Système SuperCluster

Guide de sécurité

Référence: E48457-01
Juillet 2013

Table des matières

1. Guide de sécurité du système SuperCluster 5
Présentation des principes de sécurité 5
Planification d'un environnement sécurisé 6
Sécurité du matériel 6
Sécurité des logiciels 6
Sécurité des microprogrammes 7
Microprogramme Oracle ILOM 7
Gestion d'un environnement sécurisé 8
Contrôles du matériel 8
Suivi des ressources 8
Logiciel et microprogramme 8
Accès local et à distance 8
Sécurité des données 9
Sécurité du réseau 9
Guides de sécurité connexes 10

• • • Chapitre 1

Guide de sécurité du système SuperCluster

Ce document livre des recommandations de sécurité générales visant à vous aider à protéger vos produits matériels Oracle tels que vos serveurs, vos commutateurs réseau, vos cartes d'interface réseau, etc.

Ce chapitre contient les sections suivantes :

- “Présentation des principes de sécurité” à la page 5
- “Planification d'un environnement sécurisé” à la page 6
- “Gestion d'un environnement sécurisé” à la page 8
- “Guides de sécurité connexes” à la page 10

Présentation des principes de sécurité

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

- Accès

  Les contrôles physiques et logiciels sont nécessaires pour protéger votre matériel ou vos données contre les intrusions.
  - Pour le matériel, les limites d'accès correspondent généralement à des limites d'accès *physiques*.
  - Pour les logiciels, l'accès est limité à l'aide de moyens physiques et virtuels.
  - Les microprogrammes peuvent uniquement être modifiés par le processus de mise à jour Oracle.
- Authentification

  Les systèmes d'exploitation de toutes les plates-formes fournissent des fonctions d'authentification qui peuvent être configurées de façon à s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être.

  L'authentification fournit divers degrés de sécurité grâce à des mesures telles que les badges et les mots de passe.
- Autorisation

  L'autorisation permet au personnel de la société d'utiliser uniquement le matériel et les logiciels pour lesquels ils ont été formés et certifiés. A cette fin, les administrateurs système créent des

systèmes d'autorisations de lecture/d'écriture/d'exécution pour contrôler l'accès des utilisateurs aux commandes, à l'espace disque, aux périphériques et aux applications.

- Comptabilisation

  Les fonctions logicielles et matérielles Oracle permettent au service informatique de la société de surveiller l'activité de connexion et de tenir à jour des inventaires matériels.

  - Les informations de connexion des utilisateurs peuvent être contrôlées via des journaux système. Les comptes d'administrateur système et de maintenance, en particulier, ont accès à des commandes puissantes et doivent être soigneusement contrôlés via les journaux système. Les journaux sont généralement conservés pendant une longue période, de sorte qu'il est essentiel de retirer régulièrement les fichiers journaux lorsqu'ils dépassent une taille raisonnable, conformément à la politique de la société.
  - Les ressources informatiques du client sont généralement suivies à l'aide de numéros de série. Les numéros de référence Oracle sont enregistrés au format électronique sur l'ensemble des cartes, modules et cartes mères, et peuvent être utilisés à des fins d'inventaire.

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.

Sécurité 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 dotée d'un verrou, verrouillez toujours celle-ci jusqu'à ce que vous deviez effectuer la maintenance des composants du rack.
  - Les périphériques enfichables à chaud sont retirés facilement et requièrent particulièrement un accès limité.
  - Stockez 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 des logiciels.

- Lorsqu'un nouveau système est installé, modifiez tous les mots de passe par défaut. La plupart des types d'équipement utilisent des mots de passe par défaut (comme **changeme**) courants et facilitent l'accès non autorisé. En outre, les périphériques tels que les commutateurs réseau peuvent avoir

plusieurs comptes d'utilisateur par défaut. Assurez-vous de modifier tous les mots de passe de compte.

