Guide de sécurité des serveurs Oracle SuperCluster série M7

Référence: E69651-01
Février 2016

Référence: E69651-01

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

Utilisation de cette documentation

- **Présentation** : fournit des informations sur la planification, la configuration et la gestion d'un environnement sécurisé pour les systèmes Oracle SuperCluster série M7.
- **Public visé** : les techniciens, les administrateurs système et les fournisseurs de services agréés
- **Connaissances requises** : une bonne expérience d'UNIX et de l'administration des bases de données.

Bibliothèque de documentation produit

La documentation et les ressources de ce produit et des produits associés sont disponibles à l'adresse http://www.oracle.com/goto/sc-m7/docs.

Commentaires

Faites part de vos commentaires sur cette documentation à l'adresse : http://www.oracle.com/goto/docfeedback.

Présentation des principes de sécurité

Ce guide fournit des informations sur la planification, la configuration et la gestion d'un environnement sécurisé pour les systèmes Oracle SuperCluster série M7.

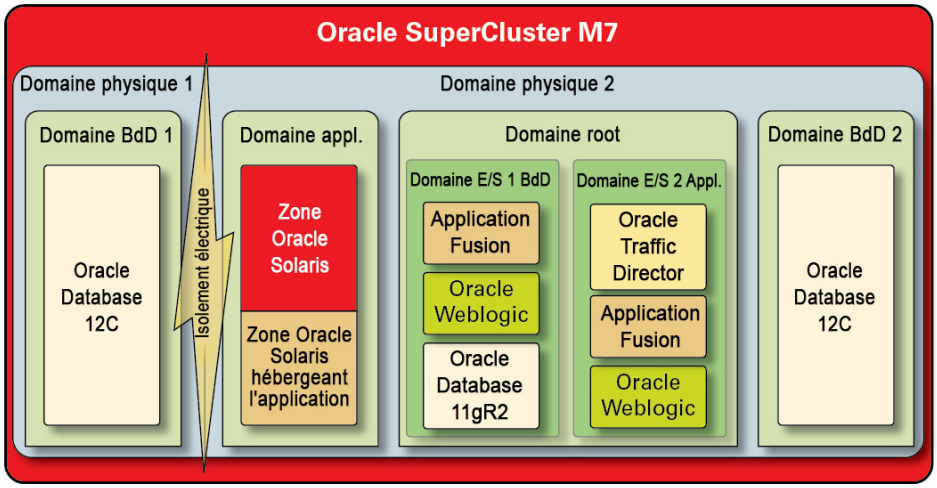
Les rubriques suivantes sont traitées dans cette section :

Isolement sécurisé

Le système SuperCluster M7 prend en charge diverses stratégies d'isolement que les fournisseurs de cloud peuvent sélectionner en fonction de leurs besoins en matière de sécurité et d'assurance. Cette flexibilité leur permet de créer une architecture multilocataire, sécurisée et personnalisée adaptée à leurs activités.

Le système SuperCluster M7 prend en charge différentes stratégies d'isolement qui ont chacune leur propre ensemble de fonctionnalités. Chaque stratégie d'implémentation peut être mise en oeuvre de manière indépendante, mais elles peuvent également être appliquées de concert dans une approche hybride qui permet aux fournisseurs de cloud de déployer des architectures capables de répondre de manière plus équilibrée à leurs besoins notamment en matière de sécurité, de performance et de disponibilité.

FIGURE 1 Isolement sécurisé avec une configuration multilocataire dynamique



Les fournisseurs de services cloud peuvent utiliser des domaines physiques (PDomain) pour des situations dans lesquelles les hôtes locataires exécutent des applications et des bases de données qui doivent être physiquement isolées des autres charges de travail. Un déploiement peut requérir des ressources physiques dédiées en raison de son importance pour l'organisation, du niveau de confidentialité des informations qu'ils contient, des impératifs de conformité, ou simplement parce que la charge de travail de la base de données ou de l'application utilise l'intégralité des ressources du système.

Les organisations qui requièrent un isolement géré par un hyperviseur peuvent utiliser des domaines Oracle VM Server for SPARC, appelés domaines dédiés, pour créer des environnements virtuels qui isolent les instances d'application et/ou de base de données. Créés dans le cadre de l'installation du SuperCluster, les domaines dédiés exécutent chacun leur propre instance du système d'exploitation Oracle Solaris. L'accès aux ressources physiques s'effectue sous la médiation matérielle d'hyperviseurs intégrés aux processeurs SPARC.

Par ailleurs, le système SuperCluster vous permet de créer d'autres domaines, appelés domaines root, qui exploitent la technologie SR-IOV (Single Root I/O Virtualization). Les domaines root possèdent un ou deux HCA InfiniBand et des cartes réseau 10 GbE. Vous pouvez choisir de créer, de manière dynamique, des domaines supplémentaires, appelés domaines d'E/S, au-dessus des domaines root. Le SuperCluster M7 inclut un outil basé sur un navigateur pour les créer et les gérer.

Néanmoins, dans chacun de ces domaines, les locataire du client cloud peuvent utiliser la technologie Oracle Solaris Zones pour créer d'autres environnements isolés. A l'aide des zones, il est possible de déployer des instances d'application ou de base de données individuelles dans un ou plusieurs conteneurs virtuels qui s'exécutent de manière collective au-dessus d'un seul noyau du système d'exploitation. Cette méthode de virtualisation simple permet de créer un cordon de sécurité plus robuste autours des services déployés.

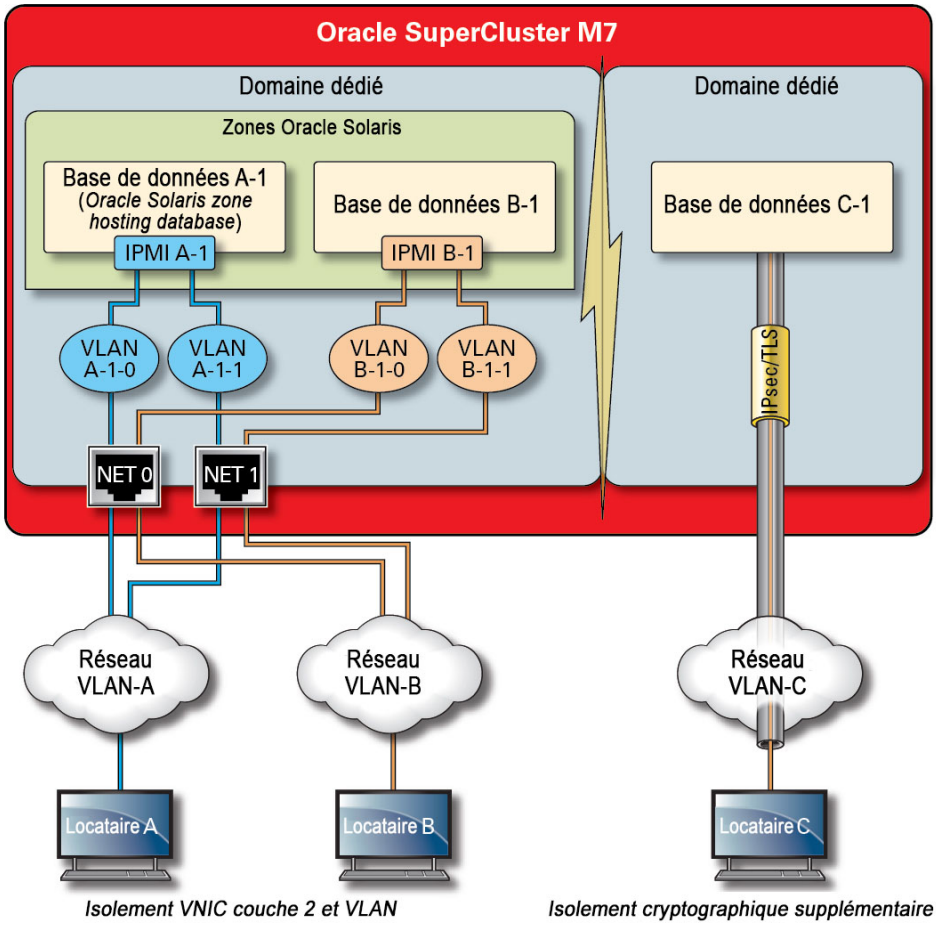
Les locataires qui hébergent plusieurs applications et bases de données sur le système SuperCluster peuvent également adopter une approche hybride, en combinant des stratégies d'isolement basées sur les zones Oracle Solaris, les domaines d'E/S et les domaines dédiés pour créer des architectures à la fois souples et résistantes qui répondent à leurs besoins en matière d'infrastructures de cloud. Grâce à une multitude d'options de virtualisation, le système SuperCluster permet aux locataires hébergés sur le cloud de s'isoler de manière sécurisée au niveau de la couche matérielle. Il fournit par ailleurs des zones Oracle Solaris pour renforcer la sécurité et l'isolement dans l'environnement d'exécution.

Une première étape positive consiste à assurer de manière efficace l'isolement des applications, des bases de données, des utilisateurs et des processus au plan individuel. Il est néanmoins tout aussi important d'examiner les trois principaux réseaux utilisés dans le système SuperCluster et la manière dont les fonctions d'isolement des réseaux et les communications qui y transitent sont protégées :

- Réseau d'accès client 10 GbE
- Réseau de service IB privé
- Réseau de gestion

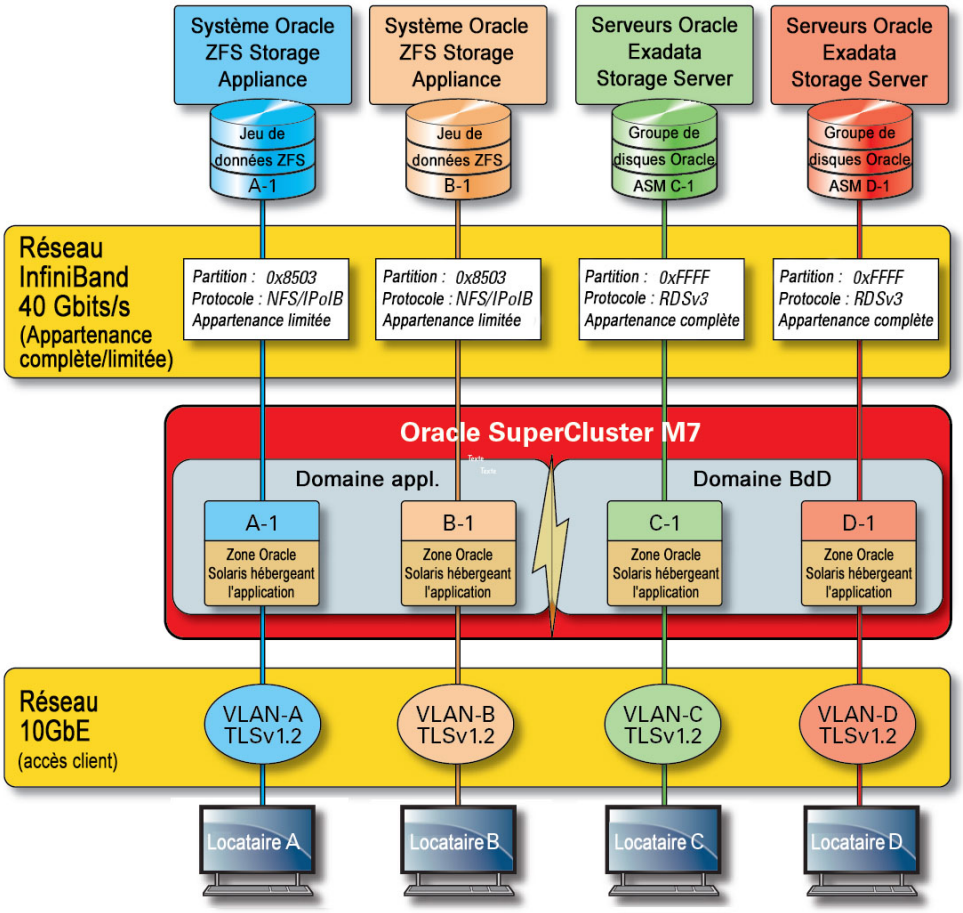
Le trafic réseau qui transite via le réseau d'accès client SuperCluster peut être isolé à l'aide de diverses techniques. La figure suivante présente une configuration possible dans laquelle quatre instances de base de données sont configurées pour fonctionner sur trois LAN virtuels (VLAN) distincts. En configurant les interfaces réseau du SuperCluster pour qu'elles utilisent des VLAN, le trafic réseau peut être isolé entre des domaines Oracle VM Server for SPARC dédiés ainsi qu'entre des zones Oracle Solaris.

FIGURE 2 Isolement sécurisé sur le réseau d'accès client



Le système SuperCluster inclut un réseau IB privé utilisé par des instances de base de données pour accéder aux informations stockées sur les serveurs Exadata Storage Server et l'appareil de stockage ZFS, et pour effectuer les communications internes nécessaires à la mise en cluster et à la haute disponibilité. Cette illustration montre l'isolement sécurisé du réseau sur le système SuperCluster M7.

FIGURE 3 Isolement sécurisé sur le réseau IB à 40 Gbits/s



Par défaut, le réseau IB du SuperCluster est divisé en six partitions distinctes au cours de l'installation et de la configuration. Il est impossible de modifier les partitions par défaut, mais Oracle prend en charge la création et l'utilisation de partitions dédiées supplémentaires lorsqu'il est nécessaire de segmenter davantage le réseau IB. De plus, le réseau IB prend en charge le principe d'appartenance à une partition avec des droits limités ou complets. Les membres avec droits limités peuvent seulement communiquer avec les membres avec des droits complets, alors que ces derniers peuvent communiquer avec tous les noeuds de la partition. Les domaines d'E/S d'application et les zones Oracle Solaris 11 peuvent être configurés en tant que membres avec droits limités de leurs partitions IB respectives. De la sorte, ils communiquent uniquement

avec l'appareil de stockage ZFS, configuré comme membre avec droits complets, sans pouvoir le faire avec les autres noeuds aux droits limités de la même partition.

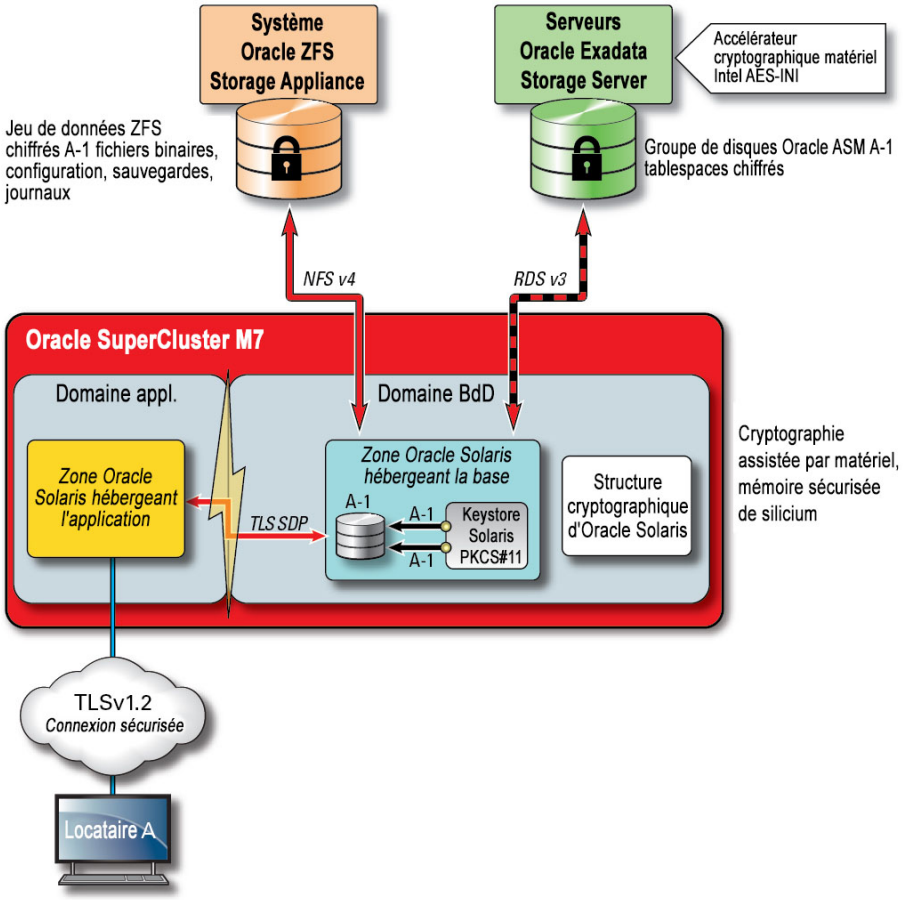
Le système SuperCluster inclut également un réseau de gestion dédié par le biais duquel tous ses principaux composants peuvent être gérés et surveillés. Cette stratégie maintient les fonctions de gestion et de surveillance confidentielles isolées des chemins d'accès réseau qui servent à traiter les demandes client. En assurant l'isolement des fonctions de gestion vis à vis du réseau de gestion, le système SuperCluster permet de réduire la surface exposée aux attaques sur les réseaux IB et d'accès client. Les fournisseurs de cloud sont vivement encouragés à suivre cette pratique recommandée, en isolant les outils de gestion et de surveillance et les fonctions connexes de manière à ce que seul le réseau de gestion puisse y accéder.

Protection des données

Les fournisseurs de cloud placent la protection des données au coeur de leur stratégie de sécurité. Etant donné l'importance des impératifs de confidentialité et de conformité, il est vivement conseillé aux organisations qui envisagent d'installer des architectures multilocataires de recourir à la cryptographie pour protéger les informations transitant vers et depuis leurs bases de données. Les services cryptographiques sont systématiquement mis en oeuvre pour assurer la confidentialité et l'intégrité des informations lorsqu'elles transitent sur le réseau ou qu'elles résident sur un disque.

Le processeur SPARC M7 dans le système SuperCluster facilite le chiffrement matériel hautement performant pour répondre aux besoins des environnements informatiques sensibles en matière de protection des données. Le processeur SPARC M7 intègre également la technologie de mémoire sécurisée de silicium qui assure la prévention des attaques malveillantes au niveau des applications, telles que la capture de données en mémoire (memory scraping), la corruption silencieuse de la mémoire (silent memory corruption), le débordement de tampon (buffer overrun) et les attaques connexes.

FIGURE 4 Protection des données fournie par l'accélérateur cryptographique matériel et la protection contre les intrusions en mémoire



Pour offrir des architectures multilocataires sécurisées, dans lesquelles la protection des données est présente dans quasiment tous les aspects de la conception, le système SuperCluster et son logiciel associé permet aux organisations d'atteindre leurs objectifs en termes de sécurité et de conformité sans sacrifier les performances. Le système SuperCluster utilise les instructions cryptographiques basées sur le coeur et les fonctionnalités de mémoire sécurisée de silicium intégrées à son processeur SPARC M7 pour accélérer les opérations cryptographiques et assurer la protection contre les intrusions en mémoire sans compromettre les performances. Ces fonctionnalités améliorent les performances de la cryptographie et fournissent un dispositif

de contrôle des intrusions en mémoire. De plus, elles renforcent les performances globales, car il est possible d'affecter plus de ressources de calcul à la gestion des charges de travail locataires.

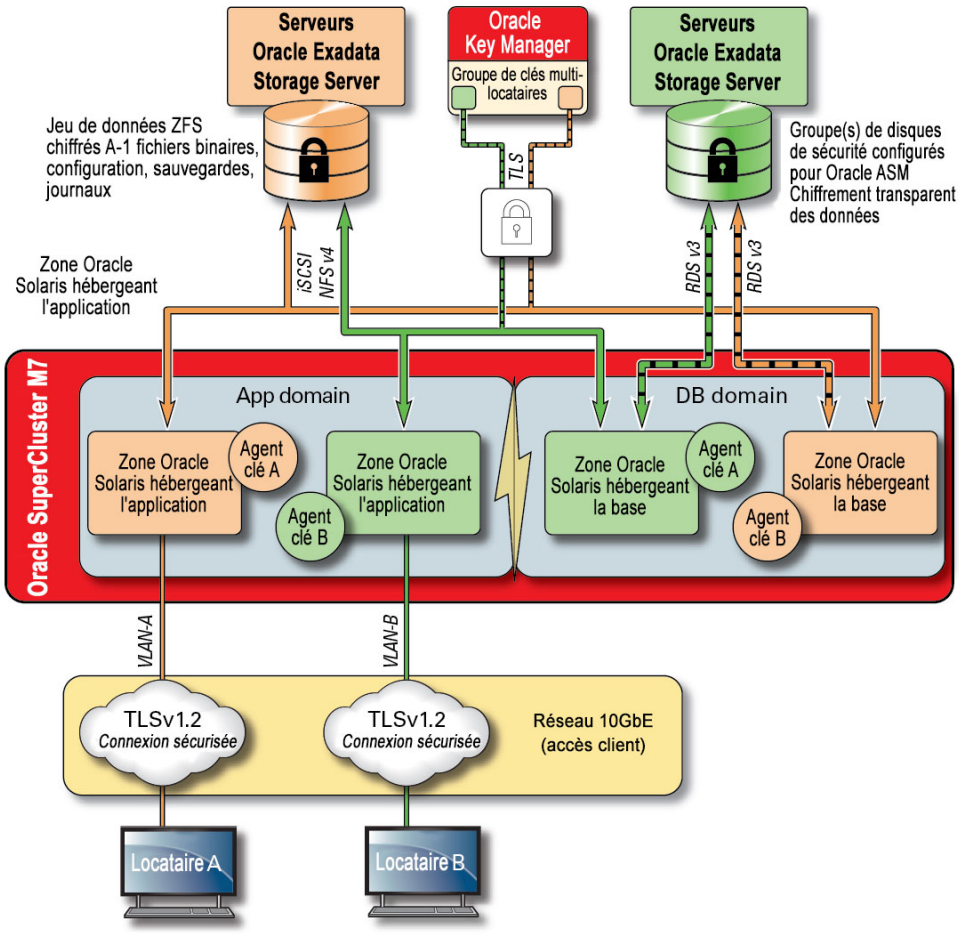
Le processeur SPARC prend en charge un accélérateur cryptographique matériel pour plus de 16 algorithmes standard. Collectivement, ces algorithmes répondent à l'essentiel des besoins modernes en matière de cryptographie, notamment le chiffrement à clé publique, le chiffrement à clé symétrique, la génération de nombres aléatoires, et le calcul et la vérification des signatures numériques et des résumés de message. De plus, au niveau du système d'exploitation, l'accélération cryptographique matérielle est activée par défaut pour la plupart des services de base, notamment le shell sécurisé, IPSec/IKE et les jeux de données ZFS chiffrés.

Oracle Database et Oracle Fusion Middleware identifient automatiquement le système d'exploitation d'Oracle Solaris et le processeur SPARC utilisés par le système SuperCluster. La base de données et l'intergiciel peuvent ainsi utiliser automatiquement les fonctions d'accélération cryptographique matérielle de la plate-forme pour exécuter des opérations de chiffrement de type TLS, WS-Security et tablespace. Cela leur permet également d'exécuter la fonction de mémoire sécurisée de silicium pour assurer la protection de la mémoire. L'intégrité des données d'application est ainsi garantie sans configuration de l'utilisateur final. Pour protéger la confidentialité et l'intégrité des communications IP interzones, spécifiques à un locataire, qui transitent par le réseau IB, utilisez les protocoles IPSec (IP Security) et IKE (Internet Key Exchange).

Toute discussion relative à la cryptographie serait incomplète sans aborder la question du mode de gestion des clés de chiffrement. La génération et la gestion des clés de chiffrement, notamment pour de vastes éventails de services, ont toujours constitué un défi majeur pour les organisations, et les difficultés vont grandissantes avec les environnements multilocataires basés sur le cloud. Sur le système SuperCluster, le chiffrement des jeux de données ZFS et le cryptage transparent des données (TDE) d'Oracle Database peuvent faire appel à un magasin de clés Oracle Solaris PKCS#11 pour protéger de manière sécurisée la clé principale. L'utilisation du magasin de clés Oracle Solaris PKCS#11 implique automatiquement l'accélérateur cryptographique matériel SPARC pour les opérations sur les clés principales. Cela permet au système SuperCluster d'améliorer de manière significative les performances des opérations de chiffrement et de déchiffrement associées au traitement des jeux de données ZFS et du tablespace d'Oracle Database, aux sauvegardes des bases de données chiffrées (à l'aide d'Oracle Recovery Manager [Oracle RMAN]), aux exportations des bases de données chiffrées (à l'aide de la fonctionnalité Data Pump d'Oracle Database) et aux fichiers de journalisation (à l'aide d'Oracle Active Data Guard).

Les locataires qui adoptent une approche de partage de portefeuille peuvent recourir à l'appareil de stockage ZFS pour créer un répertoire pouvant être partagé sur tous les noeuds d'un cluster. L'utilisation d'un magasin de clés partagé et centralisé facilite la gestion, la mise à jour et la rotation des clés par les locataires dans les architectures de bases de données en cluster, telles qu'Oracle RAC (Real Application Clusters), car les clés sont synchronisées sur tous les noeuds du cluster.

FIGURE 5 Protection des données via un scénario de gestion de clés multilocataire utilisant Oracle Key Manager



Pour résoudre les difficultés associées à la gestion de plusieurs hôtes et applications dans un environnement multilocataire basé sur le cloud, utilisez l'option Oracle Key Manager en tant que dispositif intégré au réseau de gestion. Oracle Key Manager autorise, sécurise et gère de manière centralisée l'accès aux clés de chiffrement utilisées par Oracle Database, les applications Oracle Fusion, Oracle Solaris et l'appareil de stockage ZFS. Oracle Key Manager prend également en charge les lecteurs de bande à chiffrement StorageTek d'Oracle. Etant donné que la stratégie de chiffrement et la gestion des clés s'exécutent au niveau du jeu de données

ZFS (système de fichiers), la suppression des systèmes de fichiers locataires est garantie par la destruction des clés.

