Guide de sécurité d'Oracle MiniCluster S7-2

Référence: E78270-02
Octobre 2016

Référence: E78270-02

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 MiniCluster S7-2.
- **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 du produit

La documentation et les ressources de ce produit et des produits associés sont disponibles à l'adresse http://www.oracle.com/goto/minicluster-s7-2/docs

Commentaires

Vous pouvez faire 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 MiniCluster S7-2.

Les rubriques suivantes sont traitées dans cette section :

Tâches de sécurité minimales requises

La configuration d'usine par défaut du MiniCluster en fait un système hautement sécurisé qui offre les fonctions de sécurité suivantes :

- Il est préconfiguré avec des contrôles de sécurité totalement automatisés pour toutes les machines virtuelles.
- Le chiffrement est activé par défaut pour garantir la sécurité des données en transit ou inactives.
- Les machines virtuelles sont configurées automatiquement avec un système d'exploitation renforcé et réduit, protégé par des pare-feu basés sur l'hôte.
- Le contrôle d'accès est assuré par un accès basé sur les rôles avec privilèges minimaux.
- Toutes les machines virtuelles utilisent le stockage ZFS chiffré.
- La fonction de gestion des clés centralisée s'appuie sur PKCS#11 et prend en charge la norme FIPS.
- Le système comporte une stratégie d'audit complète avec des journaux d'audit centralisés.
- Le système et toutes les machines virtuelles sont configurés selon un profil de sécurité PCI-DSS, équivalent CIS ou DISA-STIG. Remarque : ce dernier profil fait actuellement l'objet

d'un examen. N'utilisez le profil DISA-STIG que pour effectuer des expériences dans des environnements de test.

- Un tableau de bord de conformité facilement accessible prend en charge des tests de conformité faciles à exécuter.

Juste après l'installation du système MiniCluster, l'administrateur de la sécurité doit exécuter deux tâches :

- Modifier le mot de passe root Oracle ILOM. Reportez-vous à la section "Modification des mots de passe `root` par défaut d'Oracle ILOM" à la page 27.

Consultez, en outre, les informations de sécurité de ce guide pour comprendre et vérifier les fonctions de sécurité du système MiniCluster.

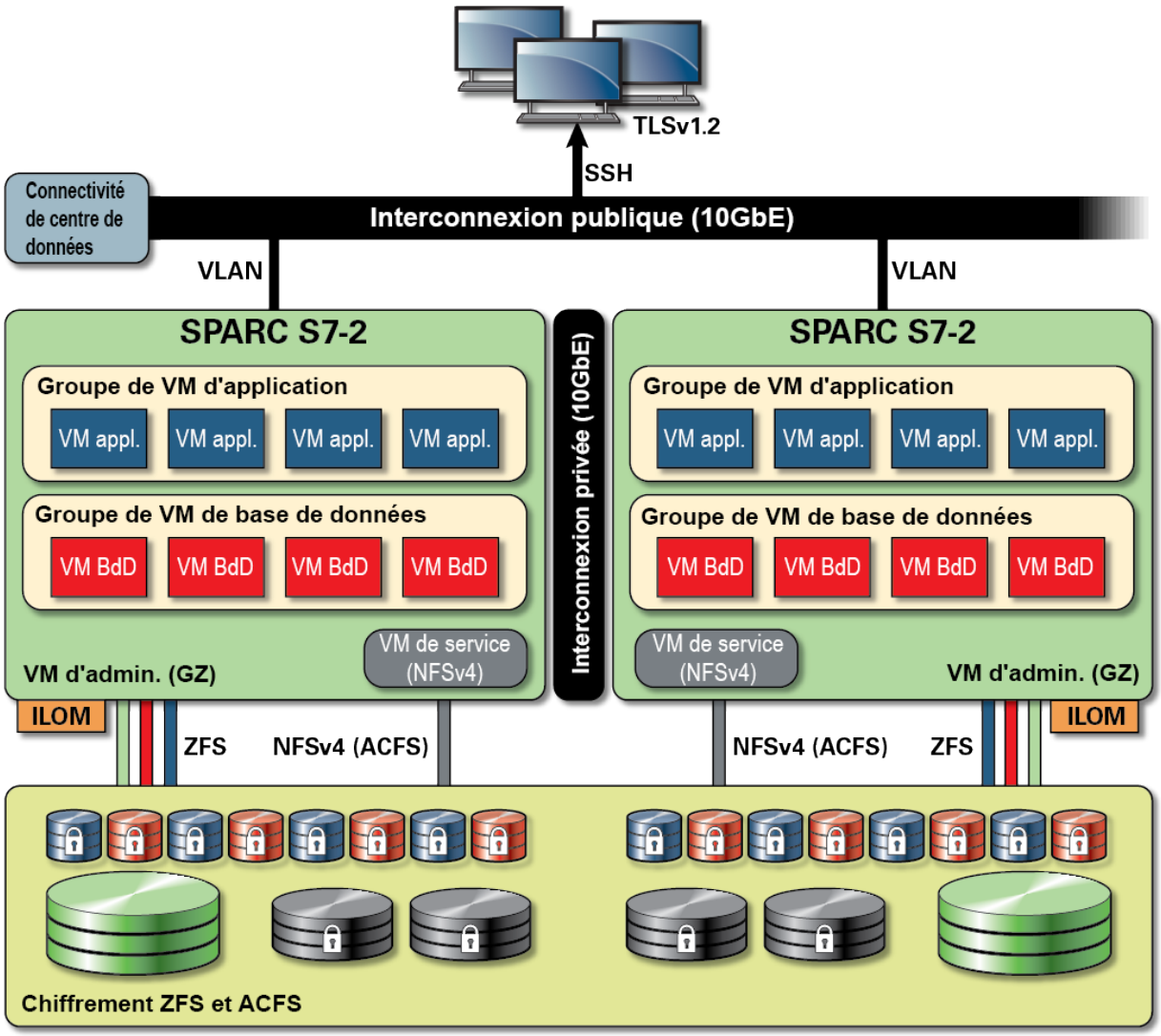
Principes de sécurité fondamentaux

MiniCluster est une plate-forme d'infrastructure cloud sécurisée pour la consolidation des applications et bases de données, parfaitement adaptée à la fourniture de services cloud basés sur une infrastructure en tant que service (IaaS) de calcul dédiée. Ce système avancé polyvalent conjugue la puissance de calcul du processeur SPARC S7 d'Oracle, l'efficacité des fonctions de virtualisation de SPARC Solaris, les performances de base de données optimisées d'Oracle Database et le stockage dédié. En outre, un réseau de 10 GbE permet aux clients d'accéder aux services s'exécutant sur le MiniCluster. Enfin, un autre réseau 10 GbE assure les communications entre l'environnement de machine virtuelle des serveurs SPARC S7 et les applications hébergées.

Le processeur SPARC S7 fournit un accélérateur cryptographique matériel qui aide les entités hébergées sur MiniCluster à protéger leurs informations en permanence, grâce à la protection des données (actives, inactives et en transit) hautement performante. Le processeur intègre également une technologie de mémoire sécurisée de silicium, qui détecte et prévient les attaques liées aux altérations de données en mémoire et à la capture de données en mémoire, et assure donc l'intégrité des données applicatives.

Par défaut, le système MiniCluster est préconfiguré avec plus de 250 contrôles de sécurité prêts à l'emploi qui réduisent la surface d'attaque du système en désactivant les services, ports et protocoles qui ne sont pas absolument nécessaires et en configurant les services exposés pour qu'ils acceptent uniquement les connexions sécurisées.

Le système prend en charge un large éventail d'options de configuration et de déploiement. La représentation ci-après illustre un déploiement type consolidant les charges de travail des applications et bases de données Oracle.



Sécurisation des machines virtuelles

La sécurité des noeuds de calcul du système MiniCluster est assurée à plusieurs niveaux. Elle commence par la sécurisation par Verified Boot des noeuds de calcul, un système d'exploitation sécurisé et réduit qui s'exécute sur des machines virtuelles isolées pour prévenir l'accès aux données et charges de travail par des systèmes ou utilisateurs non autorisés. La technologie de zones Oracle Solaris est utilisée sous forme de machines virtuelles dans le système MiniCluster pour héberger des environnements de calcul isolés et offrir un modèle d'environnement

restreint efficace et performant aux différentes applications s'exécutant sur le même système d'exploitation, afin de les protéger d'activités malveillantes ou accidentelles survenant sur d'autres machines virtuelles. Bien qu'elles s'exécutent sur le même noyau, chaque zone Solaris a sa propre identité et ses ressources, nom d'espace et processus sont isolés. En substance, les zones Solaris fournissent une virtualisation intégrée dotée d'un isolement puissant et de contrôles de ressource flexibles au niveau d'un CPU et d'une empreinte de mémoire inférieurs à celles des machines virtuelles classiques s'exécutant sur des hyperviseurs de type 1. Chaque machine virtuelle est configurée avec un profil de sécurité qui définit un jeu complet de stratégies et de contrôles de sécurité automatiquement appliqués lors du processus d'installation. L'utilisation des pools et jeux de données ZFS permet de partager et d'isoler le stockage en unités plus granulaires pour les machines virtuelles avec des stratégies de sécurité qui leur sont propres.

Contrôle d'accès

Pour protéger les données des applications, les charges de travail et l'infrastructure qui sous-tend leur exécution, le système MiniCluster offre des fonctions de contrôle d'accès complètes et flexibles aux administrateurs et aux utilisateurs. Le système MiniCluster tire pleinement parti des modes de contrôle d'accès d'Oracle Solaris pour permettre aux utilisateurs et aux applications d'accéder aux services du système. Si la traditionnelle combinaison Nom d'utilisateur/mot de passe est encore largement utilisée, il est facile d'intégrer des méthodes d'authentification plus performantes à l'aide de l'architecture PAM (Pluggable Authentication Module) d'Oracle Solaris telles que LDAP, Kerberos et l'authentification de clé publique. L'environnement de calcul du système MiniCluster s'appuie sur une fonction de contrôle d'accès basé sur les rôles (RBAC) qui offre la flexibilité nécessaire pour octroyer l'accès aux utilisateurs et administrateurs en fonction des besoins requis. En supprimant le rôle tout puissant de superutilisateur, la fonction RBAC d'Oracle Solaris permet la séparation des tâches et prend en charge les concepts de rôles d'administration, d'autorisations, de privilèges affinés et de profils de droit qui sont collectivement utilisés pour l'affectation des droits aux utilisateurs et administrateurs. La fonction RBAC est intégrée à d'autres services fondamentaux d'Oracle Solaris, notamment l'utilitaire de gestion des services (SMF) et les machines virtuelles pour offrir une architecture cohérente répondant à l'ensemble des besoins de contrôle d'accès au niveau du système d'exploitation. Le système MiniCluster utilise la fonction RBAC d'Oracle Solaris comme socle pour l'architecture de contrôle d'accès et permet aux organisations de gérer, de contrôler et d'auditer l'accès au système d'exploitation et à la gestion de la virtualisation à partir d'un point centralisé. Toutes les opérations essentielles sont exécutées en fonction du principe de séparation des tâches pris en charge par le workflow d'autorisation multiutilisateurs. Le système exige une approbation par deux utilisateurs au minimum pour toute opération sensible liée à la sécurité. Ensemble, ces fonctions permettent d'assurer une sécurité optimale concernant l'identité des utilisateurs et leur gestion d'opérations stratégiques.

