Manuel de l'utilisateur de la carte HP iLO (integrated Lights-Out)

pour microprogramme HP Integrated Lights-Out 1.91

Référence 382327-053
Mai 2007 (troisième édition)

Public visé

Ce manuel est destiné au personnel qui installe, administre et répare les serveurs et systèmes de stockage. HP suppose que vous êtes qualifié en réparation de matériel informatique et que vous êtes averti des risques inhérents aux produits capables de générer des niveaux d'énergie élevés.

Sommaire

Présentation du fonctionnement

Cette section traite des rubriques suivantes :

Présentation du manuel

Le processeur de supervision HP iLO (Integrated Lights-Out) offre plusieurs modes de configuration, de mise à jour, de fonctionnement et de gestion des serveurs à distance. Le *Manuel de l'utilisateur de HP Integrated Lights-Out* décrit chaque fonction ainsi que son mode d'utilisation avec l'interface Web et l'utilitaire RBSU (ROM-Based Setup Utility - Utilitaire de configuration basé sur la ROM). Le *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out* décrit en détail la syntaxe et les outils disponibles pour utiliser la carte iLO via une ligne de commande ou une interface de création de scripts.

Nouveautés dans cette version de iLO

Prise en charge ajoutée à la version 1.91 pour :

- Support virtuel de DVD virtuel (« iLO Virtual CD/DVD-ROM », page 103)
- Débogueur de noyau (« Utilisation d'un débogueur de noyau Windows distant », page 91)
- Verrou d'ordinateur de console distante (page 61)
- Groupes imbriqués sans schéma (page 125)
- Options améliorées de licence (« Activation de la fonctionnalité iLO avancée », page 22)
- Prise en charge pour Red Hat Enterprise Linux 5 et Microsoft® Vista™

Prise en charge ajoutée à la version 1.80 pour :

- Annuaires sans schéma (« Configuration pour l'intégration d'annuaire sans schéma », page 121)
- Authentification à deux facteurs (« Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs) », page 35)
- Création de rapports sur le régulateur d'alimentation (« Power regulator for ProLiant (Régulateur d'alimentation pour ProLiant) », page 95)
- Autorisation de clé SHH (« SSH Key Administration (Administration de clés SSH) », page 34)
- Lecteur de clé USB virtuel (« Lecteur de disquette/USB virtuel iLO », page 99)
- Réseau LAN virtuel du port réseau partagé (« Shared Network Port VLAN (Port réseau partagé VLAN) », page 48)
- Acquisition de la console distante (« Acquisition de la console distante », page 88)

iLO 1.80 ne prend plus en charge :

- Navigateurs Netscape sur clients Linux
- Expédition d'images binaires sous forme Softpaq (elles ont été remplacées par des composants de flashage en ligne)

Présentation de iLO

Trois versions de iLO sont disponibles :

- La version iLO Standard propose des possibilités essentielles de gestion et de contrôle distant telles que les fonctionnalités standard sur les serveurs ProLiant ML/DL de prochaine génération. Grâce à cette version, vous pouvez effectuer à distance des tâches d'administration système élémentaires. Vous pouvez également accéder à tout moment à des informations de supervision de système. Ces possibilités de contrôle distant réduisent le besoin d'une assistance sur site.
- La version iLO Advanced fournit des possibilités complètes de gestion distante Lights-Out pour les serveurs ProLiant. Cette version donne la liberté d'activer un contrôle distant intégral des serveurs ProLiant. Vous pouvez effectuer les mêmes tâches à distance que vous le feriez au niveau du terminal, quelles que soient les conditions du serveur ou du système d'exploitation. La version iLO Advanced est également adaptée aux tâches d'administration de routine, proposant ainsi un outil unique pour chaque situation. En outre, la version iLO Advanced comporte un cryptage complet des données, une authentification d'utilisateurs de classe d'entreprise et la possibilité d'isoler le trafic iLO sur des réseaux distincts.
- La version iLO Select est une mise à niveau facultative de Lights-Out pour les serveurs ProLiant BL. Elle fournit également une mise à niveau à bon rapport qualité-prix des fonctionnalités Lights-Out avancées sur les serveurs ProLiant des gammes 300 et 500 qui sont gérés à l'aide des consoles distantes de type texte de la version iLO Standard, généralement trouvées dans les environnements Linux.

Pour plus d'informations sur les fonctionnalités disponibles dans chaque version de iLO, reportez-vous à la section « Licence » (page 22).

Utilisation type

iLO exécute à distance plusieurs fonctions qui, sinon, requièrent une visite sur les serveurs dans le centre de données, le local informatique ou un emplacement distant. Voici quelques exemples d'utilisation des fonctionnalités iLO :

- La console distante iLO et l'alimentation virtuelle permettent de visualiser un serveur distant bloqué avec des conditions d'écran bleu sans assistance sur site.
- La console distante iLO permet de modifier des paramètres BIOS lorsque requis.
- La technologie iLO fournit une console distante hautes performances qui permet d'administrer à distance des systèmes d'exploitation et des applications dans des situations de tous les jours.
- Un lecteur virtuel de CD/DVD-ROM ou de disquette iLO permet d'installer un système d'exploitation ou un microprogramme de système flash sur le réseau à partir d'images sur des stations de travail ou des serveurs Web centralisés.
- La fonction de script iLO permet d'utiliser des possibilités d'alimentation virtuelle et de support virtuel dans d'autres outils de script afin d'automatiser le déploiement et le provisionnement.

Ces exemples illustrent comment iLO est utilisé pour superviser des serveurs HP ProLiant au bureau, à domicile ou en déplacement. Au fur et à mesure que vous utilisez iLO et que vous définissez les besoins spécifiques de votre infrastructure, ce manuel vous fournira des moyens supplémentaires vous permettant de simplifier la supervision de vos serveurs distants.

Le modèle d'utilisation courant de la carte iLO consiste à connecter un ordinateur client exécutant un navigateur pris en charge à un ou plusieurs périphériques iLO via les protocoles DHCP et DNS.

L'interface de création de scripts permet également d'accéder aux fonctionnalités de la carte iLO. Les scripts sont des fichiers texte rédigés dans un langage XML appelé RIBCL. Ces scripts RIBCL vous permettent de configurer iLO sur le réseau, pendant le déploiement initial ou à partir d'un hôte déjà déployé. Le RIBCL prend également en charge des opérations telles que le contrôle de la mise sous tension.

En outre, l'accès à la carte iLO via le protocole de ligne de commande (CLP) SMASH est rendu possible grâce à une interface à faible bande passante, qui offre des fonctions similaires à celles de l'interface Web. Le CLP est destiné aux utilisateurs préférant utiliser une interface non graphique plutôt qu'une connexion Telnet ou SSH.

iLO prend en charge diverses interfaces pour la configuration et l'exploitation. Le présent manuel décrit en détails les interfaces suivantes :

- iLO RBSU (page 15)
- Interface Web de type navigateur (« Présentation de l'interface de navigateur iLO », page 12)

Consultez le *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out* pour plus d'informations sur l'utilisation des interfaces suivantes:

- CPQLOCFG est un utilitaire Microsoft® Windows® qui envoie des scripts RIBCL à iLO via le réseau.
- CPQLODOS est un utilitaire de déploiement DOS (inclus dans la boîte à outils HP SmartStart de création de scripts) qui s'exécute sur l'hôte pendant le déploiement de SmartStart ou de RDP.
- Perl est un langage de génération de scripts permettant d'envoyer des scripts RIBCL via le réseau, depuis des clients Linux vers la carte iLO.
- HPONCFG est un utilitaire qui s'exécute sur l'hôte et qui transfère les scripts RIBCL vers la carte iLO locale. Certaines versions Windows® et Linux de cet utilitaire requièrent le pilote d'interface de gestion HP iLO.
- Plusieurs méthodes permettent d'utiliser le protocole CLP SMASH : Telnet, SSH, le port série virtuel et le port série physique.

Remote Console (Console distante) (page 80), Virtual Media (Support virtuel) (page 80), l'option Terminal Services Pass-Through (Pass-Through des Terminal Services) (page 80) et les services d'annuaire (page 80) sont des fonctions avancées. Pour plus d'informations, reportez-vous à la section « Licence » (page 22).

Intégration du pack HP ProLiant Essentials Rapid Deployment Pack

Le pack HP ProLiant Essentials Rapid Deployment Pack (Pack de déploiement rapide HP ProLiant Essentials) s'intègre avec la carte iLO pour permettre la supervision des serveurs distants et la performance des opérations de la console distante, indépendamment de l'état du système d'exploitation ou du matériel.

La fonction Deployment Server (Déploiement du serveur) permet d'utiliser les fonctionnalités de supervision de l'alimentation de la carte iLO pour la mise sous tension, la mise hors tension et la réinitialisation sur le serveur cible. Chaque fois que le serveur se connecte sur la fonctionnalité Deployment Server, cette dernière interroge le serveur cible pour vérifier si un périphérique de supervision LOM est installé. Le cas échéant, le serveur collecte les informations, notamment le nom DNS, l'adresse IP et le premier nom utilisateur. La sécurité est maintenue grâce à l'invite, faite à l'utilisateur, d'entrer le mot de passe correct pour ce nom utilisateur.

Pour plus d'informations sur le pack ProLiant Essentials Rapid Deployment Pack, reportez-vous à la documentation disponible sur le CD ProLiant Essentials Rapid Deployment Pack ou sur le site Web HP (http://www.hp.com/servers/rdp).

Présentation de l'interface de navigateur iLO

L'interface de navigateur iLO regroupe des tâches similaires pour une simplification de la navigation et du flux de travail. Ces tâches sont groupées dans des onglets de haut niveau le long de la partie supérieure de l'interface iLO. Ces onglets sont toujours visibles (pour un accès aisé) et incluent System Status (État du système), Remote Console (Console distante), Virtual Media (Support virtuel), Power Management (Gestion de l'alimentation) et Administration.

Chaque onglet iLO de haut niveau possède un menu sur le côté gauche de l'interface avec diverses options. Ce menu change à chaque fois que vous sélectionnez un onglet de haut niveau différent et reflète les options disponibles au sein de chaque onglet de haut niveau. Chaque option de menu affiche un titre de page, qui est une description des informations ou paramètres disponibles sur cette page, et peut ne pas refléter le nom affiché sur l'option de menu.

Une assistance pour toutes les pages iLO est disponible via l'aide iLO. Les liens sur chaque page d'aide fournissent des informations récapitulatives sur les fonctionnalités iLO et des informations utiles pour optimiser leur fonctionnement. Pour accéder à une page d'aide spécifique, cliquez sur le point d'interrogation (**?**) dans la partie droite de la fenêtre du navigateur.

Les tâches utilisateur typiques accèdent aux onglets System Status, Remote Console, Virtual Media et Power Management de l'interface iLO. Ces tâches sont traitées dans la section « Utilisation de la fonctionnalité iLO » (page 74) de ce manuel de l'utilisateur.

L'onglet Administration convient, en général, aux utilisateurs avancés ou aux administrateurs qui ont en charge la gestion des utilisateurs, la configuration des paramètres généraux et des paramètres du réseau, ainsi que la configuration et l'activation des fonctions les plus avancées de iLO. Ces tâches sont traitées dans les sections « Configuration de la carte iLO » (page 15) et « Sécurité iLO » (page 58) de ce manuel.

Des zones spécifiques de la fonctionnalité iLO et de son intégration sont traitées dans les sections suivantes :

- Services d'annuaire (page 117)
- Supervision distante activée via l'annuaire (page 152)
- Services de certificat (page 161)
- Utilitaires de migration d'annuaires Lights-Out (page 163)
- Intégration avec HP Systems Insight Manager (page 177)
- Résolution des problèmes de la carte iLO
- Schéma des services d'annuaire (page 214)

Systèmes d'exploitation serveur pris en charge

iLO est un microprocesseur indépendant qui exécute un système d'exploitation intégré. Cette architecture garantit la disponibilité de la plupart des fonctions de iLO, indépendamment du système d'exploitation hôte utilisé.

Pour que les opérations de fermeture du système d'exploitation s'effectuent dans les règles, l'intégration avec HP Systems Insight Manager nécessite des drivers d'état et des agents de supervision, ou l'accès à la console distante.

iLO fournit deux drivers d'interface :

- Le driver de contrôleur iLO ASM (Advanced System Management) permet d'assurer la supervision des systèmes, notamment la surveillance des composants serveurs, la consignation des événements et la prise en charge des agents de supervision.
- Le driver d'interface iLO Management permet au logiciel du système et aux agents SNMP Insight de communiquer avec iLO.

Ces drivers et ces agents sont disponibles pour les systèmes d'exploitation réseau suivants :

- Microsoft®
  - Windows® 2000 Server
  - Windows® 2000 Advanced Server
  - Windows Server™ 2003
  - Windows® Server 2003, Web Edition
  - Windows Server™ 2003, Enterprise Edition (EM64T)
  - Windows Small Business Server™ 2003
- Red Hat
  - Red Hat Enterprise Linux 4
  - Red Hat Enterprise Linux 5
- SUSE
  - SUSE LINUX Enterprise Server 9 (x86 et AMD64/EM64T)
  - SUSE LINUX Enterprise Server 10 (x86 et AMD64/EM64T)
- Novell
  - NetWare 6.5

Navigateurs et systèmes d'exploitation clients pris en charge

Les systèmes d'exploitation et navigateurs suivants sont pris en charge :

- Microsoft® Internet Explorer 6 avec Service Pack 1 ou version supérieure
  - Ce navigateur est pris en charge sur les produits Microsoft® Windows®.
  - Si vous utilisez le mode curseur simple avec la console distante ou le support virtuel, la machine virtuelle Java™ est nécessaire. HP prend en charge Java™ 1.4.2. Pour télécharger la machine virtuelle Java recommandée pour votre configuration système, reportez-vous au site Web HP (http://www.hp.com/servers/manage/jvm).

- Microsoft® Internet Explorer 7
  - Ce navigateur est pris en charge sur les produits Microsoft® Windows®.
  - Si vous utilisez le mode curseur simple avec la console distante ou le support virtuel, la machine virtuelle Java™ est nécessaire. HP prend en charge Java™ 1.4.2. Pour télécharger la machine virtuelle Java recommandée pour votre configuration système, reportez-vous au site Web HP (http://www.hp.com/servers/manage/jvm).
- Firefox 2.0
  - Ce navigateur est pris en charge sur Red Hat Enterprise Linux 3 Workstation et Novell Linux Desktop 9.
  - Si vous utilisez la console distante ou le support virtuel, Java™ 1.4.2 est nécessaire. Pour télécharger la machine virtuelle recommandée pour votre configuration système, reportez-vous au site Web HP (http://www.hp.com/servers/manage/jvm).
- Mozilla 1.7.3
  - Ce navigateur est pris en charge sur Red Hat Enterprise Linux 3 Workstation et Novell Linux Desktop 9.
  - Si vous utilisez la console distante ou le support virtuel, Java™ 1.4.2 est nécessaire. Pour télécharger la machine virtuelle recommandée pour votre configuration système, reportez-vous au site Web HP (http://www.hp.com/servers/manage/jvm).

Certaines combinaisons de navigateurs et de systèmes d'exploitation peuvent ne pas fonctionner correctement, selon la manière dont ces derniers mettent en œuvre les technologies de navigation requises.

Configuration du navigateur sous Linux

La configuration des polices du bureau et du navigateur peut affecter la position des menus de l'interface utilisateur iLO. Le positionnement adéquat de ces menus nécessite une police fixe de 12 points.

Pour modifier la taille de la police dans Mozilla, ouvrez le menu Préférences et paramétrez la taille de police minimale sur 12 dans l'écran Aspect/Polices.

Configuration de la carte iLO

Cette section traite des rubriques suivantes :

Options de configuration de la carte iLO

La carte iLO est préconfigurée avec des valeurs par défaut, notamment un compte utilisateur et un mot de passe par défaut. Si elle est connectée à un réseau qui utilise DNS ou DHCP, vous pouvez vous en servir immédiatement sans changer aucun paramètre. Pour une meilleure sécurité et fiabilité, connectez-la à un autre réseau de supervision dédié.

Certaines fonctions avancées impliquent l'installation des drivers du système d'exploitation (« Systèmes d'exploitation serveur pris en charge », page 13).

iLO propose plusieurs options de configuration :

- iLO RBSU (page 15)
- Configuration basée sur le navigateur (page 16)
- Installation distante par script à l'aide de CPQLOCFG
- Déploiement local par script à l'aide de CPQLODOS
- Installation locale (en ligne) par script à l'aide de HPONCFG

Utilitaire iLO RBSU

HP vous recommande d'utiliser iLO RBSU pour la configuration initiale de la carte iLO et des paramètres réseau associés dans les environnements n'utilisant pas DHCP, DNS ou WINS. RBSU fournit les outils de base permettant de configurer les comptes utilisateur et les paramètres permettant d'accéder à iLO sur le réseau.

iLO RBSU est conçu pour vous aider à installer la carte iLO sur un réseau ; iLO n'est pas destiné à une administration permanente. RBSU est disponible à chaque initialisation du serveur et peut être exécuté à distance à l'aide de la console distante iLO. Vous pouvez utiliser RBSU pour configurer les paramètres réseau, les paramètres d'annuaire, les paramètres généraux et les comptes utilisateur.

Vous pouvez désactiver l'utilitaire iLO RBSU dans les préférences Global Settings (Paramètres généraux). Cela évite toute reconfiguration à partir de l'hôte, sauf si le commutateur de neutralisation de la sécurité iLO est activé.

Pour exécuter l'utilitaire iLO RBSU :

1. Redémarrez le serveur ou mettez-le sous tension.
2. Appuyez sur la touche **F8** lorsque vous y êtes invité pendant l'auto-test de mise sous tension (POST). L'utilitaire iLO RBSU est exécuté.
3. Si le système vous le demande, entrez un nom d'utilisateur iLO et un mot de passe valides avec les privilèges iLO appropriés (**Administer User Accounts** (Administrer comptes utilisateur)**>Configure iLO Settings** (Configurer paramètres iLO)). Les informations relatives au compte par défaut figurent sur l'étiquette iLO Default Network Settings (Paramètres réseau par défaut iLO) apposée sur le serveur contenant le processeur de supervision iLO. Si la carte iLO n'a pas été configurée pour se connecter à RBSU, aucune invite ne s'affiche.
4. Apportez les modifications requises à la configuration de la carte iLO et enregistrez-les.
5. Quittez l'utilitaire iLO RBSU.

HP vous recommande d'utiliser DNS ou DHCP avec iLO pour faciliter l'installation. Si vous ne pouvez pas les utiliser, procédez comme suit pour les désactiver et configurer l'adresse IP et le masque de sous-réseau :

1. Redémarrez le serveur ou mettez-le sous tension.
2. Appuyez sur la touche **F8** lorsque vous y êtes invité pendant l'auto-test de mise sous tension (POST). L'utilitaire iLO RBSU est exécuté.
3. Entrez un nom d'utilisateur iLO et un mot de passe valides avec les privilèges iLO appropriés (**Administer User Accounts > Configure iLO Settings** - Administrer comptes utilisateur > Configurer paramètres iLO). L'étiquette iLO Default Network Settings (Paramètres réseau par défaut iLO) contient toutes les informations relatives au compte par défaut.
4. Sélectionnez **Network>DNS/DHCP** (Réseau>DNS/DHCP), appuyez sur la touche **Entrée**, puis sélectionnez **DHCP Enable** (Activation de DHCP). Appuyez sur la barre d'espacement pour désactiver DHCP. Vérifiez que l'option DHCP Enable (Activation de DHCP) est désactivée et enregistrez les modifications.
5. Sélectionnez **Network>NIC>TCP/IP** (Réseau>Carte réseau>TCP/IP), appuyez sur la touche **Entrée**, puis entrez les informations appropriées dans les champs IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau) et Gateway IP Address (Adresse IP de la passerelle).
6. Enregistrez les modifications.
7. Quittez l'utilitaire iLO RBSU. Les modifications s'appliquent après avoir quitté iLO RBSU.

Installation basée sur le navigateur

Utilisez la méthode d'installation basée sur le navigateur si vous pouvez vous connecter à iLO sur le réseau à l'aide d'un navigateur. Cette méthode vous permet également de reconfigurer une carte iLO déjà configurée.

1. Accédez à iLO à partir d'un client réseau distant à l'aide d'un navigateur Web pris en charge et indiquez le mot de passe, le nom utilisateur et le nom DNS par défaut. Les informations relatives au compte et au nom DNS par défaut figurent sur l'étiquette iLO Network Settings (Paramètres réseau iLO) apposée sur le serveur contenant le processeur de supervision iLO.

Une fois connecté à iLO, vous pouvez modifier les valeurs par défaut des paramètres réseau, utilisateur et des alertes SNMP via l'interface de navigation Web.

2. Saisissez la clé permettant d'activer les fonctions iLO Advanced.

   La licence des fonctions iLO Advanced vous permet de déployer votre système d'exploitation à l'aide de l'unité de disquette virtuelle et d'installer les drivers du système d'exploitation et les agents Insight Manager sur le serveur hôte distant en utilisant la console graphique distante.

   Pour les serveurs ProLiant BL p-Class, la fonctionnalité iLO Advanced est déjà activée et ne peut pas être désactivée.

Intégration avec les cartes RILOE II

La carte RILOE II est prise en charge en tant qu'option sur les serveurs dotés de la fonctionnalité iLO. Les générations précédentes de cartes Remote Insight, comme la carte Remote Insight/PCI et les cartes RILOE d'origine, ne sont pas prises en charge sur les serveurs dotés de la fonctionnalité iLO.

Le microprogramme iLO détecte la présence de cartes RILOE II et désactive automatiquement la fonctionnalité iLO. En outre, si le microprogramme iLO détecte la présence de la carte RILOE d'origine, iLO affiche un message indiquant que la configuration n'est pas valide.

Pour réactiver la fonctionnalité iLO après le retrait d'une carte RILOE II, utilisez le commutateur de neutralisation de la sécurité et l'utilitaire iLO RBSU (page 15). Sélectionnez **Settings>Enabled** (Paramètres>Activé) pour accéder au paramètre Enable Lights-Out functionality (Activer la fonctionnalité Lights-Out).

Présentation de la connexion réseau

Il existe trois principaux scénarios de connexion réseau. La carte iLO peut être connectée sur :

- Un réseau d'entreprise avec les deux ports connectés au réseau. Dans cette configuration, les deux ports réseau du serveur (carte réseau du serveur et carte réseau iLO) sont connectés à un réseau d'entreprise. Cette connexion permet d'accéder à la carte iLO depuis n'importe quel point du réseau. Le trafic du réseau d'entreprise est toutefois susceptible de perturber les performances de la carte.

  Une configuration de ce type réduit le nombre d'infrastructures et d'équipements nécessaires pour prendre en charge la carte iLO car celle-ci utilise les routeurs et serveurs DNS et DHCP existants.

- Un réseau de supervision dédié avec le port iLO connecté à un autre réseau. Un réseau distinct améliore les performances et la sécurité, et fournit un accès redondant au serveur en cas de défaillance d'un équipement sur le réseau d'entreprise. Dans cette configuration, la carte iLO n'est pas directement accessible à partir du réseau d'entreprise.

  Un réseau distinct renforce la sécurité du réseau de supervision car il permet de contrôler physiquement les stations de travail connectées au réseau.

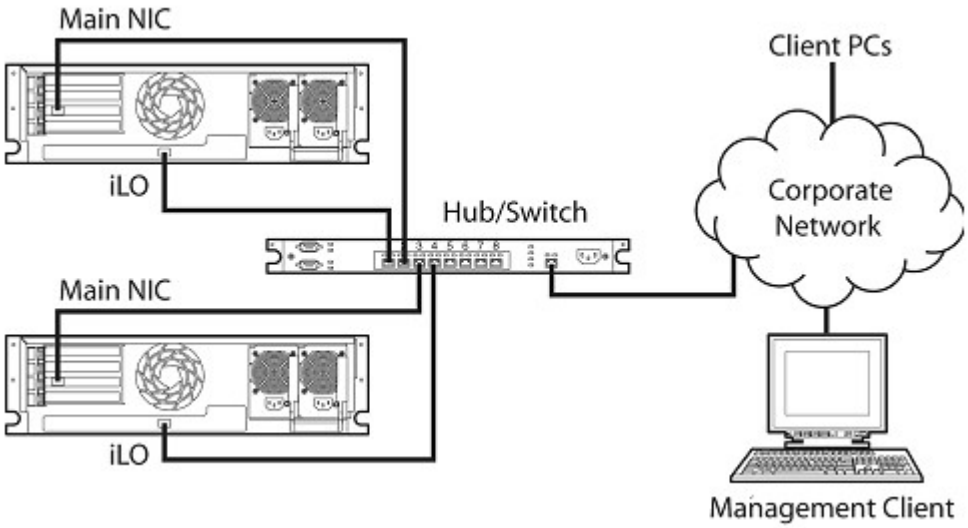
- Un port réseau partagé iLO à l'aide de la carte réseau du serveur au lieu de la carte de supervision iLO dédiée pour la supervision du serveur. Cette configuration simplifie le réseau et réduit le coût total associé. Un nombre moindre de câbles, de hubs et de commutateurs est nécessaire car le trafic réseau de iLO et régulier passe par la carte réseau système.

  Le principal inconvénient de l'utilisation du port réseau partagé iLO pour la supervision du serveur iLO est le manque de vitesse comparé à la carte réseau de supervision iLO dédiée. Par conséquent, toutes les fonctions de supervision iLO ne sont pas disponibles via cette configuration.

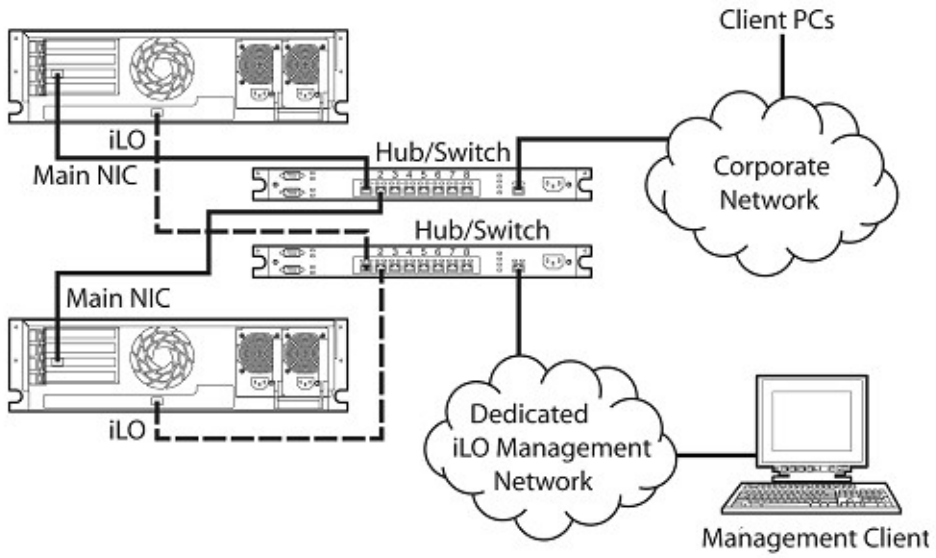
Se connecter au réseau

Généralement, iLO se connecte au réseau de l'une des deux manières suivantes, via :

- **Corporate network** (Réseau d'entreprise) où les deux ports sont connectés au réseau d'entreprise. Dans cette configuration, les deux ports réseau du serveur (carte réseau du serveur et carte réseau iLO) sont connectés à un réseau d'entreprise.



- **Dedicated management network** (Réseau de supervision dédié) où le port iLO se situe sur un réseau séparé.



Configurer l'adresse IP

Cette étape n'est nécessaire que si vous utilisez une adresse IP statique. Lors de l'utilisation de l'addressage IP dynamique, le serveur DHCP affecte automatiquement une adresse IP pour iLO. HP vous recommande d'utiliser DNS ou DHCP avec iLO pour faciliter l'installation.

Pour configurer une adresse IP statique, utilisez l'utilitaire iLO RBSU en procédant comme suit afin de désactiver DNS et DHCP, et de configurer l'adresse IP et le masque de sous-réseau :

1. Redémarrez le serveur ou mettez-le sous tension.
2. Appuyez sur la touche **F8** lorsque vous y êtes invité pendant l'auto-test de mise sous tension (POST). L'utilitaire iLO RBSU est exécuté.
3. Sélectionnez **Network>DNS/DHCP** (Réseau>DNS/DHCP), appuyez sur la touche **Entrée**, puis sélectionnez **DHCP Enable** (Activation de DHCP). Appuyez sur la barre d'espacement pour désactiver DHCP. Vérifiez que l'option DHCP Enable (Activation de DHCP) est désactivée et enregistrez les modifications.
4. Sélectionnez **Network>NIC>TCP/IP** (Réseau>Carte réseau>TCP/IP), appuyez sur la touche **Entrée**, puis entrez les informations appropriées dans les champs IP Address (Adresse IP), Subnet Mask (Masque de sous-réseau) et Gateway IP Address (Adresse IP de la passerelle).
5. Enregistrez les modifications.
6. Quittez l'utilitaire iLO RBSU. Les modifications s'appliquent après avoir quitté iLO RBSU.

Installation des drivers de périphérique iLO

Le CD SmartStart Firmware Maintenance contient tous les drivers nécessaires pour votre serveur. Vous pouvez également les télécharger à partir du site Web HP (http://www.hp.com/servers/lights-out).

Pour ce faire :

1. Cliquez sur le graphique iLO.
2. Sélectionnez **Software and Drivers** (Logiciels et drivers).

Le driver d'interface de supervision iLO permet aux logiciels système tels que les agents SNMP Insight et le service d'émulation Terminal Services de communiquer avec iLO.

Prise en charge des drivers Microsoft Windows NT, Windows 2000 et Windows 2003 Server

Les drivers de périphérique prenant en charge les fonctions iLO sont inclus dans le PSP qui se trouve sur le site Web HP (http://www.hp.com/support) ou sur le CD SmartStart. Avant d'installer les drivers Windows®, procurez-vous la documentation Windows® et le dernier Service Pack disponible pour Windows®.

Fichiers iLO prérequis pour Microsoft®

Le fichier CPQCIDRV.SYS assure la prise en charge du driver iLO Management Interface (Interface de supervision iLO).

Les fichiers CPQASM2.SYS, SYSMGMT.SYS et SYSDOWN.SYS assurent la prise en charge du driver iLO Advanced Server Management Controller (Contrôleur de supervision du serveur iLO Advanced).

Installation ou mise à jour des drivers iLO pour Microsoft®

Le PSP (ProLiant Support Pack) pour les produits Microsoft® Windows® comprend un programme d'installation qui analyse les conditions requises pour le système et installe tous les drivers.

Le PSP est disponible sur le site Web HP (http://www.hp.com/support) ou sur le CD SmartStart.

REMARQUE : si vous mettez à jour les drivers iLO, assurez-vous que la carte iLO utilise la version de microprogramme la plus récente. Celle-ci peut être obtenue sous forme de composant Smart sur le site Web HP (http://www.hp.com/servers/lights-out).

Pour installer les drivers inclus dans le PSP, téléchargez ce dernier à partir du site Web HP (http://www.hp.com/support), exécutez le fichier SETUP.EXE disponible dans la version téléchargée et suivez les instructions d'installation. Pour plus d'informations sur l'installation du PSP, lisez le fichier texte inclus dans le téléchargement.

Prise en charge des drivers de serveur Novell NetWare

Les drivers de périphérique nécessaires à la prise en charge iLO sont inclus dans le PSP disponible sur le CD SmartStart ou sur le site Web HP (http://www.hp.com/support).

Fichiers iLO prérequis pour NetWare

Le fichier CPQHLTH.NLM fournit le driver d'état (Health Driver) pour NetWare.

Le fichier CPQCI.NLM assure la prise en charge du driver iLO Management Interface (Interface de supervision iLO).

Installation ou mise à jour des drivers iLO pour NetWare

Le PSP (ProLiant Support Pack) pour Novell NetWare comprend un programme d'installation qui analyse les conditions requises pour le système et installe tous les drivers. Ce PSP est disponible sur le site Web HP (http://www.hp.com/support) et sur le CD SmartStart.

Lors de la mise à jour des drivers iLO, assurez-vous que la carte iLO utilise la version la plus récente du microprogramme iLO. Celle-ci peut être obtenue sous forme de composant Smart sur le site Web HP (http://www.hp.com/servers/lights-out).

Pour installer les drivers, téléchargez le PSP sur un serveur NetWare à partir du site Web HP (http://www.hp.com/support). Une fois le téléchargement du PSP terminé, suivez les instructions d'installation du composant NetWare pour mener à bien l'installation. Pour plus d'informations sur l'installation du PSP, lisez le fichier texte inclus dans le téléchargement.

Lorsque vous utilisez NetWare 6.X, le système d'exploitation fournit un driver vidéo RAGE-XL que vous pouvez utiliser pour obtenir un résultat optimal.

Prise en charge des drivers de serveur Red Hat Linux et SuSE Linux

Les drivers de périphérique nécessaires à la prise en charge des fonctions iLO pour Red Hat Linux et SuSE Linux sont disponibles sur le CD SmartStart, sur le CD Management ou sur le site Web HP (http://www.hp.com/support).

Fichiers iLO prérequis pour Red Hat et SuSE Linux

Vous pouvez télécharger les fichiers PSP contenant le driver iLO, les agents dits « foundation agents » et les agents d'état sur le site Web HP (http://www.hp.com/support). Les instructions sur l'installation ou la mise à jour du driver iLO sont disponibles sur le site Web. Les agents de supervision HP pour Linux sont les suivants :

- Le progiciel ASM (hpasm), qui regroupe le driver d'état, l'afficheur IML, les « foundation agents », l'agent d'état et l'agent d'équipement standard en une solution unique.
- Le progiciel RSM (hprsm), qui combine le driver RIB, le démon de rack, l'agent RIB et l'agent de rack en une seule solution.

Configuration de la taille de la police sous Linux

Pour modifier la taille de la police :

1. Ouvrez le panneau KDE Control Center (Centre de contrôle KDE) et paramétrez les polices.
2. Lancez Mozilla Firefox puis configurez les polices à l'aide de Fonts - Control Center (Police - Centre de contrôle). Paramétrez la taille de police minimale sur 12.

Installation ou mise à jour des drivers iLO pour Linux et SuSE

Désinstallez, si nécessaire, les agents antérieurs. Pour désinstaller les agents antérieurs, exécutez la procédure suivante :

- rpm -e cmanic
- rpm -e hprssm
- rpm -e hpasm

Pour charger les progiciels contenant les drivers d'état et les drivers iLO, utilisez les commandes suivantes :

```
rpm –ivh hpasm-d.vv.v-pp.Linux_version.i386.rpm
rpm –ivh hprsm-d.vv.v-pp.Linux_version.i386.rpm
```

où : *d* correspond à la distribution et à la version Linux et

vv.v-pp au numéro de version.

Pour plus d'informations, consultez le site Web Software and Drivers (Logiciels et drivers) (http://www.hp.com/support).

Pour supprimer les drivers d'état et les drivers iLO, utilisez les commandes suivantes :

```
rpm –e hprsm
rpm –e hpasm
```

Pour plus d'informations, consultez le site Web Software and Drivers (Logiciels et drivers) (http://www.hp.com/support).

Activation de la fonctionnalité iLO avancée

La page Licensing (Licence) permet de visualiser l'état de la licence en cours et de saisir la clé pour activer les fonctions sous licence de iLO. Le numéro de version iLO et les informations de la licence actuelle apparaissent dans cette section. Si une licence est installée, son numéro apparaît. Les licences d'évaluation sont également affichées. Pour installer une licence, reportez-vous à la section « Activation de fonctionnalités sous licence iLO via un navigateur » (page 23).

Vous devez utiliser une clé de licence pour activer certaines fonctionnalités iLO. Les licences en option activent les fonctionnalités fournies avec un système sans licence.

La licence iLO Select permet d'accéder aux fonctionnalités iLO suivantes en sus des fonctionnalités iLO standard :

- Authentification et autorisation basées sur les annuaires (« Supervision distante activée via l'annuaire », page 152)
- Régulateur de puissance pour ProLiant (page 95)
- Support virtuel de création de scripts (page 98)
- Support virtuel d'applet (page 98) (y compris Virtual Floppy et Virtual CD)
- Authentification à deux facteurs (« Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs) », page 35)

Outre les fonctionnalités iLO Standard et Select, le pack iLO Advanced permet d'accéder aux fonctionnalités suivantes en sus des fonctionnalités iLO Standard et Select :

- Console graphique distante (page 80)
- Option Pass-Through des Terminal Services) (page 39)

Les fonctionnalités avancées sont activées par l'utilisation sous licence du pack iLO Advanced facultatif. Le pack iLO Advanced contient une clé d'activation à entrer pour activer les fonctionnalités avancées. Vous pouvez évaluer ces fonctions avancées à l'aide d'une clé d'évaluation.

Une licence d'évaluation gratuite valable 60 jours peut être téléchargée à partir du site Web HP (http://h10018.www1.hp.com/wwsolutions/ilo/iloeval.html). La licence d'évaluation active et offre accès aux fonctionnalités avancées iLO. Vous pouvez uniquement installer une licence d'évaluation par iLO. Une fois la période d'évaluation terminée, une licence iLO Advanced est requise pour pouvoir continuer à utiliser les fonctions avancées. Les fonctions iLO avancées se désactivent automatiquement à l'expiration de la licence d'évaluation.

Licence

Les clés de licence activent des fonctionnalités en option non fournies avec un système sans licence. Pour plus d'informations, consultez le site Web HP (http://h18004.www1.hp.com/products/servers/proliantessentials/valuepack/licensing.html).

Un astérisque (*) indique qu'une fonctionnalité n'est pas prise en charge sur tous les systèmes.

- iLO Standard (sans licence) :
  - Commande d'alimentation virtuelle et de réinitialisation
  - Console série distante via POST uniquement
  - Journaux d'événements

- Voyant UID*
- SMASH CLP (CLP SMASH) DMTF
- Fonction de génération de scripts RIBCL/XML
- Accès au navigateur
- Accès SSH
- Port réseau partagé*
- Accès série*

- iLO Select :
  - Intégration d'annuaire
  - Power Regulator (Régulateur de puissance)
  - Support virtuel de création de scripts
  - Possibilité de débogage de noyau Windows®
  - Support visuel basé sur une applet
  - Authentification à deux facteurs
- iLO Advanced :
  - Intégration d'annuaire
  - Surveillance du régulateur de puissance
  - Support virtuel de création de scripts
  - Débogage de noyau
  - Support visuel basé sur une applet
  - Authentification à deux facteurs
  - Intégration de Terminal Services
  - Remote Console (Console distante)

En sus des licences mono-serveur iLO standard, deux autres options de licence sont disponibles :

- Le « Flexible Quantity License Kit » permet aux clients d'acheter une solution logicielle unique, une copie de la documentation et une seule clé de licence pour activer le nombre exact de licences requises.
- Le contrat de clé d'activation est disponible pour les clients prévoyant un achat de volume de logiciels ProLiant Essentials et Insight Control, généralement en conjonction avec de nouveaux serveurs ProLiant, acquis sur une base régulière.

Activation de fonctionnalités sous licence iLO via un navigateur

1. Connectez-vous à iLO via un navigateur pris en charge.
2. Sélectionnez l'onglet **Administration**.

3. Cliquez sur **Licensing** (Licence) pour afficher l'écran d'activation de la licence iLO.

4. Saisissez la clé d'activation dans l'espace fourni.
5. Cliquez sur **Install** (Installer). La confirmation CLUF apparaît. Les informations CLUF sont disponibles sur le site Web HP (http://www.hp.com/servers/lights-out) et dans le kit Advanced Pack License.

6. Cliquez sur **OK**.

Les fonctions avancées de la carte iLO sont maintenant activées.

Administration

Les options disponibles sous l'onglet Administration permettent de gérer les paramètres des utilisateurs, les alertes SNMP via l'intégration avec Systems Insight Manager, les paramètres de sécurité, la licence, l'administration des certificats, les paramètres d'annuaire et d'environnement réseau. Cette section fournit également une option de mise à niveau du microprogramme qui permet de conserver la carte iLO à jour.

Administration des utilisateurs

L'écran User Administration (Administration des utilisateurs) vous permet de gérer les comptes utilisateur enregistrés localement dans la mémoire iLO sécurisée. Les comptes utilisateur d'annuaire sont gérés à l'aide des composants logiciels intégrables de MMC ou de ConsoleOne. L'écran User Administration (Administration des utilisateurs) vous permet d'ajouter un nouvel utilisateur, d'afficher ou de modifier les paramètres d'un utilisateur existant ou de supprimer un utilisateur.

La carte iLO prend en charge jusqu'à 12 utilisateurs avec des droits d'accès et des noms d'ouverture de session personnalisables ainsi qu'un codage avancé des mots de passe. Les possibilités d'un utilisateur particulier sont contrôlées à l'aide de privilèges. Chaque utilisateur peut disposer de privilèges d'accès personnalisés en fonction de ses besoins.

Pour prendre en charge plus de 12 utilisateurs, iLO Advanced autorise l'intégration à un nombre quasi illimité de comptes utilisateur basés sur les annuaires.

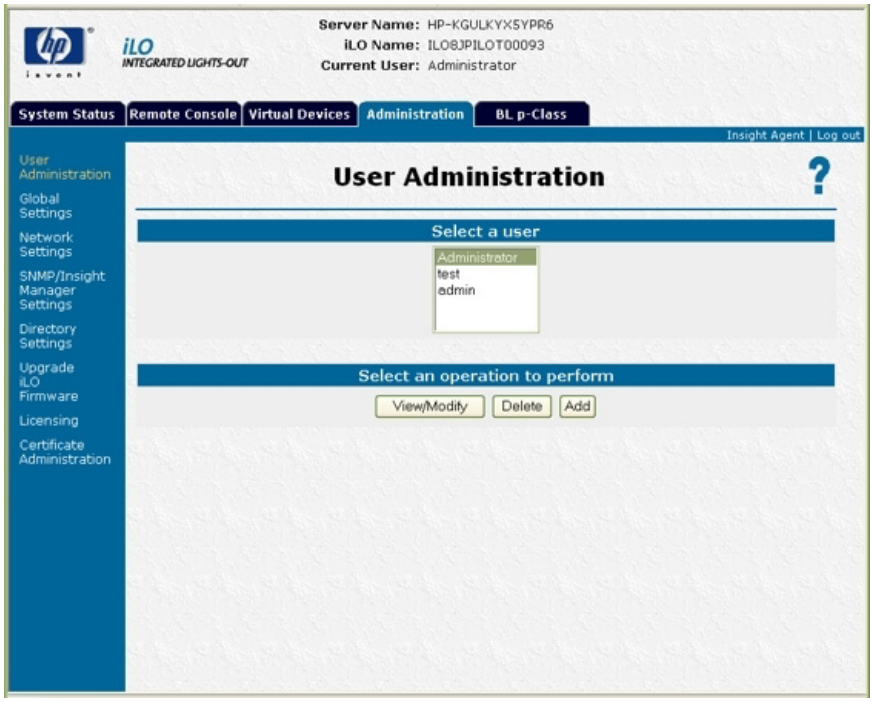
Ajout d'un nouvel utilisateur

IMPORTANT : seuls les utilisateurs dotés du privilège Administer User Accounts (Administrer comptes utilisateur) peuvent gérer d'autres utilisateurs de la carte iLO.

Vous pouvez attribuer des droits d'accès différents à chaque utilisateur. Chaque utilisateur peut avoir une combinaison unique de privilèges, adaptée aux tâches qu'il doit exécuter. Un utilisateur peut se voir refuser l'accès à des fonctions critiques, comme par exemple Remote Console (Console distante), Managing Users (Gestion des utilisateurs) et le bouton Virtual Power (Alimentation virtuelle).

Pour ajouter un nouvel utilisateur à iLO :

1. Ouvrez une session sur la carte iLO en utilisant un compte doté du privilège Administer User Accounts (Administrer comptes utilisateur). Cliquez sur **Administration**.
2. Cliquez sur User Administration (Administration des utilisateurs). Un écran similaire à celui présenté ci-dessous s'affiche.



3. Cliquez sur **Add** (Ajouter).
4. Renseignez les champs de manière appropriée pour l'utilisateur que vous ajoutez.
5. Lorsque le profil de l'utilisateur est termine, cliquez sur **Save User Information** (Enregistrer informations utilisateur) pour revenir à l'écran User Administration (Administration des utilisateurs). Pour effacer le profil saisi dans le formulaire lorsque vous entrez un nouvel utilisateur, cliquez sur le bouton **Restore User Information** (Restaurer informations utilisateur).

Affichage ou modification des paramètres d'un utilisateur existant

IMPORTANT : seuls les utilisateurs dotés du privilège Administer User Accounts (Administrer comptes utilisateur) peuvent gérer d'autres utilisateurs de la carte iLO. Tous les utilisateurs peuvent modifier leur propre mot de passe à l'aide de la fonction **View/Modify User** (Afficher/Modifier utilisateur).

1. Ouvrez une session sur la carte iLO en utilisant un compte doté du privilège Administer User Accounts (Administrer comptes utilisateur). Cliquez sur **Administration**.
2. Cliquez sur **User Administration** (Administration des utilisateurs), puis sélectionnez dans la liste l'utilisateur dont vous souhaitez modifier les informations.
3. Cliquez sur **View/Modify** (Afficher/Modifier).
4. Modifiez les informations concernant l'utilisateur dans les champs appropriés. Ceci fait, cliquez sur **Save User Information** (Enregistrer informations utilisateur) pour revenir à l'écran User Administration (Administration des utilisateurs). Pour revenir aux informations initiales de l'utilisateur, cliquez sur **Restore user Information** (Restaurer informations utilisateur). Toutes les modifications apportées au profil sont annulées.

Pour modifier vos informations de certificat utilisateur, reportez-vous à la section « Certificats utilisateur pour l'authentification à deux facteurs » (page 68).

Suppression d'un utilisateur

IMPORTANT : seuls les utilisateurs dotés du privilège Administer User Accounts (Administrer comptes utilisateur) peuvent gérer d'autres utilisateurs de la carte iLO.

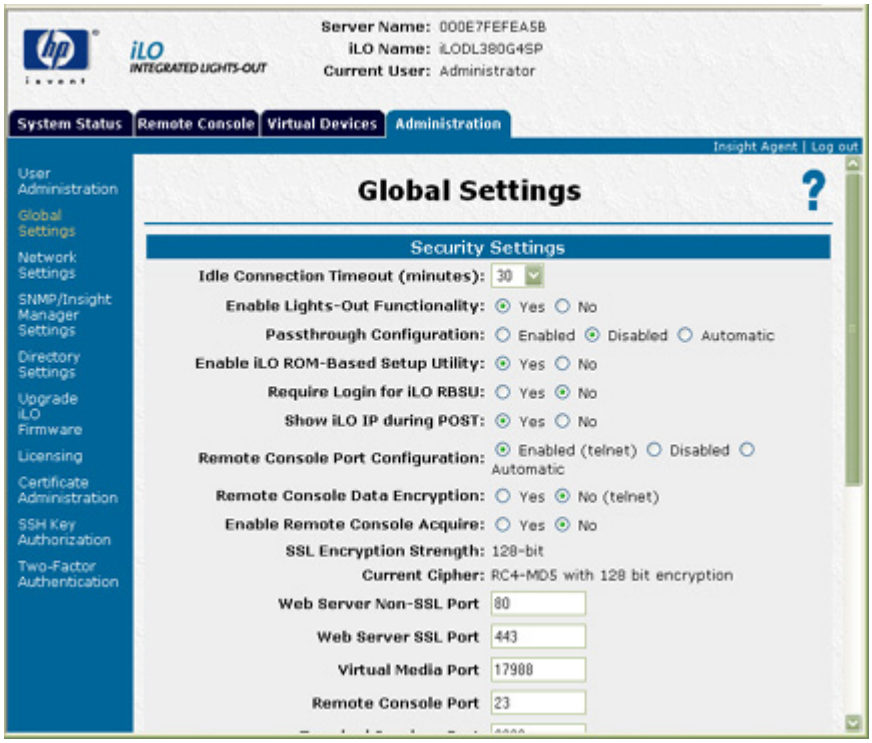
Pour supprimer les informations d'un utilisateur existant :

1. Ouvrez une session sur la carte iLO en utilisant un compte doté du privilège Administer User Accounts (Administrer comptes utilisateur). Cliquez sur **Administration**.
2. Cliquez sur **User Administration** (Administration des utilisateurs) et sélectionnez dans la liste l'utilisateur dont vous souhaitez modifier les informations.
3. Cliquez sur **Delete User** (Supprimer utilisateur). Une fenêtre s'affiche et contient le message suivant : `«Are you sure you want to delete the selected user?»` (Souhaitez-vous vraiment supprimer l'utilisateur sélectionné ?). Cliquez sur **OK**.

Paramètres généraux

L'option Global Settings (Paramètres généraux) permet d'afficher et de modifier les paramètres de sécurité de la carte iLO. Grâce à cette option, vous pouvez configurer le délai de console distante et les ports iLO à utiliser pour le serveur Web iLO, la console distante et le support virtuel. Ces paramètres sont appliqués globalement, quels que soient les paramètres utilisateur individuels.

Vous devez disposer du privilège de configuration des paramètres iLO pour modifier ces derniers. Les utilisateurs ne disposant pas de ce privilège peuvent uniquement consulter les paramètres attribués. Pour gérer ce privilège, utilisez les paramètres de configuration de périphérique local dans les composants logiciels intégrables d'administration d'annuaire pour les utilisateurs d'annuaire.



L'option Global Settings (Paramètres généraux) permet de définir les fonctions suivantes :

- Idle Connection Timeout (minutes) (Délai d'inactivité de la connexion - minutes)
- Enable Lights-Out Functionality (Activer la fonctionnalité Lights-Out)
- Passthrough Configuration (Configuration de Passthrough)
- Enable iLO ROM-Based Setup Utility (Activer utilitaire iLO RBSU)
- Require Login for iLO RBSU (Exiger connexion pour utilitaire iLO RBSU)
- Show iLO during POST (Afficher iLO pendant le test POST)
- (Remote Console Port Configuration) Configuration du port de console distante
- Remote Console Data Encryption (Codage données de console distante)
- Enable Remote Console Acquire (Activer l'acquisition de la console distante)
- SSL Encryption Strength (Capacité de codage SSL)
- Current Cipher (Codage actuel)
- Web Server Non-SSL Port (Port non SSL du serveur Web)
- Web Server SSL Port (Port SSL du serveur Web)
- Virtual Media Port (Port du support virtuel)
- Port de console distante
- Terminal Services Port (Port des Terminal Services)
- Secure Shell (SSH) Port (Port SSH)

- Secure Shell (SSH) Access (Accès SSH)
- Serial Command Line Interface Status (État de l'interface de ligne de commande série)
- Serial Command Line Interface Speed (bits/second) (Vitesse de l'interface de ligne de commande série - bits/s)
- Minimum Password Length (Longueur minimale du mot de passe)
- Remote Keyboard Model (Modèle du clavier distant)

Pour modifier les paramètres généraux iLO :

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO). Cliquez sur **Administration**.
2. Cliquez sur **Global Settings** (Paramètres généraux).
3. Modifiez les paramètres généraux en entrant vos sélections.
4. Ceci fait, cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Paramètres réseau

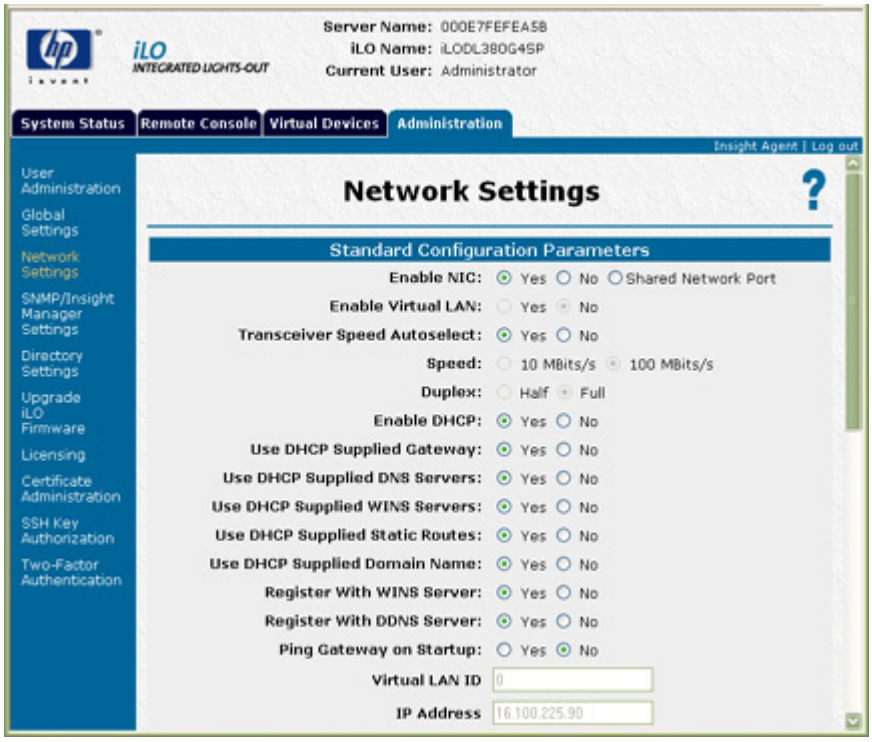
L'option Network Settings (Paramètres réseau) permet d'afficher et de modifier l'adresse IP de la carte réseau, le masque de sous-réseau et d'autres paramètres associés au protocole TCP/IP. Cet écran vous permet d'activer ou de désactiver le protocole DHCP et, pour les serveurs qui n'utilisent pas ce protocole, de configurer une adresse IP statique.

Vous devez disposer du droit de configuration des paramètres iLO pour modifier ces derniers. Les autres peuvent uniquement consulter les paramètres attribués.

Pour modifier les paramètres réseau de la carte iLO :

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO). Cliquez sur **Administration**.
2. Cliquez sur **Network Settings** (Paramètres réseau).
3. Modifiez les paramètres réseau selon vos besoins.

4. Ceci fait, cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.



Lorsque vous cliquez sur **Apply** (Appliquer), la carte iLO redémarre et la connexion de votre navigateur à la carte iLO se termine. Pour rétablir la connexion, patientez 60 secondes avant de lancer une autre session de votre navigateur et de vous connecter.

Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Paramètres de configuration du port de diagnostic iLO

Le port de diagnostic iLO à l'avant des serveurs ProLiant BL p-Class permet de consulter et de résoudre les problèmes du serveur à l'aide du câble de diagnostic. Le port de diagnostic iLO utilise une adresse IP statique. Il n'utilise pas DHCP pour obtenir une adresse IP, pour s'enregistrer auprès de WINS ou du service DNS dynamique, ou pour utiliser une passerelle. Le câble du port de diagnostic ne doit pas rester branché lorsque la connexion réseau n'est pas active car cela pourrait affecter les performances du réseau sur le port réseau iLO standard.

Les options Network Settings (Paramètres réseau) permettent de configurer les informations spécifiques au port de diagnostic. Pour plus d'informations sur l'utilisation du port et du câble de diagnostic, reportez-vous au manuel d'installation et de configuration de votre serveur lame.

Les champs suivants peuvent être configurés pour le port de diagnostic :

- Enable NIC (Activer la carte réseau)

  Si cette option est paramétrée sur Yes (Oui), le port de diagnostic est activé.
- Transceiver Speed Autoselect (Sélection automatique de la vitesse du transceiver)
- Vitesse
- Duplex
- IP Address (Adresse IP)

Utilisez ce paramètre pour attribuer une adresse IP statique à iLO sur votre réseau. Par défaut, l'adresse IP est attribuée par DHCP. Par défaut, l'adresse IP est 192.168.1.1 pour tous les ports de diagnostic iLO.

- Subnet Mask (Masque de sous-réseau)
  - Utilisez ce paramètre pour attribuer le masque de sous-réseau du port de diagnostic iLO. Par défaut, le masque de sous-réseau est 255.255.255.0 pour tous les ports de diagnostic iLO.
  - L'utilisation du port de diagnostic est détectée automatiquement lorsqu'un câble réseau actif y est raccordé. Lors du basculement entre le port de diagnostic et le port arrière, vous devez attendre que la commutation réseau soit terminée (environ 90 secondes) avant de tenter de vous connecter à l'aide du navigateur.

    REMARQUE : le port de diagnostic n'est pas commuté si une session de console distante est active ou qu'une mise à jour du microprogramme est en cours.

Récupération après l'échec d'une mise à jour du microprogramme iLO

En cas d'échec d'une mise à jour du microprogramme iLO, il existe plusieurs options de récupération. Pour chacune d'entre elles, vous devez disposer d'une image courante du microprogramme. HP vous déconseille d'utiliser une version antérieure du microprogramme iLO car celle-ci pourrait être altérée.

1. Téléchargez la version la plus récente du microprogramme. Les téléchargements iLO sont disponibles sur le site Web HP (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).
2. Déterminez si la mise à jour a échoué.
   a. Pouvez-vous tester (ping) iLO ?
   b. Parvenez-vous à vous connecter ?
   c. L'invite iLO Option ROM apparaît-elle lors du test POST du système hôte ?
   d. Les voyants d'état iLO s'allument-ils selon un schéma régulier ? Examinez les voyants d'état iLO à l'intérieur du serveur pour vérifier s'ils s'allument selon un schéma régulier (voyant 8, 7, 6, 5, 4, 3, 2, 1). Si c'est le cas, passez à l'étape 4.
3. Essayez d'exécuter un nouveau flashage réseau.

   Vous pouvez lancer une mise à jour du microprogramme à l'aide des scripts RIBCL ou d'un navigateur.

   En cas d'échec du flashage réseau, exécutez le composant de flashage en ligne. Les composant sont à la fois disponibles pour Windows® et Linux.
4. En cas d'échec du composant de flashage en ligne, essayez la disquette ROMPAQ.
   a. Créez les disquettes ROMPAQ et démarrez l'hôte à l'aide de la disquette 1.
   b. La définition du commutateur de neutralisation de la sécurité iLO peut s'avérer nécessaire. Restaurez-le une fois le processus de flashage terminé.

Paramètres SNMP/Insight Manager

L'option SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) permet de configurer les alertes SNMP, de générer une alerte de test et de configurer l'intégration avec Systems Insight Manager.

Activation des alertes SNMP

iLO prend en charge jusqu'à trois adresses IP pour la réception des alertes SNMP. Les adresses utilisées sont identiques à l'adresse IP de la console du serveur Systems Insight Manager.

Vous devez disposer du droit de configuration des paramètres iLO pour modifier les paramètres d'alerte. Les autres peuvent uniquement consulter les paramètres attribués.

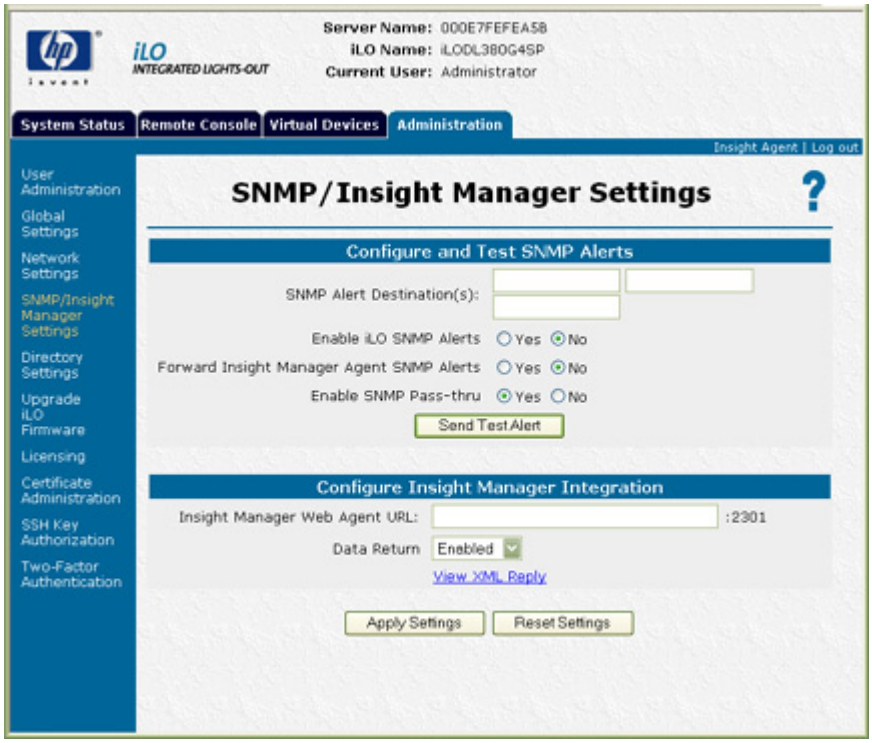
Les options d'alerte suivantes sont disponibles dans l'écran SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) :

- Enable iLO SNMP Alerts (Activer les alertes SNMP de iLO)
- Forward Insight Manager Agent SNMP Alerts (Transmettre les alertes SNMP des agents Insight Manager)
- Enable SNMP Pass-thru (Activer le Pass-Thru SNMP)
- Enable p-Class Alert Fowarding (Activer le transfert des alertes p-Class) (s'affiche sur les serveurs p-Class uniquement)

Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Pour configurer les alertes :

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO).
2. Sélectionnez **SNMP/Insight Manager Settings** (Paramètres SNMP/Insight Manager) sous l'onglet Administration.



3. Entrez jusqu'à trois adresses IP de réception des alertes SNMP.
4. Sélectionnez les options d'alerte que la carte iLO doit prendre en charge.
5. Cliquez sur **Apply Settings** (Appliquer les paramètres).

Génération d'alertes de test

Les alertes de test sont générées à l'aide de l'option SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) disponible dans la section Administration de la fenêtre de navigation de la carte iLO. Elles comportent un trap SNMP de Insight Manager et permettent de vérifier la connectivité réseau de la carte iLO dans Systems Insight Manager. Seuls les utilisateurs dotés du privilège Configure iLO Settings (Configurer paramètres iLO) peuvent envoyer des alertes de test.

Cliquez sur **Apply Settings** (Appliquer paramètres) pour enregistrer les éventuelles modifications apportées aux champs SNMP Alert Destination(s) (Destination(s) des alertes SNMP) avant d'envoyer une alerte de test.

Pour envoyer une alerte de test :

1. Sélectionnez **SNMP/Insight Manager Settings** (Paramètres SNMP/Insight Manager) sous l'onglet Administration.
2. Cliquez sur **Send Test Alert** (Envoyer alerte de test) pour générer une alerte de test et l'envoyer aux adresses TCP/IP enregistrées dans les champs SNMP Alert Destination(s) (Destination(s) des alertes SNMP).
3. Une fois l'alerte générée, un écran de confirmation s'affiche.
4. Vérifiez que le Systems Insight Manager ou la console Systems Insight Manager reçoit correctement le trap.

Configuration de l'intégration avec Insight Manager

La carte iLO vous permet de configurer l'URL (nom DNS ou adresse IP) des agents Web de Insight Manager utilisés sur le serveur hôte. Vous pouvez également configurer le niveau des données renvoyées avec les informations d'identification de Systems Insight Manager.

REMARQUE : en général, la valeur saisie dans le champ Insight Manager Web Agent URL (URL de l'agent Web Insight Manager) correspond à l'adresse IP ou au nom DNS uniquement. Il est inutile d'entrer le protocole («http://», par exemple) et l'ID de port («:2301», par exemple).

Le lien vers les agents Web Insight se trouve dans la barre d'en-tête bleue, à côté du lien Log out (Déconnexion).

Directory Settings (Paramètres d'annuaire)

L'écran Directory Settings (Paramètres d'annuaire) permet de configurer et de tester vos services d'annuaire. Pour plus d'informations sur les annuaires, reportez-vous à la section « Services d'annuaire » (page 117). Pour plus d'informations sur les paramètres de configuration des annuaires, reportez-vous à la section « Configuration des paramètres d'annuaire » (page 71).

Mise à niveau du microprogramme iLO

Les mises à niveau du microprogramme améliorent le fonctionnement de la carte iLO. Le microprogramme peut être mis à niveau à partir de n'importe quel client réseau utilisant un navigateur pris en charge. Seuls les utilisateurs dotés du privilège Update iLO Firmware (Mettre à jour microprogramme iLO) peuvent mettre à niveau le microprogramme iLO. Le microprogramme iLO le plus récent est disponible sur le site Web HP.

Pour mettre à niveau le microprogramme iLO à l'aide d'un navigateur pris en charge :

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO).
2. Cliquez sur **Upgrade iLO Firmware** (Mettre à niveau microprogramme iLO) sous l'onglet Administration.

3. Entrez le nom de fichier dans le champ New firmware image (Image du nouveau microprogramme) ou recherchez manuellement le fichier en cliquant sur Browse (Parcourir).
4. Cliquez sur **Send Firmware Image** (Envoyer image du microprogramme).
5. La mise à niveau du microprogramme prend environ deux minutes. Une barre affiche l'état de progression de la mise à niveau.

N'interrompez pas une session de mise à jour du microprogramme de la carte iLO. Si vous l'interrompez, reportez-vous à la section « Mise à niveau impossible du microprogramme iLO » (page 208).

Le système iLO est automatiquement réinitialisé à la fin d'une mise à niveau de microprogramme réussie. Le système d'exploitation et le serveur hôte ne sont pas affectés par la réinitialisation du système iLO.

Si la mise à jour du microprogramme a été interrompue ou a échoué, faites immédiatement une nouvelle tentative. Ne réinitialisez pas le système iLO avant toute nouvelle tentative de mise à niveau du microprogramme. iLO permet de récupérer la mise à niveau du microprogramme via un site FTP (« Mise à niveau impossible du microprogramme iLO », page 208) en cas d'interruption ou d'échec de cette dernière.

REMARQUE : pour les systèmes munis d'unités de disquette, vous pouvez également mettre à jour le microprogramme iLO à l'aide des disquettes ROMPaq. HP **déconseille** de mettre à niveau le microprogramme iLO à l'aide de l'unité de disquette du support virtuel.

Administration des certificats

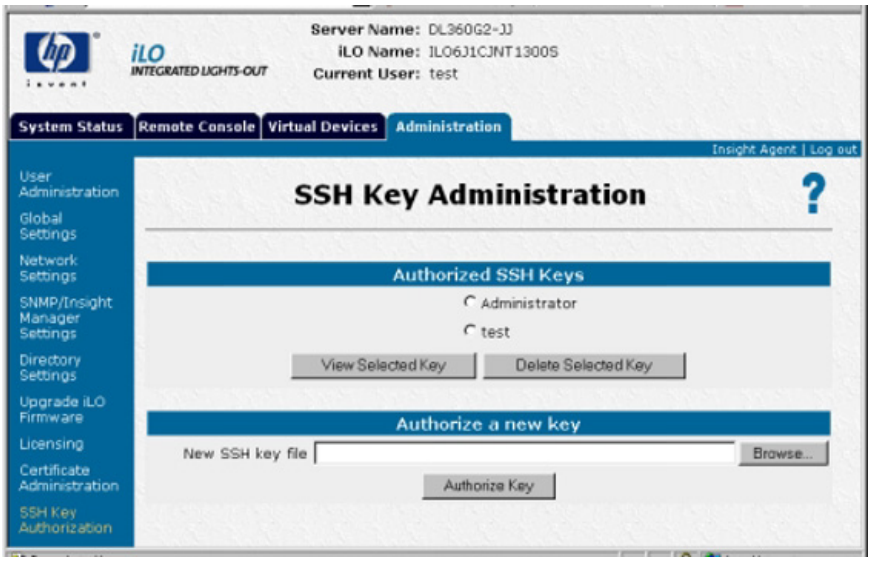
L'écran Certificate Information (Informations sur le certificat) affiche les informations associées au certificat enregistré. Les informations sont codées dans le certificat par l'autorité de certification et sont extraites par la carte iLO afin d'être affichées.

- Issued To (Envoyé à) est l'entité à laquelle le certificat a été envoyé.
- Issued By (Envoyé par) correspond à l'autorité de certification qui émet le certificat.
- Valid From (Début de validité) est la date de début de validité du certificat.
- Valid Until (Fin de validité) est la date d'expiration du certificat.
- Serial Number (Numéro de série) est le numéro de série attribué au certificat par l'autorité de certification.

La page d'importation d'un certificat affiche des informations sur la procédure d'importation d'un certificat. Pour plus d'informations sur l'importation de certificats, reportez-vous à la section « Certificats » (page 59) et au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

SSH Key Administration (Administration de clés SSH)

Cette page indique le propriétaire de chaque clé SSH autorisée. Vous pouvez sélectionner et afficher en détails ou supprimer n'importe quelle clé en cliquant respectivement sur **View Selected Key** (Afficher clé sélectionnée) ou **Delete Selected Key** (Supprimer clé sélectionnée). Un maximum de quatre clés est autorisé. Plusieurs clés peuvent appartenir à un même utilisateur.



Pour autoriser une nouvelle clé :

1. Cliquez sur **Browse** (Parcourir) et recherchez le fichier de clé.

   Le chemin du fichier de clé publique doit être envoyé à iLO. Ce fichier doit contenir le nom d'utilisateur après la fin de la clé. iLO va associer chaque clé à un compte utilisateur local. Si le compte local n'existe pas ou s'il est supprimé, la clé sera invalide (elle ne sera pas répertoriée ici si le compte local n'existe pas). Sinon, vous pouvez autoriser des clés SSH pour un serveur SIM HP en exécutant l'outil mxagentconfig à partir du serveur SIM HP, ce qui indique l'adresse et les donnés d'authentification utilisateur pour iLO. Consultez la documentation SIM HP pour plus de détails.
2. Click **Authorize Key**.

Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs)

Cette page affiche la configuration des paramètres d'authentification à deux facteurs et les informations relatives au certificat validé par l'autorité de certification. Elle propose également une méthode permettant de modifier la configuration et d'importer ou de supprimer un certificat validé par l'autorité de certification.

Le paramètre Enforce Two-Factor Authentication (Renforcer l'authentification à deux facteurs) détermine si l'authentification à deux facteurs est utilisée pour l'authentification utilisateur pendant la procédure d'identification. Si vous sélectionnez Yes (Oui) pour ce paramètre, l'authentification à deux facteurs sera requise. Si vous sélectionnez No (Non), cette fonction sera désactivée et la connexion sera possible avec le nom d'utilisateur et le mot de passe seuls. iLO ne permet pas d'attribuer la valeur Yes (Oui) à ce paramètre tant qu'aucun certificat validé par l'autorité de certification n'a été configuré. La modification de ce paramètre implique la réinitialisation du système iLO afin que les changements prennent effet. Pour fournir la sécurité nécessaire, les changements suivants seront également apportés à la configuration au moment de l'activation de l'authentification à deux facteurs :

- Remote Console Data Encryption (Codage données de console distante) : Yes (Oui) (désactive l'accès Telnet)
- Enable Secure Shell (SSH) Access (Activer l'accès SSH) : Non
- Serial Command Line Interface Status (État de l'interface de ligne de commande série) : Disabled (Désactivé)

Si l'accès requiert Telnet, SSH ou une interface de ligne de commande série, réactivez ces paramètres une fois que l'authentification à deux facteurs a été activée. Toutefois, ces méthodes d'accès n'offrant pas la possibilité d'une authentification à deux facteurs, seul un facteur est requis lors de l'accès à iLO avec Telnet, SSH ou une interface de ligne de commande série.

Lorsque l'authentification à deux facteurs est activée, l'accès via l'utilitaire CPQLOCFG est désactivé car ce dernier ne répond pas à toutes les conditions requises relatives à l'authentification. En revanche, l'utilitaire HPONCFG est opérationnel car son exécution requiert des privilèges d'administrateur sur le système hôte.

Le paramètre Check for Certificate Revocation (Contrôler la révocation de certificat) vérifie que iLO utilise l'attribut des points de distribution de la liste des révocations de certificat pour télécharger la liste la plus récente et contrôle la révocation éventuelle du certificat. Si le certificat client figure dans la liste des révocations de certificat ou si cette dernière ne peut pas être téléchargée pour quelque raison que ce soit, l'accès est refusé. Le point de distribution de la liste des révocations de certificat doit être disponible et accessible pour iLO lorsque vous attribuez la valeur Yes (Oui) au paramètre Check Certificate Revocation (Contrôler la révocation de certificat).