Oracle Key Manager est un outil de gestion de clés complet qui prend en charge les opérations de gestion des clés tout au long de leur cycle de vie et le stockage sécurisé des clés. Lorsqu'il est configuré à l'aide d'une carte PCIe Sun Crypto Accelerator 6000 d'Oracle, Oracle Key Manager offre un outil de stockage de clés certifié FIPS 140-2 de niveau 3 pour les clés de chiffrement AES de 256 bits, ainsi qu'une fonction de génération de nombres aléatoires conforme à FIPS 186-2. Dans le système SuperCluster, tous les domaines de base de données et d'application, y compris leurs zones globales et non globales, peuvent être configurés afin d'utiliser Oracle Key Manager pour la gestion de clés associées à des applications, des bases de données et des jeux de données ZFS chiffrés. En fait, Oracle Key Manager prend en charge les opérations de gestion de clés associées à des instances de base de données individuelles ou multiples, Oracle RAC, Oracle Active Data Guard, Oracle RMAN et la fonctionnalité Data Pump d'Oracle Database.

Enfin, la séparation des tâches, appliquée par Oracle Key Manager, permet à chaque locataire de conserver un contrôle total de ses clés de chiffrement en bénéficiant d'une transparence permanente des opérations de gestion de clés. Compte tenu du rôle crucial joué par les clés dans le domaine de la protection des informations, il est primordial que les locataires implémentent les niveaux appropriés d'audit et de contrôle d'accès basé sur les rôles pour assurer la protection adéquate des clés durant tout leur cycle de vie.

Informations connexes

- "Oracle Key Manager" à la page 132

Contrôle d'accès

Pour les organisations qui adoptent une stratégie reposant sur un environnement hébergé dans le cloud, le contrôle d'accès représente l'un des défis les plus importants à relever. Les locataires doivent avoir l'assurance que les informations stockées dans les infrastructures partagées sont protégées et accessibles aux seuls hôtes, services, utilisateurs, groupes et rôles autorisés. Les hôtes, les utilisateurs et les services doivent être soumis à des contraintes supplémentaires, conformément au principe du moindre privilège, selon lequel les droits et les autorisations ne sont attribués que pour exécuter une opération donnée.

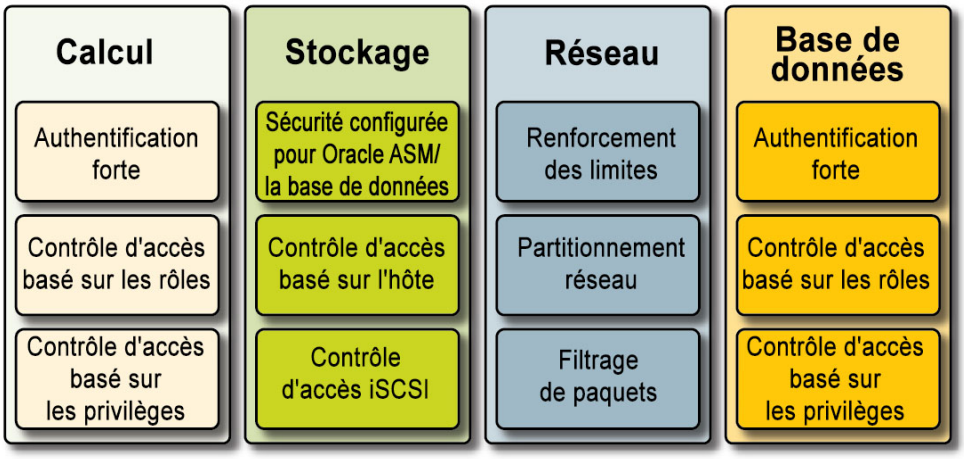
Le système SuperCluster facilite la mise en place d'une architecture de contrôle d'accès organisée en couches et offrant une grande souplesse. Elle couvre chaque niveau de la pile et remplit différents rôles, notamment utilisateur final, administrateur de base de données et administrateur système. Les organisations peuvent ainsi définir des stratégies qui protègent

les hôtes, les applications et les bases de données de manière individuelle et protéger les infrastructures de calcul, de stockage et réseau sous-jacentes sur lesquelles ces services sont exécutés.

Au niveau de la couche de virtualisation et du système d'exploitation, le contrôle d'accès commence par la réduction du nombre de services exposés sur le réseau. Cela facilite le contrôle de l'accès aux consoles, domaines et zones Oracle VM Server for SPARC. En diminuant le nombre de points d'entrée par le biais desquels les systèmes sont accessibles, il est également possible de réduire le nombre de stratégies de contrôle d'accès et leur complexité pendant la durée de vie du système.

Dans le système d'exploitation Oracle Solaris, les contrôles d'accès sont implémentés en combinant des autorisations POSIX avec l'utilitaire de contrôle d'accès basé sur les rôles (RBAC) d'Oracle Solaris. La capacité de pouvoir protéger des attaques réseau les hôtes, les applications, les bases de données et les services connexes exécutés sur le système SuperCluster est tout aussi importante. Pour y parvenir, les locataires doivent d'abord vérifier que seuls les services réseau autorisés sont exécutés et à l'écoute des connexions réseau entrantes. Lorsque la surface exposée aux attaques réseau a été minimisée, les locataires peuvent configurer le reste des services pour qu'ils écoutent les connexions entrantes uniquement sur des réseaux et des interfaces autorisés. Cette simple précaution permet de garantir que les protocoles de gestion, tels que le shell sécurisé (SSH), sont inaccessibles sauf depuis le réseau de gestion.

FIGURE 6 Récapitulatif du contrôle d'accès de bout en bout



Par ailleurs, les locataires peuvent aussi choisir d'implémenter un pare-feu basé sur un hôte, tel que le service IP Filter d'Oracle Solaris. Les pare-feu basés sur un hôte sont utiles car ils

fournissent des hôtes dotés d'un plus grand nombre de fonctionnalités pour contrôler l'accès aux services réseau. Par exemple, IP Filter permet le filtrage de paquets avec état et est capable de filtrer les paquets en fonction de leur adresse IP, du port, du protocole, de l'interface réseau et de la direction du trafic. Ces fonctionnalités sont importantes pour certaines plates-formes comme SuperCluster qui gèrent de nombreuses interfaces réseau et prennent en charge diverses communications réseau entrantes et sortantes.

Sur le système SuperCluster, le service IP Filter peut être configuré dans un domaine Oracle VM Server for SPARC ou géré depuis une zone Oracle Solaris. La stratégie de contrôle d'accès réseau peut donc être appliquée depuis le conteneur du système d'exploitation dans lequel les services de base de données sont offerts. Dans un scénario multilocataire, le volume d'activités réseau entrantes sera probablement minimal et pourra être facilement catégorisé de manière à créer une stratégie qui limite les communications à des interfaces et des destinations réseau spécifiques. Tout autre trafic est refusé et consigné, dans le cadre d'une stratégie de “refus par défaut” destinée à bloquer les communications non autorisées, tant entrantes que sortantes.

La sécurité de l'utilisateur final d'Oracle permet aux locataires d'intégrer leurs applications et bases de données à leurs services de gestion d'identité existants pour prendre en charge le service SSO (Single Sign-On, connexion unique) et la gestion centralisée des utilisateurs et des rôles. En particulier, la sécurité de l'utilisateur final d'Oracle permet de centraliser (1) le provisionnement et le déprovisionnement des utilisateurs et des administrateurs de base de données, (2) la gestion des mots de passe et la réinitialisation des mots de passe en libre-service et (3) la gestion des autorisations à l'aide de rôles de base de données globaux. Les organisations qui requièrent des méthodes d'authentification mutifacteur, telles que Kerberos ou PKI, peuvent tirer parti d'Oracle Advanced Security.

La technologie Oracle Exadata Storage Server prend en charge un ensemble prédéfini de comptes utilisateur, chacun doté de ses propres privilèges. Les administrateurs qui exécutent des tâches d'administration Oracle Exadata Storage Server doivent utiliser un de ces rôles prédéfinis pour accéder au système. L'appareil de stockage ZFS, quant à lui, prend en charge la création de comptes d'administration locaux et distants, tous deux capables d'assurer l'attribution individuelle de rôles et de privilèges.

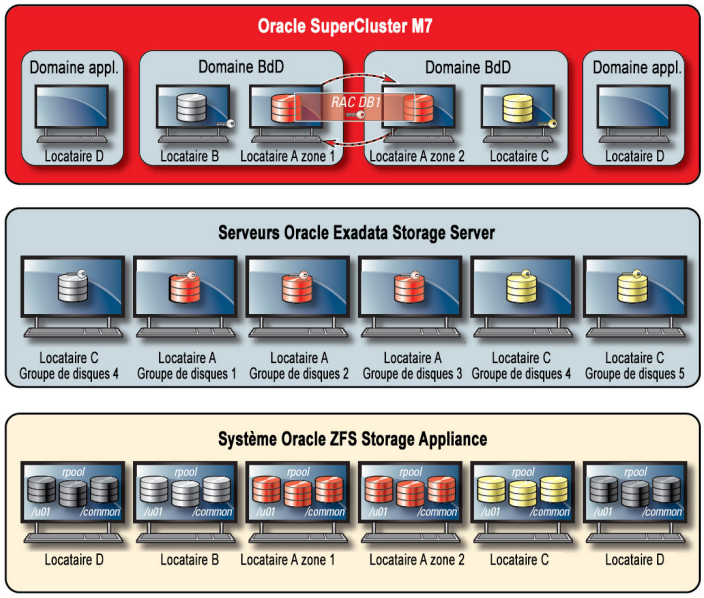
Par défaut, les serveurs Oracle Exadata Storage Server utilisés dans le système SuperCluster sont accessibles aux domaines de base de données qui utilisent l'utilitaire Oracle Automatic Storage Management. Cet utilitaire permet aux fournisseurs de cloud de créer des groupes de disques distincts pour chaque locataire capables de répondre à leurs besoins en termes de capacité, performance et disponibilité. Oracle Automatic Storage Management prend en charge trois modes de contrôle d'accès : la sécurité ouverte, la sécurité basée sur Oracle Automatic Storage Management et la sécurité au niveau base de données.

Dans un scénario multilocataire, la sécurité basée sur les bases de données est recommandée, car elle procure le plus haut niveau de précision en matière de contrôle d'accès. Dans ce mode, il est possible de configurer des groupes de disques de manière à ce qu'ils soient accessibles

à une seule base de données. En particulier, cela signifie qu'il est possible de restreindre l'accès des administrateurs et des utilisateurs de base de données aux disques de grille qui contiennent des informations pour lesquelles ils disposent de privilèges. Dans les scénarios de consolidation de bases de données dans lesquels une même base peut prendre en charge plusieurs organisations ou locataires, il est important que chaque locataire ne puisse ouvrir et manipuler que ses propres données. En particulier, en associant les stratégies d'isolement de charge de travail et de base de données, les locataires sont en mesure de cloisonner efficacement l'accès à chaque base de données.

La sécurité basée sur les bases de données est un outil efficace pour limiter l'accès aux disques de grille Oracle ASM. La figure suivante présente une architecture combinant la sécurité basée sur Oracle ASM et la sécurité ZFS. Lorsqu'un grand nombre d'instances Oracle Database sont déployées sur la plate-forme SuperCluster, il est sans doute plus pertinent d'appliquer une stratégie de sécurité basée sur Oracle ASM et applicable à chaque locataire, car elle réduit considérablement le nombre de clés devant être créées, assignées et gérées. De plus, comme la sécurité basée sur les bases de données requiert la création de groupes de disques séparés pour chaque base de données, cette méthode permet également de diminuer de manière significative le nombre de disques de grille devant être créés sur un serveur Exadata Storage Server.

FIGURE 7 Sécurité basée sur Oracle ASM par locataire



Le système SuperCluster utilise la protection des liaisons de données d'Oracle Solaris, dont l'objectif est d'éviter les dommages causés au réseau par les machines virtuelles de locataires malveillants. Cette fonctionnalité Oracle Solaris intégrée offre une protection contre les menaces de base suivantes : les usurpations d'adresse IP et MAC et de cadre L2 (par exemple, les attaques au niveau des BPDU [Bridge Protocol Data Unit]). La protection des liaisons de données d'Oracle Solaris doit être appliquée de manière individuelle à toutes les zones Oracle Solaris non globales déployées dans l'environnement multilocataire.

Comme les locataires, à titre individuel, ne devraient jamais disposer de droits au niveau administratif ou hôte pour accéder aux serveurs Exadata Storage Server, il est vivement conseillé de restreindre ce type d'accès. Les serveurs Exadata Storage Server doivent être configurés pour bloquer l'accès direct aux domaines d'E/S de base de données et aux zones non globales de locataires tout en permettant l'accès à partir des domaines de base de données SuperCluster (gérés par le fournisseur de cloud). Les serveurs Exadata Storage Server sont ainsi seulement gérés à partir d'emplacements approuvés sur le réseau de gestion.

Lorsque la configuration de la sécurité des locataires a été définie et implémentée, les fournisseurs de services peuvent passer à l'étape supplémentaire qui consiste à configurer des zones globales et non globales spécifiques aux locataires en tant qu'environnements immuables en lecture seule. Les zones immuables créent une environnement d'exploitation présentant un haut niveau de résistance et d'intégrité dans lequel les locataires peuvent exécuter leurs propres services. En tirant parti des fonctionnalités de sécurité inhérentes à Oracle Solaris, les zones immuables permettent de garantir qu'une partie (ou la totalité) des répertoires et des fichiers du système d'exploitation ne pourra pas être modifiée sans l'intervention du fournisseur de services cloud. La mise en oeuvre de cette approche en lecture seule permet d'empêcher les modifications non autorisées, de promouvoir des procédures de gestion des modifications plus robustes et d'empêcher l'introduction de programmes malveillants via le noyau ou l'utilisateur.

Audit de surveillance et de conformité

La surveillance et la journalisation proactives dans un environnement de type cloud jouent un rôle très important et contribuent généralement à atténuer les attaques provenant de failles et de vulnérabilités au niveau de la sécurité. Qu'il s'agisse de rapports de conformité ou de réponses à des incidents, la surveillance et l'audit jouent un rôle crucial pour le fournisseur de cloud. Les organisations locataires doivent ainsi mettre en oeuvre une stratégie de journalisation et d'audit bien définie pour renforcer la transparence de leur environnement d'hébergement. Le degré d'utilisation des outils de surveillance et d'audit se fonde souvent sur le niveau de risque et de sensibilité de l'environnement sous protection.

L'architecture cloud du système SuperCluster s'appuie sur le sous-système d'audit d'Oracle Solaris pour collecter, stocker et traiter les informations relatives aux événements d'audit.

Chaque zone non globale spécifique à un locataire génère des enregistrements d'audit qui sont stockés localement dans chacun des domaines dédié du système SuperCluster (zone globale). Cette méthode garantit qu'au niveau individuel les locataires sont incapables de modifier leurs informations d'audit (stratégies, configurations et données enregistrées) puisque cette responsabilité incombe aux fournisseur de services cloud. La fonctionnalité d'audit d'Oracle Solaris surveille toutes les actions d'administration, les appels de commande et même chaque appel système au niveau du noyau dans les zones et les domaines de locataires. Cet outil, hautement configurable, prend en charge des stratégies d'audit globales, par zone et par utilisateur. Lorsqu'ils sont configurés pour utiliser des zones de locataires, il est possible de stocker les enregistrements d'audit de chaque zone dans la zone globale pour les protéger de toute altération. Les domaines dédiés et d'E/S font aussi appel à l'outil d'audit natif d'Oracle Solaris pour enregistrer des actions et des opérations associées à des événements de virtualisation et à l'administration des domaines.

Les serveurs Exadata Storage Server et l'appareil de stockage ZFS prennent en charge des fonctions d'audit au niveau de la connexion, du matériel et de la configuration. Les organisations peuvent ainsi identifier qui accède à un périphérique et quelles actions sont exécutées. Bien qu'elles ne soient pas directement exposées à l'utilisateur final, les fonctions d'audit d'Oracle Solaris fournissent le contenu qui sous-tend les informations présentées par l'appareil de stockage ZFS.

D'autre part, l'audit du serveur Exadata Storage Server est une vaste collection d'événements système qui peut être associée aux informations sur les alertes portant sur le matériel et la configuration que fournit le logiciel Exadata Storage Server. Grâce à la fonctionnalité IP Filter d'Oracle Solaris, le fournisseur de cloud peut enregistrer de manière sélective les communications réseau entrantes et sortantes. Cet utilitaire peut par ailleurs être utilisé au niveau du domaine et de la zone non globale. Les organisations peuvent ainsi segmenter plus facilement leurs stratégies réseau et vérifier les enregistrements d'activité. L'appareil Oracle Audit Vault and Database Firewall peut également être déployé pour regrouper et analyser de manière sécurisée les informations d'audit provenant de diverses base de données Oracle ou non Oracle, ainsi que d'Oracle Solaris.

Grâce à son intégration à Oracle Enterprise Manager, le système SuperCluster prend en charge diverses opérations de type cloud en libre-service. Les fournisseurs de cloud peuvent définir des pools de ressources, assigner des pools et des quotas à des locataires de manière individuelle et publier des catalogues de services. Ils assurent enfin la surveillance et la journalisation des ressources d'application et de base de données.

Informations connexes

- "Audit de conformité" à la page 125
- "Surveillance de la sécurité" à la page 135

Ressources supplémentaires sur les pratiques recommandées en matière de sécurité du système SuperCluster

Pour plus d'informations sur la sécurité, l'architecture et les pratiques recommandées relatives au système SuperCluster, reportez-vous aux ressources suivantes :

- Oracle SuperCluster M7 - Platform Security Principles and Capabilities

  http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf
- Oracle SuperCluster M7 - Secure Private Cloud Architecture

  http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf
- Comprehensive Data Protection on Oracle SuperCluster

  https://community.oracle.com/docs/DOC-918251
- Secure Database Consolidation on Oracle SuperCluster

  http://www.oracle.com/technetwork/server-storage/sun-sparc-enterprise/documentation/o13-053-securedb-osc-t5-8-1990064.pdf
- Oracle SuperCluster and PCI Compliance

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle SuperCluster - Security Technical Implementation Guide (STIG) Validation and Best Practices

  http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- Developer's Guide to Oracle Solaris 11 Security

  https://docs.oracle.com/cd/E36784_01/html/E36855/index.html
- Oracle Solaris 11 and PCI Compliance

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- Oracle Solaris 11 Audit Quick Start

  http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html
- Oracle Solaris 11 Security Guidelines

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- Oracle Database Security Guide 12c Release 1 (12.1)

  https://docs.oracle.com/database/121/DBSEG/E48135-11.pdf

Vérification de la configuration de sécurité par défaut

Les rubriques suivantes décrivent la configuration de sécurité par défaut du SuperCluster M7.

Paramètres de sécurité par défaut

Le logiciel SuperCluster M7 est installé avec de nombreux paramètres se sécurité par défaut. Dans la mesure du possible, utilisez les paramètres de sécurité par défaut :

- La stratégie de sécurité impose une complexité minimale du mot de passe.
- Les tentatives de connexion ayant échoué provoquent un verrouillage après un nombre défini d'échecs.
- Tous les comptes système par défaut du système d'exploitation sont verrouillés et ne sont pas autorisés à se connecter.
- La capacité limitée à utiliser la commande `su` est configurée.
- Les protocoles et les modules inutiles sont désactivés du noyau du système d'exploitation.
- Le programme d'initialisation est protégé par un mot de passe.
- Tous les services système inutiles sont désactivés, y compris `inetd` (démon de service Internet).
- Le pare-feu logiciel est configuré sur les cellules de stockage.
- Des autorisations de fichier restrictives sont définies sur les fichiers de configuration et les fichiers exécutables clés liés à la sécurité.
- Les ports d'écoute SSH sont réservés aux réseaux de gestion et aux réseaux privés.
- SSH est limité au protocole v2.
- Les mécanismes d'authentification SSH non sécurisés sont désactivés.

- Des chiffrements cryptographiques spécifiques sont configurés.
- Les commutateurs du système sont séparés du trafic de données sur le réseau.

Comptes et mots de passe utilisateur par défaut

Ce tableau répertorie les comptes et les mots de passe utilisateur par défaut du SuperCluster M7. Des instructions supplémentaires pour modifier les mots de passe par défaut sont fournies dans les chapitre suivants pour chaque composant.

Composant	Nom d'utilisateur	Mot de passe	Informations sur les comptes et les mots de passe utilisateur
Oracle ILOM sur : ■ Serveurs de la série SPARC M7 ■ Serveurs Exadata Storage Server ■ Appareil de stockage ZFS	■ `root`	`welcome1`	Reportez-vous à la section “Configuration and Maintenance” dans la page de documentation sur Oracle ILOM à l'adresse : `http://docs.oracle.com/cd/E24707_01/html/E24528`
Serveurs de la série SPARC M7	■ `root` ■ `oracle` ■ `grid`	`welcome1` `welcome1` `welcome1`	Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55. Reportez-vous également aux ressources suivantes : ■ **Oracle Solaris 11** – Reportez-vous à la documentation sur la sécurité pour Oracle Solaris 11 à l'adresse : `http://www.oracle.com/goto/Solaris11/docs` ■ **Oracle Solaris 10** – Reportez-vous au manuel *Administration d'Oracle Solaris : Administration de base* à l'adresse : `http://docs.oracle.com/cd/E26505_01`

Serveurs Exadata Storage Server	■ `root`
	■ `celladmin`
	■ `cellmonitor`
		`welcome1`
		`welcome`
		`welcome`
			Voir "Modification des mots de passe des serveurs de stockage" à la page 98.

Oracle ZFS Storage ZS3-ES	■ `root`	`welcome1`	Voir "Modification du mot de passe `root` de l'appareil de stockage ZFS" à la page 87. Reportez-vous également à la section “Utilisateurs” du manuel *Guide d'administration des systèmes Oracle® ZFS Storage Appliance* à l'adresse : `http://www.oracle.com/goto/ZS3-ES/docs`
Commutateurs InfiniBand	■ `root` ■ `nm2user`	`welcome1`	Voir "Modification des mots de passe `root` et `nm2user`" à la page 115.

Composant	Nom d'utilisateur	Mot de passe	Informations sur les comptes et les mots de passe utilisateur
		changeme	Reportez-vous également à la section "Controlling the Chassis" du document *Sun Datacenter InfiniBand Switch 36 HTML Document Collection for Firmware Version 2.1* à l'adresse : `http://docs.oracle.com/cd/E36265_01`
InfiniBand Oracle ILOM	■ `ilom-admin` ■ `ilom-operator`	ilom-admin ilom-operator	Voir "Modification des mots de passe du commutateur IB (Oracle ILOM)" à la page 116. Reportez-vous également à la documentation sur InfiniBand à l'adresse : `http://docs.oracle.com/cd/E36265_01`
Commutateur de gestion Ethernet	■ `admin`	`welcome1`	Voir "Modification du mot de passe du commutateur Ethernet" à la page 123
Outil de création de domaine d'E/S d'Oracle	■ `admin`	welcome1	Reportez-vous au manuel *Oracle I/O Domain Administration Guide* disponible à l'adresse : `http://www.oracle.com/goto/sc-m7/docs`.
Oracle Engineered Systems Hardware Manager	■ `admin` ■ service	welcome1 welcome1	Reportez-vous au manuel *Oracle SuperCluster M7 Series Owner's Guide: Administration* disponible à l'adresse : `http://www.oracle.com/goto/sc-m7/docs`.

Remarque - Lorsque le mot de passe `root` ou `admin` de ce composant est modifié, il doit également l'être dans Oracle Engineered Systems Hardware Manager. Reportez-vous au manuel *Oracle SuperCluster M7 Series Owner's Guide: Administration* pour obtenir des instructions. Reportez-vous également à la section "Mots de passe connus par Oracle Engineered Systems Hardware Manager" à la page 31

Mots de passe connus par Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager doit être configuré avec les comptes et les mots de passe des composants de ce tableau.

Remarque - Oracle Engineered Systems Hardware Manager n'a pas besoin de connaître les mots de passe des domaines logiques ou des zones.

Composant	Compte
Toutes les instances Oracle ILOM	`Racine`

Composant	Compte
Système d'exploitation des serveurs de stockage Exadata	`Racine`
Système d'exploitation contrôleurs de stockage ZFS	`Racine`
Commutateurs IB	`root`
Commutateur de gestion Ethernet	`admin`
PDU	`admin`

Pour plus d'informations sur Oracle Engineered Systems Hardware Manager, reportez-vous à "Oracle Engineered Systems Hardware Manager" à la page 133 ainsi qu'au manuel *Guide d'administration des serveurs Oracle SuperCluster série M7* à l'adresse `http://www.oracle.com/goto/sc-m7/docs`.

Sécurisation du matériel

Les sections suivantes fournissent des recommandations pour sécuriser le matériel :

Restrictions d'accès

- Installez les systèmes de la série Oracle SuperCluster M7 et l'équipement connexe dans un local dont l'accès est restreint et dont la porte est dotée d'un verrou.
- Verrouillez les portes de rack sauf s'il est nécessaire d'intervenir au niveau de ses composants. Vous limitez ainsi l'accès aux périphériques enfichables ou remplaçables à chaud, aux ports USB, aux ports réseau et aux consoles système.
- 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.
- 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 et dont l'accès est limité.
- Limitez l'accès aux consoles USB. Les périphériques, tels que les contrôleurs système, les unités de distribution de courant (PDU) et les commutateurs réseau peuvent être équipés de connexions USB. Limiter l'accès physique constitue une méthode d'accès à un composant plus sécurisée dans la mesure où il ne risque aucune attaque réseau.

Numéros de série

- Notez les numéros de série des composants des systèmes de la série SuperCluster M7.
- 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 un registre des clés d'activation et des 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.
- Conservez en lieu sûr toutes les fiches d'information fournies avec le système.

