Sun Server X4-4

Guide de sécurité

Référence : E54165–01
Avril 2014

140617@25097

Table des matières

Vue d'ensemble

Ce document fournit des instructions générales en matière de sécurité pour vous aider à protéger le serveur Sun Server X4-4 d'Oracle, ses interfaces réseau et les commutateurs réseau auxquels il est connecté.

Cette section aborde les sujets suivants :

Présentation du système

Le serveur Sun Server X4-4 prend en charge les éléments suivants :

- Processeurs Intel Xeon® E7-8895 v2 (15 coeurs, 2,8 GHz) avec les configurations suivantes :
  - 2 processeurs installés dans les sockets 0 et 1
  - 4 processeurs installés dans les sockets 0 à 3
- Jusqu'à 8 modules riser de mémoire sont pris en charge (2 risers par CPU) dans le châssis du serveur. Chaque module riser prend en charge jusqu'à 12 DIMM enregistrés ECC DDR3-1600 basse tension, autorisant jusqu'à 24 DIMM par processeur. Les modules DIMM installés doivent être de types et de tailles identiques.
  - Système de 2 CPU utilisant 4 modules riser. Dans la configuration minimale, chaque riser contient 4 modules DIMM (DIMM 8 Go, DIMM 16 Go ou LRDIMM 32 Go). Il est possible d'ajouter des DIMM jusqu'à un maximum de 1,5 To de mémoire système.
  - Système de 4 CPU utilisant 8 modules riser. Dans la configuration minimale, chaque riser contient 4 modules DIMM (DIMM 8 Go, DIMM 16 Go ou LRDIMM 32 Go). Il est possible d'ajouter des DIMM jusqu'à un maximum de 3 To de mémoire système.
- 11 emplacements PCI Express 3.0 accueillant des cartes PCIe bas profil. Dans les configurations incluant une carte HBA SAS, celle-ci est installée à l'emplacement 2. Tous les emplacements prennent en charge les connexions PCIe x8. 2 emplacements sont également compatibles avec les cartes PCIe x16.
  - Emplacements 1-7, 9 et 10 : connecteur x8
  - Emplacements 8 et 11 : connecteur x8 ou x16

Remarque – Les emplacements PCIe 7-11 fonctionnement uniquement dans les systèmes de 4 CPU.

- Pour le stockage interne, le châssis du serveur fournit :
  - 6 baies d'unités 2,5 pouces, accessibles par le panneau avant. Toutes les baies peuvent contenir des HDD SAS-2 ou SSD SATA-3.
  - Un lecteur DVD+/-RW facultatif sur l'avant du serveur, en dessous des baies. Ce DVD SATA se connecte à un pont USB-SATA, afin qu'il apparaisse pour le logiciel du système comme un périphérique de stockage USB.
  - Options de carte SAS-2 HBA PCIe :
    - HBA Sun Storage 6 Gb SAS PCIe HBA. Niveaux RAID pris en charge : 0, 1, 10.
    - HBA Sun Storage 6 Gb SAS PCIe RAID. Niveaux RAID pris en charge : 0, 1, 1E, 10, 5, 5EE, 6 avec BBWC (Battery Backed Write Cache).
- Deux alimentations électriques remplaçables à chaud et à sélection automatique d'entrée 1030/2060 W CA.

  Un système à 2 CPU peut fonctionner avec des sources de courant basse tension 100 à 127 V. Un système à 4 CPU peut fonctionner avec des sources de courant haute tension 200 à 240 V, mais la haute tension est également prise en charge pour une configuration de système à 2 CPU.
- Baseboard Management Controller (BMC) intégré prenant en charge les éléments suivants :
  - Ensemble de fonctions IPMI standard
  - Fonctionnalités KVMS à distance, DVD et lecteur de disquette sur IP
  - Comprend un port série
  - Accès Ethernet au SP via un port de gestion 10/100/1000 RJ-45 Gigabit Ethernet (GbE) dédié et également via l'un des ports GbE hôtes (gestion Sideband)
- L'outil de configuration de serveur Oracle System Assistant, inclus dans un lecteur flash USB préinstallé.

