Oracle® Key Manager 3

Guide de sécurité

Version 3.1

E52201-02

Avril 2016

ORACLE®

Oracle® Key Manager 3
Guide de sécurité

E52201-02

Table des matières

Liste des tableaux

Préface

Ce document décrit les fonctions de sécurité du système Oracle Key Manager 3 (OKM 3).

Public

Ce guide s'adresse à toute personne pouvant être amenée à utiliser les fonctions de sécurité et à effectuer des opérations d'installation et de configuration d'OKM 3.

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.

1

Chapitre 1. Présentation

Cette section contient une présentation du produit et explique les principes généraux de sécurité de l'application.

1.1. Présentation du produit

Oracle Key Manager (OKM) crée, stocke et gère des clés de chiffrement. Il contient les composants suivants :

- Key Management Appliance (KMA) – Boîte à sécurité renforcée qui propose des services de gestion des clés du cycle de vie, d'authentification, de contrôle d'accès et d'allocation de clés basés sur une stratégie. En tant qu'autorité de confiance pour les réseaux de stockage, le KMA garantit que tous les périphériques de stockage sont enregistrés et authentifiés et que toutes les créations, allocations et suppressions de clés de chiffrement sont en conformité avec les stratégies établies.
- GUI Oracle Key Manager – Interface utilisateur graphique qui s'exécute sur une station de travail et qui communique avec le KMA sur un réseau IP pour configurer et gérer l'OKM. L'interface utilisateur graphique d'Oracle Key Manager doit être installée sur une station de travail fournie par le client.
- CLI Oracle Key Manager – Deux interfaces de ligne de commande qui s'exécutent sur une station de travail et qui communiquent avec le KMA sur un réseau IP pour automatiser les opérations d'administration les plus fréquentes. Les CLI d'Oracle Key Manager doivent être installées sur une station de travail fournie par le client.
- Cluster OKM – Ensemble complet des KMA du système. Tous ces KMA ont conscience les uns des autres et répliquent mutuellement les informations.
- Agent – Périphérique ou logiciel qui effectue le chiffrement à l'aide de clés gérées par le cluster OKM. Un lecteur de bande de chiffrement StorageTek est un exemple d'agent. Les agents communiquent avec les KMA à l'aide du protocole d'agent KMS. L'API d'agent est un ensemble d'interfaces logicielles incorporées dans le matériel ou le logiciel de l'agent.

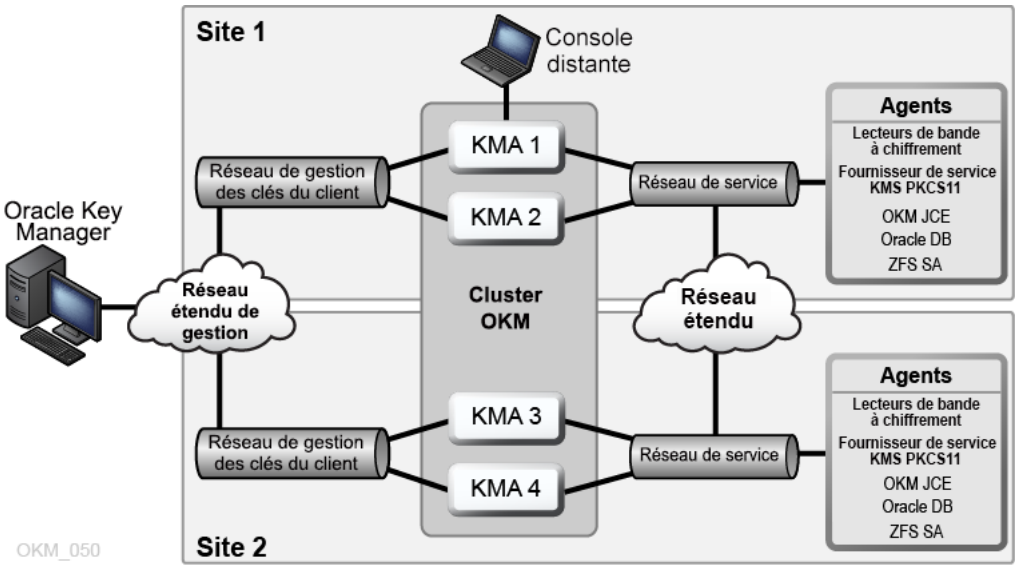
L'OKM utilise un réseau TCP/IP pour les connexions entre les KMA, les agents et les stations de travail où la GUI et les CLI d'Oracle Key Manager sont exécutées. Afin d'obtenir des connexions réseau flexibles, trois interfaces sont proposées pour les connexions réseau de chaque KMA :

- La connexion de gestion, destinée à la connexion au réseau du client
- La connexion de service, destinée à la connexion aux agents

- La connexion ILOM/ELOM, destinée à la connexion à ILOM ou ELOM sur le KMA

L'illustration suivante présente un exemple :

Figure 1.1.



