Sun Server X4-8

Guide de sécurité

Référence: E55451-01
Juin 2014

Table des matières

Sécurité de base 5
Accès 5
Authentification 6
Autorisation 6
Comptabilité et audit 7

Utilisation de la configuration du serveur et des outils de gestion de façon sécurisée 9
Sécurité d'Oracle System Assistant 9
Sécurité d'Oracle ILOM 10
Sécurité d'Oracle Hardware Management Pack 12

Planification d'un environnement sécurisé 13
Protection par mot de passe 13
Recommandations concernant la sécurité du système d'exploitation 14
Commutateurs et ports réseau 14
Sécurité des réseaux locaux virtuels (VLAN) 15
Sécurité Infiniband 16

Gestion d'un environnement sécurisé 17
Contrôle de l'alimentation 17
Suivi des ressources 17
Mises à jour des microprogrammes et des logiciels 18
Sécurité du réseau 18
Protection et sécurité des données 19
Maintenance des journaux 20

Sécurité de base

Ce document fournit des instructions générales en matière de sécurité afin de vous aider à protéger votre serveur Oracle, les interfaces réseau du serveur et les commutateurs réseau connectés.

Contactez votre responsable de la sécurité informatique pour connaître les exigences supplémentaires en matière de sécurité qui peuvent s'appliquer à votre système et à votre environnement.

Nous vous recommandons de respecter certaines principes de sécurité de base lorsque vous utilisez un matériel ou un logiciel. Cette section présente les quatre principes de sécurité de base :

- “Accès” à la page 5
- “Authentification” à la page 6
- “Autorisation” à la page 6
- “Comptabilité et audit” à la page 7

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.
- 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.
- 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 physique aux ports USB, aux ports réseau et aux consoles système. Les serveurs et les commutateurs réseau sont dotés de ports et de connexions de console, qui offrent un accès direct au système.
- Limitez la possibilité de redémarrer le système via le réseau.
- 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 la façon dont l'utilisateur est identifié ; il s'agit généralement d'informations confidentielles telles qu'un nom d'utilisateur et un mot de passe. L'authentification garantit 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 permet aux administrateurs de contrôler les tâches et les privilèges qu'un utilisateur peut exécuter ou utiliser. Le personnel peut uniquement effectuer les tâches et utiliser les privilèges qui lui ont été assignés. L'autorisation désigne les restrictions s'appliquant aux employés quant à l'utilisation du matériel et 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.

Comptabilité et audit

La comptabilité et l'audit désignent la création d'un enregistrement des activités d'un utilisateur sur le système. Les serveurs Oracle sont dotés de fonctions matérielles et logicielles permettant aux administrateurs de surveiller les connexions et de tenir à jour les inventaires de 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 qui, en cas de mauvaise utilisation, peuvent provoquer une perte de données Les accès et les commandes doivent être soigneusement contrôlés via les journaux système.
- 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 de la configuration du serveur et des outils de gestion de façon sécurisée

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” à la page 9
- “Sécurité d'Oracle ILOM” à la page 10
- “Sécurité d'Oracle Hardware Management Pack” à la page 12

Contactez votre responsable de la sécurité informatique pour connaître les exigences supplémentaires en matière de sécurité qui peuvent s'appliquer à votre système et à votre environnement.

Sécurité d'Oracle System Assistant

Oracle System Assistant est un outil préinstallé facilitant la configuration et la mise à jour 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 *Guide d'administration des serveurs Oracle de série X4* à l'adresse :

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

Les informations suivantes présentent 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. Oracle System Assistant est intégré à un environnement root amorçable Linux. 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 peuvent 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. Afin d'augmenter le niveau de sécurité, protégez l'accès physique au serveur et attribuez avec parcimonie les privilèges d'administrateur et de console aux utilisateurs d'Oracle ILOM.

Le shell d'Oracle System Assistant est conçu pour permettre aux utilisateurs ayant les privilèges appropriés d'utiliser les outils de CLI d'Oracle Hardware Management Pack à des fins de gestion du système. Le shell n'est pas destiné à fournir des services réseau. Par défaut, les services réseau sont désactivés afin de garantir un niveau optimal de sécurité et ils ne doivent pas être activés.

- **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.

  Afin de garantir un niveau optimal de sécurité, appliquez 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 et les utilisateurs ne peuvent plus 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 l'utilitaire de configuration du BIOS, afin que seuls les utilisateurs autorisés puissent réactiver Oracle System Assistant.

- **Reportez-vous à la documentation d'Oracle System Assistant.**

  Pour plus d'informations sur les fonctions d'Oracle System Assistant, reportez-vous au *Guide d'administration des serveurs Oracle de série X4* :

  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 les serveurs x86 d'Oracle et sur certains serveurs SPARC. 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.