Principes de sécurité

Il existe quatre principes de sécurité élémentaires : l'accès, l'authentification, l'autorisation et la comptabilisation.

- **Accès**

  L'accès peut désigner l'accès physique au matériel mais aussi l'accès physique ou virtuel aux logiciels.
  - Mettez en place des contrôles physiques et logiciels pour protéger votre matériel ou vos données contre les intrusions.

- Reportez-vous à la documentation qui accompagne votre logiciel pour activer les fonctionnalités de sécurité disponibles pour celui-ci.
- Installez les serveurs et l'équipement connexe dans un local dont l'accès est restreint et dont la porte est dotée d'un verrou.
- Si le matériel est installé dans un rack dont la porte est équipée d'un verrou, maintenez-la verrouillée et ne l'ouvrez que pour effectuer la maintenance des composants du rack.
- Limitez l'accès aux connecteurs et aux ports, qui peuvent offrir un accès plus aisé que les connexions SSH. Les périphériques, tels que les contrôleurs système, les unités de distribution de courant (PDU) et les commutateurs réseau fournissent des connecteurs et des ports.
- Restreignez l'accès aux périphériques enfichables ou échangeables à chaud, essentiellement parce qu'ils peuvent être facilement retirés.
- Installez les unités remplaçables sur site (FRU) et les unités remplaçables par l'utilisateur (CRU) de remplacement dans une armoire verrouillée. Limitez l'accès à l'armoire verrouillée au personnel autorisé.

- **Authentification**

  L'authentification désigne le fait de s'assurer que les utilisateurs du matériel ou des logiciels sont bien ceux qu'ils prétendent être.

  - Configurez des fonctions d'authentification, comme un système de mots de passe dans les systèmes d'exploitation de votre plate-forme, afin d'éviter toute usurpation d'identité.
  - Veillez à ce que les employés utilisent correctement leur badge pour pénétrer dans la salle informatique.
  - Pour les comptes utilisateur, établissez des listes de contrôle d'accès lorsque cette mesure est pertinente. Définissez des délais d'expiration pour les sessions prolongées, ainsi que des niveaux de privilèges pour les utilisateurs.

- **Autorisation**

  L'autorisation désigne les restrictions s'appliquant aux employés quant à l'utilisation du matériel ou des logiciels.

  - Autorisez uniquement les employés à utiliser le matériel et les logiciels pour lesquels ils ont été formés et certifiés.
  - Mettez en place un système d'autorisations en lecture, écriture et exécution pour contrôler l'accès des utilisateurs aux commandes, à l'espace disque, aux périphériques et aux applications.

- **Comptabilisation**

  La comptabilisation désigne les fonctions logicielles et matérielles permettant de surveiller les connexions et la tenue des inventaires du matériel.

  - Surveillez les connexions des utilisateurs par le biais de journaux système. Surveillez étroitement les comptes d'administrateur système et de maintenance, lesquels ont accès à des commandes puissantes.

- Enregistrez les numéros de série de l'ensemble de votre matériel. Assurez le suivi des ressources système à l'aide des numéros de série. Les numéros de référence Oracle sont enregistrés au format électronique sur les cartes, modules et cartes mères, et peuvent être utilisés à des fins d'inventaire.
- Pour détecter et effectuer le suivi des composants, apposez une marque de sécurité sur tous les éléments importants du matériel informatique, tels que les FRU. Utilisez des stylos à ultraviolet ou des étiquettes en relief.

Utilisation des outils de configuration et de gestion de serveur

Respectez les consignes de sécurité suivantes lorsque vous configurez et gérez un serveur à l'aide d'outils logiciels et de microprogrammes.

Sécurité d'Oracle System Assistant

Oracle System Assistant est un outil préinstallé facilitant la configuration et la mise à jour (en local ou à distance) du matériel d'un serveur, ainsi que l'installation des systèmes d'exploitation pris en charge. Pour plus d'informations sur l'utilisation d'Oracle System Assistant, reportez-vous au *Oracle X4 Series Servers Administration Guide* à l'adresse :

`http://www.oracle.com/goto/x86AdminDiag/docs`

Les informations suivantes vous aideront à comprendre les problèmes de sécurité liés à Oracle System Assistant.

