Guide de sécurité de Netra Modular System

Référence: E68383-01
Août 2015

Référence: E68383-01

Accessibilité de 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`.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez 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.

Table des matières

Présentation de la sécurité

Le Système modulaire Netra d'Oracle est une plate-forme préintégrée et précâblée susceptible d'être entièrement virtualisée pour réduire les coûts et le temps de déploiement dans votre centre de données. Le système modulaire inclut le matériel que vous avez spécifié, est assemblé à l'usine, puis vous est livré.

Les rubriques suivantes décrivent les concepts de sécurité et les fonctionnalités du système modulaire :

Principes de sécurité élémentaires

Suivez ces principes de sécurité de base pour tous les logiciels et matériels du système modulaire :

- 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, ou de clés partagées. L'authentification garantit que les utilisateurs du matériel ou des logiciels sont bien ceux qu'ils prétendent être. Par défaut, les noms d'utilisateur et mots de passe locaux servent à l'authentification. L'authentification par clé partagée est aussi disponible.
- Comptabilité et audit : la comptabilité et l'audit sont garants du registre des activités d'un utilisateur sur le système. Le logiciel et le matériel du système modulaire sont dotés de fonctions matérielles et logicielles permettant aux administrateurs de surveiller les connexions et de tenir à jour les inventaires de matériel :
  - Les informations de connexion des utilisateurs sont contrôlées via des journaux système. Les comptes d'administrateur système et de maintenance ont accès aux commandes qui, utilisées de façon incorrecte, sont susceptibles de causer des dommages et des pertes de données.
  - Les ressources matérielles sont suivies à l'aide de numéros de série. Les numéros de référence Oracle sont enregistrés au format électronique sur toutes les cartes, modules et cartes mères, et peuvent être utilisés à des fins d'inventaire.

Considérations relatives à la sécurité avancée

En plus des principes de sécurité de base, le système modulaire prend en charge la capacité de survie et la défense en profondeur. Le système modulaire propose un ensemble bien intégré d'outils de sécurité pour répondre aux importantes exigences et préoccupations de sécurité. Les sections suivantes décrivent ces principes :

- Capacité de survie aux charges de travail stratégiques : les organisations qui choisissent des plates-formes matérielles et logicielles pour leurs charges de travail stratégiques peuvent être sûres que le système modulaire est en mesure d'empêcher ou de minimiser les dommages causés par des événements accidentels ou malveillants auxquels ont pris part des utilisateurs internes ou des tiers. Appartenant aux meilleures pratiques Oracle Maximum Availability Architecture, les pratiques suivantes augmentent la capacité de survie :
  - Assurer que les composants utilisés ont été conçus, fabriqués et testés pour fonctionner correctement et prendre en charge les architectures de déploiement sécurisées. Le système modulaire prend en charge l'isolement de sécurité, le contrôle d'accès, la qualité de service et la gestion sécurisée.
  - Réduire la surface d'attaque par défaut des produits qui la composent permet de réduire l'exposition globale de la machine.
  - Protéger la machine, y compris ses interfaces d'exploitation et de gestion, avec un complément de protocoles ouverts et approuvés, et d'API capables de prendre en charge les objectifs de sécurité traditionnels relatifs à la robustesse de l'authentification, au contrôle d'accès, à la confidentialité, à l'intégrité et à la disponibilité.
  - Vérifier que les logiciels et le matériel contiennent les fonctionnalités en mesure d'assurer la disponibilité du service, même en cas de défaillance. Ces capacités sont utiles en cas d'attaque impliquant une tentative de désactivation d'un ou plusieurs composants individuels du système.
- Sécuriser l'environnement d'exploitation avec défense en profondeur : le système modulaire applique plusieurs contrôles de sécurité indépendants et se renforçant mutuellement pour permettre de créer un environnement d'exploitation sûr pour les charges de travail et les données. Le système modulaire prend en charge le principe de défense en profondeur comme suit :
  - Offrir un complément robuste de protections pour sécuriser les données en transit, en utilisation et inactives. Des contrôles de sécurité sont disponibles au niveau du serveur et des couches réseau. Les contrôles de sécurité uniques à chaque couche peuvent être intégrés aux autres pour permettre la création d'architectures de sécurités robustes et en couches.
  - Prendre en charge l'utilisation de normes, de protocoles et d'interfaces clairement définis et ouverts. Le système modulaire peut être intégré à des stratégies, des architectures, des pratiques et des normes de sécurité existantes.