Tous les périphériques du système MiniCluster permettent de limiter l'accès réseau aux services à l'aide de méthodes classiques (isolement du réseau par exemple), du filtrage de paquets ou de

listes de contrôle d'accès pour retreindre les communications émises depuis ou vers et entre les périphériques virtuels et physiques ainsi que les services exposés par le système. Le système MiniCluster présente un mécanisme de sécurisation par défaut dans lequel aucun service réseau à l'exception du shell sécurisé (SSH) n'est activé pour recevoir un trafic réseau entrant. D'autres services réseau sont activés pour l'écoute en interne des demandes du système d'exploitation Oracle Solaris (machine virtuelle ou zone). Ainsi, tous les services réseau sont désactivés par défaut ou configurés pour l'écoute des communications de système local uniquement. Les organisations peuvent personnaliser cette configuration en fonction de leurs exigences propres. Le système MiniCluster est préconfiguré avec un filtrage de paquets (avec conservation de statut) au niveau de la couche de transport et de réseau utilisant la fonction IP Filter d'Oracle Solaris. IP Filter offre un large éventail de fonctions réseau basées sur l'hôte, notamment le filtrage de paquets avec conservation de statut, la traduction d'adresses réseau (NAT) et la traduction d'adresses de port.

Protection des données

Le processeur SPARC S7 du système MiniCluster 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.

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 MiniCluster. La base de données et le logiciel intermédiaire 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. Le système MiniCluster prend en charge l'utilisation du protocole IPSec (IP Security). Par ailleurs, le protocole IKE (Internet Key Exchange) est recommandé pour protéger la confidentialité et l'intégrité des flux de communications spécifiques et entre des machines virtuelles sur les réseaux publics et privés.

Sur le système MiniCluster, le chiffrement des jeux de données ZFS tire parti d'un magasin de clés Oracle Solaris PKCS#11 centralisé pour protéger de manière sécurisée les clés d'encapsulation. L'utilisation du magasin de clés Oracle Solaris PKCS#11 implique automatiquement l'accélérateur cryptographique matériel SPARC pour toutes les opérations de chiffrement. Oracle peut ainsi améliorer considérablement les performances des opérations de chiffrement et de déchiffrement associées au traitement des jeux de données ZFS, à Oracle Database Transparent Data Encryption (TDE), au chiffrement de tablespace, 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 machines virtuelles de base de données peuvent adopter une approche de partage de portefeuille en exploitant le magasin de clés Oracle Solaris PKCS#11 pour créer un répertoire sur le stockage de partage ACFS afin que le portefeuille puisse être partagé par toutes les bases de données résidant sur des machines virtuelles. L'utilisation d'un magasin de clés partagé et centralisé sur chaque noeud de calcul facilite la gestion, la mise à jour et la rotation des clés d'Oracle TDE dans les architectures de bases de données en cluster basées sur l'infrastructure Oracle Grid car les clés sont synchronisées sur chacun des noeuds du cluster. Le système MiniCluster assure également la suppression sécurisée des machines virtuelles et des jeux de données ZFS associés car la stratégie de chiffrement et la gestion des clés s'exécutent au niveau du jeu de données ZFS (système de fichiers / ZVOL), la suppression étant garantie par la destruction des clés.

Audit et conformité

Le système MiniCluster s'appuie sur le sous-système d'audit d'Oracle Solaris pour collecter, stocker et traiter les informations relatives aux événements d'audit. Chaque machine virtuelle (zone non globale) génère des enregistrements d'audit qui sont stockés localement dans chaque emplacement d'audit (zone globale) du système MiniCluster. Cette approche garantit qu'au niveau individuel les machines virtuelles sont incapables de modifier leurs informations d'audit (stratégies, configurations et données enregistrées) puisque cette responsabilité incombe au 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 machines virtuelles. Cet outil, hautement configurable, prend en charge des stratégies d'audit globales, par zone et par utilisateur. Lorsque le système est configuré pour utiliser une machine virtuelle, les enregistrements d'audit pour chaque machine virtuelle peuvent être stockés dans la zone globale afin d'être protégés contre toute altération. En outre, la zone globale tire pleinement parti de la fonction d'audit Oracle Solaris native pour enregistrer des actions et des événements associés à des événements de virtualisation et à l'administration du système MiniCluster.

Le système MiniCluster fournit des outils pour évaluer la conformité (et générer des rapports connexes) d'un environnement d'exécution Oracle Solaris résidant dans des machines virtuelles. Les utilitaires de conformité sont basés sur le protocole SCAP (Security Content Automation

Protocol). Le système MiniCluster prend actuellement en charge deux profils de test de conformité de la sécurité :

- **Profil de sécurité par défaut** : profil équivalent au CIS (basé sur le test d'évaluation Center of Internet Security), plus adapté aux exigences de conformité de sécurité imposées par la réglementation, notamment HIPAA, FISMA, loi Sarbanes-Oxley, etc.
- **Profil PCI-DSS** : profil qui vérifie les exigences de conformité à la norme PCI DSS (Payment Card Industry Data Security Standard).
- **Profil DISA STIG** : normes de l'agence de défense des systèmes d'information (DISA) et du guide de mise en oeuvre technique de la sécurité (STIG). Ce profil repose sur le profil de sécurité par défaut et comprend 75 contrôles de sécurité supplémentaires, la cryptographie FIPS-140-2 et la possibilité de configurer un mot de passe S. *Remarque* : ce profil est en cours d'examen. N'utilisez ce profil que pour effectuer des expériences dans des environnements de test.

L'administrateur du système MiniCluster peut exécuter le test de conformité à la demande pour vérifier la conformité ou les potentielles anomalies de l'environnement. Ces outils de profilage mappent les commandes de sécurité sur les exigences de conformité imposées par les normes sectorielles. Les rapports de conformité associés peuvent réduire considérablement les délais et les coûts d'audit.

A partir de MiniCluster v.1.1.18, le système inclut les fonctionnalités d'audit suivantes :

- **Rôle d'auditeur** : lorsque ce rôle est affecté à un utilisateur MCMU, celui-ci peut accéder à la page d'examen de l'auditeur dans la BUI MCMU. L'utilisateur ne peut ni afficher ni effectuer d'autres tâches administratives de MiniCluster.
- **Page d'examen de l'auditeur** : il s'agit d'une page spéciale de la BUI MCMU que seuls les utilisateurs qui occupent le rôle d'auditeur peuvent afficher. La page permet d'accéder au statut de pool d'audits et permet de générer des rapports d'audit concernant l'activité de tous les utilisateurs par zone. Reportez-vous à la section "Générer un rapport d'audit" à la page 41.

Présentation de la configuration de sécurité

Ces rubriques décrivent les contrôles de sécurité du système MiniCluster :

Profils de sécurité intégrés

L'initialisation du système MiniCluster se fait à l'aide de la BUI ou de la CLI MCMU. Lors de l'initialisation, le MCMU demande au programme d'installation de choisir l'un des profils de sécurité suivants :

- **Profil de sécurité par défaut** : répond à des exigences comparables ou équivalentes aux tests de conformité définis par les évaluations CIS (Center for Internet Security) et STIG (Security Technical Implementation Guidelines).
- **Profil PCI-DSS** : respecte la norme PCI DSS (Payment Card Industry Data Security Standard) définie par le Conseil des normes de sécurité du secteur des cartes de paiement.
- **Profil DISA STIG** : normes de l'agence de défense des systèmes d'information (DISA) et du guide de mise en oeuvre technique de la sécurité (STIG). Ce profil repose sur le profil de sécurité par défaut et comprend 75 contrôles de sécurité supplémentaires, la cryptographie FIPS-140-2 et la possibilité de configurer un mot de passe EEPROM. *Remarque* : ce profil fait actuellement l'objet d'un examen. N'utilisez ce profil que pour effectuer des expériences dans des environnements de test.

En fonction de la stratégie sélectionnée, le MCMU configure les zones globales et non globales avec plus de 250 contrôles de sécurité.

Après l'initialisation, à la création des machines virtuelles, le MCMU requiert la sélection d'un des profils de sécurité pour chaque machine virtuelle. Selon vos exigences en matière de sécurité, vous pouvez avoir une combinaison de profils de sécurité sur les machines virtuelles.

Vérification du profil de sécurité d'une machine virtuelle (CLI)

Utilisez cette procédure pour vérifier ou identifier le profil de sécurité configuré pour les zones et les machines virtuelles.

Remarque - Vous devez accéder au système avec un compte utilisateur disposant du rôle `root` pour exécuter cette procédure.

Remarque - Pour identifier le profil de sécurité affecté à la zone globale, dans la BUI MCMU, affichez System Setting -> User Input Summary. Le profil de sécurité s'affiche en bas de la page.

1. **Connectez-vous à la zone globale en tant qu'utilisateur `mcinstall`.**

   Pour des instructions sur l'accès au système, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*.

2. **Prenez le rôle `root`.**

   Exemple :

   ```
   # su root
   ```

3. **Déterminez le nom du fichier journal pour la machine virtuelle en question.**

   Dans cet exemple, il y a un fichier journal pour chaque machine virtuelle :

   ```
   # cd /var/opt/oracle.minicluster/mcmubui/MCMU/verification_logs
   # ls
   verify_appvmg1-zone-1-mc4-n1.log  verify_dbvmg1-zone-3-mc4-n1.log
   verify_appvmg1-zone-1-mc4-n2.log  verify_dbvmg1-zone-3-mc4-n2.log
   verify_dbvmg1-zone-1-mc4-n2.log   verify_dbvmg1-zone-4-mc4-n1.log
   verify_dbvmg1-zone-2-mc4-n1.log   verify_dbvmg1-zone-4-mc4-n2.log
   verify_dbvmg1-zone-2-mc4-n2.log
   #
   ```

4. **Affichez les fichiers journaux de vérification.**

   Consultez les dernières lignes du fichier journal. Si `(PCI-DSS)` est affiché, le profil de sécurité de la machine virtuelle est PCI-DSS. Si aucun profil n'est répertorié, le profil de sécurité de la machine virtuelle est Equivalent CIS.