Disques

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

- Utilisez des outils d'effacement de disque tels que la commande Oracle Solaris `format(1M)` pour supprimer l'intégralité des données contenues sur l'unité.
- Les entreprises doivent se référer à leurs 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 . Reportez-vous à ce document : `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

Attention - Les logiciels d'effacement de disque peuvent échouer à supprimer certaines données sur les unités de disque dur modernes à cause de leur méthode de gestion de l'accès aux données.

OBP

Par défaut, le logiciel OBP du SPARC série M7 n'est pas protégé par mot de passe. Pour renforcer la sécurité du système, limitez l'accès au logiciel OBP en procédant comme suit :

- Implémentez la protection par mot de passe.
- Vérifiez les échecs de connexion au logiciel OBP.

- Définissez la bannière à afficher au démarrage d'OBP.

Ressources matérielles supplémentaires

Tous les principes de sécurité décrits dans le *Guide de sécurité des serveurs de la série SPARC M7* s'appliquent aux serveurs SPARC M7 du système SuperCluster. Ce guide de sécurité est disponible à l'adresse : http://www.oracle.com/goto/M7/docs

Sécurisation d'Oracle ILOM

Oracle ILOM fournit des fonctions matérielles et logicielles avancées de processeur de service pour gérer et surveiller les composants d'un système Oracle SuperCluster, notamment des serveurs de calcul, des serveurs de stockage, des appareils de stockage ZFS et des commutateurs IB.

Oracle ILOM vous permet de gérer et de surveiller de manière active les serveurs et les périphériques sous-jacents indépendamment de l'état du système d'exploitation, en offrant ainsi des capacités de gestion à distance fiables.

Pour entièrement sécuriser Oracle ILOM sur le système SuperCluster M7, vous devez appliquer les paramètres de configuration à chaque composant Oracle ILOM de manière individuelle. Il s'agit des composants Oracle ILOM suivants :

- Serveurs de calcul
- Serveurs de stockage
- Appareil de stockage ZFS
- Commutateurs IB

Effectuez les tâches suivantes pour sécuriser Oracle ILOM :

- "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38
- "Détermination de la version d'Oracle ILOM" à la page 38
- "(Si nécessaire) Activation du fonctionnement compatible avec la norme FIPS-140 (Oracle ILOM)" à la page 39
- "Comptes et mots de passe par défaut (Oracle ILOM)" à la page 40
- "Services réseau exposés par défaut (Oracle ILOM)" à la page 40
- "Renforcement de la configuration de la sécurité d'Oracle ILOM" à la page 42
- "Ressources supplémentaires sur Oracle ILOM" à la page 52

Connectez-vous à l'interface de ligne de commande d'Oracle ILOM

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**

   Dans cet exemple, remplacez *ILOM_SP_ipaddress* par l'adresse IP d'Oracle ILOM pour le composant auquel vous voulez accéder :

   - Serveurs de calcul
   - Serveurs de stockage
   - Appareil de stockage ZFS
   - Commutateurs IB

   Les adresses IP pour votre configuration sont répertoriées dans le récapitulatif de déploiement fourni par le personnel d'Oracle.

   ```
   % ssh root@ILOM_SP__ipaddress
   ```

2. **Entrez le mot de passe root Oracle ILOM.**

   Voir "Comptes et mots de passe par défaut (Oracle ILOM)" à la page 40.

Détermination de la version d'Oracle ILOM

Pour tirer parti des toutes dernières fonctionnalités, capacités et améliorations de sécurité, mettez à jour le logiciel Oracle ILOM vers la version la plus récente prise en charge.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**

   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Affichez la version d'Oracle ILOM.**

   Dans cet exemple, il s'agit de la version 3.2.4.1.b du logiciel Oracle ILOM.

   ```
   -> version
   SP firmware 3.2.4.1.b
   SP firmware build number: 94529
   SP firmware date: Thu Nov 13 16:41:19 PST 2014
   SP filesystem version: 0.2.10
   ```

Remarque - Pour mettre à jour la version d'Oracle ILOM sur l'un des composants de SuperCluster, installez le patch QFSDP du SuperCluster le plus récent disponible à partir de My Oracle Support à l'adresse `https://support.oracle.com`.

Remarque - Les systèmes intégrés Oracle tels que le système SuperCluster sont soumis à des limitations concernant les versions d'Oracle ILOM qu'ils peuvent utiliser et le mode de mise à jour de ces versions. Pour plus d'informations, contactez votre représentant Oracle.

(Si nécessaire) Activation du fonctionnement compatible avec la norme FIPS-140 (Oracle ILOM)

L'utilisation d'un dispositif cryptographique conforme à la norme FIPS 140 est requise pour les clients relevant du gouvernement fédéral des Etats-Unis.

Par défaut, Oracle ILOM ne s'exécute pas en utilisant une cryptographie conforme à la norme FIPS 140. Cependant, il est possible d'activer une cryptographie conforme à la norme FIPS 140, le cas échéant.

Certaines fonctionnalités et capacités d'Oracle ILOM ne sont pas disponibles lorsqu'elles sont configurées pour s'exécuter conformément à la norme FIPS 140. Une liste de ces fonctionnalités est présentée dans la section intitulée "Fonctions non prises en charge lorsque le mode FIPS est activé" du manuel *Guide de sécurité d'Oracle ILOM* (voir la section "Ressources supplémentaires sur Oracle ILOM" à la page 52).

Reportez-vous également à la section "Conformité FIPS-140-2 de niveau 1" à la page 128.

Attention - Cette tâche requiert la réinitialisation d'Oracle ILOM. Une réinitialisation entraîne la perte de tous les paramètres configurés par l'utilisateur. Vous devez donc activer un mode de fonctionnement compatible avec la norme FIPS 140 avant d'apporter d'autres modifications spécifiques au site à Oracle ILOM. Pour les systèmes dont la configuration a fait l'objet de modifications spécifiques au site, sauvegardez la configuration d'Oracle ILOM pour pouvoir la restaurer après la réinitialisation d'Oracle ILOM, sinon ces modifications de configuration seront perdues.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**
   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Déterminez si l'instance Oracle ILOM est configurée pour un mode de fonctionnement compatible avec la norme FIPS 140.**

```
-> show /SP/services/fips state status
/SP/services/fips
Properties:
state = enabled
status = enabled
```

Le mode compatible avec la norme FIPS 140 dans Oracle ILOM est représenté par les propriétés `state` et `status`. Les propriétés `state` et `status` représentent respectivement le mode configuré et le mode opérationnel dans Oracle ILOM. En cas de modification de la propriété `state` FIPS, le mode opérationnel (propriété `status` FIPS) reste inchangé jusqu'à la prochaine réinitialisation d'Oracle ILOM.

3. **Activez le mode de fonctionnement compatible avec la norme FIPS 140.**

```
-> set /SP/services/fips state=enabled
```

4. **Redémarrez le processeur de service d'Oracle ILOM.**

Le SP d'Oracle ILOM doit être redémarré pour que cette modification soit appliquée.

```
-> reset /SP
```

Comptes et mots de passe par défaut (Oracle ILOM)

Compte	Type	Mot de passe par défaut	Description
`root`	administrateur	`welcome1`	Il s'agit du compte par défaut fourni et activé par ce composant. Ce compte permet d'effectuer la configuration initiale et de créer d'autres comptes d'administration non partagés. Pour des raisons de sécurité, modifiez le mot de passe par défaut.

Services réseau exposés par défaut (Oracle ILOM)

Ce tableau répertorie les services réseau par défaut exposés par Oracle ILOM.

Pour plus d'informations sur ces services, reportez-vous au manuel *Oracle ILOM Security Guide* (voir "Ressources supplémentaires sur Oracle ILOM" à la page 52).

Nom du service	Protocole	Port	Description
SSH	TCP	22	Utilisé par le service de shell sécurisé (SSH) intégré pour fournir l'accès administratif à Oracle ILOM à l'aide d'une CLI.
HTTP (BUI)	TCP	80	Utilisé par le service HTTP intégré pour fournir l'accès administratif à Oracle ILOM à l'aide d'une interface de navigateur. Le port TCP/80 est généralement utilisé pour l'accès en texte clair mais, par

Nom du service	Protocole	Port	Description
			défaut, Oracle ILOM redirige automatiquement les demandes entrantes vers la version sécurisée du service exécutée sur le port TCP/443.
NTP	UDP	123	Utilisé par le service (client uniquement) NTP (Network Time Protocol) intégré qui permet de synchroniser l'horloge système locale à une ou plusieurs sources temporelles externes.
SNMP	UDP	161	Utilisé par le service SNMP intégré pour fournir une interface de gestion permettant de surveiller l'intégrité d'Oracle ILOM et les notifications de déroutement reçues.
HTTPS (BUI)	TCP	443	Utilisé par le service HTTPS intégré pour fournir l'accès administratif à Oracle ILOM via un canal (SSL/TLS) chiffré à l'aide d'une interface de navigateur.
IPMI	TCP	623	Utilisé par le service IPMI (Intelligent Platform Management Interface) intégré pour fournir une interface informatique à diverses fonctions de surveillance et de gestion. Ce service ne doit pas être désactivé, car il est utilisé par Oracle Enterprise Manager Ops Center pour collecter des données d'inventaire matériel, des descriptions FRU, des informations relatives aux capteurs matériels et des informations sur le statut des composants matériels.
KVMS à distance	TCP	5120 5121 5123 5555 5556 7578 7579	Collectivement, les ports KVMS distants fournissent un ensemble de protocoles qui prennent en charge diverses fonctionnalités à distance (clavier, vidéo, souris, stockage) utilisables avec Oracle Integrated Lights Out Manager.
ServiceTag	TCP	6481	Utilisé par le service Oracle ServiceTag. Il s'agit d'un protocole de découverte Oracle permettant d'identifier les serveurs et de faciliter les demandes d'assistance. Ce service est utilisé par certains produits tels qu'Oracle Enterprise Manager Ops Center pour la découverte du logiciel Oracle ILOM et l'intégration avec les autres solutions de services automatiques Oracle.
WS-Man sur HTTPS	TCP	8888	Utilisé par le service WS-Man intégré pour fournir une interface de services, basée sur des normes, qui permet de gérer Oracle ILOM via le protocole HTTPS. La désactivation du service empêche d'utiliser ce protocole pour gérer Oracle ILOM. Ce service n'est plus inclus dans la version 3.2 d'Oracle ILOM.
WS-Man sur HTTP	TCP	8889	Ce port est utilisé par le service WS-Man intégré pour fournir une interface de services, basée sur des normes, qui permet de gérer Oracle ILOM via le protocole HTTP. La désactivation du service empêche d'utiliser ce protocole pour gérer Oracle ILOM. Ce service n'est plus inclus dans la version 3.2 d'Oracle ILOM.
Accès avec connexion unique	TCP	11626	Ce port est utilisé par la fonction de connexion unique intégrée qui permet de réduire le nombre de saisies des noms et mots de passe utilisateur. La désactivation du service empêche de lancer KVMS sans saisir à nouveau un mot de passe.

Renforcement de la configuration de la sécurité d'Oracle ILOM

Les rubriques suivantes décrivent la procédure de sécurisation d'Oracle ILOM à l'aide de divers paramètres de configuration.

▼ Désactivation des services inutiles (Oracle ILOM)

Désactivez tous les services qui ne sont pas nécessaires au respect des exigences de la plate-forme en matière de fonctionnement et de gestion.

Par défaut, Oracle ILOM emploie une configuration réseau sécurisée par défaut où les services non essentiels sont déjà désactivés. Toutefois, en fonction de vos stratégies et impératifs de sécurité, il peut être nécessaire de désactiver des services supplémentaires.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**

   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Dressez la liste des services pris en charge par Oracle ILOM.**

```
-> show /SP/services
```

3. **Déterminez si un service donné est activé.**
   Remplacez *servicename* par le nom du service identifié à l'Étape 2.

   ```
   -> show /SP/services/servicename servicestate
   ```

   La plupart des services reconnaissent et utilisent le paramètre `servicestate` pour indiquer qu'ils sont activés ou désactivés, mais certains autres, tels que `servicetag`, `ssh`, `sso` et `wsman`, se servent d'un paramètre appelé `state`. Quel que soit le paramètre utilisé, un service est activé si le paramètre `servicestate` ou `state` renvoie la valeur `enabled`, tel qu'indiqué dans les exemples suivants :

   ```
   -> show /SP/services/https servicestate
   /SP/services/https
   Properties:
   servicestate = enabled
   ```

   ```
   -> show /SP/services/ssh state
   /SP/services/ssh
   Properties:
   state = enabled
   ```

4. **Pour désactiver un service qui n'est pas requis, définissez son état sur `disabled`.**

   ```
   -> set /SP/services/http servicestate=disabled
   ```

5. **Déterminez si l'un des services suivants doit être désactivé.**
   En fonction des outils et des méthodes employés, les services supplémentaires suivants peuvent être désactivés s'ils ne sont pas requis ou utilisés :

   - **Pour une interface d'administration de navigateur (HTTP, HTTPS), entrez** :

     ```
     -> set /SP/services/http servicestate=disabled
     -> set /SP/services/http secureredirect=disabled
     -> set /SP/services/https servicestate=disabled
     ```

   - **Pour le service KVMS (clavier, vidéo, souris et stockage), entrez** :

     ```
     -> set /SP/services/kvms servicestate=disabled
     ```

   - **Pour la gestion des services Web (WS-Man sur HTTP/HTTPS) - (Oracle ILOM version 3.1 et ultérieure), entrez** :

     ```
     -> set /SP/services/wsman state=disabled
     ```

   - **Pour les services de connexion unique (SSO), entrez** :

```
-> set /SP/services/sso state=disabled
```

Configuration de la redirection HTTP vers HTTPS (Oracle ILOM)

Par défaut, Oracle ILOM IB est configuré pour rediriger les demandes HTTP entrantes vers le service HTTPS pour garantir que toutes les communications basées sur un navigateur sont chiffrées entre Oracle ILOM et l'administrateur.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**

   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Vérifiez que la redirection sécurisée est activée.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Si la valeur par défaut a été modifiée, vous pouvez activer la redirection sécurisée.**

```
-> set /SP/services/http secureredirect=enabled
```

4. **Vérifiez le paramètre en répétant l'Étape 2.**

Désactivation des protocoles non autorisés

Consultez les rubriques suivantes pour désactiver les protocoles non autorisés :

- "Désactivation du protocole SSLv2 pour HTTPS" à la page 44
- "Désactivation du protocole SSLv3 pour HTTPS" à la page 45

Désactivation du protocole SSLv2 pour HTTPS

Par défaut, le protocole SSLv2 est désactivé pour le service HTTPS.

Pour des raisons de sécurité, il est très important de désactiver le protocole SSLv2.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**
   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Déterminez si le protocole SSLv2 est désactivé pour le service HTTP.**

```
-> show /SP/services/https sslv2
/SP/services/https
Properties:
sslv2 = disabled
```

3. **Si le service est activé, désactivez le protocole SSLv2.**

```
-> set /SP/services/https sslv2=disabled
```

4. **Vérifiez le paramètre en répétant l'Étape 2.**

▼ Désactivation du protocole SSLv3 pour HTTPS

Par défaut, le protocole SSLv3 est activé pour le service HTTPS.

Pour des raisons de sécurité, désactivez le protocole SSLv3.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**
   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Déterminez si le protocole SSLv3 est désactivé pour le service HTTP.**

```
-> show /SP/services/https sslv3
/SP/services/https
Properties:
sslv3 = enabled
```

3. **Désactivez le protocole SSLv3.**

```
-> set /SP/services/https sslv3=disabled
```

4. **Vérifiez le paramètre en répétant l'Étape 2.**

▼ Désactivation des protocoles TLS non autorisés pour HTTPS

Par défaut, les protocoles TLSv1.0, TLSv1.1 et TLSv1.2 sont activés pour le service HTTPS.

Vous pouvez désactiver une ou plusieurs versions du protocole TLS non conformes à vos stratégies de sécurité.

Pour des raisons de sécurité, utilisez TLSv1.2 sauf si la prise en charge des versions antérieures du protocole TLS est requise.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**
   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Dressez la liste des versions du protocole TLS activées pour le service HTTPS.**

```
-> show /SP/services/https tlsv1 tlsv1_1 tlsv1_2
/SP/services/https
Properties:
tlsv1 = enabled
tlsv1_1 = enabled
tlsv1_2 = enabled
```

3. **Désactivez TLSv1.0.**

```
-> set /SP/services/https tlsv1_0=disabled
```

4. **Désactivez TLSv1.1.**

```
-> set /SP/services/https tlsv1_1=disabled
```

5. **Vérifiez le paramètre en répétant l'Étape 2.**

▼ Désactivation des chiffrements SSL de complexité faible et moyenne pour HTTPS

Par défaut, Oracle ILOM désactive l'utilisation de chiffrements de complexité faible et moyenne pour le service HTTPS.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**
   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Déterminez si les chiffrements de complexité faible et moyenne sont désactivés.**

```
-> show /SP/services/https weak_ciphers
/SP/services/https
Properties:
weak_ciphers = disabled
```

3. **Si la valeur par défaut a été modifiée, vous pouvez désactiver l'utilisation de chiffrements de complexité faible et moyenne.**

```
-> set /SP/services/https weak_ciphers=disabled
```

4. **Vérifiez le paramètre en répétant l'Étape 2.**

▼ Désactivation des protocoles SNMP non autorisés (Oracle ILOM)

Par défaut, seul le protocole SNMPv3 est activé pour le service SNMP qui permet de surveiller et gérer Oracle ILOM. Veillez à laisser les anciennes versions du protocole SNMP désactivées sauf si elles sont requises.

Certains produits Oracle et tiers sont soumis à des limitations au niveau de la prise en charge des versions plus récentes du protocole SNMP. Reportez-vous à la documentation du produit associée à ces composants pour vous assurer qu'ils sont compatibles avec certaines versions spécifiques du protocole SNMP. Vérifiez qu'Oracle ILOM est configuré pour prendre en charge toutes les versions du protocole nécessaires à ces composants.

Remarque - La version 3 du protocole SNMP intègre la prise en charge du modèle USM (User-based Security Model). Cette fonctionnalité remplace les chaînes de communauté SNMP standard par des comptes d'utilisateur qui peuvent être configurés avec des protocoles et des mots de passe d'autorisation, d'authentification et de confidentialité spécifiques. Par défaut, Oracle ILOM n'inclut pas de compte USM. Configurez les comptes USM SNMPv3 en fonction de vos propres besoins en matière de déploiement, de gestion et de surveillance.

---

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**

   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Déterminez le statut de chacun des protocoles SNMP.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = disabled
v2c = disabled
v3 = enabled
```

3. **Le cas échéant, désactivez les protocoles SNMPv1 et SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

4. **Vérifiez le paramètre en répétant l'Étape 2.**

Configuration des chaînes de communauté SNMP v1 et v2c (Oracle ILOM)

Cette tâche est applicable seulement si le protocole SNMP v1 ou SNMPv2c est activé et configuré pour être utilisé.

Pour garantir le bon fonctionnement du protocole SNMP, un client et un serveur doivent s'accorder sur la chaîne de communauté à utiliser pour authentifier l'accès. Par conséquent, lorsque vous modifiez les chaînes de communauté SNMP, assurez-vous que la nouvelle chaîne est configurée sur Oracle ILOM et sur tous les composants qui tenteront de se connecter à Oracle ILOM par l'intermédiaire du protocole SNMP.

Comme le protocole SNMP est souvent utilisé pour surveiller l'intégrité du périphérique, il est important de remplacer les chaînes de communauté SNMP par défaut utilisées par le périphérique par des valeurs définies par le client.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**

   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Créez une chaîne de communauté SNMP.**

   Dans cet exemple, remplacez les éléments suivants dans la ligne de commande :

   - *string* – A remplacer par une valeur définie par le client conforme aux exigences du Ministère de la Défense des Etats-Unis relatives à la composition des chaînes de communauté SNMP.
   - *access* – A remplacer par `ro` ou `rw`, selon qu'il s'agit d'une chaîne avec accès en lecture seule ou en lecture-écriture.

   ```
   -> create /SP/services/snmp/communities/string permission=access
   ```

   Après la création de nouvelles chaînes de communauté, il convient de supprimer celles fournies par défaut.

3. **Supprimez les chaînes de communauté SNMP par défaut.**

   ```
   -> delete /SP/services/snmp/communities/public
   ```

```
-> delete /SP/services/snmp/communities/private
```

4. **Vérifiez les chaînes de communauté SNMP.**

```
-> show /SP/services/snmp/communities
```

Remplacement des certificats autosignés par défaut (Oracle ILOM)

Oracle ILOM recourt à des certificats autosignés permettant d'utiliser directement les protocoles SSL et TLS. Si possible, remplacez les certificats autosignés par des certificats dont l'utilisation est autorisée dans votre environnement et qui sont signés par une autorité de certification reconnue.

Oracle ILOM prend en charge diverses méthodes permettant d'accéder au certificat numérique et à la clé privée , y compris HTTPS, HTTP, SCP, FTP, TFTP et l'insertion d'informations directement dans une interface de navigateur Web. Pour plus d'informations, reportez-vous au manuel *Oracle ILOM - Guide de configuration et de maintenance* (voir "Ressources supplémentaires sur Oracle ILOM" à la page 52).

1. **Déterminez si Oracle ILOM utilise un certificat autosigné par défaut.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

2. **Installez le certificat de votre organisation.**

```
-> set /SP/services/https/ssl/custom_cert load_uri=URI_method
-> set /SP/services/https/ssl/custom_key load_uri=URI_method
```

Configuration du délai d'expiration en cas d'inactivité dans l'interface du navigateur d'administration

Oracle ILOM prend en charge la possibilité de déconnecter et de fermer les sessions d'administration restées inactives au-delà d'un nombre de minutes prédéfini. Par défaut, la session de l'interface du navigateur expire au bout de 15 minutes.

Les paramètres d'expiration de session associés aux services HTTPS et HTTP sont définis et gérés de manière indépendante. Veillez à définir le paramètre `sessiontimeout` associé à chaque service.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**

   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Vérifiez le paramètre de délai d'expiration en cas d'inactivité associé au service HTTPS.**

```
-> show /SP/services/https sessiontimeout
/SP/services/https
Properties:
sessiontimeout = 15
```

3. **Définissez le paramètre de délai d'expiration en cas d'inactivité.**

   Remplacez *n* par une valeur exprimée en minutes.

```
-> set /SP/services/https sessiontimeout=n
```

4. **Vérifiez le paramètre de délai d'expiration en cas d'inactivité associé au service HTTP.**

```
-> show /SP/services/http sessiontimeout
/SP/services/http
Properties:
sessiontimeout = 15
```

5. **Définissez le paramètre de délai d'expiration en cas d'inactivité.**

   Remplacez *n* par une valeur exprimée en minutes.

```
-> set /SP/services/http sessiontimeout=n
```

6. **Vérifiez le paramètre en répétant les étapes Étape 2 et Étape 4.**

▼ Configuration du délai d'expiration de l'interface d'administration (CLI d'Oracle ILOM)

Oracle ILOM prend en charge la possibilité de déconnecter et de fermer les sessions CLI restées inactives au-delà d'un nombre de minutes prédéfini.

Comme aucune valeur n'est spécifiée par défaut pour le délai d'expiration de la CLI SSH, la session des utilisateurs administratifs qui accèdent à ce service reste ouverte indéfiniment.

Pour des raisons de sécurité, réglez ce paramètre de manière à ce qu'il corresponde à la valeur associée à l'interface utilisateur du navigateur. Il peut s'agir de 15 minutes ou d'une autre valeur.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**
   Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Vérifiez le paramètre de délai d'expiration en cas d'inactivité associé à la CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Définissez le paramètre de délai d'expiration en cas d'inactivité.**
   Remplacez *n* par une valeur exprimée en minutes.

```
-> set /SP/cli timeout=n
```

4. **Vérifiez le paramètre en répétant l'Étape 2.**

Configuration de bannières d'avertissement de connexion (Oracle ILOM)

Oracle ILOM prend en charge la capacité d'afficher des messages spécifiques au client avant et après la connexion d'un administrateur au périphérique.

Le message de connexion à Oracle ILOM s'affiche avant l'authentification, alors que le message d'ouverture de session s'affiche après.

Vous pouvez également configurer Oracle ILOM pour requérir l'acceptation du message d'ouverture de session avant que l'accès aux fonctions d' Oracle ILOM ne soit accordé. Les messages de connexion et d'ouverture de session et l'exigence d'acceptation facultative sont implémentés dans l'interface du navigateur et dans l'interface de ligne de commande.

Oracle ILOM prend en charge les messages de connexion et d'ouverture de session comportant jusqu'à 1 000 caractères.

1. **Sur le réseau de gestion, connectez-vous à Oracle ILOM.**

Voir "Connectez-vous à l'interface de ligne de commande d'Oracle ILOM" à la page 38.

2. **Déterminez si les messages de connexion et d'ouverture de session sont configurés.**

```
-> show /SP/preferences/banner connect_message login_message
/SP/preferences/banner
Properties:
connect_message = (none)
login_message = (none)
```

3. **Définissez un message de connexion ou d'ouverture de session.**

```
-> set /SP/preferences/banner connect_message="Authorized Use Only"
-> set /SP/preferences/banner login_message="Authorized Use Only"
```

4. **Déterminez si l'acceptation du message d'ouverture de session est activée.**

```
-> show /SP/preferences/banner login_message_acceptance
/SP/preferences/banner
Properties:
login_message_acceptance = disabled
```

5. **(Facultatif) Activez l'acceptation du message d'ouverture de session.**

Attention - Requérir l'acceptation d'un message d'ouverture de session peut entraver le bon fonctionnement des processus de gestion automatisés qui utilisent SSH, car ils risquent de ne pas être configurés pour répondre à la demande d'acceptation ou d'y être incapables. Par conséquent, de telles connexions sont susceptibles de se bloquer ou d'expirer, dans la mesure où Oracle ILOM interdit tout usage de la CLI tant que l'exigence relative à l'acceptation du message n'a pas été satisfaite.

