Guide de sécurité des systèmes Oracle ILOM

Versions 3.0, 3.1 et 3.2 du microprogramme

Référence: E40358-03
Août 2014

Table des matières

Utilisation de cette documentation

- **Présentation** : le *Guide de sécurité des systèmes Oracle ILOM* fournit des instructions relatives aux tâches de sécurité Oracle ILOM que vous pouvez effectuer dans les interfaces Web et CLI. Consultez en parallèle les autres guides de la bibliothèque de documentation Oracle ILOM.
- **Public** : ce guide s'adresse aux techniciens, administrateurs système, fournisseurs de services Oracle autorisés (ASP) et utilisateurs expérimentés en matière de gestion de matériel système.
- **Connaissances requises** : expérience en matière de configuration et de gestion des serveurs Oracle.

Bibliothèque de documentation du produit

Ce guide et la documentation associée sont disponibles dans les bibliothèques de documentation Oracle ILOM à l'adresse http://www.oracle.com/goto/ILOM/docs.

Accès au support technique Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, rendez-vous sur le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou le site http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs si vous êtes malentendant.

Accès à la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Commentaires

Vous pouvez faire part de vos commentaires sur cette documentation à l'adresse suivante :

http://www.oracle.com/goto/docfeedback

Fonctions de sécurité par version du microprogramme Oracle ILOM

Le tableau suivant permet d'identifier la version du microprogramme dans laquelle une fonction de sécurité Oracle ILOM est devenue disponible.

Disponibilité de la version du microprogramme	Fonction de sécurité	Pour plus de détails, reportez-vous à :
Toutes	Authentification et autorisation	■ “Sécurisation de l'accès utilisateur à Oracle ILOM” à la page 23
Toutes	Connexion de gestion sécurisée dédiée	■ “Sécurisation de la connexion de gestion physique” à la page 13 ■ “Conservation d'une connexion de gestion sécurisée” à la page 55
Toutes	Ports réseau préconfigurés chiffrés	■ “Services et ports réseau préconfigurés” à la page 18
Toutes	Gestion sécurisée IPMI 2.0	■ “Configuration de l'accès à la gestion IPMI pour garantir une sécurité optimale” à la page 49
Toutes	Configuration de chiffrement par clé de shell sécurisé	■ “Utilisation des clés côté serveur pour le chiffrement des connexions SSH” à la page 45 ■ “Ajout de clés SSH aux comptes utilisateur pour l'authentification CLI automatisée” à la page 46
Toutes	Gestion sécurisée SNMP 3.0	■ “Configuration de l'accès à la gestion SNMP pour garantir une sécurité optimale” à la page 47
Toutes	Protocoles et certificats SSL	■ “Chargement d'un certificat SSL personnalisé et d'une clé privée dans Oracle ILOM” à la page 39 ■ “Obtention d'un certificat SSL et d'une clé privée à l'aide d'OpenSSL” à la page 37 ■ “Activation des propriétés du chiffrement SSL et TLS le plus fort” à la page 40
Toutes	Chiffrement de console distante et protocoles sécurisés	■ “Utilisation sécurisée de KVMS à distance” à la page 59
3.0.4 et versions ultérieures	Configuration du verrouillage de l'hôte KVMS	■ “Verrouillage de l'accès hôte à la déconnexion d'une session KVMS” à la page 32

Disponibilité de la version du microprogramme	Fonction de sécurité	Pour plus de détails, reportez-vous à :
3.0.4 et versions ultérieures	Configuration du délai d'expiration de la session	■ "Définition d'un intervalle d'expiration pour les sessions Web inactives" à la page 41 ■ "Définition d'un intervalle d'expiration pour les sessions CLI inactives" à la page 43
3.0.12 et versions ultérieures	Sessions authentifiées d'interconnexion de l'hôte local	■ "Accès à l'interconnexion de l'hôte authentifié préféré" à la page 56
3.0.8 et versions ultérieures	Configuration de la page de connexion	"Accès système sécurisé avec un message de connexion (3.0.8 et versions ultérieures)" à la page 34
De 3.0.8 à 3.1.2	Accès sécurisé à WS-Management	■ "Configuration de l'accès à WS-Management pour garantir une sécurité optimale" à la page 52
3.1.0 et versions ultérieures	Journal d'audit séparé	■ "Contrôle des événements d'audit pour détecter l'accès non autorisé" à la page 65
3.1.0 et versions ultérieures	Vérification de la présence de sécurité physique	■ "Présence de sécurité physique pour la réinitialisation du mot de passe par défaut de compte `root`" à la page 63
3.2.4 et versions ultérieures	Propriété configurable IPMI 1.5	■ "Configuration de l'accès à la gestion IPMI pour garantir une sécurité optimale" à la page 49
3.2.4 et versions ultérieures	Versions 1.1 et 1.2 du protocole TLS	■ "Activation des propriétés du chiffrement SSL et TLS le plus fort" à la page 40
3.2.4 et versions ultérieures	Nombre de sessions KVMS	■ "Limitation des sessions KVMS visionnables pour Remote System Console Plus (3.2.4 ou version ultérieure)" à la page 33
3.2.4 et versions ultérieures	Prise en charge du chiffrement de conformité FIPS	■ "Choix de configurer le mode FIPS au stade du déploiement" à la page 14 ■ "Fonctions non prises en charge lorsque le mode FIPS est activé" à la page 16 ■ "Considérations relatives à la protection de l'accès utilisateur après le déploiement" à la page 62

Informations de sécurité supplémentaires

Pour de plus amples informations sur la sécurisation d'Oracle ILOM, reportez-vous aux sections suivantes du guide :

- "Listes de contrôle des pratiques recommandées pour la sécurité d'Oracle ILOM"
- "Pratiques de sécurité de déploiement recommandées pour Oracle ILOM "
- "Pratiques recommandées en matière de sécurité après le déploiement d'Oracle ILOM"

Listes de contrôle des pratiques recommandées pour la sécurité d'Oracle ILOM

Oracle Integrated Lights Out Manager (ILOM) est un processeur de service (SP) préinstallé sur tous les serveurs Oracle et la plupart des serveurs Sun hérités. Les administrateurs système utilisent les interfaces utilisateur d'Oracle ILOM pour effectuer des tâches de gestion de serveurs distants, ainsi que des opérations de surveillance de l'intégrité des serveurs en temps réel.

Pour garantir l'implémentation des pratiques recommandées pour la sécurité d'Oracle ILOM dans votre environnement, les administrateurs système doivent consulter les tâches de sécurité recommandées dans les listes de contrôle suivantes :

- “Liste de contrôle de sécurité pour le déploiement de serveurs” à la page 9
- “Liste de contrôle de sécurité à utiliser au terme du déploiement du serveur” à la page 10

Informations connexes

- “Pratiques de sécurité de déploiement recommandées pour Oracle ILOM ”.
- “Pratiques recommandées en matière de sécurité après le déploiement d'Oracle ILOM”
- Fonctions de sécurité par version du microprogramme Oracle ILOM à la page 7

Liste de contrôle de sécurité pour le déploiement de serveurs

Pour déterminer les meilleures pratiques de sécurité Oracle ILOM lors de la planification du déploiement d'un nouveau serveur, les administrateurs système doivent consulter la liste des tâches de sécurité recommandées dans le Tableau 1, “Liste de contrôle - Configuration de la sécurité d'Oracle ILOM au stade du déploiement du serveur ” suivant.

TABLEAU 1 Liste de contrôle - Configuration de la sécurité d'Oracle ILOM au stade du déploiement du serveur

✓	Tâche de sécurité	Version(s) applicable(s) du microprogramme	Pour plus de détails, reportez-vous à :
	Etablir une connexion de gestion dédiée sécurisée à Oracle ILOM.	Toutes les versions du microprogramme	■ "Sécurisation de la connexion de gestion physique" à la page 13
	Décider si la conformité de sécurité FIPS 140-2 est requise ou non lors du déploiement ou après celui-ci.	Versions 3.2.4 et ultérieures du microprogramme	■ "Choix de configurer le mode FIPS au stade du déploiement" à la page 14 ■ "Fonctions non prises en charge lorsque le mode FIPS est activé" à la page 16
	Modifier le mot de passe par défaut fourni pour le compte `root` administrateur préconfiguré.	Toutes les versions du microprogramme	■ "Nécessité d'éviter la création de comptes utilisateur partagés" à la page 23 ■ "Modification du mot de passe par défaut pour le compte `root` à la première connexion" à la page 29
	Décider si les services Oracle ILOM préconfigurés et leurs ports réseau ouverts sont applicables pour votre environnement cible.	Toutes les versions du microprogramme	■ "Sécurisation des services et des ports réseau ouverts" à la page 17
	Configurer l'accès utilisateur à Oracle ILOM.	Toutes les versions du microprogramme	■ "Sécurisation de l'accès utilisateur à Oracle ILOM" à la page 23 ■ "Création de comptes utilisateur locaux disposant de privilèges basés sur les rôles" à la page 30
	Décider si l'accès au système d'exploitation hôte doit être verrouillé à la fermeture d'une session KVMS distante.	Versions 3.0.4 et ultérieures du microprogramme	■ "Verrouillage de l'accès hôte à la déconnexion d'une session KVMS" à la page 32
	Décider s'il convient de restreindre la visualisation par les autres utilisateurs du processeur de service des sessions KVMS distantes lancées depuis le processeur de service.	Versions 3.2.4 et ultérieures du microprogramme	■ "Limitation des sessions KVMS visionnables pour Remote System Console Plus (3.2.4 ou version ultérieure)" à la page 33
	Décider s'il convient d'afficher un message de sécurité lors de la connexion de l'utilisateur ou immédiatement après.	Versions 3.0.8 et ultérieures du microprogramme	■ "Accès système sécurisé avec un message de connexion (3.0.8 et versions ultérieures)" à la page 34
	Garantir que les propriétés de sécurité maximale sont définies pour toutes les interfaces utilisateur Oracle ILOM.	Toutes les versions du microprogramme	■ "Configuration des interfaces d'Oracle ILOM pour une sécurité optimale" à la page 36

Liste de contrôle de sécurité à utiliser au terme du déploiement du serveur

Pour déterminer les meilleures pratiques de sécurité Oracle ILOM à conserver sur les serveurs existants de votre environnement, les administrateurs système doivent consulter la liste des tâches de sécurité recommandées dans le Tableau 2, "Liste de contrôle - Gestion de la sécurité d'Oracle ILOM au terme du déploiement " suivant.

TABLEAU 2 Liste de contrôle - Gestion de la sécurité d'Oracle ILOM au terme du déploiement

✓	**Tâche de sécurité**	**Version(s) applicable(s) du microprogramme**	**Pour plus de détails, reportez-vous à :**
	Conserver une connexion de gestion sécurisée dans Oracle ILOM	Toutes les versions du microprogramme	■ “Eviter l'accès à un périphérique KCS hôte non authentifié” à la page 56 ■ “Accès à l'interconnexion de l'hôte authentifié préféré” à la page 56 ■ “Création d'un canal sécurisé à l'aide du chiffrement IPMI 2.0” à la page 57
	Garantir que les sessions en mode texte série et KVMS à distance sont lancées de manière sécurisée depuis Oracle ILOM.	Toutes les versions du microprogramme	■ “Chiffrement et communication à distance KVMS” à la page 59 ■ “Protection contre l'accès partagé KVMS à distance” à la page 60 ■ “Protection contre l'accès partagé à la console série hôte” à la page 61
	Gérer et effectuer le suivi de l'accès utilisateur à Oracle ILOM.	Toutes les versions du microprogramme	■ “Considérations relatives à la protection de l'accès utilisateur après le déploiement” à la page 62
	Actions de sécurité requises pour la réinitialisation d'un mot de passe perdu pour le compte `root` administrateur préconfiguré.	Versions 4.5 et ultérieures du microprogramme	■ “Présence de sécurité physique pour la réinitialisation du mot de passe par défaut de compte `root`” à la page 63
	Actions de sécurité requises si le mode de conformité FIPS 140-2 doit être modifié dans Oracle ILOM après le déploiement du serveur.	Versions 3.2.4 et ultérieures du microprogramme	■ “Modification du mode FIPS après le déploiement” à la page 66 ■ “Fonctions non prises en charge lorsque le mode FIPS est activé” à la page 16
	Garantir que le logiciel et le microprogramme sont à jour sur le serveur.	Toutes les versions du microprogramme	■ “Mise à jour des logiciels et microprogrammes” à la page 68

Pratiques de sécurité de déploiement recommandées pour Oracle ILOM

Les rubriques suivantes vous permettent de déterminer les pratiques de sécurité Oracle ILOM recommandées à mettre en oeuvre lors du déploiement d'un serveur.

Informations connexes

- “Listes de contrôle des pratiques recommandées pour la sécurité d'Oracle ILOM”.
- “Pratiques recommandées en matière de sécurité après le déploiement d'Oracle ILOM”
- Fonctions de sécurité par version du microprogramme Oracle ILOM à la page 7

Sécurisation de la connexion de gestion physique

Oracle ILOM est un outil de gestion out-of-band (OOB, ou hors bande) qui utilise un canal de gestion dédié au maintien et au contrôle des serveurs Oracle. Contrairement aux outils de gestion in-band, les serveurs Oracle sont fournis avec des fonctions intégrées de gestion à distance qui permettent aux administrateurs système de bénéficier d'un accès sécurisé à Oracle ILOM via un connecteur réseau distinct sur le processeur de service. Alors que les fonctions de gestion d'Oracle ILOM offrent aux administrateurs système des capacités spécifiques pour le contrôle et la gestion des serveurs Oracle, Oracle ILOM n'est pas conçu pour être un moteur de calcul général, ni pour autoriser l'accès à une connexion réseau non sécurisée.

Que vous établissiez ou non une connexion de gestion physique à Oracle ILOM via le port série local, le port de gestion réseau sécurisé ou le port réseau de données standard, il est essentiel que ce port physique sur le serveur ou ce module de contrôle de châssis (CMM) soit toujours connecté à un réseau interne de confiance, à un réseau de gestion sécurisé dédié ou à un réseau privé. Pour plus d'informations sur l'établissement d'une connexion de gestion physique à Oracle ILOM, reportez-vous au tableau suivant :

Connexion de gestion de port physique à Oracle ILOM	Matériel Oracle pris en charge	Consignes de sécurité pour la connexion de gestion
Connexion dédiée	■ Serveur (Port : NET MGT) ■ CMM (Port: NET MGT)	Installez le processeur de service (SP) sur un réseau interne dédié afin de le séparer du trafic du réseau de données général. Pour plus d'informations sur l'établissement d'une connexion de gestion réseau dédiée à Oracle ILOM, reportez-vous à la section ■ Connexion de gestion réseau dédiée, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (3.2.x)*
Connexion locale	■ Serveur (Port : SER MGT) ■ CMM (Port: SER MGT)	Utilisez une connexion de gestion série locale pour accéder à Oracle ILOM directement à partir du serveur physique ou du CMM. Pour plus d'informations sur l'établissement d'une connexion de gestion série locale à Oracle ILOM, reportez-vous à la section : ■ Connexion de gestion série locale à Oracle ILOM, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (3.2.x)*
Connexion sideband	Serveur (Ports : NET0, NET1, NET2, NET3)	Dans la mesure où cela ne nécessite pas deux connexions réseau distinctes, utilisez un réseau de données Ethernet partagé pour accéder au processeur de service (SP) lorsque cela est nécessaire afin de simplifier la gestion des câbles et la configuration réseau. Pour plus d'informations sur l'établissement d'une connexion de gestion sideband à Oracle ILOM, reportez-vous à la section ■ Connexion de gestion sideband, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (3.2.x)* **Remarque -** La gestion sideband est prise en charge sur la plupart des serveurs Oracle.

