# Oracle® Integrated Lights Out Manager (ILOM) 3.0

## Guide de démarrage

Référence 820-7381-11
Novembre 2010, Révision A

Copyright © 2008, 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA,
Inc., 500 Oracle Parkway, Redwood City, CA 94065 États-Unis.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

---

Copyright © 2008, 2010, Oracle et/ou ses sociétés affiliées. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des États-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des États-Unis, la notice suivante s'applique :

DROITS DU GOUVERNEMENT DES ÉTATS-UNIS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés.Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.

Veuillez
recycler

# Contenu

# Utilisation de cette documentation

Ce Guide de démarrage explique comment réaliser les procédures requises pour accéder au microprogramme Oracle Integrated Lights Out Manager (ILOM) 3.0 pour la première fois sur votre système.

Ces procédures portent sur les aspects suivants : connexion à ILOM, connexion réseau, création de compte utilisateur, configuration du service d'annuaire et mise à niveau du microprogramme. Ce guide s'adresse aux techniciens, administrateurs système, fournisseurs de services autorisés (ASP) et aux utilisateurs ayant de l'expérience en matière de gestion de matériel système.

Pour bien comprendre les informations contenues dans ce guide, consultez en parallèle les autres guides de la collection de documentation sur Oracle Integrated Lights Out Manager (ILOM) 3.0. Pour une description des guides qui constituent la collection de documentation sur ILOM 3.0, voir la section Documentation connexe, page vi.

Cette préface couvre les sujets suivants :

# Documentation connexe

Le tableau suivant répertorie l'ensemble de la documentation sur ILOM 3.0. Vous pouvez accéder à ces guides en ligne et les télécharger à l'adresse suivante :

http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

**Remarque –** Les documents qui constituent cette collection étaient auparavant nommés guides Sun Integrated Lights Out Manager (ILOM) 3.0.

| Titre | Contenu | Numéro de référence | Format |
|---|---|---|---|
| *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0* | Informations décrivant les fonctions et fonctionnalités d'ILOM | 820-7369 | PDF<br>HTML |
| *Guide de démarrage d'Oracle Integrated Lights Out Manager (ILOM) 3.0* | Informations et procédures relatives à la connexion réseau, à la première connexion à ILOM et à la configuration d'un compte utilisateur ou d'un service d'annuaire | 820-7381 | PDF<br>HTML |
| *Guide des procédures relatives à l'interface Web d'Oracle Integrated Lights Out Manager (ILOM) 3.0* | Informations et procédures sur l'accès aux fonctions d'ILOM à l'aide de l'interface Web d'ILOM | 820-7372 | PDF<br>HTML |
| *Guide des procédures relatives à la CLI d'Oracle Integrated Lights Out Manager (ILOM) 3.0* | Informations et procédures sur l'accès aux fonctions d'ILOM à l'aide de la CLI d'ILOM | 820-7375 | PDF<br>HTML |

| Titre | Contenu | Numéro de référence | Format |
|---|---|---|---|
| *Guide de référence des protocoles de gestion d'Oracle Integrated Lights Out Manager 3.0* | Informations et procédures pour accéder aux fonctions ILOM en utilisant SNMP, IPMI ou WS-Man et CIM | 820-7378 | PDF<br>HTML |
| *Mises à jour des fonctions Oracle Integrated Lights Out Manager (ILOM) 3.0 et notes de version* | Informations de dernière minute à propos des fonctions ILOM 3.0, des problèmes connus et de leurs solutions | 821-0646 | PDF<br>HTML |
| *Oracle Integrated Lights Out Manager (ILOM) CMM - Guide d'administration pour les systèmes modulaires Sun Blade 6000 et 6048* | Informations et procédures pour accéder aux fonctions ILOM spécifiques au module de contrôle du châssis (CMM) | 821-3082 | PDF<br>HTML |

Outre la documentation sur ILOM 3.0, un Supplément ILOM ou le Guide d'administration de la plate-forme associé présente les fonctionnalités et les tâches ILOM spécifiques à la plate-forme serveur que vous utilisez. Consultez la collection de documentation sur ILOM 3.0 en parallèle avec le Supplément ILOM ou le Guide d'administration fourni avec votre plate-forme serveur.

Les versions traduites de certains de ces documents sont disponibles sur les sites Web répertoriés ci-dessus de ce tableau. Veuillez noter que la documentation anglaise est révisée plus fréquemment. Par conséquent, elle est peut-être plus à jour que la documentation traduite.

# Documentation, support et formation

Ces sites proposent des ressources supplémentaires :

- Documentation : `http://docs.sun.com`
- Support : `http://www.sun.com/support/`
- Formation : `http://www.sun.com/training/`

# Numéros de version d'ILOM 3.0

Pour vous aider à identifier la version d'ILOM exécutée sur votre système, ILOM 3.0 introduit un nouveau schéma de numérotation de version. Ce schéma de numérotation est une chaîne de caractères composée de cinq champs, par exemple `a.b.c.d.e`, où :

- `a` – représente la version principale d'ILOM.
- `b` – représente une version mineure d'ILOM.
- `c` – représente la version mise à jour d'ILOM.
- `d` – représente une version micro d'ILOM. Les versions micro sont gérées par plate-forme ou groupe de plates-formes. Pour en savoir plus, consultez les Notes de produit relatives à votre plate-forme.
- `e` – représente une version nano d'ILOM. Les versions nano sont des itérations incrémentielles d'une version micro.

Par exemple, dans ILOM 3.1.2.1.a :

- ILOM 3 est la version principale d'ILOM
- ILOM 3.1 est une version mineure d'ILOM 3
- ILOM 3.1.2 est la seconde mise à jour d'ILOM 3.1
- ILOM 3.1.2.1 est une version micro d'ILOM 3.1.2
- ILOM 3.1.2.1.a est une version nano d'ILOM 3.1.2.1

# Commentaires sur la documentation

Pour nous envoyer vos commentaires sur ce document, cliquez sur le lien Feedback[+] à l'adresse :

`http://docs.sun.com`

Veuillez mentionner le titre et le numéro de référence du document dans vos commentaires :

*Guide de démarrage d'Oracle Integrated Lights Out Manager (ILOM) 3.0*, référence 820-7381-11

CHAPITRE 1

# Démarrage d'ILOM

**Rubriques**

| Description | Liens |
|---|---|
| Savoir comment utiliser ce guide | • À propos de ce guide, page 2 |
| Passer en revue le processus de démarrage d'ILOM et les conditions requises associées, choisir une interface et planifier la configuration d'ILOM | • Processus de démarrage d'ILOM, page 2<br>• Connexion du système à ILOM, page 5 |
| Passer en revue les conditions requises pour se connecter à ILOM | • Connexion du système à ILOM, page 5<br>• Utilisation de l'interface Web ou de la CLI, page 6<br>• Utilisation du compte `root`, page 7 |

# À propos de ce guide

Le *Guide de démarrage d'Oracle ILOM 3.0* comporte des procédures de configuration simples à suivre qui vous permettront de commencer à utiliser ILOM même avant la mise sous tension du système hôte.

Avec ILOM, vous pouvez contrôler et gérer à distance votre plate-forme serveur Oracle Sun sans recourir aux ressources du système d'exploitation. ILOM fournit des interfaces dotées de fonctionnalités complètes, y compris une interface Web, une interface de ligne de commande, une interface SNMP et une interface IPMI. Ces interfaces normalisées sont très faciles à utiliser.

Les procédures de démarrage expliquent comment connecter votre système à ILOM et configurer les paramètres ILOM initiaux requis. Le guide contient également des procédures permettant de vérifier et de mettre à jour la version du microprogramme d'ILOM. Vous trouverez des descriptions plus détaillées sur les caractéristiques et fonctions d'ILOM dans les autres documents de la collection de documentation sur ILOM 3.0. Pour consulter la liste de ces documents, voir Documentation connexe, page vi.

# Processus de démarrage d'ILOM

Vous pouvez utiliser les paramètres et la configuration par défaut d'ILOM pour accéder à ses nombreuses fonctionnalités, ou vous pouvez personnaliser certains paramètres ILOM de manière à adapter ILOM à votre environnement. Avant de commencer la configuration initiale d'ILOM, déterminez la façon d'accéder à ILOM et de le configurer pour votre système et votre environnement de centre de données.

Le TABLEAU 1-1 répertorie certaines tâches à prendre en considération avant d'utiliser ILOM pour la première fois. Chacune est reprise en détail dans les procédures qui suivent.

.

**TABLEAU 1-1** Tâches de configurations initiale et générale d'ILOM

| Tâche | Informations à prendre en compte | Se reporter à cette procédure |
|---|---|---|
| **Conditions préalables requises pour se connecter à ILOM** | | |
| Connecter votre système à ILOM, choisir l'interface Web ou la CLI ILOM, puis découvrir le compte utilisateur `root` préconfiguré | Vous pouvez vous connecter à ILOM à l'aide d'une connexion Ethernet ou série.<br>À partir de la version ILOM 3.0.12, vous pouvez utiliser un environnement réseau à double pile IPv4 et IPv6.<br>Pour configurer ILOM la première fois, vous pouvez utiliser l'interface Web ou l'interface de ligne de commande (CLI).<br>Pour la connexion initiale, vous utiliserez le compte utilisateur `root` préconfiguré. | Connexion du système à ILOM, page 5<br>Utilisation de l'interface Web ou de la CLI, page 6<br>Utilisation du compte `root`, page 7<br>Voir également la documentation de votre plate-forme |
| **Première connexion à ILOM** | | |
| Se connecter à ILOM avec le compte utilisateur `root` | ILOM démarre automatiquement dès que votre plate-forme serveur Oracle Sun est mise sous tension. ILOM est préconfiguré avec le compte utilisateur `root` et son mot de passe. Vous pouvez utiliser ce compte spécial lors de la première connexion et de la configuration de compte.<br>Pour se connecter avec le compte utilisateur `root` :<br>• User name: **`root`**<br>• Password: **`changeme`** | Première connexion à ILOM à l'aide de l'interface Web, page 10<br>Première connexion à ILOM à l'aide de la CLI, page 38 |
| **Configuration d'ILOM pour l'accès au réseau** | | |
| Configurer les paramètres réseau IPv4 ou IPv6 | Vous pouvez accepter les paramètres par défaut de double pile IPv4 (DHCPv4) et IPv6 (sans état) ou modifier ces paramètres en utilisant l'interface Web ou l'interface de ligne de commande (CLI) d'ILOM.<br>Si votre réseau prend en charge uniquement IPv4, vous pouvez également modifier les paramètres IPv4 par défaut à partir du système d'exploitation hôte à l'aide de l'utilitaire BIOS ou de l'outil IPMItool. | Configuration d'un environnement réseau IPv4 et IPv6, page 12 (Web)<br>Configuration d'un environnement réseau IPv4 et IPv6, page 39 (CLI) |
| **Création de comptes utilisateur locaux ou utilisation d'un service d'annuaire**<br>**Remarque -** Vous pouvez opter pour la création d'un compte utilisateur local ou la configuration d'un service d'annuaire. | | |

**TABLEAU 1-1** Tâches de configurations initiale et générale d'ILOM *(Continued)*

| Tâche | Informations à prendre en compte | Se reporter à cette procédure |
|---|---|---|
| Ajout d'un compte utilisateur local et assignation de rôles | Après vous être connecté à ILOM, vous pouvez créer et configurer 10 comptes utilisateur locaux au maximum. | Ajout de comptes utilisateur ou configuration d'un service d'annuaire, page 15 (Web)<br>Ajout de comptes utilisateur ou configuration d'un service d'annuaire, page 45 (CLI) |
| Configuration d'ILOM pour Active Directory | Avant de pouvoir utiliser Active Directory, vous devez entrer des données de base, telles que le serveur principal, le numéro de port et le mode de certificat, ainsi que des données facultatives comme un serveur de remplacement et les niveaux d'événement et de gravité. | Configuration d'ILOM pour Active Directory, page 18 (Web)<br>Configuration d'ILOM pour Active Directory, page 46 (CLI) |
| Configuration d'ILOM pour LDAP | ILOM peut utiliser LDAP et peut faire office de client LDAP à des fins d'authentification. Pour utiliser l'authentification LDAP, vous devez créer, sur le serveur LDAP, un compte utilisateur pouvant être authentifié par ILOM ou avec lequel il puisse établir une liaison. Ainsi, le client sera autorisé à rechercher l'annuaire pertinent sur le serveur LDAP. | Configuration du serveur LDAP, page 26 (Web)<br>Configuration d'ILOM pour LDAP, page 50 (CLI) |
| Configuration d'ILOM pour LDAP /SSL | Pour configurer LDAP avec SSL (Secure Socket Layer), vous devez entrer des données de base, telles que le serveur principal, le numéro de port et le mode de certificat, ainsi que des données facultatives comme un serveur de remplacement et les niveaux d'événement et de gravité. | Configuration d'ILOM pour LDAP /SSL, page 28 (Web)<br>Configuration d'ILOM pour LDAP /SSL, page 51 (CLI) |
| Configuration d'ILOM pour RADIUS | Pour utiliser l'authentification RADIUS, vous devez d'abord définir l'adresse IP et le numéro de port du serveur RADIUS, ainsi que le secret partagé dont vous vous servez pour accéder au serveur RADIUS. | Configuration d'ILOM pour RADIUS, page 33 (Web)<br>Configuration d'ILOM pour RADIUS, page 55 (CLI) |
| **Connexion et déconnexion d'ILOM à l'aide d'un compte utilisateur d'administration** | | |
| Connexion à ILOM à l'aide d'un compte utilisateur d'administration local | Lorsque vous avez créé un compte utilisateur local ou configuré un service d'annuaire, connectez-vous à ILOM à l'aide de ce compte utilisateur d'administration local. | Se connecter à ILOM à l'aide d'un nouveau compte utilisateur, page 34 (Web)<br>Se connecter à ILOM à l'aide d'un nouveau compte utilisateur, page 56 (CLI) |

**TABLEAU 1-1** Tâches de configurations initiale et générale d'ILOM *(Continued)*

| Tâche | Informations à prendre en compte | Se reporter à cette procédure |
|---|---|---|
| Déconnexion d'ILOM | Vous pouvez vous déconnecter de votre session ILOM tout en conservant vos paramètres de configuration. | Se déconnecter d'ILOM, page 35 (Web)<br>Se déconnecter d'ILOM, page 57 (CLI) |
| **Identification de la version et du microprogramme de mise à niveau d'ILOM** | | |
| Identification de la version d'ILOM | Vous pouvez déterminer rapidement la version d'ILOM active sur le processeur de service ou le module CMM. | Identification de la version du microprogramme ILOM, page 60 |
| Mise à jour du microprogramme d'ILOM | Vous pouvez facilement mettre à jour le microprogramme d'ILOM vers la dernière version. | Mise à jour du microprogramme ILOM vers la dernière version, page 61 |

# Connexion du système à ILOM

Vous pouvez connecter votre système à ILOM sans connexion réseau à l'aide du port série, ou via un réseau en utilisant le port de gestion réseau.