```
-> set /SP/preferences/banner login_message_acceptance=enabled
```

6. **Vérifiez le paramètre en répétant les étapes Étape 2 et Étape 4.**

Ressources supplémentaires sur Oracle ILOM

Pour plus d'informations sur les procédures d'administration et de sécurité d'Oracle ILOM, reportez-vous à la bibliothèque de documentation Oracle ILOM qui correspond à la version exécutée sur le système SuperCluster M7 :

- Guide de sécurité d'*Oracle ILOM · Microprogramme versions 3.0, 3.1 et 3.2* :

http://docs.oracle.com/cd/E37444_01/html/E37451

- Oracle Integrated Lights Out Manager version 3.2.*x* :

  http://docs.oracle.com/cd/E37444_01
- Oracle Integrated Lights Out Manager version 3.1.*x* :

  http://docs.oracle.com/cd/E24707_01
- Oracle Integrated Lights Out Manager Version 3.0.*x* :

  http://docs.oracle.com/cd/E19860-01

Sécurisation des serveurs de calcul

Un ou deux serveurs SPARC M7 (serveurs de calcul) sont installés dans le système SuperCluster M7. Chaque serveur de calcul est divisé en deux partitions matérielles (deux domaines physiques). Chaque domaine physique inclut la moitié des processeurs, de la mémoire et des emplacements d'extension PCIe possibles dans le châssis. Les deux domaines physiques fonctionnent comme un serveur distinct au sein du même châssis. Une paire redondante de modules de processeur de service (SPM) gère chaque partition.

Vous devez sécuriser chaque domaine physique.

Cette section fournit un ensemble de commandes de sécurité pour les serveurs de calcul.

▼ Connexion à un serveur de calcul et modification du mot de passe par défaut

Pour accéder à un domaine physique via Oracle ILOM, vous devez vous connecter au SPM actif qui contrôle ce domaine physique. Il est possible de mettre sous tension, réinitialiser ou gérer une partition pendant que l'autre continue de fonctionner normalement.

Il existe plusieurs méthodes différentes pour vous connecter à un serveur de calcul SuperCluster. La méthode décrite dans cette tâche implique une connexion à la CLI d'Oracle

ILOM sur le SPM du serveur de calcul. Elle vous permet d'accéder au serveur dans l'un des états suivants :

- Mode veille
- Système mis sous tension, mais l'hôte n'est pas en cours d'exécution
- Système d'exploitation en cours d'initialisation
- Système entièrement sous tension et système d'exploitation en cours d'exécution

1. **Sur le réseau de gestion, connectez-vous à l'aide de la commande `ssh`.**

```
$ ssh root@compute_server_SPM_ILOM_IP-address
```

2. **A l'invite, entrez le mot de passe.**

Le mot de passe `root` défini par défaut en usine est `welcome1`.

Si vous êtes invité à modifier le mot de passe, changez-le.

A ce stade, vous pouvez effectuer les tâches de sécurité qui sont exécutées sur Oracle ILOM sur le serveur de calcul.

3. **Si vous voulez accéder à la console hôte du serveur de calcul, démarrez-la.**

```
    -> start /Servers/PDomains/PDomain_0/HOST/console
Are you sure you want to start /Servers/PDomains/PDomain_0/HOST/console (y/n)? y

Serial console started.  To stop, type #.

root@system-identifier-pd0:~#
```

Remarque - Vous ne verrez pas l'invite du domaine physique si l'hôte n'est pas en cours d'exécution.

Remarque - Pour repasser sous l'invite d'Oracle ILOM, entrez les caractères d'échappement (`#.` sont les caractères par défaut).

4. **Si nécessaire, prenez un rôle de superutilisateur.**

Utilisez la commande `su` pour basculer vers un utilisateur configuré avec le rôle `root`.

Comptes et mots de passe par défaut (serveurs de calcul)

Compte	Mot de passe par défaut	Description
`root`	`welcome1`	Oracle ILOM requiert la modification immédiate du mot de passe par défaut après la première connexion.
`oracle`	`welcome1`	
`grid`	`welcome1`	

▼ Identification de la version du logiciel SuperCluster

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Saisissez cette commande.**

```
# svcprop -p configuration/build svc:/system/oes/id:default
```

   Dans la sortie, les chiffres ajoutés à `ssc` représentent la version du logiciel.

   Pour mettre à jour la version du logiciel SuperCluster, installez le dernier SuperCluster Quarterly Full Stack Download Patch disponible à partir de My Oracle Support à l'adresse `https://support.oracle.com`.

Remarque - Pour le système SuperCluster, des restrictions supplémentaires pourraient limiter les versions du logiciel utilisables et la manière de les mettre à jour. Dans un tel cas, contactez votre représentant Oracle.

▼ Configuration du service SSH (Secure Shell)

Effectuez cette tâche pour améliorer la configuration de la sécurité Secure Shell déployée dans l'environnement Oracle SuperCluster.

Le fichier `/etc/ssh/sshd_config` est un fichier de configuration système dans lequel vous configurez des paramètres pour le service Secure Shell.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**
   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Modifiez le fichier `/etc/ssh/sshd_config`.**

3. **Configurez le paramètre `ListenAddress` de sorte que seules les connexions provenant du réseau d'accès client SuperCluster soient acceptées.**
   Vérifiez que l'adresse IP `ListenAddress` est définie sur le réseau client.
   Ainsi, il n'est pas possible de démarrer des connexions Secure Shell entre des composants via les réseaux de gestion ou IB.

4. **Consultez les autres paramètres `sshd_config` et définissez-les en fonction des exigences du site.**
   Ces paramètres sécurisent le service Secure Shell :

```
Protocol 2
Banner /etc/issue
PermitEmptyPasswords no
PermitRootLogin no
StrictModes yes
IgnoreRhosts yes
PrintLastLog yes
X11Forwarding no
ClientAliveInterval 600
ClientAliveCountMax 0
```

5. **Enregistrez le fichier `sshd_config`.**

6. **Redémarrez le service.**
   Vous devez redémarrer le service pour que les modifications prennent effet.

```
# svcadm restart ssh
```

▼ Vérification du rôle `root`

Par défaut, Oracle Solaris est configuré de sorte que `root` soit un rôle et non un compte utilisateur. En outre, la configuration SuperCluster n'autorise pas les connexions d'utilisateurs `root` anonymes. Au lieu de cela, tous les utilisateurs doivent se connecter en tant qu'utilisateurs classiques avant de prendre le rôle root. Toutes les opérations d'administration de SuperCluster doivent être effectuées à l'aide du rôle `root`.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte.**

Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Vérifiez que les attributs `root` sont définis sur `type=role`.**

```
# grep root /etc/user_attr
root::::type=role
```

3. **(Facultatif) Affectez à un utilisateur classique le rôle `root`.**

```
# usermod -R root user_name
```

Services réseau exposés par défaut (serveurs de calcul)

Ce tableau répertorie les services réseau par défaut qui sont réexposés sur les serveurs de calcul.

Nom du service	Protocole	Port	Description
SSH	TCP	22	Utilisé par le service Secure Shell intégré pour autoriser l'accès administratif aux serveurs de calcul à l'aide d'une interface de ligne de commande (CLI).
HTTP (BUI)	TCP	80	Utilisé par le service HTTP intégré pour autoriser l'accès administratif aux serveurs de calcul à l'aide d'une interface de navigateur.
HTTPS (BUI)	TCP	443	Utilisé par le service HTTPS intégré pour autoriser l'accès administratif aux serveurs de calcul via un canal chiffré (SSL/TLS) à l'aide d'une interface de navigateur.
SNMP	UDP	161	Utilisé par le service SNMP intégré pour fournir une interface de gestion permettant de surveiller la santé des serveurs de calcul et les notifications d'interruption reçues.

Sécurisation de la configuration du serveur de calcul

Les rubriques suivantes décrivent comment sécuriser la configuration des serveurs de calcul.

Activation du service `intrd`

Le service d'équilibreur d'interruptions (`intrd`) surveille les affectations entre les interruptions et les CPU pour optimiser les performances. Pour plus d'informations, reportez-vous à la page de manuel `intrd(1M)`.

Ce service fonctionne uniquement dans la zone globale.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**
   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Démarrez le service.**

```
# svcadm enable intrd
```

Désactivation des services inutiles (serveurs de calcul)

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Désactivez le moniteur de statut NFS si le système n'est pas un serveur ou un client NFS.**

   Ce service interagit avec `lockd(1M)` pour proposer les fonctions de panne et de récupération pour les services de verrouillage sur NFS.

   ```
   # svcadm disable svc:/network/nfs/status
   ```

3. **Désactivez le service du gestionnaire de verrous NFS si vous n'utilisez pas NFS ou que vous utilisez NFSv4.**

   Le gestionnaire de verrous NFS prend en charge les opérations de verrouillage d'enregistrements sur des fichiers NFS dans NFSv2 et NFSv3.

   ```
   # svcadm disable svc:/network/nfs/nlockmgr
   ```

4. **Si le système ne monte pas de fichiers, vous pouvez désactiver le service client NFS ou désinstaller son package.**

   Le service client NFS est nécessaire uniquement si le système monte des fichiers à partir d'un serveur NFS. Pour plus d'informations, reportez-vous à la page de manuel `mount_nfs(1M)`.

   ```
   # svcadm disable svc:/network/nfs/client
   ```

5. **Désactivez le service de serveur NFS sur un système qui n'est pas un serveur de fichiers NFS.**

   Le service de serveur NFS traite les demandes du système de fichiers client via NFS versions 2, 3 et 4. Si ce système n'est pas un serveur NFS, désactivez le service.

   ```
   # svcadm disable svc:/network/nfs/server
   ```

6. **Si vous n'utilisez pas FedFS pour les enregistrements DNS SRV ou les références LDAP, désactivez le service.**

Le service client FedFS (système de fichiers fédéré) gère les valeurs par défaut et les informations de connexion pour les serveurs LDAP qui stockent les informations FedFS.

```
# svcadm disable svc:/network/nfs/fedfs-client
```

7. **Désactivez le service `rquota`.**

   Le serveur de quotas `remote` renvoie des quotas pour un utilisateur d'un système de fichiers local qui est monté via NFS. Les résultats sont utilisés par `quota(1M)` pour afficher des quotas utilisateur pour les systèmes de fichiers distants. Le démon `rquotad(1M)` est généralement appelé par `inetd(1M)`. Le démon fournit des informations sur le réseau à d'éventuels utilisateurs malveillants.

   ```
   # svcadm disable svc:/network/nfs/rquota
   ```

8. **Désactivez le service `cbd`.**

   Le service `cbd` gère les points d'extrémité de communication pour le protocole NFS version 4. Le démon `nfs4cbd(1M)` s'exécute sur le client NFS version 4 et crée un port d'écoute pour les rappels.

   ```
   # svcadm disable svc:/network/nfs/cbd
   ```

9. **Désactivez le service `mapid` si vous n'utilisez pas NFSv4.**

   Le service du démon de mappage d'ID de groupe et d'utilisateur NFS effectue la mise en correspondance avec les attributs d'identification NFS version 4 `owner` et `owner_group` et les numéros UID et GID locaux utilisés à la fois par le client et le serveur NFS version 4.

   ```
   # svcadm disable svc:/network/nfs/mapid
   ```

10. **Désactivez le service `ftp`.**

    Le service FTP fournit un service de transfert de fichiers non chiffré et utilise l'authentification en texte brut. Utilisez le programme de copie sécurisé `scp(1)` au lieu de `ftp`, car il fournit une authentification et un transfert de fichiers chiffrés.

    ```
    # svcadm disable svc:/network/ftp:default
    ```

11. **Désactivez le service du gestionnaire de volumes distants.**

    Le gestionnaire de volumes amovibles est un gestionnaire de volumes HAL qui peut automatiquement monter et démonter un média amovible et un périphérique de stockage remplaçable à chaud. Les utilisateurs risquent d'importer des programmes malveillants ou de transférer des données sensibles hors du système. Pour plus d'informations, reportez-vous à la page de manuel `rmvolmgr(1M)`.

    Ce service fonctionne uniquement dans la zone globale.

```
# svcadm disable svc:/system/filesystem/rmvolmgr
```

12. Désactivez le service `smserver`.

Le service `smserver` permet d'accéder à des périphériques de média amovibles.

```
# svcadm disable rpc/smserver:default
```

13. Indiquez `pam_deny.so.1` comme module pour la pile d'authentification pour les services `r-protocol` dans le répertoire `/etc/pam.d`.

Par défaut, les services hérités tels que `r-protocols`, `rlogin(1)` et `rsh(1),` ne sont pas installés. Toutefois, ces services sont définis dans `/etc/pam.d`. Si vous supprimez les définitions de service de `/etc/pam.d`, les services utilisent les autres services (SSH, par exemple) en cas d'activation des services hérités.

```
# cd /etc/pam.d
# cp rlogin rlogin.orig
# pfedit rlogin
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
# cp rsh rsh.orig
# pfedit rsh
auth definitive pam_deny.so.1
auth sufficient pam_deny.so.1
auth required pam_deny.so.1
```

14. Modifiez le fichier `/etc/default/keyserv` pour remplacer la valeur de `ENABLE_NOBODY_KEYS` par `NO`.

Le service `keyserv` ne peut pas utiliser la clé utilisateur `nobody`. Par défaut, la valeur de `ENABLE_NOBODY_KEYS` est `YES`.

```
# pfedit /etc/default/keyserv
. . .
ENABLE_NOBODY_KEYS=NO
```

15. Ajoutez des utilisateurs au fichier `ftpusers` pour limiter l'accès `ftp`.

Les transferts de fichiers FTP ne doivent pas être accessibles à tous les utilisateurs et doivent nécessiter l'intervention d'utilisateurs qualifiés qui indiquent leur nom et leur mot de passe. En général, les utilisateurs système ne doivent pas être autorisés à utiliser FTP. Cette vérification contrôle que les comptes système sont inclus dans le fichier `/etc/ftpd/ftpusers`, afin qu'ils ne soient pas autorisés à utiliser FTP.

Le fichier `/etc/ftpd/ftpusers` permet d'empêcher des utilisateurs d'utiliser le service FTP. Incluez au minimum tous les utilisateurs système, comme `root`, `bin`, `adm`, etc.

```
# pfedit /etc/ftpd/ftpusers
```

```
....
root
daemon
bin
...
```

16. **Définissez un masque de création de fichier par défaut renforcé pour les fichiers créés par le serveur FTP.**

    Le serveur FTP n'utilise pas nécessairement le masque de création de fichier système de l'utilisateur. La définition du masque de création de fichier utilisateur FTP garantit que les fichiers transmis via FTP utilisent un masque de création de fichier utilisateur renforcé.

    ```
    # pfedit /etc/proftpd.conf
    Umask          027
    ```

17. **Désactivez les réponses aux demandes de topologie réseau.**

    Il est important de désactiver les réponses aux demandes d'écho. Les demandes ICMP sont gérées à l'aide de la commande `ipadm`.

    Ces paramètres empêchent la dissémination d'informations relatives à la topologie réseau.

    ```
    # ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
    # ipadm set-prop -p _respond_to_echo_broadcast=0 ip
    ```

18. **Désactivez les messages de redirection ICMP.**

    Les routeurs utilisent les messages de redirection ICMP afin d'informer les hôtes de l'existence de routes plus directes vers une destination. Un message de redirection ICMP illicite risque de provoquer une attaque Man-in-the-middle.

    ```
    # ipadm set-prop -p _ignore_redirect=1 ipv4
    ```

19. **Désactivez `mesg(1)` pour empêcher l'accès `talk(1)` et `write(1)` aux terminaux distants.**

    ```
    # mesg -n
    ```

20. **(Facultatif) Passez en revue et désactivez les services inutiles en écoute sur le réseau.**

    Par défaut, `ssh(1)` est le seul service réseau qui peut envoyer et recevoir des paquets réseau.

    ```
    # svcadm disable FMRI_of_unneeded_service
    ```

▼ Activation du multihébergement strict

Pour les systèmes constituant des passerelles vers d'autres domaines, tels qu'un pare-feu ou un noeud de réseau privé virtuel (VPN), le multihébergement strict doit être activé. La propriété

`hostmodel` contrôle le comportement d'envoi et de réception de paquets IP sur un système à multihébergement. Définissez le multihébergement strict sur `1` afin que les paquets ne soient pas acceptés sur une autre interface. La valeur par défaut est `0`.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Définissez le multihébergement strict sur `1`.**

```
# ipadm set-prop -p _strict_dst_multihoming=1 ipv4
```

Activation de la fonction ASLR

Remarque - N'activez pas la fonction ASLR dans des domaines ou des zones de base de données.

Oracle Solaris étiquette un grand nombre de fichiers binaires utilisateur afin de permettre la randomisation du format d'espace d'adressage (ASLR). ASLR randomise l'adresse de début des éléments clés de l'espace d'adressage. Ce mécanisme de défense de sécurité peut entraîner l'échec des attaques ROP (Return Oriented Programming) lorsqu'elles tentent d'exploiter les vulnérabilités logicielles. Les zones héritent de ce format aléatoire pour leurs processus. Dans la mesure où l'utilisation de la fonction ASLR risque de ne pas être optimale pour tous les fichiers binaires, elle peut être configurée au niveau des zones et des fichiers binaires.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Activez la fonction ASLR.**

```
# sxadm delcust aslr
# sxadm info
EXTENSION    STATUS                 CONFIGURATION
aslr         enabled (tagged-files) System default (default)
```

Configuration des connexions TCP

La définition du nombre maximal de connexions TCP mi-ouvertes sur 4096 par adresse IP et par port permet de se défendre contre des attaques par déni de service SYN massives. La définition du nombre maximal de connexions TCP entrantes placées en file d'attente sur 1024 au minimum empêche certaines attaques par déni de service distribuées (DDoS).

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Définissez le nombre maximal de connexions TCP entrantes placées en file d'attente et mi-ouvertes.**

```
# ipadm set-prop -p _conn_req_max_q0=9096 tcp
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

Définition des journaux de l'historique du mot de passe et des politiques de mot de passe pour la conformité PCI

Le paramètre `HISTORY` dans le fichier `/etc/default/passwd` empêche les utilisateurs d'employer des mots de passe similaires grâce à la valeur `HISTORY`.

Si `MINWEEKS` est défini sur `3` et `HISTORY` sur `10`, les mots de passe ne peuvent pas être réutilisés pendant 10 mois.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Modifiez le fichier `/etc/default/passwd` et définissez les paramètres de mot de passe.**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
```

```
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **Modifiez le fichier `/etc/default/login` pour inclure ces paramètres.**

```
# pfedit /etc/default/login
. . .
# Compliance edit
#PASSLENGTH=6
PASSLENGTH=14
. . .
```

Vérification des droits d'accès appropriés pour les répertoires de base des utilisateurs

Les répertoires de base doivent être accessibles en écriture et autoriser des recherches par leurs propriétaires. En général, les autres utilisateurs n'ont pas le droit de modifier ces fichiers ou d'en ajouter au répertoire de base de l'utilisateur. Pour garantir cela, définissez des droits d'accès au répertoire de l'utilisateur.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**
   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Définissez des droits d'accès au répertoire d'un utilisateur.**

```
# chmod 750 /export/home/user_home_directory
```

Activation du pare-feu IP Filter

IP Filter est un pare-feu hôte qui assure un filtrage de paquets avec état et la translation d'adresse réseau (NAT). Le filtrage de paquets assure une protection de base contre les attaques potentielles via le réseau. IP Filter permet également le filtrage de paquets sans état, ainsi que la création et la gestion des pools d'adresses.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Activez le pare-feu IP Filter.**

```
# svcadm svc:/network/ipfilter:default
```

Vérification de l'utilisation exclusive de fichiers locaux par les services de noms

Le système d'exploitation utilise un certain nombre de bases de données d'informations sur les hôtes, `ipnodes`, utilisateurs (`passwd(4)`, `shadow(4)`, `user_attr(4)`) et `groups`. Les données pour ces éléments proviennent de diverses sources. Les noms et adresses d'hôte, par exemple, se trouvent dans `/etc/hosts`, NIS, LDAP, DNS ou DNS multidiffusion. Les systèmes situés dans des environnements à accès restreint sont plus sécurisés si seules des entrées de fichiers locaux sont utilisées pour ces éléments.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Configurez les services de noms pour qu'ils utilisent uniquement des fichiers locaux.**

```
# svccfg -s name-service/switch setprop config/default = astring: "files"
# svccfg -s name-service/switch setprop config/host = astring: "files"
# svccfg -s name-service/switch setprop config/password = astring: "files"
# svccfg -s name-service/switch setprop config/group = astring: "files"
# svccfg -s name-service/switch:default refresh
```

Activation des services sendmail et NTP

Le service sendmail doit être en cours d'exécution, sinon les courriers système importants envoyés à `root` risquent de ne pas être délivrés.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Activez sendmail.**

```
# svcadm enable smtp:sendmail
```

3. **Si nécessaire, installez le service NTP.**

Le service `ntp` doit être installé sur tous les systèmes nécessitant des fonctions de sécurité et de conformité.

```
# pkg install service/network/ntp
```

4. **Configurez le service NTP en tant que client et activez le service.**

Le démon NTP (Network Time Protocol) doit être activé et correctement configuré en tant que client. Le fichier `/etc/inet/ntp.conf` doit inclure au moins une définition de serveur. Le fichier doit également contenir la ligne `restrict default ignore` pour empêcher le client de faire aussi office de serveur.

```
# vi /etc/inet/ntp.conf
. . .
server server_IP_address iburst
restrict default ignore ...
# svcadm enable ntp
```

Désactivation de GSS (sauf en cas d'utilisation de Kerberos)

Le service de sécurité générique (`gss`) gère la génération et la validation des jetons de sécurité de l'API GSS (interface de programme d'application du service de sécurité générique). Le démon `gssd(1M)` fonctionne entre le noyau `rpc` et l'API GSS.

Remarque - Kerberos utilise ce service. Désactivez le service `rpc/gss` si Kerberos n'est pas configuré, ni en cours d'utilisation.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Activez `rpc/gss`.**

```
# svcadm enable rpc/gss
```

3. **Définissez une limite de taille pour `/tmpfs`.**
Par défaut, la taille du système de fichiers `tmpfs` n'est pas limitée. Pour assurer des performances optimales, vous pouvez limiter la taille de chaque montage du système de fichiers `tmpfs`. Pour plus d'informations, reportez-vous aux pages de manuel `mount_tmpfs(1M)` et `vfstab(4)`.

```
# pfedit /etc/vfstab
...
swap - /tmp tmpfs - yes size=sz
```

4. **Réinitialisez le serveur de calcul.**

```
# reboot
```

Définition du sticky bit pour les fichiers inscriptibles par tous

Le sticky bit sur un répertoire empêche que les fichiers d'un répertoire inscriptible par tous soient supprimés ou déplacés par un autre utilisateur que le propriétaire du fichier, ou le rôle `root`. Cela peut être utile dans les répertoires communs à de nombreux utilisateurs, comme le répertoire `/tmp`.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**
Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Définissez le sticky bit sur `/tmp` et sur tout autre fichier inscriptible par tous.**

```
# chmod 1777 /tmp
```

Protection des dumps noyau

Les dumps noyau peuvent contenir des données sensibles. Les dispositifs de protection peuvent inclure les droits d'accès aux fichiers et la journalisation des événements du dump noyau. Reportez-vous aux pages de manuel `coreadm(1m)` et `chmod(1M)`.