Remarque - Afin de vous protéger contre les attaques, **ne connectez jamais le processeur de service Oracle ILOM à un réseau public** , tel qu'Internet. Nous vous recommandons de conserver le trafic de gestion du processeur de service Oracle ILOM sur un réseau de gestion distinct et d'en donner l'accès uniquement aux administrateurs système.

Choix de configurer le mode FIPS au stade du déploiement

A partir de la version 3.2.4 du microprogramme Oracle ILOM, l'interface de ligne de commande et l'interface Web d'Oracle ILOM CLI fournissent un mode configurable pour la conformité FIPS (Federal Information Processing Standards). Lorsque ce mode est activé, Oracle utilise des algorithmes cryptographiques en conformité avec les normes de sécurité FIPS 140-2 pour protéger les données sensibles et importantes des systèmes.

Les administrateurs déployant des serveurs avec la version 3.2.4 ou ultérieure du microprogramme doivent décider s'il convient de configurer le mode FIPS avant les autres

propriétés d'Oracle ILOM. Le mode de conformité FIPS est désactivé par défaut dans Oracle ILOM. En cas de modification du mode de conformité FIPS, les valeurs par défaut de toutes les données de configuration sont rétablies.

Pour activer le mode de conformité FIPS au stade du déploiement (avant de configurer les propriétés Oracle ILOM), reportez-vous à la section “Activation du mode FIPS au stade du déploiement” à la page 15. Si les propriétés de configuration définies par l'utilisateur ont déjà été définies dans Oracle ILOM et si vous avez besoin de modifier la propriété FIPS, reportez-vous à la section “Actions pour la modification du mode FIPS après le déploiement” à la page 66.

▼ Activation du mode FIPS au stade du déploiement

Remarque - Dans Oracle ILOM, le mode de conformité FIPS est représenté par les propriétés State (Etat) et Status (Statut). Les propriétés State et Status représentent respectivement le mode configuré et le mode opérationnel dans Oracle ILOM. En cas de modification de la propriété State FIPS, le mode opérationnel (propriété Status FIPS) reste inchangé jusqu'à la prochaine réinitialisation d'Oracle ILOM.

Avant de commencer

- Par défaut, les propriétés State et Status FIPS sont désactivées.
- Si FIPS est activé (configuré et opérationnel), certaines fonctionnalités dans Oracle ILOM ne sont pas prises en charge. Pour obtenir la liste des fonctionnalités qui ne sont pas prises en charge lorsque FIPS est activé, reportez-vous au Tableau 3, “Fonctions non prises en charge dans Oracle ILOM lorsque le mode FIPS est activé”.
- Il faut disposer du rôle Admin (a) pour modifier la propriété State FIPS.
- La propriété configurable pour la conformité FIPS est disponible dans Oracle LOM à partir de la version 3.2.4 du microprogramme. Dans les versions du microprogramme antérieures à la version 3.2.4, Oracle ILOM ne fournit pas de propriété configurable pour la conformité FIPS.
- En cas de modification des propriétés State et Status du mode FIPS dans Oracle ILOM, les valeurs par défaut de tous les paramètres de configuration définis par l'utilisateur sont rétablies.

1. **Dans l'interface Web d'Oracle ILOM, cliquez sur ILOM Administration (Administration ILOM) -> Management Access (Accès à la gestion) -> FIPS.**
2. **Sur la page FIPS, suivez les étapes ci-dessous :**
   a. **Cochez la case FIPS State pour activer la propriété FIPS configurée.**

b. Cliquez sur Save (Enregistrer) pour appliquer la modification.

Pour plus d'informations sur la configuration, cliquez sur le lien `More details` (Plus de détails) de la page Web FIPS.

3. Pour modifier le statut du mode opérationnel FIPS dans Oracle ILOM, effectuez les étapes suivantes pour réinitialiser Oracle ILOM.

a. Dans l'interface Web, cliquez sur ILOM Administration (Administration ILOM) -> Maintenance -> SP Reset (Réinitialisation du SP).

b. Dans la page SP Reset, cliquez sur le bouton SP Reset.

Lors de la réinitialisation d'Oracle ILOM, les actions suivantes se produisent :

- Le dernier état FIPS (activé) est appliqué au système.
- Les valeurs par défaut de tous les paramètres de configuration définis par l'utilisateur dans Oracle ILOM sont rétablies.
- La propriété Status FIPS est mise à jour pour refléter l'état opérationnel activé en cours dans Oracle ILOM.

  Pour une liste et une description complètes des messages Status FIPS, cliquez sur le lien `More details` (Plus de détails) de la page FIPS.
- Une icône de bouclier FIPS s'affiche dans la zone de cadre masthead de l'interface Web.
- Toutes les fonctions FIPS non prises en charge sont désactivées ou supprimées de la CLI et de l'interface Web.

  Pour une liste et une description complètes des fonctions FIPS non prises en charge, cliquez sur le lien `More details` (Plus de détails) de la page FIPS.

Informations connexes

- “Fonctions non prises en charge lorsque le mode FIPS est activé” à la page 16
- “Actions pour la modification du mode FIPS après le déploiement” à la page 66
- Configuration des propriétés du mode FIPS, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (3.2.x).*

Fonctions non prises en charge lorsque le mode FIPS est activé

Lorsque la conformité FIPS est activée dans Oracle ILOM, les fonctions FIPS 140-2 non conformes suivantes ne sont pas prises en charge dans Oracle ILOM.

TABLEAU 3 Fonctions non prises en charge dans Oracle ILOM lorsque le mode FIPS est activé

Fonction du mode FIPS non prise en charge	Description
IPMI 1.5	Lorsque le mode FIPS est activé et en cours d'exécution sur le système, la propriété de configuration IPMI 1.5 est supprimée de la CLI et de l'interface Web d'Oracle ILOM. Le service IPMI 2.0 est automatiquement activé dans Oracle ILOM. IPMI 2.0 prend en charge à la fois les modes conformes et les modes non conformes à la norme FIPS.
Compatibilité du microprogramme pour Oracle ILOM System Remote Console	Dans Oracle ILOM, le mode FIPS empêche les versions antérieures du microprogramme d'Oracle ILOM Remote System Console d'être compatibles avec les versions ultérieures du microprogramme Oracle ILOM Remote System Console. Par exemple, la version 3.2.4 du microprogramme client Oracle ILOM Remote System Console est compatible avec les versions 3.2.3 et antérieures du microprogramme Oracle ILOM Remote System Console. Toutefois, les versions 3.2.2 et antérieures du microprogramme client Oracle ILOM Remote System Console ne sont pas compatibles avec les versions 3.2.4 et ultérieures du microprogramme Oracle ILOM Remote System Console. **Remarque -** Cette limite de compatibilité du microprogramme ne s'applique pas à Oracle ILOM Remote System Console Plus. Oracle ILOM Remote System Console Plus est fourni sur les systèmes de processeur de service plus récents tels que SPARC T5 et systèmes ultérieurs, et Oracle Server x4-4, x4-8 et systèmes ultérieurs. Oracle ILOM Remote System Console est fourni sur les systèmes de processeur de service plus anciens tels que SPARC T3 et T4 et Sun Server x4-2/2L/2B et systèmes antérieurs.
Lightweight Directory Access Protocol (LDAP)	Lorsque le mode FIPS est activé et en cours d'exécution sur le système, les propriétés de configuration LDAP dans Oracle ILOM sont automatiquement supprimées de la CLI et de l'interface Web d'Oracle ILOM. **Remarque -** Les services d'authentification à distance suivants sont pris en charge dans les modes conformes et non conformes à la norme FIPS : Active Directory et LDAP/SSL.
RADIUS (Remote Authentication Dial In User Service)	Lorsque le mode FIPS est activé et en cours d'exécution sur le système, les propriétés de configuration RADIUS dans Oracle ILOM sont automatiquement supprimées de la CLI et de l'interface Web d'Oracle ILOM. **Remarque -** Les services d'authentification à distance suivants sont pris en charge dans les modes conformes et non conformes à la norme FIPS : Active Directory et LDAP/SSL.
Protocole simplifié de gestion de réseau (SNMP) DES et MD5	Lorsque le mode FIPS est activé et en cours d'exécution sur le système, les propriétés de configuration SNMP pour le protocole de confidentialité DES et le protocole d'authentification MD5 ne sont pas prises en charge dans la CLI et l'interface Web d'Oracle ILOM.

Sécurisation des services et des ports réseau ouverts

Pour garantir que les services et leurs ports réseau respectifs sont correctement configurés dans Oracle ILOM, consultez les rubriques suivantes :

- “Services et ports réseau préconfigurés” à la page 18
- “Gestion des services et ports ouverts indésirables” à la page 18
- “Configuration des services et ports réseaux” à la page 20

Services et ports réseau préconfigurés

Oracle ILOM est préconfiguré avec la plupart des services activés par défaut. Cela facilite grandement son déploiement. Cela étant, chaque port réseau de service ouvert du serveur représente un point d'entrée potentiel pour un utilisateur malveillant. Il est donc important de connaître les paramètres Oracle ILOM initiaux ainsi que leurs objectifs et de déterminer les services absolument nécessaires au système déployé. Pour une sécurité accrue, activez uniquement les services requis par Oracle ILOM.

Le tableau suivant répertorie les services activés par défaut avec Oracle ILOM.

TABLEAU 4 Services et ports activés par défaut

Service	Port(s)
Redirection HTTP vers HTTPS	80
HTTPS	443
IPMI	623
KVMS à distance pour Oracle ILOM Remote Console	5120, 5121, 5122, 5123, 5555, 5556, 7578, 7579
KVMS à distance pour Oracle ILOM Remote Console Plus	5120, 5555
Service Tag	6481
SNMP	161
Connexion unique	11626
SSH	22

Le tableau suivant répertorie les services désactivés par défaut avec Oracle ILOM.

TABLEAU 5 Services et ports désactivés par défaut

Service	Port(s)
HTTP	80

Gestion des services et ports ouverts indésirables

Il est possible de désactiver chacun des services Oracle ILOM, ce qui a pour effet de fermer les ports réseau correspondants. La plupart des services sont activés par défaut, mais vous souhaiterez sans doute en désactiver certains ou modifier les paramètres par défaut pour renforcer la sécurité de l'environnement Oracle ILOM. N'importe quel service Oracle ILOM peut être désactivé, mais cette opération réduit l'étendue des fonctionnalités disponibles. La

règle d'or consiste à activer uniquement les services indispensables dans l'environnement déployé. Il faut mettre en balance la perte de certaines fonctionnalités et les avantages que présente l'activation d'un nombre réduit de services en matière de sécurité.

Le tableau suivant décrit l'impact de l'activation ou de la désactivation de chaque service.

TABLEAU 6 Services à l'état désactivé

Service	Description	Résultat de l'activation/la désactivation
HTTP	Protocole non chiffré permettant d'accéder à l'interface Web d'Oracle ILOM	L'activation de ce service assure de meilleures performances en matière de vitesse que le protocole HTTP chiffré (HTTPS). Cependant, l'utilisation de ce protocole peut entraîner l'envoi d'informations sensibles non chiffrées via Internet.
HTTPS	Protocole chiffré permettant d'accéder à l'interface Web d'Oracle ILOM	L'activation de ce service garantit des communications sécurisées entre un navigateur Web et Oracle ILOM. Cependant, dans la mesure où il nécessite l'ouverture d'un port réseau sur Oracle ILOM, il accroît la vulnérabilité, ce qui peut conduire à un déni de service.
Servicetag	Protocole de découverte Oracle permettant d'identifier les serveurs et de faciliter les demandes de service	La désactivation de ce service empêche Oracle Enterprise Manager Ops Center de détecter Oracle ILOM, ce qui bloque l'intégration à d'autres solutions de services automatiques Oracle. L'état Servicetag est configurable uniquement à partir de la CLI d'Oracle ILOM. Par exemple, pour modifier la propriété de l'état servicetag, tapez : `set /SP/services/servicetag state=`*enabled*`|`*disabled*
IPMI	Protocole de gestion standard	La désactivation de ce service peut empêcher Oracle Enterprise Manager Ops Center, ainsi que certains connecteurs de gestion Oracle à des logiciels tiers, de gérer le système.
SNMP	Protocole de gestion standard permettant de surveiller l'état d'Oracle ILOM et de contrôler les notifications de déroutement	La désactivation de ce service peut empêcher Oracle Enterprise Manager Ops Center, ainsi que certains connecteurs de gestion Oracle à des logiciels tiers, de gérer le système.
KVMS	Ensemble de protocoles permettant de fournir un clavier, une sortie vidéo, une souris et une unité de stockage à distance	La désactivation de ce service rend indisponibles la console hôte et le stockage à distance, ce qui empêche l'utilisation des applications Oracle ILOM Remote Console et Storage Redirection CLI.
SSH	Protocole sécurisé permettant d'accéder à un shell distant	La désactivation de ce service interdit l'accès à la ligne de commande sur le réseau et peut empêcher Oracle Enterprise Manager Ops Center de détecter Oracle ILOM.
SSO	Fonction de connexion unique permettant de réduire le nombre de saisies des nom et mot de passe utilisateur	La désactivation de ce service empêche le lancement de KVMS sans saisir à nouveau le mot de passe, mais autorise la navigation d'un module de contrôle de châssis (CMM) à un SP de lame sans saisir à nouveau le mot de passe.

Pour des informations sur l'activation et la désactivation de services réseau individuels, reportez-vous à la section “Configuration des services et ports réseaux” à la page 20 ci-après.

Configuration des services et ports réseaux

Pour obtenir des instructions sur la configuration des services de gestion et leurs ports réseau respectifs dans Oracle ILOM, reportez-vous aux procédures suivantes.

Vous pouvez désactiver ou activer les services et leurs ports réseau respectifs à l'aide de l'interface de ligne de commande ou de l'interface Web d'Oracle ILOM. Les procédures décrites dans cette section fournissent des instructions de navigation Web pour toutes les versions du microprogramme Oracle ILOM. Pour des instructions sur la CLI ou des informations supplémentaires sur les propriétés de configuration, reportez-vous à la documentation appropriée répertoriée à la section Informations connexes qui suit chaque procédure.

▼ Modification des états et ports de service de gestion de protocole

Avant de commencer

Avant de commencer

- Passez en revue les tableaux suivants pour déterminer quels services de protocole et ports réseau sont activés ou désactivés par défaut dans Oracle ILOM.
  - Tableau 4, “Services et ports activés par défaut”
  - Tableau 5, “Services et ports désactivés par défaut”
- Il faut disposer du rôle Admin (a) dans Oracle ILOM pour modifier la propriété State des services de protocole.

Suivez la procédure ci-après pour modifier la propriété State d'un service réseau.

1. **Accédez aux services Management Access de l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur Configuration --> System Management Access (Accès à la gestion système).**
   - **Dans l'interface Web 3.1 et version ultérieure, cliquez sur ILOM Administration (Administration ILOM) -> Management Access (Accès à la gestion).**

2. **Dans Management Access, cliquez sur l'un des onglets de service répertoriés ci-dessous :**

Management Access ->	Description
Web Server	Utilisez la page Web Server (Serveur Web) pour gérer l'état de service et les assignations de port pour l'accès à la gestion des protocoles HTTP et HTTPS.
IPMI	Utilisez la page IPMI pour gérer les propriétés d'état de service et de port pour l'accès à la gestion du protocole IPMI.
SNMP	Utilisez la page SNMP pour gérer les propriétés d'état de service et de port pour l'accès à la gestion SNMP.
SSH	Utilisez la page SSH pour gérer la propriété d'état de service pour l'accès à la gestion de shell sécurisé.