- **Oracle System Assistant contient un environnement root amorçable.**

  Oracle System Assistant est une application s'exécutant sur un lecteur flash USB interne. Il repose sur un environnement root Linux amorçable. Oracle System Assistant permet également d'accéder au shell root sous-jacent. Les utilisateurs pouvant accéder physiquement au système ou disposant d'un accès distant KVMS (clavier, vidéo, souris et stockage) au système par le biais d'Oracle ILOM seront en mesure d'accéder à Oracle System Assistant et au shell root.

  Un environnement root permet de modifier la configuration et les stratégies d'un système, ainsi que d'accéder aux données stockées sur d'autres disques. Il est donc conseillé de protéger l'accès physique au serveur et d'attribuer avec parcimonie les privilèges d'administrateur et de console aux utilisateurs d'Oracle ILOM.

- **Oracle System Assistant monte un périphérique de stockage USB accessible au système d'exploitation.**

  En plus d'être un environnement amorçable, Oracle System Assistant est également monté en tant que périphérique de stockage USB (lecteur flash) accessible au système d'exploitation hôte après installation. Cette fonctionnalité est utile pour l'accès aux outils et

aux pilotes à des fins de maintenance et de reconfiguration. Le périphérique de stockage USB d'Oracle System Assistant est accessible en lecture et en écriture et constitue une cible potentielle pour des virus.

Il est donc conseillé d'appliquer au périphérique de stockage Oracle System Assistant les mêmes mesures de protection qu'aux disques, notamment en procédant régulièrement à des analyses anti-virus et à des contrôles d'intégrité.

- **Oracle System Assistant peut être désactivé.**

  Oracle System Assistant est utile pour paramétrer le serveur, mettre à jour et configurer le microprogramme, mais aussi pour installer le système d'exploitation hôte. Toutefois, si les risques pour la sécurité décrits ci-dessus sont jugés trop importants ou si cet outil ne sert pas, il est possible de désactiver Oracle System Assistant. Après la désactivation d'Oracle System Assistant, le périphérique de stockage USB n'est plus accessible au système d'exploitation hôte. En outre, il n'est pas possible d'initialiser Oracle System Assistant.

  Vous pouvez désactiver Oracle System Assistant à partir de l'outil lui-même ou du BIOS. Après avoir été désactivé, Oracle System Assistant peut uniquement être réactivé à partir de l'utilitaire de configuration du BIOS. Il est conseillé de protéger par mot de passe la configuration du BIOS, afin que seuls les utilisateurs autorisés puissent réactiver Oracle System Assistant. Pour plus d'informations sur la désactivation et la réactivation d'Oracle System Assistant, reportez-vous au Guide d'administration des serveurs de série X4 à l'adresse :

  `http://www.oracle.com/goto/x86AdminDiag/docs`

Sécurité d'Oracle ILOM

Vous pouvez sécuriser, gérer et surveiller de manière active les composants du système à l'aide du microprogramme de gestion Oracle Integrated Lights Out Manager (ILOM) préinstallé sur ce serveur, sur d'autres serveurs x86 d'Oracle et sur certains serveurs SPARC.

Installez le processeur de service (SP) sur un réseau interne dédié afin de le séparer du réseau général. Oracle ILOM met à la disposition des administrateurs système des fonctions de contrôle et de surveillance du serveur. Selon le niveau d'autorisation accordé, ces fonctions peuvent inclure la capacité de mettre le serveur hors tension, de créer des comptes utilisateur, de monter des périphériques de stockage distants et ainsi de suite. 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.

Limitez l'utilisation du compte Administrateur par défaut (`root`) à la connexion initiale à Oracle ILOM. Ce compte Administrateur par défaut ne sert qu'à faciliter l'installation initiale du serveur. Pour assurer la sécurité optimale de l'environnement, vous devez remplacer le mot de passe par défaut de l'Administrateur, `changeme`, lors de la configuration initiale du système.