Fonctions de sécurité

Le matériel et le logiciel du système modulaire sont sécurisés. Oracle fournit également des configurations de sécurité recommandées pour les services tels que les protocoles NTP et SSH. De plus, l'architecture du système modulaire fournit des capacités de sécurité aux composants principaux. Ces fonctionnalités de sécurité sont le plus souvent appliquées par des organisations qui déploient une stratégie de sécurité en couches. Les fonctionnalités sont regroupées dans les catégories suivantes :

- "Isolement du trafic réseau" à la page 9
- "Gestion sécurisée avec Oracle ILOM" à la page 9

Isolement du trafic réseau

Si vous souhaitez consolider l'infrastructure informatique, mettre en oeuvre des architectures de service partagé et fournir des services partagés sécurisés, envisagez d'isoler le trafic du réseau. Le système modulaire fournit la flexibilité nécessaire à la mise en oeuvre des stratégies d'isolement en fonction de vos besoins.

Au niveau du réseau physique, l'accès client est isolé de la gestion des périphériques et des communications entre périphériques. Le trafic du réseau client et celui du réseau de gestion sont isolés sur des réseaux indépendants. L'accès client est fourni sur un réseau Ethernet 10 Gbps redondant qui assure un accès fiable et très rapide aux services s'exécutant sur le système. L'accès de gestion est fourni sur réseau Ethernet 1 Gbps physiquement indépendant. Cela permet une séparation entre les réseaux d'exploitation et de gestion.

Les organisations peuvent choisir de séparer davantage le trafic du réseau sur le réseau Ethernet d'accès client en configurant des réseaux virtuels (VLAN). Les réseaux virtuels séparent le trafic du réseau selon leurs exigences. Oracle recommande d'utiliser des protocoles chiffrés sur les réseaux virtuels pour assurer la confidentialité et l'intégrité des communications.

Gestion sécurisée avec Oracle ILOM

Les collectes des contrôles et des fonctionnalités de sécurité sont nécessaires pour sécuriser correctement les applications et les services individuels. Il est tout aussi important de disposer de capacités de gestion complètes pour prendre en charge la sécurité des services et des systèmes déployés. Le système modulaire utilise les capacités de gestion de sécurité d'Oracle ILOM.

Oracle ILOM est un processeur de service intégré aux noeuds de calcul du système modulaire. Oracle ILOM sert à effectuer des activités de gestion out-of-band, telles que les suivantes :

- Fournir un accès sécurisé pour effectuer une gestion à distance sécurisée des bases de données et des serveurs de stockage. L'accès inclut un accès par le Web protégé par SSL et un accès par ligne de commande avec les protocoles Secure Shell, IPMI v2.0 et SNMPv3.
- Séparer les exigences de service en utilisant un modèle de contrôle d'accès basé sur les rôles. Les utilisateurs individuels sont affectés à des rôles spécifiques qui limitent la disponibilité des fonctions.
- Fournir un registre d'audit de l'intégralité des connexions et des changements de configuration. Chaque entrée du journal d'audit répertorie l'utilisateur, l'action effectuée et un horodatage. Le registre d'audit permet aux organisations de détecter des activités ou des modifications non autorisés, et d'attribuer ces actions à des utilisateurs précis.