   - Exemple des 22 dernières lignes d'une machine virtuelle ayant un profil PCI-DSS :

     ```
     # tail -22 verify_dbvmg1-zone-1-mc4-n2.log

     (PCI-DSS) Checking /etc/cron.d/at.allow:
     Passed/Configured
     ```

```
(PCI-DSS) Checking audit configuration (user audit flags):
Passed/Configured

(PCI-DSS) Checking audit configuration (non-attributable audit flags):
Passed/Configured

(PCI-DSS) Checking audit configuration (audit_binfile plugin):
Passed/Configured

(PCI-DSS) Checking audit flags on root and tadmin roles:
Passed/Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

- Exemple des 22 dernières lignes d'une machine virtuelle ayant un profil Equivalent CIS :

```
# tail -22 verify_dbvmg1-zone-1-mc4-n2.log
Checking if NDP routing daemon is disabled:
Passed/Configured

Checking if r-protocol services are disabled:
Passed/Configured

Checking if rpc/bind is enabled and configured correctly:
Passed/Configured

Checking if NFS v2/v3 is disabled:
Passed/Configured

Checking if GDM is enabled:
Failed/Not Configured

Check if tenant-key exists in keystore:
Passed/Configured

Check if immutability is enabled:
Failed/Not Configured
```

Protection des données

Ces rubriques décrivent les technologies de protection des données du système MiniCluster :

Protection des données avec le chiffrement des jeux de données ZFS

Dans le système MiniCluster, la protection des données inactives est automatiquement configurée avec le chiffrement des jeux de données ZFS. Le chiffrement est configuré comme suit :

- Tous les jeux de données ZFS sont chiffrés dans les machines virtuelles, y compris les systèmes de fichiers root et swap.
- Tous les jeux de données ZFS sont chiffrés dans la zone globale, à l'exception des systèmes de fichiers root et swap.

Vous pouvez vérifier la configuration du chiffrement en consultant les clés de chiffrement. Reportez-vous à la section "Affichage des clés de chiffrement des jeux de données ZFS (BUI)" à la page 21.

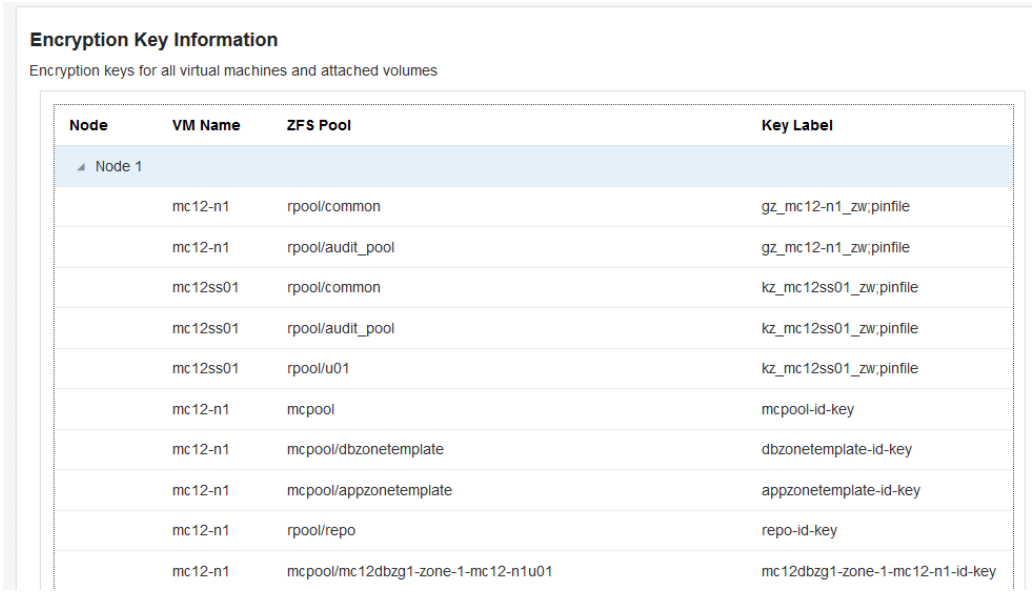
▼ Affichage des clés de chiffrement des jeux de données ZFS (BUI)

Procédez comme suit pour afficher les détails des clés de chiffrement.

1. **Accédez à la BUI MCMU.**

Pour plus d'informations sur l'accès à la BUI MCMU, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*.

2. **Dans le panneau de navigation, sélectionnez System Settings -> Security.**
Cliquez sur un noeud pour afficher les détails.



Encryption Key Information

Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label
Node 1			
	mc12-n1	rpool/common	gz_mc12-n1_zw;pinfile
	mc12-n1	rpool/audit_pool	gz_mc12-n1_zw;pinfile
	mc12ss01	rpool/common	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/audit_pool	kz_mc12ss01_zw;pinfile
	mc12ss01	rpool/u01	kz_mc12ss01_zw;pinfile
	mc12-n1	mcpool	mcpool-id-key
	mc12-n1	mcpool/dbzonetemplate	dbzonetemplate-id-key
	mc12-n1	mcpool/appzonetemplate	appzonetemplate-id-key
	mc12-n1	rpool/repo	repo-id-key
	mc12-n1	mcpool/mc12dbzg1-zone-1-mc12-n1u01	mc12dbzg1-zone-1-mc12-n1-id-key

Service shell sécurisé

Le système MiniCluster requiert l'utilisation du protocole réseau SSH pour vous permettre de vous connecter en toute sécurité aux noeuds de calcul (zones globales) et aux instances de machine virtuelle (zones non globales) du MiniCluster.

Lorsqu'un utilisateur se connecte pour la première fois à l'aide de SSH, le système génère automatiquement pour lui une nouvelle paire de clés SSH.

▼ Modification des clés SSH (BUI)

Cette procédure permet de modifier les clés SSH pour une zone ou une machine virtuelle avec l'une des configurations suivantes :

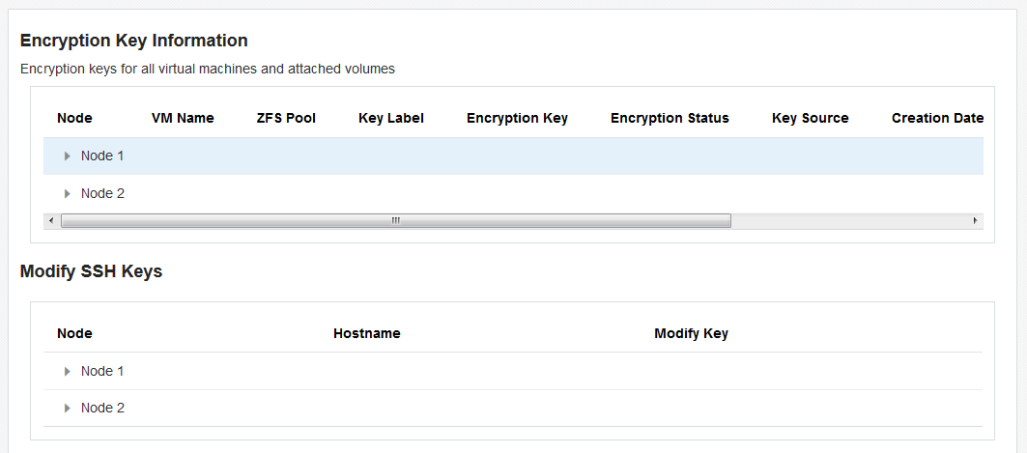
- Insérer une nouvelle clé pour autoriser un accès SSH sans mot de passe : requiert la saisie d'un nom d'utilisateur de machine virtuelle, du nom de la machine virtuelle et de la clé publique RSA.
- Générer automatiquement de nouvelles clés pour les machines virtuelles.

Remarque - Pour exécuter cette procédure à l'aide de la CLI MCMU, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*.

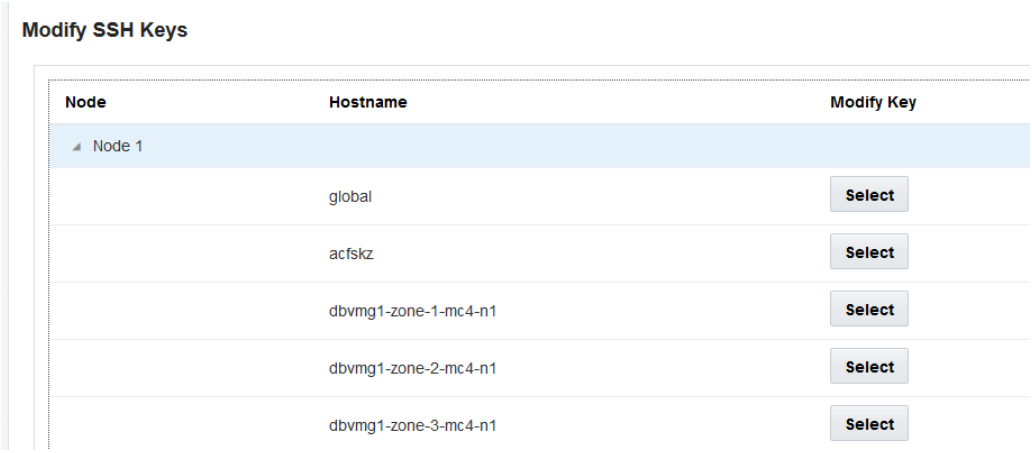
---

1. **Accédez à la BUI MCMU.**

2. **Dans le panneau de navigation, sélectionnez System Settings -> Security.**



3. **Dans le panneau Modify SSH Keys, cliquez sur un noeud pour le développer.**



4. **En regard de la machine virtuelle que vous voulez modifier, cliquez sur Select.**

5. **Sélectionnez une option dans le menu déroulant et cliquez sur Next.**
   Les options disponibles sont les suivantes :
   - Insérer une nouvelle clé pour autoriser un accès SSH sans mot de passe
   - Générer automatiquement de nouvelles clés pour les machines

6. **Cliquez sur Next.**

7. **Si vous avez sélectionné l'autorisation d'un accès SSH sans mot de passe, entrez les informations suivantes et cliquez sur Next :**
   - Nom d'utilisateur de la machine
   - Nom d'hôte de la machine
   - Clé publique RSA de la machine

8. **Cliquez sur Setup SSH.**
   La modification est appliquée.

Communication sécurisée à l'aide d'IPsec

L'utilisation du protocole IPSec (IP Security) et du protocole IKE (Internet Key Exchange) est recommandée pour protéger la confidentialité et l'intégrité des flux de communications

basés sur IP interzone et du trafic NSF sur le réseau. IPsec est recommandé car il prend en charge l'authentification des pairs au niveau du réseau, l'authentification de l'origine des données, la confidentialité des données, l'intégrité des données ainsi que la protection contre la relecture. Utilisés sur la plate-forme Oracle MiniCluster, les protocoles IPsec et IKE peuvent automatiquement tirer parti de l'accélérateur cryptographique matériel en minimisant ainsi l'impact de l'utilisation de la cryptographie sur les performances pour protéger les flux d'informations sensibles sur ce canal du réseau.

▼ Configuration d'IPsec et d'IKE

Avant la configuration d'IPsec, il est nécessaire de définir les noms d'hôte et/ou adresses IP spécifiques utilisés entre les pairs communicants.

Pour l'exemple de cette procédure, les adresses IP 10.1.1.1 et 10.1.1.2 sont utilisées pour désigner deux zones Solaris non globales exécutées par un seul locataire. La communication entre ces deux adresses est protégée par IPsec. L'exemple s'appuie sur la perspective de la zone non globale associée à l'adresse IP 10.1.1.1.

Procédez comme suit pour configurer et utiliser IPsec et IKE entre une paire de zones non globales (machines virtuelles) désignées :

1. **Définissez la stratégie de sécurité IPsec.**

   Définissez la stratégie de sécurité qui sera appliquée entre la paire de zones communicantes.

   Dans cet exemple, toutes les communications réseau entre 10.1.1.1 et 10.1.1.2 seront chiffrées :

   ```
   {laddr 10.1.1.1 raddr 10.1.1.2}
   ipsec{encr_algs aes encr_auth_algs sha256 sa shared}
   ```

2. **Stockez la stratégie dans le fichier `/etc/inet/ipsecinit.conf`.**

3. **Vérifiez que la syntaxe de la stratégie IPsec est correcte.**

   Exemple :

   ```
   # ipsecconf –c –f ipsecinit.conf
   ```

4. **Configurez le service IKE (Internet Key Exchange).**

   Configurez le service conformément aux paramètres d'hôte et d'algorithme figurant dans le fichier `/etc/inet/ike/config`.

   ```
   { label "ipsec"

   local_id_type ip

   remote_addr 10.1.1.2

   p1_xform { auth_method preshared oakley_group 5
   ```

```
auth_alg sha256 encr_alg aes } }
```

5. Configurez la clé pré-partagée.

Pour qu'IPsec puisse être activé, le matériel de la clé doit être partagé avec les noeuds pairs afin qu'ils puissent s'authentifier l'un l'autre.

L'implémentation IKE d'Oracle Solaris prend en charge divers types de clé, y compris les clés pré-partagées et les certificats. Par souci de simplicité, cet exemple utilise des clés pré-partagées qui sont stockées dans le fichier /`etc/inet/secret/ike.preshared`. Cependant, les organisations peuvent utiliser des modes d'authentification plus puissants, le cas échéant.

Modifiez le fichier /etc/inet/secret/ike.preshared et entrez les informations de clé pré-partagée. Par exemple :