En outre, vous devez configurer un nouveau compte utilisateur pour chaque nouvel utilisateur Oracle ILOM ; chaque compte utilisateur doit être associé à un mot de passe unique et se voir affecter un niveau d'autorisation approprié.

Consultez la documentation d'Oracle ILOM pour en savoir plus sur la configuration des mots de passe, la gestion des utilisateurs et l'application des fonctions de sécurité, notamment de l'authentification SSH (Secure Shell), SSL (Secure Socket Layer) et RADIUS. Pour connaître les consignes de sécurité propres à Oracle ILOM, reportez-vous au *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*, disponible dans la bibliothèque de documentation Oracle ILOM de la version d'Oracle ILOM que vous utilisez. Vous trouverez la documentation relative à Oracle ILOM à l'adresse suivante :

`http://www.oracle.com/goto/ILOM/docs`

Sécurité d'Oracle Hardware Management Pack

Oracle Hardware Management Pack est disponible pour votre serveur, ainsi que pour de nombreux serveurs x86 et certains serveurs SPARC. Ce pack se compose de deux éléments : un agent de surveillance SNMP et un ensemble d'outils d'interface de ligne de commande (outils CLI) multiplateformes pour la gestion du serveur.

Avec les plug-ins SNMP de l'agent de gestion du matériel, vous pouvez utiliser SNMP pour surveiller les serveurs Oracle et les modules serveur de votre centre de données sans avoir à vous connecter aux deux points de gestion que sont l'hôte et Oracle ILOM. Cette fonctionnalité permet d'utiliser une seule adresse IP (celle de l'hôte) pour surveiller plusieurs serveurs et modules serveur. Les plug-ins SNMP s'exécutent sur le système d'exploitation hôte des serveurs Oracle.

Vous pouvez tirer parti des outils de ligne de commande (CLI) de serveur Oracle pour configurer les serveurs Oracle. Les outils CLI sont compatibles avec les systèmes d'exploitation Oracle Solaris, Oracle Linux, Oracle VM, d'autres versions de Linux et Microsoft Windows.

Pour plus d'informations sur ces fonctions, reportez-vous à la documentation relative à Oracle Hardware Management Pack. Pour connaître les consignes de sécurité propres à Oracle Hardware Management Pack, reportez-vous au *Oracle Hardware Management Pack (HMP) Security Guide*, disponible dans la bibliothèque de documentation d'Oracle Hardware Management Pack. Vous trouverez la documentation d'Oracle Hardware Management Pack à l'adresse suivante :

`http://www.oracle.com/goto/OHMP/docs`

Planification d'un environnement sécurisé

Prenez en compte les remarques suivantes avant et pendant l'installation et la configuration d'un serveur et des équipements connexes.

Ce chapitre aborde les sujets suivants :

Recommandations concernant la sécurité du système d'exploitation

Reportez-vous à la documentation relative à votre système d'exploitation (SE) Oracle pour plus d'informations sur les points suivants :

- Utilisation des fonctions de sécurité lors de la configuration des systèmes
- Fonctionnement sécurisé lors de l'ajout d'applications et d'utilisateurs à un système
- Protection des applications réseau

Vous trouverez la documentation relative à la sécurité des systèmes d'exploitation Oracle pris en charge dans les bibliothèques de documentation des systèmes d'exploitation respectifs. Pour trouver la documentation relative à la sécurité d'un système d'exploitation Oracle donné, accédez à la bibliothèque correspondante :

Système d'exploitation	Lien
SE Oracle Solaris	http://docs.oracle.com/cd/E23824_01/html/819-3195/index.html
SE Oracle Linux	http://linux.oracle.com
SE Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

Pour obtenir des informations sur les systèmes d'exploitation d'éditeurs tiers tels que Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows et VMware ESXi, reportez-vous à la documentation des éditeurs concernés.