1.2. Principes généraux de sécurité

Les principes suivants sont essentiels pour une utilisation sécurisée des applications.

1.2.1. Mise à jour du logiciel

L'un des principes fondamentaux d'une utilisation sécurisée est l'installation régulière des dernières versions et patches du logiciel. Les derniers packages de mise à niveau et programmes d'installation d'Oracle Key Manager sont disponibles sur le site Web My Oracle Support `http://support.oracle.com`.

1.2.2. Limitation de l'accès via le réseau aux services critiques

Conservez vos applications métier derrière un pare-feu. Le pare-feu vous permet d'être certain que l'accès à ces systèmes est limité à une route réseau définie, qui peut être surveillée et restreinte le cas échéant. Un routeur peut éventuellement remplacer plusieurs pare-feux indépendants.

1.2.3. Application du principe du moindre privilège

Le principe du moindre privilège stipule qu'il ne faut octroyer aux utilisateurs que les privilèges strictement nécessaires à la réalisation de leur travail. L'octroi excessif de responsabilités, de rôles ou de droits peut entraîner des risques d'accès non autorisé au

système, particulièrement au début du cycle de vie d'une organisation, quand il y a encore peu de collaborateurs et que le travail doit être fait rapidement. Passez régulièrement en revue les privilèges des utilisateurs pour déterminer s'ils sont en accord avec les responsabilités professionnelles de ces derniers.

1.2.4. Surveillance de l'activité du système

La sécurité du système repose sur trois fondements : des protocoles de sécurité efficaces, une configuration correcte du système et la surveillance du système. Cette troisième exigence est satisfaite par la réalisation d'audits et l'examen des enregistrements d'audit. Chaque composant d'un système dispose de fonctionnalités de surveillance plus ou moins étendues. Suivez les conseils relatifs à l'audit figurant dans ce document et surveillez régulièrement les enregistrements d'audit.

1.2.5. Consultation des dernières informations de sécurité

Oracle s'efforce d'améliorer continuellement ses logiciels et la documentation associée. Consultez le site Web My Oracle Support tous les ans pour obtenir des révisions.

2

Chapitre 2. Installation et configuration sécurisées

Cette section décrit le processus de planification pour une installation sécurisée et présente plusieurs topologies recommandées de déploiement de ces systèmes.

2.1. Analyse de votre environnement

Pour mieux comprendre vos besoins en matière de sécurité, posez-vous les questions suivantes :

2.1.1. Quelles sont les ressources que je protège ?

Vous pouvez protéger plusieurs types de ressources de l'environnement de production. Lorsque vous choisissez le niveau de sécurité à mettre en oeuvre, tenez compte des ressources qui nécessitent une protection.

Les principales ressources à protéger sont en général vos données. D'autres ressources sont répertoriées ici car elles sont associées à la gestion et la protection de vos données. Les différentes préoccupations liées à la protection des données comprennent la perte de données (données non disponibles) et la compromission de données ou leur communication à des parties non autorisées.

Les clés de chiffrement sont souvent utilisées pour protéger les données contre leur divulgation non autorisée. Elles constituent par conséquent une ressource supplémentaire à protéger. Une gestion de clés très fiable est essentielle pour maintenir des données entièrement disponibles. Les autres couches de ressources à protéger incluent les ressources au sein du cluster Oracle Key Manager, notamment les KMA (Key Management Appliances).

2.1.2. Contre qui est-ce que je protège les ressources ?

Ces ressources doivent être protégées contre toutes les personnes qui ne sont pas autorisées à y accéder. Ces ressources doivent être protégées physiquement. A vous de déterminer quels employés peuvent avoir accès à ces ressources. Identifiez ensuite les types d'opérations que chaque employé doit pouvoir exécuter dans l'environnement Oracle Key Manager.