Si votre infrastructure réseau utilise un pare-feu ou des ports non conformes pour des services communs, vérifiez les assignations de port réseau par défaut documentées dans le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0.*

## Conditions requises pour la connexion

À partir d'ILOM 3.0.12, de nouveaux paramètres de configuration réseau ont été ajoutés à l'interface Web et à la CLI d'ILOM pour prendre en charge la configuration d'un environnement réseau à double pile IPv4 et IPv6. Pour plus d'informations sur les réseaux à double pile IPv4 et IPv6, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0.*

Avant d'effectuer les procédures de connexion à ILOM et de configuration des paramètres réseau, vous devez vérifier que les conditions suivantes sont satisfaites.

- Planifiez la façon de paramétrer ILOM sur votre serveur pour fonctionner dans votre environnement de centre de données. Voir la section sur l'établissement de la communication avec ILOM du *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0.*

- Connectez-vous à ILOM sans connexion réseau via un port série, ou bien via le réseau. Pour vous connecter à l'aide d'une connexion série directe, raccordez un câble série entre la station de travail, le terminal ou l'émulateur de terminal et le port SER MGT du serveur, ou le port du module de contrôle de châssis (CMM) si vous utilisez un système de châssis modulaire Sun Blade. Pour vous connecter à l'aide d'une connexion réseau, raccordez un câble Ethernet au port NET MGT du serveur ou du module CMM. Pour plus d'informations, consultez la documentation de votre plate-forme.
- Déterminez la méthode de configuration des paramètres réseau. À partir d'ILOM 3.0.12, de nouveaux paramètres de double pile IPv4 et IPv6 sont fournis pour permettre à ILOM d'être parfaitement opérationnel dans les environnements réseau IPv4 et IPv6. Avant ILOM 3.0.12, les paramètres de configuration réseau pour IPv4 étaient fournis. Vous pouvez utiliser les paramètres réseau de double pile IPv4 et IPv6, les paramètres DHCP pour IPv4, ou les paramètres Stateless (Sans état) pour IPv6. Par défaut, ILOM essaie d'extraire les paramètres réseau à l'aide du protocole DHCP.
- Vérifiez que les adresses réseau sont acceptées par ILOM pour les environnements réseau IPv4 ou que les noms d'hôte et DNS sont acceptés par ILOM pour les environnements réseau IPv6.

# Utilisation de l'interface Web ou de la CLI

Vous pouvez accéder aux fonctionnalités et aux fonctions d'ILOM par le biais de l'interface Web ou de la CLI, ainsi que d'une interface SNMP ou IPMI. Vous avez le choix d'effectuer toutes les tâches ILOM dans l'interface Web ou la CLI.

Les procédures de démarrage indiquées dans ce guide sont réparties en deux chapitres. Le Chapitre 2 explique comment réaliser les tâches de configurations initiale et générale à l'aide de l'interface Web. Le Chapitre 3 explique comment réaliser ces mêmes tâches à l'aide de la CLI. Avant de configurer ILOM, choisissez l'une des interfaces et suivez les procédures correspondantes.

# Utilisation du compte `root`

ILOM 3.0 fournit un compte utilisateur `root` préconfiguré. Pour vous connecter à ILOM la première fois, vous devez utiliser le compte `root`. Les utilisateurs ayant effectué la migration de la version 2.x à la version 3.0 d'ILOM connaissent déjà le compte utilisateur `root` et savent comment se connecter par son intermédiaire.

Le compte utilisateur `root` est permanent et disponible sur toutes les interfaces (interface Web, CLI, SSH, console série et IPMI), sauf si vous choisissez de le supprimer. Le compte `root` fournit des privilèges administratifs intégrés (accès en lecture et en écriture) à toutes les fonctions, fonctionnalités et commandes d'ILOM.

Pour se connecter à ILOM avec le compte utilisateur `root` :

- User name: **`root`**
- Password: **`changeme`**

Pour bloquer tout accès non autorisé à votre système, changez le mot de passe `root` (`changeme`) sur chaque processeur de service (SP) ou module de contrôle de châssis (CMM) de votre système. Vous pouvez également supprimer le compte `root` pour sécuriser l'accès à votre système. Toutefois, avant de supprimer le compte `root`, vous devez configurer un nouveau compte utilisateur ou configurer un service d'annuaire pour pouvoir vous connecter à ILOM.

Si vous supprimez le compte `root` avant d'avoir configuré un nouveau compte utilisateur ou un service d'annuaire pour se connecter à ILOM, vous pouvez utiliser un autre compte préconfiguré, appelé `default` (compte par défaut), comme autre moyen de vous connecter, puis recréer le compte `root`. Pour plus d'informations sur le compte utilisateur `default`, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0*.

CHAPITRE 2

# Procédures de configuration initiale d'ILOM à l'aide de l'interface Web

**Rubriques**

| Description | Liens |
|---|---|
| Première connexion à ILOM | • Première connexion à ILOM à l'aide de l'interface Web, page 10 |
| Configurer l'environnement réseau | • Configuration d'un environnement réseau IPv4 et IPv6, page 12 |
| Ajouter des comptes utilisateur ou configurer un service d'annuaire | • Ajout de comptes utilisateur ou configuration d'un service d'annuaire, page 15 |
| Rechercher des informations sur les étapes de configuration d'ILOM ultérieures | • Quelles sont les étapes ultérieures ?, page 35 |

# Première connexion à ILOM à l'aide de l'interface Web

Pour vous connecter à l'interface Web d'ILOM la première fois, utilisez le compte utilisateur `root` préconfiguré avec son mot de passe par défaut `changeme`.

## ▼ Se connecter à ILOM avec le compte utilisateur `root`

Pour vous connecter à l'interface Web d'ILOM la première fois avec le compte utilisateur `root`, ouvrez un navigateur Web et procédez comme suit :

1. **Entrez `http://`*adresse ip_système* dans le navigateur Web.**

   Si ILOM fonctionne dans un environnement réseau à double pile, vous pouvez entrer l'*adresse_ip_système* en utilisant un format d'adresse IPv4 ou IPv6.

   Par exemple :

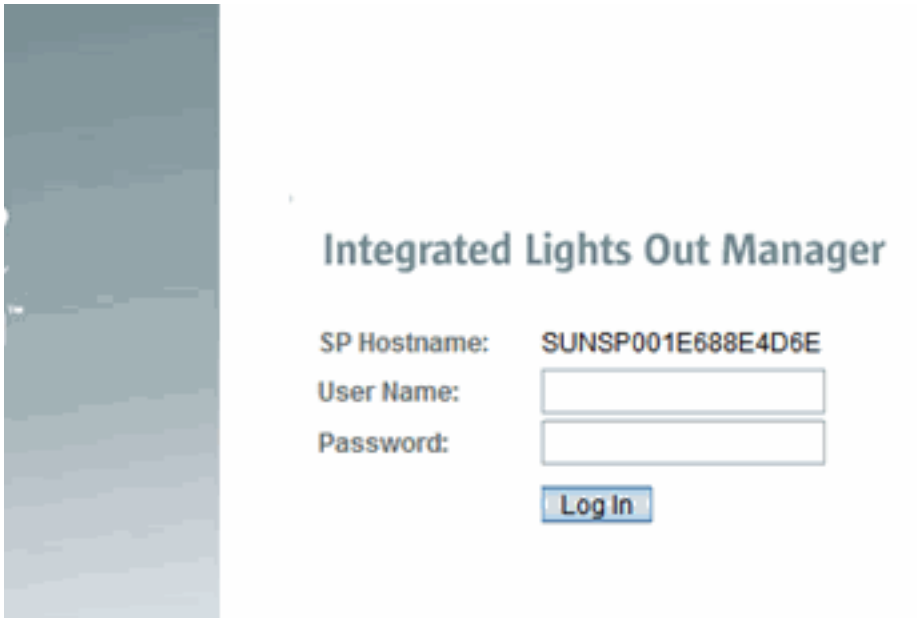
   **Pour IPv4 -** `http://10.8.183.106`

   ou

   **Pour IPv6 -** `http://[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`

   La page de connexion de l'interface Web s'affiche.

   Pour savoir comment entrer des adresses IP dans un environnement à double pile et diagnostiquer les problèmes de connexion, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0*.




2. **Entrez le nom d'utilisateur et le mot de passe du compte utilisateur** `root` **:**

   User name: **`root`**

   Password: **`changeme`**

3. **Cliquez sur Log In (Connexion).**

   La page de version de l'interface Web s'affiche.

Vous êtes maintenant prêt pour configurer les paramètres réseau et accéder à toutes les fonctions et caractéristiques d'ILOM. Pour en savoir plus sur les fonctionnalités d'ILOM et les procédures à suivre pour accéder aux fonctions d'ILOM, voir les autres documents de la collection de documentation sur ILOM 3.0. Vous pouvez accéder à la collection de documentation sur ILOM 3.0 à l'adresse suivante :

`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

# Configuration d'un environnement réseau IPv4 et IPv6

La procédure de l'interface Web suivante fournit des instructions pour configurer les versions ILOM 3.0.12 et ultérieures afin de fonctionner dans un environnement réseau à double pile IPv4 et IPv6. Pour plus d'informations sur la configuration d'ILOM dans un environnement réseau IPv4 et IPv6, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0*.

Si vous configurez ILOM pour fonctionner dans un environnement réseau IPv4 uniquement, comme le prennent en charge les versions ILOM 3.0.10 et antérieures, voir le *Guide des procédures relatives à l'interface Web d'Oracle Integrated Lights Out Manager (ILOM) 3.0*.

Par défaut, ILOM essaiera d'obtenir l'adresse IPv4 en utilisant DHCPv4 et l'adresse IPv6 en utilisant IPv6 sans état.

## ▼ Configurer les paramètres IPv4 et IPv6 en utilisant l'interface Web

1. **Connectez-vous à l'interface Web ILOM du SP ou du CMM**
2. **Accédez aux paramètres réseau IPv4 et IPv6 sur l'onglet Network (Réseau).**

   Par exemple :

   - Sur un SP de serveur, cliquez sur Configuration --> Network (Réseau).
   - Sur un CMM, procédez comme suit :
     - Sélectionnez le serveur blade (dans le volet gauche), puis dans le volet droit, cliquez sur Configuration --> Network (Réseau).
     - Dans l'onglet Network Settings (Paramètres réseau), sélectionnez le bouton radio CMM ou SP, puis cliquez sur Edit (Modifier).

---

**Remarque –** La page Network Settings (Paramètres réseau) au niveau CMM sur l'interface Web ne prend pas en charge les propriétés de double pile IPv4 et IPv6. Elle prend en charge uniquement les propriétés IPv4. Pour modifier les paramètres réseau IPv6 sur un CMM, voir Configurer les paramètres IPv4 et IPv6 en utilisant la CLI, page 39.

---

3. **Vérifiez que le paramètre réseau `State` (État) est activé.**

**Remarque –** Le paramètre réseau `State` (État) est activé par défaut aussi bien pour IPv4 que pour IPv6. Si nécessaire, vous pouvez désactiver (désélectionner) le paramètre réseau `State` (État) pour IPv6. Cependant, le paramètre réseau `State` (État) doit toujours être activé pour qu'ILOM fonctionne dans un environnement réseau IPv4 ou dans un environnement réseau à double pile IPv4 et IPv6.

4. **Effectuez les instructions de configuration réseau ci-dessous qui s'appliquent à votre environnement réseau.**
   - **Pour configurer manuellement une adresse IP statique**, voir les étapes ci-dessous pour IPv4 et/ou IPv6.
     - Étapes pour configurer manuellement une adresse IPv4 statique :

| Étapes | Description |
|---|---|
| a. | Activez le bouton radio Static IP (IP statique). |
| b. | Saisissez l'adresse IP du périphérique dans la zone de texte IP address. |
| c. | Tapez le masque de sous-réseau du réseau sur lequel le périphérique réside. |
| d. | Tapez l'adresse d'accès à la passerelle du périphérique. |

     - Étapes pour configurer manuellement une adresse IPv6 statique :

| Étape | Description |
|---|---|
| • | Saisissez l'adresse IP du périphérique dans la zone de texte IP address.<br>Les paramètres pour spécifier l'adresse IP statique et le masque de réseau pour IPv6 sont les suivants :<br>*<adresse_IPv6>*/`<longueur en bits du masque de sous-réseau>`<br>Par exemple :<br>`[fec0:a:8:b7:214:4fff:feca:5f7e/64]`<br>**Remarque -** IPv6 prend en charge l'assignation de plusieurs adresses IP pour un périphérique. Par conséquent, vous pouvez configurer manuellement une adresse IPv6 statique unique et activer une ou plusieurs options de configuration automatique IPv6 dans ILOM, si vous le souhaitez. |

   - **Pour activer l'assignation automatique par DHCP d'une adresse IPv4**, sélectionnez le bouton radio IPv4 DHCP.
   - **Pour activer une ou plusieurs options de configuration automatique IPv6**, sélectionnez les options voulues, décrites ci-dessous.

| Option de configuration automatique IPv6 | Description |
|---|---|
| `Stateless` (activée par défaut) | Si l'option de configuration automatique `Stateless` est activée, les adresses sans état IPv6 du périphérique sont détectées à partir du routeur IPv6 du réseau. |
| `DHCPv6 Stateless` | Si l'option de configuration automatique `DHCPv6 Stateless` est activée, les informations DNS du périphérique sont détectées à partir du serveur DHCPv6 du réseau.<br>**Remarque -** L'option `DHCPv6 Stateless` est disponible dans ILOM à partir de la version 3.0.14. |
| `DHCPv6 Stateful` | Si l'option de configuration automatique `DHCPv6 Stateful` est activée, les adresses IPv6 et les informations DNS du périphérique sont détectées à partir du serveur DHCPv6 du réseau.<br>**Remarque -** L'option `DHCPv6 Stateful` est disponible dans ILOM à partir de la version 3.0.14. |

**Remarque –** À partir d'ILOM 3.0.14, vous pouvez activer l'option de configuration automatique `Stateless` pour qu'elle s'exécute simultanément avec l'option `DHCPv6 Stateless`, si celle-ci est activée, ou avec l'option `DHCPv6 Stateful`, si celle-ci est activée. En revanche, les options `DHCPv6 Stateless` et `DHCPv6 Stateful` ne doivent pas être activées pour s'exécuter simultanément.