Ports et commutateurs réseau

Des commutateurs proposent chacun différents niveaux de fonctions de sécurité de port. Reportez-vous à la documentation du commutateur concerné pour savoir comment effectuer les opérations suivantes :

- Utiliser les fonctions d'authentification, d'autorisation et de comptabilisation pour l'accès local et à distance à un commutateur.
- Modifiez chaque mot de passe sur des commutateurs réseau susceptibles de comprendre plusieurs comptes utilisateur et mots de passe par défaut.
- Gérez les commutateurs out-of-band (séparés du trafic de données). Si la gestion out-of-band n'est pas réalisable, il convient de dédier un numéro de réseau local virtuel (VLAN) distinct à la gestion in-band.
- Utilisez la fonctionnalité de mise en miroir des ports du commutateur réseau pour l'accès au système de détection des intrusions (IDS).
- Conservez un fichier de configuration de commutateur hors ligne et réservez-en l'accès aux administrateurs autorisés. Le fichier de configuration doit contenir des commentaires descriptifs pour chaque paramètre.
- Implémentez la sécurité des ports pour limiter l'accès en fonction d'adresses MAC. Désactivez la jonction automatique sur tous les ports.
- Utilisez ces fonctions si elles sont disponibles sur votre commutateur :
  - La fonction **MAC Locking** implique la liaison d'une adresse MAC (Media Access Control) d'un ou de plusieurs périphériques connectés à un port physique sur un commutateur. Si vous verrouillez un port de commutateur avec une adresse MAC particulière, les superutilisateurs ne peuvent pas créer de portes dérobées sur le réseau avec des points d'accès non autorisés.
  - La fonction **MAC Lockout** empêche une adresse MAC spécifiée de se connecter à un commutateur.
  - La fonction **MAC Learning** utilise les informations sur les connexions directes de chaque port de commutateur de sorte que le commutateur réseau puisse configurer la sécurité en fonction des connexions en cours.

Sécurité des réseaux locaux virtuels (VLAN)

Si vous configurez un réseau local virtuel, sachez que les VLAN partagent de la bande passante sur un réseau et nécessitent des mesures de sécurité supplémentaires.

- Définissez des VLAN pour séparer les clusters de systèmes sensibles du reste du réseau. Vous réduisez ainsi le risque de voir des utilisateurs accéder à des informations sur ces clients et serveurs.
- Attribuez un numéro VLAN natif unique aux ports de jonction.
- Limitez les VLAN pouvant être transférés via une jonction à ceux pour qui cela est strictement nécessaire.
- Si possible, désactivez le protocole VTP (VLAN Trunking Protocol). Autrement, définissez les paramètres suivants pour ce protocole : domaine de gestion, mot de passe et nettoyage. Définissez ensuite VTP sur le mode transparent.

Sécurité Infiniband

Les hôtes Infiniband doivent rester sécurisés. La sécurité globale d'un Fabric Infiniband équivaut à celle de l'hôte Infiniband le moins sécurisé.

- Notez que le partitionnement ne protège pas un Fabric Infiniband. Le partitionnement offre uniquement l'isolation du trafic Infiniband entre les machines virtuelles d'un hôte.
- Dans la mesure du possible, utilisez la configuration de VLAN statique.
- Désactivez les ports de commutateur inutilisés et attribuez-leur un numéro VLAN non utilisé.

Sécurité physique du matériel

Le matériel physique peut être sécurisé de manière relativement simple : limitez l'accès au matériel et enregistrez les numéros de série.

- **Limiter l'accès**
  - Installez les serveurs et l'équipement connexe dans un local dont l'accès est restreint et dont la porte est dotée d'un verrou.
  - Si le matériel est installé dans un rack dont la porte est équipée d'un verrou, maintenez-la verrouillée et ne l'ouvrez que pour effectuer la maintenance des composants du rack. Verrouillez la porte après toutes les opérations de maintenance de l'équipement.
  - Limitez l'accès aux consoles USB, qui peuvent offrir un accès plus aisé que les connexions SSH. Les périphériques, tels que les contrôleurs système, les unités de distribution de courant (PDU) et les commutateurs réseau peuvent être équipés de connexions USB.