Utilisez la commande `coreadm` pour afficher et définir la configuration actuelle.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**
   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Affichez la configuration actuelle.**

```
# coreadm
global core file pattern: /var/share/cores/core.%f.%p
global core file content: default
init core file pattern: core
init core file content: default
global core dumps: enabled
per-process core dumps: enabled
global setid core dumps: disabled
per-process setid core dumps: disabled
global core dump logging: enabled
```

3. **Configurez les fichiers noyau et protégez le répertoire du dump noyau.**

```
# coreadm -g /var/cores/core_%n_%f_%u_%g_%t_%p \
          -e log -e global -e global-setid \
          -d process -d proc-setid
```

4. **Vérifiez les droits d'accès.**

```
# ls -ld /var/share/cores
drwx------ 2 root root 2 Aug 2 2015 cores/
```

5. **Définissez les droits d'accès appropriés au répertoire.**

```
# chmod 700 /var/share/cores
```

Application de piles non exécutables

L'activation de piles non exécutables est une technique très utile pour lutter contre certains types d'attaques par débordement de tampon. Lorsqu'Oracle Solaris `nxstack` est activé, le segment de mémoire de pile de processus est marqué comme non exécutable. Cette extension permet de se défendre contre les attaques qui se fondent sur l'injection de code malveillant et son exécution sur la pile.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Activez `nxstack`.**

```
# sxadm set model=all nxstack
```

3. **Vérifiez la configuration.**

```
# sxadm get all nxstack
EXTENSION     PROPERTY     VALUE
nxstack         model        all
```

Activation d'un espace de swap chiffré

Chiffrez l'espace de swap, qu'il s'agisse d'un volume ZFS ou d'un périphérique brut. Le chiffrement garantit la protection des données sensibles, telles que les mots de passe utilisateur, si le système a besoin de permuter ces pages vers le disque.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Modifiez le fichier `/etc/vfstab` et définissez la commande `swap` sur `encrypted`.**

```
# pfedit /etc/vfstab
...
/dev/zvol/dsk/rpool/swap - - swap - no encrypted
```

3. **Créez et initialisez un keystore PKCS #11.**

```
# pktool setpin keystore=pkcs11
Enter token passphrase: changeme
Create new passphrase: welcome1
Re-enter new passphrase: welcome1
```

4. **Générez une clé symétrique et stockez-la dans un keystore PKCS #11.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=globalzone-key
```

Activation de l'audit

Vérifiez que les journaux d'audit contiennent toutes les actions administratives, notamment les commandes avec leurs arguments.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Configurez la fonction d'audit.**

```
# auditconfig -setpolicy +argv
# auditconfig -setflags lo,ad,ex >& /dev/null
# auditconfig -setpolicy +zonename
```

Activation de la protection (usurpation d'adresse) de la liaison de données sur des zones globales

La protection de la liaison de données Oracle Solaris empêche le réseau de subir d'éventuels dommages pouvant être provoqués par des machines virtuelles invitées malveillantes.

L'activation de la configuration d'usurpation d'adresse à des fins d'espionnage améliore les performances du réseau en permettant au trafic du réseau de l'environnement virtuel d'être isolé du trafic général envoyé ou reçu par le système hôte. La protection de la liaison empêche le réseau de subir des dommages pouvant être provoqués par des machines virtuelles invitées potentiellement malveillantes. Cette fonction offre une protection contre les menaces de base suivantes :

- Usurpation d'adresse IP et MAC
- Usurpation de trame de niveau 2 telle que les attaques BPDU (Bridge Protocol Data Unit)

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Définissez la protection de la liaison.**

```
# dladm set-linkprop -p protection=mac-nospoof,restricted,ip-nospoof,dhcp-nospoof net0
```

3. **Confirmez la configuration.**

```
# dladm show-linkprop -p protection net0
LINK         PROPERTY     PERM     VALUE         EFFECTIVE         DEFAULT     POSSIBLE
net0         protection     rw     mac-nospoof   mac-nospoof        --         mac-nospoof,
                                   restricted    restricted         --         restricted,
                                   ip-nospoof    ip-nospoof         --         ip-nospoof,

                                   dhcp-nospoof  dhcp-nospoof       --         dhcp-nospoof
```

4. **Définissez les adresses IP autorisées sur la liaison.**

```
# dladm set-linkprop -p allowed-ips=10.0.0.1,10.0.0.2 net0
```

▼ Activation de la protection (usurpation d'adresse) de la liaison de données sur des zones non globales

La protection de la liaison de données Oracle Solaris peut également être appliquée individuellement à toutes les zones non globales Oracle Solaris déployées au sein de l'environnement SuperCluster.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Appliquez la protection de la liaison de données à une interface réseau donnée à l'aide de la commande `zonecfg(1M)`.**

   Vérifiez que la liste des adresses IP autorisées est précise et exhaustive. Elle doit inclure les adresses IP virtuelles utilisées par Oracle Solaris IPMP, Oracle Real Application Clusters, etc. Notez également que les modifications apportées à la configuration des zones non globales SuperCluster n'entrent pas en vigueur tant que la zone non globale n'est pas redémarrée.

```
# zonecfg –z zonename
zonecfg:zonename> select anet linkname=network-link-name
zonecfg:zonename:anet> set allowed-address="list_of_allowed_IP_addresses"
zonecfg:zonename:anet>  set link-protection=mac-nospoof,ip-nospoof,restricted
zonecfg:zonename:anet>  set configure-allowed-address=false
zonecfg:zonename:anet>  end
```

```
zonecfg:zonename>  commit
zonecfg:zonename>  exit
```

Création de jeux de données ZFS chiffrés

Les entreprises nécessitant une protection des *données au repos* peuvent opter pour une protection accrue des applications déployées dans les zones et des informations à l'aide de jeux de données ZFS chiffrés. Afin de s'assurer que chaque zone non globale peut démarrer sans intervention de l'administrateur, les jeux de données ZFS chiffrés sont configurés pour accéder aux clés de chiffrement ZFS qui sont stockées localement au sein de la base de données ou du domaine d'application individuel.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Créez des clés de chiffrement ZFS.**

   Une méthode simple pour créer la clé requise consiste à utiliser des commandes semblables à celles-ci :

   ```
   # zfs create zfs_pool_name/zfskeystore
   $ chown root:root /zfs_pool_name/zfskeystore
   $ chmod 700 /zfs_pool_name/zfskeystore
   $ pktool genkey keystore=file keytype=aes keylen=256 \
   outkey=/zfs_pool_name/zfskeystore/zone_name.key
   ```

3. **Créez le jeu de données ZFS chiffré.**

   ```
   # zfs create -o encryption=aes-256-ccm -o \
   keysource=raw,file:///zfs_pool_name/zone_name.key \
   zfs_pool_name/zone_name
   ```

4. **Chiffrez les jeux de données communs et u01.**

   Cette approche peut également être utilisée pour chiffrer les jeux de données communs et u01, à l'aide de la même clé (spécifique à SuperCluster) ou d'une clé unique par jeu de données en fonction des exigences et des politiques propres au site. Dans cet exemple, le jeu de données commun est créé à l'aide de la clé générée à l'Étape 3. Notez que vous pouvez également définir des paramètres de configuration ZFS supplémentaires, comme la compression, lors de la création de ces jeux de données supplémentaires.

   ```
   # zfs create -o compression=on -o encryption=aes-256-ccm -o \
   ```

```
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

(Facultatif) Définition d'une phrase de passe pour l'accès au keystore

La tâche précédente, "Création de jeux de données ZFS chiffrés" à la page 75, utilise un fichier de clés (brut) défini localement, qui doit être stocké directement sur un système de fichiers. Une autre technique de stockage de clé exploite un keystore PKCS#11 protégé par une phrase de passe : le *Softtoken Sun Software PKCS#11*. Pour utiliser cette méthode, exécutez cette tâche.

Le keystore PKCS#11 doit être déverrouillé manuellement au préalable pour que la clé soit mise à disposition dans ZFS. Cela signifie donc qu'une intervention administrative manuelle est requise pour monter le jeu de données ZFS chiffré (et démarrer la zone non globale si la zone utilise également un jeu de données ZFS chiffré). Pour plus d'informations sur d'autres stratégies de stockage de clés, reportez-vous à la page de manuel `zfs_encrypt(1M)`.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**
   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Définissez un code PIN (phrase de passe) qui sera requis pour accéder au keystore.**
   Le code PIN par défaut associé à un nouveau keystore PKCS#11 est `changeme`. Utilisez cette phrase de passe à la première invite dans cet exemple.

```
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

3. **Définissez une variable d'environnement `${SOFTTOKEN}` pour stocker la clé à un autre emplacement.**
   Les composants de clé utilisés par le Softtoken PKCS#11 sont stockés par défaut dans le répertoire `/var/user/ ${USERNAME}/pkcs11_softtoken`. La variable d'environnement `${SOFTTOKEN}` peut être définie pour stocker les composants de clé à un autre emplacement. Vous pouvez utiliser cette fonction pour autoriser un stockage spécifique à SuperCluster pour ces composants de clé protégés par une phrase de passe.

```
# export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
# pktool setpin keystore=pkcs11
```

```
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

4. **Créez une clé.**

```
# pktool genkey keystore=pkcs11 keytype=aes keylen=256 label=zone_name_rpool
Enter PIN for Sun Software PKCS#11 softtoken:
```

5. **Créez le jeu de données ZFS chiffré, en faisant référence à la clé créée à l'étape précédente.**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

Création de zones globales immuables

La résistance aux dégradations avec immutabilité permet à des zones globales et non globales de créer un environnement d'exploitation résistant, à haute intégrité, au sein duquel les serveurs de calcul SuperCluster exécutent leurs propres services. En se basant sur les fonctions de sécurité inhérentes des zones globales et non globales Oracle Solaris, les zones immuables vérifient que les fichiers et répertoires du système d'exploitation (en partie ou en totalité) ne peuvent pas être modifiés (sans intervention de l'administrateur). L'application de cette approche en lecture seule permet d'éviter les modifications non autorisées, renforce les procédures de gestion des changements et dissuade l'injection de malware au niveau de l'utilisateur et du noyau.

Remarque - Une fois qu'une zone immuable est configurée, elle ne peut être mise à jour que par la connexion Trusted Path ou lors de la réinitialisation du système en mode inscriptible à l'aide de la commande `reboot -- -w`.

Alors que vous devez toujours confirmer que le logiciel de l'application fonctionne comme prévu dans un environnement immuable, l'exécution correcte des instances Oracle Database et des clusters Oracle RAC dans des zones non globales immuables Oracle Solaris est vérifiée.

1. **Connectez-vous à la zone globale Oracle Solaris (domaine dédié, domaine root ou domaine d'E/S) en tant que superutilisateur.**
   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Modifiez la configuration de la zone globale Oracle Solaris en définissant la propriété `file-mac-profile`.**

```
# zonecfg -z global set file-mac-profile=fixed-configuration
zonecfg:global> commit
```

3. **Réinitialisez la zone globale Oracle Solaris pour que les modifications entrent en vigueur. Connectez-vous au domaine via la console ILOM.**

4. **Démarrez la console du chemin d'accès sécurisé à la zone globale immuable.**

   La zone globale immuable étant configurée, il est important de saisir les informations de connexion à la console en utilisant l'une des séquences d'interruption suivantes :

   - **Console graphique** – F1-A
   - **Console série** – <Inter> ou séquence d'interruption de remplacement (CR~ Ctrl-b)

```
trusted path console login:
```

5. **Connectez-vous à la zone globale du domaine d'E/S et prenez le rôle `root` pour effectuer des mises à jour spécifiques du système, puis réinitialisez le système pour le faire repasser en mode lecture seule.**

```
# reboot
```

▼ Configuration de zones non globales immuables

Pour configurer une zone non globale Oracle Solaris pour qu'elle soit immuable, procédez comme suit.

Remarque - Le système d'exploitation Oracle Solaris 11 prend en charge des configurations de zones immuables supplémentaires en plus de celle identifiée dans cette tâche (configuration corrigée). Pour plus d'informations sur ces options, reportez-vous à la page de manuel `zonecfg(1M)`. Toutefois, seule l'option de configuration corrigée a été testée dans le cadre de l'architecture SuperCluster.

Attention - L'ajout, la modification ou la suppression de comptes et de mots de passe d'utilisateurs de la zone ne peut pas s'effectuer une fois que l'immuabilité de la zone non globale Oracle Solaris est activée, comme décrit dans cette tâche. Toutefois, ce problème peut être résolu en déployant un répertoire LDAP afin qu'il contienne des informations spécifiques à la zone, telles que les utilisateurs, les rôles, les groupes, les profils de droits, etc.

Attention - La fonctionnalité de zone immuable Oracle Solaris est limitée aux jeux de données ZFS qui sont implémentés par défaut dans une zone non globale Oracle Solaris. Les systèmes de fichiers, pools ou jeux de données supplémentaires ne sont pas soumis à la politique de la zone immuable, bien que l'accès à ces éléments de fichier puisse être contrôlé à l'aide d'autres moyens que l'utilisation de montages loopback en lecture seule.

1. **Connectez-vous à l'un des serveurs de calcul et accédez à la console hôte en tant que superutilisateur.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Vérifiez que la zone non globale Oracle Solaris est arrêtée.**

   Si cette commande renvoie une valeur, cela signifie que la zone non globale Oracle Solaris est en cours d'exécution et que vous devez l'arrêter.

   Remarque - Alors que la zone peut être arrêtée à l'aide de la commande `zoneadm(1M)`, suivez les procédures d'arrêt adéquates définies par votre entreprise pour éviter tout risque d'interruption de service et de perte de données.

   ```
   # zoneadm list | grep -w "zone_name"
   ```

3. **Réglez la configuration de la zone non globale Oracle Solaris en définissant la propriété de configuration de zone `file-mac-profile`.**

   ```
   # zonecfg -z zone_name set file-mac-profile=fixed-configuration
   ```

4. **Si nécessaire, désactivez la configuration immuable de zone non globale.**

   ```
   # zonecfg -z zone_name set file-mac-profile=none
   ```

5. **Redémarrez la zone non globale Oracle Solaris pour que les modifications prennent effet.**

   ```
   # zoneadm -z zone_name boot
   ```

Activation de la fonction sécurisée Verified Boot (CLI d'Oracle ILOM)

Utilisez cette tâche pour activer la fonction sécurisée Verified Boot via la CLI d'Oracle ILOM. Vous pouvez également utiliser l'interface Web d'Oracle ILOM. Reportez-vous à la section "Fonction sécurisée Verified Boot (interface Web d'Oracle ILOM)" à la page 81.

Verified Boot fait référence à la vérification de modules d'objets avant l'exécution à l'aide de signatures numériques. Oracle Solaris protège contre le chargement de modules de noyau non fiables. Verified Boot accroît la sécurité et la fiabilité d'Oracle Solaris en vérifiant les modules de noyau avant l'exécution.

Si elle est activée, la fonction Verified Boot d'Oracle Solaris vérifie la signature émise en usine figurant dans un module de noyau avant le chargement et l'exécution du module. Cette vérification détecte la modification accidentelle ou malveillante d'un module. L'action effectuée est configurable et, lorsqu'elle est activée, imprime un message d'avertissement et continue le chargement et l'exécution du module, ou échoue sans charger ni exécuter le module.

1. **Accédez à Oracle ILOM sur le serveur de calcul.**

   Voir "Connexion à un serveur de calcul et modification du mot de passe par défaut" à la page 55.

2. **Activez Verified Boot.**

```
-> set /HOST/verified_boot/ module_policy=enforce
Set 'module_policy' to 'enforce'
```

3. **Accédez au certificat Oracle fourni et affichez-le.**

   Un fichier de certificat Verified Boot préinstallé, `/etc/certs/ORCLS11SE`, est fourni avec Oracle ILOM.

```
# more /etc/certs/ORCLS11SE
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----
```

4. **Lancez le chargement du certificat.**

```
-> set /HOST/verified_boot/user_certs/1 load_uri=console
```

5. **Copiez le contenu du fichier `/etc/certs/ORCLS11SE` et collez-le dans la console Oracle ILOM.**

Entrez Ctrl-z pour enregistrer et traiter les informations.

Entrez Ctrl-c pour quitter et annuler les modifications.

```
-----BEGIN CERTIFICATE-----
MIIFEzCCA/ugAwIBAgIQDfuxWi0q5YGAhus0XqR+7TANBgkqhkiG9w0BAQUFADCB
….
CXZousDBt9DdhjX6d0ZPLkdzBxqm8Bxg9H3iKtZBPuhZBl9iXvLEOzY8sS0AW7UF
UHGOvZ9U6m4Tq5+KDiJ8QXZG2ipTeat5XdzLmzA9w2jrrfx0N+NcgvIVjdPXD8C4
wgaJllToqg==
-----END CERTIFICATE-----^Z
Load successful.
```

6. Vérifiez le certificat.

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. Vérifiez que le paramètre OBP `use-nvram` est défini sur `false`.

Lorsque vous utilisez Verified Boot, le paramètre OBP `use-nvram` doit être défini sur `false`. Cela empêche la modification d'OBP en vue de la désactivation de la fonctionnalité Verified Boot. La valeur par défaut est false. Connectez-vous à Oracle Solaris et saisissez :

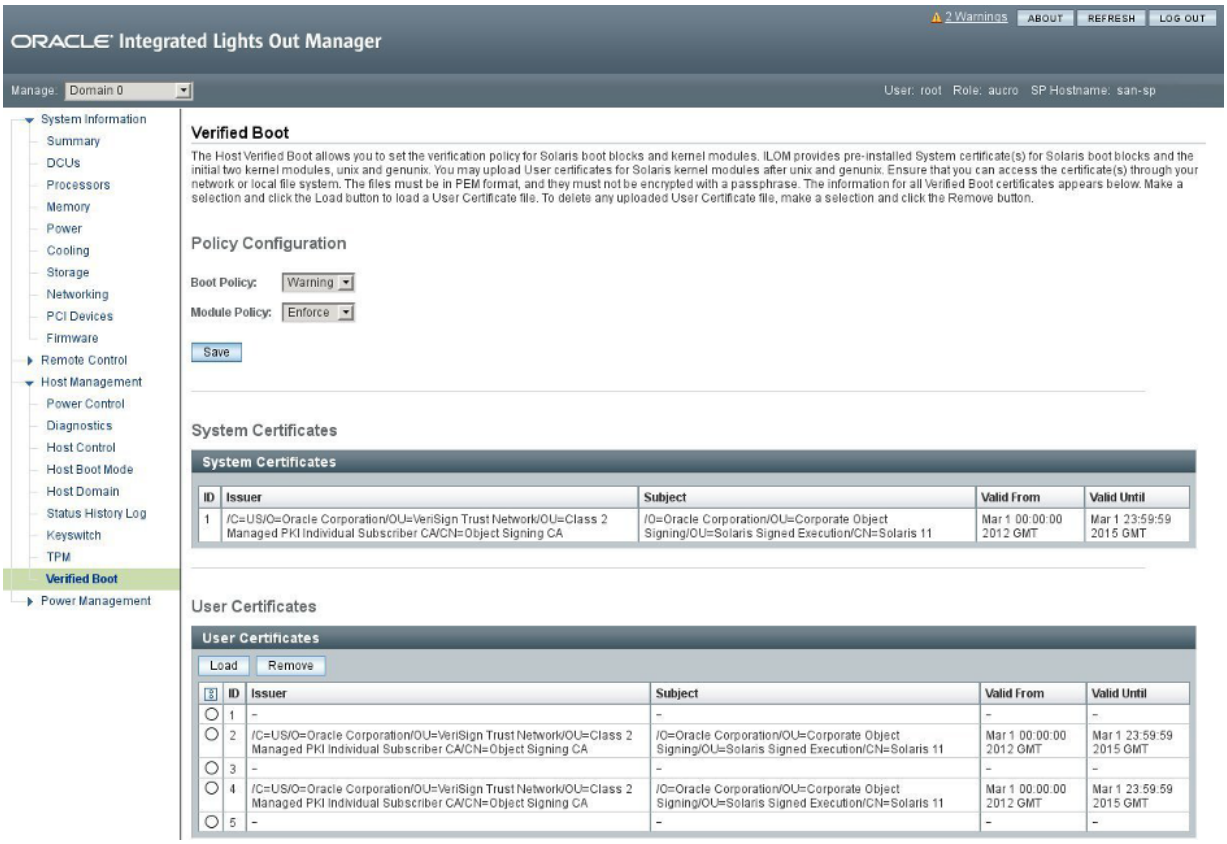
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

Fonction sécurisée Verified Boot (interface Web d'Oracle ILOM)

L'interface Web d'Oracle ILOM prend également en charge la définition des variables de stratégie Verified Boot et la gestion des fichiers de certificat, offrant ainsi la même

fonctionnalité que la CLI. Accédez au lien Verified Boot sous le menu de navigation Host Management.

Par exemple :



Ressources supplémentaires du serveur de calcul

Pour les guides de sécurité du système d'exploitation Oracle Solaris et d'Oracle Solaris Cluster, reportez-vous à la bibliothèque de la documentation correspondant à votre version du système d'exploitation. Les bibliothèques sont disponibles à l'adresse `http:/docs.oracle.com/en/operating-systems`.

Pour des informations sur la sécurité d'Oracle VM Server for SPARC, reportez-vous au guide de sécurité à l'adresse http://docs.oracle.com/cd/E62357_01.

Pour des informations sur la sécurité du matériel du serveur de calcul, reportez-vous au guide de sécurité à l'adresse http://docs.oracle.com/cd/E55211_01.

Sécurisation de l'appareil de stockage ZFS

L'appareil de stockage ZFS est l'un des composants du SuperCluster permettant la consolidation du stockage pour divers environnements de travail exigeants tels que l'informatique décisionnelle, l'entreposage de données, la virtualisation, le développement, le test et la protection des données.

L'appareil de stockage ZFS comprend deux contrôleurs de stockage ZFS redondants. Vous devez sécuriser ces deux contrôleurs.

Les sections suivantes décrivent les consignes et les fonctions de sécurité de l'appareil de stockage ZFS :

▼ Connexion à l'appareil de stockage ZFS

Pour effectuer les tâches de sécurité figurant dans cette section, vous devez vous connecter à l'appareil de stockage ZFS via le réseau de gestion.

Cette tâche décrit la procédure de connexion à l'aide de la CLI. Pour obtenir les instructions similaires permettant de se connecter à l'interface Web d'Oracle ILOM, reportez-vous au *Guide d'administration des systèmes Oracle® ZFS Storage Appliance* Voir "Ressources supplémentaires relatives à l'appareil de stockage ZFS" à la page 95.

1. **Sur votre réseau de gestion, utilisez SSH pour vous connecter à l'appareil de stockage ZFS.**

Si aucun autre utilisateur n'a été configuré pour administrer l'appareil, vous devez vous connecter en tant qu'utilisateur `root`.

```
% ssh root@ZFS_Storage_App_IPaddress_or_hostname
Password:
Last login: Mon Oct 13 15:43:05 2015
hostname:>
```

2. **Le cas échéant, consultez l'aide de la CLI.**

   La commande `help` permet d'afficher l'aide contextuelle. Il est possible d'afficher l'aide portant sur un thème particulier en saisissant le thème concerné en tant qu'argument de la commande `help`. Pour afficher les thèmes disponibles, saisissez la commande help et appuyez sur la touche de tabulation ou saisissez `help topics`.

▼ Détermination de la version du logiciel de l'appareil de stockage ZFS

Effectuez cette procédure pour identifier la version du logiciel de l'appareil de stockage ZFS.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Affichez la version du logiciel.**

```
hostname:> configuration version show
[...]
Appliance Product: Sun ZFS Storage 7320
Appliance Type: Sun ZFS Storage 7320
Appliance Version: 2013.06.05.2.10,1-2.1.1.1
[...]
```

Dans cet exemple, la version du logiciel de l'appareil de stockage ZFS est `2013.06.05.2.10`.

Pour mettre à jour la version du logiciel d l'appareil de stockage ZFS, installez le patch QFSDP du SuperCluster le plus récent disponible à partir de My Oracle Support à l'adresse `https://support.oracle.com`.

Remarque - Pour le système SuperCluster, des restrictions supplémentaires pourraient limiter les versions du logiciel de l'appareil de stockage ZFS utilisables et le mode de mise à jour de ces versions. Dans un tel cas, contactez votre représentant Oracle.

Modification du mot de passe root de l'appareil de stockage ZFS

L'appareil de stockage ZFS n'est lui-même pas préconfiguré avec un mot de passe root par défaut. La configuration initiale de l'appareil de stockage ZFS s'effectue au cours d'une session de console à partir de son instance Oracle ILOM intégrée. La définition du mot de passe root de l'appareil s'effectue au cours de cette session de configuration initiale.

La première fois que vous accédez à la console de l'appareil, un écran de configuration de l'interface du shell s'affiche. Vérifiez les informations à l'écran et saisissez les valeurs requises. La définition du mot de passe root permettant d'accéder à l'appareil de stockage ZFS s'effectue pendant ce processus.

Remarque - L'instance Oracle ILOM de l'appareil ne possède pas de compte root par défaut associé au mot de passe welcome1. Voir "Sécurisation d'Oracle ILOM" à la page 37.

Une fois que vous disposez d'un compte root, vous pouvez modifier son mot de passe à tout moment, tel qu'indiqué dans cette tâche.

Remarque - Lors de la modification du mot de passe d'un composant SuperCluster géré par Oracle Engineered Systems Hardware Manager (tel que le système d'exploitation du contrôleur de stockage AFS), vous devez également mettre à jour le mot de passe d'Oracle Engineered Systems Hardware Manager. Pour plus d'informations, reportez-vous au *Guide d'administration des serveurs Oracle SuperCluster série M7*.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Modifiez le mot de passe root.**

   Dans cet exemple, remplacez *password* par un mot de passe conforme aux stratégies de complexité des mots de passe du Ministère de la Défense des Etats-Unis.

```
hostname:> configuration users select root set initial_password=password initial_password = ************
hostname:configuration users> done
```

Pour plus d'informations sur l'installation et la configuration initiales de l'appareil de stockage ZFS, reportez-vous au *Guide d'installation des systèmes Oracle ZFS Storage Appliance*. Voir "Ressources supplémentaires relatives à l'appareil de stockage ZFS" à la page 95.

Services réseau exposés par défaut (appareil de stockage ZFS)

Ce tableau répertorie les services réseau par défaut exposés par l'appareil de stockage ZFS.

Service	Protocole	Port	Description
SSH	TCP	22	Utilisé par le service de shell sécurisé (SSH) pour fournir l'accès administratif à l'appareil de stockage ZFS à l'aide d'une CLI.
PORTMAP	TCP/UDP	111	Utilisé par le démon de mappage des ports RPC (Remote Procedure Call) (appelé `rpcbind` ou `portmap`). Ce service est requis pour la prise en charge de la version 3 du protocole NFS.
NTP	UDP	123	Utilisé par le service NTP (Network Time Protocol) intégré (client uniquement) qui permet de synchroniser l'horloge système locale à une ou plusieurs sources temporelles externes.
HTTPS (BUI)	TCP	215	Utilisé par le service HTTPS intégré pour fournir l'accès administratif à l'appareil de stockage ZFS via un canal (SSL/TLS) chiffré à l'aide d'une interface de navigateur.
Réplication distante	TCP	216	Utilisé par le service de réplication distante des données intégré. La réplication distante des données duplique et synchronise des projets et des partages entre des appareils de stockage ZFS via un canal (SSL/TLS) chiffré.
NFS	TCP/UDP	2049 4045 divers	Utilisé par le service NFS (Network File System). NFS assure le service de partage de fichiers réseau. Le nombre réel de ports dépend de la version du protocole NFS utilisée. NFS version 3 fait appel au démon de mappage des ports RPC (mentionné précédemment) et aux ports alloués de manière dynamique pour fournir les fonctions de montage, de gestion de statut et de quota, ainsi que des services connexes. Toutefois, NFS version 4 s'appuie uniquement sur le port TCP/2049. Le service de verrouillage NFS utilise le port TCP/4045.
iSCSI / iSNS	TCP	3260	Utilisé par le service iSCSI qui fournit un protocole de gestion de réseau de stockage basé sur IP pour la connexion des dispositifs de stockage de données. L'appareil de stockage ZFS peut être configuré pour partager des périphériques iSCSI (appelés LUN) avec des clients en réseau.
Service Tags	TCP	6481	Utilisé par le service Oracle ServiceTag. Il s'agit d'un protocole de découverte Oracle permettant d'identifier les serveurs et de faciliter les demandes d'assistance. Ce service est utilisé par certains produits tels qu'Oracle Enterprise Manager Ops Center pour la découverte du logiciel du logiciel de l'appareil de stockage ZFS et l'intégration avec les autres solutions de services automatiques Oracle.
NDMP	TCP	10000	Utilisé par le service NDMP (Network Data Management Protocol) qui permet à l'appareil de stockage ZFS de prendre part à des sauvegardes coordonnées à distance.

