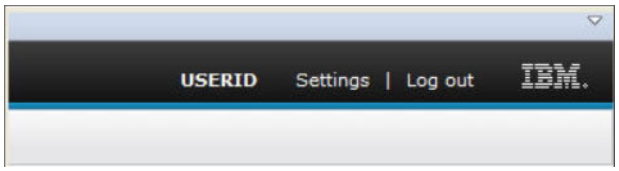
Ce chapitre présente les fonctions de l'interface utilisateur Web du module IMM2 et décrit leur mode d'utilisation.

**Important :** Cette section ne s'applique pas aux serveurs lame IBM et IBM BladeCenter. Bien que le module IMM2 soit installé en standard sur certains produits IBM BladeCenter et serveurs lame IBM, le module de gestion évolué IBM BladeCenter constitue le module de gestion principal pour les fonctions de gestion des systèmes. Les utilisateurs qui souhaitent configurer les paramètres IMM2 sur les serveurs blade doivent utiliser Advanced Settings Utility (ASU) sur le serveur blade pour effectuer ces actions.

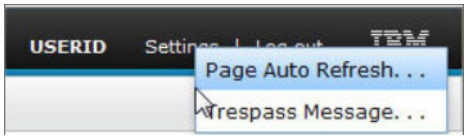
## Paramètres de session Web

Cette section fournit des informations sur les paramètres de la page principale de session d'interface Web.

La page principale IMM2 affiche les sélections de menu dans la partie supérieure droite de la page Web. Ces éléments de menu vous permettent de configurer le processus d'actualisation de la page Web ainsi que le message qui s'affiche lorsqu'un utilisateur saisit ses données d'identification pour se connecter. La figure suivante présente les sélections de menu situées dans la partie supérieure droite de la page Web.

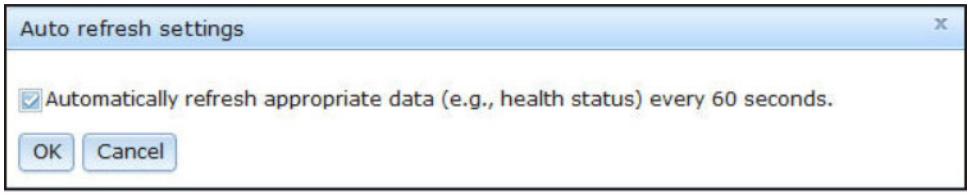



Cliquez sur l'élément **Settings** pour afficher les sélections de menu suivantes :




### Page auto refresh

Utilisez l'option **Page Auto Refresh** sous l'élément de menu Settings dans la partie supérieure droite de la page de session Web pour que le contenu de page soit automatiquement actualisé toutes les 60 secondes. Pour configurer l'actualisation du contenu de page toutes les 60 secondes, sélectionnez la case **Automatically refresh appropriate data...** et appuyez sur **OK**. Pour désactiver l'actualisation de page automatique, désélectionnez la case et appuyez sur **OK**. La figure suivante montre la fenêtre Auto refresh settings.




Certaines pages Web IMM2 sont automatiquement actualisées, même si la case d'actualisation automatique n'est pas sélectionnée. Les pages Web IMM2 qui sont automatiquement actualisées sont les suivantes :

- **System Status :**

  L'état du système et de l'alimentation est actualisé automatiquement toutes les trois secondes.
- **Server Power Actions** (sous l'onglet Server Management) **:**

  L'état d'alimentation est actualisé automatiquement toutes les trois secondes.
- **Remote Control** (sous l'onglet Server Management) **:**

  Les boutons Start remote control... sont actualisés automatiquement toutes les secondes. La table Session List est actualisée une fois toutes les 60 secondes.

**Remarques :**

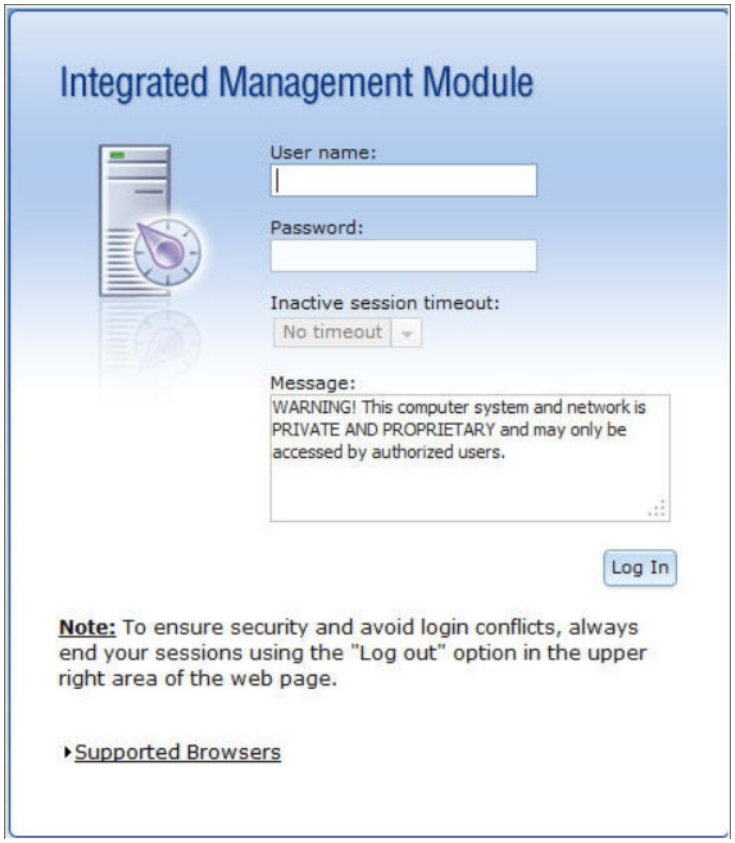
- Si vous accédez depuis votre navigateur Web à une page Web qui s'actualise de façon automatique, votre session Web ne sera pas automatiquement terminée par le délai d'attente d'inactivité.
- Si vous envoyez une requête à un utilisateur distant au moyen de la page d'option Remote Control située sous Server Management, votre session Web n'expirera pas, peu importe la nature de la page Web vers laquelle vous naviguez, tant qu'une réponse n'aura pas été reçue de l'utilisateur distant ou tant que la session de l'utilisateur distant n'aura pas expiré. Lorsque le traitement de la requête de l'utilisateur distant se termine, la fonction du délai d'attente d'inactivité reprend.

  **Remarque :** La remarque précédente s'applique à toutes les pages Web.
- Le microprogramme IMM2 prend en charge jusqu'à six sessions Web simultanées. Pour libérer une session au profit d'un autre utilisateur, déconnectez-vous de la session Web dès vous avez fini, au lieu d'attendre que le délai d'attente d'inactivité ferme votre session. Si vous laissez votre navigateur ouvert sur une page Web IMM2 qui s'actualise automatiquement, votre session Web ne se fermera pas automatiquement pour cause d'inactivité.

## Trespass message

Utilisez l'option **Trespass Message** sous l'élément de menu Settings dans la partie supérieure droite de la page de session Web pour configurer le message devant s'afficher lorsqu'un utilisateur se connecte au serveur IMM2. L'écran suivant s'affiche lorsque vous sélectionnez l'option Trespass Message. Entrez le texte du message que vous souhaitez voir s'afficher dans la zone fournie et appuyez sur **OK**.

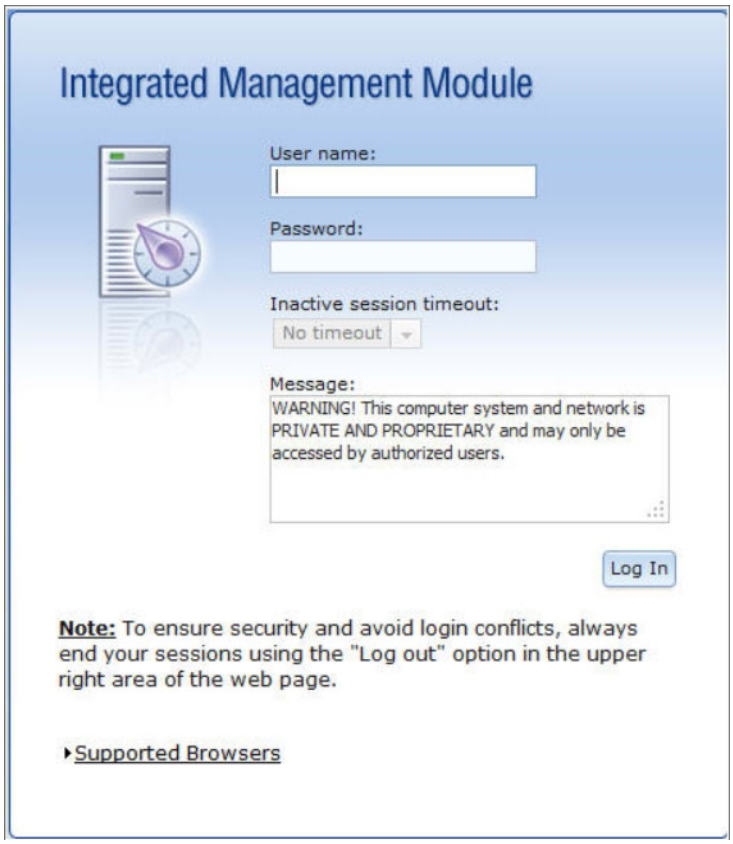

Le texte du message s'affichera dans la zone Message de la page de connexion du module IMM2 à chaque connexion d'utilisateur, comme représenté dans la figure suivante.




## Déconnexion

Pour des raisons de sécurité, déconnectez-vous de la session Web IMM2 lorsque vous avez terminé et fermez manuellement toutes les fenêtres du navigateur Web IMM2 ouvertes.

Pour vous déconnecter de la session Web, cliquez sur **Log out** dans la partie supérieure droite de la page Web. La figure Login s'affiche.

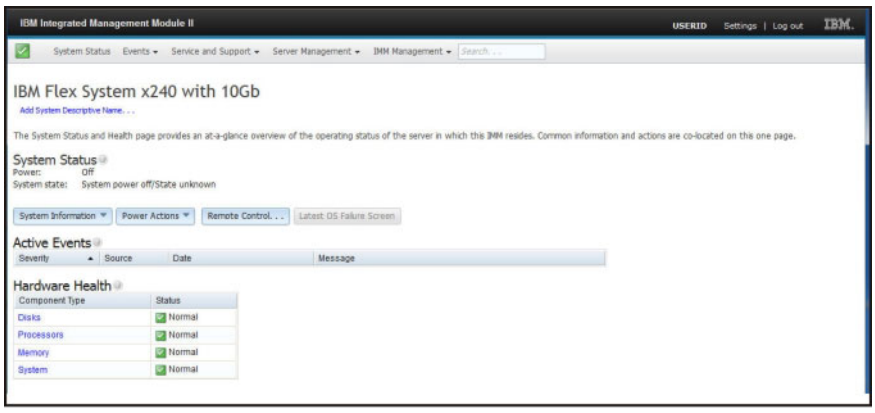



**Remarque :** Le microprogramme IMM2 prend en charge jusqu'à six sessions Web simultanées. Pour libérer une session au profit d'un autre utilisateur, déconnectez-vous de la session Web dès vous avez fini, au lieu d'attendre que le délai d'attente d'inactivité ferme votre session. Si vous laissez votre navigateur ouvert sur une page Web IMM2 qui s'actualise automatiquement, votre session Web ne se fermera pas automatiquement pour cause d'inactivité.

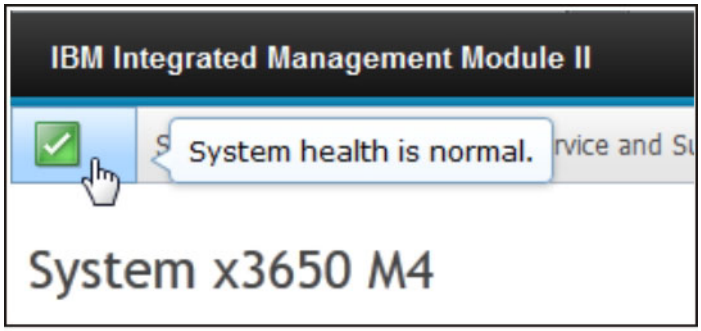
## Onglet System Status

Cette section fournit des informations sur les options de l'onglet System Status dans l'interface utilisateur Web du module IMM2.

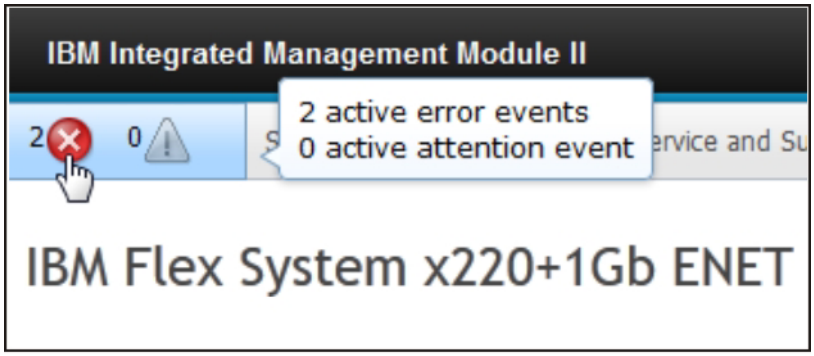
La page System Status s'affiche après vous être connecté à l'interface utilisateur Web du module IMM2 ou lorsque vous cliquez sur l'onglet System Status. Dans la page System Status, vous pouvez afficher l'état du système, les événements actifs du système et des informations sur l'état de santé du matériel. La fenêtre ci-après s'affiche lorsque vous cliquez sur l'onglet System Status ou lorsque vous vous connectez à l'interface web IMM2.



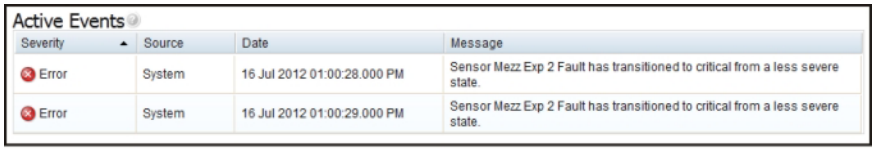

Vous pouvez cliquer sur l'icône verte (avec la coche) dans le coin supérieur gauche de la page pour obtenir un résumé rapide de l'état du serveur. Une coche indique que le serveur fonctionne normalement.



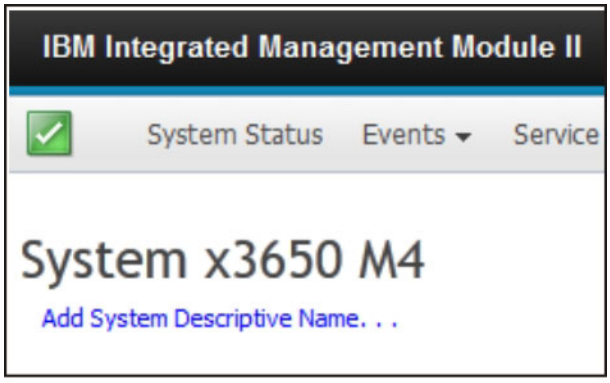

L'affichage d'un cercle rouge ou d'un triangle jaune indique la présence d'une erreur ou d'un avertissement (comme illustré ci-après).



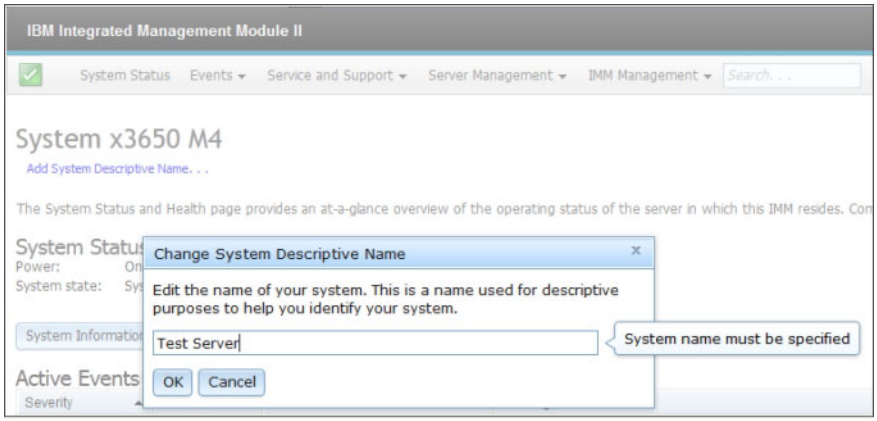

Le cercle rouge indique un cas d'erreur sur le serveur. Un triangle jaune indique une condition d'avertissement. Lorsqu'un cercle rouge ou un triangle jaune s'affiche, les événements associés à cette condition sont répertoriés dans la section Active Events de la page System Status, comme indiqué dans la figure suivante.



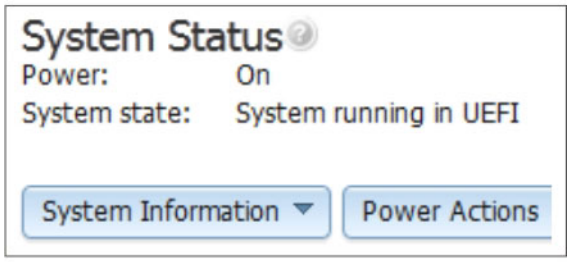

Vous pouvez ajouter un nom descriptif au serveur IMM2 pour mieux distinguer les différents serveurs IMM2. Pour affecter un nom descriptif au serveur IMM2, cliquez sur le lien **Add System Descriptive Name...** situé en-dessous du nom de produit du serveur.




Lorsque vous cliquez sur le lien **Add System Descriptive Name...**, la fenêtre suivante s'affiche pour que vous puissiez spécifier un nom associé au serveur IMM2. Vous pouvez modifier le nom descriptif du système à tout moment.




La section **System Status** de la page System Status affiche l'état d'alimentation et l'état de fonctionnement du serveur. L'état qui s'affiche correspond à l'état du serveur au moment où la page System Status est ouverte (comme indiqué dans la figure suivante).



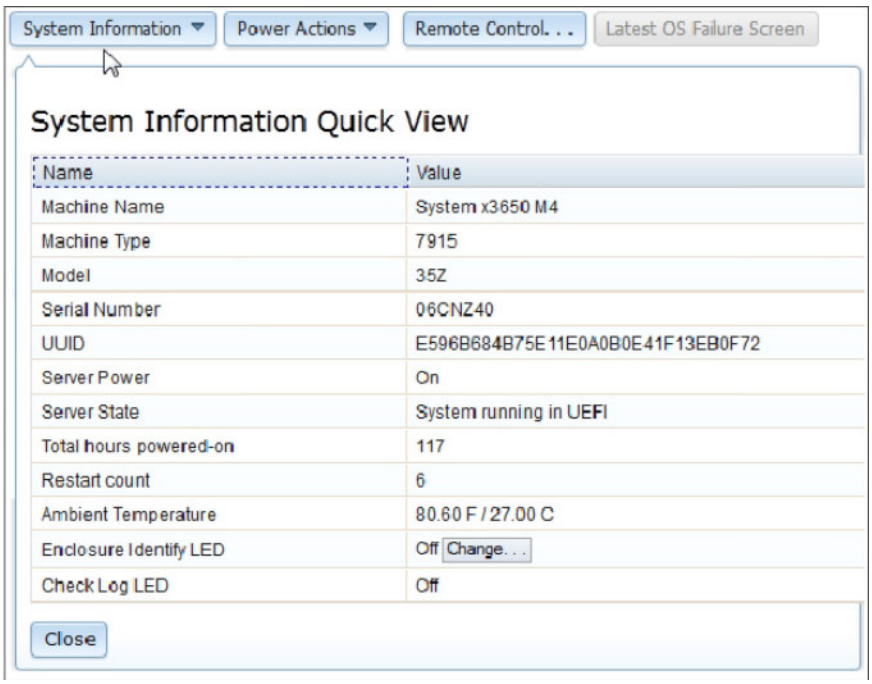

Le serveur peut se trouver dans l'un des états suivants :

*Tableau 2. Etats d'alimentation et de fonctionnement du serveur*

| **Etat du serveur** | **Description** |
|---|---|
| System power off/state unknown | Le serveur est hors tension. |
| System on/starting UEFI | Le serveur est sous tension mais UEFI n'est pas en cours d'exécution. |
| System running in UEFI | Le serveur est sous tension et UEFI est en cours d'exécution. |
| System stopped in UEFI | Le serveur est sous tension ; UEFI a détecté un problème et a été arrêté en cours d'exécution. |
| Booting OS or in unsupported OS | Le serveur peut se trouver dans cet état pour l'une des raisons suivantes :<br>• Le chargeur du système d'exploitation a démarré mais le système d'exploitation n'est pas encore en cours d'exécution.<br>• L'interface Ethernet via USB du module IMM2 est désactivée.<br>• Le système d'exploitation n'a pas chargé les pilotes prenant en charge l'interface Ethernet via USB. |
| OS booted | Le système d'exploitation du serveur est en cours d'exécution. |
| Suspend to RAM | Le serveur a été placé en mode de secours ou en mode veille. |

La page System Status contient également les onglets **System Information**, **Power Actions**, **Remote Control** et **Latest OS Failure Screen**.


Cliquez sur l'onglet **System Information** pour afficher les informations sur le serveur.

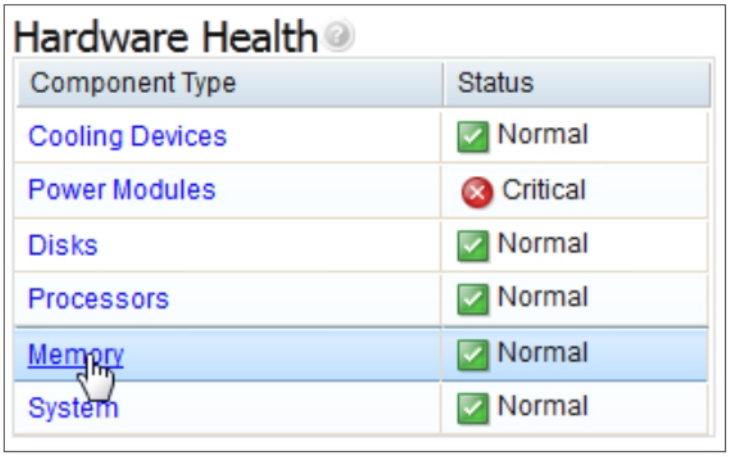



Cliquez sur l'onglet **Power Actions** pour afficher les actions vous permettant d'exercer un contrôle à distance total de l'alimentation de votre serveur, avec des actions de mise sous tension, de mise hors tension et de redémarrage. Pour plus de détails sur le contrôle à distance de l'alimentation du serveur, voir «Contrôle de l'état d'alimentation du serveur», à la page 102.

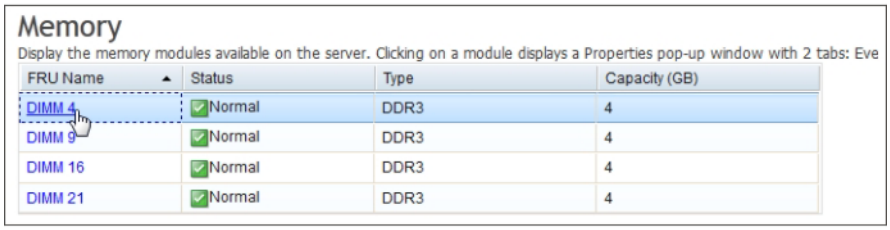
Cliquez sur l'onglet **Remote Control** pour obtenir des informations sur la façon dont vous pouvez contrôler le serveur au niveau du système d'exploitation. Pour plus de détails sur la fonction de contrôle à distance, voir «Fonctions d'intervention et de contrôle à distance», à la page 103.

Cliquez sur l'onglet **Latest OS Failure Screen** pour obtenir plus d'informations sur la façon de capturer les données du dernier écran d'erreur du système d'exploitation. Pour plus de détails sur l'onglet Latest OS Failure Screen, voir «Capture des données d'écran du dernier échec du système d'exploitation», à la page 130.

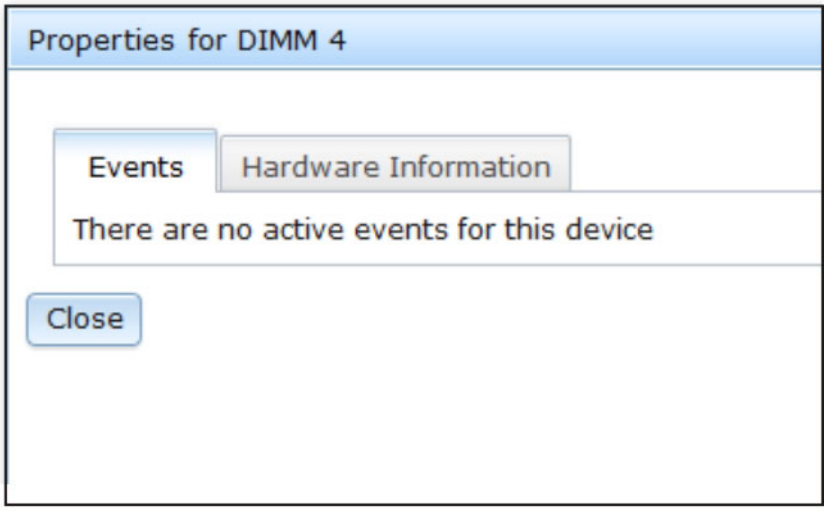
Sous la section **Hardware Health** de la page System Status, une table contient la liste des composants matériels sous surveillance et leur état de santé. L'état de santé affiché pour un composant peut refléter l'état le plus critique du composant dans la colonne Component Type de la table. Par exemple, un serveur peut avoir plusieurs modules d'alimentation installés et tous les modules fonctionnent normalement sauf un. L'état des composants Modules d'alimentation dans la table affichera un état critique en raison du module d'alimentation défaillant (comme indiqué dans l'écran suivant).



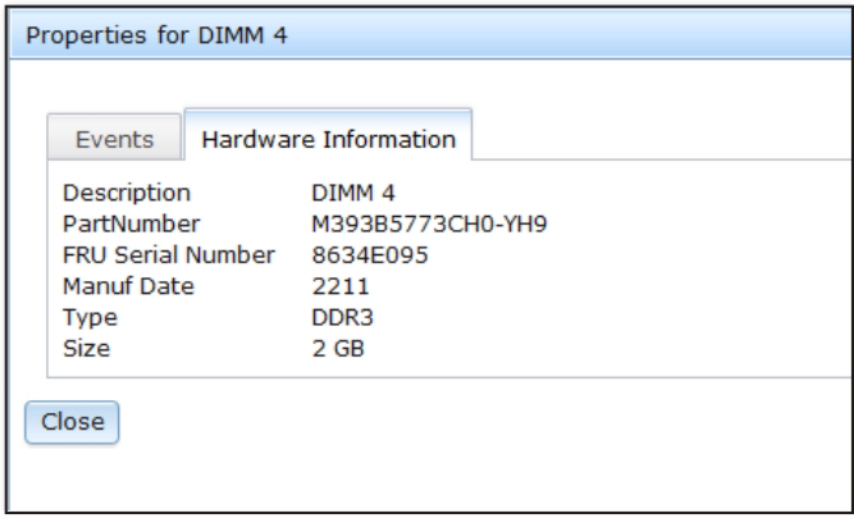

Chaque type de composant forme un lien sur lequel vous pouvez cliquer pour obtenir des informations plus détaillées. Lorsque vous cliquez sur le type de composant, une table affichant l'état de chacun des composants individuels s'affiche (comme indiqué dans l'écran suivant).




Vous pouvez cliquer sur un composant dans la colonne FRU Name de la table pour obtenir des informations supplémentaires sur ce composant. Tous les événements actifs du composant s'afficheront.



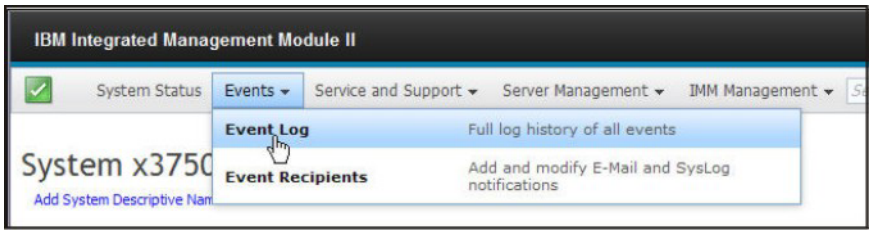
Cliquez sur l'onglet **Hardware Information** pour obtenir des informations détaillées sur le composant.




## Onglet Events

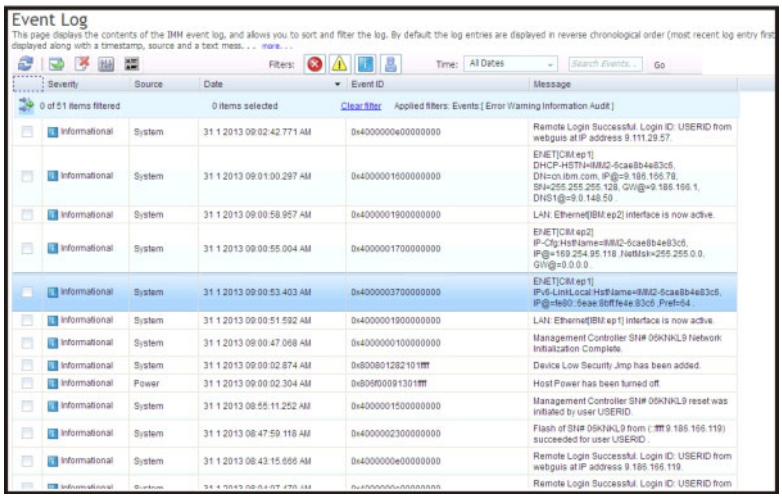
Cette section fournit des informations sur les options de l'onglet Events dans l'interface utilisateur Web du module IMM2.

Les options de l'onglet **Events** vous permettent de gérer l'historique du journal des événements et de gérer les destinataires des événements pour les notifications par courrier électronique et syslog. La figure suivante présente les options de l'onglet sur la page Web du module IMM2.

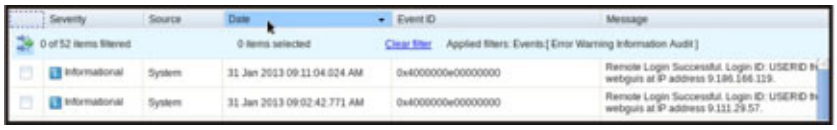



### Journal des événements

Sélectionnez **Event Log** dans l'onglet Events pour afficher la page Event Log. La page Event Log affiche la gravité des événements signalés par le module IMM2 ainsi que des informations sur les tentatives d'accès à distance et sur les modifications de configuration. Tous les événements recensés dans le journal sont accompagnés d'un horodatage qui utilise les paramètres de date et d'heure du module IMM2. Certains événements génèrent également des alertes s'ils sont configurés en conséquence sur la page Event Recipients. Vous pouvez trier et filtrer les événements dans le journal des événements. La figure suivante présente la page Event log.

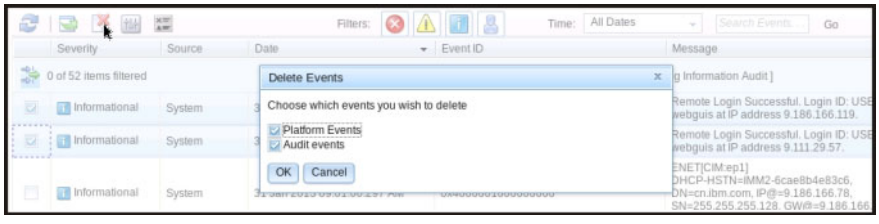



Pour trier et filtrer les événements dans le journal des événements, sélectionnez l'en-tête de colonne (comme illustré ci-après).



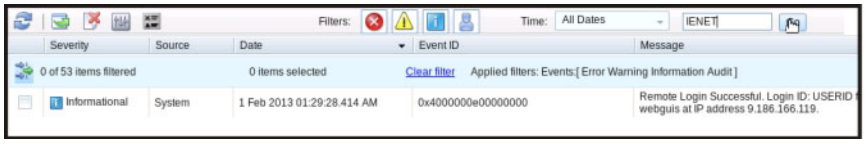

Vous pouvez sauvegarder dans un fichier une sélection d'événements ou tous les événements du journal des événements à l'aide du bouton **Export**. Pour sélectionner des événements spécifiques, sélectionnez un ou plusieurs événement sur la page principale Event Log et cliquez avec le bouton gauche de la souris sur le bouton **Export** (comme illustré ci-après).


Utilisez le bouton **Delete Events** pour sélectionner le type d'événements que vous souhaitez supprimer (comme illustré ci-après).

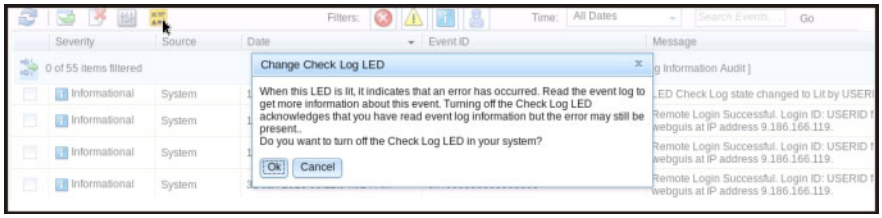


Pour sélectionner le type d'entrées que vous souhaitez afficher dans le journal des événements, cliquez sur le bouton approprié (comme illustré ci-après).

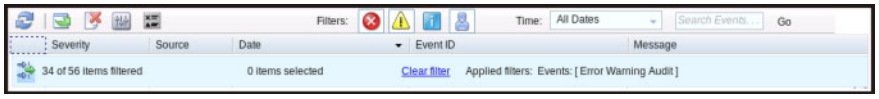

Pour rechercher un type d'événements ou de mots-clé défini, entrez le type d'événement ou mot-clé dans la case **Search Events**, puis cliquez sur **Go** (comme indiqué dans la figure suivante).




Pour éteindre le voyant Check Log alors que celui-ci est allumé et que les journaux d'événement associés sont sélectionnés, cliquez sur le bouton **Check Log LED Status** (comme illustré ci-après).

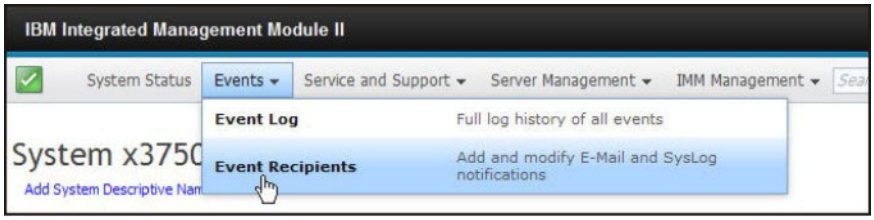



Dans la barre d'outils Event Log, vous pouvez cliquer sur l'un des boutons **Filter Events** pour les sélectionner les événements à afficher. Pour annuler le filtre et afficher tous les types d'événements, cliquez sur le lien **Clear Filter** (comme illustré ci-après).




## Destinataires des événements

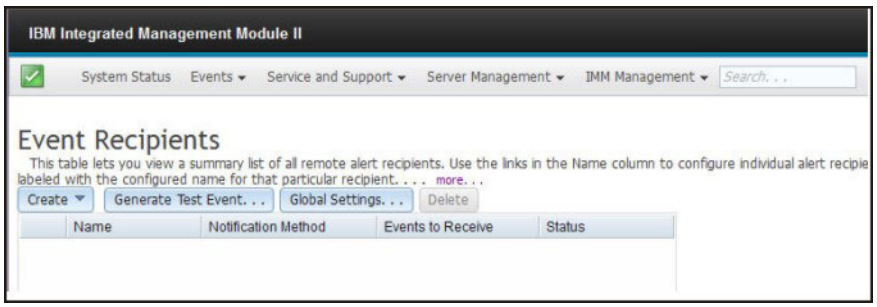
Utilisez l'option **Events Recipients** sous l'onglet Events pour ajouter ou modifier des notifications par courrier électronique et notifications syslog.



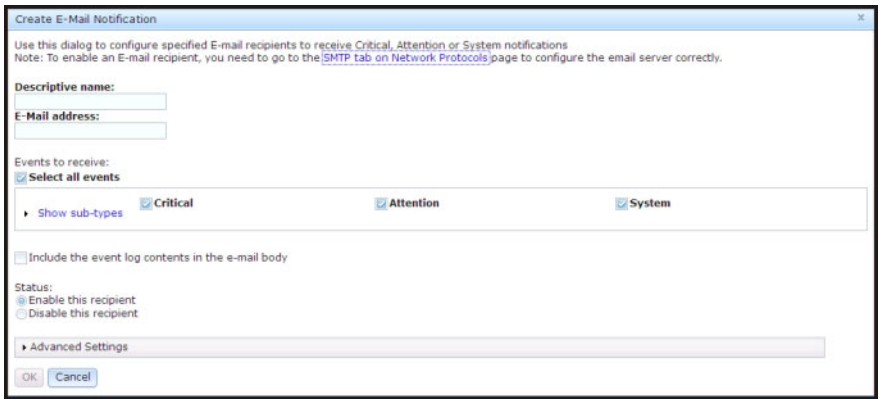

L'option Event Recipients vous permet de gérer les destinataires des notifications d'événements système. Vous pouvez configurer chaque destinataire et gérer les

paramètres applicables à tous les destinataires d'événements. Vous pouvez également générer un événement test afin de vérifier le fonctionnement du dispositif de notification.

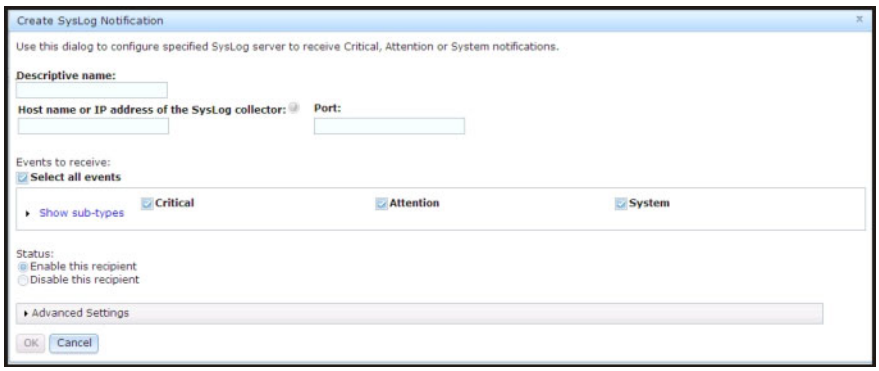
Cliquez sur le bouton **Create** pour créer des notifications par courrier électronique et notifications syslog.



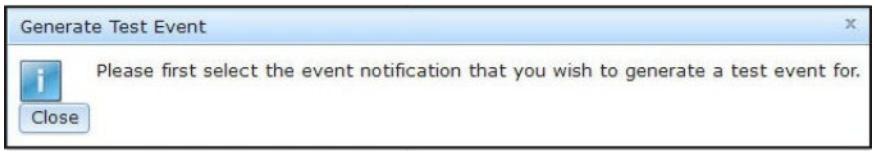

Sélectionnez l'option **Create E-mail Notification** pour configurer une adresse électronique cible et sélectionner le type d'événements pour lesquels vous souhaitez recevoir une notification. Vous pouvez également cliquer sur **Advanced Settings** pour sélectionner le numéro d'index de début. Pour inclure le journal des événements dans le courrier électronique, cochez la case **Include the event log contents in the e-mail body**. La fenêtre Create E-mail Notification est représentée ci-après.



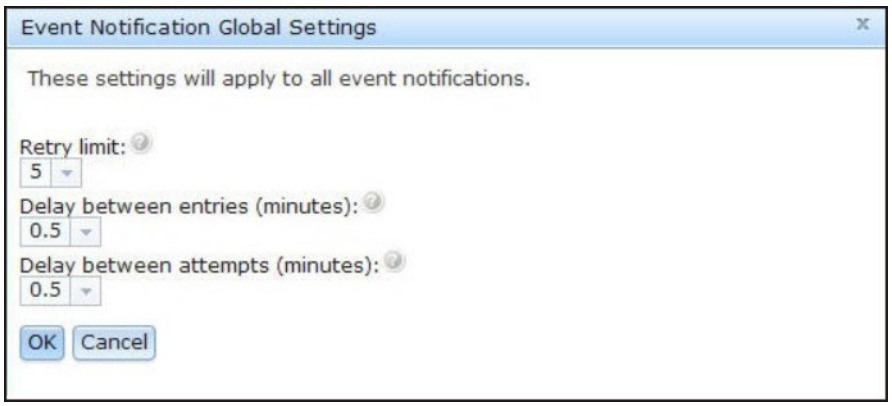

Sélectionnez l'option **Create SysLog Notification** pour configurer le nom d'hôte et l'adresse IP de la collecte SysLog et sélectionner le type d'événements pour lesquels vous souhaitez recevoir des notifications. Vous pouvez également cliquer sur **Advanced Settings** pour sélectionner le numéro d'index de début. Vous pouvez également spécifier le port que vous souhaitez utiliser pour ce type de notification. La fenêtre Create SysLog Notification est représentée ci-après.



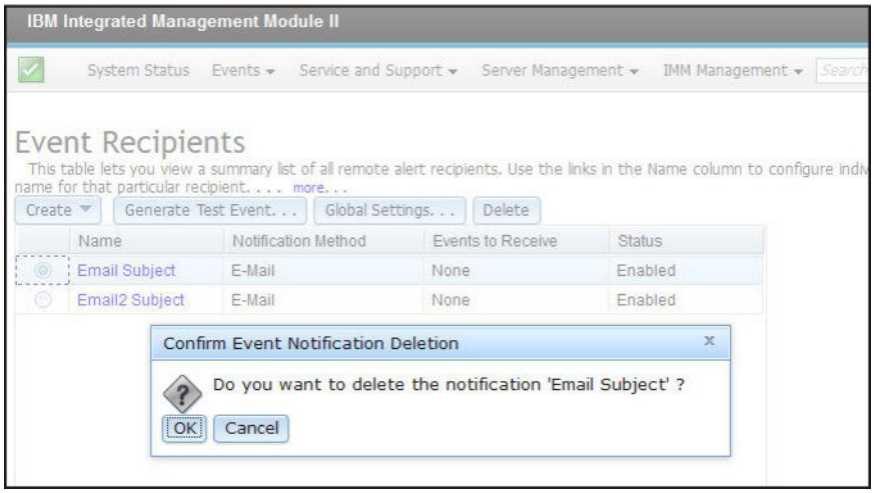

Sélectionnez le bouton **Generate Test Event** pour envoyer un courrier test à une adresse électronique cible sélectionnée (comme le montre la figure ci-après).




Sélectionnez le bouton **Global Settings** pour définir une limite pour la relance de notifications d'événements, le délai (en minutes) entre les entrées de notifications d'événements et le délai (en minutes) entre tentatives (comme le montre la figure suivante).




Si vous souhaitez supprimer une cible de notification par courrier électronique ou de notification syslog, sélectionnez le bouton **Delete**. La fenêtre suivante s'affiche.

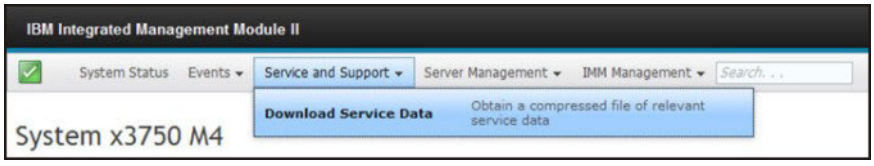



## Onglet Service and support

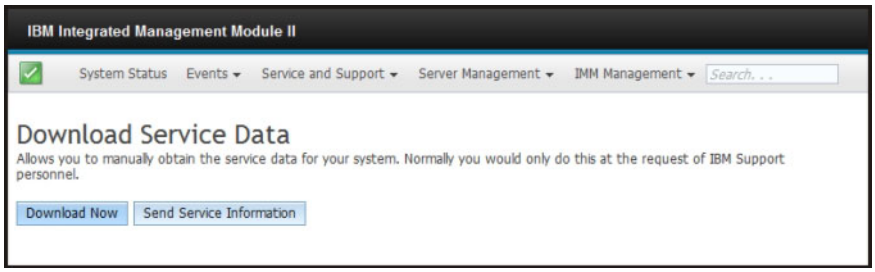
Cette section fournit des informations sur l'utilisation des options dans l'onglet Service et support sur la page de l'interface utilisateur Web IMM2.

### Téléchargement des données de service

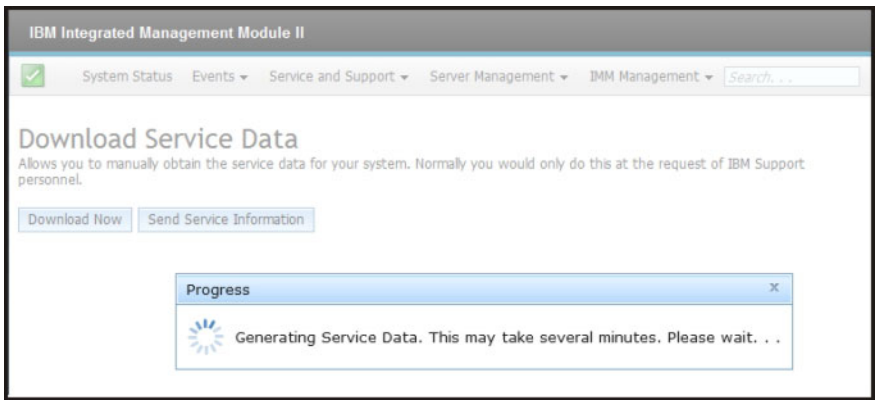
Utilisez l'option **Download Service Data** sous l'onglet Service and Support pour collecter des informations et créer un fichier compressé sur le serveur afin de l'envoyer par exemple au Support IBM pour aider à l'identification des incidents.



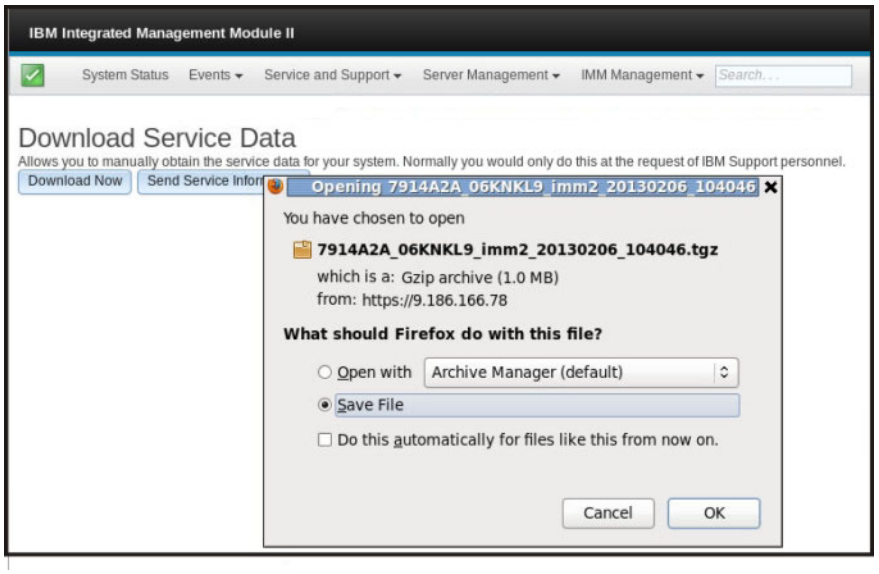

Cliquez sur le bouton **Download Now** pour télécharger les données de service et de support (comme indiqué dans la figure suivante).




Le processus de collecte de données commence. Le processus prend quelques minutes pour générer les données de service que vous pouvez ensuite enregistrer dans un fichier. Une fenêtre de progression s'affiche, indiquant que les données sont en train d'être générées.



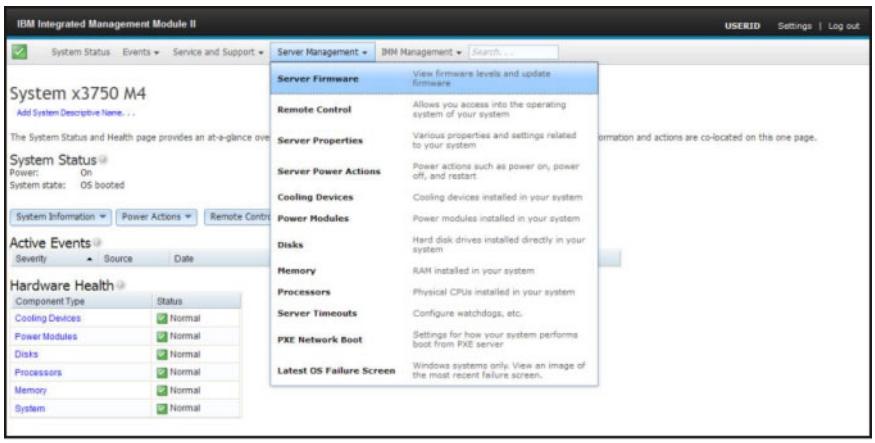

Lorsque le processus est terminé, la fenêtre suivante s'affiche et vous invite à indiquer l'emplacement où vous souhaitez sauvegarder le fichier généré.




## Onglet Server management

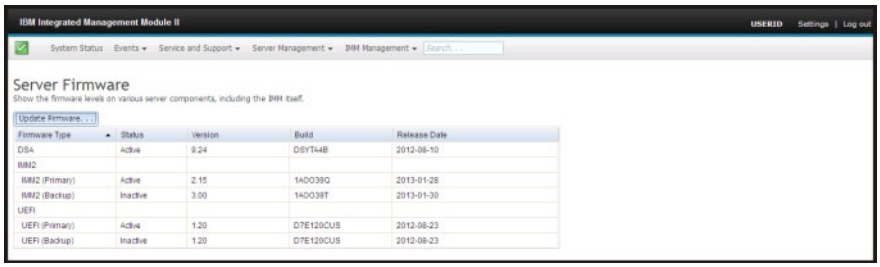
Cette section fournit des informations sur les options situées sous l'onglet Server Management de la page d'accueil de l'interface utilisateur Web IMM2.

Les options de l'onglet Server Management vous permettent d'afficher des informations sur l'état et le contrôle du microprogramme serveur, l'accès au contrôle à distance, le contrôle et l'état des propriétés serveur, les actions d'alimentation du serveur, dispositifs de refroidissement, modules d'alimentation, disques, mémoires, processeurs, délais d'attente du serveur, ainsi que sur le démarrage du réseau PXE et l'écran du dernier échec du système d'exploitation (comme illustré ci-après).




## Microprogramme de serveur

Sélectionnez l'option **Server Firmware** sous l'onglet Server Management pour afficher les niveaux des microprogrammes installés sur le serveur et appliquer les mises à jour des microprogrammes. L'illustration suivante présente les niveaux de microprogramme de serveur et vous permet de mettre à jour le microprogramme DSA, IMM2 et UEFI.



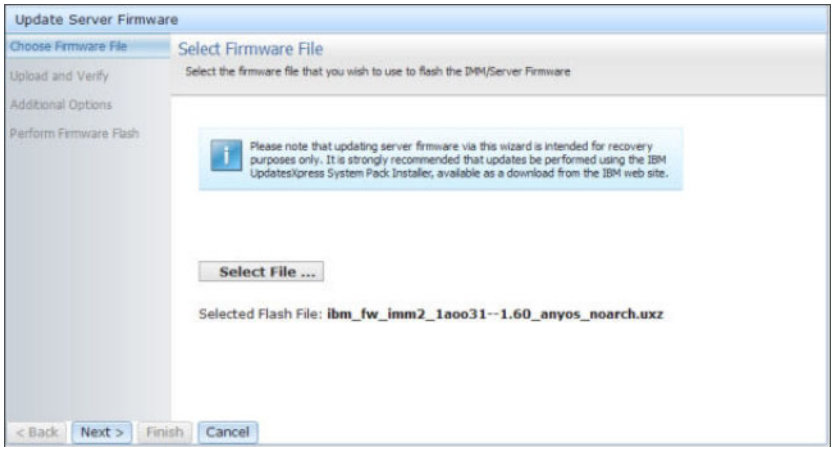

Le statut et les versions en cours des microprogrammes IMM2, UEFI, et DSA sont affichés, y compris les versions principale et de sauvegarde. Il existe trois catégories de statut de microprogramme :

- **Active :** le microprogramme est actif.
- **Inactive :** le microprogramme est inactif.
- **Pending :** le microprogramme est en instance de devenir actif.

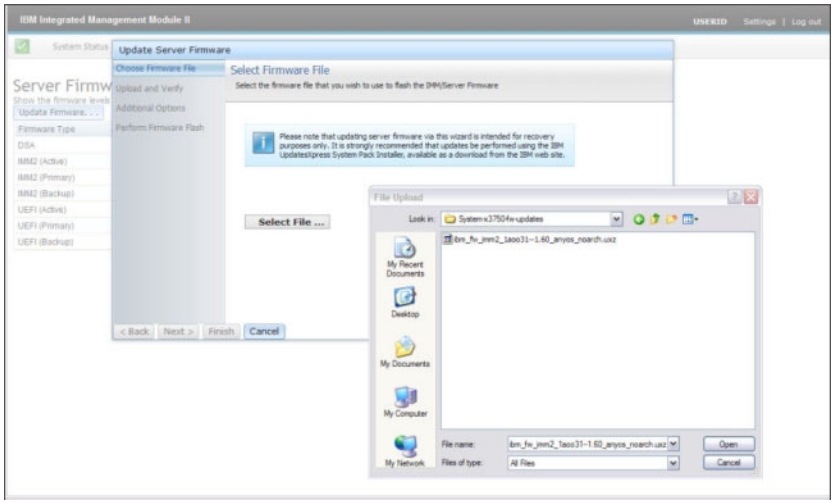
**Attention :** L'installation d'une mise à jour de microprogramme erronée peut entraîner une dysfonctionnement du serveur. Avant d'installer une mise à jour de microprogramme ou de pilote de périphérique, lisez les éventuels fichiers readme et historiques de modification qui sont fournis avec la mise à jour téléchargée. Ces fichiers contiennent des informations importantes concernant la mise à jour et la procédure d'installation de cette mise à jour, y compris toute procédure spéciale pour une mise à jour à partir d'une version antérieure de microprogramme ou de pilote de périphérique vers la version actuelle.