  - Restreignez l'accès aux périphériques enfichables ou échangeables à chaud, essentiellement parce qu'ils peuvent être facilement retirés.
  - Installez les unités remplaçables sur site (FRU) ou les unités remplaçables par l'utilisateur (CRU) de remplacement dans une armoire verrouillée. Limitez l'accès à l'armoire verrouillée au personnel autorisé.
- **Enregistrer les numéros de série**
  - Apposez une marque de sécurité sur tous les éléments importants du matériel informatique, tels que les FRU. Utilisez des stylos à ultraviolet ou des étiquettes en relief.
  - Enregistrez les numéros de série de l'ensemble de votre matériel.
  - Conservez les clés d'activation et les licences matérielles dans un emplacement sécurisé auquel l'administrateur système peut facilement accéder en cas d'urgence. Les documents imprimés peuvent être votre seule preuve de propriété.

Sécurité des logiciels

La sécurité du matériel passe en grande partie par les logiciels.

- Modifiez tous les mots de passe par défaut lorsque vous installez un nouveau système. La plupart des types d'équipement utilisent des mots de passe par défaut (comme changeme) courants et facilitent l'accès non autorisé.
- Modifiez chaque mot de passe sur des commutateurs réseau susceptibles de comprendre plusieurs comptes utilisateur et mots de passe par défaut.
- Limitez l'utilisation du compte Administrateur par défaut (root) à un seul utilisateur administrateur. Créez systématiquement un nouveau compte Oracle ILOM pour chaque nouvel utilisateur. Assurez-vous qu'un mot de passe unique et un niveau de privilèges approprié (opérateur, administrateur, etc.) sont affectés à chaque compte utilisateur Oracle ILOM.
- Utilisez un réseau dédié pour les processeurs de service afin de les séparer du réseau général.
- Protégez l'accès aux consoles USB. Les périphériques, tels que les contrôleurs système, les unités de distribution de courant (PDU) et les commutateurs réseau, peuvent avoir des connexions USB, qui permettent un accès plus puissant que les connexions SSH.
- Reportez-vous à la documentation qui accompagne votre logiciel pour activer les fonctionnalités de sécurité disponibles pour celui-ci.
- Implémentez la sécurité des ports pour limiter l'accès en fonction d'adresses MAC. Désactivez la jonction automatique sur tous les ports.

Gestion d'un environnement sécurisé

Après l'installation et la configuration initiales, servez-vous des fonctions de sécurité matérielles et logicielles Oracle pour continuer à contrôler le matériel et assurer le suivi des ressources système.

Contrôle de l'alimentation du matériel

Certains systèmes Oracle peuvent être mis sous tension et hors tension à l'aide de logiciels. Les unités de distribution de courant (PDU) de certaines armoires système peuvent être activées et désactivées à distance. Généralement, l'autorisation relative à ces commandes est définie au cours de la configuration du système et réservée aux administrateurs système et au personnel de maintenance.

Reportez-vous à la documentation de votre système ou armoire pour plus d'informations.

Suivi des ressources

Assurez le suivi de l'inventaire à l'aide des numéros de série. Les numéros de série Oracle sont incorporés dans le microprogramme des cartes d'option et des cartes mères système. Ces numéros de série peuvent être lus par le biais de connexions au réseau local.

Vous pouvez également utiliser des lecteurs d'identification par radiofréquence (RFID) pour simplifier davantage le suivi des ressources. Le livre blanc d'Oracle intitulé *How to Track Your Oracle Sun System Assets by Using RFID* est disponible à l'adresse suivante :

```
http://www.oracle.com/
technetwork/articles/systems-hardware-architecture/
o11-001-rfid-oracle-214567.pdf
```

Mises à jour des microprogrammes et des logiciels

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

- Vérifiez régulièrement la présence de mises à jour.
- Installez toujours la dernière version officielle du logiciel ou microprogramme sur votre équipement.
- Le cas échéant, installez les patches de sécurité nécessaires pour votre logiciel.
- N'oubliez pas que les périphériques tels que les commutateurs réseau et les modules Express contiennent un microprogramme et peuvent nécessiter des patches et des mises à jour spécifiques.