2.1.3. Que peut-il se passer en cas de défaillance de la protection des ressources stratégiques ?

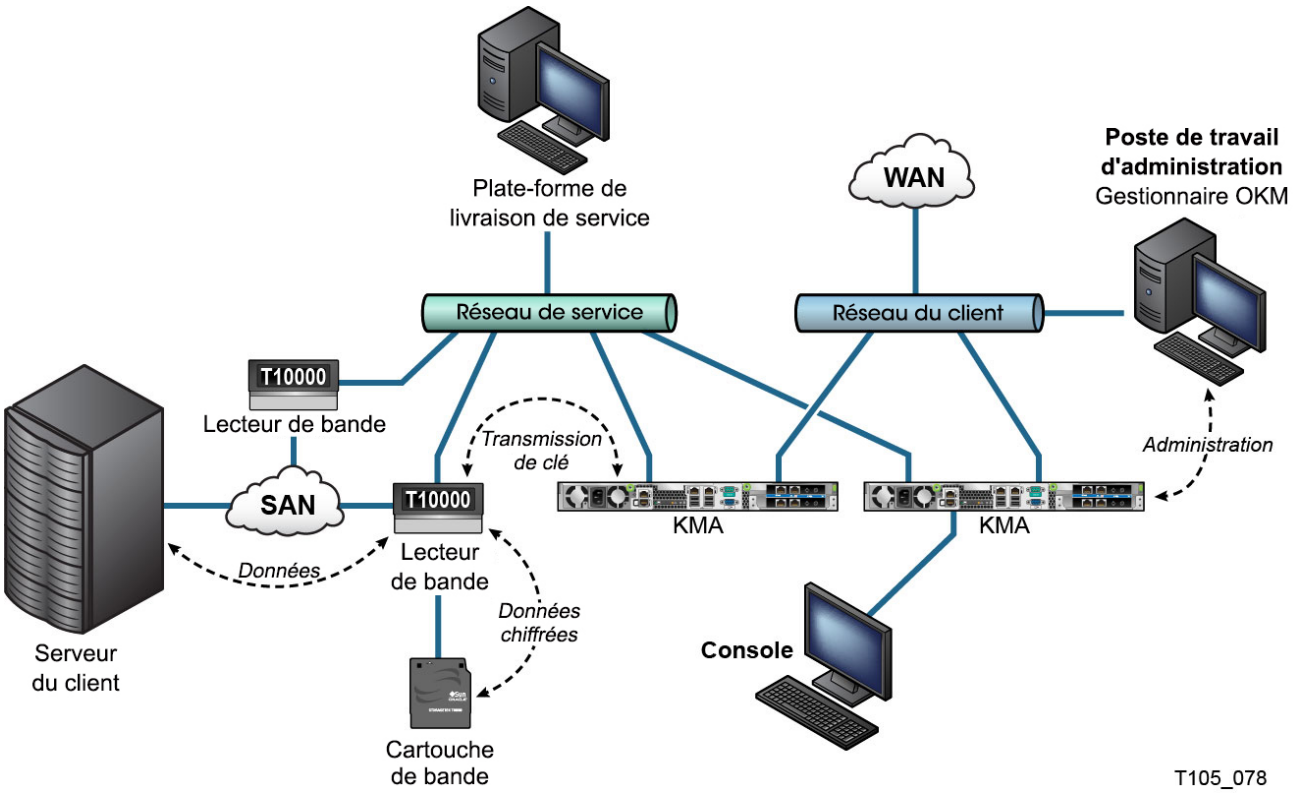
Dans certains cas, une faille du schéma de sécurité est facilement détectable et constitue un simple désagrément. Dans d'autres cas, une faille peut être lourde de conséquences pour

les entreprises ou les individus qui utilisent vos ressources. Pour protéger correctement vos ressources, vous devez comprendre toutes les implications liées à la sécurité de chaque ressource.

2.2. Topologies de déploiement recommandées

L'illustration suivante présente un déploiement standard de solution Oracle Key Manager.

Figure 2.1. Déploiement standard d'une solution OKM



2.3. Installation d'un KMA (Key Management Appliance)

Cette section explique comment installer et configurer un appareil OKM Key Management Appliance en toute sécurité.

Les KMA sont fabriqués comme des appareils sécurisés avec les fonctionnalités d'Oracle Key Manager déjà disponibles.

Voici les étapes à suivre pour installer et configurer des KMA dans un cluster OKM :

1. Installez chaque KMA dans un rack.
2. Sécurisez l'ILOM de chaque KMA.
3. Configurez le premier KMA dans le cluster OKM.

4. Ajoutez des KMA supplémentaires au cluster OKM.

Pour plus d'informations sur la manière de planifier le déploiement d'un cluster OKM, reportez-vous au *Guide de présentation et de planification* d'OKM.