Le paramètre Certificate Owner Field (Champ du propriétaire du certificat) indique l'attribut de certificat client à utiliser pour l'authentification par rapport à l'annuaire. Si vous spécifiez la valeur SAN (Réseau SAN), iLO extrait la valeur du paramètre User Principle Name (Nom principal de l'utilisateur) de l'attribut Subject Alternative Name (Autre nom de l'objet) puis l'utilise pour l'authentification par rapport à l'annuaire, par exemple nom_utilisateur@domaine.extension. Si vous spécifiez la valeur Subject (Objet), iLO déduit le nom distinct de l'utilisateur à partir de l'attribut de nom d'objet. Par exemple, si le nom d'objet est `/DC=com/DC=domain/OU=organization/CN=user`, iLO déduit :

```
CN=user,OU=organization,DC=domain,DC=com.
```

Le paramètre Certificate Owner Field (Champ du propriétaire du certificat) est utilisé uniquement lorsque l'authentification par rapport à l'annuaire est activée. La configuration de ce paramètre dépend de la version de prise en charge d'annuaire utilisée, de la configuration de l'annuaire et de la politique de délivrance de certificats de votre entreprise.

Un certificat validé par l'autorité de certification est obligatoire pour que l'authentification à deux facteurs fonctionne. iLO ne permet pas d'attribuer la valeur Yes (Oui) au paramètre Enforce Two-Factor Authentication (Renforcer l'authentification à deux facteurs) tant qu'aucun certificat validé par l'autorité de certification n'a été configuré. En outre, un certificat client doit être associé à un compte utilisateur local si des comptes d'utilisateurs locaux sont utilisés. Si iLO utilise l'authentification par rapport à l'annuaire, l'association de certificats client aux comptes d'utilisateurs locaux est facultative.

Pour modifier les paramètres de l'authentification à deux facteurs :

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO). Cliquez sur **Administration**.
2. Cliquez sur **Two-Factor Authentication Settings** (Paramètres d'authentification à deux facteurs).
3. Si nécessaire, modifiez les paramètres en renseignant les champs appropriés.
4. Ceci fait, cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Connexion à chaud du clavier

La fonction Hot-Plug Keyboard (Connexion à chaud du clavier) a été mise en œuvre sur tous les serveurs dotés de la carte iLO. Cette fonctionnalité prend en charge la connexion d'un clavier local au serveur alors que ce dernier est sous tension. Il n'est pas nécessaire de réinitialiser le serveur pour faire appliquer cette fonction après la connexion d'un clavier à chaud. Si un clavier est connecté au serveur après l'amorçage du système d'exploitation, le clavier connecté à chaud sera parfaitement fonctionnel. Un clavier peut être connecté à chaud à plusieurs reprises après l'amorçage du système d'exploitation.

Définitions relatives au clavier

- Clavier local : clavier physiquement relié au connecteur PS2 du serveur.
- Clavier de la console distante : clavier utilisé pendant une session de console distante.
- Fonctionnalité Hot-plug Keyboard : clavier local fonctionnel à 100 % après sa connexion à chaud au serveur.
- Connexion d'un clavier à chaud : consiste à brancher un clavier local au connecteur PS2 du serveur alors que le serveur est sous tension.
- Déconnexion d'un clavier à chaud : consiste à débrancher un clavier local du serveur alors que ce dernier est sous tension.

Utilisation recommandée de la fonction Hot-Plug Keyboard (Connexion à chaud du clavier)

Pour optimiser les résultats, suivez les recommandations suivantes :

- Connectez à chaud le clavier local uniquement après l'amorçage du système d'exploitation.
- Ne débranchez pas le clavier local à chaud avant l'amorçage du système d'exploitation. La connexion ou la déconnexion à chaud du clavier local avant l'amorçage du système d'exploitation peut entraîner des conséquences imprévisibles.

⚠ **AVERTISSEMENT :** évitez de modifier les paramètres réseau ou les affectations de port iLO, de réinitialiser la carte iLO, de mettre à niveau le microprogramme iLO ou de rendre la carte iLO indisponible lors de la mise sous tension du serveur ou l'amorçage du système d'exploitation sans avoir de clavier local connecté. Il est préférable d'effectuer ces actions avant la mise sous tension du serveur ou après l'amorçage du système d'exploitation. Si vous exécutez ces actions avant de mettre le serveur sous tension, attendez 30 secondes avant d'allumer l'appareil.

Le non respect de ces consignes peut provoquer le dysfonctionnement du clavier local et du clavier de la console distante.

Résolution des problèmes liés à la fonction Hot-Plug Keyboard (Connexion à chaud du clavier)

Si la connexion à chaud du clavier est indisponible ou se bloque, vérifiez les points suivants pour résoudre le problème. Pour optimiser les résultats, suivez les consignes recommandées dans la section « Utilisation recommandée de la fonction Hot-Plug Keyboard (Connexion à chaud du clavier) » (page 37).

- Si une session de console distante est active sur le serveur, le clavier local ne sera pas opérationnel après sa connexion à chaud. Cette configuration a été volontairement conçue à des fins de sécurité.
- Lorsque la carte iLO est indisponible de la mise sous tension à l'amorçage du système d'exploitation, et en l'absence d'un clavier local, le clavier de la console distante peut, selon le système d'exploitation utilisé, ne pas fonctionner lorsque la carte iLO redevient à nouveau disponible. La carte iLO peut devenir indisponible pour différentes raisons, notamment à cause de la mise à niveau du microprogramme, de la modification des paramètres réseau ou de la réaffectation des ports. Il peut s'avérer nécessaire de réinitialiser le système pour rétablir la fonctionnalité Remote Console Keyboard (Clavier de la console distante).
- Lorsque la carte iLO est indisponible de la mise sous tension à l'amorçage du système d'exploitation, et en l'absence d'un clavier local, le clavier de la console distante peut, selon le système d'exploitation utilisé, ne pas fonctionner lorsque la carte iLO redevient à nouveau disponible. La carte iLO peut devenir indisponible pour différentes raisons, notamment à cause de la mise à niveau du microprogramme, de la modification des paramètres réseau ou de la réaffectation des ports. Il peut s'avérer nécessaire de réinitialiser le système pour rétablir la fonctionnalité Remote Console Keyboard (Clavier de la console distante).
- Si la carte iLO est trop occupée pour répondre promptement aux commandes de clavier envoyées par le système d'exploitation pendant le chargement de ce dernier, et en l'absence de clavier local, le système d'exploitation considère qu'aucun clavier n'est branché. Cette situation est improbable mais peut théoriquement se produire à tout moment dès lors que la carte iLO devient extrêmement occupée. Cela peut survenir lorsque la carte iLO est confrontée à un refus de service au niveau de sa carte réseau. Dans ce cas, si un clavier est connecté à chaud après le chargement du système d'exploitation, le clavier local et celui de la console distante peuvent, selon le système d'exploitation utilisé, ne pas fonctionner. Il peut s'avérer nécessaire de réinitialiser le système pour rétablir la fonctionnalité Remote Console Keyboard (Clavier de la console distante).
- Si le clavier local est déconnecté à chaud après l'amorçage du système d'exploitation à l'aide des touches Verr maj, Verr Num ou Arrêt défil, puis reconnecté à chaud, les voyants du clavier local ne correspondent pas à l'état courant du clavier. Appuyez sur la touche de verrouillage de la fonction souhaitée jusqu'à ce que l'état du voyant soit correct.
- Si le clavier local se bloque lors de sa connexion à chaud, déconnectez-le puis branchez-le à nouveau.

Option Terminal Services Pass-Through (Pass-Through des Terminal Services)

Terminal Services est une fonctionnalité des systèmes d'exploitation Microsoft® Windows®. L'option Terminal Services Pass-Through (Pass-Through des Terminal Services) fournit une connexion entre le serveur Terminal Services du système hôte et le client Terminal Services sur le système client. Lorsqu'elle est activée, le microprogramme iLO configure un connecteur, en écoutant par défaut sur le port 3389. Toutes les données envoyées par Terminal Services sur ce port sont transmises au serveur et toutes celles envoyées par le serveur sont retransmises au connecteur. Le microprogramme considère que toutes les données reçues sur ce port le sont sous forme de paquets RDP. Les paquets RDP sont échangés entre le microprogramme iLO et le serveur Terminal Services (RDP) du serveur via l'adresse hôte locale sur le serveur. Un service est assuré pour faciliter les communications entre le microprogramme iLO et le serveur RDP, de telle sorte que le serveur RDP considère qu'une connexion RDP externe a été établie. Pour plus d'informations sur le service RDP, reportez-vous à la section « Service Windows® RDP Pass-Through (Pass-Through Windows® RDP) » (page 40).

Une session Terminal Services fournit une vue améliorée de la console du système hôte. Lorsque le système d'exploitation (ou que le serveur ou le client Terminal Services) est indisponible, c'est la console distante traditionnelle iLO qui fournit la vue de la console du système hôte. Pour plus d'informations sur la console distante et Terminal Services, reportez-vous à la section « Console distante et clients Terminal Services » (page 42).

Pour configurer l'option Terminal Services Pass-Through (Pass-Through des Terminal Services), reportez-vous aux sections « Conditions requises pour le client Terminal Services » (page 39) et « Installation de l'option Terminal Services Pass-Through (Pass-Through des Terminal Services) » (page 40).

Conditions requises pour le client Terminal Services

Le client Terminal Services est disponible sur des machines client Microsoft® Windows® exécutant :

- Windows® 2000

  Les serveurs Microsoft® Windows® 2000 requièrent l'installation de Microsoft® .NET Framework pour prendre en charge l'utilisation de Terminal Services. Après avoir installé .NET Framework, le client Terminal Services doit être installé à partir des disquettes créées par le serveur Terminal Services. Pour obtenir des instructions, reportez-vous aux manuels d'utilisation ou aux fichiers d'aide de Windows®. Installez le client Terminal Services sur Windows® 2000 dans l'emplacement par défaut. Il génère une boîte de dialogue demandant quel est le serveur Terminal Services cible à utiliser.

- Windows® Server 2003

  Sur les serveurs Windows® Server 2003, la connexion Terminal Services and RDP (Services Terminal et RDP) est intégrée. Le client fait partie intégrante du système d'exploitation et est activé à l'aide de Remote Desktop (Bureau à distance). Pour activer Remote Desktop (Bureau à distance), sélectionnez **My Computer>Properties>Remote>Remote Desktop** (Poste de travail>Propriétés>À distance>Bureau à distance). Le client Terminal Services sous Windows® Server 2003 fournit des options de ligne de commande et des lancements en toute transparence à partir de l'applet Remote Console.

- Windows® XP

  Sur les serveurs Windows® XP, la connexion Terminal Services and RDP (Services Terminal et RDP) est intégrée. Le client fait partie intégrante du système d'exploitation. Pour l'exécuter, sélectionnez **Start>Programs>Accessories>Communications>Remote Desktop** (Démarrer>Tous les programmes> Accessoires>Communications>Bureau à distance). Le client Terminal Services sous Windows® XP fournit des options de ligne de commande et des lancements en toute transparence à partir de l'applet Remote Console.

Service Windows® RDP Pass-Through (Pass-Through Windows® RDP)

Pour utiliser la fonctionnalité Terminal Services Pass-Through (Pass-Through des Terminal Services) de iLO, vous devez installer un service spécial sur le système hôte. Ce service affiche le nom du serveur Proxy iLO dans la liste des services disponibles de l'hôte. Ce service utilise l'environnement de sécurité et de fiabilité de Microsoft® .NET Framework. Une fois que le service est lancé, celui-ci interroge la carte iLO pour trouver si une connexion RDP a été établie avec le client. Lorsqu'une connexion RDP a été établie avec le client, celle-ci établit à son tour une connexion TCP avec l'hôte local et démarre l'échange de paquets. La lecture du port utilisé pour communiquer avec l'hôte local se fait depuis le registre Windows® :

```
HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp\
PortNumber
```

Il s'agit en général du port 3389.

Installation de l'option Terminal Services Pass-Through (Pass-Through des Terminal Services)

- Microsoft® Windows® 2000 et Windows® 2003

  Les serveurs Microsoft® Windows® 2000 requièrent Microsoft® .NET Framework pour prendre en charge l'utilisation de Terminal Services. Le service d'émulation Terminal Services et le driver d'interface de supervision de iLO pour Windows® 2000 et Windows® Server 2003 doivent être installés sur le serveur doté de iLO. Le service et le driver iLO sont disponibles sous forme de composants Smart sur le site Web HP et le CD HP SmartStart. Ils font également partie du ProLiant Support Pack pour Microsoft® Windows® Server 2003 et Microsoft® Windows®.

  a. Installez le driver d'interface de supervision de iLO.

  b. Installez le service. Pour installer le service, lancez le composant d'installation et suivez les instructions de l'assistant d'installation.

     Si le service est déjà installé, il faut le redémarrer manuellement ou réinitialiser le serveur lors de l'installation du service.

  c. Installez ou activez le client Terminal Services.

     Les serveurs Microsoft® Windows® 2000 requièrent l'installation de Microsoft® .NET Framework pour prendre en charge l'utilisation de Terminal Services. Après avoir installé .NET Framework, le client Terminal Services doit être installé à partir des disquettes créées par le serveur Terminal Services (Services Terminals) ou en téléchargeant le client à partir du site Web Microsoft® et en l'installant à l'aide de l'option Add or Remove Programs (Ajout/ Suppression de programmes) du Panneau de configuration. Pour obtenir des instructions, reportez-vous aux manuels d'utilisation ou aux fichiers d'aide de Windows®. Installez le client Terminal Services sur Windows® 2000 dans l'emplacement par défaut.

     Sous Windows® Server 2003, vous pouvez activer Remote Desktop (Bureau à distance) en sélectionnant My Computer (Poste de travail)>Properties (Propriétés)>**Remote** (À distance).

Si l'installation d'iLO est terminée et que la fonction Terminal Services Pass-Through (Pass-Through des Terminal Services) est spécifiée sur l'option automatique, la fonctionnalité Terminal Services s'exécute à la fin de l'installation.

- Microsoft® Windows® XP

  Sur les serveurs Windows® XP, la connexion Remote Desktop (Bureau à distance) est intégrée et ne requiert pas de spécifications d'installation supplémentaires.

Les erreurs survenues durant l'installation et l'exécution du service Pass-Through sont consignées dans la fonction Application Event Log (Journal d'événements de l'application) du serveur. Vous pouvez supprimer le service Pass-Through à l'aide de l'option Add or Remove Programs (Ajout/Suppression de programmes) du Panneau de configuration.

Modification du port Terminal Services de Windows® 2000

Si le port Terminal Services est modifié, le client Windows® 2000 doit configurer manuellement Terminal Services Client Connection Manager (Gestionnaire de connexion client Terminal Services).

1. Lancez Terminal Services Client Connection Manager (Gestionnaire de connexion client Terminal Services) et créez une nouvelle connexion au serveur.
2. Mettez en surbrillance l'icône créée, puis sélectionnez **File>Export** (Fichier>Exporter). Renommez le fichier à l'aide d'une extension .cns. Par exemple : myilo.cns.
3. Recherchez la ligne Server Port=3389 pour modifier le fichier `myilo.cns`. Remplacez 3389 par le nouveau numéro et enregistrez le fichier.
4. Dans Client Connection Manager (Gestionnaire de connexion client), mettez en surbrillance l'icône **New Connection** (Nouvelle connexion), puis cliquez sur **File>Import** (Fichier>Importer).
5. Double-cliquez sur l'icône nouvellement créée pour lancer le terminal serveur et vous connecter au nouveau port.

Activation de l'option Terminal Services Pass-Through (Pass-Through des Terminal Services)

La fonction Terminal Services pass-through (Pass-Through des Terminal Services) est désactivée par défaut et doit être activée dans Global Settings (Paramètres généraux). Jusqu'à ce qu'elle soit activée, le bouton Terminal Services de la console distante est désactivé et le message d'erreur de session de console `Remote Session already in use by another user` (Session distante déjà utilisée par un autre utilisateur) est faux.

L'utilisation de la fonction Terminal Services pass-through (Pass-Through des Terminal Services) requiert l'installation sur le serveur du driver d'interface de supervision Lights-Out et du service d'émulation Terminal Services les plus récents pour Microsoft® Windows®. Le driver d'interface doit être installé avant d'installer le service.

Lorsque l'option Terminal Services Pass-Through (Pass-Through des Terminal Services) est définie à Enabled (Activé) ou à Automatic (Automatique) sur la page Global Settings (Paramètres généraux) et que le client Terminal Services est installé sur le client Windows® (s'installe par défaut sur Windows® XP), le bouton Terminal Services est activé. Lorsque ce bouton est activé, l'applet essaye de lancer Terminal Services, même si le serveur n'exécute pas de système d'exploitation Windows®.

Vous devez respecter les spécifications de la licence Microsoft® qui sont les mêmes que pour la connexion via la carte réseau du serveur. Par exemple, lorsqu'elle est spécifiée pour un accès administrateur, la fonction Terminal Services autorise deux connexions au plus, que celles-ci aient lieu via la carte réseau serveur, la carte iLO ou les deux.

État de l'option Terminal Services Pass-Through (Pass-Through des Terminal Services)

La page iLO Status (État de la carte iLO) affiche l'état de l'option Terminal Services Pass-Through (Pass-Through des Terminal Services) comme suit :

- Server software not detected (Logiciel de serveur non détecté)
- Available for Use (Disponible)
- In Use (En cours d'utilisation)

Le voyant UID clignote chaque fois qu'une connexion Terminal Services est activée via la carte iLO. Le clignotement se fait selon une fréquence et un cycle de fonctionnement identiques à ce qui se produit lorsque la console distante est activée.

Message d'avertissement de Terminal Services

Les utilisateurs de Terminal Services sur Windows® 2003 Server peuvent être confrontés aux situations suivantes lorsqu'ils utilisent la fonction Terminal Services pass-through (Pass-Through des Terminal Services) de iLO. Si une session Terminal Services est établie via la carte iLO et qu'une deuxième session du même type l'est par un administrateur Windows® (mode Console), la première est déconnectée. Cependant, la première session ne reçoit de message d'avertissement indiquant la déconnexion qu'au terme d'un délai d'une minute environ. Pendant ce temps, la première session est disponible ou active. Cette situation est tout à fait normale, mais différente de celle observée lorsque deux sessions Terminal Services sont établies par des administrateurs Windows®. Dans ce cas, la première session reçoit immédiatement le message d'avertissement.

Affichage du bouton Terminal Services

Cette version du microprogramme iLO ne s'affiche pas correctement à l'aide du bouton Terminal Services si le système d'exploitation hôte est activé pour le fonctionnement Terminal Services. Même si le système d'exploitation n'est pas activé (par exemple le système d'exploitation est Linux, qui ne prend pas en charge le fonctionnement Terminal Services), le bouton Terminal Services peut sembler actif et laisser faussement penser que le fonctionnement Terminal Services est disponible.

Console distante et clients Terminal Services

Il est possible de recourir à une session de console distante iLO pour afficher une session Terminal Services sur l'hôte, via la connexion à un réseau de supervision iLO. Lorsque l'applet de la console distante iLO s'exécute, elle lance le client Terminal Services, basé sur la préférence utilisateur. Il est nécessaire d'installer les Machines virtuelles Sun pour exploiter pleinement cette fonctionnalité. Si les Machines virtuelles Sun ne sont pas installées, l'option double curseur de la console distante ne peut pas lancer automatiquement le client Terminal Services.

Si l'option Terminal Services Pass-Through (Pass-Through des Terminal Services) est activée et que le serveur Terminal Services est disponible, le basculement entre la console distante de iLO et le client Terminal Services se fait de façon transparente, au fur et à mesure de la progression du serveur d'un environnement préalable au système d'exploitation vers un environnement sans système d'exploitation disponible, en passant par un environnement dans lequel s'exécute un système d'exploitation. La transparence de l'opération est valable tant que le client Terminal Services n'est pas lancé avant que la console distante soit disponible. Si ces fonctionnalités sont toutes deux disponibles, la console distante lancera le client Terminal Services au moment opportun.

Lors de l'utilisation de l'option Terminal Services pass-through (Pass-Through des Terminal Services) avec Windows® 2000, le client Terminal Services démarre une minute après l'affichage de la boîte de dialogue CTRL-ALT-DEL (CTRL-ALT-SUPPR). Sous Windows® Server 2003, ce retard est d'environ 30 secondes. Ce délai représente le temps nécessaire au service pour se connecter au client RDP qui s'exécute sur le serveur. Si le serveur est réamorcé à partir du client Terminal Services, l'écran Remote Console (Console distante) devient grisé ou noir pendant près d'une minute, le temps nécessaire à la carte iLO pour constater que le serveur Terminal Services n'est plus disponible.

Si le mode Terminal Services est spécifié sur `Enabled` (Activé) mais que vous souhaitez utiliser la console distante, le client Terminal Services doit être lancé directement à partir du menu du client Terminal Services. Cela permet d'utiliser simultanément le client Terminal Services et la console distante.

La fonctionnalité Terminal Services peut être désactivée ou activée à tout moment. La modification de la configuration des Terminal Services entraîne la réinitialisation du microprogramme iLO. Cette opération provoque l'interruption de toutes les connexions ouvertes avec la carte iLO.

Lorsque le client Terminal Services est lancé à l'aide de la fonction Remonte Console (Console distante), cette dernière passe en mode veille pour éviter de consommer de la largeur de bande de l'unité centrale. Pour toutes les commandes iLO, la fonction Remote Console (Console distante) utilise toujours par défaut le port 23 de la console distante.

La carte iLO effectue une seule émulation par connexion Terminal Services à la fois. La fonctionnalité Terminal Services est limitée à deux sessions simultanées.

Lorsqu'elle est en mode veille, la console distante devient active et disponible si le client Terminal Services est interrompu pour l'une des raisons suivantes :

- le client Terminal Services est fermé par l'utilisateur ;
- le système d'exploitation Windows® est arrêté ;
- le système d'exploitation Windows® se bloque.

Résolution des problèmes liés à Terminal Services

En cas de problèmes liés à l'émulation des Terminal Services iLO, procédez aux vérifications suivantes :

1. Pour vérifier que la fonctionnalité Terminal Services est activée sur l'hôte, sélectionnez **My Computer>Properties>Remote>Remote Desktop** (Poste de travail>Propriétés>À distance>Bureau à distance).
2. Pour vérifier que la configuration Pass-Through de iLO est activée ou automatique, consultez les paramètres généraux iLO.
3. Vérifiez si la fonctionnalité iLO Advanced dispose d'une licence.
4. Pour vérifier si le driver d'interface de supervision iLO est installé sur l'hôte, sélectionnez **My Computer>Properties>Hardware>Device Manager>Multifunction Adapters** (Poste de travail>Propriétés>Matériel>Gestionnaire de périphériques>Adaptateurs multifonctions).

5. Pour vérifier si le service d'émulation Terminal Services et le serveur proxy iLO sont installés et s'exécutent sur l'hôte, sélectionnez **Control Panel>Administrative Tools>Services** (Panneau de configuration>Outils d'administration>Services) et essayez de redémarrer le service.
6. Déterminez si le journal d'événements de l'application est plein.

   Le service d'émulation Terminal Services peut rencontrer des problèmes de démarrage lorsque le journal d'événements de l'application du système d'exploitation est plein. Pour afficher ce journal, sélectionnez **Computer Management>System Tools>Event Viewer>Application** (Gestion de l'ordinateur>Outils système>Observateur d'événements>Application).
7. Vérifiez que l'affectation du port Terminal Services est correcte. Vérifiez que le client Terminal Services mstsc.exe se trouve dans \WINDOWS\SYSTEM32.

   Si ce n'est pas le cas, reconfigurez l'émulation à **Enabled** (Activée) et activez manuellement le client Terminal Services.

iLO Shared Network Port (Port réseau partagé iLO)

La fonction iLO Shared Network Port (Port réseau partagé iLO) vous permet de choisir la carte réseau système ou la carte réseau iLO dédiée pour assurer la supervision du serveur. Le trafic réseau régulier et celui d'iLO transitent par la carte réseau système lorsque cette fonction est activée. Cette fonction n'est disponible que sur un nombre limité de serveurs ProLiant, tel qu'indiqué dans la section « Configuration de la fonction iLO Shared Network Port (Port réseau partagé iLO) » (page 44).

Les fonctions de supervision iLO ne sont pas toutes disponibles lorsque vous utilisez la fonction iLO Shared Network Port (Port réseau partagé iLO). Pour connaître les fonctions de supervision iLO prises en charge et celles qui ne le sont pas, reportez-vous à la section « Caractéristiques et limites du port de supervision partagé iLO » (page 45).

Configuration de la fonction iLO Shared Network Port (Port réseau partagé iLO)

La fonction iLO Shared Network Port (Port réseau partagé iLO) est uniquement disponible sur les serveurs équipés du matériel requis pour prendre cette fonction en charge. Outre le matériel, le microprogramme iLO et la carte réseau doivent également la prendre en charge.

Serveur ProLiant	Version minimale du microprogramme iLO
DL320G3	1.64
DL360 G4	1.60
DL360 G4	1.64
DL380 G4	1.60
DL385 G1	1.64
DL580 G3	1.64
ML370 G4	1.60
ML570 G3	1.64

Lorsque vous utilisez la fonction iLO Shared Network Port (Port réseau partagé iLO), le flashage du microprogramme iLO via l'interface XML prend environ 7 minutes.

Caractéristiques et limites du port de supervision partagé iLO

Le port réseau partagé iLO et celui de la carte réseau de supervision dédié iLO ne peuvent pas être utilisés en même temps pour superviser le serveur iLO. Ils ne peuvent pas fonctionner simultanément. L'activation de la carte réseau iLO dédiée désactive le port réseau partagé iLO, et inversement.

La désactivation du port réseau partagé ne désactive pas complètement la carte réseau système. Le trafic réseau régulier transite toujours par celle-ci. Lorsque le trafic réseau du port réseau partagé est désactivé, celui à destination ou en provenance de la carte iLO ne transite pas sur celle-ci par le port réseau partagé car ce dernier n'est plus partagé avec iLO.

La vitesse du port réseau partagé est relativement faible comparée à celle du port de supervision iLO dédié. Seul un nombre limité de fonctions iLO sont prises en charge via le port réseau partagé. Ces fonctions sont les suivantes :

- Command line interface (Interface de ligne de commande)
- Scripts XML
- Virtual Serial Port (Port série virtuel)
- Text based Remote Console (Console distante texte)
- SNMP protocol (Protocole SNMP)

En raison des performances relativement faibles du port réseau partagé, certaines opérations effectuées sur la connexion Virtual Serial Port (Port série virtuel) peuvent s'exécuter à des niveaux inférieurs à ceux optimaux. En particulier, les opérations d'affichage et d'édition impliquant l'affichage d'un grand nombre de données peuvent entraîner la perte de certains caractères. Cette perte affecte uniquement l'affichage, mais pas les données stockées sur le serveur.

L'interface Web iLO n'est pas prise en charge via le port réseau partagé, notamment :

- Console graphique distante
- Virtual Media

Lorsque le port réseau partagé est sélectionné, la carte iLO doit être configurée à l'aide de l'utilitaire iLO RBSU ou XML. La configuration à l'aide de RBSU requiert le redémarrage du système.

Activation de la fonction iLO Shared Network Port (Port réseau partagé iLO)

Par défaut, la fonction iLO Shared Network Port (Port réseau partagé iLO) est désactivée. Vous pouvez l'activer à l'aide des éléments suivants :

- Utilitaire iLO RBSU
- Interface Web iLO
- Scripts XML

Lorsque la fonction iLO Shared Network Port (Port réseau partagé iLO) est désactivée, la MTU (unité de transmission maximale) de iLO est de 320 octets, et ses paquets de requête DHCP sont divisés en plusieurs (à l'aide de la fragmentation IP). Cela peut poser un problème si votre serveur DHCP se trouve sur un autre sous-réseau et que votre agent de relais DHCP (généralement votre commutateur Ethernet Layer 3) ne prend pas en charge le transfert des trames DHCP fragmentées. Le serveur DHCP ne reçoit jamais la requête DHCP envoyée par iLO, et iLO ne peut pas obtenir d'adresse IP. Dans ce cas, vous devez configurer iLO avec une adresse IP statique.

Activation de la fonction iLO Shared Network Port (Port réseau partagé iLO) à l'aide de l'interface Web

1. Connectez le port 1 de la carte réseau iLO à un réseau LAN.
2. Ouvrez un navigateur et accédez au nom DNS ou l'adresse IP iLO.
3. Sélectionnez **Administration>Network Settings** (Administration>Paramètres réseau).
4. Dans la page Network Settings (Paramètres réseau), sélectionnez **Shared Network Port** (Port réseau Partagé). La fonction Shared Network (Réseau partagé) est uniquement disponible sur des serveurs pris en charge.
5. Cliquez sur **Apply** (Appliquer) au bas de la page.
6. Cliquez sur **Yes** (Oui) dans la boîte de dialogue d'avertissement, puis sur **OK**.

Après la réinitialisation de iLO, la fonction Shared Network Port (Port réseau partagé) est active. Tout trafic réseau à destination ou en provenance de iLO est acheminé via le port 1 de la carte réseau du système.

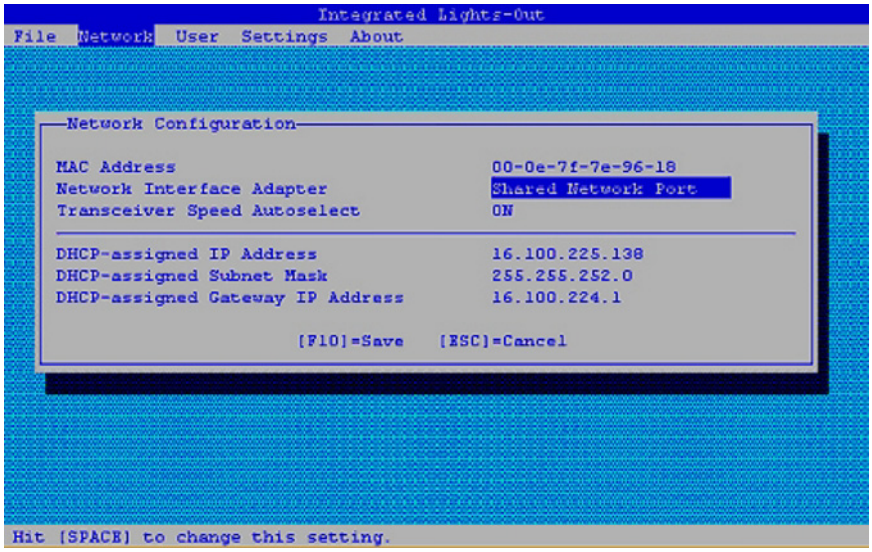
L'interface Web iLO n'est plus disponible après la réinitialisation de iLO. Pour pouvoir à nouveau y accéder, vous devez réactiver le port de supervision de la carte réseau dédiée de iLO. Pour plus d'informations, reportez-vous à la section « Réactivation du port de supervision iLO dédié » (page 47).

Le port de la carte réseau de supervision partagé et celui de la carte réseau iLO dédié ne peuvent pas être utilisés en même temps pour superviser le serveur. Ils ne peuvent pas être activés simultanément.

Activation de la fonction iLO Shared Network Port (Port réseau partagé iLO) à l'aide de l'utilitaire iLO RBSU

1. Connectez le port 1 de la carte réseau du serveur à un réseau LAN.
2. Lorsque vous y êtes invité pendant le test POST, appuyez sur la touche **F8** pour accéder à iLO RBSU.
3. Sélectionnez **Network>NIC>TCP/IP** (Réseau>Carte réseau>TCP/IP) et appuyez sur la touche **Entrée**.

4. Dans le menu Network Configuration (Configuration réseau), appuyez sur la barre d'espacement pour basculer le champ Network Interface Adapter (Adaptateur d'interface réseau) sur Shared Network Port (Port réseau partagé). L'option Shared Network Port (Port réseau partagé) est uniquement disponible sur des serveurs pris en charge.



5. Appuyez sur la touche **F10** pour enregistrer la configuration.
6. Sélectionnez **File>Exit** (Fichier>Quitter), puis appuyez sur la touche **Entrée**.

Après la réinitialisation de iLO, la fonction Shared Network Port (Port réseau partagé) est active. Tout trafic réseau à destination ou en provenance de iLO est acheminé via le port 1 de la carte réseau du système.

Réactivation du port de supervision iLO dédié

Vous devez utiliser l'utilitaire iLO RBSU ou les scripts XML (décrits dans le *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out* pour réactiver le port de supervision iLO dédié. Re-enabling iLO through RBSU requires that you reboot the system.

Pour réactiver le port de supervision dédié :

1. Connectez le port de supervision de la carte réseau dédiée iLO à un réseau LAN à partir duquel le serveur est géré.
2. Réamorcez le serveur.
3. Lorsque vous y êtes invité pendant le test POST, appuyez sur la touche **F8** pour accéder à iLO RBSU.
4. Sélectionnez **Network>NIC>TCP/IP** (Réseau>Carte réseau>TCP/IP) et appuyez sur la touche **Entrée**.
5. Dans le menu Network Configuration (Configuration réseau), appuyez sur la barre d'espacement pour basculer le champ Network Interface Adapter (Adaptateur d'interface réseau) sur **ON** (Activé).
6. Appuyez sur la touche **F10** pour enregistrer la configuration.
7. Sélectionnez **File>Exit** (Fichier>Quitter) et appuyez sur la touche **Entrée**.

Après la réinitialisation de iLO, le port de supervision de la carte réseau dédiée iLO est actif.

Shared Network Port VLAN (Port réseau partagé VLAN)

La fonction Shared Network Port VLAN (Port réseau partagé VLAN) est destinée aux clients qui souhaitent utiliser le port réseau partagé tout en séparant leur trafic réseau lié à l'administration de leur trafic réseau classique. Par exemple, vous pouvez faire en sorte que le trafic associé à l'administration pour tous les ports réseau partagés sur un réseau soit confiné à un même réseau VLAN. Le trafic réseau classique passant par les ports réseau partagés peut être limité à un même réseau LAN, réparti sur plusieurs réseaux LAN ou VLAN et ainsi de suite.

Pour communiquer avec iLO via un système client, le client doit se trouver sur le même réseau VLAN que les ports réseau partagés iLO et tous les commutateurs réseau entre le port réseau partagé iLO et le client doivent être compatibles IEEE 802.1q. Il est possible que les commutateurs gérés par IEEE 802.1q doivent être configurés afin d'activer la prise en charge du réseau VLAN.

Par défaut, la fonction iLO Shared Network Port VLAN (Port réseau partagé VLAN iLO) est désactivée. Vous pouvez l'activer et la configurer à l'aide des éléments suivants :

- Utilitaire iLO RBSU
- Interface Web iLO
- Scripts XML

La fonction VLAN est disponible uniquement sur les systèmes prenant en charge la carte réseau SNP. Tous les réseaux VLANs doivent être configurés avec un ID de VLAN. Il peut s'agir de n'importe quel nombre compris entre 1 et 4094. Seuls les utilisateurs dotés du privilège Configure iLO Settings (Configurer paramètres iLO) sont autorisés à activer ou désactiver la prise en charge de réseau VLAN et à configurer les ID de VLAN.

Activation et configuration de réseau à l'aide de l'interface iLO

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO). Cliquez sur **Administration**.

   IMPORTANT : seuls les utilisateurs dotés du privilège Configure iLO Settings (Configurer paramètres iLO) sont autorisés à modifier ces paramètres. Les autres peuvent uniquement consulter les paramètres attribués.

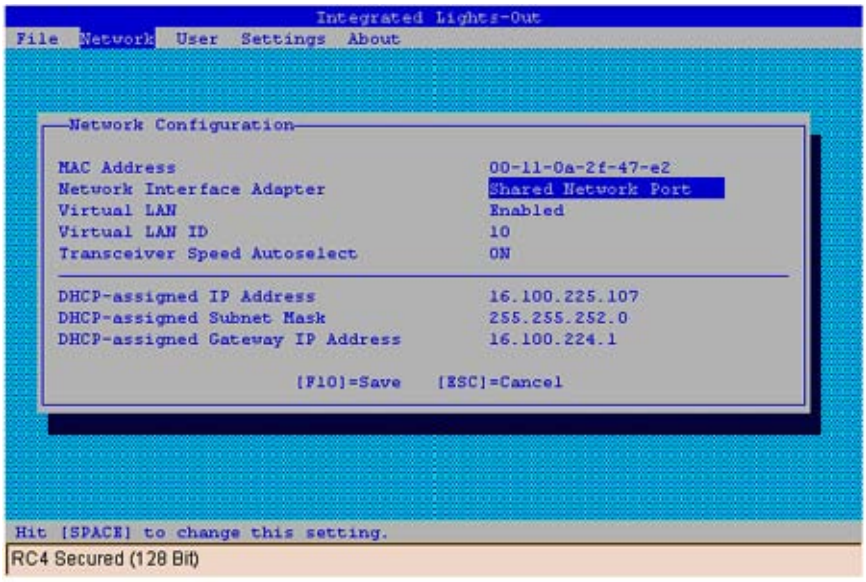
2. Cliquez sur **Network Settings** (Paramètres réseau).
3. Cliquez sur **Yes** (Oui) face à l'option Enable Virtual LAN (Activer le réseau VLAN virtuel) pour activer la fonction VLAN.

   Si l'option Shared Network Port (Port réseau partagé) n'est pas sélectionnée, les choix relatifs à la case d'option Enable Virtual LAN (Activer le réseau VLAN virtuel) et au champ VLAN ID (ID VLAN) sont désactivés et ne peuvent pas être configurés.
4. Saisissez un numéro entre 1 et 4094 dans le champ Virtual LAN ID (ID de réseau LAN virtuel).

   Si la fonction Virtual LAN (Réseau LAN virtuel) est désactivée, ce champ est désactivé et ne peut pas être configuré.
5. Cliquez sur **Apply** (Appliquer). iLO se réinitialise avec les paramètres d'ID de réseau LAN en cours.

Activation et configuration du réseau VLAN à l'aide de l'utilitaire de configuration basé sur la ROM (RBSU)

1. Redémarrez le serveur et appuyez sur **F8**. Lorsque vous y êtes invité, choisissez le RBSU iLO.
2. Sélectionnez **Network>NIC>TCP/IP** (Réseau>Carte réseau>TCP/IP), puis appuyez sur la touche **Entrée**.
3. Utilisez la barre d'espace pour sélectionner **Shared Network Port** (Port réseau partagé) dans le champ Network Interface Adapter (Adaptateur d'interface réseau).
4. Allez dans le champ Virtual LAN (Réseau LAN virtuel) et utilisez la barre d'espace pour sélectionner **Enabled** (Activé). Un champ d'ID de réseau VLAN définissable par l'utilisateur s'affiche.
5. Allez dans le champ Virtual LAN ID (ID de réseau LAN virtuel) et saisissez n'importe quel nombre entre 1 et 4094.



Activation et configuration du réseau VLAN à l'aide de XML

Vous pouvez activer ou désactiver la prise en charge de réseau VLAN via la création de scripts XML à l'aide de RIBCL. Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.

Configuration des serveurs ProLiant BL p-Class

Vous pouvez accéder aux serveurs ProLiant BL p-Class et les configurer à partir :

- du port de diagnostic iLO à l'avant du serveur,
- de la section « Installation basée sur le navigateur » (page 16) qui permet de configurer initialement le système via le port de diagnostic iLO,
- de l'assistant d'installation détaillé via l'installation HP BladeSystem

Sur les serveurs lame p-Class installés dans des boîtiers dotés de fonds de panier de supervision mis à jour prenant en charge les serveurs lame haute densité, iLO permet la configuration IP statique initiale du boîtier. La configuration initiale du compartiment 1 permet d'affecter des adresses IP prédéfinies à toutes les cartes iLO installées ultérieurement dans le boîtier. Cette fonction est prise en charge dans les versions iLO 1.55 ou ultérieures.

Spécifications relatives aux utilisateurs de serveur ProLiant BL p-Class

- Les utilisateurs doivent disposer du privilège Configure iLO Settings (Configurer paramètres iLO).
- Une connexion réseau à iLO doit être disponible et fonctionner correctement.

Configuration IP statique

La configuration IP statique, mise en œuvre à l'aide des nouveaux paramètres de configuration IP statique disponibles dans l'onglet BL p-Class, facilite le déploiement initial d'un boîtier complet, ou le déploiement ultérieur des lames d'un boîtier existant. Même si la méthode préconisée pour l'affectation d'adresses IP à chaque iLO de chacun des serveurs lame consiste à utiliser DHCP et DNS, ces protocoles ne sont pas toujours disponibles sur des réseaux autres que de production.

La configuration IP statique automatise la première étape du déploiement de serveur en lame BL p-Class, en activant le processeur de supervision iLO dans chaque connecteur de serveur afin d'obtenir une adresse IP prédéfinie sans utiliser DHCP. iLO est immédiatement accessible pour le déploiement de serveur à l'aide de Virtual Media (Support virtuel) et d'autres fonctions d'administration à distance.

La configuration IP statique utilise le mode d'adressage Static IP Bay Configuration (Configuration IP statique) vous permettant d'affecter des adresses IP à chaque iLO selon l'emplacement des connecteurs dans le boîtier de serveur respectif. En affectant un jeu d'adresses IP au boîtier, vous bénéficiez des avantages d'une configuration IP statique, sans qu'il soit nécessaire de configurer localement chaque iLO.

La configuration IP statique de iLO offre les avantages suivants :

- Pas de coûts associés à une infrastructure DHCP assurant la prise en charge de l'environnement de lames de serveur.
- Configuration plus aisée avec génération automatique des adresses iLO pour tout ou partie des compartiments sélectionnés.

Configuration d'un boîtier de serveur lame ProLiant BL p-Class

Pour configurer un boîtier de serveur lame ProLiant BL p-Class à l'aide de l'adressage IP statique :

1. Installez une lame de serveur dans le compartiment n°1 du boîtier BL p-Class. Il n'est pas nécessaire de configurer la lame de serveur ou d'installer un système d'exploitation. La lame de serveur doit être configurée avant d'en installer d'autres dans le boîtier.
2. Connectez un client au port iLO du panneau avant du serveur en lame à l'aide du câble d'E/S local. Le câble d'E/S se connecte au port d'E/S situé sur la face avant du serveur lame. Cette connexion active l'adresse IP statique 192.168.1.1 pour l'interface Web iLO.
3. Configurez le paramètre de boîtier. À l'aide de l'interface Web iLO, sélectionnez l'onglet BL p-Class pour accéder aux paramètres IP statique du boîtier. L'onglet BL p-Class fournit une interface utilisateur permettant de configurer les adresses IP statiques au niveau du boîtier.

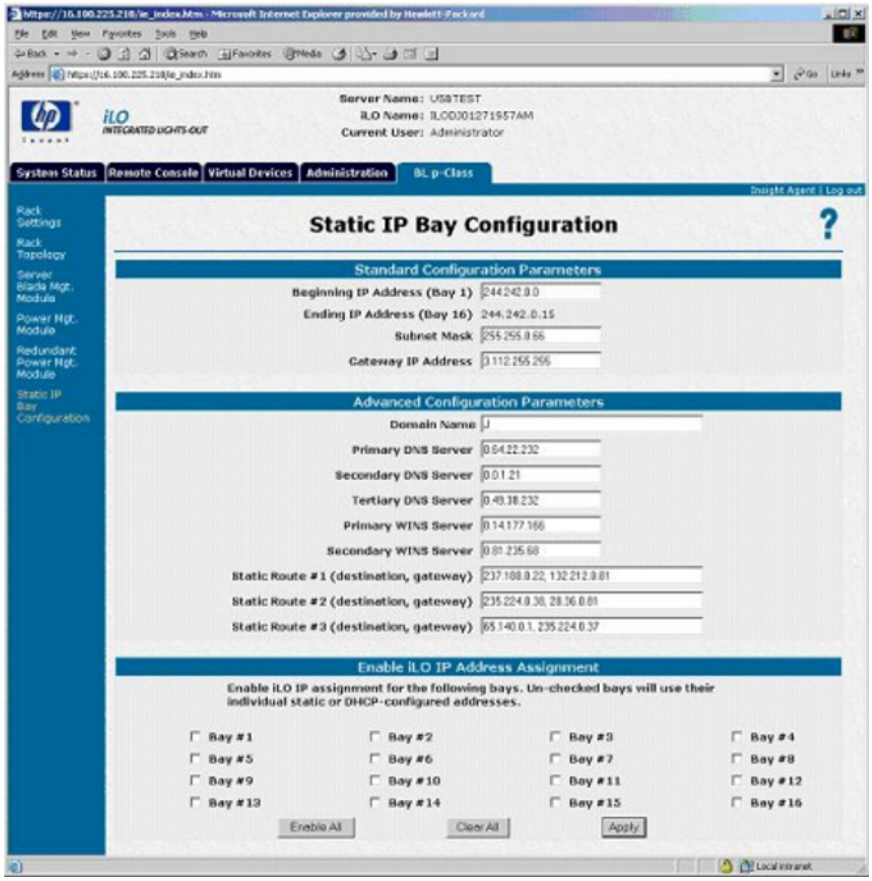
4. Sélectionnez une adresse de démarrage raisonnable, le ou les derniers chiffres correspondant au numéro de compartiment de chaque serveur lame (exemple : 192.168.100.1 à 192.168.100.16) afin de concevoir un système de numérotation facile à retenir.
5. Réinitialisez le compartiment n°1, si nécessaire. Vous devez réinitialiser le serveur lame du compartiment n°1 uniquement si vous prévoyez d'utiliser une adresse Static IP Bay Configuration (Configuration IP statique) en marquant le masque d'activation du compartiment n°1. Avant de réinitialiser le serveur lame, naviguez vers la page Network Settings (Paramètres réseau), sélectionnez **Enable Static IP Settings** (Activer les paramètres de configuration IP statique), puis cliquez sur **Apply** (Appliquer) pour forcer la réinitialisation du serveur lame et utiliser la nouvelle adresse IP statique de boîtier affectée.

Si vous déployez plusieurs boîtiers en même temps, vous pouvez facilement répéter ce processus en déplaçant un serveur lame unique dans le compartiment n°1 de chaque boîtier afin d'effectuer la configuration.

Définition des paramètres de configuration IP statique

Les paramètres de configuration IP statique disponibles dans l'onglet BL p-Class vous permettent de configurer et de déployer le serveur lame.

La case à cocher Enable Static IP Bay Configuration Settings (Activer les paramètres de configuration IP statique), disponible dans l'onglet Network Settings (Paramètres réseau) (non représenté), permet d'activer ou de désactiver Static IP Bay Configuration (Configuration IP statique). La nouvelle option Enable Static IP Bay Configuration Settings (Activer les paramètres de configuration IP statique) est uniquement disponible sur les serveurs lame. Lorsque cette option est activée, tous les champs, à l'exception de iLO Subsystem Name (Nom du sous-système iLO), sont désactivés. Les options Static IP Bay Configuration (Configuration IP statique) et DHCP ne peuvent pas être activées en même temps. Leur désactivation indique à iLO d'utiliser une adresse IP définie par l'utilisateur. L'option Enable Static IP Bay Configuration Settings (Activer les paramètres de configuration IP statique) reste désactivée si l'infrastructure ne prend pas en charge l'option Static IP Bay Configuration (Configuration IP statique).



Paramètres de configuration standard des serveurs ProLiant BL p-Class

Beginning IP Address (Bay 1) (Adresse IP de début - Compartiment 1) : affecte l'adresse IP de début. Toutes les adresses IP doivent être valides.

Ending IP Address (Bay 16) (Adresse IP de fin - Compartiment 16) : affecte l'adresse IP de fin. Toutes les adresses IP doivent être valides.

Subnet Mask (Masque de sous-réseau) : affecte le masque de sous-réseau à la passerelle par défaut. Ce champ peut être renseigné si l'option Static IP Bay Configuration (Configuration IP statique) ou DHCP est activée. La plage d'adresses IP doit être conforme au masque de sous-réseau.

Gateway IP Address (Adresse IP de passerelle) : affecte l'adresse IP du routeur de réseau qui relie le sous-réseau Remote Insight à un autre sous-réseau où réside la station de supervision. Ce champ peut être renseigné si l'option Static IP Bay Configuration (Configuration IP statique) ou DHCP est activée.

Paramètres de configuration avancés des serveurs ProLiant BL p-Class

Domain Name (Nom de domaine) : vous permet d'affecter le nom du domaine dans lequel iLO va prendre part.

Primary DNS Server (Serveur DNS primaire) : affecte une adresse IP de serveur DNS unique sur votre réseau.

Secondary DNS Server (Serveur DNS secondaire) : affecte une adresse IP de serveur DNS unique sur votre réseau.

Tertiary DNS Server (Serveur DNS tertiaire) : affecte une adresse IP de serveur DNS unique sur votre réseau.

Primary WINS Server (Serveur WINS primaire) : affecte une adresse de serveur WINS unique sur votre réseau.

Secondary WINS Server (Serveur WINS secondaire) : affecte une adresse de serveur WINS unique sur votre réseau.

Static Route #1, #2, and #3 (destination gateway) (Route statique n°1, n°2 et n°3 - passerelle de destination) : affecte l'adresse IP appropriée à la passerelle et à la destination de route statique sur votre réseau (les valeurs IP par défaut sont 0.0.0.0 et 0.0.0.0, où la première adresse IP correspond à celle de la destination, et la deuxième à celle de la passerelle).

Activation de l'affectation de l'adresse IP iLO

Les cases à cocher bay #1 (compartiment n°1) à bay #16 (compartiment n°16) permettent de sélectionner les serveurs lame BL p-Class à configurer. Vous pouvez sélectionner Enable All (Activer tout), Clear All (Effacer tout) ou Apply (Appliquer).

Installation HP BladeSystem

L'assistant d'installation HP BladeSystem fournit des instructions détaillées qui facilitent l'installation d'un serveur lame unique sans utiliser les protocoles DHCP ni PXE. La page d'installation HP BladeSystem se lance après authentification sur iLO à partir du port frontal.

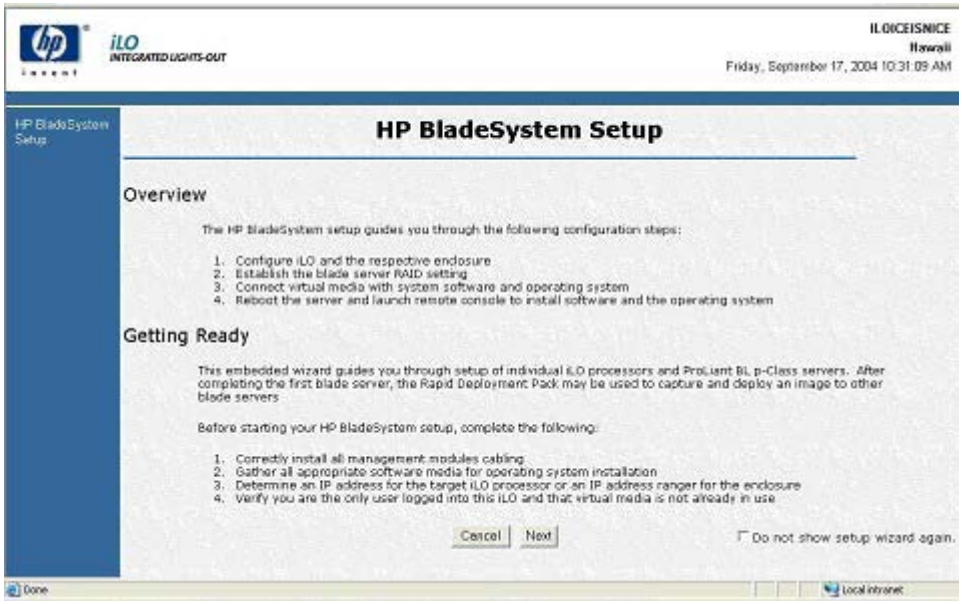
Le serveur en lame doit être correctement connecté pour assurer la connectivité iLO. Connectez le serveur lame via le port E/S du serveur lame, pendant que le serveur lame est dans le rack. Cette méthode nécessite la connexion du câble d'E/S local au port d'E/S et à un PC client. À l'aide de l'adresse IP fixe inscrite sur l'étiquette du câble d'E/S et des informations d'accès initial figurant à l'avant du serveur en lame, vous pouvez accéder au serveur en lame via la carte iLO et son interface de navigateur Web standard.

L'accès s'effectue via n'importe quel serveur lame. Par contre, lorsque la configuration IP statique est utilisée pour définir les paramètres réseau iLO, l'accès se fait au niveau du premier serveur du boîtier.

La première page de l'assistant se lance automatiquement si :

- Le serveur est nouveau et que vous vous êtes connecté à la carte iLO à partir du port frontal ;
- Vous n'avez pas fermé l'assistant en sélectionnant **Finish** (Terminer) sur la dernière page et si vous n'avez pas choisi l'option **Do not show setup wizard again** (Ne plus afficher l'assistant d'installation) et cliqué sur **Cancel** (Annuler) sur la première page ;

- Vous avez effacé les paramètres iLO NVRAM ou si vous avez réinitialisé les paramètres par défaut iLO.



Cliquez sur **Cancel** (Annuler) pour fermer l'assistant d'installation automatique. Cliquez sur **Next** (Suivant) pour configurer votre serveur lame. Suivez les instruction de l'assistant d'installation pour :

1. la configuration iLO
2. la vérification serveur RAID
3. la connexion à l'écran Virtual Media (support virtuel)
4. l'installation logicielle

Écran de configuration iLO

Cet écran vous permet de :

- Changer le mot de passe administrateur. HP vous conseille de remplacer le mot de passe par défaut.
- Changer les paramètres de configuration réseau. Les paramètres par défaut sont :
  - Enable DHCP (Activer DHCP) : Yes (oui)
  - Enable Static IP Bay Configuration (Activer la configuration IP statique) : No (non)
- d'activer Static IP Bay configuration (Configuration IP statique) pour préconfigurer l'adresse statique des autres processeurs iLO dans le boîtier, lors d'une connexion au serveur en lame dans le connecteur du boîtier 1.

Par défaut, la carte iLO mise à jour obtient son adresse IP via le protocole DHCP. Les autres processeurs iLO du boîtier doivent être configurés séparément. Si ces paramètres ne sont pas modifiés, cliquez sur **Next** (Suivant) pour afficher la page suivante de l'assistant d'installation. Si l'un de ces paramètres est modifié, iLO redémarre pour valider les paramètres mis à jour.

Les autres combinaisons de configuration sont les suivantes :

- Enable DHCP (Activer DHCP) : Yes (oui) et Enable Static IP Bay Configuration (Activer la configuration IP statique) : Yes (oui)

  Cette configuration permet à la carte iLO configurée d'obtenir son adresse IP via DHCP. La page Static IP Bay Configuration (Configuration IP statique) qui s'affiche en cliquant sur **Next** (Suivant), permet d'indiquer les adresses IP des autres cartes iLO du boîtier. Après avoir cliqué sur **Next** (Suivant), vous devez vérifier si vous souhaitez utiliser le protocole DHCP pour l'adresse IP de cette carte iLO.

- Enable DHCP (Activer DHCP) : No (non) et Enable Static IP Bay Configuration (Activer la configuration IP statique) : Yes (oui)

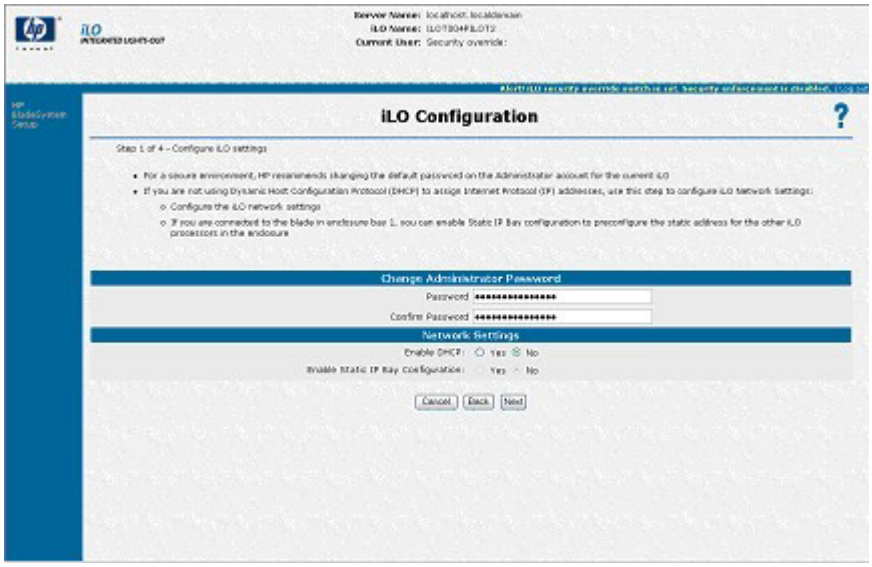
  Cette configuration permet à la carte iLO configurée de définir son adresse IP selon les paramètres indiqués à la page Static IP Bay Configuration (Configuration IP statique). Cliquez sur **Next** (Suivant) pour afficher la page Static IP Bay Configuration (Configuration IP statique).

- Enable DHCP (Activer DHCP) : No (non) et Enable Static IP Bay Configuration (Activer la configuration IP statique) : Non (non)

  Grâce à cette configuration, la carte iLO configurée peut définir son adresse IP selon les paramètres indiqués à la page Network Settings (Paramètres réseau). Cliquez sur **Next** (Suivant) pour afficher la page Network Settings (Paramètres réseau).

Pour enregistrer des modifications sur le réseau, vous devez disposer du privilège de configuration iLO.

Cliquez sur **Next** (Suivant) pour enregistrer les modifications et continuer.



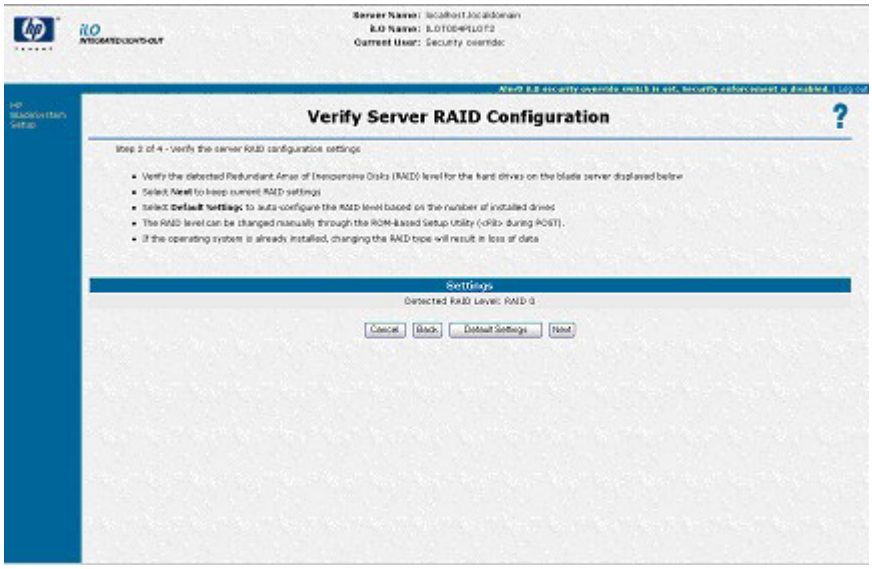
Vérification de l'écran de configuration du serveur RAID

Cette étape de l'assistant d'installation permet de vérifier et d'accepter les paramètres de configuration du serveur RAID.

- Vérifiez le niveau RAID détecté pour les disques durs sur le serveur en lame affiché sur la page Web.
- Cliquez sur **Next** (Suivant) pour conserver les paramètres RAID existants.

- Cliquez sur **Default Setting** (Paramètres par défaut) pour configurer automatiquement le niveau RAID en fonction du nombre de lecteurs installés. Le système vous demande de confirmer la réinitialisation du niveau RAID car cette opération risque d'entraîner une perte de données. Une mise sous tension ou un redémarrage du serveur est nécessaire pour réinitialiser le niveau RAID. Une page signalant cette opération apparaît. La page est actualisée automatiquement toutes les 10 secondes. Après le redémarrage du serveur, la page suivante de l'assistant d'installation s'affiche à nouveau. Si une erreur est détectée pendant l'opération de réinitialisation du niveau RAID, la page de configuration réapparaît et indique l'erreur rencontrée. Il y a plus de chances qu'une erreur se produise pendant l'auto-test de mise sous tension (POST) du serveur. Si c'est le cas, quittez tous les programmes RBSU ouverts, attendez la fin de l'auto-test puis relancez l'opération.
- Vous pouvez modifier le niveau RAID manuellement au niveau du RBSU.

Si le système d'exploitation est déjà installé, la modification du niveau RAID risque d'entraîner une perte de données.

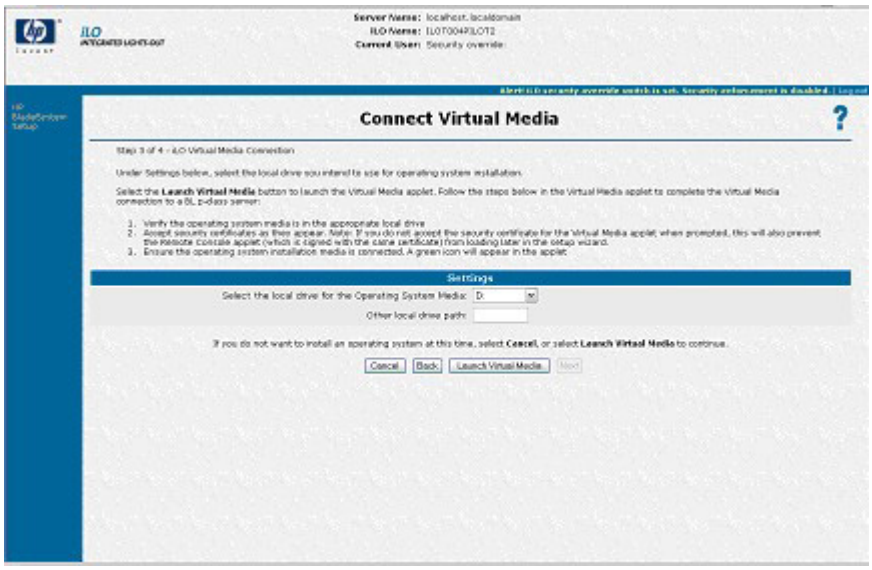


Connexion à l'écran Virtual Media (Support virtuel)

Cette étape de l'assistant d'installation permet de vérifier et d'accepter le lecteur que vous allez utiliser au cours de l'installation du système d'exploitation. Sous Settings (paramètres), sélectionnez le lecteur local et le type de support que vous souhaitez utiliser pendant l'installation du système d'exploitation. Cliquez sur **Launch Virtual Media** (Lancer le support virtuel) pour lancer l'applet Virtual Media.

- Assurez-vous que le support du système d'exploitation est connecté. Dans l'applet Virtual Media, une icône verte apparaît en regard du support sélectionné.
- Vérifiez que le support du système d'exploitation est dans le lecteur approprié.
- Acceptez les certificats de sécurité, dès qu'ils s'affichent.

Après avoir fait votre sélection, cliquez sur **Next** (Suivant) pour enregistrer vos paramètres et continuer. L'applet Virtual Media apparaît. Si l'applet est disponible, vous pouvez changer le lecteur sélectionné ou choisir d'autres options non listées dans la page de l'assistant d'installation.

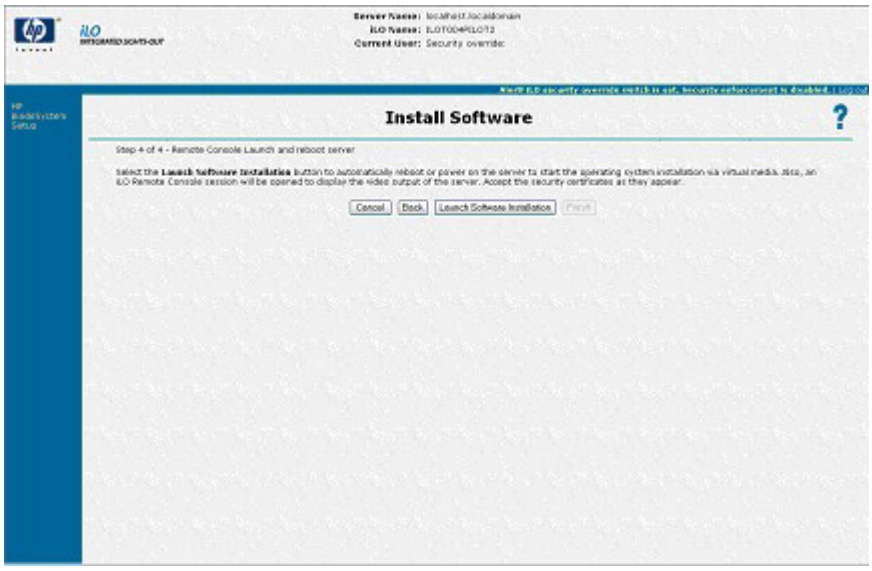


Écran d'installation logicielle

Cette étape de l'assistant d'installation permet de lancer la console distante et d'installer le système d'exploitation. Pour démarrer le processus d'installation du système d'exploitation :

- Cliquez sur **Launch Software Installation** (Lancer l'installation du logiciel) pour lancer la console distante. Automatiquement, iLO met sous tension ou redémarre le serveur pour lancer l'installation du système d'exploitation via le support virtuel sélectionné précédemment.
- Acceptez les certificats de sécurité, dès qu'ils s'affichent.

Cliquez sur **Finish** (Terminer) pour terminer le processus d'installation.



Sécurité iLO

Cette section traite des rubriques suivantes :

Fonctionnalités de sécurité

La carte iLO fournit les fonctionnalités de sécurité suivantes :

- Ports TCP/IP définis par l'utilisateur (« Paramètres réseau », page 28)
- Actions utilisateurs consignées dans le journal des événements de la carte iLO
- Temporisations progressives pour tentatives de connexion infructueuses (« Sécurité de la connexion », page 64)
- Prise en charge de certificats X.509 signés par l'autorité de certification (page 59)
- Prise en charge de paramètres RBSU (« Sécurisation de RBSU », page 61)
- Prise en charge de l'authentification et de l'autorisation des services d'annuaire basés sur LDAP en option (requiert iLO Advanced)
- Communication codée utilisant les protocoles SSL et SSH.

Consignes générales de sécurité

Cette section présente les principes généraux applicables à la carte iLO en matière de sécurité :

- Pour une sécurité maximale, installez la carte iLO sur un réseau de supervision distinct.
- La carte iLO ne doit pas être directement connectée à Internet.
- Utilisez un navigateur possédant une capacité de codage de 128 bits.

Principes relatifs aux mots de passe

La liste suivante indique les principes recommandés pour le choix des mots de passe.

- Ne jamais conserver de trace écrite ou enregistrée des mots de passe.
- Ne jamais partager les mots de passe avec d'autres utilisateurs.
- Ne pas utiliser des mots courants du dictionnaire ou des mots faciles à deviner tels que le nom de votre entreprise, le nom d'un produit, le nom de l'utilisateur ou son identifiant.

- Les mots de passe doivent satisfaire au moins trois des quatre caractéristiques suivantes :
  - au moins un caractère numérique ;
  - au moins un caractère spécial ;
  - au moins un caractère minuscule ;
  - au moins un caractère majuscule.

Les mots de passe délivrés pour un ID utilisateur temporaire, une réinitialisation du mot de passe ou un ID utilisateur verrouillé doivent également respecter ces normes. Chaque mot de passe doit avoir une longueur comprise entre 0 et 39 caractères. La longueur minimale par défaut est de 8 caractères. HP vous déconseille de définir la longueur minimale du mot de passe sur moins de 8 caractères, sauf si vous disposez d'un réseau de supervision sécurisé physiquement qui ne s'étend pas au-delà du centre de données sécurisé.

Certificats

Par défaut, iLO crée un certificat « à signature automatique » utilisable dans les connexions SSL. Ce certificat permet à la carte iLO de fonctionner sans autre étape de configuration. Les fonctions de sécurité iLO peuvent être étendues par l'importation d'un certificat validé.

- **Create Certificate Request** (Créer demande de certificat) : iLO peut créer une demande de certificat (au format PKCS#10) qui peut être envoyée à une autorité de certification. Cette demande de certificat est codée en base64. Une autorité de certification traite cette demande et envoie une réponse (certificat X.509) qui peut être importée dans iLO.

  La demande de certificat contient une paire de clés publique/privée permettant de valider les communications entre le navigateur du client et la carte iLO. La demande de certificat générée étant conservée en mémoire jusqu'à la génération d'une nouvelle, l'importation d'un certificat par ce processus ou la réinitialisation de iLO, vous pouvez donc générer la demande et la copier dans le presse-papiers du client, permettre au site Web iLO d'extraire le certificat, puis retourner afin d'importer le certificat.

  Lorsque vous soumettez la demande à l'autorité de certification, assurez-vous :

  - D'utiliser le nom iLO répertorié dans l'écran System Status (État du système) en tant qu'URL du serveur.
  - De demander que le certificat soit généré au format RAW.
  - D'inclure les lignes de certificat Begin et End.

  Chaque fois que vous cliquez sur le bouton **Create Certificate Request** (Créer demande de certificat), une nouvelle demande de certificat est générée, même si le nom de la carte iLO est le même.

- **Import Certificate** (Importer certificat) : si vous revenez sur la page Create Certificate Request (Créer demande de certificat) avec un certificat à importer, cliquez sur le bouton **Import Certificate** (Importer certificat) pour accéder directement à l'écran Certificate Import (Importation de certificat) sans générer de nouvelle demande. Ceci est important dans la mesure où un certificat donné ne fonctionne qu'avec les clés contenues dans la demande de certificat à partir de laquelle il a été généré. Si la carte iLO a été réinitialisée ou qu'une autre demande de certificat a été générée depuis que la demande utilisée pour demander le certificat a été émise, une nouvelle demande doit être générée et un nouveau certificat obtenu auprès de l'autorité de certification.

Vous pouvez créer une demande de certificat ou importer un certificat existant à l'aide des commandes RIBCL XML. Ces commandes permettent de générer le script et le déploiement automatique de certificat des serveurs iLO au lieu de déployer manuellement les certificats via l'interface Web. Pour en savoir plus, reportez-vous à « CERTIFICATE_SIGNING_REQUEST » et à « IMPORT_CERTIFICATE » dans la section « Langage de commande de la carte Remote Insight ».

Les commandes CERTIFICATE_SIGNING_REQUEST et IMPORT_CERTIFICATE ne peuvent pas être utilisées avec l'utilitaire CPQLOCFG standard. Néanmoins, vous pouvez utiliser la version PERL de CPQLOCFG avec ces commandes.

Administration du commutateur de neutralisation de la sécurité iLO

Le commutateur de neutralisation de la sécurité iLO permet à l'administrateur d'accéder intégralement au processeur iLO. Cela peut être nécessaire dans les cas suivants :

- La carte iLO doit être réactivée après avoir été désactivée ;
- Tous les comptes utilisateur dotés du privilège Administer User Accounts (Administrer comptes utilisateur) ont été verrouillés ;
- Une configuration erronée empêche la carte iLO d'apparaître sur le réseau et l'utilitaire RBSU a été désactivé ;
- Le bloc d'initialisation doit être flashé.

L'utilisation du commutateur de neutralisation de la sécurité a les conséquences suivantes :

- Tous les contrôles d'autorisation de sécurité sont désactivés lorsque le commutateur est activé ;
- L'utilitaire iLO RBSU s'exécute en cas de réinitialisation du serveur hôte ;
- La carte iLO n'est pas désactivée et peut apparaître sur le réseau comme étant configurée ;
- Si la carte iLO est désactivée pendant que le commutateur de neutralisation est actif, elle n'est plus en mesure de déconnecter l'utilisateur ni de terminer le processus et cela jusqu'au prochain cycle de mise hors/sous tension du serveur ;
- Le ROMPaq Option iLO est en mesure de reprogrammer la ROM de la carte iLO, même si le microprogramme iLO n'est pas en cours d'exécution ;
- Le bloc d'initialisation est exposé à la programmation.

Un message d'avertissement s'affiche sur les pages du navigateur iLO, indiquant que le commutateur de neutralisation de la sécurité iLO est en cours d'utilisation. Une entrée est ajoutée au journal iLO pour enregistrer l'utilisation de ce commutateur. Une alerte SNMP peut également être envoyée après activation ou désactivation de celui-ci.

L'activation du commutateur de neutralisation de la sécurité iLO vous permet également de flasher le bloc d'initialisation iLO. HP ne prévoit pas que vous aurez besoin de mettre à jour le bloc d'initialisation iLO. Si cela s'avère nécessaire, vous devez intervenir physiquement au niveau du serveur pour reprogrammer le bloc d'initialisation et réinitialiser la carte iLO. Le bloc d'initialisation reste alors exposé jusqu'à la réinitialisation de la carte iLO. Pour une sécurité optimale, HP vous recommande de déconnecter la carte iLO du réseau tant que la réinitialisation n'est pas terminée. Le commutateur de neutralisation de la sécurité iLO se trouve à l'intérieur du serveur. Vous ne pouvez dès lors pas y accéder sans ouvrir le boîtier du serveur.