Pour mettre à jour le microprogramme, sélectionnez le bouton **Update Firmware...**. La fenêtre Update Server Firmware s'affiche. Vous pouvez cliquer sur **Cancel** et revenir à la fenêtre Server Firmware précédente ou cliquer sur le bouton **Select File...** afin de sélectionner le fichier microprogramme à utiliser pour copier instantanément le microprogramme de serveur.

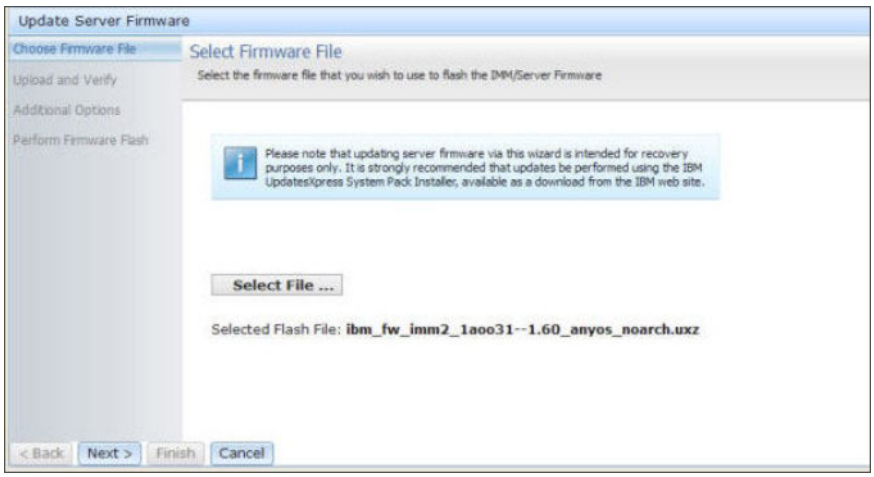
**Remarque :** Avant de cliquer sur le bouton **Select File...**, lisez l'avertissement affiché dans l'invite de fenêtre avant de continuer.



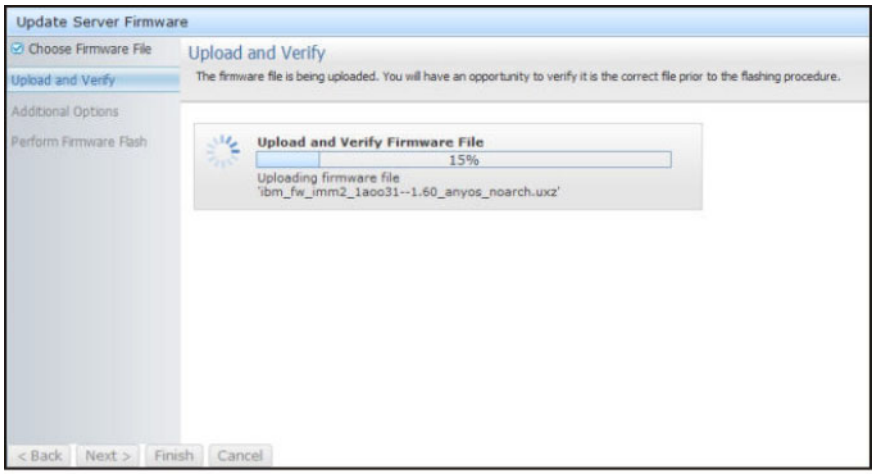

Lorsque vous cliquez sur le bouton **Select File...**, la fenêtre File Upload s'affiche, dans laquelle vous pouvez rechercher le fichier de votre choix.



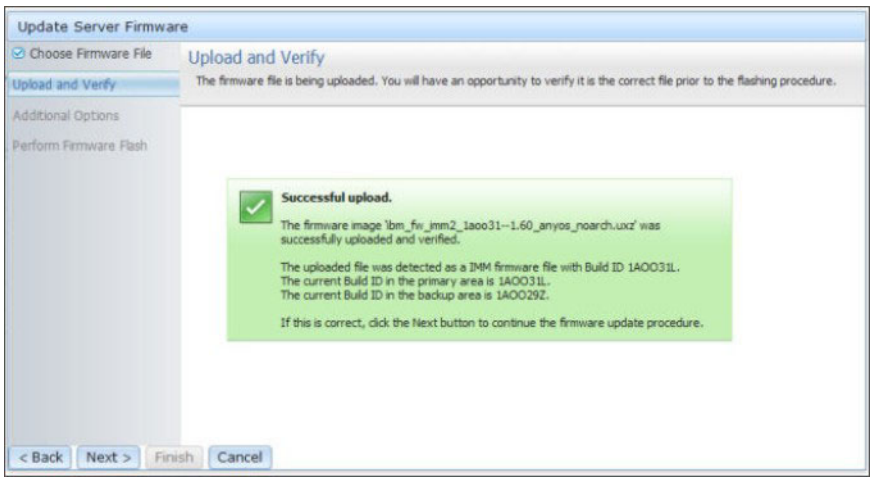

Une fois que vous avez accédé au fichier que vous souhaitez sélectionner, cliquez sur le bouton **Open**. Vous retournez alors à la fenêtre Update Server Firmware avec le fichier choisi affiché (comme illustré ci-après).



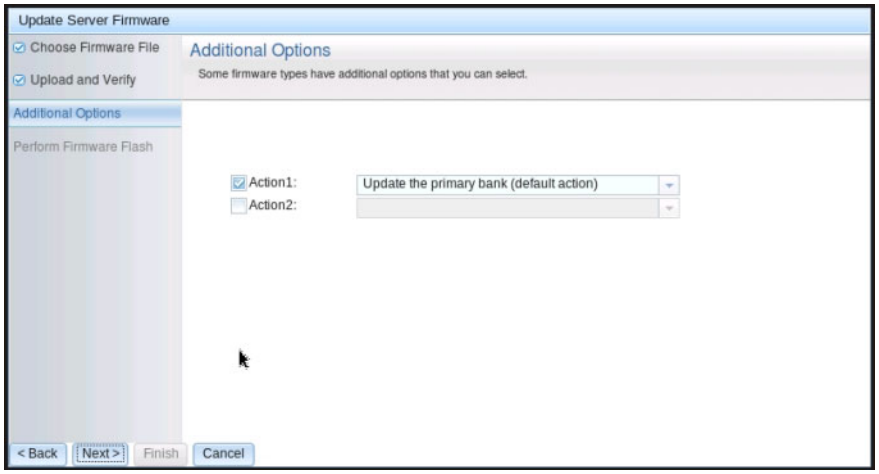

Clquez sur le bouton **Next >** pour commencer le processus de téléchargement et de vérification sur le fichier sélectionné (comme illustré ci-après). Une barre de progression s'affiche pendant toute la durée du téléchargement et de la vérification du fichier.



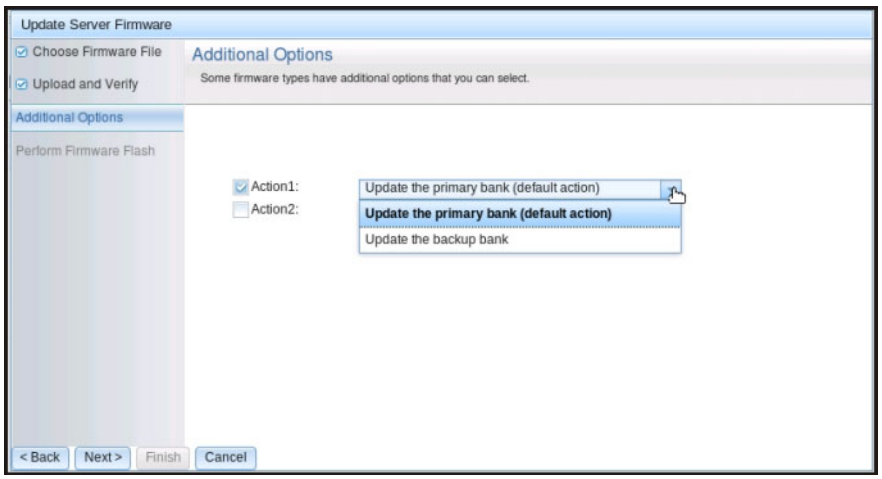

Une fenêtre d'état s'affiche (comme illustré ci-après) pour vous permettre de vérifier que le fichier que vous avez sélectionné pour la mise à jour est bien le fichier correct. La fenêtre contiendra des informations sur le type de fichier de microprogramme devant être mis à jour, tel que DSA, IMM2 ou UEFI. Si les informations sont correctes, cliquez sur le bouton **Next >**. Si vous souhaitez modifier l'une des sélections, cliquez sur le bouton **< Back**.




Lorsque vous cliquez sur le bouton Next >, un ensemble d'options supplémentaires s'affiche, comme illustré ci-après.



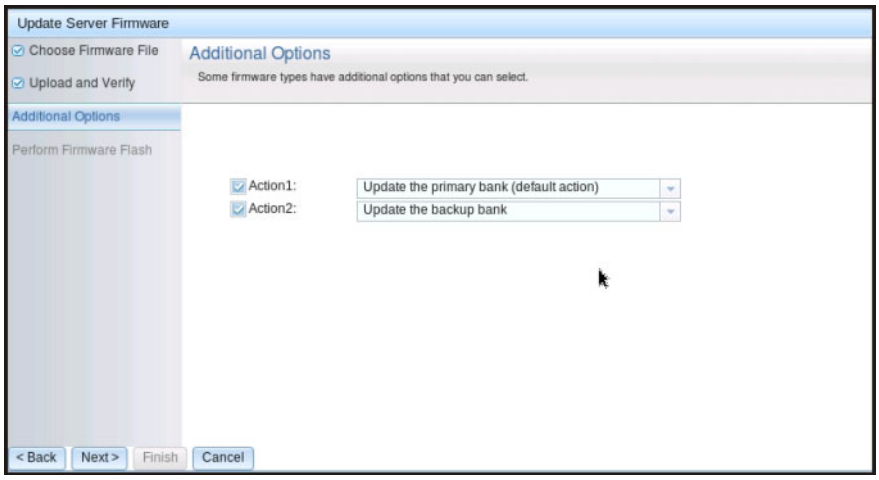

Le menu déroulant situé en regard de **Action 1** (illustré ci-après) vous donne le choix entre **Update the primary bank (default action)** ou **Update the backup bank**.



Après avoir sélectionné une action, vous retournez à la fenêtre précédente pour autoriser des actions supplémentaires en sélectionnant la case à cocher **Action 2**.

Lorsque l'action est chargée, l'action sélectionnée s'affiche ainsi qu'un nouveau menu déroulant **Action 2** (comme illustré ci-après).

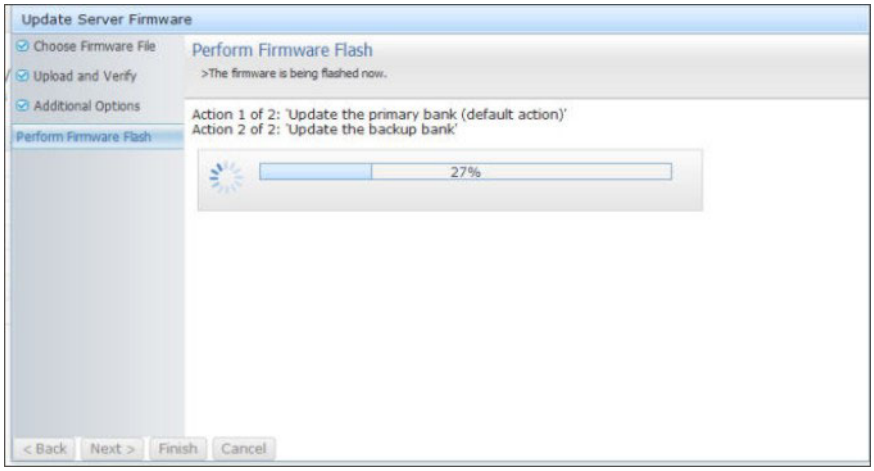
**Remarque :** Pour désactiver une action, cliquez sur la case à cocher en regard de l'action concernée.



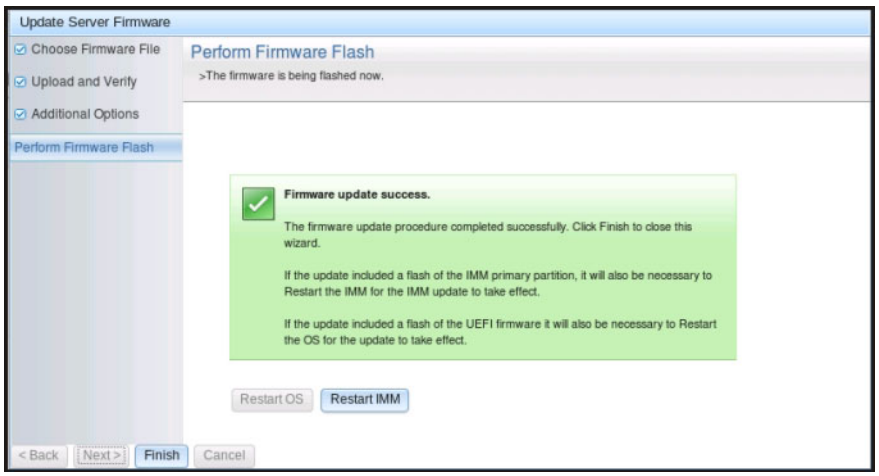

L'écran précédent montre que pour l'Action 1, la banque principale a été sélectionnée pour être mise à jour. Vous pouvez également sélectionner la mise à jour de la banque de sauvegarde sous Action 2 (comme le montre la fenêtre précédente). La banque principale et la banque de sauvegarde sont mises à jour en même temps lorsque vous cliquez sur **Next >**.

**Remarque :** L'Action 1 doit être différente de l'Action 2.

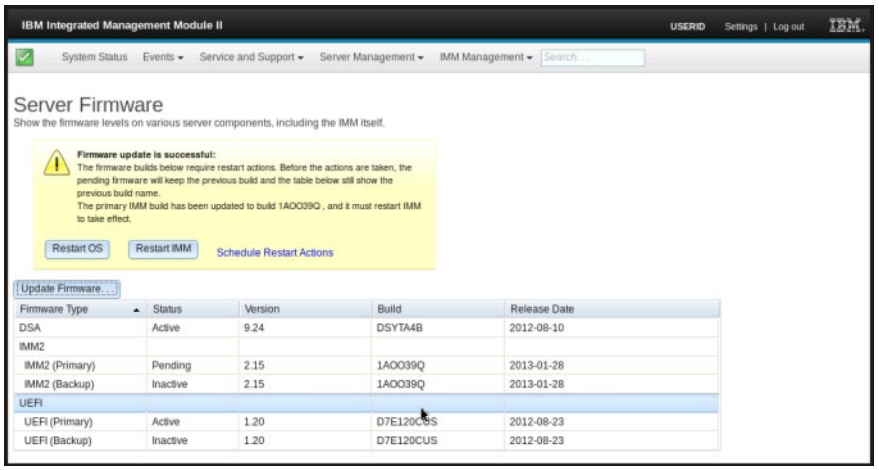
Une barre de progression affiche la progression de la mise à jour du microprogramme (comme illustré ci-après).




Lorsque la mise à jour du microprogramme se termine correctement, la fenêtre ci-après s'affiche. Sélectionnez l'opération associée en fonction du contenu affiché afin de terminer le processus de mise à jour.




Si la mise à jour de microprogramme principal n'a pas abouti, la fenêtre ci-après s'affiche.




## Contrôle à distance

Cette section fournit des informations sur la fonction de contrôle à distance.

Le client ActiveX et le client Java sont des consoles graphiques distantes qui permettent d'afficher à distance l'écran vidéo du serveur et d'interagir avec lui à l'aide du clavier et de la souris client.

**Remarques :**

- Le client ActiveX est uniquement disponible avec le navigateur Internet Explorer.
- Pour utiliser le client, le plug-in Java 1.5 ou version ultérieure est requis.
- Le client Java est compatible avec IBM Java 6 SR9 FP2 ou version ultérieure.

La fonction de contrôle à distance se compose de deux fenêtres séparées :

- **Video Viewer**

  La fenêtre Video Viewer utilise une console distante pour la gestion des systèmes distants. Une console distante est un affichage interactif de l'interface graphique utilisateur (GUI) du serveur, visible sur votre ordinateur. Votre moniteur affiche exactement ce qui apparaît sur la console du serveur et vous pouvez contrôler la console via le clavier et la souris.

- **Virtual Media Session**

  La fenêtre Virtual Media Session répertorie toutes les unités sur le client pouvant être mappées en tant qu'unités distantes et permet de mapper les fichiers d'image 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. La fenêtre Virtual Media Session s'ouvre depuis la barre de menu Tools de la fenêtre Video Viewer.

  **Remarques :**

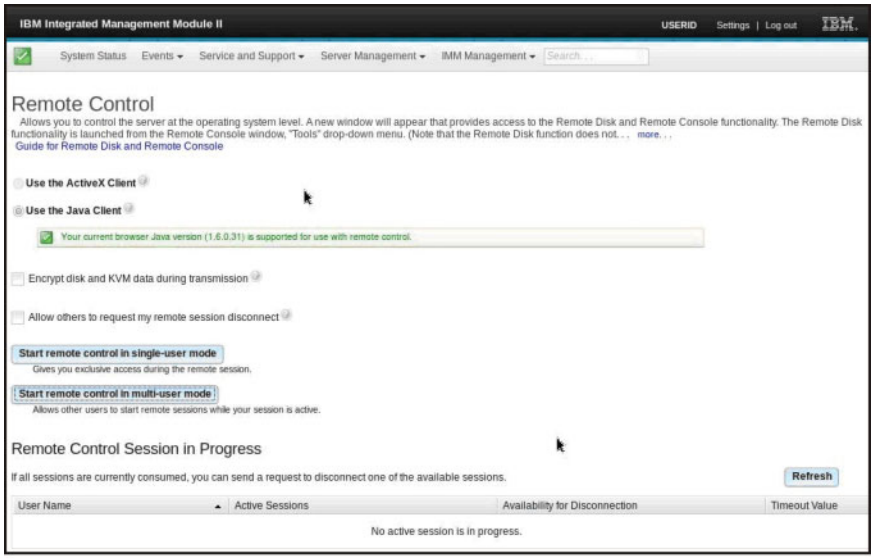
  – La fenêtre Virtual Media Session ne peut être utilisée que par un client de session de contrôle à distance à la fois.

  – Si le client ActiveX est utilisé, une fenêtre parent s'ouvre et cette fenêtre doit rester ouverte jusqu'à ce que la session à distance se termine.

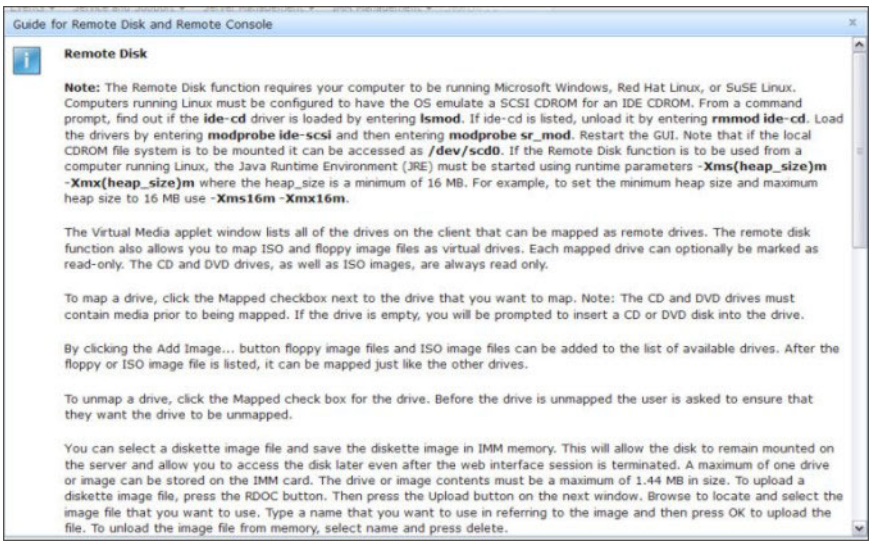
Pour accéder à distance à une console serveur, procédez comme suit.

1. Connectez-vous au module IMM2 (pour plus d'informations, voir «Connexion au module IMM2», à la page 10).
2. Accédez à la page Remote Control en sélectionnant l'une des options de menu suivantes :
   - Cliquez sur **Remote Control** dans l'onglet Server Management.
   - Cliquez sur **Remote Control...** dans la page System Status.

   La page Remote Control s'ouvre comme illustré dans la figure suivante.

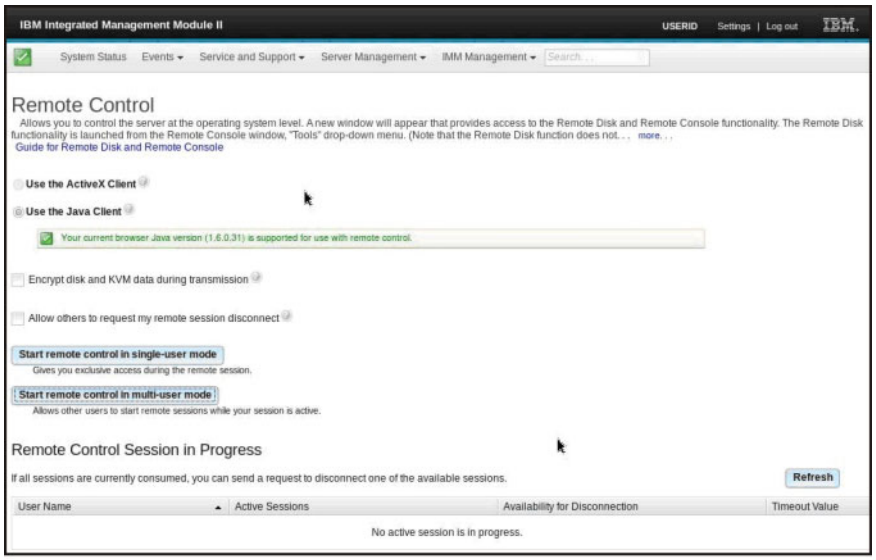



3. Vous pouvez cliquer sur le lien **Guide for Remote Disk and Remote Console** pour obtenir des informations supplémentaires. La figure suivante représente la fenêtre Guide for Remote Disk and Remote Console.




a. Cliquez sur **Close** pour quitter la fenêtre Guide for Remote Disk and Remote Console.

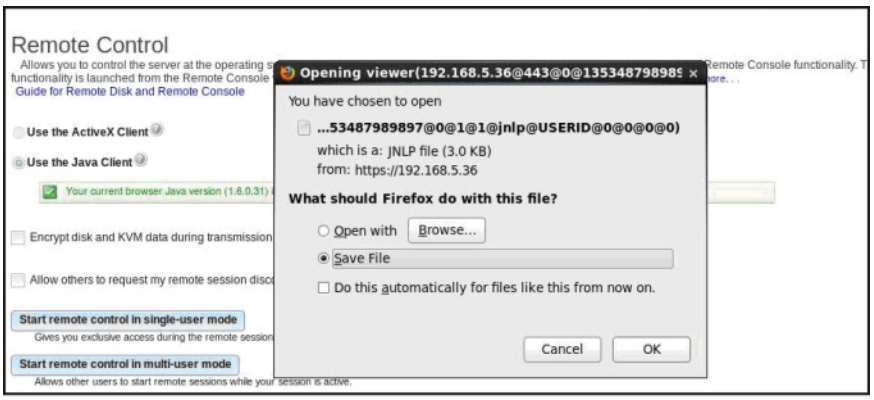
4. Sélectionnez l'une des options de console graphique distante suivantes :
   - Pour utiliser Internet Explorer comme navigateur, sélectionnez **Use the ActiveX Client**.
   - Pour utiliser le client Java, sélectionnez **Use the Java Client**, comme représenté dans la figure suivante.




**Remarques :**

- Si vous n'utilisez pas le navigateur Internet Explorer, seul le client Java peut être sélectionné.
- Les clients ActiveX et Java ont une fonctionnalité identique.
- Une ligne d'état s'affiche, indiquant si votre client est pris en charge.

La fenêtre suivante s'ouvre. Elle affiche l'information que le navigateur (par exemple, le navigateur Firefox) utilisera pour ouvrir le fichier Viewer.

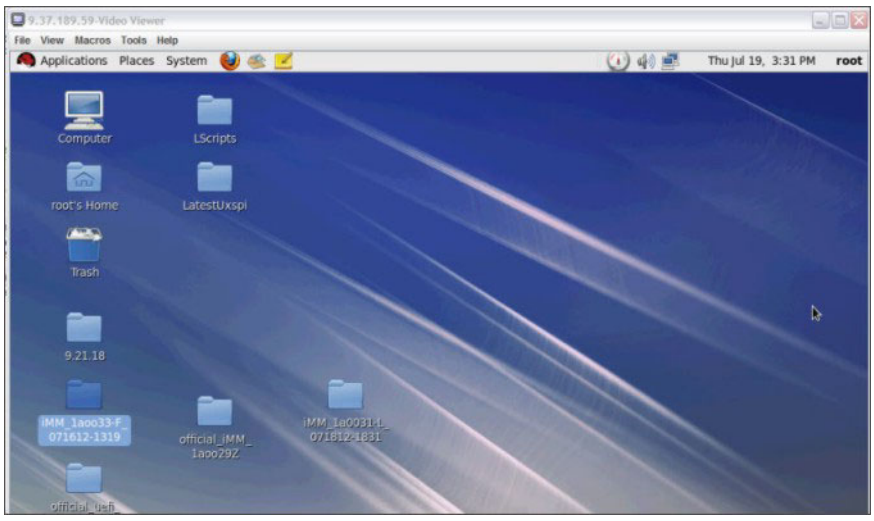



5. Une fois que le navigateur a téléchargé et ouvert le fichier Viewer, une fenêtre de confirmation s'ouvre et affiche un avertissement sur la vérification du certificat du site Web (comme représenté dans la figure suivante). Cliquez sur **Yes** pour accepter le certificat.


6. Pour contrôler le serveur à distance, sélectionnez l'une des options de menu suivantes :
   - Pour bénéficier d'un accès distant exclusif au cours de votre session, cliquez sur **Start remote control in single User mode**.
   - Pour autoriser d'autres utilisateurs à disposer d'un accès à la console distante durant votre session, cliquez sur **Start remote control in multi user mode**.

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

     La fenêtre Video Viewer s'ouvre (comme illustré ci-après).Cette fenêtre permet d'accéder à la fonctionnalité Remote Console.




7. Fermez les fenêtres Video Viewer et Virtual Media Session quand vous avez fini d'utiliser la fonction Remote Control.

**Remarques :**

- La fenêtre Video Viewer fermera automatiquement la fenêtre Virtual Media Session.
- Ne fermez *pas* la fenêtre Virtual Media Session si un disque distant est actuellement mappé. Voir «Disque distant», à la page 113 pour les instructions de fermeture et d'annulation du mappage d'un disque distant.
- Si vous rencontrez des problèmes avec le clavier ou la souris lorsque vous utilisez la fonction de contrôle à distance, consultez l'aide accessible depuis la page Remote Control dans l'interface Web.
- Si vous utilisez la console distante pour modifier des paramètres IMM2 dans l'utilitaire Setup, il se peut que le serveur redémarre le module IMM2. Vous perdrez dans ce cas la console distante et la session de connexion. Après un bref délai, vous pourrez vous reconnecter à IMM2 en ouvrant une nouvelle session, redémarrer la console distante et quitter l'utilitaire Setup.

**Important :** le module IMM2 utilise une applet Java ou une applet ActiveX pour exécuter la fonction d'intervention à distance. Lorsqu'IMM2 est mis à jour vers le niveau du microprogramme le plus récent, 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 IMM2, il se peut que l'applet Java utilisée par le serveur ne soit pas au niveau le plus récent.

Pour corriger ce problème, désactivez la mise en cache. La méthode utilisée dépend de la plateforme et de la version Java. Les étapes suivantes sont pour Oracle Java 1.5 sous Windows :

1. Cliquez sur **Démarrer → Paramètres → Panneau de configuration**.
2. Cliquez deux fois sur **Java Plug-in 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 :
   - Désélectionnez la case **Enable Caching** de sorte que la mise en cache Java soit toujours désactivée.

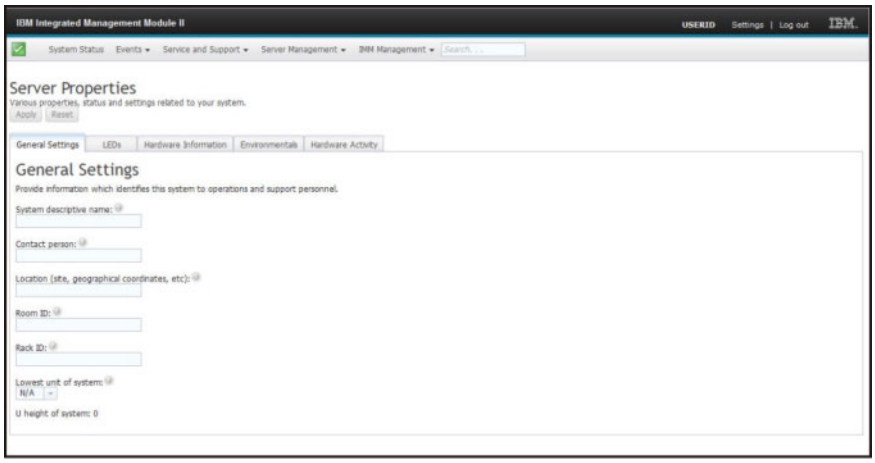
- Cliquez sur **Vider le cache**. Si vous sélectionnez cette option, vous devez cliquer sur **Clear Caching** après chaque mise à jour du microprogramme IMM2.

Pour plus d'informations sur la mise à jour du microprogramme IMM2, voir «Mise à jour du microprogramme de serveur», à la page 116.

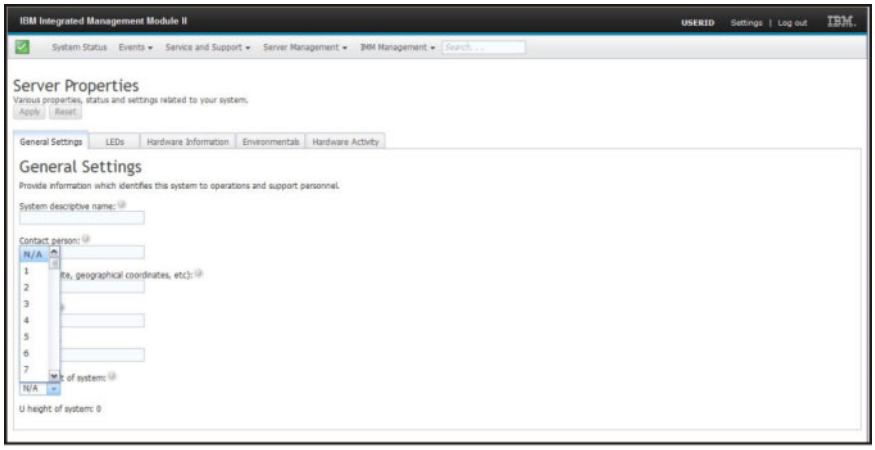
Pour plus d'informations sur la fonction de contrôle à distance, voir «Fonctions d'intervention et de contrôle à distance», à la page 103.

## Propriétés serveur

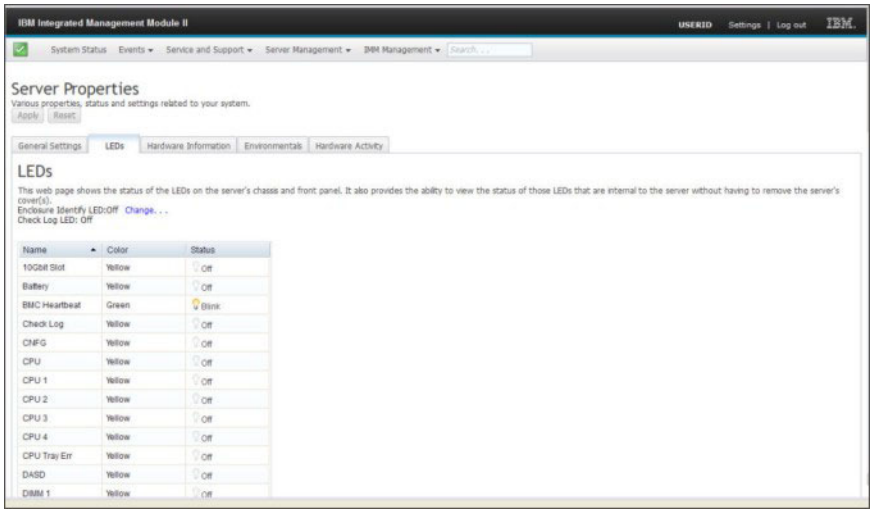
Sélectionnez l'option **Server Properties** sous l'onglet Server Management pour afficher la fenêtre suivante. Cette option vous permet de définir divers paramètres aidant à identifier le système. Cela inclut un nom descriptif, une personne à contacter, un lieu, etc. Les informations entrées dans ces zones prennent effet lorsque vous cliquez sur **Apply**. Pour supprimer les informations saisies dans les zones depuis les dernières modifications, cliquez sur **Reset**.



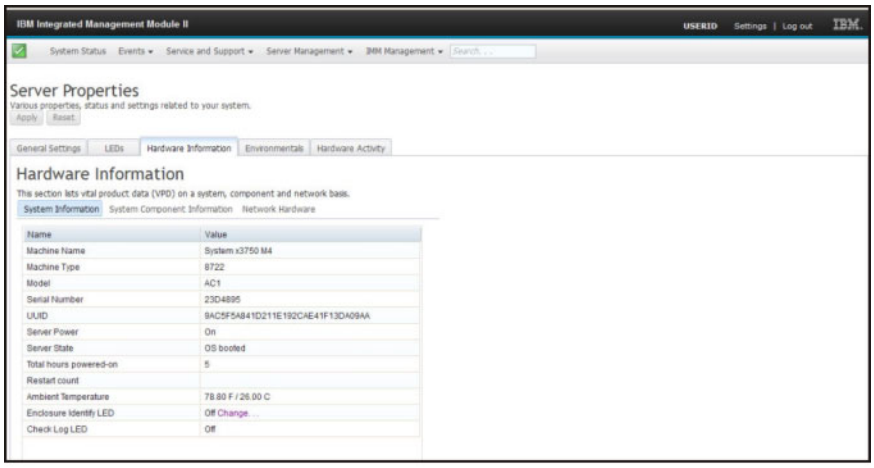

Dans l'illustration ci-après, vous pouvez indiquer quelle est la plus petite unité du système dans la zone **Lowest unit of the system**. La zone **Lowest unit of the system** requiert une connexion au module de gestion (par exemple le module Advanced Management Module ou CMM).



Pour afficher les voyants du système, cliquez sur l'onglet **LED**. La fenêtre suivante s'ouvre.

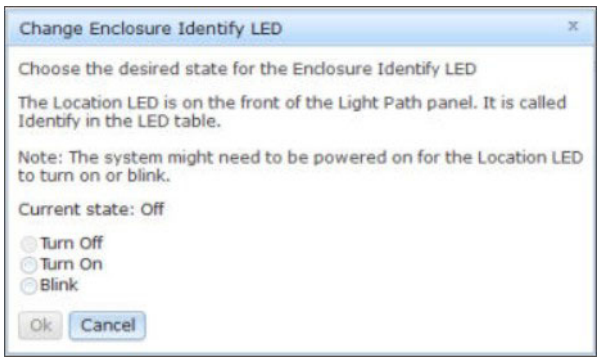



Pour afficher des informations sur le système, les composants du système et le matériel réseau, cliquez sur l'onglet **Hardware Information**. Sélectionnez l'onglet approprié sous l'onglet Hardware Information pour afficher diverses informations sur les données techniques essentielles. L'onglet **System Information** fournit des informations telles que le nom, le numéro de série et le modèle de la machine. La figure ci-après présente la fenêtre System Information.

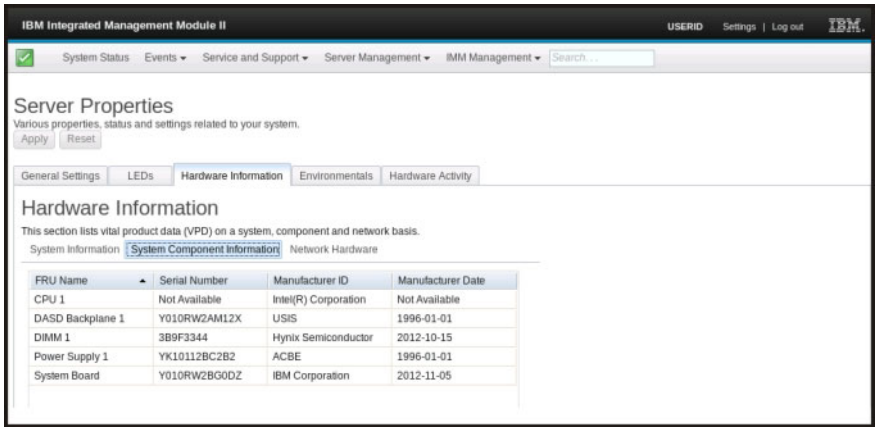



**Enclosure Identify LED** affiche l'état du voyant d'identification du boîtier et peut être modifié dans la fenêtre System Information. Pour modifier l'état de l'option **Enclosure Identify LED**, cliquez sur le lien **Change...**. La fenêtre suivante s'ouvre.

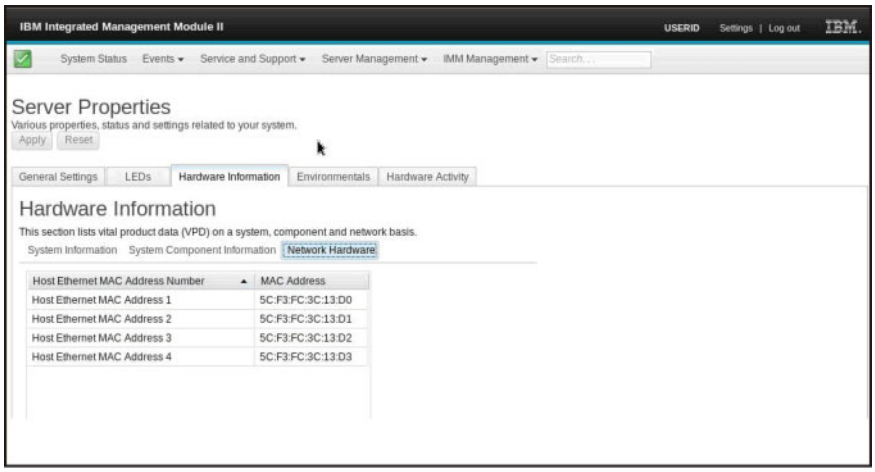
**Remarque :** Le voyant Enclosure Identity se trouve sur le devant du panneau Light Path.



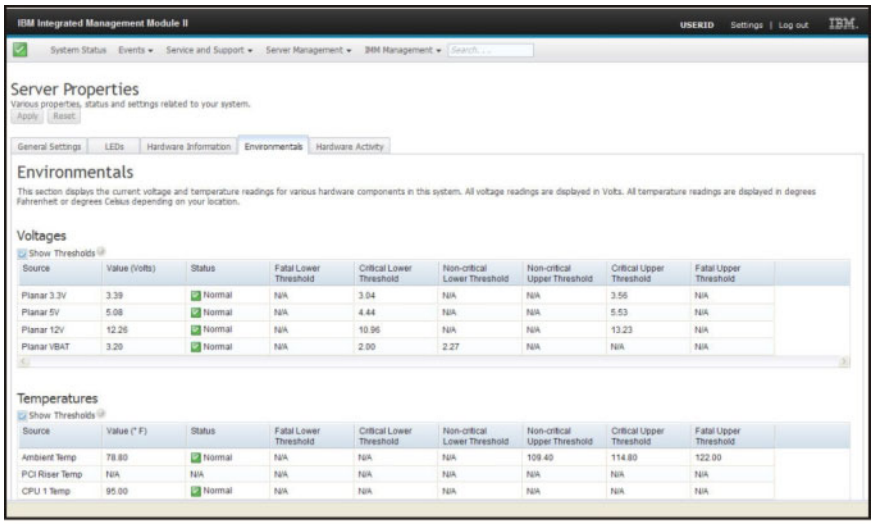

Sélectionnez l'onglet **System Component Information** pour afficher les informations sur les composants. Les informations sur les composants incluent le nom de l'unité remplaçable sur site (FRU), le numéro de série, l'ID du fabricant et la date de fabrication. La figure suivante affiche les informations que vous voyez lorsque vous cliquez sur l'onglet **System Component Information**.



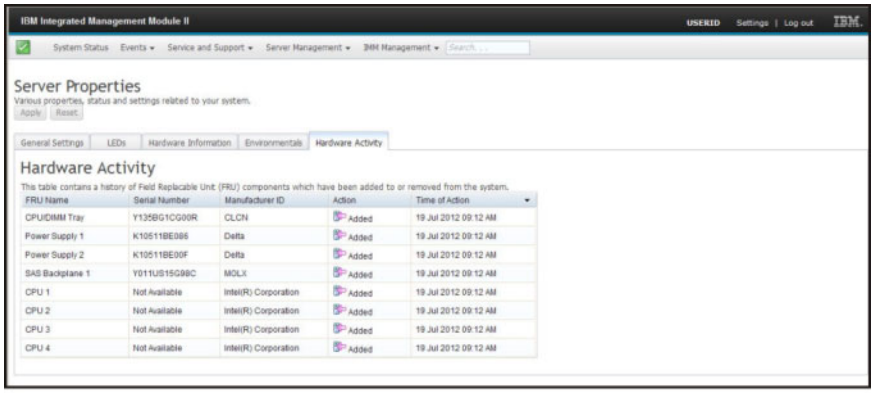

Sélectionnez l'onglet **Network Hardware** pour afficher les informations sur le matériel réseau. Les informations sur le matériel réseau incluent le numéro d'adresse MAC Ethernet hôte et l'adresse MAC. La figure suivante montre les informations qui s'affichent lorsque vous cliquez sur l'onglet Network Hardware.



Sélectionnez l'onglet **Environmentals** dans la page Server Properties pour afficher les tensions et températures des composants matériels du système. La fenêtre suivante s'ouvre. La colonne **Status** de la table indique si l'activité est normale ou s'il existe des zones à problème dans le serveur.



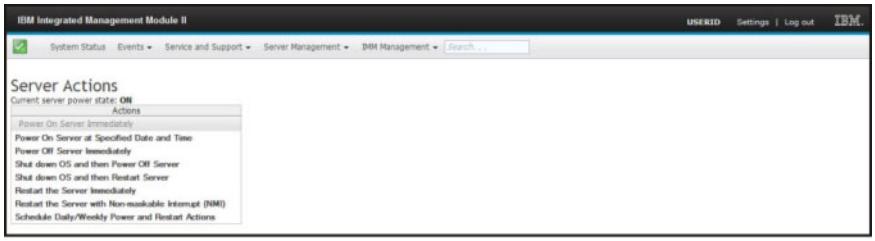

L'onglet **Hardware Activity** dans la page Server Properties fournit un historique du matériel ajouté ou supprimé dans le système. La figure suivante montre les informations qui s'affichent lorsque vous cliquez sur l'onglet Hardware Activity.




## Actions de contrôle de l'alimentation serveur

Cette section fournit des informations sur l'option Server Power Actions située sour l'onglet Server Management de la page d'accueil de l'interface Web IMM2.

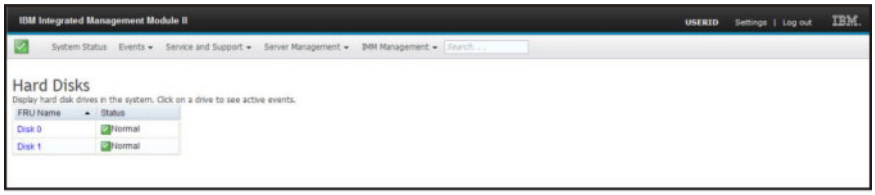
Sélectionnez l'option **Server Power Actions** sous l'onglet Server Management pour afficher une liste des actions que vous pouvez utiliser pour contrôler l'alimentation du système. La fenêtre Server Power Actions est représentée ci-après.




Vous pouvez choisir de mettre le serveur sous tension immédiatement ou à une heure planifiée. Vous pouvez également choisir d'arrêter et de redémarrer le système d'exploitation. Pour plus d'informations sur le contrôle de l'alimentation serveur, voir «Contrôle de l'état d'alimentation du serveur», à la page 102.

## Disques

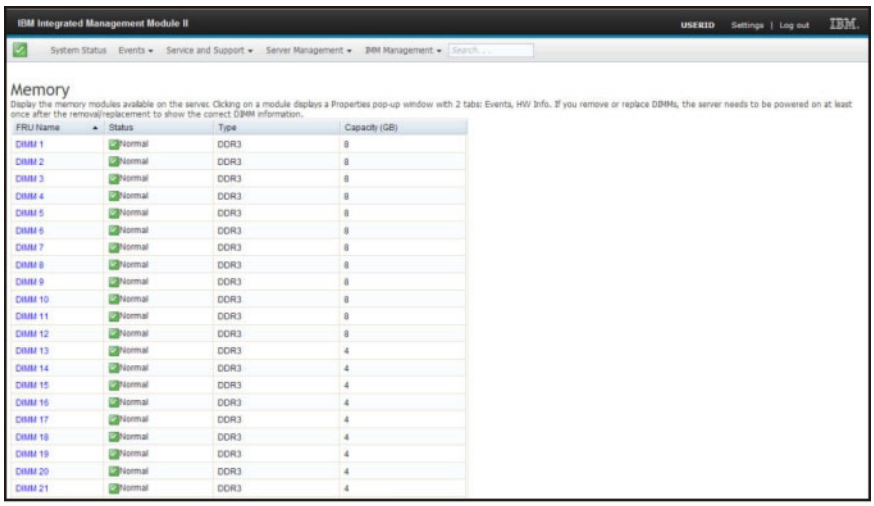
Sélectionnez l'option **Disks** dans l'onglet Server Management pour afficher les unités de disque dur sur le système. L'écran suivant s'affiche. Cliquez sur une unité de disque dur pour afficher les événements associés à l'unité de disque dur.



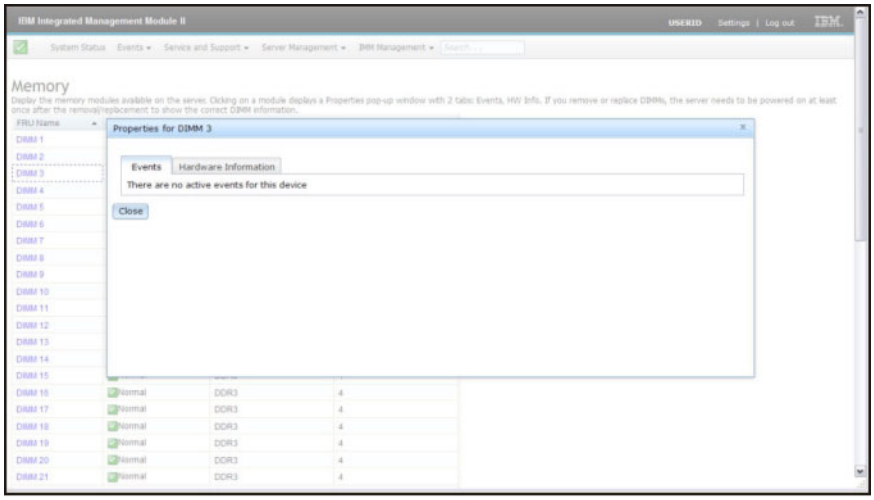

## Mémoire

Sélectionnez l'option **Memory** dans l'onglet Server Management pour afficher les informations sur les modules de mémoires installés sur le système. La fenêtre suivante s'ouvre. Chaque module de mémoire est affiché dans le tableau sous forme de lien que vous pouvez sélectionner pour obtenir des informations plus détaillées sur le module de mémoire. Le tableau affiche également l'état de la barrette DIMM, ainsi que son type et sa capacité.

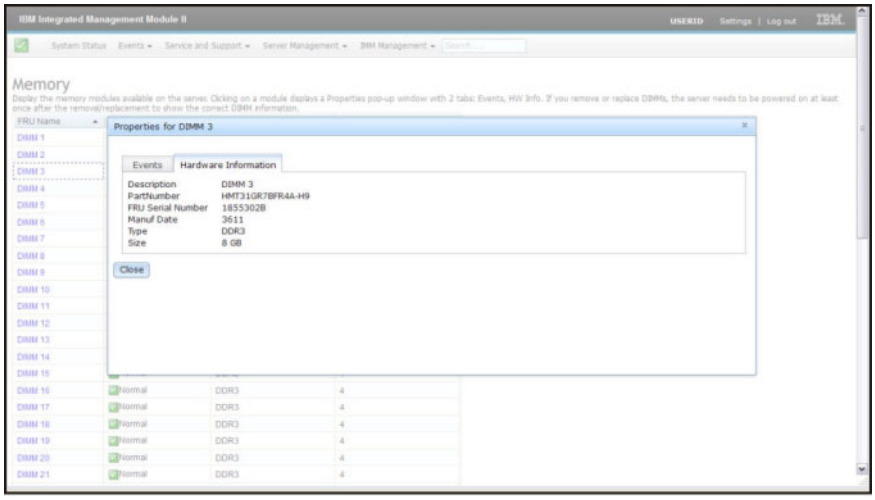
**Remarque :** Si vous supprimez ou remplacez une barrette DIMM, vous devez redémarrer le système pour afficher les informations mises à jour suite aux modifications effectuées sur les DIMM du système.




Cliquez sur un lien **DIMM** dans la table pour afficher tous les événements actifs ainsi que des informations supplémentaires sur le composant (comme illustré dans l'écran ci-après).

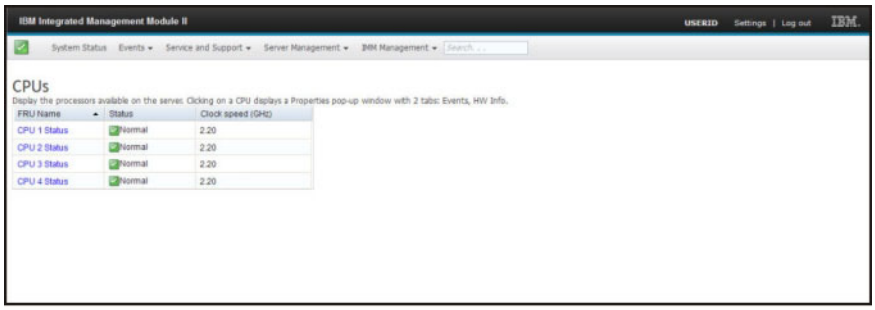



Cliquez sur l'onglet **Hardware Information** pour afficher les détails du composant, tels que la description, le numéro de composant, le numéro de série de l'unité remplaçable sur site (FRU), la date de fabrication (semaine/année), le type (par exemple, DDR3) et la taille en gigaoctets (comme illustré ci-après).

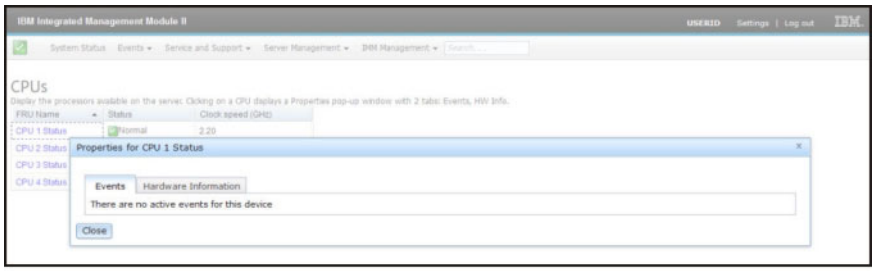



## Processeurs

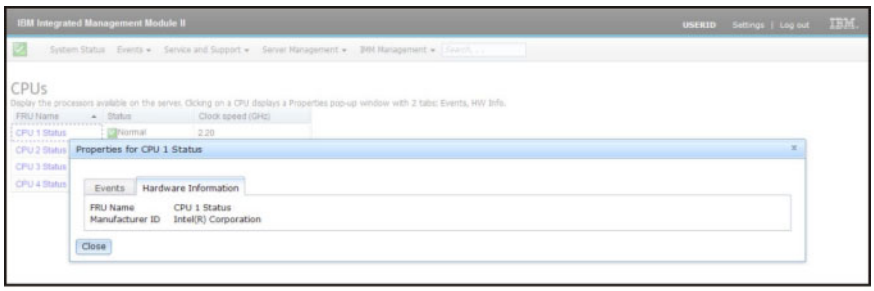
Sélectionnez l'option **Processors** dans l'onglet Server Management pour afficher des informations sur les microprocesseurs installés sur le système. La fenêtre suivante s'ouvre.




Cliquez sur un lien **CPU** dans la table pour afficher tous les événements actifs ainsi que des informations supplémentaires sur le composant (comme illustré ci-après).




Cliquez sur l'onglet **Hardware Information** pour afficher des détails sur le composant tels que le nom FRU et l'ID de fabricant (comme illustré ci-après).

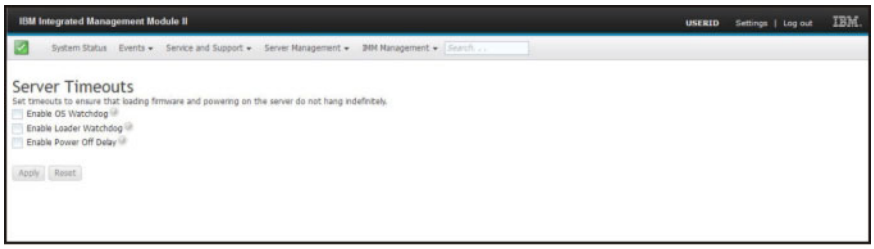



## Délais d'attente serveur

Sélectionnez l'option **Server Timeouts** sous l'onglet Server Management pour définir les délais d'attente afin d'éviter que le système ne se bloque indéfiniment lors d'une mise sous tension ou mise à jour de microprogramme sur le système. Vous pouvez activer cette fonction en définissant des valeurs pour ces options.