2.3.1. Installation d'un KMA dans un rack

Un technicien de maintenance du service client Oracle installe un KMA dans un rack selon les procédures définies dans le *Manuel d'installation et d'entretien d'Oracle Key Manager*. Le personnel d'entretien d'Oracle peut avoir recours à ce manuel pour plus d'informations.

2.3.2. Sécurisation de l'ILOM d'un KMA

Les KMA Oracle Key Manager sont fabriqués avec des microprogrammes ILOM récents. L'ILOM d'un KMA doit être sécurisé par un technicien de maintenance du service client d'Oracle ou par le client. L'ILOM doit également être sécurisé après une mise à niveau du microprogramme ILOM.

La sécurisation de l'ILOM consiste à définir des paramètres ILOM particuliers en vue d'empêcher toute modification susceptible de compromettre la sécurité. Pour obtenir des instructions détaillées, reportez-vous à la section "Sécurisation d'ILOM" de l'annexe "Procédures du processeur de service" dans le *Guide d'administration* d'Oracle Key Manager.

2.3.3. Configuration du premier KMA dans un cluster OKM

Avant de configurer le premier KMA, identifiez les références de scission de clés ainsi que les ID utilisateur et les phrases de passe à définir dans ce cluster OKM. A cet effet, vous pouvez utiliser une feuille de saisie telle que celle disponible dans le *Manuel d'installation et d'entretien* d'OKM (réservé à un usage interne). Contactez votre représentant du support technique Oracle.

Confiez ces références de scission de clés, ID utilisateur et phrases de passe au personnel approprié. Pour plus d'informations, reportez-vous à la section " Protection de quorum ", plus loin dans ce document.

Remarque:

Conservez et protégez les références de scission de clés ainsi que les ID utilisateur et les phrases de passe.

Ouvrez un navigateur Web, lancez la console distante et lancez l'utilitaire OKM QuickStart dans la console distante. Pour initialiser le cluster OKM sur ce KMA, suivez la procédure correspondante décrite dans le *Guide d'administration d'Oracle Key Manager*, lequel est inclus dans les bibliothèques de documentation Oracle Key Manager.

Les références de scission de clés et un utilisateur avec des privilèges d'agent de sécurité sont définis pendant cette procédure. Une fois que la procédure QuickStart est terminée, l'agent de sécurité doit se connecter au KMA et définir les utilisateurs OKM supplémentaires.

2.3.4. Considérations relatives à la définition des références de scission de clés

Il est plus commode de définir un moindre nombre d'ID utilisateur et de phrases de passe de scission de clés et un seuil moins important, mais cette méthode est moins sécurisante. Il est moins commode de définir un nombre important d'ID utilisateur et de phrases de passe de scission de clés et un seuil plus élevé, mais cette méthode est plus sécurisante.

2.3.5. Considérations relatives à la définition d'utilisateurs OKM supplémentaires

Il est plus commode de définir un moindre nombre d'utilisateurs OKM dont certains détiennent plusieurs rôles, mais cette méthode est moins sécurisante. Il est moins commode de définir un nombre important d'utilisateurs OKM dont la plupart détiennent un seul rôle, mais cette méthode est plus sécurisante car elle facilite le suivi des opérations effectuées par un utilisateur OKM donné.

2.3.6. Ajout de KMA supplémentaires au cluster OKM

Ouvrez un navigateur Web, lancez la console distante et lancez l'utilitaire OKM QuickStart dans la console distante. Pour ajouter ce KMA au cluster OKM, suivez la procédure correspondante décrite dans le *Guide d'administration d'Oracle Key Manager*, à l'adresse suivante :

`http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto`

2.3.7. Considérations relatives à l'ajout de KMA supplémentaires

Oracle Key Manager propose l'option pratique de déverrouillage autonome pour chaque KMA. Cette option est définie pendant la procédure QuickStart pour le premier KMA et les KMA supplémentaires dans un cluster et elle peut être modifiée ultérieurement par l'agent de sécurité.

Si l'option de déverrouillage autonome est activée, le KMA se déverrouille automatiquement au démarrage et il est prêt à fournir des clés sans nécessiter d'approbation de quorum. Si l'option de déverrouillage autonome est désactivée, le KMA reste verrouillé au démarrage et ne fournit pas de clés jusqu'à ce que l'agent de sécurité demande son déverrouillage et qu'un quorum approuve cette demande.