- **Utilisez un réseau interne sécurisé de confiance.**

  Que vous établissiez une connexion de gestion physique à Oracle ILOM via le port série local, le port de gestion réseau dédié ou le port réseau de données standard, il est essentiel que ce port physique sur le serveur soit toujours connecté à un réseau interne de confiance, à un réseau de gestion sécurisé dédié ou à un réseau privé.

  Ne connectez jamais le processeur de services 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.

- **Limitez l'utilisateur du compte Administrateur par défaut.**

  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. Si une personne non autorisée parvient à se connecter au compte Administrateur par défaut, elle dispose d'un accès illimité à toutes les fonctions d'Oracle ILOM. De plus, créez de nouveaux comptes utilisateur avec des mots de passe uniques et des niveaux d'autorisation (rôles utilisateur) pour tous les nouveaux utilisateurs d'Oracle ILOM.

- **Tenez compte des risques potentiels lorsque vous connectez le port série à un serveur terminal.**

  Les périphériques terminaux ne fournissent pas toujours les niveaux adéquats d'authentification utilisateur ou d'autorisation nécessaires à la protection du réseau contre les utilisateurs malveillants. Pour protéger votre système contre les intrusions réseau indésirables, n'établissez pas de connexion série (port série) à Oracle ILOM via tout type de périphérique de redirection réseau, tel qu'un serveur terminal, sauf si le serveur dispose de contrôles d'accès suffisants.

  De plus, certaines fonctions d'Oracle ILOM, telles que la réinitialisation du mot de passe et le menu de préinitialisation, sont uniquement disponibles lors de l'utilisation du port série physique. La connexion du port série à un réseau utilisant un serveur terminal non authentifié élimine la nécessité d'accès physique et réduit le niveau de sécurité associé à ces fonctions.

- **L'accès au menu de préinitialisation nécessite l'accès physique au serveur.**

  Le menu de préinitialisation d'Oracle ILOM est un utilitaire puissant permettant de rétablir les valeurs par défaut d'Oracle ILOM et de flasher le microprogramme si Oracle ILOM ne répond plus. Après la réinitialisation d'Oracle ILOM, l'utilisateur doit appuyer sur un bouton du serveur (le bouton par défaut) ou saisir un mot de passe. La propriété Présence physique d'Oracle ILOM contrôle ce comportement (`check_physical_presence= true`). Afin d'assurer un niveau de sécurité optimal lors de l'accès au menu de préinitialisation, ne modifiez pas le réglage par défaut (`true`) afin que l'accès au menu de préinitialisation nécessite toujours l'accès physique au serveur.

- **Reportez-vous à la documentation d'Oracle ILOM.**

Reportez-vous à la documentation d'Oracle ILOM pour en savoir plus sur la configuration des mots de passe, la gestion des utilisateurs et l'utilisation de fonctions liées à la sécurité. Pour connaître les consignes de sécurité spécifiques d'Oracle ILOM, reportez-vous au *Guide de sécurité d'Oracle ILOM*, disponible dans la bibliothèque de documentation Oracle ILOM. 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 et pour de nombreux autres serveurs x86 Oracle ainsi que certains serveurs Oracle 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.

- **Utilisez les plug-ins SNMP de l'agent de gestion du matériel.**

  Le protocole standard SNMP permet de surveiller ou de gérer un système. Avec les plug-ins SNMP de l'agent de gestion du matériel, vous pouvez surveiller les serveurs Oracle de votre centre de données par le biais de SNMP 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.

  Les plug-ins SNMP s'exécutent sur le système d'exploitation hôte des serveurs Oracle. Le module plug-in SNMP étend l'agent SNMP natif dans le système d'exploitation hôte de manière à offrir des fonctions Oracle MIB supplémentaires. Oracle Hardware Management Pack ne contient pas d'agent SNMP. Pour Linux, un module est ajouté à l'agent net-snmp. Pour Oracle Solaris, un module est ajouté à l'agent de gestion Oracle Solaris. Pour Microsoft Windows, le plug-in étend le service SNMP natif. Tous les paramètres de sécurité liés à SNMP d'Oracle Hardware Management Pack sont déterminés par les paramètres de l'agent ou service SNMP natif, et non par le plug-in.

  Les versions SNMPv1 et SNMPv2c n'offrent pas de chiffrement et procèdent à l'authentification à l'aide de chaînes de communauté. En revanche, SNMPv3 est plus sécurisé et est la version que nous vous recommandons d'utiliser car elle met en oeuvre le chiffrement pour fournir un canal sécurisé, ainsi que des noms et mots de passe utilisateur individuels.