**Remarque –** Si vous activez la configuration automatique `DHCPv6 Stateful` ou `DHCPv6 Stateless`, ILOM va identifier dans la page Network Settings (Paramètres réseau) l'ID DHCP unique du serveur DHCPv6 dernièrement utilisé pour récupérer les informations DHCP.

5. **Cliquez sur `Save` (Enregistrer) pour appliquer les changements.**

   Tous les changements apportés aux paramètres réseau sont mis en attente dans la session ILOM tant que vous ne cliquez pas sur Save.

**Remarque –** Le changement de l'adresse IP statique du périphérique (SP ou CMM) va clore toutes les sessions ILOM actives vers le périphérique. Un message apparaîtra vous invitant à fermer votre session de navigateur. Vous devrez vous reconnecter à ILOM en utilisant l'adresse IP statique nouvellement assignée.

**Remarque –** Les adresses IPv6 détectées pour le périphérique par l'une quelconque des options de configuration automatique n'affecteront pas les sessions ILOM actives vers le périphérique. Vous pouvez vérifier les nouvelles adresses configurées automatiquement sur l'onglet Network (Réseau).

Pour tester la configuration réseau IPv4 ou IPv6 à partir d'ILOM, utilisez les outils de test réseau (Ping ou Ping6). Pour plus de détails, voir le *Guide des procédures relatives à l'interface Web d'Oracle Integrated Lights Out Manager (ILOM) 3.0.*

# Ajout de comptes utilisateur ou configuration d'un service d'annuaire

Une fois connecté à ILOM à l'aide du compte utilisateur `root`, vous pouvez créer un compte utilisateur local ou bien configurer un service d'annuaire. Pour plus d'informations sur les comptes utilisateur et les services d'annuaire ILOM, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0.*

**Rubriques**

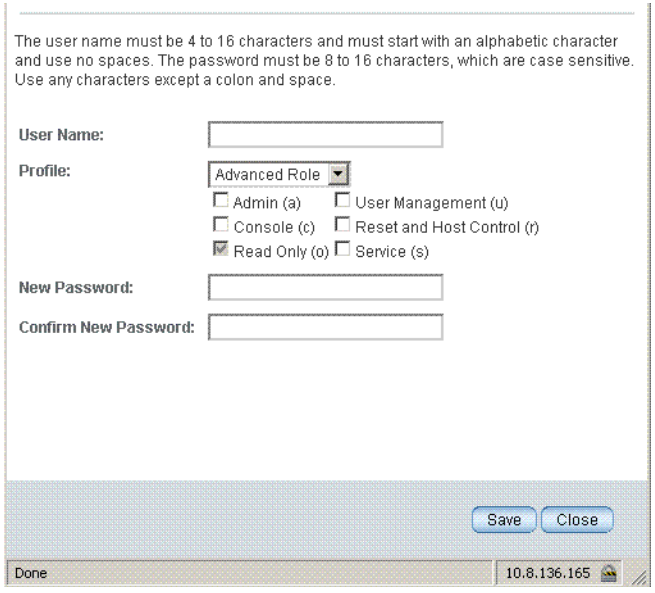
| Description | Liens |
|---|---|
| Comment ajouter un compte utilisateur et assigner des rôles utilisateur (privilèges) | • Ajout d'un compte utilisateur et assignation de privilèges, page 16 |
| Comment configurer ILOM pour Active Directory | • Configuration d'ILOM pour Active Directory, page 18 |
| Comment configurer le serveur LDAP | • Configuration du serveur LDAP, page 26 |
| Comment configurer ILOM pour LDAP | • Configuration d'ILOM pour LDAP, page 27 |
| Comment configurer ILOM pour LDAP/SSL | • Configuration d'ILOM pour LDAP /SSL, page 28 |
| Comment éditer les tables SSL | • Modification des tables LDAP/SSL, page 32 |
| Comment configurer ILOM pour RADIUS | • Configuration d'ILOM pour RADIUS, page 33 |
| Comment vérifier que le nouveau compte utilisateur ou le service d'annuaire fonctionne correctement | • Se connecter à ILOM à l'aide d'un nouveau compte utilisateur, page 34 |
| Comment se déconnecter d'ILOM | • Se déconnecter d'ILOM, page 35 |

## ▼ Ajout d’un compte utilisateur et assignation de privilèges

1. **Connectez-vous à l’interface Web d’ILOM.**
2. **Choisissez User Management (Gestion des utilisateurs) --> User Accounts (Comptes utilisateur).**

   La page User Account Settings (Paramètres des comptes utilisateur) s’affiche.
3. **Dans le tableau Users (Utilisateurs), cliquez sur Add (Ajouter).**

   La boîte de dialogue Add User (Ajout d’un utilisateur) s’affiche.




4. **Complétez les informations suivantes :**

   a. **Saisissez un nom d’utilisateur dans le champ User Name (Nom d’utilisateur).**

   b. **Choisissez un profil. Parmi les options, vous trouverez le rôle avancé** `Advanced Role` **pour toutes les nouvelles installations d’ILOM 3.0.**

**c. Sélectionnez les rôles appropriés.**

Reportez-vous au tableau suivant pour une description des rôles avancés pour les comptes utilisateur.

| Rôles | Définition | Privilèges |
|---|---|---|
| a | Admin (Administrateur) | Un utilisateur ayant le rôle d'Admin (Administrateur) (a) est autorisé à afficher et à modifier l'état des variables de configuration d'ILOM. À l'exception des tâches réservées aux utilisateurs auxquels les rôles User Management (Gestion des utilisateurs), Console et Reset and Host Control (Réinitialisation et contrôle d'hôte) sont assignés, les utilisateurs disposant du rôle Admin sont autorisés à utiliser toutes les autres fonctions d'ILOM. |
| u | User Management (Gestion des utilisateurs) | Un utilisateur ayant le rôle de User Management (Gestion des utilisateurs) (u) est autorisé à créer et à supprimer des comptes utilisateur, à modifier des mots de passe utilisateur, à modifier les rôles attribués aux autres utilisateurs, et à activer ou désactiver les spécifications d'accès physique au compte utilisateur `default`. Un utilisateur ayant ce rôle est également autorisé à installer LDAP, LDAP/SSL, RADIUS et Active Directory. |
| c | Console | Un utilisateur ayant le rôle de Console (c) est autorisé à accéder à ILOM Remote Console, ainsi qu'à la console du processeur de service et peut afficher et modifier l'état des variables de configuration d'ILOM. |
| r | Reset and Host Control (Réinitialisation et contrôle de l'hôte) | Un utilisateur ayant le rôle de Reset and Host Control (Réinitialisation et contrôle de l'hôte) (r) est autorisé à contrôler le système, et peut commander la mise sous tension, réinitialiser, effectuer des connexions à chaud, activer et désactiver des composants et gérer les pannes. Ce rôle est très semblable à celui d'un utilisateur ILOM 2.0 avec des privilèges d'opérateur. |
| o | Read Only (Lecture seule) | Un utilisateur ayant un rôle Read Only (Lecture seule) (o) est autorisé à afficher l'état des variables de configuration d'ILOM, mais il ne peut pas apporter de modifications. Un utilisateur ayant ce rôle peut également modifier le mot de passe et le paramètre du délai d'attente de session de son propre compte. |
| s | Maintenance | Un utilisateur ayant le rôle de maintenance Service (s) peut aider les techniciens de maintenance Oracle lorsqu'une intervention sur site est requise. |

**d. Entrez un mot de passe dans le champ New Password (Nouveau mot de passe).**

Le mot de passe doit comporter 8 caractères au minimum et 16 caractères au maximum. Il respecte la casse des caractères. Utilisez des lettres, des chiffres et des caractères spéciaux pour renforcer la sécurité. Tous les caractères sont autorisés, hormis les deux-points (:). N'incluez pas d'espaces dans les mots de passe.

e. **Ressaisissez le mot de passe dans le champ de confirmation.**

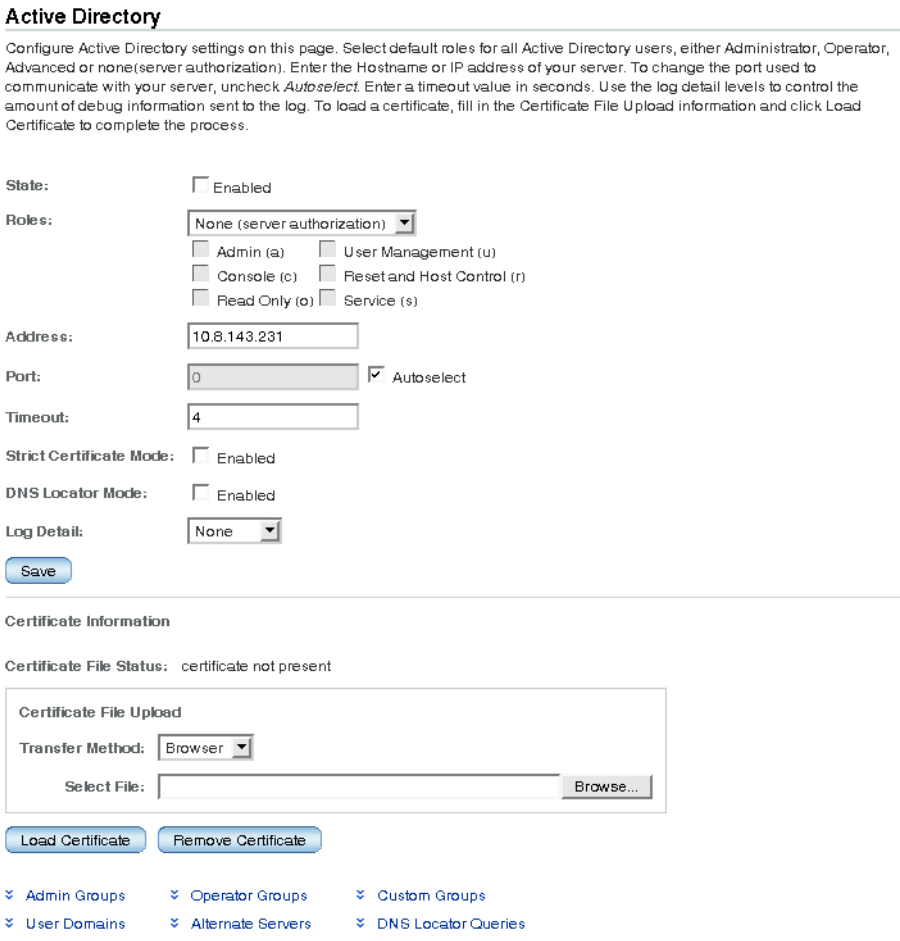
f. **Une fois les informations relatives au nouvel utilisateur fournies, cliquez sur Save (Enregistrer).**

   La page User Accounts Settings (Paramètres des comptes utilisateur) s'affiche à nouveau. Le nouveau compte utilisateur et les informations associées sont indiqués sur la page User Account Settings (Paramètres des comptes utilisateur).

## ▼ Configuration d'ILOM pour Active Directory

1. **Connectez-vous à l'interface Web d'ILOM**
2. **Choisissez User Management (Gestion des utilisateurs) --> Active Directory.**

   La page Active Directory s'affiche.