Pour une sécurité maximale, Oracle déconseille d'activer le déverrouillage autonome. Pour plus d'informations concernant l'option de déverrouillage autonome, reportez-vous au document *Oracle Key Manager Version 3.0 Security and Authentication White Paper* (livre

blanc sur la sécurité et l'authentification d'Oracle Key Manager version 3.0), à l'adresse suivante :

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

2.3.8. Caractéristiques des KMA sécurisés

Comme mentionné ci-dessus, les KMA sont fabriqués comme des appareils sécurisés avec les fonctionnalités d'Oracle Key Manager déjà disponibles. En tant qu'appareils sécurisés, ils présentent les caractéristiques suivantes :

- Les packages Solaris inutiles ne sont pas inclus dans l'image Solaris. Par exemple, les services et les utilitaires ftp et telnet n'apparaissent pas dans l'image Solaris.
- Les KMA ne produisent pas de fichiers noyau.
- L'utilitaire de connexion(1) Solaris standard a été remplacé par la console OKM. Ainsi les utilisateurs ne peuvent pas se connecter à la console Solaris.
- Le service ssh est désactivé par défaut. Pour des raisons de support client, l'agent de sécurité peut activer le service ssh et définir un compte support pour une durée limitée. Ce compte est le seul compte disponible qui a des autorisations et un accès limités. L'audit Solaris suit les commandes auxquelles le compte de support fait appel.
- Le compte root est désactivé et configuré en tant que rôle.
- Les KMA ne sont pas équipés d'un lecteur de DVD.
- Les ports USB sont désactivés de manière effective.
- Les ports réseau non utilisés sont fermés.
- Les piles non exécutables sont activées.
- La randomisation de la recherche d'espace d'adressage est configurée.
- Les segments de mémoire non exécutables sont activés.
- Le chiffrement ZFS est utilisé pour les systèmes de fichiers sensibles à la sécurité.
- Solaris est configuré pour être compatible avec le test d'évaluation PCI-DSS SCAP.
- Les services SMF inutiles sont désactivés.
- La fonction Verified Boot d'Oracle Solaris peut être configurée sur les KMA basés sur SPARC T7-1 pour sécuriser le processus d'initialisation du système, assurant ainsi la protection contre la corruption des modules de noyau et l'insertion de rootkits ou d'autres programmes malveillants.
- Les nouveaux KMA basés sur les serveurs SPARC T7-1 et Netra SPARC T4-1 sont inviolables (panne d'ILOM) lorsque l'on accède à la porte du châssis alors que le système est sous tension.
- Le microprogramme ILOM 3.2 est désormais certifié FIPS 140-2 niveau 1 et peut être configuré en mode FIPS.
- L'outil de génération de rapports d'audit de base (BART) s'exécute périodiquement pour faciliter les investigations. Ces rapports sont inclus dans les dumps système OKM.

- La structure de sécurité cryptographique Solaris est configurée conformément aux stratégies de sécurité FIPS 140-2 niveau 1 (documentées pour Solaris 11.1), avec ou sans module HSM (Hardware Security Module).

2.4. Connexions TCP/IP et KMA

Si un pare-feu existe entre les entités (gestionnaire ou agents OKM et autres KMA du même cluster) et le KMA, il doit permettre à l'entité d'établir des connexions TCP/IP avec le KMA sur les ports suivants :

- Les communications entre le gestionnaire OKM et les KMA utilisent les ports 3331, 3332, 3333 et 3335.
- Les communications entre les agents et les KMA utilisent les ports 3331, 3332, 3334 et 3335.
- Les communications d'un KMA à un autre utilisent les ports 3331, 3332 et 3336.

Remarque:

Pour les utilisateurs configurant leurs KMA pour utiliser des adresses IPv6, les pare-feux de périmètre basés sur IPv4 doivent être configurés pour rejeter tous les paquets sortants 41 du protocole IPv4 et les paquets du port UDP 3544, afin d'empêcher les hôtes Internet d'utiliser du trafic transitant par des tunnels IPv6 sur IPv4 pour atteindre des hôtes internes.

Reportez-vous à la documentation de configuration de votre pare-feu pour obtenir davantage d'informations. Le Tableau 2.1, « Connexions aux ports des KMA » répertorie les ports que les KMA utilisent de façon explicite ou les ports auxquels les KMA fournissent des services.