**Remarque :** Les délais d'attente de serveurs requièrent que l'interface USB intrabande (ou LAN via USB) soit activée pour utiliser des commandes. Pour plus d'informations sur la configuration de l'interface USB, voir «Configuration USB», à la page 80.

La figure suivante présente la fenêtre Server Timeouts.




Pour plus d'informations sur les délais d'attente de serveurs, voir «Configuration des délais d'attente du serveur», à la page 54.

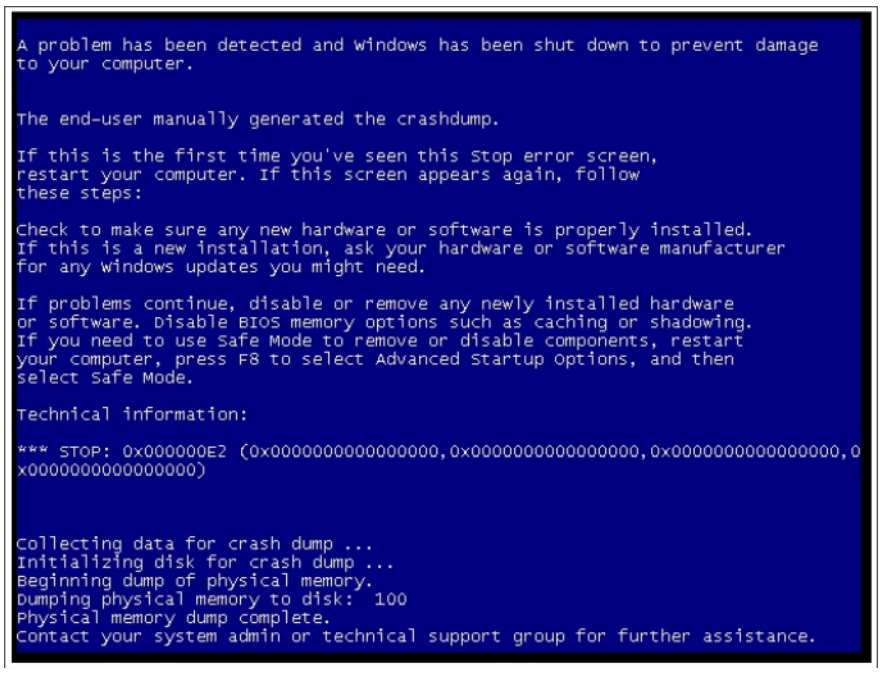
## Amorçage réseau PXE

Sélectionnez l'option **PXE Network Boot** dans l'onglet Server Management pour configurer votre serveur afin de tenter un amorçage réseau PXE au prochain redémarrage du serveur. Pour plus d'informations sur la configuration d'un amorçage réseau PXE, voir «Configuration de l'amorçage réseau PXE», à la page 115.

## Derniers échecs du système d'exploitation

Sélectionnez l'option **Latest OS Failure Screen** sous l'onglet Server Management pour afficher et supprimer les données d'écran des derniers échecs du système d'exploitation sauvegardées par le module IMM2. Le module IMM2 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.

La figure suivante offre un exemple d'écran d'échec du système d'exploitation.




Pour plus d'informations sur l'option Latest OS Failure Screen, voir «Capture des données d'écran du dernier échec du système d'exploitation», à la page 130.

## Onglet IMM Management

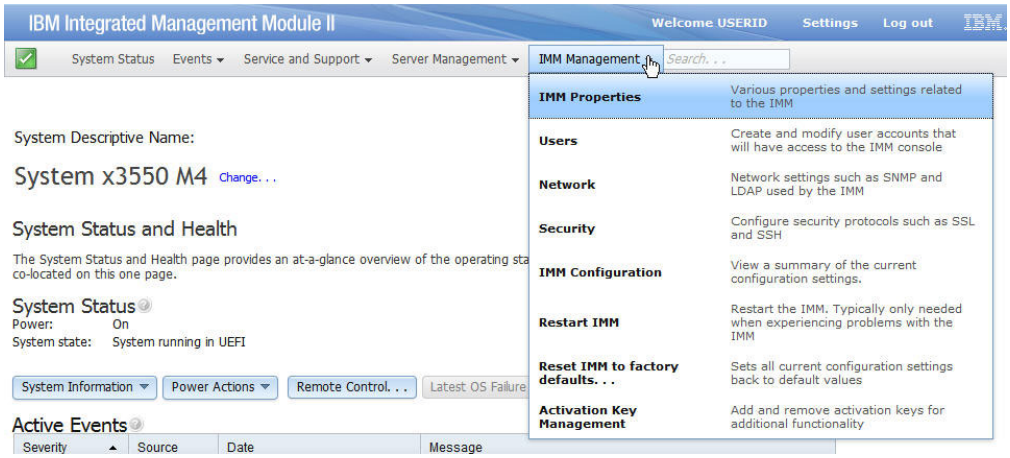
Cette section offre des informations sur les options de l'onglet IMM Management situé sur la page d'accueil de l'interface utilisateur Web IMM2.

Les options de l'onglet IMM Management vous permettent d'afficher et de modifier les paramètres IMM2. Pour obtenir une liste des options ainsi que des renseignements sur la façon dont les options peuvent être utilisées pour configurer le module IMM2, voir Chapitre 4, «Configuration du module IMM2», à la page 51.

# Chapitre 4. Configuration du module IMM2

L'onglet IMM Management contient les options de configuration du module IMM2. Utilisez l'onglet IMM Management pour afficher et modifier les paramètres du module IMM2. Les options suivantes sont répertoriées dans l'onglet IMM Management (comme illustré ci-après).

- IMM Properties
- Users
- Network
- Security
- IMM Configuration
- Restart IMM
- Reset IMM to factory defaults
- Activation Key Management




Dans la page Properties du module Integrated Management Module (IMM), vous pouvez réaliser les opérations suivantes :

- Accéder aux informations du microprogramme de serveur
- Définir la date et l'heure :
  - Sélectionner la méthode de réglage de l'heure IMM2 : manuelle ou NTP
  - Régler la date et l'heure du module IMM2 pour la méthode de réglage manuel
  - Définir l'information sur le protocole NTP pour la méthode de réglage NTP
  - Définir l'information sur le fuseau horaire du module IMM2
- Accéder à l'information sur le port série du module IMM2 :
  - Configurer le port série IMM2
  - Définir les séquences de touches de l'interface de ligne de commande du module IMM2

Dans la page User Accounts, vous pouvez réaliser les opérations suivantes :

- Gérer les comptes utilisateurs du module IMM2 :
  - Créer un compte utilisateur

  - Cliquer sur un nom d'utilisateur pour éditer les propriétés de cet utilisateur :
    - Editer un nom d'utilisateur
    - Définir un mot de passe utilisateur
    - Configurer les paramètres SNMPv3 pour l'utilisateur
    - Gérer les clés d'authentification publique Secure Shell (SSH) pour l'utilisateur
  - Supprimer un compte utilisateur
- Configurer les paramètres globaux de connexion d'utilisateur :
  - Définir la méthode d'authentification des utilisateurs
  - Définir le délai d'attente d'inactivité Web
  - Configurer les niveaux de sécurité de compte utilisateur disponibles pour le module IMM2
- Afficher les utilisateurs actuellement connectés au module IMM2

Dans la page Network Protocol Properties, vous pouvez réaliser les opérations suivantes :

- Configurer les paramètres Ethernet :
  - Paramètres Ethernet :
    - Nom d'hôte
    - Paramètres d'adresse et d'activation IPv4 et IPv6
  - Paramètres Ethernet avancés :
    - Activation de la négociation automatique
    - Gestion d'adresse MAC
    - Définir l'unité de transmission maximale
- Configurer les paramètres SNMP :
  - Configuration et activation de SNMPv1 :
    - Définir les informations de contact
    - Configuration et activation des alertes SNMP
    - Gestion de communautés
  - Configuration et activation de SNMPv3 :
    - Définir les informations de contact
    - Configuration des comptes utilisateurs
- Configurer les paramètres DNS :
  - Définir la préférence d'adressage DNS (IPv4 ou IPv6)
  - Configuration et activation d'adressage de serveur DNS supplémentaire
- Configurer les paramètres DDNS :
  - Activation DDNS
  - Sélectionner la source de nom de domaine (personnalisée ou serveur DHCP)
    - Définir le nom de domaine personnalisé pour une source personnalisée spécifiée manuellement
    - Afficher le nom de domaine spécifié par le serveur DHCP
- Configurer les paramètres SMTP :
  - Définir le nom d'hôte ou l'adresse IP du serveur SMTP
  - Définir le numéro de port du serveur SMTP
  - Tester la connexion SMTP

- Configurer les paramètres LDAP :
  - Définir la configuration du serveur LDAP (DNS ou préconfiguré) :
    - Si la configuration du serveur LDAP spécifiée est DNS, définir le domaine de recherche :
      - Extraire le domaine de recherche à partir de l'ID de connexion
      - Nom de service et domaine de recherche spécifiés manuellement
      - Tenter d'extraire le domaine de recherche à partir de l'ID de connexion, puis utiliser le nom de service et le domaine de recherche spécifiés manuellement
    - Si un serveur LDAP préconfiguré est utilisé :
      - Définir l'adresse IP et le nom d'hôte du serveur LDAP
      - Définir le numéro de port du serveur LDAP
  - Définir le nom distinctif racine du serveur LDAP
  - Définir l'attribut de recherche UID
  - Sélectionner la méthode de liaison (anonyme, avec données d'identification configurées, avec justificatifs d'identité pour l'ouverture de session) :
    - Pour les données d'identification configurées, définir le mot de passe et le nom distinctif client
  - Activation de la sécurité étendue basée sur les rôles pour les utilisateurs Active Directory :
    - Si désactivé :
      - Définir le filtre de groupe
      - Définir l'attribut de recherche de groupe
      - Définir l'attribut d'autorisation de connexion
    - Si activé, définir le nom cible du serveur
- Configurer les paramètres Telnet :
  - Activation de l'accès Telnet
  - Définir le nombre maximal de sessions Telnet
- Configurer les paramètres USB :
  - Activation d'Ethernet via USB
  - Activation et gestion du réacheminement de port Ethernet externe à Ethernet via USB
- Configurer les affectations de port :
  - Afficher les numéros de ports ouverts
  - Définir les numéros de port utilisés par les services IMM2 :
    - HTTP
    - HTTPS
    - CLI Telnet
    - CLI SSH
    - Agent SNMP
    - SNMP Traps
    - Remote Control
    - CIM via HTTPS
    - CIM via HTTP

Dans la page Security, vous pouvez réaliser les opérations suivantes :

- Activation du serveur HTTPS et gestion des certificats

- Activation de CIM via HTTPS et gestion des certificats
- Sélection de la sécurité LDAP et gestion des certificats
- Activation du serveur SSH et gestion des certificats

Dans la page IMM Configuration, vous pouvez réaliser les opérations suivantes :
- Afficher un récapitulatif de configuration du module IMM2
- Sauvegarder ou restaurer la configuration du module IMM2
- Afficher l'état de sauvegarde et de restauration
- Restaurer la configuration du module IMM2 à ses paramètres usine par défaut
- Accès à l'assistant de configuration initiale du module IMM2

Dans la page Restart IMM, vous pouvez réinitialiser le module IMM2.

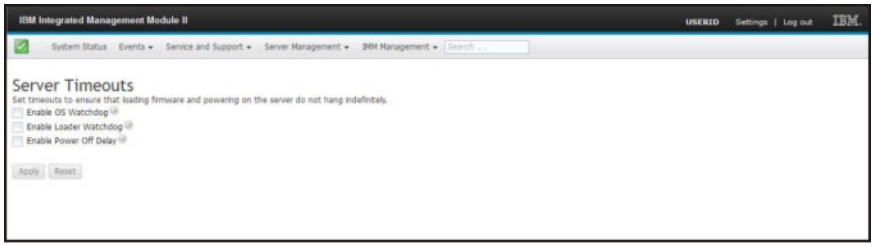
Dans la page Reset IMM2 to factory defaults..., vous pouvez restaurer la configuration du module IMM2 à ses paramètres usine par défaut.

Dans la page Activation Key Management, vous pouvez gérer les clés d'activation des dispositifs en option Features on Demand (FoD) du serveur ou du module IMM2. Pour plus d'informations sur la gestion des clés d'activation FoD, voir Chapitre 7, «Features on Demand», à la page 137.

## Configuration des délais d'attente du serveur

Utilisez l'option Server Timeouts pour définir les délais d'attente afin de s'assurer que le serveur ne se bloque pas indéfiniment lors de la mise sous tension ou la mise à jour d'un microprogramme sur le serveur. Vous pouvez activer cette fonction en définissant une valeur pour cette option, comme indiqué dans la figure suivante.

**Remarque :** Les délais d'attente de serveurs requièrent que l'interface USB intrabande (ou LAN via USB) soit activée pour utiliser des commandes. Pour plus d'informations sur l'activation et la désactivation de l'interface USB, voir «Configuration USB», à la page 80.




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

1. Connectez-vous au module IMM2 où vous souhaitez définir les délais d'attente de serveur. (voir «Connexion au module IMM2», à la page 10).
2. Cliquez sur **Server Management** puis sélectionnez **Server Timeouts**.

   Vous pouvez configurer IMM2 afin de répondre automatiquement aux événements suivants :
   - Blocage du système d'exploitation
   - Echec du chargement du système d'exploitation

3. Activez les délais d'attente du serveur correspondant aux événements auxquels vous souhaitez que le module IMM2 réponde automatiquement. Voir "Sélections des délais d'attente du serveur" pour obtenir une description de chaque option.
4. Cliquez sur **Apply**.

   **Remarque :** Vous pouvez utiliser le bouton **Reset** pour effacer tous les délais d'attente de façon simultanée.

### Sélections des délais d'attente du serveur

**Enable OS Watchdog**
Utilisez la zone **Enable OS Watchdog** pour spécifier le nombre de minutes séparant les vérifications du système d'exploitation par le module IMM2. Si le système d'exploitation ne répond pas à l'une de ces vérifications, IMM2 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 **Enable OS Watchdog** et sélectionnez un intervalle de temps dans le menu. Pour désactiver ce programme de surveillance, désélectionnez **Enable OS Watchdog**. Pour pouvoir effectuer des captures d'écran des échecs du système d'exploitation, vous devez activer le programme de surveillance dans la zone **Enable OS Watchdog**.

**Enable Loader Watchdog**
Utilisez la zone **Enable Loader Watchdog** pour spécifier le nombre de minutes pendant lesquelles IMM2 doit patienter entre l'achèvement des vérifications POST et le lancement du système d'exploitation. Si ce délai est dépassé, IMM2 génère une alerte de délai d'attente du programme de chargement et redémarre 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 IMM2 doit attendre l'achèvement du chargement du système d'exploitation. Pour désactiver ce programme de surveillance, désélectionnez **Enable Loader Watchdog** dans le menu.

**Enable Power Off Delay**
Utilisez la zone **Enable Power Off Delay** pour spécifier le nombre de minutes pendant lesquelles le sous-système IMM2 doit attendre l'arrêt du système d'exploitation avant de mettre le système hors tension. Pour définir la valeur du délai d'attente de mise hors tension, sélectionnez la limite de temps pendant laquelle IMM2 doit attendre après la mise hors tension du système d'exploitation. Pour désactiver ce programme de surveillance, désélectionnez **Enable Loader Watchdog** dans le menu.

## Réglage de la date et de l'heure du module IMM2

**Remarque :** Les paramètres de date et d'heure du module IMM2 ne peuvent pas être modifiés dans IBM Flex System.

Sélectionnez l'onglet **Date and Time** pour afficher ou modifier la date et l'heure du module IMM2. Le module IMM2 utilise sa propre horloge en temps réel pour

horodater tous les événements listés dans le journal des événements. Les alertes envoyées par courrier électronique et le protocole Simple Network Management Protocol (SNMP) utilisent l'horloge en 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 des administrateurs gérant les systèmes sur des fuseaux horaires différents. Vous pouvez accéder à distance au journal des événements même si le serveur est hors tension ou désactivé.

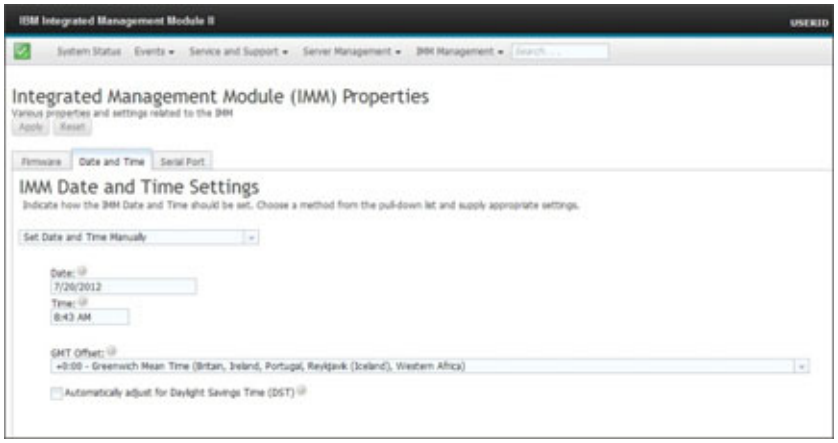
Le paramètre de date et heure IMM2 affecte uniquement l'horloge IMM2 et non celle du serveur. L'horloge en temps réel du module IMM2 et celle du serveur sont des horloges distinctes et indépendantes qui peuvent être réglées différemment.

## Modification du paramètre de date et heure (mode manuel)

Pour modifier manuellement le paramètre de date et heure, procédez comme suit.

1. Dans la liste de menu **Indicate how the IMM date and time should be set**, cliquez sur **Set Date and Time Manually**.
2. Dans la zone **Date**, entrez le mois, le jour et l'année en cours.
3. Dans la zone **Time**, entrez les chiffres correspondant à l'heure et aux minutes.
   - L'heure doit être un nombre de 1 à 12, comme sur une horloge au format 12 heures.
   - Les minutes doivent être des nombres compris entre 00 et 59.
   - Sélectionnez **AM** ou **PM**.
4. Dans la zone **GMT Offset**, sélectionnez le chiffre indiquant le décalage, en heures, par rapport à l'heure GMT. Ce chiffre doit correspondre au fuseau horaire sur lequel le serveur est situé.
5. Sélectionnez ou désélectionnez la case **Automatically adjust for Daylight Saving Time (DST)** pour spécifier si l'horloge IMM2 doit être automatiquement corrigée lors du passage de l'heure standard à l'heure d'été.

La figure suivante présente l'onglet IMM Date and Time lors du réglage manuel de la date et de l'heure.

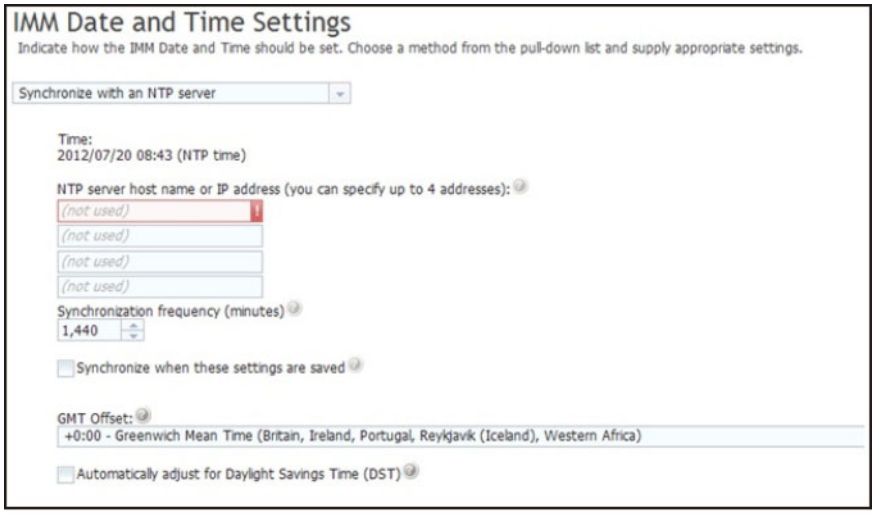



## Modification des paramètres de date et heure (mode serveur NTP)

Pour synchroniser l'horloge IMM2 avec l'horloge du serveur, procédez comme suit.

1. Dans la liste de menu **Indicate how the IMM date and time should be set**, cliquez sur **Synchronize with an NTP server**.
2. Dans la zone **NTP server host name or IP address**, indiquez le nom du serveur NTP à utiliser pour la synchronisation de l'horloge.
3. Dans la zone **Synchronization frequency (in minutes)**, indiquez l'intervalle approximatif entre les demandes de synchronisation. Entrez une valeur comprise entre 3 et 1440 minutes.
4. Cochez la case **Synchronize when these settings are saved** pour demander une synchronisation immédiate (lorsque vous cliquez sur **Apply**), au lieu d'attendre l'écoulement du délai spécifié.
5. Dans la zone **GMT Offset**, sélectionnez le nombre indiquant le décalage, en heures, par rapport à l'heure GMT, correspondant au fuseau horaire sur lequel le serveur est situé.
6. Sélectionnez ou désélectionnez la case **Automatically adjust for Daylight Saving Time (DST)** pour spécifier si l'horloge IMM2 doit être automatiquement corrigée lors du passage de l'heure standard à l'heure d'été.

La figure suivante présente l'onglet IMM Date and Time lors de la synchronisation avec l'horloge du serveur.




## Configuration des paramètres de port série

Sélectionnez l'option **Serial Port** pour spécifier la redirection du port série de l'hôte. Le module IMM2 comporte deux ports série qui sont utilisés pour la redirection série :

**Port série 1 (COM1)**

Le port série 1 (COM1) sur les serveurs System x est utilisé pour SOL (Serial over LAN) IPMI. COM1 ne peut être configuré que via l'interface IPMI.

**Port série 2 (COM2)**

Sur les serveurs lame, le port série 2 (COM2) est utilisé pour SOL. Sur les serveurs rack System x et IBM Flex System, 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.

Remplissez les zones suivantes pour la redirection de port série :

**Baud Rate**
Dans cette zone, spécifiez 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, entre 9600 et 115200, correspondant à votre connexion de port série.

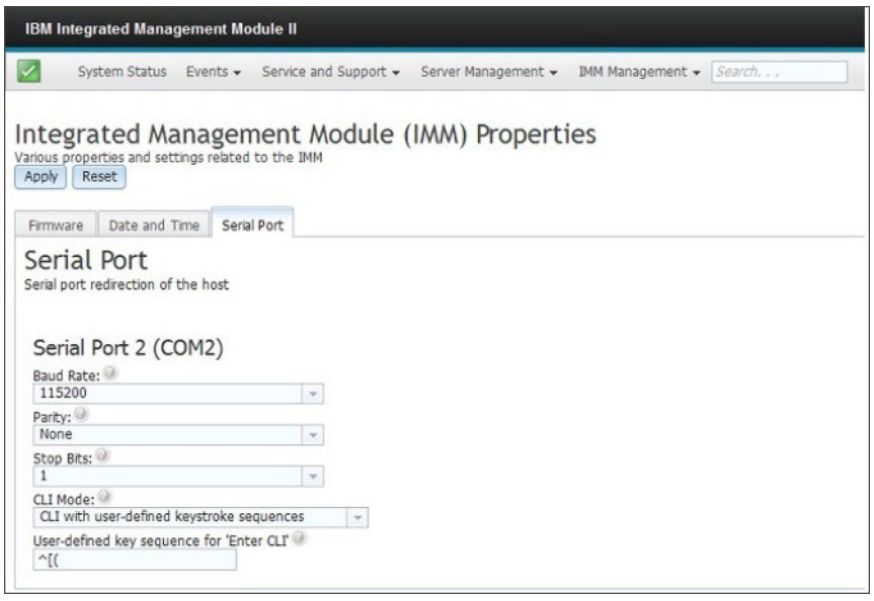
**Parity** Dans cette zone, spécifiez les bits de parité de votre connexion de port série. Les options disponibles sont None, Odd et Even.

**Stop Bits**
Dans cette zone, spécifiez le nombre de bits d'arrêt de votre connexion de port série. Les options disponibles sont 1 ou 2.

**CLI Mode**
Dans cette zone, sélectionnez **CLI with IMM2 compatible keystroke sequences** ou **CLI with user defined keystroke sequences**, si vous souhaitez utiliser votre propre séquence de touches. Si vous sélectionnez **CLI with user defined keystroke sequences**, vous devez définir la séquence de touches dans la zone **User-defined key sequence for 'Enter CLI'**.

Une fois que la redirection série commence, elle continue jusqu'à ce que la séquence de touches de sortie soit saisie. Lorsque la séquence de touches de sortie est saisie, la redirection série s'arrête et vous êtes ramené au mode de commande dans la session Telnet ou SSH. Utilisez la zone **User-defined key sequence for 'Enter CLI'** pour spécifier la séquence de touches de sortie.

La figure suivante présente l'onglet Serial Port.




## Configuration des comptes utilisateurs

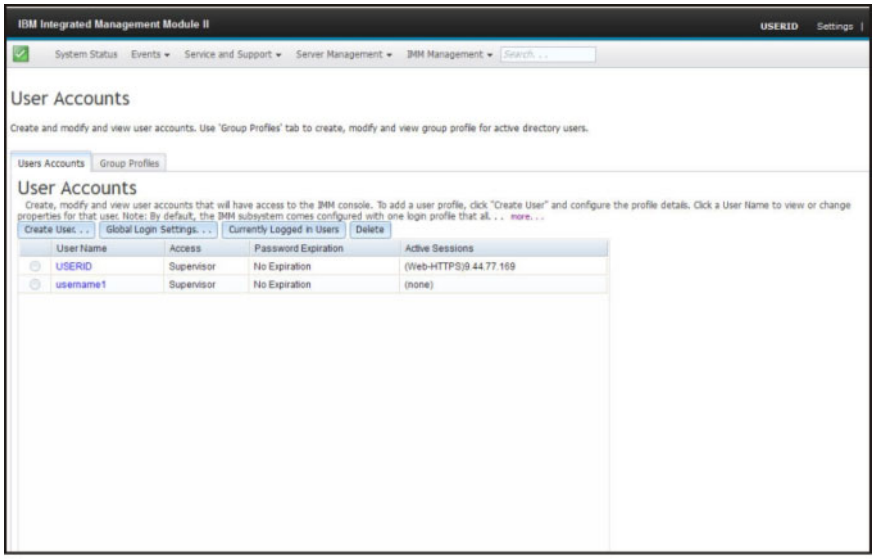
Sélectionnez l'option **Users** dans l'onglet IMM Management pour créer et modifier les comptes utilisateurs du module IMM2 et afficher les profils de groupes. Le message d'information suivant s'affichera à l'écran.

**Remarque :** Dans IBM Flex System, les comptes utilisateurs IMM2 sont gérés par le CMM.


## Comptes utilisateur

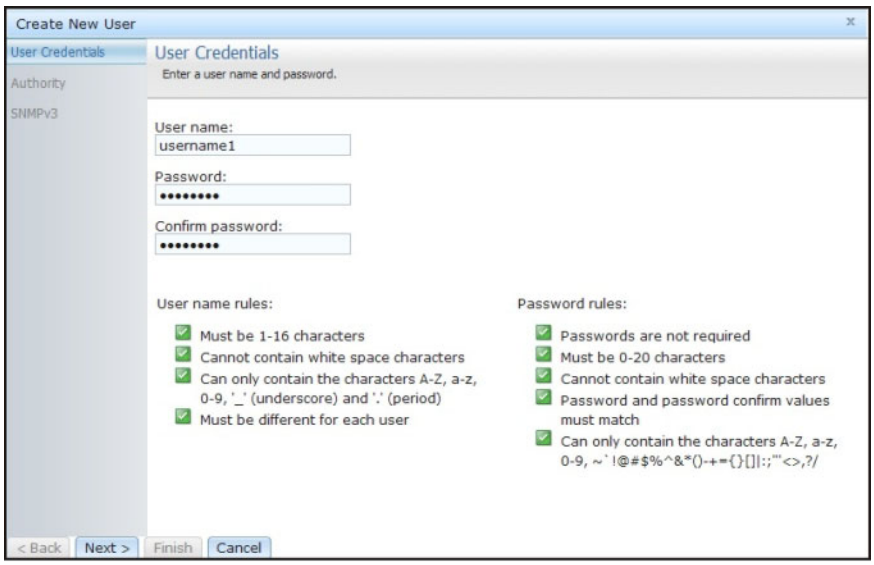
Sélectionnez l'onglet **Users Accounts** pour créer, modifier et afficher les comptes d'utilisateurs, comme illustré dans l'écran ci-après.

**Remarque :** Le sous-système IMM2 est fourni avec un profil de connexion.



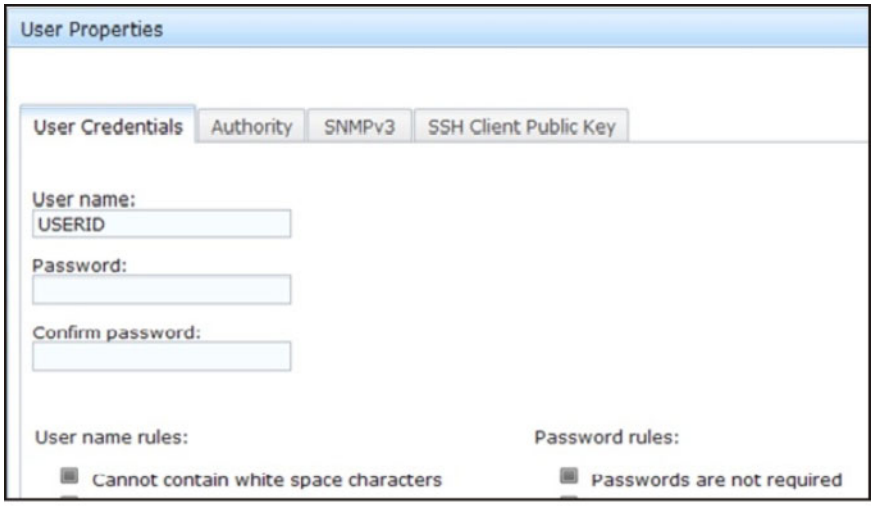

### Création d'un utilisateur

Cliquez sur l'onglet **Create User...** pour créer un nouveau compte utilisateur. Complétez les zones suivantes : **User name**, **Password** et **Confirm Password** (comme illustré ci-après).




## Propriétés utilisateur

Cliquez sur l'onglet **User Properties** pour modifier les comptes utilisateurs existants (comme indiqué dans la figure ci-après).




## Autorisations de l'utilisateur

Cliquez sur l'onglet **Authority** pour définir les autorisations de l'utilisateur. Les niveaux d'autorisation suivants sont disponibles pour l'utilisateur :

**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**
Permet de définir un profil d'autorisation plus personnalisé pour l'utilisateur grâce à la définition d'actions que l'utilisateur est autorisé à effectuer.

### Droits d'accès SNMP

Cliquez sur l'onglet **SNMPv3** pour définir l'accès SNMP du compte. Les options d'accès utilisateur suivantes sont disponibles :

**Authentication protocol**
Spécifiez **HMAC-MD5** ou **HMAC-SHA** comme protocole d'authentification. Il s'agit des algorithmes utilisés par le modèle de sécurité SNMPv3 pour l'authentification. Si l'option **Authentication Protocol** n'est pas activée, aucun protocole d'authentification ne sera 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 sur **HMAC-MD5** ou **HMAC-SHA**.

**Privacy password**
Indiquez le mot de passe de chiffrement dans cette zone.

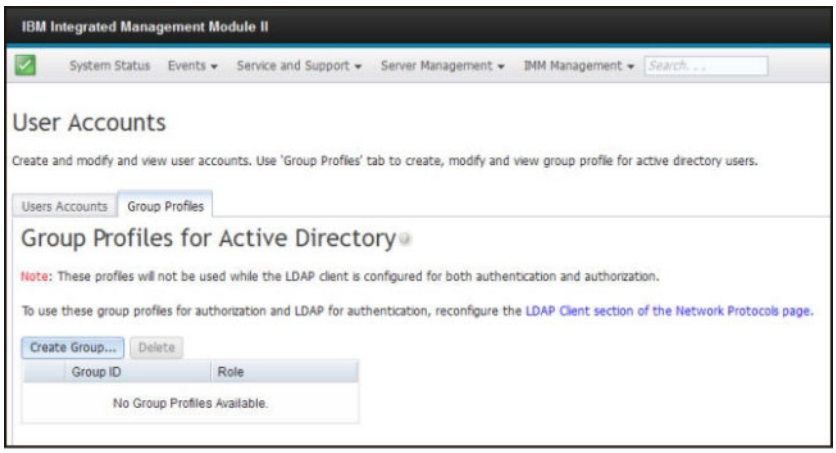
**Confirm privacy password**
Indiquez à nouveau le mot de passe de chiffrement pour confirmation.

**Access type**
Choisissez **Get** ou **Set** comme type d'accès. Les utilisateurs SNMPv3 utilisant le type d'accès **Get** ne peuvent effectuer que des opérations de requêtes. Les utilisateurs SNMPv3 utilisant le type d'accès **Set** peuvent effectuer des requêtes et modifier les paramètres (par exemple, configurer le mot de passe d'un utilisateur).

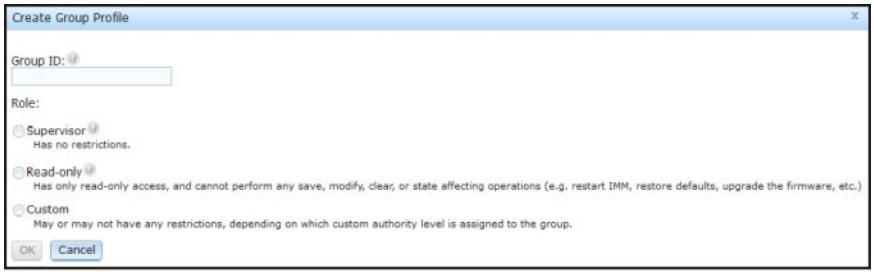
**Hostname/IP address for traps**
Spécifiez la destination des alertes pour l'utilisateur. Il peut s'agir d'une adresse IP ou d'un nom d'hôte. En utilisant des alertes, l'agent SNMP avise la station de gestion des événements survenus (par exemple, lorsque la température d'un processeur dépasse la limite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

## Profils de groupe

Sélectionnez l'onglet **Group Profiles** pour créer, modifier et afficher les profils de groupe (comme illustré ci-après).

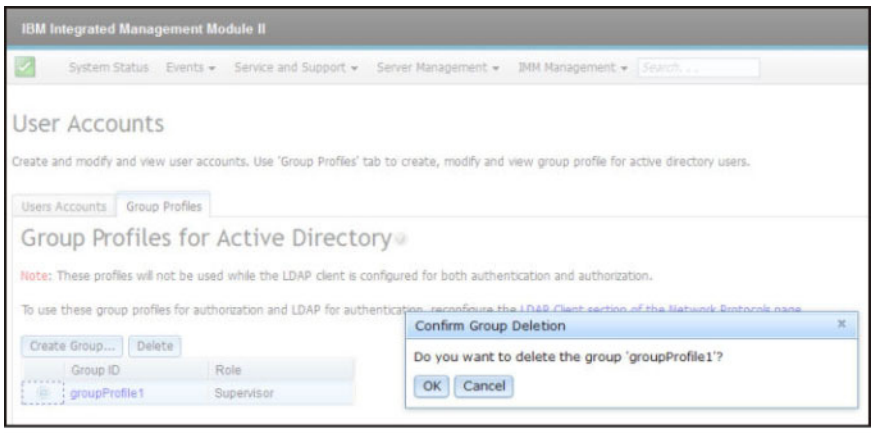



Cliquez sur **Create Group** pour créer un nouveau groupe d'utilisateurs. La figure suivante présente la fenêtre Create Group Profile.




Entrez un ID de groupe sous **Group ID** et sélectionnez le **rôle** (pour obtenir des informations sur les niveaux d'autorisation des utilisateurs, voir «Autorisations de l'utilisateur», à la page 60).

Si vous avez besoin de supprimer un groupe, cliquez sur **Delete**. La figure ci-après présente la fenêtre Confirm Group Deletion.




## Configuration des paramètres de connexion globale

Utilisez l'onglet Global login settings pour configurer les paramètres de connexion s'appliquant à tous les utilisateurs.

## Paramètres généraux

Cliquez sur l'onglet **General** pour sélectionner la façon dont les tentatives de connexion utilisateur sont authentifiées et indiquez combien de temps, en minutes, le module IMM2 doit attendre avant de déconnecter une session Web inactive. Dans la zone **User authentication method**, vous pouvez spécifier comment authentifier les utilisateurs qui tentent de se connecter. Vous pouvez sélectionner l'une des méthodes d'authentification suivantes :

- **Local only :** Les utilisateurs sont authentifiés par une recherche du compte utilisateur local configuré sur le module IMM2. Si l'ID et le mot de passe de l'utilisateur ne correspondent pas, l'accès est refusé.
- **LDAP only :** Le module IMM2 tente d'authentifier l'utilisateur par le biais d'un serveur LDAP. Les comptes utilisateurs locaux se trouvant sur IMM2 ne sont *pas* recherchés avec 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.

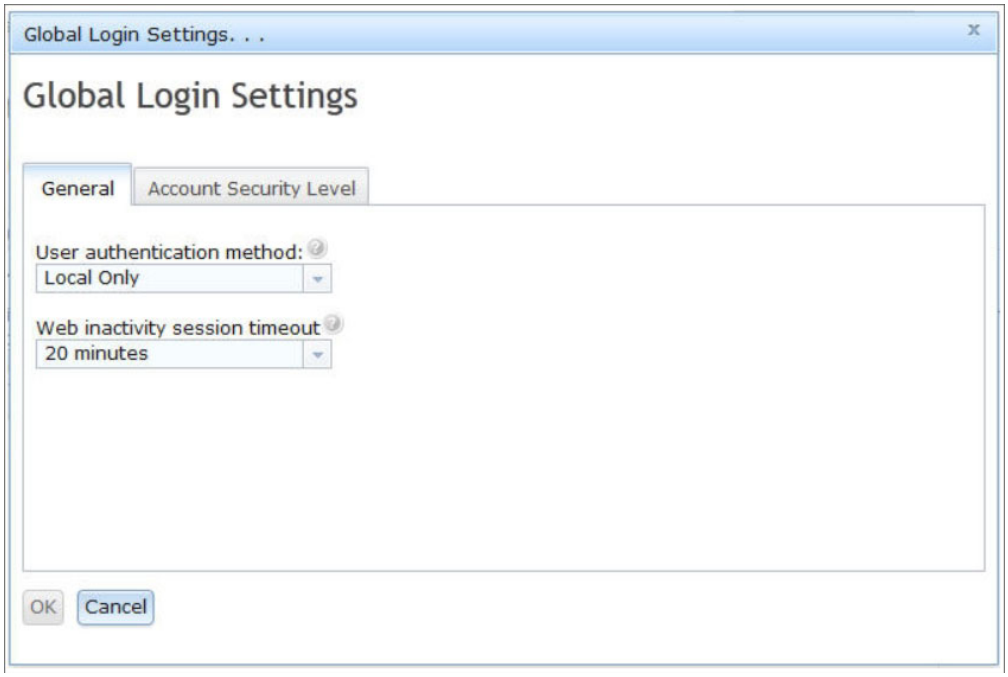
**Remarques :**

- Seuls les comptes administrés au niveau local sont partagés avec les interfaces IPMI et SNMP. Ces interfaces ne prennent pas en charge l'authentification LDAP.
- Les utilisateurs IPMI et SNMP peuvent se connecter à l'aide des comptes administrés au niveau local lorsque la zone **User authentication method** est définie sur **LDAP only**.

Dans la zone **Web inactivity session timeout**, vous pouvez spécifier combien de temps, en minutes, le module IMM2 doit attendre avant de déconnecter une session Web inactive. Sélectionnez **No timeout** pour désactiver cette fonction. Sélectionnez **User picks timeout** pour sélectionner le délai d'attente lors du processus de connexion.

Le délai d'attente d'inactivité s'applique uniquement aux pages Web qui ne s'actualisent *pas* automatiquement. Si un navigateur Web demande continuellement une mise à jour de la page Web lorsqu'un utilisateur accède à une page Web qui s'actualise automatiquement, le délai d'attente d'inactivité ne terminera pas automatiquement la session de l'utilisateur. Les utilisateurs peuvent choisir s'ils souhaitent ou non que le contenu de la page Web soit automatiquement actualisé toutes les 60 secondes. Pour plus d'informations sur le paramètre d'actualisation automatique, voir «Page auto refresh», à la page 15.

La figure ci-après présente l'onglet General.




Certaines pages Web IMM2 sont automatiquement actualisées même si le paramètre d'actualisation automatique n'est pas sélectionné. Les pages Web IMM2 qui sont automatiquement actualisées sont les suivantes :

- **System Status :** L'état du système et de l'alimentation est actualisé automatiquement toutes les trois secondes.
- **Server Power Actions :** L'état d'alimentation est actualisé automatiquement toutes les trois secondes.
- **Remote Control :** Les boutons de démarrage du contrôle à distance sont actualisés automatiquement à chaque seconde. La table Session List est actualisée automatiquement une fois toutes les minutes.

Le microprogramme IMM2 prend en charge jusqu'à six sessions Web simultanées. Pour libérer une session au profit d'un autre utilisateur, il est recommandé de se déconnecter de la session Web dès vous avez fini, au lieu d'attendre que le délai d'attente d'inactivité ferme votre session.

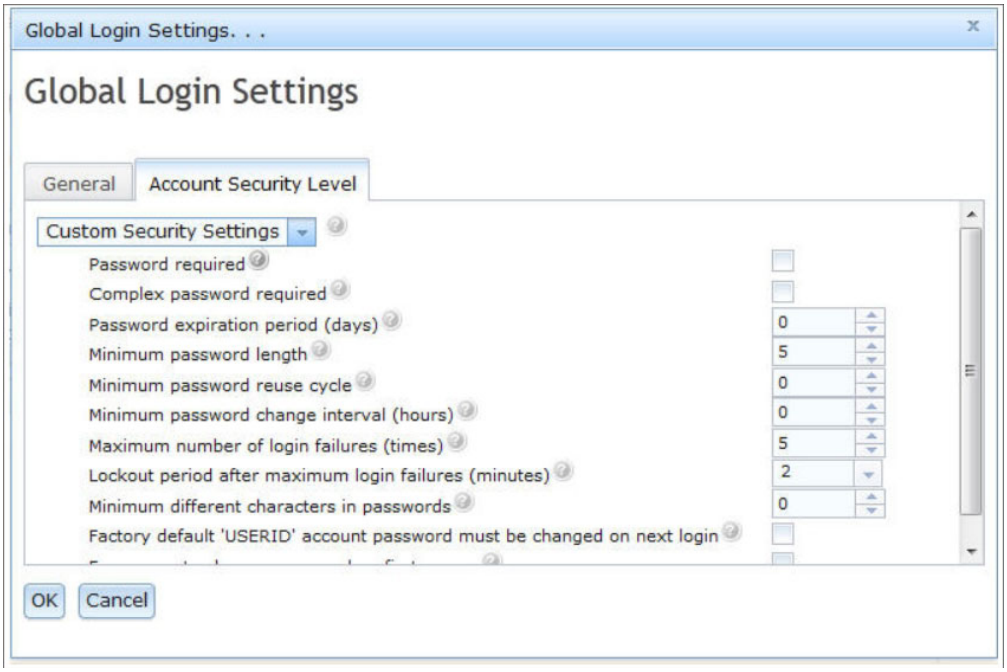
**Remarque :** Si vous laissez votre navigateur ouvert sur une page Web IMM2 qui s'actualise automatiquement, votre session Web ne se fermera pas automatiquement pour cause d'inactivité.

## Paramètres des règles de sécurité des comptes

Cliquez sur l'onglet **Account Security Level** pour sélectionner les paramètres des règles de sécurité des comptes. Il existe trois niveaux de paramètres :

- Legacy Security Settings (paramètres de sécurité existants)
- High Security Settings (paramètres de sécurité élevés)
- Custom Security Settings (paramètres de sécurité personnalisés)

La figure ci-après présente l'onglet Account Security Level.




Sélectionnez le niveau souhaité dans la liste d'éléments. Les options Legacy Security Settings et High Security Settings contiennent des valeurs de paramètres prédéfinies et ne peuvent pas être modifiées. L'option Custom Security Settings permet aux utilisateurs de personnaliser les règles de sécurité en fonction de leurs besoins.

Le tableau suivant affiche les valeurs des différents niveaux de paramètres de sécurité.

*Tableau 3. Valeurs des règles des paramètres de sécurité*

| **Paramètre de règle/zone** | **Paramètres de sécurité existants** | **Paramètres de sécurité élevés** | **Paramètres de sécurité personnalisés** |
|---|---|---|---|
| Password required (Mot de passe obligatoire) | Non | Oui | Oui ou Non |
| Complex password required (Mot de passe complexe obligatoire) | Non | Oui | Oui ou Non |
| Password expiration period (days) (Délai d'expiration du mot de passe (jours)) | Aucun | 90 | 0 – 365 |
| Minimum password length (Longueur minimale du mot de passe) | Aucun | 8 | 5 – 20 |
| Minimum password reuse cycle (Cycle de réutilisation minimal du mot de passe) | Aucun | 5 | 0 – 5 |

*Tableau 3. Valeurs des règles des paramètres de sécurité (suite)*

| Paramètre de règle/zone | Paramètres de sécurité existants | Paramètres de sécurité élevés | Paramètres de sécurité personnalisés |
|---|---|---|---|
| Minimum password change interval (hours) (Intervalle minimum de changement du mot de passe (heures)) | Aucun | 24 | 0 – 240 |
| Maximum number of login failures (times) (Nombre maximal d'échecs de connexion (nombre de fois)) | 5 | 5 | 0 – 10 |
| Lockout period after maximum login failures (minutes) (Période de verrouillage après maximum d'erreurs de connexion (minutes)) | 2 | 60 | 0 – 240 |
| Minimum different characters in passwords (Nombre minimal de caractères différents dans les mots de passe) | Aucun | 2 | 0 – 19 |
| Factory default 'USERID' account password must be changed on next login (Modifier le mot de passe usine par défaut du compte 'USERID' à la prochaine connexion) | Non | Oui | Oui ou Non |
| Force user to change password on first access (Obliger l'utilisateur à changer le mot de passe au premier accès) | Non | Oui | Oui ou Non |

Les informations suivantes offrent une description des zones de configuration des paramètres de sécurité.

**Password required**

Cette zone indique s'il est possible de créer des ID de connexion sans mot de passe. Si la case **Password required** est cochée, tous les ID de connexion sans mot de passe existants devront définir un mot de passe lors de la prochaine connexion de l'utilisateur.

**Complex password required**

Si des mots de passe complexes sont requis, les règles suivantes doivent être respectées :

- Les mots de passe doivent avoir un minimum de huit caractères.
- Les mots de passe doivent contenir au moins trois des quatre catégories suivantes :
  - Au moins un caractère alphabétique en minuscules.
  - Au moins un caractère alphabétique en majuscules.
  - Au moins un caractère numérique.
  - Au moins un caractère spécial.
- Les espaces ou caractères espace blancs ne sont pas autorisés.
- Les mots de passe ne peuvent pas avoir plus de trois caractères identiques consécutifs (par exemple, aaa).
- Les mots de passe ne doivent pas répéter ou inverser l'ID utilisateur associé.

Si les mots de passe complexes ne sont pas requis, le mot de passe :

- Doit avoir un minimum de cinq caractères (ou le nombre spécifié dans la zone **Minimum password length**).
- Ne peut pas contenir d'espace ou de caractère espace blanc.
- Doit contenir au moins un caractère numérique.
- Peut être vide (uniquement si la case **Password Required** est désactivée).

**Password expiration period (days)**

Cette zone contient l'âge maximal autorisé du mot de passe, avant lequel il devra être modifié. Les valeurs 0 à 365 jours sont prises en charge. La valeur par défaut de cette zone est 0 (désactivé).

**Minimum password length**

Cette zone contient la longueur minimale du mot de passe. 5 à 20 caractères sont pris en charge dans cette zone. Si la case **Complex password required** est cochée, le mot de passe devra comporter au moins huit caractères.

**Minimum password reuse cycle**

Cette zone contient le nombre de mots de passe antérieurs ne pouvant 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. La valeur par défaut de cette zone est 0 (désactivé).

**Minimum password change interval (hours)**

Cette zone contient la durée nécessaire à attendre pour que l'utilisateur puisse à nouveau changer son mot de passe. Les valeurs 0 à 240 heures sont prises en charge. La valeur par défaut de cette zone est 0 (désactivé).

**Maximum number of login failures (times)**

Cette zone contient le nombre d'échecs de tentatives de connexion autorisé avant que l'utilisateur soit verrouillé pendant une période définie. Les valeurs 0 à 10 sont prises en charge. La valeur par défaut de cette zone est 0 (désactivé).

**Lockout period after maximum login failures (minutes)**

Cette zone indique la durée (en minutes) pendant laquelle le sous-système IMM2 désactivera les tentatives de connexion à distance pour tous les utilisateurs après avoir détecté plus de cinq échecs de connexion consécutifs provoqués par l'un des utilisateurs.

**Minimum different characters in passwords**
Cette zone indique le nombre de caractères devant différer entre le nouveau mot de passe et le mot de passe précédent. Les valeurs 0 à 19 sont prises en charge.

**Factory default 'USERID' account password must be changed on next login**
Une option de fabrication est fournie pour réinitialiser le profil USERID par défaut après la première connexion réussie. Lorsque cette case est cochée, le mot de passe par défaut doit être modifié avant de pouvoir utiliser le compte. Le nouveau mot de passe est soumis à toutes les règles de mise en application des mots de passe actives.

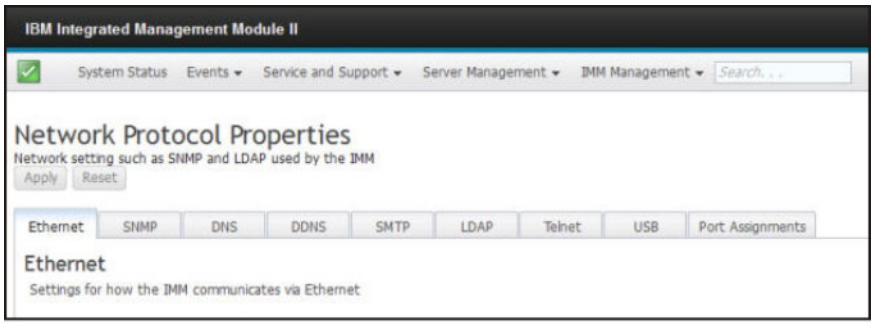
**Force user to change password on first access**
Après avoir défini un nouvel utilisateur avec un mot de passe par défaut, la sélection de cette case forcera l'utilisateur à modifier son mot de passe lors de sa première connexion.

# Configuration des protocoles réseau

Cliquez sur l'option **Network** dans l'onglet de gestion du module IMM pour afficher et définir les paramètres réseau.

## Configuration des paramètres Ethernet

Cliquez sur l'onglet **Ethernet** pour afficher ou modifier les paramètres Ethernet du module IMM2 (comme illustré ci-après).




Pour utiliser une connexion Ethernet IPv4, procédez comme suit.

1. Sélectionnez l'option **IPv4** , puis sélectionnez la case à cocher correspondante.

   **Remarque :** La désactivation de l'interface Ethernet empêche l'accès au module IMM2 depuis le réseau externe.
2. Dans la liste **Configure IP address settings**, sélectionnez l'une des options suivantes :
   - Obtain an IP address from a DHCP server
   - Use static IP address
3. Si vous souhaitez que le module IMM2 utilise une adresse IP statique par défaut en cas de ne pas pouvoir contacter un serveur DHCP, sélectionnez la case correspondante.
4. Dans la zone **Static address**, entrez l'adresse IP du module IMM2.

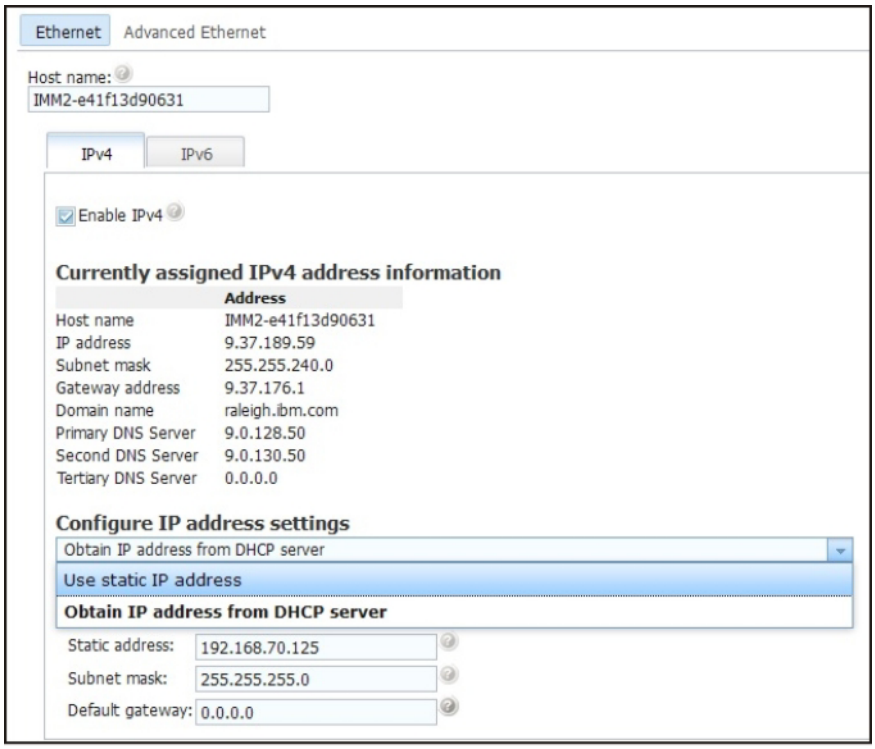
   **Remarque :** L'adresse IP doit contenir quatre nombres entiers compris entre 0 et 255, sans espace et séparés par des points.