Active Directory
Configure Active Directory settings on this page. Select default roles for all Active Directory users, either Administrator, Operator, Advanced or none(server authorization). Enter the Hostname or IP address of your server. To change the port used to communicate with your server, uncheck Autoselect. Enter a timeout value in seconds. Use the log detail levels to control the amount of debug information sent to the log. To load a certificate, fill in the Certificate File Upload information and click Load Certificate to complete the process.
State:
Enabled
Roles:
None (server authorization)
Admin (a)
User Management (u)
Console (c)
Reset and Host Control (r)
Read Only (o)
Service (s)
Address:
10.8.143.231
Port:
0
Autoselect
Timeout:
4
Strict Certificate Mode:
Enabled
DNS Locator Mode:
Enabled
Log Detail:
None
Save
Certificate Information
Certificate File Status: certificate not present
Certificate File Upload
Transfer Method:
Browser
Select File:
Browse...
Load Certificate
Remove Certificate
Admin Groups
Operator Groups
Custom Groups
User Domains
Alternate Servers
DNS Locator Queries

3. **Configurez les paramètres Active Directory.**

   Reportez-vous au tableau suivant pour une description des paramètres Active Directory.

| Propriété (Web) | Propriété (CLI) | Par défaut | Description |
|---|---|---|---|
| State (État) | `state` | Désactivé | Enabled (activé) \| Disabled (désactivé)<br>Indique si le client Active Directory est ou non activé. |
| Rôles | `defaultRole (a\|u\|c\|r\|o\|s)` | (aucune) | Administrator \| Operator \| Advanced roles \| none<br>Rôle d'accès accordé à tous les utilisateurs Active Directory authentifiés. Cette propriété prend en charge les rôles hérités d'administrateur ou d'opérateur ou de toute autre combinaison de plusieurs ID de rôle individuel 'a', 'u', 'c', 'r', 'o' et 's'. Par exemple, `aucros`, où `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`=Read Only et `s`=Service. Si vous ne configurez pas de rôle, le serveur Active Directory est utilisé pour le déterminer. |
| Adresse | `MAC` | 0.0.0.0 | Adresse IP ou nom DNS du serveur Active Directory. Si le nom DNS est utilisé, le DNS doit être configuré et fonctionnel. |
| Port | `Port` | 0 | Port utilisé pour communiquer avec le serveur ; ou alors activez `autoselect` (qui assigne la valeur 0 au port).<br>Disponible dans le cas peu probable où un port TCP non standard est utilisé. |
| Timeout (Délai d'attente) | `timeout` | 4 | Valeur du délai d'attente en secondes.<br>Délai d'attente en secondes avant la fin des transactions individuelles. Cette valeur ne représente pas la durée totale de toutes les transactions, car le nombre de transactions varie en fonction de la configuration. Cette propriété permet de régler le temps d'attente lorsqu'un serveur ne répond pas ou n'est pas joignable. |

| Propriété (Web) | Propriété (CLI) | Par défaut | Description |
|---|---|---|---|
| Strict Certificate Mode (Mode de certificat strict) | `strictcertmode` | Désactivé | Enabled (activé) \| Disabled (désactivé)<br>Si ce mode est activé, le contenu du certificat du serveur est vérifié par les signatures numériques au moment de l'authentification. Le certificat doit être chargé avant que le mode Strict Certificate (certificat strict) puisse être défini sur Enabled (activé). |
| DNS Locator Mode | `dnslocatormode` | Désactivé | Enabled (activé) \| Disabled (désactivé)<br>Si ce paramètre est activé, une recherche du serveur Active Directory est lancée, selon les requêtes du localisateur DNS configurées. |
| Log Detail (Détail du journal) | `logdetail` | Aucune | None \| High \| Medium \| Low<br>Définit le niveau de détail du diagnostic consigné dans le journal des événements. |

4. **Cliquez sur Save (Enregistrer) pour que vos paramètres soient pris en compte.**

5. **Affichez les informations sur le certificat Active Directory.**

   Reportez-vous au tableau suivant pour une description des paramètres de certificat Active Directory :

| Propriété (Web) | Propriété (CLI) | Affiche | Description |
|---|---|---|---|
| Certificate File Status (Statut du fichier de certificat) | `certstatus` | `certificate not present` | L'indicateur de lecture seule qui signale si un certificat existe. |
| Certificate File Status (Statut du fichier de certificat) | `certstatus` | `certificate present (details)` | Cliquez sur "details" pour obtenir des informations sur l'émetteur, l'objet, le numéro de série, les valeurs de variable valid_from, valid_to et la version. |

6. **Complétez la section Certificate File Upload (Chargement du fichier de certificat) en sélectionnant un mode de transfert pour charger le fichier de certificat et les paramètres requis.**

**Remarque –** Cette section doit être remplie uniquement si le mode Strict Certificate est utilisé.

Le tableau suivant décrit les paramètres requis pour chaque mode de transfert :

| Mode de transfert | Paramètres obligatoires |
|---|---|
| Navigateur | Nom du fichier |
| TFTP | Hôte<br>Chemin d'accès au fichier |
| FTP | Hôte<br>Chemin d'accès au fichier<br>Nom d'utilisateur<br>Mot de passe |
| SCP | Hôte<br>Chemin d'accès au fichier<br>Nom d'utilisateur<br>Mot de passe |

7. **Cliquez sur le bouton Load Certificate (Charger le certificat) ou sur le bouton Remove Certificate (Supprimer le certificat).**

8. **Si un certificat est chargé, les détails en lecture seule suivants s'affichent si vous avez sélectionné "certificate present (details)" (certificat présent (détails)) :**

| Élément | Description |
|---|---|
| `issuer` | Autorité de certificat qui a émis le certificat. |
| `subject` | Serveur ou domaine auquel le certificat s'adresse. |
| `valid_from` | Date à laquelle le certificat sera valide. |
| `valid_until` | Date à laquelle le certificat ne sera plus valide. |
| `serial_number` | Numéro de série du certificat. |
| `version` | Numéro de version du certificat. |

9. **En bas de la page Active Directory, sélectionnez le bouton radio en regard de l'option que vous souhaitez configurer :**
   - Admin Groups
   - les groupes d'opérateur ;
   - Custom Groups
   - les domaines des utilisateurs.
   - Alternate Servers
   - DNS Locator Queries
10. **Entrez les données requises dans les tables.**

    Les tables **Admin Groups**, **Operator Groups** et **Custom Groups** contiennent les noms des groupes Microsoft Active Directory au format de nom distinctif (DN), de nom simple ou de nom NT. Les groupes personnalisés nécessitent que les rôles utilisateur soient configurés de manière à disposer de privilèges Advanced Roles (Rôles avancés) ou Administrator/Operator (Administrateur/Opérateur) pour effectuer diverses tâches.

    **User Domains** correspondent aux domaines d'authentification utilisés pour authentifier un utilisateur. Lorsque l'utilisateur se connecte, le format du nom utilisé suit le modèle du format du nom de domaine spécifique, visible dans la cellule. Durant l'authentification, le nom de connexion de l'utilisateur vient remplacer `<USERNAME>`. Le format principal ou de nom distinctif d'origine est pris en charge. Une tentative d'authentification utilisateur est lancée sur la base du nom d'utilisateur saisi et des domaines d'utilisateurs configurés.

    La table **Alternate Servers** fournit une redondance pour l'authentification. Si aucun certificat n'est fourni, un certificat principal de premier niveau est utilisé. Les serveurs de remplacement sont associés aux mêmes règles et aux mêmes

conditions que le mode de certificat de premier niveau. Chaque serveur dispose de son propre état de certificat et de sa propre commande de certificat pour extraire le certificat s'il est nécessaire.

La table **DNS Locator Queries** permet d'interroger des serveurs DNS pour connaître les hôtes à utiliser dans le cadre de l'authentification. Les requêtes de localisateur DNS sont utilisées uniquement lorsque DNS Locator est activé et que le DNS est configuré et fonctionne.

Dans les tables suivantes, les données par défaut indiquent le format attendu des données Active Directory.

- **Table Admin Groups (Groupes d'administrateurs) :**

  Le nom répertorié dans l'entrée 1 utilise le format de nom distinctif.

| ID | Nom |
|---|---|
| 1 | `CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com` |

- **Table Operator Groups (Groupes d'opérateurs) :**

  Le nom répertorié dans l'entrée 1 utilise le format de nom distinctif.

| ID | Nom |
|---|---|
| 1 | `CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com` |

- **Table Custom Groups (Groupes personnalisés)** :

  Le nom répertorié dans l'entrée 1 utilise le format de nom simple.

| ID | Nom | Rôles |
|---|---|---|
| 1 | `custom_group_1` | `Admin, User Management, Console, Reset and Host Control, Read Only (aucro)` |

- **Table User Domains (Domaines utilisateur) :**

  Le domaine répertorié dans l'entrée 1 est présenté dans le format principal utilisé lors de la première tentative d'authentification de l'utilisateur. L'entrée 2 affiche le nom distinctif complet qu'Active Directory utilise si la tentative d'authentification avec la première entrée échoue.

**Remarque –** Dans l'exemple ci-dessous, <USERNAME> représente le nom de connexion d'un utilisateur. Durant l'authentification, le nom de connexion de l'utilisateur vient remplacer <USERNAME>.

| ID | Domaine |
|---|---|
| 1 | <USERNAME>@sales.east.oracle.com |
| 2 | CN=<USERNAME>,OU=Users,DC=sales,DC=east,DC=oracle,DC=com |

- **Table Alternate Servers (Serveurs de remplacement) :**

  Les entrées ci-dessous fournissent une redondance pour l'authentification.

| ID | Adresse | Port | Certificate Status (État du certificat) |
|---|---|---|---|
| 1 | 10.8.168.99 | 0 | Certificat non présent |
| 2 | 10.8.143.230 | 0 | Certificat non présent |

- **Table DNS Locator Queries (Requêtes au localisateur DNS) :**

  La requête de service du localisateur DNS identifie le service DNS nommé. L'ID de port fait généralement partie de l'enregistrement, mais peut être remplacé en utilisant le format <PORT:636>. De plus, vous pouvez spécifier les services nommés particuliers au domaine authentifié à l'aide du marqueur de substitution <DOMAIN>.

| Nom | Domaine |
|---|---|
| 1 | _ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269> |
| 2 | _ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636> |

11. **Cliquez sur Save (Enregistrer) pour que vos modifications soient prises en compte.**

# ▼ Configuration du serveur LDAP

Pour configurer le serveur LDAP, suivez les étapes ci-dessous. Pour obtenir des instructions détaillées, reportez-vous à la documentation LDAP.

1. **Assurez-vous que tous les utilisateurs s'authentifiant auprès d'ILOM disposent de mots de passe stockés au format de « cryptage » ou dotés de l'extension GNU de cryptage, communément appelée « cryptage MD5 ».**

   Par exemple :

   ```
   userPassword: {CRYPT}ajCa2He4PJhNo
   ```

   ou

   ```
   userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.
   ```

   ILOM prend uniquement en charge l'authentification LDAP pour les mots de passe stockés dans ces deux variantes du format de cryptage.

2. **Ajoutez les classes d'objets `posixAccount` et `shadowAccount`, puis spécifiez les valeurs de propriété requises pour ce schéma (RFC 2307).**

| Propriété requise | Description |
|---|---|
| uid | Nom d'utilisateur permettant de se connecter à ILOM |
| uidNumber | Tout nombre unique |
| gidNumber | Tout nombre unique |
| userPassword | Mot de passe |
| homeDirectory | N'importe quelle valeur (propriété non prise en compte par ILOM) |
| loginShell | N'importe quelle valeur (propriété non prise en compte par ILOM) |

3. **Configurez le serveur LDAP pour activer l'accès au serveur LDAP pour les comptes utilisateur ILOM.**

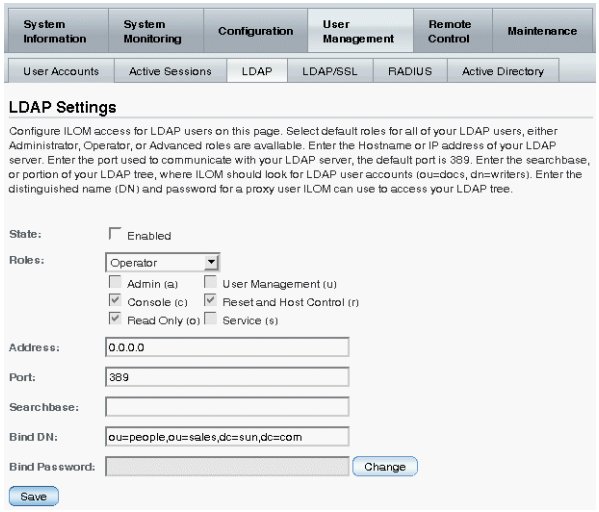
   Activez le serveur LDAP pour qu'il accepte les liaisons anonymes ou créez dessus un utilisateur proxy doté d'un accès en lecture seule à tous les comptes utilisateur qui s'authentifieront via ILOM.

   Reportez-vous à la section Configuration d'ILOM pour LDAP, page 27.

# ▼ Configuration d'ILOM pour LDAP

1. **Connectez-vous à l'interface Web d'ILOM.**
2. **Choisissez User Management (Gestion des utilisateurs) --> LDAP.**

   La page LDAP Settings (Paramètres LDAP) s'affiche.




3. **Saisissez les valeurs suivantes :**
   - **State** (État) : cochez la case Enabled (Activé) pour authentifier les utilisateurs LDAP.
   - **Role** (Rôle) : sélectionnez Administrator ou Operator, ou n'importe quelle combinaison de rôles d'ID individuel comme a, u, c, r, o, et s.
   - **Address** (Adresse) : adresse du serveur LDAP ou nom DNS. Si le nom DNS est utilisé, le DNS doit être configuré et fonctionnel.
   - **Port** (Port) : numéro de port sur le serveur LDAP.
   - **Searchbase** (Base de recherche) : saisissez la branche du serveur LDAP sur laquelle vous voulez rechercher des utilisateurs.
   - **Bind DN** (DN de base) : saisissez le nom distinctif (DN) d'un utilisateur proxy en lecture seule sur le serveur LDAP. Le logiciel ILOM doit disposer d'un accès en lecture seule au serveur LDAP pour rechercher et authentifier les utilisateurs.
   - **Bind Password** (Lier le mot de passe) : saisissez le mot de passe de l'utilisateur en lecture seule.

4. **Cliquez sur Save (Enregistrer) pour que vos modifications soient prises en compte.**

5. **Pour vérifier que l'authentification LDAP fonctionne, connectez-vous à ILOM en utilisant un nom d'utilisateur et un mot de passe LDAP.**

---

**Remarque –** ILOM recherche les utilisateurs locaux avant les utilisateurs LDAP. Si un nom d'utilisateur LDAP existe en tant qu'utilisateur local, ILOM utilise le compte local pour l'authentification.