Tableau 2.1. Connexions aux ports des KMA

Numéro de port	Protocole	Direction	Description
22	TCP	Ecoute	SSH (uniquement lorsque le support technique est activé)
123	TCP/UDP	Ecoute	NTP
3331	TCP	Ecoute	Service CA OKM
3332	TCP	Ecoute	Service de certificats OKM
3333	TCP	Ecoute	Service de gestion OKM
3334	TCP	Ecoute	Service d'agent OKM
3335	TCP	Ecoute	Service de découverte OKM
3336	TCP	Ecoute	Service de réplication OKM

Le Tableau 2.2, « Autres services » présente les autres services à l'écoute sur des ports qui ne sont pas forcément utilisés.

Tableau 2.2. Autres services

Numéro de port	Protocole	Direction	Description
53	TCP/UDP	Connexion	DNS (uniquement lorsque le KMA est configuré pour utiliser le protocole DNS)

Numéro de port	Protocole	Direction	Description
68	UDP	Connexion	DHCP (uniquement lorsque le KMA est configuré pour utiliser le protocole DHCP)
111	TCP/UDP	Ecoute	RPC (les KMA répondent aux demandes rpcinfo). Ce port est ouvert aux demandes externes uniquement sur KMS 2.1 et versions antérieures
161	UDP	Connexion	SNMP (uniquement lorsque des gestionnaires SNMP sont définis)
161	UDP	Ecoute	SSH (uniquement lorsque Hardware Management Pack est activé)
514	TCP	Connexion	Système syslog distant (uniquement lorsque les serveurs syslog distants sont définis et configurés pour utiliser le protocole TCP non chiffré)
546	UDP	Connexion	DHCPv6 (uniquement lorsque le KMA est configuré pour utiliser les protocoles DHCP et IPv6)
4045	TCP/UDP	Ecoute	Démon de verrouillage NFS (KMS 2.0 uniquement)
6514	TLS sur TCP	Connexion	Système syslog distant (uniquement lorsque les serveurs syslog distants sont définis et configurés pour utiliser le protocole TCP)

Remarque:

Le port 443 doit être ouvert pour permettre aux clients d'accéder à l'interface Web du processeur de services et à la console OKM via le pare-feu. Reportez-vous au *Manuel d'installation et d'entretien d'Oracle Key Manager* (usage interne uniquement) pour voir les ports ELOM et ILOM.

Le Tableau 2.3, « Ports ELOM/ILOM » dresse la liste des ports ELOM/ILOM des KMA. Ces ports seront activés si l'accès à ELOM/ILOM est requis depuis l'extérieur du pare-feu. Sinon, il n'est pas nécessaire qu'ils soient activés pour l'adresse IP ELOM/ILOM :

Tableau 2.3. Ports ELOM/ILOM

Numéro de port	Protocole	Direction	Description
22	TCP	Ecoute	SSH (pour l'interface de ligne de commande d'ELOM/ILOM)
53	TCP/UDP	Connexion	DNS (nécessaire uniquement lorsque DNS est configuré)
68	UDP	Connexion	Si DHCP est nécessaire pour l'ELOM/ILOM. **Remarque** : Il n'existe pas de documentation pour le protocole DHCP et ELOM/ILOM ; il est néanmoins pris en charge.
80	TCP	Ecoute	HTTP (pour l'interface Web d'ELOM/ILOM) Si HTTP est nécessaire ; sinon, les utilisateurs trouveront les instructions de connexion à la console distante à l'adresse suivante : ELOM : `http://docs.oracle.com/cd/E19121-01/sf.x2100m2/819-6588-14/819-6588-14.pdf` ILOM :

Numéro de port	Protocole	Direction	Description
			http://docs.oracle.com/cd/E19860-01/index.html
161	UDP	Ecoute / Connexion	SNMPv3 (configurable, celui-ci est le port par défaut)
443	TCP /TLS	Ecoute	Embedded/Integrated Lights Out Manager Services Web DMTF (Desktop Management Task Force) pour Management Protocol (WS-Man) sur TLS (Transport Layer Security)
623	UDP	Ecoute	IPMI (Intelligent Platform Management Interface)

3

Chapitre 3. Fonctions de sécurité

Cette section décrit les mécanismes de sécurité spécifiques qu'offre le produit.

3.1. Menaces potentielles

Les clients qui ont des agents pour lesquels le chiffrement est activé doivent se préoccuper principalement des problèmes suivants :

- Divulgation d'informations à l'encontre de la stratégie
- Perte ou destruction de données
- Délai inacceptable de restauration des données en cas de panne catastrophique (par exemple, sur un site de continuité des activités)
- Modification non détectée de données

3.2. Objectifs des fonctions de sécurité

Les objectifs des fonctions de sécurité d'Oracle Key Manager sont les suivants :

- Protéger les données chiffrées de la divulgation.
- Limiter les possibilités d'attaque.
- Garantir une fiabilité et une disponibilité suffisamment élevées.