L'appareil de stockage ZFS prend également en charge divers autres services désactivés par défaut, notamment `HTTP`, `FTP`, `SFTP`, `TFTP`, `WebDAV`, etc. Des ports réseau supplémentaires peuvent être exposés si ces services sont activés après l'installation.

Renforcement de la configuration de sécurité de l'appareil de stockage ZFS

Les rubriques suivantes décrivent la procédure de renforcement de la configuration de la sécurité de l'appareil de stockage ZFS :

▼ Implémentation du renforcement de la configuration de sécurité d'Oracle ILOM

L'appareil de stockage ZFS inclut une instance Oracle ILOM intégrée dans le produit. Comme pour les autres implémentations d'Oracle ILOM, vous pouvez implémenter des modifications de configuration liées à la sécurité pour améliorer la configuration de sécurité par défaut du périphérique.

- **Sécurisez l'interface Oracle ILOM de l'appareil de stockage ZFS en effectuant les procédures figurant à la section "Sécurisation d'Oracle ILOM" à la page 37.**

▼ Désactivation des services inutiles (appareil de stockage ZFS)

Désactivez tous les services qui ne sont pas nécessaires au respect des exigences de la plate-forme en matière de fonctionnement et de gestion.

Par défaut, l'appareil de stockage ZFS emploie une configuration réseau *sécurisée par défaut* où les services non essentiels sont désactivés. Toutefois, en fonction de vos stratégies et impératifs de sécurité, il peut être nécessaire d'activer ou de désactiver des services supplémentaires.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Affichez la liste des services pris en charge par l'appareil de stockage ZFS.**

```
hostname:> configuration services
```

3. **Déterminez si un service donné est activé.**

   Remplacez *servicename* par le nom du service identifié à l'Étape 2.

```
hostname:> configuration services servicename get <status>
```

   Un service est activé si son paramètre d'état renvoie la valeur `enabled`. Par exemple :

```
hostname:> configuration services iscsi get <status>
<status> = online
```

4. **Désactivez un service devenu inutile.**

   Définissez l'état du service sur disable. Par exemple :

```
hostname:> configuration services iscsi disable
```

▼ Désactivation du routage dynamique

L'appareil de stockage ZFS est configuré pour exécuter le protocole de routage dynamique par défaut.

Avant de désactiver le service de routage dynamique, assurez-vous que l'appareil de stockage ZFS est directement connecté au réseau avec lequel il doit communiquer ou qu'il a été configuré pour utiliser le routage statique ou un itinéraire par défaut. Cette étape est nécessaire pour éviter toute perte de connectivité après la désactivation du routage dynamique.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Désactivez le routage dynamique.**

```
hostname:> configuration services dynrouting disable
```

3. **Pour déterminer si le routage dynamique est activé, entrez :**

```
hostname:> configuration services dynrouting get <status>
```

Restriction de l'accès root distant à l'aide du shell sécurisé

Par défaut, l'appareil de stockage ZFS est configuré pour autoriser l'accès administratif distant au compte root à l'aide du service de shell sécurisé (SSH).

Utilisez cette procédure pour désactiver l'accès root distant avec SSH.

Une fois la configuration ainsi modifiée, le compte root ne peut plus accéder au système à l'aide du service SSH. Le compte root est néanmoins en mesure d'accéder à ce système à partir de l'interface d'administration HTTPS.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Désactivez l'accès root à distance.**

```
hostname:> configuration services ssh set permit_root_login=false
```

3. **Vérifiez que le compte root n'est plus autorisé à accéder au système à l'aide du service SSH.**

```
hostname:> configuration services ssh get permit_root_login
```

4. **Si l'accès administratif SSH est requis, créez au moins un compte non-root.**

   Pour obtenir des instructions, reportez-vous au manuel *Guide d'administration des systèmes Oracle® ZFS Storage Appliance* correspondant à la version exécutée sur l'appareil de stockage ZFS. Voir "Ressources supplémentaires relatives à l'appareil de stockage ZFS" à la page 95.

Configuration du délai d'expiration en cas d'inactivité de l'interface d'administration (HTTPS)

L'appareil de stockage ZFS prend en charge la possibilité de déconnecter et de fermer les sessions d'administration restées inactives au-delà d'un nombre de minutes prédéfini. Par défaut, l'interface utilisateur du navigateur (HTTPS) met fin à une session au bout de 15 minutes.

Remarque - Aucun paramètre équivalent n'applique de délai d'expiration en cas d'inactivité de l'interface de ligne de commande SSH de l'appareil de stockage ZFS.

Effectuez cette procédure pour attribuer une valeur personnalisée au paramètre régissant le délai d'expiration en cas d'inactivité.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Affichez le paramètre de délai d'expiration en cas d'inactivité actuel associé à l'interface de navigateur.**

```
hostname:> configuration preferences get session_timeout
session_timeout = 15
```

3. **Configurez le paramètre de délai d'expiration.**

   La valeur `session_timeout` est exprimée en minutes (10 minutes dans cet exemple).

```
hostname:> configuration preferences set session_timeout=10
session_timeout = 10
```

4. **Vérifiez le paramètre de délai d'expiration en répétant l'Étape 2.**

Désactivation des protocoles SNMP non autorisés

Par défaut, les protocoles SNMPv1 et SNMPv2c sont activés sur l'appareil de stockage ZFS. L'appareil de stockage ZFS est compatible avec les protocoles SNMPv1/v2c sur toutes les versions du produit prises en charge. A partir de la version 2013.1.2, l'appareil de stockage ZFS prend également en charge SNMPv3.

Remarque - La version 3 du protocole SNMP intègre la prise en charge du modèle USM (User-based Security Model). Cette fonctionnalité remplace les chaînes de communauté SNMP standard par des comptes d'utilisateur qui peuvent être configurés avec des protocoles et des mots de passe d'autorisation, d'authentification et de confidentialité spécifiques. Par défaut, l'appareil de stockage ZFS n'inclut pas de nom d'utilisateur ou de mot de passe pour le compte USM (en lecture seule) intégré. Pour des raisons de sécurité, configurez les informations d'identification et les protocoles USM en fonction des exigences en matière de déploiement, de gestion et de surveillance.

Assurez-vous que les versions inutilisées ou antérieures du protocole SNMP sont désactivées sauf si elles sont requises.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Identifiez la version du protocole SNMP utilisée par le périphérique.**

```
hostname:> configuration services snmp get version
version = v2
```

3. **Activez l'utilisation du protocole SNMPv3 (s'il est disponible).**

   Les protocoles SNMPv1/v2c et SNMPv3 s'excluent mutuellement, de sorte que si vous activez SNMPv3, les protocoles SNMPv1/v2c sont désactivés.

```
hostname:> configuration services snmp set version=v3
version = v3
```

4. **Vérifiez la version du protocole SNMP.**

```
hostname:> configuration services snmp get version
version = v3
```

▼ Configuration de chaînes de communauté SNMP

Effectuez cette tâche seulement si l'appareil de stockage ZFS est configuré pour utiliser les protocoles SNMPv1 ou v2.

Comme le protocole SNMP est souvent utilisé pour surveiller l'intégrité du périphérique, il est important de remplacer la chaîne de communauté SNMP par défaut utilisée par le périphérique par une valeur définie par le client.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Modifiez la chaîne de communauté SNMP.**

   Dans cet exemple, remplacez *string* par une valeur conforme aux exigences du Ministère de la Défense des Etats-Unis relatives à la composition des chaînes de communauté SNMP.

```
hostname:> configuration services snmp set community=string
community = value
```

3. **Vérifiez la chaîne de communauté SNMP.**

```
hostname:> configuration services snmp get community
```

Configuration de réseaux autorisés SNMP

Effectuez cette tâche seulement si l'appareil de stockage ZFS est configuré pour utiliser les protocoles SNMPv1 ou v2.

Pour minimiser la divulgation d'informations relatives à la configuration du système, les demandes SNMP doivent uniquement être acceptées à partir de sources réseau ou hôte approuvées.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Définissez le paramètre de configuration des réseaux autorisés SNMP.**

```
hostname:> configuration services snmp set network=127.0.0.1/8
network = 127.0.0.1/8
```

3. **Vérifiez la valeur du paramètre de configuration des réseaux autorisés SNMP.**

   Dans cet exemple, l'attribution de la valeur `127.0.0.1/8` au paramètre network entraîne le blocage de toutes les requêtes SNMP. Il convient d'ajuster cette valeur, le cas échéant, pour autoriser les hôtes et les réseaux approuvés.

   La valeur `0.0.0.0/0` autorise les requêtes provenant d'un emplacement réseau.

```
hostname:> configuration services snmp get network
network = 127.0.0.1/8
```

Restriction de l'accès au réseau de gestion

En plus de ces procédures de renforcement de la sécurité, les interfaces de gestion exposées par l'appareil de stockage ZFS doivent être déployées sur un réseau de gestion dédié et isolé. Cette étape permet de protéger l'appareil de stockage ZFS de tout trafic réseau d'administration non autorisé ou inopportun. Vous devez contrôler rigoureusement la connexion au réseau de gestion en accordant des autorisations aux seuls administrateurs qui ont besoin d'un tel niveau d'accès.

Par ailleurs, il est possible de configurer l'appareil de stockage ZFS pour activer ou désactiver l'accès aux fonctions d'administration (de gestion) sur des interfaces réseau spécifiques. Cette modification peut être implémentée à l'aide de la procédure suivante.

1. **Connectez-vous à l'appareil de stockage ZFS.**

   Voir "Connexion à l'appareil de stockage ZFS" à la page 85.

2. **Configurez les interfaces réseau de gestion.**

   Dans cet exemple, remplacez la valeur *interface* par le nom de l'interface réseau pour laquelle ce paramètre est appliqué.

```
hostname:> configuration net interfaces select interface set admin=false
```

Ressources supplémentaires relatives à l'appareil de stockage ZFS

Pour des consignes de sécurité supplémentaires relatives à l'appareil de stockage ZFS, reportez-vous au guide de sécurité correspondant à la version exécutée sur l'appareil. Voir "Détermination de la version du logiciel de l'appareil de stockage ZFS" à la page 86.

Les guides suivants fournissent des informations supplémentaires sur les fonctionnalités, les capacités et les options de configuration relatives à la sécurité :

- *Guide de sécurité des systèmes Oracle ZFS Storage Appliance, version 2013.1.4.0*

  http://docs.oracle.com//cd/E56047_01
- *Guide de sécurité des systèmes Oracle ZFS Storage Appliance, version 2013.1.3.0*

  http://docs.oracle.com/cd/E56021_01
- *Guide de sécurité des systèmes Oracle ZFS Storage Appliance, version 2013.1.2.0*

  http://docs.oracle.com/cd/E51475_01

Sécurisation des serveurs Exadata Storage Server

Les serveurs Exadata Storage Server (serveurs de stockage) sont les éléments constitutifs du stockage du système SuperCluster. Chaque serveur de stockage est fourni préinstallé et intégré dans le système SuperCluster M7 avec tous les composants de calcul, de stockage et logiciels nécessaires.

Remarque - Vous êtes seulement autorisé à modifier la configuration par l'application de méthodes, de patchs et de mises à jour approuvés. Le logiciel des serveurs de stockage ne peut être modifié d'aucune autre manière.

Le système SuperCluster M7 dispose d'au moins trois serveurs de stockage. Des serveurs de stockage supplémentaires peuvent être installés dans le rack SuperCluster principal et dans les racks d'extension facultatifs. Vous devez sécuriser individuellement chaque serveur de stockage.

Les rubriques suivantes décrivent la procédure de sécurisation des serveurs de stockage :

▼ Connexion au système d'exploitation des serveurs de stockage

- **Sur le réseau de gestion, connectez-vous à l'un des serveurs de stockage en tant qu'utilisateur `celladmin`.**

Pour obtenir le mot de passe par défaut, reportez-vous à la section "Comptes et mots de passe par défaut" à la page 98.

```
# ssh celladmin@Storage_Server_IP_address
```

Comptes et mots de passe par défaut

Ce tableau répertorie les comptes et les mots de passe par défaut des serveurs de stockage.

Nom de compte	Type	Mot de passe par défaut	Description
`root`	Administrateur	`welcome1`	Permet d'accéder au système d'exploitation des serveurs de stockage pour exécuter des actions administratives générales et mettre à jour le logiciel des serveurs de stockage.
`celladmin`	Administrateur de cellule	`welcome`	Permet d'effectuer l'installation et la configuration des serveurs de stockage. Par ailleurs, tous les services de stockage de la plate-forme fonctionnent à l'aide de ce compte.
`cellmonitor`	Moniteur	`welcome`	Est utilisé à des fins de surveillance uniquement. Ce compte exploite un shell restreint pour garantir que la configuration et les objets résidant sur le serveur de stockage ne puissent pas être modifiés à partir de lui.

▼ Modification des mots de passe des serveurs de stockage

Pour obtenir une liste des comptes et des mots de passe par défaut, reportez-vous à la section "Comptes et mots de passe par défaut" à la page 98.

Remarque - Lors de la modification du mot de passe d'un composant SuperCluster géré par Oracle Engineered Systems Hardware Manager (tel que le système d'exploitation des serveurs Exadata Storage Server), vous devez également mettre à jour le mot de passe d'Oracle Engineered Systems Hardware Manager. Pour plus d'informations, reportez-vous au *Guide d'administration des serveurs Oracle SuperCluster série M7*.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**

   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Modifiez un mot de passe par défaut à l'aide de l'une des méthodes suivantes.**

- **Modifiez le mot de passe d'un compte sur le serveur auquel vous êtes connecté.**

  ```
  # passwd account_name
  ```

- **Modifiez le mot de passe d'un compte sur tous les serveurs de stockage.**

  L'élément `cell_group` est un fichier texte simple répertoriant les noms d'hôte de tous les serveurs de stockage (un par ligne).

  Dans cet exemple, remplacez les éléments de ligne de commande suivants :

  - *new_password* – Remplacez par le nouveau mot de passe compatible avec les stratégies du site.
  - *account_name* – Remplacez par le nom du compte Oracle Linux.

  ```
  # dcli -g cell_group -l root "echo new_password | passwd --stdin account_name"
  ```

Détermination de la version du logiciel Exadata Storage Server

1. **Connectez-vous à l'un des serveurs de stockage.**

   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Saisissez cette commande.**

   Dans cet exemple, la version du logiciel du serveur de stockage est 12.1.2.1.1.150316.2.

   ```
   # imageinfo -ver
   12.1.2.1.1.150316.2
   ```

   Pour mettre à jour la version du logiciel, installez le patch QFSDP du système SuperCluster le plus récent disponible à partir de My Oracle Support à l'adresse `https://support.oracle.com`.

   Remarque - Pour le système SuperCluster, des restrictions supplémentaires pourraient limiter les versions du logiciel utilisables et la manière de les mettre à jour. Dans un tel cas, contactez votre représentant Oracle.

Services réseau exposés par défaut (serveurs de stockage)

Nom du service	Protocole	Port	Description
SSH	TCP	22	Utilisé par le service de shell sécurisé (SSH) intégré au logiciel du serveur de stockage pour fournir l'accès administratif au système à l'aide d'une CLI. Par défaut, le serveur de shell sécurisé (SSH) est configuré pour répondre aux demandes de connexion seulement sur les réseaux de gestion (NET 0) et IB (BONDIB0).

Le serveur de stockage communique également avec des domaines de base de données Oracle sur le système SuperCluster à l'aide du protocole RDSv3 (Reliable Datagram Sockets version 3) via des interfaces RDMA (Remote Direct Memory Access). Cette communication point à point, qui n'utilise pas le protocole TCP/IP, est limitée à la partition réseau IB interne sur laquelle résident les domaines de base de données Oracle du SuperCluster et les serveurs de stockage.

Renforcement de la configuration de sécurité des serveurs de stockage

Remarque - Le serveur de stockage inclut une instance Oracle ILOM intégrée dans le produit. Comme pour les autres implémentations d'Oracle ILOM, il est possible d'implémenter des modifications de configuration liées à la sécurité pour améliorer la configuration de sécurité par défaut du périphérique. Pour plus d'informations, reportez-vous à la section "Sécurisation d'Oracle ILOM" à la page 37.

Les rubriques suivantes décrivent la procédure de renforcement de la sécurité des serveurs de stockage :

Restrictions de configuration de sécurité

L'utilitaire `host_access_control` est la seule méthode autorisée et prise en charge pour implémenter des modifications de configuration de la sécurité sur des serveurs de stockage. Vous n'êtes pas autorisé à apporter des modifications manuelles à la configuration de ces systèmes selon la notice 1068804.1 du support Oracle. De plus, avant d'utiliser cet outil, vous devez d'abord obtenir l'approbation explicite du support Oracle SuperCluster pour modifier la configuration de sécurité des serveurs de stockage. Pour requérir cette approbation, ouvrez une demande de service auprès du support technique Oracle.

La commande `host_access_control`, disponible à partir de la version 11.2.3.3.0 du logiciel Exadata, permet d'implémenter un ensemble limité de paramètres de configuration d'accès et de sécurité :

- Restriction de l'accès root distant
- Restriction de l'accès au réseau à certains comptes
- Implémentation de stratégies relatives au vieillissement et à la complexité des mots de passe
- Implémentation de bannières d'avertissement de connexion
- Définition de stratégies de verrouillage de compte et d'expiration de session

▼ Affichage des configurations de sécurité disponibles avec `host_access_control`

Pour connaître les éléments disponibles dans l'utilitaire `host_access_control`, procédez comme suit.

1. **Connectez-vous au système d'exploitation du serveur de stockage.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **(Facultatif) Affichez l'aide de l'utilitaire `host_access_control` pour plus d'informations.**

```
# /opt/oracle.cellos/host_access_control --help
```

Configuration d'un mot de passe pour le programme d'initialisation du système

Vous pouvez configurer les serveurs de stockage pour qu'ils requièrent un mot de passe pour le programme d'initialisation du système lorsqu'un administrateur tente d'accéder au programme d'initialisation GRUB ou à l'interface de commande.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Configurez un mot de passe pour le programme d'initialisation du système.**

```
# /opt/oracle.cellos/host_access_control grub-password
New GRUB password: password
Retype new GRUB password: password
[...]
```

3. **Vérifiez le paramètre.**
   Si la commande renvoie une valeur similaire à cet exemple, l'installation d'un mot de passe pour le programme d'initialisation est terminée.

```
# grep "^password" /etc/grub.conf
password --md5 $1$Hdner/$Q2VoiZeTJwmNQsFnH9oFy.
```

Désactivation de l'accès à la console système Oracle ILOM

Chaque serveur de stockage inclut une instance Oracle ILOM intégrée pour activer la gestion et la surveillance à distance. Oracle ILOM permet également de fournir un accès à distance à la console système des serveurs de stockage.

Effectuez cette procédure si vous voulez désactiver l'accès au serveur de stockage via Oracle ILOM.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Désactivez l'accès à la console système Oracle ILOM.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --lock
```

3. **Vérifiez le paramètre.**

```
# /opt/oracle.cellos/host_access_control access-ilomweb --status
```

Restriction de l'accès `root` à distance avec SSH

Par défaut, l'utilisateur `root` est autorisé à accéder à distance à chacun des serveurs de stockage.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Désactivez l'accès `root` à distance via SSH.**

```
# /opt/oracle.cellos/host_access_control rootssh --lock
```

3. **Vérifiez le paramètre.**

```
# /opt/oracle.cellos/host_access_control rootssh --status
```

Configuration du verrouillage de compte système

Par défaut, les serveurs de stockage sont configurés pour verrouiller les comptes système après l'échec de cinq tentatives d'authentification successives.

Pour modifier ce seuil, procédez comme suit.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Modifiez le seuil.**
   Pour respecter les exigences en matière de sécurité du Ministère de la Défense des Etats-Unis, spécifiez la valeur `3`. Si nécessaire, remplacez-la par une valeur compatible avec la stratégie de votre site local.

```
# /opt/oracle.cellos/host_access_control pam-auth --deny 3
```

3. **Vérifiez le paramètre.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep deny=
```

Configuration de règles de complexité de mot de passe

Par défaut, les serveurs de stockage n'implémentent aucune restriction significative régissant la complexité des mots de passe de compte système.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Définissez une stratégie de complexité des mots de passe.**
   Syntaxe :

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc N0,N1,N2,N3,N4
```

Remplacez *N0,N1,N2,N3,N4* par un ensemble de cinq valeurs séparées par des virgules. Ces cinq valeurs définissent collectivement la stratégie de complexité des mots de passe système. Il s'agit des valeurs suivantes (qui figurent également dans la page de manuel `passwdqc.conf(5)`) :

- *N0* – Utilisé pour les mots de passe comportant une seule classe de caractères (chiffres, minuscules, majuscules et caractères spéciaux). En général, ce paramètre est défini sur `disabled`, car les mots de passe simples ne sont pas sécurisés.
- *N1* – Utilisé pour les mots de passe comportant deux classes de caractères qui ne répondent pas aux conditions requises pour former une phrase de passe. Pour que cette règle s'applique, le mot de passe doit comporter au moins N1 caractères.
- *N2* – Utilisé pour les mots de passe formant une phrase de passe. Pour que cette règle s'applique, le mot de passe doit comporter au moins N2 caractères et répondre à l'exigence relative aux phrases de passe.
- *N3* – Utilisé pour les mots de passe comportant au moins trois classes de caractères. Pour que cette règle s'applique, le mot de passe doit comporter au moins N3 caractères.

- *N4* – Utilisé pour les mots de passe comportant au moins quatre classes de caractères. Pour que cette règle s'applique, le mot de passe doit comporter au moins *N4* caractères.

Pour respecter les exigences en matière de sécurité du Ministère de la Défense des Etats-Unis, définissez les paramètres *N0,N1,N2,N3,N4* sur `disabled,disabled,disabled,disabled,15`. Cela garantit que seuls les mots de passe qui comportent au moins quatre classes de caractères (caractères majuscules, minuscules, numériques et spéciaux) et 15 caractères sont acceptés.

Remarque - Les lettres majuscules au début du mot de passe et les chiffres à la fin ne sont pas pris en compte lors du calcul du nombre de classes de caractères.

Par exemple, pour définir une complexité des mots de passe conforme aux exigences du Ministère de la Défense des Etats-Unis, entrez :

```
# /opt/oracle.cellos/host_access_control pam-auth --passwdqc disabled,disabled,disabled,disabled,15
```

3. **Vérifiez l'état actuel de ce paramètre.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep min=
```

Configuration d'une stratégie relative à l'historique des mots de passe

Par défaut, les serveurs de stockage définissent une stratégie relative à l'historique des mots de passe qui empêche les utilisateurs de réutiliser leurs dix (10) derniers mots de passe.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**

   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Affichez le paramètre actuel.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep remember=
```

3. **Modifiez l'historique des mots de passe.**

   Pour respecter les exigences du Ministère de la Défense des Etats-Unis en matière de sécurité et de normes PCI-DSS, définissez la stratégie relative à l'historique des mots de passe sur `5`. Ce paramètre interdit à un compte de réutiliser l'un des cinq derniers mots de passe qui lui ont été attribués. Si nécessaire, remplacez-le par une valeur compatible avec les stratégies de votre site local.

```
# /opt/oracle.cellos/host_access_control pam-auth --remember 5
```

4. **Pour vérifier le paramètre, répétez l'Étape 2.**

Configuration du délai de verrouillage après un échec d'authentification

Par défaut, les serveurs de stockage implémentent une stratégie provoquant le verrouillage d'un compte système pendant 10 minutes après l'échec d'une seule tentative d'authentification.

Pour modifier ce seuil, procédez comme suit.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**

   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Affichez le paramètre actuel.**

```
# /opt/oracle.cellos/host_access_control pam-auth --status | grep lock_time=
```

3. **Modifiez le seuil.**

   Pour respecter les exigences en matière de sécurité du Ministère de la Défense des Etats-Unis, définissez la valeur sur 4 (secondes). Si nécessaire, remplacez-la par une valeur compatible avec les stratégies de votre site local.