---

## ▼ Configuration d'ILOM pour LDAP /SSL

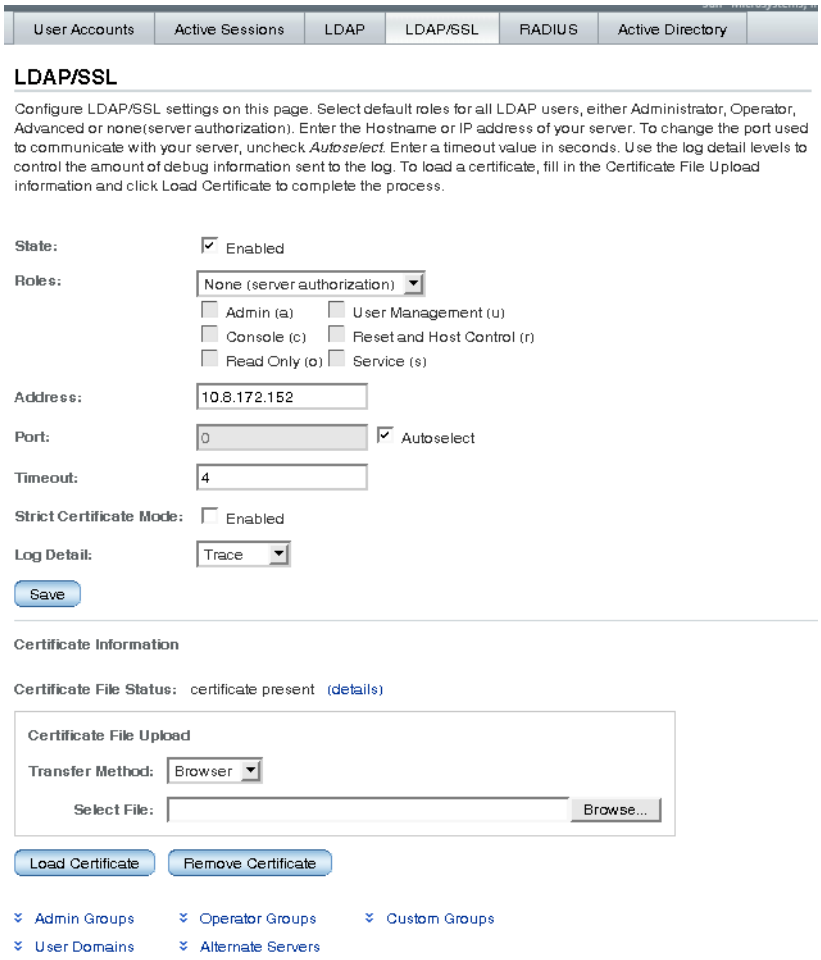
LDAP/SSL offre une sécurité renforcée aux utilisateurs de LDAP par l'intermédiaire de la technologie SSL (Secure Socket Layer). Les certificats sont facultatifs si le mode Strict Certificate est activé.

Pour configurer ILOM pour LDAP/SSL, suivez les étapes ci-dessous :

1. **Connectez-vous à l'interface Web d'ILOM.**

2. **Sélectionnez User Management --> LDAP/SSL.**

   La page LDAP/SSL qui s'ouvre indique les paramètres de configuration et les tables LDAP/SSL.




### 3. Configurez les paramètres LDAP/SSL.

Reportez-vous au tableau suivant pour une description des paramètres LDAP/SSL.

| Propriété (Web) | Propriété (CLI) | Par défaut | Description |
|---|---|---|---|
| State (État) | `state` | Désactivé | Enabled (activé) \| Disabled (désactivé)<br>Indique si le client LDAP/SSL est ou non activé. |
| Rôles | `defaultRole (a\|u\|c\|r\|o\|s)` | (aucune) | Administrator \| Operator \| Advanced roles \| none<br>Rôle d'accès accordé à tous les utilisateurs LDAP/SSL authentifiés. Cette propriété prend en charge les rôles hérités d'administrateur ou d'opérateur ou de toute autre combinaison de plusieurs ID de rôle individuel 'a', 'u', 'c', 'r', 'o' et 's'. Par exemple, `aucros`, où `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`=Read Only et `s`=Service. Si vous ne configurez pas de rôle, le serveur LDAP/SSL est utilisé pour le déterminer. |
| Adresse | `MAC` | 0.0.0.0 | Adresse IP ou nom DNS du serveur LDAP/SSL. Si le nom DNS est utilisé, le DNS doit être configuré et fonctionnel. |
| Port | `Port` | 0 | Port utilisé pour communiquer avec le serveur ; ou alors activez `autoselect` (qui assigne la valeur 0 au port).<br>Disponible dans le cas peu probable où un port TCP non standard est utilisé. |
| Timeout (Délai d'attente) | `timeout` | 4 | Valeur du délai d'attente en secondes.<br>Délai d'attente en secondes avant la fin des transactions individuelles. Cette valeur ne représente pas la durée totale de toutes les transactions, car le nombre de transactions varie en fonction de la configuration.<br>Cette propriété permet de régler le temps d'attente lorsqu'un serveur ne répond pas ou n'est pas joignable. |
| Strict Certificate Mode (Mode de certificat strict) | `strictcertmode` | Désactivé | Enabled (activé) \| Disabled (désactivé)<br>Si ce mode est activé, le contenu du certificat du serveur est vérifié par les signatures numériques au moment de l'authentification. Le certificat doit être chargé avant que le mode Strict Certificate (certificat strict) puisse être défini sur Enabled (activé). |
| Log Detail (Détail du journal) | `logdetail` | Aucune | None \| High \| Medium \| Low<br>Définit le niveau de détail du diagnostic consigné dans le journal des événements. |

**4. Cliquez sur Save (Enregistrer) pour que vos paramètres soient pris en compte.**

5. **Affichez les informations sur le certificat LDAP/SSL dans la section centrale de la page LDAP/SSL.**

   Reportez-vous au tableau suivant pour une description des paramètres de certificat LDAP/SSL.

| Propriété (Web) | Propriété (CLI) | Affiche | Description |
|---|---|---|---|
| Certificate File Status (Statut du fichier de certificat) | `certstatus` | `certificate not present` | L'indicateur de lecture seule qui signale si un certificat existe. |
| Certificate File Status (Statut du fichier de certificat) | `certstatus` | `certificate present (details)` | Cliquez sur "details" pour obtenir des informations sur l'émetteur, l'objet, le numéro de série, les valeurs de variable valid_from, valid_to et la version. |

6. **Complétez la section Certificate File Upload (Chargement du fichier de certificat) en sélectionnant un mode de transfert pour charger le fichier de certificat et les paramètres requis.**

**Remarque –** Cette section doit être remplie uniquement si le mode Strict Certificate est utilisé.

Le tableau suivant décrit les paramètres requis pour chaque mode de transfert.

| Mode de transfert | Paramètres obligatoires |
|---|---|
| Navigateur | Nom du fichier |
| TFTP | Hôte<br>Chemin d'accès au fichier |
| FTP | Hôte<br>Chemin d'accès au fichier<br>Nom d'utilisateur<br>Mot de passe |
| SCP | Hôte<br>Chemin d'accès au fichier<br>Nom d'utilisateur<br>Mot de passe |

7. **Cliquez sur le bouton Load Certificate (Charger le certificat) ou sur le bouton Remove Certificate (Supprimer le certificat).**

8. **Si un certificat est chargé, les détails en lecture seule suivants s'affichent si vous avez sélectionné "certificate present (details)" (certificat présent (détails)) :**

| Élément | Description |
|---|---|
| `issuer` | Autorité de certificat qui a émis le certificat. |
| `subject` | Serveur ou domaine auquel le certificat s'adresse. |
| `valid_from` | Date à laquelle le certificat sera valide. |
| `valid_until` | Date à laquelle le certificat ne sera plus valide. |
| `serial_number` | Numéro de série du certificat. |
| `version` | Numéro de version du certificat. |

## ▼ Modification des tables LDAP/SSL

Suivez les étapes ci-dessous pour modifier les informations Admin Groups, Operator Groups, Custom Groups, User Domains ou Alternate Servers :

1. **Connectez-vous à l'interface Web d'ILOM.**

2. **Sélectionnez User Management --> LDAP/SSL.**

   La page LDAP/SSL s'affiche.

3. **En bas de la page LDAP/SSL, sélectionnez les liens situés en regard du type d'information que vous souhaitez modifier :**
   - Admin Groups
   - les groupes d'opérateur ;
   - Custom Groups
   - les domaines des utilisateurs.
   - Alternate Servers

4. **Sélectionnez le bouton radio situé en regard de chaque table que vous souhaitez modifier, puis cliquez sur Edit (Modifier).**

   La page appropriée s'affiche : Edit LDAP/SSL **Admin Groups**, Edit LDAP/SSL **Operator Groups**, Edit LDAP/SSL **Custom Groups**, Edit LDAP/SSL **User Domains** ou Edit LDAP/SSL **Alternate Servers**.

5. **Dans chaque page Edit, modifiez des informations.**

   Reportez-vous à la procédure Configuration d'ILOM pour Active Directory, page 18 pour voir des exemples d'informations que vous pouvez ajouter ou modifier dans les tables LDAP/SSL. Les informations des tables Active Directory sont similaires à celles des tables LDAP/SSL.

   Par exemple, dans la table User Domains (Domaines d'utilisateurs), renseignez le champ de texte Name (Nom). Utilisez le marqueur de substitution `<USERNAME>` pour réserver une place pour le nom de l'utilisateur.

   ```
   domain=uid=<USERNAME>,OU=people,DC=sales,DC=east,DC=oracle,
   DC=com
   ```

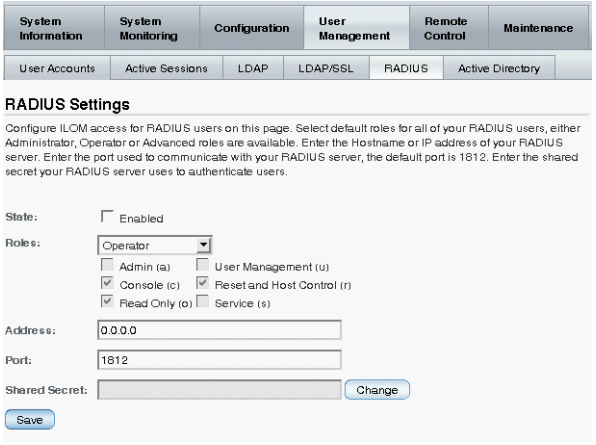
   Vous seriez authentifié sous ILOM avec le nom fourni.

6. **Cliquez sur Save (Enregistrer) pour que vos modifications soient prises en compte.**

# ▼ Configuration d'ILOM pour RADIUS

1. **Connectez-vous à l'interface Web d'ILOM.**
2. **Choisissez User Management (Gestion des utilisateurs) --> RADIUS.**

La page RADIUS Settings (Paramètres RADIUS) s'affiche.



3. **Complétez les paramètres RADIUS.**

| Propriété (Web) | Propriété (CLI) | Par défaut | Description |
|---|---|---|---|
| State (État) | `state` | Désactivé | Enabled (activé) \| Disabled (désactivé)<br>Indique si le client RADIUS est ou non activé. |
| Role (Rôle) | `defaultrole`<br>`a\|u\|c\|r\|o\|s` | Read Only (Lecture seule) (`o`) | Administrator \| Operator \| Advanced Roles<br>Rôle d'accès accordé à tous les utilisateurs RADIUS authentifiés. Cette propriété prend en charge les rôles hérités d'administrateur ou d'opérateur ou de toute autre combinaison de plusieurs ID de rôle individuel '`a`', '`u`', '`c`', '`r`', '`o`' et '`s`'. Par exemple, `aucros`, où `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`= Read Only et `s`=Service. |
| Adresse | `ipaddress` | 0.0.0.0 | Adresse IP ou nom DNS du serveur RADIUS. Si le nom DNS est utilisé, le DNS doit être configuré et fonctionnel. |
| Port | `port` | 1812 | Définit le numéro du port utilisé pour communiquer avec le serveur RADIUS. La valeur par défaut est le port 1812. |
| Shared Secret (Secret partagé) | `secret` | (aucune) | Définit le secret partagé utilisé pour protéger des données sensibles et pour s'assurer que le client et le serveur se reconnaissent mutuellement. |

4. **Cliquez sur Save (Enregistrer) pour que vos paramètres soient pris en compte.**

## ▼ Se connecter à ILOM à l'aide d'un nouveau compte utilisateur

Pour vous connecter à l'interface Web d'ILOM en utilisant un compte utilisateur autre que `root`, ouvrez un navigateur Web et procédez comme suit :

1. **Entrez `http://`*adresse ip_système* dans le navigateur Web.**

   Si ILOM fonctionne dans un environnement réseau à double pile, vous pouvez entrer l'*adresse_ip_système* en utilisant un format d'adresse IPv4 ou IPv6.

   Par exemple :

   **Pour IPv4 -** `http://10.8.183.106`

   ou

   **Pour IPv6 -** `http://[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`

   La page de connexion de l'interface Web s'affiche.

   Pour savoir comment entrer des adresses IP dans un environnement à double pile et diagnostiquer les problèmes de connexion, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0*.

2. **Entrez le nom d'utilisateur et le mot de passe du compte utilisateur :**

   `User Name:` **<***nom d'utilisateur assigné***>**

   `Password:` **<***mot de passe assigné***>**

3. **Cliquez sur Log In (Connexion).**

   L'interface Web d'ILOM s'ouvre et affiche la page Version.

## ▼ Se déconnecter d'ILOM

- **Cliquez sur le bouton Log Out (Déconnexion) dans l'interface Web d'ILOM.**

  Il se trouve dans le coin supérieur droit de l'interface Web d'ILOM. N'utilisez pas le bouton de déconnexion de votre navigateur Web pour quitter ILOM.

# Quelles sont les étapes ultérieures ?

Vous pouvez continuer à personnaliser la configuration d'ILOM pour votre système et environnement de centre de données. Avant de configurer ILOM pour votre environnement, reportez-vous au *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager 3.0* pour vous faire une idée générale des nouvelles caractéristiques et fonctionnalités d'ILOM 3.0. Déterminez en quoi les fonctionnalités d'ILOM affecteront votre environnement pour configurer plus efficacement les paramètres d'ILOM et pouvoir accéder à l'ensemble de ses fonctionnalités depuis votre système et centre de données.

Reportez-vous également aux guides des procédures d'Oracle ILOM 3.0 pour savoir comment effectuer des tâches ILOM à l'aide d'une interface utilisateur spécifique et au Supplément ILOM ou au Guide d'administration correspondant à votre plate-forme pour obtenir des instructions de configuration propres à votre plate-forme.