Pour paramétrer le commutateur de neutralisation de la sécurité iLO :

1. Mettez le serveur hors tension.
2. Paramétrez le commutateur.
3. Mettez le serveur sous tension.

Inversez la procédure pour désactiver le commutateur de neutralisation de la sécurité iLO.

Selon le serveur utilisé, le commutateur de neutralisation de la sécurité iLO peut être un simple cavalier ou une position spécifique sur un panneau de commutateurs à positions multiples. Pour le localiser et y accéder, reportez-vous à la documentation de votre serveur. Vous pouvez également utiliser les diagrammes figurant sur le panneau d'accès du serveur.

Sécurisation de RBSU

L'utilitaire iLO RBSU permet aux utilisateurs d'afficher et de modifier la configuration de la carte iLO. Les paramètres d'accès à RBSU sont configurables à l'aide de l'utilitaire RBSU, du navigateur, des scripts RIBCL et du commutateur de neutralisation de la sécurité iLO. RBSU comporte trois niveaux de sécurité :

- RBSU Disabled (RBSU désactivé) (niveau maximal)

  Si iLO RBSU est désactivé, l'accès utilisateur n'est pas autorisé. Cela empêche toute modification à l'aide de l'interface RBSU.

- RBSU Login Required (Connexion RBSU requise) (niveau élevé)

  Si la connexion RBSU est requise, les menus de configuration actifs sont contrôlés par les droits d'accès de l'utilisateur authentifié.

- RBSU Login Not Required (Connexion RBSU non requise) (niveau par défaut)

  Les utilisateurs qui peuvent accéder à l'hôte pendant l'auto-test de mise sous tension (POST) peuvent accéder à l'utilitaire iLO RBSU pour afficher et modifier les paramètres de configuration. Ce paramètre est valide si l'accès à l'hôte est contrôlé.

Encryption (Codage)

La carte iLO assure une supervision distante fortement sécurisée dans les environnements informatiques décentralisés, grâce à la norme de codage SSL de 128 bits des données HTTP transitant sur le réseau. Le codage SSL assure la sécurisation des données HTTP pendant leur transmission sur le réseau.

Les données de la console distante sont protégées grâce à un codage bidirectionnel de 128 bits RC4.

Remote Console Computer Lock (Verrou d'ordinateur de console distante)

La fonction Remote Console Computer Lock améliore la sécurité d'un serveur supervisé par iLO en verrouillant automatiquement un système d'exploitation ou en déconnectant un utilisateur à la fin d'une session de console distante ou encore lors de la perte d'une liaison réseau à iLO. À la différence de la console distante, cette fonction est standard et ne requiert pas de licence supplémentaire. Il en résulte que, si vous ouvrez une fenêtre de session de console distant et que cette fonction est configurée, elle verrouille le système d'exploitation lorsque la fenêtre est fermée, même si des licences de fonctions supplémentaires ne sont pas installées.

Vous pouvez visualiser et configurer les paramètres Remote Console Computer Lock via les onglets Administration et Remote Console dans l'interface iLO. La fonction Remote Console Computer Lock est désactivée par défaut.

Pour modifier les paramètres Remote Console Computer Lock :

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO).
2. Sélectionnez **Computer Lock Settings** (Paramètres de verrou d'ordinateur). L'écran correspondant s'affiche.

3. Modifiez les paramètres suivant les besoins.
   - Windows : Utilisez cette option pour configurer iLO afin de verrouiller un serveur supervisé exécuté sous un système d'exploitation Windows®. Le serveur affiche automatiquement la boîte de dialogue Computer Locked (Ordinateur verrouillé) lorsqu'une session de console distante est terminée ou que la liaison réseau à iLO est perdue.
   - Custom (Personnalisé) : Utilisez cette option pour configurer iLO afin d'utiliser une clé personnalisée pour verrouiller un serveur supervisé ou pour déconnecter un utilisateur sur ce serveur. Vous pouvez sélectionner jusqu'à cinq clés dans la liste. La séquence de clés sélectionnées est automatiquement envoyée au système d'exploitation du serveur lorsqu'une session de console distante est terminée ou que la liaison réseau à iLO est perdue.
   - Disabled (Désactivé) : Utilisez cette option pour désactiver la fonction Remote Console Computer Lock. La fin d'une session de console distante ou la perte d'une liaison réseau à iLO ne verrouille pas le serveur supervisé.

   Vous pouvez créer une séquence de clés Remote Console Computer Lock en utilisant les clés répertoriées dans le tableau suivant .

ESC	F4	1	e
L_ALT	F5	2	f
R_ALT	F6	3	g
L_SHIFT (L_MAJ)	F7	4	h
R_SHIFT (R_MAJ)	F8	5	i
L-CTRL	F9	6	j
R_CTRL	F10	7	k
L_GUI	F11	8	l
R_GUI	F12	9	m
INS (INSER)	" " (Espace)	:	n
DEL (SUPPR)	!	;	o
HOME (ORIGINE)	"	<	p
END (Fin)	#	=	q
PG_UP	$	>	r
PG_DN	%	?	s

ENTER (ENTRÉE)	&	@	t
TAB	`	[	u
BREAK	(	\	v
BACKSPACE (RETOUR ARRIÈRE)	)	]	w
NUM PLUS	*	^	x
NUM MINUS	+	_	y
SCRL LCK (ARRÊT DÉFIL)	,	`	z
SYS RQ	-	a	{
F1	.	b	}
F2	/	c	|
F3	0	d	~

4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Cette fonction peut également être configurée en utilisant des scripts ou des lignes de commande. Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out.*

Comptes utilisateur

La carte iLO prend en charge la configuration de 12 comptes utilisateur locaux maximum. Chacun de ces comptes peut être géré par l'intermédiaire des éléments suivants :

- Privilèges
- Paramètres de sécurité généraux
- Sécurité de la connexion

Une alternative aux comptes utilisateur iLO locaux consiste à intégrer l'authentification utilisateur iLO dans des services d'annuaire. Cette configuration autorise l'intégration d'un nombre quasi illimité d'utilisateurs et s'adapte aisément au nombre de périphériques Lights-Out d'une entreprise. En outre, l'annuaire fournit un point central d'administration aux utilisateurs et périphériques Lights-Out et peut faire appliquer une stratégie de mot de passe plus stricte. iLO vous permet d'intégrer des utilisateurs locaux, d'annuaire ou les deux.

Privilèges

La carte iLO permet à l'administrateur de contrôler l'accès des comptes utilisateur aux fonctions iLO par l'intermédiaire de privilèges. Lorsqu'un utilisateur essaie d'utiliser une fonction, le système iLO vérifie s'il dispose du privilège requis avant de l'autoriser à se servir de la fonction.

Toutes les fonctions disponibles via la carte iLO sont contrôlables via des privilèges, y compris Administer User Accounts (Administrer comptes utilisateur), Remote Console Access (Accès console distante), Virtual Power and Reset (Alimentation et réinitialisation virtuelles), Virtual Media (Support virtuel) et Configure iLO Settings. Vous pouvez configurer les privilèges pour chaque utilisateur sur la page User Administration (Administration des utilisateurs) de l'onglet Administration.

Sécurité de la connexion

La carte iLO propose plusieurs fonctions pour assurer la sécurité de la connexion. Après l'échec d'une tentative initiale d'ouverture de session, la carte iLO impose un temps d'attente de cinq secondes. Après l'échec de la deuxième tentative, la carte iLO impose un temps d'attente de dix secondes. Après l'échec de la troisième tentative, la carte iLO impose un délai de 60 secondes. En cas d'échec des tentatives d'ouverture de session suivantes, les délais d'attente suivent le même cycle. Une page d'information s'affiche pendant chaque délai d'attente. Le processus se poursuit jusqu'à l'ouverture d'une session valide. Cette fonction contribue à une défense contre des attaques éventuelles à l'encontre du port de connexion du navigateur.

La carte iLO enregistre par ailleurs une entrée de journal détaillée pour les tentatives de connexion non abouties imposant un délai de 60 secondes.

Paramètres de sécurité généraux

Les paramètres de sécurité généraux permettent à l'administrateur de contrôler l'accès aux fonctions ou de contrôler individuellement les actions spécifiques des fonctions activées au niveau général. Vous pouvez par exemple contrôler l'accès à l'utilitaire iLO RBSU, activer ou désactiver la fonctionnalité Lights-Out, paramétrer le délai d'attente de la console distante ainsi que les ports SSL et non SSL du serveur Web, le port du support virtuel et la longueur minimale du mot de passe.

Authentification à deux facteurs

iLO est un outil puissant de gestion des serveurs HP ProLiant. Afin d'empêcher toute utilisation incorrecte de cet outil, l'accès à iLO est soumis à une authentification utilisateur fiable. La version 1.80 du micrologiciel offre une structure d'authentification plus performante pour iLO grâce à deux facteurs d'authentification. Les utilisateurs doivent confirmer leur identité en fournissant ces deux facteurs. Il s'agit d'un mot de passe ou code d'identification personnel, associé à une clé privée pour leur certificat numérique. Les utilisateurs ont la possibilité de stocker leurs certificats numériques et clés privées où ils le souhaitent, par exemple sur une carte à puce, une clé USB ou un disque dur.

Configuration de l'authentification à deux facteurs pour la première fois

Cette section décrit comment configurer l'authentification à deux facteurs pour la première fois à l'aide de comptes utilisateur locaux ou de comptes utilisateur de l'annuaire. Pour plus d'informations sur les paramètres de l'authentification à deux facteurs, reportez-vous à la section (« Two-Factor Authentication Settings » (Paramètres d'authentification à deux facteurs) page 35).

Configuration des comptes utilisateur locaux :

1. Obtenez le certificat public auprès de l'autorité de certification qui délivre les certificats utilisateur ou les cartes à puce dans votre entreprise.
2. Exportez ce certificat au format codé en base64 dans un fichier sur votre bureau, par exemple CAcert.txt.
3. Procurez-vous le certificat public de l'utilisateur qui doit accéder à iLO.
4. Exportez ce certificat au format codé en base64 dans un fichier sur votre bureau, par exemple Usercert.txt.

5. Ouvrez le fichier CAcert.txt dans le Bloc-notes, sélectionnez tout le texte et copiez-le en appuyant sur les touches **Ctrl+C**.
6. Connectez-vous à iLO et accédez à la page **Two-Factor Authentication Settings** (Paramètres d'authentification à deux facteurs).
7. Cliquez sur **Import Trusted CA Certificate** (Importer le certificat validé par l'autorité de certification). Une autre page s'affiche.
8. Cliquez dans la zone de texte blanche afin d'y placer le curseur, puis collez le contenu du Presse-papiers en appuyant sur les touches **Ctrl+V**.
9. Cliquez sur **Import Root CA Certificate** (Importer le certificat racine de l'autorité de certification). La page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs) s'affiche à nouveau, avec les informations indiquées sous Trusted CA Certificate Information (Informations sur le certificat validé par l'autorité de certification).
10. À partir de votre bureau, ouvrez le fichier Usercert.txt dans le Bloc-notes, sélectionnez tout le texte et copiez-le en appuyant sur les touches **Ctrl+C**.
11. Naviguez jusqu'à la page **User Administration** (Administration des utilisateurs) dans iLO, puis sélectionnez l'utilisateur pour lequel vous avez obtenu un certificat public ou créez un nouvel utilisateur.
12. Cliquez sur **View/Modify** (Afficher/Modifier).
13. Cliquez sur **Add a certificate** (Ajouter un certificat).
14. Cliquez dans la zone de texte blanche afin d'y placer votre curseur, puis collez le contenu du Presse-papiers en appuyant sur les touches (**Ctrl+V)**.
15. Cliquez sur **Add user Certificate** (Ajouter un certificat utilisateur). La page Modify User (Modifier utilisateur) s'affiche à nouveau, avec un nombre à 40 chiffres dans le champ Thumbprint (Empreinte). Ce nombre peut être comparé à l'empreinte affichée pour le certificat dans Microsoft® Certificate Viewer.
16. Naviguez jusqu'à la page **Two-Factor Authentication Settings** (Paramètres d'authentification à deux facteurs).
17. Attribuez la valeur **Yes** (Oui) au paramètre Enforce Two-Factor Authentication (Renforcer l'authentification à deux facteurs).
18. Remplacez la valeur du paramètre Check for Certificate Revocation (Contrôler la révocation de certificat) par **No (default)** (Non (par défaut)).
19. Cliquez sur **Appliquer**. iLO est alors réinitialisé. Lorsque iLO tente d'atteindre à nouveau la page d'identification, votre navigateur affiche la fenêtre Client Authentication (Authentification client), avec une liste des certificats disponibles pour ce système.

REMARQUE : si le certificat utilisateur n'est pas enregistré sur la machine client, vous ne pouvez pas le voir dans la liste. Le certificat utilisateur doit être enregistré sur le système client pour que vous puissiez le voir. S'il n'y a pas de certificats client sur le système client, il est possible que vous n'obteniez pas la fenêtre Client Authentication (Authentification client) mais plutôt une page d'erreur indiquant Page cannot be displayed (Impossible d'afficher la page). Pour pallier à cela, vous devez enregistrer le certificat client sur la machine client. Pour en savoir plus sur l'exportation et l'enregistrement de certificats client, reportez-vous à la documentation de votre carte à puce ou à l'autorité de certification.

20. Choisissez le certificat qui a été ajouté à l'utilisateur dans iLO. Cliquez sur **OK**.
21. Si vous y êtes invité, insérez la carte à puce ou saisissez votre code d'identification personnel ou mot de passe.

Une fois que vous aurez terminé le processus d'authentification, vous aurez accès à iLO.

Configuration des comptes utilisateur d'annuaire :

1. Obtenez le certificat public auprès de l'autorité de certification qui délivre les certificats utilisateur ou les cartes à puce dans votre entreprise.
2. Exportez ce certificat au format codé en base64 dans un fichier sur votre bureau, par exemple CAcert.txt.
3. Ouvrez le fichier CAcert.txt dans le Bloc-notes, sélectionnez tout le texte et copiez-le en appuyant sur les touches **Ctrl+C**.
4. Connectez-vous à iLO et accédez à la page **Two-Factor Authentication Settings** (Paramètres d'authentification à deux facteurs).
5. Cliquez sur **Import Trusted CA Certificate** (Importer le certificat validé par l'autorité de certification). Une autre page s'affiche.
6. Cliquez dans la zone de texte blanche afin d'y placer votre curseur, puis collez le contenu du Presse-papiers en appuyant sur les touches **Ctrl+V**.
7. Cliquez sur **Import Root CA Certificate** (Importer le certificat racine de l'autorité de certification). La page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs) s'affiche à nouveau, avec les informations indiquées sous Trusted CA Certificate Information (Informations sur le certificat validé par l'autorité de certification).
8. Attribuez la valeur **Yes** (Oui) au paramètre Enforce Two-Factor Authentication (Renforcer l'authentification à deux facteurs).
9. Remplacez la valeur du paramètre Check for Certificate Revocation (Contrôler la révocation de certificat) par **No (default)** (Non (par défaut)).
10. Attribuez au paramètre (Certificate Owner Field) Champ du propriétaire du certificat la valeur **SAN** (Réseau SAN). Pour en savoir plus, reportez-vous à la section (« Two-Factor Authentication Settings » (Paramètres d'authentification à deux facteurs) page 35).
11. Cliquez sur **Appliquer**. iLO est alors réinitialisé. Lorsque iLO tente d'atteindre à nouveau la page d'identification, votre navigateur affiche la fenêtre Client Authentication (Authentification client), avec une liste des certificats disponibles pour ce système.
12. Choisissez le certificat qui a été ajouté à l'utilisateur dans iLO. Cliquez sur **OK**.
13. Si vous y êtes invité, insérez la carte à puce ou saisissez votre code d'identification personnel ou mot de passe. La page d'identification doit s'afficher avec l'adresse e-mail de l'utilisateur dans le champ Directory User (Utilisateur de l'annuaire). Vous ne pouvez pas modifier ce champ.
14. Saisissez le mot de passe de l'utilisateur de l'annuaire. Cliquez sur **Login** (Connexion).

Une fois que vous aurez terminé le processus d'authentification, vous aurez accès à iLO. Reportez-vous à la section « Directory Settings » (Paramètres d'annuaire) (page 70) pour plus d'informations sur la configuration des utilisateurs et privilèges d'annuaire.

Connexion avec l'authentification à deux facteurs

Lorsque vous vous connectez à un système iLO configuré de telle sorte qu'il fasse appel à une authentification à deux facteurs, la fenêtre Client Authentication (Authentification client) vous invite à sélectionner le certificat à utiliser. Elle répertorie ensuite tous les certificats disponibles pour authentifier un client. Sélectionnez le certificat associé à un utilisateur local dans iLO ou, plus précisément, le certificat utilisateur délivré pour l'authentification par rapport à ce domaine.

Une fois que vous avez sélectionné un certificat, si ce dernier est protégé par mot de passe ou stocké sur une carte à puce, une deuxième fenêtre s'affiche et vous invite à saisir le code d'identification personnel ou mot de passe associé au certificat choisi.

Celui-ci est alors examiné par iLO, qui s'assure qu'il a bien été émis par l'autorité de certification validée en comparant la signature par rapport au certificat de l'autorité configuré dans iLO. iLO va déterminer si le certificat a été révoqué et s'il correspond à un utilisateur de la base de données des utilisateurs locaux d'iLO. Si tous ces tests sont couronnés de succès, l'interface utilisateur iLO classique s'affiche.

Si les données d'authentification utilisateur échouent, la page Login Failed (Échec d'ouverture de session) s'affiche. Dans ce cas, vous êtes invité à fermer le navigateur, ouvrir une nouvelle fenêtre du navigateur et réessayer. Si l'authentification par rapport à l'annuaire est activée et si l'authentification de l'utilisateur échoue, iLO affiche un écran d'ouverture de session avec le champ du nom d'utilisateur dans l'annuaire renseigné par la valeur du paramètre User Principal Name (Nom principal de l'utilisateur) du certificat ou celle du paramètre Distinguished name (Nom distinctif) (dérivé de l'objet du certificat). iLO demande le mot de passe pour ce compte utilisateur. Une fois qu'il a saisi le mot de passe, l'utilisateur est authentifié.

Pour cette version, iLO n'établit pas l'authentification à deux facteurs via la console distante. Au lieu de cela, elle repose sur la prise en charge des lecteurs de carte à puce interne à RDP pour offrir un accès aux systèmes qui requièrent une authentification par carte à puce pour le système d'exploitation distant. iLO fournit un accès à RDP à l'aide de la fonction Terminal Services Pass-Through (Pass-Through des Terminal Services). L'authentification par carte à puce est requise pour un serveur distant uniquement si un système d'exploitation est installé et opérationnel. La prise en charge des cartes à puce dans RDP requiert que la version du système d'exploitation du serveur distant soit Microsoft® Windows® Server 2003. Reportez-vous à la section « Option Terminal Services Pass-Through (Pass-Through des Terminal Services) » (page 39) pour de plus amples informations.

Certificats utilisateur pour l'authentification à deux facteurs

Pour procéder localement sur iLO à l'authentification d'un utilisateur à l'aide de l'authentification à deux facteurs, vous devez associer un certificat à son nom d'utilisateur local. Dans la page Administration>Modify User (Administration>Modifier utilisateur), si un certificat a été associé à l'utilisateur, une empreinte (un hachage SHA1 du certificat) s'affiche, ainsi qu'un bouton permettant la suppression du certificat. Si aucun certificat n'a été associé à l'utilisateur, le message « `Thumbprint: A certificate has NOT been mapped to this user (Empreinte : AUCUN certificat n'a été associé à cet utilisateur)` » s'affiche, accompagné d'un bouton permettant de démarrer le processus d'importation de certificat.

Pour définir un utilisateur pour l'authentification à deux facteurs et ajouter un certificat utilisateur :

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO). Cliquez sur **Administration**.
2. Sélectionnez un utilisateur.
3. Cliquez sur **View/Modify** (Afficher/Modifier).

4. Dans la section User Certificate Information (Informations sur le certificat utilisateur), cliquez sur **Add a certificate** (Ajouter un certificat).
5. Dans la page Map User Certificate (Associer un certificat utilisateur), collez le certificat utilisateur dans la zone de texte, puis cliquez sur **Import Certificate** (Importer certificat).

Pour plus d'informations sur l'administration des utilisateurs, reportez-vous à la section « User administration (Administration des utilisateurs) » (page 24).

Utilisation de l'authentification à deux facteurs avec l'authentification d'annuaire

Dans certains cas, la configuration de l'authentification à deux facteurs avec l'authentification d'annuaire est compliquée. iLO peut utiliser le schéma HP Extended ou le schéma Default Directory pour l'intégration aux services d'annuaire. Pour assurer la sécurité lorsque l'authentification à deux facteurs est renforcée, iLO utilise un attribut du certificat client en tant que nom de connexion de l'utilisateur à l'annuaire. Le paramètre de configuration qui détermine quel attribut de certificat client est utilisé par iLO est Certificate Owner (Propriétaire du certificat) sur la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs). Si la valeur attribuée à ce paramètre est SAN (Réseau SAN), iLO obtient le nom de connexion de l'utilisateur à l'annuaire à partir de l'attribut UPN du réseau SAN. Si le paramètre Certificate Owner (Propriétaire du certificat) possède la valeur Subject (Objet), iLO obtient le nom distinctif de l'utilisateur dans l'annuaire à partir de l'objet du certificat.

Le choix de ces paramètres dépend de la méthode d'intégration d'annuaire utilisée, de la manière dont l'architecture de l'annuaire est construite et des informations contenues dans les certificats utilisateur émis. Les exemples suivants présupposent que vous disposez des autorisations appropriées.

Authentification à l'aide du schéma Default Directory, partie 1 : le nom distinctif d'un utilisateur dans l'annuaire est CN=John Doe,OU=IT,DC=MyCompany,DC=com et les attributs du certificat de John Doe sont les suivants :

- Subject: DC=com/DC=MyCompany/OU=IT/CN=John Doe
- SAN/UPN: john.doe@MyCompany.com

L'authentification auprès d'iLO avec le nom d'utilisateur username:john.doe@MyCompany.com et le mot de passe va fonctionner si l'authentification à deux facteurs n'est **pas** renforcée. Une fois que l'authentification à deux facteurs a été renforcée, si la valeur SAN (Réseau SAN) est sélectionnée sur la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs), la page d'ouverture de session renseigne automatiquement le champ Directory User (Utilisateur d'annuaire) avec la valeur john.doe@MyCompany.com. Le mot de passe peut être saisi, mais l'utilisateur ne sera **pas** authentifié. En effet, john.doe@MyCompany.com, qui a été obtenu à partir du certificat, n'est pas le nom distinctif de l'utilisateur dans l'annuaire. Dans ce cas, vous devez sélectionner la valeur **Subject** (Objet) dans la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs). Le champ Directory User (Utilisateur d'annuaire) est alors automatiquement renseigné avec la valeur CN=John Doe,OU=IT,DC=MyCompany,DC=com, ce qui correspond au nom distinctif réel de l'utilisateur. Si le mot de passe saisi est correct, l'utilisateur est authentifié.

Authentification à l'aide du schéma Default Directory, partie 2 : le nom distinctif d'un utilisateur dans l'annuaire est CN=john.doe@MyCompany.com,OU=IT,DC=MyCompany,DC=com et les attributs du certificat de John Doe sont les suivants :

- Subject: DC=com/DC=MyCompany/OU=Employees/CN=John Doe/E=john.doe@MyCompany.com

- SAN/UPN: john.doe@MyCompany.com
- Le contexte de recherche sur la page Directory Settings (Paramètres d'annuaire) est défini sur : OU=IT,DC=MyCompany,DC=com

Dans cet exemple, si la valeur SAN (Réseau SAN) est sélectionnée sur la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs), le champ Directory User (Utilisateur d'annuaire) de la page d'ouverture de session est renseigné avec la valeur john.doe@MyCompany.com. Une fois que le mot de passe correct est saisi, l'utilisateur est authentifié. Il est authentifié même si john.doe@MyCompany.com n'est pas son nom distinctif. En effet, iLO tente de l'authentifier à l'aide des champs du contexte de recherche (CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com) configurés dans la page Directory Settings (Paramètres d'annuaire). Comme il s'agit du nom distinctif correct de l'utilisateur, iLO le retrouve dans l'annuaire.

REMARQUE : si vous sélectionnez Subject (Objet) dans la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs), l'authentification échoue car l'objet du certificat ne constitue pas le nom distinctif de l'utilisateur dans l'annuaire.

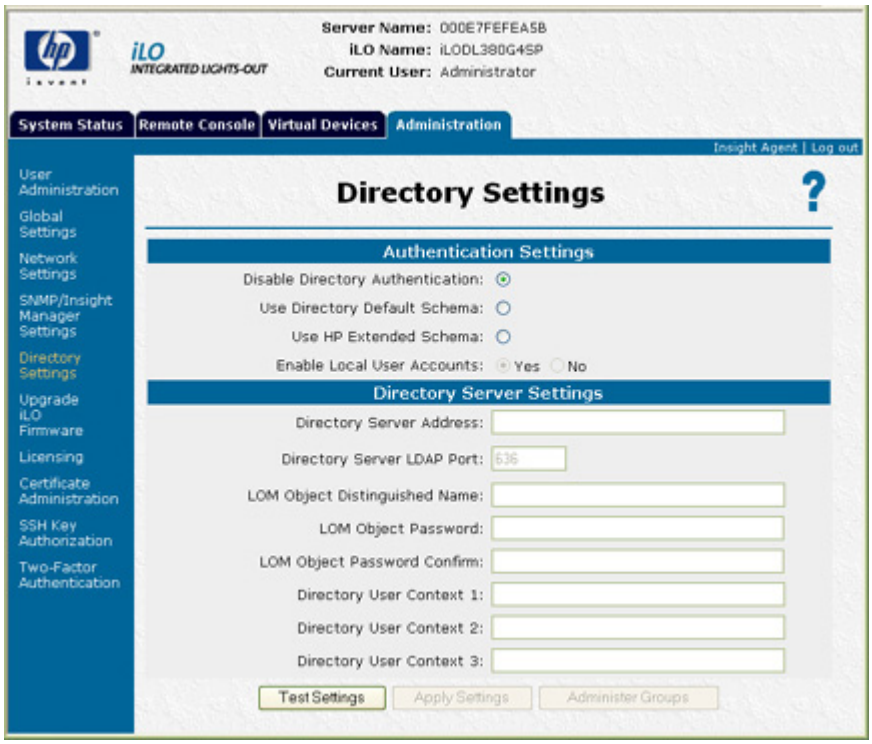
Lorsque vous utilisez la méthode de schéma HP Extended, HP recommande de sélectionner l'option SAN (Réseau SAN) dans la page Two-factor Authentication Settings (Paramètres d'authentification à deux facteurs).

Directory Settings (Paramètres d'annuaire)

iLO se connecte aux services d'annuaire Microsoft® Active Directory, Novell e-Directory et autres services d'annuaire compatibles LDAP 3.0 pour l'authentification et l'autorisation d'utilisateurs. Vous pouvez configurer iLO pour authentifier et autoriser des utilisateurs en utilisant l'intégration d'annuaires de schéma HP ou l'intégration d'annuaires sans schéma. iLO se connecte uniquement aux services d'annuaire en employant des connexions sécurisées SSL vers le port LDAP du serveur d'annuaires. Le port LDAP sécurisé par défaut est 636. La prise en charge des services d'annuaire est une fonction sous licence disponible avec l'achat de licences facultatives. Pour plus d'informations, reportez-vous à la section « LicenceError! No bookmark name given. » (page 22). Pour des informations complémentaires sur les annuaires, reportez-vous à la section « Services d'annuaire » (page 117).

Les comptes utilisateur stockés localement (trouvés sur la page User Administration) peuvent êtres actifs lorsque la prise en charge d'annuaires iLO est activée. Cette prise en charge active les accès utilisateur locaux et basés sur les les annuaires. Généralement, un administrateur peut supprimer des comptes utilisateur locaux (excepté, peut-être un compte d'accès d'urgence) une fois que iLO est correctement configuré pour accéder au service d'annuaire. Vous pouvez également désactiver l'accès à ces comptes si la prise en charge d'annuaires est activée.

Configuration des paramètres d'annuaire



L'écran Directory Settings (Paramètres d'annuaire) contient les options suivantes :

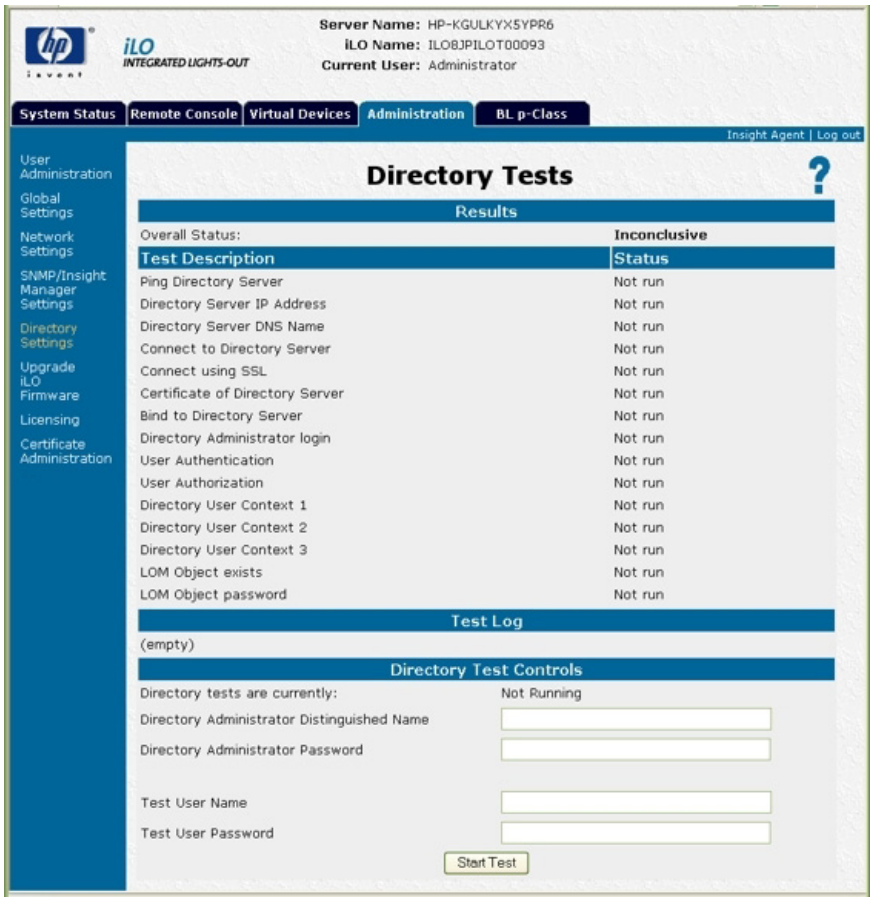
- Disable Directory Authentication (Désactiver l'authentification d'annuaire)
- Use Directory Default Schema (Utiliser le schéma Directory Default)
- Use HP Extended Schema (Utiliser le schéma HP Extended)
- Enable Local User Accounts (Activer comptes utilisateur locaux)
- Directory Server Address (Adresse du serveur d'annuaire)
- Directory Server LDAP Port (Port LDAP du serveur d'annuaire)
- LOM Object Distinguished Name (Nom distinctif de l'objet LOM)
- LOM Object Password Confirm (Confirmation du mot de passe de l'objet LOM)
- Directory User Context 1 (Contexte 2 de l'utilisateur d'annuaire)
- Directory User Context 2 (Contexte 2 de l'utilisateur d'annuaire)
- Directory User Context 3 (Contexte 2 de l'utilisateur d'annuaire)

Cliquez sur **Apply Settings** (Appliquer paramètres) pour enregistrer les modifications. Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out.*

Pour tester la communication entre le serveur d'annuaire et la carte iLO, cliquez sur **Test Settings** (Tester paramètres). Pour plus d'informations, reportez-vous à la section « Tests d'annuaire » (page 72).

Tests d'annuaire

Pour valider les paramètres d'annuaire actuels de la carte iLO, cliquez sur **Test Settings** (Tester paramètres) dans la page Directory Settings (Paramètres d'annuaire). La page Directory Tests (Tests d'annuaire) s'affiche.



La page de test affiche les résultats d'une série de tests simples conçus pour valider les paramètres actuels de l'annuaire. Elle inclut en outre un journal de test qui affiche les résultats des tests ainsi que les éventuels problèmes détectés. Après avoir configuré correctement les paramètres de votre annuaire, vous ne devez pas réexécuter ces tests. L'écran Directory Tests (Test d'annuaire) ne requiert pas que l'utilisateur se connecte en tant qu'utilisateur d'annuaire.

Pour vérifier vos paramètres d'annuaire :

1. Entrez le nom distinctif et le mot de passe d'un administrateur d'annuaire ; L'idéal serait de prendre les données d'authentification utilisées lors de la création des objets iLO dans l'annuaire. Ces données ne sont pas enregistrées par la carte iLO. Elles sont utilisées pour vérifier l'objet iLO et les contextes de recherche utilisateur.
2. Entrez également un nom d'utilisateur et un mot de passe tests. En général, on utilise un compte destiné à accéder à la carte iLO testée. Il peut s'agir du même compte que l'administrateur d'annuaire. Toutefois, les tests ne permettent pas de vérifier l'authentification de l'utilisateur avec un compte « superutilisateur ». Ces données ne sont pas enregistrées par la carte iLO.

3. Cliquez sur **Start Test** (Démarrer test). Plusieurs tests sont lancés en arrière-plan, du ping réseau de l'utilisateur de l'annuaire à l'établissement d'une connexion SSL au serveur, en passant par l'évaluation des privilèges utilisateur tels qu'ils seraient contrôlés lors d'une connexion normale.

   Pendant l'exécution des tests, la page est rafraîchie à intervalles réguliers. Pendant l'exécution du test, vous pouvez à tout moment arrêter le test ou rafraîchir la page manuellement.
4. Consultez le lien d'aide sur la page pour obtenir des informations sur les tests et les actions à prendre en cas de problèmes.

Utilisation de la fonctionnalité iLO

Cette section traite des rubriques suivantes :

Première connexion à iLO

La carte iLO est configurée avec un nom d'utilisateur, un mot de passe et un nom DNS par défaut. Les informations utilisateur par défaut se trouvent sur l'étiquette iLO Network Settings (Paramètres réseau iLO) apposée sur le serveur contenant le processeur de supervision iLO. Utilisez ces valeurs pour accéder à la carte iLO depuis un client réseau distant à l'aide d'un navigateur Internet standard.

Pour des raisons de sécurité, HP recommande de modifier les paramètres par défaut après le premier accès à la carte iLO.

Les valeurs par défaut sont :

- Nom d'utilisateur : Administrator
- Mot de passe : chaîne alphanumérique aléatoire de 8 caractères
- DNS Name (Nom DNS) : *ILOXXXXXXXXXXXX*, où les *X* correspondent au numéro de série du serveur

REMARQUE : les noms d'utilisateur et les mots de passe respectent la casse.

Temporisations progressives pour les tentatives de connexion infructueuses

Après un échec d'ouverture de session initiale, la carte iLO impose un délai de sécurité. Pour plus d'informations sur la sécurité de connexion, reportez-vous à la section « Sécurité de la connexion » (page 64).

Aide

Une assistance pour toutes les options de la carte iLO est disponible par l'intermédiaire de l'option Help (Aide) de la carte iLO. Ces liens fournissent des informations récapitulatives sur les fonctions de la carte iLO et des informations utiles pour l'optimisation de son fonctionnement. Pour accéder à une page d'aide spécifique, cliquez sur **?** dans la partie droite de la fenêtre du navigateur.

System Status (État du système)

Les options suivantes sont disponibles sur l'onglet System Status (État du système).

Status Summary (Résumé de l'état)

L'écran Status Summary (Résumé de l'état) fournit des informations générales sur la carte iLO, telles que l'utilisateur actuel, le nom et l'état du serveur, l'adresse IP et le nom de la carte iLO, ainsi que les dernières entrées du journal. Il indique également si iLO a été configuré pour utiliser les agents de supervision Web de HP et les agents de supervision Web Insight.

iLO Status (État de la carte iLO)

L'option iLO Status (État de la carte iLO) fournit des informations complètes sur l'état de la carte iLO, y compris :

- Current user (Utilisateur actuel)
- L'état et la disponibilité de la console distante ;
- Ll'état et la disponibilité du Pass-Through des Terminal Services ;
- La date et l'heure actuelles de la carte iLO ;

  REMARQUE : la date et l'heure sont définies pendant le test POST (auto-test de mise sous tension) et gérées par les agents de supervision MP.

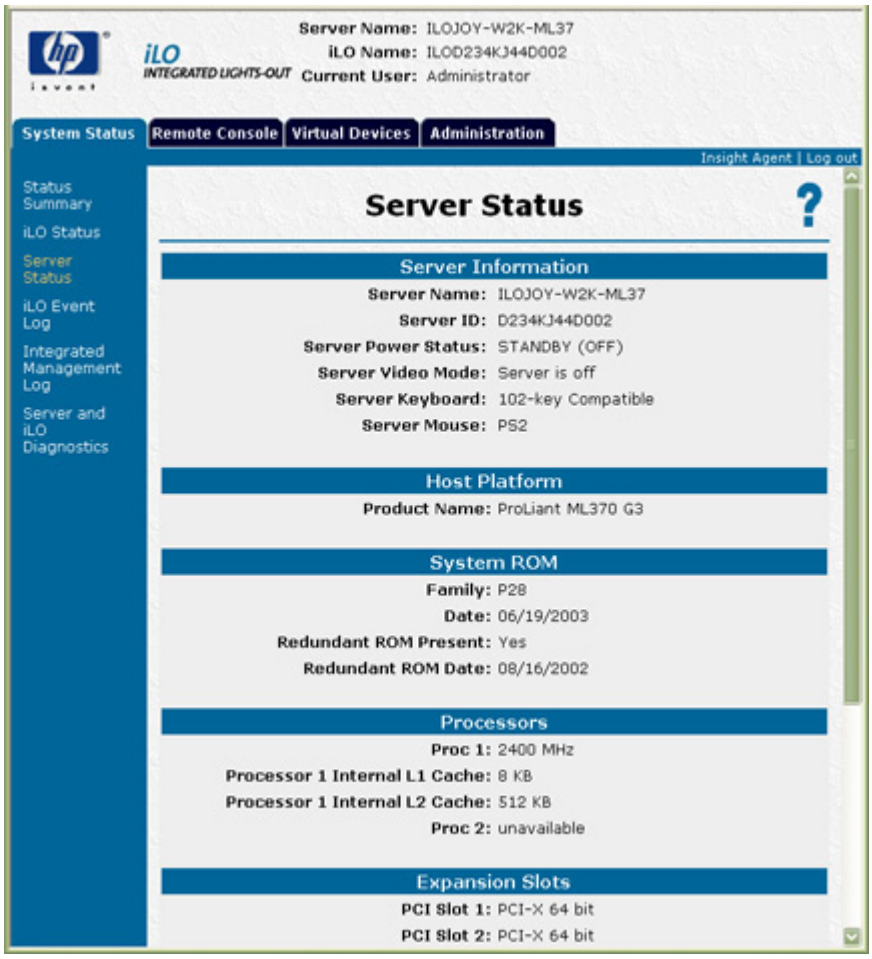
- Les informations de révision du microprogramme iLO ;
- La version du produit (iLO Standard ou iLO Advanced).

Server Status (État du serveur)

L'option Server Status (État du serveur) fournit des informations complètes sur l'état du serveur, notamment sur :

- Le nom du serveur associé au processeur de supervision iLO ;

  Le champ Server Name (Nom du serveur) indique `host is unnamed` (l'hôte n'est pas nommé) si les agents de supervision HP n'ont pas été chargés sur le serveur hôte.
- Server power status (État d'alimentation du serveur)
- Le mode vidéo du serveur ;
- Le type de clavier et de souris du serveur tels qu'ils sont simulés par la console distante ;
- Les données SMBIOS, telles que la plate-forme hôte, la ROM système, les processeurs, les adresses MAC intégrées, les connecteurs d'expansion et les modules mémoire présents lors de l'auto-test de mise sous tension (POST).



Journal des événements de iLO

Le journal des événements de iLO est un enregistrement des événements majeurs détectés par iLO. Les événements consignés comprennent les principaux événements du serveur tels que les interruptions d'alimentation ou les réinitialisations du serveur. Le journal des événements contient également un enregistrement des événements iLO, notamment les tentatives de connexion non autorisées.

Les autres événements enregistrés incluent toutes les tentatives d'ouverture de session, réussies ou infructueuses, au niveau du navigateur et de la console distante, les événements d'alimentation virtuelle et de cycle de mise sous tension et les actions d'effacement du journal des événements. Certaines modifications de la configuration, par exemple la création ou la suppression d'un utilisateur, sont également enregistrées.

La carte iLO assure le codage sécurisé des mots de passe, effectue le suivi de toutes les tentatives d'ouverture de session et conserve un enregistrement de tous les échecs d'ouverture de session. Lorsque la tentative de connexion échoue, iLO génère également des alertes et les envoie à une console de supervision distante.

Les événements enregistrés par des versions ultérieures du microprogramme iLO peuvent ne pas être pris en charge par des versions antérieures Si un événement est enregistré par un microprogramme non pris en charge, l'événement est répertorié en tant que `UNKNOWN EVENT TYPE` (Type d'événement inconnu). Pour résoudre ce problème, vous pouvez effacer le journal des événements afin de supprimer ces entrées ou mettre à niveau le microprogramme à la dernière version prise en charge.

Pour effacer le journal des événements :

1. Cliquez sur **Clear Event Log** (Effacer journal des événements) pour effacer toutes les informations consignées dans le journal des événements.
2. Cliquez sur **OK** pour confirmer la suppression des enregistrements du journal. Une ligne indiquant que le journal a été effacé est consignée dans le journal.

Integrated Management Log (journal de maintenance intégré)

Le journal de maintenance intégré (IML) est un enregistrement des événements majeurs survenus sur la plate-forme hôte. Les événements sont générés par la ROM système et des services tels que le driver d'état System Management (Supervision du système). iLO gère le journal de maintenance du système (IML) accessible à l'aide d'un navigateur pris en charge, même si le serveur est éteint. Cette fonctionnalité peut être utile lors de la résolution des problèmes d'un serveur hôte distant.

Le journal de maintenance intégré (IML) permet d'afficher les événements consignés relatifs au serveur distant. Les événements enregistrés incluent tous les événements propres au serveur enregistrés par le driver d'état du système, y compris les informations du système d'exploitation et les codes POST basés sur la ROM. Pour plus d'informations, reportez-vous au manuel de votre serveur.

1. Cliquez sur **Clear Event Log** (Effacer journal des événements) pour effacer toutes les informations consignées dans le journal des événements.
2. Cliquez sur **OK** pour confirmer la suppression des enregistrements du journal. Une ligne indiquant que le journal a été effacé est consignée dans le journal.

Diagnostics du serveur et de la carte iLO

L'option Server and iLO Diagnostics (Diagnostics du serveur et de la carte iLO) fournit des informations complètes sur le diagnostic, comme indiqué dans les sections suivantes :

- Résultats des diagnostics du test POST pour le serveur hôte (page 78)
- Liste des variables d'environnement NVRAM (page 79)
- Bouton NMI virtuel (page 79)
- Résultats de l'auto-test iLO (page 79)

REMARQUE : lorsque vous vous connectez via Diagnostics Port (Port de diagnostics), le serveur d'annuaire n'est pas disponible. Vous pouvez uniquement ouvrir une session à l'aide d'un compte local.

Résultats des diagnostics du test POST pour le serveur hôte

En tant que processeur de supervision intégré, la carte iLO contrôle la progression du processus d'amorçage du serveur. La mémoire ROM du serveur hôte écrit des codes POST pendant l'amorçage. La carte iLO enregistre et affiche ces codes.

Les codes POST documentent le processus d'amorçage du Bios de la mémoire ROM. Un code indique le début d'une phase donnée du processus d'amorçage. Les résultats des codes POST peuvent être utilisés pour déterminer la phase générale au cours de laquelle le processus d'amorçage a été interrompu. L'utilisation des seuls codes POST ne suffit généralement pas à diagnostiquer la cause première réelle de l'interruption du processus d'amorçage. Pour cela, les codes POST doivent être utilisés en association avec d'autres outils, tels que le journal de maintenance intégré (IML), la console locale ou distante iLO et les utilitaires de diagnostic.

La liste suivante reprend tous les codes POST et les résultats de diagnostic du serveur hôte surveillé par une carte iLO pour une séquence d'amorçage de routine sur des serveurs ProLiant.

Code	Début de phase
FE04	Initialisation de EISA
FE08	Initialisation de PCI
FE0C	Initialisation du processeur
FE10	Initialisation de la vidéo
FE14	Initialisation du cache
FE18	Initialisation de USB
FE1C	Test de la mémoire
FE20	Initialisation de la mémoire
FE24	Démarrage de USB
FE28	Test des contrôleurs de disquette
FE2C	Initialisation de la ROM d'option
FE30	Initialisation de la mémoire ROM d'option ATAPI
FE34	Initialisation de BBS
FE38	Début du processus BOOT
FE3C	Tentative d'amorçage de CD SCSI
FE40	Tentative d'amorçage de la disquette
FE44	Tentative d'amorçage du disque dur
FE48	Tentative d'amorçage du CD
FE4C	Tentative d'amorçage de PXE
FE50	Transfert de contrôle au code du secteur d'amorçage
FE54	Pas de périphériques amorçables

Liste des variables d'environnement NVRAM

HP utilise la mémoire RAM non volatile (NVRAM) pour stocker les variables d'environnement du serveur, par exemple l'ordre d'initialisation du contrôleur hôte. Ces informations peuvent être utiles aux ingénieurs HP et aux utilisateurs avancés possédant une connaissance approfondie de l'architecture de supervision du système HP.

Bouton Virtual NMI (NMI virtuel)

Le bouton Virtual NMI (NMI virtuel) arrête le système d'exploitation pour le déboguer. Il s'agit d'une fonction avancée qui doit être exclusivement utilisée pour un débogage au niveau du noyau.
Cette fonction permet également :

- De faire la démonstration du fonctionnement de ASR ;

  Si le driver d'état System Management (Supervision du système) est chargé et que ASR est activé, l'hôte se réinitialise automatiquement après une interruption NMI.

- D'effectuer le débogage ;

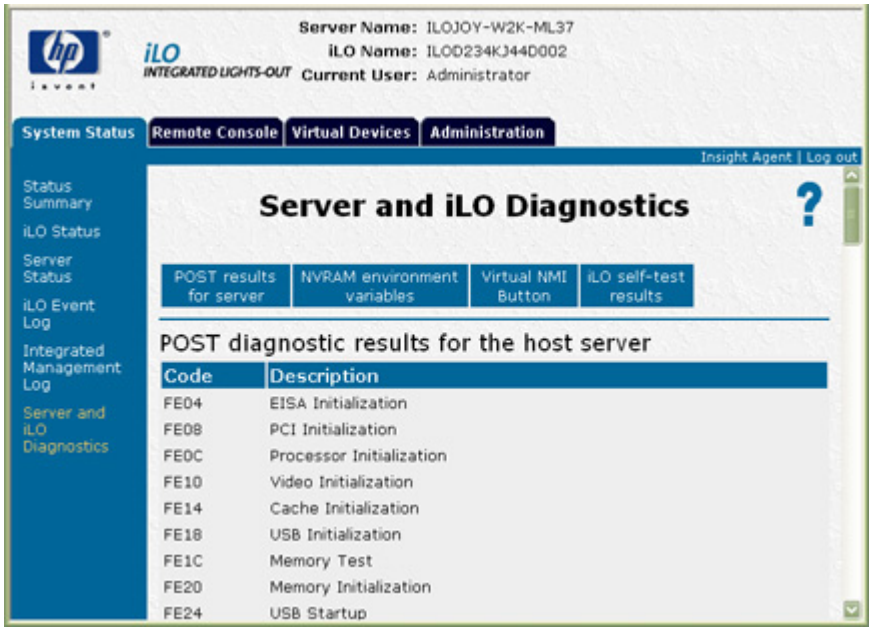
  Si une application logicielle arrête le système, la fonctionnalité NMI permet de lancer le programme de débogage du système d'exploitation.

- D'effectuer le vidage d'un hôte qui ne répond pas.

  Un fournisseur peut être intéressé par la capture du contexte du serveur.

Résultats de l'auto-test iLO

Les résultats de l'auto-test iLO s'affichent dans l'écran Server and iLO Diagnostics (Diagnostics du serveur et de la carte iLO). Tous les sous-systèmes testés doivent indiquer `Passed` (Test réussi) en situation normale.



Remote Console (Console distante)

L'onglet Remote Console (Console distante) vous permet d'accéder aux différentes vues de la console distante et de définir des séquences de raccourcis qui seront transmises au serveur hôte distant en appuyant sur une touche d'activation. La carte iLO standard propose des fonctionnalités intégrées de console distante basée sur le matériel utilisant un écran en mode texte. La console, qui est indépendante du système d'exploitation, prend en charge les modes texte permettant d'afficher les activités du serveur hôte distant, comme les opérations d'arrêt et de démarrage.

La fonction Graphical Remote Console (Console graphique distante) peut être activée en faisant l'acquisition de la licence du pack iLO Advanced, disponible en option. Les fonctionnalités de la console graphique distante transforment n'importe quel navigateur standard en un poste de travail virtuel, permettant ainsi à l'utilisateur de contrôler totalement l'écran, le clavier et la souris du serveur hôte. La console, qui est indépendante du système d'exploitation, prend en charge les modes graphiques permettant d'afficher les activités du serveur hôte distant, comme les opérations d'arrêt et de démarrage.

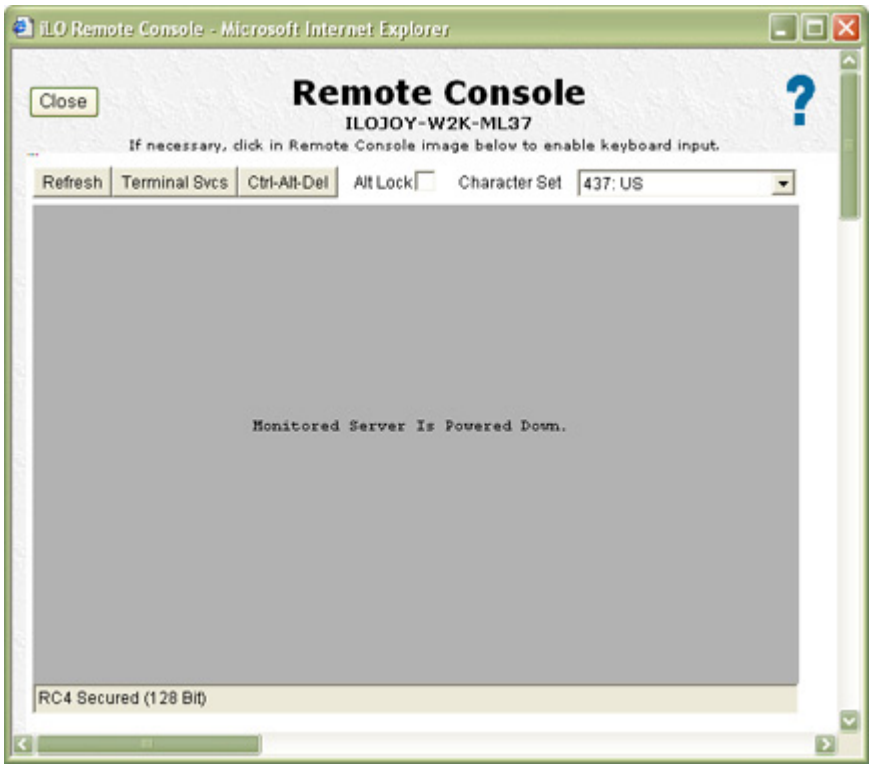
Option Remote Console (Console distante)

L'option Remote Console (Console distante) réoriente la console du serveur hôte vers le navigateur du client réseau, lui permettant ainsi d'accéder aux modes vidéo graphiques et texte intégral (standard), au clavier et à la souris du serveur hôte distant (à condition de posséder la licence du pack iLO Advanced).

La console distante permet de contrôler totalement un serveur hôte distant comme si vous vous trouviez sur place. Vous pouvez accéder au système de fichiers distant et aux unités réseau. La console distante permet de modifier les paramètres du matériel et des logiciels du serveur hôte distant, d'installer des applications et des drivers, de modifier la résolution de l'écran du serveur distant et d'arrêter le système distant de façon ordonnée.

Elle permet également d'observer les messages POST d'amorçage au moment où le serveur hôte distant redémarre et lance les routines de configuration basée sur la ROM pour configurer le matériel du serveur hôte distant. Lors de l'installation de systèmes d'exploitation à distance, la console graphique distante (si sous licence) permet d'afficher et de contrôler l'écran du serveur hôte pendant toute la procédure d'installation.

Pour obtenir des performances optimales, configurez l'écran de votre système d'exploitation hôte tel qu'indiqué dans la section « Optimisation des performances de la fonction Graphical Remote Console » (Console graphique distante) (page 82).



Options Remote Console Information (Informations sur la console distante)

L'option Remote Console Information (Informations sur la console distante) affiche les options disponibles de la console distante, ainsi qu'un lien permettant de télécharger une version actualisée de Java™ Runtime Environment, indispensable pour utiliser la console distante avec l'option curseur simple (« Mode curseur simple », page 87).

Il est possible de connecter simultanément 10 utilisateurs à la carte iLO. Cependant, un seul utilisateur à la fois est habilité à accéder à la console distante. Si vous essayez d'ouvrir la console distante alors que vous l'utilisez déjà, un message d'avertissement s'affiche indiquant qu'un autre utilisateur l'utilise. Si la valeur du paramètre Enable Remote Console Acquire (Activer l'acquisition de la console distante) dans la page Global Settings (Paramètres généraux) est définie sur Yes (Oui), un bouton Acquire (Acquérir) est disponible dans la page Remote Console (Console distante). Si vous cliquez sur **Acquire** (Acquérir), la session de console distante de l'autre utilisateur se terminera et votre session de console distante commencera dans votre fenêtre actuelle.

La console distante n'est pas disponible lorsque l'option Remote Console Port Configuration (Configuration du port de la console distante) sous l'onglet Global Settings (Paramètres généraux) est désactivée.

Fonctions avancées de Remote Console (Console distante)

L'applet Remote Console contient des boutons qui ajoutent des fonctions avancées à la carte iLO. Ces boutons ont les fonctions suivantes :

- **Refresh** (Rafraîchir) : force iLO à rafraîchir l'écran.
- **Terminal Svcs** (Serv. Terminal) : lance le client Microsoft® Terminal Services installé sur votre système. Ce bouton est désactivé si la fonction Terminal Services est désactivée ou non installée sur le serveur.
- **Ctrl-Alt-Del** (Ctrl+Alt+Suppr) : permet d'entrer cette combinaison de touches dans la console distante.
- **Alt Lock** (Verr Alt) : lorsque vous cliquez sur ce bouton, chaque touche sur laquelle vous appuyez est transmise au serveur comme si vous aviez appuyé simultanément sur cette dernière et sur la touche Alt.
- **High Performance Mouse** (Souris hautes performances) : lorsque vous sélectionnez cette option, l'émulation de la souris passe d'un modèle PS2 à un modèle HID USB, ce qui améliore considérablement ses performances.
- **Character Set** (Jeu de caractères) : modifie le jeu de caractères par défaut utilisé par la console distante. La modification du jeu de caractères de la console distante garantit l'affichage correct des caractères.
- **Close** (Fermer) : ferme la fenêtre Remote Console (Console distante) et met fin à la session de console distante.
- **Acquire** (Acquérir) : vous permet de prendre le contrôle d'une fenêtre de session de console distante lorsqu'elle est utilisée par un autre utilisateur et démarre une nouvelle session de console distante dans votre fenêtre actuelle. La valeur du paramètre Enable Remote Console Acquire (Activer l'acquisition de la console distante) dans la page Global Settings (Paramètres généraux) doit être définie sur Yes (Oui) pour que ce bouton soit visible.

Optimisation des performances de la fonction Graphical Remote Console (Console graphique distante)

HP vous recommande d'utiliser les paramètres client et serveur suivants en fonction du système d'exploitation utilisé.

Paramètres client recommandés

Dans l'idéal, il convient que la résolution d'affichage du système d'exploitation du serveur distant soit égale ou inférieure à celle de l'ordinateur qui le consulte. Une résolution de serveur supérieure permet de transmettre plus d'informations, mais ralentit les performances générales.

Utilisez les paramètres suivants pour le client et le navigateur, de façon à optimiser les performances :

- **Propriétés d'affichage**
  - Choisissez une résolution d'écran supérieure à 256 couleurs.
  - Choisissez une résolution d'écran supérieure à celle du serveur distant.
  - Propriétés d'affichage de Linux X : dans l'écran X Preferences (Préférences X), paramétrez la taille de la police sur **12**.

- **Remote Console (Console distante)**
  - Pour la vitesse de la console distante, il est conseillé d'utiliser un client de 700 MHz ou plus rapide, avec 128 Mo de mémoire minimum.
  - Pour l'exécution de l'applet Java™ Remote Console, HP vous recommande d'utiliser un client à processeur unique.
- **Propriétés de la souris**
  - Réglez le paramètre Mouse Pointer (Pointeur de la souris) sur une vitesse moyenne.
  - Réglez le paramètre Mouse Pointer Acceleration (Accélération du pointeur) sur une valeur faible ou désactivez-le.

Paramètres de souris hautes performances

Lorsque vous utilisez la console distante, vous avez la possibilité d'activer la fonctionnalité High Performance Mouse (Souris hautes performances). Une souris hautes performances améliore grandement les performances et la précision sous Windows Server™ 2003 et Windows Server™ 2000 Service Pack 3 (ou version ultérieure). Cette fonction fait passer l'émulation de la souris d'une souris PS/2 conventionnelle à une souris HID USB. La souris HID consigne les mises à jour dans un repère absolu au lieu d'un repère relatif (à l'instar d'une souris PS/2) et élimine les problèmes de synchronisation de souris.

La souris hautes performances fonctionne uniquement sous les systèmes d'exploitation Windows®. Du fait qu'elle utilise une connexion USB, elle est susceptible d'interférer avec le support virtuel. Vous ne pouvez pas activer ou désactiver cette fonction lorsqu'un support virtuel est connecté. Le serveur hôte doit exécuter Windows Server™ 2000 Service Pack 3 (ou version ultérieure) ou Windows Server™ 2003.

> **REMARQUE :** lorsque vous utilisez la console distante pendant une installation de système d'exploitation assistée par SmartStart, désactivez la prise en charge de la fonctionnalité High Performance Mouse (Souris hautes performances).

Pour obtenir des performances optimales, configurez le serveur hôte afin qu'il utilise le curseur de la souris matérielle. Modifiez les paramètres suivants dans le Panneau de configuration :

1. Sélectionnez **Souris>Pointeurs>Modèle>Windows par défaut** (modèle système). Cliquez sur **OK**.
2. Désactivez **Souris > Pointeurs > Activer l'ombre du pointeur**. Cliquez sur **OK**.
3. Sélectionnez **Affichage>Paramètres>Avancé>Dépannage>Accélération matérielle>Complète**. Cliquez sur **OK**.
4. Sélectionnez **Système>Avancé>Performances>Paramètres>Effets visuels>Ajuster afin d'obtenir les meilleures performances.** Click **OK**.

Alternativement, l'utilitaire de configuration en ligne HP (HPONCFG) règle automatiquement ces paramètres. Vous pouvez également modifier les paramètres de la fonctionnalité High Performance Mouse à l'aide de la commande XML MOD_GLOBAL_SETTINGS. Pour plus d'informations, reportez-vous au *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out.*

Paramètres Linux de la console distante

Lorsque vous utilisez la console distante iLO pour afficher des écrans texte dans Linux, il arrive que les caractères de bordure ou autres caractères de tracé ne s'affichent pas correctement.

Pour configurer correctement le jeu de caractères du mode texte dans la console distante :

1. Cliquez sur le menu contextuel **Character Set** (Jeu de caractères) dans l'applet Remote Console.
2. Sélectionnez le jeu de caractères **Lat1–16**.

Paramètres serveur recommandés

La liste ci-dessous indique les paramètres recommandés pour les serveurs en fonction des différents systèmes d'exploitation.

> **REMARQUE :** pour afficher entièrement l'écran du serveur hôte sur l'applet de la console distante du client, paramétrez l'écran du serveur sur une résolution inférieure ou égale à celle du client.

Paramètres de Microsoft® Windows NT® 4.0 et Windows® 2000

Pour optimiser les performances, utilisez les paramètres suivants :

- **Propriétés d**'affichage du serveur
  - Fond neutre (aucun motif)
  - Résolution de l'écran de 800 x 600 ou 1024 x 768 pixels
  - Résolution couleur de 256 couleurs ou 24 bits
- **Propriétés de la souris** du serveur
  - Sélectionnez **None** (Aucun) pour le paramètre Scheme (Modèle) du pointeur de souris.
  - Désactivez l'option **Enable Pointer Shadow** (Activer l'ombre du pointeur).
  - Sélectionnez **Motion** (Mouvement) ou **Pointer Options** (Options du pointeur) et réglez le curseur Speed (Vitesse) du pointeur sur la position médiane.
  - Paramétrez Pointer Acceleration (Accélération du pointeur) sur **None** (Aucune).

Paramètres de Microsoft® Windows® Server 2003

Pour optimiser les performances, utilisez les paramètres suivants :

- **Propriétés d'affichage** du serveur
  - Fond neutre (aucun motif)
  - Résolution de l'écran de 800 x 600 ou 1024 x 768 pixels
  - Résolution couleur de 256 couleurs ou 24 bits
- **Propriétés de la souris** du serveur
  - Sélectionnez **None** (Aucun) pour le paramètre Scheme (Modèle) du pointeur de souris.
  - Sélectionnez **Disable Pointer Trails** (Désactiver la trace du pointeur).
  - Désactivez l'option **Enable Pointer Shadow** (Activer l'ombre du pointeur).
  - Sélectionnez **Motion** (Mouvement) ou **Pointer Options** (Options du pointeur) et réglez le curseur Speed (Vitesse) du pointeur sur la position médiane.
  - Désactivez l'option **Enhanced pointer precision** (Améliorer la précision du pointeur).

Pour paramétrer automatiquement la configuration optimale de la souris, téléchargez l'utilitaire Lights-Out Optimization (Optimisation de Lights-Out) depuis le site Web HP (http://www.hp.com/servers/lights-out). Cliquez d'abord sur le graphique **Best Practices** (Meilleures pratiques) puis sur les liens **Maximize Performance** (Maximaliser performances).

Paramètres des serveurs Red Hat Linux et SuSE Linux

Pour optimiser les performances, utilisez les paramètres suivants :

- **Propriétés d'affichage** du serveur
  - Résolution : 1024 x 768 pixels ou moins
  - 256 couleurs
- **Propriétés de la souris** du serveur
  - Paramétrez **Pointer Acceleration** (Accélération du pointeur) sur **1x**. Pour KDE, accédez au panneau **KDE Control Center** (Centre de contrôle KDE), sélectionnez **Peripherals/Mouse** (Périphériques/Souris), puis sélectionnez l'onglet **Advanced** (Avancé).
- Propriétés d'affichage X
  - Dans l'écran **X Preferences** (Préférences X), paramétrez la taille de la police sur **12**.

Paramètres de Novell NetWare

Pour optimiser les performances, utilisez les paramètres suivants :

Propriétés d'affichage du serveur

- Résolution : 800 x 600 pixels ou moins
- 256 couleurs

Touches d'activation de la console distante

La fonction Remote Console Hot keys (Touches d'activation de la console distante) permet de définir jusqu'à six combinaisons de touches multiples pouvant être affectées à chaque touche d'activation (« Touches d'activation prises en charge », page 86). Lorsque vous appuyez sur une touche d'activation dans la console distante, au niveau des systèmes clients, la combinaison de touches définie (toutes les touches enfoncées simultanément) est transmise au serveur hôte distant à la place de la touche d'activation.

Les touches d'activation de la console distante sont actives durant une session de console distante via l'applet Remote Console et pendant une session de console distante texte via un client Telnet.

Pour définir une touche d'activation de la console distante :

1. Cliquez sur **Remote Console Hot Keys** (Touches d'activation de la console distante) sous l'onglet Remote Console (Console distante).
2. Sélectionnez la touche d'activation à définir et utilisez les zones contextuelles pour sélectionner la combinaison de touches à transmettre au serveur hôte lorsque vous appuyez sur la touche d'activation.
3. Cliquez sur **Save Hot Keys** (Enregistrer les touches d'activation) lorsque vous avez fini de définir les combinaisons de touches.

L'écran Remote Console Hot Keys (Touches d'activation de la console distante) propose aussi l'option Reset Hot Keys (Réinitialiser touches d'activation). Cette option efface toutes les entrées des champs de touches d'activation. Cliquez sur **Save Hot Keys** (Enregistrer touches d'activation) pour enregistrer les champs effacés.

Touches d'activation prises en charge

La page Program Remote Console Hot Keys (Touches d'activation de la console distante du programme) permet de définir jusqu'à 6 jeux différents de touches d'activation à utiliser durant une session de console distante. Chaque touche d'activation représente une combinaison de 5 touches différentes qui sont envoyées sur la machine hôte toutes les fois que vous appuyez sur une touche d'activation pendant une session de console distante. Les touches sélectionnées ainsi combinées (toutes les touches doivent être activées en même temps) sont transmises en une seule fois. Pour plus d'informations, reportez-vous à la section « Touches d'activation de la console distante » (page 85). Le tableau suivant dresse la liste de touches disponibles pour être utilisées dans les combinaisons de séquences de touches d'activation de la console distante.

ESC	F12	:	o
L_ALT	" " (Espace)	<	p
R_ALT	!	>	q
L_SHIFT (L_MAJ)	#	=	r
R_SHIFT (R_MAJ)	$	?	s
INS (INSER)	%	@	t
DEL (SUPPR)	&	[	u
HOME (ORIGINE)	~	]	v
END (Fin)	(	\	w
PG UP (PG PRÉC)	)	^	x
PG DN (PG SUIV)	*	_	y
ENTER (ENTRÉE)	+	a	z
TAB	-	b	{
BREAK	.	c	}
F1	/	d	|
F2	0	e	;
F3	1	f	‘
F4	2	g	L_CTRL
F5	3	h	R_CTRL
F6	4	i	NUM PLUS
F7	5	j	NUM MINUS
F8	6	k	SCRL LCK (ARRÊT DÉFIL)

F9	7	l	BACKSPACE (RETOUR ARRIÈRE)
F10	8	m	SYS RQ
F11	9	n	

Modes simple et double curseur de la console graphique distante

La console graphique distante peut utiliser les modes simple ou double curseur. Une JVM appropriée peut s'avérer nécessaire pour la prise en charge.

Mode curseur simple

Le mode curseur simple signifie que le curseur local ne s'affiche pas lorsque le curseur de la souris se trouve dans l'écran Remote Console (Console distante). La nécessité de synchroniser les curseurs étant éliminée, la navigation est facilitée sur l'écran de la console distante.

Sur le client, téléchargez et installez la machine virtuelle Java™ (JVM) version 1.3.1_02 pour Microsoft® Internet Explorer ou Java™ 1.4.2 Runtime Environment, Édition standard pour les navigateurs Linux. Le serveur distant ne nécessite aucun autre logiciel pour activer un pointeur de souris unique.

Les liens permettant de télécharger les Machines virtuelles requises sont disponibles dans l'écran Remote Console Information (Informations sur la console distante).

Vous serez redirigé depuis le site principal vers le site Web de Java (http://java.sun.com). HP vous recommande d'utiliser la version spécifiée dans les pages d'aide de la console distante. Vous pouvez obtenir la version spécifiée de Microsoft® Internet Explorer à partir du site Web de Java (http://java.sun.com) ou du CD SmartStart.

Mode curseur double

Toutes les fonctions présentées dans la section « Remote Console » (Console distante) (page 80) sont également disponibles avec l'option double curseur. Lorsque vous sélectionnez cette option, deux curseurs s'affichent à l'écran : le curseur principal et un curseur secondaire. Lorsque le curseur principal passe sur la fenêtre Remote Console (Console distante), le curseur secondaire le suit.

Le curseur de souris de l'ordinateur client s'affiche dans Remote Console (Console distante) sous la forme d'une croix. Certains utilisateurs de iLO préfèrent voir exactement à quel endroit se trouve le curseur de souris de l'ordinateur client. Pour des performances optimales, configurez l'écran de votre système d'exploitation hôte tel qu'indiqué dans la section « Optimisation des performances de la fonction Graphical Remote Console (Console graphique distante) » (page 82).

L'option double curseur est la seule option disponible dans l'option Remote Console (Console distante) pour clients Microsoft® Windows si vous choisissez de ne pas télécharger une mise à jour de Java™ Runtime Environment. Cette option est prise en charge par la Machine virtuelle Java™ version 1.1 et ultérieure. Pour synchroniser les curseurs distant et local en cas de désynchronisation :

1. Cliquez sur le bouton droit de la souris et déplacez le pointeur local afin de le ramener vers le curseur de la souris du serveur distant.

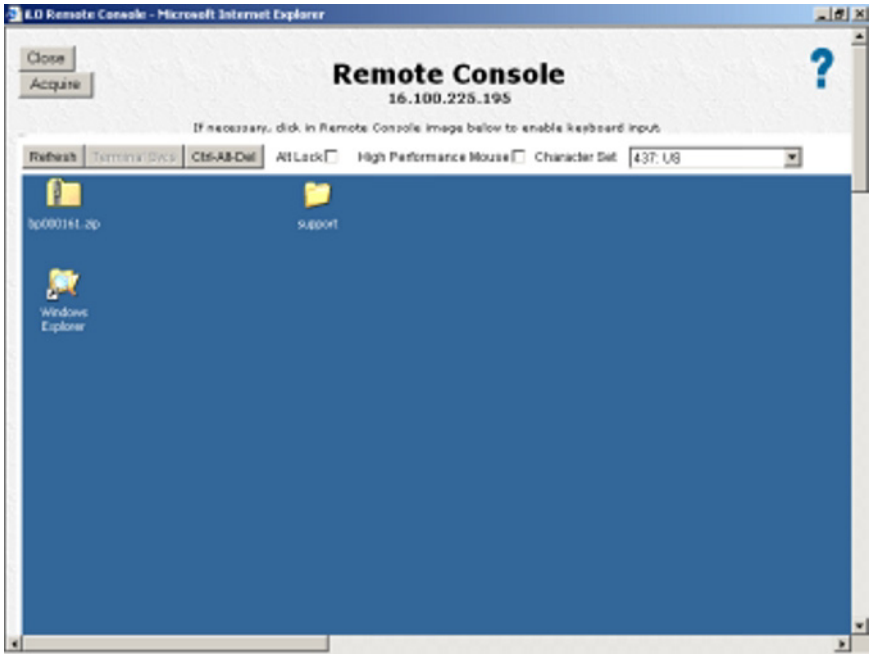
2. Tout en maintenant la touche **Ctrl** enfoncée, amenez le curseur local en forme de croix sur le curseur du serveur distant.

L'option double curseur a l'avantage de vous permettre de voir quand le curseur sort de la fenêtre de l'applet Remote Console. Dans le cas des systèmes d'exploitation basés sur du texte, HP vous recommande d'utiliser le mode double curseur.

En mode double curseur, le curseur local prend la forme du curseur distant. Le curseur s'affiche sous la forme d'un curseur simple si le curseur local et le curseur distant s'alignent parfaitement et que l'accélérateur est défini à Full (Complet) sur le serveur géré.

Acquisition de la console distante

Lorsque la valeur du paramètre Enable Remote Console Acquire (Activer l'acquisition de la console distante) dans la page Global Settings (Paramètres généraux) est définie sur Yes (Oui), un bouton Acquire (Acquérir) est disponible dans la page Remote Console (Console distante). Si vous avez ouvert cette dernière et êtes alors informé qu'un autre utilisateur est en train d'utiliser la console distante, l'action de cliquer sur le bouton Acquire (Acquérir) mettra fin à la session de console distante de l'utilisateur en question et démarrera une session de console distante dans votre fenêtre en cours.



Lorsque vous cliquez sur Acquire (Acquérir), vous êtes invité à confirmer que vous souhaitez interrompre la session de l'utilisateur tiers. Ce dernier reçoit alors un avertissement l'informant qu'un tiers a acquis la session de console distante après avoir perdu la connexion. Aucun avertissement préalable n'est émis. Une fois que vous avez confirmé que vous souhaitez poursuivre l'opération d'acquisition, vous êtes informé, par une fenêtre d'alerte, que l'opération peut prendre 30 secondes ou plus pour être réalisée. Ne cliquez pas à nouveau sur le bouton Acquire (Acquérir) pendant ce laps de temps.