```
{
localidtype IP
localid 10.1.1.1
remoteid type IP
key "This is an ASCII phrAz, use strOng p@sswords"
}
```

6. Activez les services IPsec et IKE sur les deux pairs.

Les services doivent être activés sur les pairs communicants pour que la communication chiffrée soit possible.

Exemple :

```
# svcadm enable svc:/network/ipsec/policy:default
# svcadm enable svc:/network/ipsec/ike:default
```

Contrôle de l'accès

Ces rubriques décrivent les fonctions de contrôle d'accès disponibles dans le système MiniCluster :

▼ Modification des mots de passe `root` par défaut d'Oracle ILOM

Le système est livré avec des mots de passe par défaut affectés aux comptes root Oracle ILOM sur les deux noeuds. La procédure d'installation peut ainsi être exécutée avec un compte d'accès initial prédéfini. Immédiatement après l'installation, modifiez les mots de passe par défaut pour garantir une sécurité optimale.

1. **Connectez-vous à Oracle ILOM sur le noeud 1 en tant que `root`.**

   Exécutez la commande `ssh` pour vous connecter à Oracle ILOM.

   Pour obtenir les noms d'hôte Oracle ILOM, dans la BUI sélectionnez System Settings -> System Information. Les noms d'hôte sont affichés sous la colonne ILOM.

   Syntaxe :

   ```
   % ssh root@node1_ILOM_hostname_or_IPaddress
   ```

Entrez le mot de passe root Oracle ILOM par défaut : welcome1

2. **Modifiez le mot de passe `root` Oracle ILOM.**

```
-> set /SP/users/root password
Enter new password: *********
Enter new password again: **********
```

3. **Répétez ces étapes pour modifier le mot de passe `root` Oracle ILOM sur le noeud 2.**

4. **Mettez à jour Oracle Engineered Systems Hardware Manager avec les nouveaux mots de passe.**

   Reportez-vous à la section "Mise à jour des mots de passe des composants" du manuel *Guide d'administration d'Oracle MiniCluster S7-2*.

Configuration des mots de passe EEPROM

Chaque noeud MiniCluster dispose d'un EEPROM, parfois appelé OpenBoot PROM, un microprogramme de bas niveau qui contient certains paramètres de configuration et des pilotes qui facilitent le démarrage du système. Le mot de passe EEPROM est désactivé par défaut.

Dans les environnements sécurisés, utilisez cette procédure pour activer et définir le mot de passe. Le mot de passe est automatiquement activé et appliqué aux deux noeuds.

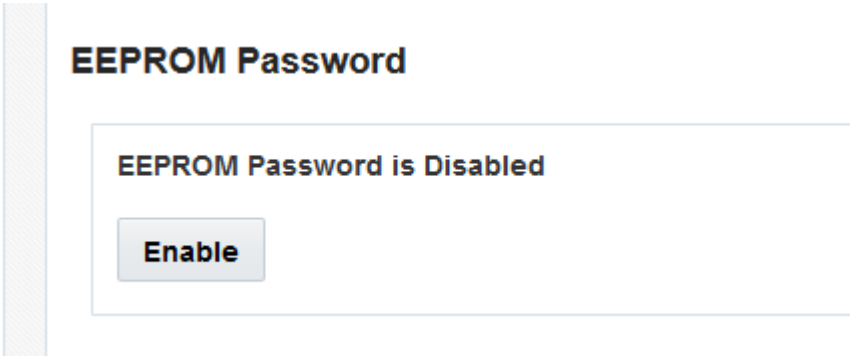
Cette procédure remplace les méthodes plus anciennes à l'aide desquelles le mot de passe était défini soit avec l'invite de commande `ok` d'OpenBoot, soit dans Oracle Solaris avec la commande `eeprom`.

Attention - Il est important de ne pas oublier le mot de passe. Si vous oubliez le mot de passe, vous devez appeler les services d'assistance pour que votre système puisse à nouveau être amorçable.

Remarque - Cette procédure décrit comment définir les mots de passe avec la BUI MCMU. Autrement, vous pouvez utiliser la commande `mcmu security -e`.

1. **Connectez-vous à MCMU en tant qu'administrateur principal, tel que `mcinstall`.**

2. **Dans le panneau de navigation, sélectionnez System Settings -> Security**



3. **Procédez à l'une des actions suivantes :**

   - Pour activer et définir le mot de passe, cliquez sur Activer, entrez deux fois le mot de passe et cliquez sur Définir le mot de passe.
   - Pour désactiver cette fonctionnalité, cliquez sur Désactiver, puis sur Confirmer.
   - Pour modifier un mot de passe existant, cliquez sur Modifier le mot de passe, entrez deux fois le nouveau mot de passe, puis cliquez sur Mettre à jour.

Provisionnement des utilisateurs

Lors de l'installation du système MiniCluster, vous devez créer et enregistrer le premier utilisateur MCMU appelé `mcinstall`. Les informations sur l'utilisateur, notamment l'adresse électronique et le numéro de téléphone sont collectées. L'utilisateur `mcinstall` est le premier compte administrateur principal. Lors de la première connexion `mcinstall`, l'utilitaire requiert que `mcinstall` crée un nouveau mot de passe respectant les stratégies de mot de passe Oracle Solaris associées au profil de sécurité.

Pendant l'enregistrement de l'utilisateur `mcinstall`, vous devez indiquer le nom de la personne qui servira de superviseur MCMU. Le superviseur n'est identifié que par un nom et une adresse électronique. Le superviseur n'est pas un utilisateur MCMU et n'a pas d'informations d'identification de connexion.

Les utilisateurs superviseur et mcinstall sont associés à des noms et des adresses électroniques de personnes réelles.

Quand de nouveaux utilisateurs MCMU sont provisionnés, chaque compte utilisateur est affecté à un rôle d'administrateur principal ou d'administrateur secondaire (voir "Contrôle d'accès

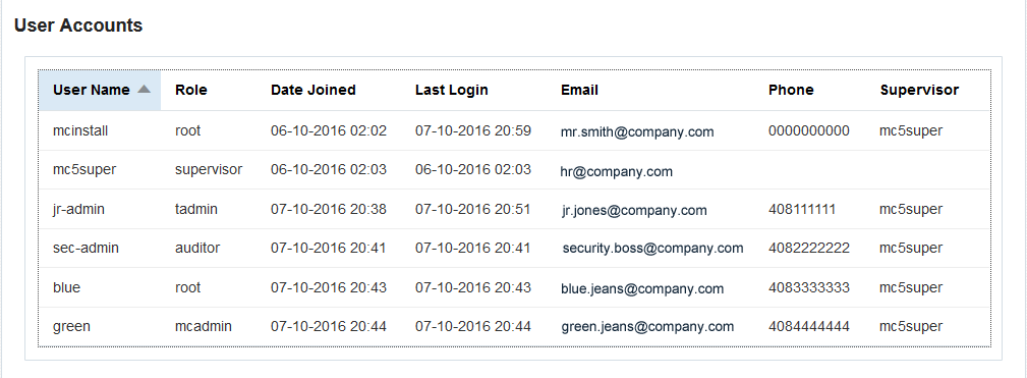
basé sur les rôles " à la page 31). Pour que le nouveau compte soit activé, l'utilisateur `mcinstall` et le superviseur doivent tous les deux approuver le nouveau compte utilisateur au moyen d'une URL qu'ils reçoivent par e-mail (voir "Processus d'approbation utilisateur MCMU" à la page 30). A la première connexion, l'utilisateur doit définir un mot de passe respectant les stratégies de mot de passe MCMU. Reportez-vous à la section "Stratégies de mot de passe et authentification utilisateur" à la page 33.

Processus d'approbation utilisateur MCMU

Tous les comptes utilisateur MCMU requièrent une approbation par deux personnes, soit le superviseur et l'administrateur principal MCMU. Le processus est le suivant :

1. L'utilisateur potentiel (ou un administrateur MCMU agissant pour son compte) accède à la page d'enregistrement MCMU et fournit les détails obligatoires suivants :
   - Nom d'utilisateur MCMU
   - Adresse électronique
   - Nom complet
   - Numéro de téléphone
   - Rôle MCMU
2. MCMU envoie au superviseur et à l'administrateur principal MCMU un e-mail demandant l'approbation ou le refus. L'e-mail inclut une URL vers la fonction d'approbation/de refus MCMU ainsi qu'un identifiant de clé unique.
3. Quand le superviseur et l'administrateur principal approuvent tous les deux le compte, le compte utilisateur est activé et MCMU envoie au nouvel utilisateur un e-mail confirmant l'activation du compte. L'utilisateur reçoit un compte MCMU accessible au moyen de la BUI ou de la CLI MCMU. L'utilisateur reçoit également un compte Oracle Solaris. Si l'utilisateur existe dans un LDAP d'entreprise et que le système MiniCluster est configuré avec un client LDAP, l'utilisateur peut uniquement utiliser LDAP pour le compte Oracle Solaris.

Tous les utilisateurs enregistrés sont stockés dans le référentiel MCMU. Un administrateur MCMU peut vérifier les utilisateurs, notamment leurs rôles et le superviseur en affichant MCMU System Settings -> User Accounts. Exemple :



User Accounts

User Name	Role	Date Joined	Last Login	Email	Phone	Supervisor
mcinstall	root	06-10-2016 02:02	07-10-2016 20:59	mr.smith@company.com	0000000000	mc5super
mc5super	supervisor	06-10-2016 02:03	06-10-2016 02:03	hr@company.com		
jr-admin	tadmin	07-10-2016 20:38	07-10-2016 20:51	jr.jones@company.com	408111111	mc5super
sec-admin	auditor	07-10-2016 20:41	07-10-2016 20:41	security.boss@company.com	4082222222	mc5super
blue	root	07-10-2016 20:43	07-10-2016 20:43	blue.jeans@company.com	4083333333	mc5super
green	mcadmin	07-10-2016 20:44	07-10-2016 20:44	green.jeans@company.com	4084444444	mc5super

Les rubriques suivantes de cette section décrivent comment effectuer ces tâches.

Contrôle d'accès basé sur les rôles

Il n'y a pas d'utilisateur `root` dans le système MiniCluster. A la place, root est un rôle qui est affecté aux utilisateurs MCMU enregistrés comme administrateurs principaux.

Lorsque vous créez un utilisateur MCMU, vous affectez à l'utilisateur un des rôles suivants :

- **Rôle d'administrateur principal (rôle `root`)** : Le rôle `root` définit les droits et les privilèges des administrateurs principaux du système MiniCluster, dont l'ensemble de ses noeuds de calcul, réseaux, base de données et stockage. Les utilisateurs dotés du rôle `root` peuvent effectuer toutes les opérations d'installation et d'administration clés sans aucune contrainte. En tant qu'administrateurs principaux, ils peuvent déléguer des opérations et approuver l'ajout et la suppression d'utilisateurs, y compris des nouveaux administrateurs principaux et secondaires. L'utilisateur doit se connecter avec ses propres données d'identification. Toutes les actions et opérations effectuées sont journalisées et auditées en fonction de l'identifiant de l'utilisateur et pas de l'identifiant du rôle.
- **Rôle d'administrateur secondaire (rôle `mcadmin`)** : Ce rôle définit les droits et les privilèges des administrateurs secondaires sur les domaines et zones non globales du système MiniCluster. Ce rôle n'active par défaut que l'accès en lecture seule au MCMU. Toutes les actions et opérations effectuées sont journalisées et auditées en fonction de l'identifiant de l'utilisateur et pas de l'identifiant du rôle.
- **Rôle d'administrateur locataire (rôle `tadmin`)** : Ce rôle définit les droits et les privilèges des administrateurs d'une machine virtuelle du système MiniCluster. Ce rôle définit les droits et les privilèges d'un administrateur de machine virtuelle impliqué dans les opérations administratives quotidiennes prenant en charge les installations et le déploiement des applications. Toutes les actions sont auditées en fonction de l'identifiant de l'utilisateur et pas de l'identifiant du rôle.

- **Auditeur (**rôle `auditor`**)** : les utilisateurs qui occupent ce rôle n'ont accès qu'à la page d'examen d'audit de la BUI MCMU, où ils peuvent consulter le statut de pool d'audits et générer des rapports d'activité des utilisateurs. Seuls les utilisateurs qui occupent ce rôle peuvent accéder à la page d'examen d'audit. Les auditeurs ne peuvent pas accéder au MCMU (hormis la page d'audit) et ne peuvent pas se connecter aux zones ou aux VM du noyau.

Comptes utilisateur

Le système MiniCluster inclut les comptes utilisateur répertoriés dans le tableau suivant.

Utilisateur	Mot de passe	Rôle	Description
`mcinstall`	Le mot de passe est configuré lors de l'installation. Il peut être réinitialisé et modifié au moyen du MCMU.	`root`	Le processus d'installation vous demande de créer `mcinstall` en tant qu'administrateur MCMU principal et de créer un mot de passe. Ce compte est conçu pour être celui de l'administrateur principal de MCMU. Ce compte utilisateur est utilisé pour les activités suivantes : ■ Initialisation du système au moment de l'installation en exécutant `installmc`. ■ Administration du système, y compris les VM, avec la BUI MCMU et la CLI `mcmu`. ■ Pour prendre le rôle `root` (`su` pour root) sur les machines virtuelles de l'application et dans la zone globale et les zones de noyau pour des privilèges superutilisateur.
Superviseur MCMU : Nom du compte déterminé au moment de l'installation.	N/A	N/A	Dans le logiciel MiniCluster, l'utilisateur superviseur n'est identifié que par un nom et une adresse électronique. Il n'a pas d'informations d'identification de connexion. Vous pouvez utiliser ce compte pour fournir un second niveau dans le processus d'approbation utilisateur MCMU. Cet utilisateur reçoit un e-mail chaque fois qu'un utilisateur MCMU est créé. Le nouvel utilisateur doit être approuvé par le superviseur et l'administrateur principal pour que son compte soit activé. Vous pouvez utiliser ce compte pour fournir une seconde couche dans le processus d'approbation utilisateur MCMU en affectant une personne autre que l'administrateur principal en tant que superviseur.
(Facultatif) *Administrateur locataire* : nom du compte déterminé au moment de l'enregistrement utilisateur.	Déterminé au moment de la connexion initiale.	`tadmin`	Cet utilisateur peut effectuer toutes les tâches postérieures à l'installation uniquement sur les VM. Cet utilisateur ne peut pas accéder aux zones globales ou de noyau, et ne peut pas exécuter la BUI ou la CLI MCMU.
(Facultatif) *Administrateur secondaire* : Nom du compte déterminé au	Déterminé au moment de la connexion initiale.	`mcadmin`	Lorsqu'un utilisateur MCMU est créé en tant qu'administrateur secondaire et dispose d'un accès en lecture seule aux zones non globales.

Utilisateur	Mot de passe	Rôle	Description
moment de l'enregistrement utilisateur.			
`oracle`	Le mot de passe est identique au mot de passe pour `mcinstall`.	`root`	Ce compte utilisateur est utilisé pour les activités suivantes : ■ Utilisé comme compte de connexion initial aux machines virtuelles de base de données, à partir duquel vous pouvez configurer les machines virtuelles de base de données avec une base de données, des données et d'autres comptes, le cas échéant. ■ Pour prendre le rôle root (`su` pour root) sur les machines virtuelles de la base de données pour des privilèges superutilisateur.

Le mot de passe MCMU par défaut utilisé lors de la première connexion est `welcome1`. Une fois `welcome1` entré, l'utilitaire oblige l'utilisateur à créer un nouveau mot de passe conforme aux stratégies de mot de passe. Reportez-vous à la section "Stratégies de mot de passe et authentification utilisateur" à la page 33.

Toutes les actions effectuées par tous les utilisateurs MCMU sont journalisées en fonction de l'identifiant de l'utilisateur. Pour obtenir des informations sur les rapports d'audit, reportez-vous à la section "Rapports d'audit et de conformité" à la page 39.

Remarque - Les comptes utilisateur MCMU ne servent pas à l'utilisation quotidienne du système, notamment l'exploitation des applications et bases de données. Ces comptes utilisateur sont gérés via Oracle Solaris, l'application, la base de données sur les machines virtuelles et au moyen des services de nom de votre site.

Stratégies de mot de passe et authentification utilisateur

Tous les utilisateurs provisionnés dans le système MiniCluster se voient affecter un rôle avec des stratégies de mot de passe strictes et un chiffrement de mot de passe appliqué par le profil de sécurité.

La stratégie de sécurité par défaut établit les exigences de mot de passe MCMU suivantes :

- Le mot de passe doit contenir au moins 14 caractères.
- Le mot de passe doit contenir au moins un caractère numérique.
- Le mot de passe doit contenir au moins un caractère alphanumérique en majuscule.
- Le nouveau mot de passe doit comporter au moins trois caractères différents de l'ancien mot de passe.
- Le mot de passe ne doit correspondre à aucun des dix mots de passe précédents.

Tous les utilisateurs doivent se connecter à leur compte Oracle Solaris à l'aide de leur propre mot de passe.

▼ Vérification des rôles utilisateur Oracle Solaris

1. **Connectez-vous à la zone globale du système MiniCluster et prenez le rôle root.**
   Pour plus de détails, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*.

2. **Vérifiez la liste des rôles disponibles.**