La collection de documentation sur ILOM 3.0 est disponible à l'adresse suivante :

`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

CHAPITRE 3

# Procédures de configuration initiale d'ILOM à l'aide de la CLI ILOM

**Rubriques**

| Description | Liens |
|---|---|
| Première connexion à ILOM | • Première connexion à ILOM à l'aide de la CLI, page 38 |
| Configurer l'environnement réseau | • Configuration d'un environnement réseau IPv4 et IPv6, page 39 |
| Ajouter des comptes utilisateur ou configurer un service d'annuaire | • Ajout de comptes utilisateur ou configuration d'un service d'annuaire, page 45 |
| Rechercher des informations sur les étapes de configuration d'ILOM ultérieures | • Quelles sont les étapes ultérieures ?, page 57 |

# Première connexion à ILOM à l'aide de la CLI

Pour vous connecter à la CLI d'ILOM la première fois, utilisez le compte utilisateur `root` préconfiguré avec son mot de passe par défaut `changeme`. Après avoir paramétré votre environnement réseau, vous pouvez établir un compte utilisateur administratif en utilisant un compte utilisateur assigné et son mot de passe.

## ▼ Se connecter à ILOM avec le compte utilisateur `root`

Pour vous connecter à la CLI d'ILOM la première fois, utilisez SSH et le compte utilisateur `root`.

1. **Pour vous connecter la CLI d'ILOM avec le compte utilisateur `root`, entrez :**

   `$` **`ssh root@`***`adresse_ip_système`*

   Si ILOM fonctionne dans un environnement réseau à double pile, vous pouvez entrer l'*adresse_ip_système* en utilisant un format d'adresse IPv4 ou IPv6.

   Par exemple :

   **Pour IPv4 -** `10.8.183.106`

   ou

   **Pour IPv6 -** `[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`

   L'invite de connexion à ILOM s'affiche.

   Pour savoir comment entrer des adresses IP dans un environnement à double pile, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0*.

2. **Tapez les nom d'utilisateur et mot de passe par défaut :**

   <*nom_hôte*>: **`root`**

   `Password:` **`changeme`**

   L'invite de la CLI d'ILOM s'affiche (->).

# Configuration d'un environnement réseau IPv4 et IPv6

La procédure CLI suivante fournit des instructions pour configurer ILOM afin de fonctionner dans un environnement réseau à double pile IPv4 et IPv6. Pour plus d'informations sur la configuration d'ILOM dans un environnement réseau IPv4 et IPv6, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0*.

Si vous configurez ILOM pour fonctionner dans un environnement réseau IPv4 uniquement, comme le prennent en charge les versions ILOM 3.0.10 et antérieures, voir le *Guide des procédures relatives à la CLI d'Oracle Integrated Lights Out Manager (ILOM) 3.0.*

Par défaut, ILOM essaiera d'obtenir l'adresse IPv4 en utilisant DHCPv4 et l'adresse IPv6 en utilisant IPv6 sans état.

## ▼ Configurer les paramètres IPv4 et IPv6 en utilisant la CLI

1. **Connectez-vous à la CLI ILOM du SP ou du CMM**

   Établissez une connexion depuis la console série locale ou une connexion SSH avec le processeur de service du serveur ou le CMM.

2. **Effectuez les instructions de configuration réseau qui s'appliquent à votre environnement réseau :**

   - Pour configurer les paramètres réseau IPv4, effectuez les opérations de l'Étape 3 à l'Étape 5 de cette procédure.
   - Pour configurer les paramètres réseau IPv6, effectuez les opérations de l'Étape 6 à l'Étape 10 de cette procédure.

3. **Pour les configurations réseau IPv4, utilisez la commande** `cd` **pour accéder au répertoire de travail** `/`*`x`*`/network` **du périphérique.**

   Par exemple :

   - Pour un SP de serveur monté en rack, tapez : `cd /SP/network`
   - Pour un CMM de châssis, tapez : `cd /CMM/network`
   - Pour un SP de serveur blade en châssis, tapez : `cd /CH/BL`*`n`*`/network`
   - Pour un serveur blade en châssis ayant plusieurs nœuds SP, tapez : `cd /CH/BL`*`n`*`/Node`*`n`*`/network`

4. **Utilisez la commande** `show` **pour afficher les paramètres réseau IPv4 configurés sur le périphérique.**

5. **Pour définir les paramètres réseau IPv4 DHCP ou statiques, effectuez l'une des opérations suivantes :**

   - **Pour configurer les paramètres réseau IPv4 DHCP**, définissez les valeurs des propriétés suivantes :

| Propriété | Définir la valeur de propriété | Description |
|---|---|---|
| `state` | `set state=enabled` | Le paramètre réseau `state` (état) est `enabled` (activé) par défaut pour IPv4.<br>**Remarque -** Pour activer l'option réseau DHCP pour IPv4, `state` (état) doit être défini sur `enabled` (activé). |
| `pendingipdiscovery` | `set pendingipdiscovery=dhcp` | La valeur de la propriété `ipdiscovery` est définie sur `dhcp` par défaut pour IPv4.<br>**Remarque -** Si la valeur par défaut de la propriété `dhcp` a été remplacée par `static`, vous devez la définir sur `dhcp`. |
| `commitpending=` | `set commitpending=true` | Tapez `set commitpending=true` pour valider les changements apportés aux propriétés `state` et `ipdiscovery`. |

- **Pour configurer les paramètres réseau IPv4 statiques**, définissez les valeurs des propriétés suivantes :

| Propriété | Définir la valeur de propriété | Description |
|---|---|---|
| `state` | `set state=enabled` | Le paramètre réseau `state` (état) est `enabled` (activé) par défaut pour IPv4.<br>**Remarque -** Pour activer l'option réseau IPv4 statique, `state` (état) doit être défini sur `enabled` (activé). |
| `pendingipdiscovery` | `set pendingipdiscovery=static` | Pour activer la configuration réseau IPv4 statique, vous devez définir la propriété `pendingipdiscovery` sur la valeur `static`.<br>**Remarque -** La valeur de la propriété `ipdiscovery` est définie sur `dhcp` par défaut pour IPv4. |
| `pendingipaddress`<br>`pendingipnetmask`<br>`pendingipgateway` | `set pendingipaddress=`<*adresse IP*> `pendingipnetmask=`<*masque de réseau*> `pendingipgateway=`<*passerelle*> | Pour assigner plusieurs paramètres réseau statiques, tapez la commande `set` suivie par la commande `pending` pour chaque valeur de propriété (adresse IP, masque de réseau et passerelle), puis tapez la valeur statique à assigner. |
| `commitpending=` | `set commitpending=true` | Tapez `set commitpending=true` pour valider les changements apportés aux propriétés `state` et `ipdiscovery` et aux paramètres réseau. |

6. **Pour les configurations réseau IPv6, utilisez la commande** `cd` **pour accéder au répertoire de travail** `/`*x*`/network/ipv6` **du périphérique.**

   Par exemple :

   - Pour un SP de serveur monté en rack, tapez : `cd /SP/network/ipv6`
   - Pour un CMM de châssis, tapez : `cd /CMM/network/ipv6`
   - Pour un SP de serveur blade en châssis, tapez : `cd /CH/BL`*n*`/network/ipv6`
   - Pour un serveur blade en châssis ayant plusieurs nœuds SP, tapez : `cd /CH/BL`*n*`/Node`*n*`/network/ipv6`

7. **Utilisez la commande** `show` **pour afficher les paramètres réseau IPv6 configurés sur le périphérique.**

   Par exemple, observez les valeurs résultats de l'exemple suivant pour les propriétés IPv6 sur un périphérique SP de serveur :

```
-> show

 /SP/network/ipv6
    Targets:

    Properties:
        state = enabled
        autoconfig = stateless
        dhcpv6_server_duid = (none)
        link_local_ipaddress = fe80::214:4fff:feca:5f7e/64
        static_ipaddress = ::/128
        ipgateway = fe80::211:5dff:febe:5000/128
        pending_static_ipaddress = ::/128
        dynamic_ipaddress_1 = fec0:a:8:b7:214:4fff:feca:5f7e/64

    Commands:
        cd
        show
```

---

**Remarque –** La valeur par défaut de la propriété IPv6 `autoconfig` dans ILOM 3.0.14 (et ultérieur) est `autoconfig=stateless`. Cependant, si ILOM 3.0.12 est installé sur votre CMM ou votre serveur, la valeur par défaut de la propriété `autoconfig` est `autoconfig=stateless_only`.

---

---

**Remarque –** Si la propriété `autoconfig` est définie sur `dhcpv6_stateful` ou `dhcpv6_stateless`, la propriété en lecture seule `dhcpv6_server_duid` va identifier l'ID DHCP unique du serveur DHCPv6 dernièrement utilisé par ILOM pour récupérer les informations DHCP.

---

8. **Pour configurer une option de configuration automatique IPv6, utilisez la commande `set` pour spécifier les valeurs de propriété suivantes.**

| Propriété | Définir la valeur de propriété | Description |
|---|---|---|
| `state` | `set state=enabled` | Le paramètre réseau IPv6 `state` (état) est `enabled` (activé) par défaut. Pour activer une option de configuration automatique IPv6, state (état) doit être défini sur `enabled` (activé). |
| `autoconfig` | `set autoconfig=`<*valeur*> | Spécifiez cette commande suivie par la valeur `autoconf` à définir.<br>Les options possibles sont ::<br>• `stateless` (paramètre par défaut fourni dans ILOM 3.0.14 ou ultérieur)<br>ou<br>`stateless_only` (paramètre par défaut fourni dans ILOM 3.0.12)<br>Assigne automatiquement l'adresse IP détectée sur le routeur réseau IPv6.<br>• `dhcpv6_stateless`<br>Assigne automatiquement les informations DNS détectées sur le serveur DHCP.<br>La valeur de propriété `dhcpv6_stateless` est disponible dans ILOM à partir de la version 3.0.14.<br>• `dhcpv6_stateful`<br>Assigne automatiquement l'adresse IPv6 détectée sur le serveur DHCPv6.<br>La valeur de propriété `dhcpv6_stateful` est disponible dans ILOM à partir de la version 3.0.14.<br>• `disable`<br>Désactive toutes les valeurs de propriété de configuration automatique et définit la valeur de propriété en lecture seule pour l'adresse locale de liaison. |

Les informations suivantes s'appliquent aux options `autoconfig` IPv6 :

- Les options `auto-config` IPv6 prennent effet dès leur définition. Vous n'avez pas à valider ces changements sous la cible `/network`.
- Les adresses `auto-config` IPv6 détectées pour le périphérique n'affecteront pas les sessions ILOM actives vers le périphérique. Vous pouvez vérifier les nouvelles adresses configurées automatiquement sur la cible `/network/ipv6`.
- À partir d'ILOM 3.0.14, vous pouvez activer l'option `auto-config stateless` pour qu'elle s'exécute simultanément avec l'option `dhcpv6_stateless`, si celle-ci est activée, ou avec l'option `dhcpv6_stateful`, si celle-ci est activée. En revanche, les options `auto-config dhcpv6_stateless` et `dhcpv6_stateful` ne doivent pas être activées pour s'exécuter simultanément.

9. **Pour définir une adresse IPv6 statique en attente, spécifiez les valeurs des propriétés suivantes ::**

| Propriété | Définir la valeur de propriété | Description |
|---|---|---|
| `state` | `set state=enabled` | Le paramètre réseau IPv6 `state` (état) est `enabled` (activé) par défaut. Pour activer une adresse IPv6 statique, `state` (état) doit être défini sur `enabled` (activé). |
| `pendingipaddress` | `set pending_static_ipaddress=` *<adresse IP>/<longueur en bits du masque de sous-réseau>* | Saisissez cette commande suivie par la valeur de propriété pour l'adresse IPv6 statique et le masque de réseau à assigner au périphérique.<br>Exemple d'adresse IPv6 :<br>`fec0:a:8:b7:214:4fff:feca:5f7e/64` |

10. **Pour valider les paramètres réseau statiques IPv6 en attente, effectuez les opérations suivantes :**

    a. **Utilisez la commande** `cd` **pour accéder au répertoire cible** `network` **du périphérique.**

    Par exemple :

    - Pour un serveur monté en rack, tapez : `cd /SP/network`
    - Pour un CMM de châssis, tapez : `cd /CMM/network`
    - Pour un SP de serveur blade en châssis, tapez : `cd /CH/BL`*n*`/network`
    - Pour un SP de serveur blade en châssis ayant plusieurs nœuds, tapez : `cd /CH/BL`*n*`/Node`*n*`/network`

    b. **Saisissez la commande suivante pour valider les valeurs de propriété modifiées pour IPv6 :**

    ```
    set commitpending=true
    ```

**Remarque –** L'assignation d'une nouvelle adresse IP statique au périphérique (SP ou CMM) va clore toutes les sessions ILOM actives vers le périphérique. Pour vous reconnecter à ILOM, vous devrez créer une nouvelle session de navigateur en utilisant l'adresse IP nouvellement assignée.

Pour tester la configuration réseau IPv4 ou IPv6 à partir d'ILOM, utilisez les outils de test réseau (Ping ou Ping6). Pour plus de détails, voir le *Guide des procédures relatives à la CLI d'Oracle Integrated Lights Out Manager (ILOM) 3.0.*

# Ajout de comptes utilisateur ou configuration d'un service d'annuaire

Une fois connecté à ILOM à l'aide du compte utilisateur `root`, vous pouvez créer un compte utilisateur local ou bien configurer un service d'annuaire. Pour plus d'informations sur les comptes utilisateur et les services d'annuaire ILOM, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0*.