Seule une commande Acquire (Acquérir) est autorisée par utilisateur et par période de cinq minutes. Si un autre utilisateur a récemment acquis la console distante, le fait de cliquer sur le bouton Acquire (Acquérir) peut générer une page vous informant que la période de désactivation de l'acquisition de cinq minutes est en vigueur. Fermez la fenêtre et relancez la console distante pour réessayer. Le bouton Acquire (Acquérir) est désactivé dans la nouvelle page jusqu'à expiration de la période désactivation de l'acquisition. Lorsque le bouton Acquire (Acquérir) est activé (cela se produit automatiquement, vous n'avez pas besoin de rafraîchir la page), vous pouvez tenter d'acquérir à nouveau la console distante.

Une seule tentative d'acquisition peut être effectuée par fenêtre de session de console distante. Si vous êtes parvenu à acquérir la console distante et que quelqu'un l'acquiert à son tour à vos dépens, vous devez ouvrir une nouvelle fenêtre de console distante afin de tenter d'en acquérir une nouvelle session.

Virtual Serial Port (Port série virtuel)

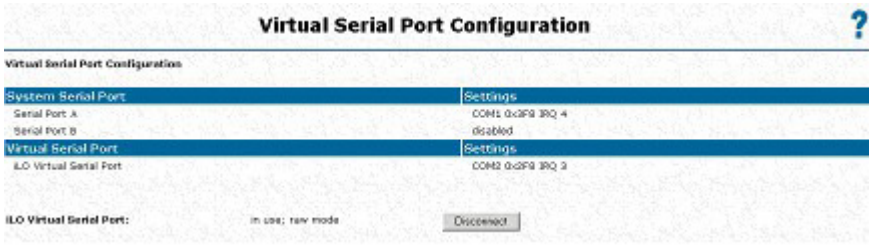
La fonction Virtual Serial Port (Port série virtuel) est un flux bidirectionnel de données du flux de données apparaissant sur le port série du serveur via une applet Java™ qui active une connexion vers le port série du serveur. L'applet Java™ propose une émulation de terminal VT320 afin d'accéder à des applications configurées pour le port série. Vous pouvez l'exploiter tel quel si une connexion série physique est présente sur le port série du serveur. Trois types de données peuvent apparaître sur le port série d'un serveur ProLiant :

- Console Windows® EMS
- Session utilisateur Linux via tty série (ttyS0)
- Boîte de dialogue System POST (Test POST du système), si la redirection de la console série BIOS est activée

Si la fonction Remote Console Data Encryption (Codage données de console distante) est activée, le flux de données du port série virtuel est codé au moment du transfert des données entre le système iLO et l'applet d'affichage.

La configuration du port série affiche les informations de configuration du serveur, les ports série disponibles et l'état du port série virtuel. L'état apparaît comme suit :

- Available (Disponible) : Le port série virtuel n'est pas utilisé
- In use (En cours d'utilisation) : Mode normal lorsque le port série virtuel est connecté normalement
- In use (En cours d'utilisation) : Mode brut lorsque l'utilitaire WiLODbg.exe est utilisé pour la connexion



Lorsque le port série virtuel est utilisé, le bouton Disconnect (Déconnecter) est activé et peut être utilisé pour mettre fin à tout type de connexion de port série virtuel.

Console Windows® EMS

Lorsqu'elle est activée, la console Windows® EMS permet d'exécuter l'EMS (Emergency Management Services) lorsque des fonctions vidéo, des drivers de périphérique ou d'autres fonctionnalités du système d'exploitation empêchent le fonctionnement normal du système et l'exécution d'actions correctives normales.

Cependant, iLO vous permet d'utiliser EMS sur le réseau à l'aide d'un navigateur Web. La fonction Microsoft® EMS permet d'afficher les processus en cours d'exécution, de modifier leur priorité et de les arrêter. La console EMS et la console distante iLO peuvent être utilisées simultanément.

Le port série Windows® EMS doit être activé via l'utilitaire RBSU du système hôte. La configuration permet d'activer ou de désactiver le port EMS, ainsi que de sélectionner le port COM. Le système iLO détecte automatiquement si le port EMS est activé ou désactivé et le port COM sélectionné.

Pour accéder à l'invite `SAC>`, il peut s'avérer nécessaire de taper `Enter` après s'être connecté via la console du port série virtuel.

Pour plus d'informations sur l'utilisation des fonctions EMS, reportez-vous à la documentation de Windows® Server 2003.

Mode brut de port série virtuel

Vous pouvez utiliser la fonction de port série virtuel de iLO pour connecter un débogueur de noyau Windows® à partir d'un client distant utilisant WiLODbg.exe. WiLODbg.exe contourne le décodage des octets par le microprogamme iLO. Une fois le décodage des octets contourné, le port série virtuel passe en mode RAW (non-traité) et directement envoyé au port série.

WiLODbg.exe est un utilitaire qui est exécuté sur un système client avec l'application Microsoft® WinDBG.exe ou KD.exe installée. Lorsque vous exécutez WiLODbg.exe, il établit une connexion de port série virtuel vers iLO et active le mode RAW. WiLODbg.exe démarre également automatiquement WinDBG.exe avec les commutateurs appropriés nécessaires pour que WinDBG.exe se connecte au périphérique iLO distant.

Pour configurer le serveur, vous devez configurer l'utilitaire RBSU pour celui-ci :

1. Définissez le port série virtuel sur **Enable (**Activer).
2. Définissez le port de console série sur **Disable BIOS** (Désactiver le BIOS) ou configurez-le sur le même port qu'un port série intégré.
3. Définissez la console EMS sur **Disable EMS** (Désactiver EMS) ou configurez-la sur le même port qu'un port série intégré.
4. Définissez le port de débogage Microsoft® Windows® sur le même port que le port série virtuel. Vous pouvez utiliser la commande bootcfg ou modifier le fichier boot.ini.

   Exemple d'utilisation de la commande `bootcfg` :

   À l'invite de commande sur un serveur Windows®, entrez la commande suivante :

   ```
   Bootcfg /debug on /port com2 /baud 115200 /id 1
   ```

   Exemple de fichier boot.ini :

   ```
   [boot loader]
   timeout=5
   default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
   [operating systems]
   multi(0)disk(0)rdisk(0)partition(1)\WINDOWS=«Windows Debug (com2)»
   /fastdetect /debug /debugport=com2 /baudrate=115200
   ```

   Si le serveur est configuré en mode de débogage et qu'une connexion de port série virtuel normale est établie au démarrage du serveur, plusieurs octets de données de débogage sont envoyés au client du port série virtuel. Pour éviter ceci, ne démarrez pas le serveur en mode de débogage lorsqu'une connexion de port série virtuel normale est utilisée.

La configuration du port série affiche les informations de configuration du serveur, les ports série disponibles et l'état du port série virtuel. L'état apparaît comme suit :

- Available (Disponible) : Le port série virtuel n'est pas utilisé
- In use (En cours d'utilisation) : Mode normal lorsque le port série virtuel est connecté normalement
- In use (En cours d'utilisation) : Mode brut lorsque l'utilitaire WiLODbg.exe est utilisé pour la connexion

Lorsque le port série virtuel est utilisé, le bouton Disconnect (Déconnecter) est activé et peut être utilisé pour mettre fin à tout type de connexion de port série virtuel. L'utilisation des fonctions Disconnect (Déconnecter) pour mettre fin à une connexion de port série virtuel établie à l'aide de SSH déconnecte complètement la connexion SSH et ne revient pas à l'invite `</>hpiLO->`. Une déconnexion similaire se produit si la connexion de port série virtuel est établie à l'aide de telnet. Si une applet de connexion série distante est utilisée pour réaliser la connexion à partir d'un navigateur, l'applet est déconnectée. La fenêtre de l'applet doit être fermée et rouverte pour réétablir la connexion série distante.

Utilisation d'un débogueur de noyau Windows distant

Pour démarrer un débogueur de noyau Windows®, vous devez lancer l'utilitaire WiLODbg.exe sur un système client doté de Microsoft® WinDBG.exe ou KD.exe installé, puis redémarrer le serveur distant en mode de débogage pour relier le débogueur. WiLODbg démarre automatiquement WinDBG.exe ou KD.exe. Par exemple :

```
WiLODbg <Adresse IP>[ -c Ligne_commande][ -e][ -k][ -p Mot_passe]
[ -s Numéro_socket][
 -t][ -u Nom_utilisateur]
Si un paramètre comporte un espace, entourez-le de guillemets.
```

Paramètres obligatoires :

`Adresse IP = <Chaîne>` - Adresse IP au format en points ou nom UNC complet. <Chaîne> = une série de caractères. Les paramètres obligatoires doivent apparaître dans l'ordre illustré dans l'exemple.

Paramètres facultatifs :

- `-c Ligne_commande = <Chaîne>` - Fournit des paramètres de ligne de commande supplémentaires au débogueur sélectionné. Si des espaces ou des tirets (-) sont présents, entourez-les de guillemets anglais. <Chaîne> = une série de caractères.
- `-e = <Booléen>` - Active le cryptage pour la liaison de communication. Le cryptage fonctionne uniquement avec l'option telnet dans cette version. Il est désactivé par défaut.
- `-k = <Booléen>` - Utilise KD au lieu de WinDbg. La valeur par défaut est d'utiliser WinDbg.
- `-p Mot_passe = <Chaîne>` - Définit le mot de passe à utiliser pour la connexion à iLO. Si non fourni, un mot de passe est demandé. <Chaîne> = une série de caractères.
- `-s Numéro_socket = <Entier>` - Définit le numéro de socket pour la connexion à iLO. Le numéro de socket doit correspondre au paramètre de port de données série brut sur la carte iLO à laquelle vous vous connectez. La socket 3002 est la valeur par défaut. `<Entier> = [signe]chiffres`.
- `-t = <Booléen>` - Utilise une connexion telnet indirectement via cet utilitaire à partir du débogueur. La connexion de socket à la socket 3002 est le paramètre par défaut.
- `-u Nom_utilisateur = <Chaîne>` - Définit le nom d'utilisateur pour la connexion à iLO. Si non fourni, un nom d'utilisateur est demandé. <Chaîne> = une série de caractères. Les options peuvent apparaître dans tout ordre.

Exemples de ligne de commande :

- Pour se connecter à iLO à l'adresse 16.100.226.57, valider l'utilisateur avec le nom d'utilisateur admin et le mot de passe mon_mot_passe, puis démarrer WinDBG.exe avec la ligne de commande supplémentaire :

  ```
  wilodbg 16.100.226.57 -c «-b» -u admin -p mon_mot_passe
  ```

  Cet exemple démarre WinDBG.exe avec une ligne de commande supplémentaire `–b` et utilise une connexion de socket directe de WinDBG.exe vers iLO sur le port 3002.

- Pour se connecter à iLO à l'adresse 16.100.226.57, valider l'utilisateur iLO avec le nom d'utilisateur `admin` et le mot de passe mon_mot_passe, puis démarrer `kd` avec une ligne de commande supplémentaire `-b` pour `kd` :

  ```
  wilodbg 16.100.226.57 - k c «-b» -u admin -p mon_mot_passe-s 7734
  ```

  Cet exemple démarre kd avec une ligne de commande supplémentaire – `b` pour `kd`, et utilise une connexion de socket directe de `kd` iLO sur le port 7734. Pour utiliser cet exemple, vous devez configurer iLO pour utiliser le port 7734.

- Pour se connecter à iLO à l'adresse 16.100.226.57 et demander un nom d'utilisateur et un mot de passe :

  ```
  wilodbg 16.100.226.57 -c «-b» -t -e
  ```

  Cet exemple démarre WinDBG.exe avec une ligne de commande supplémentaire `–b`, utilise une connexion telnet cryptée entre WiLODbg et iLO et passe les données WinDBG.exe via l'utilitaire à la connexion telnet cryptée.

Virtual Serial Port (Port série virtuel) et Linux

Le périphérique `/dev/ttyS0`, lorsqu'il est configuré, permet d'obtenir des sessions `tty` série via la console du port série virtuel iLO. Le système Linux doit être configuré correctement. Reportez-vous à la mise en œuvre spécifique à votre système Linux pour obtenir les commandes appropriées. Les instructions générales sont les suivantes :

- La fonction Virtual Serial Port (Port série virtuel) doit être activée à l'aide de l'utilitaire RBSU du système hôte. La configuration permet d'activer ou de désactiver la fonctionnalité Remote Virtual Serial Port (Port série virtuel distant). Pour plus d'informations, reportez-vous à la section relative à l'utilitaire RBSU du système hôte dans la documentation spécifique au serveur. En général, l'utilitaire RBSU contient l'onglet BIOS Serial Console/EMS Support (Console série BIOS/Prise en charge EMS). Si vous sélectionnez cet onglet, l'onglet EMS Console (Console EMS) apparaît et doit être configuré à Remote (Distant). Cela permet d'activer les options Virtual Serial Port (Port série virtuel) et Windows® EMS Console (Console Windows® EMS).
- Pour démarrer une session interface utilisateur sous la configuration UART, il faut lancer le processus Linux approprié. Pour ce faire, vous pouvez utilisez le shell, mais ce processus est généralement configuré dans le fichier /etc/inittab afin de le rendre disponible après l'initialisation du noyau du système.

  ```
  s0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
  ```

- Linux s'attend à ce que le port série apparaisse dans l'adresse standard d'E/S UART ; toutefois, LOM_short_name> présente le port à l'adresse non standard 0x408. Pour en informer Linux, utilisez la commande ci-dessous. Cette commande peut être placée dans le fichier rc.serial généralement appelé à partir de /etc/rc.local au démarrage du système.

  ```
  setserial /dev/ttyS0 uart 16550A port 0x0408 irq 4
  ```

Linux exige que le terminal soit répertorié dans le fichier /etc/securetty pour se connecter. Ajoutez la ligne suivante à la fin du fichier :

```
ttyS0
```

Sur certains systèmes BL p-Class, l'adresse standard d'E/S UART (0x3F8) est utilisée lorsqu'il n'y a pas de conflit. Sur ces systèmes, la commande setserial n'est pas requise.

Prise en charge complète Linux

Par défaut, le port série virtuel utilise l'adresse d'E/S 0x0408 et INTERRUPT 4 pour la communication. Le port série virtuel est configuré et activé lorsque l'utilitaire RBSU iLO est sélectionné et que la fonction Virtual Serial Port (Port série virtuel) est activée. Il s'agit d'une limitation de la fonction Virtual Serial Port (Port série virtuel) pour la prise en charge Linux, car cette adresse d'E/S n'est pas une adresse standard prise en charge. La commande `setserial` permet de configurer agetty, mais le noyau doit être reconstruit afin de prendre en charge GRUB pour la redirection de l'amorçage et du noyau. Pour la configurabilité, des adresses d'E/S UART standards sont fournies dans la version 1.60 du microprogramme iLO, mais une ROM de système hôte compatible est nécessaire. Si une ROM de système hôte compatible est disponible pour le serveur spécifique, la commande `setserial` n'est pas nécessaire, et la redirection d'amorçage GRUB apparaît sur le port série virtuel utilisant le noyau standard.

Port série virtuel et BREAK (SAUT) série

Le port série virtuel iLO prend en charge le BREAK (SAUT) série. L'événement BREAK (SAUT) série peut être transmis au système hôte via le port série virtuel en appuyant sur la séquence de touches **Échap Ctrl+B**. Cette séquence de touches permet à l'applet Virtual Serial Port (Port série virtuel), à Telnet et aux applications SSH fonctionnant sur des réseaux TCP/IP de transmettre l'événement BREAK (SAUT) série à l'hôte lorsque vous utilisez le port série virtuel.

L'événement BREAK (SAUT) série iLO prend en charge la fonction du système d'exploitation Linux de Magic SysRq. Le noyau Linux prend en charge la fonction Magic SysRq sur une console sur tty0 via la combinaison de touches Alt+SysRq. Lorsque le noyau gère une console sur une connexion série, ttyS0 ou autre, l'événement BREAK (SAUT) est utilisé pour mettre en œuvre Magic SysRq.

Lorsque Magic SysRq est correctement configuré :

- La console est définie sur une connexion tty série (ttyS0 ou autre) dans LILO ou GRUB.
- Le noyau approprié est configuré avec with /proc/sys/kernel/sysrq.
- La commande agetty appropriée (ou équivalente) est configurée pour tty série (ttyS0 ou autre).

La séquence de touches Echap Ctrl+B génère un événement BREAK (SAUT) série, ce qui déclenche l'événement Magic SysRq. Une touche Magic SysRq supplémentaire après la séquence de touches Echap Ctrl+B permet de sélectionner une commande spécifique. Reportez-vous à votre documentation Linux pour obtenir des détails et connaître les conséquences de l'activation de Magic SysRq en termes de sécurité.

Périphériques virtuels

L'onglet Virtual Devices (Périphériques virtuels) comporte les options suivantes :

- Virtual Power (Alimentation virtuelle) (page 94)
- Régulateur de puissance pour ProLiant (page 95)
- Virtual Media (Support virtuel) (page 98)
- Virtual Indicators (Témoins virtuels) (page 108)
- Virtual serial port (Port série virtuel) (page 89)

Alimentation virtuelle

Le bouton Virtual Power (Alimentation virtuelle) permet de contrôler l'état d'alimentation du serveur distant et de simuler l'activation de l'interrupteur d'alimentation physique du serveur. Si le serveur hôte distant ne répond pas, cette fonction permet à un administrateur de déclencher un redémarrage à froid ou à chaud pour rétablir la connexion du serveur.

Certaines de ces fonctions n'arrêtent pas le système d'exploitation de façon ordonnée. La fermeture du système d'exploitation doit être initiée à l'aide de la console distante avant d'utiliser le bouton Virtual Power (Alimentation virtuelle).

Utilisez la fonction de rafraîchissement du navigateur pour mettre à jour l'état du voyant d'alimentation.

Pour utiliser le bouton Virtual Power (Alimentation virtuelle), sélectionnez l'option d'alimentation souhaitée, puis cliquez sur **Virtual Power** (Alimentation virtuelle) pour lancer l'option.

Les options d'alimentation disponibles sont les suivantes :

- **Momentary Press** (Pression brève) : cette option simule une brève pression de l'interrupteur d'alimentation. Ce type de pression est habituellement suffisant pour mettre un serveur hors tension s'il est sous tension, ou pour mettre un serveur sous tension s'il est hors tension. Cette option permet d'obtenir la fermeture ordonnée du système d'exploitation, cela dépend du système d'exploitation hôte concerné. Pour utiliser cette option, sélectionnez **Momentary Press** (Pression brève) et cliquez sur le bouton **Virtual Power** (Alimentation virtuelle).
- **Press and Hold** (Pression prolongée) : cette option simule une pression de l'interrupteur d'alimentation d'une durée de six secondes. Ce type de pression permet de forcer la mise hors tension lorsque le système d'exploitation ne répond pas à une brève pression.

  Cette fonction n'arrête pas le système d'exploitation de façon ordonnée.
- **Cold Boot of system** (Démarrage à froid du système) : cette option met le serveur hors tension, puis sous tension. Pour redémarrer le système, sélectionnez **Cold Boot of system** (Démarrage à froid du système) et cliquez ensuite sur le bouton **Virtual Power** (Alimentation virtuelle). L'alimentation du système est immédiatement coupée. Il redémarre après environ six secondes. Cette option n'apparaît pas lorsque le serveur est hors tension.
- **Warm Boot of system** (Démarrage à chaud du système) : cette option provoque la réinitialisation du système, sans le mettre hors tension. Pour utiliser cette option, sélectionnez **Warm Boot of system** (Démarrage à chaud du système) et cliquez sur le bouton **Virtual Power** (Alimentation virtuelle). Cette option n'apparaît pas lorsque le serveur est hors tension.

  Cette fonction n'arrête pas le système d'exploitation de façon ordonnée.
- **Manual Override for BL p-Class** (Neutralisation manuelle pour BL p-Class) : cette option s'affiche uniquement en cas de connexion à un serveur ProLiant BL p-Class. Elle vous permet de forcer la mise sous tension d'un serveur, même si le rack signale une alimentation insuffisante. En effet, si le rack est mal configuré ou qu'il rencontre des problèmes de communication, cela peut empêcher la mise sous tension du serveur, même en cas d'alimentation suffisante. N'utilisez cette option que lorsque vous êtes certain que le rack dispose d'une alimentation suffisante.

  △ **ATTENTION :** il est possible qu'en utilisant l'option **Manual Override for BL p-Class** (Neutralisation manuelle pour BL p_Class), vous mettiez sous tension des serveurs qui nécessitent une alimentation supérieure à celle disponible via les modules d'alimentation. Ceci peut provoquer la perte de tous les serveurs sur le rack, des pannes de serveurs et la perte ou la corruption de données. HP vous recommande de corriger les problèmes de configuration ou de communication afin d'assurer un fonctionnement fiable.
- **Automatically Power On Server** (Mise sous tension automatique du serveur) : cette option met automatiquement le serveur sous tension dès que celui-ci reçoit du courant, si toutefois l'option Yes (Oui) est sélectionnée. Du courant est reçu lorsqu'un onduleur est activé après une coupure de l'alimentation. Le serveur est automatiquement mis sous tension et entame le processus d'amorçage normal.

Power regulator for ProLiant (Régulateur d'alimentation pour ProLiant)

Vous pouvez activer la page Power regulator for ProLiant (Régulateur d'alimentation pour ProLiant) en souscrivant à la licence du pack iLO Advanced, disponible en option. Si vous ne possédez pas cette licence, le message `iLO feature not licensed` (Aucune licence pour cette fonction iLO) s'affiche.

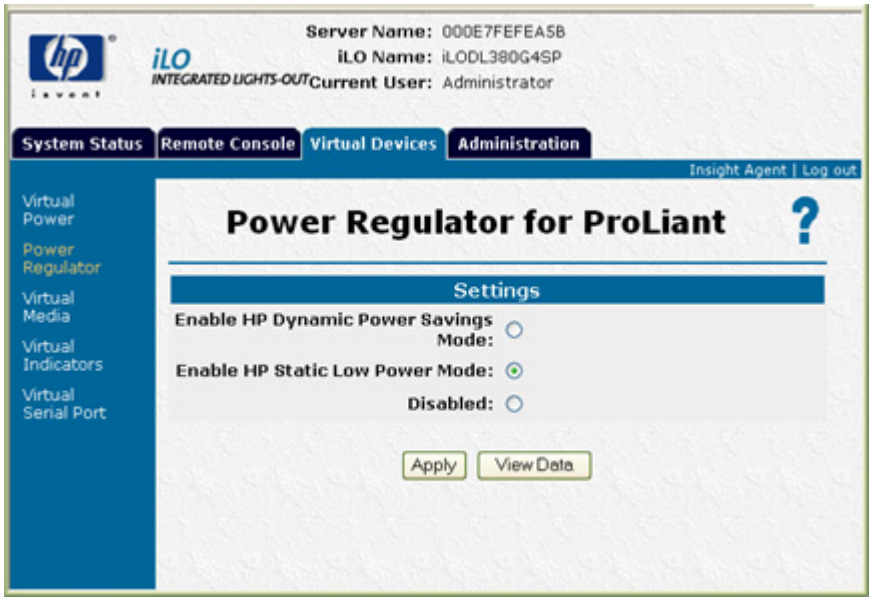
La page Power regulator for ProLiant (Régulateur d'alimentation pour ProLiant) permet la modification dynamique des niveaux de fréquence et de tension des processeurs sur la base des conditions de fonctionnement afin d'offrir des économies d'énergie avec un effet minimal sur les performances. Les états de la tension et de la fréquence des processeurs prenant en charge la fonction de régulation sont prédéfinis et appelés p-states. Le logiciel peut faire basculer dynamiquement le processeur d'un état (p-state) à l'autre. P-0 est la combinaison fréquence/tension la plus élevée prise en charge par le processeur. La modification du p-state du processeur en fonction de l'utilisation de l'unité centrale réduit la tension et la fréquence du processeur lorsque le système est inactif, et réciproquement, permettant ainsi une réelle économie d'énergie tout en évitant une diminution des performances. Pour permettre au processeur de définir lui-même le niveau d'alimentation en fonction de l'utilisation, sélectionnez **Enable HP Dynamic Power Savings Mode** (Activer le mode Alimentation dynamique HP). Pour attribuer au processeur la puissance minimale, sélectionnez **Enable HP Static Low Power Mode** (Activer le mode Alimentation faible HP). Pour définir la puissance maximale pour le processeur, sélectionnez **Disabled** (Désactivée).

REMARQUE : le processeur système détermine si l'option Power Regulator (Régulateur d'alimentation) est prise en charge. Elle est disponible sur les serveurs suivants uniquement :

- ProLiant ML350 G4
- ProLiant ML350 G4p
- ProLiant ML320 G3
- ProLiant DL360 G4
- ProLiant DL360 G4p
- ProLiant DL380 G4
- ProLiant DL380 G4p
- ProLiant BL20p G3
- ProLiant ML570 G3
- ProLiant DL580 G3

La révision du micrologiciel de la ROM système doit être datée au minimum du 01/06/05. Si votre processeur système ne prend pas en charge l'option de régulation de l'alimentation (différents p-states de processeur), la page Power Regulator (Régulateur d'alimentation) affiche le message suivant : « `HP Power Regulator for ProLiant not supported by iLO` (Régulateur d'alimentation HP pour Proliant non pris en charge par iLO) ».

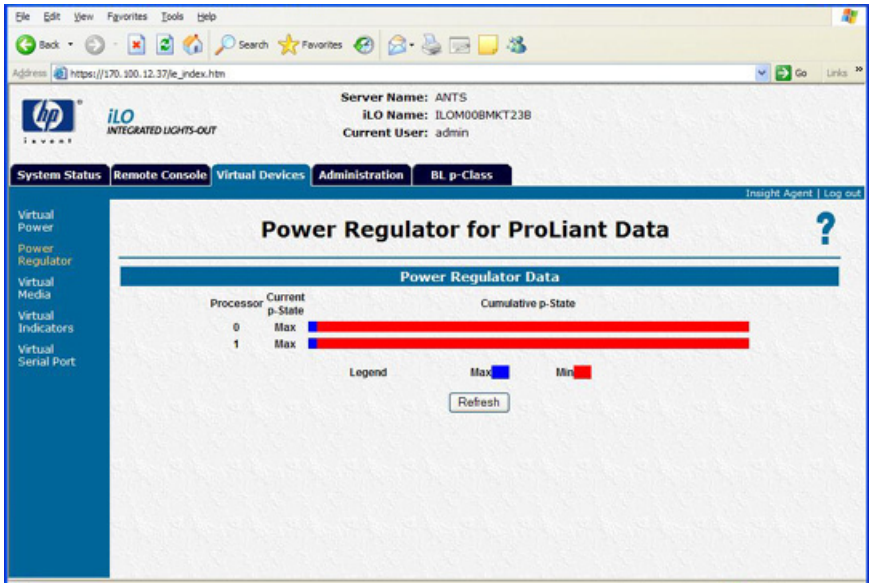
Les paramètres de l'option Power Regulator for ProLiant (Régulateur d'alimentation pour Proliant) peuvent être appelés via iLO uniquement sur les serveurs disposant de la prise en charge de la régulation d'alimentation de la ROM hôte. Certains serveurs peuvent prendre en charge la modification du niveau d'alimentation du processeur via l'utilitaire RBSU système. Consultez le manuel de l'utilisateur de votre système pour plus d'informations.



- L'option **Enable HP Dynamic Power Savings Mode** (Activer le mode Alimentation dynamique HP) permet au processeur de définir lui-même le niveau d'alimentation en fonction de l'utilisation.
- L'option **Enable HP Static Low Power Mode** (Activer le mode Alimentation faible HP) attribue au processeur la puissance minimale.
- L'option **Disabled** (Désactivée) offre au processeur la puissance maximale.

Cliquez sur **Apply** (Appliquer) pour enregistrer le paramètre souhaité. Le serveur doit être redémarré pour que le nouveau paramètre soit validé. Si le serveur ne prend pas en charge cette fonctionnalité, le message suivant s'affiche sur la page : « `HP Power Regulator for ProLiant not supported by iLO` » (Régulateur d'alimentation HP pour Proliant non pris en charge par iLO).

Cliquez sur **View Data** (Afficher les données) pour accéder à la page Power Regulator for ProLiant Data (Données du régulateur d'alimentation pour ProLiant) et afficher le p-state en cours, ainsi qu'une moyenne continue du pourcentage de temps que chacun des processeurs a passé dans chacun des états p-state. La page des données requiert le pack iLO Advanced. Reportez-vous à la page Licensing (Informations sur la licence) pour plus d'informations sur l'obtention d'une licence pour le pack iLO Advanced.



Les données de p-state de chaque processeur logique dans le système hôte sont collectées par iLO lorsque le système hôte est mis sous tension et qu'il n'est pas dans l'état POST (auto-test de mise sous tension). L'état p-state en cours et une moyenne mobile des données collectées pendant les 12 dernières heures sont affichées. Une barre multicolore présente le pourcentage de temps que chacun des processeurs a passé dans chacun des états p-state. Les données sont réinitialisées lors du redémarrage d'iLO.

Support virtuel

La fonction Virtual Media (Support virtuel) peut être activée par l'acquisition de la licence du pack iLO Advanced, disponible en option. Si vous ne possédez pas cette licence, le message `iLO feature not licensed` (Aucune licence pour cette fonction iLO) s'affiche.

L'option iLO Virtual Media (Support virtuel iLO) vous propose un lecteur de disquette, un lecteur de clé USB et un lecteur de CD/DVD virtuels, pour amener un serveur hôte distant à s'initialiser et à utiliser un support standard depuis n'importe quel endroit du réseau. Les lecteurs Virtual Media (Support virtuel) sont disponibles lorsque le système hôte démarre. Les lecteurs de support virtuel iLO se connectent au serveur hôte à l'aide de la technologie USB. L'utilisation de la technologie USB apporte aussi de nouvelles fonctionnalités aux périphériques de support virtuel iLO lorsqu'ils sont connectés à des systèmes d'exploitation qui prennent en charge USB. Les différents systèmes d'exploitation offrent des niveaux de prise en charge USB variables. La fonction iLO Virtual Media (Support virtuel iLO) peut être configurée pour traiter ces différents niveaux de prise en charge (« Prise en charge USB par les systèmes d'exploitation », page 106).

- Si la fonctionnalité Virtual Floppy/USB Key (Disquette/Clé USB virtuelle) est activée, le lecteur de disquette et de clé USB sera inaccessible depuis le système d'exploitation client.
- Si la fonctionnalité Virtual CD (CD virtuel) est activée, l'unité de CD-ROM sera inaccessible depuis le système d'exploitation client.

Sous certaines conditions, vous pouvez accéder au lecteur de disquette et de clé USB virtuel à partir du système d'exploitation client lorsque celui-ci est connecté. Cependant, il est important de ne pas tenter d'accéder à la disquette ou à la clé USB virtuels depuis un système d'exploitation client lorsque celui-ci est connecté en tant que périphérique de support virtuel, au risque de perdre les données contenues sur l'unité de disquette. Veillez toujours à déconnecter le support virtuel avant d'essayer d'y accéder à partir d'un système d'exploitation client.

Utilisation des périphériques de support virtuel iLO

Vous pouvez accéder à un support virtuel sur un serveur hôte à partir d'un client via une interface graphique à l'aide d'une applet Java™ et via une interface de scripts à l'aide d'un moteur XML.

Pour accéder aux périphériques de support virtuel iLO à l'aide de l'interface graphique, sélectionnez l'option **Virtual Media** (Support virtuel) sous l'onglet Virtual Devices (Périphériques virtuels). Une applet est chargée afin de prendre en charge le périphérique de disquette virtuelle ou de CD/DVD-ROM virtuelle.

Lecteur de disquette/USB virtuel iLO

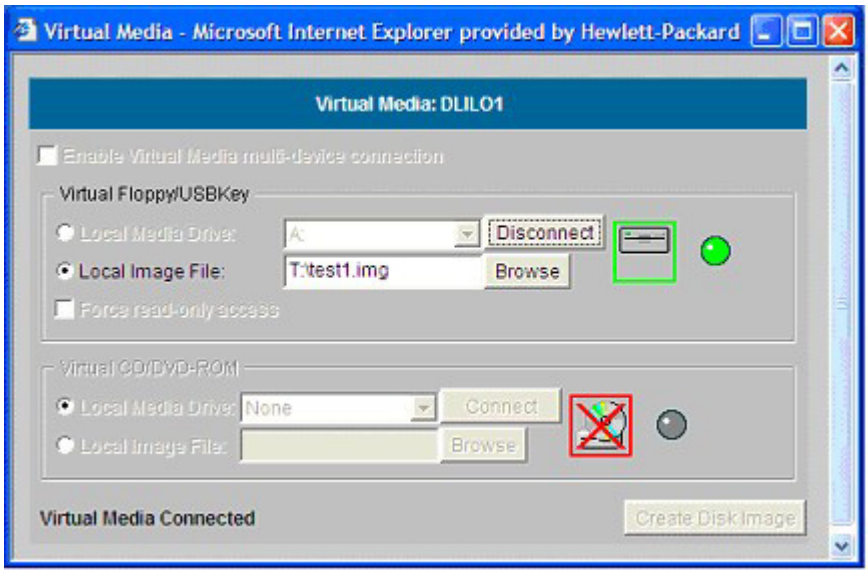
L'unité de disquette virtuelle iLO est disponible pour tous les systèmes d'exploitation au moment de l'initialisation du système. L'initialisation depuis la disquette virtuelle iLO permet notamment de mettre à niveau la mémoire ROM du système hôte, d'installer un système d'exploitation depuis des unités en réseau ou d'effectuer une récupération après un incident survenu sur un système d'exploitation. Si le système d'exploitation du serveur hôte prend en charge les périphériques de mémoire de masse USB, le lecteur de disquette/clé USB virtuel iLO est alors également disponible après le chargement du système d'exploitation du serveur hôte. Le lecteur de disquette/clé USB virtuel iLO peut notamment vous servir lorsque le système d'exploitation du serveur hôte exécute une mise à niveau des drivers de périphérique, crée une disquette de réparation d'urgence et exécute d'autres tâches. Le fait de disposer d'une disquette virtuelle lorsque le serveur est en cours d'utilisation peut s'avérer particulièrement utile si vous devez diagnostiquer et résoudre un problème au niveau du driver de la carte réseau.

L'option Virtual Floppy/USB Key peut être l'unité de disquette ou le lecteur de clé USB physique sur lequel vous exécutez le navigateur Web ou un fichier image sur votre disque dur local ou sur une unité réseau. Pour obtenir des performances optimales, HP recommande d'utiliser des fichiers image locaux stockés sur le disque dur du PC client, ou sur une unité réseau accessible via une liaison haut débit.

Pour utiliser une unité de disquette ou un lecteur de clé USB physique dans votre ordinateur client, procédez comme suit :

1. Dans la section Virtual Floppy/USBKey, sélectionnez **Local Media Drive** (Unité de support locale).
2. Dans le menu déroulant, sélectionnez la lettre correspondant à l'unité locale de disquette ou de clé USB physique souhaitée du PC client. Pour vous assurer que la disquette ou le fichier image source n'est pas modifié pendant l'utilisation, sélectionnez l'option **Force read-only access** (Forcer l'accès en lecture seule).
3. Cliquez sur **Connect** (Connecter).

L'icône et le voyant du lecteur connecté changent pour refléter l'état en cours de l'unité de disquette virtuelle.



Pour utiliser un fichier image :

1. Dans la section Virtual Floppy/USBKey de l'applet Virtual Media, sélectionnez **Local Image File** (Fichier image local).
2. Saisissez le chemin et le nom de fichier de l'image dans la zone de texte ou cliquez sur **Browse** (Parcourir) pour trouver le fichier image à l'aide de la boîte de dialogue Choose Disk Image File (Choisir le fichier d'image disque). Pour vous assurer que la disquette ou le fichier image source n'est pas modifié pendant l'utilisation, sélectionnez l'option **Force read-only access** (Forcer l'accès en lecture seule).
3. Cliquez sur **Connect** (Connecter).

L'icône et le voyant du lecteur connecté changent pour refléter l'état en cours de l'unité de disquette ou de clé USB virtuelle. Une fois les périphériques virtuels connectés, le serveur hôte peut y accéder jusqu'à ce que vous fermiez l'applet Virtual Media. Lorsque vous avez fini d'utiliser la disquette/clé USB virtuelle, vous pouvez déconnecter le périphérique du serveur hôte ou fermer l'applet.

REMARQUE : l'applet Virtual Media doit rester ouverte dans votre navigateur tant que vous continuez d'utiliser un périphérique de support virtuel.

La disquette/clé USB virtuelle iLO est mise à la disposition du serveur hôte au moment de l'exécution si le système d'exploitation de celui-ci prend en charge les unités de disquette ou de clé USB. Reportez-vous à la section « Prise en charge USB par les systèmes d'exploitation » (page 106) pour plus d'informations sur les systèmes d'exploitation prenant actuellement en charge le stockage de masse USB.

La disquette/clé USB virtuelle iLO est reconnue par votre système d'exploitation au même titre que n'importe quel autre lecteur. Lorsque vous utilisez iLO pour la première fois, le système d'exploitation hôte peut vous demander d'exécuter un Assistant New Hardware Found (Nouveau matériel détecté).

Lorsque vous avez fini d'utiliser le support virtuel iLO et que vous le déconnectez, le système d'exploitation peut vous envoyer un message d'avertissement indiquant le retrait non sécurisé d'un périphérique. Cet avertissement peut être évité à l'aide de la fonction fournie par le système d'exploitation, qui permet d'arrêter le périphérique avant de le déconnecter du support virtuel.

Remarques concernant les systèmes d'exploitation de disquette/clé USB virtuelle

- MS-DOS

  Au cours du démarrage et de sessions MS-DOS, le périphérique de disquette virtuelle apparaît sous forme d'unité de disquette BIOS standard. Ce périphérique apparaît en tant qu'unité A. Si une unité de disquette reliée physiquement existe, elle est obscurcie et indisponible durant cette période. Vous ne pouvez pas utiliser simultanément une unité de disquette physique locale et la fonction Virtual Floppy (Disquette virtuelle).

- Windows® 2000 SP3 ou version ultérieure et Windows Server™ 2003

  Les lecteurs de disquette et de clé USB virtuels s'affichent automatiquement dès que Microsoft® Windows® a reconnu le montage du périphérique USB. Utilisez-les comme vous le feriez d'un périphérique connecté localement.

  Pour utiliser la fonctionnalité Virtual Floppy (Disquette virtuelle) pour recourir à une disquette de drivers lors d'une installation Windows®, désactivez l'unité de disquette intégrée à l'hôte RBSU, car c'est lui qui oblige la disquette virtuelle à apparaître sous la lettre d'unité A.

  Pour utiliser la fonctionnalité Virtual USB Key (Clé USB virtuelle) pour recourir à une disquette de drivers lors d'une installation Windows®, modifiez l'ordre d'initialisation du lecteur de clé USB dans l'utilitaire RBSU du système. HP recommande de placer le lecteur de clé USB en premier dans l'ordre d'initialisation.

- Windows Vista™

  La fonctionnalité Virtual Media ne fonctionne pas correctement sous Windows Vista™ lors de l'utilisation de Internet Explorer 7 avec le mode protégé activé. Si vous tentez d'utiliser un support virtuel avec le mode protégé activé, divers messages d'erreur s'affichent, notamment `could not open cdrom (the parameter is incorrect` (Impossible d'ouvrir le CD-ROM. Paramètre incorrect). Pour utiliser le support virtuel, cliquez sur **Outils/Options Internet/Sécurité**, désactivez l'option **Activer le mode protégé**, puis cliquez sur **Appliquer**. Une fois le mode protégé désactivé, vous devez fermer toutes les instances du navigateur ouvertes, puis redémarrer le navigateur.

- NetWare 6.5

  NetWare 6.5 prend en charge l'utilisation d'unités de disquette et de clé USB. Reportez-vous à la section « Montage d'une disquette/clé virtuelle USB sous NetWare 6.5 » (page 101) pour obtenir des instructions détaillées.

- Red Hat et SUSE Linux

  Linux prend en charge l'utilisation d'unités de disquette et de clé USB. Reportez-vous à la section « Montage d'une disquette/clé virtuelle USB sous Linux » (page 102) pour obtenir des instructions détaillées.

Montage d'une disquette/clé virtuelle USB sous NetWare 6.5

1. Accédez à la carte iLO à l'aide d'un navigateur.
2. Cliquez sur **Virtual Media** (Support virtuel) sous l'onglet Virtual Devices (Périphériques virtuels).
3. Introduisez le support dans l'unité de disquette locale, sélectionnez l'unité de disquette puis cliquez sur **Connect** (Connecter). Vous pouvez également sélectionner une image de disquette à utiliser et cliquer sur **Connect** (Connecter).

Sous NetWare 6.5, tapez la commande `lfvmount` sur la console du serveur pour affecter au périphérique une lettre correspondant à l'unité de disquette.

Le système d'exploitation NetWare 6.5 choisit la première lettre disponible pour l'unité de disquette virtuelle. Les commandes `volumes` peuvent alors être utilisées par la console du serveur pour afficher l'état de montage de cette nouvelle unité.

Lorsque la lettre choisie pour représenter la nouvelle unité s'affiche indiquant que cette dernière est à présent montée, l'unité est alors accessible via l'interface graphique du serveur et la console système.

Lorsque l'unité de disquette virtuelle est montée, si le support est changé dans l'unité de disquette locale, la commande `lfvmount` devra être une nouvelle fois émise à partir de la console du serveur afin que le nouveau support soit visible dans le système d'exploitation NetWare 6.5.

Montage d'un support/clé virtuel USB sous Linux

1. Accédez à la carte iLO à l'aide d'un navigateur.
2. Cliquez sur **Virtual Media** (Support virtuel) sous l'onglet Virtual Devices (Périphériques virtuels).
3. Sélectionnez un lecteur ou une image de disquette.
   a. Pour un lecteur ou une image de disquette, sélectionnez Local Media Drive (Unité de support locale) ou Local Image File (Fichier image local) et cliquez sur **Connect** (Connecter).
   b. Pour un lecteur ou une image de clé USB, sélectionnez Local Image File (Fichier image local) et cliquez sur **Connect** (Connecter).

      Pour un lecteur de clé USB physique, saisissez `/dev/sda` dans la zone de texte Local Image File (Fichier image local).
4. Chargez les drivers USB à l'aide des commandes suivantes :

```
modprobe usbcore
modprobe usb-storage
modprobe usb-ohci
```

5. Chargez le driver de disquettes SCSI à l'aide de la commande suivante :

```
modprobe sd_mod
```

6. Montez le lecteur.
   - Pour monter le lecteur de disquette, utilisez la commande suivante :

     ```
     mount /dev/sda  /mnt/floppy –t vfat
     ```
   - Pour monter le lecteur de clé USB, utilisez la commande suivante :

     ```
     mount /dev/sda1  /mnt/keydrive
     ```

REMARQUE : utilisez la commande `man mount` pour d'autres types de systèmes de fichiers.

L'unité de disquette et de clé peut être utilisée comme un système de fichiers Linux, si elle est formatée comme telle avec la commande `mount`. Cependant, les disquettes de 1,44 Mo de capacité sont en général accessibles à l'aide des utilitaires mtools fournis avec Red Hat et SLES. La configuration des utilitaires mtools par défaut ne reconnaît pas une disquette connectée via l'USB. Pour activer les différentes commandes m permettant d'accéder au périphérique Virtual Floppy (Disquette virtuelle), modifiez le fichier /etc/mtools.conf existant et ajoutez la ligne suivante :

```
drive v: file=«/dev/sda» exclusive
```

Pour activer les différentes commandes mtools permettant d'accéder au lecteur de clé USB virtuel, modifiez le fichier /etc/mtools.conf existant et ajoutez la ligne suivante :

```
drive v: file=«/dev/sda1» exclusive
```

Pour afficher la table des partitions du lecteur de clé USB virtuel afin de rechercher la partition souhaitée, utilisez la commande suivante :

```
fdisk -l /dev/sda
```

Cette modification permet au progiciel mtools d'accéder au périphérique Virtual Floppy (Disquette virtuelle) en le désignant à l'aide de la lettre v. Par exemple :

```
mcopy /tmp/XXX.dat v:
mdir v:
mcopy v:foo.dat /tmp/XXX
```

Changement de disquette

Lorsque vous utilisez l'unité de disquette ou de clé USB virtuelle iLO et que l'unité de disquette physique du client est une unité de disquette USB, les changements de disquette ne sont pas reconnus. Par exemple, dans cette configuration, si une liste des répertoires provient d'une disquette et que vous changez cette dernière, les listes de répertoires ultérieures correspondront à celle de la première disquette utilisée. Si des changements de disque sont nécessaires lors de l'utilisation d'une disquette ou clé USB virtuelle iLO, assurez-vous que la machine client contient une unité de disquette non-USB.

iLO Virtual CD/DVD-ROM (CD/DVD-ROM virtuel iLO)

La fonctionnalité iLO Virtual CD/DVD-ROM est disponible durant le démarrage du serveur pour les systèmes d'exploitation spécifiés dans la section « Prise en charge USB par les systèmes d'exploitation », page 106). L'initialisation depuis le CD-ROM virtuel iLO permet notamment de déployer un système d'exploitation depuis des unités en réseau et d'effectuer une récupération après un incident survenu sur un système d'exploitation.

Si le système d'exploitation du serveur hôte prend en charge les périphériques de mémoire de masse USB, le CD/DVD-ROM virtuel iLO est alors également disponible après le chargement du système d'exploitation du serveur hôte. You can use the iLO Virtual CD/DVD-ROM when the host server operating system is running to upgrade device drivers, install software, and perform other tasks. Le fait de disposer d'un CD/DVD-ROM virtuel lorsque le serveur est en cours d'utilisation peut s'avérer particulièrement utile si vous devez diagnostiquer et résoudre un problème au niveau du driver de la carte réseau.

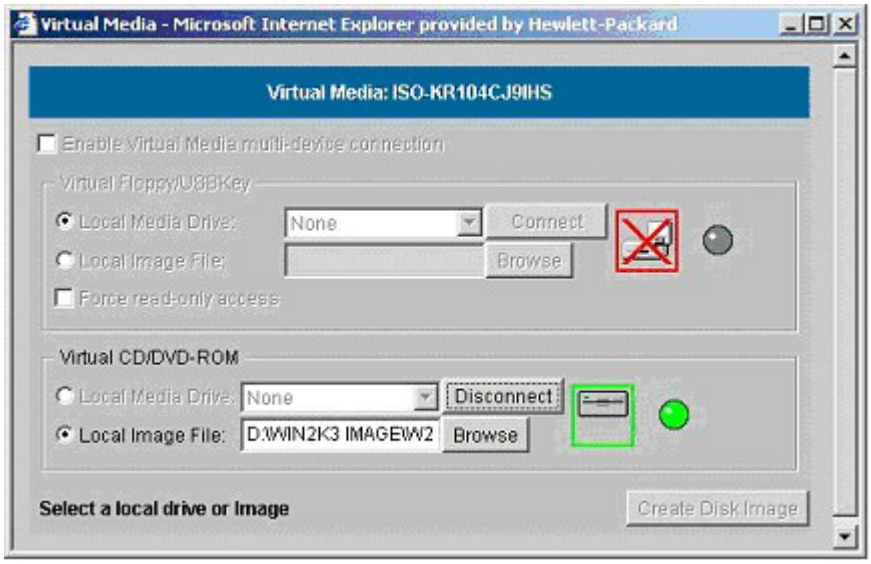
Le CD/DVD-ROM virtuel peut être l'unité de CD/DVD-ROM physique sur laquelle vous exécutez le navigateur Web ou un fichier image sur votre disque dur local ou sur une unité réseau.

> **REMARQUE :** pour de meilleures performances, utilisez des fichiers image. HP vous recommande d'utiliser des fichiers image locaux stockés sur le disque dur de votre PC client, ou sur une unité réseau accessible via une liaison haut débit.

Pour utiliser une unité de CD/DVD-ROM physique dans votre PC client :

1. Dans la section Virtual CD/DVD-ROM, sélectionnez **Local Media Drive** (Unité de support locale).
2. Dans le menu déroulant, sélectionnez la lettre correspondant à l'unité CD/DVD-ROM physique souhaitée du PC client.

3. Cliquez sur **Connect** (Connecter).



Pour utiliser un fichier image :

1. Dans la section Virtual CD/DVD-ROM de l'applet Virtual Media, sélectionnez **Local Image File** (Fichier image local).
2. Saisissez le chemin et le nom de fichier de l'image dans la zone de texte ou cliquez sur **Browse** (Parcourir) pour trouver le fichier image à l'aide de la boîte de dialogue Choose Disk Image File (Choisir le fichier d'image disque).
3. Cliquez sur **Connect** (Connecter).

L'icône et le voyant de l'unité connectée changent pour refléter l'état en cours de l'unité de CD/DVD-ROM virtuel. Une fois les périphériques virtuels connectés, le serveur hôte peut y accéder jusqu'à ce que vous fermiez l'applet Virtual Media. Lorsque vous avez fini d'utiliser le CD/DVD-ROM virtuel, vous pouvez déconnecter le périphérique du serveur hôte ou fermer l'applet. L'applet Virtual Media doit rester ouverte lorsque vous utilisez un périphérique de support virtuel.

Le CD/DVD-ROM de support virtuel iLO est mis à la disposition du serveur hôte au moment de l'exécution si le système d'exploitation de celui-ci prend en charge les unités de disquette USB. Reportez-vous à la section « Prise en charge USB par les systèmes d'exploitation » (page 106) pour plus d'informations sur les systèmes d'exploitation prenant en charge le stockage de masse USB.

Le CD/DVD-ROM de support virtuel iLO est reconnu par votre système d'exploitation au même titre que tout autre CD/DVD-ROM. Lorsque vous utilisez iLO pour la première fois, le système d'exploitation hôte peut vous demander d'exécuter un Assistant New Hardware Found (Nouveau matériel détecté).

Lorsque vous avez fini d'utiliser le support virtuel iLO et que vous le déconnectez, le système d'exploitation peut vous envoyer un message d'avertissement indiquant le retrait non sécurisé d'un périphérique. Cet avertissement peut être évité à l'aide de la fonction fournie par le système d'exploitation, qui permet d'arrêter le périphérique avant de le déconnecter du support virtuel.

Remarques sur les systèmes d'exploitation exécutant des CD/DVD-ROM virtuels

- MS-DOS

  Le CD/DVD-ROM virtuel n'est pas pris en charge sous MS-DOS.

- Windows® 2000 SP3 ou version supérieure et Windows® Server 2003

  La fonctionnalité de CD/DVD-ROM virtuel s'affiche automatiquement dès que Windows® a reconnu le montage du périphérique USB. Utilisez-la comme vous utiliseriez une unité de CD/DVD-ROM reliée localement.

  Sous Windows® 2000 SP3 et versions ultérieures, My Computer (Poste de travail) sur le serveur hôte affiche une unité de CD-ROM supplémentaire lorsque l'applet Virtual Media est connectée. Si le système d'exploitation du serveur est en cours d'exécution et que vous essayez d'effectuer une déconnexion puis une reconnexion dans l'applet Virtual Media, le serveur peut tomber en panne. L'icône passe au vert mais l'unité CD-ROM supplémentaire ne s'affiche pas dans My Computer (Poste de travail).

  Pour résoudre ce problème, réamorcez le serveur hôte et, une fois que le système d'exploitation est disponible, le CD/DVD-ROM virtuel est prêt à l'emploi. Ce problème se produit uniquement sur les serveurs ne possédant pas d'unité de CD/DVD-ROM physique.

- Linux
  - Red Hat Linux

    Sur les serveurs équipés d'une unité de CD/DVD-ROM IDE reliée localement, l'unité de CD/DVD-ROM virtuel est accessible via la commande /dev/cdrom1. Cependant, sur les serveurs sans unité de CD/DVD-ROM reliée localement, tels que les serveurs lame BL-class, le CD/DVD-ROM virtuel est le premier CD/DVD-ROM accessible via la commande /dev/cdrom.

    Le CD/DVD-ROM virtuel peut être monté comme une unité de CD/DVD-ROM normale, à l'aide de la commande :

    mount /mnt/cdrom1

  - SLES 9

    Le système d'exploitation SLES 9 place les CD/DVD-ROM connectés via USB dans un emplacement différent. Par conséquent, il est possible de trouver le CD/DVD-ROM virtuel grâce à la commande /dev/scd0, sauf s'il existe déjà un CD/DVD-ROM local relié via USB, auquel cas il faut utiliser pour ce faire la commande /dev/scd1.

    Le CD/DVD-ROM virtuel peut être monté comme une unité de CD/DVD-ROM normale, à l'aide de la commande :

    mount /dev/scd0 /media/cdrom11

  Reportez-vous à la section « Montage d'un CD/DVD-ROM de support virtuel USB sous Linux » (page 105) pour obtenir des instructions détaillées.

Montage d'un CD/DVD-ROM de support virtuel USB sous Linux

1. Accédez à la carte iLO à l'aide d'un navigateur.
2. Cliquez sur **Virtual Media** (Support virtuel) sous l'onglet Virtual Devices (Périphériques virtuels).
3. Sélectionnez le CD/DVD-ROM à utiliser, puis cliquez sur **Connect** (Connecter).
4. Montez l'unité de CD-ROM à l'aide de la commande suivante :

   ```
   mount /dev/cdrom1  /mnt/cdrom1
   ```

Pour SLES 9 :

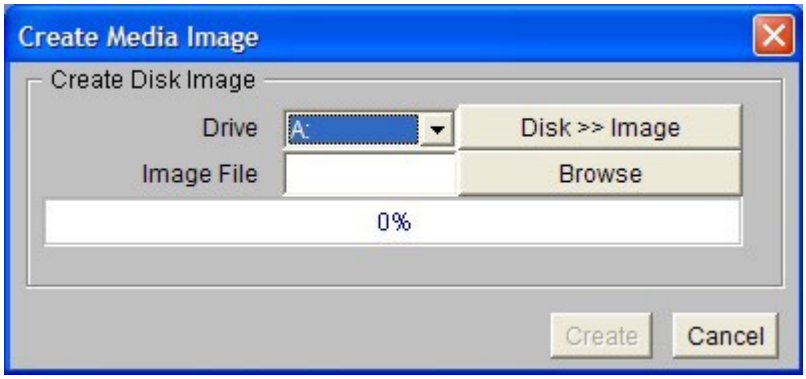
```
mount /dev/scd0  /media/cdrom1
```

Création de fichiers d'image disque iLO

La fonction Virtual Media (Support virtuel) de iLO vous permet de créer des fichiers image de disquette et de CD-ROM dans la même applet. La création de fichiers d'image DVD à l'aide de l'applet Virtual Media (Support virtuel) n'est pas prise en charge. Les fichiers image créés à partir de l'applet sont des images du système de fichiers ISO-9660. Le support virtuel iLO est plus performant lorsque des fichiers image sont utilisés. L'utilitaire permettant de créer des fichiers d'image disque de disquette et de CD-ROM iLO est intégré dans l'applet Virtual Media. Cependant, vous pouvez également créer des images à l'aide d'outils standard tels que DD.

Pour créer un fichier image :

1. Cliquez sur **Create Disk Image** (Créer image disque).
2. Sélectionnez l'unité de support locale dans le menu déroulant.
3. Entrez le chemin ou nom de fichier dans la zone de texte ou cliquez sur **Browse** (Parcourir) pour sélectionner un fichier image existant ou changer le répertoire dans lequel créer le fichier image.
4. Cliquez sur **Create** (Créer). L'applet Virtual Media (Support virtuel) lance la procédure de création du fichier image. La procédure est terminée lorsque la barre de progression atteint 100 %. Pour annuler la création d'un fichier image, cliquez sur **Cancel** (Annuler).



L'option Disk>>Image (Disque>>Image) permet de créer des fichiers image à partir de disquettes ou de CD-ROM physiques. L'option Image>>Disk (Image>>Disque) n'est pas valide pour une image de CD-ROM virtuel. Le bouton Disk>>Image (Disque>>Image) devient alors le bouton Image>>Disk (Image>>Disque) lorsque vous cliquez dessus. Utilisez ce bouton pour basculer de la création de fichiers image depuis des disquettes physiques à la création de disquettes physiques à partir de fichiers image.

Prise en charge USB par les systèmes d'exploitation

Pour pouvoir utiliser les lecteurs du support virtuel, votre système d'exploitation doit prendre en charge les périphériques USB. Il doit également prendre en charge les périphériques de mémoire de masse USB. Actuellement, les systèmes d'exploitation suivants sont compatibles : Windows® 2000 SP4 et versions ultérieures, Windows® 2003, RedHat Enterprise Linux 3 et 4, et SUSE SLES 9. Il se peut que d'autres systèmes d'exploitation prennent également en charge les périphériques de mémoire de masse USB.

Au démarrage du système, le BIOS de la mémoire BIOS offre un support USB jusqu'à ce que le système d'exploitation soit chargé. Étant donné que MS-DOS utilise le BIOS pour communiquer avec les périphériques de stockage, les disquettes d'utilitaires permettant de lancer DOS fonctionneront également avec le support virtuel.

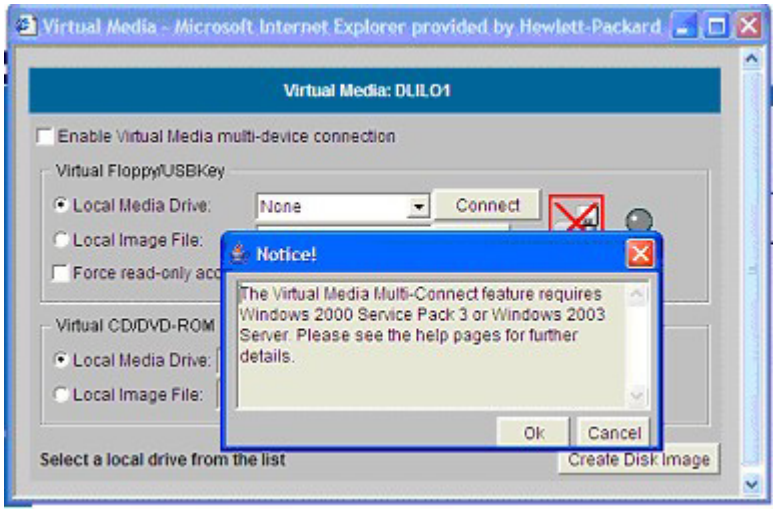
REMARQUE : sous RedHat Enterprise Linux 3, vous ne pouvez pas utiliser de disquette de driver à l'aide du support virtuel.

Prise en charge multi-périphériques de Virtual Media (Support virtuel)

La prise en charge multi-périphériques de support virtuel permet de connecter simultanément l'unité de disquette/clé USB virtuelle et le lecteur de CD/DVD-ROM à l'hôte. L'unité sélectionnée peut être un disque physique, un fichier image ou toute autre combinaison des deux.

Le mode multi-périphériques du support virtuel avec plusieurs périphériques USB est pris en charge sur Microsoft® Windows® 2000 Service Pack 3 et Windows® 2003, mais pas sur Linux. Certains serveurs requièrent peut-être une mise à jour de la ROM système pour ce mode de fonctionnement.

Pour activer une connexion multi-périphériques, activez la case à cocher **Enable Virtual Media multi-device connection** (Activer la prise en charge multi-périphériques pour le support virtuel). La connexion en mode multi-périphériques ne fonctionne correctement que sur des systèmes d'exploitation qui prennent en charge les périphériques USB composites. Pour chaque session, une fenêtre comportant un message d'avertissement initial s'affiche.



Pour utiliser une connexion multi-périphériques :

1. Dans la section Virtual Floppy/USBKey, choisissez **Local Floppy Drive** (Unité de disquette locale), puis sélectionnez une des options suivantes :
   - Dans le menu déroulant, sélectionnez la lettre correspondant à l'unité locale de disquette ou de clé USB physique souhaitée de votre PC client.
   - Sélectionnez **Local Image File** (Fichier image local) dans la section Virtual Floppy (Disquette virtuelle) de l'applet Virtual Media, puis entrez le nom de l'image de disquette dans la zone de texte.
   - Cliquez sur **Browse** (Parcourir) pour repérer les fichiers image.
2. Cliquez sur **Connect** (Connecter).

   Si le support virtuel est configuré pour la prise en charge de périphériques composites, les deux périphériques sont visibles par le système d'exploitation chaque fois que vous vous connectez simplement à l'un d'eux. Cependant, le système d'exploitation ne peut accéder qu'au périphérique connecté. L'autre périphérique affiche le message `Please insert a disk into drive` (Insérez une disquette dans l'unité) si vous essayez d'y accéder. Une fois l'autre périphérique connecté, le système d'exploitation peut correctement accéder aux deux périphériques.

3. Dans la section Virtual CD-ROM, choisissez **Local CD/DVD-ROM Drive** (Unité de CD/DVD-ROM locale), puis sélectionnez une des options suivantes :
   - Dans le menu déroulant, sélectionnez la lettre correspondant au lecteur de CD-ROM physique souhaité de votre PC client.
   - Sélectionnez **Local Image File** (Fichier image local) dans la section **Virtual CD-ROM** (CD-ROM virtuel) de l'applet Virtual Media, puis entrez le nom de l'image de CD-ROM dans la zone de texte appropriée.
   - Cliquez sur **Browse** (Parcourir) pour repérer les fichiers image.
4. Cliquez sur **Connect** (Connecter).

Le système d'exploitation peut maintenant accéder à l'unité de disquette et au lecteur de CD-ROM de support virtuel.

Privilège Virtual Media (Support virtuel) de iLO

L'utilisation de la fonction de support virtuel iLO est régie par un privilège utilisateur. Les utilisateurs autorisés doivent disposer du privilège Virtual Media (Support virtuel) pour pouvoir sélectionner un périphérique de support virtuel et le connecter au serveur hôte.

N'utilisez pas la disquette virtuelle iLO pour mettre à niveau le microprogramme iLO depuis une disquette ROMPaq. Si vous tentez une mise à niveau d'iLO à distance à l'aide de l'utilitaire ROMPaq, iLO se réinitialise, perd la connexion et ne se reconnecte pas. L'utilisation du navigateur rend la perte de connexion temporaire et pour mettre à niveau iLO permet de vous reconnecter automatiquement. HP vous recommande d'utiliser l'option Upgrade iLO Firmware (Mettre à niveau microprogramme iLO) sous l'onglet Administration pour mettre à niveau le microprogramme iLO à distance.

Témoins virtuels

Le voyant d'ID de l'unité correspond au voyant bleu du serveur HP qui permet d'identifier les systèmes présents dans un rack rempli de serveurs. La carte iLO vous permet d'afficher l'état du voyant d'ID de l'unité et de modifier cet état à l'aide des pages Web iLO.

De plus, le voyant d'ID de l'unité clignote chaque fois qu'une tâche critique de supervision distante, ne devant pas être interrompue, est en cours d'exécution sur le serveur.

Le voyant d'ID de l'unité clignote dans les cas suivants :

- le serveur est sous le contrôle actif de la console distante iLO ;
- les paramètres iLO sont en cours de modification via un script XML ;
- lors de la mise à jour du microprogramme iLO.

Ne mettez jamais le serveur hors tension si le voyant d'ID de l'unité clignote.

Supervision avancée des serveurs ProLiant BL p-Class

iLO Advanced est un composant standard des serveurs lame ProLiant BL p-Class qui assure l'intégrité du serveur et permet de le superviser aisément à distance. Ses fonctionnalités sont accessibles à partir d'un périphérique client réseau à l'aide d'un navigateur Web pris en charge. En outre, iLO Advanced offre des fonctionnalités de clavier, de souris et de vidéo (texte et graphique) à un serveur en lame, quel que soit l'état du système d'exploitation hôte ou du serveur en lame hôte.

Le système iLO comprend un microprocesseur intelligent, une mémoire sécurisée et une interface réseau dédiée. Cette conception le rend indépendant du serveur hôte et de son système d'exploitation. iLO permet d'accéder à distance à n'importe quel client réseau autorisé, envoie des alertes et fournit d'autres fonctionnalités de supervision de serveur en lame.

À l'aide d'un navigateur compatible, vous pouvez effectuer les tâches suivantes :

- Accéder à distance à la console de la lame de serveur hôte, notamment à tous les écrans en mode texte et en mode graphique, et à toutes les commandes de clavier et de souris.
- Mettre la lame de serveur hôte sous et hors tension à distance ou la redémarrer.
- Démarrer un serveur lame hôte à distance sur une image de disquette virtuelle pour effectuer une mise à niveau de la ROM ou pour installer un système d'exploitation.
- Envoyer des alertes à partir d'iLO Advanced, quel que soit l'état du serveur en lame hôte.
- Accéder aux fonctionnalités avancées de résolution des problèmes fournies par iLO Advanced.
- Lancer un navigateur Web, utiliser les alertes SNMP et diagnostiquer le serveur lame à l'aide de HP Systems Insight Manager.
- Configurer des paramètres de compartiment IP statique pour les cartes réseau de supervision iLO dédiées sur chaque serveur en lame d'un boîtier pour un déploiement plus rapide.

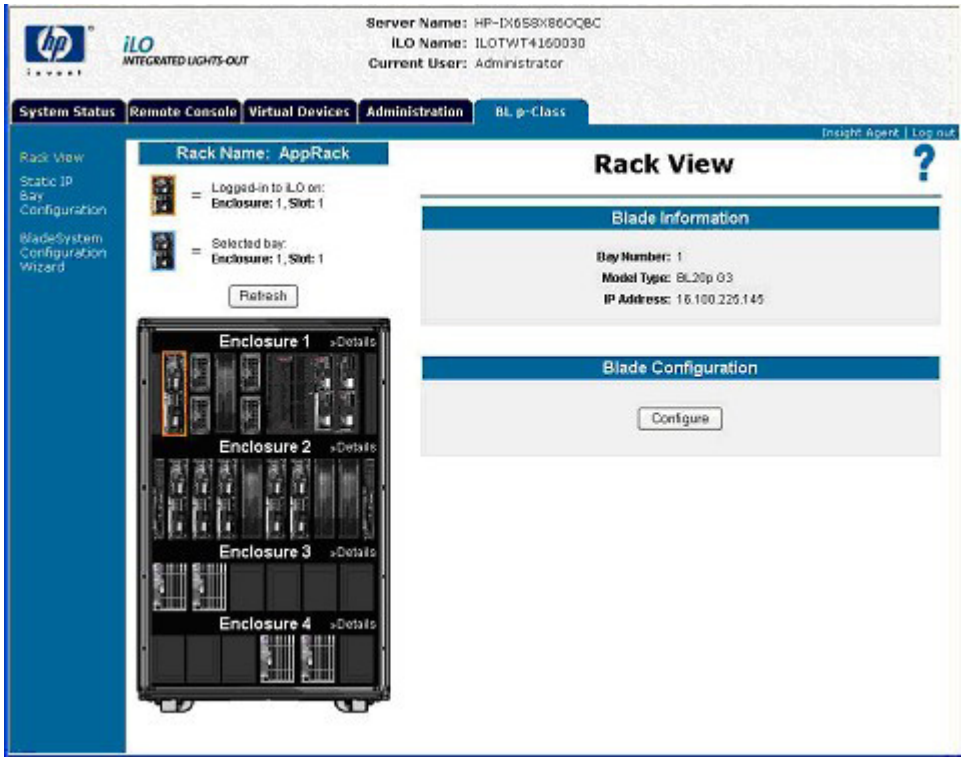
Le serveur en lame doit être correctement connecté pour assurer la connectivité iLO. Connectez-vous à la lame de serveur en utilisant l'une des méthodes suivantes :

- Via un réseau existant (dans le rack) : cette méthode nécessite d'installer la lame de serveur dans son boîtier et de lui affecter une adresse IP (manuellement ou via DHCP).
- Via le port d'E/S du serveur lame
  - Dans le rack : cette méthode nécessite de connecter le câble d'E/S local au port d'E/S et à un PC client. À l'aide de l'adresse IP fixe inscrite sur l'étiquette du câble d'E/S et des informations d'accès initial à l'avant du serveur en lame, vous pouvez accéder au serveur en lame avec la console distante iLO Advanced.
  - Hors du rack, à l'aide de la station de diagnostic : cette méthode nécessite la mise sous tension du serveur lame avec la station de diagnostic en option et la connexion à un ordinateur externe à l'aide de l'adresse IP fixe et du câble d'E/S local. Pour les instructions de câblage, reportez-vous à la documentation livrée avec la station de diagnostic ou au CD Documentation.
  - Via les connecteurs du panneau arrière du serveur lame (hors du rack, à l'aide de la station de diagnostic) : cette méthode permet de configurer un serveur lame hors du rack en l'alimentant à l'aide de la station de diagnostic et en le connectant à un réseau existant via un hub. L'adresse IP est attribuée par un serveur DHCP présent sur le réseau.

L'onglet BL p-Class permet de contrôler des paramètres propres au rack des serveurs lame ProLiant BL p-Class. La carte iLO propose également des diagnostics basés sur le Web pour le rack des serveurs ProLiant BL p-Class.

Vue du rack

La page Rack View (Afficher rack) présente les boîtiers ainsi que leurs serveurs lame, composants réseau et modules d'alimentation. Lorsqu'un composant est présent, il peut être sélectionné à partir de l'écran Rack View (Afficher rack). Vous ne pouvez pas sélectionner les compartiments vides. Les informations propres au composant, comme le nom du serveur lame, l'adresse IP et le type de produit s'affichent lorsque vous positionnez le curseur sur le chaque composant. Cliquez sur le composant pour afficher des informations supplémentaires et des options de configuration dans un écran.



Les champs suivants sont accessibles à partir de l'écran Rack View (Afficher rack) :

- Nom du rack
- Logged-in iLO Location (Emplacement iLO intégré)

  Cette section annote la lame à laquelle l'utilisateur est connecté. L'utilisateur peut configurer les paramètres de lame pour cette lame uniquement.
- Selected Bay Location (Emplacement compartiment sélectionné)

  Cette section annote le compartiment sélectionné. Vous pouvez visualiser les données des différents types de composants, comme les lames, les blocs d'alimentation, les composants réseau et les boîtiers.
- Enclosure Details (Détails boîtier)

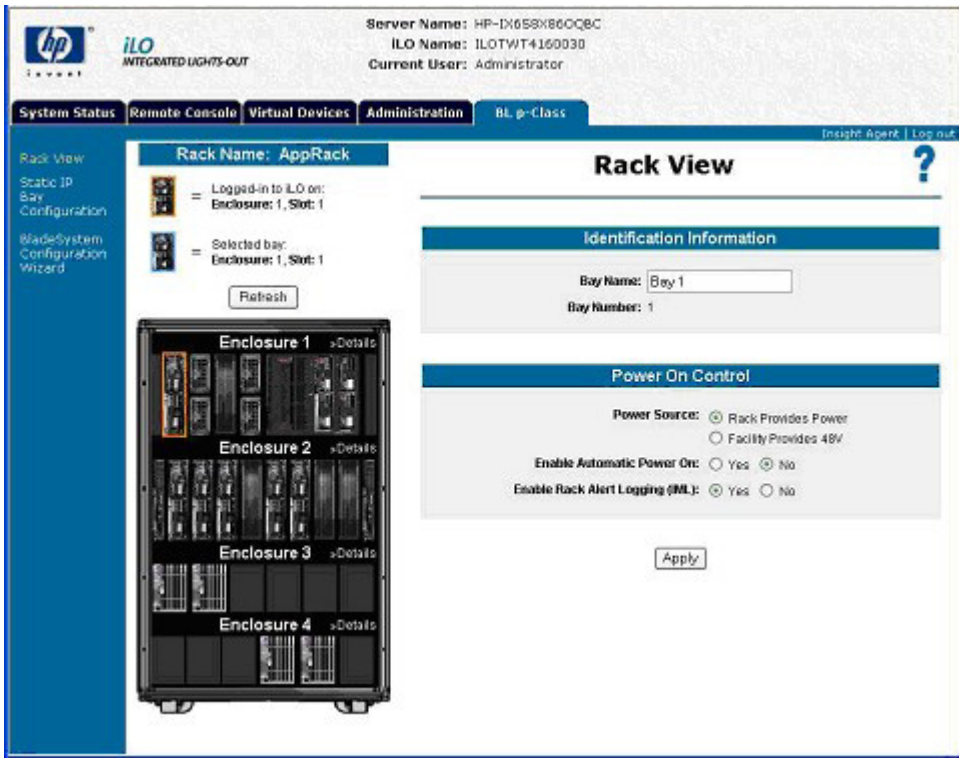
  Pour afficher des informations sur un boîtier donné, sélectionnez **Details** (Détails) sur les en-têtes de boîtier énumérés.

Le bouton Refresh (Rafraîchir) permet d'obtenir des informations sur l'écran Rack View (Afficher rack). Cliquez sur **Refresh** (Rafraîchir) pour forcer la représentation graphique du rack à redessiner. Cette opération peut durer quelques instants.