```
# logins -r
```

3. **Vérifiez le rôle utilisateur et le mot de passe requis pour l'authentification :**

```
# grep root /etc/user_attr
root::::audit_flags=lo\:no;type=role;roleauth=user
mcinstall::::auths=solaris.system.maintenance;roles=root
```

Suppression sécurisée des machines virtuelles

Seul l'administrateur principal MCMU peut supprimer des machines virtuelles et des groupes de machines virtuelles. Quand un composant de machine virtuelle est supprimé, les clés correspondantes sont automatiquement supprimées et un e-mail est envoyé à l'administrateur principal.

Pour vérifier cette fonction, avant de supprimer un composant de machine virtuelle, connectez-vous à la BUI MCMU en tant qu'administrateur principal et affichez les clés de chiffrement (System Settings -> Security). Supprimez le composant de machine virtuelle et affichez de nouveau les clés. La machine virtuelle et le libellé de clé associé pour le composant supprimé ne s'affichent plus.

▼ Vérification des règles de pare-feu basées sur l'hôte

Tous les environnements de calcul, y compris les zones globales, les zones de noyau et les zones non globales sont configurées automatiquement avec des pare-feu IP Filter. Aucune intervention manuelle n'est requise.

Pour vérifier qu'IP Filter est actif, procédez comme suit.

1. **Connectez-vous à la zone globale sur le noeud 1 en tant qu'utilisateur `mcinstall` et prenez le rôle `root`.**
   Pour obtenir des instructions sur la connexion à Oracle ILOM, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: ***************
```

```
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. Vérifiez la configuration IP Filter.

Assurez-vous que les règles du fichier `/etc/ipf/ipf.conf` correspondent à la sortie d'écran suivante.

```
# cat /etc/ipf/ipf.conf
block in log on all
block out log on ipmppub0 all
pass in quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 22 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 111 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 443 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1159 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 1158 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port 5499 >< 5550 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 4900 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1522 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 1523 flags S keep state
pass in quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp from any to any port = 2049 flags S keep state
pass out quick on ipmppub0 proto tcp/udp from any to any port = domain keep state
pass in quick on ipmppub0 proto icmp icmp-type echo keep state
pass out quick on ipmppub0 proto icmp icmp-type echo keep state
pass in quick on ipmppub0 proto udp from any to any port = 123 keep state
pass out quick on ipmppub0 proto udp from any to any port = 123 keep state
block return-icmp in proto udp all
```

3. Vérifiez que tous les services IPF sont en ligne.

```
# svcs | grep svc:/network/ipfilter:default
online         22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:            in 0    out 0
 IPv6 packets:          in 0 out 0
 input packets:         blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:         blocked 0 passed 596143 nomatch 595516 counted 0 short 0
 input packets logged:  blocked 0 passed 0
output packets logged:  blocked 0 passed 0
 packets logged:        input 0 output 0
 log failures:          input 0 output 0
fragment state(in):     kept 0  lost 0  not fragmented 0
fragment reassembly(in):        bad v6 hdr 0     bad v6 ehdr 0  failed reassembly 0
fragment state(out):    kept 0  lost 0  not fragmented 0
packet state(in):       kept 0  lost 0
packet state(out):      kept 0  lost 0
ICMP replies:   0       TCP RSTs sent:  0
Invalid source(in):     0
Result cache hits(in):  0       (out):  0
IN Pullups succeeded:   0       failed: 3462
OUT Pullups succeeded:  0       failed: 0
Fastroute successes:    0       failures:       0
TCP cksum fails(in):    0       (out):  0
IPF Ticks:      92894
Packet log flags set: (0)
        none
```

4. **Veillez à ce que vos bases de données et applications soient accessibles sans modification des règles de pare-feu.**

Vérification de l'environnement Verified Boot

Oracle Solaris Verified Boot est une fonction antimalware qui permet de réduire les risques d'introduction de composants du noyau ou d'initialisation essentiels modifiés par accident ou de manière malveillante. Cette fonction vérifie les signatures cryptographiques du microprogramme, du système d'initialisation et du noyau.

Par défaut, les zones globales du système MiniCluster sont configurées avec Oracle Solaris Verified Boot. Pour vérifier que le système est configuré avec Verified Boot, procédez comme suit.

1. **Connectez-vous à Oracle ILOM sur l'un des noeuds.**

   Pour obtenir des instructions sur la connexion à Oracle ILOM, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*.

2. **Vérifiez la configuration Verified Boot dans Oracle ILOM.**

   Assurez-vous que `boot_policy` est défini sur `warning`.