5. Dans la zone **Subnet mask**, entrez le masque de sous-réseau utilisé par le module IMM2.

   **Remarque :** Le masque de sous-réseau doit contenir quatre nombres entiers compris entre 0 et 255, sans espace ni points consécutifs et séparés par des points. La valeur par défaut est 255.255.255.0.
6. Dans la zone **Default Gateway**, entrez le routeur de votre passerelle réseau.

   **Remarque :** L'adresse de passerelle doit contenir quatre nombre entiers compris entre 0 et 255, sans espace ni points consécutifs et séparés par des points.

La figure suivante présente l'onglet Ethernet.



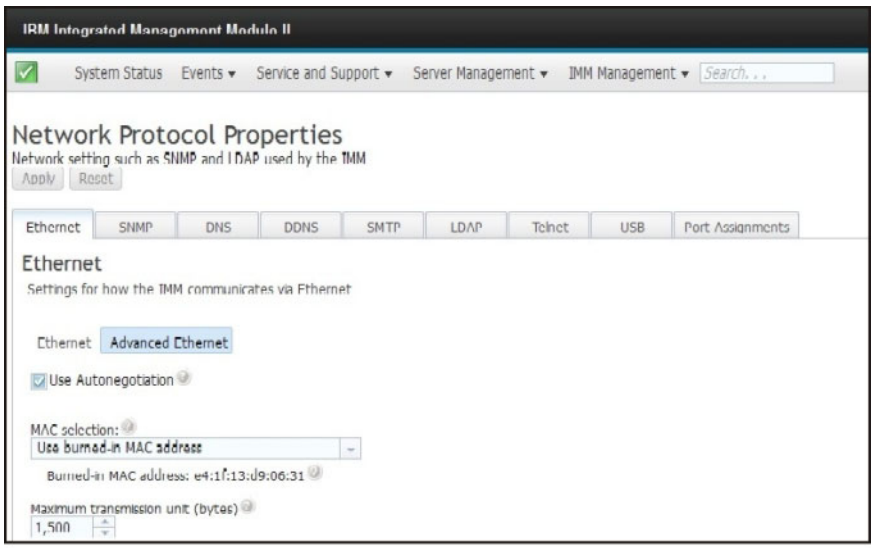

## Configuration des paramètres Ethernet avancés

Cliquez sur l'onglet **Advanced Ethernet** pour définir des paramètres Ethernet supplémentaires. Dans la liste **MAC selection**, sélectionnez l'une des options suivantes :

- Used burned in MAC address
  - L'option Burned-in MAC address est une adresse physique unique attribuée à ce module IMM2 par le fabricant. L'adresse constitue une zone en lecture seule.
- Used locally administered MAC address
  - 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 être au format *xx:xx:xx:xx:xx:xx* où *X* est un nombre compris entre 0 et 9. Le module IMM2 ne prend pas en charge l'utilisation d'une adresse de

multidiffusion. Le premier octet d'une adresse de multidiffusion est un nombre impair (le bit le moins significatif est défini sur 1), par conséquent, le premier octet doit être un nombre pair.

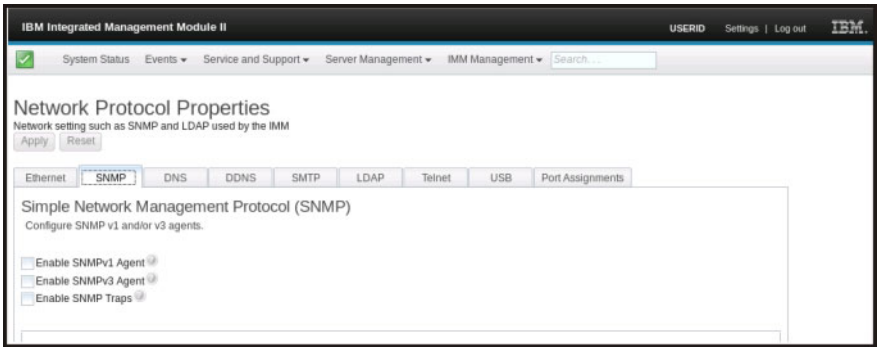
Dans la zone **Maximum transmission unit**, spécifiez l'unité de transmission maximale d'un paquet (en octets) pour votre interface réseau. L'unité de transmission maximale est comprise entre 60 et 1500. La valeur par défaut de cette zone est 1500. La figure suivante présente l'onglet Advanced Ethernet et les zones associées.




## Configuration des paramètres d'alerte SNMP

Procédez comme suit pour configurer le paramètre SNMP IMM2.

1. Cliquez sur l'onglet **SNMP** (comme illustré ci-après).




2. Sélectionnez la case à cocher correspondante pour activer l'agent SNMPv1, l'agent SNMPv3 ou les alertes SNMP.
3. Si l'agent SNMPv1 est activé, passez à l'étape 4. Si l'agent SNMPv3 est activé, passez à l'étape 5, à la page 71. Si les alertes SNMP sont activées, passez à l'étape 6, à la page 71
4. Si l'agent SNMPv1 est activé, complétez les zones suivantes :
   a. Cliquez sur l'onglet **Contact**. Dans la zone **Contact person**, entrez le nom de la personne à contacter. Dans la zone **Location**, entrez le site (coordonnées géographiques).

b. Cliquez sur l'onglet **Communities** pour configurer une communauté afin de définir la relation d'administration entre les agents SNMP et les gestionnaires SNMP. Vous devez définir au moins une communauté.

   **Remarques :**

   - Si un message d'erreur apparaît, modifiez les zones mentionnées en conséquence, puis accédez au haut de la page et cliquez sur **Apply** pour sauvegarder vos corrections.
   - Vous devez configurer au moins une communauté pour activer cet agent SNMP.

   Renseignez les zones suivantes :

   1) Dans la zone **Community Name**, entrez un nom ou une chaîne d'authentification pour indiquer une communauté.
   2) Dans la zone **Access type**, sélectionnez un type d'accès.
      - Sélectionnez **Trap** pour autoriser tous les hôtes de la communauté à recevoir des alertes.
      - Sélectionnez **Get** pour autoriser tous les hôtes de la communauté à recevoir des alertes et interroger les objets de bases d'information de gestion (MIB).
      - Sélectionnez **Set** pour autoriser tous les hôtes de la communauté à recevoir des alertes, interroger et définir des objets MIB.

c. Dans la zone **Host Name** ou **IP Address**, entrez le nom d'hôte ou l'adresse IP de chaque gestionnaire de communauté.

d. Cliquez sur **Apply** pour appliquer les modifications effectuées.

5. Si l'agent SNMPv3 est activé, complétez les zones suivantes :

   a. Cliquez sur l'onglet **Contact**. Dans la zone **Contact person**, entrez le nom de la personne à contacter. Dans la zone **Location**, entrez le site (coordonnées géographiques).

   b. Cliquez sur l'onglet **Users** pour afficher la liste des comptes utilisateurs locaux de la console.

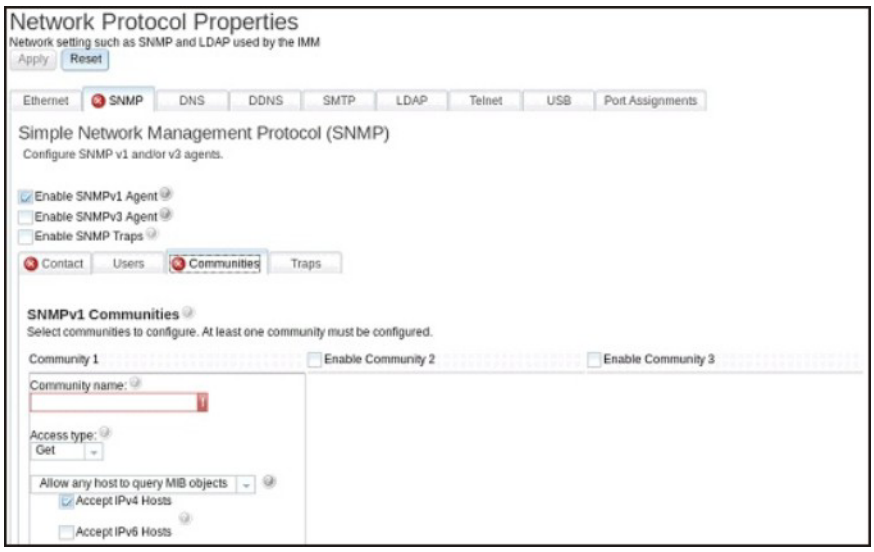
      **Remarque :** Il s'agit de la même liste que celle qui figure dans l'option Users. Vous devez configurer SNMPv3 pour chaque compte utilisateur ayant besoin d'un accès SNMPv3.

   c. Cliquez sur **Apply** pour appliquer les modifications effectuées.

6. Si les alertes SNMP sont activées, configurez les événements faisant l'objet d'une alerte sous l'onglet **Traps**.

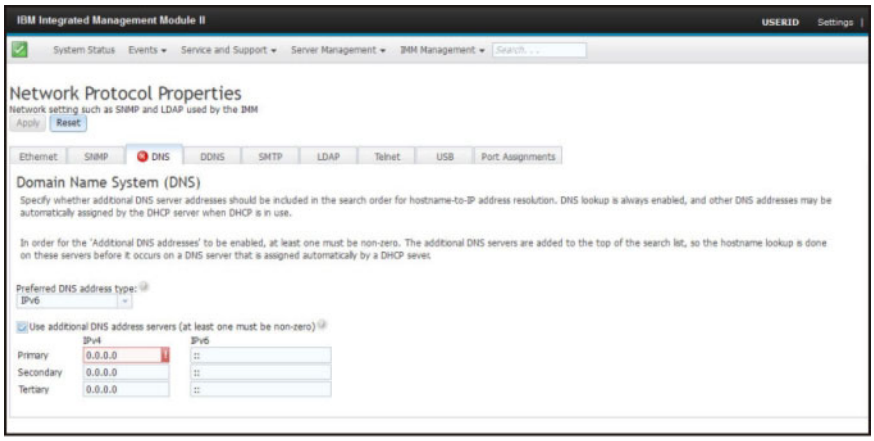
**Remarque :** Lors de la configuration SNMP, les zones obligatoires n'ayant pas été complétées ou contenant des valeurs incorrectes sont mises en évidence avec un X rouge qui peut être utilisé pour vous guider jusqu'à la fin des zones obligatoires.

La figure suivante présente l'onglet SNMP lors de la configuration de l'agent SNMPv1.




## Configuration DNS

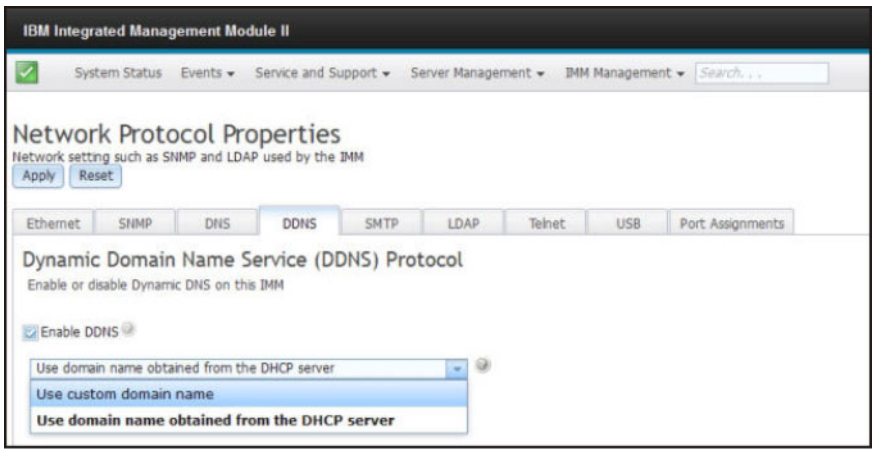
Cliquez sur l'onglet **DNS** pour afficher ou modifier les paramètres du système de noms de domaine IMM2. Si vous cliquez sur la case à cocher **Use additional DNS address servers**, spécifiez les adresses IP de jusqu'à trois serveurs DNS sur votre réseau. Chaque adresse IP doit contenir des entiers compris entre 0 et 255, séparés par des points (comme illustré ci-après).




## Configuration du DDNS

Cliquez sur l'onglet **DDNS** pour afficher ou modifier les paramètres du système de noms de domaine dynamique (DDNS) IMM2. Cliquez sur la case à cocher **Enable DDNS** pour activer le DDNS. Lorsque le DDNS est activé, le module IMM2 indique à un DNS de modifier, en temps réel, la configuration DNS active des noms d'hôte, adresses ou autres informations configurées, stockées dans le DNS.

Sélectionnez une option dans la liste des éléments pour définir la façon dont vous souhaitez que le nom de domaine du module IMM2 soit sélectionné (comme illustré ci-après).




## Configuration de SMTP

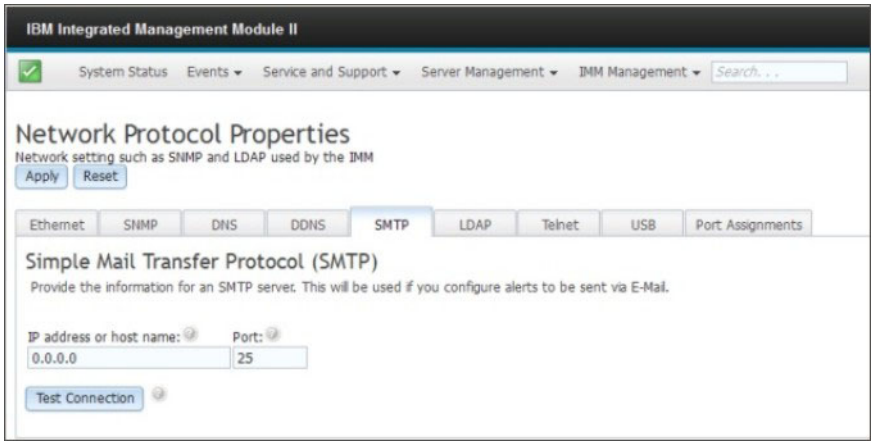
Cliquez sur l'onglet **SMTP** pour afficher ou modifier les paramètres SMTP du module IMM2. Renseignez les zones suivantes pour afficher ou modifier les paramètres SMTP :

**IP address or host name**
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.

**Port** Spécifiez le numéro de port du serveur SMTP. La valeur par défaut est 25.

**Test connection**
Cliquez sur **Test Connection**. Un courrier électronique test sera envoyé pour vérifier que vos paramètres SMTP sont corrects.

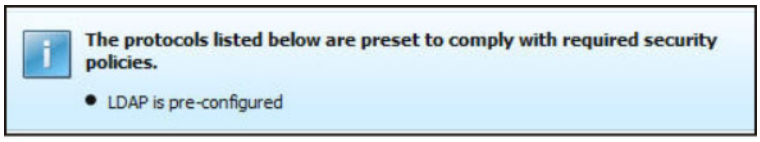
La figure suivante présente l'onglet SMTP.




## Configuration de LDAP

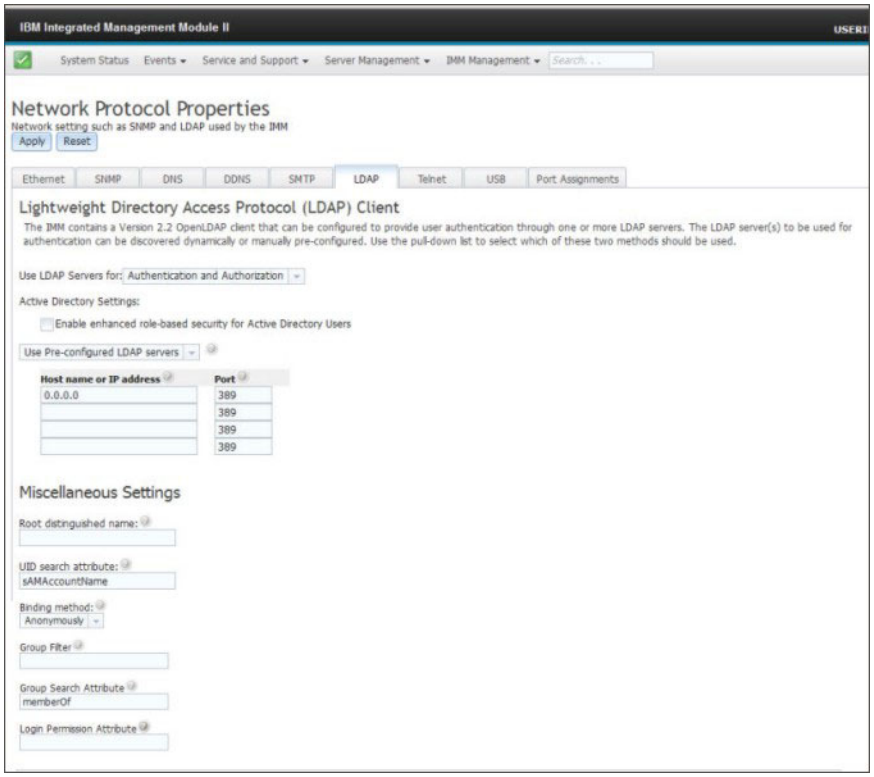
Cliquez sur l'onglet **LDAP** pour afficher ou modifier les paramètres client LDAP du module IMM2.

**Remarque :** Dans un environnement IBM Flex System, le module IMM2 est configuré pour utiliser le serveur LDAP exécuté sur le CMM. Un message d'information vous rappellera que les paramètres LDAP ne peuvent pas être modifiés (comme illustré ci-après).




Si vous utilisez un serveur LDAP, le module IMM2 peut authentifier un utilisateur en lançant des requêtes ou des recherches dans un annuaire LDAP sur un serveur LDAP au lieu d'utiliser une base de données d'utilisateurs locale. Le module IMM2 peut authentifier à distance les accès utilisateurs via un serveur LDAP central. Vous pouvez 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 IMM2 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 IMM2 peut être associé à un ou plusieurs groupes et l'utilisateur ne passerait l'authentification de groupe que s'il appartient au moins à un groupe associé à l'IMM2.

La figure suivante présente l'onglet LDAP.




Pour utiliser un serveur LDAP préconfiguré, complétez les zones suivantes :

**LDAP server configuration item list**

Sélectionnez **Use Pre-Configured LDAP Server** dans la liste des éléments. Le numéro de port de chaque serveur est facultatif. Si cette zone est vide, la valeur par défaut 389 est utilisée pour les connexions LDAP non

sécurisées. Pour les connexions sécurisées, la valeur par défaut est 636. Vous devez configurer au moins un serveur LDAP.

**Root distinguished name**
Il s'agit du nom distinctif (DN) de l'entrée racine de l'arborescence de répertoires sur le serveur LDAP (par exemple, dn=mycompany,dc=com). Ce nom distinctif est utilisé comme objet de base pour toutes les recherches.

**UID search attribute**
Lorsque la méthode de liaison est définie sur **Anonymously** ou **With Configured Credentials**, la liaison initiale vers le serveur LDAP est suivie d'une demande de recherche qui extrait des informations spécifiques sur l'utilisateur, y compris son nom distinctif, ses droits de connexion et son appartenance à un groupe. Cette demande de recherche doit spécifier le nom d'attribut représentant les ID d'utilisateur sur ce serveur. Ce nom d'attribut est configuré dans cette zone. Sur les serveurs Active Directory, le nom d'attribut est normalement **sAMAccountName**. Sur les serveurs Novell eDirectory et OpenLDAP, le nom d'attribut est **uid**. Si cette zone est laissée vide, la valeur par défaut est **uid**.

**Binding method**
Avant de pouvoir effectuer une recherche ou lancer une requête sur le serveur LDAP, vous devez envoyer une demande de liaison. Cette zone contrôle la façon dont cette liaison initiale au serveur LDAP est réalisée. Les méthodes de liaison suivantes sont disponibles :

- Anonymously
  - Utilisez cette méthode pour effectuer une liaison sans nom distinctif ou mot de passe. Cette méthode est fortement déconseillée car la plupart des serveurs sont configurés de sorte à ne pas autoriser les demandes de recherche sur des enregistrements d'utilisateurs spécifiques.
- With Configured Credentials
  - Utilisez cette méthode pour effectuer une liaison avec un nom distinctif ou un mot de passe client configuré.
- With Login Credentials
  - Utilisez cette méthode pour effectuer une liaison avec les données d'identification fournies au cours du processus de connexion. L'ID utilisateur peut être fourni en indiquant une valeur DN (nom distinctif), un nom de domaine complet ou un ID utilisateur correspondant au **UID Search Attribute** configuré sur le module IMM2. Si la liaison initiale réussit, une recherche a lieu pour trouver une entrée sur le serveur LDAP appartenant à l'utilisateur qui tente de se connecter. Si nécessaire, une seconde tentative de liaison a lieu, cette fois avec le nom distinctif récupéré de l'enregistrement LDAP de l'utilisateur et le mot de passe entré pendant le processus de connexion. Si l'opération échoue, le système refuse l'accès à l'utilisateur. La seconde liaison est effectuée uniquement lorsque les méthodes de liaison **Anonymous** (anonyme) ou **With Configured Credentials** (avec données d'identification configurées) sont utilisées.

**Group Filter**
La zone **Group Filter** est utilisée pour l'authentification des groupes. L'authentification de groupe est tentée une fois que la vérification des données d'identification de l'utilisateur a été réalisée avec succès. Si l'authentification de groupe échoue, la tentative de connexion de

l'utilisateur est refusée. Lorsque le filtre de groupe est configuré, il est utilisé pour spécifier à quels groupes le processeur de service appartient. Cela signifie que l'utilisateur doit appartenir au moins à l'un des groupes configurés pour que l'authentification de groupe réussisse. Si la zone **Group Filter** est laissée vide, l'authentification de groupe réussit automatiquement. Si le filtre de groupe est configuré, le système vérifie si au moins un groupe de la liste correspond à l'un des groupes auxquels l'utilisateur appartient. 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 réussit.

Les comparaisons sont sensibles à la casse. Le filtre est limité à 511 caractères et peut comprendre un ou plusieurs noms de groupe. Le signe deux-points (:) doit être utilisé pour délimiter 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. Une option offre la possibilité d'autoriser ou non l'utilisation de caractères génériques. Le filtre peut être un nom de groupe spécifique (par exemple, IMMWest), un astérisque (*) utilisé en tant que caractère générique pour remplacer n'importe quel caractère, ou un caractère accompagné d'un préfixe (par exemple, IMM*). Le filtre par défaut est IMM*. Si les règles de sécurité de votre installation interdissent l'utilisation de caractères génériques, vous pouvez choisir de ne pas autoriser leur utilisation. Le caractère générique (*) est alors considéré comme un caractère normal et non comme un caractère générique. 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 adminGroup.

Dans les environnements Active Directory uniquement, l'appartenance à un groupe imbriqué est prise en charge. Par exemple, si un utilisateur est membre de GroupA et GroupB, et que GroupA est également membre de GroupC, l'utilisateur est considéré comme étant également membre de GroupC. Les recherches imbriquées s'arrêtent lorsque 128 groupes ont été recherchés. Les groupes d'un niveau sont recherchés avant les groupes appartenant à un niveau inférieur. Les boucles ne sont pas détectées.

**Group Search Attribute**

Dans un environnement Active Directory ou Novell eDirectory, la zone **Group Search Attribute** spécifie le nom d'attribut utilisé pour identifier les groupes auxquels un utilisateur appartient. Dans un environnement Active Directory, le nom d'attribut est **memberOf**. Dans un environnement eDirectory, le nom d'attribut est **groupMembership**. Dans un environnement de serveur OpenLDAP, les utilisateurs sont généralement affectés aux groupes pour lesquels objectClass correspond à PosixGroup. Dans ce contexte, cette zone spécifie le nom d'attribut utilisé pour identifier les membres d'un groupe PosixGroup particulier. Ce nom d'attribut est **memberUid**. Si cette zone est laissée vide, le nom d'attribut du filtre correspond par défaut à **memberOf**.

**Login Permission Attribute**

Lorsqu'un utilisateur s'authentifie avec succès à travers un serveur LDAP, les droits de connexion de l'utilisateur doivent être récupérés. Pour récupérer les droits de connexion, le filtre de recherche envoyé au serveur doit indiquer le nom d'attribut associé aux droits de connexion. La zone **Login Permission Attribute** indique le nom d'attribut. Si cette zone est laissée vide, l'utilisateur obtient les droits de lecture seule par défaut, dans la mesure où l'authentification de groupe et d'utilisateur a réussi.

La valeur d'attribut renvoyée par le serveur LDAP recherche la chaîne de mot clé IBMRBSPermissions=. Cette chaîne de mot clé doit être immédiatement suivie d'une chaîne de bits correspondant à 12 occurrences consécutives du chiffre 0 ou du chiffre 1. Chaque bit représente un ensemble 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. Si une position de bit a la valeur 1, la fonction associée à cette position de bit est activée. Si une position de bit a la valeur 0, la fonction associée à cette position de bit est désactivée.

La chaîne IBMRBSPermissions=010000000000 est un exemple valide. Le mot clé IBMRBSPermissions= est utilisé pour être placé à n'importe quel endroit dans cette zone. Ceci permet à l'administrateur LDAP de réutiliser un attribut existant, évitant ainsi une extension du schéma LDAP. Cela permet également d'utiliser l'attribut pour sa fonction initiale. Vous pouvez ajouter la chaîne de mot clé n'importe où dans cette zone. L'attribut utilisé permet une chaîne au format libre. Lorsque l'attribut est récupéré avec succès, la valeur renvoyée par le serveur LDAP est interprétée conformément à l'information du tableau suivant.

*Tableau 4. Bits d'autorisation*

| **Position de bit** | **Fonction** | **Signification** |
|---|---|---|
| 0 | Deny Always | L'authentification de l'utilisateur échoue toujours. Cette fonction peut être utilisée pour bloquer un ou plusieurs utilisateurs associés à un groupe spécifique. |
| 1 | Supervisor Access | L'utilisateur obtient les privilèges d'administrateur. Il 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 | Read Only Access | 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) ni effectuer de modifications (par exemple, les fonctions de sauvegarde, suppression ou 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 | Networking and Security | L'utilisateur peut modifier la configuration des pages Security, Network Protocols, Network Interface, Port Assignments et Serial Port. |
| 4 | User Account Management | L'utilisateur peut ajouter, modifier ou supprimer des utilisateurs et modifier les paramètres de connexion globaux (Global Login Settings) dans la fenêtre Login Profiles. |

*Tableau 4. Bits d'autorisation (suite)*

| Position de bit | Fonction | Signification |
|---|---|---|
| 5 | Remote Console Access | L'utilisateur peut accéder à la console du serveur distant. |
| 6 | Remote Console and Remote Disk Access | L'utilisateur peut accéder à la console du serveur distant et aux fonctions de disque distant du serveur distant. |
| 7 | Remote Server Power/Restart Access | L'utilisateur peut accéder aux fonctions de mise sous tension et de redémarrage du serveur distant. |
| 8 | Basic Adapter Configuration | L'utilisateur peut modifier les paramètres de configuration dans les fenêtres System Settings et Alerts. |
| 9 | Ability to Clear Event Logs | L'utilisateur peut effacer les journaux d'événements.<br>**Remarque :** Tous les utilisateurs peuvent afficher les journaux des événements mais ce niveau d'autorisation est requis pour pouvoir effacer leur contenu. |
| 10 | Advanced Adapter Configuration | L'utilisateur n'est soumis à aucune restriction lorsqu'il configure le module IMM2. De plus, il possède les droits d'accès administrateur au module IMM2. L'utilisateur peut exécuter les fonctions avancées suivantes : mises à jour de microprogramme, amorçage réseau PXE, restauration des paramètres usine par défaut de l'IMM2, modification et restauration de la configuration de l'adaptateur depuis un fichier de configuration et redémarrage/réinitialisation de l'IMM2. |

*Tableau 4. Bits d'autorisation (suite)*

| Position de bit | Fonction | Signification |
|---|---|---|
| 11 | Reserved | Cette position de bit est réservée pour un usage ultérieur. Si aucun bit n'est défini, l'utilisateur obtient les droits de lecture seule. Le système donne la priorité aux droits de connexion récupérés directement de l'enregistrement utilisateur.<br><br>Si l'attribut d'autorisation de connexion ne figure pas dans l'enregistrement utilisateur, le système tente de récupérer les droits des groupes auxquels l'utilisateur appartient. Ceci fait partie de la phase d'authentification de groupe. L'utilisateur reçoit l'opérateur inclusif OR de tous les bits pour tous les groupes.<br><br>Le bit Read Only Access (position 2) est uniquement défini si tous les autres bits sont définis sur zéro. Si le bit Deny Always (position 0) est défini pour l'un des groupes, l'accès est refusé à l'utilisateur. Le bit Deny Always (position 0) prévaut toujours sur les autres. |

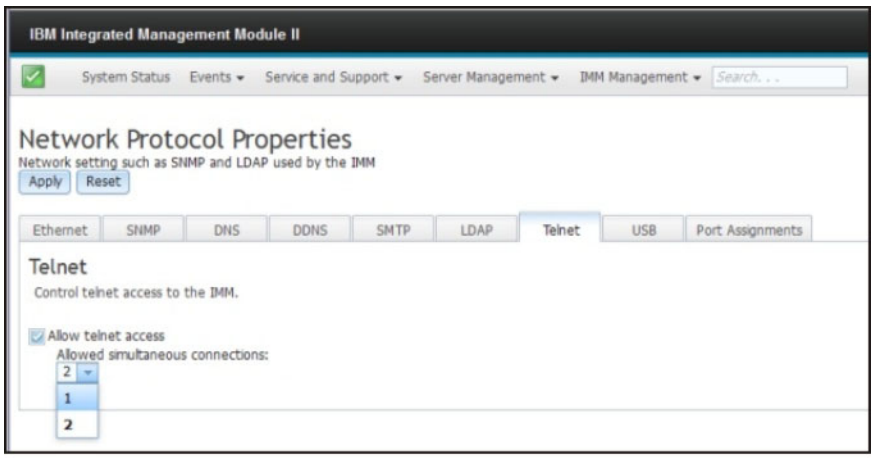
## Configuration de Telnet

Sélectionnez l'onglet **Telnet** pour afficher ou modifier les paramètres Telnet du module IMM2. Remplissez les zones suivantes pour afficher ou modifier les paramètres Telnet :

**Allow telnet access**
Cochez la case si vous souhaitez que le module IMM2 autorise l'accès Telnet.

**Allowed simultaneous connections**
Utilisez la liste **Allowed simultaneous connections** pour sélectionner le nombre de connexions Telnet simultanées autorisées.

La figure suivante présente l'onglet Telnet.

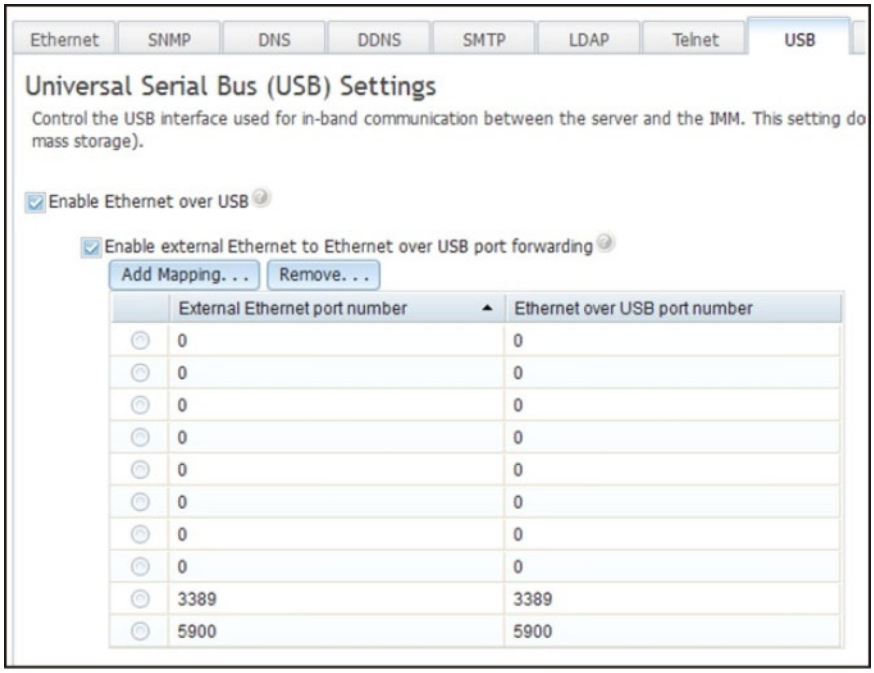



## Configuration USB

Sélectionnez l'onglet **USB** pour afficher ou modifier les paramètres USB du module IMM2. L'interface USB intrabande, ou LAN via USB, est utilisée pour les communications intrabande avec IMM2. Cliquez sur la case **Enable Ethernet over USB** pour activer ou désactiver l'interface LAN via USB du module IMM2.

**Important :** Si vous désactivez l'interface USB intrabande, vous ne pouvez plus effectuer une mise à jour intrabande du microprogramme IMM2, du microprogramme du serveur ou DSA à l'aide des utilitaires de flashage de Linux ou Windows. Si l'interface USB intrabande est désactivée, utilisez l'option Firmware Server sous l'onglet Server Management pour mettre à jour le microprogramme. Si vous désactivez l'interface USB intrabande, désactivez également les délais d'attente du programme de surveillance pour empêcher des redémarrages intempestifs du serveur.

La figure suivante présente l'onglet USB.



Le mappage de numéros de port Ethernet externes vers des numéros de port Ethernet via USB s'effectue en cliquant sur la case à cocher **Enable external Ethernet to Ethernet over USB port forwarding** et en complétant les données de mappage pour les ports que vous souhaitez réacheminer.

## Configuration des affectations de ports

Sélectionnez l'onglet **Port Assignments** pour afficher ou modifier les affectations de port du module IMM2. Renseignez les zones suivantes pour afficher ou modifier les affectations de ports :

**HTTP** Dans cette zone, indiquez le numéro de port du serveur HTTP du module IMM2. La valeur par défaut est 80. Les valeurs valides pour le numéro de port sont comprises entre 1 et 65535.

**HTTPS**
Dans cette zone, spécifiez le numéro de port utilisé pour le trafic HTTPS Secure Sockets Layer (SSL) de l'interface Web. Valeur par défaut : 443. Les valeurs valides pour le numéro de port sont comprises entre 1 et 65535.

**CLI Telnet**
Dans cette zone, spécifiez le numéro de port sur lequel l'interface CLI antérieure se connecte à travers le service Telnet. Valeur par défaut : 23. Les valeurs valides pour le numéro de port sont comprises entre 1 et 65535.

**SSH Legacy CLI**
Dans cette zone, spécifiez le numéro de port configuré pour que l'interface CLI antérieure se connecte à travers le protocole SSH. La valeur par défaut est 22.

**SNMP Agent**
Dans cette zone, spécifiez le numéro de port pour l'agent SNMP s'exécutant sur le module IMM2. Valeur par défaut : 161. Les valeurs valides pour le numéro de port sont comprises entre 1 et 65535.

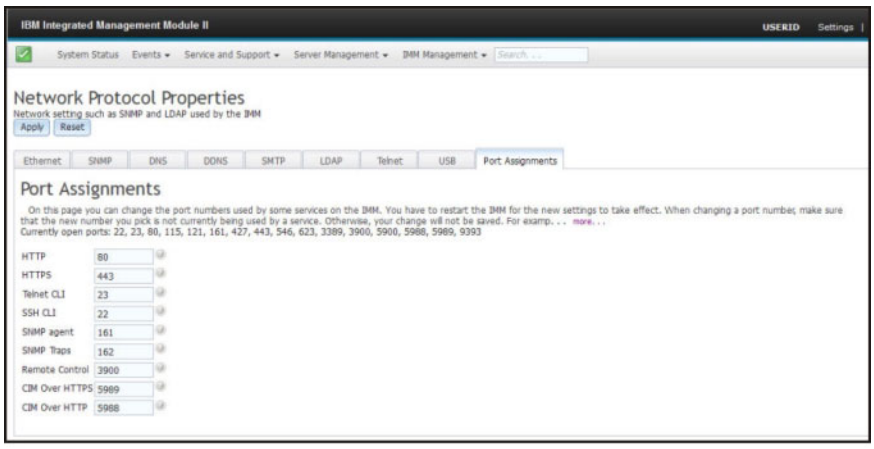
**SNMP Traps**
Dans cette zone, spécifiez le numéro de port utilisé pour les alertes SNMP. Valeur par défaut : 162. Les valeurs valides pour le numéro de port sont comprises entre 1 et 65535.

**Remote Control**
Dans cette zone, spécifiez le numéro de port utilisé par la fonction de contrôle à distance pour afficher et interagir avec la console du serveur. La valeur par défaut est 3900 pour les serveurs montés en armoire et en tour.

**CIM via HTTP**
Dans cette zone, spécifiez le numéro de port pour CIM via HTTP. La valeur par défaut est 5988.

**CIM via HTTPS**
Dans cette zone, spécifiez le numéro de port pour CIM via HTTPS. La valeur par défaut est 5989.

La figure suivante présente l'onglet Port Assignments.




## Configuration des paramètres de sécurité

Cliquez sur l'option **Security** dans l'onglet IMM Management (comme illustré ci-après) pour accéder aux paramètres, état et propriétés de sécurité de votre IMM2 et les configurer.

Pour appliquer vos modifications, cliquez sur le bouton **Apply** dans la partie supérieure gauche de la fenêtre IMM Security. Pour réinitialiser toutes les modifications, cliquez sur le bouton **Reset Values**.

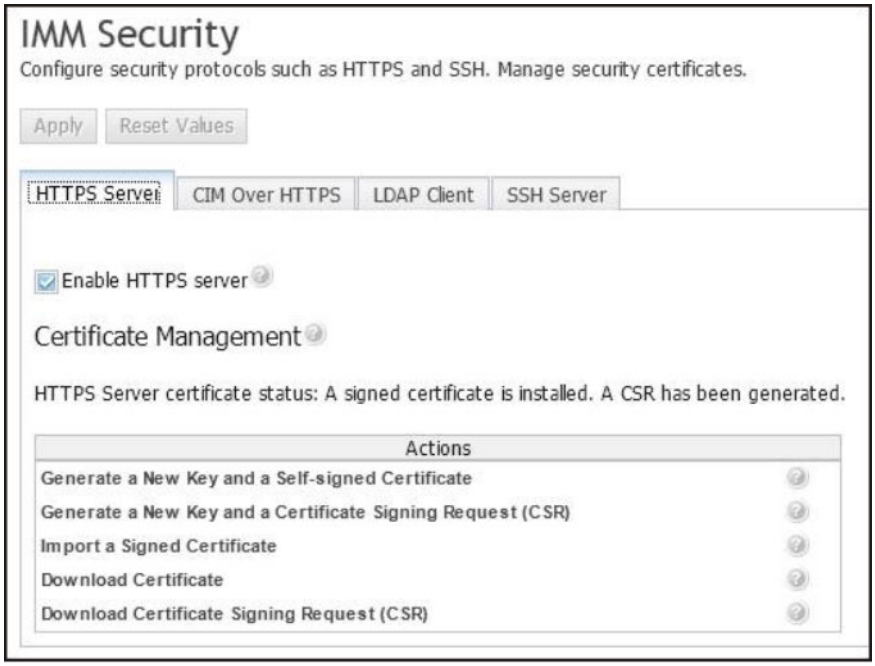

## Configuration du protocole HTTPS

Cliquez sur l'onglet **HTTPS Server** pour configurer l'interface Web IMM2 pour utiliser le protocole HTTPS, plus sécurisé que le protocole HTTP par défaut.

**Remarques :**

- Un seul protocole peut être activé à la fois.
- L'activation de cette option requiert la configuration supplémentaire des certificats SSL.
- Lorsque vous modifiez des protocoles, vous devez redémarrer le serveur Web IMM2.

Pour plus d'information sur SSL, voir «Présentation de SSL», à la page 87. La figure suivante présente l'onglet HTTPS Server.




**Remarque :** Sur certains serveurs, les niveaux de sécurité IMM2 peuvent être contrôlés par un autre système de gestion. Dans de tels environnements, vous pouvez désactiver les actions ci-dessus dans l'interface Web IMM2.

### Traitement des certificats HTTPS

Utilisez les options du menu Actions pour le traitement des certificats HTTPS. Si une option est désactivée, il sera éventuellement nécessaire de réaliser d'abord une autre action pour l'activer. Lorsque vous travaillez avec des certificats HTTPS, il est recommandé de désactiver le serveur HTTPS. Pour plus d'information sur le traitement des certificats, voir «Traitement des certificats SSL», à la page 87.

**Remarque :** Une fois la configuration du traitement des certificats terminée, redémarrez le IMM2 pour que vos modifications prennent effet.

## Configuration du CIM via le protocole HTTPS

Cliquez sur l'onglet **CIM over HTTPS** pour configurer l'interface Web IMM2 afin d'utiliser le CIM via le protocole HTTPS, plus sécurisé que le CIM via le protocole HTTP activé par défaut.

**Remarques :**

- Un seul protocole peut être activé à la fois.

- L'activation de cette option requiert la configuration supplémentaire des certificats SSL.
- Lorsque vous modifiez des protocoles, vous devez redémarrer le serveur Web IMM2.

Pour plus d'information sur SSL, voir «Présentation de SSL», à la page 87. La figure suivante présente l'onglet CIM over HTTPS.


### Traitement des certificats du CIM via le protocole HTTPS

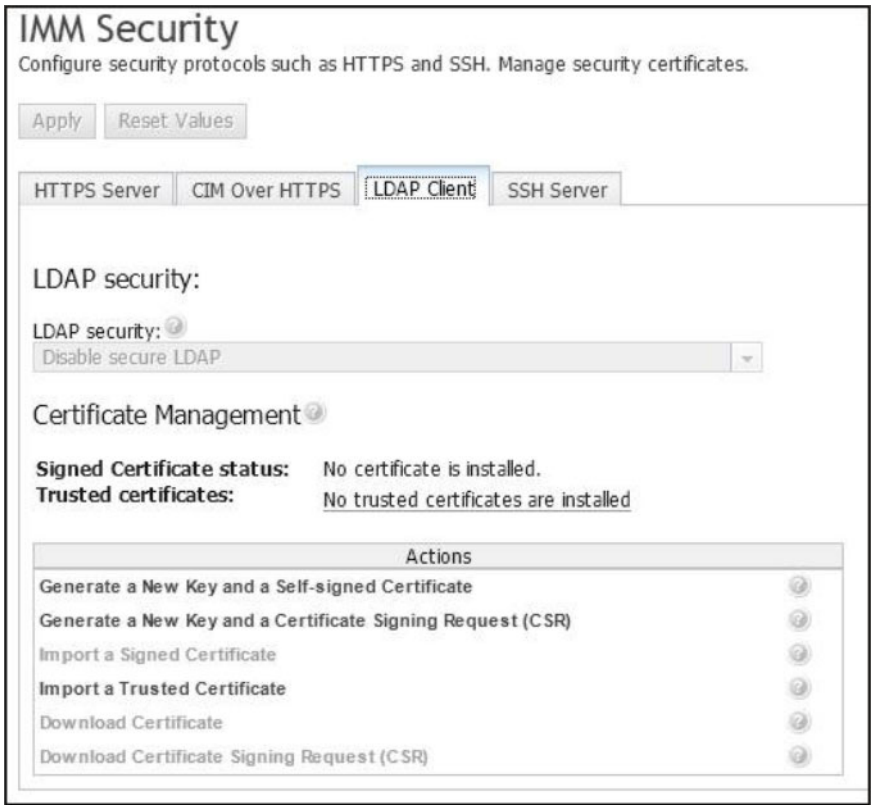
Utilisez les options du menu Actions pour le traitement des certificats CIM via HTTPS. Si une option est désactivée, il sera éventuellement nécessaire de réaliser d'abord une autre action pour l'activer. Pour plus d'information sur le traitement des certificats, voir «Traitement des certificats SSL», à la page 87.

**Remarque :** Une fois la configuration du traitement des certificats terminée, redémarrez le IMM2 pour que vos modifications prennent effet.

## Configuration du protocole client LDAP

Cliquez sur l'option **LDAP Client** pour utiliser le protocole LDAP sur SSL, plus sécurisé que le protocole LDAP par défaut.

**Remarque :** L'activation de cette option requiert la configuration supplémentaire des certificats SSL.
Pour plus d'information sur SSL, voir «Présentation de SSL», à la page 87. La figure ci-après présente l'onglet LDAP Client.

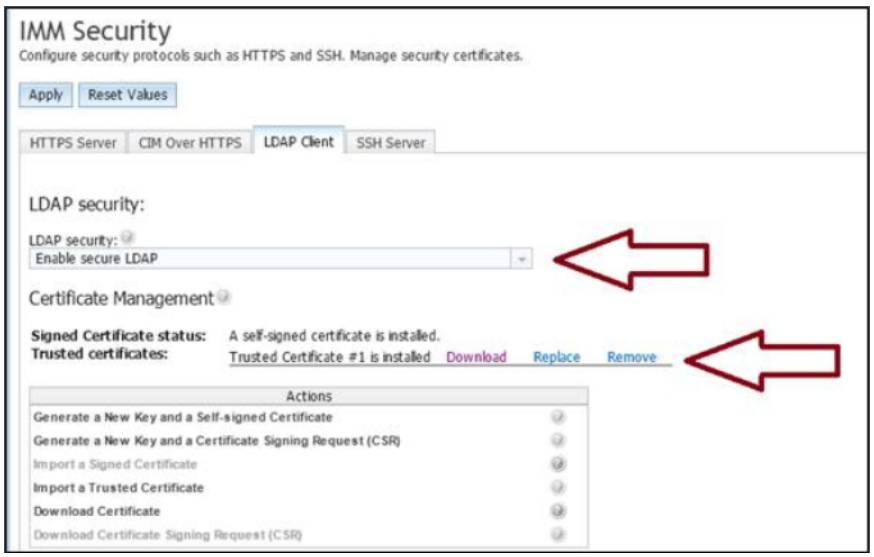



## Traitement des certificats clients LDAP sécurisés

Utilisez les options du menu Actions pour le traitement des certificats LDAP sur SSL. Si une option est désactivée, il sera éventuellement nécessaire de réaliser d'abord une autre action pour l'activer. Lors de la manipulation des certificats HTTPS, vous devez désactiver le serveur HTTPS. Pour plus d'information sur le traitement des certificats, voir «Traitement des certificats SSL», à la page 87. Une fois que vous avez installé le certificat sécurisé, vous pouvez activer le protocole LDAP sur SSL comme indiqué dans la figure suivante.

**Remarques :**

- Les modifications apportées à votre IMM2 prendront effet immédiatement.
- Votre serveur LDAP doit prendre en charge Secure Socket Layer 3 (SSL3) ou Transport Layer security (TLS) pour être compatible avec le client LDAP sécurisé IMM2.




## Configuration du serveur Secure Shell

Cliquez sur l'onglet **SSH Server** pour configurer l'interface Web IMM2 pour utiliser le protocole SSH plus sécurisé, plutôt que le protocole Telnet par défaut.

**Remarque :**

- Aucune gestion de certificat n'est requise pour utiliser cette option.
- Le module IMM2 crée initialement une clé de serveur SSH. Si vous souhaitez générer une nouvelle clé de serveur SSH, cliquez sur **Generate SSH Server Private Host Key** dans le menu Actions.
- Une fois l'action terminée, redémarrez le module IMM2 pour que vos modifications prennent effet.

La figure suivante présente l'onglet SSH Server.

## Présentation de SSL

SSL est un protocole de sécurité qui assure la confidentialité des communications. SSL permet aux applications client/serveur de communiquer en empêchant les écoutes, la contrefaçon et la falsification des messages. Vous pouvez configurer IMM2 afin d'utiliser la prise en charge SSL pour différents types de connexions, comme le serveur Web sécurisé (HTTPS), la connexion LDAP sécurisée (LDAPS), CIM via HTTPS et le serveur SSH. Vous pouvez afficher ou modifier les paramètres SSL au moyen de l'option Security située dans l'onglet IMM Management. Vous pouvez également activer ou désactiver SSL et gérer les certificats requis pour SSL.

## Traitement des certificats 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 mineur car 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 Web IMM2 pour intercepter les données échangées entre le serveur Web IMM2 actuel et le navigateur Web de l'utilisateur. Si le certificat autosigné est importé dans le magasin de certificats du navigateur lors de la première connexion entre le navigateur et IMM2, toutes les communications futures avec le navigateur seront sécurisées (sous réserve que la première connexion n'a pas été compromise par une attaque).

Pour un sécurité accrue, vous pouvez utiliser un certificat signé par une autorité de certification (CA). Pour obtenir un certificat signé, cliquez sur **Generate a New Key and a Certificate Signing Request (CSR)** dans le menu Actions. Vous devez ensuite envoyer cette demande de signature de certificat (CSR) à une autorité de certification et convenir avec celle-ci de la délivrance d'un certificat final. Après réception du certificat final, cliquez sur **Import a Signed Certificate** dans le menu Actions pour importer le certificat dans IMM2.

La fonction de l'autorité de certification est de vérifier l'identité du module IMM2. Le certificat contient les signatures numériques de l'autorité de certification et du module IMM2. 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 IMM2.

Le module IMM2 requiert un certificat pour son utilisation avec le serveur HTTPS, CIM via HTTPS et le client LDAP sécurisé. De même, le client LDAP sécurisé a besoin d'importer 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 des certificats SSL

Lors de la gestion des certificats IMM2, une liste d'actions (ou un sous-ensemble de celles-ci) vous est présentée (comme illustré ci-après).


Si un certificat est déjà installé, vous pourrez utiliser l'action **Download Certificate** dans le menu Actions pour télécharger le certificat actuellement installé ou la demande de signature de certificat (CSR). Les certificats qui sont grisés ne sont *pas* actuellement installés. Le client LDAP sécurisé requiert l'importation d'un certificat sécurisé par l'utilisateur. Cliquez sur **Import a Trusted Certificate** dans le menu Actions. Après la génération d'une CSR, cliquez sur **Import a Signed Certificate** dans le menu Actions.

Lorsque l'une des actions "Generate" est exécutée, la fenêtre Generate New Key and Self-signed Certificate s'ouvre (comme illustré ci-après).


La fenêtre Generate New Key and Self-signed Certificate vous demande de compléter les zones obligatoires et facultatives. Les zones obligatoires *doivent impérativement* être renseignées. Une fois que vous avez entré l'information, cliquez sur **OK** pour terminer la tâche. La fenêtre Certificate Generated s'ouvre (comme illustré ci-après).


## Restauration et modification de votre configuration IMM

Sélectionnez l'option **IMM Configuration** dans l'onglet IMM Management pour que les options exécutent les actions suivantes :

- Afficher un récapitulatif de configuration du module IMM2
- Sauvegarder ou restaurer la configuration du module IMM2
- Afficher l'état de sauvegarde et de restauration
- Restaurer la configuration du module IMM2 à ses paramètres usine par défaut
- Accès à l'assistant de configuration initiale du module IMM2

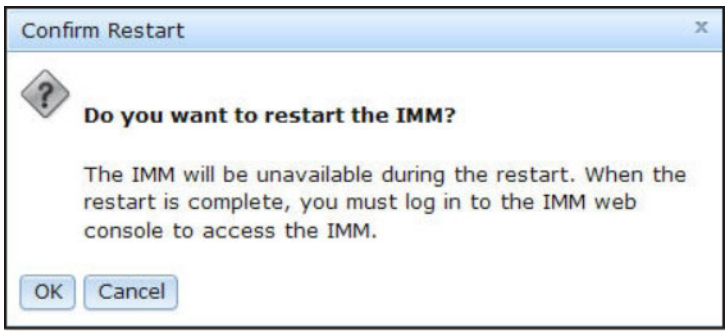
## Redémarrage du module IMM2

Sélectionnez l'option **Restart IMM** dans l'onglet IMM Management pour redémarrer le module IMM2. Seules les personnes possédant les droits de superviseur sont autorisées à exécuter cette fonction. Lorsque les connexions Ethernet sont temporairement supprimées, vous devez vous connecter au module IMM2 pour accéder à l'interface Web IMM2.

Pour redémarrer le module IMM2, procédez comme suit.

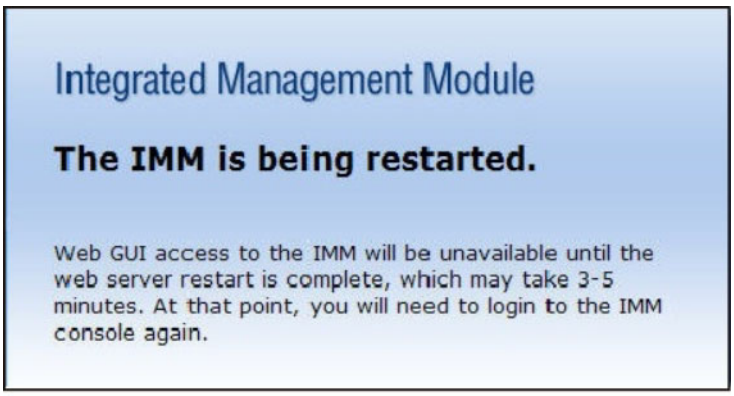
1. Connectez-vous au module IMM2. Pour plus d'informations, voir «Connexion au module IMM2», à la page 10.
2. Cliquez sur l'onglet **IMM Management** puis cliquez sur **Restart IMM**.
3. Cliquez sur le bouton **OK** dans la fenêtre Confirm Restart. Le module IMM2 sera redémarré.