3. **Modifiez la propriété State dans Management Access -> la page de service, puis cliquez sur Save (Enregistrer) pour appliquer la modification.**

Notez que la désactivation de la propriété State d'un service de protocole entraîne la fermeture du port réseau de service de protocole respectif et empêche l'utilisation du service de protocole avec Oracle ILOM.

Informations connexes

- Services de gestion et propriétés réseau par défaut, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*.
- Services de gestion et propriétés réseau par défaut, *Guide de configuration et de maintenance d'Oracle ILOM 3.1* .
- Configuration des paramètres réseau, *Guide des procédures relatives à la CLI d'Oracle ILOM 3.0*
- Configuration des paramètres réseau, *Procédures relatives à l'interface Web d'Oracle ILOM 3.0*

▼ Modification de l'état du service KVMS et des ports

Avant de commencer

Avant de commencer

- Dans Oracle ILOM, la propriété State du service KVMS est activée par défaut. Pour une liste des ports réseau ouverts associés au service KVMS, reportez-vous au Tableau 4, “Services et ports activés par défaut”.
- Il faut disposer du rôle Admin (a) pour modifier la propriété State KVMS dans Oracle ILOM.

1. **Accédez à l'onglet KVMS dans l'interface Web d'Oracle ILOM.**

Par exemple :

- **Dans l'interface Web 3.0.x, cliquez sur Remote Control (Contrôle à distance) --> KVMS.**

- **Dans l'interface Web 3.1 et version ultérieure, cliquez sur Remote Console (Contrôle à distance) --> KVMS.**

2. **Dans l'onglet KVMS, modifiez la propriété State KVMS, puis cliquez sur Save pour appliquer la modification.**

   Notez que la désactivation de la propriété State entraîne la fermeture du service KVMS ouvert correspondant, ce qui empêche d'utiliser : a) la console hôte distante et b) Oracle ILOM Remote Console et la CLI d'Oracle ILOM Remote Storage ; ou Oracle ILOM Remote Console Plus.

Informations connexes

- Configuration des paramètres KVMS du client local, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Configuration des paramètres KVMS du client local, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*
- Tâches de configuration initiale, *Guide de la CLI et de l'interface Web des consoles de redirection à distance Oracle ILOM 3.0*

▼ Modification de l'état et du port du service Single Sign-On

Avant de commencer

Avant de commencer

- Dans Oracle ILOM, la propriété State du service Single Sign-On (SSO) et le port réseau correspondant (1126) sont activés par défaut.
- Il faut disposer du rôle Admin (a) dans Oracle ILOM pour modifier la propriété State du service SSO.

1. **Accédez à l'onglet User Account (Compte utilisateur) dans l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, choisissez User Management (Gestion des utilisateurs) --> User Account (Compte utilisateur).**

   - **Dans l'interface Web 3.1 et version ultérieure, cliquez sur ILOM Administration (Administration ILOM) -> User Account (Compte utilisateur).**

2. **Dans l'onglet User Account, modifiez la propriété State du service SSO, puis cliquez sur Save (Enregistrer) pour appliquer la modification.**

   Notez que la désactivation de la propriété State du service SSO dans Oracle ILOM a les effets suivants : a) fermeture du port réseau SSO ouvert ; b) invitation des utilisateurs à saisir de nouveau leur mot de passe au lancement d'une console KVMS ; et c) autorisation des utilisateurs CMM à accéder à un SP de serveur lame sans devoir saisir de nouveau le mot de passe.

Informations connexes

- Service Single Sign-On, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Service Single Sign-On, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*
- Configuration de Single Sign-On, *Guide des procédures relatives à la CLI d'Oracle ILOM 3.0*
- Configuration de Single Sign-On, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*

Sécurisation de l'accès utilisateur à Oracle ILOM

Pour sécuriser l'accès utilisateur dans Oracle ILOM, consultez les rubriques suivantes :

Nécessité d'éviter la création de comptes utilisateur partagés

Conservez un environnement sécurisé en évitant de créer des comptes partagés. Il s'agit de comptes utilisateur partageant le même mot de passe. Plutôt que de créer des comptes partagés pour gérer les comptes utilisateur, mieux vaut associer un mot de passe unique à chacun des utilisateurs qui ont accès à Oracle ILOM. Assurez-vous que chaque combinaison de compte utilisateur et de mot de passe n'est connue que par un seul utilisateur.

Remarque - Oracle ILOM prend en charge 10 comptes utilisateur locaux. Si un nombre plus important d'utilisateurs doivent accéder à Oracle ILOM, vous pouvez configurer des services d'annuaire, comme LDAP ou Active Directory, pour prendre en charge davantage de comptes à l'aide d'une base de données centralisée. Pour plus d'informations, reportez-vous à la section “Services d'authentification à distance et profils de sécurité” à la page 27.

Une fois des mots de passe uniques définis pour les comptes utilisateur individuels, l'administrateur système doit s'assurer qu'un mot de passe unique a été assigné au compte `root` Administrateur préconfiguré. Sinon, sans mot de passe unique, le compte `root` Administrateur préconfiguré est considéré comme un compte partagé. Pour s'assurer que les utilisateurs non autorisés n'utilisent pas le compte `root` Administrateur préconfiguré, vous devez modifier le mot de passe ou supprimer le compte `root` préconfiguré d'Oracle ILOM. Pour plus d'informations sur le compte `root` Administrateur préconfiguré, reportez-vous à la section “Modification du mot de passe par défaut pour le compte `root` à la première connexion” à la page 29.

Pour plus d'informations sur la création de comptes sécurisés associés à des mots de passe uniques, reportez-vous à la section “Directives de sécurité relatives à la gestion des comptes utilisateur et des mots de passe” à la page 25.

Pour des informations sur la configuration de comptes utilisateur, reportez-vous à la section “Configuration de l'accès utilisateur pour une sécurité maximale” à la page 28.

Affectation de privilèges basés sur les rôles

Tous les comptes utilisateur Oracle ILOM disposent d'un ensemble de privilèges basés sur les rôles. Ces privilèges basés sur les rôles permettent d'accéder à des fonctions discrètes au sein d'Oracle ILOM. Il est possible de définir un compte pour que l'utilisateur puisse surveiller le système sans pouvoir apporter de modifications à la configuration. Vous pouvez également autoriser un utilisateur à modifier la plupart des options de configuration, mais pas à créer ni modifier de comptes utilisateur. D'autre part, il est possible de restreindre le contrôle de l'alimentation du serveur et l'accès à la console distante. Il est important de comprendre les niveaux de privilèges et de les accorder avec discernement aux utilisateurs de l'organisation.

Le tableau suivant répertorie les privilèges que vous pouvez assigner à un compte utilisateur Oracle ILOM.

TABLEAU 7 Descriptions des privilèges de compte utilisateur

Rôle	Description
`Admin` (a)	Ce rôle permet de modifier toutes les options de configuration d'Oracle ILOM, à l'exception des options expressément autorisées par d'autres privilèges (gestion des utilisateurs, par exemple).

Rôle	Description
`User Management` (`u`)	Ce rôle permet d'ajouter et de supprimer des utilisateurs, de modifier des mots de passe et de configurer des services d'authentification. Dans la mesure où il autorise la création d'un deuxième compte utilisateur disposant de tous les privilèges, ce rôle détient le plus haut niveau de privilèges.
`Console` (`c`)	Ce rôle permet d'accéder à la console hôte à distance. Cet accès à la console à distance peut permettre à l'utilisateur d'accéder au BIOS ou à OpenBoot PROM (OBP), qui lui donne la possibilité de modifier le comportement d'initialisation de façon à pouvoir accéder au système.
`Reset and Host Control` (`r`)	Ce rôle permet de contrôler l'alimentation de l'hôte et de réinitialiser Oracle ILOM.
`Read-only` (`o`)	Ce rôle permet d'accéder aux interfaces utilisateur d'Oracle ILOM en lecture seule. Tous les utilisateurs disposent de ce privilège, qui les autorise à consulter les journaux, les informations relatives à l'environnement et les paramètres de configuration.

Pour plus d'informations sur la création d'un compte utilisateur local et l'assignation de privilèges basés sur les rôles, reportez-vous à la section “Création de comptes utilisateur locaux disposant de privilèges basés sur les rôles” à la page 30.

Directives de sécurité relatives à la gestion des comptes utilisateur et des mots de passe

Prenez en compte les directives de sécurité suivantes pour la gestion des comptes utilisateur et des mots de passe Oracle ILOM :

Directives relatives à la gestion des comptes utilisateur

Directive relative à la gestion des comptes utilisateur	Description
N'encouragez jamais le partage des comptes utilisateur	Chaque utilisateur d'Oracle ILOM doit disposer d'un compte utilisateur distinct. Oracle ILOM prend en charge jusqu'à 10 comptes utilisateur locaux. Si vous gérez un grand site et que vous avez besoin de plus de 10 comptes utilisateur, utilisez un service d'authentification tiers tel que LDAP ou Active Directory. Pour plus d'informations sur l'utilisation de l'authentification des utilisateurs dans Oracle ILOM via un service d'authentification externe, reportez-vous à la section “Services d'authentification à distance et profils de sécurité” à la page 27.
Sélectionnez des noms adéquats pour les comptes utilisateur locaux	Lorsque vous sélectionnez un nom d'utilisateur pour un compte utilisateur Oracle ILOM local, le nom d'utilisateur doit :

Directive relative à la gestion des comptes utilisateur	Description
	■ Contenir entre 4 et 16 caractères, le premier devant être une lettre. ■ Etre unique dans votre organisation ■ Ne contenir aucun espace, point (.) ou deux points (:)
Sélectionnez des mots de passe adéquats pour les comptes utilisateur locaux	Lorsque vous sélectionnez un mot de passe pour un compte utilisateur Oracle ILOM local, le mot de passe doit : ■ toujours être un mot de passe complexe contenant jusqu'à 16 caractères. ■ contenir des minuscules et des majuscules, ainsi qu'un ou plusieurs caractères spéciaux afin de former un mot de passe complexe. ■ ne contenir aucun espace, point (.) ou deux points (:). ■ être conforme à la politique de gestion des mots de passe de votre entreprise. Pour plus d'informations sur la gestion des mots de passe dans Oracle ILOM, reportez-vous à la section “Directives de sécurité relatives à la gestion des comptes utilisateur et des mots de passe” à la page 25.
Limitez les privilèges des comptes utilisateur selon le rôle des utilisateurs (*Principe du moindre privilège*)	Le principe du moindre privilège établit que, par souci de sécurité, il faut octroyer à un utilisateur le minimum de droits possibles pour pouvoir effectuer son travail. L'octroi excessif de responsabilités, de rôles, etc. (particulièrement au début du cycle de vie d'une organisation) peut entraîner des risques d'accès non autorisé au système. Revoyez régulièrement les privilèges utilisateur pour déterminer la pertinence des responsabilités actuelles de chaque utilisateur. Oracle ILOM permet de contrôler les privilèges de chaque utilisateur. Veillez à accorder les droits adéquats à chaque utilisateur selon sa fonction au sein de la société. Pour des informations sur la création d'un compte utilisateur disposant de privilèges basés sur le rôle, reportez-vous à la section “Création de comptes utilisateur locaux disposant de privilèges basés sur les rôles” à la page 30

Directives sur la gestion des mots de passe

Directive sur la gestion des mots de passe	Description
Modifiez le mot de passe par défaut (`changeme`) immédiatement après la connexion initiale	Pour permettre une première connexion et un premier accès à Oracle ILOM, un compte administrateur `root` est fourni avec le système. Pour créer un environnement sécurisé, vous devez modifier le mot de passe administrateur fourni (`changeme`) après votre première connexion à Oracle ILOM. Si une personne non autorisée parvient à se connecter au compte `root` administrateur, elle dispose d'un accès illimité à toutes les fonctions d'Oracle ILOM. Il est donc essentiel de définir un mot de passe fiable et sécurisé.
Changez régulièrement tous les mots de passe de compte Oracle ILOM	Afin d'empêcher toute activité malveillante et de garantir que les mots de passe restent conformes aux politiques relatives aux mots de passe actuelles, modifiez régulièrement tous les mots de passe pour Oracle ILOM.
Mettez en place des pratiques courantes afin de créer des mots de passe complexes	Mettez en place les pratiques courantes suivantes afin de créer des mots de passe complexes : ■ N'utilisez jamais moins de 16 caractères pour votre mot de passe.

Directive sur la gestion des mots de passe	Description
	■ N'utilisez pas de mot de passe contenant le nom de l'utilisateur, le nom de l'employé ou les noms des membres de sa famille. ■ N'utilisez pas de mots de passe trop faciles à deviner. ■ N'utilisez pas de suite de chiffres consécutifs telle que 12345. ■ N'utilisez pas de mots de passe contenant un mot ou une chaîne facile à deviner grâce à une simple recherche sur Internet. ■ N'autorisez pas les utilisateurs à réutiliser le même mot de passe sur plusieurs systèmes. ■ N'autorisez pas les utilisateurs à réutiliser des mots de passe déjà utilisés.
Contactez votre responsable de la sécurité informatique pour connaître les politiques relatives aux mots de passe	Contactez votre responsable de la sécurité informatique pour vous assurer que les mots de passe répondent aux exigences et aux politiques de votre entreprise concernant la gestion des mots de passe.

Services d'authentification à distance et profils de sécurité

Il est possible de configurer Oracle ILOM pour gérer une base d'utilisateurs centralisée externe plutôt que de définir des utilisateurs locaux sur chaque instance d'Oracle ILOM. Cette opération présente un double avantage : les administrateurs peuvent créer et modifier les informations d'identification des utilisateurs de manière centralisée, et les utilisateurs peuvent accéder à différents systèmes.

Avant de choisir et de configurer un service d'authentification, prenez soin de comprendre le mode de fonctionnement de chacun des services présentés, ainsi que leurs exigences en matière de configuration. Outre l'authentification, chaque service pris en charge permet de configurer des règles d'autorisation qui définissent l'attribution de privilèges Oracle ILOM à un utilisateur distant. Veillez à attribuer les privilèges ou rôles utilisateur à bon escient.

Le tableau suivant répertorie les services d'authentification des utilisateurs pris en charge par Oracle ILOM.

TABLEAU 8 Services d'authentification à distance et profils de sécurité

Nom du service	Profil de sécurité	Informations
Active Directory	Elevé	■ Ce service est sécurisé par défaut. ■ L'activation d'un mode de certification strict nécessite un serveur de certificats mais ajoute une couche supplémentaire de sécurité.
LDAP/SSL (Lightweight Directory Access Protocol/ Secure Socket Layer)	Elevé	■ Ce service est sécurisé par défaut. ■ L'activation d'un mode de certification strict nécessite un serveur de certificats mais ajoute une couche supplémentaire de sécurité.
LDAP propriétaire	Faible	■ Activez ce service sur des réseaux sécurisés privés exempts d'utilisateurs potentiellement malveillants.

Nom du service	Profil de sécurité	Informations
RADIUS (Remote Authentication Dial In User Service)	Faible	■ Activez ce service sur des réseaux sécurisés privés exempts d'utilisateurs potentiellement malveillants.