Pour plus d'informations à propos de la sécurité d'Oracle ILOM, reportez-vous au *Guide de sécurité d'Oracle ILOM* à l'adresse suivante : `http://www.oracle.com/goto/ILOM/docs`.

Planification d'un environnement sécurisé

Établissez les consignes de sécurité avant l'arrivée du Système modulaire Netra. Une fois le système installé, révisez et ajustez régulièrement les consignes de sécurité afin de rester conforme avec les exigences de votre organisation en matière de sécurité.

Ces rubriques indiquent les consignes de sécurité pour l'installation du Système modulaire Netra.

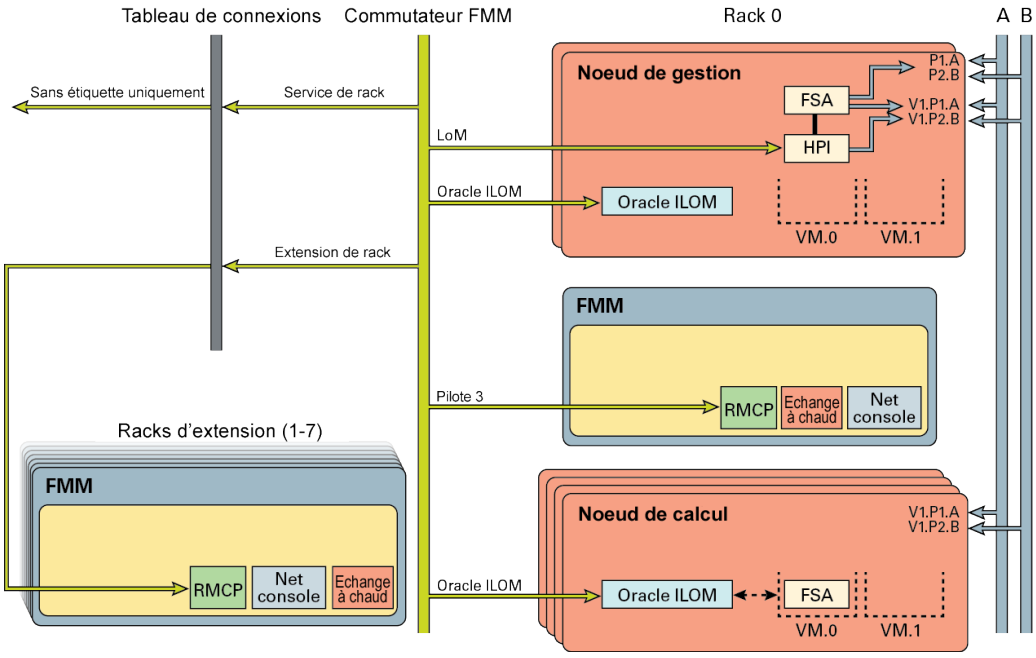
- "Réseau par défaut" à la page 11
- "Comptes utilisateur" à la page 12
- "Paramètres de sécurité par défaut" à la page 12

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.

Réseau par défaut

Les illustrations et descriptions suivantes expliquent le réseau par défaut du Système modulaire Netra.

- Le réseau système / de télémesures (light green network) inclut le port LoM du noeud de gestion sur réseau virtuel 4090 via le commutateur FMM.
- Le réseau ILOM de télémesures sur le réseau virtuel 4094 interne via FMM inclut des noeuds de calcul Oracle ILOM et des noeuds réseau Oracle ILOM via le commutateur FMM.
- Le tableau de connexion prolonge le réseau de télémesures aux racks 1 à 7. Une configuration multi-rack prend en charge les mêmes sous-réseaux et réseaux virtuels avec un différent ID de rack
- Le réseau virtuel (1) fournit d'autres services au réseau de télémesures via une authentification adéquate.
- Les réseaux de données (A &B) fournissent un accès in-band au noeud FSA.
- L'application HA peut gérer les racks via les interfaces exposées du système modulaire (JMX, C- API, etc.).