**Rubriques**

| Description | Liens |
|---|---|
| Comment ajouter un compte utilisateur et assigner des rôles utilisateur (privilèges) | • Ajout d'un compte utilisateur et assignation de privilèges, page 45 |
| Comment configurer ILOM pour Active Directory | • Configuration d'ILOM pour Active Directory, page 46 |
| Comment configurer ILOM pour LDAP | • Configuration d'ILOM pour LDAP, page 50 |
| Comment configurer ILOM pour LDAP/SSL | • Configuration d'ILOM pour LDAP /SSL, page 51 |
| Comment configurer ILOM pour RADIUS | • Configuration d'ILOM pour RADIUS, page 55 |
| Comment vérifier que le nouveau compte utilisateur ou le service d'annuaire fonctionne correctement | • Se connecter à ILOM à l'aide d'un nouveau compte utilisateur, page 56 |
| Comment se déconnecter d'ILOM | • Se déconnecter d'ILOM, page 57 |

## ▼ Ajout d'un compte utilisateur et assignation de privilèges

1. **Connectez-vous à la CLI d'ILOM.**
2. **Pour ajouter un compte utilisateur local, tapez la commande suivante et votre mot de passe :**

   –> **create /SP/users/***nom_utilisateur* **password=***mot_de_passe*

   Par exemple :

   ```
   -> create /SP/users/user5
   Creating user...
   ```

```
Enter new password: ********
Enter new password again: ********
Created /SP/users/user5
```

3. **Pour assigner des rôles à un compte utilisateur, tapez la commande suivante :**

   –> **set /SP/users/***nom_utilisateur* **role=aucr**

   Par exemple :

   ```
   -> set /SP/users/user5 role=aucr
   Set 'role' to 'aucr'
   ```

   Pour une description des rôles de compte utilisateur, reportez-vous à la section Ajout d'un compte utilisateur et assignation de privilèges, page 45.

## ▼ Configuration d'ILOM pour Active Directory

1. **Connectez-vous à la CLI d'ILOM avec le compte utilisateur** `root`**.**

2. **Utilisez la commande** `show` **pour afficher les propriétés de premier niveau. Tapez :**

```
-> cd /SP/clients/activedirectory
/SP/clients/activedirectory

-> show

 /SP/clients/activedirectory
    Targets:
        admingroups
        alternateservers
        cert
        customgroups
        dnslocatorqueries
        opergroups
        userdomains

    Properties:
        address = 10.5.121.321
        defaultrole = Administrator
        dnslocatormode = enabled
        logdetail = trace
        port = 0
        state = disabled
        strictcertmode = disabled
        timeout = 4

    Commands:
        cd
        set
        show
```

3. **Utilisez la commande** `show` **pour afficher les informations contenues dans les tables. Tapez :**

   -> **show /SP/clients/activedirectory/***nom***/***n*

   Où *n* est compris entre **1** et **5** et *nom* est l'un des noms suivants :

   - **admingroups** (pour les propriétés Admin Groups)
   - **opergroups** (pour les propriétés Operator Groups)
   - **customgroups** (pour les propriétés Custom Groups)
   - **userdomains** (pour les propriétés User Domains)
   - **alternateservers** (pour les propriétés Alternate Servers)
   - **dnslocatorqueries** (pour les propriétés DNS Locator Queries)
   - **cert** (pour les propriétés de certificat - `cert` n'étant pas une table, la valeur comprise entre 1 et 5 de *n* ne s'applique pas)

Vous pouvez utiliser la commande `show` pour extraire les propriétés de certificat :

```
-> show /SP/clients/activedirectory/cert
 /SP/clients/activedirectory/cert
    Targets:

    Properties:
        certstatus = certificate not present
        clear_action = (none)
        issuer = (none)
        load_uri = (none)
        serial_number = (none)
        subject = (none)
        valid_from = (none)
        valid_until = (none)
        version = (none)
```

Vous pouvez utiliser la commande `show` pour extraire les propriétés de certificat du serveur de remplacement :

```
-> show /SP/clients/activedirectory/alternateservers/1/cert
 /SP/clients/activedirectory/alternateservers/1/cert
    Targets:

    Properties:
        certstatus = certificate not present
        clear_action = (none)
        issuer = (none)
        load_uri = (none)
        serial_number = (none)
        subject = (none)
        valid_from = (none)
        valid_until = (none)
        version = (none)
```

4. **Utilisez la commande** `set` **pour configurer les propriétés de premier niveau.**

   Par exemple :

```
-> set address=10.5.121.321
Set 'address' to 10.5.121.321
->set ...etc. for defaultrole, dnslocator, logdetail, port, state,
stricmode, timeout
```

5. **Utilisez la commande** `set` **pour charger un certificat ou modifier des propriétés.**

   Par exemple :

- **Pour charger un certificat Active Directory :**

```
-> set /SP/clients/activedirectory/cert load_uri=
tftp://10.6.143.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.143.192/sales/cert.cert'
```

- **Pour charger un certificat de serveur de remplacement :**

```
-> set /SP/clients/activedirectory/alternateservers/1/cert
load_uri=tftp://10.6.143.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.143.192/sales/cert.cert'
```

- **Pour modifier les propriétés de la table Admin Groups :**

```
-> set /SP/clients/activedirectory/admingroups/1 name=CN=
spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=
com'
```

- **Pour modifier les propriétés de la table Operator Groups :**

```
-> set /SP/clients/activedirectory/opergroups/1 name=CN=
spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=
com'
```

- **Pour modifier les propriétés de la table Custom Groups** :

---

**Remarque –** Vous pouvez définir le rôle sur un rôle individuel ou une combinaison des rôles Admin (a), User Management (u), Console (c), Reset and Host Control (r) ou Read Only (o). Les rôles hérités d'administrateur ou d'opérateur sont également pris en charge.

---

```
-> set /SP/clients/activedirectory/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=
com'
-> set /SP/clients/activedirectory/customgroups/1 roles=au
Set 'roles' to au
```

- **Pour modifier les propriétés de la table User Domains :**

```
-> set /SP/clients/activedirectory/userdomains/1 domain=
username@sales.oracle.com
Set 'domain' to 'username@sales.oracle.com'
```

- **Pour modifier les propriétés de la table Alternate Servers :**

```
-> set /SP/clients/activedirectory/alternateservers/1 address=
ip_address
```

- **Pour modifier les propriétés de la table DNS Locator Queries :**

```
-> set /SP/clients/activedirectory/dnslocatorqueries/1 service=
_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
```

La requête de service du localisateur DNS identifie le service DNS nommé. L'ID de port fait généralement partie de l'enregistrement, mais peut être remplacé en utilisant le format <PORT:636>. De plus, vous pouvez spécifier les services nommés particuliers au domaine authentifié à l'aide du marqueur de substitution <DOMAIN>.

| Nom | Domaine |
|---|---|
| 1 | _ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269> |
| 2 | _ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636> |

# ▼ Configuration d'ILOM pour LDAP

1. **Connectez-vous à la CLI d'ILOM.**
2. **Utilisez la commande** `set` **pour entrer le nom et le mot de passe de l'utilisateur proxy.**

   Par exemple :

   –> **set /SP/clients/ldap binddn="cn=proxyuser, ou=people, ou=sales, dc=oracle, dc=com" bindpw**=*mot_de_passe*
3. **Entrez l'adresse IP ou le nom DNS du serveur LDAP. Tapez :**

   –> **set /SP/clients/ldap address=***adresse_ip_ldap* | *nom_DNS*

4. **(Facultatif) Assignez le port utilisé pour communiquer avec le serveur LDAP ; le port par défaut est le port 389. Tapez :**

   -> **set /SP/clients/ldap port=***port_ldap*

5. **Indiquez le nom distinctif de la branche de l'arborescence LDAP contenant les utilisateurs et les groupes. Tapez :**

   -> **set /SP/clients/ldap searchbase="ou=people, ou=sales, dc=oracle, dc=com"**

   Il s'agit de l'emplacement dans l'arborescence LDAP où vous souhaitez rechercher l'authentification de l'utilisateur.

6. **Définissez l'état du service LDAP sur « enabled » (Activé). Tapez :**

   -> **set /SP/clients/ldap state=enabled**

7. **Pour vérifier que l'authentification LDAP fonctionne, connectez-vous à ILOM en utilisant un nom d'utilisateur et un mot de passe LDAP.**

---

**Remarque –** ILOM recherche les utilisateurs locaux avant les utilisateurs LDAP. Si un nom d'utilisateur LDAP existe en tant qu'utilisateur local, ILOM utilise le compte local pour l'authentification.

---

## ▼ Configuration d'ILOM pour LDAP /SSL

LDAP/SSL offre une sécurité renforcée aux utilisateurs de LDAP par l'intermédiaire de la technologie SSL (Secure Socket Layer). Les certificats sont facultatifs si le mode Strict Certificate est activé.

Pour configurer ILOM pour LDAP/SSL, suivez les étapes ci-dessous :

1. **Connectez-vous à la CLI d'ILOM.**

2. **Utilisez la commande** `show` **pour afficher les propriétés de premier niveau. Tapez :**

```
-> cd /SP/clients/ldapssl
/SP/clients/ldapssl

-> show

 /SP/clients/ldapssl
    Targets:
        admingroups
        alternateservers
        cert
        customgroups
        opergroups
        userdomains

    Properties:
        address = 10.5.121.321
        defaultrole = Administrator
        logdetail = trace
        port = 0
        state = disabled
        strictcertmode = disabled
        timeout = 4

    Commands:
        cd
        set
        show
```

3. **Utilisez la commande** `show` **pour afficher les informations contenues dans les tables. Tapez :**

   -> **show /SP/clients/ldapssl/***nom***/***n*

   Où *n* est compris entre **1** et **5** et *nom* est l'un des noms suivants :

   - **admingroups** (pour les propriétés Admin Groups)
   - **opergroups** (pour les propriétés Operator Groups)
   - **customgroups** (pour les propriétés Custom Groups)
   - **userdomains** (pour les propriétés User Domains)
   - **alternateservers** (pour les propriétés Alternate Servers)
   - **cert** (pour les propriétés de certificat - `cert` n'étant pas une table, la valeur comprise entre 1 et 5 de *n* ne s'applique pas)

Vous pouvez utiliser la commande `show` pour extraire les propriétés de certificat :

```
-> show /SP/clients/ldapssl/cert
 /SP/clients/ldapssl/cert
    Targets:

    Properties:
        certstatus = certificate not present
        clear_action = (none)
        issuer = (none)
        load_uri = (none)
        serial_number = (none)
        subject = (none)
        valid_from = (none)
        valid_until = (none)
        version = (none)
```

Vous pouvez utiliser la commande `show` pour extraire les propriétés de certificat du serveur de remplacement :

```
-> show /SP/clients/ldapssl/alternateservers/1/cert
 /SP/clients/ldapssl/alternateservers/1/cert
    Targets:

    Properties:
        certstatus = certificate not present
        clear_action = (none)
        issuer = (none)
        load_uri = (none)
        serial_number = (none)
        subject = (none)
        valid_from = (none)
        valid_until = (none)
        version = (none)
```

4. **Utilisez la commande `set` pour configurer les propriétés de premier niveau.**

   Par exemple :

```
-> set address=10.5.121.321
Set 'address' to 10.5.121.321
->set ...etc. for defaultrole, logdetail, port, state, strictmode,
timeout
```

5. **Utilisez la commande `set` pour charger un certificat ou modifier des propriétés.**

   Par exemple :

- **Pour charger un certificat LDAP/SSL :**

```
-> set /SP/clients/ldapssl/cert load_uri=
tftp://10.6.142.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.142.192/sales/cert.cert'
```

- **Pour charger un certificat de serveur de remplacement :**

```
-> set /SP/clients/ldapssl/alternateservers/1/cert load_uri=
tftp://10.6.142.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.142.192/sales/cert.cert'
```

- **Pour modifier les propriétés Admin Groups :**

```
-> set /SP/clients/ldapssl/admingroups/1 name=CN=
spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=
com'
```

- **Pour modifier les propriétés Operator Groups :**

```
-> set /SP/clients/ldapssl/opergroups/1 name=CN=spSuperOper,OU=
Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=
com'
```

- **Pour modifier les propriétés Custom Groups** :

---

**Remarque –** Vous pouvez définir le rôle sur un rôle individuel ou une combinaison des rôles Admin (a), User Management (u), Console (c), Reset and Host Control (r) ou Read Only (o). Les rôles hérités d'administrateur ou d'opérateur sont également pris en charge.

---

```
-> set /SP/clients/ldapssl/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=
com'
-> set /SP/clients/ldapssl/customgroups/1 roles=au
Set 'roles' to au
```

- **Pour modifier les propriétés User Domains :**

---

**Remarque –** Dans l'exemple ci-dessous, <USERNAME> représente le nom de connexion d'un utilisateur. Durant l'authentification, le nom de connexion de l'utilisateur vient remplacer <USERNAME>.

---

```
-> set /SP/clients/ldapssl/userdomains/1 name=<USERNAME>@uid=
<USERNAME>,OU=people,DC=oracle,DC=com
Set 'domain' to 'uid=<USERNAME>,OU=people,DC=oracle,DC=com'
```

- **Pour modifier les propriétés Alternate Servers :**

```
-> set /SP/clients/ldapssl/alternateservers/1 address=ip_address
```

# ▼ Configuration d'ILOM pour RADIUS

1. **Connectez-vous à la CLI d'ILOM.**
2. **Pour afficher les propriétés de RADIUS, tapez :**

   -> **show /SP/clients/radius**

   Par exemple :

```
-> show /SP/clients/radius
/SP/clients/radius
   Targets:

   Properties:
     address = 0.0.0.0
     defaultrole = Operator
     port = 1812
     secret = (none)
     state = disabled
```

3. **Utilisez la commande** `set` **pour modifier les propriétés.**

   Par exemple :

```
-> set /SP/clients/radius ipaddress=1.2.3.4 port=1812 state=
enabled defaultrole=administrator secret=changeme
```

Pour une description des paramètres RADIUS, reportez-vous à la section Configuration d'ILOM pour RADIUS, page 55.

## ▼ Se connecter à ILOM à l'aide d'un nouveau compte utilisateur

Utilisez cette procédure pour vous connecter à ILOM et vérifier que le compte utilisateur autre que `root` fonctionne correctement.