Les services dotés d'un profil de sécurité élevé conviennent à des environnements hautement sécurisés dans la mesure où ils sont validés par des certificats et d'autres formes de chiffrement fort en vue de protéger le canal. Les services dotés d'un profil de sécurité faible sont désactivés par défaut. Activez ces profils uniquement si vous comprenez et acceptez les limites de ce faible niveau de sécurité.

Pour obtenir des informations sur la configuration des services d'authentification à distance, reportez-vous à la documentation relative à Oracle ILOM appropriée :

- Configuration et gestion des comptes utilisateur, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Configuration et gestion des comptes utilisateur, *Guide de configuration et de maintenance* d'Oracle ILOM 3.1
- Gestion des comptes utilisateur, *Guide des procédures relatives à la CLI d'Oracle ILOM 3.0*
- Gestion des comptes utilisateur, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*

Configuration de l'accès utilisateur pour une sécurité maximale

Reportez-vous aux rubriques suivantes pour savoir comment configurer au mieux l'accès utilisateur d'Oracle ILOM et garantir une sécurité maximale.

- “Modification du mot de passe par défaut pour le compte `root` à la première connexion” à la page 29
- “Création de comptes utilisateur locaux disposant de privilèges basés sur les rôles” à la page 30
- “Verrouillage de l'accès hôte à la déconnexion d'une session KVMS” à la page 32
- “Limitation des sessions KVMS visionnables pour Remote System Console Plus (3.2.4 ou version ultérieure)” à la page 33
- “Accès système sécurisé avec un message de connexion (3.0.8 et versions ultérieures)” à la page 34

Vous pouvez configurer les propriétés d'accès utilisateur dans Oracle ILOM à l'aide de l'interface de ligne de commande (CLI) ou l'interface Web. Les procédures décrites dans cette section fournissent des instructions de navigation Web pour toutes les versions du

microprogramme Oracle ILOM. Pour des instructions sur la CLI ou des informations supplémentaires sur les propriétés de configuration, reportez-vous à la documentation appropriée répertoriée à la section Informations connexes qui suit chaque procédure.

▼ Modification du mot de passe par défaut pour le compte root à la première connexion

Pour permettre une première connexion et un premier accès à Oracle ILOM, un compte root Administrateur préconfiguré et un mot de passe par défaut (changeme) sont fournis avec le système. Pour empêcher un accès non autorisé à Oracle ILOM, le mot de passe par défaut (changeme) fourni avec le compte root préconfiguré doit être modifié à la première connexion. Sinon, le compte root préconfiguré et le mot de passe par défaut (changeme) seront considérés comme un compte partagé en permettant l'accès administrateur à tout utilisateur.

Utilisez les instructions Web pour modifier le mot de passe par défaut (changeme) associé au compte root Administrateur préconfiguré.

Remarque - Si vous n'avez pas accès au compte root préconfiguré et si vous avez besoin d'accéder aux fonctions d'administrateur d'Oracle ILOM, contactez votre administrateur système pour obtenir un compte utilisateur disposant de privilèges administrateur.

Avant de commencer

- Consultez les “Directives de sécurité relatives à la gestion des comptes utilisateur et des mots de passe” à la page 25.

Remarque - Il est important d'assigner un mot de passe fiable et sécurisé au compte root afin d'empêcher tout accès non autorisé aux fonctions d'Oracle ILOM. Un mot de passe doit contenir une combinaison de caractères en minuscule et en majuscule, et au moins un caractère spécial tel que % ou $.

- Le rôle User Management (Gestion des utilisateurs) (u) est indispensable pour modifier des mots de passe de comptes utilisateur locaux dans Oracle ILOM.

1. **Accédez à la page User Account (Compte utilisateur) de l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur User Management (Gestion des utilisateurs) --> User Accounts (Comptes utilisateur).**

- **Dans l'interface Web 3.1 ou ultérieure, cliquez sur User Management (Gestion des utilisateurs) --> User Accounts (Comptes utilisateur).**

2. **Dans la page User Account, cliquez sur Edit (Modifier) pour le compte `root`.**

   Une boîte de dialogue Edit: User Root (Modifier : Compte root utilisateur) s'affiche.

3. **Dans la boîte de dialogue Edit: User Root, effectuez les actions suivantes :**

   - **Saisissez un mot de passe unique dans la zone de texte New Password (Nouveau mot de passe), puis saisissez-le à nouveau dans la zone de texte Confirm Password (Confirmation du mot de passe).**
   - **Cliquez sur Save (Enregistrer) pour appliquer la modification.**

Informations connexes

- Configuration d'un compte utilisateur local, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Configuration de comptes utilisateur locaux, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM 3.1*
- Modification d'un compte utilisateur, *Guide des procédures relatives à la CLI d'Oracle Integrated Lights Out Manager (ILOM) 3.0*
- Modification d'un compte utilisateur, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*
- “Présence de sécurité physique pour la réinitialisation du mot de passe par défaut de compte `root`” à la page 63

▼ Création de comptes utilisateur locaux disposant de privilèges basés sur les rôles

Avant de commencer

Oracle ILOM prend en charge la création et le stockage de 10 comptes utilisateur locaux sur un seul module de contrôle de châssis ou SP (CMM). Les utilisateurs d'Oracle ILOM disposent d'un ensemble de privilèges qui leur permet d'utiliser des fonctions dans la limite autorisée par leur compte configuré.

Remarque - Les administrateurs système peuvent également configurer Oracle ILOM pour prendre en charge des comptes utilisateur supplémentaires par le biais d'un service d'authentification à distance. Avec la configuration d'un service d'authentification à distance, les connexions, les mots de passe et les privilèges sont dérivés d'une base d'utilisateurs externe. Pour plus d'informations, reportez-vous à la section “Services d'authentification à distance et profils de sécurité” à la page 27.

Pour obtenir des instructions Web relatives à la configuration d'un compte utilisateur local disposant de privilèges basés sur le rôle, consultez les instructions suivantes.

Avant de commencer

- Consultez les “Directives de sécurité relatives à la gestion des comptes utilisateur et des mots de passe” à la page 25.
- Consultez le Tableau 7, “Descriptions des privilèges de compte utilisateur”.
- Dans Oracle ILOM, le rôle User Management (Gestion des utilisateurs) (u) est indispensable pour créer un compte utilisateur local disposant de privilèges.

1. **Accédez à la page User Account (Compte utilisateur) de l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur User Management (Gestion des utilisateurs) --> User Accounts (Comptes utilisateur).**
   - **Dans l'interface Web 3.1 ou ultérieure, cliquez sur User Management (Gestion des utilisateurs) --> User Accounts (Comptes utilisateur).**

2. **Dans la page User Account (Compte utilisateur), cliquez sur Edit (Modifier).**

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

3. **Dans la boîte de dialogue Add User (Ajout d'un utilisateur), effectuez les actions suivantes :**

   a. **Spécifiez le nom de l'utilisateur dans la zone de texte Name (Nom).**

   b. **Dans la liste déroulante Roles (Rôles), sélectionnez le profil de rôle utilisateur (administrateur, opérateur ou avancé).**

c. **Saisissez un mot de passe unique dans la zone de texte New Password (Nouveau mot de passe), puis saisissez-le à nouveau dans la zone de texte Confirm Password (Confirmation du mot de passe).**

d. **Cliquez sur Save (Enregistrer) pour appliquer les modifications.**

Informations connexes

- Création d'un compte utilisateur et assignation de rôles, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Création d'un compte utilisateur et assignation de rôles, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*
- Ajout d'un compte utilisateur et assignation de rôles, *Guide des procédures relatives à la CLI d'Oracle ILOM 3.0*
- Ajout d'un compte utilisateur et assignation de rôles, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*

▼ Verrouillage de l'accès hôte à la déconnexion d'une session KVMS

Dans la mesure où la console hôte est considérée comme une ressource réseau partagée lors de l'utilisation de KVMS à distance, si un utilisateur se connecte à cette console et ferme les applications Oracle ILOM Remote Console, Remote Console Plus ou Storage Redirection CLI sans se déconnecter du système d'exploitation hôte, un autre utilisateur qui se connecte à la même console par le biais de KVMS à distance peut accéder à la session authentifiée en cours. C'est pourquoi Oracle ILOM permet de verrouiller automatiquement le système d'exploitation hôte lorsqu'une session KVMS à distance est interrompue. Pour une sécurité accrue, activez ou configurez cette fonction dans Oracle ILOM.

Pour verrouiller le bureau d'hôte distant après avoir mis fin à une session KVMS, reportez-vous aux instructions Web suivantes. Pour obtenir des informations sur l'activation de la fonction de verrouillage de l'hôte, reportez-vous au *Guide de l'administrateur sur la configuration et la maintenance d'Oracle (microprogramme 3.2.x)*.

Avant de commencer

- Il faut disposer du rôle Console (c) pour modifier la propriété du mode de verrouillage de l'hôte dans Oracle ILOM.
- La version 3.0.4 ou une version ultérieure du microprogramme est requise pour utiliser ce mode de verrouillage de l'hôte dans Oracle ILOM.
- La fonctionnalité de mode de verrouillage de l'hôte est désactivée par défaut.

1. **Accédez à la page KVMS dans l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur Remote Console (Console distante) --> KVMS.**
   - **Dans l'interface Web 3.1 et version ultérieure, cliquez sur Remote Console (Console distante) --> KVMS.**

2. **Dans la section Host Lock Settings (Paramètres de verrouillage de l'hôte) de la page KVMS, effectuez l'une des tâches suivantes :**

   - **Spécifiez un mode de verrouillage (Windows, Custom (Personnalisé) ou Disabled (Désactivé)).**
   - **Cliquez sur Save (Enregistrer) pour appliquer la modification.**

Informations connexes

- Verrouillage du bureau de l'hôte, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (3.2.x)*
- Verrouillage du bureau de l'hôte, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*
- Verrouillage KVMS, *Guide de la CLI et de l'interface Web des consoles de redirection à distance d'Oracle ILOM 3.0*

▼ Limitation des sessions KVMS visionnables pour Remote System Console Plus (3.2.4 ou version ultérieure)

Avant de commencer

A partir de la version 3.2.4 du microprogramme, un utilisateur Remote System Console Plus principal peut empêcher d'autres utilisateurs de session connectés sur le SP d'afficher des données confidentielles au cours d'une session de redirection de vidéo en définissant la propriété Maximum Client Session Count (Nombre maximum de sessions client) sur un (1) visionneur de session. Par défaut, la propriété Maximum Client Session Count pour Oracle ILOM Remote System Console Plus est définie sur quatre visionneurs de session.

Pour modifier la propriété Maximum Client Session Count pour Oracle ILOM Remote System Console Plus, reportez-vous aux instructions Web suivantes.

Avant de commencer

- La propriété KVMS Maximum Client Session Count (nombre maximum de session client KVMS) pour Oracle ILOM Remote System Console Plus est disponible à partir de la version 3.2.4 du microprogramme.

Remarque - La propriété KVMS Maximum Client Session Count n'est pas configurable sur les systèmes prenant en charge Oracle ILOM Remote Console.

- Oracle ILOM Remote System Console Plus est disponible uniquement sur les nouveaux systèmes SP à partir de la version 3.2.1 du microprogramme.
- Il faut disposer du rôle Console (c) dans Oracle ILOM pour modifier la propriété KVMS Maximum Client Session Count.
- Lors de la réinitialisation de la propriété Maximum Client Session Count dans Oracle, toutes les sessions vidéo Oracle ILOM Remote System Console Plus actives sur le SP seront fermées.
- Par défaut, un maximum de quatre sessions de redirection vidéo Remote System Console Plus, par SP, peuvent être lancées à partir de la page Redirection dans Oracle ILOM.

1. **Accédez à la page KVMS dans l'interface Web d'Oracle ILOM en cliquant sur Remote Console (Contrôle à distance) -> KVMS.**
2. **Dans la page KVMS, modifiez la propriété Maximum Client Session Count (valeur admise :** *4* **(valeur par défaut)|***1***|***2***|***3***).**
3. **Cliquez sur Save (Enregistrer) pour appliquer la modification.**

Informations connexes

- Propriétés de redirection de périphérique distant, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*

▼ Accès système sécurisé avec un message de connexion (3.0.8 et versions ultérieures)

Avant de commencer

A partir de la version 3.0.8 du microprogramme, Oracle ILOM permet aux administrateurs système d'afficher un message d'accueil à tous les utilisateurs lors de la connexion à la CLI et à l'interface Web d'Oracle ILOM. L'utilisation d'un message de connexion peut assurer la protection contre les accès système non autorisés de périphériques distants, et informer les utilisateurs autorisés et légitimes quant à leurs obligations relatives à l'utilisation du système.

Le message d'accueil que vous utilisez doit être rédigé en conformité avec votre stratégie de sécurité des informations. Pour obtenir davantage de directives sur le message écrit, contactez votre administrateur de site ou votre responsable de la sécurité.

Pour afficher un message d'accueil à tous les utilisateurs qui se connectent, reportez-vous aux instructions Web suivantes.

Avant de commencer

- Pour créer un message d'accueil, vous devez disposer du rôle Admin (a).
- Le message d'accueil est disponible pour configuration à partir de la version 3.0.8 du microprogramme Oracle ILOM.
- Les administrateurs peuvent configurer le message d'accueil pour l'afficher sur la page de connexion, ou dans une boîte de dialogue qui s'affiche immédiatement après la connexion de l'utilisateur à Oracle ILOM.

1. **Accédez à la page Banner Message (Message d'accueil) dans l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur System Information (Informations système) --> Banner Messages (Messages d'accueil).**
   - **Dans l'interface Web 3.1 et version ultérieure, cliquez sur ILOM Administration (Administration ILOM) -> Management Access (Accès à la gestion) -> Banner Messages (Messages d'accueil).**

2. **Sur la page Banner Message (Message d'accueil), effectuez les actions suivantes :**

   a. **Si vous souhaitez que le message apparaisse sur la page de connexion, saisissez-le dans la zone de texte Connect Message (Message de connexion). Sinon, saisissez le message dans la zone de texte Login Message (Message de connexion) afin qu'il s'affiche dans une boîte de dialogue après la connexion de l'utilisateur.**

   b. **Activez la case Login Message Acceptance (Acceptation du message de connexion) pour afficher le message ou désactivez-la afin que le message ne s'affiche pas.**

   c. **Cliquez sur Save (Enregistrer) pour appliquer les modifications.**

Informations connexes

- Propriétés de configuration du message d'accueil, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Propriétés de configuration du message d'accueil, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*

- Affichage du message d'accueil, *Guide des procédures relatives à la CLI d'Oracle ILOM 3.0*
- Affichage du message d'accueil, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*

Configuration des interfaces d'Oracle ILOM pour une sécurité optimale

Pour configurer les interfaces d'Oracle ILOM pour garantir une sécurité optimale, reportez-vous aux sections suivantes :

Configuration de l'interface Web pour une sécurité optimale

Reportez-vous aux rubriques suivantes pour savoir comment configurer l'interface Web d'Oracle ILOM en vue d'atteindre un niveau de sécurité maximal.

Remarque - Vous pouvez configurer les propriétés de l'interface de gestion Web dans Oracle ILOM à l'aide de l'interface de ligne de commande (CLI) ou l'interface Web. Les procédures décrites dans cette section fournissent des instructions de navigation Web pour toutes les versions du microprogramme Oracle ILOM. Pour des instructions sur la CLI ou des informations supplémentaires sur les propriétés de configuration, reportez-vous à la documentation appropriée répertoriée à la section Informations connexes qui suit chaque procédure.