- Limitez l'utilisation du compte superutilisateur `root`. Utilisez plutôt dans la mesure du possible des comptes Oracle Integrated Lights Out Manager (Oracle ILOM), tels que `ilom-operator` et `ilom-admin`.
- Utilisez un réseau dédié pour les processeurs de service afin de les séparer du réseau général.
- Au cours du processus d'installation d'Oracle Solaris, vous serez invité à créer un compte utilisateur et un mot de passe, ainsi qu'un mot de passe **root** pour le système. Dans le cadre de ce processus, l'utilisateur **root** est un rôle que vous prenez. Si vous souhaitez modifier les paramètres de ce compte, vous pouvez supprimer le compte d'utilisateur **root** et attribuer le rôle root à un utilisateur doté de privilèges moindres.
- 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.
- Un serveur peut être initialisé en toute sécurité avec l'initialisation via connexion WAN ou l'initialisation iSCSI. Pour plus d'informations, reportez-vous au manuel *Guide d'installation d'Oracle Solaris : Installations basées sur réseau* de votre version d'Oracle Solaris.

Le document Directives de sécurité d'Oracle Solaris fournit les informations suivantes :

- Sécurisation d'Oracle Solaris
- Utilisation des fonctions de sécurité Oracle Solaris lorsque vous configurez vos systèmes
- Fonctionnement sécurisé lors de l'ajout d'applications et d'utilisateurs à un système
- Protection des applications réseau

Les documents détaillant les recommandations de sécurité pour Oracle Solaris sont disponibles à l'adresse suivante :

- http://www.oracle.com/technetwork/indexes/documentation/index.html#sys_sw

Sécurité des microprogrammes

Les comptes utilisateur standard ne peuvent pas modifier le programme OpenBoot PROM (OBP) ou d'autres microprogrammes Oracle. Le système d'exploitation Oracle Solaris utilise un processus contrôlé de mise à jour des microprogrammes pour empêcher les modifications non autorisées des microprogrammes. Seul le superutilisateur peut utiliser le processus de mise à jour.

Pour plus d'informations sur la configuration des variables de sécurité OBP, reportez-vous au manuel *OpenBoot 4.x Command Reference Manual* à l'adresse suivante :

- http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

Microprogramme Oracle ILOM

Oracle Integrated Lights Out Manager (Oracle ILOM) est un microprogramme de gestion système préinstallé sur certains serveurs SPARC. Oracle ILOM vous permet de gérer et de contrôler de manière active les composants installés sur le système. Votre utilisation d'Oracle ILOM a une incidence sur la sécurité de votre système. Pour en savoir plus sur l'utilisation de ce microprogramme lors de la configuration des mots de passe, de la gestion des utilisateurs et de l'application des fonctions de

sécurité, y compris l'authentification SSH (Secure Shell), SSL (Secure Socket Layer) et RADIUS, reportez-vous à la documentation d'Oracle ILOM :

- http://www.oracle.com/pls/topic/lookup?ctx=E19860-01

Gestion d'un environnement sécurisé

Le matériel et les logiciels Oracle fournissent un certain nombre de fonctions de sécurité qui permettent de contrôler le matériel et d'effectuer le suivi des ressources.

Contrôles du matériel

Certains systèmes Oracle peuvent être configurés de sorte à être activés ou désactivés à l'aide de commandes logicielles. En outre, les unités de distribution de courant (PDU) de certaines armoires système peuvent être activées et désactivées à distance à l'aide de commandes logicielles. 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

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

Les lecteurs d'identification par radiofréquence (RFID) peuvent 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 :

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

Logiciel et microprogramme

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

Accès local et à distance

Suivez les recommandations ci-dessous pour garantir la sécurité des accès local et à distance à vos systèmes :