Si des informations erronées s'affichent dans l'écran Rack View, un message d'erreur apparaît à la place des composants. Vous pouvez de nouveau cliquer sur le bouton Refresh (Actualiser) pour tenter d'afficher les données correctes dans l'écran Rack View. Pour un meilleur affichage, la fonctionnalité Rack View requiert l'utilisation de la version 2.10 ou ultérieure du microprogramme Server Blade et Power Management Module.

Configuration et informations relatives à la lame

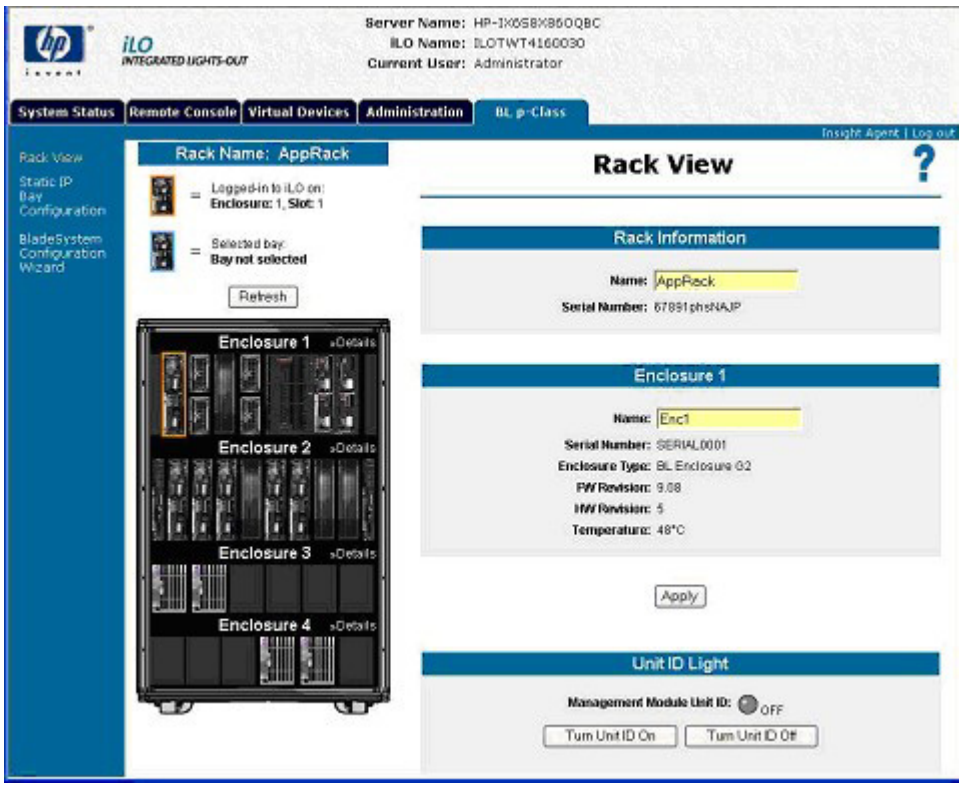
L'option de configuration de la lame fournit des informations sur l'identité, l'emplacement et l'adresse réseau de la lame sélectionnée sur la page Rack View (Afficher rack). Pour afficher ces paramètres, sélectionnez un composant de lame et choisissez l'option **Configure** (Configurer) sur la page Rack View (Afficher rack) (page 110). Vous pouvez modifier certains des paramètres de la lame à laquelle vous êtes connectée. Pour enregistrer ces modifications, cliquez sur **Apply** (Appliquer).



Les champs disponibles sont les suivants :

- Identification Information (Informations d'identification)
  - Bay Name (Nom du compartiment)
  - Bay Number (Numéro de compartiment)
- Power On Control (Bouton de mise sous tension)
  - Power Source (Source d'alimentation)
  - Enable Automatic Power On (Activer la mise sous tension automatique)
  - Enable Rack Alert Logging (IML) (Activer la consignation des alertes du rack - IML)

Informations relatives au boîtier



Les informations relatives au boîtier sont spécifiques au boîtier sélectionné. Pour afficher des informations sur un boîtier donné, sélectionnez **Details** (Détails) sur les en-têtes de boîtier énumérés. Un nombre limité d'informations de rack sont disponibles, comprenant :

- Nom du rack
- Rack Serial Number (Numéro de série du rack)

Un ensemble d'informations de base est disponible pour les boîtiers qui ne contiennent pas de lame où vous êtes connecté. Ces informations comprennent :

- Nom de boîtier
- Enclosure Serial Number (Numéro de série du boîtier)
- Enclosure Type (Type de boîtier)

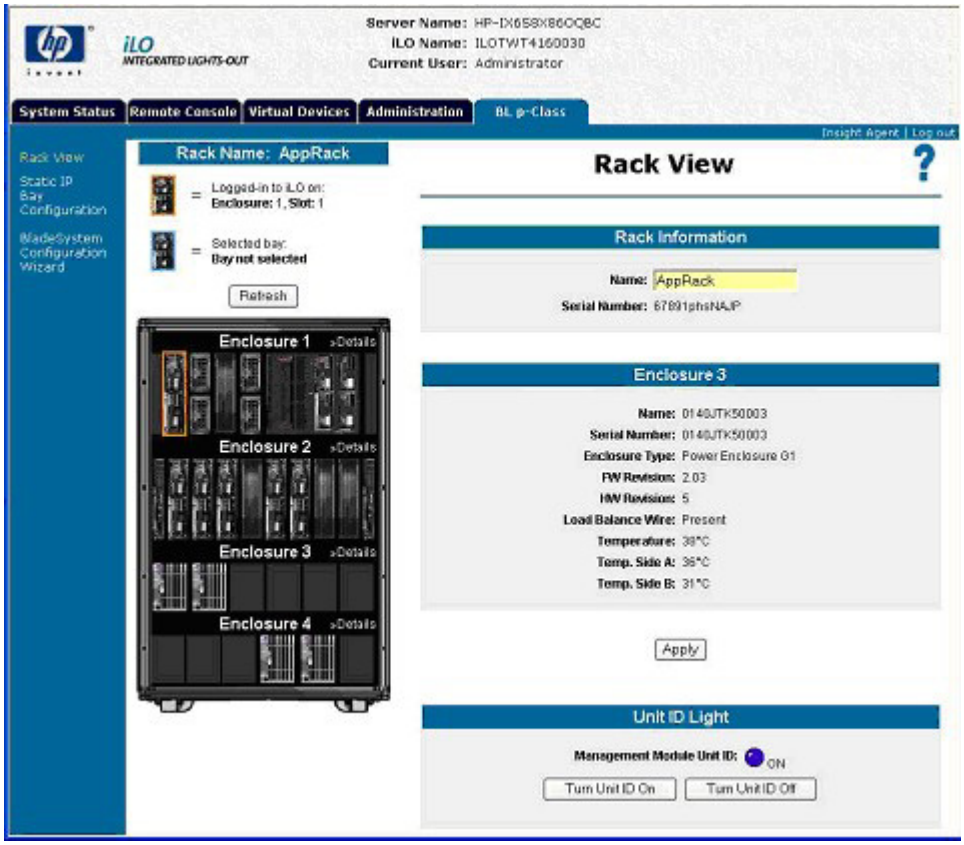
Un ensemble de détails est disponible pour le boîtier qui contient le compartiment auquel vous êtes connecté. Ces détails comprennent :

- Nom de boîtier
- Enclosure Serial Number (Numéro de série du boîtier)
- Enclosure Type (Type de boîtier)
- Firmware Revision (Révision du microprogramme)
- Hardware Revision (Révision du matériel)
- Enclosure Temperature (Température du boîtier)
- Management Module Unit ID (ID unité module supervision)

Vous pouvez mettre à jour certains champs à l'aide du bouton Apply (Appliquer).

Informations relatives au boîtier d'alimentation

La page Power Enclosure Information (Informations relatives au boîtier d'alimentation) fournit des informations de diagnostic sur le module PMM et les composants contenus dans le boîtier d'alimentation. Ces informations offrent un aperçu de l'état de marche du boîtier et des composants d'alimentation.



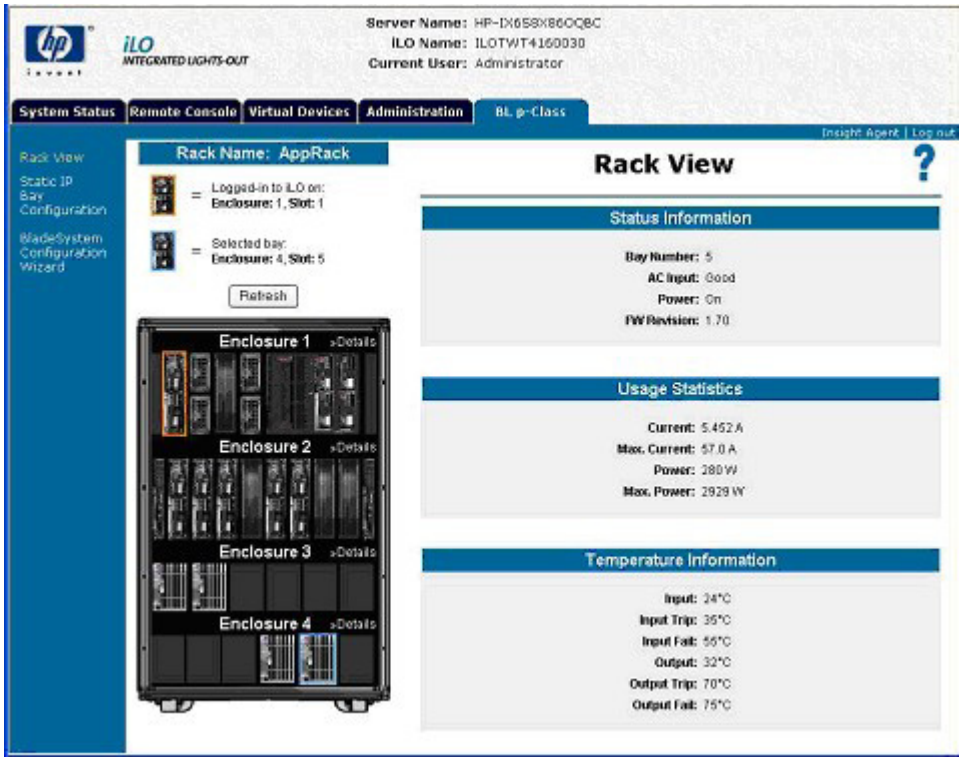
Les champs disponibles sont les suivants :

- Nom du rack
- Rack Serial Number (Numéro de série du rack)
- Nom de boîtier
- Enclosure Serial Number (Numéro de série du boîtier)
- Enclosure Type (Type de boîtier)
- Firmware Revision (Révision du microprogramme)
- Hardware Revision (Révision du matériel)
- Load Balance Wire (Canal balance de charge)
- Enclosure Temperature (Température du boîtier)
- Enclosure Temperature Side A and B (Température du boîtier face A et B)
- Management Module UID (ID unique module de gestion)

Vous pouvez mettre à jour certains champs à l'aide du bouton Apply (Appliquer).

Informations relatives aux composants d'alimentation

La sélection d'un composant d'alimentation sur la page Rack View (Afficher rack) (page 110) permet d'afficher l'emplacement général, le statut, la puissance fournie et les mesures de température du composant sélectionné dans le boîtier d'alimentation.



La section Status Information (Informations de l'état) fournit les informations suivantes :

- Bay Number (Numéro de compartiment)
- AC Input (Alimentation CA)
- Power (Alimentation)
- Firmware Revision (Révision du microprogramme)

La section Usage Statistics (Statistiques d'utilisation) comprend les champs suivants :

- Current (Courant)
- Courant maximal
- Power (Alimentation)
- Maximum Power (Alimentation maximale)

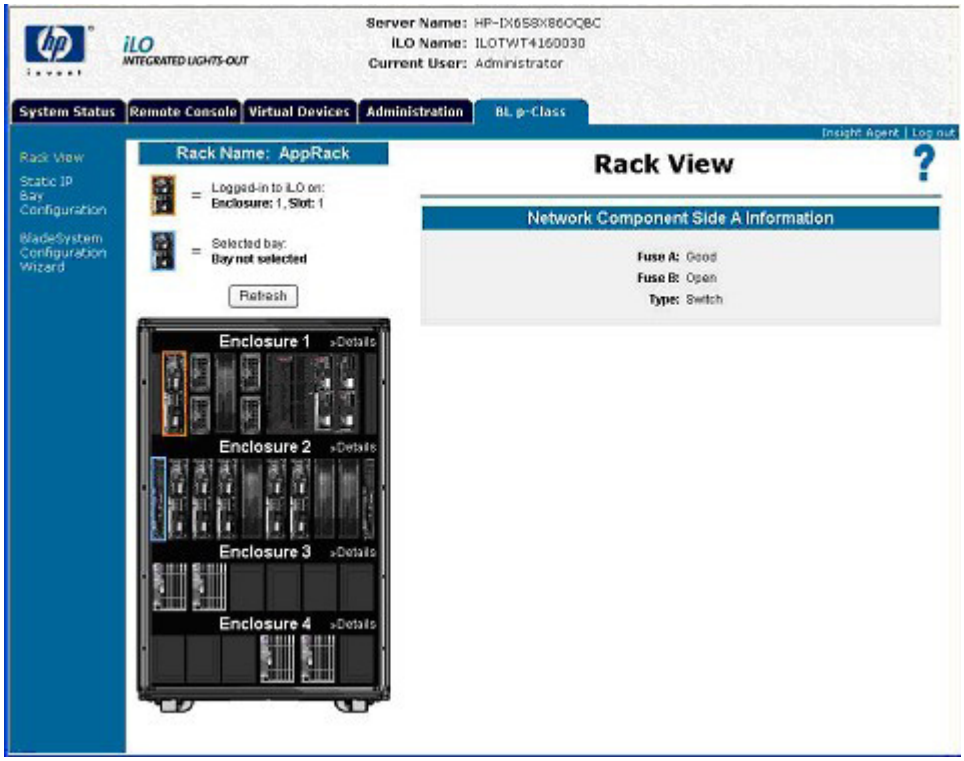
La section Temperature Information (Informations température) contient les paramètres de température qui représentent les valeurs actuelles et les seuils pour les températures d'entrée et de sortie. Ces champs sont les suivants :

- Entrée
- Input Trip (Déclenchement en entrée)
- Input Fail (Échec en entrée)
- Sortie

- Output Trip (Déclenchement en sortie)
- Output Fail (Échec en sortie)

Informations relatives aux composants réseau

Ces informations affichent l'état du panneau à interconnexions qui a été sélectionné.



Les informations suivantes sont disponibles :

- Fuse A (Fusible A)
- Fuse B (Fusible B)
- Network Component Type (Type de composant réseau)

Contrôle par la carte iLO des voyants du serveur ProLiant BL p-Class

La carte iLO supervise les serveurs BL p-Class via le suivi des messages POST et le voyant d'état du serveur.

Suivi des messages POST de serveur

Les possibilités de feedback sont limitées pendant l'amorçage du serveur étant donné la structure non centralisée des serveurs ProLiant BL p-Class. La carte iLO propose un feedback au moment de l'amorçage en faisant clignoter le voyant vert de supervision du serveur pendant le test POST. Le voyant devient orange et ne clignote plus si l'amorçage échoue. Il devient vert et cesse de clignoter lorsque l'amorçage est réussi.

Après un amorçage réussi, le contrôle du voyant d'état du serveur est renvoyé au serveur, qui peut alors l'éteindre ou en modifier la couleur pour indiquer le bon état de fonctionnement du matériel.

Notification d'alimentation insuffisante

La carte iLO allume le voyant d'état du serveur en rouge si elle ne parvient pas à le mettre sous tension en raison d'une alimentation insuffisante dans l'infrastructure du rack.

Transfert des alertes ProLiant BL p-Class

La carte iLO prend en charge les traps (alertes) SNMP de l'infrastructure lame grâce à la fonction pass-through. La prise en charge du système d'exploitation n'est pas nécessaire pour que la carte iLO indique l'état de l'infrastructure lame. Les traps sont générés par Enclosure Manager (Gestionnaire du boîtier) et Power Supply Manager (Gestionnaire de l'alimentation) et sont transmis à la carte iLO. Le microprogramme p-Class transfère les alertes relatives à l'infrastructure sous forme de traps SNMP vers une console de supervision correctement configurée. Ces messages permettent à la console de supervision SNMP de contrôler les alertes p-Class.

Le transfert des alertes p-Class est désactivé par défaut. Cette fonction peut être activée depuis la page Web SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager).

Les alertes suivantes sont identifiées et transférées par la carte iLO :

ID de l'alerte	Description
22005	Erreur de température du boîtier
22006	Température du boîtier anormale
22007	Température du boîtier OK
22008	Panne du ventilateur du boîtier
22009	Mauvais fonctionnement du ventilateur du boîtier
22010	Ventilateur du boîtier OK
22013	Coupure de l'alimentation du rack
22014	Alimentation du rack défectueuse
22015	Alimentation du rack OK
22023	Panne du rack serveur : alimentation insuffisante

Services d'annuaire

Cette section traite des rubriques suivantes :

Présentation de l'intégration d'annuaire

iLO peut être configuré afin d'utiliser un annuaire pour authentifier et autoriser ses utilisateurs. Avant de configurer iLO pour les annuaires, vous devez décider si vous souhaitez utiliser l'option de schéma HP Extended.

Les avantages de l'option du schéma HP Extended sont les suivants :

- Vous disposez d'une souplesse beaucoup plus grande concernant le contrôle de l'accès. Par exemple, l'accès peut être restreint à une tranche horaire dans la journée ou à une certaine plage d'adresses IP.
- Les groupes sont gérés dans l'annuaire et non dans chaque iLO.
- RILOE et RILOE II fonctionnent uniquement avec le schéma HP Extended (l'option sans schéma sera ajoutée à RILOE II ultérieurement).

iLO, RILOE et RILOE II fonctionnent avec eDirectory uniquement dans le cadre de l'option HP Extended.

Consultez la liste complète des avantages disponible dans la section « Avantages de l'intégration d'annuaire » (page 117). La section « Supervision distante activée via l'annuaire » (page 152) explique en détail comment activer et appliquer les rôles, les groupes et la sécurité à l'aide des annuaires. Pour plus d'informations sur l'intégration d'annuaire, des livres blancs sont également disponibles sur le site Web HP (http://www.hp.com/servers/lights-out).

Avantages de l'intégration d'annuaire

- Évolutivité : l'annuaire peut être configuré pour prendre en charge des milliers d'utilisateurs sur des milliers de cartes iLO.
- Sécurité : des stratégies de mot de passe évoluées sont héritées de l'annuaire. La complexité, la fréquence de changement et l'expiration des mots de passe utilisateur sont des exemples de stratégie.
- Anonymat (manque) : dans certains environnements, les utilisateurs partagent des comptes Lights-Out, ce qui empêche de connaître l'auteur d'une opération mais pas le compte (ou rôle) utilisé.
- Administration basée sur les rôles : vous pouvez créer des rôles (par exemple, bureau, contrôle à distance de l'hôte, contrôle complet) et y associer des utilisateurs ou groupes. Toute modification apportée à un rôle s'applique à l'ensemble des utilisateurs et périphériques Lights-Out associés.

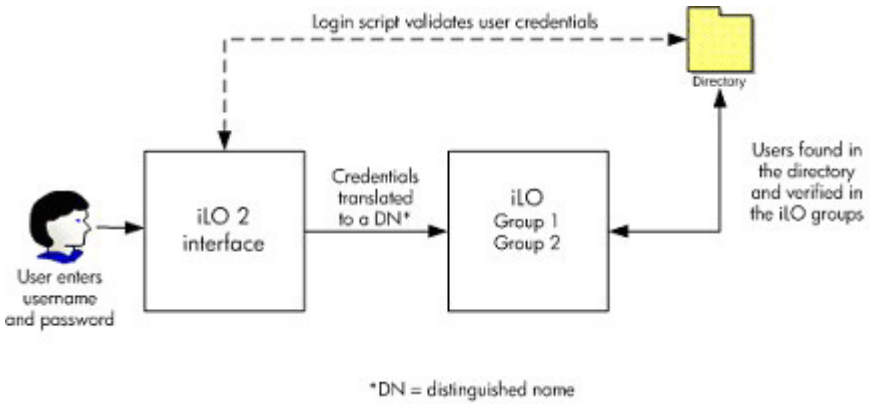
- Point unique d'administration : vous pouvez utiliser des outils d'administration natifs tels que MMC et ConsoleOne pour administrer les utilisateurs Lights-Out.
- Imminence : toute modification apportée à l'annuaire s'applique immédiatement aux processeurs Lights-Out associés. Cela évite d'écrire le script de ce processus.
- Élimination d'un autre mot de passe et nom d'utilisateur : vous pouvez utiliser des comptes utilisateur et des mots de passe existants dans l'annuaire sans qu'il soit nécessaire d'enregistrer ou de rappeler un nouveau jeu de données pour Lights-Out.
- Souplesse : vous pouvez créer un rôle unique pour un utilisateur unique sur une carte iLO unique, ou créer un rôle unique pour plusieurs utilisateurs sur plusieurs cartes iLO, ou utiliser une combinaison de rôles adaptée aux besoins spécifiques de votre entreprise.
- Compatibilité : l'intégration d'annuaire Lights-Out s'applique aux produits iLO, RILOE et RILOE II. L'intégration prend en charge Active Directory et eDirectory.
- Normes : la prise en charge d'annuaire Lights-Out est basée sur la norme LDAP 2.0 pour un accès sécurisé aux annuaires.

Avantages et inconvénients d'annuaires sans schéma et d'annuaire de schéma HP

Les annuaires améliorent la sécurité, en permettant de gérer l'accès et les droits à partir d'un emplacement centralisé. Les annuaires proposent également une souplesse de configuration. Certaines pratiques de configuration d'annuaires fonctionnent mieux avec iLO que d'autres. Avant de configurer iLO pour des annuaires, vous devez décider si vous souhaitez utiliser l'annuaire sans schéma ou les méthodes d'intégration d'annuaire de schéma HP. Répondez aux questions suivantes pour vous aider à évaluer vos exigences d'intégration d'annuaire :

1. Pouvez-vous appliquer des extensions de schéma à votre annuaire ?
   - Non : Utilisez-vous Microsoft Active Directory ?
     - Non - L'intégration d'annuaire peut ne pas être adaptée à votre environnement. Envisagez de déployer un serveur d'annuaire d'évaluation afin d'évaluer les avantages de l'intégration d'annuaire.
     - Oui : Utilisez une intégration d'annuaire sans schéma basée sur les groupes.
   - Oui - Passez à la question 2.
2. Votre configuration est-elle dimensionnable ? Répondez aux questions suivantes :
   a. Envisagez-vous de modifier les droits ou privilèges d'un groupe d'utilisateurs d'annuaire ?
   b. Rédigerez-vous régulièrement des scripts de modification iLO ?
   c. Utilisez-vous plus de cinq groupes pour contrôler les privilèges iLO ?
   - Non : Déployez une instance de l'intégration d'annuaire sans schéma pour évaluer si la méthode d'intégration d'annuaire correspond à vos exigences de stratégie et de procédure. Si nécessaire, vous pouvez déployer une intégration d'annuaire de schéma HP ultérieurement.
   - Oui : Utilisez l'intégration d'annuaire de schéma HP.

Intégration d'annuaire sans schéma : Lors de l'utilisation de la méthode d'intégration d'annuaire sans schéma, users and group memberships résident dans l'annuaire, mais les privilèges de groupe résident dans la carte iLO individuelle. iLO utilise les informations d'authentification de connexion pour lire l'objet utilisateur dans l'annuaire et extrait les appartenances de groupe de l'utilisateur. Ces groupes sont comparés à ceux stockés dans iLO. Si une correspondance existe, l'autorisation est accordée. Par exemple :



Avantages de l'utilisation de l'intégration d'annuaire sans schéma :

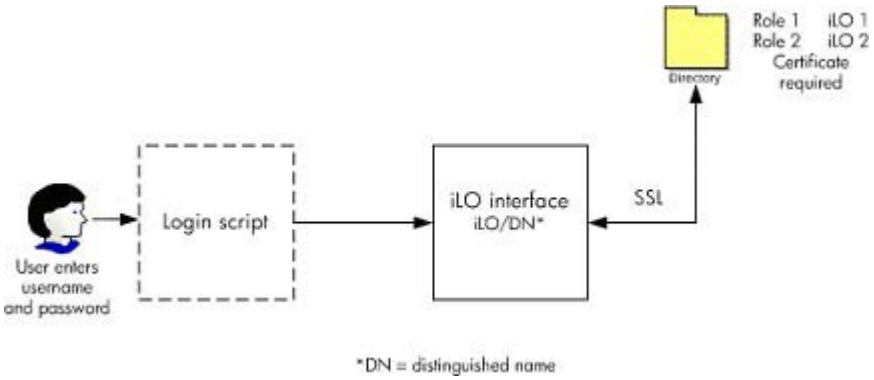
- Vous n'avez pas besoin d'étendre le schéma de l'annuaire.
- Lorsque les contrôles ActiveX sont activés dans le navigateur, la connexion à l'aide de NetBIOS et les formats d'e-mail sont pris en charge.
- Aucune ou peu de configuration n'est requis pour les utilisateurs dans l'annuaire. En cas d'absence de configuration, l'annuaire utilise les utilisateurs et appartenances de groupe existants pour accéder à iLO. Par exemple, si vous disposez d'une administration de domaine nommée Utilisateur1, vous pouvez copier le nom distinctif du groupe de sécurité d'administration de domaine vers iLO et lui accorder des privilèges complets. Utilisateur1 aura ensuite accès à iLO.

Inconvénients de l'utilisation de l'intégration d'annuaire sans schéma :

- Prend uniquement en charge Microsoft Active Directory.
- Les privilèges de groupe sont administrés sur chaque iLO. Toutefois, cet inconvénient est minimisé par les rares modifications de privilèges de groupe, et la tâche de modification d'appartenance de groupe est administrée dans l'annuaire et non sur chaque iLO distinct. HP propose des outils qui permettent de modifier simultanément un nombre important de cartes iLO.

L'intégration d'annuaire de schéma HP est constituée d'une classe nommée hpqRole (une sous-classe de Group), une classe nommée hpqTarget (une sous-classe de User), ainsi que d'autres classes d'assistance. Une instance d'un hpqRole est simplement un rôle. Une instance d'un hpqTarget est équivalente à une carte iLO.

Un rôle contient une ou plusieurs cartes iLO et un ou plusieurs utilisateurs, ainsi qu'une liste des privilèges dont disposent les utilisateurs avec la carte iLO dans le rôle. Tous les accès iLO sont gérés en ajoutant et supprimant des utilisateurs et cartes iLO sur le rôle, et en supervisant les privilèges sur le rôle.
Par exemple :



Avantages de l'utilisation de l'intégration d'annuaire de schéma HP :

- Plus grande souplesse de contrôle d'accès. Par exemple, vous pouvez limiter l'accès à une période de la journée, ou à partir d'une plage données d'adresses IP.
- Les groupes et les permissions sont conservés dans l'annuaire, non sur chaque iLO, et HP fournit les composants logiciels intégrables requis pour la supervision des cibles et groupes HP pour les utilisateurs et groupes Active Directory et pour eDirectory ConsoleOne.
- Intégration avec eDirectory.

Inconvénients de l'intégration d'annuaire de schéma HP

- Le schéma d'annuaire doit être étendu. Toutefois, cette tâche est minimisée car HP fournit le fichier .kdf et un assistant destiné à étendre le schéma, et les versions les plus récentes de Active Directory permettent d'annuler les modifications de schéma.

  Pour plus d'informations sur la procédure d'extension du schéma et la configuration de paramètres d'annuaire, reportez-vous au document « Integrating HP ProLiant Lights-Out processors with Microsoft® Active Directory » (Intégration de processeurs HP ProLiant Lights-Out avec Microsoft® Active Directory)
  (http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00190541/c00190541.pdf).

- Exigences de certificat

  iLO doit communiquer avec l'annuaire en utilisant LDAP sur SSL. Cette communication requiert que le serveur d'annuaire dispose d'un certificat. L'installation du certificat pour le domaine le réplique dans l'ensembles des contrôleurs de domaine dans le domaine. Pour plus d'informations sur l'installation du certificat, reportez-vous à l'avis à la clientèle disponible sur le site Web HP (http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_EM030604_CW01&locale=en_US).

- Options de basculement

  Pour activer le basculement (redondance), utilisez le nom du domaine comme nom de serveur d'annuaire lors de la configuration de la carte iLO. La plupart des serveurs DNS apparient un nom de domaine à un serveur d'annuaire fonctionnel (contrôleur de domaine).

- Format de connexion

  Les formats de noms NetBIOS, UPN et distinctifs sont acceptés comme noms de connexion. Le script de connexion pour iLO appelle le système d'exploitation du client système et tente de convertir le nom de connexion en un nom distinctif d'annuaire. Pour que le script de connexion puisse réaliser cela, le nom d'annuaire doit être un nom DNS, et non une adresse IP. En outre, le client et la carte iLO doivent pouvoir accéder au serveur d'annuaire en utilisant le même nom. Le client et la carte iLO doivent être dans le même domaine DNS.

- Cibles multiples

  Vous n'avez pas à utiliser des cibles multiples dans l'annuaire. L'intégration d'annuaire de schéma HP requiert uniquement un objet hpqTarget, qui peut représenter plusieurs périphériques LOM.

Configuration pour l'intégration d'annuaire sans schéma

Avant de configurer l'option sans schéma, votre système doit répondre à toutes les conditions requises décrites dans la section « Préparation d'Active Directory » (page 121).

Vous pouvez configurer iLO pour les annuaires de trois manières différentes :

- manuellement à l'aide d'un navigateur (« Installation sans schéma basée sur le navigateur », page 123)
- à l'aide d'un script (« Installation sans schéma par script », page 123)
- à l'aide de HPLOMIG (« Installation sans schéma basée sur HPLOMIG », page 124)

Préparation d'Active Directory

L'option sans schéma est prise en charge sur les systèmes d'exploitation suivants :

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory

SSL doit être activé au niveau de l'annuaire. Pour activer SSL, installez un certificat pour le domaine dans Active Directory. iLO communique avec l'annuaire uniquement via une connexion SSL sécurisée. Pour plus d'informations, reportez-vous à l'article 247078 de la Base de connaissances Microsoft® : *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers* (Activation des communications SSL via LDAP pour les contrôleurs de domaine Windows® 2000) sur le site Web Microsoft® (http://support.microsoft.com/).

Pour valider la configuration, vous devez avoir au minimum le nom distinctif dans l'annuaire d'un utilisateur et le nom distinctif d'un groupe de sécurité dont l'utilisateur est membre.

Introduction aux services de certificat

Les services de certificat permettent d'émettre des certificats numériques signés sur les hôtes du réseau. Les certificats permettent d'établir des connexions SSL avec l'hôte et de vérifier son authenticité.

L'installation des services de certificat permet à Active Directory de recevoir un certificat autorisant les processeurs Lights-Out à se connecter au service d'annuaire. Sans certificat, iLO ne peut pas se connecter au serveur d'annuaire.

Chaque serveur d'annuaire auquel vous souhaitez que iLO se connecte doit disposer d'un certificat. Si vous installez un service de certificat d'entreprise, Active Directory peut automatiquement demander et installer des certificats pour tous les contrôleurs Active Directory du réseau.

Installation des services de certificat

1. Sélectionnez **Start>Settings>Control Panel** (Démarrer>Paramètres> Panneau de configuration).
2. Double-cliquez sur **Add/Remove Programs** (Ajout/Suppression de programmes).
3. Cliquez sur **Add/Remove Windows Components** (Ajout/Suppression de composants Windows) pour lancer l'assistant Composants Windows.
4. Cochez la case **Certificate Services** (Services de certificat). Cliquez sur **Next** (Suivant).
5. Cliquez sur **OK** au message d'avertissement indiquant que le serveur ne peut pas être renommé. L'option Enterprise root CA (Autorité de certification d'entreprise) est sélectionnée car aucune autorité de certification n'est enregistrée dans Active Directory .
6. Entrez les informations appropriées pour votre site et votre organisation. Acceptez la période par défaut de deux ans pour le champ Valid for (Valide pendant). Cliquez sur **Next (**Suivant).
7. Acceptez les emplacements par défaut de la base de données de certificats et du journal de base de données. Cliquez sur **Next** (Suivant).
8. Accédez au dossier c:\I386 lorsque le système vous demande d'insérer le CD Windows® 2000 Advanced Server.
9. Click **Finish** to close the wizard.

Vérification des services de certificat

Étant donné que les processeurs de supervision communiquent avec Active Directory via SSL, vous devez créer un certificat ou installer Certificate Services (Services de certificat). Vous devez installer une autorité de certification d'entreprise car vous enverrez des certificats aux objets dans votre domaine organisationnel.

Pour vérifier l'installation des services de certificat, sélectionnez **Start>Programs>Administrative Tools>Certification Authority** (Démarrer>Programmes>Outils d'administration>Autorité de certification). Si les services de certification ne sont pas installés, un message d'erreur s'affiche.

Configuration de demande de certificat automatique

Pour spécifier l'émission d'un certificat sur le serveur :

1. Sélectionnez **Start>Run** (Démarrer>Exécuter), puis entrez `mmc`.
2. Cliquez sur **Add** (Ajouter).
3. Sélectionnez **Group Policy password** (Stratégie de groupe), et cliquez sur **Add** (Ajouter) pour ajouter le composant logiciel intégrable dans MMC.
4. Cliquez sur **Browse** (Parcourir) et sélectionnez l'objet **Default Domain Policy** (Stratégie de domaine par défaut). Cliquez sur **OK**.
5. Sélectionnez **Finish>Close>OK** (Terminer>Fermer>OK).
6. Cliquez sur **Computer Configuration>Windows Settings>Security Settings>Public Key Policies** (Configuration de l'ordinateur>Paramètres Windows>Paramètres de sécurité>Stratégies de clé publique).

7. Cliquez avec le bouton droit sur **Automatic Certificate Requests Settings** (Paramètres des demandes de certificat automatiques) et sélectionnez **New>Automatic Certificate Request** (Nouvelle demande de certificat automatique).
8. Cliquez sur **Next** (Suivant) lorsque l'assistant Automatic Certificate Request Setup (Configuration de demande de certificat automatique) démarre.
9. Sélectionnez le modèle **Domain Controller** (Contrôleur de domaine), puis cliquez sur **Next** (Suivant).
10. Sélectionnez l'autorité de certification listée. (Il s'agit de la même que celle définie lors de l'installation des services de certificat). Cliquez sur **Next** (Suivant).
11. Cliquez sur **Finish** (Terminer) pour fermer l'Assistant.

Installation sans schéma basée sur le navigateur

L'installation sans schéma peut se faire via l'interface iLO basée sur le navigateur.

1. Connectez-vous à la carte iLO en utilisant un compte doté du privilège Configure iLO Settings (Configurer paramètres iLO). Cliquez sur **Administration**.

IMPORTANT : seuls les utilisateurs dotés du privilège Configure iLO Settings (Configurer paramètres iLO) sont autorisés à modifier ces paramètres. Les autres peuvent uniquement consulter les paramètres attribués.

2. Cliquez sur **Directory Settings** (Paramètres d'annuaire).
3. Sélectionnez **Use Directory Default Schema** (Utiliser le schéma d'annuaire par défaut) dans la section Authentication Settings (Paramètres d'authentification). Pour plus d'informations, reportez-vous à la section « Options d'installation sans schéma » (page 124).
4. Cliquez sur **Apply Settings** (Appliquer les paramètres).
5. Cliquez sur **Test Settings** (Tester paramètres).

Installation sans schéma par script

Pour installer l'option d'annuaires sans schéma à l'aide de la rédaction de scripts XMS RIBCL :

1. Téléchargez et consultez le manuel des ressources de la ligne de commande et des scripts.
2. Rédigez un script qui configure iLO pour la prise en charge d'annuaires sans schéma et exécutez-le. Le script suivant peut servir de modèle.

```
<RIBCL VERSION=«2.0»>
<LOGIN USER_LOGIN=«admin» PASSWORD=«password»>
   <DIR_INFO MODE = «write»>
      <MOD_DIR_CONFIG>
      <DIR_ENABLE_GRP_ACCT value = «yes»/>
      <DIR_GRPACCT1_NAME value
      ="CN=Administrators,CN=Builtin,DC=HP,DC=com »/>
      <DIR_GRPACCT1_PRIV value = «1»/>
      <MOD_DIR_CONFIG>
   </DIR_INFO>
<LOGIN
</RIBCL>
```

Installation sans schéma basée sur HPLOMIG

HPLOMIG est la méthode la plus simple pour installer un grand nombre de processeurs LOM pour des annuaires. Pour utiliser HPLOMIG, téléchargez l'utilitaire du même nom et la documentation qui l'accompagne via le site Web HP (http://www.hp.com/servers/lights-out). HP recommande l'utilisation de HPLOMIG lorsque vous configurez de nombreux processeurs LOM pour des annuaires. Pour plus d'informations sur l'utilisation de HPLOMIG, reportez-vous à la section « HPLOMIG Operation (Fonctionnement de HPLOMIG) ».

Options de l'installation sans schéma

Les options d'installation sont les mêmes, quelle que soit la méthode (navigateur, HPQLOMIG ou script) que vous utilisez pour configurer l'annuaire.

Après avoir activé les annuaires et sélectionné l'option sans schéma, vous avez les possibilités suivantes :

Souplesse d'ouverture de session minimale

- Saisissez le nom DNS ou l'adresse IP et le port LDAP du serveur d'annuaire. Généralement, le port LDAP pour une connexion SSL est 636.
- Saisissez le nom distinctif d'un groupe au moins. Il peut s'agir d'un groupe de sécurité (par exemple : « CN=Administrators,CN=Builtin,DC=HP,DC=com ») ou tout autre groupe, à condition que les utilisateurs iLO qui font l'objet de l'installation en soient membres.

  Avec une configuration minimale, vous pouvez vous connecter à iLO à l'aide de votre distinctif complet et de votre mot de passe. Vous devez être membre d'un groupe reconnu par iLO.

Souplesse d'ouverture de session améliorée

- Outre les paramètres minimaux, indiquez au moins un contexte utilisateur d'annuaire.

  Au moment de l'ouverture de session, le nom de connexion et le mot de passe sont combinés pour former le nom distinctif de l'utilisateur. Par exemple, si l'utilisateur se connecte en tant que « JOHN.SMITH » et qu'un contexte utilisateur est défini en tant que « CN=USERS,DC=HP,DC=COM », alors le nom distinctif qui sera utilisé par iLO sera « CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM ».

Souplesse d'ouverture de session maximale

- Configurez iLO conformément à la description.
- Configurez iLO avec un nom de DNS et non une adresse IP pour l'adresse réseau du serveur d'annuaire. Le nom de DNS doit être résolvable en adresse IP à la fois à partir d'iLO et du système client.
- Activez les contrôles ActiveX dans votre navigateur. Le script de connexion iLO va tenter d'appeler un contrôle Windows® pour convertir le nom de connexion en nom distinctif.

  La configuration d'iLO avec le niveau maximum de souplesse d'ouverture de session vous permet de vous connecter avec votre nom distinctif complet et votre mot de passe, votre nom tel qu'il apparaît dans l'annuaire, le format NetBIOS (domaine/nom_connexion) ou le format d'e-mail (nom_connexion@domaine).

REMARQUE : vos paramètres de sécurité du système ou vos logiciels installés peuvent empêcher le script de connexion d'appeler le contrôle ActiveX Windows®. Dans ce cas, votre navigateur affiche un message d'avertissement dans la barre d'état ou une zone de message, ou bien il cesse de répondre. Pour essayer d'identifier le logiciel ou paramètre à l'origine du problème, créez un autre profil et connectez-vous au système.

Dans certains cas, il est possible que vous ne puissiez pas faire fonctionner l'option de souplesse d'ouverture de session maximale. Par exemple, si le client et iLO se trouvent dans des domaines DNS différents, il peut arriver que l'un des deux soit dans l'impossibilité de résoudre le nom du serveur d'annuaire en adresse IP.

Groupes imbriqués sans schéma

De nombreuses organisations répartissent les utilisateurs et administrateurs en groupes. Disposer de cette organisation de groupes existants est pratique car vous pouvez les associer à un ou plusieurs objets de rôle Integrated Lights-Out Management. Lorsque les périphériques sont associés à des objets de rôle, l'administrateur contrôle l'accès aux périphériques Lights-Out associés au rôle en ajoutant ou supprimant des membres au sein des groupes.

Lors de l'utilisation de Microsoft® Active Directory, vous pouvez placer un groupe au sein d'un autre, en créant ainsi un groupe imbriqué. Les objets de rôle sont considérés comme des groupes et peuvent en inclure d'autres directement. You can add the existing nested group directly to the role and assign the appropriate rights and restrictions. De nouveaux utilisateurs peuvent venir s'ajouter au groupe existant ou au rôle.

Dans les mises en œuvres antérieures, seul un utilisateur sans schéma qui était un membre direct du groupe principal était autorisé à se connecter à iLO. En utilisant l'intégration sans schéma,les utilisateurs qui sont des membres indirects (membres d'un groupe qui est un groupe imbriqué du groupe principal) sont autorisés à se connecter à iLO.

Novell eDirectory n'autorise pas l'imbrication des groupes. Dans eDirectory, tout utilisateur pouvant lire un rôle est considéré comme l'un de ses membres. Lors de l'ajout d'un groupe existant, d'une unité organisationnelle ou d'une organisation à un rôle, ajoutez l'objet en tant qu'administrateur en lecture de ce rôle. Tous les membres de cet objet sont considérés comme membres de ce rôle. Il est possible d'ajouter de nouveaux utilisateurs au groupe existant ou au rôle.

Lors de l'utilisation d'affectations de privilèges d'annuaire ou administrateur dans le but d'augmenter le nombre des membres du rôle, les utilisateurs doivent pouvoir lire l'objet LOM correspondant au périphérique LOM. Certains environnements requièrent que les administrateurs d'un rôle soient également administrateurs en lecture de l'objet LOM afin d'authentifier correctement les utilisateurs.

Configuration de l'intégration d'annuaire dans le cadre du schéma HP

Lorsque vous utilisez l'intégration d'annuaire dans le cadre du schéma HP, iLO prend en charge à la fois Active Directory et eDirectory. Toutefois, ces services d'annuaire requièrent une extension du schéma.

Fonctionnalités prises en charge par l'intégration d'annuaire dans le cadre du schéma HP

La fonctionnalité iLO Directory Services (Services d'annuaire iLO) vous permet d'effectuer les tâches suivantes :

- Authentifier des utilisateurs à partir d'une base de données utilisateur évolutive, consolidée et partagée ;
- Contrôler les privilèges utilisateur (autorisation) à l'aide du service d'annuaire ;
- Utiliser des rôles dans le service d'annuaire pour l'administration au niveau du groupe des processeurs de supervision iLO et des utilisateurs iLO.

Cette opération doit être effectuée par un administrateur de schéma. La base de données des utilisateurs locaux est conservée. Le client peut choisir de ne pas utiliser d'annuaire, de recourir à une combinaison d'annuaires et de comptes locaux ou de faire appel à des annuaires exclusivement pour l'authentification.

REMARQUE : lorsque vous vous connectez via Diagnostics Port (Port de diagnostics), le serveur d'annuaire n'est pas disponible. Vous pouvez uniquement ouvrir une session à l'aide d'un compte local.

Configuration des services d'annuaire

Pour activer correctement la supervision via l'annuaire sur n'importe quel processeur de supervision Lights-Out :

1. Planification

   Passez en revue les sections suivantes :

   - « Services d'annuaire » (page 117)
   - « Schéma des services d'annuaire » (page 214)
   - « Supervision distante activée via l'annuaire » (page 152)

2. Installation

   a. Téléchargez la solution HP Lights-Out Directory Package contenant le programme d'installation de schémas, le programme d'installation de composants logiciels intégrables de supervision et les utilitaires de migration depuis le site Web HP (http://www.hp.com/servers/lights-out).

   b. Exécutez le programme d'installation de schémas (page 128) une seule fois pour étendre le schéma.

   c. Exécutez le programme d'installation de composants logiciels intégrables de supervision (page 131) et installez le composant logiciel intégrable approprié à votre service d'annuaire sur une ou plusieurs stations de supervision.

3. Mise à jour
   a. Réécrivez la ROM (voir « Mise à niveau du microprogramme iLO » page 32) sur le processeur de supervision Lights-Out à l'aide du microprogramme activé via l'annuaire.
   b. Configurez les paramètres du serveur d'annuaire et le nom distinct des objets processeur de supervision dans la page de paramètres d'annuaire (page 70) de l'interface graphique utilisateur de la carte iLO.
4. Supervision
   a. Créez un objet de périphérique de supervision et un objet de rôle (« Objets de services d'annuaire », page 137) à l'aide du composant logiciel intégrable.
   b. Affectez des droits à l'objet de rôle, selon les besoins, et associez le rôle à l'objet de périphérique de supervision.
   c. Ajoutez des utilisateurs aux objets de rôle.

   Pour plus d'informations sur la supervision du service d'annuaire, reportez-vous à la section « Supervision distante activée via l'annuaire » (page 152). Des exemples sont disponibles dans les sections « Services d'annuaire pour Active Directory » (page 131) et « Services d'annuaire pour eDirectory » (page 131).
5. Gestion des exceptions
   - Les utilitaires de migration Lights-Out sont plus faciles à utiliser avec un rôle Lights-Out unique. Si vous prévoyez de créer plusieurs rôles dans l'annuaire, il peut s'avérer nécessaire d'utiliser des utilitaires de génération de scripts d'annuaire tels que le script LDIFDE ou VB pour créer des combinaisons de rôles complexes. Pour plus d'informations, reportez-vous à la section « Utilisation des outils d'importation en masse » (page 159).
   - Si votre ancien microprogramme est doté de processeurs iLO ou RILOE, il peut s'avérer nécessaire de le mettre à jour manuellement à l'aide d'un navigateur. La configuration minimale requise pour mettre à jour le microprogramme à distance à l'aide des scripts RIBCL et de l'utilitaire de migration d'annuaire est la suivante :

Produit LOM	**Version minimale du microprogramme**
RILOE	2.41
RILOE II	Toutes versions
iLO	1.4x
iLO 2	1.1x

Une fois le schéma étendu, vous pouvez procéder à la configuration des services d'annuaire à l'aide des utilitaires de migration des annuaires HP Lights-Out (page 163). Les utilitaires de migration sont inclus dans la solution HP Lights-Out Directory Package. La version 1.13 de l'utilitaire de migration d'annuaire permet à Lights-Out d'importer et d'exporter, et prend en charge les diverses données utilisateur pour chaque processeur Lights-Out.

Documentation sur les schémas

Pour vous aider dans le processus de planification et d'approbation, HP fournit de la documentation sur les modifications apportées au schéma au cours de la procédure de configuration de ce dernier. Pour passer en revue les modifications apportées au schéma existant, reportez-vous à la section « Schéma des services d'annuaire » (page 214).

Prise en charge des services d'annuaire

Avec l'intégration d'annuaire dans le cadre du schéma HP, iLO prend en charge les services d'annuaire suivants :

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Novell eDirectory 8.7.3
- Novell eDirectory 8.7.1

Le logiciel iLO est conçu pour être utilisé avec les outils de supervision Microsoft® Active Directory Users and Computers (Utilisateurs et ordinateurs Active Directory) et Novell ConsoleOne, ce qui vous permet de superviser des comptes utilisateur sur Microsoft Active Directory ou Novell eDirectory. Cette solution ne fait aucune distinction entre les services eDirectory utilisés sur NetWare, Linux ou Windows®. L'extension du schéma de eDirectory requiert la version 1.4.0 ou ultérieure de la Machine virtuelle Java™ pour l'authentification SSL.

La carte iLO prend en charge l'utilisation de Microsoft® Active Directory sur les systèmes d'exploitation suivants :

- La famille de produits Windows® 2000 ;
- La famille de produits Windows® Server 2003 ;

iLO prend en charge eDirectory sous Red Hat Enterprise Linux AS 2.1.

Logiciels requis pour les schémas

La carte iLO requiert des logiciels spécifiques pour étendre le schéma et fournir des composants logiciels intégrables permettant de superviser votre réseau iLO. Un composant HP Smart téléchargeable contient le programme d'installation de schémas et de composants logiciels intégrables de supervision. Il est téléchargeable à partir du site Web (http://www.hp.com/servers/lights-out).

Programme d'installation de schémas

Le programme d'installation de schémas est fourni avec un ou plusieurs fichiers .xml. Ces fichiers contiennent le schéma à ajouter à l'annuaire. En général, un des fichiers contient le schéma central commun à tous les services d'annuaire pris en charge. Les autres contiennent uniquement des schémas propres au produit. .NET Framework est obligatoire pour utiliser le programme d'installation.

Le programme d'installation comporte trois écrans importants :

- Schema Preview (Aperçu du schéma)
- Configuration
- Results (Résultats)

Schema Preview (Aperçu du schéma)

L'écran Schema Preview (Aperçu du schéma) permet à l'utilisateur de visualiser les extensions proposées du schéma. Cet écran lit les fichiers de schéma sélectionnés, analyse le code XML et l'affiche sous la forme d'une arborescence. Il répertorie tous les détails des attributs et des classes qui seront installés.

Configuration

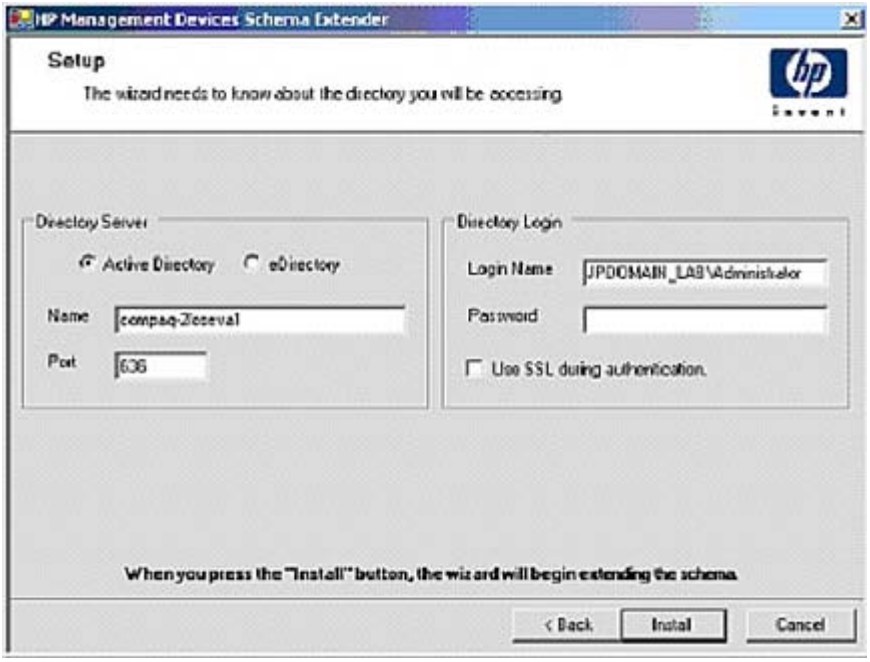
L'écran Setup (Configuration) permet d'entrer les informations pertinentes avant l'extension du schéma.

La section Directory Server (Serveur d'annuaire) de l'écran Setup (Configuration) permet de sélectionner Active Directory ou eDirectory et de paramétrer le nom de l'ordinateur et le port à utiliser pour les communications LDAP.

IMPORTANT : pour pouvoir étendre le schéma sur Active Directory, il faut que l'utilisateur soit un administrateur de schémas authentifié, que le schéma ne soit pas protégé en écriture et que l'annuaire soit propriétaire du rôle FSMO dans l'arborescence. Le programme d'installation tâchera de faire du serveur d'annuaire cible le contrôleur de schéma FSMO de la forêt.

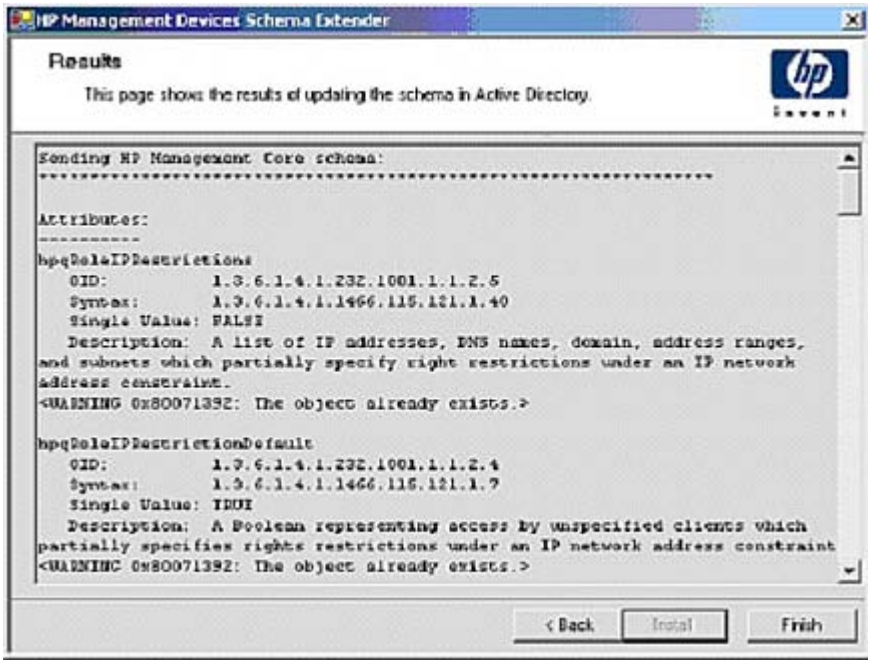
Pour obtenir un accès en écriture au schéma sur Windows® 2000, il convient de modifier le verrouillage de sécurité du registre. Si l'utilisateur sélectionne l'option **Active Directory**, le composant d'extension de schéma essaiera d'effectuer cette modification. Pour que cette opération aboutisse, l'utilisateur doit obligatoirement disposer des droits appropriés. L'accès en écriture au schéma est automatiquement activé sur Windows® Server 2003.

La section Directory Login (Connexion à l'annuaire) de l'écran Setup (Configuration) vous permet d'entrer votre nom de connexion et votre mot de passe. Ils peuvent s'avérer nécessaires pour procéder à l'extension du schéma. L'option Use SSL during authentication (Utiliser SSL pendant authentification) détermine le type d'authentification sécurisée à utiliser. Si cette option est sélectionnée, le protocole SSL permet d'authentifier l'annuaire. Si elle ne l'est pas et que la fonction Active Directory l'est, c'est l'authentification Windows NT® qui est utilisée. Si elle ne l'est pas et que la fonction eDirectory l'est, l'authentification de l'administrateur et l'extension du schéma s'effectuent à l'aide d'une connexion non codée (texte en clair).



Results (Résultats)

L'écran Results (Résultats) affiche les résultats de l'installation, notamment si le schéma a été étendu et les attributs qui ont été modifiés.



Programme d'installation de composants logiciels intégrables de supervision

Le programme d'installation de composants logiciels intégrables de supervision installe les composants nécessaires pour superviser les objets iLO dans l'annuaire Microsoft® Active Directory Users and Computers (Utilisateurs et ordinateurs) ou Novell ConsoleOne.

Les composants logiciels intégrables iLO sont utilisés pour exécuter les tâches suivantes lors de la création d'un annuaire iLO :

- Création et supervision des objets iLO et des objets de rôle (les objets de stratégie seront pris en charge ultérieurement) ;
- Création d'associations entre les objets iLO et les objets de rôle (ou de stratégie).

Services d'annuaire pour Active Directory

Les sections suivantes décrivent les conditions préalables à l'installation des services d'annuaire pour Active Directory, ainsi que les procédures de préparation et un exemple pratique. HP fournit un utilitaire permettant d'automatiser un grand nombre de processus de configuration d'annuaire. Vous pouvez télécharger la prise en charge des annuaires HP pour les processeurs de supervision sur le site Web HP (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Conditions préalables à l'installation de Active Directory

- Active Directory doit disposer d'un certificat numérique pour permettre à iLO de se connecter sur le réseau en toute sécurité.
- Active Directory doit disposer du schéma étendu pour décrire les propriétés et classes d'objet Lights-Out.
- La version du microprogramme doit être iLO v1.40 ou version ultérieure, ou iLO v1.00 ou version ultérieure.
- Les fonctions iLO Advanced doivent disposer d'une licence.

  Vous pouvez évaluer iLO Advanced avec une clé de licence d'évaluation gratuite téléchargeable à partir du site Web HP (http://h10018.www1.hp.com/wwsolutions/ilo/iloeval.html).

Les services d'annuaire de la carte iLO utilisent le protocole LDAP sur SSL pour communiquer avec les serveurs d'annuaire. Avant d'installer les composants logiciels intégrables et le schéma correspondant à Active Directory, lisez et gardez à disposition la documentation suivante :

IMPORTANT : l'installation de la fonction Directory Services (Services d'annuaire) pour la carte iLO requiert l'extension du schéma de Active Directory. Cette extension doit être réalisée par un administrateur de schémas Active Directory.

- Extending the Schema (Extension du schéma) dans le kit Microsoft® Windows® 2000 Server Resource Kit, disponible sur le site Web Microsoft® (http://msdn.microsoft.com).
- *Installing Active Directory* (Installation de Active Directory) dans le kit Microsoft® Windows® 2000 Server Resource Kit.
- Articles de la base de connaissances Microsoft®.

Ces articles sont accessibles à l'aide de l'option Knowledge Base Article ID Number Search (Recherche de numéro d'ID d'article de la base de connaissances) disponible sur le site Web Microsoft® (http://support.microsoft.com/).

- 216999 *Installing the remote server administration tools in Windows® 2000* (Installation des outils d'administration du serveur distant sous Windows® 2000)
- 314978 *Using the Adminpak.msi to install a server administration tool in Windows® 2000* (Utilisation de Adminpak.msi pour installer un outil d'administration du serveur sous Windows® 2000)
- 247078 *Enabling SSL communication over LDAP for Windows® 2000 domain controllers* (Activation de la communication SSL sur LDAP pour les contrôleurs de domaine Windows® 2000)
- 321051 *Enabling LDAP over SSL with a third-party certificate authority* (Activation de LDAP sur SSL par une autorité de certification tierce)
- 299687 *MS01-036 Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed (La fonction concernée par l'utilisation du protocole LDAP via SSL peut activer les mots de passe à modifier)*

La carte iLO nécessite une connexion sécurisée pour communiquer avec le service d'annuaire. Ceci requiert l'installation de Microsoft® CA. Reportez-vous à l'article 321051 de la base de connaissances de références techniques Microsoft® : *How to Enable LDAP over SSL with a Third-Party Certification Authority (Activation du protocole LDAP sur SSL avec une autorité de certification tierce).*

Préparation des services d'annuaire pour Active Directory

Pour configurer les services d'annuaire afin de les utiliser avec les processeurs de supervision iLO :

1. Installez Active Directory. Pour plus d'informations, reportez-vous au document *Installing Active Directory* (Installation de Active Directory) disponible dans le kit de ressources de Microsoft® Windows® 2000 Server.
2. Installez le Microsoft® Admin Pack (le fichier ADMINPAK.MSI, situé dans le sous-répertoire i386 du CD Windows® 2000 Server ou Advance Server). Pour plus d'informations, reportez-vous à l'article 216999 de la Base de connaissances Microsoft®.
3. Dans Windows® 2000, le verrouillage de sécurité qui empêche toute écriture accidentelle sur le schéma doit être temporairement désactivé. L'utilitaire d'extension du schéma permet de le faire si le service de registre distant est exécuté et que l'utilisateur dispose des privilèges appropriés. Vous pouvez également paramétrer `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ServicesParameters\Schema Update Allowed` (Jeu de commande en cours\Paramètres de services\Mise à jour schéma autorisée) dans le registre sur une valeur autre que zéro (voir « Déroulement du traitement lors de l'extension du schéma » du fichier *Installation of Schema Extensions* (Installation des extensions de schéma) du kit Windows® 2000 Server Resource Kit) ou exécuter la procédure suivante. Cette étape n'est pas nécessaire sous Windows® 2003 Server.

IMPORTANT : la modification incorrecte du registre peut gravement endommager votre système. HP vous recommande de créer une copie de sauvegarde de toutes les données importantes contenues sur l'ordinateur avant de modifier le registre.

a. Démarrez MMC.
b. Installez le composant logiciel intégrable Active Directory Schema (Schéma Active Directory) dans MMC.
c. Cliquez avec le bouton droit sur **Active Directory Schema** (Schéma Active Directory) et sélectionnez **Operations Master** (Maître des opérations).
d. Sélectionnez **The Schema may be modified on this Domain Controller** (Le schéma peut être modifié sur ce contrôleur de domaine).
e. Cliquez sur **OK**.

Il peut s'avérer nécessaire de développer le dossier **Active Directory Schema** (Schéma Active Directory) pour que la case à cocher apparaisse.

4. Créez un certificat ou installez Certificate Services (Services de certificat). Cette étape est nécessaire pour créer un certificat ou installer Certificate Services (Services de certificat) dans la mesure où la carte iLO communique avec Active Directory à l'aide de SSL. Vous devez installer Active Directory avant Certificate Services (Services de certificat).
5. Pour spécifier l'émission d'un certificat sur le serveur qui exécute Active Directory :
   a. Lancez Microsoft® Management Console (Console de supervision Microsoft) sur le serveur et ajoutez le composant logiciel intégrable de stratégie du domaine par défaut (Group Policy - Stratégie de groupe), puis naviguez jusqu'à Default domain policy object (Objet de stratégie du domaine par défaut).
   b. Cliquez sur **Computer Configuration>Windows Settings>Security Settings>Public Key Policies** (Configuration de l'ordinateur>Paramètres Windows>Paramètres de sécurité>Stratégies de clé publique).
   c. Cliquez avec le bouton droit sur **Automatic Certificate Requests Settings** (Paramètres des demandes de certificat automatiques) et sélectionnez **new>automatic certificate request** (Nouvelle demande de certificat automatique).
   d. Utilisez l'assistant pour sélectionner le modèle de contrôleur de domaine et l'autorité de certification de votre choix.
6. Téléchargez le composant Smart qui contient les programmes d'installation relatifs à l'utilitaire d'extension de schéma et aux composants logiciels intégrables. Il est téléchargeable à partir du site Web HP (http://www.hp.com/servers/lights-out).
7. Exécutez le programme d'installation de schéma pour étendre le schéma. Ce programme ajoute les objets HP appropriés au schéma.

   Le programme d'installation de schémas associe les composants logiciels intégrables Active Directory au nouveau schéma. L'utilitaire de configuration de l'installation des composants logiciels intégrables est un script de configuration Windows MSI qui est exécuté partout où MSI est pris en charge (Windows® XP, Windows® 2000, Windows® 98). Certaines parties de l'application d'extension du schéma ont toutefois besoin de .NET Framework, téléchargeable sur le site Web Microsoft® (http://www.microsoft.com).

Installation et initialisation des composants logiciels intégrables pour Active Directory

1. Exécutez l'application d'installation des composants logiciels intégrables.
2. Configurez le service d'annuaire de manière à disposer des objets et des relations appropriés pour la supervision de la carte iLO.

a. Utilisez les composants logiciels intégrables de supervision de HP pour créer des objets iLO, de stratégie et de rôle administrateur et utilisateur.
b. Utilisez les composants logiciels intégrables de supervision de HP pour créer des associations entre l'objet iLO, l'objet de stratégie et l'objet de rôle.
c. Reliez l'objet iLO aux objets de rôle administrateur et utilisateur (les rôles administrateur et utilisateur renvoient automatiquement à l'objet iLO).

Pour plus d'informations sur les objets iLO, reportez-vous à la section « Objets des services d'annuaire » (page 137).

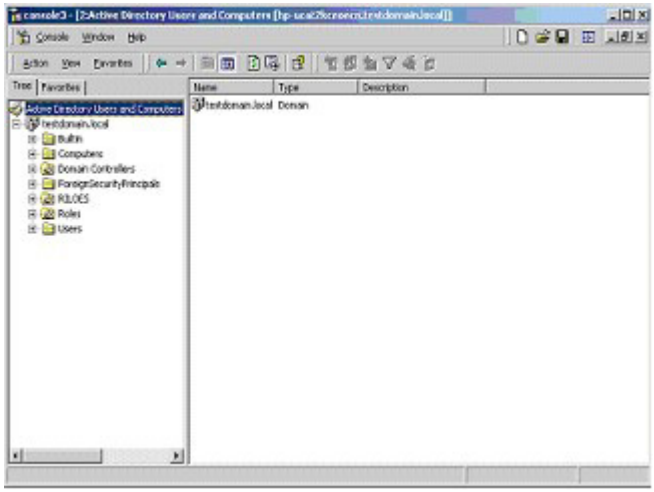
Vous devez au minimum créer :

- Un objet de rôle contenant un ou plusieurs utilisateurs et un ou plusieurs objets iLO ;
- Un objet iLO correspondant à chaque processeur de gestion iLO qui utilisera l'annuaire.

Exemple : création et configuration d'objets d'annuaire destinés à être utilisés avec la carte iLO dans Active Directory

L'exemple suivant explique comment configurer des rôles et des périphériques HP dans un annuaire d'entreprise dont le domaine est *domainetest.local* qui est constitué de deux unités organisationnelles, *Rôles* et *Cartes RILOE*.

Imaginons qu'une société possède un annuaire d'entreprise incluant le domaine *domainetest.local*, organisé comme illustré dans l'écran suivant.

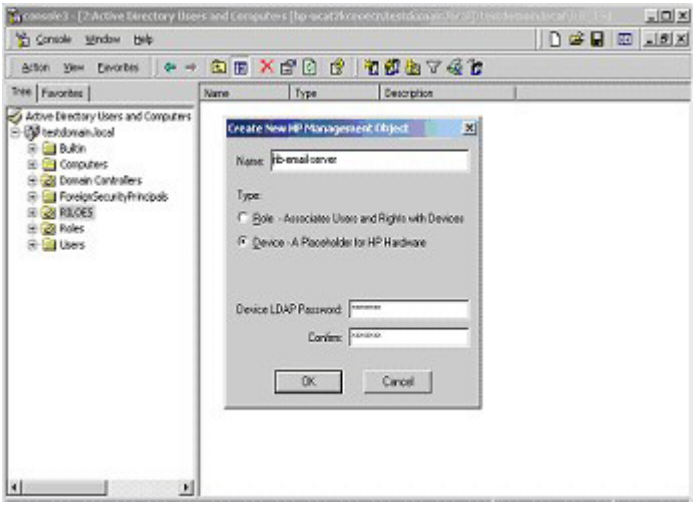


Créez une unité organisationnelle qui contiendra les périphériques Lights-Out supervisés par le domaine. Dans cet exemple, deux unités organisationnelles sont créées : *Rôles* et *Cartes RILOE*.

1. Utilisez les composants logiciels intégrables Active Directory Users and Computers (Utilisateurs et ordinateurs) fournis par HP pour créer des objets de supervision Lights-Out dans l'unité organisationnelle *CartesRILOE* pour plusieurs périphériques iLO.
   a. Cliquez avec le bouton droit sur l'unité organisationnelle Cartes RILOE localisée dans le domaine *domainetest.local* et sélectionnez **NewHPObject** (Nouvel objet HP).
   b. Sélectionnez **Device** (Périphérique) dans la boîte de dialogue Create New HP Management Object (Créer nouvel objet de supervision HP).
   c. Entrez un nom approprié dans le champ Name (Nom) de la boîte de dialogue. Dans cet exemple, le nom d'hôte DNS du périphérique iLO, *rib-email-serveur*, est le nom de l'objet de supervision Lights-Out, tandis que le nom de famille est *RILOEII*.

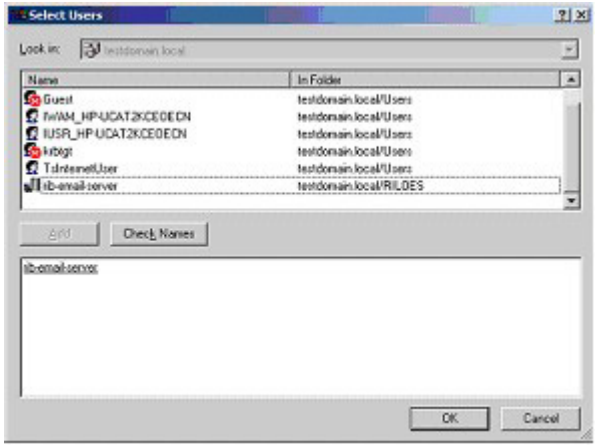
Entrez et confirmez le mot de passe dans les champs Device LDAP Password (Mot de passe LDAP du périphérique) et Confirm (Confirmation). Le périphérique utilise ce mot de passe pour authentifier l'annuaire, il doit donc être unique. Ce mot de passe est celui utilisé dans l'écran Directory Settings (Paramètres d'annuaire) de la carte iLO.

d. Cliquez sur **OK**.

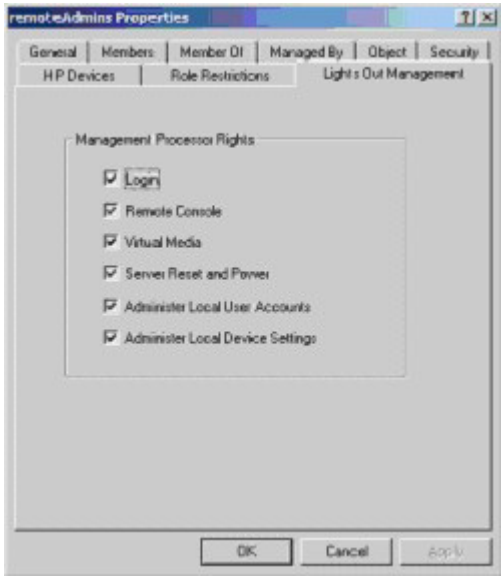


2. Utilisez les composants logiciels intégrables Active Directory Users and Computers (Utilisateurs et ordinateurs) fournis par HP pour créer des objets de rôle HP dans l'unité organisationnelle *Roles*.
   a. Cliquez avec le bouton droit sur l'unité organisationnelle Rôles, puis sélectionnez **New** (Nouveau) et **Object** (Objet).
   b. Sélectionnez **Role** (Rôle) dans le champ Type de la boîte de dialogue Create New HP Management Object (Créer nouvel objet de supervision HP).
   c. Entrez un nom approprié dans le champ Name (Nom) de la boîte de dialogue New HP Management Object (Nouvel objet de supervision HP). Dans cet exemple, le rôle regroupera les utilisateurs approuvés pour l'administration du serveur distant. Il sera baptisé *Adminsdistants*. Cliquez sur **OK**.
   d. Répétez cette procédure en créant un rôle pour les moniteurs de serveur distant (*Superviseursdistants*).
3. Utilisez les composants logiciels intégrables Active Directory Users and Computers (Utilisateurs et ordinateurs) fournis par HP pour attribuer des privilèges de rôle et associer les rôles à des utilisateurs et des périphériques.
   a. Cliquez avec le bouton droit sur le rôle **remoteAdmins** (Adminsdistants) dans l'unité organisationnelle Rôles du domaine *domainetest.local*, puis sélectionnez **Properties** (Propriétés).
   b. Sélectionnez l'onglet **HP Devices** (Périphériques HP), puis cliquez sur **Add** (Ajouter).

c. Dans la boîte de dialogue Select Users (Sélectionner des utilisateurs), cliquez sur l'objet Lights-Out Management (Supervision Lights-Out) créé à l'étape 2, *rib-email-serveur*, dans le dossier domainetest.local/Cartes RILOE. Cliquez sur **OK** pour fermer la boîte de dialogue, puis sur **Apply** (Appliquer) pour enregistrer la liste.



d. Ajoutez des utilisateurs au rôle. Cliquez sur l'onglet **Members** (Membres) et ajoutez des utilisateurs à l'aide du bouton Add (Ajouter) et de la boîte de dialogue Select Users (Sélectionner utilisateurs). Les périphériques et les utilisateurs sont à présent associés.



4. Utilisez l'onglet Lights Out Management (Supervision Lights Out) pour définir les privilèges associés au rôle. Tous les utilisateurs et groupes d'un rôle disposent des privilèges attribués au rôle sur tous les périphériques iLO supervisés par celui-ci. Dans cet exemple, les utilisateurs du rôle *Adminsdistants* accèdent aux fonctions iLO. Sélectionnez les cases en regard de chaque privilège, puis cliquez sur **Apply** (Appliquer). Cliquez sur **OK** pour fermer la feuille des propriétés.
5. En suivant la même procédure que celle décrite à l'étape 4, modifiez les propriétés du rôle *Superviseursdistants*, ajoutez le périphérique *rib-email-serveur* à la liste Managed Devices (Périphériques supervisés) de l'onglet HP Devices (Périphériques HP) et ajoutez des utilisateurs au rôle *Superviseursdistants* à l'aide de l'onglet Members (Membres). Puis, dans l'onglet Lights Out Management (Supervision Lights Out), sélectionnez la case en regard de Login (Connexion). Cliquez sur **Apply** (Appliquer), puis sur **OK**. Les membres du rôle Superviseursdistants pourront désormais s'authentifier et visualiser l'état du serveur.