Amélioration de la sécurité à l'aide d'un certificat SSL de confiance et d'une clé privée

Les certificats SSL (Secure Socket Layer) assurent à la fois le chiffrement des communications sur un réseau et l'authentification d'un serveur ou d'un client. Oracle ILOM inclut un certificat SSL autogénéré qui permet d'utiliser directement le protocole HTTP sur SSL, sans télécharger de certificat. Lors de la connexion initiale à l'interface Web d'Oracle ILOM, l'utilisateur est invité à accepter l'usage d'un certificat autosigné. Grâce au certificat fourni, les communications entre le navigateur Web et Oracle ILOM sont totalement chiffrées.

Il est cependant possible de créer et télécharger un certificat de confiance dans le but de renforcer la sécurité. Un certificat de ce type est accordé par une autorité de certification de confiance. L'utilisation d'un certificat de confiance émis par une autorité connue garantit l'authentification du serveur Web d'Oracle ILOM. En revanche, l'utilisation de certificats non sécurisés (autosignés) laisse la porte ouverte à une attaque du type Man-in-the-middle (MITM).

Pour obtenir et charger un certificat autosigné temporaire ou un certificat signé par un organisme de certification, reportez-vous aux procédures suivantes.

- “Obtention d'un certificat SSL et d'une clé privée à l'aide d'OpenSSL” à la page 37
- “Chargement d'un certificat SSL personnalisé et d'une clé privée dans Oracle ILOM” à la page 39

▼ Obtention d'un certificat SSL et d'une clé privée à l'aide d'OpenSSL

Cette procédure est une description simplifiée de la création d'un certificat SSL et d'une clé privée à l'aide de la boîte à outils OpenSSL.

Remarque - Oracle ILOM *ne requiert pas* l'utilisation d'OpenSSL pour la génération de certificats SSL. OpenSSL est utilisé dans cette procédure à des fins de démonstration uniquement. D'autres outils permettent de générer des certificats SSL.

La nécessité d'utiliser un certificat autosigné temporaire ou un certificat signé par un organisme de certification est déterminée par votre administrateur de site ou votre responsable de la sécurité. Si vous devez obtenir un certificat SSL (autosigné temporaire ou signé par un organisme de certification), vous pouvez suivre les exemples d'instructions de ligne de commande OpenSSL ci-dessous.

Remarque - Si vous avez besoin d'instructions OpenSSL supplémentaires pour générer le certificat SSL, consultez la documentation utilisateur fournie avec la boîte à outils OpenSSL.

---

1. **Créez un partage réseau ou un répertoire local pour stocker le certificat et la clé privée.**

2. **Pour générer une nouvelle clé privée RSA à l'aide de la boîte à outils OpenSSL, tapez :**

   `openssl genrsa -out <foo>.key 2048`

   Où <*foo*> représente le nom de la clé privée.

   Remarque - Cette clé privée est une clé RSA 2 048 bits stockée au format PEM de sorte qu'elle peut être lue sous forme de texte ASCII.

3. **Pour générer une demande de signature de certificat (CSR) à l'aide de la boîte à outils OpenSSL, tapez :**

   `openssl req -new -key <foo>.key -out <foo>.csr`

   Où <*foo*> représente le nom de la demande de signature de certificat.

   Remarque - Au cours de la génération de la demande de signature de certificat, vous serez invité à fournir diverses informations.

   Un fichier `<foo>.csr` doit maintenant se trouver dans votre répertoire de travail en cours.

4. **Pour générer un certificat SSL, effectuez l'une des tâches suivantes :**

   - **Générez un certificat autosigné temporaire (valide pendant 365 jours).**

     Le certificat SSL autosigné est généré à partir de la clé privée `server.key` et des fichiers `server.csr`.

     A l'aide de la boîte à outils OpenSSL, tapez :

     `openssl x509 -req -days 365 -in <foo>.csr`

     `-signkey <foo>.key -out <foo>.cert`

     Où <*foo*> représente le nom assigné à la clé privée (`.key`) ou au certificat (`.cert`).

     Remarque - Ce certificat temporaire générera une erreur dans le navigateur client de sorte que l'organisme de certificat de signature apparaît comme n'étant ni connu ni fiable. Si cette erreur n'est pas acceptable, vous devez demander à l'organisme de certification de vous fournir un certificat signé.

- **Obtenez un certificat signé officiellement auprès d'un organisme de certification.**

  Soumettez votre demande de signature de certificat (*<foo>*`.csr`) à un organisme de certification SSL. La plupart des organismes de certification vous demande de copier et coller votre sortie CSR dans un écran d'application Web. Il peut s'écouler jusqu'à 7 jours ouvrables avant la réception du certificat signé.

5. **Chargez un nouveau certificat SSL personnalisé et une clé privée dans Oracle ILOM.**

   Reportez-vous à la section "Chargement d'un certificat SSL personnalisé et d'une clé privée dans Oracle ILOM" à la page 39 ci-après.

▼ Chargement d'un certificat SSL personnalisé et d'une clé privée dans Oracle ILOM

Avant de commencer

- Il faut disposer du rôle Admin (a) pour modifier les propriétés du serveur Web dans Oracle ILOM.
- Obtenez le nouveau certificat (autosigné temporaire ou signé par un organisme de certification) HTTPS et la clé privée. Pour obtenir des instructions sur l'utilisation de la boîte à outils OpenSSL, reportez-vous à la section "Obtention d'un certificat SSL et d'une clé privée à l'aide d'OpenSSL" à la page 37.
- Assurez-vous de pouvoir accéder au nouveau certificat HTTPS et à la clé privée via le réseau ou le système de fichiers local.

1. **Accédez à la page SSL Certificate (Certificat SSL) dans l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur Configuration --> System Management Access (Accès à la gestion du système) --> SSL Certificate (Certificat SSL).**

   - **Dans l'interface Web 3.1 et version ultérieure, cliquez sur ILOM Administration (Administration ILOM) -> SSL Certificate (Certificat SSL).**

2. **Sur la page de serveur SSL, suivez les étapes ci-dessous :**

a. **Cliquez sur le bouton Load Certificate (Charger le certificat) pour télécharger le fichier de certificat personnalisé indiqué dans les propriétés File Transfer Method (Méthode de transfert de fichier).**

b. **Cliquez sur le bouton Load Custom Private Key (Charger la clé privée personnalisée) pour télécharger le fichier de clé privée personnalisée indiqué dans les propriétés File Transfer Method.**

c. **Cliquez sur Save (Enregistrer) pour appliquer les modifications.**

Informations connexes

- Propriétés de configuration du certificat SSL et de la clé privée, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Propriétés de configuration du certificat SSL et de la clé privée, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*
- Chargement d'un certificat, *Guide des procédures relatives à la CLI d'Oracle ILOM*
- Chargement d'un certificat, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*

▼ Activation des propriétés du chiffrement SSL et TLS le plus fort

Par défaut, Oracle ILOM autorise uniquement les protocoles (SSLv3 et TLS v1.0, v1.1 et v1.2) de chiffrement Secure Socket Layer le plus fort avec les chiffrements les plus forts. Toutefois, l'activation de chiffrements SSLv2 ou faibles peut être nécessaire pour prendre en charge l'utilisation de navigateurs Web plus anciens.

Remarque - La prise en charge de SSL et TLSv1.0 a commencé à partir de la version 3.1.0 du microprogramme. Dans Oracle ILOM, la prise en charge de TLS v1.1 et v1.2 est effective à compter de la version 3.1 du microprogramme.

Dans la mesure du possible, vous devez configurer l'interface Web avec les paramètres de sécurité de serveur Web par défaut fournis avec votre système. Pour afficher ou modifier les propriétés de sécurité de serveur Web, reportez-vous aux instructions Web suivantes :

Avant de commencer

- Il faut disposer du rôle Admin (a) pour modifier les propriétés du serveur Web dans Oracle ILOM.

- SSLv3 et TLS 1.0 sont pris en charge et activés par défaut sur les SP de serveur exécutant les versions 3.1.x, 3.2.1, 3.2.2 et 3.2.3 du microprogramme.
- SSLv3 et TLS 1.0, 1.1 et 1.2 sont pris en charge et activés par défaut sur les SP de serveur exécutant les versions 3.2.4 et ultérieures du microprogramme.
- Les propriétés des chiffrements SSLv2 et faibles sont désactivés par défaut.

1. **Dans l'interface Web d'Oracle ILOM, cliquez sur ILOM Administration (Administration ILOM) -> Management Access (Accès à la gestion) -> Web Server (Serveur Web).**
2. **Dans la page Web Server (Serveur Web), affichez ou modifiez les propriétés de sécurité Web pour les chiffrements SSL, TLS ou faibles.**
3. **Cliquez sur Save (Enregistrer) pour appliquer les modifications.**

Informations connexes

- Propriétés de configuration du serveur Web, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Propriétés de configuration du serveur Web, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*

▼ Définition d'un intervalle d'expiration pour les sessions Web inactives

Les intervalles d'expiration de session Web Oracle ILOM permettent d'assurer la sécurité des utilisateurs d'accès Web qui oublient de se déconnecter. Ces intervalles déterminent le temps (en minutes) qui doit s'écouler avant qu'une session Web (HTTP ou HTTPS) inactive ne soit automatiquement interrompue. Cette fonction réduit les risques d'accès d'un utilisateur non autorisé qui trouverait un ordinateur sans surveillance sur lequel une session Web authentifiée établie à Oracle ILOM est en cours.

Pour afficher ou modifier les intervalles d'expiration de session Web définis pour les sessions HTTP et HTTPS, reportez-vous aux instructions Web suivantes :

Avant de commencer

- L'intervalle d'expiration de session Web défini pour les connexions HTTP et HTTPS est de 15 minutes.

Remarque - Si vous réduisez cet intervalle, les utilisateurs devront sans doute saisir leurs nom et mot de passe plus souvent après l'expiration d'une session. Toutefois, la réduction de l'intervalle raccourcit la durée pendant laquelle les sessions Web authentifiées non surveillées restent actives.

- Il faut disposer du rôle Admin (a) pour modifier les propriétés du serveur Web.
- Dans Oracle ILOM, les propriétés d'intervalle d'expiration des sessions HTTP et HTTPS sont configurables uniquement pour les SP de serveur qui exécutent les versions 3.0.4 ou ultérieures du microprogramme.

1. **Accédez à la page Web Server (Serveur Web).**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur Configuration --> System Management Access (Accès à la gestion système) -> Web Server (Serveur Web).**
   - **Dans l'interface Web 3.1 et version ultérieure, cliquez sur ILOM Administration (Administration ILOM) -> Management Access (Accès à la gestion) -> Web Server (Serveur Web).**

2. **Sur la page Web Server (Serveur Web), suivez les étapes ci-dessous :**

   a. **Accédez à la propriété HTTP ou HTTP Session Timeout (Intervalle de session HTTP).**

   b. **Saisissez une valeur comprise entre 1 et 720 minutes pour indiquer la durée qui doit s'écouler avant qu'une session Web inactive ne soit automatiquement interrompue.**

   c. **Cliquez sur Save (Enregistrer) pour appliquer les modifications.**

Informations connexes

- Propriétés de configuration du serveur Web, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Propriétés de configuration du serveur Web, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*
- Définition de l'intervalle d'expiration de session, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*

Configuration de la CLI pour garantir une sécurité optimale

Reportez-vous aux rubriques suivantes pour savoir comment configurer l'interface de ligne de commande d'Oracle ILOM en vue d'atteindre un niveau de sécurité maximal.

Vous pouvez configurer les propriétés de gestion de la CLI dans Oracle ILOM à l'aide de l'interface de ligne de commande (CLI) ou l'interface Web. Les procédures décrites dans cette section fournissent des instructions de navigation Web pour toutes les versions du microprogramme Oracle ILOM. Pour des instructions sur la CLI ou des informations supplémentaires sur les propriétés de configuration, reportez-vous à la documentation appropriée répertoriée à la section Informations connexes qui suit chaque procédure.

▼ Définition d'un intervalle d'expiration pour les sessions CLI inactives

L'interface de ligne de commande d'Oracle ILOM, à laquelle vous accédez en vous connectant à Oracle ILOM par le biais du protocole SSH (Secure Shell) ou d'une connexion série, permet de configurer l'intervalle d'expiration de session pour fermer les sessions CLI inactives. Une fois configurée, cette fonction réduit les risques d'accès d'un utilisateur non autorisé qui trouverait un ordinateur sans surveillance sur lequel une session CLI authentifiée à Oracle ILOM est en cours.

Pour une sécurité optimale, configurez un intervalle d'expiration de session CLI dans un environnement où vous utilisez l'interface de ligne de commande d'Oracle ILOM sur une console partagée. Idéalement, il est recommandé de définir l'intervalle d'expiration de session CLI sur 15 minutes ou moins.

Pour afficher ou modifier la propriété d'intervalle d'expiration pour les sessions de la CLI d'Oracle ILOM, reportez-vous aux instructions Web suivantes.

Avant de commencer

Avant de commencer

- Il faut disposer du rôle Admin (a) pour modifier les propriétés de la CLI.
- Par défaut, l'intervalle d'expiration de session de la CLI pour les connexions SSH est désactivé et défini sur 0 (zéro) minute.

Remarque - Si cet intervalle est défini sur 0 (zéro), Oracle ILOM ne ferme pas les sessions CLI inactives quelle que soit leur durée d'inactivité.

- Dans Oracle ILOM, les propriétés d'intervalle d'expiration des sessions de la CLI sont configurables uniquement pour les SP de serveur qui exécutent les versions 3.0.4 ou ultérieures du microprogramme.

1. **Accédez à la page CLI dans l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur Configuration --> System Management Access (Accès à la gestion système) --> CLI.**
   - **Dans l'interface Web 3.1 et version ultérieure, cliquez sur ILOM Administration (Administration ILOM) -> Management Access (Accès à la gestion) -> CLI.**

2. **Dans la page CLI, définissez un intervalle d'expiration de session de la CLI en effectuant les opérations suivantes.**

   a. **Cochez la case Enable (Activer).**

   b. **Saisissez une valeur comprise entre 1 et 1 440 minutes pour indiquer la durée qui doit s'écouler avant qu'une session de ligne de commande inactive ne soit automatiquement interrompue.**

   c. **Cliquez sur Save (Enregistrer) pour appliquer les modifications.**

Informations connexes

- Propriétés de configuration du délai d'expiration de session dans la CLI, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Propriétés de configuration du délai d'expiration de session dans la CLI, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*.
- Configuration du délai d'expiration de session de la CLI, *Guide des procédures relatives à la CLI d'Oracle ILOM 3.0*

▼ Utilisation des clés côté serveur pour le chiffrement des connexions SSH

Oracle ILOM offre une capacité de serveur SSH (Secure Shell) qui permet aux clients distants de se connecter à Oracle ILOM de manière sécurisée pour gérer Oracle ILOM par le biais de l'interface de ligne de commande. Le protocole SSH chiffre le canal de gestion et sécurise toutes les communications par le biais de clés côté serveur. Les clients SSH utilisent eux aussi ces clés pour authentifier le serveur SSH.

Oracle ILOM génère un ensemble de clés SSH uniques lors de la première initialisation d'un système par défaut défini en usine. Si de nouvelles clés côté serveur s'avèrent nécessaires, Oracle ILOM permet de générer manuellement des clés côté serveur SSH supplémentaires.