```
-> show /HOST/verified_boot

 /HOST/verified_boot
    Targets:
        system_certs
        user_certs

    Properties:
        boot_policy = warning

    Commands:
        cd
        show
```

3. **Vérifiez le paramètre de la stratégie Verified Boot.**

   Assurez-vous que `module_policy` est défini sur `enforce`.

```
-> show /HOST/verified_boot module_policy

  /HOST/verified_boot
    Properties:
        module_policy = enforce
```

4. **Démarrez la console hôte pour accéder à la zone globale.**

   Connectez-vous en tant qu'utilisateur `mcinstall`.

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

Serial console started.  To stop, type #.
```

```
Minicluster Setup successfully configured
mc4-n1 console login: mcinstall
Password: **************
Last login: Tue Jun 28 10:17:38 2016 on rad/47
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall %
```

5. **Vérifiez la zone globale pour vous assurer que le système s'est initialisé dans une configuration Verified Boot.**

   Vérifiez dans le fichier des `messages` la présence de la chaîne `NOTICE: Verified boot enabled; policy=warning`.

```
mcinstall % cat /var/adm/messages | grep Verified
Jun 29 11:39:15 mc4-n1 unix: [ID 402689 kern.info] NOTICE: Verified boot enabled;
 policy=warning
```

Restriction de l'accès au stockage partagé

MiniCluster comprend une unité de stockage qui combine disques SSD et HDD. Les unités de disque dur peuvent être configurées pour fournir le stockage partagé aux machines virtuelles.

MiniCluster comprend une fonctionnalité d'isolement de stockage partagé sous la forme d'un commutateur qui permet d'isoler un stockage partagé qui ne s'applique qu'aux zones globales et de noyau. Cela permet d'isoler un groupe de VM de sécurité et de conformité pour l'empêcher de partager des fichiers avec les zones globales et de noyau. Cela permet de garantir que les groupes de VM ne sont plus attachés aux montages NFS, et que les services NFS sont désactivés.

Pour des environnements hautement sécurisés, n'activez pas le stockage partagé pour les machines virtuelles de base de données et les machines virtuelles d'application. Si le stockage partagé est activé, le système de fichiers doit être accessible pour les machines virtuelles en lecture seule. Pour obtenir des instructions sur la façon d'activer ou de désactiver le stockage partagé, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2* disponible sur `http://docs.oracle.com/cd/E69469_01`.

Le répertoire `/sharedstore` est le point de montage du stockage partagé :

- **Selon vos besoins de sécurité, configurez le stockage partagé en tenant compte des recommandations suivantes :**

  - Assurez-vous que le stockage partagé n'est pas disponible pour les machines virtuelles de base de données et les machines virtuelles d'application, ou qu'il est en lecture seule.
  - Dans les déploiements de production, assurez-vous que les deux zones de noyau ne sont pas disponibles sur les réseaux publics et qu'ils ne sont pas directement accessibles par le client. Tous les accès directs et l'utilisation des services de stockage partagé à partir des réseaux publics ou de l'accès client doivent être interrompus. Si les machines virtuelles requièrent

l'accès au système de fichiers `/sharedstore` via NFS, assurez-vous qu'il est donné au moyen de canaux IPSEc/IKE.

Rapports d'audit et de conformité

Ces rubriques décrivent les fonctions de rapport d'audit et de conformité disponibles dans le système MiniCluster :

▼ Vérification des stratégies d'audit

La stratégie d'audit est configurée lors de l'installation des zones globales et non globales à la sélection d'un profil de conformité (équivalent CIS ou PCI-DSS par défaut).

Pour vérifier que les stratégies d'audit sont activées, procédez comme suit.

1. **Connectez-vous à la zone globale en tant qu'utilisateur `mcinstall` et prenez le rôle `root`.**

   Pour obtenir des instructions sur la connexion à Oracle ILOM, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: **************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: **************
#
```

2. **Assurez-vous que le service d'audit est en ligne.**

```
# svcs | grep svc:/system/auditd
online         22:14:37 svc:/system/auditd:default
```

3. **Vérifiez que le plug-in d'audit est actif.**

```
# auditconfig -getplugin audit_binfile
Plugin: audit_binfile (active)
        Attributes: p_age=0h;p_dir=/var/audit;p_fsize=0;p_minfree=1
```

4. **Vérifiez les stratégies d'audit actives.**

```
# auditconfig -getpolicy
configured audit policies = argv,cnt,perzone,zonename
active audit policies = argv,cnt,perzone,zonename
```

5. **Vérifiez que tous les rôles sont présents pour la stratégie d'audit `cusa`.**

```
# userattr audit_flags root
cusa:no
# userattr audit_flags mcadmin
fw,fc,fd,ps,lo,ex,ua,as,cusa:no
```

▼ Vérification des journaux d'audit

1. **Connectez-vous à la zone globale en tant qu'utilisateur `mcinstall` et prenez le rôle `root`.**

   Pour obtenir des instructions sur la connexion à Oracle ILOM, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*.

```
% ssh mcinstall@mc4-n1
Password: ***************
Last login: Tue Jun 28 10:47:38 2016 on rad/59
Oracle Corporation      SunOS 5.11      11.3    June 2016
Minicluster Setup successfully configured
Unauthorized modification of this system configuration strictly prohibited
mcinstall@mc4-n1:/var/home/mcinstall % su root
Password: ***************
#
```

2. **Exécutez la commande `auditreduce`, comme indiqué ci-dessous.**

   Voici la syntaxe pour consulter les journaux d'audit :

   `auditreduce -z` *vm_name audit_file_name* `| praudit -s`

```
# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce  -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
```

```
file,2016-06-27 23:02:30.000 -07:00,
```

Générer un rapport d'audit

Utilisez cette procédure pour générer des rapports d'audit pour un noeud, des VM individuelles et des zones globales.

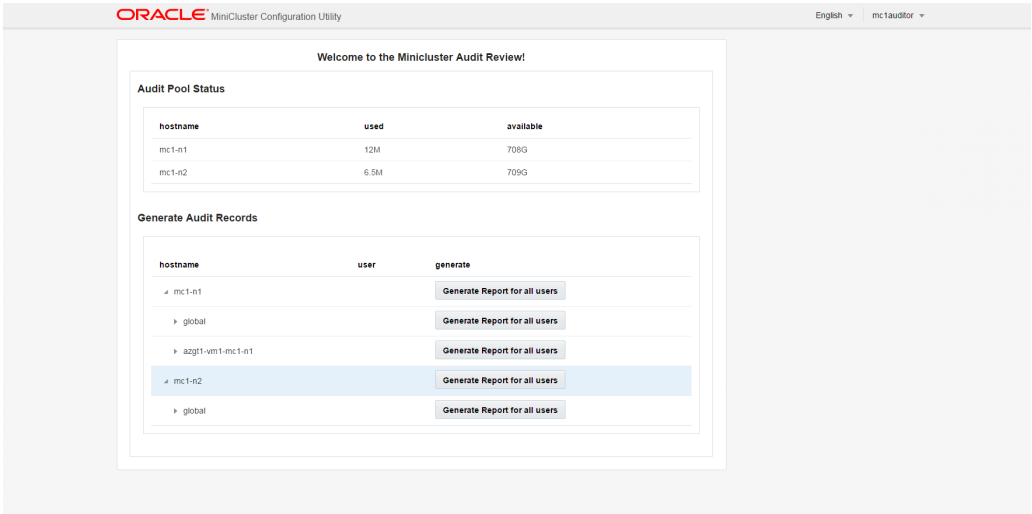
1. **Connectez-vous à MCMU en tant qu'utilisateur qui occupe un rôle d'auditeur.**

   Pour obtenir des informations sur les utilisateurs et les rôles MCMU, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*, disponible sur `http://docs.oracle.com/cd/E69469_01`.

2. **Dans le panneau de navigation, sélectionnez System Settings -> Security.**

   La page Examen d'audit s'affiche.

   Remarque - Seuls les utilisateurs MCMU qui occupent un rôle d'auditeur peuvent afficher cette page.



3. **Consultez la section Statut de pool d'audits.**

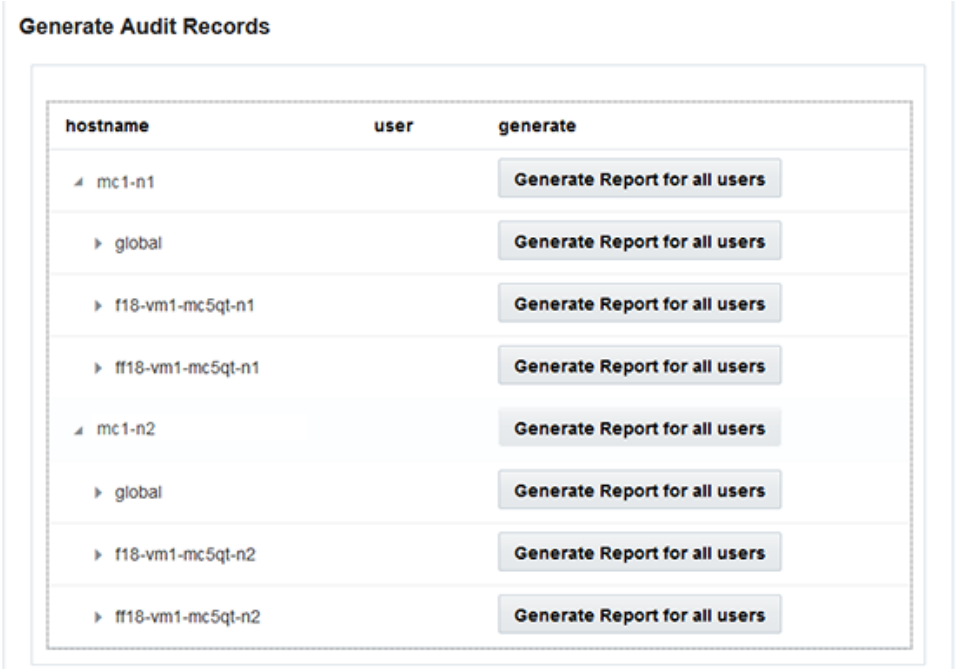
   Cette section répertorie la quantité d'espace utilisée et d'espace disponible pour les pools d'audit sur chaque noeud.

4. **Pour générer un rapport concernant le noeud entier, cliquez sur le bouton Générer de l'un des noeuds, puis allez à Étape 6**

Sinon, vous pouvez générer un rapport concernant une VM ou une zone spécifique. Reportez-vous à la section Étape 5

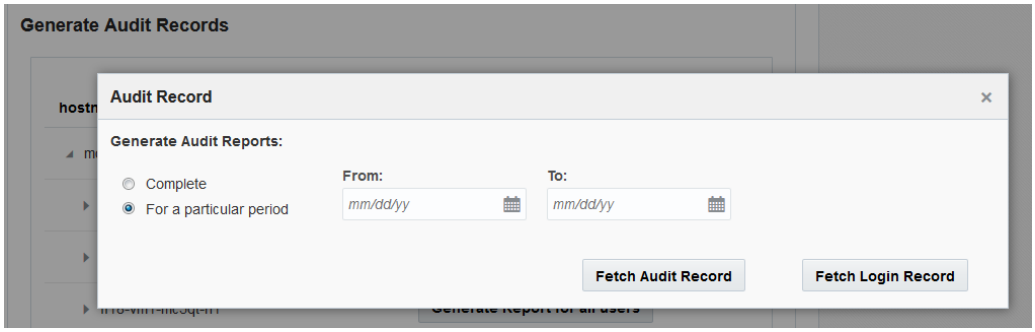
5. **Pour générer un rapport concernant une VM spécifique ou une zone globale, procédez comme suit.**

   a. **Cliquez sur le triangle situé à côté du noeud pour développer son contenu.**



   b. **Pour la VM ou la zone globale, cliquez sur Générer le rapport pour tous les utilisateurs.**

6. **Dans la boîte de dialogue d'enregistrement d'audit, configurez les paramètres d'enregistrement d'audit.**



Vos choix sont les suivants :

- **Complet** : génère un rapport qui inclut tous les enregistrements d'audit.
- **Pour une période donnée** : spécifiez une période précise en entrant une date de début et une date de fin.

7. **Cliquez sur l'un des boutons d'extraction.**
   Vos choix sont les suivants :

   - **Extraire l'enregistrement d'audit** : génère un enregistrement d'audit complet.
   - **Extraire l'enregistrement de connexion** : extrait les activités de l'utilisateur, telles que les connexions, les déconnexions et d'autres actions.

8. **Cliquez sur le bouton Cliquez ici, puis téléchargez le fichier XML.**
   Le fichier XML peut être importé dans les applications d'analyse d'audit, telles qu'Oracle Audit Vault.

9. **Cliquez sur Fermer.**

(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 décrite dans le *Guide de sécurité d'Oracle ILOM* à la section intitulée "Fonctions non prises en charge lorsque le mode FIPS est activé".

Reportez-vous également à la section "Conformité FIPS-140-2 de niveau 1" à la page 45.

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 du site à Oracle ILOM. Pour les systèmes dont la configuration a fait l'objet de modifications spécifiques du 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.**

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
```