Les privilèges utilisateur relatifs à un périphérique iLO correspondent à la somme de tous les privilèges attribués par l'ensemble des rôles dont l'utilisateur est membre et dans lesquels le périphérique iLO en question est supervisé. Si l'on se base sur les exemples précédents, un utilisateur appartenant à la fois aux rôles *Adminsdistants* et *Superviseursdistants* disposera de tous les droits, dans la mesure où ces droits sont affectés au rôle *Adminsdistants*.

Pour configurer un périphérique iLO et l'associer à un objet de supervision Lights-Out utilisé dans cet exemple, il faut recourir à des paramètres similaires à ceux qui sont présentés dans l'écran Directory Settings (Paramètres d'annuaire) ci-dessous.

```
RIB Object DN = cn=rib-email-server,ou=RILOES,dc=testdomain,dc=local
Directory User Context 1 = cn=Users,dc=testdomain,dc=local
```

Par exemple, pour obtenir un accès, l'utilisateur *Mel Moore*, qui possède l'ID unique *MooreM*, localisé dans l'unité organisationnelle *utilisateurs* dans le domaine *domainetest.local*, et qui est également repris dans les rôles *Adminsdistants* ou *Superviseursdistants*, est autorisé à se connecter à la carte iLO. Vous devez taper `testdomain\moorem ou moorem@testdomain.local ou Mel Moore`, dans le champ Login Name (Nom de connexion) de l'écran de connexion iLO et utiliser son mot de passe Active Directory dans le champ Password (Mot de passe) de cet écran.

Objets de services d'annuaire

Une parfaite virtualisation des périphériques supervisés dans le service d'annuaire constitue l'une des clés de la supervision basée sur les annuaires. Cette virtualisation permet en effet à l'administrateur d'établir des relations entre le périphérique supervisé et les utilisateurs ou groupes déjà présents dans le service d'annuaire. La supervision de la carte iLO par un utilisateur requiert trois objets de base dans le service d'annuaire :

- Supervision Lights-Out
- Rôle
- Utilisateur

Chaque objet représente un périphérique, un utilisateur ou une relation nécessaire pour la supervision basée sur les annuaires.

> **REMARQUE :** une fois les composants logiciels intégrables installés, vous devez redémarrer ConsoleOne et MMC pour visualiser les nouvelles entrées.

Une fois le composant logiciel intégrable installé, vous pouvez créer des objets et des rôles iLO dans l'annuaire. L'outil Users and Computers (Utilisateurs et ordinateurs) permet d'effectuer les tâches suivantes :

- Créer des objets iLO et des objets de rôle ;
- Ajouter des utilisateurs aux objets de rôle ;
- Définir des privilèges et des restrictions pour les objets de rôle.

Composants logiciels intégrables de Active Directory

Les sections suivantes traitent des options de supervision supplémentaires disponibles dans l'outil Active Directory Users and Computers (Utilisateurs et ordinateurs) après l'installation des composants logiciels intégrables HP.

HP Devices (Périphériques HP)

L'onglet HP Devices (Périphériques HP) permet d'ajouter à un rôle des périphériques HP à superviser. Cliquez sur **Add** (Ajouter) pour accéder à un périphérique spécifique et l'ajouter à la liste des périphériques membres. Cliquez sur **Remove** (Supprimer) pour accéder à un périphérique spécifique et le supprimer de la liste des périphériques membres.

Members (Membres)

Lorsque des objets utilisateur ont été créés, l'onglet Members (Membres) permet de superviser les utilisateurs appartenant au rôle. Cliquez sur **Add** (Ajouter) pour accéder à l'utilisateur à ajouter. Mettez un utilisateur existant en surbrillance et cliquez sur **Remove** (Supprimer) pour le supprimer de la liste des membres valides.

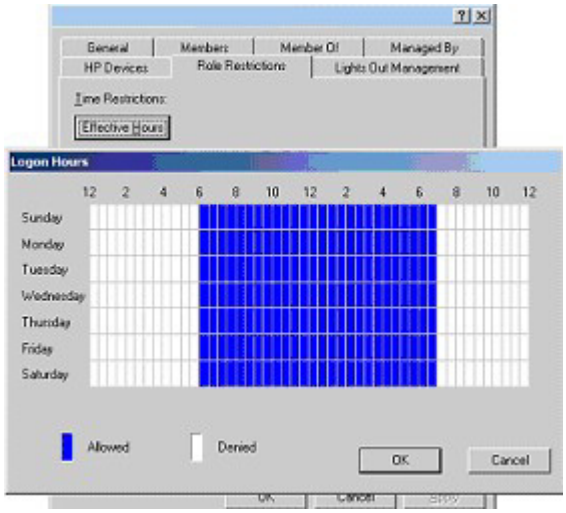
Restrictions de rôle de la fonction Active Directory

Le sous-onglet Role Restrictions (Restrictions de rôle) permet de définir des restrictions de connexion pour le rôle. Celles-ci incluent :

- Restrictions de temps
- Restrictions liées aux adresses réseau IP
  - IP/Mask (IP/Masque)
  - IP range (Plage d'adresses IP)
  - DNS name (Nom DNS)

Restrictions de temps

Vous pouvez superviser les heures de connexion mises à la disposition des membres du rôle en cliquant sur **Effective Hours** (Heures effectives) dans l'onglet Role Restrictions (Restrictions de rôle). La fenêtre contextuelle Logon Hours (Heures de connexion) permet de sélectionner le nombre d'heures disponibles pour la connexion, chaque jour de la semaine, par incréments d'une demi-heure. Vous pouvez modifier un seul carré en cliquant dessus ou modifier un ensemble de carrés en cliquant sur l'un d'eux et en maintenant le bouton de la souris enfoncé, puis en faisant glisser le curseur sur les carrés à modifier et en relâchant le bouton de la souris. Par défaut, l'accès est autorisé en permanence.



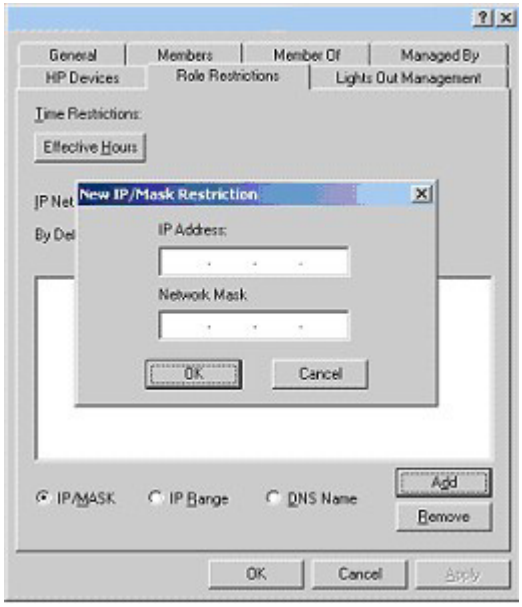
Accès à l'adresse IP ou au nom DNS du client

Il est possible d'accorder ou de refuser l'accès à une adresse IP, une plage d'adresses IP ou des noms DNS.

1. Dans le menu contextuel By Default (Par défaut), sélectionnez **Grant** (Autoriser) ou **Deny** (Refuser) pour autoriser ou refuser l'accès à partir de toutes les adresses, à l'exception des adresses IP, des plages d'adresses IP et des noms DNS spécifiés.
2. Sélectionnez les adresses à ajouter et le type de restriction, puis cliquez sur **Add** (Ajouter).
3. Dans la nouvelle fenêtre contextuelle de restriction, entrez les informations requises et cliquez sur **OK**. La nouvelle fenêtre s'affiche.

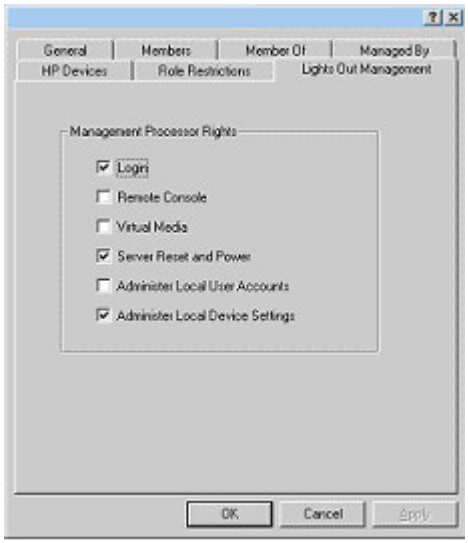
   L'option DNS Name (Nom DNS) permet de limiter l'accès à un nom DNS ou un sous-domaine unique, entré dans le formulaire host.company.com ou *.domain.company.com.
4. Cliquez sur **OK** pour enregistrer les modifications.

Pour supprimer une des entrées, mettez-la en surbrillance dans la liste et cliquez sur **Remove** (Supprimer).



Supervision de Lights-Out dans Active Directory

Après avoir créé un rôle, vous pouvez sélectionner les droits y afférents. Vous pouvez à présent définir les objets Utilisateurs et Groupes comme membres du rôle et attribuer ainsi aux utilisateurs ou à un groupe d'utilisateurs les droits accordés par le rôle. Les privilèges sont gérés dans l'onglet Lights Out Management (Supervision Lights Out).



Les privilèges disponibles sont les suivants :

- **Login** (Connexion) : cette option détermine si les utilisateurs peuvent se connecter aux périphériques associés.
- **Remote Console** (Console distante) : cette option permet à l'utilisateur d'accéder à la console distante.
- **Virtual Media** (Support virtuel) : cette option permet à l'utilisateur d'accéder aux fonctions du support virtuel iLO.
- **Server Reset and Power** (Réinitialisation et mise sous tension du serveur) : cette option permet à l'utilisateur d'accéder au bouton **Virtual Power** (Alimentation virtuelle) de la carte iLO afin de réinitialiser le serveur ou de le mettre hors tension à distance.
- **Administer Local User Accounts** (Administrer comptes utilisateur locaux) : cette option permet à l'utilisateur d'administrer des comptes. Il peut ainsi modifier les paramètres de son propre compte, ceux d'autres comptes, ajouter des utilisateurs ou encore en supprimer.
- **Administer Local Device Settings** (Administrer paramètres du périphérique local) : cette option permet à l'utilisateur de configurer les paramètres du processeur de supervision iLO. Ces paramètres incluent les options disponibles dans les écrans Global Settings (Paramètres généraux), Network Settings (Paramètres réseau), SNMP Settings (Paramètres SNMP) et Directory Settings (Paramètres d'annuaire) du navigateur de la carte iLO.

Services d'annuaire pour eDirectory

Les sections suivantes décrivent les conditions préalables à l'installation des services d'annuaire pour eDirectory, ainsi que les procédures de préparation et un exemple pratique.

Conditions préalables à l'installation de eDirectory

Les services d'annuaire de la carte iLO utilisent le protocole LDAP sur SSL pour communiquer avec les serveurs d'annuaire. Le logiciel iLO est conçu pour installer une arborescence eDirectory, version 8.6.1 et ultérieures. HP déconseille d'installer ce produit si vous possédez des serveurs eDirectory d'une version inférieure à 8.6.1. Avant d'installer les composants logiciels intégrables et les extensions de schéma pour eDirectory, lisez et gardez à disposition les documents d'information techniques suivants, disponibles sur le site Novell Support (http://support.novell.com).

L'installation de la fonction Directory Services (Services d'annuaire) pour la carte iLO requiert l'extension du schéma eDirectory. Cette extension doit être effectuée par un administrateur.

- TID10066591 *Novell eDirectory 8.6 NDS compatibility* (Compatibilité de Novell eDirectory 8.6 NDS)
- TID10057565 *Unknown objects in a mixed environment* (Objets inconnus dans un environnement mixte)
- TID10059954 *How to test whether LDAP is working correctly* (Tester le bon fonctionnement du protocole LDAP)
- TID10023209 *How to configure LDAP for SSL (secure) connections* (Configurer LDAP pour les connexions SSL sécurisées)
- TID10075010 *How to test LDAP authentication (Tester l'*authentification LDAP)

Installation et initialisation des composants logiciels intégrables pour eDirectory

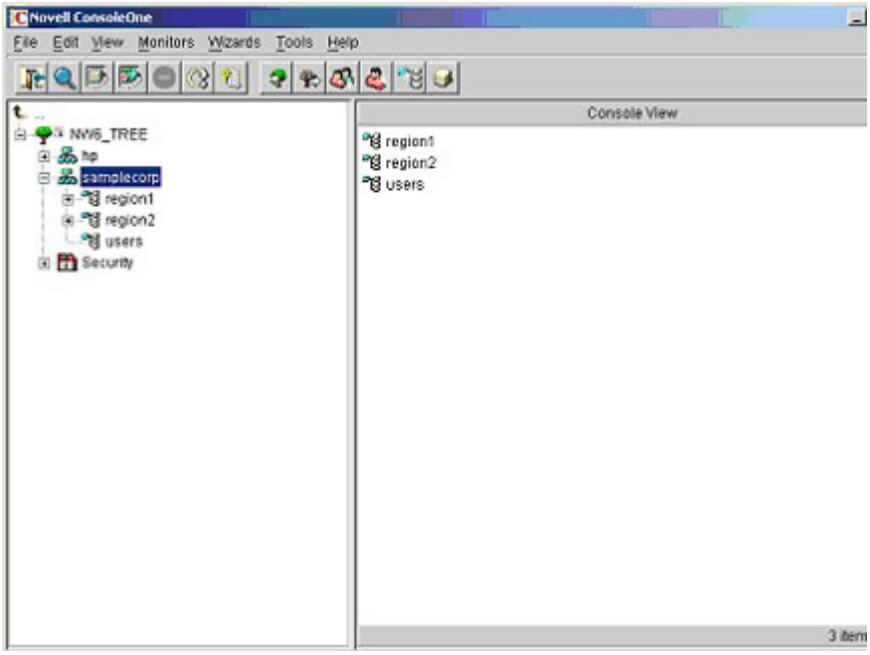
Pour obtenir des instructions pas à pas sur l'utilisation de l'application d'installation des composants logiciels intégrables, reportez-vous à la section « Installation et initialisation des composants logiciels intégrables pour Active Directory » (page 133).

REMARQUE : une fois les composants logiciels intégrables installés, vous devez redémarrer ConsoleOne et MMC pour visualiser les nouvelles entrées.

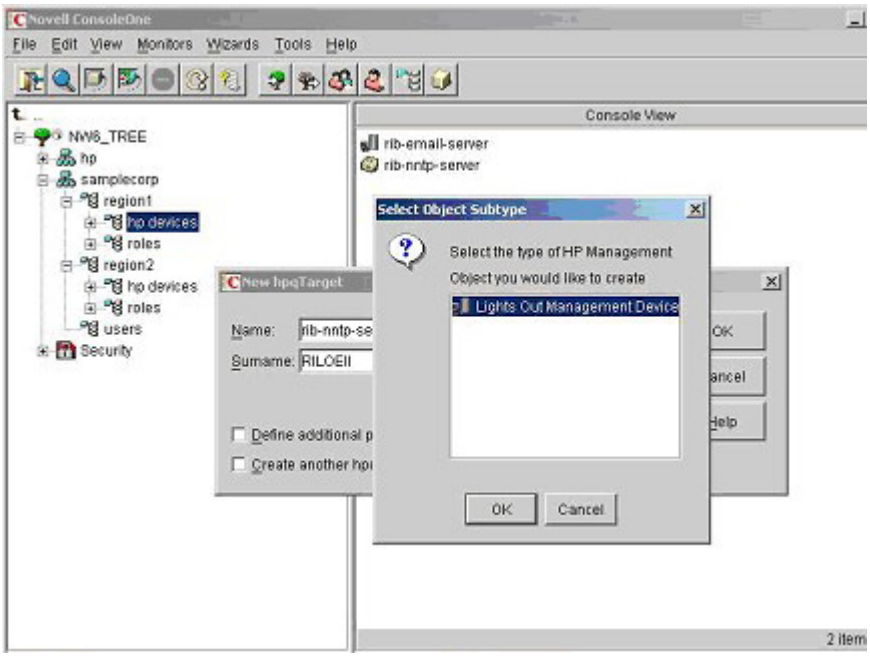
Exemple : Création et configuration d'objets d'annuaire destinés à être utilisés avec les périphériques LOM dans eDirectory

L'exemple suivant illustre la configuration de rôles et de périphériques HP dans une entreprise du nom de *stéexemple*, qui comprend deux régions : *région1* et *région2*.

Supposons que l'annuaire de *stéexemple* soit organisé conformément à l'illustration suivante.

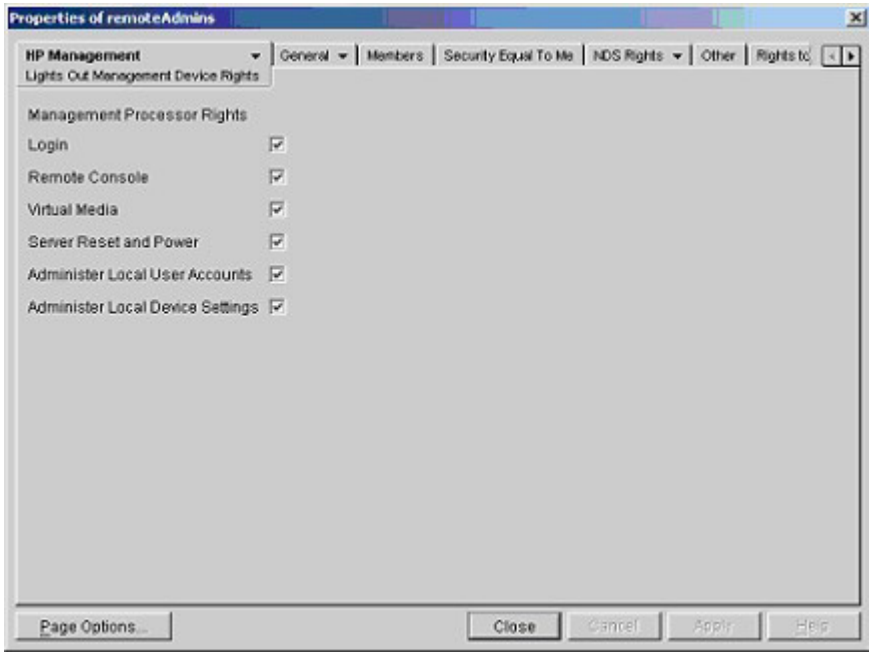


1. Créez des unités organisationnelles dans chaque région. Chacune d'elles est censée contenir les périphériques LOM et les rôles spécifiques à cette région. Dans cet exemple, deux unités organisationnelles, *rôles* et *périphériques hp*, sont créées dans chaque unité (*région1* et *région2*).
2. Créez les objets LOM dans les unité organisationnelles *périphériques hp* pour plusieurs périphériques iLO à l'aide des logiciels intégrables ConsoleOne fournis par HP.
   a. Cliquez avec le bouton droit sur l'unité organisationnelle **hp devices** (Périphériques HP) se trouvant dans l'unité organisationnelle *region1* (*région1)* et sélectionnez **New>Object** (Nouveau>Objet).
   b. Sélectionnez **hpqTarget** (Cible hpq) dans la liste de classes, puis cliquez sur **OK**.
   c. Entrez le prénom et le nom de famille appropriés à la page **New hpqTarget**. Dans cet exemple, le nom d'hôte DNS du périphérique iLO, *rib-email-serveur,* est utilisé comme nom de l'objet de supervision LOM, tandis que le nom de famille est *RILOEII*. Cliquez sur **OK.** La page Select Object Subtype (Sélectionner le sous-type de l'objet) s'affiche.
   d. Sélectionnez **Lights Out Management Device** (Périphérique de supervision Lights Out) et cliquez sur **OK**.
   e. Répétez la procédure pour d'autres périphériques iLO avec les noms DNS *rib-nntp-serveur* et *rib-file-serveur-utilisateurs1* dans *périphériques hp sous région1 et rib-file-serveur-utilisateurs2 et rib-app-serveur dans périphériques* hp sous région2.



3. Créez les objets HP Role dans l'unité organisationnelle *roles* à l'aide des logiciels intégrables ConsoleOne fournis par HP.
   a. Cliquez avec le bouton droit sur l'unité organisationnelle *roles* se trouvant dans l'unité organisationnelle *region2* et sélectionnez **New>Object** (Nouveau>Objet).
   b. Sélectionnez **hpqRole** (Rôle hpq) dans la liste de classes, puis cliquez sur **OK**.
   c. Entrez un nom approprié à la page **New hpqRole**. Dans cet exemple, le rôle regroupera les utilisateurs approuvés pour l'administration du serveur distant. Il sera baptisé *Adminsdistants*. Cliquez sur **OK**. La page Select Object Subtype (Sélectionner le sous-type de l'objet) s'affiche.
   d. Dans la mesure où ce rôle doit gérer les privilèges des périphériques de supervision Lights-Out, sélectionnez **Lights Out Management Devices** (Périphériques de supervision Lights Out) dans la liste et cliquez sur **OK**.
   e. Répétez cette procédure en créant un rôle pour les moniteurs de serveur distant (*Superviseursdistants*) dans rôles sous région1, ainsi que des rôles *Adminsdistants* et *Superviseursdistants* dans rôles sous région2.
4. Affectez des droits au rôle et associez les rôles à des utilisateurs et périphériques à l'aide des logiciels intégrables ConsoleOne fournis par HP.
   a. Cliquez avec le bouton droit sur le rôle **remoteAdmins** de l'unité organisationnelle *roles* (*rôles)* dans l'unité organisationnelle *region1* (*région1)* et sélectionnez **Properties** (Propriétés).
   b. Sélectionnez l'onglet **Role Managed Devices** (Périphériques supervisés par le rôle) de l'option HP Management (Supervision HP), puis cliquez sur **Add** (Ajouter).
   c. Utilisez la page Select Objects (Sélectionner des objets) pour accéder à l'unité organisationnelle *périphériques hp* sous *region1*. Sélectionnez les trois objets LOM créés à l'étape 2. Cliquez sur **OK>Apply** (OK>Appliquer).
   d. Cliquez sur l'onglet **Members** (Membres) et ajoutez des utilisateurs au rôle à l'aide du bouton **Add** (Ajouter) de la page Select Object (Sélectionner un objet). Les périphériques et les utilisateurs sont à présent associés.

e. Définissez les droits associés au rôle à l'aide de l'option Lights Out Management Device Rights (Privilèges des périphériques de supervision Lights Out) de l'onglet HP Management. Tous les utilisateurs d'un rôle disposent des privilèges attribués au rôle sur tous les périphériques iLO supervisés par celui-ci. Dans cet exemple, les utilisateurs du rôle *Adminsdistants* accèdent aux fonctions iLO. Sélectionnez les cases en regard de chaque privilège, puis cliquez sur **Apply** (Appliquer). Pour fermer la feuille des propriétés, cliquez sur **Close** (Fermer).



5. Modifiez les propriétés du rôle *Superviseursdistants* en suivant la même procédure que celle décrite à l'étape 4.
   a. Ajoutez les trois périphériques iLO dans *périphériques hp sous région1* à la liste **Managed Devices** (Périphériques supervisés) sous le sous-onglet Role Managed Devices (Périphériques supervisés par des rôles) de l'onglet HP Management (Supervision HP).
   b. Ajoutez des utilisateurs au rôle *Superviseursdistants* à l'aide de l'onglet Members (Membres).
   c. Sélectionnez la case Login (Connexion), puis cliquez sur **Apply** (Appliquer)**>Close** (Fermer). L'option Lights Out Management Device Rights de l'onglet HP Management permet aux membres du rôle *Superviseursdistants* de s'authentifier et visualiser l'état du serveur.

Les privilèges utilisateur relatifs à un périphérique LOM correspondent à la somme de tous les privilèges attribués par l'ensemble des rôles dont l'utilisateur est membre et dans lesquels le périphérique LOM en question est supervisé. Si l'on se base sur les exemples précédents, un utilisateur appartenant à la fois aux rôles Adminsdistants et Superviseursdistants disposera de tous les droits, dans la mesure où ces droits sont affectés au rôle Adminsdistants.

Pour configurer un périphérique LOM et l'associer à un objet de supervision LOM utilisé dans cet exemple, utilisez des paramètres similaires à ceux présentés ci-dessous dans l'écran Directory Settings (Paramètres d'annuaire).

REMARQUE : utilisez des virgules, et non des points, dans les noms distinctifs LDAP pour délimiter chaque composant.

```
RIB Object DN = cn=rib-email-server,ou=hp
devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

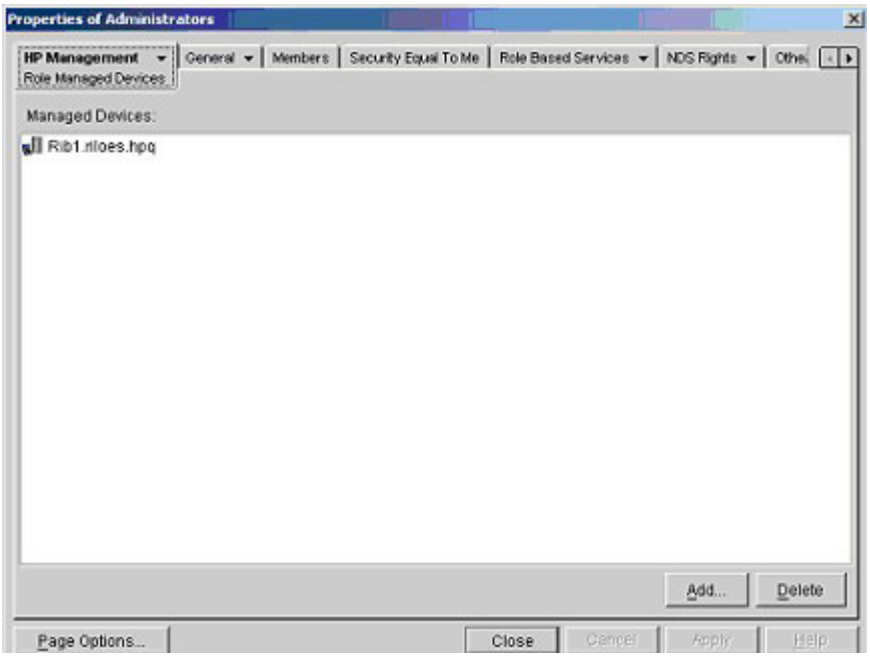
Par exemple, l'utilisateur CSmith, localisé dans l'unité organisationnelle utilisateurs de l'organisation stéexemple, qui est également membre de l'un des rôles *Adminsdistants ou Superviseursdistants*, est autorisé à se connecter à la carte iLO. Il peut taper `csmith` (peu importe la casse) dans le champ Login Name (Nom de connexion) de l'écran de connexion iLO et utiliser son mot de passe eDirectory dans le champ Password (Mot de passe) pour obtenir l'accès.

Objets de services d'annuaire pour eDirectory

Les objets de services d'annuaire activent la virtualisation des périphériques supervisés et les relations entre le périphérique supervisé et l'utilisateur ou les groupes déjà présents dans le service d'annuaire.

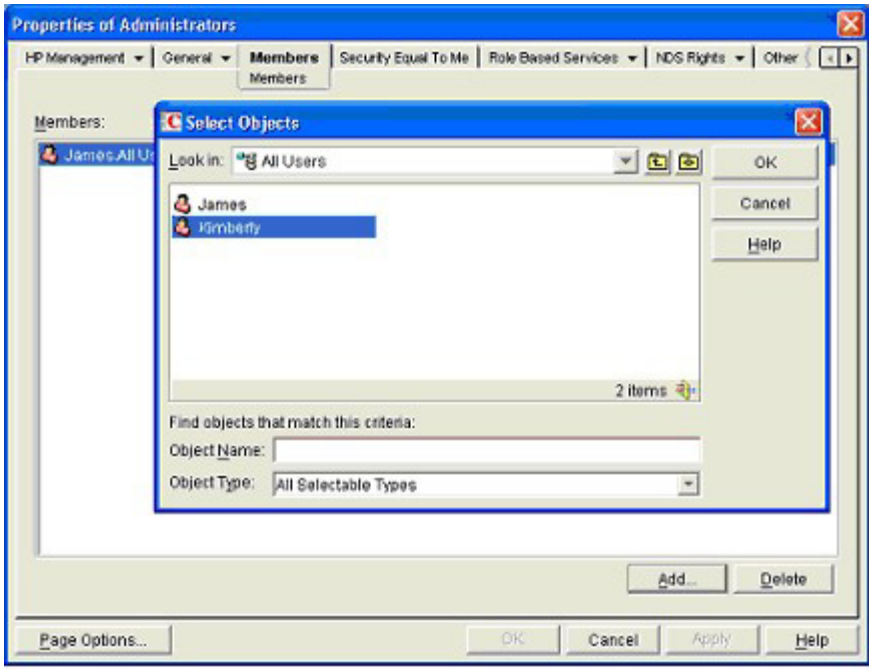
Périphériques supervisés par des rôles

Le sous-onglet Role Managed Devices (Périphériques supervisés par des rôles) permet d'ajouter les périphériques HP à superviser à un rôle. Le bouton **Add** (Ajouter) permet d'accéder à un périphérique HP en particulier et de l'ajouter comme périphérique supervisé.



Members (Membres)

Une fois que des objets utilisateur ont été créés, l'onglet Members (Membres) permet de superviser les utilisateurs appartenant au rôle. Cliquez sur **Add** (Ajouter) pour accéder à l'utilisateur à ajouter. Pour supprimer un utilisateur de la liste des membres valides, sélectionnez-le et cliquez sur le bouton **Delete** (Supprimer).

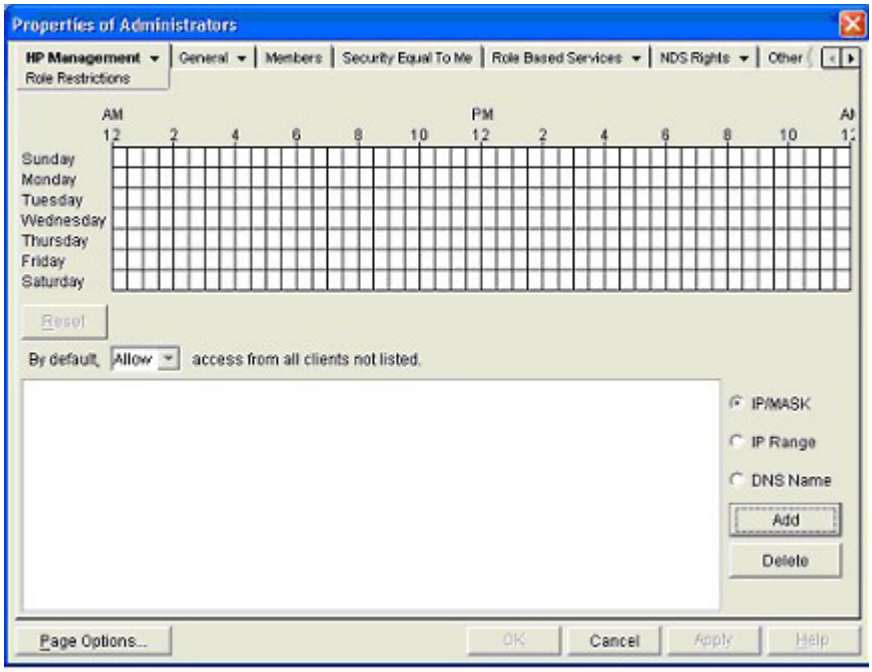


Role Restrictions (Restrictions de rôle) dans eDirectory

Le sous-onglet Role Restrictions (Restrictions de rôle) permet de définir des restrictions de connexion pour le rôle. Celles-ci incluent :

- Restrictions de temps
- Restrictions liées aux adresses réseau IP
  - IP/Mask (IP/Masque)
  - IP range (Plage d'adresses IP)

- DNS name (Nom DNS)



Restrictions de temps

Vous pouvez superviser les heures de connexion mises à la disposition des membres du rôle en utilisant la grille horaire affichée dans le sous-onglet Role Restrictions (Restrictions de rôle). Vous pouvez sélectionner les heures de connexion autorisées par incrément d'une demi-heure, et ce, pour chaque jour de la semaine. Vous pouvez modifier l'état d'un carré en cliquant sur celui-ci. Pour un groupe de carrés, cliquez sur le bouton de la souris et maintenez-le enfoncé, faites glisser le curseur sur les carrés à modifier, puis relâchez le bouton de la souris. Par défaut, l'accès est autorisé en permanence.

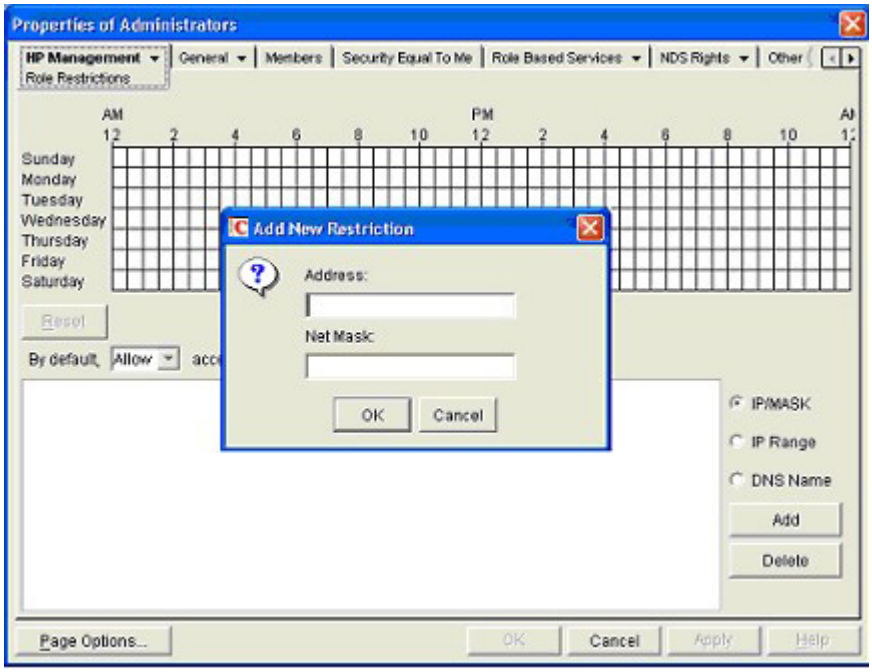
Accès à l'adresse IP ou au nom DNS du client

Il est possible d'accorder ou de refuser l'accès à une adresse IP, une plage d'adresses IP ou des noms DNS.

1. Dans le menu contextuel By Default (Par défaut), sélectionnez **Allow** (Autoriser) ou **Deny** (Refuser) pour autoriser ou refuser l'accès à toutes les adresses, à l'exception des adresses IP, des plages d'adresses IP et des noms DNS spécifiés.
2. Sélectionnez les adresses à ajouter et le type de restriction, puis cliquez sur **Add** (Ajouter).
3. Dans la fenêtre contextuelle Add New Restriction (Ajouter nouvelle restriction), entrez les informations requises et cliquez sur **OK**. La fenêtre contextuelle Add New Restriction (Ajouter nouvelle restriction) de l'option IP/Mask (IP/Masque) s'affiche.

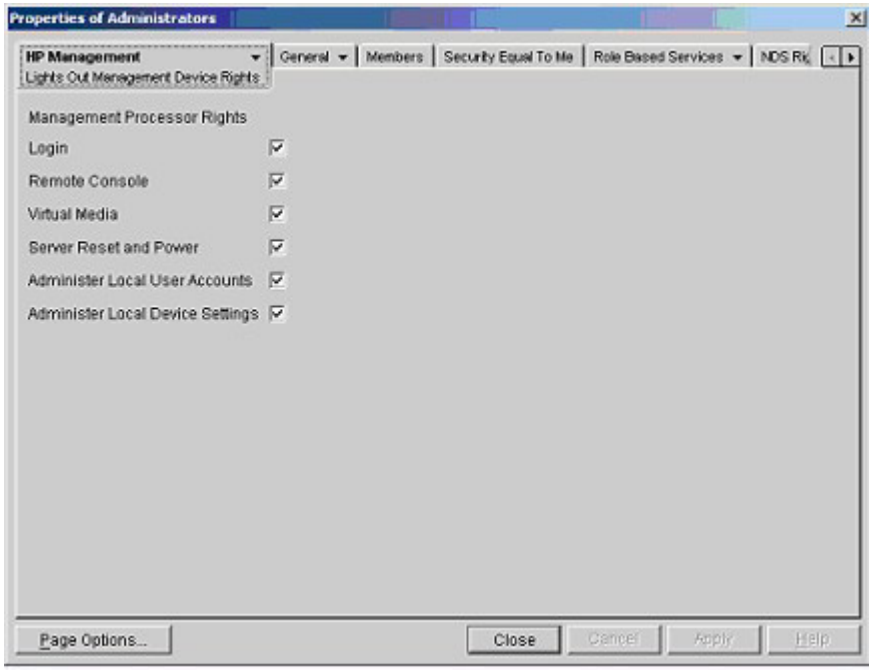
   L'option DNS Name (Nom DNS) permet de limiter l'accès à un nom DNS ou un sous-domaine unique, entré dans le formulaire host.company.com ou *.domain.company.com.
4. Cliquez sur **Apply** (Appliquer) pour enregistrer les modifications.

Pour supprimer une entrée, sélectionnez-la dans le champ, puis cliquez sur **Delete** (Supprimer).



Lights-Out Management (Supervision Lights-Out)

Après avoir créé un rôle, vous pouvez sélectionner les droits y afférents. Vous pouvez à présent définir les objets Utilisateurs et Groupes comme membres du rôle et attribuer ainsi aux utilisateurs ou à un groupe d'utilisateurs les droits accordés par le rôle. La gestion des droits s'effectue dans le sous-onglet Lights Out Management Device Rights (Privilèges des périphériques de supervision Lights Out) de l'onglet HP Management (Supervision HP).



Les privilèges disponibles sont les suivants :

- **Login** (Connexion) : cette option permet de contrôler la connexion des utilisateurs aux périphériques associés.

  L'accès à la connexion permet de créer un utilisateur chargé de la maintenance qui reçoit des alertes de la carte, mais n'a pas accès à la carte RILOE II.
- **Remote Console** (Console distante) : cette option permet à l'utilisateur d'accéder à la console distante.
- **Virtual Media** (Support virtuel) : cette option permet à l'utilisateur d'accéder à la fonction de disquette virtuelle et de support virtuel de la carte RILOE II.
- **Server Reset and Power** (Réinitialisation et mise sous tension du serveur) : cette option permet à l'utilisateur de réinitialiser le serveur ou de le mettre hors tension à distance.
- **Administer Local User Accounts** (Administrer comptes utilisateur locaux) : cette option permet à l'utilisateur d'administrer des comptes. Il peut ainsi modifier les paramètres de son propre compte, ceux d'autres comptes, ajouter des utilisateurs ou encore en supprimer.
- **Administer Local Device Settings** (Administrer les paramètres de périphériques locaux) : cette option permet à l'utilisateur de configurer les paramètres de la carte RILOE II. Ces paramètres incluent les options disponibles dans les écrans **Global Settings** (Paramètres généraux), **Network Settings** (Paramètres réseau), **SNMP Settings** (Paramètres SNMP) et **Directory Settings** (Paramètres d'annuaire) du navigateur Web RILOE II.

Connexion utilisateur via les services d'annuaire

Le champ Login Name (Nom de connexion) de la page de connexion iLO accepte tous les éléments suivants :

- Utilisateurs d'annuaire
- Noms distinctifs LDAP complets

  Exemple : CN=John Smith,CN=Users,DC=HP,DC=COM ou @HP.com

  REMARQUE : la forme simplifiée du nom d'utilisateur n'indique pas à l'annuaire le domaine auquel vous souhaitez accéder. Vous devez fournir le nom du domaine ou utiliser le nom distinctif LDAP de votre compte.
- Forme DOMAINE\nom d'utilisateur (Active Directory uniquement)

  Exemple : HP\jsmith
- Forme nom_utilisateur@domaine (Active Directory uniquement)

  Exemple : jsmith@hp.com

  REMARQUE : les utilisateurs d'annuaire spécifiés à l'aide de la forme consultable @ peuvent se trouver dans l'un des trois contextes consultables configurés dans Directory Settings (Paramètres d'annuaire).
- Forme « Nom d'utilisateur »

  Exemple : John Smith

  REMARQUE : les utilisateurs d'annuaire spécifiés à l'aide d'une forme du nom d'utilisateur peuvent se trouver dans l'un des trois contextes consultables configurés dans Directory Settings (Paramètres d'annuaire).

- Utilisateurs locaux - Id de connexion

  REMARQUE : sur la page de connexion iLO, la longueur maximale de Login Name (Nom de connexion) est de 39 caractères pour les utilisateurs locaux. Dans le cas des utilisateurs de services d'annuaire, elle est de 256 caractères.

Supervision distante activée via l'annuaire

Cette section traite des rubriques suivantes :

Introduction à la supervision distante activée via l'annuaire

Cette section est destinée aux administrateurs qui sont familiers avec les services d'annuaire et du produit iLO et souhaitent utiliser l'option d'intégration d'annuaire dans le cadre du schéma HP pour iLO. Vous devez d'abord vous familiariser avec la section « Services d'annuaire » (page 117), maîtriser la configuration et bien comprendre les exemples fournis.

La supervision distante activée via l'annuaire permet d'effectuer les tâches suivantes :

- Créer des objets de supervision Lights-Out

  Vous devez créer un objet de périphérique LOM pour représenter chaque périphérique qui utilisera le service d'annuaire pour authentifier et autoriser des utilisateurs. Reportez-vous à la section « Services d'annuaire »(page 117) pour plus d'informations sur la création des objets de périphérique LOM pour Active Directory (voir « Services d'annuaire pour Active Directory » page 117) et pour eDirectory (voir « Services d'annuaire pour eDirectory » page 117). En général, vous pouvez utiliser les composants logiciels intégrables fournis par HP pour créer des objets. Il est utile d'attribuer aux objets de périphérique LOM des noms significatifs, tel que l'adresse réseau du périphérique, le nom DNS, le nom du serveur hôte ou le numéro de série.

- Configurer des périphériques de supervision Lights-Out

  Chaque périphérique LOM utilisant le service d'annuaire pour authentifier et autoriser des utilisateurs doit être configuré avec les paramètres d'annuaire appropriés. Reportez-vous à la section « Configuration des paramètres d'annuaire » (page 71) pour plus d'informations sur les paramètres d'annuaire spécifiques. En général, vous pouvez configurer chaque périphérique avec l'adresse du serveur d'annuaire appropriée, le nom distinctif de l'objet LOM et tout autre contexte utilisateur. L'adresse du serveur est soit l'adresse IP ou le nom DNS du serveur de l'annuaire local ou pour plus de redondance, un nom DNS multi-hôte.

Création de rôles en fonction de la structure organisationnelle

Souvent, les administrateurs d'une organisation sont placés selon un ordre hiérarchique, dans lequel les administrateurs subordonnés doivent affecter les privilèges indépendamment des administrateurs responsables. Dans ce cas, il est utile d'avoir un rôle représentant les privilèges affectés par des administrateurs de grade élevé et d'autoriser les administrateurs subordonnés à créer et superviser leurs propres rôles.

Utilisation des groupes existants

De nombreuses organisations voudront répartir leurs utilisateurs et leurs administrateurs en groupes. Dans de nombreux cas, il convient d'utiliser les groupes existants et de les associer avec un ou plusieurs objets de rôle de supervision Lights-Out. Lorsque les périphériques sont associés à des objets de rôle, l'administrateur contrôle l'accès aux périphériques Lights-Out associés au rôle en ajoutant ou supprimant des membres au sein des groupes.

Lors de l'utilisation de Microsoft® Active Directory, il est possible de placer un groupe dans un autre ou des groupes imbriqués. Les objets de rôle sont considérés comme des groupes et peuvent en inclure d'autres directement. Ajoutez directement le groupe imbriqué existant au rôle et affectez les privilèges et les restrictions appropriés. De nouveaux utilisateurs peuvent venir s'ajouter au groupe existant ou au rôle.

Novell eDirectory n'autorise pas l'imbrication des groupes. Dans eDirectory, tout utilisateur pouvant lire un rôle est considéré comme l'un de ses membres. Lors de l'ajout d'un groupe existant, d'une unité organisationnelle ou d'une organisation à un rôle, ajoutez l'objet en tant qu'administrateur en lecture de ce rôle. Tous les membres de cet objet sont considérés comme membres de ce rôle. Il est possible d'ajouter de nouveaux utilisateurs au groupe existant ou au rôle.

Lors de l'utilisation d'affectations de privilèges d'annuaire ou administrateur dans le but d'augmenter le nombre des membres du rôle, les utilisateurs doivent pouvoir lire l'objet LOM correspondant au périphérique LOM. Certains environnements requièrent que les administrateurs d'un rôle soient également administrateurs en lecture de l'objet LOM afin d'authentifier correctement les utilisateurs.

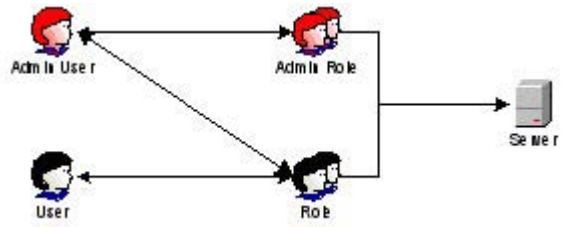
Utilisation des rôles multiples

La plupart des déploiements n'exigent pas qu'un même utilisateur soit dans les différents rôles qui supervisent un périphérique donné. Cependant, ces configurations sont utiles pour la construction de relations de privilèges complexes. Lors de la construction de relations de rôles multiples, les utilisateurs reçoivent tous les privilèges affectés par chaque rôle applicable. Les rôles peuvent uniquement accorder des privilèges mais pas les révoquer. Si un rôle accorde un privilège à un utilisateur, l'utilisateur disposera de ce privilège, même si l'utilisateur appartient, par ailleurs, à un autre rôle qui ne lui accorde pas ce privilège.

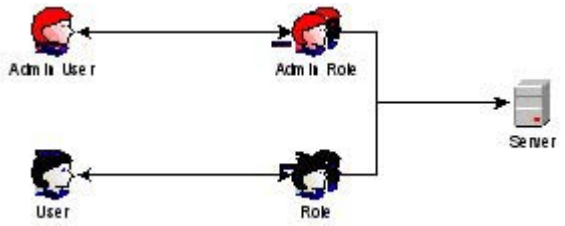
Généralement, un administrateur d'annuaire crée un rôle de base avec un nombre minimum de privilèges affectés, puis il crée des rôles supplémentaires pour ajouter des privilèges supplémentaires. Ces privilèges supplémentaires sont ajoutés dans des circonstances spécifiques ou à un sous-ensemble spécifique d'utilisateurs de rôles de base.

Par exemple, une organisation peut avoir deux types d'utilisateurs, des administrateurs du périphérique LOM ou du serveur hôte et des utilisateurs du périphérique LOM. Dans ce cas, il serait sensé de créer deux rôles, l'un pour les administrateurs et l'autre pour les utilisateurs. Si les deux rôles incluent certains périphériques identiques, ils n'accordent pas les mêmes privilèges. Parfois, il est utile d'affecter des privilèges génériques au rôle de moindre importance et d'y inclure des administrateurs LOM ainsi que le rôle administratif.

Un utilisateur admin accède au privilège de connexion par l'intermédiaire du groupe d'utilisateurs ordinaire. Des privilèges plus avancés sont affectés via Admin role, le rôle administrateur, qui affecte les privilèges supplémentaires : Server Reset (Réinitialisation du serveur) et Remote Console (Console distante).

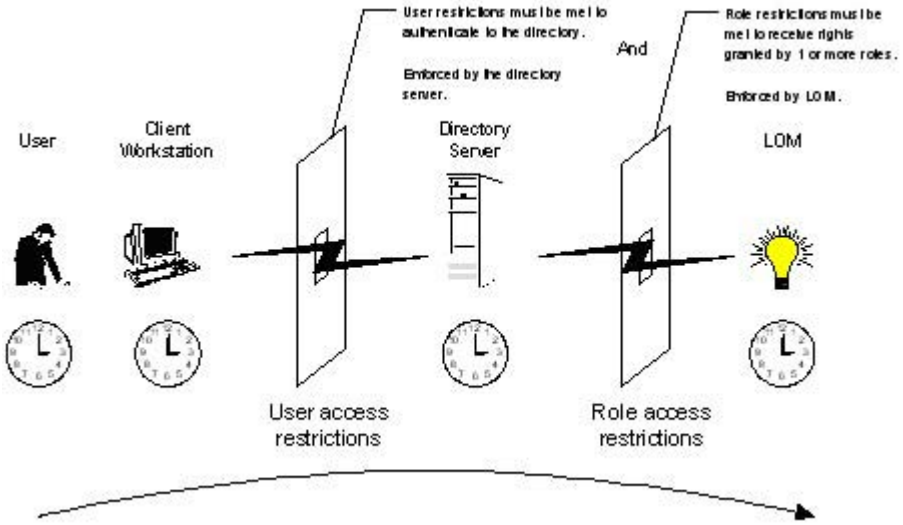


Admin Role, le rôle administrateur, affecte tous les privilèges administrateur : Server Reset (Réinitialisation du serveur), Remote Console (Console distante) et Login (Connexion).



Application des restrictions de connexion à l'annuaire

Il existe deux jeux de restrictions qui limitent potentiellement l'accès d'un utilisateur d'annuaire aux périphériques LOM. Les restrictions d'accès utilisateur limitent l'accès utilisateur à l'authentification de l'annuaire. Les restrictions d'accès de rôle limitent la capacité d'un utilisateur authentifié à recevoir les privilèges LOM, en fonction des privilèges spécifiés dans un ou plusieurs rôles.



Restrictions de rôles

Les restrictions permettent aux administrateurs de limiter le champ d'application d'un rôle. Un rôle n'accorde des privilèges qu'aux utilisateurs satisfaisant aux restrictions du rôle en question. Le recours à des rôles restreints permet de doter les utilisateurs de privilèges dynamiques qui changent en fonction de l'heure de la journée et de l'adresse réseau du client.

IMPORTANT : lorsque des annuaires sont activés, l'accès à un iLO donné est basé sur la condition que l'utilisateur a un accès en lecture sur un objet Rôle qui contient l'objet iLO correspondant. Ceci inclut, mais sans s'y limiter, les membres répertoriés dans l'objet Rôle. Si le rôle est configuré pour autoriser la propogation de permissions héritées d'un parent, les membres du parent ayant des privilèges d'accès en lecture peuvent également accès à iLO. Pour afficher la liste de contrôle d'accès, naviguez vers Utilisateurs et ordinateurs, ouvrez l'écran de propriétés de l'objet rôle, puis sélectionnez l'onglet **Sécurité**.

Pour obtenir des instructions pas à pas sur la création de restrictions liées à l'heure et au réseau, reportez-vous aux sections « Restrictions de rôle de la fonction Active Directory » (page 139) et « Role Restrictions (Restrictions de rôle) dans eDirectory » (page 147).

Restrictions de temps sur les rôles

Les administrateurs peuvent placer des restrictions de temps sur les rôles LOM. Les utilisateurs bénéficient de privilèges spécifiés pour les périphériques LOM listés dans le rôle, seulement s'ils sont membres du rôle et s'ils satisfont aux restrictions de temps définies pour ce rôle.

Les périphériques LOM utilisent le temps de l'hôte local pour appliquer des restrictions de temps. Si l'horloge du périphérique LOM n'est pas réglée, la restriction de temps imposée au rôle échoue, sauf si aucune restriction temporelle n'a été spécifiée pour ce rôle.

Les restrictions de temps basées sur les rôles ne sont satisfaites que si le temps est paramétré sur le périphérique LOM. Le temps est normalement réglé lors de l'amorçage de l'hôte. Il est maintenu par l'exécution des agents du système d'exploitation hôte, qui permet au périphérique LOM de compenser les années bissextiles et minimiser la désynchronisation de l'horloge par rapport à l'hôte. Les événements tels qu'une panne inopinée de courant ou le flashage du microprogramme LOM peuvent empêcher le réglage de l'horloge du périphérique LOM. Le temps de l'hôte doit également être correct afin que le périphérique LOM puisse garder l'heure exacte pendant le flashage du microprogramme.

Restrictions d'adresses de rôles

Les restrictions d'adresses de rôles sont appliquées par le microprogramme LOM, en fonction de l'adresse IP réseau du client. Lorsque les restrictions d'adresses sont satisfaites pour un rôle donné, les privilèges accordés par ce rôle s'appliquent.

Les restrictions d'adresses peuvent être difficiles à gérer si l'accès est tenté via le coupe-feu ou le serveur proxy réseau. Ces deux mécanismes peuvent modifier l'adresse réseau apparente du client, provoquant ainsi l'application des restrictions d'adresses de manière inattendue.

Restrictions utilisateur

Vous avez la possibilité de limiter l'accès à l'annuaire en définissant des restrictions temporelles ou des restrictions liées aux adresses.

Restrictions d'adresses utilisateur

Les administrateurs peuvent placer des restrictions d'adresses réseau sur un compte utilisateur d'annuaire. Ces restrictions sont alors appliquées par le serveur d'annuaire. Reportez-vous à la documentation relative au service d'annuaire pour plus d'informations sur l'application des restrictions d'adresses aux clients LDAP, par exemple pour un utilisateur qui se connecte à un périphérique LOM.

Les restrictions d'adresses réseau placées sur l'utilisateur dans l'annuaire peuvent ne pas s'appliquer comme prévu si l'utilisateur d'annuaire se connecte via un serveur proxy. Lorsqu'un utilisateur se connecte à un périphérique LOM en tant qu'utilisateur d'annuaire, le périphérique LOM tente une authentification sur l'annuaire, en tant qu'utilisateur d'annuaire. Cela qui signifie que les restrictions d'adresse placées sur le compte utilisateur s'appliquent lors de l'accès au périphérique LOM. Cependant, du fait que l'utilisateur est relié par un serveur proxy au périphérique LOM, l'adresse réseau de la tentative d'authentification est celle du périphérique LOM et non celle du poste de travail client.

Restrictions de la plage d'adresses IP

Les restrictions de la plage d'adresses IP permettent à l'administrateur de spécifier les adresses réseau dont l'accès est accordé ou refusé par la restriction. La plage d'adresses est généralement spécifiée dans un format de plage inférieur/supérieur. Une plage d'adresses peut être spécifiée pour accorder ou refuser l'accès à une seule adresse. Les adresses appartenant à la plage d'adresses IP inférieure/supérieure obéissent à la restriction d'adresse IP.

Restrictions liées au masque de réseau et à l'adresse IP

Les restrictions liées à l'adresse IP et au masque de sous-réseau permettent à l'administrateur de spécifier une plage d'adresses dont l'accès est accordé ou refusé par la restriction. Ce format possède des capacités similaires à celles d'une plage d'adresses IP mais peut être plus natif pour votre environnement réseau. Une plage d'adresses IP et de masques de sous-réseau est généralement spécifiée à l'aide d'une adresse de sous-réseau et d'une adresse de masque en bit, qui identifie les adresses se trouvant sur le même réseau logique.

En mode binaire, si les bits d'une adresse de système client, augmentée des bits du masque de sous-réseau, correspondent à l'adresse de sous-réseau de restriction, le système client obéit à la restriction.

Restrictions basées sur le protocole DNS

Les restrictions basées sur le protocole DNS utilisent le service d'attribution de nom de réseau pour examiner le nom logique du système client en recherchant les noms de système affectés aux adresses IP du client. Les restrictions DNS requièrent un serveur doté d'un nom fonctionnel. Si le service d'attribution de nom est inaccessible ou en panne, les restrictions DNS ne peuvent être mises en correspondance et elles échouent.

Les restrictions basées sur le protocole DNS peuvent limiter l'accès à un nom de système spécifique ou à des systèmes partageant un suffixe de domaine commun. Par exemple, la restriction DNS www.hp.com correspond à des hôtes auxquels est affecté le nom de domaine www.hp.com. Cependant, la restriction DNS *.hp.com correspond à tous les systèmes HP.

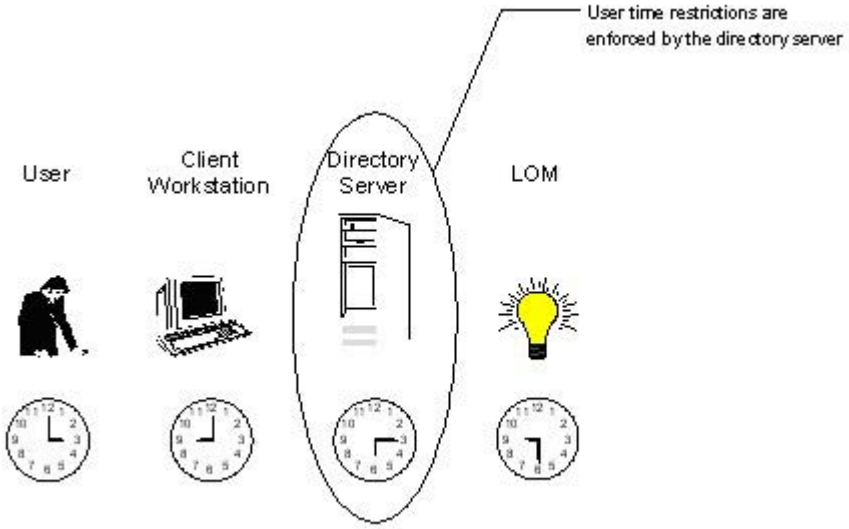
Les restrictions DNS risquent de susciter des ambiguïtés car un système hôte peut avoir plusieurs points d'origine. Les restrictions DNS ne correspondent pas nécessairement en tous points à un seul système.

L'utilisation des restrictions basées sur le protocole DNS peut créer des complications au niveau de la sécurité. Les protocoles de services d'attribution de noms ne sont pas sécurisés. Un individu mal intentionné, ayant accès au réseau, peut placer un service DNS de terminaison sur le réseau, créant de faux critères de restrictions d'adresses. Les stratégies en matière de sécurité organisationnelle devraient être prises en compte lors de l'implémentation de restrictions d'adresses basées sur le protocole DNS.

Application des restrictions de temps à l'utilisateur

Les administrateurs peuvent placer des restrictions de temps sur les comptes des utilisateurs d'annuaire. Les restrictions de temps limitent la capacité de l'utilisateur à se connecter (s'authentifier) à l'annuaire. Généralement, les restrictions de temps sont appliquées à l'aide du temps défini sur le serveur d'annuaire. Cependant, si le serveur d'annuaire est situé dans un fuseau horaire différent ou que l'accès ait lieu à une réplique se trouvant dans fuseau horaire différent, les informations relatives au fuseau horaires émanant de l'objet supervisé pourront être utilisées pour effectuer les ajustements horaires nécessaires.

Le serveur d'annuaire évalue les restrictions de temps utilisateur, mais la détermination peut être compliquée par les changements de fuseau horaire ou le mécanisme d'authentification.



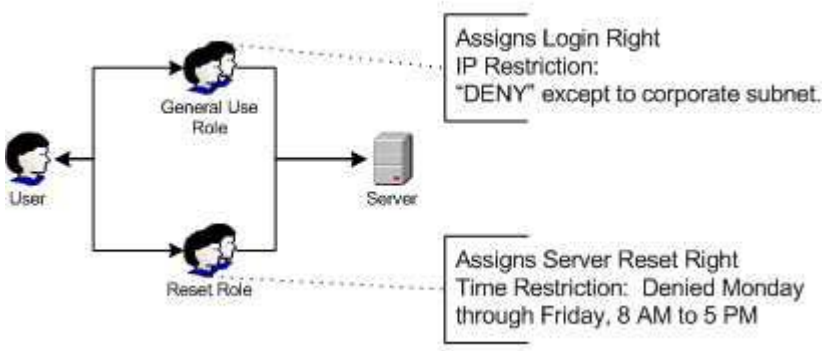
Création de restrictions et de rôles multiples

L'application la plus utile au niveau des rôles multiples consiste à restreindre un ou plusieurs privilèges de sorte que ces derniers ne s'appliquent pas à toutes les situations. D'autres rôles fournissent différents privilèges sous d'autres contraintes. L'utilisation de restrictions et de rôles multiples permet à l'administrateur de créer des relations de privilèges complexes et arbitraires avec un nombre minimum de rôles.

Par exemple, une organisation peut avoir une stratégie de sécurité dans laquelle les administrateurs LOM sont autorisés à utiliser le périphérique LOM à partir du réseau entreprise mais ne peuvent réinitialiser le serveur qu'en dehors des heures ouvrées.

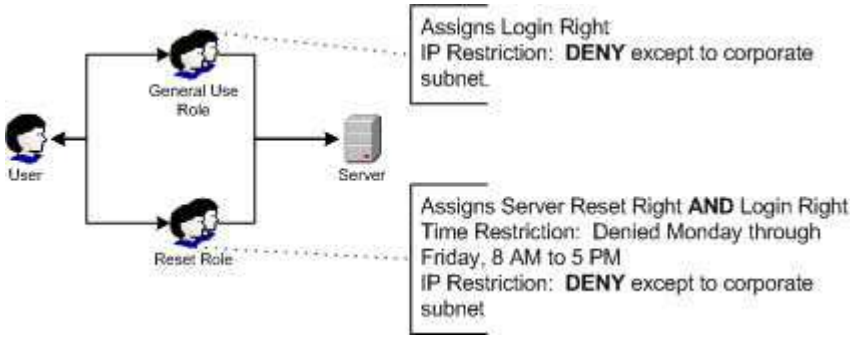
Les administrateurs d'annuaire pourraient être tentés de créer deux rôles pour remédier à cette situation, mais il faut être extrêmement prudent à ce sujet. En effet, créer un rôle fournissant les privilèges de réinitialisation de serveur requis et restreindre son application aux heures non ouvrées permettrait à des administrateurs extérieurs au réseau de l'entreprise de réinitialiser le serveur, ce qui est contraire à la plupart des stratégies de sécurité.

Dans l'exemple donné, la stratégie de sécurité édicte que l'utilisation générale soit restreinte aux clients appartenant au sous-réseau d'entreprise et que la capacité de réinitialisation du serveur soit restreinte, en plus, après les heures d'ouverture normales.



Alternativement, l'administrateur d'annuaire pourrait créer un rôle qui accorderait le privilège de connexion et le restreindrait au réseau d'entreprise, puis en créerait un autre qui accorderait uniquement le privilège de réinitialisation de serveur et en restreindrait l'exercice après les heures d'ouverture normales. Cette configuration est plus facile à superviser mais elle est plus risquée car une administration en continu peut créer un autre rôle qui accorderait le privilège de connexion aux utilisateurs dotés d'adresses extérieures au réseau d'entreprise. Cela pourrait permettre d'accorder, de façon fortuite, aux administrateurs LOM relevant du rôle de réinitialisation du serveur, la capacité de réinitialiser le serveur depuis n'importe où, à condition qu'ils satisfassent aux contraintes de temps spécifiques à ce rôle.

La précédente configuration répond aux exigences de la stratégie de sécurité de l'entreprise. Cependant, le fait d'ajouter un nouveau rôle qui accorderait le privilège de connexion pourrait, par inadvertance, accorder les privilèges de réinitialisation du serveur depuis l'extérieur du sous-réseau d'entreprise après les heures de travail. Une solution plus gérable consisterait à restreindre le rôle Reset (Réinitialisation) ainsi que le rôle General Use (Utilisation générale).



Utilisation des outils d'importation en masse

L'ajout et la configuration d'objets LOM en grand nombre requièrent beaucoup de temps. HP fournit plusieurs utilitaires permettant de vous assister dans ces tâches. Vous trouverez ci-dessous une brève description des utilitaires disponibles.

- Utilitaire de migration HP Lights-Out

  HPQLOMIG.EXE, l'utilitaire de migration HP Lights-Out, permet d'importer et de configurer plusieurs périphériques LOM. Il comporte une interface graphique qui fournit une approche étape par étape à l'implémentation ou la mise à niveau des processeurs de supervision en grand nombre. HP recommande d'utiliser cette méthode de l'interface graphique lors de la mise à niveau de plusieurs processeurs de supervision. Pour plus d'informations, reportez-vous à la section « Utilitaires de migration d'annuaires Lights-Out » (page 163).

- Utilitaire de commande de migration Lights-Out HP

  HPQLOMGC.EXE, l'utilitaire de commande de migration Lights-Out HP, offre une approche de la migration basée sur la ligne de commande plutôt que sur l'interface graphique. Cet utilitaire fonctionne conjointement avec les fonctionnalités de lancement des applications et de requête de Systems Insight Manager pour configurer simultanément plusieurs périphériques. Les clients qui doivent configurer un nombre limité de périphériques LOM pour utiliser les services d'annuaire peuvent opter pour l'approche de ligne de commande. Pour plus d'informations, reportez-vous à la section « Utilitaires de migration d'annuaires Lights-Out » (page 163).

- Possibilités de Systems Insight Manager :
  - supervision de plusieurs périphériques LOM ;
  - identification des périphériques LOM en tant que processeurs de supervision à l'aide de CPQLOCFG pour envoyer un fichier de scripts RIBCL XML vers un groupe de périphériques LOM pour superviser ces derniers. Les processeurs LOM exécutent alors les actions spécifiées dans le fichier RIBCL et envoient une réponse au ficher journal de CPQLOCFG. Pour plus d'informations, reportez-vous aux sections « Administration de groupe et génération de scripts iLO 2 » et « Langage de commande de la carte Remote Insight » du *Manuel des ressources de génération de scripts et de ligne de commande du processeur de supervision HP Integrated Lights-Out*.
- Utilitaires d'importation traditionnels

  Les administrateurs familiarisés avec des outils tels que LDIFDE ou NDS Import/Export Wizard (Assistant d'importation/exportation NDS) peuvent recourir à ces utilitaires pour importer ou créer plusieurs objets de périphériques LOM dans l'annuaire. Toutefois, les administrateurs doivent toujours configurer les périphériques manuellement, comme décrit précédemment, mais peuvent effectuer cette procédure à tout moment. Les interfaces de création de scripts ou de programmes permettent également de créer des objets de périphériques LOM de la même façon que les utilisateurs ou d'autres objets. La section « Schéma des services d'annuaire » (page 214) fournit des détails sur les attributs et les formats de données d'attribut pour la création d'objets LOM.

Services de certificat

Cette section traite des rubriques suivantes :

Introduction aux services de certificat

Les services de certificat permettent d'émettre des certificats numériques signés sur les hôtes du réseau. Les certificats permettent d'établir des connexions SSL avec l'hôte et de vérifier son authenticité.

L'installation des services de certificat permet à Active Directory de recevoir un certificat autorisant les processeurs Lights-Out à se connecter au service d'annuaire. Sans certificat, iLO ne peut pas se connecter au serveur d'annuaire.

Chaque serveur d'annuaire auquel vous souhaitez que iLO se connecte doit disposer d'un certificat. Si vous installez un service de certificat d'entreprise, Active Directory peut automatiquement demander et installer des certificats pour tous les contrôleurs Active Directory du réseau.

Installation des services de certificat

1. Sélectionnez **Start>Settings>Control Panel** (Démarrer>Paramètres> Panneau de configuration).
2. Double-cliquez sur **Add/Remove Programs** (Ajout/Suppression de programmes).
3. Cliquez sur **Add/Remove Windows Components** (Ajout/Suppression de composants Windows) pour lancer l'assistant Composants Windows.
4. Cochez la case **Certificate Services** (Services de certificat). Cliquez sur **Next** (Suivant).
5. Cliquez sur **OK** au message d'avertissement indiquant que le serveur ne peut pas être renommé. L'option Enterprise root CA (Autorité de certification d'entreprise) est sélectionnée car aucune autorité de certification n'est enregistrée dans Active Directory .
6. Entrez les informations appropriées pour votre site et votre organisation. Acceptez la période par défaut de deux ans pour le champ `Valid for` (Valide pendant). Cliquez sur **Next** (Suivant).
7. Acceptez les emplacements par défaut de la base de données de certificats et du journal de base de données. Cliquez sur **Next** (Suivant).
8. Accédez au dossier c:\I386 lorsque le système vous demande d'insérer le CD Windows® 2000 Advanced Server.
9. Cliquez sur **Finish** (Terminer) pour fermer l'Assistant.

Vérification des services d'annuaire

Les processeurs de supervision communiquant avec Active Directory via SSL, il est nécessaire de créer un certificat ou d'installer des services de certificat. Vous devez installer une autorité de certification d'entreprise car vous enverrez des certificats aux objets dans votre domaine organisationnel.

Pour vérifier que les services de certificat sont installés :

1. Sélectionnez **Start>Programs>Administrative Tools>Certification Authority** (Démarrer>Tous les programmes>Outils d'administration>Autorité de certification).
2. Si les services de certification ne sont pas installés, un message d'erreur s'affiche.

Configuration de demande de certificat automatique

Pour spécifier l'émission d'un certificat sur le serveur :

1. Sélectionnez **Start>Run** (Démarrer>Exécuter), puis entrez `mmc`.
2. Cliquez sur **Add** (Ajouter).
3. Sélectionnez **Group Policy password** (Stratégie de groupe), et cliquez sur **Add** (Ajouter) pour ajouter le composant logiciel intégrable dans MMC.
4. Cliquez sur **Browse** (Parcourir) et sélectionnez l'objet Default Domain Policy (Stratégie de domaine par défaut). Cliquez sur **OK**.
5. Sélectionnez **Finish>Close>OK** (Terminer>Fermer>OK).
6. Cliquez sur **Computer Configuration>Windows Settings>Security Settings>Public Key Policies** (Configuration de l'ordinateur>Paramètres Windows>Paramètres de sécurité>Stratégies de clé publique).
7. Cliquez avec le bouton droit sur **Automatic Certificate Requests Settings** (Paramètres des demandes de certificat automatiques) et sélectionnez **New>Automatic Certificate Request** (Nouvelle demande de certificat automatique).
8. Cliquez sur **Next** (Suivant) lorsque l'assistant Automatic Certificate Request Setup (Configuration de demande de certificat automatique) démarre.
9. Sélectionnez le modèle **Domain Controller** (Contrôleur de domaine), puis cliquez sur **Next** (Suivant).
10. Sélectionnez l'autorité de certification listée. (Il s'agit de la même que celle définie lors de l'installation des services de certificat). Cliquez sur **Next (**Suivant).
11. Cliquez sur **Finish** (Terminer) pour fermer l'Assistant.

Utilitaires de migration d'annuaires Lights-Out

Cette section traite des rubriques suivantes :

Introduction aux utilitaires de migration Lights-Out

Pour les clients dotés de processeurs de supervision précédemment installés, HP a mis au point deux utilitaires pour simplifier la migration de ces processeurs vers une supervision par les annuaires. Il s'agit des utilitaires HPQLOMIG et HPQLOMGC. Ils automatisent certaines des étapes de migration indispensables pour que les processeurs de supervision puissent prendre en charge les services d'annuaire. Ces utilitaires permettent d'exécuter les tâches suivantes :

- Identifier les processeurs de supervision dans le réseau (HPQLOMIG uniquement) ;
- Mettre à niveau le microprogramme des processeurs de supervision avec la version prenant en charge Directory Services (Services d'annuaire) ou les services sans schéma ;
- Attribuer un nom aux processeurs de supervision afin de les identifier dans l'annuaire ;
- Créer des objets dans l'annuaire correspondant à chaque processeur de supervision et les associer à un rôle ;
- Configurer les processeurs de supervision pour leur permettre de communiquer avec l'annuaire.

L'utilitaire HPQLOMIG automatise le processus de migration des processeurs de supervision en créant des objets correspondant à chacun des processeurs de supervision dans l'annuaire et en les associant à un rôle. Il est doté d'une GUI et propose à l'utilisateur un assistant pour la mise en œuvre ou la mise à niveau d'une quantité importante de processeurs de supervision.

HPQLOMGC est un utilitaire de ligne de commande qui permet de migrer des processeurs de supervision individuels. Utilisé conjointement à Systems Insight Manager, l'utilitaire HPQLOMGC met à niveau le microprogramme du processeur de supervision et si nécessaire, configure le processeur de supervision et les paramètres d'annuaire. Il crée également un objet de périphérique dans l'annuaire, en utilisant soit le nom figurant dans le fichier XML, soit le nom du réseau, selon si l'utilisateur l'a sélectionné à partir de la ligne de commande, puis l'associe à un rôle. Vous pouvez également lancer HPQLOMGC seul ou à partir d'un script (par exemple, un fichier batch ou un script Perl).

Compatibilité

HPQLOMIG et HPQLOMGC s'exécutent sous des versions de Microsoft® Windows® prenant en charge Microsoft® .NET Framework. Microsoft® .NET Framework est obligatoire. Pour plus d'informations sur .NET Framework et son téléchargement, reportez-vous au site Web http://www.microsoft.com/net/. Les deux utilitaires prennent en charge les systèmes d'exploitation suivants :

- Active Directory
  - Windows® 2000
  - Windows® Server 2003
- Novell eDirectory 8.6.2
  - Red Hat Linux 7,2.
  - Red Hat Linux 7,3.
  - Windows® 2000
  - NetWare 6,0

Liste de contrôle préalable à la migration

1. Vérifiez que votre version actuelle du microprogramme prend en charge les utilitaires HPQLOMIG et HPQLOMGC.

Processeur de supervision	Version minimale du microprogramme
RILOE	2.41
RILOE II	Toutes versions
iLO	1.10

2. Installez Microsoft® .NET Framework.
3. Téléchargez le microprogramme du processeur de supervision qui prend en charge Directory Services à partir du site Web HP (http://www.hp.com/servers/lights-out).
4. Téléchargez HP Lights-Out Directory Services Smart Component à partir du site Web HP (http://www.hp.com/servers/lights-out).
5. Appliquez les extensions de schéma HP Lights-Out à l'annuaire.
6. Créez un rôle pour les utilisateurs du processeur de supervision à l'aide du composant logiciel intégrable de supervision HP Lights-Out.

Solution HP Lights-Out Directory Package

Tous les logiciels de migration, ainsi que le programmes d'installation du support d'extension de schéma et des composants logiciels intégrables, sont regroupés sous la forme d'un composant HP Smart. Pour pouvoir terminer la migration de vos processeurs de supervision, vous devez étendre le schéma et installer les composants logiciels intégrables de supervision avant de lancer l'outil de migration. Le composant Smart est téléchargeable à partir du site Web HP Lights-Out Management (http://www.hp.com/servers/lights-out).

Pour installer les utilitaires de migration, cliquez sur **LDAP Migration Utility** (Utilitaire de migration LDAP) dans le composant Smart. Un programme d'installation Microsoft® MSI est lancé, qui installe les utilitaires HPQLOMIG, HPQLOMGC, les fichiers DLL requis, le contrat de licence ainsi que d'autres fichiers dans le répertoire C:\Program Files\Hewlett-Packard\HP Lights-Out Migration Tool. Vous pouvez sélectionner un autre répertoire. Un fichier échantillon XML est également installé et un raccourci vers HPQLOMIG créé dans le menu Start (Démarrer).

REMARQUE : l'utilitaire d'installation affiche un message d'erreur et se ferme s'il détecte que .NET Framework n'est pas installé.

Fonctionnement de HPQLOMIG

L'utilitaire de ligne de commande est conçu pour être utilisé conjointement avec Insight Manager 7 et Systems Insight Manager. Si vous n'utilisez pas Systems Insight Manager, utilisez l'utilitaire HPQLOMIG.

IMPORTANT : l'installation de la prise en charge des annuaires pour les processeurs de supervision nécessite le téléchargement du composant HP Smart. Pour plus d'informations, reportez-vous aux sections « Liste de contrôle préalable à la migration » (page 164) et « Solution HP Lights-Out Directory Package ». Cette opération doit être effectuée par un administrateur de schéma.

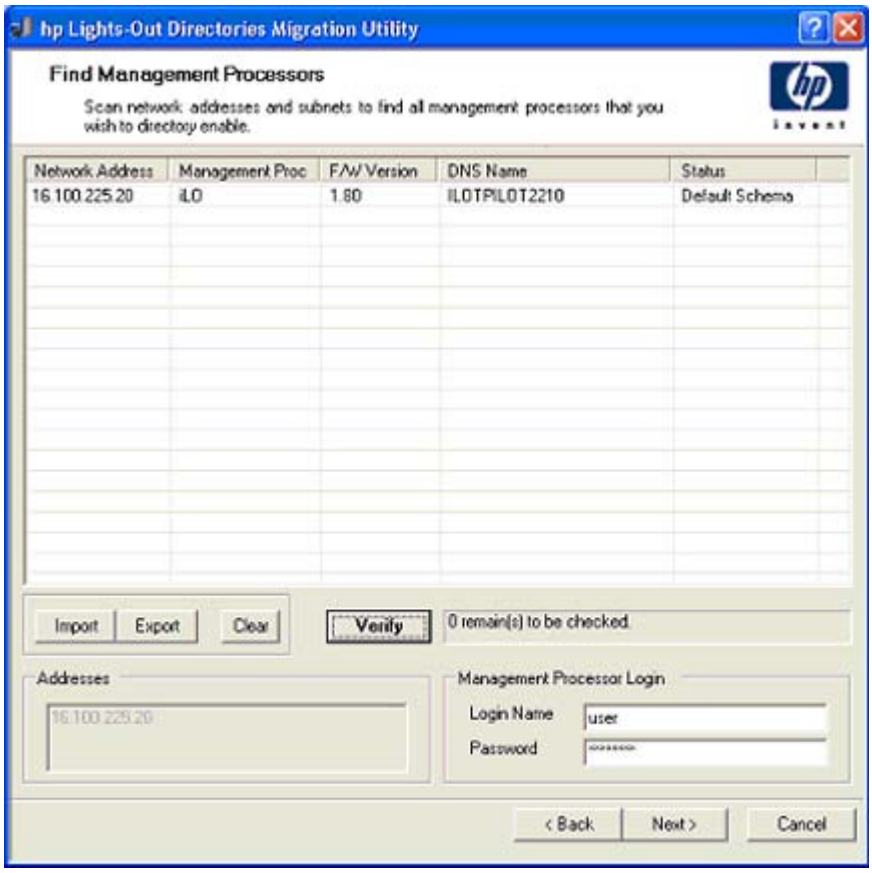
L'utilitaire HPQLOMIG requiert des privilèges de connexion et de mise à niveau de microprogramme pour chaque processeur de supervision. L'installation des services d'annuaire nécessite la modification des privilèges de paramétrage de l'annuaire.

Localisation de processeurs de supervision

La première étape du processus de migration consiste à localiser tous les processeurs de supervision à activer pour les services d'annuaire. Vous pouvez rechercher les processeurs de supervision à l'aide de noms DNS, d'adresses IP ou de caractères génériques d'adresse IP. Les règles suivantes s'appliquent aux variables entrées dans le champ Addresses (Adresses) :

- Les noms DNS, les adresses IP et les adresses IP en caractères génériques doivent être délimités par un point-virgule.
- Le caractère générique d'adresse IP fait appel au caractère « * » dans les champs des troisième et quatrième octets. Par exemple, l'adresse IP 16.100.*.* est valide alors que l'adresse IP 16.*.*.* ne l'est pas.
- Vous pouvez également préciser des plages de valeurs à l'aide d'un tiret. Par exemple, 192.168.0.2-10 est une plage de valeurs correcte. Le tiret est pris en charge uniquement dans l'octet le plus à droite.
- Une fois que vous avez cliqué sur le bouton **Find** (Rechercher), HPQLOMIG envoie une commande PING et se connecte au port 443 (port SSL par défaut). L'objectif est de déterminer rapidement si l'adresse du réseau cible est un processeur de supervision. Si le périphérique ne répond pas à la commande PING ou ne se connecte pas correctement au port 443, il n'est pas considéré comme un processeur de supervision.

Si vous cliquez sur le bouton **Next** (Suivant) ou **Back** (Précédent) ou que vous quittez l'application en cours de recherche, les opérations sur le réseau en cours sont menées à leur terme, mais celles sur les adresses de réseau suivantes sont annulées.



Pour lancer le processus de recherche de vos processeurs de supervision :

1. Cliquez sur **Démarrer** et sélectionnez **Programmes>Hewlett-Packard>Utilitaire de migration Lights-Out HP** pour démarrer le processus de migration.
2. Cliquez sur **Next** (Suivant) pour passer outre l'écran d'accueil Welcome.
3. Entrez les variables pour exécuter la recherche du processeur de supervision dans le champ Addresses (Adresses).
4. Saisissez votre nom de connexion et votre mot de passe, puis cliquez sur le bouton **Find** (Rechercher). Celui-ci se transforme en bouton Verify (Vérifier) une fois la recherche terminée.

   Vous pouvez également entrer une liste de processeurs de supervision en cliquant sur **Import** (Importer). Le fichier est un simple fichier texte avec un processeur de supervision par ligne. Les champs sont séparés par des points-virgules. Les champs sont les suivants :

   - Network Address (Adresse réseau)
   - Management Processor Type (Type de processeur de supervision)
   - Firmware Version (Version du microprogramme)
   - DNS Name (Nom DNS)
   - User Name (Nom de l'utilisateur)
   - Password (Mot de passe)
   - Directory Configuration (Configuration de l'annuaire)

Par exemple, une ligne peut se présenter comme suit :