Pour afficher ou générer manuellement les clés de chiffrement côté serveur SSH, reportez-vous aux instructions Web suivantes :

Avant de commencer

- Il faut disposer du rôle Admin (a) pour modifier les propriétés du serveur SSH.

1. **Accédez à la page SSH Server (Serveur SSH) dans l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur System Management (Gestion des systèmes) --> SSH Server (Serveur SSH).**
   - **Dans l'interface Web 3.1 et versions ultérieures, cliquez sur ILOM Administration (Administration ILOM) -> SSH Server (Serveur SSH).**

2. **Dans la page SSH Server (Serveur SSH), passez en revue les informations sur les clés RSA et DSA générées, ou effectuez les actions suivantes :**

   a. **Cliquez sur Generate RSA Key (Générer une clé RSA) pour générer une nouvelle clé.**

   b. **Cliquez sur Generate DSA Key (Générer une clé DSA) pour générer une nouvelle clé.**

Informations connexes

- Propriétés de configuration du serveur SSH, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Propriétés de configuration du serveur SSH *Guide de configuration et de maintenance d'Oracle ILOM 3.1*

- Génération d'une nouvelle clé SSH, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*
- Génération d'une nouvelle clé SSH, *Guide des procédures relatives à la CLI d'Oracle ILOM 3.0*

▼ Ajout de clés SSH aux comptes utilisateur pour l'authentification CLI automatisée

Les paires de clés SSH personnalisées générées (DSA ou RSA) peuvent être utilisées pour les comptes individuels, la clé publique étant chargée dans Oracle ILOM. Cela s'avère utile lors de l'utilisation de scripts qui s'exécutent sans intervention manuelle et n'incluent pas de mots de passe au format texte intégrés. Les utilisateurs peuvent écrire des scripts afin d'exécuter automatiquement et/ou périodiquement des commandes du processeur de service via une connexion SSH réseau à partir d'un système distant.

Pour charger et ajouter un compte Oracle ILOM avec une clé SSH publique générée, reportez-vous aux instructions Web suivantes.

Avant de commencer

- Générez les clés SSH privées et publiques à l'aide d'un outil de connectivité SSH, tel que ssh-keygen, puis stockez les fichiers de la clé SSH générée sur un système SSH distant.
- Le rôle User Management (Gestion des utilisateurs) (u) est indispensable pour ajouter des clés publiques SSH aux comptes d'autres utilisateurs.
- Le rôle Read Only (Lecture seule) (o) est indispensable pour ajouter une clé publique SSH à votre propre compte utilisateur.

1. **Accédez à la page User Account (Compte utilisateur) de l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur User Management (Gestion des utilisateurs) --> User Accounts (Comptes utilisateur).**
   - **Dans l'interface Web 3.1 et versions ultérieures, sélectionnez ILOM Administration (Administration ILOM) -> User Management (Gestion des utilisateurs) -> User Accounts (Comptes utilisateur).**

2. **Dans la page User Account (Compte utilisateur), effectuez les actions suivantes :**

   a. **Accédez à la section SSH Keys (Clés SSH) et cliquez sur (Add) Ajouter.**

b. **Sélectionnez un compte utilisateur dans la liste User (Utilisateur).**

c. **Sélectionnez une méthode de transfert dans la liste, puis spécifiez les propriétés de méthode de transfert requises pour le chargement de la clé SSH publique.**

3. **Cliquez sur Load (Charger) pour charger la clé SSH publique et ajoutez-la au compte utilisateur sélectionné.**

Informations connexes

- Authentification de la CLI à l'aide de la clé SSH locale, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Authentification de la CLI à l'aide de la clé SSH locale, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*
- Gestion des comptes utilisateur, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*
- Gestion des comptes utilisateur, *Guide des procédures relatives à la CLI d'Oracle ILOM 3.0*

Configuration de l'accès à la gestion SNMP pour garantir une sécurité optimale

Le protocole standard SNMP permet de surveiller ou de gérer un système. Oracle ILOM offre une solution SNMP pour réaliser à la fois des tâches de gestion et de surveillance, mais une configuration préalable est nécessaire. Il est important de comprendre les implications des différentes options SNMP configurables par l'utilisateur en matière de sécurité avant de paramétrer ce service. Pour plus de détails, reportez-vous aux informations suivantes :

- “Utilisation du chiffrement SNMPv3 et de l'authentification utilisateur” à la page 47
- “MIB SNMP Sun prenant en charge les objets configurables” à la page 49

▼ Utilisation du chiffrement SNMPv3 et de l'authentification utilisateur

Les versions SNMPv1 et SNMPv2c n'offrent pas de chiffrement et procèdent à l'authentification à l'aide de chaînes de communauté. Ces chaînes de communauté, envoyées sous forme de texte clair sur le réseau, sont généralement partagées par un groupe d'utilisateurs, et non réservées à un seul utilisateur. En revanche, SNMPv3 met en oeuvre le chiffrement pour fournir un canal sécurisé, ainsi que des noms et mots de passe utilisateur individuels. Les mots de passe

utilisateur SNMPv3 étant localisés, ils peuvent être stockés de manière sécurisée sur les stations de gestion.

Les versions SNMPv1, SNMPv2c et SNMPv3 sont toutes prises en charge par Oracle ILOM, et peuvent être activées ou désactivées séparément. En outre, il est possible d'activer ou de désactiver le paramètre "sets" pour ajouter une couche supplémentaire de sécurité. Cette option détermine si le service SNMP autorise ou non la définition de propriétés MIB SNMP configurables. La désactivation du paramètre sets rend le service SNMP opérationnel pour la surveillance uniquement.

Les protocoles SNMPv1 et SNMPv2c sont désactivés par défaut. SNMPv3 est activé par défaut, mais il faut créer un ou plusieurs utilisateurs SNMP pour l'appliquer. Aucun utilisateur SNMPv3 n'est préconfiguré.

Pour configurer la gestion SNMP dans Oracle ILOM, reportez-vous aux instructions Web suivantes.

Avant de commencer

- Pour une sécurité accrue, activez SNMPv1 et SNMPv2c uniquement dans le cadre de la surveillance et n'activez pas le paramètre sets lorsque ces versions moins sécurisées sont appliquées.
- Les ensembles SNMP doivent être activés uniquement pour la gestion SNMPv3. La propriété SNMP Set est désactivée par défaut.
- Les ensembles SNMPv3 requiert la configuration de comptes utilisateur SNMPv3. Des comptes utilisateur SNMPv3 préconfigurés ne sont pas disponibles.
- La propriété State du service SNMP est activée par défaut.
- Les privilèges du rôle Admin (a) sont nécessaires pour modifier les propriétés SNMP.
- Des privilèges de gestion utilisateur (u) sont nécessaires pour ajouter ou modifier les comptes utilisateur SNMPv3.

1. **Accédez à la page SNMP dans l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur System Management Access (Accès à la gestion système) -> SNMP.**
   - **Dans l'interface Web 3.1 et version ultérieure, cliquez sur ILOM Administration (Administration ILOM) -> Management Access (Accès à la gestion) -> SNMP.**

2. **Dans la page SNMP, affichez ou modifiez la propriété SNMP, puis cliquez sur Save (Enregistrer) pour appliquer les modifications.**

Pour des instructions supplémentaires, reportez-vous à la documentation de la section Informations connexes qui suit cette procédure. Les utilisateurs exécutant la version 3.2. ou une version ultérieure du microprogramme doivent cliquer sur le lien `More details` (Plus de détails) de la page SNMP pour obtenir des informations supplémentaires.

Informations connexes

- Configuration des paramètres SNMP, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (3.2.x)*
- Configuration des paramètres SNMP, *Référence de gestion des protocoles d'Oracle ILOM pour SNMP et IPMI (microprogramme 3.2.x)*
- Configuration des paramètres SNMP, *Guide de référence sur la gestion des protocoles SNMP, IPMI, CIM et WS-MAN d'Oracle ILOM 3.1*
- Configuration des paramètres SNMP, *Guide de référence sur la gestion des protocoles SNMP, IPMI, CIM et WS-MAN d'Oracle ILOM 3.0*

MIB SNMP Sun prenant en charge les objets configurables

Les MIB Sun Oracle prenant en charge les objets configurables et auxquels le paramètre "sets" est applicable sont les suivants :

- `SUN-HW-CTRL-MIB` – Ce MIB permet d'établir des stratégies en matière de matériel, comme des règles de gestion de l'alimentation.
- `SUN-ILOM-CONTROL-MIB` – Ce MIB permet de configurer des fonctions Oracle ILOM, et notamment de créer des utilisateurs et configurer des services.

Remarque - Vous pouvez configurer un objet MIB lorsque : 1) l'objet MIB prend en charge la modification ; 2) l'élément `MAX-ACCESS` de l'objet MIB est défini sur `read-write` ; et 3) l'utilisateur qui tente de procéder à la configuration est autorisé à le faire.

Configuration de l'accès à la gestion IPMI pour garantir une sécurité optimale

Reportez-vous aux rubriques suivantes pour savoir comment configurer l'accès à la gestion IPMI d'Oracle ILOM en vue d'atteindre un niveau de sécurité maximal.

- “Utilisation d'IPMI 2.0 pour l'optimisation de l'authentification et du chiffrement des paquets” à la page 50
- “Directives et pratiques recommandées relatives à la sécurité d'IPMI” à la page 51

- “Prise en charge de la suite de chiffrement d'authentification IPMI 2.0” à la page 52

▼ Utilisation d'IPMI 2.0 pour l'optimisation de l'authentification et du chiffrement des paquets

Bien qu'Oracle ILOM prenne en charge IPMI 1.5 et 2.0 pour la gestion à distance, les administrateurs système doivent toujours utiliser l'interface IPMI 2.0 -I lanplus pour gérer les serveurs Oracle de façon sécurisée. L'interface -I lanplus fournit des vérifications avancées de l'authentification et de l'intégration des données pour la version 2.0 d'IPMI.

A partir de la version 3.2.4 du microprogramme, Oracle ILOM fournit une propriété configurable qui permet d'activer et de désactiver les sessions IPMI 1.5. Pour garantir un niveau de sécurité élevé, la propriété IPMI 1.5 est désactivée par défaut. Lorsqu'elle est désactivée, toutes les connexions de session IPMI à Oracle ILOM sont empêchées (bloquées).

Reportez-vous à la procédure suivante pour afficher ou modifier la propriété State du service IPMI, ou la propriété IPMI 1.5 configurable, qui est disponible à partir de la version 3.2.4 du microprogramme.

Avant de commencer

- Il faut disposer du rôle Admin (a) pour modifier les propriétés IPMI dans Oracle ILOM.
- La propriété State du service IPMI est activée par défaut. Avant toute utilisation, les comptes utilisateur doivent être configurés dans Oracle ILOM avec les privilèges basés sur le rôle appropriés (Administrator (Administrateur), Operator (Opérateur)) pour utiliser les fonctions de gestion IPMI.
- Pour les SP exécutant la version 3.2.4 ou ultérieure du microprogramme d'Oracle ILOM, les sessions de gestion IPMI 2.0 sont prises en charge et les sessions de gestion IPMI 1.5, par défaut, ne le sont pas. La propriété IPMI 1.5 est configurable dans Oracle ILOM.

Remarque - Lorsque les sessions IPMI 1.5 sont désactivées dans Oracle ILOM, les utilisateurs d'IPMItool doivent utiliser l'option -I lanplus IPMI 2.0.

- Pour les SP exécutant la version 3.2.3 ou ultérieure du microprogramme d'Oracle ILOM, les sessions de gestion IPMI 2.0 et 1.5 sont prises en charge par Oracle ILOM. La propriété IPMI 1.5 n'est pas configurable dans Oracle ILOM.

Remarque - Les sessions IPMI 1.5 ne prennent pas en charge l'authentification et le chiffrement de paquet optimisés. Pour optimiser l'authentification et le chiffrement de paquet IPMI, vous devez utiliser IPMI 2.0.

---

1. **Accédez à la page IPMI dans l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0, cliquez sur Configuration --> System Management Access (Accès à la gestion système) -> IPMI.**
   - **Dans l'interface Web 3.1 et versions ultérieures, cliquez sur ILOM Administration (Administration ILOM) -> Management Access (Accès à la gestion) -> IPMI.**

2. **Dans la page IPMI, affichez ou configurez la propriété IPMI, puis cliquez sur Save (Enregistrer) pour appliquer les modifications.**

   Pour des instructions supplémentaires sur la configuration d'IPMI, reportez-vous à la documentation appropriée répertoriée à la section Informations connexes ci-après.

Informations connexes

- Gestion des serveurs à l'aide d'IPMI, *Référence de gestion des protocoles d'Oracle ILOM pour SNMP et IPMI (microprogramme 3.2.x)*
- Gestion des serveurs à l'aide d'IPMI, *Référence sur la gestion des protocoles SNMP, IPMI, CIM et WS-MAN d'Oracle ILOM 3.1*
- Gestion des serveurs à l'aide d'IPMI, *Référence sur la gestion des protocoles SNMP, IPMI, CIM et WS-MAN d'Oracle ILOM 3.0*
- “Directives et pratiques recommandées relatives à la sécurité d'IPMI” à la page 51
- “Prise en charge de la suite de chiffrement d'authentification IPMI 2.0” à la page 52

Directives et pratiques recommandées relatives à la sécurité d'IPMI

Pour garantir que les sessions de gestion système IPMI établies sont sécurisées et ne sont pas vulnérables aux attaques, les administrateurs système doivent respecter les points suivants :

- Ne jamais établir de session IPMI de gestion à distance à l'aide de la version 1.5 d'IPMI (interface IPMItool `-I lan`). Utiliser explicitement la version 2.0 d'IPMI lors de l'application d'utilitaires de ligne de commande tels qu'IPMItool (interface IPMItool `-I lanplus`).
- Modifier le mot de passe IPMI de façon régulière. S'assurer de la gestion appropriée du cycle de vie des comptes utilisateur Oracle ILOM.

  Pour plus d'informations, reportez-vous à la section “Sécurisation de l'accès utilisateur à Oracle ILOM” à la page 23.
- Limiter l'accès au réseau depuis le monde extérieur. Utiliser le canal de gestion Ethernet dédié pour communiquer avec Oracle ILOM.

Pour plus d'informations, reportez-vous à la section “Sécurisation de la connexion de gestion physique” à la page 13.

- Collaborez avec votre responsable de la sécurité informatique afin de définir un ensemble de pratiques recommandées et de politiques concernant la gestion du serveur et la sécurité IPMI.

Prise en charge de la suite de chiffrement d'authentification IPMI 2.0

Les contrôles de l'authentification, de la confidentialité et de l'intégrité dans la version 2.0 d'IPMI sont pris en charge via des programmes de chiffrement. Ceux-ci utilisent le protocole d'échange de clés authentifiées RMCP+ décrit dans les spécifications d'IPMI 2.0.

Oracle ILOM prend en charge les algorithmes de clés de programme de chiffrement suivants pour l'établissement de sessions IPMI 2.0 sécurisées entre le client et le serveur.

- **Programme de chiffrement 2** : le programme de chiffrement 2 utilise des algorithmes d'authentification et d'intégrité.
- **Programme de chiffrement 3** : le programme de chiffrement 3 utilise des algorithmes d'authentification, de confidentialité et d'intégrité.

Remarque - Afin de garantir que l'intégralité du trafic IPMI 2.0 est chiffrée, Oracle ILOM ne prend pas en charge le mode IPMI 2.0 Cipher Type 0 (non chiffré).