   La figure ci-après présente la fenêtre Confirm Restart.




   Lorsque vous redémarrez le module IMM2, vos connexions TCP/IP ou modem sont coupées.

   La figure suivante présente la fenêtre de notification qui s'affiche lorsque le module IMM2 est redémarré.




4. Connectez-vous à nouveau pour utiliser l'interface Web IMM2 (voir «Connexion au module IMM2», à la page 10 pour obtenir des instructions).

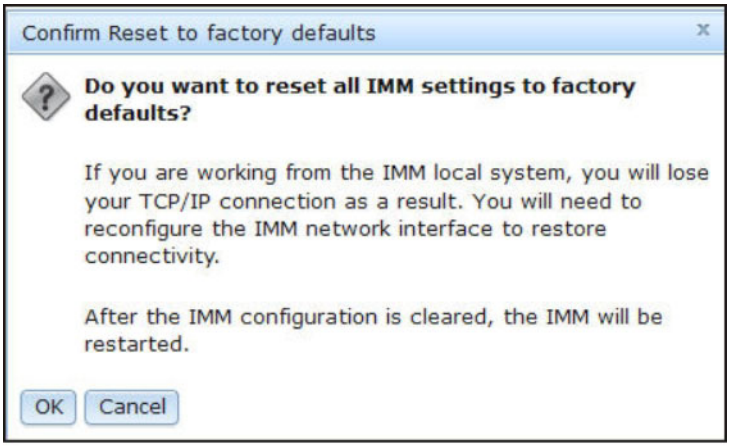
## Réinitialisation du module IMM2 aux paramètres usine par défaut

Sélectionnez l'option **Reset IMM to factory defaults...** dans l'onglet IMM Management pour restaurer les paramètres usine par défaut du module IMM2. Seules les personnes possédant les droits de superviseur sont autorisées à effectuer cette fonction. Lorsque les connexions Ethernet sont temporairement supprimées, vous devez vous connecter au module IMM2 pour accéder à l'interface Web IMM2.

**Avertissement :** Lorsque vous utilisez l'option Reset IMM to factory defaults, vous perdez toutes les modifications effectuées sur le module IMM2.

Pour restaurer les paramètres usine par défaut du module IMM2, procédez comme suit.

1. Connectez-vous au module IMM2. Pour plus d'informations, voir «Connexion au module IMM2», à la page 10.
2. Cliquez sur l'onglet **IMM Management** puis sur **IMM Reset to factory defaults...**.
3. Cliquez sur le bouton **OK** dans la fenêtre Confirm Reset to factory defaults (comme illustré ci-après).




**Remarque :** Une fois sa configuration terminée, le module IMM2 est redémarré. 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.

4. Connectez-vous à nouveau au module IMM2 pour utiliser l'interface Web IMM2 (voir «Connexion au module IMM2», à la page 10 pour obtenir des instructions).
5. Reconfigurez l'interface réseau pour restaurer la connectivité.

## Clé de gestion de l'activation

Cliquez sur l'option **Activation Key Management** dans l'onglet IMM Management pour gérer les clés d'activation pour les dispositifs en option Features on Demand (FoD) du serveur ou du module IMM2. Pour plus d'informations sur la gestion des clés d'activation FoD, voir Chapitre 7, «Features on Demand», à la page 137.

# Chapitre 5. Surveillance de l'état du serveur

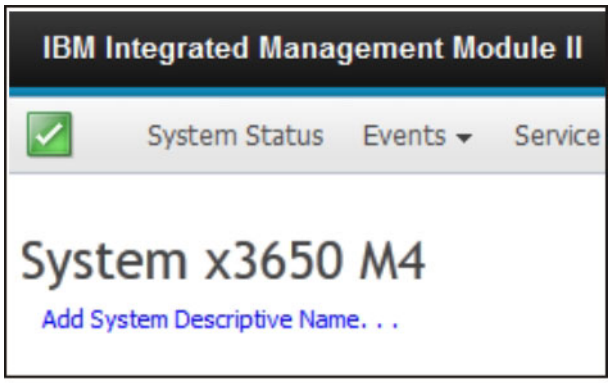
Ce chapitre fournit des informations sur la manière d'afficher et de contrôler les informations sur le serveur auquel vous accédez.

## Affichage de l'état du système

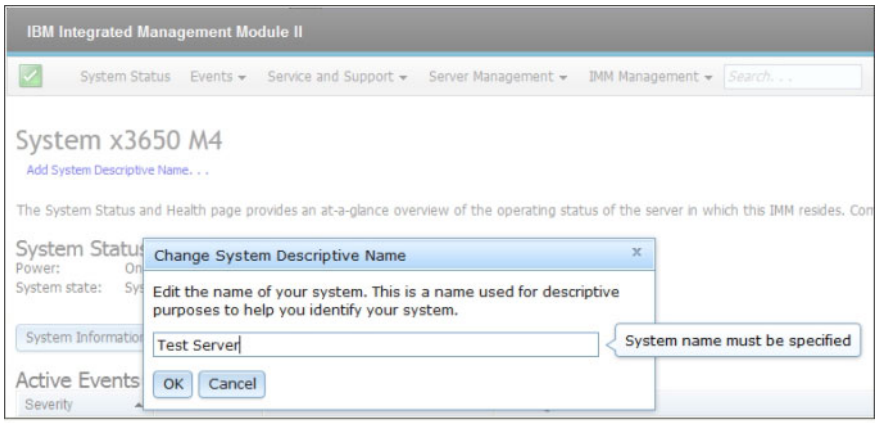
La page System Status offre un aperçu de l'état de fonctionnement du serveur IMM2. Cette page affiche également l'état de santé du matériel et tous les événements actifs se produisant sur le serveur.

**Remarque :** Si vous accédez à une autre page à partir de la page System Status, vous pouvez retourner à la page System Status en cliquant sur **System Status** dans les éléments de menu situés en haut de la page.

Vous pouvez ajouter un nom descriptif au module IMM2 pour mieux distinguer les différents modules IMM2. Cliquez sur le lien **Add System Descriptive Name...** situé au-dessous du nom de produit du serveur pour désigner un nom à associer au module IMM2 (comme illustré ci-après).

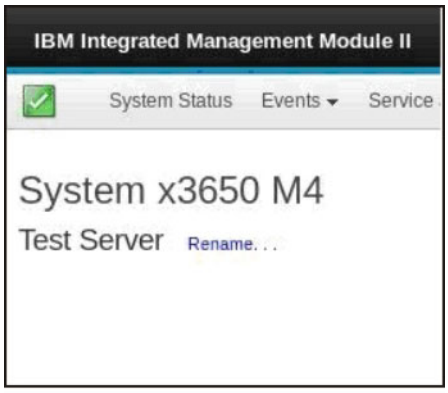



Dans la fenêtre Change System Descriptive Name, indiquez un nom à associer au module IMM2 (comme illustré ci-après).



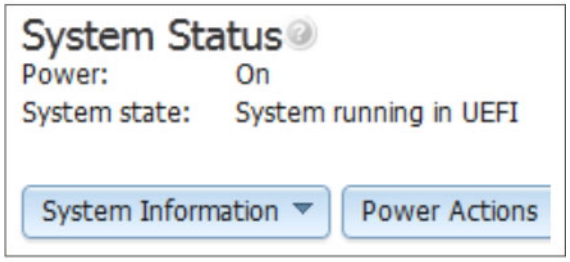
Vous pouvez renommer le nom descriptif du système en cliquant sur le lien **Rename...** situé à côté du nom descriptif du système.

La figure suivante montre le lien Rename.




La page System Status affiche l'état d'alimentation et l'état de fonctionnement du serveur. L'état affiché correspond à l'état du serveur au moment où la page System Status est ouverte.

La figure suivante présente les zones **Power** et **System state**.




Le serveur peut se trouver dans l'un des états de système listés dans le tableau suivant.

*Tableau 5. Descriptions des états de système*

| Etat | Description |
|---|---|
| System power off/State unknown (Système hors tension/Etat inconnu) | Le serveur est hors tension. |
| System on/starting UEFI (Système sous tension/démarrage UEFI) | Le serveur est sous tension mais UEFI n'est pas en cours d'exécution. |
| System running in UEFI (Système en cours d'exécution dans UEFI) | Le serveur est sous tension et UEFI est en cours d'exécution. |
| System stopped in UEFI (Arrêt du système dans UEFI) | Le serveur est sous tension ; UEFI a détecté un problème et a été arrêté en cours d'exécution. |

*Tableau 5. Descriptions des états de système (suite)*

| Etat | Description |
|---|---|
| Booting OS or in unsupported OS (Système d'exploitation en cours d'amorçage ou non pris en charge) | Le serveur peut se trouver dans cet état pour l'une des raisons suivantes :<br>• Le chargeur du système d'exploitation (OS) a démarré mais le système d'exploitation n'est pas en cours d'exécution<br>• L'interface Ethernet via USB du module IMM2 est désactivée.<br>• Le système d'exploitation n'a pas chargé les pilotes prenant en charge l'interface Ethernet via USB. |
| OS booted (Système d'exploitation démarré) | Le système d'exploitation du serveur est en cours d'exécution. |
| Suspend to RAM (Interrompre en mémoire RAM) | Le serveur a été placé en mode de secours ou en mode veille. |

Les options de menu suivantes de la page System Status fournissent des informations supplémentaires sur le serveur et une liste d'actions pouvant être effectuées sur le serveur.

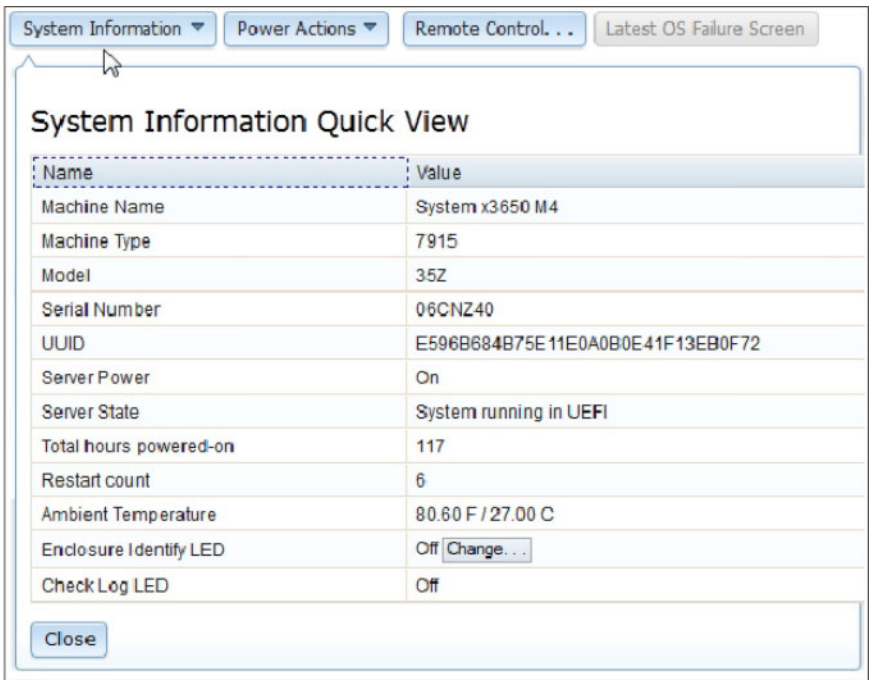
- System Information
- Power Actions
- Remote Control (pour plus d'informations, voir «Fonctions d'intervention et de contrôle à distance», à la page 103).
- Latest OS Failure Screen (pour plus d'informations, voir «Capture des données d'écran du dernier échec du système d'exploitation», à la page 130).

## Affichage des informations système

Le menu System Information offre un récapitulatif des informations serveur communes. Cliquez sur l'onglet **System Information** dans la fenêtre System Status pour afficher les informations suivantes :

- Machine name (nom de machine)
- Machine type (type de machine)
- Model (modèle)
- Serial number (numéro de série)
- Universally Unique Identifier (UUID) (Identificateur unique universel)
- Server power (alimentation serveur)
- Server state (état du serveur)
- Total hours powered on (total heures sous tension)
- Restart count (nombre de redémarrage)
- Ambient temperature (température ambiante)
- Enclosure identity LED (voyant d'identité boîtier)
- Check log LED (voyant de vérification de journal)

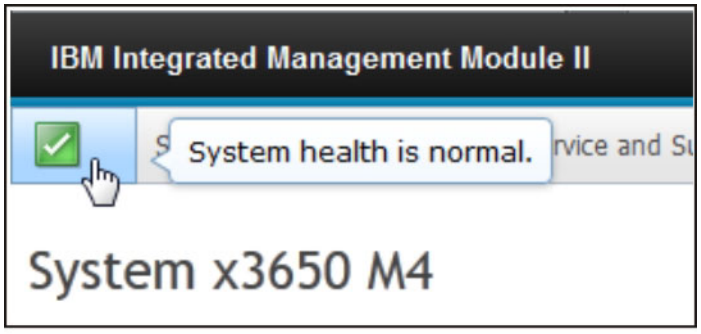
La figure ci-après présente la fenêtre System Information.




## Affichage de l'état de santé du serveur

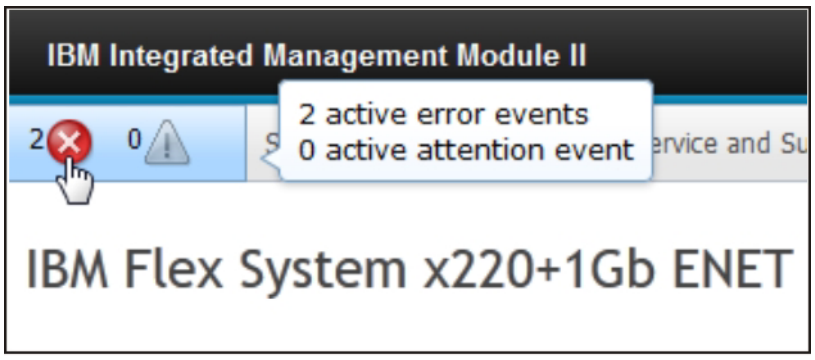
L'état de santé du serveur s'affiche sous forme d'icône dans la barre de titre située dans le coin supérieur gauche de la page System Status. Une coche verte indique que le matériel du serveur fonctionne normalement. Déplacez votre curseur sur la coche verte pour obtenir une indication rapide de l'état de santé du serveur.

La figure suivante montre l'exemple d'un serveur fonctionnant normalement.



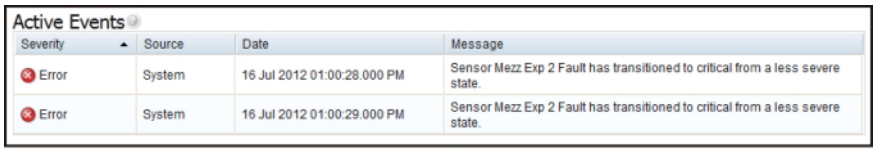

Un triangle jaune indique une condition d'avertissement. Un cercle rouge indique un cas d'erreur.

La figure suivante montre l'exemple d'un serveur présentant des événements d'erreur actifs.




Si une icône d'avertissement (triangle jaune) ou une icône d'erreur (cercle rouge) s'affiche, cliquez sur l'icône pour afficher les événements correspondants dans la section Active Events de la page System Status.

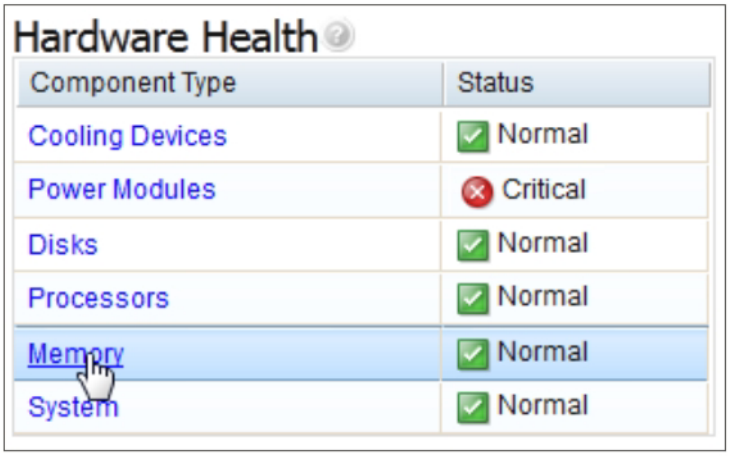
La figure suivante montre un exemple de la section Active Events contenant des cas d'erreurs.




## Affichage de l'état de santé du matériel

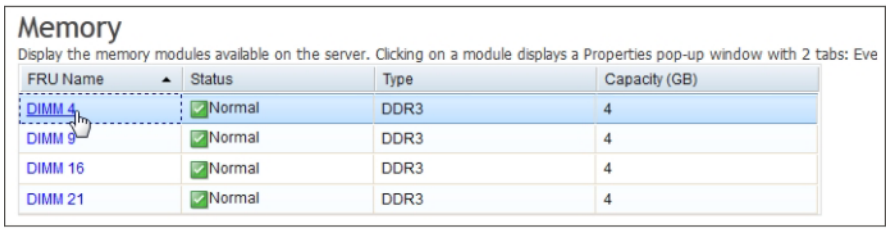
La section Hardware Health de la page System Status offre une liste des composants matériels du serveur et affiche l'état de santé de chaque composant surveillé par le module IMM2. L'état de santé affiché pour un composant peut refléter l'état le plus critique de tous les composants individuels d'un type de composant. Par exemple, un serveur peut avoir plusieurs modules d'alimentation installés et tous les modules fonctionnent normalement sauf un. L'état du composant Modules d'alimentation sera critique à cause du module d'alimentation qui ne fonctionne pas normalement.

La figure suivante montre la section Hardware Health de la page System Status.



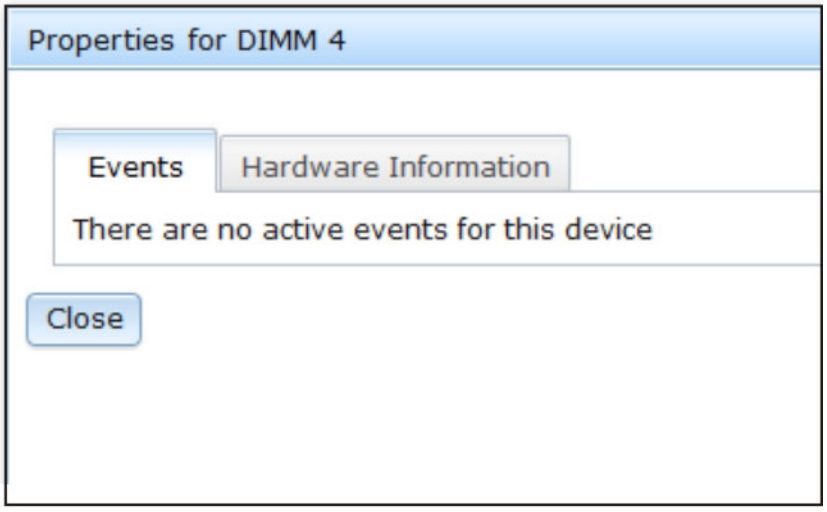
Chaque type de composant s'affiche sous forme de lien sur lequel vous pouvez cliquer pour obtenir des informations plus détaillées. Lorsque vous sélectionnez un type de composant à afficher, une table répertoriant l'état de tous les composants s'affiche pour ce type de composant.

La figure suivante montre les composants du type de composant Memory.



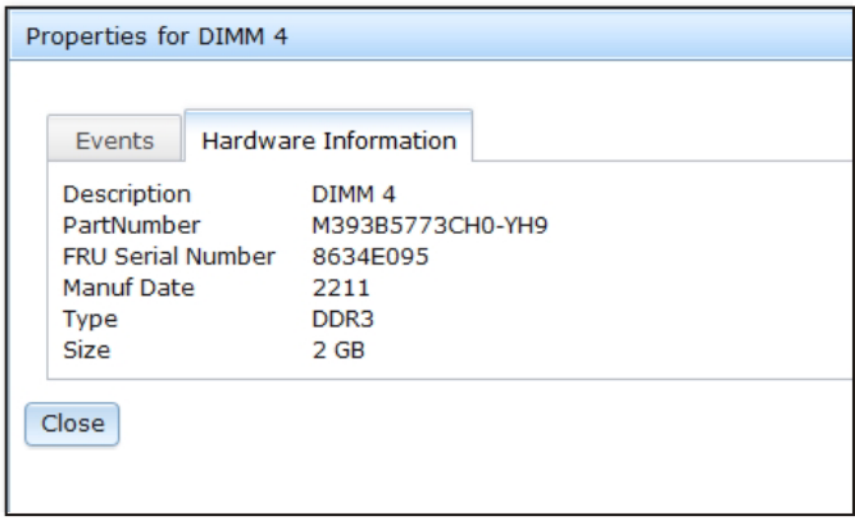

Vous pouvez cliquer sur un lien FRU (unité remplaçable sur site) individuel dans la table pour obtenir des informations supplémentaires sur ce composant. Tous les événements actifs du composant s'affichent alors dans l'onglet Events.

La figure suivante montre l'onglet Events pour DIMM 4.




Le cas échéant, des informations supplémentaires sur le composant peuvent être fournies dans l'onglet Hardware Information.

La figure suivante montre l'onglet Hardware Information pour DIMM 4.


Properties for DIMM 4
Events
Hardware Information
Description DIMM 4
PartNumber M393B5773CH0-YH9
FRU Serial Number 8634E095
Manuf Date 2211
Type DDR3
Size 2 GB
Close

# Chapitre 6. Exécution de tâches IMM2

Vous pouvez utiliser les informations de cette section et du Chapitre 3, «Présentation de l'interface utilisateur Web IMM2», à la page 15 pour exécuter les tâches suivantes permettant de contrôler le module IMM2.

Dans l'onglet System Status, vous pouvez effectuer les tâches suivantes :

- Afficher l'état d'intégrité du serveur
- Afficher l'information sur le serveur, par exemple, le nom, le type et le numéro de série de la machine
- 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
- Afficher les événements actifs
- Afficher l'état d'intégrité matérielle des composants serveur

**Remarque :** La page System Status s'affiche après la connexion à l'IMM2. Cette page contient des actions et informations communes.

Dans l'onglet Events, vous pouvez réaliser les tâches suivantes :

- Gérer l'historique des événements
- Gérer les destinataires d'événements pour les notifications par courrier électronique
- Gérer les destinataires d'événements pour les notifications syslog

Dans l'onglet Services and Support, vous pouvez effectuer les tâches suivantes :

- Obtenir manuellement les données de service de votre serveur

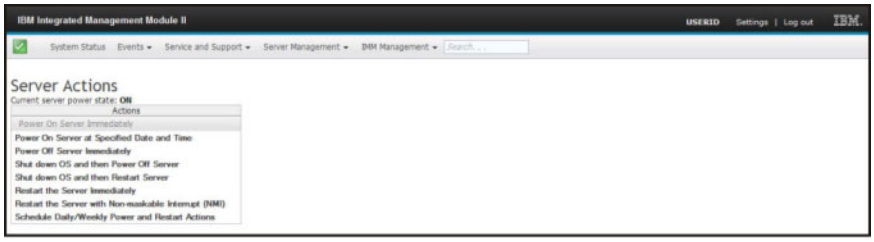
Dans l'onglet Server Management, des options vous permettent d'effectuer les tâches suivantes :

- A partir de l'option Server Firmware, afficher et mettre à jour les niveaux de microprogrammes des composants serveur.
- A partir de l'option Remote Control, afficher à distance la console du serveur et interagir avec elle :
  - Contrôler à distance le statut d'alimentation du serveur
  - Accéder à distance à la console du serveur
  - Affecter à distance une unité de CD, une unité de DVD, une unité de disquette, une clé USB ou une image de disque au serveur
- A partir de l'option Server Properties, vous pouvez définir les paramètres permettant d'aider à identifier le serveur.
- A partir de l'option Server Power Actions, vous pouvez exécuter des actions de mise sous tension, mise hors tension et redémarrage.
- A partir de l'option Disks, vous pouvez afficher les unités de disque dur ainsi que les événements associés aux unités de disque dur installées sur le serveur.
- A partir de l'option Memory, vous pouvez afficher des informations sur les modules de mémoire installés sur le serveur.

- A partir de l'option Processor, vous pouvez afficher des informations sur les microprocesseurs installés sur le serveur.
- A partir de l'option Server Timeouts, vous pouvez définir des délais d'attente afin de s'assurer que le serveur ne se bloque pas indéfiniment lors de la mise à jour d'un microprogramme ou la mise sous tension du serveur.
- A partir de l'option PXE Network Boot, vous pouvez configurer les tentatives d'amorçage préliminaires de l'environnement d'exécution du serveur.
- A partir de l'option Latest OS Failure Screen, vous pouvez capturer les données d'écran d'échec du système d'exploitation et les stocker.
- A partir de l'option Power Management, vous pouvez voir l'utilisation de l'alimentation système et la capacité de l'alimentation électrique, puis définir des paramètres pour l'utilisation de l'alimentation système.

## Contrôle de l'état d'alimentation du serveur

L'option Power Actions contient une liste d'actions que vous pouvez entreprendre pour contrôler l'alimentation du serveur (comme illustré ci-après). Vous pouvez choisir de mettre le serveur sous tension immédiatement ou à une heure planifiée. Vous pouvez également choisir d'arrêter et de redémarrer le système d'exploitation.




Pour effectuer des actions d'alimentation et de redémarrage du serveur, procédez comme suit.

1. Accédez au menu Power Actions en exécutant l'une des étapes suivantes :
   - Cliquez sur l'onglet **Power Actions** dans la page System Status.
   - Cliquez sur **Server Power Actions** dans l'onglet Server Management.
2. Sélectionnez l'action de serveur dans la liste du menu Actions.

La table suivante contient une description des actions d'alimentation et de redémarrage pouvant être réalisées sur le serveur.

*Tableau 6. Actions d'alimentation et descriptions*

| Action d'alimentation | Description |
|---|---|
| Power on server immediately | Sélectionnez cette action pour mettre le serveur sous tension et démarrer le système d'exploitation. |
| Power on server at specified date and time | Sélectionnez cette action pour programmer le serveur afin qu'il se mette sous tension à une date et une heure spécifiques. |
| Power off server immediately | Sélectionnez cette action pour mettre le serveur hors tension sans arrêter le système d'exploitation. |

*Tableau 6. Actions d'alimentation et descriptions (suite)*

| Action d'alimentation | Description |
|---|---|
| Shut down operating system and then power off server [1] | Sélectionnez cette action pour arrêter le système d'exploitation et mettre le serveur hors tension. |
| Shut down operating system and then restart server [1] | Sélectionnez cette action pour redémarrer le système d'exploitation. |
| Restart the server immediately | Sélectionnez cette action pour éteindre et rallumer le serveur immédiatement, sans arrêter le système d'exploitation. |
| Restart the server with non-maskable interrupt (NMI) | Sélectionnez cette action pour forcer une interruption non masquable (NMI) sur un système "bloqué". La sélection de cette action permet au système d'exploitation de la plateforme d'effectuer un vidage de mémoire pouvant être utilisé pour déboguer l'état de blocage du système. Le microprogramme IMM2 utilise le paramètre de redémarrage automatique sur NMI depuis le UEFI F1 du menu Setup pour déterminer si un redémarrage est nécessaire après l'interruption non masquable. |
| Schedule daily/weekly power and restart actions | Sélectionnez cette action pour programmer des actions d'alimentation et de redémarrage quotidiennes et hebdomadaires pour le serveur. |
| 1. Si le système d'exploitation se trouve en mode écran de veille ou en mode de verrouillage lorsqu'une demande "Shut Down" est traitée, il se peut que le module IMM2 ne puisse pas déclencher un arrêt normal. Le module IMM2 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. | |

## Fonctions d'intervention et de contrôle à distance

Vous pouvez utiliser la fonction de contrôle ou d'intervention à distance IMM2 de l'interface Web IMM2 pour afficher la console serveur et interagir avec elle. Vous pouvez affecter au serveur une unité de CD ou de DVD, une unité de disquette, une clé USB ou une image de disque se trouvant sur votre ordinateur. La fonctionnalité d'intervention à distance est proposée avec les fonctionnalités IMM2 Premium et elle est uniquement disponible à travers l'interface Web IMM2. Pour utiliser les fonctions de contrôle à distance, vous devez vous connecter à IMM2 avec un ID disposant d'un accès Superviseur. Pour plus d'informations sur la mise à niveau du module IMM2 de base ou standard à IMM2 Premium, voir «Mise à niveau du module IMM2», à la page 4. Consultez la documentation de votre serveur pour obtenir des informations sur le niveau IMM2 installé sur votre serveur.

Utilisez les fonctionnalités de contrôle à distance pour effectuer les actions suivantes :

- Afficher une vidéo à distance avec une résolution graphique allant jusqu'à 1600 x 1200 à 75 Hz, indépendamment de l'état du serveur.
- Accéder au serveur à distance à l'aide du clavier et de la souris depuis un client distant.

- Mapper l'unité de CD ou DVD, l'unité de disquette et la clé USB sur un client distant et mapper les fichiers d'image ISO et de disquette comme unités virtuelles disponibles pour leur utilisation sur le serveur.
- Télécharger une image de disquette vers la mémoire IMM2 et la mapper sur le serveur comme unité virtuelle.

## Mise à jour de votre microprogramme IMM2 et applet Java ou ActiveX

Cette section offre des informations sur la mise à jour du microprogramme et de l'applet Java et ActiveX.

**Important :** le module IMM2 utilise une applet Java ou une applet ActiveX pour exécuter la fonction d'intervention à distance. Lorsqu'IMM2 est mis à jour vers le niveau du microprogramme le plus récent, 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 IMM2, il se peut que l'applet Java utilisée par le serveur ne soit pas au niveau le plus récent.

Pour corriger ce problème, désactivez la mise en cache. La méthode utilisée dépend de la plateforme et de la version Java. Les étapes suivantes sont pour Oracle Java 1.5 sous Windows :

1. Cliquez sur **Démarrer → Paramètres → Panneau de configuration**.
2. Cliquez deux fois sur **Java Plug-in 1.5**. La fenêtre Java Plug-in Control Panel s'ouvre.
3. Cliquez sur l'onglet **Cache**.
4. Sélectionnez l'une des options suivantes :
   - Désélectionnez 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 sélectionnez cette option, vous devez cliquer sur **Clear Caching** après chaque mise à jour du microprogramme IMM2.

Pour plus d'informations sur la mise à jour du microprogramme IMM2, voir «Mise à jour du microprogramme de serveur», à la page 116.

## Activation de la fonction d'intervention à distance

La fonction d'intervention à distance de IMM2 est uniquement disponible dans la version IMM2 Premium. Pour plus d'informations sur la mise à niveau de module standard vers IMM Premium, voir «Mise à niveau du module IMM2», à la page 4.

Un fois la clé d'activation achetée et récupérée pour la mise à niveau IMM Premium, installez-la (voir «Installation d'une clé d'activation», à la page 137).

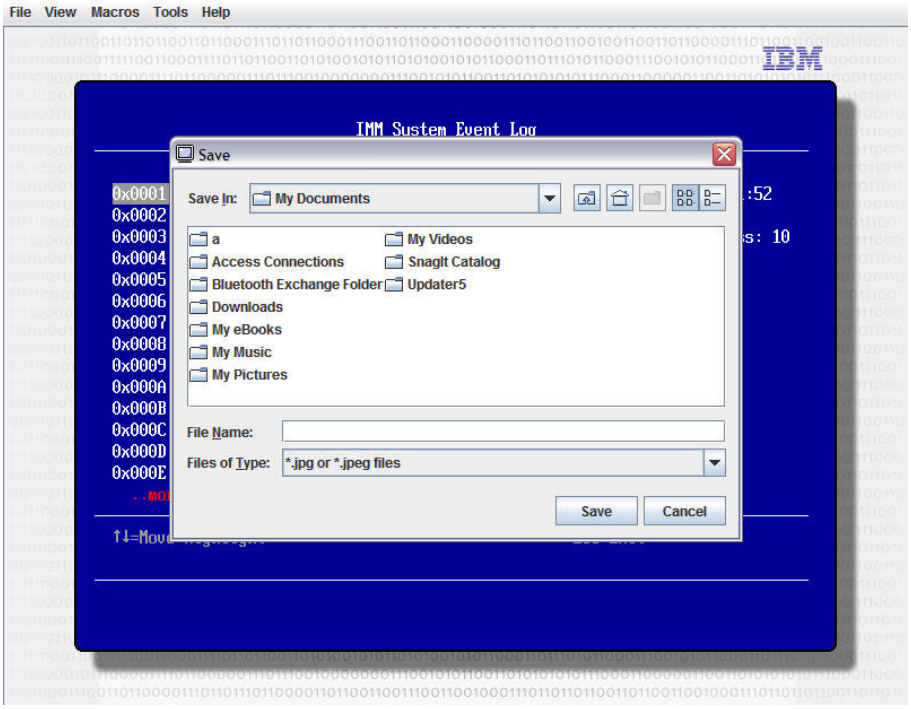
## Capture d'écran par la fonction de contrôle à distance

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 :** Le client Java sauvegarde l'image de capture d'écran sous la forme d'un fichier JPG. Le client ActiveX sauvegarde l'image de capture d'écran sous la forme d'un fichier BMP.

La figure suivante présente la fenêtre dans laquelle vous indiquez l'emplacement du fichier image et entrez le nom du fichier image.




## Modes 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 :

**Hide Status Bar**
Masquer la barre d'état qui affiche l'état des touches Verr Maj, Verr Num et Arrêt défil. Cette option n'est disponible que lorsque la barre d'état s'affiche.

**Show Status Bar**
Afficher la barre d'état qui affiche l'état des touches Verr Maj, Verr Num, et Arrêt défil. Cette option n'est disponible que lorsque la barre d'état est masquée.

**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 ou barre de défilement supplémentaire. Ceci requiert que le bureau du client soit suffisamment spacieux pour afficher la fenêtre redimensionnée.

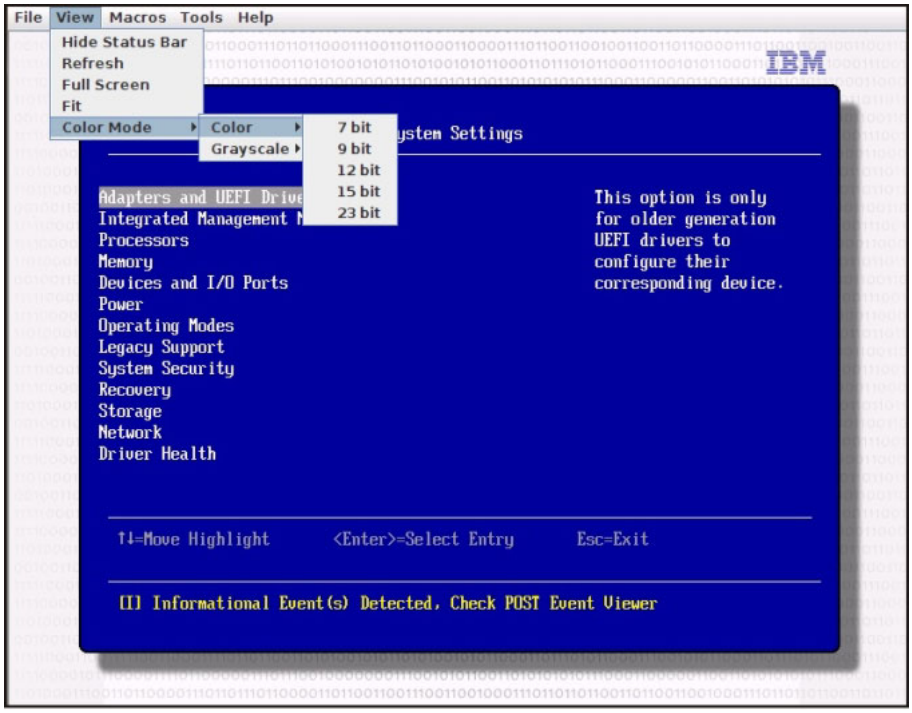
## Mode couleur vidéo de la fonction de contrôle à distance

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 :** Le module IMM2 comporte un élément de menu permettant un ajustement de la profondeur de couleur afin de réduire la quantité de données transmises en cas de bande passante étroite. Cet élément de menu remplace le curseur de bande passante utilisé dans l'interface Remote Supervisor Adapter II.

Pour changer le mode couleur vidéo, procédez comme suit.

1. Dans la fenêtre Video Viewer, cliquez sur **View**.
2. Cliquez sur **Color Mode**. Deux options de mode couleur sont disponibles (comme illustré ci-après) :
   - Color : 7, 9, 12, 15 et 23-bit
   - Grayscale : 16, 32, 64 et 128 teintes



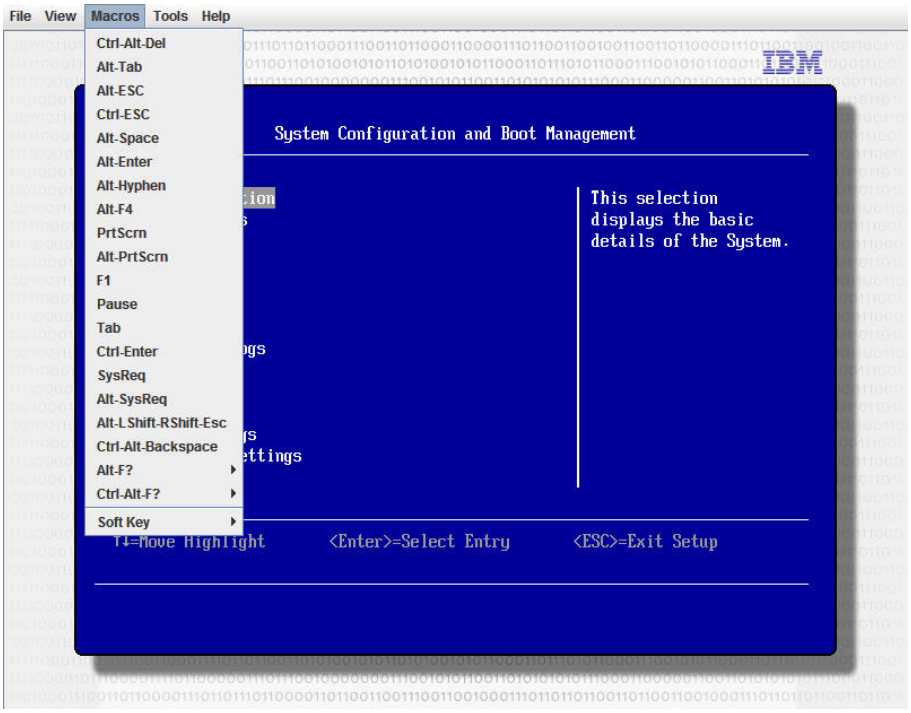

3. Sélectionnez le paramètre Color ou Grayscale.

## 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 (comme illustré ci-après).




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 qui s'ouvre après avoir sélectionné **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)

Le mode clavier pass-through désactive le traitement de la plupart des combinaisons de touches spéciales de façon à pouvoir les transmettre directement au serveur. Ceci offre 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 Virtual Console 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'ouvre, cliquez sur l'onglet **General**.
4. Sélectionnez ou désélectionnez la case **Pass all keystrokes to target** pour activer ou désactiver le mode clavier pass-through.
5. Cliquez sur **OK** pour enregistrer votre sélection.

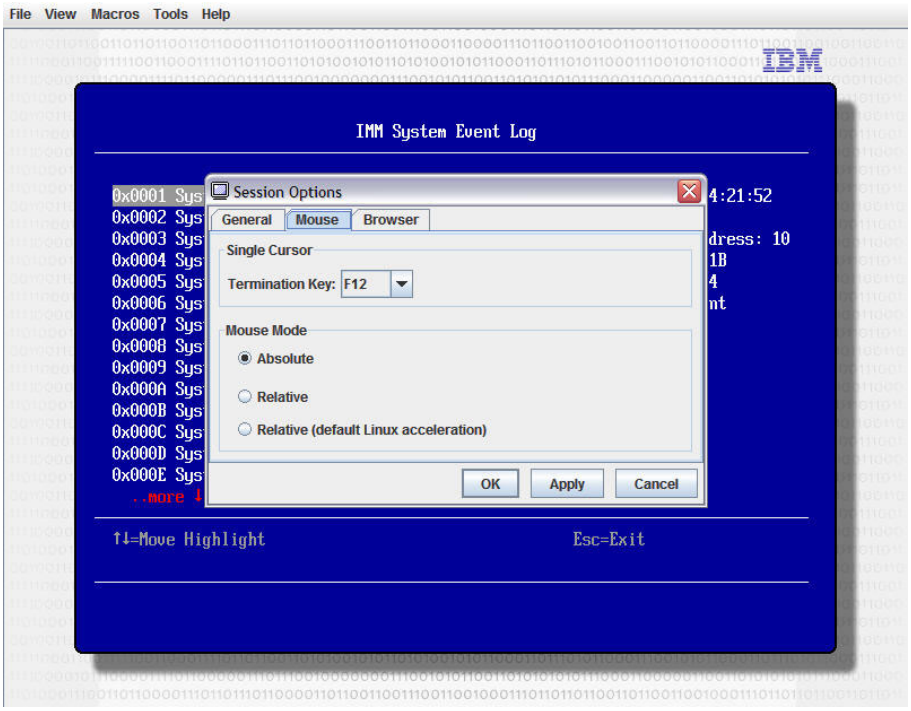
## Prise en charge de la souris par la fonction de contrôle à distance

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** (comme illustré ci-après).




4. Sélectionnez l'un des **modes souris** suivants :
   - **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, cliquez sur **Tools > Single Cursor** dans la fenêtre Video Viewer.

**Remarque :** 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 car il n'existe pas de curseur local.

Pour désactiver le mode de curseur unique, appuyez sur la touche **Defined Termination**. 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. Cliquez sur **Power**. Sélectionnez l'une des commandes suivantes :

   **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 performance Video Viewer dans la fenêtre Video Viewer, cliquez sur **Tools**, puis 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 affichée 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 utiliser un client RDP au lieu du client KVM. Le serveur distant doit être configuré pour recevoir les connexions RDP.

## Description de la fonction toc-toc

Lorsque toutes les sessions de contrôle à distance sont occupées (mode un utilisateur unique ou mode quatre utilisateurs multiples), un autre utilisateur Web a la possibilité d'envoyer une demande de déconnexion à l'utilisateur du contrôle à distance ayant activé la fonction toc-toc si cet utilisateur n'est pas déjà en train de traiter une demande de déconnexion provenant d'un autre utilisateur Web.

Si l'utilisateur du contrôle à distance ayant activé la fonction toc-toc accepte la demande ou ne répond pas à la demande dans les délais établis, la session de contrôle à distance sera terminée et réservée à l'utilisateur Web à l'origine de la demande. Si l'utilisateur Web envoyant la demande de déconnexion ne lance pas une session de contrôle à distance Java ou ActiveX avec la session de contrôle à distance réservée dans les 5 minutes qui suivent, la session de contrôle à distance cesse de lui être réservée.

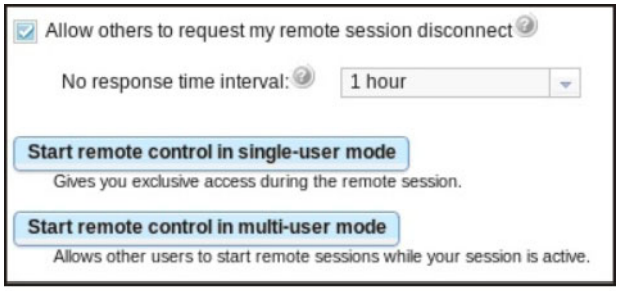
Pour activer la fonction toc-toc, procédez comme suit.

1. Accédez à la page Remote Control en sélectionnant l'une des options de menu suivantes :
   - Cliquez sur **Remote Control** dans l'onglet Server Management.
   - Cliquez sur **Remote Control...** dans la page System Status.
2. Cliquez sur la case à cocher **Allow others to request my remote session disconnect**.

   **Remarque :** Lorsque la fonction de contrôle à distance est utilisée, un ou plusieurs utilisateurs supplémentaires doivent avoir sélectionné la case à cocher **Allow others to request my remote session disconnect**.
3. Sélectionnez un intervalle de temps dans la zone **No response time interval**.
4. Démarrez la session de contrôle à distance en sélectionnant le mode utilisateur. Sélectionnez l'un des modes suivants :
   - Start remote control in single-user mode
   - Start remote control in multi-user mode

   **Remarque :** La fonction toc-toc est activée automatiquement.

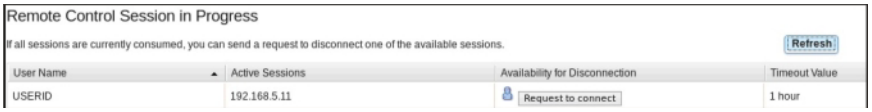
La figure suivante montre les zones décrites dans les étapes 2 à 4.




Pour envoyer une demande de session à distance, procédez comme suit.

1. Cliquez sur **Refresh** pour afficher la session de contrôle à distance en cours.

   La figure suivante montre la fenêtre Remote Control Session in Progress.



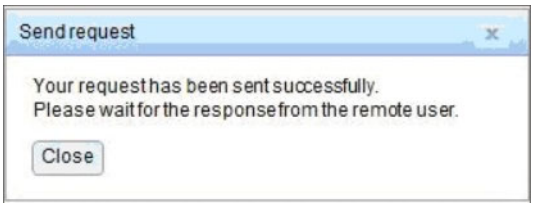

   L'une des réponses suivantes s'affichera dans la zone **Availability for Disconnection** :
   - **Request to connect :** Ce texte s'affiche lorsque l'utilisateur du contrôle à distance active la fonction toc-toc et n'est pas déjà en train de traiter une demande de déconnexion d'un autre utilisateur Web. L'utilisateur Web en cours n'a pas envoyé de demande de déconnexion à l'utilisateur du contrôle à distance.
   - **Waiting for response :** Ce texte s'affiche lorsque l'utilisateur du contrôle à distance est en train de traiter la demande de déconnexion provenant de l'utilisateur Web en cours. L'utilisateur Web en cours peut envoyer une demande d'annulation à l'utilisateur du contrôle à distance en cliquant sur le bouton **Cancel**.
   - **Other request is pending :** Ce texte s'affiche lorsque l'une des conditions suivantes se présente.

- L'utilisateur du contrôle à distance est en train de traiter la demande de déconnexion venant d'un autre utilisateur Web.
- L'utilisateur du contrôle à distance a activé la fonction toc-toc et l'utilisateur Web en cours attend la réponse à la demande de déconnexion d'un autre utilisateur de contrôle à distance.

• **Not available :** Ce texte s'affiche lorsque l'une des conditions suivantes se présente :
- Les sessions de contrôle à distance ne sont pas toutes occupées. Le fait que l'utilisateur du contrôle à distance ait activé ou non la fonction toc-toc n'a aucun effet sur cette condition.
- Toutes les sessions de contrôle à distance sont occupées et l'utilisateur du contrôle à distance n'a pas activé la fonction toc-toc.
- Cette connexion de contrôle à distance est réservée à un autre utilisateur pendant cinq minutes.

2. Cliquez sur **Request to connect** pour envoyer une demande de déconnexion à l'utilisateur du contrôle à distance.

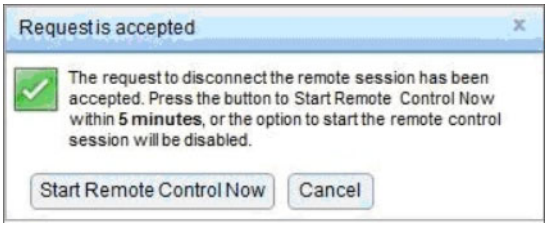
   La figure suivante montre la fenêtre qui s'affiche lorsque la demande est envoyée avec succès.



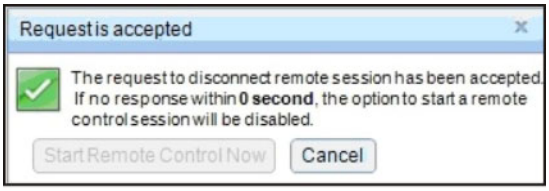

   Si l'utilisateur du contrôle à distance accepte la demande de déconnexion, l'utilisateur Web doit démarrer la session de contrôle à distance dans les cinq minutes qui suivent. Si l'utilisateur Web ne démarre pas la session dans un intervalle de cinq minutes, la session cesse d'être réservée.

   Les illustrations suivantes montrent les fenêtres qui s'affichent lorsque la demande de déconnexion est acceptée.

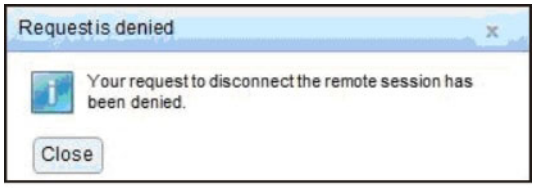
   La figure suivante montre la demande de déconnexion à l'état réservé.



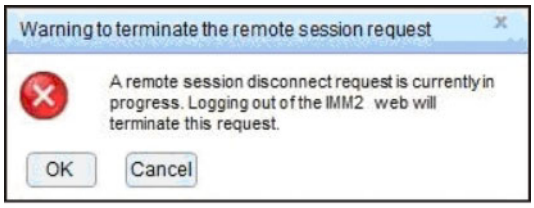

   La figure suivante montre la demande de déconnexion à l'état non réservé.




   Si l'utilisateur du contrôle à distance refuse la demande de déconnexion, l'utilisateur à l'origine de la demande de déconnexion recevra un message indiquant que la demande a été rejetée (comme illustré ci-après).

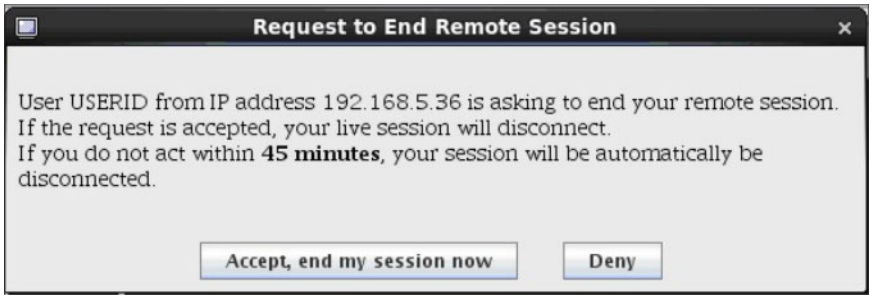



Si l'utilisateur Web tente de se déconnecter du module IMM2 avant de recevoir un message à propos de sa demande, il recevra un message (comme illustré ci-après).

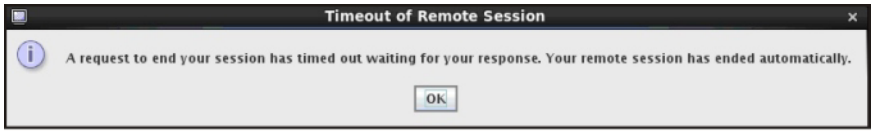



Une fois que l'utilisateur du contrôle à distance reçoit la demande, l'utilisateur doit déterminer s'il souhaite libérer la session à distance à l'intérieur de l'intervalle sélectionné avant de démarrer la session de contrôle à distance. La fenêtre Request to End Remote Session s'affiche pour rappeler à l'utilisateur du contrôle à distance le temps restant.

La figure suivante présente la fenêtre Request to End Remote Session.




Si l'utilisateur du contrôle à distance sélectionne l'option **Accept, end my session now**, l'afficheur distant sera automatiquement fermé. Si l'utilisateur du contrôle à distance sélectionne l'option **Deny**, l'utilisateur du contrôle à distance conservera la session à distance. Une fois la demande de clôture de la session à distance terminée, la session à distance est automatiquement libérée et la fenêtre suivante s'affiche.




## Disque distant

Depuis la fenêtre Virtual Media Session, vous pouvez affecter au serveur une unité de CD ou de DVD, une unité de disquette, une clé USB se trouvant 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 accéder au disque distant. Les unités et les images de disque sont affichées en tant qu'unités USB sur le serveur.

**Remarques :**

- Les systèmes d'exploitation serveur suivants prennent en charge les unités USB. La prise en charge USB est requise pour la fonctionnalité de disque distant.
  - Microsoft Windows Server 2003 : Web, Std, Ent, DC (SP2, R2, SBS)
  - Microsoft Windows Server 2008 SP2 : Std, SBS, EBS
  - Microsoft Windows Server 2008 R2
  - SUSE Linux Enterprise Server V10 SP3 : x86_64
  - SUSE Linux Enterprise Server V11 : x86,_64
  - Red Hat Enterprise Linux Enterprise Servers V3.7 : x86, x86_64
  - Red Hat Enterprise Linux Enterprise Servers V4.8 : x86, x86_64
  - Red Hat Enterprise Linux Enterprise Servers V5.5 : x86, x86_64
  - Red Hat Enterprise Linux Enterprise Servers V6.0 : x86, x86_64
  - ESX 4.5 : 4.0 U1
- Le serveur du client requiert le plug-in Java 1.5, ou ultérieur.
- 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. Dans la fenêtre Video Viewer, cliquez sur **Tools**.
2. Cliquez sur **Launch Virtual Media**. La fenêtre Video Viewer s'ouvre.

**Remarque :** Si la case **Encrypt disk and KVM data during transmission** a été cochée avant l'ouverture de la fenêtre Video Viewer, les données du disque seront 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

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.

Lorsqu'une image est ajoutée à la liste et que la case à cocher **Map** est sélectionnée (si l'image peut être chargée à la mémoire IMM2 pour la fonction RDOC), une fenêtre s'ouvre, offrant la possibilité de transférer l'image au serveur. Si vous sélectionnez **Yes**, entrez un nom pour l'image.