Conformité FIPS-140-2 de niveau 1

Les applications cryptographiques hébergées sur un système MiniCluster 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, ainsi que 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 43.

Ce tableau répertorie les algorithmes approuvés par FIPS qui sont pris en charge par Oracle Solaris sur MiniCluster.

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		

Clé ou CSP	Numéro de certificat	
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`.

Evaluation de la conformité de la sécurité

Ces rubriques décrivent la fonction de test de conformité de la sécurité du système MiniCluster :

Tests de conformité de la sécurité

Quand le système est installé, un profil de sécurité (PCI-DSS, équivalent CIS et DISA-STiG) est sélectionné et le système est automatiquement configuré pour satisfaire ce profil de sécurité. Pour garantir que le système continue de fonctionner conformément aux profils de sécurité, le MCMU permet d'exécuter des tests de conformité de la sécurité et d'accéder aux rapports y afférents. Vous pouvez administrer les tests de conformité de la sécurité à l'aide de la BUI MCMU et de la CLI.

L'exécution des tests de conformité de la sécurité offre les avantages suivants :

- Elle vous permet d'évaluer l'état de sécurité actuel des machines virtuelles d'application et de base de données.
- Les tests d'évaluation de conformité de la sécurité prennent en charge les normes PCI-DSS, équivalent CIS (par défaut) et DISA-STiG en fonction du niveau de sécurité configuré lors de l'installation.
- Ces tests s'exécutent automatiquement quand le système est initialisé et peuvent être lancés à la demande ou selon des intervalles planifiés.
- A la disposition des administrateurs principaux du MCMU uniquement, les rapports et notes de conformité sont facilement accessibles depuis la BUI MCMU.
- Les rapports de conformité fournissent des recommandations de solution.

Remarque - Le profil DISA-STIG fait actuellement l'objet d'un examen. N'utilisez ce profil que pour effectuer des expériences dans des environnements de test.

Planification d'un test de conformité de la sécurité (BUI)

Utilisez la procédure ci-dessous pour planifier un test de conformité de la sécurité à l'aide de la BUI MCMU. Pour exécuter cette procédure à l'aide de la CLI MCMU, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2* afin d'obtenir des instructions.

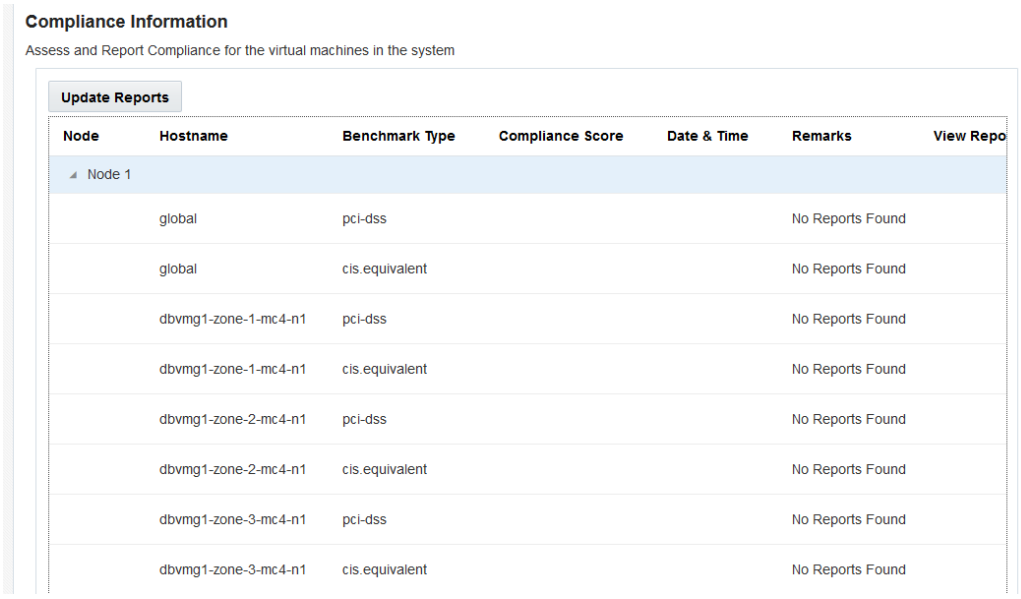
1. **Connectez-vous à la BUI MCMU en tant qu'administrateur principal.**

   Pour obtenir des instructions, reportez-vous au *Guide d'administration d'Oracle MiniCluster S7-2*

2. **Dans la page d'accueil, faites défiler l'écran vers le bas pour atteindre le panneau Compliance Information.**

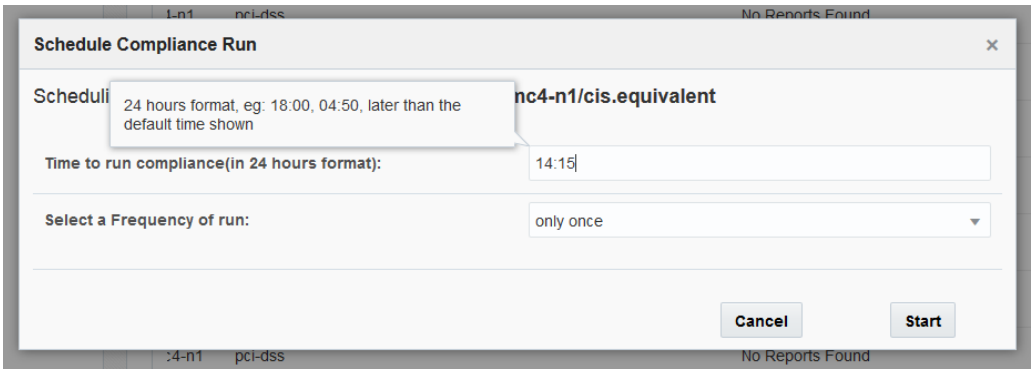
3. **Cliquez sur un noeud pour développer ses détails.**

   Chaque zone et chaque machine virtuelle ont été configurées avec un profil de sécurité (équivalent CIS ou PCI-DSS). Quand vous planifiez un test de conformité, sélectionnez un test correspondant au profil de sécurité du composant.



4. **Faites défiler l'écran vers la droite et cliquez sur le bouton Schedule en regard de l'une des machines virtuelles.**

La page Schedule Compliance Run s'affiche.



5. **Spécifiez l'heure et la fréquence et cliquez sur Start.**

   Une fois le test de conformité de la sécurité exécuté à l'heure planifiée, affichez le rapport. Reportez-vous à la section "Affichage des rapports de test de conformité (BUI)" à la page 49.

▼ Affichage des rapports de test de conformité (BUI)

Voici les résultats de test de conformité acceptables :

	Equivalent CIS	PCI-DSS
Zones globales	approx. 88%	approx. 88%
Machines virtuelles	approx. 90%	approx. 93%

Voici les échecs de test de conformité connus en raison de problèmes Oracle Solaris :

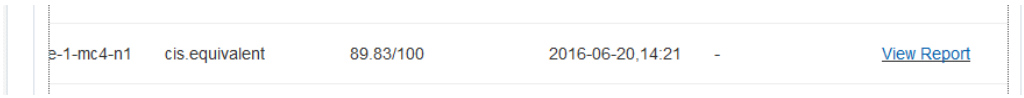
- Intégrité de package (système d'exploitation principal, rad-python)
- GDM
- Démon de routage
- Adresses loopback SSH – L'atténuation ne corrige pas le problème.
- Les services de noms ne reconnaissent pas DNS
- Client LDAP

Voici les échecs de test de conformité connus en raison de problèmes de configuration requis par le client MiniCluster :

- Services client NFS – La sélection de services doit être disponible.
- Définition du mot de passe eeprom – Paramètre facultatif.