Configuration de l'accès à WS-Management pour garantir une sécurité optimale

A compter des versions 3.0.8 à 3.1.2 du microprogramme, Oracle ILOM fournit une interface de services Web standard permettant de contrôler l'intégrité du serveur et d'obtenir des informations d'inventaire à l'aide d'un protocole nommé Ws-Management (Ws-Man).

L'interface Ws-Man d'Oracle ILOM permet également le contrôle homologue de l'hôte et la réinitialisation du SP d'Oracle ILOM lui-même. Ws-Man est un protocole reposant sur SOAP (Simple Object Access Protocol) et qui va au-delà des avantages des protocoles HTTP(S). Il est possible d'utiliser l'interface Ws-Man d'Oracle ILOM avec HTTP ou HTTPS comme protocole de transport. Avec HTTPS, le canal est chiffré à l'aide d'un certificat SSL. Pour plus d'informations sur les avantages des certificats SSL en matière de sécurité, et sur la différence entre les certificats autosignés et les certificats de confiance, reportez-vous à la section “Amélioration de la sécurité à l'aide d'un certificat SSL de confiance et d'une clé privée” à la page 37.

Accédez à cette interface de services Web uniquement si des certificats SSL sont appliqués. Pour une sécurité accrue, utilisez HTTPS comme protocole de transport. Pour plus d'informations sur la configuration des propriétés de serveur Web, reportez-vous à la section “Configuration de l'interface Web pour une sécurité optimale” à la page 36.

Pratiques recommandées en matière de sécurité après le déploiement d'Oracle ILOM

Les rubriques suivantes vous permettent de déterminer les pratiques de sécurité Oracle ILOM recommandées à mettre en oeuvre après le déploiement d'un serveur.

Informations connexes

- “Pratiques de sécurité de déploiement recommandées pour Oracle ILOM ”
- “Listes de contrôle des pratiques recommandées pour la sécurité d'Oracle ILOM”

Conservation d'une connexion de gestion sécurisée

Tenez compte des informations suivantes pour conserver une connexion de gestion sécurisée dans Oracle ILOM.

Eviter l'accès à un périphérique KCS hôte non authentifié

Les serveurs Oracle prennent en charge une connexion bas débit standard entre l'hôte et Oracle ILOM, appelée interface KCS (Keyboard Controller Style). Cette interface KCS prise en charge est totalement conforme à la spécification Intelligent Platform Management Interface (IPMI) Version 2.0 et, à ce titre, ne peut pas être désactivée.

Bien que l'accès au périphérique KCS puisse constituer un moyen pratique de configurer Oracle ILOM à partir de l'hôte, il représente également un risque pour la sécurité dans la mesure où tout utilisateur d'un système d'exploitation disposant d'un accès de type noyau ou pilote au périphérique KCS physique peut modifier les paramètres d'Oracle ILOM sans s'authentifier. Généralement, seuls les utilisateurs `root` ou Administrateur peuvent accéder au périphérique KCS. Il est cependant possible de configurer la plupart des systèmes d'exploitation pour offrir un accès plus large au périphérique KCS.

Un utilisateur d'un système d'exploitation disposant d'un accès KCS peut effectuer les opérations suivantes :

- Ajouter et créer des utilisateurs Oracle ILOM
- Modifier les mots de passe utilisateur
- Accéder à l'interface de ligne de commande d'Oracle ILOM en tant qu'administrateur d'ILOM
- Accéder aux journaux et informations relatives au matériel

Généralement, le périphérique est nommé `/dev/kcs0` ou `/dev/bmc` sous Linux ou Oracle Solaris, et `ipmidrv.sys` ou `imbdrv.sys` sous Microsoft Windows. Il faut soigneusement contrôler l'accès à ce périphérique, également appelé pilote BMC (Baseboard Management Controller) ou IPMI, à l'aide des mécanismes adaptés qui sont intégrés au système d'exploitation hôte.

Pour configurer les paramètres Oracle ILOM, envisagez d'utiliser l'interface d'interconnexion Oracle ILOM au lieu du périphérique KCS IPMI hôte. Pour plus d'informations, reportez-vous à la section “Accès à l'interconnexion de l'hôte authentifié préféré” à la page 56

Pour plus d'informations sur le contrôle ou la protection de l'accès aux périphériques matériels tels que le périphérique KCS, reportez-vous à la documentation accompagnant le système d'exploitation hôte.

Accès à l'interconnexion de l'hôte authentifié préféré

Pour tirer parti d'une alternative plus rapide que l'interface KCS, les clients résidant sur le système d'exploitation hôte peuvent communiquer avec Oracle ILOM par le biais d'une

interconnexion haut débit interne. Cette interconnexion est implémentée par une connexion USB Ethernet interne qui exécute une pile IP. Oracle ILOM se voit attribuer une adresse IP interne non routable à laquelle un client de l'hôte peut se connecter.

Contrairement à l'interface KCS, qui repose sur un accès protégé au périphérique matériel, l'interconnexion LAN est accessible à tous les utilisateurs du système d'exploitation par défaut. Aussi, la connexion à Oracle ILOM par le biais d'une interconnexion LAN impose une authentification, comme si la connexion s'effectuait sur le réseau au port de gestion d'Oracle ILOM.

En outre, tous les services ou protocoles exposés sur le réseau de gestion sont accessibles par le biais de l'interconnexion LAN à l'hôte. Il est possible d'accéder à l'interface Web d'Oracle ILOM dans un navigateur sur l'hôte ou à l'interface de ligne de commande d'Oracle ILOM dans un client SSH (Secure Shell, shell sécurisé). Dans tous les cas de figure, il faut fournir un nom et un mot de passe utilisateur valides lors de l'interconnexion LAN.

L'interconnexion LAN est désactivée par défaut. A ce stade, aucun périphérique Ethernet n'est visible au système d'exploitation hôte et le canal n'existe pas. Le pack de gestion du matériel Oracle facilite la mise à disposition et la configuration de l'interconnexion LAN.

Pour obtenir des informations sur la gestion d'Oracle ILOM par le biais d'une connexion d'interconnexion hôte dédiée et sécurisée, reportez-vous aux documents suivants :

- Pour les versions 3.2 ou ultérieures du microprogramme, reportez-vous à la section Connexion de gestion du SP d'interconnexion dédiée du *Guide de configuration et de maintenance de l'administrateur d'Oracle ILOM (microprogramme 3.2x)*
- Pour les versions 3.1 du microprogramme, reportez-vous à la section Connexion de gestion du SP d'interconnexion dédiée du *Guide de configuration et de maintenance d'Oracle ILOM 3.1*.
- Pour les versions 3.0.12 à 3.0.16 du microprogramme, reportez-vous à la section Configuration de l'interface d'interconnexion locale du *Guide des procédures relatives à l'interface Web Oracle ILOM 3.0.*

Création d'un canal sécurisé à l'aide du chiffrement IPMI 2.0

Intelligent Platform Management Interface (IPMI) version 2.0 prend en charge un protocole réseau chiffré nommé Remote Management and Control Protocol+ (RMCP+). Ce protocole met en oeuvre un mécanisme symétrique de question-réponse reposant sur une clé pour chiffrer le canal. Ce mécanisme garantit qu'aucune donnée sensible n'est transmise en clair sur le réseau ; un mot de passe utilisateur est requis pour chiffrer et déchiffrer le trafic. Afin de garantir que l'intégralité du trafic IPMI 2.0 est chiffrée, Oracle ILOM ne prend pas en charge le mode IPMI 2.0 Cipher Type 0 (non chiffré).

Dans l'utilitaire IPMtool, insérez l'indicateur `-I lanplus` pour préciser qu'il faut établir une session RMCP+ chiffrée.

Pour plus d'informations, consultez la documentation relative à `ipmitool`.

Remarque - A partir de la version 3.2.4 du microprogramme, Oracle ILOM fournit une propriété configurable IPMI 1.5. Par défaut, la propriété IPMI 1.5 est désactivée. Pour plus d'informations, reportez-vous à la section “Utilisation d'IPMI 2.0 pour l'optimisation de l'authentification et du chiffrement des paquets” à la page 50.

Gestion à distance via les protocoles sécurisés

Oracle ILOM est compatible avec un grand nombre de protocoles de gestion à distance. Dans certains cas, les versions chiffrées et non chiffrées d'un même protocole sont prises en charge. Pour des raisons de sécurité, choisissez autant que possible le protocole le plus sécurisé. Le tableau suivant répertorie les protocoles chiffrés et non chiffrés pris en charge.

TABLEAU 9 Protocoles sécurisés pris en charge

Catégorie	Sécurisé/Chiffré	Non chiffré
Accès par navigateur Web	HTTPS	HTTP
Accès par ligne de commande	SSH	Aucun pris en charge
Accès IPMI	IPMI v2.0	IPMI v1.5
Accès par protocole	SNMPv3	SNMPv1/v2c

Etablissement d'une connexion de gestion réseau fiable et sécurisée

Les serveurs Oracle équipés d'Oracle ILOM ont tous un port de gestion dédié pour se connecter à Oracle ILOM sur un réseau. L'utilisation de ce port dédié offre un réseau privé sécurisé à des fins de gestion. Certains systèmes prennent également en charge la gestion sideband, qui permet d'accéder à la fois à l'hôte et à Oracle ILOM par le biais des ports de données serveur standard. Dans la mesure où elle ne nécessite pas deux connexions réseau distinctes, la gestion sideband simplifie la configuration réseau et la fixation des câbles. Cependant, cette fonction peut potentiellement entraîner l'envoi du trafic Oracle ILOM sur un réseau non sécurisé si le port de gestion dédié ou sideband n'est pas connecté à un réseau de confiance.

Pour garantir la fiabilité et la sécurité de l'environnement d'Oracle ILOM, il faut donc que le port de gestion réseau dédié ou le port de gestion sideband sur le serveur soient en permanence connectés à un réseau interne de confiance ou à un réseau de gestion/privé sécurisé dédié.

Etablissement d'une connexion de gestion série locale sécurisée

Vous pouvez connecter un serveur de terminal ou un terminal de vidage à Oracle ILOM via le port série de gestion physique situé sur le serveur. Afin de maintenir une connexion de gestion locale sécurisée à Oracle ILOM, évitez de connecter un périphérique de terminal au port de gestion série local si ce périphérique est également connecté à un réseau interne ou privé.

Utilisation sécurisée de KVMS à distance

Oracle ILOM permet de rediriger le clavier, la sortie vidéo et la souris du serveur hôte vers un client distant, et de monter une unité de stockage distante. Ces fonctions sont collectivement appelées KVMS à distance. Grâce à KVMS à distance, vous pouvez afficher la console graphique du système d'exploitation hôte sur le serveur en exécutant les applications Java nommées Oracle ILOM Remote Console, Remote Console Plus et Storage Redirection CLI sur une machine client.

Pour garantir que les sessions en mode texte série et KVMS à distance sont lancées de manière sécurisée depuis Oracle ILOM, prenez en compte les points suivants :

- “Chiffrement et communication à distance KVMS” à la page 59
- “Protection contre l'accès partagé KVMS à distance” à la page 60
- “Protection contre l'accès partagé à la console série hôte” à la page 61

Chiffrement et communication à distance KVMS

Les applications Oracle ILOM Remote System Console, Remote System Console Plus et CLI Storage Redirection mettent en oeuvre une série de protocoles réseau pour communiquer à distance avec Oracle ILOM. Grâce à ces applications Java, vous pouvez également contrôler le clavier et la souris de l'hôte et monter un périphérique de stockage local (comme un lecteur de CD ou DVD) sur le serveur distant.

Le tableau suivant décrit plus en détail le mode de transmission des informations KVMS à distance sur le réseau.

TABLEAU 10 Chiffrement et fonctions KVMS

Fonction KVMS	Chiffré ou non chiffré	Description
Redirection de la souris	Chiffré	Les coordonnées de la souris sont envoyées à Oracle ILOM de façon sécurisée sur le réseau.

Fonction KVMS	Chiffré ou non chiffré	Description
Redirection du clavier	Chiffré	Tous les caractères que vous tapez sur la machine client sont transmis à Oracle ILOM par le biais d'un protocole chiffré.
Redirection de la vidéo	Chiffré	Les données vidéo sont transmises par le biais d'un protocole chiffré entre le client Java et Oracle ILOM.
Redirection du stockage	Non chiffré	Les données lues et écrites sur un périphérique de stockage sont transmises en clair à Oracle ILOM sur le réseau.

Pour obtenir la liste des ports réseau activés par le biais de KVMS à distance, reportez-vous au Tableau 4, “Services et ports activés par défaut”.

Protection contre l'accès partagé KVMS à distance

Grâce à une console vidéo de KVMS à distance, vous visualisez ce que vous verriez si vous vous trouviez effectivement face au moniteur physique connecté au serveur. Même s'il est possible d'établir une session KVMS à Oracle ILOM sur plusieurs clients distants, chaque session affiche exactement les mêmes données puisque, sauf exception, un serveur génère une seule sortie vidéo.

De la même manière, tout ce que vous tapez au clavier au cours d'une session KVMS à distance est visible pour les autres utilisateurs KVMS connectés à la même machine. Plus important encore, si un seul utilisateur se connecte au système d'exploitation hôte par le biais des applications Oracle ILOM Remote Console, Remote Console Plus et Storage Redirection CLI avec les privilèges appropriés, tous les autres utilisateurs KVMS peuvent partager la session authentifiée. Il est donc important de comprendre que la fonction KVMS à distance autorise les connexions partagées.

Pour vous protéger contre les sessions du système d'exploitation authentifiées restant inactives au terme d'une session de redirection KVMS à distance, vous devez :

- Configurer Oracle ILOM pour qu'il verrouille automatiquement le système d'exploitation hôte lorsqu'une session de redirection KVMS à distance prend fin.

  Vous trouverez des instructions à la section “Verrouillage de l'accès hôte à la déconnexion d'une session KVMS” à la page 32.
- Configurer un intervalle d'expiration dans le système d'exploitation hôte pour fermer automatiquement les sessions utilisateur authentifiées.

  Pour obtenir des instructions, reportez-vous à la documentation utilisateur relative à votre système d'exploitation hôte.

Si vous utilisez Oracle ILOM Remote System Console Plus et que vous devez limiter le nombre de sessions KVMS affichables ouvertes à partir d'Oracle ILOM, reportez-vous à la section

“Limitation des sessions KVMS visionnables pour Remote System Console Plus (3.2.4 ou version ultérieure)” à la page 33.

Protection contre l'accès partagé à la console série hôte

La console hôte adaptée à la plupart des systèmes d'exploitation est également disponible sous la forme d'une console série en mode texte. Pour l'afficher, il faut exécuter la commande `start /HOST/console` dans la ligne de commande d'Oracle ILOM. Comme c'est le cas pour la console graphique, une seule console série est à la disposition de tous les utilisateurs d'Oracle ILOM. Elle est donc considérée comme une ressource partagée. Si un utilisateur se connecte au système d'exploitation hôte par le biais de la console série, puis met fin à la redirection de la console sans se déconnecter, un autre utilisateur de la console série peut accéder à la session authentifiée en cours.

Oracle ILOM envoie un signal DTR (Data Transfer Request, demande de transfert de données) au système d'exploitation hôte lorsqu'une session de redirection de console est interrompue. La plupart des systèmes d'exploitation déconnectent automatiquement un utilisateur dès la réception de ce signal. Cependant, certains systèmes d'exploitation ne prennent pas en charge cette fonction :

- Oracle Linux 5 prend en charge le signal DTR, qui fonctionne par défaut.
- Oracle Linux 6 prend en charge le signal DTR, mais il convient de l'activer manuellement.
- Oracle Solaris ne prend pas en charge le signal DTR. Pour réduire les risques de sécurité, les utilisateurs peuvent configurer un délai d'expiration de la session au système d'exploitation hôte.