```
# /opt/oracle.cellos/host_access_control pam-auth --lock 4
```

4. **Pour vérifier le paramètre, répétez l'Étape 2.**

Configuration de stratégies de contrôle du vieillissement des mots de passe

Les serveurs de stockage prennent en charge divers contrôles de vieillissement des mots de passe, notamment des paramètres permettant de contrôler le nombre maximal de jours d'utilisation d'un mot de passe, le nombre minimal de jours entre deux changements de mot de passe et le moment d'envoi d'une notification d'expiration de mot de passe.

Pour respecter les exigences du Ministère de la Défense des Etats-Unis en matière de sécurité et de normes PCI-DSS, utilisez les valeurs qu'il recommande et qui figurent dans le tableau suivant :

Stratégie	Valeur par défaut d'Oracle	Valeur pour le Ministère de la Défense américain
Durée de vie maximale du mot de passe	90 jours	60 jours
Durée de vie minimale du mot de passe	1 jour	1 jour
Longueur minimale du mot de passe	8 caractères	15 caractères
Avertissement d'expiration du mot de passe	7 jours	7 jours

Pour modifier l'un de ces paramètres, procédez comme suit.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Affichez les paramètres actuels.**

```
# /opt/oracle.cellos/host_access_control password-policy --status
```

3. **Configurez les stratégies suivantes en fonction des stratégies de mot de passe de votre site.**

   - **Pour modifier le paramètre de durée de vie maximale du mot de passe, entrez :**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MAX_DAYS 60
```

   - **Pour modifier le paramètre de durée de vie minimale du mot de passe, entrez :**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_DAYS 1
```

   - **Pour modifier le paramètre de longueur minimale du mot de passe, entrez :**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_MIN_LEN 15
```

   - **Pour modifier le paramètre d'avertissement d'expiration du mot de passe, entrez :**

```
# /opt/oracle.cellos/host_access_control password-policy --PASS_WARN_AGE 7
```

4. **Pour vérifier les paramètres, répétez l'Étape 2.**

Configuration du délai d'expiration en cas d'inactivité de l'interface d'administration (shell de connexion)

Le serveur de stockage prend en charge la capacité de mettre fin à des sessions administratives restées inactives pendant une durée supérieure à un nombre de secondes prédéfini.

Pour définir le délai d'expiration en cas d'inactivité de l'interface d'administration pour un shell de connexion de compte système, procédez comme suit.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Affichez le paramètre actuel.**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
```

3. **Définissez le délai d'expiration en cas d'inactivité de l'interface d'administration.**
   Pour respecter les exigences du Ministère de la Défense des Etats-Unis en matière de sécurité et de normes PCI-DSS, spécifiez la valeur `900` (secondes). Si nécessaire, remplacez-la par une valeur compatible avec la stratégie de votre site local.

```
# /opt/oracle.cellos/host_access_control idle-timeout --shell 900
```

4. **Pour vérifier le paramètre, répétez l'Étape 2.**

Configuration du délai d'expiration en cas d'inactivité de l'interface d'administration (Secure Shell)

Le serveur de stockage prend en charge la capacité de mettre fin à des sessions SSH administratives restées inactives pendant une durée supérieure à un nombre de secondes prédéfini.

Pour définir le délai d'expiration en cas d'inactivité de l'interface d'administration pour une session SSH, procédez comme suit.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**

   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Affichez le paramètre actuel.**

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
   ```

3. **Définissez un délai d'expiration en cas d'inactivité de l'interface d'administration pour une session SSH.**

   Pour respecter les exigences en matière de sécurité du Ministère de la Défense des Etats-Unis, spécifiez la valeur `900` (secondes). Si nécessaire, remplacez-la par une valeur compatible avec la stratégie du site local.

   ```
   # /opt/oracle.cellos/host_access_control idle-timeout --client 900
   ```

4. **Pour vérifier le paramètre, répétez l'Étape 2.**

Configuration d'une bannière d'avertissement de connexion (serveur de stockage)

Le serveur de stockage prend en charge la capacité d'afficher des messages spécifiques au client avant qu'un utilisateur ne parvienne à s'authentifier sur le système.

Pour définir une bannière d'avertissement de connexion avant authentification, procédez comme suit.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**

   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Déterminez les paramètres actuels.**

   ```
   # /opt/oracle.cellos/host_access_control banner --status
   ```

3. **Créez un fichier texte qui contient la bannière d'avertissement de connexion approuvée.**

4. **Définissez une bannière d'avertissement de connexion avant authentification.**

   Pour respecter les exigences du Ministère de la Défense des Etats-Unis en matière de sécurité, remplacez *filename* par le chemin d'accès et le nom d'un fichier qui contient le message d'avertissement de connexion approuvée.

   ```
   # /opt/oracle.cellos/host_access_control banner --file filename
   ```

5. **Pour vérifier le paramètre, répétez l'Étape 2.**

Limitation de l'accès réseau à distance

Vous pouvez limiter l'accès réseau à distance entrant en implémentant un ensemble de règles de filtrage. Vous pouvez également ajuster l'accès réseau en définissant un ensemble de règles personnalisées.

Utilisez les procédures suivantes pour limiter l'accès à distance.

- "Isolement du réseau de gestion des serveurs de stockage" à la page 110
- "Limitation de l'accès réseau à distance" à la page 110

Isolement du réseau de gestion des serveurs de stockage

Le serveur de stockage est déployé sur un réseau de gestion dédié et isolé. Cela permet de protéger le serveur de stockage de tout trafic réseau non autorisé ou inopportun. Il convient de contrôler strictement la connexion au réseau de gestion en accordant des autorisations aux seuls administrateurs qui ont besoin d'un tel niveau d'accès.

▼ Limitation de l'accès réseau à distance

Vous disposez de plusieurs méthodes pour limiter l'accès réseau à distance sur des serveurs de stockage. Vous pouvez restreindre l'accès réseau entrant au serveur de stockage en implémentant un ensemble de règles de filtrage descendant qui définit l'accès selon l'origine et le compte de l'utilisateur. Vous pouvez également définir un ensemble de règles personnalisées pour accorder ou refuser l'accès en fonction des exigences du Ministère de la Défense des Etats-Unis et des normes PCI-DSS.

Attention - Faites preuve de prudence en implémentant des stratégies autres que par défaut pour éviter toute interruption d'accès au système. Lorsque vous ajoutez de nouvelles règles individuelles, les modifications prennent effet immédiatement.

Pour implémenter un ensemble de règles, procédez comme suit.

1. **Connectez-vous au serveur de stockage en tant qu'utilisateur `celladmin`.**
   Voir "Connexion au système d'exploitation des serveurs de stockage" à la page 97.

2. **Examinez l'ensemble de règles actif.**

   ```
   # /opt/oracle.cellos/host_access_control access --status
   ```

3. **Exportez l'ensemble de règles actuel dans un fichier et enregistrez-le en tant que copie de sauvegarde.**
   La commande suivante exporte l'ensemble de règles dans un fichier texte ASCII :

   ```
   # /opt/oracle.cellos/host_access_control access-export --file filename
   ```

4. **Configurez l'ensemble de règles en exécutant une ou plusieurs des commandes suivantes, selon la méthode que vous souhaitez utiliser pour le créer :**

   - **Pour implémenter un ensemble de règles ouvert qui supprime les restrictions réseau entrantes, entrez :**

     ```
     # /opt/oracle.cellos/host_access_control access --open
     ```

   - **Pour implémenter un ensemble de règles fermé qui autorise uniquement l'accès entrant avec SSH, entrez :**

     ```
     # /opt/oracle.cellos/host_access_control access --close
     ```

   - **Pour modifier l'ensemble de règles existant, entrez :**
     Exportez l'ensemble de règles actuel dans un fichier texte ASCII :

     ```
     # /opt/oracle.cellos/host_access_control access-export --file filename
     ```

     Utilisez un éditeur pour modifier le fichier texte afin de configurer l'ensemble de règles.

     Importez l'ensemble de règles du fichier texte, en remplaçant l'existant :

     ```
     # /opt/oracle.cellos/host_access_control access-import --file filename
     ```

- **Pour ajouter des règles spécifiques individuellement :**

  Cette méthode permet d'accorder et de refuser l'accès en fonction des paramètres suivants :

  - **Nom d'utilisateur** – Les valeurs valides incluent le mot clé `all` ou un ou plusieurs noms d'utilisateur valides pour un compte local.
  - **Origine** – Les valeurs valides incluent le mot clé `all` ou des entrées individuelles qui décrivent la source de l'accès au système, notamment la console, la console virtuelle, Oracle ILOM, l'adresse IP, l'adresse réseau, le nom d'hôte ou le domaine DNS.

  Dans cet exemple, l'accès au serveur de stockage est accordé à l'utilisateur `celladmin` lorsque la connexion est initiée à partir de l'hôte `trusted.example.org`, ou de tout hôte du domaine `.trusted.domain.com`.

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.domain.com
```

Ressources supplémentaires relatives aux serveurs de stockage

Reportez-vous au manuel Exadata Database Machine Security Guide à l'adresse http://docs.oracle.com/cd/E50790_01/welcome.html.

Sécurisation des commutateurs IB et Ethernet

Le commutateur InfiniBand 36 pour centre de données d'Oracle Sun utilisé par le système SuperCluster fournit le socle réseau permettant de prendre en charge un backplane hautement performant et évolutif entièrement redondant sur tous les composants internes.

Les commutateurs IB connectent les serveurs de calcul, les cellules de stockage et les appareils de stockage ZFS. Ils incorporent une instance Oracle ILOM intégrée pour offrir des capacités de gestion et de surveillance avancées. Oracle ILOM permet notamment de surveiller et de contrôler les utilisateurs, le matériel, les services, les protocoles et les autres paramètres de configuration.

Le système SuperCluster M7 dispose d'au minimum deux commutateurs IB, avec d'autres installés si nécessaire pour les plus grandes organisations. Vous devez sécuriser individuellement chaque commutateur IB.

Les rubriques suivantes décrivent la procédure de sécurisation des commutateurs IB dans le système SuperCluster M7 :

▼ Connexion à un commutateur IB

Cette tâche décrit comment se connecter à l'interface d'Oracle ILOM sur le commutateur où la majorité des tâches d'administration sont effectuées.

- **Sur le réseau de gestion, connectez-vous à Oracle ILOM sur le commutateur IB en tant qu'utilisateur `ilom-admin`.**

  Pour obtenir les mots de passe par défaut, reportez-vous à la section "Comptes et mots de passe par défaut (commutateur IB)" à la page 115.

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

Détermination de la version du microprogramme du commutateur IB

Pour tirer parti des toutes dernières fonctionnalités, capacités et améliorations de sécurité, veillez à mettre à jour le commutateur IB vers la plus récente version du microprogramme prise en charge.

1. **Connectez-vous à un commutateur IB en tant qu'utilisateur `ilom-admin`.**

   Voir "Connexion à un commutateur IB" à la page 113.

2. **Affichez la version du microprogramme.**

   Dans cet exemple, la version du microprogramme du commutateur IB est `2.1.5-1`.

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

Pour mettre à jour la version du microprogramme du commutateur IB, installez le patch QFSDP du SuperCluster le plus récent disponible à partir du site My Oracle Support à l'adresse `https://support.oracle.com`.

Remarque - Pour le système SuperCluster M7, des restrictions supplémentaires pourraient limiter les versions du logiciel du commutateur IB utilisables. Les restrictions régissent également la manière dont le microprogramme est mis à jour. Dans un tel cas, contactez votre représentant Oracle.

Comptes et mots de passe par défaut (commutateur IB)

Nom de compte	Type	Mot de passe par défaut	Description
`root`	Administrateur	`welcome1`	Permet d'accéder au système d'exploitation du commutateur IB. Généralement, les comptes `ilom-admin`, `ilom-operator` ou ceux définis par le client sont utilisés de préférence à ce compte.
`ilom-admin`	Administrateur	`ilom-admin`	Permet d'exécuter des fonctions d'administration sur le logiciel Oracle ILOM intégré, d'effectuer des mises à niveau logicielles, de configurer des utilisateurs et des services et d'exécuter des fonctions de gestion de topologie Fabric et de diagnostic de commutateur IB.
`ilom-operator`	Opérateur	`ilom-operator`	Utilisé uniquement pour les fonctions de diagnostic InfiniBand Fabric et de surveillance d'Oracle ILOM.
`nm2user`	Lecture seule	`changeme`	Ce compte dispose uniquement de privilèges en lecture seule pour accéder à l'interface d'administration de ligne de commande du commutateur IB. Ce compte est souvent utilisé par Oracle Enterprise Manager pour prendre en charge la surveillance matérielle et logicielle du commutateur.

▼ Modification des mots de passe `root` et `nm2user`

Le commutateur IB gère les comptes système dans deux emplacements. Les comptes `root` et `nm2user` sont configurés et exposés par le système d'exploitation sous-jacent du commutateur. L'ajout, la suppression et la modification des comptes ne sont pas pris en charge au niveau de cette couche, mais vous devez modifier les mots de passe par défaut.

Pour les autres comptes et mots de passe, reportez-vous à la section "Modification des mots de passe du commutateur IB (Oracle ILOM)" à la page 116.

Le commutateur IB est dans l'incapacité de définir ou d'appliquer des règles relatives à la complexité, au vieillissement et à l'historique des mots de passe ou toute autre règle. Vous devez vous assurer que les mots de passe assignés respectent les exigences du Ministère de la Défense des Etats-Unis en matière de complexité des mots de passe et que les processus sont implémentés afin de garantir que les mots de passe sont mis à jour conformément à la stratégie du Ministère de la Défense des Etats-Unis.

Pour plus d'informations sur la gestion des comptes de commutateur IB, notamment sur la procédure de création de comptes, d'attribution d'autorisations à des comptes existants ou de suppression de comptes, reportez-vous aux documents *Oracle Sun Data Center InfiniBand Switch 36 Hardware Security Guide* et *Oracle Integrated Lights Out Manager Supplement for*

the Oracle Sun Data Center InfiniBand Switch 36. Voir "Ressources supplémentaires relatives au commutateur IB" à la page 123.

Remarque - Lors de la modification du mot de passe d'un composant de SuperCluster géré par Oracle Engineered Systems Hardware Manager (tel que les commutateurs IB), vous devez également mettre à jour le mot de passe d'Oracle Engineered Systems Hardware Manager. Pour plus d'informations, reportez-vous au *Guide d'administration des serveurs Oracle SuperCluster série M7*.

---

1. **Connectez-vous au commutateur IB en tant qu'utilisateur `root`.**

```
# ssh root@IB_Switch_IP_address
```

Pour obtenir les mots de passe par défaut, reportez-vous à la section "Comptes et mots de passe par défaut (commutateur IB)" à la page 115.

2. **Modifiez le mot de passe `root`.**

```
$ passwd root
```

3. **Modifiez le mode de passe `nm2user`.**

```
$ passwd nm2user
```

Modification des mots de passe du commutateur IB (Oracle ILOM)

Le commutateur IB gère les comptes système dans deux emplacements. Cette section décrit la procédure de modification des mots de passe dans l'interface d'Oracle ILOM du commutateur IB. Pour les autres comptes et mots de passe, reportez-vous à la section "Modification des mots de passe `root` et `nm2user`" à la page 115.

Les comptes de commutateur IB par défaut et tous les comptes définis par l'utilisateur sont gérés via l'instance Oracle ILOM intégrée aux commutateurs IB.

Pour afficher les comptes et modifier les mots de passe, procédez comme suit.

1. **Connectez-vous à un commutateur IB en tant qu'utilisateur `ilom-admin`.**

Voir "Connexion à un commutateur IB" à la page 113.

Pour obtenir les mots de passe par défaut, reportez-vous à la section "Comptes et mots de passe par défaut (commutateur IB)" à la page 115.

2. **Affichez les comptes Oracle ILOM configurés sur le commutateur IB.**

```
-> show /SP/users
```

3. **Modifiez le mot de passe du compte `ilom-admin`.**

```
-> set /SP/users/ilom-admin password=password
```

Isolement du réseau de commutateurs IB

L'interface de gestion du commutateur IB est déployée sur un réseau de gestion dédié et isolé. Cela protège le commutateur IB de tout trafic réseau non autorisé ou inopportun.

Il convient de contrôler strictement la connexion à ce réseau de gestion en accordant des autorisations aux seuls administrateurs qui ont besoin d'un tel niveau d'accès.

Services réseau exposés par défaut (commutateur IB)

Nom du service	Protocole	Port	Description
SSH	TCP	22	Utilisé par le service de shell sécurisé (SSH) pour fournir l'accès administratif au commutateur IB à l'aide d'une CLI.
HTTP (BUI)	TCP	80	Utilisé par le service HTTP intégré pour fournir l'accès administratif au commutateur IB à l'aide d'une interface de navigateur. Le port TCP/80 est généralement utilisé pour l'accès en texte clair mais, par défaut, le commutateur IB redirige automatiquement les demandes entrantes vers la version sécurisée du service exécutée sur le port TCP/443.
NTP	UDP	123	Utilisé par le service (client uniquement) NTP (Network Time Protocol) intégré qui permet de synchroniser l'horloge système locale à une ou plusieurs sources temporelles externes.
SNMP	UDP	161	Utilisé par le service SNMP intégré pour fournir une interface de gestion permettant de surveiller l'intégrité du commutateur IB et les notifications de déroutement reçues.
HTTPS (BUI)	TCP	443	Utilisé par le service HTTPS intégré pour fournir l'accès administratif au commutateur IB via un canal (SSL/TLS) chiffré à l'aide d'une interface de navigateur.
IPMI	TCP	623	Utilisé par le service IPMI (Intelligent Platform Management Interface) intégré pour fournir une interface informatique à diverses fonctions de surveillance et de gestion. Ne désactivez pas ce service, car il est utilisé par Oracle Enterprise Manager Ops Center pour collecter des données d'inventaire matériel, des

Nom du service	Protocole	Port	Description
			descriptions d'unités remplaçables sur site, des informations relatives aux capteurs matériels et des informations sur le statut des composants matériels.
ServiceTag	TCP	6481	Utilisé par le service Oracle ServiceTag. Il s'agit d'un protocole de découverte Oracle permettant d'identifier les serveurs et de faciliter les demandes d'assistance. Ce service est utilisé par certains produits tels qu'Oracle Enterprise Manager Ops Center pour la découverte du logiciel du commutateur IB et l'intégration avec les autres solutions de services automatiques Oracle.

Renforcement de la configuration du commutateur IB

Les rubriques suivantes décrivent la procédure de sécurisation du commutateur IB à l'aide de divers paramètres de configuration.

▼ Désactivation des services inutiles (commutateur IB)

Désactivez tous les services qui ne sont pas nécessaires au respect des exigences de la plate-forme en matière de fonctionnement et de gestion. Par défaut, le commutateur IB emploie une configuration réseau sécurisée par défaut où les services non essentiels sont déjà désactivés. Toutefois, en fonction des stratégies et des impératifs de sécurité du client, il peut être nécessaire de désactiver des services supplémentaires.

1. **Connectez-vous à un commutateur IB en tant qu'utilisateur `ilom-admin`.**

   Voir "Connexion à un commutateur IB" à la page 113.

2. **Dressez la liste des services pris en charge par le commutateur IB.**

```
-> show /SP/services
```

3. **Déterminez si un service donné est activé.**

   Remplacez *servicename* par le nom d'un service de l'Étape 2.

   ```
   -> show /SP/services/servicename servicestate
   ```

   La plupart des services reconnaissent et utilisent le paramètre `servicestate` pour indiquer qu'ils sont activés ou désactivés, mais certains autres, tels que `servicetag`, `ssh`, `sso` et `wsman`, se servent d'un paramètre appelé `state`. Quel que soit le paramètre utilisé, un service est activé si son paramètre d'état renvoie la valeur `enabled`, tel qu'indiqué dans les exemples suivants :

   ```
   -> show /SP/services/https servicestate
   /SP/services/https
   Properties:
   servicestate = enabled
   ```

   ```
   -> show /SP/services/ssh state
   /SP/services/ssh
   Properties:
   state = enabled
   ```

4. **Pour désactiver un service qui n'est plus requis, définissez son état sur `disabled`.**

   ```
   -> set /SP/services/http servicestate=disabled
   ```

5. **Déterminez si l'un des services suivants doit être désactivé.**

   En fonction des outils et des méthodes employés, les services de navigateur HTTP et HTTPS peuvent être désactivés s'ils ne sont pas requis ou utilisés. Entrez :

   ```
   -> set /SP/services/http servicestate=disabled
   -> set /SP/services/http secureredirect=disabled
   -> set /SP/services/https servicestate=disabled
   ```

   - Interface d'administration de navigateur (HTTP, HTTPS) :
     - -> **set /SP/services/http servicestate=disabled**
     - -> **set /SP/services/http secureredirect=disabled**
     - -> **set /SP/services/https servicestate=disabled**

▼ Configuration de la redirection HTTP vers HTTPS (commutateur IB)

Par défaut, le commutateur IB est configuré pour rediriger les demandes HTTP entrantes vers le service HTTPS pour garantir que toutes les communications basées sur un navigateur sont chiffrées entre le commutateur et l'administrateur.

1. **Connectez-vous à un commutateur IB en tant qu'utilisateur `ilom-admin`.**
   Voir "Connexion à un commutateur IB" à la page 113.

2. **Vérifiez que la redirection sécurisée est activée.**

```
-> show /SP/services/http secureredirect
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Si la valeur par défaut a été modifiée, vous pouvez activer la redirection sécurisée.**

```
-> set /SP/services/http secureredirect=enabled
```

Désactivation des protocoles SNMP non autorisés (commutateur IB)

Par défaut, les protocoles SNMPv1, SNMPv2c et SNMPv3 sont tous activés pour le service SNMP qui permet de surveiller et gérer le commutateur IB. Veillez à laisser les anciennes versions du protocole SNMP désactivées sauf si elles sont requises.

Remarque - La version 3 du protocole SNMP intègre la prise en charge du modèle USM (User-based Security Model). Cette fonctionnalité remplace les chaînes de communauté SNMP standard par des comptes d'utilisateur qui peuvent être configurés avec des protocoles et des mots de passe d'autorisation, d'authentification et de confidentialité spécifiques. Par défaut, le commutateur IB n'inclut pas de compte USM. Configurez les comptes USM SNMPv3 en fonction de vos propres besoins en matière de déploiement, de gestion et de surveillance.

---

1. **Connectez-vous à un commutateur IB en tant qu'utilisateur `ilom-admin`.**
   Voir "Connexion à un commutateur IB" à la page 113.

2. **Déterminez le statut de chacun des protocoles SNMP.**

```
-> show /SP/services/snmp v1 v2c v3
/SP/services/snmp
Properties:
v1 = enabled
v2c = enabled
v3 = enabled
```

3. **Le cas échéant, désactivez les protocoles SNMPv1 et SNMPv2c.**

```
-> set /SP/services/snmp v1=disabled
-> set /SP/services/snmp v2c=disabled
```

Configuration de chaînes de communauté SNMP (commutateur IB)

Cette tâche est applicable seulement si le protocole SNMP v1 ou SNMPv2c est activé et configuré pour être utilisé.

Comme le protocole SNMP est souvent utilisé pour surveiller l'intégrité du périphérique, il est important de remplacer les chaînes de communauté SNMP par défaut utilisées par le périphérique par des valeurs définies par le client.

1. **Connectez-vous à un commutateur IB en tant qu'utilisateur `ilom-admin`.**

   Voir "Connexion à un commutateur IB" à la page 113.

2. **Créez une chaîne de communauté SNMP.**

   Dans cet exemple, remplacez les éléments suivants dans la ligne de commande :

   - *string* – A remplacer par une valeur définie par le client conforme aux exigences du Ministère de la Défense des Etats-Unis relatives à la composition des chaînes de communauté SNMP.
   - *access* – A remplacer par `ro` ou `rw`, selon qu'il s'agit d'une chaîne avec accès en lecture seule ou en lecture-écriture.

   ```
   -> create /SP/services/snmp/communities/string permission=access
   ```

   Après la création de nouvelles chaînes de communauté, il convient de supprimer celles fournies par défaut.

3. **Supprimez les chaînes de communauté SNMP par défaut.**

   ```
   -> delete /SP/services/snmp/communities/public
   -> delete /SP/services/snmp/communities/private
   ```

4. **Vérifiez les chaînes de communauté SNMP.**

   ```
   -> show /SP/services/snmp/communities
   ```

Remplacement des certificats autosignés par défaut (commutateur IB)

Les commutateurs IB utilisent des certificats autosignés permettant d'utiliser directement le protocole HTTPS. Une pratique recommandée consiste à remplacer les certificats autosignés par des certificats dont l'utilisation est autorisée dans votre environnement et qui sont signés par une autorité de certification reconnue.

Le commutateur IB prend en charge diverses méthodes permettant d'accéder au certificat et à la clé privée SSL/TLS, y compris HTTPS, HTTP, SCP, FTP, TFTP et l'insertion d'informations directement dans une interface de navigateur Web. Pour plus d'informations, reportez-vous au document *Oracle Integrated Lights Out Manager Supplement for the Oracle Sun Data Center InfiniBand Switch 36*. Voir "Ressources supplémentaires relatives au commutateur IB" à la page 123.

1. **Connectez-vous à un commutateur IB en tant qu'utilisateur `ilom-admin`.**
   Voir "Connexion à un commutateur IB" à la page 113.

2. **Déterminez si le commutateur IB utilise un certificat autosigné par défaut.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **Installez le certificat de votre organisation.**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

Configuration du délai d'expiration d'une session CLI d'administration (commutateur IB)

Les commutateurs IB prennent en charge la possibilité de déconnecter et de fermer les sessions d'administration CLI restées inactives au-delà d'un nombre de minutes prédéfini.

Par défaut, la CLI expire au bout de 15 minutes.

1. **Connectez-vous à un commutateur IB en tant qu'utilisateur `ilom-admin`.**
   Voir "Connexion à un commutateur IB" à la page 113.

2. **Vérifiez le paramètre de délai d'expiration en cas d'inactivité associé à la CLI.**

```
-> show /SP/cli timeout
/SP/cli
Properties:
timeout = 15
```

3. **Définissez le paramètre de délai d'expiration en cas d'inactivité.**

   Remplacez *n* par une valeur exprimée en minutes.

```
-> set /SP/cli timeout=n
```

Ressources supplémentaires relatives au commutateur IB

Pour plus d'informations sur les procédures d'administration et de sécurité du commutateur IB, reportez-vous à la bibliothèque de documentation Sun Datacenter InfiniBand Switch 36 à l'adresse http://docs.oracle.com/cd/E36265_01.