3.3. Modèle de sécurité

Cette section du guide de sécurité donne un bon aperçu des menaces que le système doit bloquer et de la façon dont les fonctions de sécurité individuelles se coordonnent pour éviter ces attaques.

Les principales fonctions de sécurité qui assurent ces protections sont les suivantes :

- Authentification – Garantit que seules les personnes autorisées ont accès au système et aux données.
- Autorisation – Contrôle d'accès aux privilèges système et aux données ; ce contrôle d'accès s'appuie sur l'authentification pour garantir que les utilisateurs ne disposent que d'un accès correspondant à leurs besoins.

- Audit – Permet aux administrateurs de détecter les tentatives de violation du mécanisme d'authentification et les tentatives réussies ou non de violation du contrôle d'accès.

Pour plus d'informations concernant les aspects sécurité et authentification d'Oracle Key Manager, reportez-vous au document *Oracle Key Manager Version 3.0 Security and Authentication White Paper* (livre blanc sur la sécurité et l'authentification d'Oracle Key Manager Version 3.0) à l'adresse :

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf

3.4. Authentification

L'architecture d'Oracle Key Manager propose une authentification mutuelle entre tous les éléments du système : entre KMA, entre agents et KMA et entre la GUI ou CLI d'Oracle Key Manager et les KMA pour les opérations utilisateur.

Chaque élément du système (par exemple, un nouvel agent de chiffrement) est inscrit dans le système via la création d'un ID et d'une phrase de passe dans l'OKM qui est ensuite saisi dans l'élément à ajouter. Par exemple, lorsqu'un lecteur de bande est ajouté au système, l'agent et le KMA exécutent automatiquement un protocole de question/réponse en fonction de la phrase de passe partagée. De ce fait l'agent obtient un certificat d'autorité de certification (CA) racine, une nouvelle paire de clés et un certificat signé. Avec le certificat d'autorité de certification racine, le certificat d'agent et une nouvelle paire de clés, l'agent peut exécuter le protocole TLS (Transport Layer Security) pour toutes les communications ultérieures avec les KMA. Tous les certificats sont des certificats X.509.

L'OKM se comporte comme une autorité de certification racine pour générer un certificat racine que les KMA utilisent à leur tour pour dériver (auto-signer) les certificats utilisés par les agents, les utilisateurs et les nouveaux KMA.

3.5. Contrôle d'accès

Le contrôle d'accès présente l'un des types suivants :

- Contrôle d'accès basé sur les utilisateurs et les rôles
- Protection de quorum

3.5.1. Contrôle d'accès basé sur les utilisateurs et les rôles

Oracle Key Manager permet de définir plusieurs utilisateurs, chacun possédant un ID utilisateur et une phrase de passe. Chaque utilisateur reçoit un ou plusieurs rôle prédéfinis. Ces rôles déterminent quelles opérations un utilisateur est autorisé à exécuter sur un système Oracle Key Manager. Il s'agit des rôles suivants :

- Agent de sécurité – Exécute la configuration et la gestion d'Oracle Key Manager

- Opérateur – Effectue la configuration de l'agent et les opérations quotidiennes
- Agent de conformité – Définit les groupes de clés et contrôle l'accès des agents aux groupes de clés
- Opérateur de sauvegarde – Réalise des opérations de sauvegarde
- Auditeur – Vérifie les pistes d'audit du système
- Membre du quorum – Inspecte et approuve les opérations en attente du quorum

Un agent de sécurité est défini lors du processus QuickStart qui configure un KMA dans un cluster OKM. Plus tard, un utilisateur doit se connecter au cluster en tant qu'agent de sécurité à l'aide de la GUI d'Oracle Key Manager afin de définir les utilisateurs supplémentaires. L'agent de sécurité peut choisir d'attribuer plusieurs rôles à un utilisateur particulier ou un rôle particulier à plusieurs utilisateurs.

Pour plus d'informations sur les opérations autorisées par chaque rôle et sur la façon dont un agent de sécurité crée des utilisateurs et leur assigne des rôles, reportez-vous au *Guide d'administration Oracle Key Manager* inclus dans les bibliothèques de documentation d'Oracle Key Manager à l'adresse suivante :

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto

Ce contrôle d'accès basé sur les rôles prend en charge les rôles opérationnels définis dans la publication spéciale (SP) 800-60 du NIST (National Institute of Standards and Technology) pour séparer les fonctions opérationnelles.