Pour obtenir des instructions sur la protection contre les sessions du système d'exploitation authentifiées restant inactives au terme d'une session de redirection série de l'hôte, consultez ce qui suit :

- Déterminez si la fonction du signal DTR sur le système d'exploitation hôte est prise en charge, et si tel est le cas, vérifiez qu'elle est activée par défaut.

  Pour plus d'informations sur le signal DTR, reportez-vous à la documentation utilisateur relative à votre système d'exploitation hôte.
- Configurez un intervalle d'expiration de la session sur le système d'exploitation hôte.

  Pour plus d'informations sur la configuration d'un intervalle d'expiration de session dans le système d'exploitation hôte, reportez-vous à la documentation utilisateur relative à votre système d'exploitation hôte.

Considérations relatives à la protection de l'accès utilisateur après le déploiement

Pour garantir que la sécurité de l'accès utilisateur est conservée, prenez en compte les points suivants :

Application de la gestion des mots de passe

Changez régulièrement tous les mots de passe Oracle ILOM. Cette opération réduit les risques d'activité malveillante et garantit la conformité des mots de passe avec les stratégies en vigueur.

En règle générale, les utilisateurs modifient leur mot de passe eux-mêmes. Toutefois, les administrateurs système disposant de privilèges de gestion des utilisateurs ont la capacité de modifier les mots de passe associés aux comptes d'autres utilisateurs.

Pour modifier le mot de passe associé à un compte utilisateur Oracle ILOM, reportez-vous aux instructions Web suivantes.

Remarque - Pour des instructions sur la CLI ou des informations supplémentaires sur les propriétés de configuration de gestion des utilisateurs, reportez-vous à la documentation répertoriée à la section Informations connexes dans la procédure suivante.

▼ Modification du mot de passe d'un compte utilisateur local

Avant de commencer

- Consultez les "Directives de sécurité relatives à la gestion des comptes utilisateur et des mots de passe" à la page 25.
- Le rôle User Management (Gestion des utilisateurs) (u) est indispensable pour modifier des mots de passe ou privilèges associés aux comptes d'autres utilisateurs.
- Le rôle Operator (Opérateur) (o) autorise les utilisateurs à modifier le mot de passe de leur compte.

1. **Accédez à la page User Account (Compte utilisateur) de l'interface Web d'Oracle ILOM.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur User Management (Gestion des utilisateurs) --> User Accounts (Comptes utilisateur).**
   - **Dans l'interface Web 3.1 ou ultérieure, cliquez sur User Management (Gestion des utilisateurs) --> User Accounts (Comptes utilisateur).**

2. **Dans la page User Account (Compte utilisateur), cliquez sur Edit (Modifier) pour le compte que vous souhaitez modifier.**

   La boîte de dialogue Edit: User Name (Modifier : nom d'utilisateur) s'ouvre.

3. **Dans cette boîte de dialogue, effectuez les actions suivantes :**

   - **Saisissez un mot de passe unique dans la zone de texte New Password (Nouveau mot de passe), puis saisissez-le à nouveau dans la zone de texte Confirm Password (Confirmation du mot de passe).**
   - **Cliquez sur Save (Enregistrer) pour appliquer la modification.**

Informations connexes

- Configuration d'un compte utilisateur local, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Configuration d'un compte utilisateur local, *Guide de configuration et de maintenance* d'Oracle ILOM 3.1
- Modification d'un compte utilisateur, *Guide des procédures relatives à la CLI d'Oracle Integrated Lights Out Manager (ILOM) 3.0*
- Modification d'un compte utilisateur, *Guide des procédures relatives à l'interface Web d'Oracle ILOM 3.0*

Présence de sécurité physique pour la réinitialisation du mot de passe par défaut de compte `root`

Il est possible de réinitialiser le mot de passe de l'utilisateur `root` associé à Oracle ILOM en cas de perte. Pour réinitialiser le mot de passe `root`, connectez-vous à Oracle ILOM via le port série. La plupart du temps, cette opération nécessite d'accéder physiquement au système.

Cependant, la console série peut être connectée à un serveur de terminal, lequel offre un accès réseau au port série physique.

Pour éviter d'avoir à réinitialiser le mot de passe `root` sur le réseau si vous disposez d'un serveur de terminal, vous pouvez tirer parti de la fonction de vérification de la présence physique adaptée à la plupart des serveurs. Pour prouver l'accès physique au serveur, il suffit d'appuyer sur un bouton situé sur le serveur. Pour une sécurité optimale, veillez à activer cette fonction de vérification lorsque le port série d'Oracle ILOM est connecté à un serveur de terminal.

Pour afficher ou modifier la fonction de vérification de la présence physique, reportez-vous aux instructions Web suivantes :

Remarque - Pour des instructions sur la CLI ou des informations supplémentaires sur les propriétés de compte `root`, reportez-vous à la documentation répertoriée à la section Informations connexes dans la procédure suivante.

▼ Configuration de la vérification de la présence physique

Avant de commencer

- Dans Oracle ILOM, le mode Physical Presence Check (Vérification de présence physique) est activé par défaut.
- La version 3.1 ou une version ultérieure du microprogramme est requise pour utiliser ce mode dans Oracle ILOM.

1. **Dans l'interface Web du SP d'Oracle ILOM, cliquez sur ILOM Administration -> Identification**
2. **Dans la page Identification, accédez à la propriété Physical Presence Check et effectuez une des opérations suivantes :**

   - **Activez la case Physical Presence (Présence physique). Lorsqu'elle est activée, vous devez appuyer sur le bouton Locator du système physique afin de récupérer le mot de passe d'Oracle ILOM par défaut.**

     -ou-

   - **Désactivez la case Physical Presence (Présence physique). Lorsque cette case est désactivée, le mot de passe root par défaut de l'administrateur d'Oracle ILOM peut être réinitialisé sans appuyer sur le bouton Locator du système physique.**

3. **Cliquez sur Save (Enregistrer) pour appliquer la modification.**

Informations connexes

- Propriétés de configuration de l'identification d'un périphérique, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (3.2.x)*
- Propriétés de configuration de l'identification d'un périphérique, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*
- Récupération du mot de passe du compte `root`, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*
- Récupération du mot de passe du compte `root`, *Guide de configuration et de maintenance d'Oracle ILOM 3.1*

Contrôle des événements d'audit pour détecter l'accès non autorisé

Le journal d'audit Oracle ILOM consigne l'intégralité des connexions et des changements de configuration. Chaque entrée du journal d'audit précise le nom d'utilisateur et l'heure associés à l'événement. Les événements d'audit peuvent s'avérer utiles pour effectuer le suivi des modifications apportées, mais également pour détecter les changements et accès non autorisés à Oracle ILOM.

Pour afficher des événements dans le journal d'audit d'Oracle ILOM, reportez-vous aux instructions Web suivantes.

Remarque - Pour des instructions sur la CLI ou des informations supplémentaires sur le journal d'audit, reportez-vous à la documentation répertoriée à la section Informations connexes dans la procédure suivante.

▼ Affichage du journal d'audit

Avant de commencer

- Le journal d'audit est disponible dans Oracle ILOM à compter de la version 3.1 du microprogramme. Avant la version 3.1 du microprogramme, les événements d'audit étaient capturés dans le journal des événements d'Oracle ILOM.
- Il faut disposer des privilèges du rôle Admin (a) dans Oracle ILOM pour effacer les entrées du journal d'audit.

1. **Dans l'interface Web, cliquez sur ILOM Administration -> Logs (Journaux) -> Audit.**

2. **Dans la page du journal d'audit, utilisez les contrôles pour filtrer les entrées du journal ou en effacer les événements.**

   Les utilisateurs exécutant la version 3.2. ou une version ultérieure du microprogramme doivent cliquer sur le lien `More details` (Plus de détails) de la page Audit pour obtenir des informations supplémentaires.

Informations connexes

- Gestion des entrées du journal d'Oracle ILOM, *Guide de l'utilisateur sur la surveillance du système et les diagnostics d'Oracle ILOM (microprogramme 3.2.x)*
- Gestion des entrées du journal d'Oracle ILOM, *Guide de l'utilisateur d'Oracle ILOM 3.1*

Actions pour la modification du mode FIPS après le déploiement

A partir de la version 3.2.4 du microprogramme, Oracle ILOM fournit une propriété configurable pour la conformité FIPS. Par défaut, cette propriété est désactivée. Suite à la modification de l'état opérationnel de la conformité FIPS dans Oracle ILOM, les paramètres par défaut de toutes les propriétés de configuration définies par l'utilisateur sont rétablis. Pour éviter de perdre les paramètres de configuration définis par l'utilisateur dans Oracle ILOM, la conformité FIPS doit être modifiée avant qu'un autre paramètre Oracle ILOM ne soit configuré. Si la conformité FIPS doit être modifiée après le déploiement de la configuration d'Oracle ILOM, reportez-vous aux instructions suivantes pour éviter de perdre les paramètres définis par l'utilisateur.

▼ Modification du mode FIPS après le déploiement

Procédez comme suit si vous devez modifier l'état opérationnel du mode FIPS après la mise à jour du microprogramme ou la spécification de propriétés de configuration définies par l'utilisateur dans Oracle ILOM.

Remarque - Le mode de conformité FIPS dans Oracle ILOM est représenté par une propriété State et Status. Les propriétés State et Status représentent respectivement le mode configuré et le mode opérationnel dans Oracle ILOM. En cas de modification de la propriété State FIPS, le mode opérationnel (propriété Status FIPS) reste inchangé jusqu'à la prochaine réinitialisation d'Oracle ILOM.

Avant de commencer

- La propriété configurable pour le conformité FIPS est disponible dans Oracle ILOM à partir de la version 3.2.4 du microprogramme. Dans les versions du microprogramme antérieures à la version 3.2.4, Oracle ILOM ne fournit pas de propriété configurable pour la conformité FIPS.
- Si FIPS est activé (configuré et opérationnel), certaines fonctionnalités dans Oracle ILOM ne sont pas prises en charge. Pour obtenir la liste des fonctionnalités qui ne sont pas prises en charge lorsque FIPS est activé, reportez-vous à la section “Fonctions non prises en charge lorsque le mode FIPS est activé” à la page 16.
- Pour effectuer cette procédure, vous devez disposer du rôle Admin (a).

1. **Dans l'interface Web d'Oracle ILOM, sauvegardez la configuration d'Oracle ILOM.**

   Par exemple :

   a. **Cliquez sur ILOM Administration > Configuration Management (Gestion de la configuration) > Backup/Restore (Sauvegarder/Restaurer).**

   b. **Dans la page Backup/Restore (Sauvegarder/Restaurer), cliquez sur le lien More details (Plus de détails) pour obtenir des instructions supplémentaires.**

Remarque - L'activation des options de mise à jour de microprogramme Preserve Configuration simplifie la reconnexion à Oracle ILOM après la mise à jour du microprogramme.

Remarque - Si vous effectuez l'étape 2 avant l'étape 1, vous devez modifier le fichier de configuration XML sauvegardé et supprimer le paramètre FIPS. Sinon, la configuration entre le fichier XML Oracle ILOM sauvegardé et l'état du mode FIPS opérationnel exécuté sur le serveur sera incohérente, ce qui n'est pas autorisé.

---

2. **Si vous devez mettre à jour le microprogramme, effectuez la procédure suivante :**

   a. **Cliquez sur ILOM Administration > Maintenance > Firmware Upgrade (Mise à jour du microprogramme).**

   b. **Dans la page Firmware Update (Mise à jour du microprogramme), cliquez sur le lien More details (Plus de détails) pour obtenir des instructions supplémentaires.**

3. **Modifiez le mode de conformité FIPS dans Oracle ILOM comme suit :**

a. **Cliquez sur ILOM Administration > Management Access (Accès à la gestion) > FIPS.**

b. **Dans la page FIPS, cliquez sur le lien `More details` (Plus de détails) pour obtenir des instructions sur les opérations suivantes :**

   - **Modification de la configuration de l'état FIPS**
   - **Mise à jour de l'état opérationnel FIPS sur le système par réinitialisation du processeur de service**

4. **Restaurez la configuration Oracle ILOM sauvegardée comme suit :**

   a. **Cliquez sur ILOM Administration > Configuration Management (Gestion de la configuration) > Backup/Restore (Sauvegarder/Restaurer).**

   b. **Dans la page Backup/Restore (Sauvegarder/Restaurer), cliquez sur le lien `More details` (Plus de détails) pour obtenir des instructions supplémentaires.**

Informations connexes

- “Choix de configurer le mode FIPS au stade du déploiement” à la page 14
- “Fonctions non prises en charge lorsque le mode FIPS est activé” à la page 16
- Configuration des propriétés du mode FIPS, *Guide de l'administrateur sur la configuration et la maintenance d'Oracle ILOM (microprogramme 3.2.x)*.

Mise à jour des logiciels et microprogrammes

Maintenez à jour les versions des microprogrammes et des logiciels sur votre serveur.

- Vérifiez régulièrement si des mises à jour sont disponibles sur My Oracle Support.
- Tirez profit des correctifs et améliorations en installant la dernière version officielle des logiciels et microprogrammes pour votre serveur.
- Installez les patchs de sécurité requis pour tous les logiciels installés.

Pour mettre à jour le microprogramme Oracle ILOM sur votre serveur, reportez-vous aux instructions suivantes.

▼ Mise à jour du microprogramme Oracle ILOM

Avant de commencer

- Dans Oracle ILOM, vous devez disposer du rôle Admin (a) pour mettre à jour le microprogramme Oracle ILOM.
- Avertissez tous les utilisateurs Oracle ILOM de la mise à jour planifiée du microprogramme et demandez-leur de fermer toutes les sessions client jusqu'à la fin de l'opération.
- La mise à jour du microprogramme prend plusieurs minutes. Il est déconseillé d'effectuer d'autres tâches Oracle ILOM pendant ce temps.

1. **Téléchargez la dernière mise à jour logicielle disponible pour votre serveur sur le site Web My Oracle Support (MOS).**

   Au besoin, reportez-vous à la documentation livrée avec votre serveur pour en savoir plus sur l'obtention des mises à jour logicielles sur MOS.

   Remarque - La version la plus récente du microprogramme Oracle ILOM disponible pour votre serveur est incluse dans le dernier patch logiciel publié sur MOS pour votre serveur.

   ---

2. **Placez l'image du microprogramme sur un lecteur partagé local ou réseau.**

3. **Accédez à la page Firmware Update (Mise à jour du microprogramme) dans l'interface Web.**

   Par exemple :

   - **Dans l'interface Web 3.0.x, cliquez sur Maintenance -> Firmware (Microprogramme).**
   - **Dans l'interface Web 3.1 ou ultérieure, cliquez sur ILOM Administration > Maintenance > Firmware Upgrade (Mise à jour du microprogramme).**

4. **Dans la page Firmware Upgrade (Mise à jour du microprogramme), cliquez sur Enter Firmware Upgrade Mode (Activer le mode de mise à niveau du microprogramme) et répondez aux invites.**

   Les utilisateurs exécutant la version 3.2. ou une version ultérieure du microprogramme doivent cliquer sur le lien `More details` (Plus de détails) de la page Firmware Upgrade (Mise à jour du microprogramme).