Comptes utilisateur

Ce tableau répertorie les utilisateurs et mots de passe par défaut des composants du système modulaire. Modifiez tous les mots de passe par défaut après avoir installé le Système modulaire Netra.

Composant	Nom d'utilisateur et mot de passe
Commutateurs Ethernet	`root/changeme` **Remarque -** Sécurisez les valeurs `enable mode password` et `secret` de l'utilisateur `admin`.
Noeuds de gestion et de calcul	`root/changeme`

Paramètres de sécurité par défaut

Le système modulaire est installé avec de nombreux paramètres de sécurité par défaut. Dès que vous en avez l'occasion, configurez les paramètres de sécurité par défaut. Reportez-vous

aux paramètres par défaut de votre version d'Oracle ILOM à l'adresse suivante : http://www.oracle.com/goto/ILOM/docs.

Sécurisation du matériel

L'isolement physique et le contrôle d'accès constituent la base de votre architecture de sécurité. Un système physique installé dans un environnement sécurisé est protégé contre tout accès non autorisé. De même, le fait d'enregistrer tous les numéros de série permet d'empêcher l'utilisation de composants matériels non autorisés.

Les sections ci-après fournissent des recommandations générales concernant la sécurité matérielle des systèmes modulaires

Restrictions d'accès

- Installez les systèmes 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 dotée d'un verrou, verrouillez toujours celle-ci jusqu'à ce que vous deviez effectuer la maintenance des composants du rack. Le verrouillage des portes permet également de restreindre l'accès aux périphériques enfichables ou échangeables à chaud.
- Stockez toute les pièces de rechange dans une armoire verrouillée. Limitez l'accès à l'armoire verrouillée au personnel autorisé.
- Vérifiez régulièrement l'état et l'intégrité des verrous du rack et de l'armoire contenant les disques de rechange afin de vous assurer qu'ils ne sont pas abîmés ou que les portes n'ont pas été laissées déverrouillées.
- Conservez les clés de l'armoire dans un endroit sécurisé dont l'accès est limité.
- Limitez l'accès aux consoles USB. Les périphériques, tels que les contrôleurs système, les unités de distribution de courant et les commutateurs réseau peuvent être équipés de connexions USB. L'accès physique constitue une méthode d'accès à un composant plus sécurisée dans la mesure où il ne risque aucune attaque réseau.
- Connectez la console à un périphérique KVM externe afin d'activer l'accès à la console à distance. Les périphériques KVM prennent souvent en charge une authentification à deux facteurs, un contrôle des accès centralisé et des procédures d'audit. Pour plus d'informations

sur les recommandations en matière de sécurité et les bonnes pratiques relatives aux périphériques KVM, reportez-vous à la documentation fournie avec le périphérique KVM.

Numéros de série

Empêchez l'utilisation de composants matériels non autorisés en enregistrant soigneusement tous les numéros de série lors de la réception et de la mise en stock des composants. Avant l'installation ou l'utilisation d'un composant, vérifiez qu'il est authentique en comparant son numéro de série avec celui qui a été enregistré au moment de sa réception. Pour la sécurité du matériel, respectez la procédure suivante :

- Enregistrez les numéros de série de l'ensemble de votre matériel.
- Apposez une marque de sécurité sur tous les éléments importants du matériel informatique, tels que les pièces de rechange. Utilisez des stylos à ultraviolet ou des étiquettes en relief.
- 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.

Les lecteurs d'identification par radiofréquence (RFID) peuvent simplifier davantage le suivi des ressources. Reportez-vous au livre blanc d'Oracle intitulé *How to Track Your Oracle Sun System Assets by Using RFID* disponible à l'adresse suivante : `http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf`.

Unités de disque dur

Les unités de disque dur servent généralement à stocker des informations sensibles. Pour protéger ces informations d'une divulgation non autorisée, nettoyez les unités de disque dur avant de les réutiliser, ou de les mettre hors service ou au rebut.