- 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.
- 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.
- Une fois votre système SuperCluster entièrement configuré, le programme d'installation désactive toutes les clés SSH et fait également expirer tous les mots de passe par mesure de sécurité pour votre système. Si vous ne souhaitez pas que les clés SSH soient désactivées ou que les mots de passe expirent, paramétrez le programme d'installation en conséquence à la fin de l'installation du système SuperCluster.
- Les versions plus anciennes de SNMP ne sont pas sécurisées et transmettent les données d'authentification sous forme de texte non chiffré. Seule la version 3 de SNMP peut fournir des transmissions sécurisées.
- Certains produits sont livrés avec PUBLIC défini en tant que chaîne de communauté SNMP par défaut. 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 service SNMP est nécessaire, remplacez la chaîne de communauté SNMP par défaut par une chaîne de communauté fiable.
- Activez la journalisation et envoyez les journaux à un hôte de journal sécurisé dédié.
- Configurez la journalisation pour 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.
- Si le contrôleur système utilise une interface de navigateur, pensez à vous déconnecter après utilisation.

Sécurité des données

Suivez les recommandations ci-dessous 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. La suppression de tous les fichiers ou le reformatage du disque dur supprime uniquement les tables d'adresses sur le disque ; il est toujours possible de récupérer les informations sur le disque après suppression des fichiers ou le reformatage. Utilisez un logiciel de nettoyage de disque pour effacer complètement toutes les données d'un disque.

Sécurité du réseau

Suivez les recommandations ci-après pour optimiser la sécurité de votre réseau :

- Dans la plupart des cas, les commutateurs permettent de définir des réseaux locaux virtuels (VLAN). Si vous utilisez votre commutateur pour définir des VLAN, séparez 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.
- Gérez les commutateurs out-of-band (séparés du trafic de données). Si la gestion out-of-band n'est pas réalisable, dédiez un numéro VLAN distinct à la gestion in-band.
- 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.
- 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.
- 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.
- Affectez 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). Sinon, définissez les paramètres suivants pour ce protocole : domaine de gestion, mot de passe et nettoyage. Définissez ensuite VTP sur le mode transparent.
- Désactivez les services réseau inutiles, tels que les petits serveurs TCP ou HTTP. Activez les services réseau nécessaires et configurez-les de manière sécurisée.
- Différents commutateurs proposent différents niveaux de fonctions de sécurité de port. Utilisez ces fonctions si elles sont disponibles sur votre commutateur :
  - MAC Locking (verrouillage MAC) : cette fonction 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 dans votre réseau avec des points d'accès non autorisés.
  - MAC Lockout (verrouillage MAC) : cette option permet d'empêcher une adresse MAC spécifiée de se connecter à un commutateur.
  - MAC Learning (apprentissage MAC) : utilisez les informations sur les connexions directes de chaque port de commutateur afin que le commutateur puisse configurer la sécurité en fonction des connexions en cours.

Guides de sécurité connexes

Des guides de sécurité spécifiques au produit peuvent exister pour les composants matériels et logiciels utilisés dans le système SuperCluster. La liste ci-après répertorie les composants utilisés dans le système SuperCluster et l'emplacement des guides de sécurité spécifiques au produit correspondants, si ces guides sont disponibles pour les composants en question :

- Serveur SPARC T4-4 :

  http://www.oracle.com/pls/topic/lookup?ctx=E23411_01
- Serveur SPARC T5-8 :

  http://www.oracle.com/pls/topic/lookup?ctx=E35078_01

- Appareil Sun ZFS Storage 7320 :

  http://www.oracle.com/pls/topic/lookup?ctx=ZFS_Storage_7x20_2011.1
- Commutateur Sun Datacenter InfiniBand Switch 36 :

  http://www.oracle.com/pls/topic/lookup?ctx=E19197-01
- Exadata Storage Server : documentation installée dans le répertoire **/opt/oracle/cell/doc** sur le serveur Exadata Storage Server
- Système d'exploitation Oracle Solaris :

  http://www.oracle.com/technetwork/documentation/index.html#sys_sw