**Remarque :** Veillez à ne pas entrer de caractères spéciaux tels que le signe perluète (&) ou des espaces dans le nom.

Le téléchargement d'une image vers la mémoire IMM2 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'IMM2. Plusieurs images peuvent être stockées sur le module IMM2 mais l'espace total ne peut pas dépasser 50 mégabits. Pour décharger le fichier image de la mémoire, sélectionnez son nom dans la fenêtre RDOC Setup et cliquez sur **Delete**.

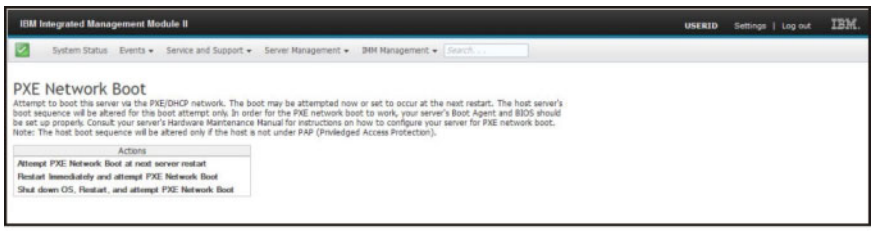
### Sortie de la fonction Remote Control (Contrôle à distance)

Fermez les fenêtres Video Viewer et Virtual Media Session quand vous avez fini d'utiliser la fonction Remote Control.

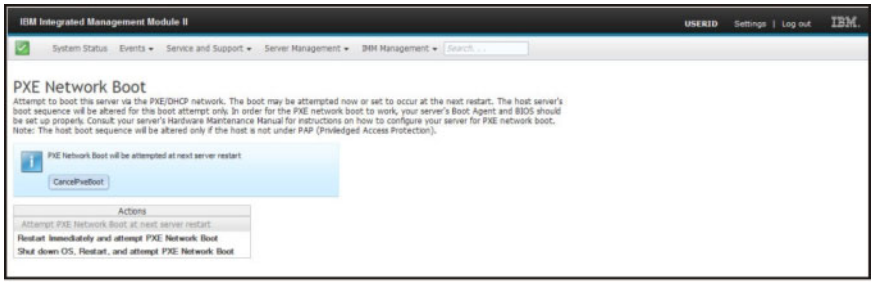
## Configuration de l'amorçage réseau PXE

Utilisez l'option PXE Network Boot pour configurer les tentatives d'amorçage préliminaires de l'environnement d'exécution du serveur. Pour configurer votre serveur pour tenter un amorçage réseau PXE (Preboot Execution Environment) au prochain redémarrage du serveur, procédez comme suit.

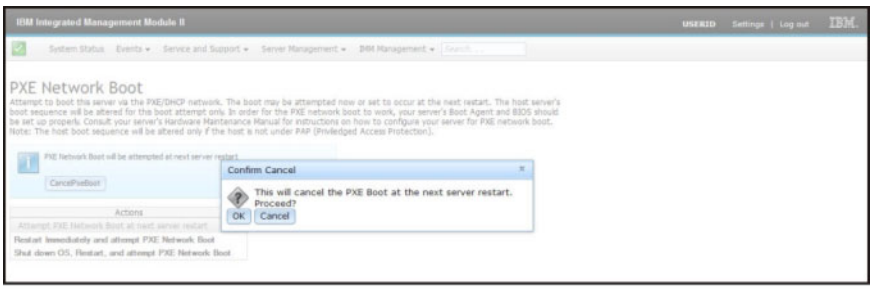
1. Connectez-vous au module IMM2. Pour plus d'information, voir «Connexion au module IMM2», à la page 10.
2. Cliquez sur **Server Management**, puis sélectionnez **PXE Network Boot**.
   La fenêtre suivante s'ouvre.




3. Sélectionnez **Attempt PXE Network Boot at next server restart** dans les options Action. La fenêtre suivante s'ouvre.



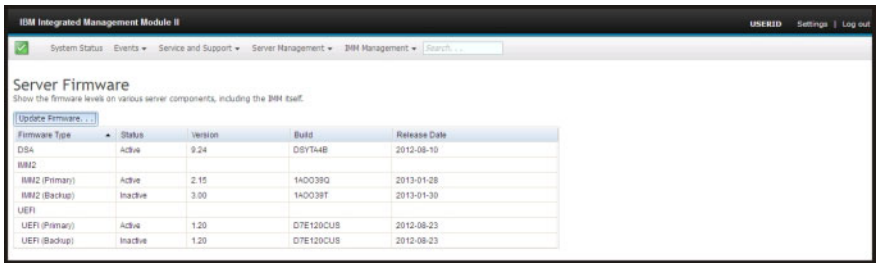

   Si vous souhaitez annuler la sélection, cliquez sur **CancelPxeBoot**. La fenêtre Confirm Cancel suivante s'ouvre.




## Mise à jour du microprogramme de serveur

L'option Server Firmware affiche les niveaux de microprogrammes et vous permet de mettre à jour les microprogrammes DSA, IMM2 et UEFI. Les versions actuelles des microprogrammes IMM2, UEFI et DSA sont affichées. Elles comprennent les versions Active (active), Primary (principale) et Backup (de sauvegarde).

La figure suivante présente la page Server Firmware.



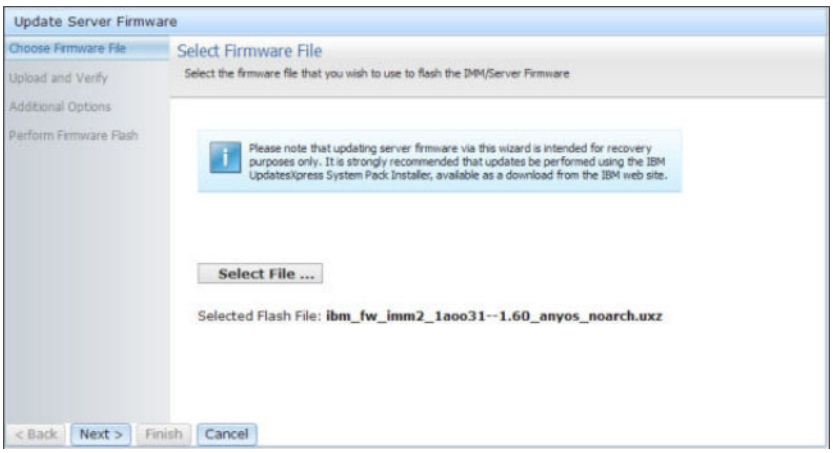

Le statut et les versions en cours des microprogrammes IMM2, UEFI, et DSA sont affichés, y compris les versions principale et de sauvegarde. Il existe trois catégories de statut de microprogramme :

- **Active :** le microprogramme est actif.
- **Inactive :** le microprogramme est inactif.
- **Pending :** le microprogramme est en instance de devenir actif.

**Attention :** L'installation d'une mise à jour de microprogramme erronée peut entraîner une dysfonctionnement du serveur. Avant d'installer une mise à jour de microprogramme ou de pilote de périphérique, lisez les éventuels fichiers readme et historiques de modification qui sont fournis avec la mise à jour téléchargée. Ces fichiers contiennent des informations importantes concernant la mise à jour et la procédure d'installation de cette mise à jour, y compris toute procédure spéciale pour une mise à jour à partir d'une version antérieure de microprogramme ou de pilote de périphérique vers la version actuelle.

Pour mettre à jour le microprogramme de serveur, procédez comme suit.

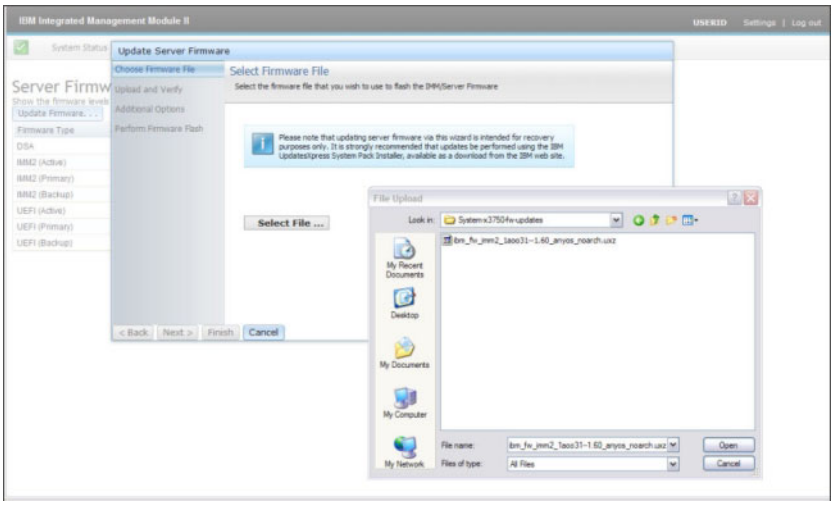
1. Cliquez sur **Server Firmware** dans la liste de menu Server Management.
2. Cliquez sur **Update Firmware**. La fenêtre Update Server Firmware s'ouvre (comme illustré ci-après).



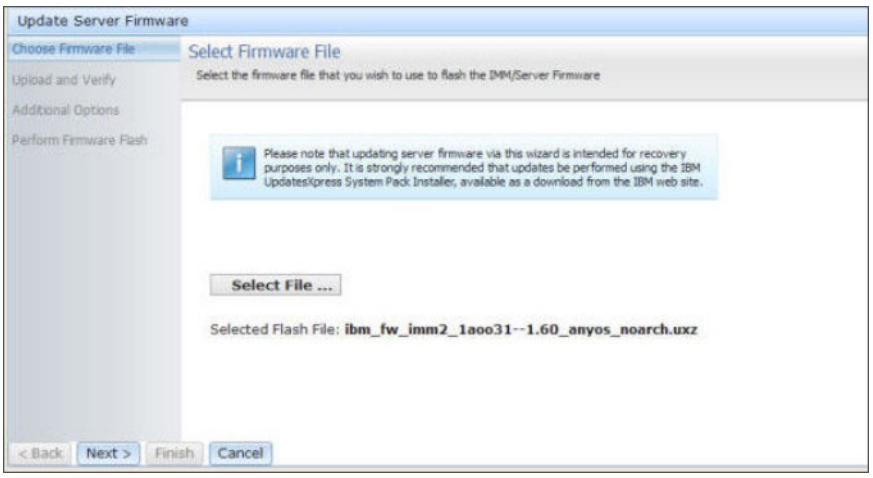

3. Lisez la note d'avertissement avant de passer à l'étape suivante.
4. Effectuez l'une des étapes suivantes :
   - Cliquez sur **Cancel** et retournez à la fenêtre Server Firmware précédente.
   - Cliquez sur **Select File...** pour sélectionner le fichier de microprogramme que vous souhaitez utiliser pour effectuer une copie instantanée du microprogramme de serveur.

     **Remarque :** Toutes les autres options sont grisées lorsque la fenêtre Update Server Firmware s'ouvre initialement.

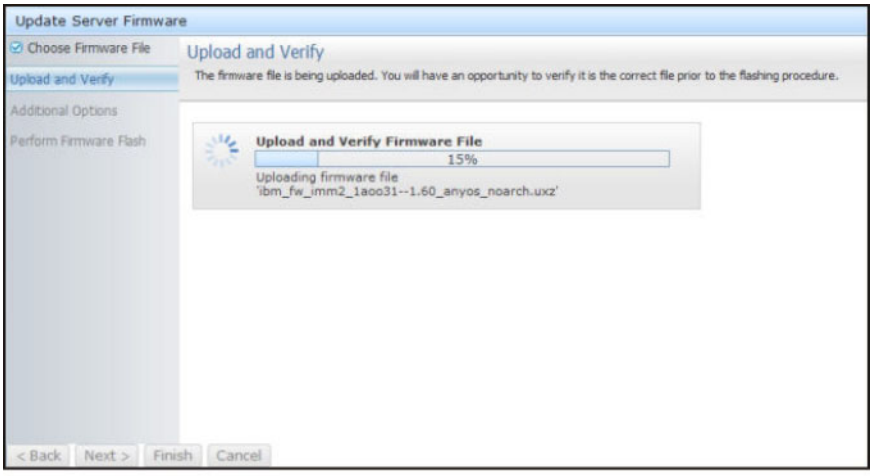
     Lorsque vous cliquez sur **Select File...**, une fenêtre File Upload s'ouvre (comme illustré ci-après). La fenêtre vous permet de naviguer vers le fichier désiré.




5. Naviguez vers le fichier que vous souhaitez sélectionner et cliquez sur **Open**. Vous retournez à la fenêtre Update Server Firmware avec le fichier sélectionné affiché (comme illustré dans la figure ci-après).

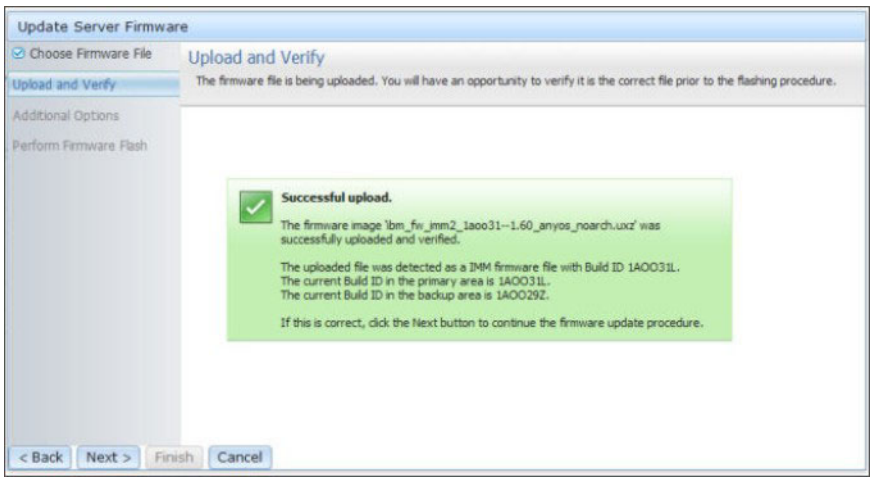



6. Cliquez sur **Next >** pour commencer le téléchargement et vérifier le processus pour le fichier sélectionné. Une barre de progression s'affiche pendant toute la durée du téléchargement et de la vérification du fichier (comme illustré dans la figure ci-après).



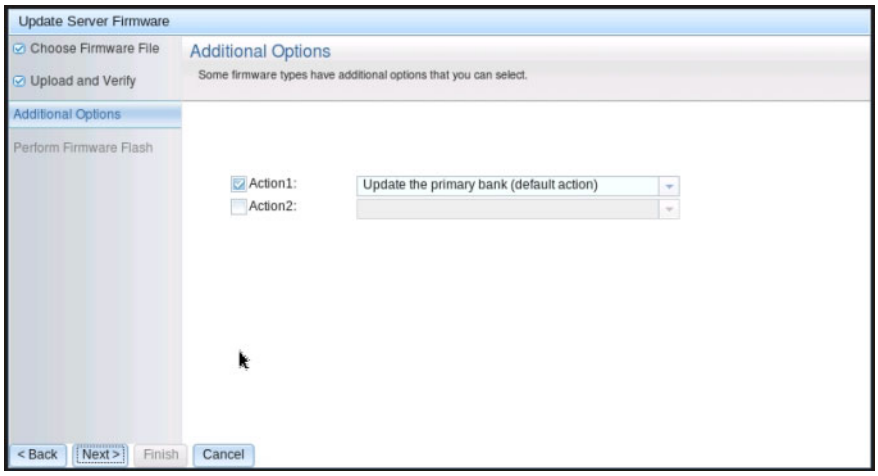

Vous pouvez afficher cette fenêtre d'état pour vérifier que le fichier que vous avez sélectionné pour la mise à jour est bien le fichier correct. La fenêtre d'état contiendra des informations sur le type de fichier de microprogramme devant être mis à jour, tel que DSA, IMM ou UEFI.

Une fois le fichier de microprogramme correctement téléchargé et vérifié, une fenêtre s'ouvre indiquant que le téléchargement a réussi (comme illustré dans la figure ci-après).

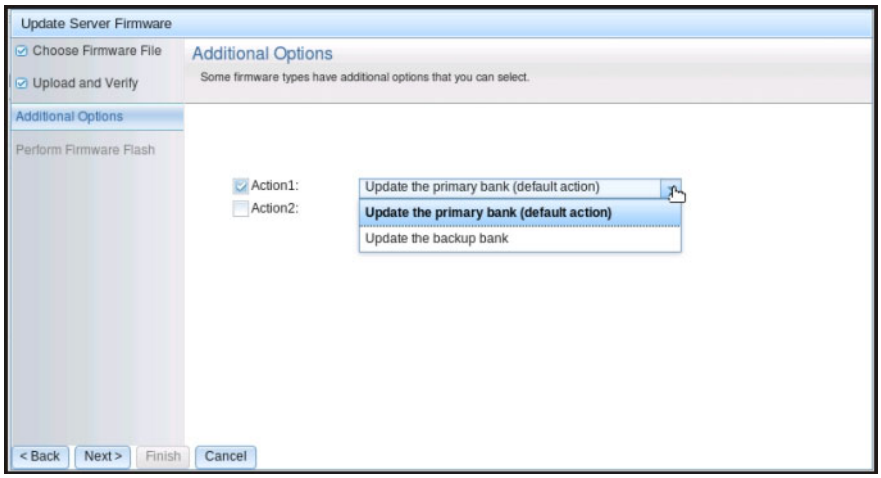



7. Cliquez sur **Next >** si l'information est correcte. Cliquez sur **< Back** si vous souhaitez répéter l'une des sélections.

   Si vous cliquez sur **Next >**, un ensemble d'options supplémentaires s'affiche (comme illustré dans la figure ci-après).



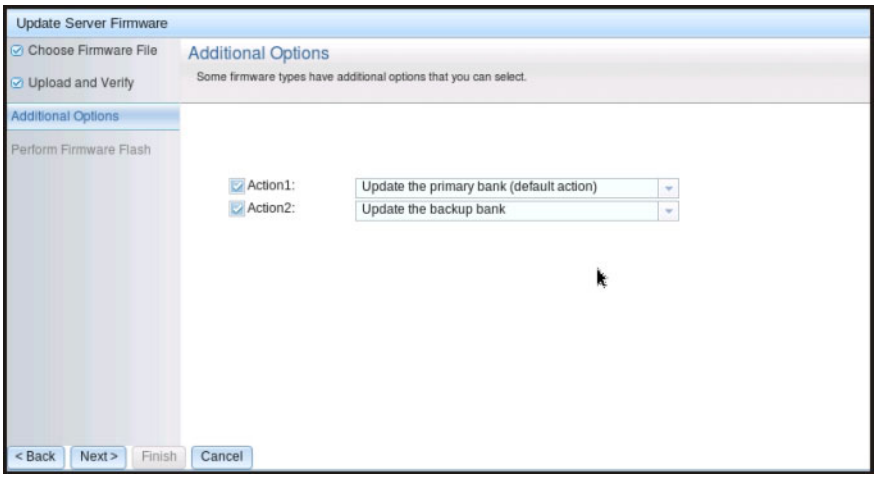

8. Le menu déroulant situé en regard de la zone **Action 1** vous donne le choix entre **Update the primary bank (default action)** ou **Update the backup bank** (comme illustré ci-après).




   Après avoir sélectionné une action, vous retournez à l'écran précédent dans lequel s'affiche l'action supplémentaire demandée.

Une fois que l'action choisie est chargée, elle s'affiche ainsi qu'un nouveau menu déroulant **Action 2** (comme illustré ci-après).

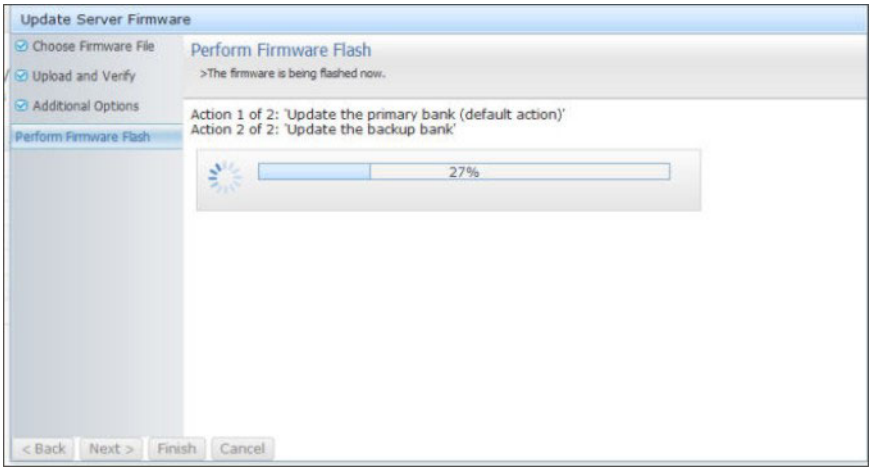
**Remarque :** Pour désactiver une action et reprendre le processus d''ajout d'une option supplémentaire, cliquez sur la case à cocher en regard de l'action concernée.



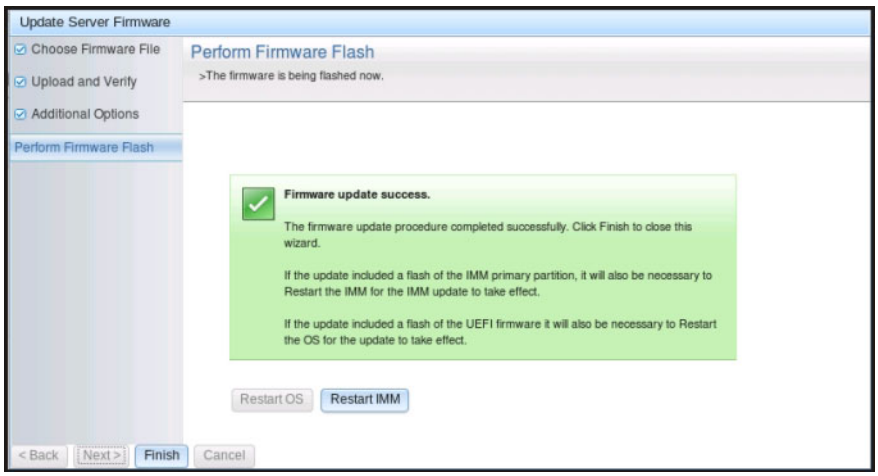

L'écran précédent montre que pour l'Action 1, la banque principale a été sélectionnée pour être mise à jour. Vous pouvez également sélectionner la mise à jour de la banque de sauvegarde sous Action 2 (comme illustré dans l'écran précédent). La banque principale et la banque de sauvegarde sont mises à jour en même temps lorsque vous cliquez sur **Next >**.

**Remarque :** L'Action 1 doit être différente de l'Action 2.

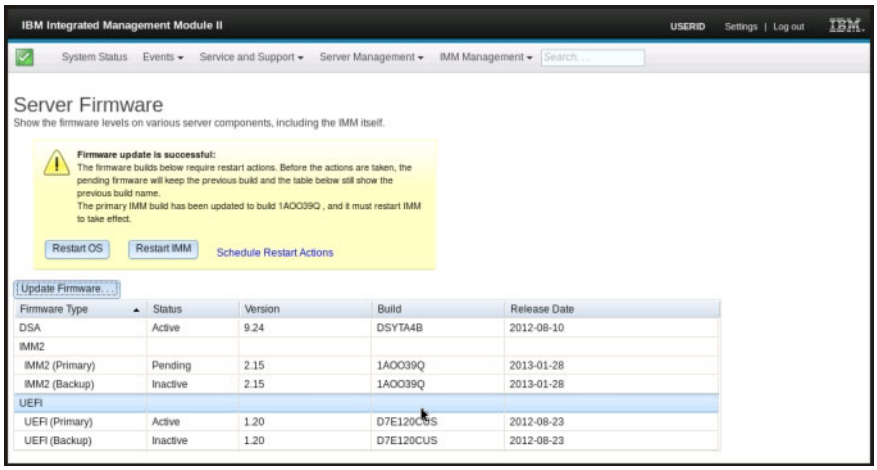
Une barre de progression affiche l'état d'avancement de la mise à jour de la banque principale et de la banque de sauvegarde (comme illustré dans la figure ci-après).




Lorsque la mise à jour du microprogramme se termine correctement, la fenêtre ci-après s'affiche. Sélectionnez l'opération associée en fonction du contenu affiché afin de terminer le processus de mise à jour.




Si la mise à jour de microprogramme principal n'a pas abouti, la fenêtre ci-après s'affiche lors de l'ouverture de l'écran Server Firmware.



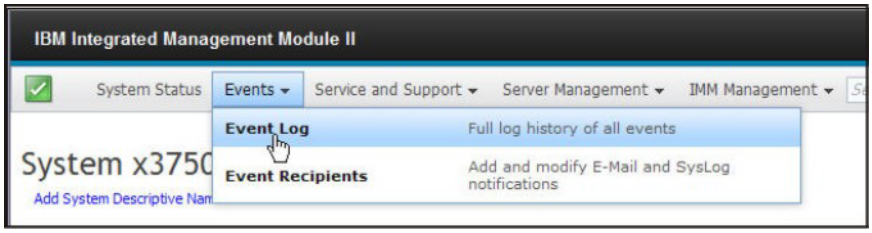

## Gestion des événements système

Le menu Events vous permet de gérer l'historique des événements et de gérer les destinataires des événements pour les notifications par courrier électronique et syslog.

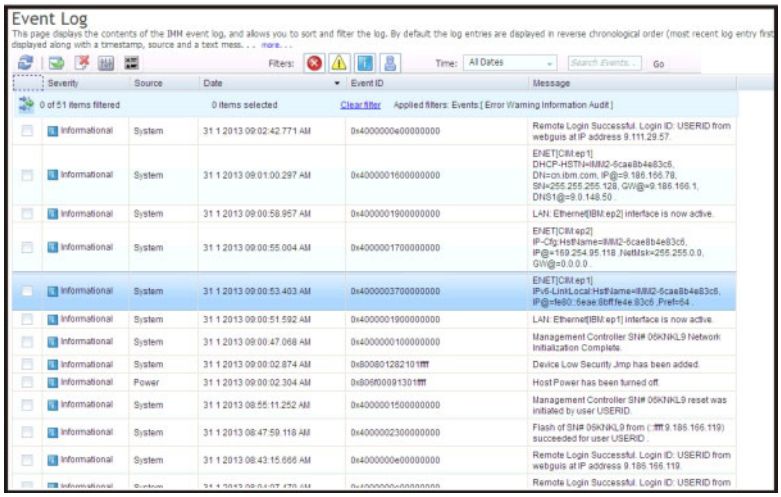
### Gestion du journal des événements

Cliquez sur l'option **Event Log** pour afficher la fenêtre Event Log. La fenêtre Event Log contient une description des événements signalés par le module IMM2 et des informations sur toutes les tentatives d'accès à distance et modifications de configuration. Tous les événements recensés dans le journal sont accompagnés d'un horodatage qui utilise les paramètres de date et d'heure du module IMM2. Certains événements génèrent des alertes s'ils sont configurés en conséquence dans la fenêtre Event Recipients. Vous pouvez également trier et filtrer les événements dans le journal des événements.

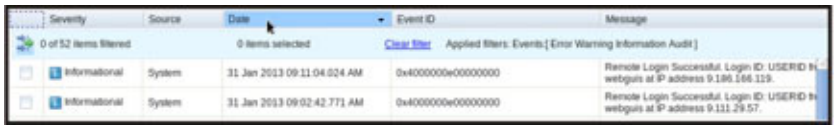
Cliquez sur l'option **Event Log**. La fenêtre suivante s'ouvre.




Lorsque l'option Event Log est sélectionnée, la fenêtre suivante s'ouvre.



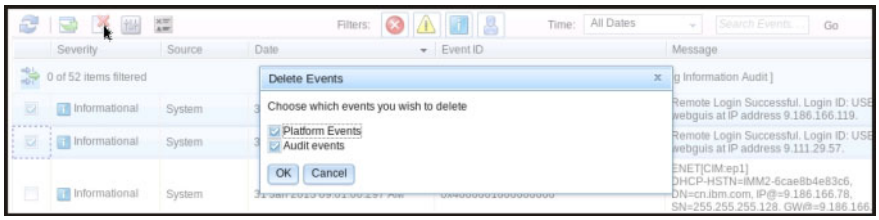

Pour trier et filtrer les événements dans le journal des événements, sélectionnez l'en-tête de colonne (comme illustré ci-après).




Vous pouvez sauvegarder dans un fichier une sélection d'événements ou tous les événements du journal des événements à l'aide du bouton **Export**. Pour sélectionner des événements spécifiques, sélectionnez un ou plusieurs événement sur la page principale Event Log et cliquez avec le bouton gauche de la souris sur le bouton **Export** (comme illustré ci-après).

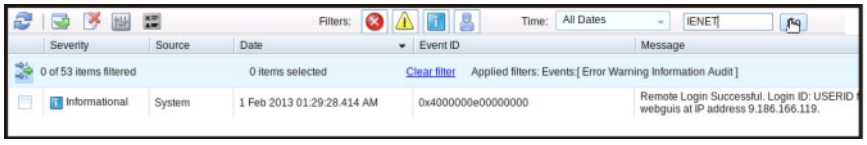
Pour choisir le type d'événements que vous souhaitez supprimer, cliquez sur **Delete Events**. Vous devez sélectionner la catégorie d'événements que vous souhaitez supprimer.

La figure suivante montre la fenêtre Delete Events.




Pour sélectionner le type d'entrées que vous souhaitez afficher dans le journal des événements, cliquez sur le bouton approprié (comme illustré ci-après).

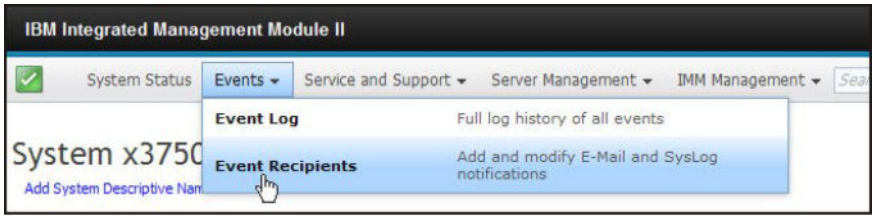

Pour rechercher un type d'événements ou de mots-clé défini, entrez le type d'événement ou mot-clé dans la zone **Search Events**, puis cliquez sur **Go** (comme illustré ci-après).




## Notification des événements système

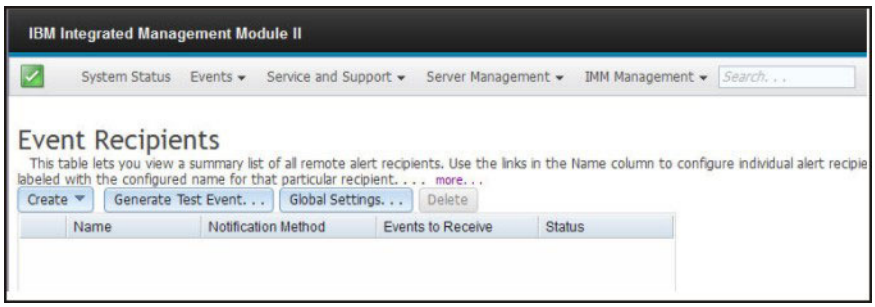
Sélectionnez l'option **Event Recipients** pour ajouter et modifier les notifications par courrier électronique et notifications syslog.

La figure suivante montre la sélection de l'option Event Recipients.

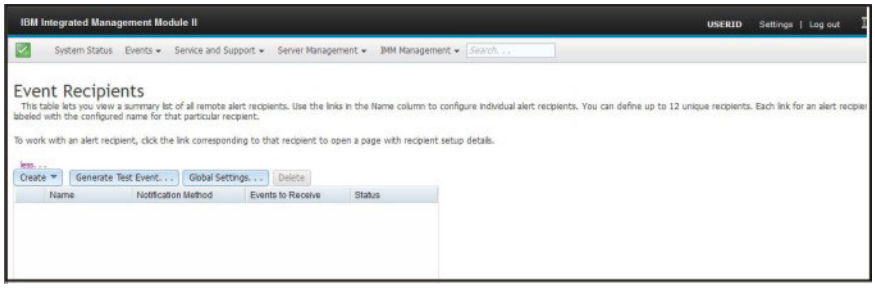



L'option Event Recipients vous permet de gérer les destinataires des notifications d'événements système. Vous pouvez configurer chaque destinataire de manière individuelle et gérer des paramètres applicables à tous les destinataires d'événements. Vous pouvez également générer un événement test afin de vérifier le fonctionnement du dispositif de notification.

La figure suivante montre la page Event Recipients.



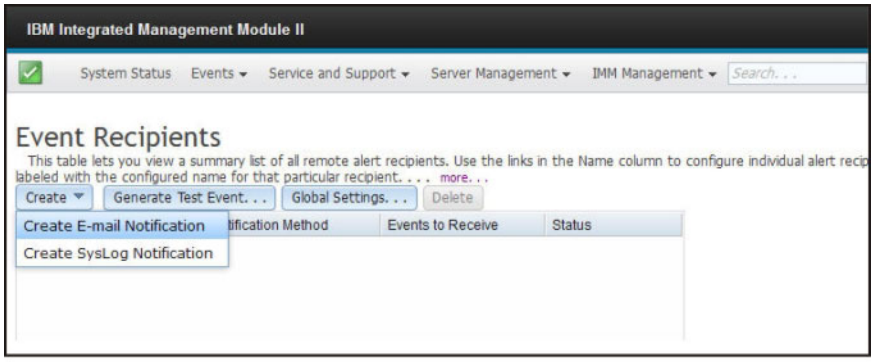

La figure suivante affiche les informations supplémentaires qui s'affichent lorsque vous cliquez sur le lien **more** de la page Event Recipients.




## Création de notifications par courrier électronique et notifications syslog

Sélectionnez l'onglet **Create** pour créer des notifications par courrier électronique ou notifications syslog.

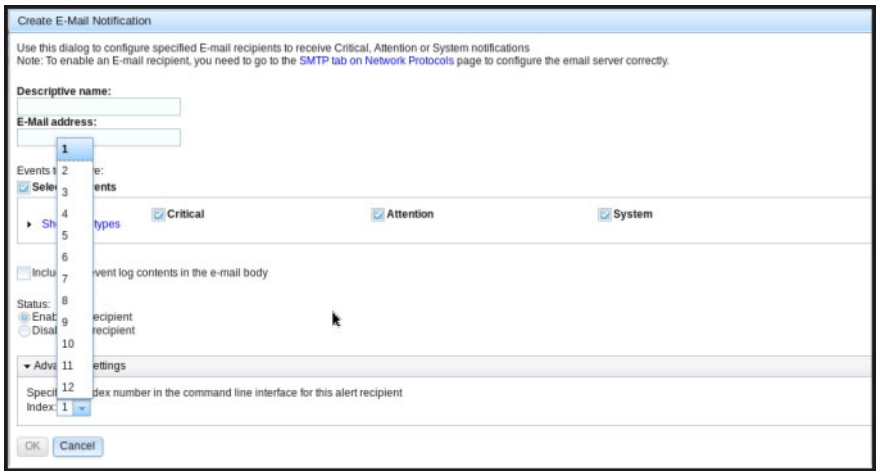
La figure suivante montre les options disponibles dans le menu Create.




Dans l'option **Create E-mail Notification**, vous pouvez configurer une adresse de courrier électronique cible et sélectionner les types d'événements pour lesquels vous souhaitez recevoir une notification. Vous pouvez également cliquer sur **Advanced Settings** pour sélectionner le numéro d'index de début. Pour inclure le journal des événements dans le courrier électronique, cochez la case **Include the event log contents in the e-mail body**.

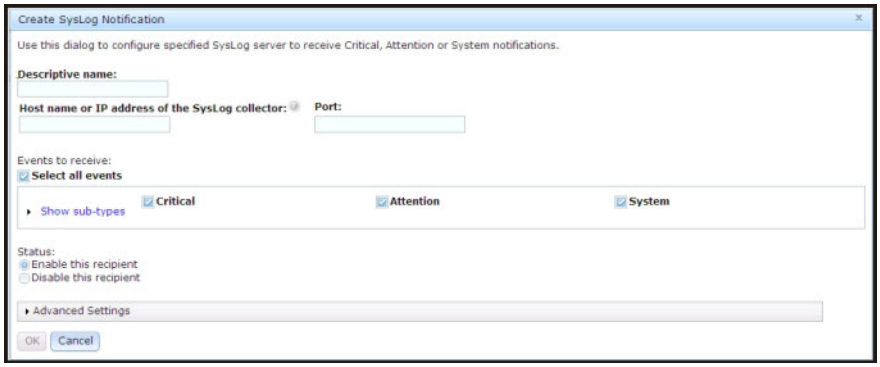
La figure suivante montre l'écran Create E-mail Notification.


La figure suivante montre les sélections du panneau Advanced Settings.

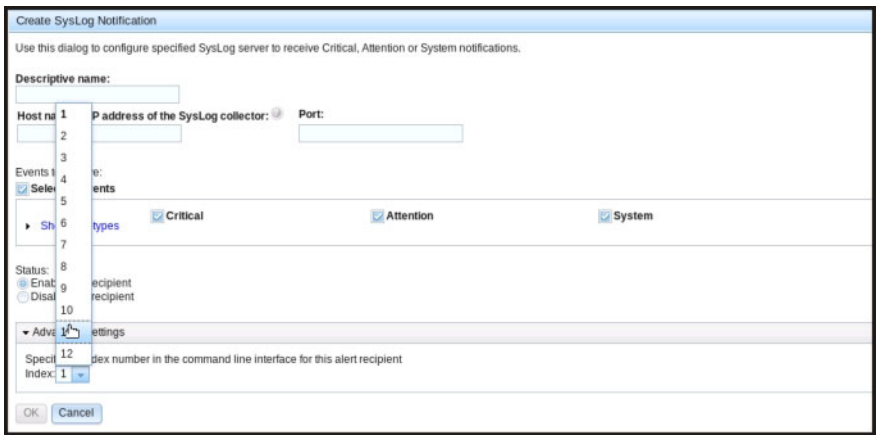



Dans l'option **Create Syslog Notification**, vous pouvez configurer le nom d'hôte et l'adresse IP de la collecte syslog et sélectionner les types d'événements pour lesquels vous souhaitez recevoir des notifications. Vous pouvez cliquer sur **Advanced Settings** pour sélectionner le numéro d'index de début. Vous pouvez également spécifier le port que vous souhaitez utiliser pour ce type de notification.

La figure suivante montre l'écran Create Syslog Notification.



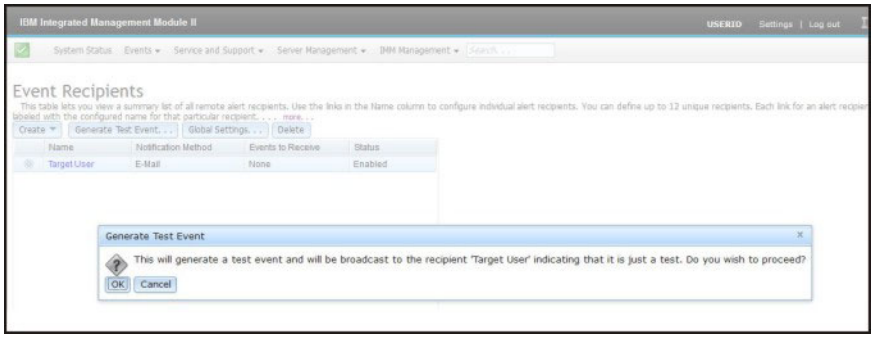

La figure suivante montre les sélections du panneau Advanced Settings.




## Génération d'événements test

Utilisez l'onglet **Generate Test Event...** pour envoyer un courrier électronique test à une adresse électronique cible sélectionnée. Après avoir sélectionné la notification d'événement, cliquez sur **OK** pour générer l'événement test. L'événement test est envoyé au destinataire avec une notification indiquant qu'il s'agit d'un test.

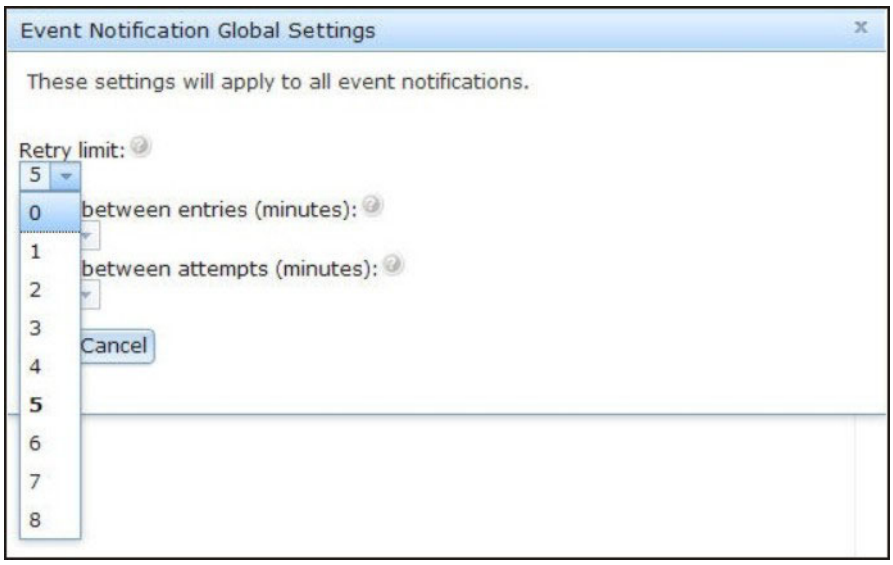
La figure suivante montre la fenêtre Generate Test Event.



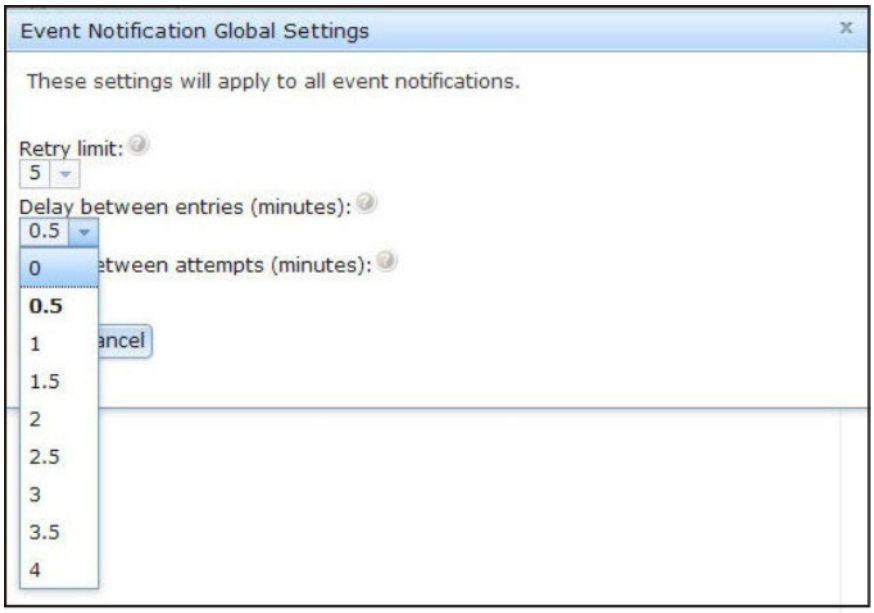

## Définition de limites pour la relance de notifications

Utilisez l'onglet **Global Settings...** pour définir une limite pour la relance de notifications d'événements, la relance du délai entre les entrées de notifications d'événements (en minutes) et la relance du délai entre tentatives (en minutes).

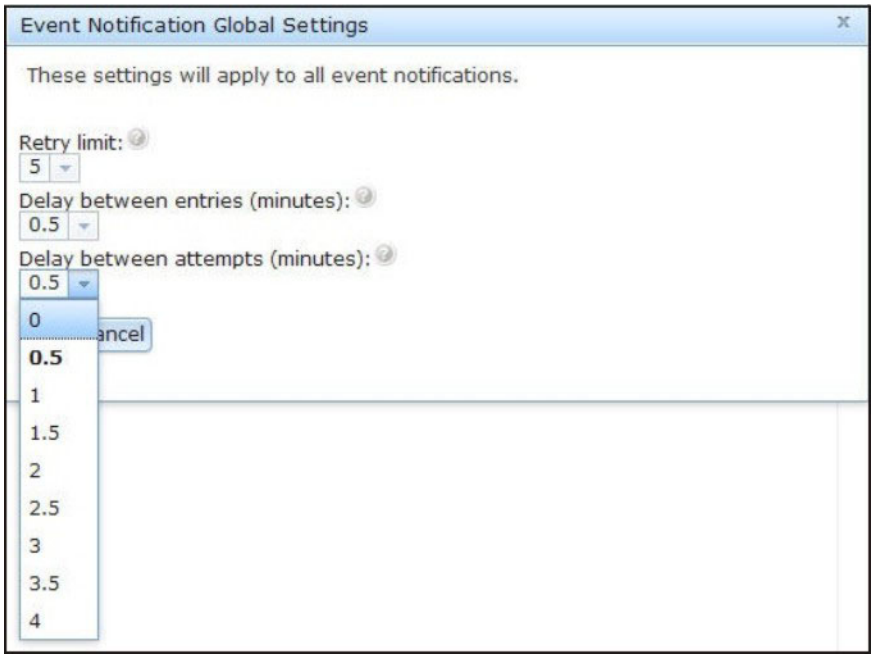
La figure suivante montre les paramètres de l'option Retry limit.




La figure suivante montre les paramètres de l'option Delay between entries (minutes).



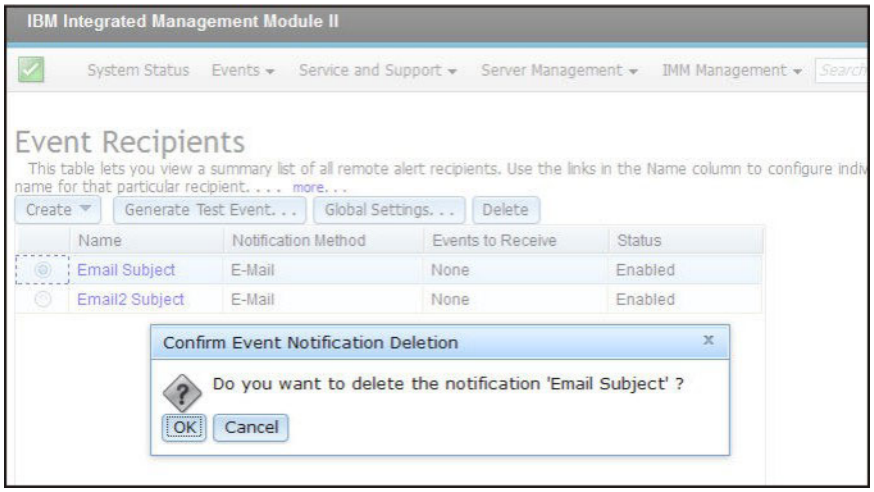

La figure suivante montre les paramètres de l'option Delay between attempts (minutes).




### Suppression des notifications par courrier électronique et notifications syslog

Utilisez l'onglet **Delete** pour supprimer une cible de notification par courrier électronique ou notification syslog.

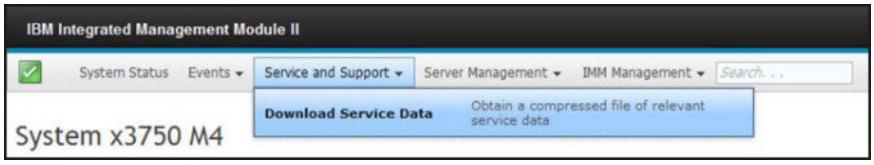
La figure suivante montre la fenêtre Confirm Event Notification Deletion.




## Collecte des informations de service et de support

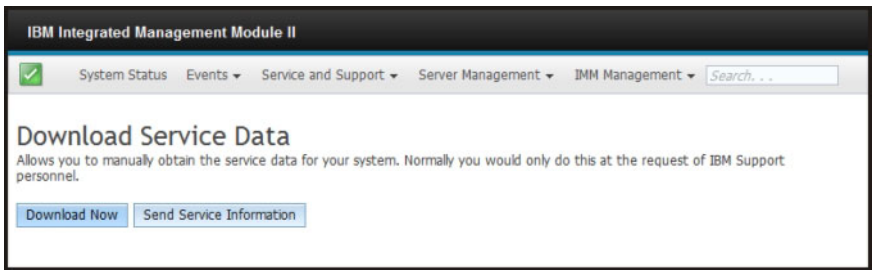
Cliquez sur l'option **Download Service Data** sous le menu Service and Support pour collecter des informations sur le serveur pouvant être utilisées par le support IBM pour vous aider en cas de problème.

La figure suivante montre le menu Service and Support.



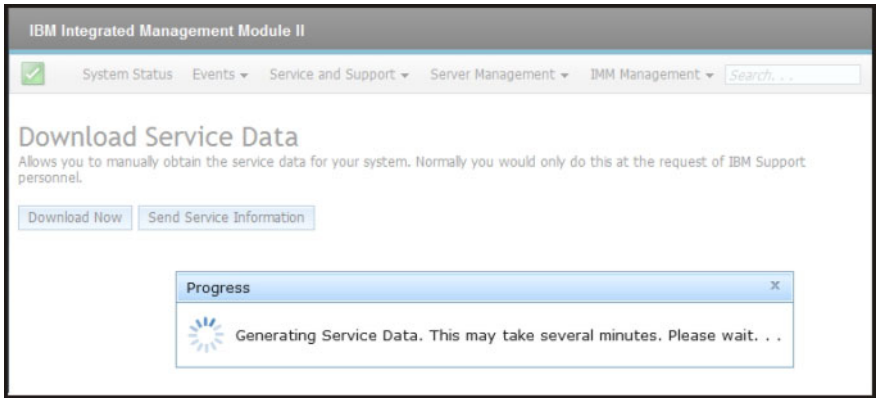

Cliquez sur le bouton **Download Now** si vous souhaitez télécharger les données de service et de support.

La figure suivante montre la fenêtre Download Service Data.

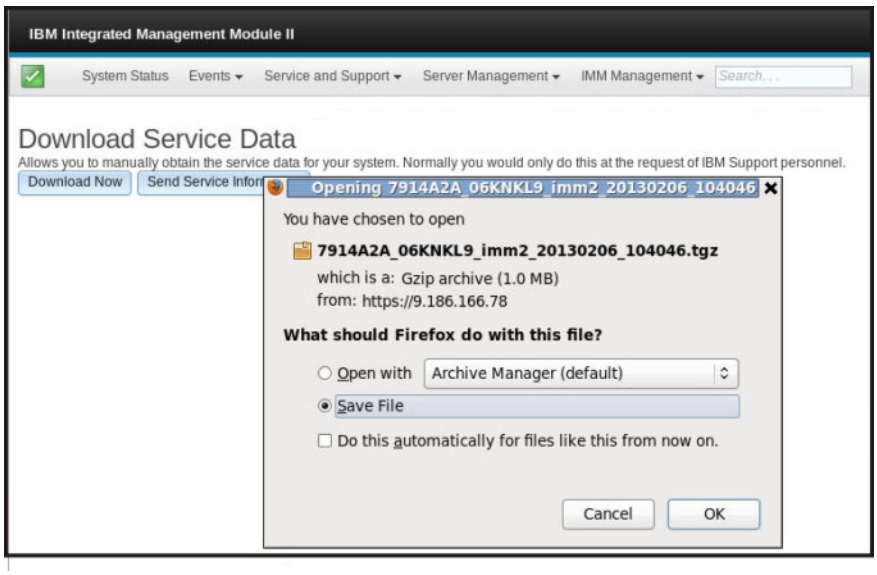



Le processus de collecte des données de service et de support démarre. Ce processus tarde quelques minutes à générer les données de service que vous pouvez enregistrer dans un fichier.

La fenêtre Progress ci-après s'affiche lors de la génération des données de service.




Lorsque le processus est terminé, vous êtes invité à entrer l'emplacement de sauvegarde du fichier. Reportez-vous à la figure suivante pour voir un exemple.




## Capture des données d'écran du dernier échec du système d'exploitation

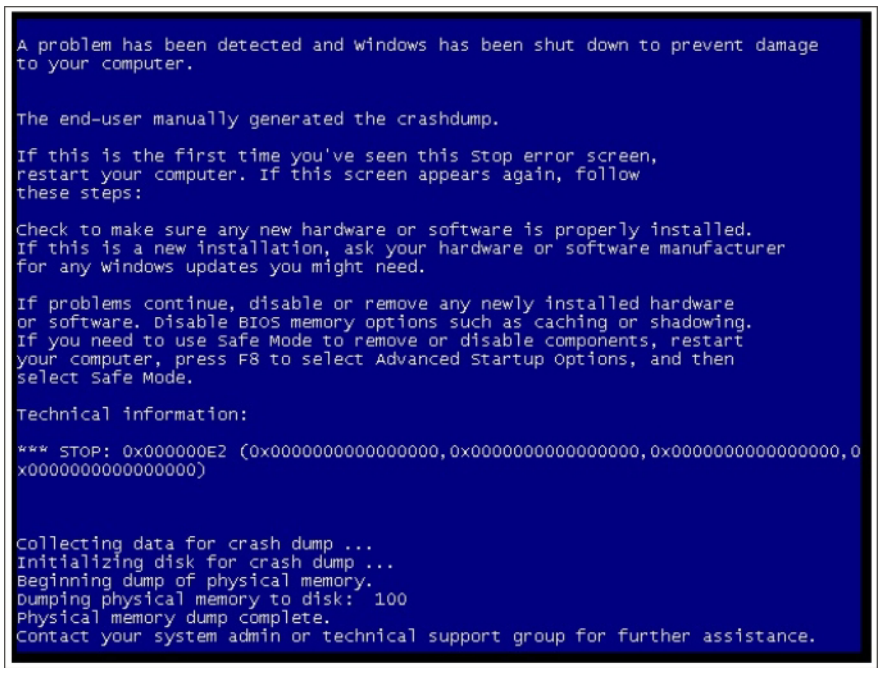
Utilisez l'option Latest OS Failure Screen pour capturer et stocker les données d'écran d'échec du système d'exploitation. Le module IMM2 ne stocke que les informations de l'événement d'erreur le plus récent, en écrasant les données d'écran d'échec du système d'exploitation plus anciennes lorsqu'un nouvel événement d'erreur survient. La fonctionnalité de surveillance du système d'exploitation doit être activée pour capturer l'écran d'échec du système d'exploitation. Si un événement se produit et cause l'arrêt du système d'exploitation, la fonctionnalité de surveillance du système d'exploitation est déclenchée. La capture d'écran d'échec du système d'exploitation est uniquement disponible avec la fonctionnalité de niveau avancé du module IMM2. Consultez la documentation de votre serveur pour obtenir des informations sur le niveau IMM2 installé sur votre serveur.