- Reportez-vous aux stratégies de protection des données afin d'identifier la méthode la plus adaptée pour nettoyer les unités de disque dur.
- Si nécessaire, utilisez le service de conservation des périphériques et des données client d'Oracle.

  `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

Sécurisation du logiciel

La sécurité du matériel passe en grande partie par des logiciels. Les sections ci-après fournissent des recommandations générales concernant la sécurité logicielle du Système modulaire Netra.

▼ Protection contre les accès non autorisés (Oracle Linux)

- **Utilisez les commandes du SE Oracle Linux Solaris pour limiter l'accès au logiciel, sécuriser le SE, utiliser des fonctions de sécurité et protéger les applications.**

  Reportez-vous au *Guide de sécurité d'Oracle Linux Release 6* à l'adresse suivante : `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`

▼ Protection contre les accès non autorisés (Oracle ILOM)

- **Utilisez les commandes Oracle ILOM pour limiter l'accès au microprogramme Oracle ILOM, modifier le mot de passe défini en usine, limiter l'utilisation du compte de superutilisateur root et sécuriser le réseau privé au niveau du processeur de service.**

  Reportez-vous à votre version du *Guide de sécurité d'Oracle ILOM* à l'adresse suivante : `http://www.oracle.com/goto/ILOM/docs`.

▼ Protection contre les accès non autorisés (Oracle VM Server With Oracle Linux)

- **Utilisez les commandes d'Oracle Linux Solaris pour limiter l'accès au logiciel Oracle VM Server, utiliser des fonctions de sécurité et protéger les applications.**

  Reportez-vous au *Guide de sécurité d'Oracle VM Security Release 3* à l'adresse suivante : `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`.

Sécurité d'Oracle Hardware Management Pack

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 système.

- Plug-ins SNMP agent de gestion du matériel : SNMP est un protocole standard qui contrôle ou gère un système. Avec les plug-ins SNMP de l'agent de gestion du matériel, vous pouvez surveiller les systèmes Oracle de votre centre de données par le biais de SNMP sans avoir à vous connecter aux deux points de gestion: l'hôte et Oracle ILOM. Cette fonctionnalité permet d'utiliser une seule adresse IP (celle de l'hôte) pour surveiller plusieurs systèmes.

  Les plug-ins SNMP s'exécutent sur le SE hôte des systèmes Oracle. Le plug-in SNMP étend l'agent SNMP natif dans le SE hôte de manière à offrir des fonctions Oracle MIB supplémentaires. Oracle Hardware Management Pack ne contient pas d'agent SNMP. Pour Oracle Linux, un module est ajouté à l'agent `net-snmp`. 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.
- Documentation d'Oracle Hardware Management Pack : pour connaître les consignes de sécurité propres à Oracle Hardware Management Pack, reportez-vous au *Guide de sécurité d'Oracle Hardware Management Pack (HMP)* à l'adresse suivante : `http://www.oracle.com/goto/OHMP/docs`.

Localisation des guides de sécurité connexes

Guides de sécurité

Ces guides décrivent les stratégies et les procédures pour assurer la sécurité des produits connexes :

- *Oracle Server X5-2 Security Guide*
- *Oracle Switch ES2-72 and Oracle Switch ES2-64 Security Guide*
- *Guide de sécurité d'Oracle Linux Release 6* à l'adresse suivante : `http://docs.oracle.com/cd/E37670_01/E36387/html/index.html`
- *Guide de sécurité d'Oracle ILOM* à l'adresse suivante : `http://www.oracle.com/goto/ILOM/docs`
- *Guide de sécurité d'Oracle VM Release 3.3* à l'adresse suivante : `http://docs.oracle.com/cd/E50245_01/E50254/html/index.html`
- *Guide de sécurité d'Oracle Hardware Management Pack (HMP)* à l'adresse suivante : `http://www.oracle.com/goto/OHMP/docs`