```
16.100.225.20;iLO;1.80;ILOTPILOT2210;user;password;Default Schema
```

Si, pour des raisons de sécurité, le nom d'utilisateur et le mot de passe ne peuvent pas figurer dans le fichier, laissez ces champs vides mais conservez les points-virgules.

Mise à niveau du microprogramme des processeurs de supervision

L'écran de mise à niveau du microprogramme permet de mettre à jour les processeurs de supervision à la version du microprogramme qui prend en charge les annuaires. Cet écran permet également de spécifier l'emplacement de l'image du microprogramme pour chaque processeur de supervision en entrant le chemin ou en cliquant sur **Browse** (Parcourir).

IMPORTANT : les images binaires du microprogramme des processeurs de supervision doivent être accessibles à partir du système qui exécute l'utilitaire de migration. Ces images binaires peuvent être téléchargées à partir du site Web HP (http://www.hp.com/servers/lights-out).

Processeur de supervision	Version minimale du microprogramme
RILOE	2.50
RILOE II	1.10
iLO	1.40

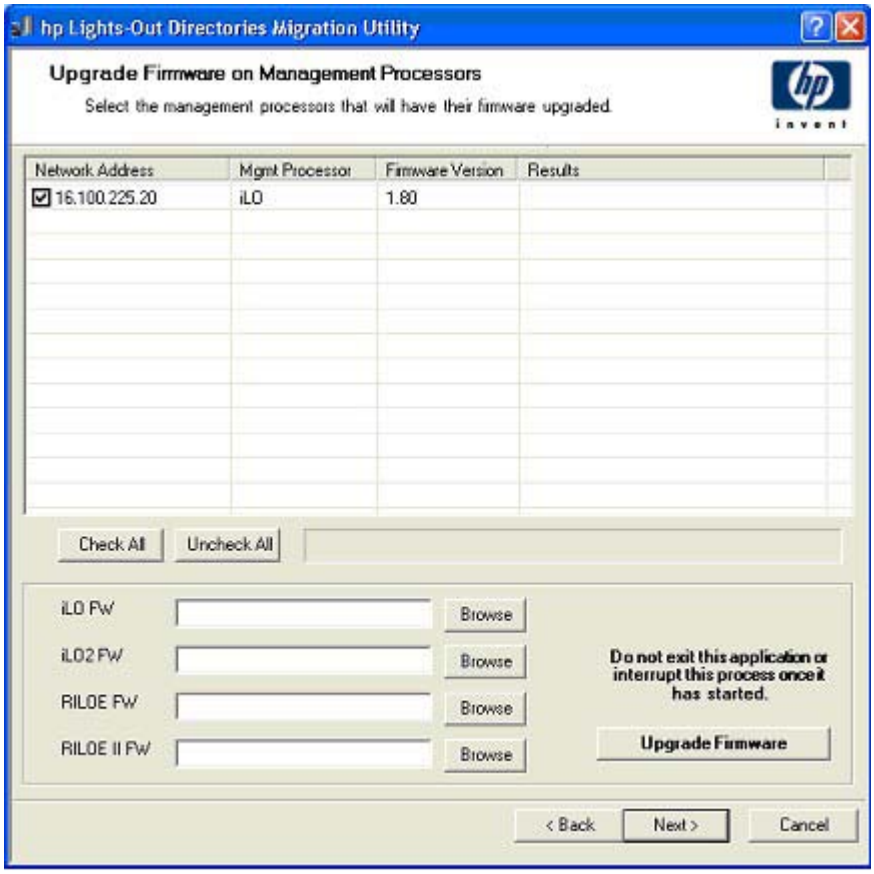
Le processus de mise à niveau peut prendre du temps, selon le nombre de processeurs de supervision sélectionné. La mise à niveau du microprogramme d'un seul processeur de supervision peut prendre jusqu'à cinq minutes. Si la mise à niveau échoue, un message s'affiche dans la colonne Results (Résultats) et l'utilitaire HPQLOMIG continue de mettre à niveau les autres processeurs de supervision identifiés.

IMPORTANT : hp vous recommande de tester le processus de mise à niveau et de vérifier les résultats dans un environnement de test avant de lancer l'utilitaire sur un réseau de production. En effet, le transfert incomplet de l'image du microprogramme vers un processeur de supervision pourrait entraîner la reprogrammation locale du processeur de supervision à l'aide d'une disquette.

Pour mettre à niveau le microprogramme de vos processeurs de supervision :

1. Sélectionnez les processeurs de supervision à mettre à niveau.
2. Pour chaque type de processeur de supervision localisé, saisissez le chemin correct vers l'image du microprogramme ou utilisez le bouton Browse (Parcourir) pour l'atteindre.
3. Cliquez sur le bouton **Upgrade Firmware** (Mettre à jour le microprogramme). Les processeurs de supervision sélectionnés sont mis à niveau. Même si cet utilitaire permet de mettre à niveau des centaines de processeurs de supervision, seuls 25 processeurs peuvent être mis à niveau simultanément. L'activité du réseau est considérable pendant la durée de l'opération.

4. Une fois la mise à niveau terminée, cliquez sur le bouton **Next** (Suivant).

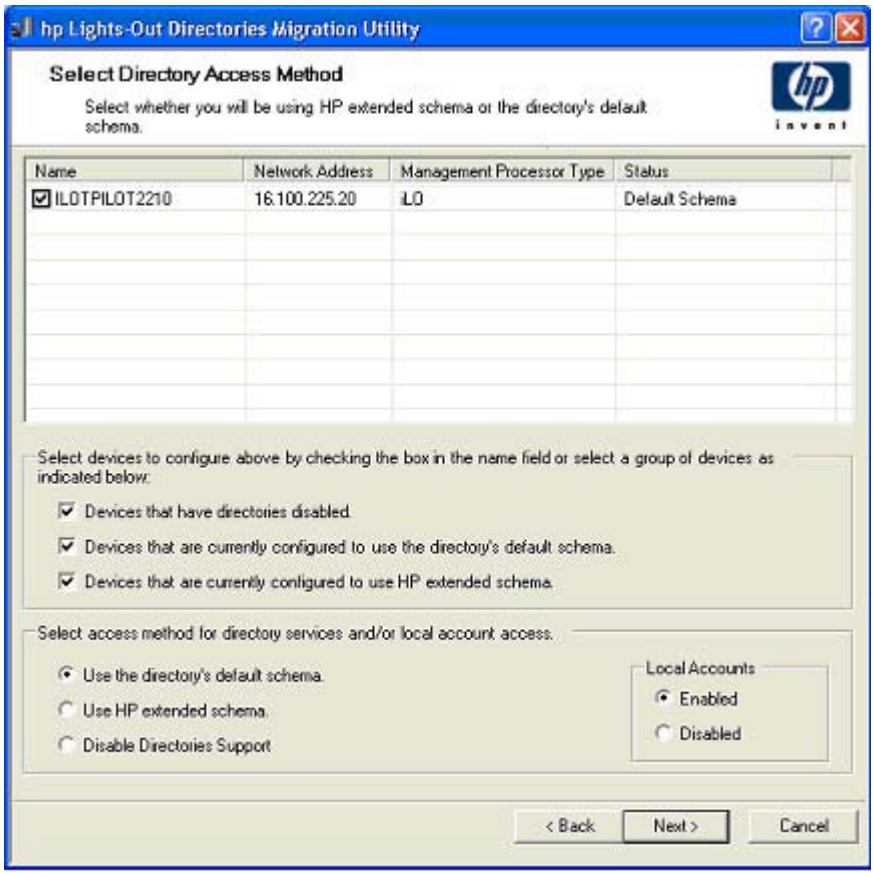


Au cours du processus de mise à niveau du microprogramme, tous les boutons sont désactivés pour empêcher la navigation. Vous pouvez tout de même fermer l'application à l'aide du « X » situé dans le coin supérieur droit de l'écran. Si vous fermez l'interface pendant la programmation du microprogramme, l'application continue de fonctionner en arrière-plan et met à niveau le microprogramme sur tous les périphériques sélectionnés.

Sélection d'une méthode d'accès à l'annuaire

Après la page Firmware Upgrade (Mettre à jour le microprogramme), la page Select Directory Access Method (Sélectionner une méthode d'accès à l'annuaire) s'affiche. Vous pouvez sélectionner les processeurs de supervision à configurer (conformément à l'utilisation ou non du schéma) et la manière dont ils seront configurés. La page Select Directory Access Method (Sélectionner une méthode d'accès à l'annuaire) contribue à empêcher l'écrasement accidentel d'iLO déjà configurés pour un schéma HP ou d'iLO dont les annuaires sont désactivés.

Elle détermine les pages de configuration de la prise en charge qui vont suivre : schéma HP Extended, sans schéma (schéma par défaut) ou pas d'annuaires.



Pour configurer le processeur de supervision pour :

- Directory Services, reportez-vous à la section « Configuration des annuaires avec le schéma HP Extended sélectionné » (page 170) ;
- la prise en charge d'annuaires sans schéma (schéma par défaut), reportez-vous à la section « Configuration pour l'intégration d'annuaire sans schéma » (page 121).

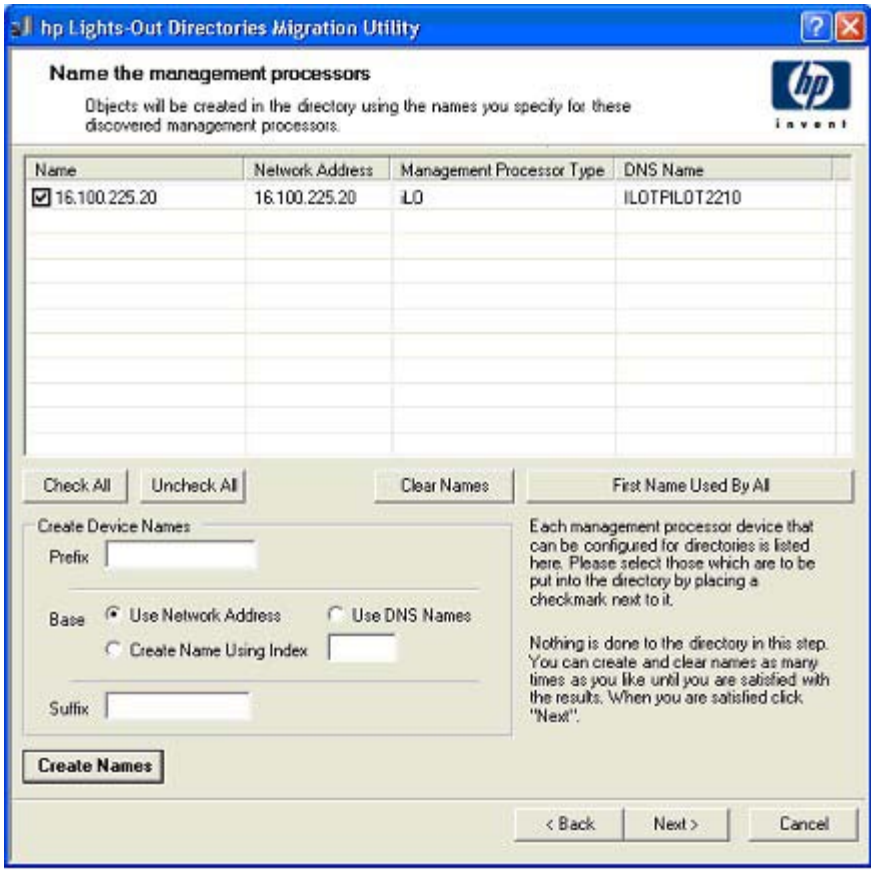
Attribution de noms aux processeurs de supervision

Cet écran permet d'attribuer un nom aux objets de périphérique Lights-Out Management dans l'annuaire et de créer des objets de périphériques correspondants pour tous les processeurs de supervision à gérer. Vous pouvez créer des noms à l'aide d'un ou de plusieurs des éléments suivants :

- L'adresse du réseau
- Le nom de DNS
- Un index
- Manuellement
- Un préfixe commun à tous les noms
- Un suffixe commun à tous les noms

Pour attribuer un nom aux processeurs de supervision, cliquez sur le champ **Name** (Nom) et entrez le nom souhaité ou bien :

1. Utilisez la case d'option **Use Network Address** (Utiliser l'adresse du réseau), **Use DNS Names** (Utiliser les noms de DNS) ou **Create Name Using Index** (Créer un nom à l'aide d'un index). Vous pouvez également nommer chaque objet d'annuaire de processeur de supervision en cliquant deux fois sur le champ du nom, en laissant un petit intervalle de temps entre les clics.
2. Saisissez le texte destiné à servir de préfixe ou de suffixe à tous les noms (facultatif).
3. Cliquez sur le bouton **Generate Names** (Créer des noms). Les noms s'affichent dans la colonne Name (Nom) dans l'état dans lequel ils sont générés. Pour le moment, les noms ne sont pas écrits dans l'annuaire ou dans les processeurs de supervision. Ils sont stockés jusqu'à la page suivante.
4. Pour changer ces noms (facultatif), cliquez sur le bouton **Clear All Names** (Effacer tous les noms) et attribuez un nouveau nom aux processeurs de supervision.
5. Lorsque les noms sont corrects, cliquez sur le bouton **Next** (Suivant).



Configuration des annuaires avec le schéma HP Extended sélectionné

L'écran Configure Directory (Configurer annuaire) permet de créer un objet de périphérique pour chaque processeur de supervision identifié et d'associer ce nouvel objet à un rôle précédemment défini. Par exemple, l'annuaire définit un utilisateur comme étant membre d'un rôle (tel qu'administrateur) disposant d'une série de droits sur un objet de périphérique spécifique (comme une carte RILOE II).

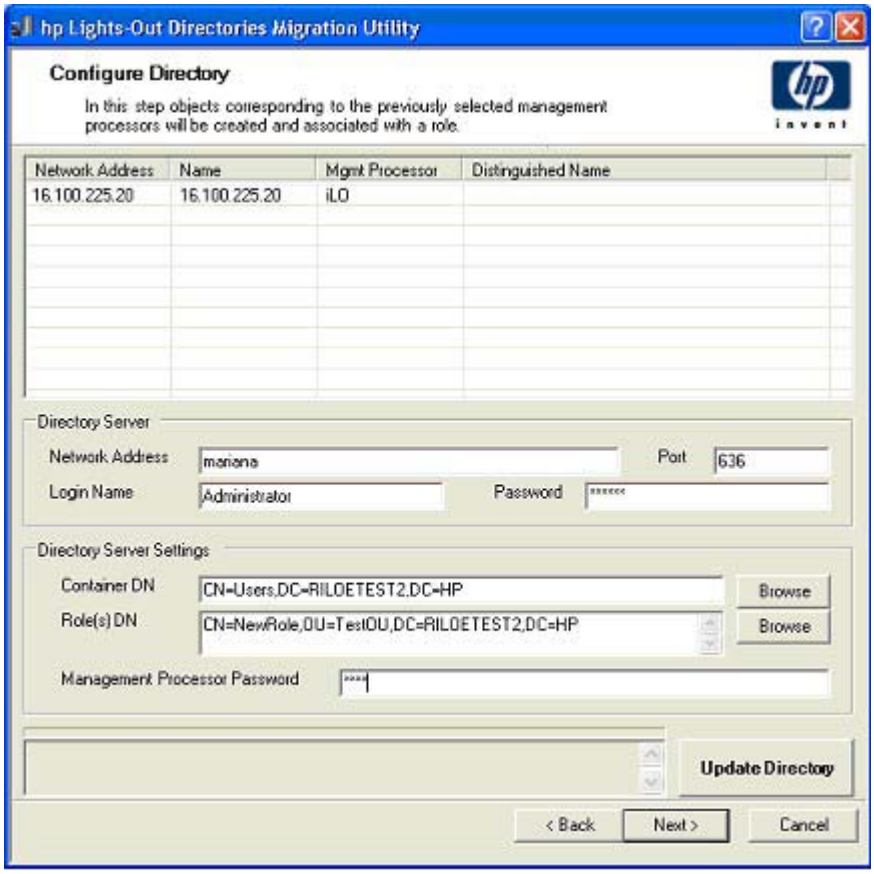
Les champs de l'écran Configure Directory (Configurer annuaire) sont les suivants :

- **Network Address** (Adresse réseau) : adresse réseau du serveur d'annuaire qui peut être une adresse IP ou un nom DNS valide.
- **Port** : Port SSL vers l'annuaire. L'entrée par défaut est 636. Les processeurs de supervision peuvent communiquer avec l'annuaire uniquement par le biais du protocole SSL.
- **Login Name** (Nom de connexion) et **Password** (Mot de passe) : ces champs permettent la connexion à l'aide d'un compte doté d'un droit d'accès administrateur de domaine à l'annuaire.
- **Container DN** (Conteneur DN) : une fois que vous disposez des informations relatives à l'adresse réseau, au port et à la connexion, vous pouvez cliquer sur **Browse** (Parcourir) pour accéder au nom distinctif du conteneur et du rôle. Le nom distinctif du conteneur est l'endroit où l'utilitaire de migration va créer tous les objets de processeur de supervision dans l'annuaire.
- **Role DN** (Rôle DN) : le nom distinctif du rôle signale l'emplacement du rôle auquel vont être associés les objets de périphérique. Il doit être créé avant l'exécution de l'utilitaire concerné.

Pour configurer les objets de périphérique à associer à un rôle :

1. Entrez l'adresse réseau, le nom de connexion et le mot de passe pour le serveur d'annuaire spécifié.
2. Entrez le nom distinctif du conteneur dans le champ Container DN (Conteneur DN) ou cliquez sur **Browse** (Parcourir).
3. Associez les objets de périphérique à un membre de rôle en entrant le nom distinctif du rôle dans le champ Role DN (Rôle DN) ou cliquez sur Browse (Parcourir).
4. Cliquez sur **Update Directory** (Mettre à jour l'annuaire). L'outil se connecte à l'annuaire, crée les objets de processeur de supervision, puis les ajoute aux rôles sélectionnés.

5. Une fois les objets de périphériques associés à un rôle, cliquez sur le bouton **Next** (Suivant).

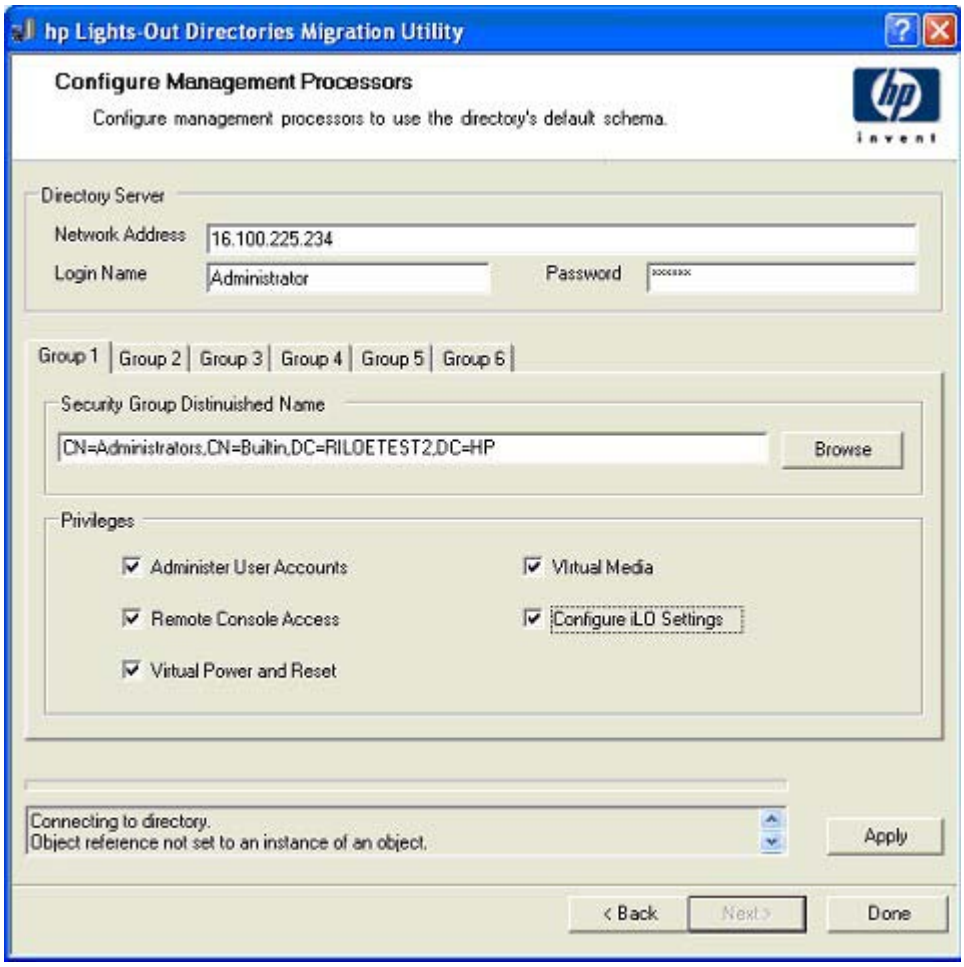


Configuration pour l'intégration d'annuaire sans schéma

Les champs de l'écran Configure Management Processors (Configurer les processeurs de supervision) sont les suivants :

- **Network Address** (Adresse réseau) : adresse réseau du serveur d'annuaire qui peut être une adresse IP ou un nom DNS valide.
- **Login Name** (Nom de connexion) et **Password** (Mot de passe) : ces champs permettent la connexion à l'aide d'un compte doté d'un droit d'accès administrateur de domaine à l'annuaire.
- **Security Group Distinguished Name** (Nom distinctif du groupe de sécurité) : nom distinctif du groupe dans l'annuaire qui contient un ensemble d'utilisateurs iLO partageant un ensemble commun de privilèges. Si le nom d'annuaire, le nom de connexion et le mot de passe sont corrects, vous pouvez cliquer sur le bouton **Browse** (Parcourir) pour naviguer jusqu'au groupe et le sélectionner.
- **Privileges** (Privilèges) : privilèges iLO associés au groupe sélectionné. Le privilège de connexion est implicite si l'utilisateur est membre du groupe.

Les réglages du paramètre Configure Management Processors (Configurer les processeurs de supervision) sont stockés jusqu'à la page suivante de l'Assistant.



Configuration des processeurs de supervision pour les annuaires

La dernière étape du processus de migration consiste à configurer les processeurs de supervision pour qu'ils puissent communiquer avec l'annuaire. Cet écran permet de créer des contextes utilisateur.

Les contextes utilisateurs permettent d'utiliser un nom abrégé ou un nom d'objet utilisateur pour se connecter, plutôt que le nom distinctif complet. Par exemple, le contexte utilisateur CN=Users,DC=RILOETEST2,DC=HP permet à l'utilisateur « John Smith » de se connecter en tant que John Smith plutôt que CN=John Smith,CN=Users, DC=RILOETEST2,DC=HP. Le format @ est également pris en charge. Par exemple, @RILOETEST2.HP dans un champ de contexte permet à l'utilisateur de se connecter en tant que jsmith (en supposant qu'il s'agit de son nom abrégé).

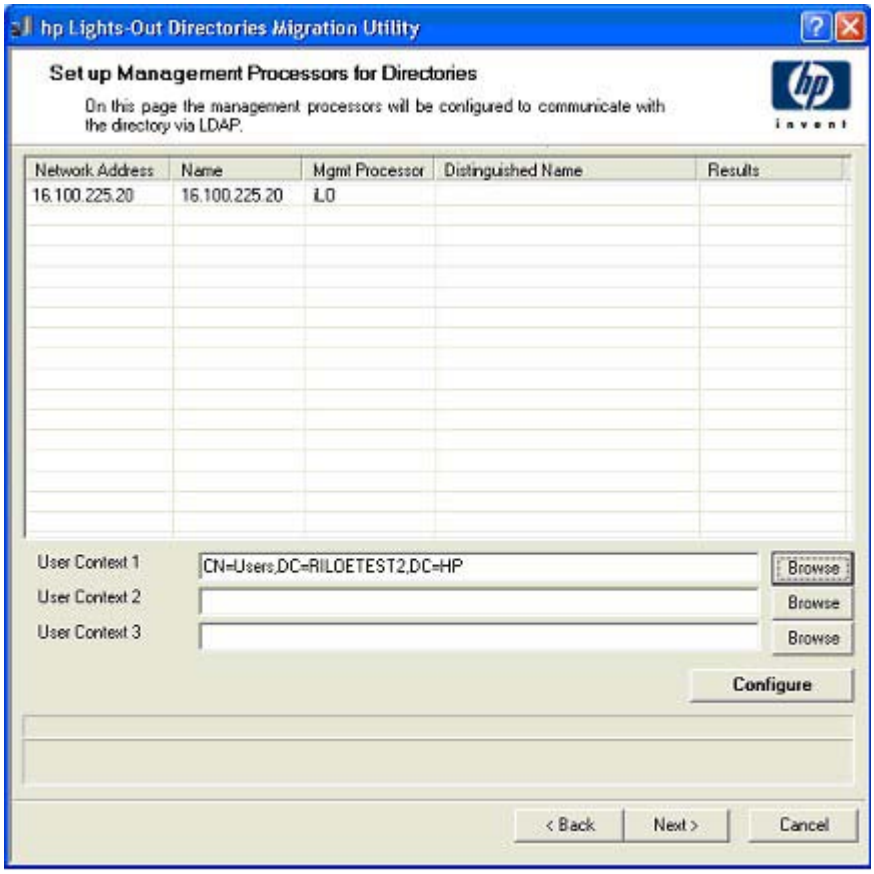
Pour configurer les processeurs de supervision pour qu'ils communiquent avec l'annuaire :

1. Entrez les contextes utilisateur ou cliquez sur **Browse** (Parcourir).
2. Pour les options Directory Support (Prise en charge des annuaires) et Local Accounts (Comptes locaux), sélectionnez **Enabled** (Activé) ou **Disabled** (Désactivé).

   L'accès distant est désactivé si les deux fonctionnalités Directory Support (Prise en charge des annuaires) et Local Accounts (Comptes locaux) le sont. Pour rétablir l'accès, redémarrez le serveur et utilisez RBSU F8.

3. Cliquez sur **Configure** (Configurer). L'utilitaire de migration se connecte à tous les processeurs de supervision sélectionnés et met à jour leur configuration comme vous l'avez spécifié.
4. Une fois le processus terminé, cliquez sur le bouton **Done** (Terminé).

REMARQUE : à ce stade, la fonctionnalité associée au champ Management Processor Password (Mot de passe du processeur de supervision) est indisponible. Ce champ est conçu en prévision de la compatibilité avec les versions à venir.



Fonctionnement de HPQLOMGC

L'utilitaire de ligne de commande est conçu pour être utilisé conjointement avec Insight Manager 7 et Systems Insight Manager. Si vous n'utilisez pas Systems Insight Manager, utilisez l'utilitaire HPQLOMIG. Le mode de ligne de commande n'est pas doté d'une GUI et fonctionne en mode autonome. Il est destiné à fonctionner conjointement avec la fonctionnalité Application launch (Lancement des applications).

IMPORTANT : l'installation de la prise en charge des annuaires pour les processeurs de supervision nécessite le téléchargement du composant HP Smart. Pour plus d'informations, reportez-vous aux sections « Liste de contrôle préalable à la migration » (page 164) et « Solution HP Lights-Out Directory Package ». Cette opération doit être effectuée par un administrateur de schéma.

Pour mettre en œuvre la prise en charge des annuaires sur un petit nombre de processeurs de supervision :

1. Utilisez Systems Insight Manager pour localiser tous les processeurs de supervision présents sur le réseau.
2. Exécutez l'utilitaire HPQLOMGC.
3. Appelez le fichier XML pour migrer le processeur de supervision.

HPQLOMGC effectue la migration d'un processeur de supervision en trois phases.

1. **Validation et mise à jour le cas échéant de la version du microprogramme.**

   HPQLOMGC détermine le type de processeur de supervision et le niveau du microprogramme. Si le microprogramme ne satisfait pas aux conditions de configuration minimales (voir la section « Mise à niveau du microprogramme des processeurs de supervision », page 167), HPQLOMGC le met à niveau et réinitialise le processeur de supervision. Une fois le processeur de supervision réinitialisé, l'utilitaire HPQLOMGC passe à la phase suivante.
2. **Les paramètres d'annuaire du processeur de supervision sont mis à jour.**

   HPQLOMGC utilise l'interface de création de scripts pour envoyer les paramètres de l'annuaire au processeur de supervision.
3. **L'annuaire est mis à jour.**

   HPQLOMGC crée un objet de périphérique dans l'annuaire à l'emplacement précisé par l'utilisateur. HPQLOMGC utilise soit le nom de l'objet précisé dans le fichier XML soit le nom réseau du processeur de supervision. Une fois l'objet de périphérique créé, l'objet de rôle spécifié est modifié pour inclure l'objet de périphérique qui vient d'être créé.

Lancement de l'utilitaire HPQLOMGC à l'aide de la fonction Application Launch (Lancement des applications)

La fonction Application Launch (Lancement des applications) permet de créer des tâches associées à l'administration des processeurs de supervision. Elle permet, par exemple, de localiser les processeurs de gestion permettant de configurer automatiquement de nouveaux processeurs de supervision lors de leur ajout au réseau.

Pour créer une tâche Application Launch (Lancement des applications) :

1. Cliquez sur **Device** (Périphérique) dans la barre de navigation située dans le coin supérieur gauche de l'écran.
2. Cliquez sur **Tasks** (Tâches) pour ouvrir l'écran du même nom.
3. Cliquez sur **New Control Task** (Nouvelle tâche de contrôle). Un menu contextuel s'affiche.
4. Dans le menu contextuel, cliquez sur **Application Launch** (Lancement des applications) pour ouvrir l'écran Create/Edit Task (Créer/Éditer tâche).
5. Saisissez le chemin d'accès complet et le nom de l'utilitaire de commande de migration Lights-Out dans la zone appropriée. Par exemple, si le fichier HPQLOMGC.exe se trouve dans le répertoire racine du lecteur C, le chemin d'accès est le suivant : C:\HPQLOMGC.exe.
6. Entrez les paramètres dans la zone appropriée.

   Les commutateurs de ligne de commande permettent de désigner les éléments tels que le processeur de supervision devant être mis à niveau, le fichier XML à utiliser et l'emplacement sur lequel le fichier log doit être généré.

-S <adresse réseau> : ce commutateur contient l'adresse IP ou le nom DNS du processeur de supervision. Par défaut, l'adresse IP du processeur de supervision est automatiquement fournie. La variable d'environnement <DEVICEIPADDRESS0> permet également de préciser une adresse du réseau.

Utilisez le commutateur -S pour neutraliser le comportement par défaut. Lorsque ce commutateur est présent, il a la priorité sur la variable d'environnement de l'adresse IP <DEVICEIPADDRESS0>.

-F <nom_fichier> : ce commutateur contient le chemin d'accès au fichier XML dans lequel sont consignés les paramètres d'annuaire du processeur de supervision et l'emplacement des images du microprogramme. Il provoque une erreur en l'absence de désignation d'adresse IP.

-A : ce commutateur utilise le nom de réseau comme nom de l'objet de périphérique créé dans le répertoire.

-V : ce commutateur facultatif définit HPQLOMGC en mode détaillé.

-L <nom_fichier> : ce commutateur définit si le fichier journal est généré. Il provoque une erreur en l'absence de désignation d'adresse IP.

-Q : ce commutateur facultatif définit HPQLOMGC en mode silencieux.

7. Cliquez sur **Next** (Suivant). Un écran affiche des options pour nommer la tâche, définir l'association de requêtes et planifier la tâche.
8. Entrez un nom de tâche dans le champ Enter a name for this task (Entrer un nom pour cette tâche).
9. Sélectionnez la requête qui a été créée précédemment, par exemple « Mgmt processors ».
10. Cliquez sur **Schedule** (Planifier) pour définir le moment où la tâche de lancement des applications sera exécutée. Une fenêtre de configuration de planification s'affiche.
11. Cliquez sur **OK** pour fixer la planification.

    REMARQUE : la valeur de planification par défaut d'une tâche de contrôle est **Now** (Maintenant).

12. Cliquez sur **Finish** (Terminer) pour enregistrer la tâche de lancement des applications.
13. Cliquez sur l'icône **Execute a Task** (Exécuter tâche) (le triangle vert) pour exécuter l'administration des groupes.

Intégration de HP SIM (Systems Insight Manager)

Cette section traite des rubriques suivantes :

Intégration de la carte iLO avec Systems Insight Manager

La carte iLO s'intègre avec HP Systems Insight Manager dans les principaux environnements d'exploitation. L'intégration totale avec Systems Insight Manager offre également une console de supervision unique permettant de lancer un navigateur standard. Lorsque le système d'exploitation est opérationnel, vous pouvez établir une connexion à la carte iLO à l'aide de Systems Insight Manager.

L'intégration avec Systems Insight Manager offre les fonctionnalités suivantes :

- Prise en charge de la remise de traps SNMP à une console Systems Insight Manager.

  La remise de traps SNMP à une console Systems Insight Manager peut être configurée pour transférer les traps SNMP vers un pager ou une adresse e-mail.

- Prise en charge de la supervision SNMP.

  Systems Insight Manager est habilité à accéder aux informations des agents de supervision Insight via la carte iLO.

- Prise en charge d'un processeur de supervision.

  Systems Insight Manager prend en charge un nouveau type de périphérique, le processeur de supervision. Tous les périphériques iLO installés sur les serveurs au sein du réseau sont identifiés en tant que processeurs de supervision dans Systems Insight Manager. Les processeurs de supervision sont associés aux serveurs sur lesquels ils sont installés.

- Regroupement des processeurs de supervision iLO.

  Tous les périphériques iLO peuvent être regroupés logiquement et être affichés sur la même page. Cette fonction permet d'accéder à la carte iLO à partir d'un point unique dans Systems Insight Manager.

- Liens hypertexte de iLO.

  Systems Insight Manager propose un lien hypertexte sur la page des périphériques serveur pour lancer la carte iLO et s'y connecter.

- Agents de supervision HP.

  La carte iLO, associée aux agents de supervision HP, permet d'accéder à distance aux informations de supervision du système via son interface de navigateur Web.

Présentation du fonctionnement de Systems Insight Manager

Le logiciel Systems Insight Manager vous permet d'effectuer les tâches suivantes :

- Identification des processeurs iLO.
- Création d'une association entre une carte iLO et son serveur.
- Création de liens entre une carte iLO et son serveur.
- Affichage des informations relatives à iLO et au serveur, ainsi que de leur état.
- Contrôle du niveau de détail affiché pour iLO.
- Création de la visualisation de l'infrastructure de rack ProLiant BL p-Class.

Les sections suivantes résument chacune de ces fonctions. Pour obtenir des informations détaillées sur ces avantages et pour savoir comment utiliser Systems Insight Manager, reportez-vous au manuel *HP Systems Insight Manager Technical Reference Guide* (*Manuel de référence technique de Systems Insight Manager*), fourni avec Systems Insight Manager et disponible sur le site Web HP (http://www.hp.com/go/hpsim).

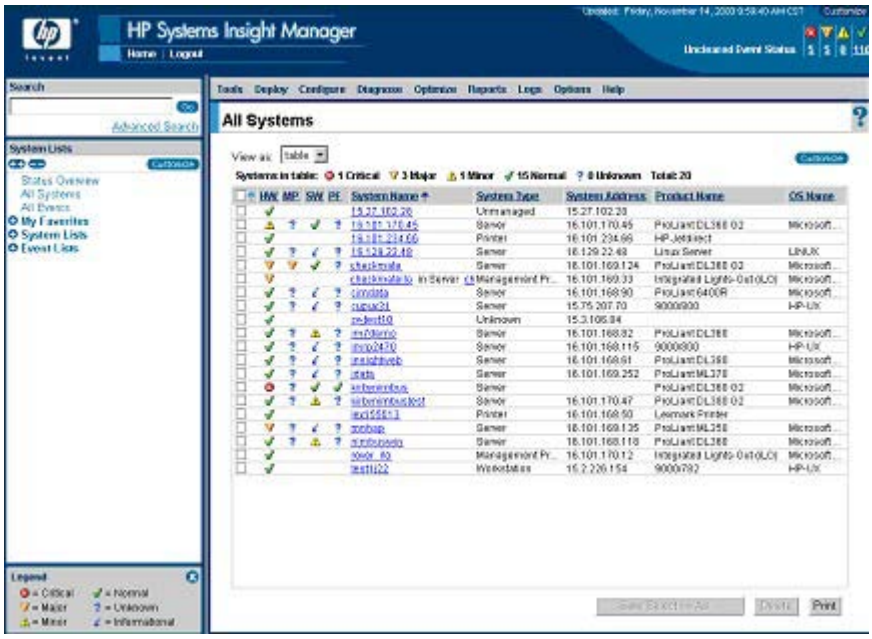
Identification et association dans Systems Insight Manager

Systems Insight Manager peut identifier un processeur iLO et créer une association entre la carte iLO et le serveur. L'administrateur du périphérique iLO peut configurer la carte iLO pour qu'elle réponde aux demandes d'identification de Systems Insight Manager.

État dans Systems Insight Manager

Dans Systems Insight Manager, la carte iLO est identifiée comme un processeur de supervision. Systems Insight Manager affiche l'état du processeur de supervision dans la liste des systèmes.

Le processeur de supervision iLO apparaît sous la forme d'une icône dans la liste des périphériques, sur la même ligne que son serveur hôte. La couleur de l'icône correspond à l'état du processeur de supervision.



Pour obtenir la liste complète des états de périphérique, reportez-vous au manuel *HP Systems Insight Manager Technical Reference Guide* (*Manuel de référence technique de HP Systems Insight Manager*), disponible sur le site Web HP (http://www.hp.com/go/hpsim).

Liens dans Systems Insight Manager

Pour simplifier la supervision, Systems Insight Manager crée des liens vers les éléments suivants :

- La carte iLO et le serveur hôte depuis n'importe quelle liste System (Système) ;
- Le serveur depuis la page System (Système) de iLO ;
- La carte iLO depuis la page System (Système) du serveur.

Les pages Systems List (Liste systèmes) affichent la carte iLO, le serveur et la relation entre ces deux composants. La page peut, par exemple, afficher le serveur, le nom iLO en regard et la relation *iLO name* **IN** *server* (*nom iLO DANS nom du serveur)* dans le champ System Name (Nom de système) correspondant à la carte iLO.

Lorsque vous cliquez sur l'icône d'état correspondant à la carte iLO, vous accédez à l'interface Web iLO. Si vous cliquez sur l'icône d'état du matériel, vous accédez aux agents Insight Management du périphérique concerné. Cliquez sur iLO ou sur le nom de serveur pour accéder à la page System (Système) du périphérique en question. La page System (Système) contient les onglets Identity (Identité), Links (Liens) et Event (Événement). Ces onglets fournissent des informations sur l'identité, l'état, les événements et les liens du périphérique associé.

Listes Système dans Systems Insight Manager

Les processeurs de supervision iLO sont visualisables dans Systems Insight Manager. Un utilisateur disposant de tous les droits de configuration peut créer et utiliser des collections de systèmes personnalisées pour les regrouper. Pour obtenir des informations détaillées, reportez-vous au manuel *HP Systems Insight Manager Technical Reference Guide* (Manuel de référence technique de HP Systems Insight Manager), disponible sur le site Web HP (http://www.hp.com/go/hpsim).

Réception des alertes SNMP dans Systems Insight Manager

Vous pouvez configurer la carte iLO pour transférer les alertes des agents de supervision du système d'exploitation hôte et pour envoyer les alertes générées par la carte iLO vers la console Systems Insight Manager.

Systems Insight Manager assure la prise en charge de la supervision SNMP intégrale, tandis que la carte iLO prend en charge la remise de traps SNMP à Systems Insight Manager. Vous pouvez afficher le journal des événements, sélectionner l'événement et afficher des informations complémentaires sur l'alerte.

La configuration de la réception des alertes SNMP dans Systems Insight Manager se fait en deux étapes. Cette opération nécessite la détection, par Systems Insight Manager, de la carte iLO et la configuration de cette dernière pour activer les alertes SNMP.

1. Pour permettre à la carte iLO d'envoyer des alertes SNMP, cliquez sur l'option **SNMP/Insight Manager Settings** (Paramètres SNMP/Insight Manager) sous l'onglet Administration de la fenêtre de navigation iLO, afin d'activer les alertes SNMP et fournir une adresse IP de trap SNMP à la carte iLO. Cette adresse IP devrait être celle de l'ordinateur exécutant Systems Insight Manager. Reportez-vous à la section « Activation des alertes SNMP » (page 31) pour plus d'informations.
2. Pour détecter la carte iLO dans Systems Insight Manager, il faut la configurer en tant que périphérique supervisé dans Systems Insight Manager. L'ajout de la carte iLO à Systems Insight Manager permet à l'interface réseau de iLO de fonctionner comme un port de supervision dédié, isolant ainsi le trafic de supervision de l'interface réseau du serveur hôte distant.
   a. Lancez Systems Insight Manager.
   b. Sélectionnez **Options>Discovery>Automatic Discovery** (Options>Découverte>Découverte automatique) pour localiser l'onglet.
   c. Sélectionnez la tâche de localisation à exécuter, puis cliquez sur Edit (Modifier).
   d. Sélectionnez **IP range pinging** (PING pour plage d'adresses IP). Si l'adresse IP ne se trouve pas dans la plage des adresses susceptibles de répondre à la commande PING, les modèles et/ou la section des fichiers hôtes files, entrez-la manuellement.
   e. Cliquez sur **OK**.
   f. Cliquez sur **Save and Run** (Enregistrer et exécuter) pour ajouter la carte iLO dans Systems Insight Manager. Une fois la détection terminée, les requêtes suivantes affichent le périphérique en tant que processeur de supervision.

Il peut s'avérer nécessaire de modifier la chaîne de communauté de lecture SNMP (en la remplaçant par « public » par exemple) pour que la carte iLO apparaisse dans la liste des systèmes supervisés. Il est possible de modifier la « community string » de lecture SNMP en accédant à la page Systems Protocol Settings (Paramètres de protocole système). Pour accéder à ces paramètres, sélectionnez **Options>Protocol Settings>System Protocol Settings** (Options>Paramètres de protocole>Paramètres de protocole système).

Vous pouvez également cliquer sur **Options>Protocol Settings>Global Protocol Settings** (Options>Paramètres de protocole>Paramètres de protocole généraux) et paramétrer les « community strings » sous Default SNMP Settings (Paramètres SNMP par défaut) afin de les utiliser pendant la détection. Une fois le paramétrage effectué, vous pouvez effectuer les étapes de a à f pour exécuter à nouveau la fonctionnalité Discovery (Détection).

Pour les événements principaux non effacés, les traps de la carte iLO s'affichent dans All Events (Tous les événements). Vous pouvez utiliser le bouton orange situé en haut de l'écran pour accéder aux événements principaux non effacés. Pour plus d'informations sur cet événement, cliquez sur **Event Type** (Type de l'événement).

REMARQUE : la supervision de la carte iLO nécessite l'installation des agents HP Insight pour iLO sur le serveur distant. Pour plus d'informations sur l'installation et la configuration des agents, reportez-vous à la section « Installation des drivers de périphérique iLO » (page 19).

Correspondance du port dans Systems Insight Manager

Systems Insight Manager est configuré pour démarrer une session HTTP et rechercher la carte iLO sur le port 80. Ce port est modifiable. Si vous souhaitez modifier le numéro du port, vous devez également le modifier dans Network Settings (Paramètres réseau) et dans Systems Insight Manager.

Pour changer le numéro du port dans Systems Insight Manager, ajoutez le port au fichier \config\identification\additionalWsDisc.props, dans le répertoire où le programme Systems Insight Manager est installé. L'entrée doit commencer par le numéro de port HTTP pour iLO. Il n'est pas nécessaire d'avoir une entrée pour la carte iLO dans ce fichier si celle-ci reste connectée sur le port 80 standard. Il est très important que l'entrée soit sur une seule ligne et que le numéro de port y figure en premier, avec tous les autres éléments en tous points identiques à ce qui apparaît dans l'exemple suivant (y compris pour les lettres majuscules).

L'exemple suivant désigne la configuration de l'entrée si la carte iLO était détectée sur le port 55000 (cette écriture doit tenir sur une seule ligne dans le fichier) :

```
55000=iLO, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser
```

Consultation des informations concernant la licence du pack Advanced dans Systems Insight Manager

Systems Insight Manager affiche l'état de licence des processeurs de supervision iLO. Vous pouvez consulter ces informations pour déterminer le nombre et l'identité des périphériques iLO qui disposent d'une licence du pack iLO Advanced.

Pour afficher les informations concernant la licence, cliquez sur **Deploy>License Manager>Manage Keys** (Déployer>Gestionnaire de licences>Gérer les clés). Pour s'assurer de la pertinence de ces données, exécutez la tâche d'identification des systèmes pour vos processeurs de supervision. Reportez-vous à la documentation de Systems Insight Manager pour plus d'informations sur l'initialisation de tâches.

Résolution des problèmes de la carte iLO

Cette section traite des rubriques suivantes :

Conditions requises

- Clients Windows Server™
  - Windows® 2000
  - Microsoft® Internet Explorer 6.0 avec cryptage sur 128 bits
  - Java™ 1.4.2 JVM
- Clients Linux
  - Red Hat 7.3
  - Mozilla 1.60 ou Firefox 2.0 avec codage 128 bits
  - JVM Java™ 1.4.2 ou version ultérieure

Pour obtenir une liste complète des navigateurs et systèmes d'exploitation pris en charge, reportez-vous à la section « Navigateurs et systèmes d'exploitation clients pris en charge » (page 13). Pour télécharger la machine virtuelle recommandée pour votre configuration système, reportez-vous au site Web HP (http://www.hp.com/servers/manage/jvm).

Voyants du POST iLO

Pendant l'amorçage initial du système iLO, les voyants POST clignotent pour indiquer la progression du processus. Une fois l'amorçage effectué, le voyant Heartbeat (HB) clignote toutes les secondes. Le voyant 7 clignote aussi à intervalles réguliers pendant le fonctionnement normal.

Les voyants 1 à 6 s'allument après l'initialisation du système pour indiquer une panne du matériel. Dans ce cas, vous devez réinitialiser iLO. Pour l'emplacement des voyants, reportez-vous à la documentation de votre serveur.

Si une panne survient pendant l'exécution de iLO, le voyant HB et le voyant 7 restent allumés ou éteints en permanence. Une panne de ce type peut aussi être signalée par le clignotement répété des huit voyants. Si une erreur se produit pendant l'exécution, réinitialisez iLO.

Un clignotement séquentiel des voyants 1, 2, 3, 4, 5, 6, 7 et 8, se répétant à l'infini, indique l'échec d'un flashage (mise à niveau du microprogramme) au niveau de la carte iLO et signale que cette dernière est en mode de récupération par flashage. Pour plus d'informations, reportez-vous à la section « Récupération de iLO par flashage réseau » (page 208).

Les voyants ont les affectations suivantes :

HB	7	6	5	4	3	2	1

Voyants	**Code POST (activité terminée)**	**Description**	**Panne indiquée**
Aucun	00	Configurer les sélections de puces.	
1 ou 2	02—Fonctionnement normal	Déterminer la plate-forme.	
2 et 1	03	Définir le bit RUNMAP.	
3	04	Initialiser le contrôleur de SDRAM.	
3 et 2	06	Activer le cache I.	
3, 2 et 1	07	Initialiser (uniquement) le cache D.	
4	08	Copier le chargeur secondaire dans la RAM.	Impossibilité de copier le chargeur secondaire.
4 et 1	09	Vérifier le chargeur secondaire.	Défaut d'exécution du chargeur secondaire.
4 et 2	0a	Lancer le chargeur secondaire.	Échec du test de la mémoire SDRAM.
4, 2 et 1	0b	Copier la ROM dans la RAM.	Impossibilité de copier le bloc d'amorçage.
4 et 3	0c	Vérifier l'image de la ROM dans la RAM.	Échec de l'exécution du bloc d'amorçage.
4, 3 et 1	0d	Main du bloc d'amorçage démarré.	Le bloc d'amorçage n'a pas trouvé d'image valide.
Aucun		Démarrer l'initialisation de C Runtime.	
4, 3 et 2	0e	Main() a reçu le contrôle.	Échec de l'autotest de Main.
Variable	Variable	Chaque sous-système peut effectuer un auto-test.	
4, 3, 2 et 1	0f	Démarrer ThreadX	Échec du démarrage de RTOS.

Voyants	Code POST (activité terminée)	Description	Panne indiquée
Aucun	00	Main_init() terminé	Échec du démarrage du sous-système.
HB et 7		Clignote pendant que le processeur iLO exécute le code du microprogramme. Ne change pas la valeur des six voyants inférieurs.	

Le microprogramme du microprocesseur iLO comporte un code qui effectue des contrôles de cohérence. En cas d'échec de l'un de ces contrôles, le microprocesseur exécute le FEH. Le FEH présente les informations à l'aide des voyants du POST iLO. Les codes FEH se distinguent par le clignotement alternatif du numéro 99 et du reste du code d'erreur.

Code FEH	Contrôle de cohérence	Explication
9902	TXAPICHK	Une fonction RTOS a été appelée avec une valeur inadéquate ou à partir d'un appelant inapproprié.
9903	TXCONTEXT	Le contenu enregistré d'un ou plusieurs threads a été altéré.
9905	TRAP	Le test d'une pile a échoué, l'adresse de retour n'est pas valide ou une instruction de trap non valide a été détectée.
9966	NMIWR	Une écriture inattendue a été effectuée dans la mémoire basse.
99C1	CHKNULL	Le vecteur de réinitialisation a été modifié.

Entrées du journal d'événements

Affichage du journal d'événements	Explication
Server power failed (Panne d'alimentation du serveur)	S'affiche lorsque l'alimentation du serveur tombe en panne.
Browser login (Ouverture de session via le navigateur) : *Adresse IP*	Affiche l'adresse IP du navigateur qui a ouvert la session.
Server power restored (Alimentation du serveur rétablie)	S'affiche lorsque l'alimentation du serveur est rétablie.
Browser logout (Fermeture de session via le navigateur) : *Adresse IP*	Affiche l'adresse IP du navigateur qui a fermé la session.
Server reset (Serveur réinitialisé)	S'affiche lorsque le serveur est réinitialisé.
Failed Browser login - IP Address (Échec d'ouverture de session via le navigateur - adresse IP) : *Adresse IP*	S'affiche lorsque l'ouverture de session par un navigateur échoue.
iLO Self-Test Error (Erreur de l'auto-test iLO) : #	S'affiche lorsque iLO a échoué lors d'un test interne. La cause probable est la panne d'un composant critique. HP vous déconseille de continuer à utiliser iLO sur ce serveur.

Affichage du journal d'événements	Explication
iLO reset (Réinitialisation de iLO)	S'affiche lorsque iLO est réinitialisé.
On-board clock set; was (Horloge intégrée mise à l'heure ; l'heure était) #:#:#:#:#:#	S'affiche lorsque l'horloge intégrée est mise à l'heure.
Server logged critical error(s) (Erreur(s) critique(s) enregistrées par le serveur)	S'affiche lorsque le serveur enregistre des erreurs critiques.
Event log cleared by (Journal d'événements effacé par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur efface le journal d'événements.
iLO reset to factory defaults (iLO réinitialisé avec les valeurs d'usine)	S'affiche lorsque les paramètres par défaut de iLO sont restaurés.
iLO ROM upgrade to # (Mise à niveau de la ROM iLO avec la version #)	S'affiche lorsque la ROM a été mise à niveau.
iLO reset for ROM upgrade (iLO réinitialisé après mise à niveau de la ROM)	S'affiche lorsque iLO est réinitialisé pour une mise à niveau de la ROM.
iLO reset by user diagnostics (iLO réinitialisé par les diagnostics utilisateur)	S'affiche lorsque iLO est réinitialisé par un diagnostic utilisateur.
Power restored to iLO (Alimentation de iLO rétablie)	S'affiche lorsque l'alimentation de iLO est rétablie.
iLO reset by watchdog (iLO réinitialisé par le chien de garde)	S'affiche lorsqu'une erreur s'est produite dans iLO et que iLO s'est réinitialisé. Si l'erreur persiste, contactez l'assistance technique.
iLO reset by host (iLO réinitialisé par l'hôte)	S'affiche lorsque le serveur réinitialise iLO.
Recoverable iLO error, code # (Erreur iLO récupérable, code #)	S'affiche lorsqu'une erreur non critique s'est produite dans iLO et que iLO s'est réinitialisé. Si l'erreur persiste, contactez l'assistance technique.
SNMP trap delivery failure (Échec d'envoi du trap SNMP) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Test SNMP trap alert failed for (Échec de l'alerte du trap SNMP de test pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Power outage SNMP trap alert failed for (Échec de l'alerte du trap SNMP de coupure d'alimentation pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Server reset SNMP trap alert failed for (Échec de l'alerte du trap SNMP de réinitialisation de serveur pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Illegal login SNMP trap alert failed for (Échec de l'alerte du trap SNMP d'ouverture de session illégale pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Diagnostic error SNMP trap alert failed for (Échec de l'alerte du trap SNMP d'erreur de diagnostic pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
Host generated SNMP trap alert failed for (Échec de l'alerte du trap SNMP généré par l'hôte pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.

Affichage du journal d'événements	Explication
Network resource shortage SNMP trap alert failed for (Échec de l'alerte du trap SNMP de manque de ressources réseau pour) : *Adresse IP*	S'affiche lorsque le trap SNMP ne se connecte pas à l'adresse IP spécifiée.
iLO network link up (Liaison réseau iLO)	S'affiche lorsque le réseau est connecté à iLO.
iLO network link down (Rupture de liaison réseau iLO)	S'affiche lorsque le réseau n'est pas connecté à iLO.
iLO Firmware upgrade started by (Mise à niveau du microprogramme iLO initiée par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur lance la mise à niveau d'un microprogramme.
Host server reset by (Serveur hôte réinitialisé par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur réinitialise le serveur hôte.
Host server powered OFF by (Serveur hôte mis hors tension par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur met un serveur hôte hors tension.
Host server powered ON by (Serveur hôte mis sous tension par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur met un serveur hôte en tension.
Virtual Floppy in use by (Disquette virtuelle utilisée par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur commence à utiliser une disquette virtuelle.
Remote Console login (Ouverture de session sur la console distante) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur ouvre une session sur une console distante.
Remote Console Closed (Console distante fermée)	S'affiche lorsqu'une session d'une console distante est fermée.
Failed Console login - IP Address (Échec d'ouverture de session sur la console distante - adresse IP) : *Adresse IP*	Affiche le nom et l'adresse IP utilisés pour une tentative d'ouverture de session sur une console distante qui a échoué.
Added User (Utilisateur ajouté) : *User (Utilisateur)*	S'affiche en cas d'ajout d'un utilisateur local.
User Deleted by (Utilisateur supprimé par) : *User (Utilisateur)*	S'affiche en cas de suppression d'un utilisateur local.
Modified User (Utilisateur modifié) : *User (Utilisateur)*	S'affiche en cas de modification d'un utilisateur local.
Browser login (Ouverture de session via le navigateur) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur valide ouvre une session iLO à l'aide d'un navigateur Internet.
Browser logout (Fermeture de session via le navigateur) : User (Utilisateur)	S'affiche lorsqu'un utilisateur ferme une session iLO à l'aide d'un navigateur Internet.
Failed Browser login - IP Address (Échec d'ouverture de session via le navigateur - adresse IP) : *Adresse IP*	S'affiche lorsque l'ouverture de session par un navigateur échoue.
Remote Console login (Ouverture de session sur la console distante) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé ouvre une session à l'aide du port de la console distante.
Remote Console Closed (Console distante fermée)	S'affiche lorsqu'un utilisateur autorisé de la console distante a fermé une session ou lorsque le port de la console distante est fermé à la suite d'une tentative d'ouverture de session manquée.

Affichage du journal d'événements	Explication
Failed Console login - IP Address (Échec d'ouverture de session par la console distante - adresse IP) : *Adresse IP*	S'affiche lorsqu'un utilisateur non autorisé a échoué dans trois essais d'ouverture de session en utilisant le port de la console distante.
Added User (Utilisateur ajouté) : *User (Utilisateur)*	S'affiche lorsqu'une nouvelle entrée est portée à la liste des utilisateurs non autorisés.
User Deleted by (Utilisateur supprimé par) : *User (Utilisateur)*	S'affiche lorsqu'une entrée est retirée de la liste des utilisateurs non autorisés. La section Utilisateur affiche l'utilisateur qui a demandé la suppression.
Event Log Cleared (Journal d'événement effacé) : *User (Utilisateur)*	S'affiche lorsque l'utilisateur efface le journal d'événements.
Power Cycle (Reset) (Cycle d'alimentation - Réinitialisation) : *User (Utilisateur)*	S'affiche lorsque l'alimentation a été réinitialisée.
Virtual Power Event (Événement d'alimentation virtuelle) : *User (Utilisateur)*	S'affiche en cas d'utilisation du bouton virtuel d'alimentation.
Security Override Switch Setting is On (Le commutateur de neutralisation de la sécurité est activé)	S'affiche lorsque le système est amorcé tandis que le commutateur de neutralisation de la sécurité est activé.
Security Override Switch Setting Changed to Off (Passage du commutateur de neutralisation de la sécurité de l'état activé à l'état désactivé)	S'affiche lorsque le système est amorcé avec passage du commutateur de neutralisation de l'état activé à l'état désactivé.
On-board clock set; was [NOT SET] (Horloge intégrée mise à l'heure ; l'heure était auparavant [NON DÉFINIE])	S'affiche lorsque l'horloge intégrée est mise à l'heure. Affiche l'heure précédente ou l'indication "NOT SET" (Non définie) si l'heure n'avait pas été définie auparavant.
Logs full SNMP trap alert failed for (Échec de l'alerte du trap SNMP de saturation des journaux) : *Adresse IP*	S'affiche lorsque les journaux sont saturés et que l'alerte du trap SNMP a échoué pour une adresse IP spécifiée.
Security disabled SNMP trap alert failed for (Échec de l'alerte du trap SNMP de désactivation de la sécurité pour) : *Adresse IP*	S'affiche lorsque la sécurité a été désactivée et que l'alerte du trap SNMP a échoué pour une adresse IP spécifiée.
Security enabled SNMP trap alert failed for (Échec de l'alerte du trap SNMP d'activation de la sécurité pour) : *Adresse IP*	S'affiche lorsque la sécurité a été activée et que l'alerte du trap SNMP a échoué pour une adresse IP spécifiée.
Virtual Floppy connected by *User* (Disquette virtuelle connectée par *Utilisateur*).	S'affiche lorsqu'un utilisateur autorisé connecte la disquette virtuelle.
Virtual Floppy disconnected by *User* (Disquette virtuelle déconnectée par *Utilisateur*).	S'affiche lorsqu'un utilisateur autorisé déconnecte la disquette virtuelle.
License added by (Licence ajoutée par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé ajoute une licence.
License removed by (Licence retirée par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé supprime une licence.
License activation error by (Erreur d'activation de licence par) : *User (Utilisateur)*	S'affiche lorsqu'une erreur d'activation de licence se produit.
iLO RBSU user login (Ouverture d'une session de l'utilitaire iLO RBSU par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé ouvre une session de l'utilitaire iLO RBSU.

Affichage du journal d'événements	Explication
Power on request received by (Demande de mise sous tension reçue par) : *Type*	Une demande de mise sous tension d'un des types suivants a été reçue : Power Button (Bouton de mise sous tension) Wake-On LAN (Réveil en réseau) Mise sous tension automatique
Virtual NMI selected by (NMI virtuel sélectionné par) : *User (Utilisateur)*	S'affiche lorsqu'un utilisateur autorisé sélectionne le bouton NMI virtuel.
Virtual Serial Port session started by (Session de port série virtuel initiée par) : *User (Utilisateur)*	S'affiche au lancement d'une session de port série virtuel.
Virtual Serial Port session stopped by (Session de port série virtuel arrêtée par) : *User (Utilisateur)*	S'affiche lors de l'arrêt d'une session de port série virtuel.
Virtual Serial Port session login failure from (Echec d'ouverture de session de port série virtuel de) : *User (Utilisateur)*	S'affiche en cas d'échec d'une ouverture de session de port série virtuel.

Problèmes matériels et logiciels relatifs à la liaison

Les sections suivantes présentent les éléments à prendre en considération lorsque vous essayez de résoudre des problèmes matériels ou logiciels relatifs à la liaison.

Matériels

iLO utilise un câblage Ethernet standard, et notamment CAT5 UTP avec des connecteurs RJ-45. Un câblage point à point est nécessaire pour établir une liaison matérielle vers un concentrateur Ethernet standard. Utilisez un câble croisé pour une connexion PC directe.

Logiciels

Le port de supervision iLO doit être connecté à un réseau, lui-même connecté à un serveur DHCP, et iLO doit se trouver sur le réseau avant la mise sous tension. DHCP envoie une demande aussitôt après la mise sous tension. Si la demande DHCP n'a pas reçu de réponse lors de la première initialisation de iLO, elle est réémise toutes les 90 secondes.

Le serveur DHCP doit être configuré pour fournir une résolution des noms DNS et WINS. La carte iLO peut être configurée pour fonctionner avec une adresse IP statique soit dans la configuration de l'option F8 soit dans la page Web Network Settings (Paramètres réseau).

Le nom DNS par défaut apparaît sur l'étiquette des paramètres réseau et permet de localiser iLO sans connaître l'adresse IP qui lui a été attribuée.

Si une connexion directe à un PC est employée, une adresse IP statique doit être utilisée en l'absence d'un serveur DHCP sur la liaison.

Dans l'utilitaire de configuration sur ROM (RBSU) de iLO, vous pouvez appuyer sur la touche **F1** à l'intérieur de la page DNS/DHCP des options avancées pour consulter l'état des demandes DHCP de iLO.

Problèmes d'ouverture de session

Utilisez les informations suivantes pour essayer de résoudre les problèmes d'ouverture de session :

- Utilisez le nom de connexion par défaut indiqué sur l'étiquette des paramètres réseau.
- Si vous oubliez votre mot de passe, un administrateur doté du privilège Administer User Accounts (Administrer comptes utilisateur) peut le redéfinir.
- Si un administrateur oublie son mot de passe, il doit utiliser le commutateur de neutralisation de la sécurité ou créer un mot de passe et un compte administrateur à l'aide de HPONCFG.
- Vérifiez les problèmes classiques :
  - Le mot de passe respecte-t-il les restrictions applicables aux mots de passe ? Par exemple, le mot de passe inclut-il des caractères majuscules et minuscules ?
  - Le navigateur utilisé est-il pris en charge ?

Nom et mot de passe d'ouverture de session refusés

Si vous vous êtes connecté à iLO, mais qu'il n'accepte pas votre nom et mot de passe d'ouverture de session, vous devez vérifier que les informations d'ouverture de session ont été correctement configurées. Demandez à un utilisateur doté du privilège d'administration des comptes utilisateur d'ouvrir une session, puis de changer votre mot de passe. Si vous ne parvenez toujours pas à vous connecter, demandez à l'utilisateur de rouvrir une session et de supprimer, puis de rajouter votre compte utilisateur.

REMARQUE : l'utilitaire RBSU peut également servir à corriger des problèmes d'ouverture de session.

Fermeture de session prématurée par l'utilisateur de l'annuaire

Des erreurs de réseau peuvent obliger la carte iLO à conclure qu'une connexion à l'annuaire n'est plus valide. Si la carte iLO ne peut pas détecter l'annuaire, elle met fin à la connexion à l'annuaire. Toutes les tentatives visant à continuer d'utiliser la connexion interrompue redirigent le navigateur sur la page de connexion.

La redirection sur la page de connexion peut correspondre une expiration de session prématurée. Une expiration de session prématurée peut se produire au cours d'une session active dans les cas suivants :

- La connexion au réseau est interrompue ;
- Le serveur d'annuaire est arrêté.

Pour reprendre une session arrêtée prématurément, il faut se reconnecter et continuer d'utiliser la carte iLO. Si le serveur d'annuaire est indisponible, vous devez utiliser un compte local.

Accès impossible au port de supervision iLO par son nom

Le port de supervision iLO peut s'enregistrer sur un serveur WINS, soit un serveur DNS dynamique (DDNS) pour fournir la résolution nom-vers-adresse IP nécessaire pour accéder au port de supervision iLO par le nom. Le serveur WINS ou DDNS doit être actif et en cours d'exécution avant la mise sous tension du port de supervision iLO et ce dernier doit avoir un chemin valide vers le serveur WINS ou DDNS.

Il faut aussi que le port de supervision iLO soit configuré avec l'adresse IP du serveur WINS ou DDNS. DHCP permet de configurer le serveur DHCP avec les adresses IP nécessaires. Vous pouvez aussi entrer les adresses IP par l'intermédiaire de l'utilitaire RBSU ou de l'option **Network Settings** (Paramètres réseau) de l'onglet Administration. Le port de supervision iLO doit être configuré pour s'enregistrer sur un serveur WINS ou DDNS. Ces options sont activées par défaut et peuvent être modifiées par l'intermédiaire de l'utilitaire RBSU ou de l'option **Network Settings** (Paramètres réseau) de l'onglet Administration.

Les clients utilisés pour accéder au port de supervision iLO doivent être configurés pour utiliser le même serveur DDNS que celui sur lequel l'adresse IP du port de supervision iLO a été enregistrée.

Avec un serveur WINS et un serveur DNS non dynamique, l'accès au port de supervision iLO peut être nettement plus rapide si vous configurez le serveur DNS afin qu'il utilise le serveur WINS pour la résolution des noms. Pour plus d'informations, reportez-vous à la documentation Microsoft® appropriée.

Indisponibilité de iLO RBSU après la réinitialisation de iLO et du serveur

Si vous réinitialisez le processeur iLO et directement après le serveur, il y a un faible risque que le microprogramme de la carte iLO ne soit pas totalement initialisé lorsque le serveur démarre et tente d'invoquer l'utilitaire iLO RBSU. Dans ce cas, l'utilitaire iLO RBSU sera indisponible ou le code ROM de l'option de iLO sera omis. Si cela se produit, réinitialisez le serveur une seconde fois. Pour éviter ce problème, laissez s'écouler quelques secondes entre la réinitialisation du processeur iLO et celle du serveur.

Accès impossible à la page d'ouverture

Si vous ne parvenez pas à accéder à la page d'ouverture de session, vérifiez que le niveau de cryptage SSL est configuré à 128 bits. Le niveau de cryptage SSL dans iLO est configuré à 128 bits et n'est pas modifiable. Ce niveau doit être le même sur les deux dispositifs.

Accès impossible à iLO par Telnet

Si vous ne parvenez pas à accéder à iLO à l'aide de Telnet, vérifiez la configuration du port de console distante (paramètre Remote Console Port Configuration) et le cryptage des données de la console distante (paramètre Remote Console Data Encryption) dans l'écran Global Settings (Paramètres généraux). Si la configuration du port de console distante (Remote Console Port Configuration) a la valeur Automatic (Automatique), l'applet Remote Console active le port 23, lance une session et ferme le port une fois la session terminée. Telnet ne pouvant pas activer automatiquement le port 23, il échoue. Pour plus d'informations sur les paramètres Telnet, reportez-vous à la section relative à la prise en charge de Telnet.

Accès impossible au support virtuel ou à la console graphique distante

Le support virtuel et la console distante graphique ne sont accessibles qu'avec la licence du pack iLO Advanced, disponible en option. Un message s'affiche pour vous informer que ces fonctions ne sont disponibles qu'avec une licence. Bien que 10 utilisateurs maximum soient autorisés à ouvrir une session iLO, un seul d'entre eux peut accéder à la console distante. Un message d'avertissement s'affiche pour signaler que la console distante est déjà utilisée.

Connexion à iLO impossible après la modification des paramètres réseau

Vérifiez que les deux extrémités de la connexion (carte réseau et commutateur) possèdent les mêmes paramètres de sélection automatique de la vitesse de l'émetteur récepteur, de vitesse et de duplex. Ainsi, si une extrémité est configurée pour sélectionner automatiquement la connexion, l'autre doit l'être aussi. Les paramètres de la carte réseau iLO sont configurés dans l'écran Network Settings (Paramètres réseau).

Connexion impossible au port de diagnostic iLO

Si vous ne parvenez pas à vous connecter au port de diagnostic iLO par l'intermédiaire de la carte réseau, prenez en compte les éléments suivants :

- L'utilisation du port de diagnostic est détectée automatiquement lorsqu'un câble réseau actif y est raccordé. Lors du basculement entre le port de diagnostic et le port arrière, vous devez attendre une minute environ que la commutation réseau soit exécutée avant d'essayer de vous connecter par l'intermédiaire du navigateur Web.
- Si une activité importante est en cours, le port de diagnostic est inutilisable tant que celle-ci n'est pas achevée. Les activités importantes sont les suivantes :
  - mise à niveau des microprogrammes ;
  - session de la console distante ;
  - initialisation de SSL.
- Si vous utilisez une station de travail client contenant plusieurs cartes réseau activées, telles qu'une carte sans fil et une carte réseau, un problème de routage peut vous empêcher d'accéder au port de diagnostic. Pour résoudre ce problème :

1. Activez une seule carte réseau sur la station de travail client. Désactivez par exemple la carte réseau sans fil.
2. Configurez l'adresse IP du réseau de la station de travail client de manière à ce qu'elle corresponde au réseau du port de diagnostic iLO.
   a. Le paramètre de l'adresse IP doit être 192.168.1.*X*, où *X* est un nombre autre que 1, car l'adresse IP du port de diagnostic est 192.168.1.1.
   b. Le masque de sous-réseau doit être 255.255.255.0.

Connexion impossible au processeur iLO via la carte réseau

Si vous ne parvenez pas à vous connecter au processeur iLO par l'intermédiaire de la carte réseau, essayez l'une des méthodes de résolution des problèmes suivantes :

- Assurez-vous que le voyant vert (état de la liaison) du connecteur iLO RJ-45 est allumé. Celui-ci indique que la connexion est établie entre la carte réseau PCI et le concentrateur réseau.
- Vérifiez que le voyant vert clignote. Cela indique un trafic normal sur le réseau.
- Exécutez l'utilitaire iLO RBSU pour vous assurer que la carte réseau est activée et vérifier l'adresse IP et le masque de sous-réseau qui lui ont été attribués.
- Exécutez l'utilitaire iLO RBSU puis utilisez l'onglet F1 - Advanced (F1 - Avancé) de la page DNS/DHCP pour afficher l'état des demandes DHCP.
- Testez (ping) l'adresse IP de la carte réseau à partir d'une autre station de travail du réseau.

- Essayez de vous connecter avec le navigateur en tapant l'adresse IP de la carte réseau en tant qu'URL. Vous pouvez voir la page d'accueil iLO depuis cette adresse.
- Réinitialisez iLO.

  REMARQUE : si une connexion réseau est établie, vous devrez peut-être attendre pendant 90 secondes la demande du serveur DHCP.

Les serveurs ProLiant BL p-Class proposent un port de diagnostic. Si vous connectez un câble réseau permanent au port de diagnostic, iLO bascule automatiquement du port iLO vers le port de diagnostic. Lors du basculement entre le port de diagnostic et le port arrière, vous devez attendre une minute environ que la commutation réseau soit exécutée avant d'essayer de vous connecter par l'intermédiaire du navigateur Web.

Connexion à iLO impossible après l'installation du certificat iLO

Si le certificat à signature automatique iLO est installé de manière permanente dans certains navigateurs, et que la carte iLO est réinitialisée, il peut s'avérer impossible de se reconnecter à iLO car celle-ci génère un nouveau certificat à signature automatique à chaque réinitialisation. Lorsqu'un certificat est installé dans le navigateur, il est indexé par le nom qu'il contient. Ce nom est unique à chaque carte iLO. À chaque fois que la carte iLO se réinitialise, elle génère un nouveau certificat portant le même nom.

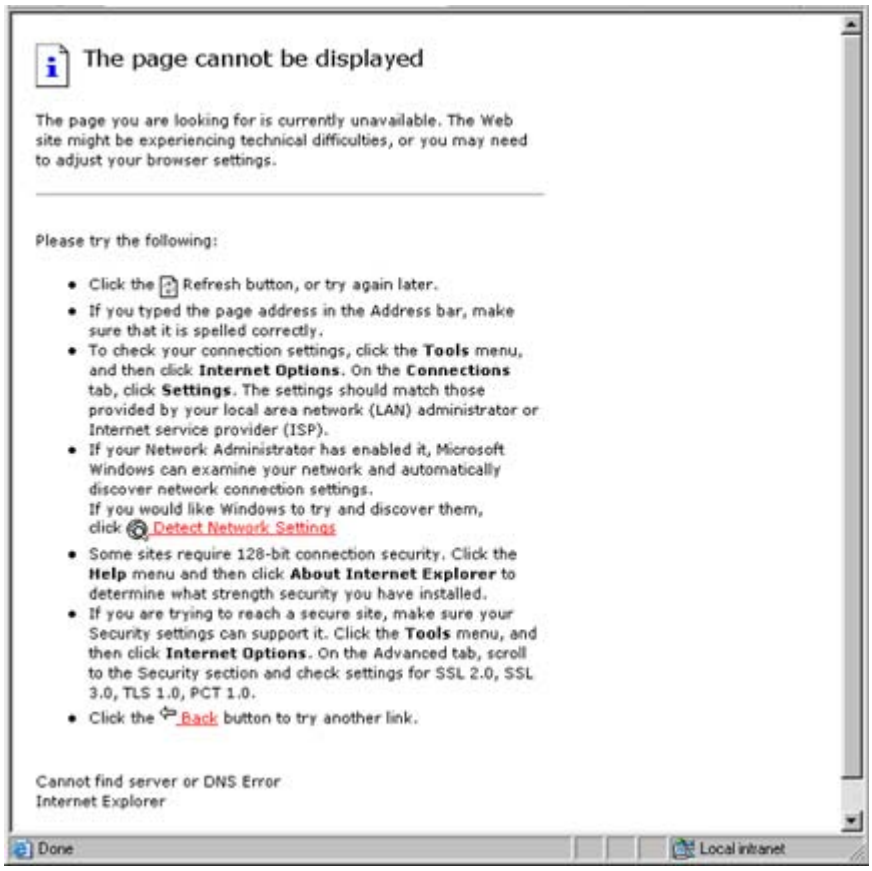
Pour éviter ce problème, n'installez pas le certificat à signature automatique iLO dans l'emplacement de stockage des certificats du navigateur. Vous devez demander un certificat permanent à une autorité de certification et l'importer dans la carte iLO. Vous pouvez ensuite l'installer dans l'emplacement de stockage du navigateur.

Problèmes de pare-feu

iLO communique par l'intermédiaire de plusieurs ports TCP/IP configurables. Si ces ports sont bloqués, l'administrateur doit configurer le pare-feu de façon à autoriser les communications sur ces ports. Pour consulter ou modifier la configuration des ports, reportez-vous à l'option Global Settings (Paramètres généraux) de l'onglet Administration.

Échec de connexion avec l'authentification à deux facteurs

Lorsque l'authentification échoue, le type de page suivant s'affiche.



La connexion à iLO à l'aide de l'authentification à deux facteurs par carte à puce échoue si :

- Le certificat sélectionné à la page Client Authentication (Authentification client) n'est pas émis par l'autorité de certification approuvée.
- Le certificat a été émis par l'autorité de certification approuvée mais n'a pas été associé à un compte utilisateur local.
- L'authentification d'annuaire est activée (une autre page s'affiche).

  Dans ce cas, le champ du nom d'utilisateur est renseigné par le nom principal de l'utilisateur obtenu à partir du certificat ou par le nom distinctif de l'utilisateur dans l'annuaire, lequel est déduit à partir de l'objet du certificat. Ce paramètre est configuré grâce au champ Certificate Owner (Propriétaire du certificat) de la page Two-Factor Authentication Settings (Paramètres d'authentification à deux facteurs) sur iLO. Le champ du nom d'utilisateur ne peut pas être modifié. iLO n'autorise aucune tentative d'authentification émanant d'un utilisateur d'annuaire autre que celui pour lequel a été émis le certificat.

Pour remédier à ces problèmes, assurez-vous qu'un certificat est émis par l'autorité de certification et associé à l'utilisateur. Pour en savoir plus, reportez-vous à la section « Two-Factor Authentication Settings » (Paramètres d'authentification à deux facteurs) (page 35).

Problèmes de serveur proxy

Si votre navigateur Web est configuré pour utiliser un serveur proxy, il ne se connectera pas à l'adresse IP de la carte iLO. Pour résoudre ce problème, configurez-le de manière à ce qu'il n'utilise pas le serveur proxy pour l'adresse IP de la carte iLO. Par exemple, dans Internet Explorer, sélectionnez **Outils>Options Internet>Connexions>Paramètres du réseau local>Avancé**, puis entrez l'adresse IP ou le nom DNS iLO dans le champ Exceptions.

Résolution des problèmes liés aux alertes et aux traps

Alerte	Explication
Test Trap (Trap de test)	Ce trap est généré par un utilisateur via la page de configuration Web.
Server Power Outage (Panne de courant du serveur)	Le serveur n'est plus alimenté.
Server Reset (Réinitialisation du serveur)	Le serveur a été réinitialisé.
Failed Login Attempt (Échec de tentative d'ouverture de session)	Une tentative d'ouverture de session à distance par un utilisateur a échoué.
General Error (Erreur générale)	Cette condition d'erreur n'est pas prédéfinie par la MIB codée en dur.
Logs (Journaux)	Le journal circulaire est saturé.
Security Override Switch Changed: On/Off (Commutateur de neutralisation de la sécurité activé/désactivé)	L'état du commutateur de neutralisation de la sécurité a changé (activé/désactivé).
Rack Server Power On Failed (Échec de la mise sous tension du serveur du rack)	Le serveur n'a pas pu être mis sous tension, car le rack BL p-Class a indiqué que l'alimentation disponible était insuffisante effectuer cette opération.
Rack Server Power On Manual Override (Neutralisation manuelle de la mise sous tension du serveur du rack)	Le client a forcé manuellement la mise sous tension du serveur bien que le rack BL p-Class ait signalé l'insuffisance de l'alimentation.
Rack Name Changed (Modification du nom du rack)	Le nom du rack ProLiant BL p-Class a été modifié.

Réception impossible des alarmes de Insight Manager 7 ou Systems Insight Manager (traps SNMP) à partir de iLO

Un utilisateur autorisé à configurer les paramètres iLO (privilège Configure iLO Settings) doit se connecter à la carte iLO pour configurer les paramètres des traps SNMP. Lorsque vous êtes connecté à iLO, assurez-vous que les types d'alertes et les destinations de traps corrects sont activés dans l'écran SNMP/Insight Manager Settings (Paramètres SNMP/Insight Manager) de l'application de la console iLO.

Commutateur de neutralisation de la sécurité iLO

Le commutateur de neutralisation de la sécurité iLO ouvre un accès d'urgence à l'administrateur avec un contrôle physique de la carte système du serveur. En activant le commutateur de neutralisation de la sécurité iLO, vous disposez d'un droit de connexion, avec tous les privilèges, sans ID d'utilisateur ni mot de passe.

Le commutateur de neutralisation de la sécurité iLO se trouve à l'intérieur du serveur. Vous ne pouvez dès lors pas y accéder sans ouvrir le boîtier du serveur. Pour activer le commutateur de neutralisation de la sécurité iLO, mettez d'abord le serveur hors tension et débranchez-le. Activez le commutateur, puis mettez le serveur sous tension. Inversez la procédure pour désactiver le commutateur de neutralisation de la sécurité iLO.

Un message d'avertissement s'affiche sur les pages Web iLO, indiquant que le commutateur de neutralisation de la sécurité iLO est en cours d'utilisation. Une entrée est ajoutée au journal iLO pour enregistrer l'utilisation du commutateur de neutralisation de la sécurité iLO. Une alerte SNMP peut également être envoyée après activation ou désactivation du commutateur de neutralisation de la sécurité iLO.

Dans le cas improbable où cela s'avérerait nécessaire, l'activation du commutateur de neutralisation de la sécurité iLO permet également de flasher le bloc d'amorçage iLO. Ce dernier est alors exposé jusqu'à la réinitialisation de iLO. HP vous recommande de déconnecter la carte iLO du réseau tant que la réinitialisation n'est pas terminée.

Suivant le serveur utilisé, le commutateur de neutralisation de la sécurité iLO peut être un simple cavalier ou une position de commutateur spécifique sur un panneau de commutateurs à positions multiples. Pour y accéder, reportez-vous à la documentation de votre serveur.

Message d'erreur de code d'authentification

Sous un navigateur Mozilla, vous pouvez recevoir un message d'erreur de code d'authentification de message incorrect, vous indiquant que le code et le certificat publics ou privés utilisés pour lancer la session SSL du navigateur ont changé. Ce message d'erreur peut survenir lorsque vous n'utilisez pas de certificat fourni par le client, car la carte iLO crée son propre certificat à signature automatique toutes les fois qu'elle est réinitialisée.

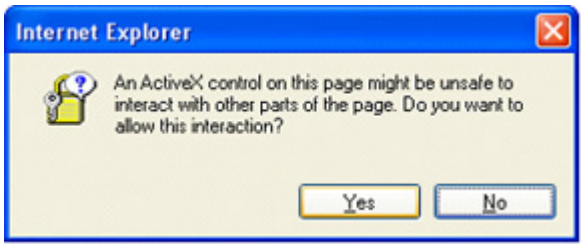
Pour résoudre ce problème, fermez et redémarrez le navigateur Web ou installez vos propres certificats sur la carte iLO.

Résolution des problèmes liés à l'annuaire

Les sections suivantes expliquent comment résoudre les problèmes liés à l'annuaire.

Je ne peux pas me connecter en utilisant le format domaine/nom mais j'y parviens avec le nom distinctif complet

Pour vous connecter en utilisant le format domaine/nom, les contrôles ActiveX doivent être activés. Pour vérifier que votre navigateur laisse le processus de connexion appeler des contrôles ActiveX, ouvrez Internet Explorer et définissez le paramètre ActiveX sur la valeur **Prompt** (Demander). Vous devez alors voir un message semblable à celui-ci :



Les contrôles ActiveX sont activés et j'obtiens le message mais la connexion au format domaine/nom ne fonctionne pas

1. Connectez-vous avec un compte local et recherchez le nom du serveur d'annuaire.
2. Vérifiez que ce nom est bien un nom et non une adresse IP.
3. Vérifiez que vous pouvez interroger le nom du serveur d'annuaire depuis votre client avec la commande ping.
4. Exécutez des tests de configuration de l'annuaire. Vérifiez que la commande ping a été correctement reçue. Pour plus d'informations sur les tests des paramètres d'annuaire, reportez-vous à la section « Tests d'annuaire » (page 72).

Les contextes utilisateur ne semblent pas fonctionner

Contactez votre administrateur réseau. Le nom distinctif complet de votre objet utilisateur doit figurer dans l'annuaire. Votre nom de connexion correspond à ce qui apparaît après la première occurrence de CN=. Le reste du nom distinctif doit apparaître dans l'un des champs de contexte utilisateur. Les contextes utilisateur ne font pas la distinction majuscules/minuscules. Cependant, tout le reste, notamment les espaces, fait partie du contexte utilisateur.

Résolution des problèmes liés à la souris

Les sections suivantes expliquent comment résoudre les problèmes matériels et logiciels liés à la souris.

Souris USB locale et Linux

Si vous exécutez Linux sur votre serveur et que vous disposez d'une souris USB locale, celle-ci ne fonctionne pas dans la console distante. Pour résoudre ce problème, configurez le système pour qu'il utilise deux souris. Ajoutez les lignes suivantes à votre fichier XF86Config :

- Dans la section ServerLayout, ajoutez les commandes suivantes :