Pour afficher une image de l'écran d'échec du système d'exploitation à distance, sélectionnez l'une des options de menu suivantes :

- **Latest OS Failure Screen** dans l'onglet Server Management
- Onglet **Latest OS Failure Screen** dans la page System Status

**Remarque :** Si aucun écran d'échec du système d'exploitation n'a été capturé, l'onglet Latest OS Failure Screen de la page System Status sera grisé et ne pourra pas être sélectionné.

La figure suivante montre l'écran d'échec du système d'exploitation.

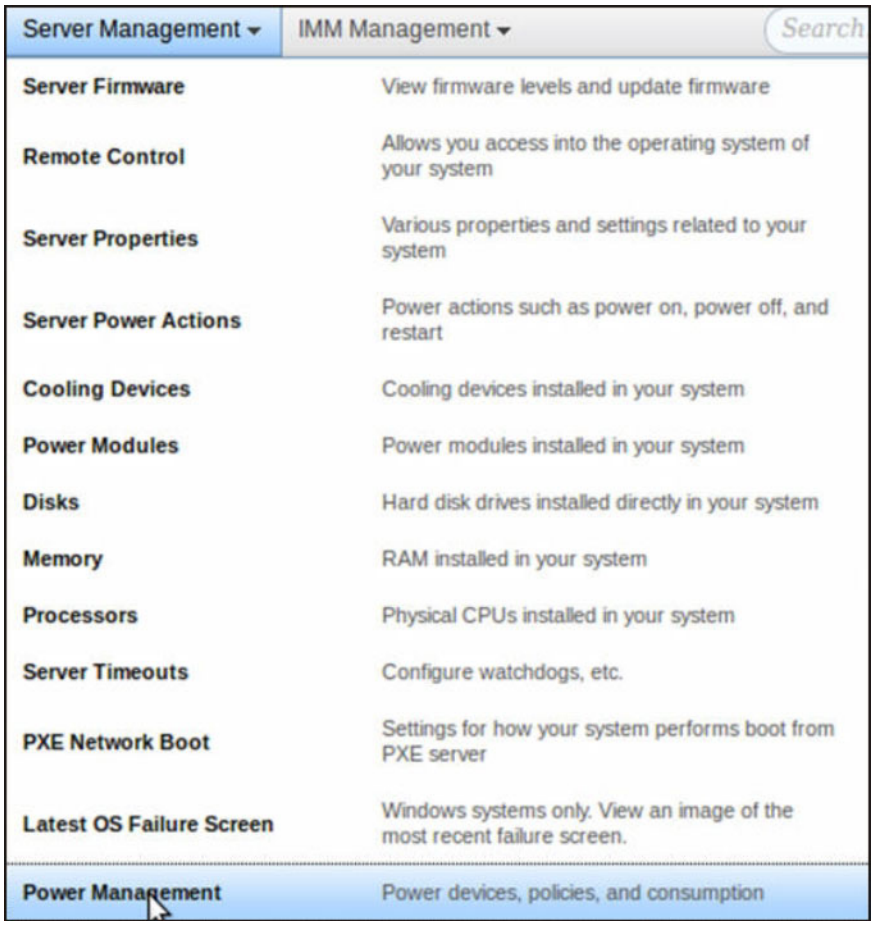



## Gestion de l'alimentation serveur

Utilisez l'onglet Power Management pour effectuer les tâches suivantes :

- Afficher les informations relatives aux alimentations électriques
- Contrôler le mode de gestion de l'"alimentation" de l'alimentation électrique.
- Contrôler l'alimentation système totale.
- Afficher les informations relatives à la capacité des alimentations électriques installées et de l'alimentation électrique actuelle
- Afficher l'historique de la quantité d'énergie utilisée.

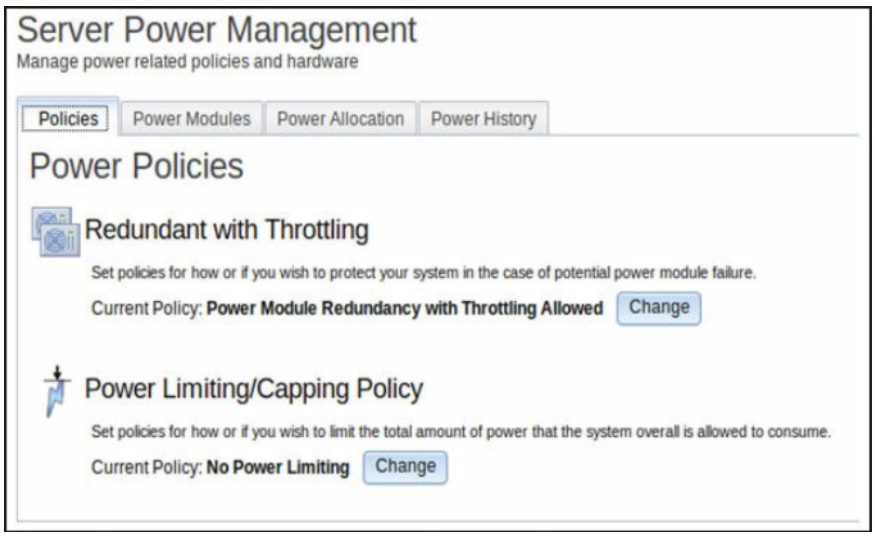
Sélectionnez l'option **Power Management** sous l'onglet Server Management pour afficher les informations de gestion de l'alimentation et effectuer des fonctions de gestion de l'alimentation (comme illustré ci-après).




## Contrôle de l'alimentation électrique et de toute l'alimentation système

Cliquez sur l'onglet **Policies** pour contrôler le mode de gestion de l'alimentation électrique et éventuellement contrôler la totalité de l'alimentation électrique avec Active Energy Manager en définissant une règle de plafonnement (comme illustré ci-après).

**Remarque :** L'onglet **Policies** n'est pas disponible dans IBM Flex System.




Pour sélectionner la règle à utiliser pour la protection de votre serveur en cas de défaillance du module d'alimentation, cliquez sur le bouton **Change** en regard de Current Policy pour l'option Redundant with Throttling dans la fenêtre Power Policies.

**Remarque :** Le choix d'une règle d'alimentation vous permet de trouver un compromis entre la redondance et l'alimentation disponible.

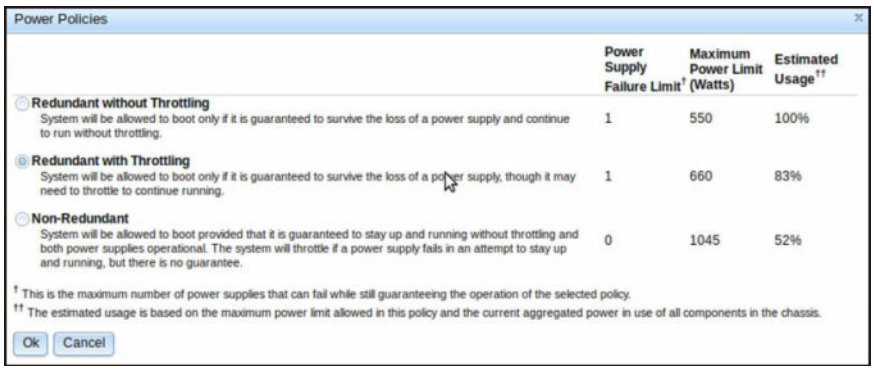
Les règles d'alimentation proposées sont les suivantes :

**Redundant without Throttling**
Le serveur est autorisé à s'amorcer s'il est assuré de supporter la perte d'alimentation électrique et de continuer à s'exécuter sans régulation.

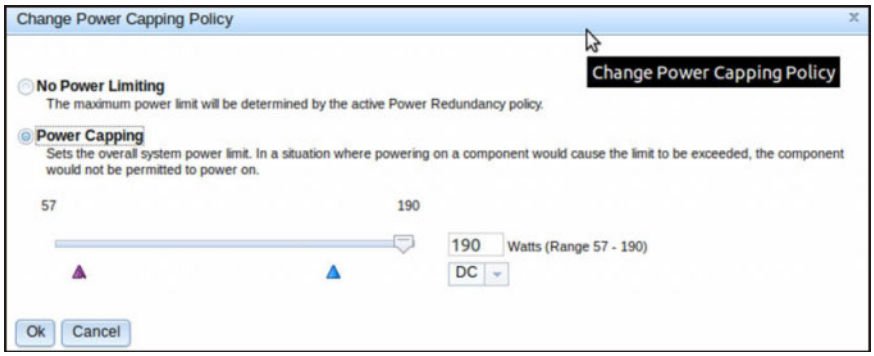
**Redundant with Throttling**
Le serveur est autorisé à s'amorcer s'il est assuré de supporter la perte d'alimentation électrique, même si une régulation est nécessaire pour continuer à s'exécuter.

**Non-Redundant**
Le serveur est autorisé à s'amorcer à condition qu'il puisse continuer à s'exécuter sans régulation et que les deux alimentations électriques soient opérationnelles. Le serveur se régule en cas de défaillance d'une alimentation électrique qui tenterait de continuer à s'exécuter ; il n'y a cependant aucune garantie.

La fenêtre ci-après s'affiche lorsque vous cliquez sur le bouton **Change** en regard de l'option Redundant with Throttling.



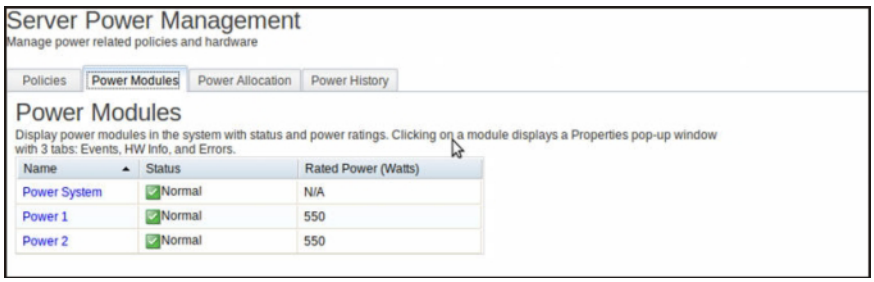

Avec Active Energy Manager, vous pouvez limiter la quantité totale d'alimentation que le serveur est autorisé à utiliser. Pour définir une limite d'utilisation de l'alimentation serveur, cliquez sur le bouton **Change** en regard de Current Policy pour l'option Power Limiting/Capping Policy dans la fenêtre Power Policies. La fenêtre Change Power Capping Policy s'ouvre (comme illustré ci-après).




Cliquez sur le bouton **Power Capping** et faites glisser le curseur sur la puissance souhaitée. La flèche située à droite au-dessous du curseur indique le réglage minimum qui peut être garanti par Active Energy Manager. La flèche située à gauche au-dessous du curseur indique l'utilisation électrique maximum du système au cours des dernières 24 heures. Les deux flèches permettent de définir une limite de plafonnement de puissance.

## Affichage des alimentations électriques actuellement installées

Cliquez sur l'onglet **Power Modules** pour afficher les informations relatives aux alimentations électriques actuellement installées (comme illustré ci-après).

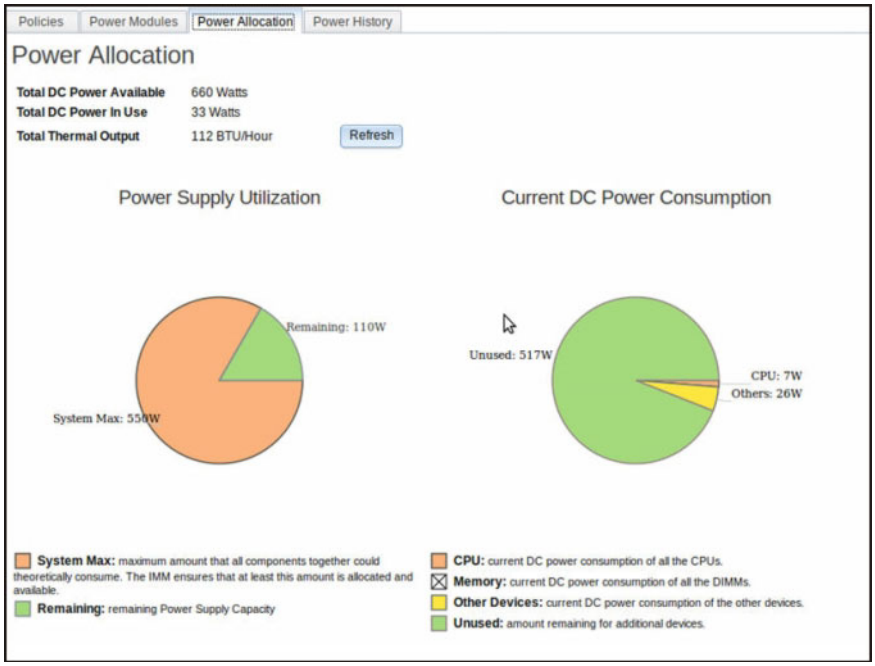



Le nom de chaque module d'alimentation présent sur le serveur est affiché accompagné de son statut et de sa puissance. Pour afficher des informations

supplémentaires sur un module d'alimentation, cliquez sur son nom. Une fenêtre Properties s'affiche avec trois onglets : Events, HW Info et Errors pour le module d'alimentation concerné.

## Affichage de la capacité de l'alimentation électrique

Cliquez sur l'onglet **Power Allocation** pour afficher la capacité d'alimentation électrique en cours d'utilisation et la consommation électrique en courant continu (CC) du serveur (comme illustré ci-après).




## Affichage de l'historique d'alimentation

Cliquez sur l'onglet **Power History** pour afficher la quantité d'énergie qui est utilisée par le système au cours d'une période sélectionnée. Depuis l'onglet **Chart** de la page Power History, vous pouvez sélectionner la période et vous avez aussi la possibilité de préciser si la puissance affichée doit être ac ou dc. L'utilisation minimum, moyenne et maximum de l'alimentation est affichée (comme illustrée ci-après).


Policies
Power Modules
Power Allocation
Power History
Power History
Chart
Table
The chart below shows the DC power consumption history. You can check the average, maximum, and minimum DC power for the system.
Previous hour
DC
Refresh
Power (watts)
Avg Max Min
Polling Interval: 5 Data Points
Note: Based on the polling interval and the trend period selected, if the total number of data points returned cannot be clearly displayed due to the width of this chart, some data points may be omitted and the time periods between those displayed may not match the chassis polling interval setting.

# Chapitre 7. Features on Demand

Les fonctions Features on Demand (FoD) du système IMM2 vous permettent d'installer et de gérer les fonctions facultatives de gestion du serveur et des systèmes.

Plusieurs niveaux de fonctions et fonctionnalités du microprogramme IMM2 sont disponibles sur votre serveur. Le niveau de fonctions du microprogramme IMM2 installé sur votre serveur varie en fonction du type de matériel. Pour plus d'informations sur le type de fonctions et matériel IMM2 de votre serveur, consultez la documentation fournie avec le serveur.

Vous pouvez mettre à niveau la fonctionnalité IMM2 en achetant et en installant une clé d'activation FoD. Pour obtenir des informations détaillées sur les fonctions FoD, consultez le guide *Features on Demand User's Guide* à l'adresse http://www.ibm.com/systems/x/fod/.

**Remarque :** Sur les serveurs équipés avec la fonctionnalité de base IMM2, une mise à niveau vers le modèle standard du module IMM d'IBM est requise avant de pouvoir effectuer une mise à niveau vers le modèle avancé.

Pour commander une clé d'activation FoD, contactez votre représentant ou partenaire commercial IBM ou rendez-vous sur le site http://www.ibm.com/systems/x/fod/.

Utilisez l'interface Web IMM2 ou l'interface de ligne de commande IMM2 pour installer manuellement une clé d'activation FoD vous permettant d'utiliser la fonction facultative achetée. Avant d'activer une clé :

- La clé d'activation FoD doit être sur le système que vous utilisez pour vous connecter au module IMM2.
- Vous devez avoir commandé l'option FoD et reçu son code d'autorisation par courrier ou courrier électronique.

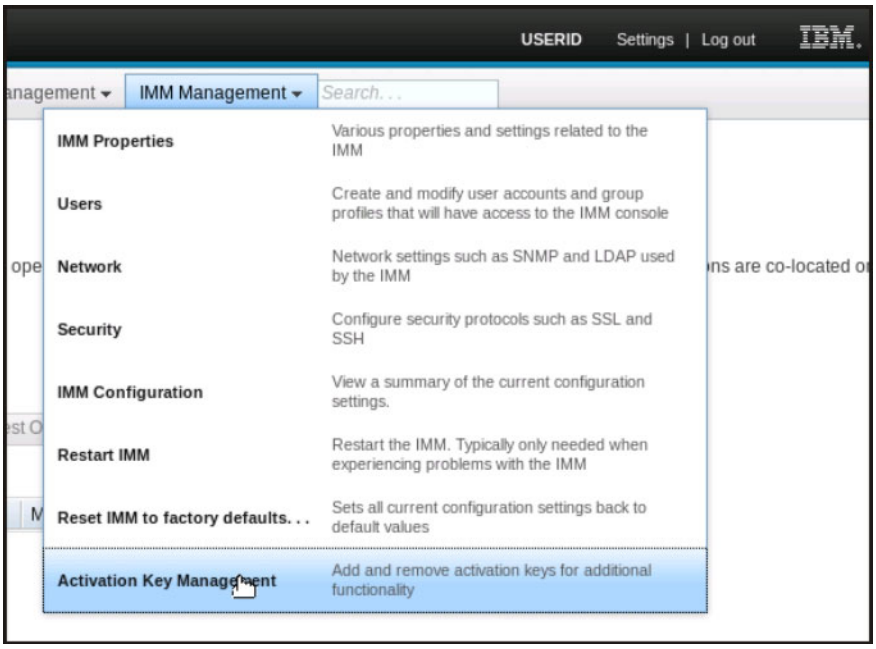
Pour obtenir des informations sur la gestion d'une clé d'activation FoD à l'aide de l'interface Web IMM2, voir «Installation d'une clé d'activation», «Suppression d'une clé d'activation», à la page 139 ou «Exportation d'une clé d'activation», à la page 141. Pour obtenir des informations sur la gestion d'une clé d'activation FoD à l'aide de l'interface de ligne de commande IMM2, voir «Commande keycfg», à la page 170.

## Installation d'une clé d'activation

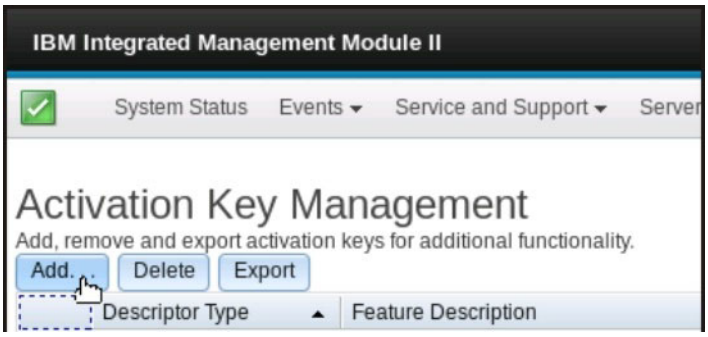
Installez une clé d'activation FoD pour ajouter une fonction facultative à votre serveur.

Pour installer une clé d'activation FoD, procédez comme suit.

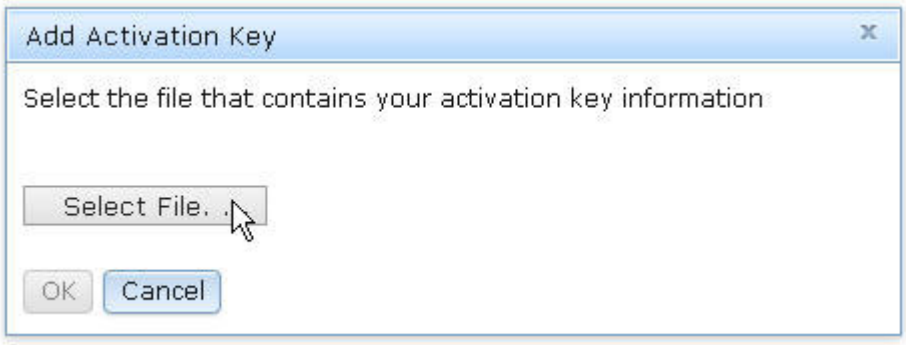
1. Connectez-vous au module IMM2. Pour plus d'informations, voir «Connexion au module IMM2», à la page 10.
2. Dans l'interface Web IMM2, cliquez sur l'onglet **IMM Management**, puis sur **Activation Key Management**.



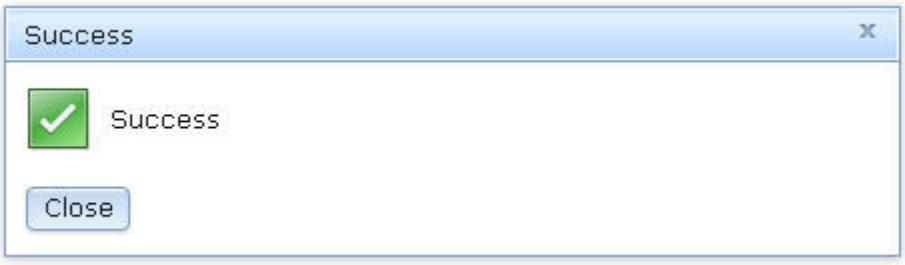

3. A partir de la page Activation Key Management, cliquez sur **Add...**.




4. Dans la fenêtre Add Activation Key, cliquez sur **Select File...**, puis sélectionnez le fichier de clé d'activation à ajouter dans la fenêtre File Upload et cliquez sur **Open** pour ajouter le fichier ou cliquez sur **Cancel** pour arrêter l'installation. Pour finaliser l'ajout de la clé, cliquez sur **OK** dans la fenêtre Add Activation Key ou cliquez sur **Cancel** pour arrêter l'installation.

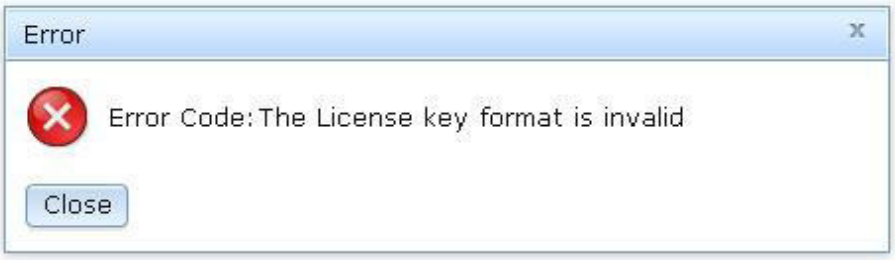



La fenêtre Success indique que la clé d'activation est installée.

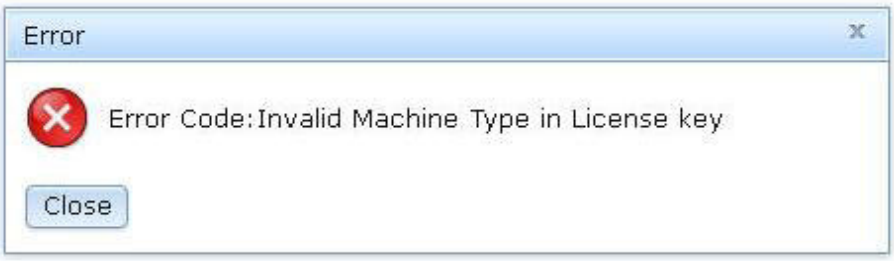



**Remarque :**

- Si la clé d'activation n'est pas valide, la fenêtre d'erreur suivante s'affiche.

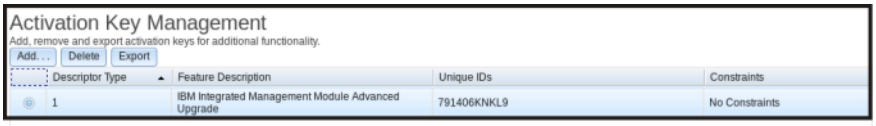



- Si vous tentez d'installer la clé d'activation sur un type de machine qui ne prend pas en charge la fonction FoD, la fenêtre d'erreur suivante s'affiche.




5. Cliquez sur **OK** pour fermer la fenêtre Success.

   La clé d'activation sélectionnée est ajoutée au serveur et apparaît dans la page Activation Key Management.

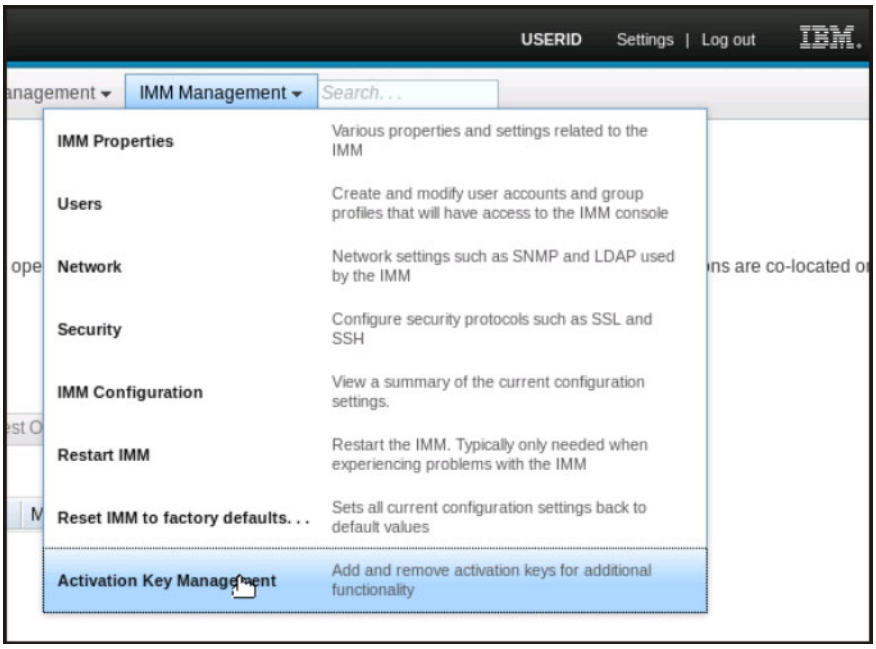



## Suppression d'une clé d'activation

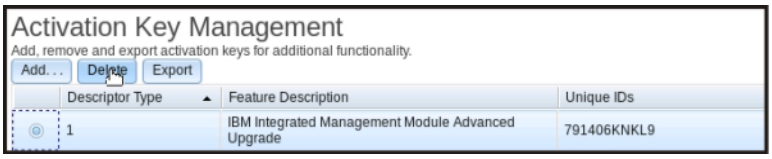
Supprimez une clé d'activation FoD pour supprimer une fonction facultative de votre serveur.

Pour supprimer une clé d'activation FoD, procédez comme suit.

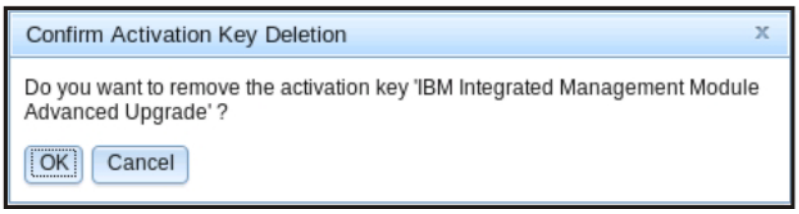
1. Connectez-vous au module IMM2. Pour plus d'informations, voir «Connexion au module IMM2», à la page 10.
2. Dans l'interface Web IMM2, cliquez sur l'onglet **IMM Management**, puis sur **Activation Key Management**.



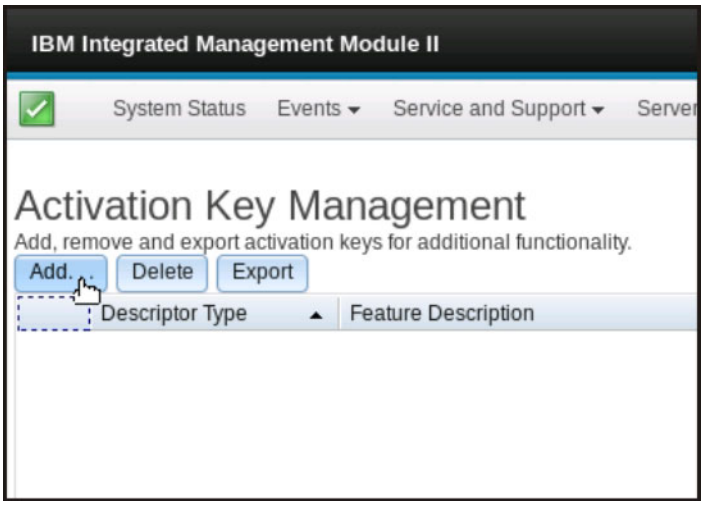

3. A partir de la page Activation Key Management, sélectionnez la clé d'activation à retirer, puis cliquez sur **Delete**.




4. Dans la fenêtre Confirm Activation Key Deletion, cliquez sur **OK** pour confirmer la suppression de la clé d'activation ou cliquez sur **Cancel** pour conserver le fichier de clés.




La clé d'activation sélectionnée est retirée du serveur et n'apparaît plus dans la page Activation Key Management.

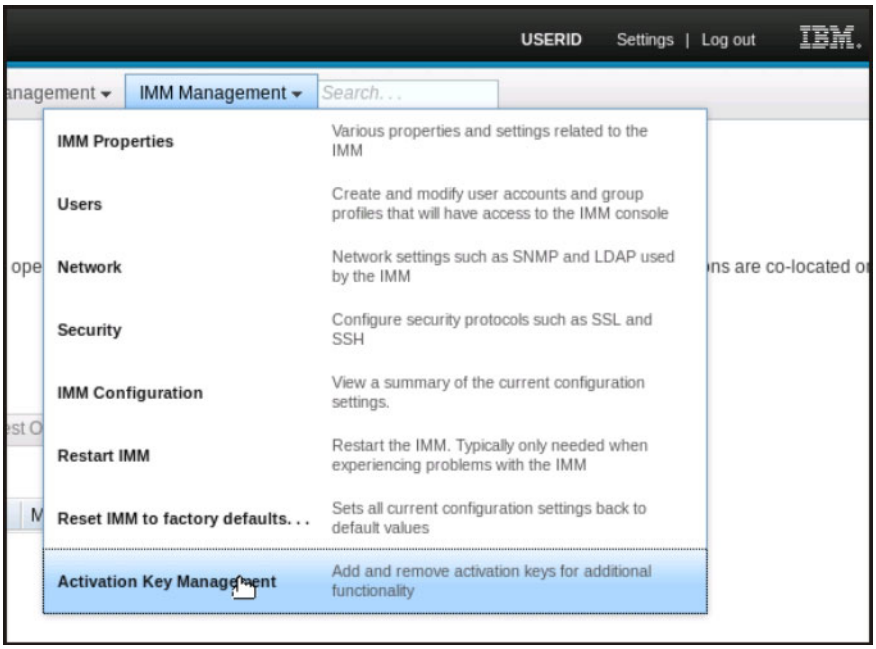



## Exportation d'une clé d'activation

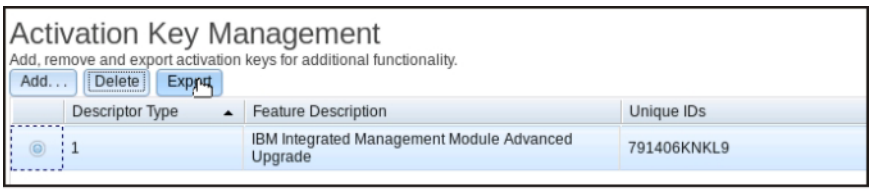
Exportez une clé d'activation FoD pour exporter une fonction facultative de votre serveur.

Pour exporter une clé d'activation FoD, procédez comme suit.

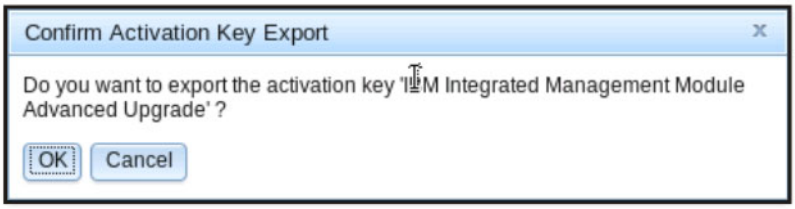
1. Connectez-vous au module IMM2. Pour plus d'informations, voir «Connexion au module IMM2», à la page 10.
2. Dans l'interface Web IMM2, cliquez sur l'onglet **IMM Management**, puis sur **Activation Key Management**.




3. A partir de la page Activation Key Management, sélectionnez la clé d'activation à exporter, puis cliquez sur **Export**.




4. Dans la fenêtre Confirm Activation Key Export, cliquez sur **OK** pour confirmer l'exportation de la clé d'activation ou cliquez sur **Cancel** pour annuler le demande d'exportation de clé.




5. Sélectionnez le répertoire de sauvegarde du fichier. La clé d'activation sélectionnée est exportée du serveur.

# Chapitre 8. Interface de ligne de commande

Vous pouvez utiliser l'interface de ligne de commande (CLI) d'IMM2 pour accéder au module IMM2 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 IMM2 avant de pouvoir lancer des commandes dans l'interface CLI.

## Gestion du module IMM2 avec IPMI

Le module IMM2 est livré avec l'ID utilisateur 1 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 :** Pour une sécurité accrue, modifiez ce nom d'utilisateur et ce mot de passe lors de votre configuration initiale.

Le module IMM2 fournit également des fonctions IPMI de gestion de serveur à distance :

**Interfaces de ligne de commande**
L'interface de ligne de commande fournit un accès direct aux fonctions de gestion de serveur via le protocole IPMI 2.0. Vous pouvez utiliser IPMItool pour émettre des commandes de contrôle de l'alimentation du serveur, afficher des informations sur le serveur et identifier le serveur. Pour plus d'informations sur IPMItool, voir «Utilisation d'IPMItool».

**SOL (Serial over LAN)**
Pour gérer des serveurs depuis un site distant, utilisez IPMItool afin d'établir une connexion SOL (Serial over LAN). Pour plus d'informations sur IPMItool, voir «Utilisation d'IPMItool».

### 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 le module IMM2.

Pour plus d'informations sur IPMItool ou pour le télécharger, visitez le site http://sourceforge.net/.

## Accès à l'interface de ligne de commande

Pour accéder à l'interface de ligne de commande, ouvrez une session Telnet ou SSH à l'adresse IP du module IMM2 (voir «Configuration de la redirection série à Telnet ou SSH», à la page 144 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 IMM2.
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 IMM2.

   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 déconnecté et la session prend fin.

## 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 IMM2 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. IMM2 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 (
```

Entrez la séquence de touche quitter pour revenir à l'interface de ligne de commande. Dans cet exemple, appuyez sur la touche Echap, puis entrez une parenthèse gauche. L'invite CLI s'affiche pour indiquer le retour à l'interface de ligne de commande IMM2.

```
system>
```

## 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 plusieurs 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 IMM2A00096B9E003A
-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 dans la configuration de votre système. 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> ?
```

## Liste des commandes par ordre alphabétique

Vous trouverez ci-après la liste complète de toutes les commandes de l'interface de ligne de commande IMM2, par ordre alphabétique :

## Commandes d'utilitaire

Les commandes d'utilitaire sont les suivantes :



### Commande exit

Utilisez la commande **exit** pour vous déconnecter et mettre fin à la session d'interface CLI.

### Commande help

Utilisez la commande **help** pour afficher la liste et une brève description de chacune des commandes. Vous pouvez également **?** 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 IMM2A00096B9E003A
-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 :

- «Commande clearlog»
- «Commande fans»
- «Commande ffdc», à la page 149
- «Commande led», à la page 150
- «Commande readlog», à la page 151
- «Commande show», à la page 153
- «Commande syshealth», à la page 153
- «Commande temps», à la page 153
- «Commande volts», à la page 154
- «Commande vpd», à la page 154

## Commande clearlog

Utilisez la commande **clearlog** pour effacer le journal des événements du module IMM2. 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 ffdc

Utilisez la commande **ffdc** (capture de données à la première défaillance) pour générer et transférer les données de service au support IBM.

La liste suivante montre les commandes pouvant être utilisées avec la commande **ffdc** :

- **generate**, crée un nouveau fichier de données de service
- **status**, vérifie l'état du fichier de données de service
- **copy**, copie les données de service existantes
- **delete**, supprime les données de service existantes

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -t | Numéro type | 1 (cliché de processeur) et 4 (données de service). La valeur par défaut est 1. |
| -f [1] | Répertoire cible sftp ou nom de fichier distant. | Pour sftp, utilisez le chemin d'accès complet ou le signe / de fin sur le nom de répertoire (~/ ou /tmp/). La valeur par défaut est le nom généré par le système. |
| --ip [1] | Adresse du serveur tftp/sftp | |
| -pn [1] | Numéro de port du serveur tftp/sftp | La valeur par défaut est 69/22. |
| -u [1] | Nom d'utilisateur du serveur sftp | |
| -pw [1] | Mot de passe du serveur sftp | |
| 1. Argument supplémentaire pour les commandes **generate** et **copy** | | |

Syntaxe :

```
ffdc [options]
option :
  -t 1 ou 4
  -f
  -ip adresse_ip
  -pn numéro_port
  -u nom_utilisateur
  -pw mot_de_passe
```

Exemple :

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
```

```
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_imm2_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_imm2_120926-105320.tgz
system>
```

## Commande led

Utilisez la commande **led** pour afficher et définir les états de voyants.

- L'exécution de la commande **led** sans option affiche l'état des voyants du panneau frontal.
- L'option de commande **led -d** doit être utilisée avec l'option de commande **led -identify on**.

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -l | Obtenir l'état de tous les voyants du système et de ses sous-composants | |
| -chklog | Désactiver le voyant de vérification des journaux | désactivé |
| -identify | Changer l'état du voyant d'identification du boîtier | désactivé, activé, clignotement |
| -d | Activer le voyant d'identification pour la période spécifiée | Période (secondes) |

Syntaxe :

```
led [options]
option :
  -l
  -chklog off
  -identify état
  -d temps
```

Exemple :

```
system> led
Fault                 Off
Identify              On            Blue
Chklog                Off
Power                 Off
```

```
system> led -l
Label                Location                State         Color
Battery              Planar                  Off
BMC Heartbeat        Planar                  Blink         Green
BRD                  Lightpath Card          Off
Channel A            Planar                  Off
Channel B            Planar                  Off
Channel C            Planar                  Off
Channel D            Planar                  Off
Channel E            Planar                  Off
Chklog               Front Panel             Off
CNFG                 Lightpath Card          Off
CPU                  Lightpath Card          Off
CPU 1                Planar                  Off
CPU 2                Planar                  Off
DASD                 Lightpath Card          Off
DIMM                 Lightpath Card          Off
DIMM 1               Planar                  Off
DIMM 10              Planar                  Off
DIMM 11              Planar                  Off
DIMM 12              Planar                  Off
DIMM 13              Planar                  Off
DIMM 14              Planar                  Off
DIMM 15              Planar                  Off
DIMM 16              Planar                  Off
DIMM 2               Planar                  Off
DIMM 3               Planar                  Off
DIMM 4               Planar                  Off
DIMM 5               Planar                  Off
DIMM 6               Planar                  Off
DIMM 7               Planar                  Off
DIMM 8               Planar                  Off
DIMM 9               Planar                  Off
FAN                  Lightpath Card          Off
FAN 1                Planar                  Off
FAN 2                Planar                  Off
FAN 3                Planar                  Off
Fault                Front Panel (+)         Off
Identify             Front Panel (+)         On            Blue
LINK                 Lightpath Card          Off
LOG                  Lightpath Card          Off
NMI                  Lightpath Card          Off
OVER SPEC            Lightpath Card          Off
PCI 1                FRU                     Off
PCI 2                FRU                     Off
PCI 3                FRU                     Off
PCI 4                FRU                     Off
Planar               Planar                  Off
Power                Front Panel (+)         Off
PS                   Lightpath Card          Off
RAID                 Lightpath Card          Off
Riser 1              Planar                  Off
Riser 2              Planar                  Off
SAS ERR              FRU                     Off
SAS MISSING          Planar                  Off
SP                   Lightpath Card          Off
TEMP                 Lightpath Card          Off
VRM                  Lightpath Card          Off
system>
```

## Commande readlog

Utilisez la commande **readlog** pour afficher les entrées du journal des événements IMM2 par groupe de cinq. 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 -a** affiche toutes les entrées dans le journal des événements, en commençant par les plus récentes.

**readlog -f** réinitialise le compteur et affiche les 5 premières entrées dans le journal des événements, en commençant par la plus récente.

**readlog -date** *date* affiche les entrées du journal des événements pour la date indiquée au format mm/jj/aa. Il peut s'agir d'une liste de dates séparées par des barres verticales (|).

**readlog -sev** *gravité* affiche les entrées du journal des événements pour le niveau de gravité indiqué (E, W, I). Il peut s'agir d'une liste de niveaux de gravité séparés par des barres verticales (|).

**readlog -i** *adresse_ip* définit l'adresse IP IPv4 ou IPv6 du serveur TFTP ou SFTP où le journal des événements est sauvegardé. Les options de commande **-i** et **-l** sont utilisées conjointement pour indiquer l'emplacement.

**readlog -l** *nom_fichier* définit le nom du fichier contenant le journal des événements. Les options de commande **-i** et **-l** sont utilisées conjointement pour indiquer l'emplacement.

**readlog -pn** *numéro_port* affiche ou définit le numéro de port du serveur TFTP ou SFTP (69/22 par défaut).

**readlog -u** *nom_utilisateur* indique le nom d'utilisateur du serveur SFTP.

**readlog -pw** *mot_de_passe* indique le mot de passe du serveur SFTP.

Syntaxe :

```
readlog [options]
option :
  -a
  -f
  -date date
  -sev gravité
  -i adresse_ip
  -l nom_fichier
  -pn numéro_port
  -u nom_utilisateur
  -pw mot_de_passe
```

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 show

Utilisez la commande **show** pour afficher les paramètres simples du module IMM2.

- La commande **show** affiche les valeurs définies à l'aide de la commande **set**.
- Les paramètres sont organisés comme une arborescence de répertoires. L'option de commande **show -r** permet d'afficher l'arborescence entière.
- Certains de ces paramètres, tels que les variables d'environnement, sont utilisés par l'interface de ligne de commande.

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| *valeur* | Chemin d'accès ou valeur de paramètre à afficher | |
| -r | Afficher les paramètres de manière récursive | |

Syntaxe :

```
show [options]
option :
  valeur
  -r
```

## Commande syshealth

Utilisez la commande **syshealth** pour afficher un récapitulatif de l'état de santé du serveur. L'état d'alimentation, l'état du système, le nombre de redémarrages et l'état du logiciel IMM2 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  90/32
DASD1  66/19  73/23  82/28  88/31  92/33
Amb    59/15  70/21  83/28  90/32  95/35
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 IMM2 (imm), pour le système BIOS du serveur (uefi), pour le programme Dynamic System Analysis Preboot du serveur(dsa), pour le microprogramme serveur (fw) et pour les composants serveur (comp). Les informations qui s'affichent sont les mêmes que dans l'interface Web.

Syntaxe :

```
vpd [options]
option :
  -sys
  -imm
```

```
-uefi
-dsa
-fw
-comp
```

Utilisez la commande vpd pour afficher les données techniques essentielles des différents composants du serveur.

| Option | Description |
|---|---|
| -sys | Affiche les données techniques essentielles du système |
| -imm | Affiche les données techniques essentielles du contrôleur IMM2 |
| -uefi | Affiche les données techniques essentielles du système BIOS |
| -dsa | Affiche les données techniques essentielles Diag |
| -fw | Affiche les données techniques essentielles du microprogramme du système |
| -comp | Affiche les données techniques essentielles des composants système |

Exemple :

```
system> vpd -dsa
Type     Version      Build     ReleaseDate
----     -------      -----     ------
DSA      9,25         DSYTA5A   2012/07/31
system>
```

# Commande de contrôle de l'alimentation et du redémarrage du serveur

Les commandes d'alimentation et de redémarrage du serveur sont les suivantes :

- «Commande power»
- «Commande pxeboot», à la page 156
- «Commande reset», à la page 156

## 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 pxeboot

Utilisez la commande **pxeboot** pour afficher et définir la condition du PXE (Preboot eXecution Environment).

L'exécution de **pxeboot** sans option renvoie les paramètres actuels du Preboot eXecution Environment. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -en | Définit la condition du Preboot eXecution Environment pour le prochain redémarrage du système | enabled, disabled |

Syntaxe :

```
pxeboot [options]
option :
  -en état
```

Exemple :

```
system> pxeboot
-en disabled
system>
```

## 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 : la «Commande console».

## Commande console

Utilisez la commande **console** pour lancer un session console de redirection série vers le port série IMM2 désigné.

Syntaxe :

```
console 1
```

# Commandes de configuration

Les commandes de configuration sont les suivantes :

- «Commande accseccfg», à la page 157
- «Commande alertcfg», à la page 159
- «Commande asu», à la page 160

## Commande accseccfg

Utilisez la commande **accseccfg** pour afficher et configurer les paramètres de sécurité de compte.

L'exécution de la commande **accseccfg** sans option affiche toutes les informations de sécurité des comptes. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -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 | |

| Option | Description | Valeurs |
|---|---|---|
| -custom | Définit la sécurité du compte d'après les valeurs définies par l'utilisateur | |
| -am | Définit la méthode d'authentification des utilisateurs | local, ldap, localldap, ldaplocal |
| -lp | Période de verrouillage après maximum d'erreurs de connexion (minutes) | 0, 1, 2, 5, 10, 15, 20, 30, 60, 120, 180 ou 240 minutes. La valeur par défaut est 60 si l'option "High Security" est activée et 2 si l'option "Legacy Security" est activée. La valeur zéro désactive cette fonction. |
| -pe | Délai d'expiration du mot de passe (jours) | 0 à 365 jours |
| -pr | Mot de passe requis | On, Off (activé/désactivé) |
| -pc | Règles de complexité des mots de passe | On, Off (activé/désactivé) |
| -pd | Nombre minimal de caractères différents du mot de passe | 0 à 19 caractères |
| -pl | Longueur du mot de passe | 1 à 20 caractères |
| -ci | Intervalle minimum de changement de mot de passe (heures) | 0 à 240 heures |
| -lf | Nombre maximal d'échecs de connexion | 0 à 10 |
| -chgdft | Modifier le mot de passe par défaut après la première connexion | On, Off (activé/désactivé) |
| -chgnew | Modifier le mot de passe du nouvel utilisateur après la première connexion | On, Off (activé/désactivé) |
| -rc | Cycle de réutilisation du mot de passe | 0 à 5 |
| -wt | Délai d'attente de session en cas d'inactivité Web (minutes) | 1, 5, 10, 15, 20, none ou user |

Syntaxe :

```
accseccfg [options]
option :
  -legacy
  -high
  -custom
  -am méthode_authentification
  -lp période_verrouillage
  -pe période_temps
  -pr état
  -pc état
  -pd nombre_caractères
  -pl nombre_caractères
```

```
  -ci intervalle_minimum
  -lf nombre_échecs
  -chgdft état
  -chgnew état
  -rc cycle_réutilisation
  -wt délai
```

Exemple :

```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

## Commande alertcfg

Utilisez la commande **alertcfg** pour afficher et configurer les paramètres d'alerte à distance IMM2 globaux.

L'exécution de la commande **alertcfg** sans option affiche tous les paramètres d'alerte à distance globaux. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -dr | Définit le temps d'attente entre deux tentatives avant que le module IMM2 renvoie une alerte | 0 à 4,0 minutes, par incréments de 0,5 minute |
| -da | Définit le temps d'attente avant que le module IMM2 envoie une alerte au prochain destinataire de la liste | 0 à 4,0 minutes, par incréments de 0,5 minute |
| -rl | Définit combien de fois le module IMM2 tentera d'envoyer un alerte, si les tentatives précédentes ont échoué | 0 à 8 |

Syntaxe :

```
alertcfg [options]
  options :
   -rl limite_tentatives
   -dr délai_tentative
   -da délai_agent
```

Exemple :

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

## Commande asu

Les commandes asu (Advanced Settings Utility) sont utilisées pour définir les paramètres UEFI. Le système hôte doit être redémarré pour que les modifications des paramètres UEFI prennent effet.

Le tableau suivant contient un sous-ensemble de commandes pouvant être utilisé avec la commande **asu**.

*Tableau 7. Commandes asu*

| Commande | Description | Valeur |
|---|---|---|
| delete | Utilisez cette commande pour supprimer une instance ou un enregistrement de paramètre. Le paramètre doit être une instance qui autorise la suppression, par exemple, iSCSI.AttemptName.1. | *paramètre_instance* |
| help | Utilisez cette commande pour afficher des informations d'aide pour un ou plusieurs paramètres. | *paramètre* |
| set | Utilisez cette commande pour modifier la valeur d'un paramètre. Définissez le paramètre UEFI à la valeur d'entrée.<br>**Remarques :**<br>• Définissez une ou plusieurs paires paramètre/valeur.<br>• Le paramètre peut contenir des caractères génériques s'il se développe en un seul paramètre.<br>• La valeur doit être placée entre guillemets si elle contient des espaces.<br>• Les valeurs de liste triées sont séparées par le symbole égal (=). Par exemple, set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network." | *valeur de paramètre* |

*Tableau 7. Commandes asu (suite)*

| Commande | Description | Valeur |
|---|---|---|
| showgroups | Utilisez cette commande pour afficher les groupes de paramètres disponibles. Cette commande affiche les noms des groupes connus. Les noms de groupes peuvent varier en fonction des périphériques installés. | *paramètre* |
| show | Utilisez cette commande pour afficher la valeur actuelle d'un ou plusieurs paramètres. | *paramètre* |
| showvalues | Utilisez cette commande pour afficher toutes les valeurs possibles d'un ou plusieurs paramètres.<br>**Remarques :**<br>• Cette commande affiche des informations sur les valeurs admises pour le paramètre.<br>• Le minimum et le maximum d'instances autorisé pour le paramètre s'affiche.<br>• La valeur par défaut s'affiche, si disponible.<br>• La valeur par défaut est entourée des signes inférieur et supérieur (< et >).<br>• Les valeurs textuelles affichent la longueur minimale et maximale et l'expression régulière. | *paramètre* |
| **Remarques :**<br>• Dans la syntaxe de commande, *paramètre* est le nom d'un paramètre que vous souhaitez afficher ou modifier, et *valeur* est la valeur que vous placez sur le paramètre.<br>• *Paramètre* peut contenir plus d'un nom, sauf lorsque vous utilisez la commande **set**.<br>• *Paramètre* peut contenir des caractères génériques, par exemple, un astérisque (*) ou un point d'interrogation (?).<br>• *Paramètre* peut être un groupe, un nom de paramètre ou **all** (tous). | | |

La liste suivante présente quelques exemples de la syntaxe de commande **asu** :

- Pour afficher toutes les options de commande asu, entrez `asu --help`.
- Pour afficher l'aide détaillée pour toutes les commandes, entrez `asu -v --help`.
- Pour afficher l'aide détaillée pour une commande, entrez `asu -v set --help`.
- Pour modifier une valeur, entrez `asu set` *`valeur de paramètre`*.
- Pour afficher la valeur en cours, entrez `asu show` *`paramètre`*.
- Pour afficher les paramètres au format long par lots, entrez `asu show -l -b all`

- Pour afficher toutes les valeurs possibles pour un paramètre, entrez `asu showvalues` *`paramètre`*.

  Exemple de commande **show values** :

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -b[1] | Affichage au format par lots | |
| --help[3] | Affichage de l'utilisation de la commande et de ses options. L'option --help est placée avant la commande, par exemple **asu --help show**. | |
| --help[3] | Affichage de l'aide pour la commande. L'option --help est placée après la commande, par exemple **asu show --help**. | |
| -l[1] | Nom de paramètre au format long (inclure le jeu de configuration). | |
| -m[1] | Nom de paramètre au format mixte (utiliser l'ID de configuration). | |
| -v[2] | Sortie détaillée. | |

1. Les options -b, -l et -m sont uniquement utilisées avec les commandes **show**.
2. L'option -v est uniquement utilisée entre **asu** et la commande.
3. L'option --help peut être utilisée avec n'importe quelle commande.

Syntaxe :

```
asu [options] commande [cmdopts]
options :
   -v sortie détaillée
   --help affichage de l'aide principale
cmdopts :
   --help aide de la commande
```

**Remarque :** Pour plus d'options de commandes, voir les commandes individuelles.

Utilisez les commandes de transaction asu pour définir plusieurs paramètres UEFI et créer et exécuter les commandes en mode de traitement par lots. Utilisez les commandes **tropen** et **trset** pour créer un fichier de transaction contenant plusieurs paramètres à appliquer. Une transaction avec un ID donné est ouverte à l'aide de la commande **tropen**. Les paramètres sont ajoutés au jeu à l'aide de la commande **trset**. La transaction terminée est validée à l'aide de la commande **trcommit**. Une fois la transaction terminée, vous pouvez la supprimer à l'aide de la commande **trrm**.

**Remarque :** L'opération de restauration des paramètres UEFI créera une transaction avec un ID utilisant un numéro aléatoire à trois chiffres.

Le tableau suivant contient les commandes de transaction pouvant être utilisées avec la commande **asu**.