▼ Modification du mot de passe du commutateur Ethernet

Remarque - Lors de la modification du mot de passe d'un composant de SuperCluster géré par Oracle Engineered Systems Hardware Manager (tel que le commutateur Ethernet), vous devez également mettre à jour le mot de passe d'Oracle Engineered Systems Hardware Manager. Pour plus d'informations, reportez-vous au *Guide d'administration des serveurs Oracle SuperCluster série M7*.

1. **Connectez un câble série de la console du commutateur Ethernet à un ordinateur portable ou un périphérique similaire.**

   La vitesse du port série par défaut est de 9 600 bauds, 8 bits, sans parité et sans protocole de transfert.

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **Activez le commutateur.**

```
sscsw-adm0> enable
```

3. **Définissez le mot de passe.**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **Enregistrez la configuration.**

```
sscsw-adm0# copy running-config startup-config
```

5. **Quittez la session.**

```
sscsw-adm0# exit
```

6. **Déconnectez l'ordinateur portable du commutateur Ethernet.**

Audit de conformité

Servez-vous de l'utilitaire de conformité d'Oracle Solaris pour évaluer et présenter sous forme d'états la conformité d'un système à un test d'évaluation connu.

La commande `compliance`d'Oracle Solaris mappe les exigences d'un test d'évaluation avec une sortie de code, de fichier ou de commande pour vérifier la conformité à une exigence particulière. Oracle SuperCluster prend actuellement en charge deux profils de test d'évaluation de conformité de la sécurité :

- **Recommended** (recommandé) – Profil basé sur le test d'évaluation Center of Internet Security.
- **PCI-DSS** – Profil qui vérifie les exigences de conformité à la norme PCI DSS (Payment Card Industry Data Security Standard).

Ces outils de profilage mappent les commandes de sécurité sur les exigences de conformité et les états de conformité générés peuvent réduire considérablement le temps d'audit. En outre, la fonctionnalité de conformité fournit des guides qui contiennent les raisons de chaque contrôle de sécurité et les étapes à suivre pour corriger une vérification ayant échoué. Les guides peuvent être utiles dans le cadre de formations et en guise d'instructions pour les tests ultérieurs. Par défaut, des guides sont créés pour chaque profil de sécurité lors de l'installation. L'administrateur de SuperCluster Solaris peut ajouter ou modifier un test d'évaluation et créer un guide.

Ces rubriques expliquent comment exécuter des états de conformité et décrivent la conformité FIPS-140 :

- "Génération d'une évaluation de conformité" à la page 125
- "Exécution d'états de conformité avec un travail `cron` (facultatif)" à la page 128
- "Conformité FIPS-140-2 de niveau 1" à la page 128

▼ Génération d'une évaluation de conformité

Pour effectuer cette tâche, vous devez disposer du profil de droits d'installation de logiciels afin d'ajouter des packages au système. Vous devez disposer de droits d'administration pour la plupart des commandes de conformité.

1. **Installez le package compliance.**

```
# pkg install compliance
```

Le message suivant indique que le package est installé :

```
No updates necessary for this image.
```

Pour plus d'informations, reportez-vous à la page de manuel `pkg(1)`.

Remarque - Installez le package dans chaque zone dans laquelle vous prévoyez d'exécuter des tests de conformité.

---

2. **Répertoriez les tests d'évaluation disponibles, les profils et les évaluations précédentes, le cas échéant.**

Cet exemple contient deux tests d'évaluation.

- **`pci-dss`** – inclut un profil : `Solaris_PCI-DSS`.
- **`solaris`** – inclut deux profils : `Baseline` et `Recommended`.

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **Génération d'une évaluation de conformité**

Exécutez la commande `compliance` avec la syntaxe suivante :

`compliance assess -b` *benchmark* `-p` *profile*

`-b`	Indique un test d'évaluation particulier. Si cette option n'est pas spécifiée, la valeur par défaut est `solaris`.
`-p`	Indique le profil. Le nom du profil est sensible à la casse. Si cette option n'est pas indiquée, le premier profil est utilisé par défaut.

Exemples :

- Utilisation du profil `Recommended` :

```
# compliance assess -b solaris -p Recommended
```

La commande crée dans `/var/share/compliance/assessments` un répertoire qui contient l'évaluation dans trois fichiers : un fichier journal, un fichier XML et un fichier HTML.

- Utilisation du profil PCI-DSS :

```
# compliance assess -b pci-dss
```

Remarque - Le test d'évaluation `pci-dss` ne contenant qu'un profil, l'option de profil (`-p`) n'est pas requise sur la ligne de commande.

4. Vérifiez que les fichiers de conformité ont été créés.

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

Remarque - Si vous exécutez de nouveau la même commande `compliance`, les fichiers ne sont pas remplacés. Vous devez supprimer les fichiers avant de réutiliser un répertoire d'évaluation.

5. Créez un état personnalisé (facultatif).

Vous pouvez exécuter des états personnalisés de façon répétée. Toutefois, vous ne pouvez exécuter l'évaluation qu'une seule fois dans le répertoire d'origine.

Dans cet exemple, l'option `-s` est utilisée pour sélectionner les types de résultats à afficher dans l'état.

Par défaut, tous les types de résultats apparaissent dans l'état, à l'exception de `notselected` et `notapplicable`. Les types de résultats sont indiqués sous forme de liste séparée par des virgules qui s'affiche en plus des valeurs par défaut. Pour supprimer des types de résultats individuels, faites-les précéder du signe `-`. En outre, faites débuter la liste par un signe `=` pour indiquer exactement les types de résultats à inclure. Les types de résultats sont les suivants : `pass`, `fixed`, `notchecked`, `notapplicable`, `notselected`, `informational`, `unknown`, `error` et `fail`.

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/filename_timestamp/report_A.html
```

Cette commande crée un état contenant des éléments ayant subi un échec et des éléments non sélectionnés au format HTML. L'état est exécuté par rapport à la dernière évaluation.

6. Affichez l'état complet.

Vous pouvez visualiser le fichier journal dans un éditeur de texte, visualiser le fichier HTML dans un navigateur ou visualiser le fichier XML dans une visionneuse de XML. Par exemple, pour afficher l'état HTML personnalisé de l'étape qui précède, saisissez l'entrée suivante dans le navigateur :

```
file:///var/share/compliance/assessments/filename_timestamp/report_A.html
```

7. Corrigez tous les points en échec dont la réussite est nécessaire pour votre stratégie de sécurité.

Si la correction inclut la réinitialisation du système, réinitialisez le système avant d'exécuter à nouveau l'évaluation.

8. **Répétez l'évaluation jusqu'à l'élimination complète des échecs.**

▼ Exécution d'états de conformité avec un travail `cron` (facultatif)

- **Connectez-vous en tant que superutilisateur et utilisez la commande `crontab -e` pour ajouter l'entrée appropriée au fichier `crontab`.**

  Cette liste fournit des exemples d'entrées `crontab` :

  - Exécute des évaluations de conformité tous les jours à 2h30.

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

  - Exécute des évaluations de conformité tous les dimanches à 1h15.

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```

  - Exécute des évaluations le premier jour de chaque mois à 4h.

    ```
    0 4 1 * * /usr/bin/compliance assess -b pci-dss
    ```

  - Exécute des évaluations le premier lundi du mois à 3h45.

    ```
    45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
    ```

Conformité FIPS-140-2 de niveau 1

Les applications cryptographiques hébergées sur un système SuperCluster se fondent sur la structure cryptographique d'Oracle Solaris, qui est validée pour la conformité FIPS 140-2 de niveau 1. Cette structure est le point central pour les opérations cryptographiques d'Oracle Solaris. Elle fournit deux modules vérifiés par FIPS 140, qui prennent en charge les processus au niveau espace utilisateur et noyau. Ces modules de bibliothèque assurent des fonctions de chiffrement, de déchiffrement, de hachage, de génération et de vérification de signature, de génération et de vérification de certificat, ou encore d'authentification de message pour les applications. Les applications de niveau utilisateur qui appellent ces modules s'exécutent en mode FIPS 140.

En complément de la structure cryptographique d'Oracle Solaris, le module OpenSSL intégré à Oracle Solaris et validé pour la conformité FIPS 140-2 de niveau 1 assure la cryptographie pour les applications basées sur les protocoles SSH (Secure Shell) et TLS. Le fournisseur

de services de cloud peut choisir d'activer les hôtes locataires dans des modes conformes à la norme FIPS 140. Lors d'une exécution conforme à la norme FIPS 140, Oracle Solaris et OpenSSL, qui sont des fournisseurs FIPS 140-2, utilisent des algorithmes cryptographiques validés par FIPS 140.

Reportez-vous également à la section "(Si nécessaire) Activation du fonctionnement compatible avec la norme FIPS-140 (Oracle ILOM)" à la page 39.

Ce tableau répertorie les algorithmes approuvés par FIPS qui sont pris en charge par Oracle Solaris sur les serveurs SuperCluster série M7.

Clé ou CSP	**Numéro de certificat**	
	v1.0	**v1.1**
Clé symétrique		
AES : modes ECB, CBC, CFB-128, CCM, GMAC, GCM et CTR pour les tailles de clé 128, 192 et 256 bits	n°2311	n°2574
AES : mode XTS pour les tailles de clé 256 et 512 bits	n°2311	n°2574
TripleDES : modes CBC et ECB pour l'option de clé 1	n°1458	n°1560
Clé asymétrique		
Génération/vérification de signature RSA PKCS n°1.5 : 1024, 2048 bits (avec SHA-1, SHA-256, SHA-384, SHA-512)	n°1194	n°1321
Génération/vérification de signature ECDSA : P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571	n°376	n°446
Norme de hachage sécurisé (SHS)		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	n°1425	n°1596
Authentification de message basée sur le hachage (à clé)		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	n°1425	n°1596
Générateurs de numéros aléatoires		
Générateur de numéros aléatoires FIPS 186-2 swrand	n°1154	n°1222
Générateur de numéros aléatoires FIPS 186-2 n2rng	n°1152	n°1226

Oracle Solaris propose deux fournisseurs d'algorithmes cryptographiques qui sont validés pour la norme FIPS 140-2 de niveau 1.

- La structure cryptographique d'Oracle Solaris est le point central de stockage pour les opérations cryptographiques sur un système Oracle Solaris et fournit deux modules FIPS 140. Le module utilisateur fournit la cryptographie pour les applications exécutées dans l'espace utilisateur, tandis que le module noyau la fournit aux processus au niveau noyau. Ces modules de bibliothèque assurent des fonctions de chiffrement, de déchiffrement, de hachage, de génération et de vérification de signature, de génération et de vérification de certificat, ainsi que d'authentification de message pour les applications.

Les applications au niveau de l'utilisateur qui appellent ces modules s'exécutent en mode FIPS 140, par exemple, la commande `passwd` et IKEv2. Les consommateurs au niveau du noyau, par exemple Kerberos et IPsec, utilisent des API propriétaires pour appeler la structure cryptographique du noyau.

- Le module OpenSSL fournit la cryptographie aux applications SSH et Web. OpenSSL est la boîte à outils Open Source des protocoles Secure Sockets Layer (SSL) et Transport Layer Security (TLS) et fournit une bibliothèque de cryptographie. Dans Oracle Solaris, SSH et le serveur Web Apache sont des consommateurs du module OpenSSL FIPS 140. Oracle Solaris fournit une version FIPS 140 d'OpenSSL avec Oracle Solaris 11.2, qui est accessible à tous les consommateurs, mais la version livrée avec Oracle Solaris 11.1 est disponible pour Solaris SSH uniquement. Etant donné que les modules de fournisseur FIPS 140 2 peuvent nécessiter un grand nombre de CPU, ils sont désactivés par défaut. En tant qu'administrateur, vous êtes responsable de l'autorisation des fournisseurs en mode FIPS 140 et de la configuration des consommateurs.

Pour plus d'informations sur l'activation des fournisseurs FIPS 140 sur Oracle Solaris, reportez-vous au document intitulé *Using a FIPS 140 Enabled System in Oracle Solaris 11.2* (en anglais uniquement), disponible sous l'en-tête Sécurisation du système d'exploitation Oracle Solaris 11 à l'adresse : `http://docs.oracle.com/cd/E36784_01`.

Sécurisation des systèmes SuperCluster série M7

Ces rubriques décrivent les fonctionnalités que vous pouvez utiliser pour garantir la sécurité du système SuperCluster série M7 tout au long de son cycle de vie :

Gestion de la sécurité des serveurs SuperCluster

Les serveurs SuperCluster M7 utilisent les fonctionnalités de gestion de la sécurité d'un vaste éventail de produits, notamment Oracle ILOM, Oracle Enterprise Manager Ops Center, Oracle Enterprise Manager et la suite Oracle Identity Management. Les sections suivantes décrivent ces produits en détail :

Gestion sécurisée avec Oracle ILOM

Oracle ILOM est un processeur de service intégré dans de nombreux composants du SuperCluster M7. Oracle ILOM permet d'effectuer les activités de gestion hors bande suivantes :

- Fournir un accès sécurisé pour gérer à distance les composants du SuperCluster en toute sécurité. 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 RBAC. Affecter à des utilisateurs individuels 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. Cette fonctionnalité vous permet de détecter une activité ou des modifications non autorisées et de réaffecter ces actions à des utilisateurs spécifiques.

Pour plus d'informations, reportez-vous à la documentation d'Oracle Integrated Lights Out Manager à l'adresse : http://docs.oracle.com/en/hardware/?tab=4

Suite Oracle Identity Management

La suite Oracle Identity Management gère en intégralité le cycle de vie des identités et des comptes utilisateur au sein d'une entreprise. Elle prend en charge l'accès avec connexion unique, le contrôle d'accès Web, la sécurité des services Web, l'administration des identités, l'authentification renforcée, ainsi que la gestion des identités et des accès.

Oracle Identity Management peut fournit un point unique pour la gestion des identités et des accès, non seulement pour les applications et les services exécutés sur un système Oracle SuperCluster, mais également pour l'infrastructure sous-jacente et les services chargés de la gérer.

Pour plus d'informations, reportez-vous à la documentation d'Oracle Identity Management à l'adresse :

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Oracle Key Manager

Oracle Key Manager est un système de gestion de clés (KMS) complet, qui simplifie la gestion et et la surveillance des clés de chiffrement qui protègent les informations inutilisées.

Oracle Key Manager prend en charge des environnements d'entreprise dotés d'une architecture hautement évolutive et disponible, qui peuvent gérer des milliers de périphériques et des millions de clés. Cette fonction s'exécute dans un environnement d'exploitation sécurisé, applique un contrôle strict des accès et une séparation des rôles pour les opérations de gestion

des clés et de surveillance, et prend éventuellement en charge le stockage sécurisé des clés dans sur la carte PCIe Sun Crypto Accelerator 6000 d'Oracle, un module matériel sécurisé FIPS 140-2.

Dans le contexte d'un système SuperCluster, Oracle Key Manager peut autoriser, sécuriser et gérer l'accès aux clés de chiffrement utilisées par les lecteurs de bande à chiffrement Oracle StorageTek, aux bases de données Oracle utilisant un chiffrement de données transparent et aux systèmes de fichiers ZFS chiffrés disponibles sur le système d'exploitation Oracle Solaris 11.

Pour plus d'informations, reportez-vous à la documentation d'Oracle Key Manager à l'adresse :

http://docs.oracle.com/cd/E26076_02

Oracle Engineered Systems Hardware Manager

Oracle Engineered Systems Hardware Manager est un outil de gestion du matériel au niveau du rack basé sur la BUI, conçu pour être utilisé par le personnel d'Oracle Service. Pour plus de détails, reportez-vous au manuel *Oracle SuperCluster M7 Series Owner's Guide: Administration*.

Oracle Engineered Systems Hardware Manager inclut deux ensembles d'informations d'authentification :

- **Mots de passe des composants du SuperCluster M7**

  Oracle Engineered Systems Hardware Manager stocke de façon sécurisée les mots de passe de tous les comptes d'usine pour l'ensemble des composants matériels du SuperCluster M7. Le logiciel utilise ces mots de passe pour gérer les composants du SuperCluster M7.

  Lorsque l'un de ces mots de passe est modifié, vous devez mettre à jour l'application Oracle Engineered Systems Hardware Manager à l'aide des nouveaux mots de passe.
- **Authentification locale**

  Oracle Engineered Systems Hardware Manager dispose de deux comptes utilisateur locaux. L'un est utilisé par les clients pour personnaliser Oracle Engineered Systems Hardware Manager pour leur environnement et pour gérer le compte de service. L'autre est utilisé par le personnel de maintenance Oracle pour configurer, prendre en charge et réparer les composants matériels du SuperCluster M7.

Oracle Engineered Systems Hardware Manager fournit les ressources de gestion locales ci-dessous.

- **Politique de mot de passe** : en configurant les mots de passe d'application en fonction des politiques de mot de passe définies pour votre société, vous êtes assuré que les mots de passe sont conformes aux normes de votre entreprise.

Remarque - Contactez votre responsable de la sécurité informatique pour connaître les paramètres de la politique de mot de passe.

- **Certificats** : Oracle Engineered Systems Hardware Manager utilise des certificats pour sécuriser la communication entre les serveurs de calcul et le serveur Oracle Engineered Systems Hardware Manager et la BUI. Ces certificats sont automatiquement créés lors de l'installation et sont propres à chaque instance de SuperCluster. Toutefois, ils peuvent être remplacés par des certificats et des clés fournis par le client.
- **Ports** : les ports réseau utilisés par Oracle Engineered Systems Hardware Manager peuvent être configurés en cas de conflit avec la politique de votre entreprise. Les ports 8001 à 8004 (inclus) sont utilisés.

Pour obtenir des instructions de configuration, reportez-vous au manuel *Oracle SuperCluster M7 Series Owner's Guide: Administration*.

Oracle Enterprise Manager

La suite Oracle Enterprise Manager est une solution de gestion de cloud complète et intégrée qui se concentre sur la gestion du cycle de vie des applications, du middleware, des bases de données, ainsi que de l'infrastructure physique et virtuelle (à l'aide d'Oracle Enterprise Manager Ops Center). Oracle Enterprise Manager fournit les technologies de gestion suivantes :

- Il prend en charge la surveillance détaillée, la notification d'événements, l'application de patchs, la gestion des modifications, la configuration continue, la gestion de la conformité, ainsi que la génération d'états pour l'application, le middleware et la base de données.
- Il vous permet de gérer de façon centralisée les paramètres de configuration de la sécurité, ainsi que le contrôle des accès et les stratégies d'audit pour des groupes de bases de données. L'accès à ces fonctions peut être limité à certaines personnes autorisées, ce qui permet de s'assurer que l'accès à la gestion prend en charge des mandats de conformité pour la séparation du service, le moindre privilège et l'imputabilité.
- Il prend en charge l'authentification renforcée à l'aide de diverses méthodes, de contrôles d'accès détaillés et d'un audit complet, afin de vérifier que la gestion de l'environnement SuperCluster peut s'effectuer de façon sécurisée.

Pour plus d'informations, reportez-vous à la documentation d'Oracle Enterprise Manager à l'adresse : `http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html`

Oracle Enterprise Manager Ops Center (facultatif)

Oracle Enterprise Manager Ops Center est une technologie facultative que vous pouvez utiliser pour gérer certains aspects de la sécurité des serveurs Oracle SuperCluster.

Composant de la suite Oracle Enterprise Manager, Oracle Enterprise Manager Ops Center est une solution de gestion matérielle convergée qui fournit une interface administrative unique pour les serveurs, les systèmes d'exploitation, les microprogrammes, les machines virtuelles, les zones, le stockage et les structures réseau.

Vous pouvez utiliser Oracle Enterprise Manager Ops Center pour affecter un accès administratif à des collections de systèmes physiques et virtuels, surveiller l'activité de l'administrateur, détecter les pannes, et configurer et gérer les alertes. Oracle Enterprise Manager Ops Center prend en charge divers états qui vous permettent de comparer des systèmes par rapport à des lignes de base de configuration connues, des niveaux de patch et des failles de sécurité.

Pour plus d'informations, reportez-vous à la documentation d'Oracle Enterprise Manager Ops Center à l'adresse : `http://docs.oracle.com/cd/E27363_01/index.htm`

Remarque - Dans les versions précédentes d'Oracle Enterprise Manager Ops Center, le logiciel Ops Center était installé et exécuté à partir du système SuperCluster. A partir d'Oracle Enterprise Manager Ops Center 12c version 2 (12.2.0.0.0), le logiciel Ops Center doit être installé et exécuté sur un système situé en dehors du système SuperCluster.

Surveillance de la sécurité

Qu'il s'agisse d'états de conformité ou de réponses aux incidents, la surveillance et l'audit sont des fonctions essentielles que vous devez utiliser pour accroître la visibilité sur l'environnement informatique. Le degré d'utilisation de la surveillance et de l'audit se fonde souvent sur le risque ou la nature critique de l'environnement.

Les systèmes SuperCluster série M7 offrent des fonctionnalités complètes de surveillance et d'audit au niveau du serveur, du réseau, de la base de données et du stockage, afin de garantir l'accès aux informations pour prendre en charge les exigences requises en matière d'audit et de conformité.

Les sections suivantes décrivent la surveillance et l'audit de la base de données et de la charge globale :

- "Surveillance de la charge globale" à la page 136

Surveillance de la charge globale

Le système d'exploitation Oracle Solaris dispose d'une fonction complète d'audit, qui permet de surveiller les opérations d'administration, les appels sur la ligne de commande et même les appels système individuels au niveau du noyau. Cet outil, hautement configurable, prend en charge des stratégies d'audit globales, par zone et par utilisateur.

Lorsque le système est configuré pour utiliser des zones Oracle Solaris, les enregistrements d'audit pour chaque zone peuvent être stockés dans la zone globale afin d'être protégés contre toute altération.

L'audit Oracle Solaris permet d'envoyer des enregistrements d'audit vers des points de collecte distants à l'aide de la fonction de journal système (`syslog`). De nombreux services commerciaux de prévention et de détection des intrusions peuvent utiliser les enregistrements d'audit Oracle Solaris comme entrée supplémentaire pour l'analyse et la génération d'états.

Oracle VM Server for SPARC exploite la fonction d'audit Oracle Solaris native pour enregistrer des actions et des événements associés à des événements de virtualisation et à l'administration de domaine.

Pour plus d'informations, reportez-vous à la section Surveillance et maintenance de la sécurité d'Oracle Solaris dans les Directives de sécurité d'Oracle Solaris à l'adresse :

`http://docs.oracle.com/cd/E26502_01`

Surveillance de l'activité de la base de données et audit

La prise en charge d'un audit détaillé par Oracle Database vous permet de définir des stratégies qui déterminent de façon sélective le moment où les enregistrements d'audit sont générés. Cette fonction vous aide à vous concentrer sur d'autres activités de la base de données et réduit le temps système qui est souvent associé aux activités d'audit.

Oracle Audit Vault and Database Firewall centralise la gestion des paramètres d'audit de la base de données et automatise la consolidation des données d'audit dans un référentiel sécurisé.

Ce logiciel inclut une fonction intégrée de génération d'états, qui permet de surveiller un large éventail d'activités, notamment celle des utilisateurs privilégiés et les modifications apportées aux structures de base de données. Les états générés par Oracle Audit Vault and Database Firewall offrent de la visibilité sur diverses activités d'application et de base de données d'administration, et fournissent des informations détaillées pour prendre en charge l'imputabilité des actions.

Oracle Audit Vault and Database Firewall permet de détecter et de signaler de façon proactive des activités pouvant indiquer des tentatives d'accès non autorisé ou d'utilisation abusive des privilèges système. Ces alertes peuvent inclure des conditions et des événements définis à la fois par l'utilisateur et le système, comme la création de comptes utilisateur privilégiés ou la modification de tableaux contenant des informations sensibles.

Oracle Audit Vault and Database Firewall Remote Monitor peut proposer une surveillance de la sécurité de la base de données en temps réel. Cette fonctionnalité interroge les connexions de base de données pour détecter le trafic malveillant, comme le contournement d'application, une activité non autorisée, une injection SQL et d'autres menaces. A l'aide d'une approche précise basée sur la syntaxe SQL, ce logiciel vous aide à identifier rapidement les activités suspectes sur la base de données.

Pour plus d'informations, reportez-vous à la documentation d'Oracle Audit Vault and Database Firewall à l'adresse : `http://docs.oracle.com/cd/E37100_01/index.htm`

Surveillance du réseau

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

Suivez les recommandations suivantes pour garantir la sécurité des accès locaux et distants au système :

- Consultez les journaux afin de rechercher d'éventuels incidents et archivez-les conformément aux stratégies de sécurité de votre entreprise.
- Effectuez des contrôles périodiques du réseau d'accès client pour garantir l'intégrité des paramètres hôte et Oracle ILOM.

Pour plus d'informations, reportez-vous aux guides de sécurité du système d'exploitation Oracle Solaris :

- Système d'exploitation Oracle Solaris 11 – `http://www.oracle.com/goto/Solaris11/docs`
- Système d'exploitation Oracle Solaris 10 – `http://www.oracle.com/goto/Solaris10/docs`

Mise à jour de logiciels et de microprogrammes

Des mises à jour du système SuperCluster série M7 sont fournies dans QFSDP. L'installation de QFSDP met à jour tous les composants en même temps. Cette pratique garantit que tous les composants continuent de s'exécuter sur une combinaison de versions logicielles qui ont été intégralement testées ensemble par Oracle.

Procurez-vous la dernière version de QFSDP à partir de My Oracle Support à l'adresse : `http://support.oracle.com`

Pour plus de détails sur les logiciels et microprogrammes pris en charge, reportez-vous aux *Notes de produit des serveurs Oracle SuperCluster série M7*. Les instructions permettant d'accéder aux Notes de produit sont disponibles dans la note 1605591.1 sur le site My Oracle Support.

Remarque - Mettez à niveau ou à jour des composants individuels, ou appliquez-leur un patch uniquement dans le cadre d'une réparation réactive sur les conseils du support technique Oracle.

Index

C

P

R

S

U

V

Z