- **Reportez-vous à la documentation d'Oracle Hardware Management Pack :**

  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

Des instructions en matière de sécurité doivent être mises en place avant la livraison du système. Après la livraison du système, les instructions de sécurité doivent être contrôlées et adaptées de façon régulière afin de rester conforme avec les exigences de votre société en matière de sécurité. Utilisez les informations de cette section avant et pendant l'installation et la configuration d'un serveur et des équipements associés.

Cette section aborde les sujets suivants :

- “Protection par mot de passe” à la page 13
- “Recommandations concernant la sécurité du système d'exploitation” à la page 14
- “Commutateurs et ports réseau” à la page 14
- “Sécurité des réseaux locaux virtuels (VLAN)” à la page 15
- “Sécurité Infiniband” à la page 16

Contactez votre responsable de la sécurité informatique pour connaître les exigences supplémentaires en matière de sécurité qui peuvent s'appliquer à votre système et à votre environnement.

Protection par mot de passe

Les mots de passe représentent un aspect important de la sécurité : des mots de passe trop faibles peuvent entraîner des accès non autorisés aux ressources de la société. La mise en place de pratiques recommandées pour la gestion des mots de passe permet de garantir que les utilisateurs respectent un ensemble de directives pour la création et la protection de leurs mots de passe. Les composants habituels d'une stratégie de mot de passe doivent définir les éléments suivants :

- Longueur et niveau de sécurité du mot de passe
- Durée du mot de passe
- Pratiques courantes en matière de mot de passe

Mettez en place les pratiques standard suivantes afin de créer des mots de passe complexes :

- 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.

Modifiez régulièrement vos mots de passe. Cela permet de réduire les risques d'activité malveillante et garantit la conformité des mots de passe aux stratégies en vigueur.

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://www.oracle.com/technetwork/documentation/ol-1-1861776.html
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, Microsoft Windows et VMware ESXi, reportez-vous à la documentation des éditeurs concernés.

Commutateurs et ports réseau

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

- Utilisez 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.

- Séparez les clusters de systèmes sensibles du reste du réseau lorsque vous utilisez des VLAN. 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.
- Dans la mesure du possible, utilisez des configurations de VLAN statiques.

- Désactivez les ports de commutateur inutilisés et attribuez-leur un numéro VLAN non utilisé.

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.

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 les logiciels.

- “Contrôle de l'alimentation” à la page 17
- “Suivi des ressources” à la page 17
- “Mises à jour des microprogrammes et des logiciels” à la page 18
- “Sécurité du réseau” à la page 18
- “Protection et sécurité des données” à la page 19
- “Maintenance des journaux” à la page 20

Contactez votre responsable de la sécurité informatique pour connaître les exigences supplémentaires en matière de sécurité qui peuvent s'appliquer à votre système et à votre environnement.

Contrôle de l'alimentation

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 (LAN).

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

Les améliorations de sécurité sont intégrées via de nouvelles versions du logiciel et des patchs. La gestion efficace et proactive des patchs est une partie essentielle de la sécurité du système. Afin d'optimiser la sécurité de votre système, mettez celui-ci à jour avec les dernières versions de logiciels et tous les patchs de sécurité nécessaires.

- Vérifiez régulièrement l'existence de mises à jour logicielles et de patchs de sécurité.
- Installez toujours la dernière version officielle d'un logiciel ou d'un microprogramme.
- Le cas échéant, installez les patchs de sécurité nécessaires pour votre logiciel.
- N'oubliez pas que les périphériques comme les commutateurs réseau contiennent également un microprogramme et peuvent nécessiter des patchs et des mises à jour spécifiques.

Sécurité du réseau

Une fois que les réseaux sont configurés selon des principes de sécurité, vous devez assurer un contrôle et une maintenance réguliers.

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 de réseau local (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.
- Créez un message d'accueil qui s'affiche lors de la connexion afin d'informer l'utilisateur que tout accès non autorisé est interdit. Vous pouvez également informer les utilisateurs de toute stratégie ou règle importante. Un message d'accueil permet par exemple d'avertir les utilisateurs de restrictions d'accès particulières à un système spécifique ou de leur rappeler les stratégies définies en matière de mots de passe et leur utilisation appropriée.
- Utilisez les listes de contrôle d'accès appropriées pour appliquer des restrictions.
- 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 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.
- Appliquez les mesures de sécurité LDAP lorsque vous utilisez le protocole LDAP pour accéder au système.
- 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.

Pour plus d'informations sur la sécurité réseau, reportez-vous au *Guide de sécurité d'Oracle ILOM*, qui appartient à la bibliothèque de documentation Oracle ILOM. Vous trouverez la documentation relative à Oracle ILOM à l'adresse suivante :

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

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.

Maintenance 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.
- Effectuez des analyses planifiées régulière des fichiers journaux des périphériques réseau afin de détecter toute activité ou accès inhabituels sur le réseau.
- 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.