  ```
  InputDevice  «Mouse1» «SendCoreEvents»
  ```

  Par exemple :

  ```
  Section «ServerLayout»
     Identifier «Default Layout»
     Screen 0  «Screen0» 0 0
     InputDevice     «Mouse0» «CorePointer»
     InputDevice     «Mouse1» «SendCoreEvents»
     InputDevice     «Keyboard0» «CoreKeyboard»
  EndSection
  ```

- Dans la section InputDevice, ajoutez les commandes suivantes :

  ```
  Section «InputDevice»
     Identifier  «Mouse1»
     Driver      «mouse»
     Option    «Protocol» «PS/2»
     Option    «Device" «/dev/psaux»
     Option    «Emulate3Buttons» «yes»
  EndSection
  ```

Après avoir mis le fichier de configuration à jour, deux sections InputDevice s'affichent. Chacune d'elle contient des informations pour la souris. Réglez l'identificateur afin qu'il corresponde à l'étiquette utilisée dans la section ServerLayout.

Le format varie en fonction du système d'exploitation utilisé. Il peut s'avérer nécessaire de modifier celui des exemples donnés pour votre système d'exploitation. Par exemple, Red Hat 3.0 utilise Mouse0 pour l'étiquette par défaut, alors que SUSE 8 utilise Mouse[1]. Respectez les conventions de nom de votre système d'exploitation. Utilisez une étiquette unique pour chaque souris. La section InputDevice décrit la souris USB actuellement utilisée et s'avère utile lors de la configuration de la deuxième souris. Après avoir enregistré les modifications, redémarrez le système.

Problème de souris sous SuSE Linux

Les utilisateurs de SuSE Linux Enterprise 8.0 sous United Linux 1.0 risquent de rencontrer des problèmes liés à la souris lors d'une réinitialisation avec la console distante. Pour corriger cela, sélectionnez la souris PS/2 (port Aux) à l'invite de l'application de configuration de la souris YaST en mode texte.

Si la fonction de console distante iLO est fermée, et qu'il est nécessaire d'utiliser une souris à molette connectée au serveur, exécutez YaST2 Control Center et sélectionnez la souris Intelli/Wheel (port Aux).

Problème de contrôle de la souris de la console distante

Lorsque vous utilisez la console distante sur un serveur fonctionnant sous Microsoft® Windows® Server 2003, il peut arriver que les mouvements de la souris soient lents et que vous ayez du mal à déplacer le curseur dans les coins de l'écran. Lorsque vous essayez d'atteindre un coin éloigné de l'écran, la souris peut même disparaître complètement.

REMARQUE : ce comportement de la souris est plus prononcé lorsque la session de la console distante est lancée dans une fenêtre d'applet du navigateur dont la taille est plus petite que l'écran du serveur et que vous devez faire défiler l'écran pour afficher l'intégralité de son contenu.

Pour résoudre ce problème :

1. Sélectionnez **Start>Settings>Control Panel>Mouse Properties** (Démarrer>Paramètres>Panneau de configuration>Propriétés de souris) dans l'applet du bureau de Windows® Server 2003.
2. Désactivez le paramètre Enhance pointer precision (Améliorer la précision du pointeur).

Si le mouvement de la souris est toujours lent :

1. Sélectionnez **Start>Settings>Control Panel>Display>Settings> Advanced>Troubleshooting** (Démarrer>Paramètres>Panneau de configuration>Affichage>Paramètres>Avancé>Dépannage) dans l'applet du bureau de Windows® Server 2003.
2. Définissez l'accélération matérielle à Full (Complète).

Pour plus d'informations, reportez-vous à la section « Optimisation des performances de la fonction Graphical Remote Console (Console graphique distante) » (page 82).

Émulation d'un clavier PS/2 dans un environnement de serveur sans clavier

iLO permet d'émuler un clavier PS/2 dans un environnement de serveur sans clavier. Lorsque la carte iLO détecte que le serveur est sur le point de subir un auto-test de mise sous tension (POST), elle recherche un clavier PS/2. Si aucun clavier PS/2 n'est détecté, iLO sert de clavier PS/2 au serveur.

Résolution des problèmes liés à la console distante

Les sections suivantes expliquent comment résoudre les problèmes liés à la console distante. En règle générale :

- Les bloqueurs de publicité empêchent le port série virtuel et de console distante de démarrer.
- Ceux configurés pour empêcher l'ouverture automatique de nouvelles fenêtres empêchent le port série virtuel et de console distante de s'exécuter. Désactivez tous les programmes de ce type avant de démarrer le port série virtuel et de console distante.

Console distante Linux

Lorsque vous utilisez un client Linux avec une JVM autre que la version 1.4.2, vous pouvez rencontrer des problèmes avec la console distante. Par exemple, si vous redimensionnez la fenêtre de la console distante, elle peut s'afficher en grisé. Ces problèmes sont dus à la JVM. Pour y remédier, utilisez la JVM 1.4.2. Les versions 1.4.2 et 1.4.2_02 sont différentes, et des problèmes observés dans la version 1.4.2_02 n'apparaissent pas dans la version 1.4.2. La JVM 1.4.2 est prise en charge sur les combinaisons de navigateur et de système d'exploitation suivantes :

- Red Hat 3.0 WS
  - Mozilla 1.7
  - Firefox 1.02
- Novell Linux Desktop
  - Mozilla 1.7
  - Firefox 1.02

L'applet Remote Console présente une croix rouge lorsqu'elle exécute un navigateur client Linux

Les navigateurs Mozilla doivent être configurés pour pouvoir accepter les cookies.

1. Sous Préférences, sélectionnez **Privacy & Security>Cookies** (Confidentialité et sécurité>Cookies).
2. Sélectionnez **Allow cookies based on privacy settings** (Accepter les cookies en fonction des paramètres de confidentialité), puis cliquez sur **View** (Afficher).
3. Sur l'écran Cookies, sélectionnez **Allow Cookies based on privacy settings** (Accepter les cookies en fonction des paramètres de confidentialité).

Le niveau de confidentialité doit être défini sur Medium (Moyenne) ou Low (Faible).

Déplacement impossible du curseur de la console distante dans les coins de la fenêtre

Dans certains cas, il arrive que vous ne parveniez pas à déplacer le curseur de la souris dans les coins de la fenêtre de la console distante. Dans ce cas, cliquez sur le bouton droit de la souris et faites glisser le curseur en dehors de la fenêtre de la console distante, puis ramenez-le à l'intérieur de celle-ci.

Si la souris ne fonctionne toujours pas correctement ou que le problème se produit fréquemment, vérifiez que les paramètres de la souris correspondent à ceux recommandés dans la section « Optimisation des performances de la fonction Graphical Remote Console (Console graphique distante) » (page 82).

La console distante ne s'ouvre plus dans la session du navigateur en cours

L'ajout de la fonction Terminal Services Pass-Through (Pass-Through des Terminal Services) induit un comportement de l'applet de la console distante qui est légèrement différent de ce qu'il en est dans les précédentes versions du microprogramme iLO. Si une session de console distante est déjà ouverte, et que vous cliquez à nouveau sur le lien de la console, la session de la console distante ne sera pas relancée. Il peut sembler à l'utilisateur que la session de la console distante s'est bloquée.

Par exemple, lorsque les étapes suivantes sont exécutées :

1. Connectez-vous à iLO à partir du client-1 et ouvrez une session de console distante.
2. Connectez-vous à iLO à partir du client-2 et ouvrez une session de console distante ; le message `Remote console is already opened by another session` (La console distante est déjà ouverte par une autre session) s'affiche ; ceci est tout à fait normal puisqu'il n'est possible de prendre en charge qu'une seule console distante à la fois.
3. Retournez sur le client-1 et fermez la session de console distante.
4. Cliquez sur le lien Remote Console à partir du client-2 tout en gardant ouverte l'applet de l'ancienne console distante ; la session de console distante ne s'actualise pas et l'ancien message mentionné à l'étape 2 est toujours à l'écran.

Bien qu'il soit différent de ce qu'il en était dans les versions précédentes du microprogramme iLO, c'est ce comportement qui prévaut dans la version actuelle du microprogramme iLO. Pour éviter les problèmes de cette nature, veillez à toujours fermer une session de console distante ouverte avant d'essayer de la rouvrir.

Mise à jour incorrecte de la fenêtre texte de la console distante

Lorsque vous utilisez la console distante pour afficher des fenêtres texte dont la vitesse de défilement est très rapide, il arrive que la fenêtre ne soit pas mise à jour correctement. En effet, les mises à jour de l'affichage vont trop vite pour pouvoir être détectées et affichées par le microprogramme de la carte iLO. En général, seul le coin supérieur gauche de la fenêtre est mis à jour, tandis que le reste demeure statique. À la fin du défilement, cliquez sur **Refresh** (Actualiser) pour mettre à jour correctement la fenêtre texte.

Ce problème se produit notamment lors des processus d'amorçage et d'auto-test de Linux, au cours desquels certains messages POST peuvent être perdus. Le processus d'amorçage peut dès lors demander d'entrer une réponse depuis le clavier. Pour éviter ce problème, HP vous recommande de ralentir le processus d'amorçage et d'auto-test en modifiant le script de démarrage de Linux afin de laisser plus de temps aux réponses en provenance du clavier.

La console distante devient grisée ou noire

L'écran de la console distante devient grisé ou noir lorsque le serveur est réinitialisé à partir du client Terminal Services. L'écran reste grisé ou noir de 30 secondes à une minute. Le client se ferme car le serveur Terminal Services est indisponible. La console distante iLO devrait prendre le relais mais l'écran Remote Console (Console distante) devient grisé ou noir. Dès que l'écran redevient normal, les fonctions de la console distante sont à nouveau opérationnelles.

Résolution des problèmes liés aux protocoles SSH et Telnet

Les sections suivantes expliquent comment résoudre les problèmes liés aux protocoles SSH et Telnet.

Entrée initiale dans PuTTY lente

Lors de la connexion initiale à l'aide d'un client PuTTY, l'entrée prend environ 5 secondes. Pour y remédier, modifiez les options de configuration du client sous les options de connexion TCP bas débit : décochez l'option **Disable Nagle's algorithm** (Désactiver l'algorithme de Nagle). Sous les options Telnet, définissez le mode de négociation Telnet à **Passive** (Passif).

Le client PuTTY ne répond pas avec le port réseau partagé

Lorsque vous utilisez le client PuTTY avec le port réseau partagé, la session PuTTY peut ne pas répondre lorsqu'un volume important de données est transféré ou que vous utilisez un port série virtuel ou une console distante. Pour résoudre ce problème, fermez le client PuTT, et relancez la session.

Prise en charge SSH du mode texte à partir d'une session de la console distante

L'accès Telnet et SSH à partir de la console distante texte prend en charge la configuration standard 80 x 25 de l'écran texte. Ce mode est compatible pour la console distante texte de la majorité des interfaces texte disponibles dans les systèmes d'exploitation actuels. La configuration en mode texte étendu supérieure à 80 x 25 ne s'affiche pas correctement lorsque vous utilisez Telnet ou SSH. HP vous recommande de configurer l'application texte en mode 80 x 25 ou d'utiliser l'applet iLO Remote Console fournie par l'interface Web.

Résolution des problèmes liés aux Terminal Services

Les sections suivantes expliquent comment résoudre les problèmes liés aux Terminal Services.

Le bouton Terminal Services ne fonctionne pas

L'option Terminal Services ne fonctionne plus si l'option Deny (Refuser) est sélectionnée dans l'avertissement de sécurité de Java. Lorsque vous sélectionnez l'option Deny (Refuser), vous indiquez au navigateur que l'applet de la console distante n'est pas fiable. La console distante n'est plus autorisée à exécuter de code nécessitant un niveau supérieur de sécurité. Si l'option Deny (Refuser) est sélectionnée, la console distante ne sera pas autorisée à lancer le code requis pour activer le bouton Terminal Services. Si vous regardez dans la console Java, vous y verrez le message « `Security Exception - Access denied` » (Exception de sécurité - accès refusé).

Le serveur proxy des Terminal Services ne répond pas

À chaque réinitialisation de iLO (tel que la modification des paramètres réseau ou généraux), le Pass-Through des Terminal Services n'est pas disponible pendant deux minutes à compter du début de la réinitialisation. iLO prend 60 secondes pour se réinitialiser et effectuer le test POST avec une mémoire tampon de 60 secondes avant de continuer. Au bout de deux minutes, l'état passe à Available (Disponible) et le Pass-Through des Terminal Services est alors utilisable.

Résolution des problèmes de vidéo et de moniteur

Les sections suivantes présentent les éléments à prendre en considération lorsque vous essayez de résoudre des problèmes de vidéo ou de moniteur.

Principes généraux

- La résolution d'écran du client doit être supérieure à celle du serveur distant.
- La console distante iLO prend uniquement en charge la puce vidéo ATI Rage XL qui est intégrée au système. La fonction de console distante de iLO ne fonctionne pas si vous installez une carte vidéo enfichable. Par contre, toutes les autres fonctions iLO sont disponibles.
- La console distante n'est accessible qu'à un seul utilisateur à la fois. Vérifiez si un autre utilisateur a ouvert une session iLO.

Affichage incorrect de Telnet sous DOS®

Lorsque vous utilisez la session Telnet iLO pour afficher des écrans de texte dans une fenêtre DOS® agrandie et que l'écran du serveur dépasse une taille de 80 x 25, la session Telnet ne parvient à représenter que la partie supérieure de l'écran.

Pour corriger cela, adaptez les propriétés de la fenêtre DOS® de façon à limiter sa taille à 80 x 25 avant de l'agrandir.

- Dans la barre de titre de la fenêtre DOS®, cliquez à l'aide du bouton droit de la souris et sélectionnez **Properties** (Propriétés), puis **Layout** (Mise en forme).
- Dans l'onglet Layout (Mise en forme), attribuez la valeur 25 au paramètre Screen Buffer Size (Taille du buffer d'écran).

Absence d'affichage des applications vidéo dans la console distante

Certaines applications vidéo, telles que Microsoft® Media Player, ne s'affichent pas, ou alors de manière incorrecte, dans la console distante. Ce problème est principalement rencontré avec les applications qui utilisent des registres de superposition vidéo. De façon générale, les applications qui mettent les vidéos en flux utilisent des registres de superposition vidéo. La carte iLO n'est pas destinée à fonctionner avec ce type d'application.

Résolution des problèmes liés au support virtuel

Les sections suivantes expliquent comment résoudre les problèmes liés au support virtuel.

Liste des lecteurs virtuels

Lorsque vous utilisez le Pass-Through des Terminal Services sur un serveur exécutant Windows® 2000, une session Virtual CD-ROM (CD-ROM virtuel) n'apparaît pas sur le serveur. Ce problème ne se produit pas si le serveur exécute Windows® 2003. Il se produit également lorsque vous vous connectez directement à Terminal Services. Il ne s'agit pas d'un problème lié à la fonction n'est pas dû à la fonction iLO Terminal Services pass-through (Pass-Through des Terminal Services iLO).

L'applet Virtual Media est signalée par un X rouge et ne s'affiche pas

L'applet Virtual Media peut être signalée par un X rouge si une JVM ou un navigateur non pris en charge est utilisé ou si l'option Enable All Cookies (Activer tous les cookies) n'est pas activée. Pour résoudre ce problème, vérifiez que vous utilisez une JVM ou un navigateur pris en charge sur votre client en consultant le tableau de support présenté dans la section « Navigateurs et systèmes d'exploitation clients pris en charge » (page 13). Assurez-vous également que la fonction Enable All Cookies (Activer tous les cookies) est sélectionnée dans le menu Options ou Preferences (Préférences) du navigateur. Certains navigateurs n'activent pas les cookies par défaut.

L'applet Virtual Floppy Media ne répond pas

L'applet iLO Virtual Floppy Media peut ne plus répondre si la disquette physique contient une erreur de support.

Pour éviter ce problème, exécutez CHKDSK.EXE (ou un utilitaire du même type) afin de vérifier que la disquette ne contient pas d'erreur. Si elle en contient, rechargez l'image correspondante sur une nouvelle disquette physique.

Résolution de problèmes divers

Les sections suivantes expliquent comment résoudre des problèmes matériels et logiciels divers.

Cookies partagés entre les instances de navigateur et la carte iLO

La carte iLO utilise des cookies pour les sessions de navigateur, en partie pour distinguer les différentes ouvertures de session individuelles, chaque fenêtre de navigateur s'affichant comme une ouverture de session distincte, tout en partageant la même session active avec la carte iLO. Ces ouvertures de sessions multiples peuvent provoquer une confusion au niveau du navigateur. Cette confusion peut apparaître du fait qu'un problème relatif à la carte iLO traduit généralement un comportement relatif au navigateur.

Plusieurs processus peuvent obliger le navigateur à ouvrir des fenêtres supplémentaires. Les fenêtres du navigateur ouvertes à partir d'un navigateur ouvert représentent différents aspects du même programme en mémoire. Par conséquent, chaque fenêtre du navigateur partage les mêmes propriétés que celles de la fenêtre parent, y compris en ce qui concerne les cookies.

Instances communes

Lorsque iLO ouvre une nouvelle fenêtre du navigateur, comme par exemple Remote Console (Console distante), Virtual Media (Support virtuel) ou Help (Aide), cette fenêtre partage la même connexion à la carte iLO et le cookie de la session.

Le serveur Web iLO prend des décisions URL basées sur chaque requête reçue. Par exemple, si une requête ne dispose pas de privilèges d'accès, elle est redirigée vers la page de connexion, quelle que soit la requête d'origine. La redirection basée sur le serveur Web, en sélectionnant **File>New>Window** (Fichier>Nouveau>Fenêtre) ou en appuyant sur les touches **Ctrl+N**, ouvre une instance dupliquée du navigateur d'origine.

Comportement de l'ordre des cookies

Durant la connexion, la page de connexion crée un cookie de navigateur qui relie la fenêtre à la session appropriée du microprogramme. Le microprogramme surveille les ouvertures de session du navigateur en tant que sessions distinctes, listées dans la section Active Sessions (Sessions actives) de la page Status (État) de iLO.

Par exemple, lorsque l'utilisateur User1 ouvre une session, le serveur Web génère les cadres initiaux de la vue avec l'utilisateur actuel : User1 (Utilisateur1) est dans le volet supérieur, les éléments de menu dans le volet de gauche et les données de page dans le volet inférieur droit. Au fur et à mesure que User1 clique sur les liens, seuls les éléments de menu et les données de page sont mis à jour.

Alors que User1 est connecté, si un autre utilisateur User2 (Utilisateur2) ouvre une nouvelle fenêtre de navigateur sur le même client et s'y connecte, la deuxième ouverture de session remplace le cookie généré dans la session originale de l'utilisateur User1. En supposant que User2 est un compte utilisateur distinct, un nouveau cadre est généré et une nouvelle session accordée. Le deuxième session s'affiche dans la section Active Sessions (Sessions actives) de la page Status (État) de iLO avec, comme utilisateur actuel : User2 (Utilisateur2).

La deuxième ouverture de session a en effet rendu la première session (User1, Utilisateur1) orpheline, en effaçant le cookie généré pendant l'ouverture de session de User1. Ce comportement est identique à la fermeture du navigateur de User1 (Utilisateur1) sans cliquer sur le lien Log Out (Déconnexion). La session orpheline de User1 est exigée à l'expiration du délai de la session.

Le cadre de l'utilisateur actuel n'étant pas mis à jour sauf si le navigateur est obligé d'actualiser la page entière, User1 (Utilisateur1) peut continuer de naviguer en utilisant sa fenêtre de navigation. Cependant, le navigateur fonctionne à présent en utilisant les paramètres du cookie de la session de User2 (Utilisateur2), même si cela ne s'avère pas apparent.

Si User1 (Utilisateur1) continue de naviguer sous ce mode (User1 et User2 partageant le même processus du fait que User2 s'est connecté et a réinitialisé le cookie de la session), il peut se produire ce qui suit :

- La session de User1 se comporte de manière cohérente avec les privilèges affectés à User2.
- L'activité de User1 permet de maintenir la session de User2 en activité, mais la session de User1 peut s'interrompre à tout moment de façon inopinée.
- La déconnexion de l'une ou l'autre des fenêtres provoque l'arrêt des deux sessions ; l'activité suivante dans la deuxième fenêtre peut rediriger l'utilisateur sur la page d'ouverture de session, comme dans le cas d'un délai de session ou d'un délai prématuré.
- Si vous cliquez sur le lien Log Out (Déconnexion) à partir de la seconde session (User2), cela entraîne la déconnexion : `unknown page to display before redirecting the user to the login page.`
- Si User2 se déconnecte puis se reconnecte à nouveau en tant que User3, User1 prend en charge la session de User3.
- Si User1 est en cours de connexion et User2 est déjà connecté, User1 peut changer d'URL pour être redirigé sur la page d'index. Il apparaîtra alors que User1 a accédé à iLO sans s'y connecter.

Ces comportements dureront tant que les fenêtres dupliquées resteront ouvertes. Toutes les activités sont attribuées au même utilisateur, en utilisant l'ensemble de cookies de la dernière session.

Affichage du cookie de session actuel

Une fois connecté, vous pouvez obliger le navigateur à afficher le cookie de session actuel en entrant `javascript:alert(document.cookie)` dans la barre de navigation de l'URL. Le premier champ visible est l'ID de session. Si l'ID de session est le même pour les différentes fenêtres du navigateur, ces dernières partagent une session iLO commune.

Vous pouvez forcer le navigateur à actualiser et à révéler votre véritable identité en appuyant sur la touche **F5**, en sélectionnant **View>Refresh** (Affichage>Actualiser) ou en utilisant le bouton d'actualisation.

Prévention des problèmes utilisateur liés aux cookies

Pour éviter les problèmes de comportement basés sur les cookies :

- Lancez un nouveau navigateur pour chaque ouverture de session en double-cliquant sur l'icône du navigateur ou son raccourci.
- Cliquez sur le lien **Log Out** (Déconnexion) pour fermer la session iLO avant de fermer la fenêtre du navigateur.

Comment accéder aux anciennes pages BL p-Class ?

Les pages BL p-Class précédentes sont directement accessibles aux adresses URL suivantes : ces URL sont accessibles uniquement à partir d'une session iLO. Pour accéder aux pages BL p-Class, reportez-vous aux pages suivantes :

- Topologie du rack : https://<adresse réseau iLO>/dtopo.htm
- Supervision de la lame de serveur : https://<adresse réseau iLO>/dservmm.htm
- Module de supervision de l'alimentation : https://<adresse réseau iLO>/dpwrmm.htm
- Module de supervision de l'alimentation redondante : https://<adresse réseau iLO>/dpwrsmm.htm

Option ProLiant Power Regulator (Régulateur d'alimentation) désactivée

Le processeur système détermine si l'option Power Regulator (Régulateur d'alimentation) est prise en charge. Elle est disponible sur les serveurs suivants uniquement :

- ProLiant ML350 G4
- ProLiant ML350 G4p
- ProLiant ML320 G3
- ProLiant DL360 G4
- ProLiant DL360 G4p
- ProLiant DL380 G4
- ProLiant DL380 G4p
- ProLiant BL20p G3
- ProLiant ML570 G3
- ProLiant DL580 G3

La révision du micrologiciel de la ROM système doit être datée au minimum du 01/06/05. Si votre processeur système ne prend pas en charge l'option de régulation de l'alimentation (différents p-states de processeur), la page Power Regulator (Régulateur d'alimentation) affiche le message suivant : « `HP Power Regulator for ProLiant not supported by iLO` (Régulateur d'alimentation HP pour Proliant non pris en charge par iLO) ».

Extraction impossible des informations SNMP à partir de Insight Manager 7 ou de Systems Insight Manager

Les agents utilisés sur le serveur géré fournissent des informations SNMP à Systems Insight Manager. Pour que les agents puissent transférer les informations via iLO, les drivers de périphérique iLO doivent être installés. Reportez-vous à la section « Installation des drivers de périphérique iLO » (page 19) pour obtenir les instructions d'installation.

Si vous avez installé les drivers et les agents pour iLO, vérifiez que iLO et le PC de supervision se trouvent sur le même sous-réseau. Vous pouvez effectuer cette vérification rapidement en testant (ping) iLO depuis le PC de supervision. Consultez votre administrateur réseau pour connaître les chemins d'accès à l'interface réseau de iLO.

Heure ou date incorrecte des entrées dans le journal d'événements

Vous pouvez mettre à jour la date et l'heure sur iLO en exécutant l'utilitaire RBSU. Celui-ci configure automatiquement l'heure et la date du processeur en fonction de l'heure et de la date du serveur. Ces données sont également mises à jour par les agents Insight Management sur les systèmes d'exploitation réseau pris en charge.

Mise à niveau impossible du microprogramme iLO

Si vous essayez de mettre à niveau le microprogramme iLO et que celui-ci ne répond pas, n'accepte pas la mise à niveau ou s'arrête avant la fin de la mise à niveau, vous pouvez choisir entre les options suivantes :

- Récupération de iLO par flashage réseau
- ROMPaq

Récupération de iLO par flashage réseau

La puissance de ce processus permet d'effectuer la récupération à partir de l'échec d'une mise à niveau du microprogramme. La récupération par flashage utilise le FTP, accessible uniquement lorsque la récupération est active, pour transférer l'image du microprogramme vers iLO. La récupération par flashage ne doit être utilisée que dans l'un des cas suivants :

- Les tentatives précédentes de mise à niveau du microprogramme ont échoué.
- Vous ne parvenez pas à vous connecter au navigateur Web.
- Aucune autre option de mise à niveau du microprogramme n'est disponible. Les serveurs équipés d'une unité de disquette peuvent utiliser l'option ROMPaq. Les serveurs ProLiant BL p-Class, par contre, doivent utiliser la récupération par flashage.

Si l'image du microprogramme iLO est endommagée, absente ou altérée de toute autre façon, le processus de récupération par flashage de iLO permet de reflasher iLO. La récupération par flashage a pour seul objectif de reflasher le système. Aucun autre processus ne peut être exécuté tant que la récupération n'est pas terminée.

Étapes de diagnostic

Avant de tenter une récupération par flashage du microprogramme, vérifiez-en la nécessité à l'aide des étapes de diagnostic suivantes :

1. Essayez de vous connecter à iLO par l'intermédiaire du navigateur Web. Si vous n'y parvenez pas, cela signifie qu'il y a un problème de communication.
2. Essayez de tester (ping) iLO. Si vous y parvenez, cela signifie que le réseau fonctionne.
3. Essayez d'ouvrir une session FTP avec l'adresse IP ou le nom DNS de iLO. Si vous y parvenez, cela signifie que la récupération par flashage est active et que vous devez l'utiliser pour mettre le microprogramme à niveau.
4. Si vous ne parvenez pas à ouvrir une session FTP, cela signifie que le système n'est pas en mode de récupération. Tentez de réinitialiser iLO en suivant les étapes décrites à la section « Réinitialisation de iLO » (page 212).

Processus de récupération par flashage

Si les étapes de diagnostic ont confirmé la nécessité de lancer une récupération par flashage :

1. Ouvrez une session FTP avec l'adresse IP ou le nom DNS de iLO.
2. Connectez-vous à iLO en utilisant le nom d'utilisateur fixe `flash` et le mot de passe `recovery`. Le nom d'utilisateur et le mot de passe sont sensibles à la casse.
3. Lorsque l'invite FTP apparaît, entrez la commande « `put` » et le nom de fichier de l'image du microprogramme.

Exemple d'entrées utilisées avec le processus de récupération par flashage :

```
ftp 192.168.177.142
   login: flash
   password: recovery
   put \iLO160.bin
```

- Si le fichier est trouvé, la commande « put » transfère le fichier vers iLO, l'image est validée et le processus de flashage commence.
- Si le fichier n'est pas trouvé, certaines versions de la commande « put » ne signalent pas la présence d'un message d'erreur.
- Si le chemin du répertoire comprend des espaces, placez le nom du chemin et du fichier entre guillemets.

Après le transfert de l'image du microprogramme, le processus de récupération calcule le total de contrôle, valide la signature numérique et indique si l'image est valide. La reprogrammation par flashage démarre si l'image est correcte. La progression du flashage est alors signalée au client.

REMARQUE : le décryptage de la valeur de hachage enregistrée et le calcul d'une valeur de hachage par le processus de récupération de l'image avec laquelle effectuer la comparaison ne durent que quelques secondes. Si l'image est valide, le serveur FTP commence à la programmer dans le flash et à mettre les états à jour.

Une fois le processus terminé, le module de récupération par flashage se déconnecte et réamorce le processeur iLO. Si la récupération par flashage échoue, faites un nouvel essai en recherchant les éventuelles erreurs pendant la progression du processus. Il peut s'avérer nécessaire d'utiliser une autre image du microprogramme pour le processus.

ROMPaq

La mise à niveau du microprogramme iLO avec le ROMPaq implique une double procédure : la première peut être exécutée sur n'importe quel serveur, tandis que la seconde doit l'être sur le serveur hôte iLO.

Exécutez la procédure suivante sur n'importe quel serveur :

1. Téléchargez le dernier microprogramme SoftPaq de iLO. Sélectionnez l'image SoftPaq utilisée pour les disquettes et enregistrez-la sur le disque dur. Cet utilitaire est téléchargeable sur le site Web HP (http://www.hp.com/servers/lights-out).
2. Exécutez le SoftPaq pour créer des disquettes.

Exécutez la procédure suivante sur le serveur hôte iLO uniquement :

1. Amorcez le système à partir de la disquette ROMPaq.
2. Appuyez sur la touche **Entrée** dans l'écran d'accueil ROMPaq. Un écran affiche les périphériques de votre serveur qui peuvent être mis à niveau.
3. À l'aide des curseurs, sélectionnez **iLO Management** (Supervision de iLO), puis appuyez sur la touche **Entrée**. Un écran affiche les images de microprogramme que le ROMPaq peut installer.
4. À l'aide des curseurs, mettez en surbrillance l'image appropriée, puis appuyez sur la touche **Entrée**.
5. Appuyez de nouveau sur la touche **Entrée**. Le ROMPaq lit l'image du microprogramme. Si le système vous demande d'entrer d'autres disquettes, insérez-les et appuyez sur la touche **Entrée**.
6. Appuyez de nouveau sur la touche **Entrée** pour lancer la reprogrammation de la ROM. Évitez d'effectuer un cycle de mise sous tension, de réamorcer ou de mettre hors tension votre système pendant le déroulement de cette procédure.

7. Après réception d'un message indiquant que la programmation par flashage s'est terminée avec succès, appuyez sur la touche **Entrée**.
8. Appuyez sur la touche **Entrée** pour reprogrammer un autre périphérique ou sur la touche **Echap** pour revenir à l'invite A:\.

Il peut s'avérer nécessaire de configurer le commutateur de neutralisation de la sécurité pour pouvoir effectuer la mise à niveau avec le ROMPaq. Si c'est le cas, le programme ROMPaq vous en informe.

Si vous ne parvenez toujours pas à résoudre le problème :

1. Mettez le serveur hors tension et retirez la pile système.
2. Patientez quelques minutes.
3. Remplacez la pile et remettez le serveur sous tension.

Cette opération peut réinitialiser iLO à ses paramètres par défaut.

Changements d'adresse IP statique du boîtier non pris en compte

Les conditions suivantes doivent être remplies pour qu'un serveur en lame utilise automatiquement l'adresse IP statique du boîtier :

1. L'enregistrement de l'adresse IP statique de boîtier doit contenir une plage IP valide.
2. L'enregistrement de l'adresse IP statique du boîtier doit avoir un compartiment identifié comme étant celui participant à l'adresse statique.

Cet enregistrement n'aura pas de plage IP valide pour les nouveaux boîtiers. Si vous connectez les serveurs à ce boîtier avant de configurer l'enregistrement de l'adresse IP statique, cela forcera tous les serveurs lame à utiliser le paramétrage par défaut DHCP. Si c'est le cas et que vous voulez utiliser l'adresse IP statique du boîtier, vous devez d'abord configurer l'enregistrement sur le premier serveur lame. Après avoir configuré l'enregistrement, vous devez vous connecter à tous les autres serveurs lame et modifier les paramètres réseau pour pouvoir utiliser l'adresse IP statique. Vous pouvez utiliser l'interface ou un script XML. Pour configurer plus facilement chaque serveur lame, il suffit d'utiliser le chariot frontal pour se connecter à chaque serveur lame et d'effectuer les modifications sur le réseau.

Pour superviser le réseau iLO à l'aide de l'adresse IP statique du boîtier :

1. Connectez un serveur lame dans le premier emplacement du boîtier, en laissant le reste du boîtier vide.
2. Connectez-vous à ce serveur lame via le chariot frontal. L'adresse IP par défaut est 192.168.1.1.
3. Configurez l'adresse IP statique à l'aide de l'assistant d'installation du serveur lame ou grâce à l'onglet d'installation de l'adresse IP statique du boîtier.
4. Enregistrez les paramètres.

Une fois que tous les paramètres sont enregistrés, tous les autres serveurs lame peuvent être insérés dans le boîtier.

N'insérez pas d'autres serveurs lame dans le boîtier tant que l'enregistrement de l'adresse IP statique du boîtier n'a pas été sauvegardé. Une fois que les autres serveurs lame sont insérés, iLO initialise son réseau sur l'adresse indiquée dans l'enregistrement de l'adresse IP statique du boîtier, en supposant que :

- Le nouveau serveur lame est livré directement sans alimentation auxiliaire ;
- Le nouveau serveur lame utilisait précédemment l'adresse IP statique du boîtier et a été déplacé vers Le nouveau boîtier où l'adresse IP a été configurée.

Si l'une de ces instructions est fausse, le réseau iLO ne peut pas utiliser l'adresse IP attendue par le client et identifiée dans l'enregistrement de l'adresse IP statique.

iLO ne répond pas aux requêtes SSL

iLO ne répond pas aux requêtes SSL lorsqu'un avertissement Java™ s'affiche. Si un utilisateur se connecte à une connexion du navigateur iLO et interrompt le processus de connexion en répondant à l'avertissement de certificat Java, iLO ne répond pas aux requêtes ultérieures du navigateur. L'utilisateur doit poursuivre le processus de connexion pour libérer le serveur Web iLO.

Test de SSL

Le test suivant vérifie que l'invite de la boîte de dialogue de sécurité est correcte. Si le serveur ne fonctionne pas, le message « `Page cannot be displayed` » (affichage impossible d'une page) s'affiche. En cas d'échec du test, votre contrôleur de domaine n'accepte pas les connexions SSL et n'a probablement pas reçu de certificat.

1. Ouvrez un navigateur et naviguez vers <https://*<contrôleur de domaine>*:636.

   Vous pouvez indiquez *<domaine>* au lieu de *<contrôleur de domaine>* qui accède au serveur DNS et vérifie quel contrôleur gère les requêtes du domaine. Testez plusieurs contrôleurs de domaine afin de vérifier qu'ils ont tous reçu un certificat.
2. Si SSL fonctionne correctement sur le contrôleur de domaine (un certificat est émis), un message de sécurité s'affiche vous demandant si vous souhaitez toujours accéder au site, ou afficher le certificat du serveur. Le fait de cliquer sur **Yes** (Oui) ne permet pas d'afficher une page Web. C'est normal. Ce processus est automatique, mais peut nécessiter un redémarrage. Pour éviter d'avoir à le redémarrer :
   a. Ouvrez MMC et ajoutez le composant logiciel intégrable des certificats. À l'invite, sélectionnez **Computer Account** (Compte ordinateur) ou le type des certificats à afficher. Cliquez sur **OK** pour retourner au composant logiciel intégrable des certificats.
   b. Sélectionnez le dossier **Personal>Certificates** (Personnel>Certificats). Cliquez avec le bouton droit sur le dossier et sélectionnez **Request New Certificate** (Demander nouveau certificat).
   c. Vérifiez que Type contient le contrôleur de domaine et cliquez sur **Next** (Suivant) jusqu'à ce qu'un certificat soit utilisé.

Vous pouvez également utiliser l'outil Microsoft® LDP pour vérifier les connexions SSL. Pour plus d'informations sur l'outil LDP, consultez le site Web Microsoft® (http://www.microsoft.com/support).

Un ancien certificat peut poser les mêmes problèmes que SSL sur le pointage du contrôleur de domaine lorsqu'il pointe vers une autorité de certification agréée portant le même nom. Ce cas est rare mais peut se produire si un service de certificat est ajouté et supprimé, puis à nouveau ajouté sur le contrôleur de domaine. Pour supprimer les anciens certificats et en émettre un autre, suivez les instructions données à l'étape 2.

Réinitialisation de iLO

Dans certains cas, rares, il peut s'avérer nécessaire de réinitialiser iLO, notamment lorsqu'il ne répond pas au navigateur. Pour réinitialiser iLO, vous devez mettre le serveur hors tension et déconnecter complètement les blocs d'alimentation.

Dans certains cas, il peut arriver que iLO se réinitialise de lui-même. Par exemple, une horloge de surveillance iLO interne se réinitialise si le microprogramme détecte un problème lié à iLO. iLO se réinitialise aussi après une mise à niveau du microprogramme ou une modification des paramètres réseau.

Les agents de supervision HP version 5.40 et ultérieures sont aussi en mesure de réinitialiser iLO. Pour réinitialiser iLO, utilisez l'option **Reset** (Réinitialiser iLO) de la page Web **HP Management Agent** (Agents de supervision HP), dans la section **iLO**.

Vous pouvez aussi forcer manuellement la réinitialisation du processeur de supervision de iLO en cliquant sur **Apply** (Appliquer) dans la page Network Settings (Paramètres réseau). Il n'est pas nécessaire de modifier des paramètres avant de cliquer sur Apply (Appliquer).

La fonction Rack View (Afficher rack) ne permet pas d'afficher les composants

Si le message d'erreur : `Unable to collect rack data` (impossible de rassembler les données de rack) continue à s'afficher, il est préférable de mettre à jour votre microprogramme dans le boîtier de supervision avec la version 2.10 ou supérieure.

L'écran Rack View (Afficher rack) n'affichera aucun composant dans les situations suivantes :

1. Plusieurs serveurs lame tentent d'afficher ou de réactualiser la page Rack View (Afficher rack) en même temps. Patientez un peu, puis recommencez ultérieurement. Un seul serveur lame peut charger la page Rack View (Afficher rack) simultanément.
2. Les modules SMM ou PMM doivent avoir la version 2.10 ou ultérieure de microprogramme. Le dernier microprogramme est accessible sur le site Web HP (http://h18000.www1.hp.com/support/files/server/us/download/21000.html).
3. Les modules SMM et PMM sont mal reliés. Pour obtenir des instructions de câblage, reportez-vous à la documentation des boîtiers P-Class.

Le nom du serveur est encore présent après l'exécution de l'utilitaire ERASE

Le champ Server Name (Nom du serveur) est communiqué à iLO par les agents Insight Manager. Pour modifier le champ Server Name (Nom du serveur) après un redéploiement de serveur, chargez les agents Insight Manager pour mettre à jour ce champ avec le nom du nouveau serveur.

Pour supprimer le champ Server Name (Nom du serveur) après le redéploiement d'un serveur, utilisez la fonctionnalité Reset to Factory Defaults (Réinitialisation aux valeurs d'usine par défaut) de l'utilitaire iLO RBSU pour effacer la valeur dans le champ Server Name.

Cette procédure efface toutes les informations de configuration iLO et non seulement les informations relatives au nom du serveur.

Résolution des problèmes d'un hôte distant

Pour résoudre les problèmes d'un serveur hôte distant, il peut s'avérer nécessaire de redémarrer le système distant. Pour ce faire, utilisez les options de l'onglet Virtual Devices (Périphériques virtuels).

Schéma des services d'annuaire

Cette section traite des rubriques suivantes :

Classes et attributs d'identificateurs d'objets (OID) LDAP centraux dans HP Management

Les modifications apportées au schéma lors de sa configuration portent sur deux types d'éléments :

- Classes centrales (page 214)
- Attributs centraux (page 214)

Classes centrales

Nom de classe	OID affecté
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Attributs centraux

Nom d'attribut	OID affecté
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Définitions des classes centrales

Les classes centrales de supervision HP sont définies comme suit :

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1
Description	Cette classe définit les objets cibles (Target), qui constituent la base des produits HP faisant appel à la supervision activée via l'annuaire.
Type de classe	Structurel
SuperClasses	Utilisateur
Attributs	hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership—1.3.6.1.4.1.232.1001.1.1.2.2
Commentaires	Aucun

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Description	Cette classe définit les objets de rôle (Role), qui constituent la base des produits HP faisant appel à la supervision activée via l'annuaire.
Type de classe	Structurel
SuperClasses	Groupe
Attributs	hpqRoleIPRestrictions—1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault—1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction—1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership—1.3.6.1.4.1.232.1001.1.1.2.3
Commentaires	Aucun

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Description	Cette classe définit les objets de stratégie (Policy), qui constituent la base des produits HP faisant appel à la supervision activée via l'annuaire.
Type de classe	Structurel
SuperClasses	Supérieure
Attributs	hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1
Commentaires	Aucun

Définitions des attributs centraux

Les attributs de classe centraux de supervision HP sont définis comme suit :

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
Description	Nom distinctif de la stratégie contrôlant la configuration générale de cette cible.
Syntaxe	Nom distinctif—1.3.6.1.4.1.1466.115.121.1.12
Options	Valeur unique
Commentaires	Aucun

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Description	Fournit la liste d'objets cibles hpq à laquelle appartient cet objet.
Syntaxe	Nom distinctif—1.3.6.1.4.1.1466.115.121.1.12
Options	Valeur multiple
Commentaires	Aucun

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Description	Fournit la liste d'objets cibles hpq appartenant à cet objet.
Syntaxe	Nom distinctif—1.3.6.1.4.1.1466.115.121.1.12
Options	Valeur multiple
Commentaires	Aucun

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	Chaîne booléenne représentant l'accès par des clients non spécifiés, qui indique partiellement des restrictions de privilèges sous une contrainte d'adresse réseau IP.
Syntaxe	Booléen — 1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Si cet attribut est spécifié sur la valeur TRUE, les restrictions IP seront satisfaites pour les clients réseau non exceptionnels. Si cet attribut est spécifié sur la valeur FALSE, les restrictions IP seront insatisfaites pour les clients réseau non exceptionnels.

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Description	Fournit une liste d'adresses IP, de noms DNS, de domaines, de plages d'adresses et de sous-réseaux qui spécifient de façon partielle des restrictions de privilèges sous une contrainte d'adresse réseau IP.
Syntaxe	Chaîne d'octets—1.3.6.1.4.1.1466.115.121.1.40
Options	Valeur multiple
Commentaires	Cet attribut est utilisé uniquement sur les objets de rôles. Les restrictions IP sont satisfaites lorsque l'adresse correspond et l'accès général est refusé, et insatisfaites lorsque l'adresse correspond et l'accès général est accordé. Les valeurs prennent la forme d'un octet d'identification suivi par un nombre d'octets de type spécifique, qui indiquent une adresse réseau. • Pour les sous-réseaux IP, l'identificateur est <0x01>, suivi de l'adresse réseau IP par ordre de réseau, elle-même suivie du masque de sous-réseau IP par ordre de réseau. Par exemple, le sous-réseau IP 127.0.0.1/255.0.0.0 serait représenté sous la forme <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. Pour les plages IP, l'identificateur est <0x02>, suivi par l'adresse IP supérieure liée, suivie par l'adresse IP inférieure liée. Toutes deux sont inclusives et par ordre de réseau. Par exemple, la plage IP 10.0.0.1 to 10.0.10.255 serait représentée comme <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>. • Pour les noms ou les domaines DNS, l'identificateur est <0x03>, suivi par le nom DNS en code ASCII. Les noms DNS peuvent être préfixés avec * (ASCII 0x2A), pour indiquer qu'ils doivent correspondre à tous les noms se terminant par la chaîne spécifiée. Par exemple, le domaine DNS *.acme.com est représenté sous la forme <0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. L'accès général est accordé.

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Description	Grille de temps de sept jours, avec une résolution de 30 minutes, qui spécifie les restrictions de privilège sous une contrainte de temps.
Syntaxe	Chaîne d'octets {42}—1.3.6.1.4.1.1466.115.121.1.40
Options	Valeur unique

Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Les restrictions de temps sont satisfaites lorsque le bit correspondant au temps local réel du périphérique est 1 et insatisfaites lorsque le bit est 0. • Le bit le moins significatif du premier octet correspond à dimanche, de minuit (00:00) à dimanche, 12:30. • Le bit suivant le plus significatif et son octet séquentiel correspondent aux blocs de demi-heure consécutifs suivants dans une même semaine. • Le bit le plus significatif, le 8ème du 42ème octet correspond à la période commençant le samedi à 22:30 jusqu'à dimanche à minuit (00:00).

Classes et attributs d'identificateurs d'objets (OID) LDAP spécifiques de la supervision Lights-Out

Le schéma suivant des attributs et des classes peut dépendre des attributs ou des classes définis dans les attributs et classes centraux de supervision HP.

Classes de supervision Lights-Out

Nom de classe	OID affecté
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Attributs de supervision Lights-Out

Nom de classe	OID affecté
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.1
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.6

Définitions des classes de supervision Lights-Out

Les classes centrales de supervision Lights-Out sont définies comme suit :

hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Description	Cette classe définie les privilèges et les paramètres utilisés dans les produits HP Lights-Out Management.
Type de classe	Auxiliaire
SuperClasses	Aucun
Attributs	hpqLOMRightConfigureSettings : 1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin : 1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin : 1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole : 1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset : 1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia : 1.3.6.1.4.1.232.1001.1.8.2.6
Commentaires	Aucun

Définitions des attributs de supervision Lights-Out

Les attributs centraux de supervision Lights-Out sont définis comme suit :

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Privilège de connexion pour les produits HP Lights-Out Management.
Syntaxe	Booléen : 1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Significatif uniquement pour les objets ROLE. Lorsque le paramétrage est spécifié sur TRUE, le privilège est accordé aux membres du rôle.

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Privilège de la console distante pour les produits de supervision Lights-Out. Significatif uniquement pour les objets ROLE.
Syntaxe	Booléen : 1.3.6.1.4.1.1466.115.121.1.7

Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Description	Privilège du support virtuel pour les produits HP Lights-Out Management.
Syntaxe	Booléen : 1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Description	Privilège de réinitialisation du serveur distant et privilège du bouton d'alimentation pour les produits HP Lights-Out Management.
Syntaxe	Booléen : 1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Privilège administratif des bases de données de l'utilisateur local pour les produits HP Lights-Out Management.
Syntaxe	Booléen : 1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Privilège de configuration des paramètres de périphérique pour les produits HP Lights-Out Management.
Syntaxe	Booléen : 1.3.6.1.4.1.1466.115.121.1.7
Options	Valeur unique
Commentaires	Cet attribut est utilisé uniquement sur les objets ROLE. Si l'attribut est spécifié sur TRUE, le privilège sera accordé aux membres du rôle.

Assistance technique

Cette section traite des rubriques suivantes :

Contacter HP

Pour obtenir le nom du Revendeur Agréé HP le plus proche :

- Aux États-Unis, consultez la page Web de recherche de service HP US (http://www.hp.com/service_locator).
- Dans les autres pays, visitez la page Web de contacts dans le monde (en anglais) (http://welcome.hp.com/country/us/en/wwcontact.html).

Assistance technique HP :

- Aux États-Unis, pour connaître les options de contact, consultez la page Web de contacts HP (http://welcome.hp.com/country/us/en/contact_us.html). Pour contacter HP par téléphone :
  - Appelez le 1-800-HP-INVENT (1-800-474-6836). Ce service est disponible 24 h/24 et 7 j/7. Vos appels peuvent faire l'objet d'un enregistrement ou d'un contrôle, et ce dans le but d'améliorer en permanence la qualité du service.
  - Si vous avez acheté un Care Pack (mise à jour de service), composez le 1-800-633-3600. Pour plus d'informations sur les Care Packs, connectez-vous au site Web HP (http://www.hp.com).
- Dans les autres pays, visitez la page Web de contacts dans le monde (en anglais) (http://welcome.hp.com/country/us/en/wwcontact.html).

Avant de contacter HP

Avant d'appeler HP, munissez-vous des informations suivantes :

- Numéro d'enregistrement auprès de l'assistance technique (le cas échéant)
- Numéro de série du produit
- Nom et numéro du modèle de produit
- Messages d'erreur obtenus, le cas échéant
- Cartes ou matériels complémentaires
- Matériel ou logiciel de fabricants tiers
- Type et niveau de version du système d'exploitation

Acronymes et abréviations

ACPI

Advanced Configuration and Power Interface (Interface avancée de configuration et de courant électrique)

ARP

Address Resolution Protocol (Protocole de résolution d'adresse)

ASCII

American Standard Code for Information Interchange (Code américain normalisé pour l'échange d'information)

ASM

Advanced Server Management (Supervision avancée de serveur)

ASR

Automatic Server Recovery (Récupération automatique du serveur)

CA

Certificate authority (Autorité de certification)

CGI

Common Gateway Interface (Interface de passerelle commune)

CLI

Interface de ligne de commande

CLP

Command line protocol (Protocole de ligne de commande)

CR

Certificate Request (Demande de certificat)

CRL

Certificate revocation list (Liste des révocations de certificat)

DAV

Distributed Authoring and Versioning (Système d'auteur et de contrôle des versions distribué)

DDNS

Dynamic Domain Name System (Système de noms de domaine dynamique)

DHCP

Dynamic Host Configuration Protocol (protocole de configuration de serveur dynamique)

DLL

Dynamic link library (Bibliothèque de liens dynamiques)

DMTF

Distributed Management Task Force (Groupe de travail sur la gestion répartie)

DNS

Domain Name System (Système de noms de domaine)

DSA

Digital Signature Algorithm (Algorithme de signature numérique)

EMS

Emergency Management Services (Services de gestion d'urgence)

EULA

End user license agreement (Contrat de licence utilisateur final ou CLUF)

FEH

Fatal Exception Handler (Gestionnaire d'exceptions fatales)

GUI

Graphical User Interface (Interface utilisateur graphique)

HB

Heartbeat (Message persistant)

HPONCFG

HP Lights-Out Online Configuration (Utilitaire de configuration en ligne HPONCFG)

HPQLOMGC

HP Lights-Out Migration Command Line (Utilitaire HP de ligne de commande de migration Lights-Out)

HPQLOMIG

HP Lights-Out Migration (Utilitaire HP de migration Lights-Out)

ICMP

ICMP (Protocole de message de commande Internet)

iLO

Integrated Lights-Out

IML

Integrated Management Log (journal de maintenance intégré)

IP

Internet Protocol (Protocole Internet)

ISIP

IP fixe du boîtier

JVM

Java Virtual Machine (Machine virtuelle Java)

LAN

Réseau local

LDAP

Lightweight Directory Access Protocol

LED

Light Emitting Diode (Diode émettant de la lumière)

LOM

Lights-Out Management (Supervision Lights-Out)

LSB

Least Significant Bit (Bit le moins significatif)

MAC (MAC)

Medium Access Control

MLA

Master License Agreement (Accord de licence principal)

MMC

Microsoft® Management Console

MP

Multilink Point-to-Point Protocol (Protocole point à point multilien)

MTU

Maximum Transmission Unit (Unité de transmission maximale)

NIC

Network Interface Controller (Carte réseau)

NMI

Non-Maskable Interrupt (Interruption non masquable)

NVRAM

Mémoire non volatile

PERL

Practical Extraction and Report Language (Langage PERL)

PKCS

Public-Key Cryptography Standards (Normes de cryptographie à clé publique)

POST

Power-On Self-Test (auto-test de mise sous tension)

PSP

ProLiant Support Pack (Pack de support Proliant)

RAS

Remote Access Service (Service d'accès distant)

RBSU

ROM-Based Setup Utility (Utilitaire de configuration basé sur la mémoire morte)

RDP

Remote Desktop Protocol (Protocole de bureau à distance)

RIB

Remote Insight Board (Carte Remote Insight)

RIBCL

Remote Insight Board Command Language (Langage de commande de la carte Remote Insight)

RILOE

Remote Insight Lights-Out Edition

RILOE II

Remote Insight Lights-Out Edition II

RSA

Clé de codage public Rivest, Shamir et Adelman

RSM

Remote Server Management (Supervision des serveurs à distance)

SLES

SUSE LINUX Enterprise Server

SMASH

System Management Architecture for Server Hardware (Architecture de la supervision du système pour le matériel du serveur)

SNMP

Simple Network Management Protocol (Protocole simple de gestion de réseau)

SSH

Secure Shell

SSL

Secure Sockets Layer

TCP

Transmission Control Protocol (Protocole de contrôle de transmission)

UART

Universal asynchronous receiver-transmitter (Transmetteur récepteur asynchrone universel)

UID

Unit Identification (Identification d'unité)

USB

Universal Serial Bus (Bus série universel)

VLAN

Virtual local-area network (Réseau local virtuel)

VM

Virtual Machine (Machine virtuelle)

VPN

Virtual Private Networking (Réseau privé virtuel)

WINS

Acronyme de Windows® Internet Naming Service

XML

eXtensible Markup Language (Langage de balisage extensible)

Index

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

X