1. **Connectez-vous à la BUI MCMU.**
2. **Dans la page d'accueil, faites défiler l'écran vers le bas pour atteindre le panneau Compliance Information.**
3. **Cliquez sur Update Reports.**

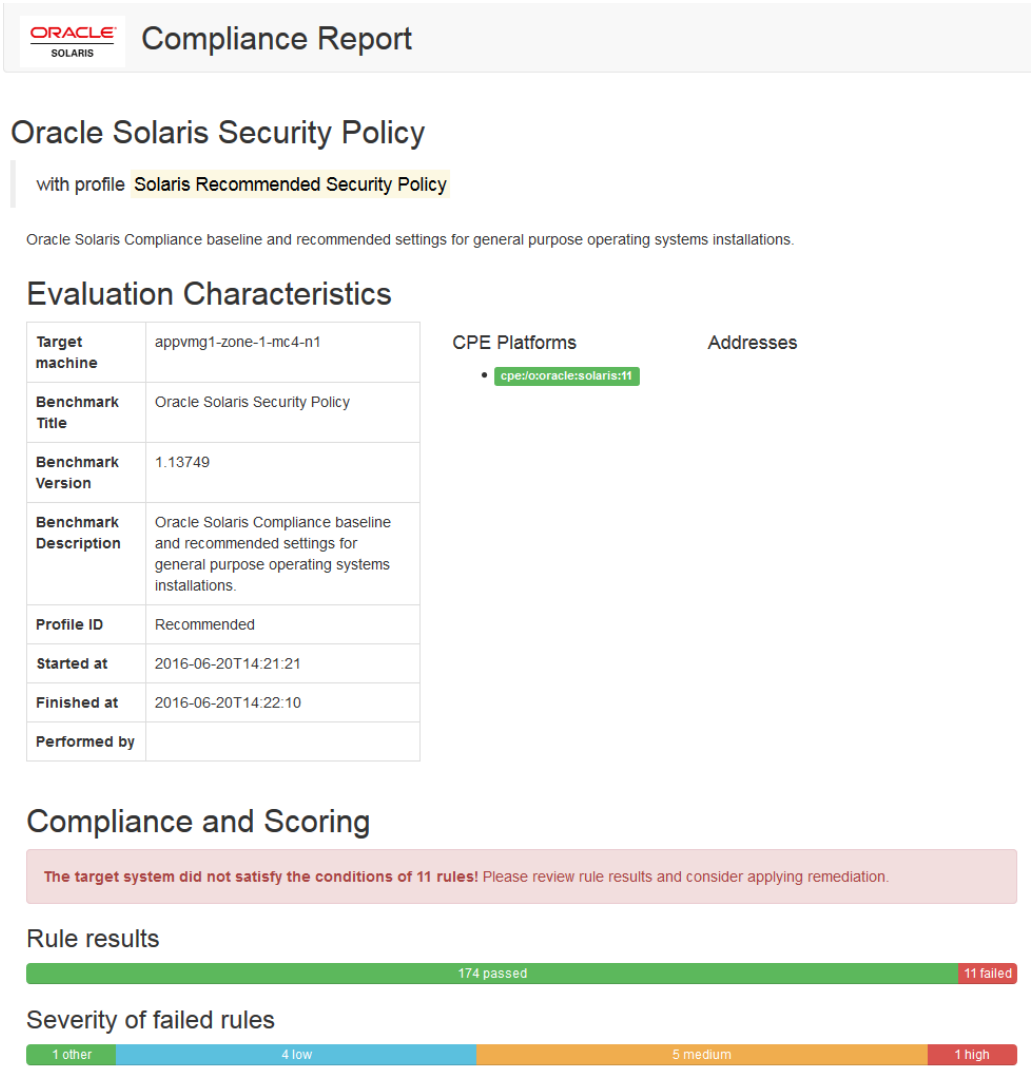
   La mise à jour dure environ une minute.
4. **Développez l'affichage du noeud et identifiez le rapport de conformité.**



5. **Faites défiler l'écran vers la droite et cliquez sur View Report.**

   Le rapport de test de conformité apparaît.

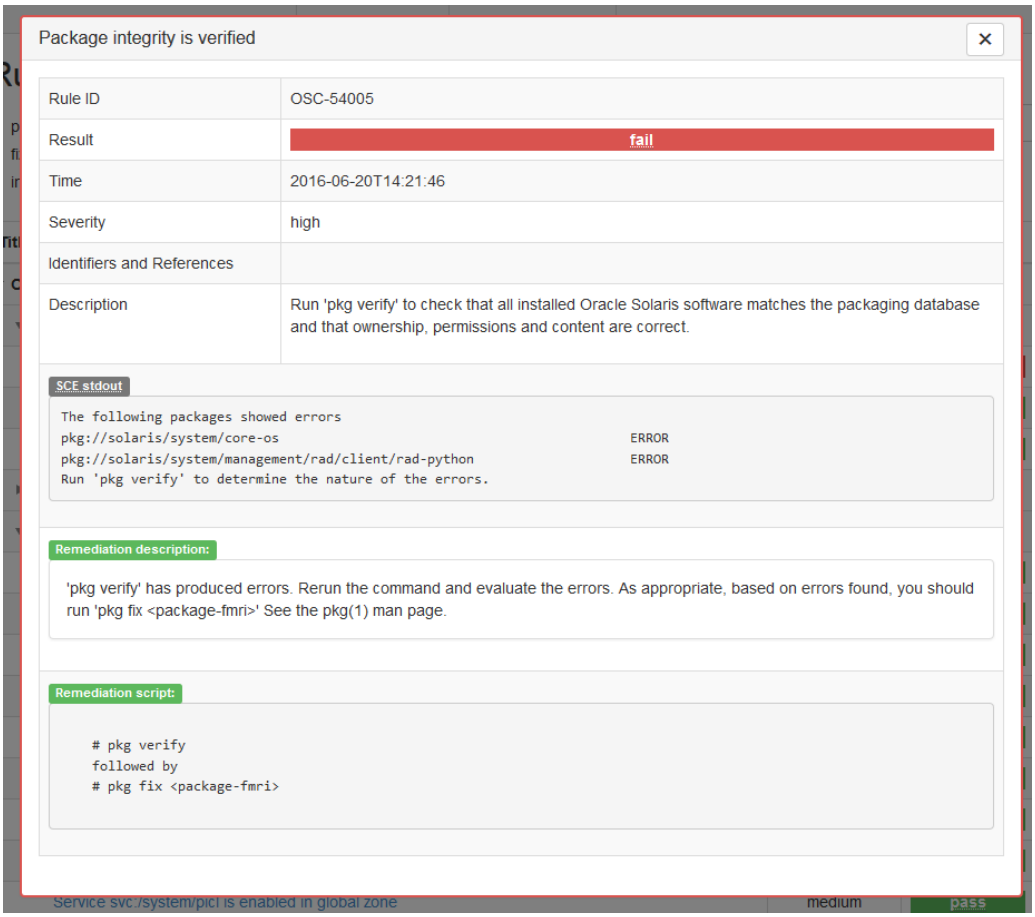
Sous Rule Overview, vous pouvez sélectionner les types de test à afficher en fonction de leurs résultats. Vous pouvez également spécifier une chaîne à rechercher dans le champ de recherche.



6. **En consultant le rapport, vous pouvez vérifier les contrôles de sécurité, les notes de conformité, les anomalies et les solutions.**

7. **Cliquez sur le nom d'un test pour obtenir des détails et des informations sur la solution recommandée.**

Remarque - Vous pouvez afficher tous les détails de tous les tests en cliquant sur Show all Result Details au bas du rapport.



Présentation des contrôles de sécurité du serveur SPARC S7-2

Ces rubriques présentent les contrôles de sécurité pour le matériel et l'environnement OpenBoot.

Présentation de la sécurité du matériel

L'isolement physique et le contrôle d'accès constituent la base de votre architecture de sécurité. Un serveur physique installé dans un environnement sécurisé est protégé contre tout accès non autorisé. De même, l'enregistrement de tous les numéros de série protège l'équipement contre les risques de vol, de revente ou au niveau de la chaîne logistique (autrement dit, le risque que des composants de contrefaçon soient intégrés à la chaîne logistique de votre organisation).

Les sections ci-après fournissent des recommandations générales concernant la sécurité matérielle du système MiniCluster.

Restrictions d'accès

- Installez les serveurs et les équipements connexes dans un local interdit d'accès et fermé à clé.
- Si le matériel est installé dans un rack dont la porte est dotée d'un verrou, verrouillez toujours celle-ci jusqu'à ce que vous deviez effectuer la maintenance des composants du rack. Le verrouillage des portes permet également de restreindre l'accès aux périphériques enfichables ou échangeables à chaud.

- Installez 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 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. L'accès physique constitue une méthode d'accès à un composant plus sécurisée dans la mesure où il ne risque aucune attaque réseau.
- Connectez la console à un périphérique KVM externe afin d'activer l'accès à la console à distance. Les périphériques KVM prennent souvent en charge une authentification à deux facteurs, un contrôle des accès centralisé et des procédures d'audit. Pour plus d'informations sur les recommandations en matière de sécurité et les bonnes pratiques relatives aux périphériques KVM, reportez-vous à la documentation fournie avec le périphérique KVM.

Numéros de série

- Conservez un enregistrement des numéros de série de tous les équipements.
- Apposez une marque de sécurité sur tous les éléments importants du matériel informatique, tels que les pièces de rechange. Utilisez des stylos à ultraviolet ou des étiquettes en relief.
- Conservez les clés d'activation et les licences matérielles dans un emplacement sécurisé auquel l'administrateur système peut facilement accéder en cas d'urgence. Les documents imprimés peuvent être votre seule preuve de propriété.

Les lecteurs d'identification par radiofréquence (RFID) peuvent simplifier davantage le suivi des ressources. Le livre blanc d'Oracle intitulé *How to Track Your Oracle Sun System Assets by Using RFID* est disponible à l'adresse :

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

Unités de disque dur

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

- Utilisez des outils d'effacement de disque tels que la commande Oracle Solaris `format` (1M) pour supprimer l'intégralité des données contenues dans l'unité de disque.

- 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

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

Restriction de l'accès à OpenBoot

Les rubriques suivantes décrivent comment limiter l'accès à l'invite OpenBoot.

Pour obtenir des instructions sur la façon de configurer un mot de passe pour OpenBoot, reportez-vous à la section "Configuration des mots de passe EEPROM" à la page 28.

- "Accès à l'invite OpenBoot" à la page 55
- "Vérification des échecs de connexion" à la page 56
- "Création d'un message relatif à la mise sous tension" à la page 56

Pour plus d'informations sur la configuration des variables de sécurité OpenBoot, reportez-vous à la documentation OpenBoot à l'adresse suivante :

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

▼ Accès à l'invite OpenBoot

Cette procédure explique comment accéder à l'invite OpenBoot sur les noeuds de calcul MiniCluster pour configurer les contrôles de sécurité.

Vous devez arrêter le système pour accéder à l'invite OpenBoot. Suivez les procédures appropriées pour arrêter les machines virtuelles proprement, comme décrit dans le *Guide d'administration d'Oracle MiniCluster S7-2*.

1. **Connectez-vous à Oracle ILOM sur un noeud et exécutez la commande suivante.**

```
-> set /HOST/bootmode script="setenv auto-boot? false
-> start /HOST/console
```

Connectez-vous à la console hôte en tant qu'utilisateur `mcinstall` et définissez la commande `su` sur `root`.

2. **Une fois toutes les machines virtuelles arrêtées, en tant que rôle root, arrêtez la zone globale.**

```
# init 0
```

```
.
.
.
{0} ok
```

Vérification des échecs de connexion

1. **Vous pouvez vérifier si un utilisateur a tenté de se connecter et n'a pas réussi à accéder à l'environnement OpenBoot en utilisant le paramètre `security-#badlogins`, comme dans l'exemple suivant.**

   ```
   {0} ok printenv security-#badlogins
   ```

   Si cette commande renvoie une valeur supérieure à zéro, cela signifie qu'une tentative d'accès à l'environnement OpenBoot a échoué.

2. **Réinitialisez le paramètre en tapant cette commande.**

   ```
   {0} ok setenv security-#badlogins 0
   ```

Création d'un message relatif à la mise sous tension

Bien qu'il ne serve pas de contrôle préventif ou de détection, un message peut être utilisé pour les raisons suivantes :

- Confirmer la propriété.
- Avertir les utilisateurs sur l'utilisation acceptable du serveur.
- Indiquer que l'accès ou les modifications apportées aux paramètres OpenBoot est restreint au personnel autorisé.

- **Utilisez les commandes suivantes pour activer un message d'avertissement personnalisé.**

  ```
  {0} ok setenv oem-banner banner-message
  {0} ok setenv oem-banner? true
  ```

  Le message peut comporter jusqu'à 68 caractères. Tous les caractères imprimables sont acceptés.

Index

M

N

O

P

R

S

T

U

V