

Netra Server X3-2 (anciennement serveur Sun Netra X4270 M3)

Guide de sécurité

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

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

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Table des matières

- Guide de sécurité du serveur Netra Server X3-25
 - Présentation du système5
 - Principes de sécurité5
 - Utilisation des outils de configuration et de gestion de serveur7
 - Planification d'un environnement sécurisé9
 - Gestion d'un environnement sécurisé 11

Guide de sécurité du serveur Netra Server X3-2

Ce document formule des recommandations générales en matière de sécurité pour vous aider à protéger le serveur Netra Server X3-2 (anciennement serveur Sun Netra X4270 M3) d'Oracle, ses interfaces réseau et les commutateurs réseau auxquels il est connecté.

Ce chapitre contient les sections suivantes :

- [“Présentation du système” à la page 5](#)
- [“Principes de sécurité” à la page 5](#)
- [“Utilisation des outils de configuration et de gestion de serveur” à la page 7](#)
- [“Planification d'un environnement sécurisé” à la page 9](#)
- [“Gestion d'un environnement sécurisé” à la page 11](#)

Présentation du système

Le Netra Server X3-2, serveur au format 2U de qualité professionnelle, compatible avec la norme NEBS et doté de deux processeurs, prend en charge 16 modules DIMM DDR3 (huit par processeur), six emplacements PCIe Gen3, ainsi que six ou huit unités de stockage SAS/SATA. Le modèle à six unités comprend également un lecteur de DVD.

Le serveur inclut un processeur de service (SP) Oracle Integrated Lights Out Manager (Oracle ILOM) intégré. Un outil de configuration nommé Oracle System Assistant est également inclus sur une unité USB en tant que partie intégrante de la configuration du serveur.

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.
- Consultez la documentation qui accompagne votre logiciel pour activer les fonctionnalités de sécurité disponibles.

- Installez les serveurs et l'équipement connexe dans un local dont l'accès est restreint et dont la porte est fermée à clé.
- 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 comme les contrôleurs système, les unités de distribution de courant 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.
- Stockez les unités remplaçables sur site et les unités remplaçables par l'utilisateur 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'autorisation 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 mère.
- 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 *Guide d'administration* à l'adresse :

http://docs.oracle.com/cd/E27124_01

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 sont en mesure d'accéder à Oracle System Assistant et au shell root.

Un environnement root permet d'accéder à la configuration et aux stratégies d'un système, ainsi qu'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 lors de 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, ce qui constitue une faille 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 être réactivé uniquement 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* à l'adresse :

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 le serveur, sur d'autres serveurs x86 d'Oracle et sur certains serveurs SPARC.

Installez le processeur de service sur un réseau dédié afin de le séparer du réseau général. Limitez l'utilisation du compte superutilisateur root. Dans la mesure du possible, attribuez plutôt des comptes Oracle ILOM comme `ilom-operator` et `ilom-admin`. 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.

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 manuel *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*, disponible dans la bibliothèque de documentation d'Oracle ILOM 3.1. Vous trouverez la documentation relative à Oracle ILOM 3.1 à l'adresse suivante :

http://docs.oracle.com/cd/E24707_01

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 surveiller les serveurs Oracle et les modules serveur 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 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) 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 manuel *Guide de sécurité d'Oracle Hardware Management Pack (HMP)*, 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://docs.oracle.com/cd/E20451_01

Planification d'un environnement sécurisé

Consultez les informations suivantes lors de l'installation et de la configuration du serveur et du matériel associé.

Consignes sur les systèmes d'exploitation Oracle

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 :

- **Oracle Solaris** : http://docs.oracle.com/cd/E23824_01
- **Oracle Linux** : <http://linux.oracle.com/documentation/>
- **Oracle VM** : <http://www.oracle.com/technetwork/documentation/vm-096300.html>

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.
- Modifier chaque mot de passe sur des commutateurs réseau susceptibles de comprendre plusieurs comptes utilisateur et mots de passe par défaut.
- Gérer 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.
- Utiliser la fonctionnalité de mise en miroir des ports du commutateur réseau pour l'accès au système de détection des intrusions (IDS).
- Conserver un fichier de configuration de commutateur hors ligne et en réserver l'accès aux administrateurs autorisés. Le fichier de configuration doit contenir des commentaires descriptifs pour chaque paramètre.
- Implémenter la sécurité des ports pour limiter l'accès en fonction d'une adresse MAC. Désactiver la jonction automatique sur tous les ports.
- Utiliser 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 d'un réseau local virtuel (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 les VLAN dans des clusters de systèmes sensibles séparés 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 libres et attribuez-leur un numéro VLAN non utilisé.

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. Pour plus d'informations, reportez-vous à la documentation relative à votre système ou votre armoire.

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 d'un logiciel ou d'un microprogramme.
- Le cas échéant, installez les patches de sécurité nécessaires aux logiciels.
- N'oubliez pas que les périphériques comme les commutateurs réseau contiennent également un microprogramme et peuvent nécessiter des patches et des mises à jour spécifiques.

Accès 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-les de manière sécurisée.

Protection des données

Respectez les consignes suivantes pour optimiser la sécurité des données.

- Sauvegardez les données importantes à l'aide de périphériques tels que des disques durs externes, des clés USB ou des cartes mémoire MS. 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.
- Archivez régulièrement les fichiers journaux lorsque leur taille devient excessive, puis réinitialisez les journaux. Vous pouvez vous servir des fichiers archivés pour référence ou en vue d'une analyse statistique.