Suivez les étapes ci-dessous pour vous connecter à ILOM en tant que compte utilisateur autre que `root` :

1. **À l'aide d'une session SSH, connectez-vous à ILOM en entrant votre nom d'utilisateur et l'adresse IP du processeur de service du serveur ou du module CMM.**

   `$` **`ssh root@`***`adresse_ip_système`*

   Ou

   `$` **`ssh -l`** *nom_utilisateur adresse_ip*

   Si ILOM fonctionne dans un environnement réseau à double pile, vous pouvez entrer l'*adresse_ip_système* en utilisant un format d'adresse IPv4 ou IPv6.

   Par exemple :

   **Pour IPv4** - `10.8.183.106`

   ou

   **Pour IPv6** - `[fec0:a:8:b7:214:4fff:5eca:5f7e/64]`

   L'invite de connexion à ILOM s'affiche.

   Pour savoir comment entrer des adresses IP dans un environnement à double pile et diagnostiquer les problèmes de connexion, voir le *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager (ILOM) 3.0*.

2. **Entrez le nom d'utilisateur et le mot de passe du compte utilisateur :**

   <*nom_hôte*>: <*nom_utilisateur_assigné*>

   `Password:` <*mot de passe assigné*>

   L'invite de la CLI d'ILOM s'affiche (->).

## ▼ Se déconnecter d'ILOM

- **À l'invite de commande, tapez :**

```
-> exit
```

# Quelles sont les étapes ultérieures ?

Vous pouvez continuer à personnaliser la configuration d'ILOM pour votre système et environnement de centre de données. Avant de configurer ILOM pour votre environnement, reportez-vous au *Guide des notions fondamentales sur Oracle Integrated Lights Out Manager 3.0* pour vous faire une idée générale des nouvelles caractéristiques et fonctionnalités d'ILOM 3.0. Déterminez en quoi les fonctionnalités d'ILOM affecteront votre environnement pour configurer plus efficacement les paramètres d'ILOM et pouvoir accéder à l'ensemble de ses fonctionnalités depuis votre système et centre de données.

Reportez-vous également aux guides des procédures d'Oracle ILOM 3.0 pour savoir comment effectuer des tâches ILOM à l'aide d'une interface utilisateur spécifique et au Supplément ILOM ou au Guide d'administration correspondant à votre plate-forme pour obtenir des instructions de configuration propres à votre plate-forme.

La collection de documentation sur ILOM 3.0 est disponible à l'adresse suivante :

http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

CHAPITRE 4

# Microprogramme ILOM

**Rubriques**

| Description | Liens |
|---|---|
| Identifier la version du microprogramme ILOM | • Identification de la version du microprogramme ILOM, page 60 |
| Mettre à jour le microprogramme ILOM | • Mise à jour du microprogramme ILOM vers la dernière version, page 61 |

# Identification de la version du microprogramme ILOM

Vous pouvez facilement identifier la version du microprogramme d'ILOM active sur le processeur de service du serveur. Pour ce faire, vous devez activer le rôle Read Only (o).

## ▼ Identifier la version d'ILOM à l'aide de l'interface Web

1. **Connectez-vous à l'interface Web d'ILOM.**
2. **Sélectionnez System Information (Informations sur le système) --> Version.**

   Les informations sur la version actuelle du microprogramme s'affichent.

## ▼ Identifier la version d'ILOM à l'aide de la CLI

1. **Connectez-vous à la CLI d'ILOM.**
2. **À l'invite de commande, tapez** `version`**.**

   Les informations sur la version actuelle du microprogramme s'affichent. Par exemple :

```
SP firmware 3.0.0.1
SP firmware build number: 38000
SP firmware date: Fri Nov 28 14:03:21 EDT 2008
SP filesystem version: 0.1.22
```

# Mise à jour du microprogramme ILOM vers la dernière version

Vous pouvez utiliser l'interface Web ou la CLI d'ILOM pour mettre à jour le microprogramme ILOM. Voir :

- Mise à jour du microprogramme d'ILOM à l'aide de l'interface Web, page 62
- Mise à jour du microprogramme d'ILOM à l'aide de la CLI, page 64

## Avant de commencer

Avant d'effectuer les procédures indiquées dans cette section, les conditions suivantes doivent être remplies :

- Identifiez la version d'ILOM actuellement active sur votre système.
- Téléchargez l'image du microprogramme correspondant à votre serveur ou module CMM depuis le site Web des produits de la plate-forme Reportez-vous à la section Mise à jour du microprogramme du *Guide des procédures relatives à l'interface Web d'Oracle Integrated Lights Out Manager (ILOM) 3.0* ou du *Guide des procédures relatives à la CLI d'Oracle Integrated Lights Out Manager (ILOM) 3.0.*
- Copiez l'image du microprogramme sur un serveur à l'aide d'un protocole pris en charge (TFTP, FTP, HTTP, HTTPS). Pour effectuer une mise à jour de la CLI, copiez l'image sur un serveur local. Pour effectuer une mise à jour de l'interface Web, copiez l'image sur le système sur lequel s'exécute le navigateur Web.
- Si la plate-forme vous le demande, arrêtez le système d'exploitation de l'hôte avant de mettre à jour le microprogramme du processeur de service de votre serveur.
- Procurez-vous le nom d'utilisateur et le mot de passe ILOM disposant de privilèges de compte du rôle Admin (`a`). Vous devez disposer de privilèges Admin (`a`) pour mettre à niveau le microprogramme sur le système.
- La mise à jour du microprogramme prend environ six minutes. Pendant ce temps, n'effectuez aucune autre tâche dans ILOM. Une fois la mise à jour du microprogramme terminée, le système redémarre.

## ▼ Mise à jour du microprogramme d'ILOM à l'aide de l'interface Web

1. **Connectez-vous à l'interface Web d'ILOM en tant qu'utilisateur doté des privilèges de compte du rôle Admin (a).**
2. **Choisissez Maintenance --> Firmware Upgrade (Mise à niveau du microprogramme).**

   La page Firmware Upgrade (Mise à niveau du microprogramme) s'affiche.
3. **Dans la page Firmware Upgrade, cliquez sur Enter Upgrade Mode (Accéder au mode de mise à niveau).**

   Une boîte de dialogue Upgrade Verification (Vérification de la mise à niveau) s'affiche et indique que les autres utilisateurs connectés verront leur session se fermer une fois les processus de mise à niveau terminés.
4. **Dans la boîte de dialogue Upgrade Verification, cliquez sur OK pour continuer.**

   La page Firmware Upgrade (Mise à niveau du microprogramme) s'affiche.
5. **Dans la page Firmware Upgrade (Mise à niveau du microprogramme), procédez comme suit :**

   a. **Spécifiez l'emplacement de l'image avec l'une des méthodes suivantes :**
      - Cliquez sur **Browse (Parcourir)** pour sélectionner l'emplacement de l'image du programme que vous souhaitez installer.
      - Si votre système le permet, cliquez sur **Specify URL (Spécifier une URL)** pour entrer une URL qui localisera l'image du microprogramme. Ensuite, entrez l'URL dans la zone de texte.

   b. **Cliquez sur le bouton Upload (Télécharger) pour charger et valider le fichier.**

      Patientez jusqu'à la fin du chargement et de la validation du fichier.

      La page Firmware Verification (Vérification du microprogramme) s'affiche.
6. **Dans la page Firmware Verification, activez l'une des options suivantes :**
   - **Preserve Configuration.** Activez cette option pour enregistrer la configuration existante dans ILOM et la rétablir une fois la mise à jour terminée.
   - **Delay BIOS upgrade until next server power-off (Différer la mise à niveau BIOS jusqu'à la prochaine mise hors tension du serveur).** Activez cette option pour reporter la mise à niveau du BIOS au prochain redémarrage du système.

**Remarque –** L'invite du BIOS ne s'ouvre que sur les systèmes x86 sur lesquels la version 3.x du microprogramme ILOM est actuellement exécutée. Si vous répondez à l'invite par oui (`y`), le système reporte la mise à niveau du BIOS à son prochain redémarrage. Si vous répondez non (`n`) à l'invite, le système met à jour automatiquement le BIOS, si nécessaire, lors de la mise à jour du microprogramme du SP.

Si vous choisissez de mettre à jour le BIOS, le système remplace automatiquement les paramètres actuels du BIOS, puis assigne les paramètres par défaut de fabrique du BIOS.

7. **Cliquez sur Start Upgrade (Commencer la mise à niveau) pour lancer la mise à niveau ou sur Exit (Quitter) pour quitter le processus.**

   Lorsque vous cliquez sur Start Upgrade, le chargement commence, et une invite s'ouvre pour vous demander de poursuivre le processus.

8. **À l'invite, cliquez sur OK pour continuer.**

   La page Update Status (État de la mise à jour) s'ouvre et donne des détails sur l'avancement de la mise à jour. Lorsque l'avancement atteint 100 %, cela signifie que la mise à jour du microprogramme est terminée.

   Une fois la mise à jour terminée, le système redémarre *automatiquement* .

**Remarque –** Il arrive que l'interface Web d'ILOM ne s'actualise pas correctement une fois la mise à jour terminée. S'il manque des informations dans la page Web d'ILOM ou si cette dernière présente un message d'erreur, pensez à afficher la version mise en cache de la page entre la version précédente et la mise à jour. Effacez le cache du navigateur et actualisez ce dernier avant de poursuivre.

9. **Reconnectez-vous à l'interface Web d'ILOM à l'aide du nom d'utilisateur et du mot de passe que vous avez entrés à l'étape 1 de cette procédure.**

   Si vous n'avez pas conservé la configuration d'ILOM avant la mise à niveau du microprogramme, vous devez suivre les procédures de configuration initiale d'ILOM pour vous reconnecter à ILOM.

10. **Vérifiez que la version adéquate du microprogramme a été installée. Sélectionnez System Information (Informations sur le système) --> Version.**

    Vérifiez que la version du microprogramme sur le processeur de service ou le module CMM correspond à l'image du microprogramme que vous avez installée.

## ▼ Mise à jour du microprogramme d'ILOM à l'aide de la CLI

1. **Connectez-vous à la CLI d'ILOM en tant qu'utilisateur doté des privilèges de compte du rôle Admin (**a**).**

2. **Vérifiez que vous disposez d'une connectivité réseau pour mettre à jour le microprogramme.**

   Par exemple :

   - Pour vérifier la connectivité réseau sur un SP de serveur, tapez :

     -> **show /SP/network**

   - Pour vérifier la connectivité réseau sur un CMM, tapez :

     -> **show /CMM/network**

3. **Pour charger l'image du microprogramme ILOM, tapez la commande suivante :**

   -> **load -source**
   *<protocole_supporté>*:*//<adresse_ip_serveur>/<chemin_image_microprogramme>/<nom_fichier.xxx>*

   Vous voyez ensuite s'afficher une remarque concernant la mise à jour du microprogramme, suivie de messages vous invitant à charger l'image. Le contenu de la remarque dépend de votre plate-forme.

4. **À l'invite de chargement du fichier spécifié, tapez** y **pour oui ou** n **pour non.**

   L'invite permettant de conserver la configuration s'ouvre.

   Par exemple :
   `Do you want to preserve the configuration (y/n)?`

5. **À l'ouverture du message en question, tapez** y **pour oui ou** n **pour non.**

   Entrez y pour enregistrer votre configuration ILOM existante et la rétablir une fois la mise à jour terminée.

---

**Remarque –** Si vous entrez n à l'invite d'enregistrement de la configuration, une autre invite spécifique à la plate-forme s'ouvre.

---

6. **Effectuez l'une des opérations suivantes :**

   - Si la **version 2.x du microprogramme est installée** sur votre système, ce dernier entre dans un mode spécial permettant de charger le nouveau microprogramme. Par la suite, le système redémarrera automatiquement pour finaliser la mise à jour du microprogramme. Passez à l'étape 7.

- Si la **version 3.x du microprogramme est installée sur un système SPARC**, ce dernier entre dans un mode spécial permettant de charger le nouveau microprogramme. Par la suite, le système redémarrera automatiquement pour finaliser la mise à jour du microprogramme. Passez à l'étape 7.
- Si la version **3.x du microprogramme est installée sur un système x86**, un message vous invitant à différer la mise à jour du BIOS apparaît.

  Par exemple :

  ```
  Do you want to force the server off if BIOS needs to be upgraded
  (y/n)?
  ```

**a. À l'invite pour différer la mise à jour du BIOS, tapez `y` pour oui ou `n` pour non.**

Le système entre dans un mode spécial pour charger le nouveau microprogramme, puis le système redémarre automatiquement pour finaliser la mise à jour du microprogramme.

---

**Remarque –** L'invite du BIOS ne s'ouvre que sur les systèmes x86 sur lesquels la version 3.x du microprogramme ILOM est actuellement exécutée. Si vous répondez à l'invite par oui (`y`), le système reporte la mise à niveau du BIOS à son prochain redémarrage. Si vous répondez non (`n`) à l'invite, le système met à jour automatiquement le BIOS, si nécessaire, lors de la mise à jour du microprogramme du SP.

Si vous choisissez de mettre à jour le BIOS, le système remplace automatiquement les paramètres actuels du BIOS, puis assigne les paramètres par défaut de fabrique du BIOS.

---

**b. Passez à l'étape 7.**

**7. Reconnectez-vous au processeur de service du serveur ILOM ou au module CMM au moyen d'une connexion SSH, en utilisant le nom d'utilisateur et le mot de passe que vous avez fournis à l'étape 1 de cette procédure.**

Si vous n'avez pas conservé la configuration d'ILOM avant la mise à niveau du microprogramme, vous devez suivre les procédures de configuration initiale d'ILOM pour vous reconnecter à ILOM.

**8. Vérifiez que la version adéquate du microprogramme a été installée. À l'invite de la CLI, tapez :**

```
-> Version
```

Vérifiez que la version du microprogramme sur le processeur de service ou le module CMM correspond à l'image du microprogramme que vous avez installée.