Sécurité du réseau

Respectez les consignes suivantes pour garantir la sécurité des accès locaux et distants aux systèmes :

- Limitez la configuration à distance à des adresses IP spécifiques à l'aide de SSH plutôt que Telnet. En effet, Telnet transmet les noms d'utilisateur et mots de passe en texte clair, si bien que toute personne présente sur le segment LAN peut éventuellement voir les informations d'identification. Définissez un mot de passe fiable pour SSH.
- Utilisez la version 3 du protocole SNMP (Simple Network Management Protocol) pour garantir des transmissions sécurisées. Les versions plus anciennes de SNMP ne sont pas sécurisées et transmettent les données d'authentification sous forme de texte non chiffré.
- Si SNMP est nécessaire, remplacez la chaîne de communauté SNMP par défaut par une chaîne de communauté fiable. Dans certains produits, la chaîne de communauté SNMP par défaut est PUBLIC. Des personnes malveillantes peuvent interroger une communauté afin de dessiner un plan très complet du réseau et, le cas échéant, modifier des valeurs de la base d'informations de gestion (MIB).
- Si le contrôleur système emploie une interface de navigateur, veillez à toujours vous en déconnecter après utilisation.
- Désactivez les services réseau non indispensables, tels que TCP (Transmission Control Protocol) ou HTTP (Hypertext Transfer Protocol). Activez les services réseau nécessaires et configurez ces services de manière sécurisée.
- Appliquez les mesures de sécurité LDAP lorsque vous utilisez le protocole LDAP pour accéder au système. Reportez-vous au Guide de sécurité d'Oracle ILOM à l'adresse : `http://www.oracle.com/goto/ILOM/docs`
- Créez une bannière afin d'indiquer que l'accès non autorisé est interdit.
- Utilisez les listes de contrôle d'accès appropriées.

- Définissez des délais d'expiration pour les sessions prolongées, ainsi que des niveaux de privilèges.
- Utilisez les fonctions d'authentification, d'autorisation et de comptabilité (AAA) pour l'accès local et à distance à un commutateur.
- Dans la mesure du possible, utilisez les protocoles de sécurité RADIUS et TACACS+ :
  - RADIUS (Remote Authentication Dial-In User Service) est un protocole client/serveur qui permet de sécuriser les réseaux contre les accès non autorisés
  - TACACS+ (Terminal Access Controller Access-Control System) est un protocole qui permet à un serveur d'accès à distance de communiquer avec un serveur d'authentification pour déterminer si un utilisateur a accès au réseau.
- Utilisez la fonctionnalité de mise en miroir des ports du commutateur pour l'accès au système de détection des intrusions (IDS).
- Implémentez la sécurité des ports pour limiter l'accès en fonction d'une adresse MAC. Désactivez la jonction automatique sur tous les ports.

Protection et sécurité des données

Respectez les consignes suivantes pour optimiser la protection et la sécurité des données :

- Sauvegardez les données importantes à l'aide de périphériques tels que des disques durs externes ou des périphériques de stockage USB. Stockez les données sauvegardées dans un second emplacement sécurisé, hors site.
- Sécurisez les informations confidentielles stockées sur les disques durs à l'aide d'un logiciel de chiffrement des données.
- Lors du retrait d'un ancien disque dur, détruisez-le physiquement ou effacez complètement les données qu'il contient. Il est encore possible de récupérer des données d'un disque après la suppression de fichiers ou le reformatage du disque. Les opérations de suppression des fichiers ou de reformatage d'un disque ont uniquement pour effet de supprimer les tables d'adresses sur le disque. Effacez complètement les données d'un disque à l'aide d'un logiciel de nettoyage de disque.

Gestion des journaux

Contrôlez et assurez à intervalles réguliers la maintenance des fichiers journaux. Sécurisez les fichiers journaux en suivant les méthodes ci-dessous :

- Activez la journalisation et envoyez les journaux système à un hôte de journal sécurisé dédié.
- Configurez la journalisation de manière à inclure des informations horaires exactes, à l'aide du protocole NTP et d'horodatages.
- Consultez les journaux afin de rechercher d'éventuels incidents et archivez-les conformément à la stratégie de sécurité.

- Retirez régulièrement les fichiers journaux lorsque leur taille devient excessive. Conservez des copies des fichiers retirés pour pouvoir vous y reporter à l'avenir ou en vue d'une analyse statistique.