*Tableau 8. Commandes de transaction*

| Commande | Description | Valeur |
|---|---|---|
| tropen *id* | Cette commande crée un nouveau fichier de transaction contenant plusieurs paramètres à définir. | *Id* est la chaîne identifiante, 1 à 3 caractères alphanumériques. |
| trset *id* | Cette commande ajoute un ou plusieurs paramètres ou paires de valeurs à une transaction. | *Id* est la chaîne identifiante, 1 à 3 caractères alphanumériques. |
| trlist *id* | Cette commande affiche d'abord le contenu du fichier de transaction. Cela peut être utile lorsque le fichier de transaction est créé dans l'interpréteur de ligne de commande. | *Id* est la chaîne identifiante, 1 à 3 caractères alphanumériques. |
| trcommit *ID* | Cette commande valide et exécute le contenu du fichier de transaction. Les résultats de l'exécution et les erreurs seront affichés. | *Id* est la chaîne identifiante, 1 à 3 caractères alphanumériques. |
| trrm *id* | Cette commande supprime le fichier de transaction après avoir été validé. | *Id* est la chaîne identifiante, 1 à 3 caractères alphanumériques. |

Exemple d'établissement de plusieurs paramètres UEFI :

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

## Commande backup

Utilisez la commande **backup** pour créer un fichier de sauvegarde contenant les paramètres de sécurité actuels du système.

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -f | Nom du fichier de sauvegarde | Nom de fichier valide |

| Option | Description | Valeurs |
|---|---|---|
| -pp | Mot de passe ou phrase passe utilisé(e) pour chiffrer les mots de passe dans le fichier de sauvegarde | Mot de passe valide ou phrase passe entre guillemets |
| -ip | Adresse IP du serveur TFTP/SFTP | Adresse IP valide |
| -pn | Numéro de port du serveur TFTP/SFTP | Numéro de port valide (par défaut 69/22) |
| -u | Nom d'utilisateur du serveur SFTP | Nom d'utilisateur valide |
| -pw | Mot de passe du serveur SFTP | Mot de passe valide |
| -fd | Nom de fichier pour la description XML des commandes CLI de sauvegarde | Nom de fichier valide |

Syntaxe :

```
backup [options]
option :
  -f nom_de_fichier
  -pp mot_de_passe
  -ip adresse_ip
  -pn numéro_port
  -u nom_utilisateur
  -pw mot_de_passe
  -fd nom_de_fichier
```

Exemple :

```
system> backup –f imm-back.cli –pp xxxxxx –ip 192.168.70.200
ok
system>
```

## 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     : IMM2A-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 |
| -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 et définir la configuration DNS du module IMM2.

L'exécution de la commande **dns** sans option affiche toute l'information sur la configuration DNS. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -state | Etat du DNS | On, Off (activé/désactivé) |
| -ddns | Etat du DDNS | enabled, disabled |
| -i1 | Adresse IP du serveur DNS IPv4 principal | Adresse IP au format d'adresse IP à notation décimale à point. |
| -i2 | Adresse IP du serveur DNS IPv4 secondaire | Adresse IP au format d'adresse IP à notation décimale à point. |
| -i3 | Adresse IP du serveur DNS IPv4 tertiaire | Adresse IP au format d'adresse IP à notation décimale à point. |
| -i61 | Adresse IP du serveur DNS IPv6 principal | Adresse IP au format IPv6. |
| -i62 | Adresse IP du serveur DNS IPv6 secondaire | Adresse IP au format IPv6. |
| -i63 | Adresse IP du serveur DNS IPv6 tertiaire | Adresse IP au format IPv6. |
| -p | Priorité IPv4/IPv6 | ipv4, ipv6 |

Syntaxe :

```
dns [options]
option :
  -state état
  -ddns état
  -i1 première_adresse_ip_ipv4
  -i2 seconde_adresse_ip_ipv4
  -i3 troisième_adresse_ip_ipv4
  -i61 première_adresse_ip_ipv6
  -i62 seconde_adresse_ip_ipv6
  -i63 troisième_adresse_ip_ipv6
  -p priorité
```

**Remarque :** L'exemple suivant présente une configuration IMM2 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
-ddn    : ibm.com
-ddncur  : ibm.com
-dnsrc  : dhcp
-p     : ipv6

system>
```

La tableau suivant décrit la sortie de cet exemple.

| Option | Description |
|---|---|
| -state | Etat du DNS (on ou off) |
| -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) |
| -ddn | DDN spécifié manuellement |
| -ddncur | DDN en cours (lecture seule) |
| -p | Serveurs DNS préférés (ipv4 or ipv6) |

## Commande ethtousb

Utilisez la commande **ethtousb** pour afficher et configurer le mappage de port Ethernet vers Ethernet-via-USB.

La commande vous permet de mapper un numéro de port Ethernet externe à un numéro de port différent Ethernet-via-USB.

L'exécution de la commande **ethtousb** sans option affiche l'information sur Ethernet-via-USB. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -en | Etat de Ethernet-via-USB | enabled, disabled |
| -m*x* | Configurer le mappage de port pour l'index *x* | Paire de ports, séparés par deux points (:), au format *port1:port2*<br><br>Où :<br>• Le numéro d'index de port, *x*, est spécifié en tant que nombre entier compris entre 1 et 10 dans l'option de commande.<br>• *port1* de la paire de ports correspond au numéro de port Ethernet externe.<br>• *port2* de la paire de ports correspond au numéro de port Ethernet-via-USB. |
| -rm | Supprimer le mappage de port pour l'index indiqué | 1 à 10<br><br>Les index de mappage de port sont affichés à l'aide de la commande **ethtousb** sans option. |

Syntaxe :

```
ethtousb [options]
option :
  -en état
  -mx paire_de_ports
  -rm index_mappage
```

Exemple :

```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

## Commande gprofile

Utilisez la commande **gprofile** pour afficher et configurer les profils de groupe pour le module IMM2.

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. |

| Option | Description | Valeurs |
|---|---|---|
| -a | Niveau d'autorisation basé sur les rôles | supervisor, operator, rbs <role list>: nsc \| am \| rca \| rcvma \| pr \| bc \| cel \| ac<br><br>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 [numéro_emplacement_profil_de_groupe 1 - 16] [options]
options :
-clear état
-n  nom_groupe
-a  niveau d'autorisation:
    -nsc réseau et sécurité
    -am gestion des comptes utilisateurs
    -rca accès à la console distante
    -rcvma accès à la console distante et au disque distant
    -pr accès au démarrage/redémarrage du serveur à distance
    -bc configuration de l'adaptateur de base
    -cel possibilité d'effacer les journaux des événements
    -ac configuration d'adaptateur avancée
-h aide
```

## 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 |
| -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. |
| -r | Débit de données | 10, 100, auto |
| -d | Mode duplex | full, half, auto |
| -m | MTU | Valeur numérique comprise entre 60 et 1500 |

| Option | Description | Valeurs |
|---|---|---|
| -l | LAA | Format d'adresse MAC. Les adresses de multidiffusion ne sont pas autorisés (le premier octet doit être pair). |
| -dn | Nom de domaine | Nom de domaine avec format valide |
| -auto | Paramètre de négociation automatique qui détermine si les paramètres réseau Data rate et Duplex sont configurables | true, false |
| -nic | Accès réseau | partagé, dédié |
| -address_table | Table des adresses IPv6 générées automatiquement et de leurs longueurs de préfixes<br>**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. |
| -ipv6 | Etat IPv6 | disabled, enabled |
| -lla | Adresse lien-local<br>**Remarque :** L'adresse lien-local n'apparaît que si IPv6 est activé. | L'adresse lien-local est déterminée par IMM2. 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 |

Syntaxe :

```
ifconfig eth0 [options]
options :
  -state état_interface
  -c méthode_config
  -i adresse_ip_ipv4_statique
  -g adresse_passerelle_ipv4
  -s masque_sous-réseau
  -n nom_hôte
  -r débit_données
  -d mode_duplex
  -m max_unité_transmission
  -l MAC_administré_localement
  -dn nom_domaine
  -auto état
  -nic état
  -address_table
  -ipv6 état
  -ipv6static état
```

```
-sa6 état
-i6 adresse_ip_ipv6_statique
-g6 adresse_passerelle_ipv6
-p6 longueur
```

Exemple :

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-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 IMM2.
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 keycfg

Utilisez la commande **keycfg** pour afficher, ajouter ou supprimer les clés d'activation. Ces clés contrôlent l'accès aux fonctions facultatives IMM2 Features on Demand (FoD).

- Lorsque **keycfg** est exécutée sans option, la liste des clés d'activation installées s'affiche. L'information sur les clés qui s'affiche inclut un numéro d'index pour chaque clé d'activation, le type de clé d'activation, la date à laquelle la clé a été validée, le nombre d'utilisations restantes, l'état de la clé et une description de la clé.
- Ajouter de nouvelles clés d'activation par le biais de transfert de fichier.
- Supprimer d'anciennes clés en indiquant le numéro de la clé ou le type de clé. Lorsque les clés sont supprimées par type, seule la première clé d'un type défini est supprimée.

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -add | Ajouter une clé d'activation | Valeurs des options de commandes -ip, -pn, -u, -pw et -f. |
| -ip | Adresse IP du serveur TFTP avec clé d'activation à ajouter | Adresse IP valide du serveur TFTP. |
| -pn | Numéro de port du serveur TFTP/SFTP avec clé d'activation à ajouter | Numéro de port valide du serveur TFTP/SFTP (69/22 par défaut). |
| -u | Nom d'utilisateur du serveur SFTP avec clé d'activation à ajouter | Nom d'utilisateur valide du serveur SFTP. |

| Option | Description | Valeurs |
|---|---|---|
| -pw | Mot de passe du serveur SFTP avec clé d'activation à ajouter | Mot de passe valide du serveur SFTP. |
| -f | Nom de fichier de la clé d'activation à ajouter | Nom de fichier valide du fichier de la clé d'activation. |
| -del | Supprimer une clé d'activation par numéro d'index | Numéro d'index de la clé d'activation valide de la liste **keycfg**. |
| -deltype | Supprimer une clé d'activation par type de clé | Valeur de type de clé valide. |

Syntaxe :

```
keycfg [options]
option :
  -add
     -ip adresse_ip
     -pn numéro_port
     -u nom_utilisateur
     -pw mot_de_passe
     -f nom_de_fichier
  -del index_clé
  -deltype type_clé
```

Exemple :

```
system> keycfg
ID  Type  Valid         Uses  Status   Description
1   4     10/10/2010    5     "valid"  "IMM remote presence"
2   3     10/20/2010    2     "valid"  "IMM feature"
system>
```

## 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 |
|---|---|---|
| -a | Méthode d'authentification d'utilisateur | local only, LDAP only, local first then LDAP, LDAP first then local |
| -aom | Mode d'authentification uniquement | enabled, disabled |
| -b | Méthode de liaison | anonymous, bind with ClientDN and password, bind with Login Credential |
| -c | Nom distinctif du client | Chaîne pouvant comprendre jusqu'à 127 caractères pour *nom_distinctif_client* |
| -d | Domaine de recherche | Chaîne pouvant comprendre jusqu'à 63 caractères pour *domaine_recherche* |
| -f | Filtre de groupe | Chaîne pouvant comprendre jusqu'à 127 caractères pour *filtre_groupe* |

| Option | Description | Valeurs |
|---|---|---|
| -fn | Nom de la forêt | Pour environnements Active Directory. Chaîne pouvant comprendre jusqu'à 127 caractères. |
| -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* |
| -pc | Confirme le mot de passe du client | Chaîne pouvant comprendre jusqu'à 15 caractères pour *confirmation_mot_de_passe*<br><br>Syntaxe de la commande : ldap -p *mot_de_passe_client* -pc *confirmation_mot_de_passe*<br><br>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*. La commande échoue si les arguments ne concordent pas. |
| -r | Nom distinctif d'entrée racine (DN) | Chaîne pouvant comprendre jusqu'à 127 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 127 caractères ou adresse IP pour *nom_d'hôte/adresse_IP* |
| -s2ip | Nom d'hôte/adresse IP de Server 2 | Chaîne pouvant comporter jusqu'à 127 caractères ou adresse IP pour *nom_d'hôte/adresse_IP* |
| -s3ip | Nom d'hôte/adresse IP de Server 3 | Chaîne pouvant comporter jusqu'à 127 caractères ou adresse IP pour *nom_d'hôte/adresse_IP* |
| -s4ip | Nom d'hôte/adresse IP de Server 4 | Chaîne pouvant comporter jusqu'à 127 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 l'outil du composant logiciel enfichable Role-Based Security (RBS). |
| -u | Attribut de recherche d'UID | Chaîne pouvant comprendre jusqu'à 63 caractères pour *attribut_recherche* |
| -v | Obtention de l'adresse du serveur LDAP via DNS | off, on |

| Option | Description | Valeurs |
|---|---|---|
| -h | Affiche la syntaxe et les options de la commande | |

Syntaxe :

```
ldap [options]
options :
   -a loc|ldap|locld|ldloc
   -aom activer/désactivé
   -b anon|client|login
   -c nom_distinctif_client
   -d domaine_de_recherche
   -f filtre_groupe
   -fn nom_forêt
   -g attribut_recherche_groupe
   -l chaîne
   -p mot_de_passe_client
   -pc confirmation_mot_de_passe
   -r nom_distinctif_racine
   -rbs activer/désactivé
   -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[1] | Nom ou adresse IP du serveur Network Time Protocol. Il s'agit du numéro d'index du serveur Network Time Protocol. | Nom du serveur NTP à utiliser pour la synchronisation d'horloge. L'intervalle des numéros d'index du serveur NTP est de -i1 à -i4. |
| -f | La fréquence (en minutes) à laquelle l'horloge IMM2 est synchronisée 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. |

| Option | Description | Valeurs |
|---|---|---|
| 1. -i correspond à i1. | | |

Syntaxe :

```
ntp [options]
options :
-en état
-i  nom d'hôte/adresse_ip
-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
```

## Commandes ports

Utilisez la commande **ports** pour afficher et configurer les ports IMM2.

L'exécution de la commande **ports** sans option affiche des informations sur tous les ports IMM2. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -open | Afficher les ports ouverts | |
| -reset | Restaurer les ports aux paramètres par défaut | |
| -httpp | Numéro de port HTTP | Numéro de port par défaut : 80 |
| -httpsp | Numéro de port HTTPS | Numéro de port par défaut : 443 |
| -telnetp | Numéro de port CLI existant Telnet | Numéro de port par défaut : 23 |
| -sshp | Numéro de port CLI existant SSH | Numéro de port par défaut : 22 |
| -snmpap | Numéro de port de l'agent SNMP | Numéro de port par défaut : 161 |
| -snmptp | Numéro de port d'alertes SNMP | Numéro de port par défaut : 162 |
| -rpp | Numéro de port d'intervention à distance | Numéro de port par défaut : 3900 |
| -cimhp | Numéro de port CIM via HTTP | Numéro de port par défaut : 5988 |
| -cimhsp | Port CIM via HTTPS | Numéro de port par défaut : 5989 |

Syntaxe :

```
ports [options]
option :
  -open
  -reset
  -httpp numéro_port
  -httpsp numéro_port
  -telnetp numéro_port
  -sshp numéro_port
  -snmpap numéro_port
  -snmptp numéro_port
  -rpp numéro_port
  -cimhp numéro_port
  -cimhsp numéro_port
```

Exemple :

```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
```

```
-snmptp 162
-sshp 22
-telnetp 23
-cimhp 5988
-cimhsp 5989
system>
```

## Commande portcfg

Utilisez la commande **portcfg** pour configurer IMM2 pour la fonction de redirection série.

Le module IMM2 doit être configuré pour correspondre aux paramètres du port série interne du serveur. 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.

**Remarque :** Le port série externe du serveur peut uniquement être utilisé par le module IMM2 pour la fonctionnalité IPMI. L'interface CLI n'est pas prise en charge via le port série. Les options **serred** et **cliauth** présentes dans l'interface CLI du Remote Supervisor Adapter II ne sont pas prises en charge.

L'exécution de la commande **portcfg** sans option affiche la configuration du port série. Le tableau suivant présente les arguments pour les options.

**Remarque :** Le nombre de bits d'information (8) est défini dans le matériel et ne peut pas être modifié.

| Option | Description | Valeurs |
|---|---|---|
| -b | Débit en bauds | 9600, 19200, 38400, 57600, 115200 |
| -p | Parité | none, odd, even |
| -s | Bits d'arrêt | 1, 2 |
| -climode | Mode CLI | 0, 1, 2<br>Où :<br>• 0 = none : l'interface de ligne de commande est désactivée<br>• 1 = cliems : l'interface de ligne de commande est activée avec des séquences de touches compatibles avec EMS<br>• 2 = cliuser : l'interface de ligne de commande est activée avec des séquences de touches définies par l'utilisateur |

Syntaxe :

```
portcfg [options]
 options :
   -b débit en bauds
   -p parité
   -s bits d'arrêt
   -climode mode
```

Exemple :

```
system> portcfg
-b       :    57600
-climode :    2 (CLI with user defined keystroke sequence)
-p  :    even
-s       :    1
system> portcfg -b 38400
ok
system>
```

## Commande restore

Utilisez la commande **restore** pour restaurer les paramètres systèmes à partir d'un fichier de sauvegarde.

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -f | Nom du fichier de sauvegarde | Nom de fichier valide |
| -pp | Mot de passe ou phrase passe utilisé(e) pour chiffrer les mots de passe dans le fichier de sauvegarde | Mot de passe valide ou phrase passe entre guillemets |
| -ip | Adresse IP du serveur TFTP/SFTP | Adresse IP valide |
| -pn | Numéro de port du serveur TFTP/SFTP | Numéro de port valide (par défaut 69/22) |
| -u | Nom d'utilisateur du serveur SFTP | Nom d'utilisateur valide |
| -pw | Mot de passe du serveur SFTP | Mot de passe valide |

Syntaxe :

```
restore [options]
option :
  -f nom_de_fichier
  -pp mot_de_passe
  -ip adresse_ip
  -pn numéro_port
  -u nom_utilisateur
  -pw mot_de_passe
```

Exemple :

```
system> restore –f imm-back.cli –pp xxxxxx –ip 192.168.70.200
ok
system>
```

## Commande restoredefaults

Utilisez la commande **restoredefaults** pour restaurer tous les paramètres IMM2 aux paramètres usines par défaut.

- La commande **restoredefaults** ne possède aucune option.
- Il vous sera demandé pour confirmer la commande avant son traitement.

Syntaxe :

```
restoredefaults
```

Exemple :

```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults...
```

## Commande set

Utilisez la commande **set** pour modifier les paramètres du module IMM2.

- Certains paramètres du module IMM2 peuvent être modifiés à l'aide d'une simple commande **set**.
- Certains de ces paramètres, tels que les variables d'environnement, sont utilisés par l'interface de ligne de commande.
- Utilisez la commande **show** pour afficher les valeurs définies à l'aide de la commande **set**.

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| *valeur* | Définit une valeur pour le chemin d'accès ou le paramètre spécifié | Valeur appropriée pour le chemin d'accès ou le paramètre spécifié. |

Syntaxe :

```
set [options]
option :
  valeur
```

## Commande smtp

Utilisez la commande **smtp** pour afficher et configurer les paramètres de l'interface SMTP.

L'exécution de la commande **smtp** sans option affiche toutes les informations sur l'interface SMTP. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -auth | Prise en charge de l'authentification SMTP | enabled, disabled |
| -authepw | Mot de passe chiffré de l'authentification SMTP | Chaîne de mot de passe valide |

| Option | Description | Valeurs |
|---|---|---|
| -authmd | Méthode d'authentification SMTP | CRAM-MD5, LOGIN |
| -authn | Nom d'utilisateur d'authentification SMTP | Chaîne (limitée à 256 caractères) |
| -authpw | Mot de passe d'authentification SMTP | Chaîne (limitée à 256 caractères) |
| -pn | Numéro de port SMTP | Numéro de port valide |
| -s | Nom d'hôte ou adresse IP du serveur SMTP | Nom d'hôte ou adresse IP valide (63 caractères maximum) |

Syntaxe :

```
smtp [options]
option :
  -auth activé|désactivé
  -authepw mot_de_passe
  -authmd CRAM-MD5|LOGIN
  -authn nom_utilisateur
  -authpw mot_de_passe
  -s adresse_ip_ou_nom_hôte
  -pn numéro_port
```

Exemple :

```
system> smtp
-s test.com
-pn 25
system>
```

## Commande snmp

Utilisez la commande **snmp** pour afficher et configurer les informations sur l'interface SNMP.

L'exécution de la commande **snmp** sans option affiche toutes les informations sur l'interface SNMP. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -a | Agent SNMPv1 | On, Off (activé/désactivé)<br>**Remarque :** Pour activer l'agent SNMPv1, les critères suivants doivent être remplis :<br>• Contact IMM2 spécifié à l'aide de l'option de commande -cn.<br>• Emplacement du module IMM2 spécifié à l'aide de l'option de commande -l.<br>• Au moins un nom de communauté SNMP spécifié à l'aide de l'une des options de commandes -c*x*.<br>• Au moins une adresse IP valide est spécifiée pour chaque communauté SNMP à l'aide de l'une des options de commande *xiy*. |

| Option | Description | Valeurs |
|---|---|---|
| -a3 | Agent SNMPv3 | On, Off (activé/désactivé)<br>**Remarque :** Pour activer l'agent SNMPv3, les critères suivants doivent être remplis :<br>• Contact du module IMM2 spécifié à l'aide de l'option de commande -cn.<br>• Emplacement du module IMM2 spécifié à l'aide de l'option de commande -l. |
| -t | Alertes SNMP | On, Off (activé/désactivé) |
| -l | Emplacement du module IMM2 | Chaîne (47 caractères maximum).<br>**Remarque :**<br>• Les arguments contenant des espaces doivent figurer entre guillemets. Ils ne peuvent pas contenir d'espace de début ou de fin.<br>• Pour effacer l'emplacement du module IMM2, ne spécifiez aucun argument ou spécifiez une chaîne vide comme argument (par exemple ""). |
| -cn | Nom de contact du module IMM2 | Chaîne (47 caractères maximum).<br>**Remarque :**<br>• Les arguments contenant des espaces doivent figurer entre guillemets. Ils ne peuvent pas contenir d'espace de début ou de fin.<br>• Pour effacer le nom de contact du module IMM2, ne spécifiez aucun argument ou spécifiez une chaîne vide comme argument (par exemple ""). |
| -c*x* | Nom de la communauté SNMP *x* | Chaîne (15 caractères maximum).<br>**Remarque :**<br>• *x* apparaît comme 1, 2, ou 3 dans l'option de commande pour indiquer le numéro de la communauté.<br>• Les arguments contenant des espaces doivent figurer entre guillemets. Ils ne peuvent pas contenir d'espace de début ou de fin.<br>• Pour effacer un nom de communauté SNMP, ne spécifiez aucun argument ou spécifiez une chaîne vide comme argument (par exemple ""). |
| -c*x*i*y* | Nom d'hôte ou adresse IP *y* de la communauté SNMP *x* | Nom d'hôte ou adresse IP valide (63 caractères maximum).<br>**Remarque :**<br>• *x* apparaît comme 1, 2 ou 3 dans l'option de commande pour indiquer le numéro de communauté.<br>• *y* apparaît comme 1, 2 ou 3 dans l'option de commande pour indiquer le numéro du nom d'hôte ou de l'adresse IP.<br>• Une adresse IP ou un nom d'hôte peut uniquement contenir des points, traits de soulignement, signes moins, lettres et chiffres. Les espaces imbriqués ou points consécutifs ne sont pas autorisés.<br>• Pour effacer un nom d'hôte ou une adresse IP de communauté SNMP, ne spécifiez aucun argument. |

| Option | Description | Valeurs |
|---|---|---|
| -ca*x* | Type d'accès *x* de la communauté SNMPv3 | get, set, trap<br>**Remarque :** *x* apparaît comme 1, 2 ou 3 dans l'option de commande pour indiquer le numéro de communauté. |

Syntaxe :

```
snmp [options]
option :
  -a état
  -a3 état
  -t état
  -l emplacement
  -cn nom_contact
  -c1 nom_communauté_snmp_1
  -c2 nom_communauté_snmp_2
  -c3 nom_communauté_snmp_3
  -c1i1 nom_hôte_ou_adresse_ip_1_communauté_1
  -c1i2 nom_hôte_ou_adresse_ip_2_communauté_1
  -c1i3 nom_hôte_ou_adresse_ip_3_communauté_1
  -c2i1 nom_hôte_ou_adresse_ip_1_communauté_2
  -c2i2 nom_hôte_ou_adresse_ip_2_communauté_2
  -c2i3 nom_hôte_ou_adresse_ip_3_communauté_2
  -c3i1 nom_hôte_ou_adresse_ip_1_communauté_3
  -c3i2 nom_hôte_ou_adresse_ip_2_communauté_3
  -c3i3 nom_hôte_ou_adresse_ip_3_communauté_3
  -ca1 type_adresse_communauté_1
  -ca2 type_adresse_communauté_2
  -ca3 type_adresse_communauté_3
```

Exemple :

```
system> snmp
-a Enabled
-a3 Enabled
-t Enabled
-l RTC,NC
-cn Snmp Test
-c1 public
-c1i1 192.44.146.244
-c1i2 192.44.146.181
-c1i3 192.44.143.16
-ca1 set
-ch1 specific
-c2 private
-c2i1 192.42.236.4
-c2i2
-c2i3
-ca2 get
-ch2 specific
-c3
-c3i1
-c3i2
-c3i3
-ca3 get
-ch3 ipv4only
system>
```

## Commande snmpalerts

Utilisez la commande **snmpalerts** pour gérer les alertes envoyées via SNMP.

L'exécution de **snmpalerts** sans option affiche tous les paramètres d'alerte SNMP. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -status | Etat de l'alerte SNMP | On, Off (activé/désactivé) |
| -crt | Définit les événements critiques devant envoyer des alertes | all, none, custom:te \| vo \| po \| di \| fa \| cp \| me \| in \| re \| ot<br><br>Les paramètres d'alertes critiques personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales au format **snmpalerts -crt custom:te \| vo**, où les valeurs personnalisées sont :<br>• te : seuil de température critique dépassé<br>• vo : seuil de tension critique dépassé<br>• po : coupure d'alimentation critique<br>• di : panne du disque dur<br>• fa : panne de ventilateur<br>• cp : panne du microprocesseur<br>• me : panne de mémoire<br>• in : incompatibilité matérielle<br>• re : défaillance de la redondance de l'alimentation<br>• ot : tous les autres événements critiques |
| -crten | Envoie des alertes d'événements critiques | enabled, disabled |
| -wrn | Définit les événements d'avertissement envoyant des alertes | all, none, custom:rp \| te \| vo \| po \| fa \| cp \| me \| ot<br><br>Les paramètres d'alerte des avertissements personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales au format **snmpalerts -wrn custom:rp \| te**, où les valeurs personnalisées sont :<br>• rp : avertissement de redondance de l'alimentation<br>• te : seuil de température d'avertissement dépassé<br>• vo : seuil de tension d'avertissement dépassé<br>• po : seuil d'alimentation d'avertissement dépassé<br>• fa : événement de ventilateur non critique<br>• cp : microprocesseur dégradé<br>• me : avertissement de mémoire<br>• ot : tous les autres événements d'avertissement |
| -wrnen | Envoie des alertes d'événements d'avertissement | enabled, disabled |

| Option | Description | Valeurs |
|---|---|---|
| -sys | Définit les événements de routine envoyant des alertes | all, none, custom:lo\|tio\|ot\|po\|bf\|til\|pf\|el\|ne<br><br>Les paramètres d'alerte de routine personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales au format **snmpalerts -sys custom:lo\|tio**, où les valeurs personnalisées sont :<br>• lo : connexion à distance réussie<br>• tio : délai d'attente du système d'exploitation<br>• ot : tous les autres événements d'information et de système<br>• po : alimentation système on/off<br>• bf : échec d'amorçage du système d'exploitation<br>• til : délai d'attente du programme de surveillance du chargeur de système d'exploitation<br>• pf : échec prévu (PFA)<br>• el : journal des événements complet à 75%<br>• ne : changement de réseau |
| -sysen | Envoie des alertes d'événements de routine | enabled, disabled |

Syntaxe :

```
snmpalerts [options]
   options :
     -status état
     -crt type_événement
     -crten état
     -wrn type_événement
     -wrnen état
     -sys type_événement
     -sysen état
```

## Commande srcfg

Utilisez la commande **srcfg** pour indiquer la séquence de touches permettant d'accéder à l'interface CLI à partir du mode de redirection série. 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.

**Remarque :** Le matériel IMM2 n'offre pas la possibilité de passer d'un port série à un port série passe-système. Par conséquent, les options `-passthru` et `entercliseq` qui sont présentes dans l'interface CLI du Remote Supervisor Adapter II ne sont pas prises en charge.

L'exécution de la commande **srcfg** sans option affiche la séquence de frappe de la redirection série en cours. La table suivante présente les arguments pour l'option de commande `srcfg -entercliseq`.

| Option | Description | Valeurs |
|---|---|---|
| -entercliseq | Séquence de touches pour accéder à une interface CLI | Séquence de touches définie par l'utilisateur permettant d'accéder à l'interface CLI.<br>**Remarque :** Cette séquence doit comporter un caractère minimum et 15 caractères maximum. Le symbole caret (^) possède une signification spéciale dans cette séquence. Il représente Ctrl dans le mappage des touches aux séquences Ctrl (par exemple, ^[ pour la touche Echap et ^M pour le retour chariot). Toutes les occurrences de ^ sont interprétées comme faisant partie d'une séquence Ctrl. Pour obtenir une liste complète des séquences Ctrl, reportez-vous à une table de conversion ASCII-touche. La valeur par défaut de cette zone est ^[( ce qui correspond à Esc suivi de (. |

Syntaxe :

```
srcfg [options]
options :
-entercliseq séqtouche_accèscli
```

Exemple :

```
system> srcfg
-entercliseq ^[Q
system>
```

## Commande sshcfg

Utilisez la commande **sshcfg** pour afficher et configurer les paramètres SSH.

L'exécution de la commande **sshcfg** sans option affiche tous les paramètres SSH. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -cstatus | Etat de l'interface de ligne de commande SSH | enabled, disabled |
| -hk gen | Générer la clé privée du serveur SSH | |
| -hk rsa | Afficher la clé publique RSA du serveur | |

Syntaxe :

```
sshcfg [options]
option :
  -cstatus état
  -hk gen
  -hk rsa
```

Exemple :

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

## Commande ssl

Utilisez la commande **ssl** pour afficher et configurer les paramètres SSL.

**Remarque :** Avant de pouvoir activer un client SSL, un certificat client doit être installé.

L'exécution de la commande **ssl** sans option affiche les paramètres SSL. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -ce | Active ou désactive un client SSL | On, Off (activé/désactivé) |
| -se | Active ou désactive un serveur SSL | On, Off (activé/désactivé) |
| -cime | Active ou désactive le CIM via HTTPS sur le serveur SSL | On, Off (activé/désactivé) |

Syntaxe :

```
portcfg [options]
 options :
  -ce état
  -se état
  -cime état
```

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 sslcfg

Utilisez la commande **sslcfg** pour afficher et configurer SSL pour le module IMM2 et gérer les certificats.

L'exécution de la commande **sslcfg** sans option affiche toute l'information sur la configuration SSL. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -server | Etat du serveur SSL | enabled, disabled<br>**Remarque :** Le serveur SSL peut uniquement être activé si un certificat valide est en place. |
| -client | Etat du client SSL | enabled, disabled<br>**Remarque :** Le client SSL peut uniquement être activé si un certificat client ou serveur valide est en place. |
| -cim | Etat CIM via HTTPS | enabled, disabled<br>**Remarque :** CIM via HTTPS peut uniquement être activé si un certificat client ou serveur valide est en place. |
| -cert | Générer un certificat auto-signé | server, client, sysdir<br>**Remarque :**<br>• Les valeurs des options de commande **-c**, **-sp**, **-cl**, **-on** et **-hn** sont requises lors de la génération d'un certificat auto-signé.<br>• Les valeurs des options de commande **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** et **-dq** sont facultatives lors de la génération d'un certificat auto-signé. |

| Option | Description | Valeurs |
|---|---|---|
| -csr | Générer une demande de signature de certificat | server, client, sysdir<br>**Remarque :**<br>• Les valeurs des options de commande **-c**, **-sp**, **-cl**, **-on** et **-hn** sont requises lors de la génération d'une demande de signature de certificat.<br>• Les valeurs des options de commande **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** et **-un** sont facultatives lors de la génération d'une demande de signature de certificat. |
| -i | Adresse IP du serveur TFTP/SFTP | Adresse IP valide<br>**Remarque :** Une adresse IP du serveur TFTP ou SFTP doit être spécifiée lors du téléchargement d'un certificat ou d'une demande de signature de certificat. |
| -pn | Numéro de port du serveur TFTP/SFTP | Numéro de port valide (par défaut 69/22) |
| -u | Nom d'utilisateur du serveur SFTP | Nom d'utilisateur valide |
| -pw | Mot de passe du serveur SFTP | Mot de passe valide |
| -l | Nom de fichier du certificat | Nom de fichier valide<br>**Remarque :** Un nom de fichier est requis lors du téléchargement d'un certificat ou d'une demande de signature de certificat. Si aucun nom de fichier n'est spécifié pour un téléchargement, le nom par défaut du fichier est utilisé et affiché. |
| -dnld | Télécharger le fichier de certificat | Cette option ne prend aucun argument mais doit également spécifier des valeurs pour l'option de commande **-cert** ou **-csr** (suivant le type de certificat étant téléchargé). Cette option ne prend aucun argument mais doit également spécifier des valeurs pour l'option de commande **-i** et l'option de commande **-l** (facultatif). |
| -upld | Importe le fichier de certificat | Cette option ne prend aucun argument mais doit également spécifier des valeurs pour les options de commande **-cert**, **-i** et **-l**. |
| -tc*x* | Certificat sécurisé *x* pour client SSL | import, download, remove<br>**Remarque :** Le numéro de certificat sécurisé, *x*, est spécifié en tant que nombre entier allant de 1 à 3 dans l'option de commande. |
| -c | Pays | Code pays (2 lettres)<br>**Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -sp | Département ou province | Chaîne entre guillemets (60 caractères maximum)<br>**Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -cl | Ville ou localité | Chaîne entre guillemets (50 caractères maximum)<br>**Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |

| Option | Description | Valeurs |
|---|---|---|
| -on | Nom de l'organisation | Chaîne entre guillemets (60 caractères maximum)<br>**Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -hn | Nom d'hôte du module IMM2 | Chaîne (60 caractères maximum)<br>**Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -cp | Personne à contacter | Chaîne entre guillemets (60 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -ea | Adresse électronique de la personne à contacter | Adresse e-mail valide (60 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -ou | Unité organisationnelle | Chaîne entre guillemets (60 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -s | Nom de famille | Chaîne entre guillemets (60 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -gn | Prénom | Chaîne entre guillemets (60 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -in | Initiales | Chaîne entre guillemets (20 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -dq | Qualificatif du nom de domaine | Chaîne entre guillemets (60 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat. |
| -cpwd | Mot de passe de demande d'authentification | Chaîne (6 caractères minimum, 30 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'une demande de signature de certificat. |
| -un | Nom non structuré | Chaîne entre guillemets (60 caractères maximum)<br>**Remarque :** Facultatif lors de la génération d'une demande de signature de certificat. |

Syntaxe :

```
sslcfg [options]
option :
  -server état
  -client état
  -cim état
  -cert type_certificat
  -csr type_certificat
  -i adresse_ip
  -pn numéro_port
```

```
  -u nom_utilisateur
  -pw mot_de_passe
  -l nom_fichier
  -dnld
  -upld
  -tcx action
  -c code_pays
  -sp département_ou_province
  -cl ville_ou_localité
  -on nom_organisation
  -hn nom_hôte_imm
  -cp personne_à_contacter
  -ea adresse_électronique
  -ou unité_organisationnelle
  -s nom_de_famille
  -gn prénom
  -in initiales
  -dq qualificatif_nom_domaine
  -cpwd mot_de_passe_demande_authentification
  -un nom_non_structuré
```

Exemple :

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
system>
```

## Commande telnetcfg

Utilisez la commande **telnetcfg** pour afficher et configurer les paramètres Telnet.

L'exécution de la commande **telnetcfg** sans option affiche l'état du protocole Telnet. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -en | Etat du protocole Telnet | disabled, 1, 2<br>**Remarque :** S'il n'est pas désactivé, Telnet est activé pour un ou deux utilisateurs. |

Syntaxe :

```
telnetcfg [options]
option :
  -en état
```

Exemple :

```
system> telnetcfg
-en 1
system>
```

## Commande thermal

Utilisez la commande **thermal** pour afficher et configurer les règles du mode thermal du système hôte.

L'exécution de la commande **thermal** sans option affiche les règles du mode thermal. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -mode | Sélection du mode thermal | normal, performance |

Syntaxe :

```
thermal [options]
option :
  -mode mode_thermal
```

Exemple :

```
system> thermal
-mode normal
system>
```

## 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 suivant 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 |
|---|---|---|---|
| -f | Délai de mise hors tension | minutes | disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120 |
| -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 |
| -o | Délai d'attente du système d'exploitation | minutes | disabled, 2.5, 3, 3.5, 4 |

Syntaxe :

```
timeouts [options]
options :
-f option_du_programme_de_surveillance_du_délai_de_mise_hors_tension
-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 ou désactiver l'interface LAN via USB intrabande.

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 utilisateurs et à leurs niveaux d'autorisation. La commande **users** est également utilisée pour créer de nouveaux comptes utilisateurs et modifier les comptes existants.

L'exécution de la commande **users** sans option affiche une liste des utilisateurs et des informations de base les concernant. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| *-index_util* | Numéro d'index du compte utilisateur | 1 à 12 inclus ou `all` pour tous les utilisateurs. |
| -n | Nom du compte utilisateur | Chaîne unique contenant uniquement des chiffres, lettres, points et traits de soulignement. Minimum de 4 caractères et maximum de 16 caractères. |
| -p | Mot de passe du compte utilisateur | Chaîne qui contient au moins un caractère alphabétique et un caractère non alphabétique. Minimum de 6 caractères et maximum de 20 caractères. Null crée un compte sans mot de passe que l'utilisateur doit définir au cours de la première connexion. |

| Option | Description | Valeurs |
|---|---|---|
| -a | Niveau du droit d'utilisateur | super, ro, custom<br><br>Où :<br>• `super` (superviseur)<br>• `ro` (lecture seule)<br>• `custom` est suivi par deux points et une liste de valeurs séparées par un trait vertical (`\|`), au format `custom:am\|rca`. Ces valeurs peuvent être utilisées dans n'importe quelle combinaison.<br>`am` (accès à la gestion de compte utilisateur)<br>`rca` (accès à distance à la console)<br>`rcvma` (accès à distance à la console et aux médias virtuels)<br>`pr` (accès à distance au démarrage/redémarrage du serveur)<br>`cel` (possibilité d'effacement des journaux d'événements)<br>`bc` (configuration de l'adaptateur - de base)<br>`nsc` (configuration de l'adaptateur - réseau et sécurité)<br>`ac` (configuration de l'adaptateur - avancée) |
| -ep | Mot de passe de chiffrement (pour sauvegarde/ restauration) | Mot de passe valide |
| -clear | Effacer le compte utilisateur spécifié | Le numéro d'index du compte utilisateur à effacer doit être spécifié au format :<br><br>`users -clear -`*`index_utilisateur`* |
| -curr | Afficher les utilisateurs actuellement connectés | |
| -sauth | Protocole d'authentification SNMPv3 | HMAC-MD5, HMAC-SHA, none |
| -spriv | Protocole de confidentialité SNMPv3 | CBC-DES, AES, none |
| -spw | Mot de passe de confidentialité SNMPv3 | Mot de passe valide |
| -sepw | Mot de passe de confidentialité SNMPv3 (chiffré) | Mot de passe valide |
| -sacc | Type d'accès SNMPv3 | get, set |
| -strap | Nom d'hôte de message d'alerte SNMPv3 | Nom d'hôte valide |

| Option | Description | Valeurs |
|---|---|---|
| -pk | Afficher la clé publique SSH pour l'utilisateur | Numéro d'index du compte utilisateur.<br>**Remarque :**<br>• Chaque clé SSH assignée à l'utilisateur est affichée avec un numéro d'index de la clé d'identification.<br>• Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option *-userindex*), au format : `users -2 -pk`.<br>• Toutes les clés sont au format OpenSSH. |
| -e | Afficher la clé SSH entière au format OpenSSH<br><br>*(option de clé publique SSH)* | Cette option ne prend pas d'argument et son utilisation exclut toutes les autres options `users -pk`.<br>**Remarque :** Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option *-userindex*), au format : `users -2 -pk -e`. |
| -remove | Supprimer la clé publique SSH de l'utilisateur<br><br>*(option de clé publique SSH)* | Le numéro d'index de clé publique à supprimer doit être indiqué en tant que *-key_index* spécifique ou comme `-all` pour toutes les clés assignées à l'utilisateur.<br>**Remarque :** Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option *-userindex*), au format : `users -2 -pk -remove -1`. |
| -add | Ajouter la clé publique SSH pour l'utilisateur<br><br>*(option de clé publique SSH)* | Clé entre guillemets au format OpenSSH<br>**Remarque :**<br>• L'utilisation de l'option `-add` exclut toutes les autres options de commande `users -pk`.<br>• Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option *-userindex*), au format :<br>`users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N50R6MbNcwlsx+mTEAvvcpJhug a70UNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="` |
| -upld | Télécharger une clé publique SSH<br><br>*(option de clé publique SSH)* | Nécessite que les options `-i` et `-l` indiquent l'emplacement de la clé.<br>**Remarque :**<br>• L'utilisation de l'option `-upld` exclut toutes les autres options de commande `users -pk` (à l'exception de `-i` et `-l`).<br>• Pour remplacer une clé par une nouvelle clé, vous devez spécifier un *-key_index*. Pour ajouter une clé à la fin de la liste des clés en cours, n'indiquez aucun index de clé.<br>• Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option *-userindex*), au format : `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`. |

| Option | Description | Valeurs |
|---|---|---|
| -dnld | Télécharger la clé publique SSH indiquée<br><br>*(option de clé publique SSH)* | Nécessite qu'une option *-key_index* indique la clé à télécharger et que les options `-i` et `-l` indiquent l'emplacement de téléchargement sur un autre ordinateur exécutant un serveur TFTP.<br>**Remarque :**<br>• L'utilisation de l'option `-dnld` exclut toutes les autres options de commande `users -pk` (à l'exception de `-i`, `-l` et *-key_index*).<br>• Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option *-userindex*), au format : `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`. |
| -i | Adresse IP du serveur TFTP/SFTP pour le téléchargement d'un fichier de clés<br><br>*(option de clé publique SSH)* | Adresse IP valide<br>**Remarque :** L'option `-i` est requise par les options de commande `users -pk -upld` et `users -pk -dnld`. |
| -pn | Numéro de port du serveur TFTP/SFTP<br><br>*(option de clé publique SSH)* | Numéro de port valide (par défaut 69/22)<br>**Remarque :** Un paramètre facultatif pour les options de commande `users -pk -upld` et `users -pk -dnld`. |
| -u | Nom d'utilisateur du serveur SFTP<br><br>*(option de clé publique SSH)* | Nom d'utilisateur valide<br>**Remarque :** Un paramètre facultatif pour les options de commande `users -pk -upld` et `users -pk -dnld`. |
| -pw | Mot de passe du serveur SFTP<br><br>*(option de clé publique SSH)* | Mot de passe valide<br>**Remarque :** Un paramètre facultatif pour les options de commande `users -pk -upld` et `users -pk -dnld`. |
| -l | Nom de fichier pour le téléchargement d'un fichier de clés via TFTP ou SFTP<br><br>*(option de clé publique SSH)* | Nom de fichier valide<br>**Remarque :** L'option `-l` est requise par les options de commande `users -pk -upld` et `users -pk -dnld`. |
| -af | Accepter les connexions venant de l'hôte<br><br>*(option de clé publique SSH)* | Une liste de noms d'hôte et adresses IP séparée par des virgules et limitée à 511 caractères. Les caractères valides incluent : les caractères alphanumériques, virgules, astérisques, points d'interrogations, points d'exclamation, points, traits d'union, deux points et le symbole pourcentage. |
| -cm | Commentaire<br><br>*(option de clé publique SSH)* | Chaîne entre guillemets pouvant comprendre jusqu'à 255 caractères.<br>**Remarque :** Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option *-userindex*), au format : `users -2 -pk -cm "Ceci est mon commentaire."`. |

Syntaxe :

```
users [options]
 options :
   -index_utilisateur
   -n nom_utilisateur
   -p mot_de_passe
   -a niveau_autorité
   -ep mot_de_passe_chiffrement
   -clear
   -curr
   -sauth protocole
   -spriv protocole
   -spw mot_de_passe
   -sepw mot_de_passe
   -sacc état
   -strap nom_hôte
users -pk [options]
 options :
   -e
   -remove index
   -add clé
   -upld
   -dnld
   -i adresse_ip
   -pn numéro_port
   -u nom_utilisateur
   -pw mot_de_passe
   -l nom_fichier
   -af liste
   -cm commentaire
```

Exemple :

```
system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration
4.  <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSW0RD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID Read/Write
Password Expires: no expiration
2. test    Read/Write
Password Expires: no expiration
3. test2   Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest  custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>
```

# Commandes de contrôle IMM2

Les commandes de contrôle du module IMM2 sont les suivantes :



## Commande alertentries

Utilisez la commande **alertentries** pour gérer les destinataires d'alertes.

- **alertentries** sans option affiche tous les paramètres d'entrée d'alerte.
- **alertentries -number -test** génère une alerte test au numéro d'index du destinataire indiqué.
- **alertentries -number** (nombre compris entre 0 et 12) affiche les paramètres d'entrée d'avertissement du numéro d'index du destinataire indiqué et permet de modifier les paramètres d'alerte de ce destinataire.

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -number | Numéro d'index du destinataire de l'alerte à afficher, ajouter, modifier ou supprimer | 1 à 12 |
| -status | Etat du destinataire de l'alerte | On, Off (activé/désactivé) |
| -type | Type d'alerte | e-mail, syslog |
| -log | Inclure le journal des événements dans l'e-mail d'alerte | On, Off (activé/désactivé) |
| -n | Nom du destinataire de l'alerte | Chaîne |
| -e | Adresse électronique du destinataire de l'alerte | Adresse électronique valide |
| -ip | Nom d'hôte ou adresse IP syslog | Nom d'hôte ou adresse IP valide |
| -pn | Numéro de port syslog | Numéro de port valide |
| -del | Supprimer le numéro d'index du destinataire indiqué | |
| -test | Générer une alerte test au numéro d'index du destinataire spécifié | |

| Option | Description | Valeurs |
|---|---|---|
| -crt | Définit les événements critiques devant envoyer des alertes | all, none, custom:te \| vo \| po \| di \| fa \| cp \| me \| in \| re \| ot<br><br>Les paramètres d'alerte critique personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres telle que **alertentries -crt custom:te \| vo**, où les valeurs personnalisées sont :<br>• te : seuil de température critique dépassé<br>• vo : seuil de tension critique dépassé<br>• po : coupure d'alimentation critique<br>• di : panne du disque dur<br>• fa : panne de ventilateur<br>• cp : panne du microprocesseur<br>• me : panne de mémoire<br>• in : incompatibilité matérielle<br>• re : défaillance de la redondance de l'alimentation<br>• ot : tous les autres événements critiques |
| -crten | Envoyer les alertes d'événements critiques | enabled, disabled |
| -wrn | Définit les événements d'avertissement envoyant des alertes | all, none, custom:rp \| te \| vo \| po \| fa \| cp \| me \| ot<br><br>Les paramètres d'alerte des avertissements personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales telle que **alertentries -wrn custom:rp \| te**, où les valeurs personnalisées sont :<br>• rp : avertissement de redondance de l'alimentation<br>• te : seuil de température d'avertissement dépassé<br>• vo : seuil de tension d'avertissement dépassé<br>• po : seuil d'alimentation d'avertissement dépassé<br>• fa : événement de ventilateur non critique<br>• cp : microprocesseur dégradé<br>• me : avertissement de mémoire<br>• ot : tous les autres événements d'avertissement |
| -wrnen | Envoyer des alertes d'événements d'avertissement | enabled, disabled |

| Option | Description | Valeurs |
|---|---|---|
| -sys | Définit les événements de routine envoyant des alertes | all, none, custom:lo \| tio \| ot \| po \| bf \| til \| pf \| el \| ne<br><br>Les paramètres d'alertes de routine personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales au format **alertentries -sys custom:lo \| tio**, où les valeurs personnalisées sont :<br>• lo : connexion à distance réussie<br>• tio : délai d'attente du système d'exploitation<br>• ot : tous les autres événements d'information et de système<br>• po : alimentation système on/off<br>• bf : échec d'amorçage du système d'exploitation<br>• til : délai d'attente du programme de surveillance du chargeur de système d'exploitation<br>• pf : échec prévu (PFA)<br>• el : journal des événements complet à 75%<br>• ne : changement de réseau |
| -sysen | Envoyer des alertes d'événements de routine | enabled, disabled |

Syntaxe :

```
alertentries [options]
   options :
   -number numéro_destinataire
      -status état
      -type type_alerte
      -log inclure_état_journal
      -n nom_destinataire
      -e adresse_e-mail
      -ip adresse_ip_ou_nom_hôte
      -pn numéro_port
      -del
      -test
      -crt type_événement
      -crten état
      -wrn type_événement
      -wrnen état
      -sys type_événement
      -sysen état
```

Exemple :

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
```

```
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

## Commande batch

Utilisez la commande **batch** pour exécuter une ou plusieurs commandes d'interface de ligne de commande contenues dans un fichier.

- Les lignes commentaires dans le fichier batch commencent par #.
- Lors de l'exécution d'un fichier de traitement par lots, les commandes qui échouent sont renvoyées avec un code de retour signalant l'échec.
- Les commandes de fichiers de traitement par lots qui contiennent des options de commandes non reconnues peuvent générer des avertissements.

Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -f | Nom du fichier de traitement par lots | Nom de fichier valide |
| -ip | Adresse IP du serveur TFTP/SFTP | Adresse IP valide |
| -pn | Numéro de port du serveur TFTP/SFTP | Numéro de port valide (par défaut 69/22) |
| -u | Nom d'utilisateur du serveur SFTP | Nom d'utilisateur valide |
| -pw | Mot de passe du serveur SFTP | Mot de passe valide |

Syntaxe :

```
batch [options]
option :
  -f nom_de_fichier
  -ip adresse_ip
  -pn numéro_port
  -u nom_utilisateur
  -pw mot_de_passe
```

Exemple :

```
system> batch –f sslcfg.cli –ip 192.168.70.200
1 : sslcfg –client –dnld –ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

## Commande clearcfg

Utilisez la commande **clearcfg** pour rétablir la configuration IMM2 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 IMM2, le module IMM2 est redémarré.

## Commande clock

Utilisez la commande **clock** pour afficher la date et l'heure actuelle d'après l'horloge IMM2 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, -7, -6, -5, -4, ou -3, des paramètres d'heure d'été spéciaux sont requis :
  - Pour +2, les options d'heure d'été sont les suivantes : off (désactivation), ee (Europe orientale), mik (Minsk), tky (Turquie), bei (Beyrouth), amm (Amman), jem (Jérusalem).
  - Pour -7, les options d'heure d'été sont les suivantes : off (désactivation), mtn (Mountain), maz (Mazatlan).
  - Pour -6, les options d'heure d'été sont les suivantes : off (désactivation), mex (Méxique), cna (Centre de l'Amérique du Nord).
  - Pour -5, les options d'heure d'été sont les suivantes : off (désactivation), cub (Cuba), ena (Est de l'Amérique du Nord).
  - Pour -4, les options d'heure d'été sont les suivantes : off (désactivation), asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantique).
  - Pour -3, les options d'heure d'été sont les suivantes : off (désactivation), gtb (Godthab), moo (Montevideo), bre (Brésil - Est).
- 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
12/12/2011 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2011
ok
system> clock
12/31/2011 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 info

Utilisez la commande **info** pour afficher et configurer les informations sur le module IMM2.

L'exécution de la commande **info** sans option affiche toutes les informations de contact et d'emplacement du module IMM2. Le tableau suivant présente les arguments pour les options.

| Option | Description | Valeurs |
|---|---|---|
| -name | Nom du module IMM2 | Chaîne |
| -contact | Nom de la personne à contacter IMM2 | Chaîne |
| -location | Emplacement du module IMM2 | Chaîne |
| -room[1] | Identificateur de la salle du module IMM2 | Chaîne |
| -rack[1] | Identificateur de l'armoire du module IMM2 | Chaîne |
| -rup[1] | Position du module IMM2 dans l'armoire | Chaîne |
| -ruh | Hauteur de l'armoire | Lecture seule |
| -bbay | Emplacement de la baie lame | Lecture seule |

1. La valeur est en lecture seule et ne peut pas être restaurée si le module IMM2 réside sur IBM Flex System.

Syntaxe :

```
info [options]
option :
  -name nom_imm
  -contact nom_de_contact
  -location  emplacement_imm
  -room id_salle
  -rack id_armoire
  -rup position_armoire
  -ruh hauteur_armoire
  -bbay baie_lame
```

## Commande resetsp

Utilisez la commande **resetsp** pour redémarrer le module IMM2. Vous devez disposer au moins des droits Advanced Adapter Configuration pour émettre cette commande.

## Commande spreset

Utilisez la commande **spreset** pour redémarrer le module IMM2. Vous devez disposer au moins des droits Advanced Adapter Configuration pour émettre cette commande.

# 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 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** sur le côté droit de la page. 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 9. 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].<br>• 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.<br>• L'humidité relative déliquescente de la contamination particulaire doit être supérieure à 60 %[2].<br>• 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]<br>• 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 à 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
Téléphone : +49 7032 15 2941
Adresse électronique : 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 à la classe A Electromagnetic Interference (EMI) de Russie

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

## Consigne d'émission électronique de 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

# V

Référence : 47C9124

(1P) P/N: 47C9124