3.5.2. Protection de quorum

Certaines opérations très critiques nécessitent un niveau de sécurité supplémentaire. Il s'agit notamment de l'ajout d'un KMA sur un cluster OKM, du déverrouillage d'un KMA, de la création d'utilisateurs et de l'attribution de rôles aux utilisateurs. Pour implémenter cette sécurité, le système utilise un ensemble de références de scission de clés en plus de l'accès basé sur les rôles décrit ci-dessus.

Les références de scission de clés se composent de paires ID utilisateur / phrase de passe et du nombre minimum de ces paires qui est nécessaire au système pour permettre l'exécution de certaines opérations. Les références de scission de clés sont également appelées "le quorum" et le nombre minimum est appelé "le seuil du quorum".

Oracle Key Manager permet de définir jusqu'à 10 paires ID utilisateur / phrase de passe de scission de clés et un seuil. Ils sont définis lors du processus QuickStart, lorsque le premier KMA d'un cluster OKM est configuré. Les ID utilisateur et phrases de passe de scission de clés sont différents des ID utilisateur et phrases de passe utilisés pour se connecter au système. Lorsqu'un utilisateur tente une opération qui nécessite l'approbation du quorum, le nombre seuil d'utilisateurs et phrases de passe de scission de clés doit avoir accepté cette opération pour que le système l'exécute.

3.6. Audits

Chaque KMA enregistre des événements d'audit pour les opérations qu'il exécute, notamment celles émises par les agents, les utilisateurs et les KMA pairs dans le cluster OKM. Les KMA enregistrent également des événements d'audit chaque fois qu'un agent, utilisateur ou KMA pair échoue lors de son authentification. Les événements d'audit qui indiquent une violation de sécurité sont répertoriés. Un échec d'authentification est un exemple d'événement d'audit indiquant une violation de sécurité. Si des agents SNMP sont identifiés dans le cluster OKM, les KMA envoient également des SNMP INFORM à ces agents SNMP s'ils rencontrent une violation de sécurité. Si le service syslog distant est configuré, un KMA transfère également ces messages d'audit aux serveurs distants configurés. Voir la section " *Syslog distant* ".

Un utilisateur doit se connecter correctement au cluster OKM et doit être assigné à un rôle pour pouvoir consulter les événements d'audit.

Les KMA gèrent leurs événements d'audit. Les KMA suppriment les anciens événements d'audit en fonction des conditions et des limites (quantitatives) de conservation. L'agent de sécurité peut modifier ces conditions et limites de conservation, si nécessaire.

3.7. Autres fonctions de sécurité

Oracle Key Manager propose d'autres fonctions de sécurité. Pour plus d'informations concernant ces fonctions de sécurité et les autres fonctions OKM, reportez-vous à la *Présentation d'Oracle Key Manager* à l'adresse suivante :

`http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf`

3.7.1. Sécurisation de la communication

Le protocole de communication est le même entre un agent et un KMA, un utilisateur et un KMA et un KMA et un KMA pair. Dans chaque cas, le système utilise la phrase de passe pour que l'entité qui démarre la communication exécute un protocole de question/réponse. Si elle réussit, l'entité reçoit un certificat et la clé privée correspondante. Ce certificat et cette clé privée peuvent établir un canal TLS (Transport Layer Security) (secure sockets). Une authentification mutuelle est effectuée : chaque extrémité d'une connexion authentifie l'autre partie. Les KMA OKM 3.1+ utilisent toujours TLS 1.2 pour leur trafic de réplication entre pairs.

3.7.2. Module HSM

Les KMA proposent un module matériel de sécurité (HSM - Hardware Security Module), disponible par commande séparée. Ce module est une carte Sun Cryptographic Accelerator (SCA) 6000 certifiée FIPS 140-2 niveau 3 qui fournit des clés de chiffrement AES (Advanced Encryption Standard) 256 bits. (Ce certificat a expiré le 31/12/2015 et n'est pas renouvelé ;

un autre module HSM sera fourni dans une version ultérieure.) La carte SCA 6000 prend en charge un mode d'opération FIPS 140-2 de niveau 3 et OKM l'utilise toujours de cette manière. Lorsque le cluster OKM fonctionne en mode FIPS conforme, les clés de chiffrement ne dépassent pas la limite cryptographique de la carte SCA 6000 sous forme déballée. La carte SCA 6000 utilise un générateur de nombre aléatoire approuvé par FIPS, comme indiqué dans le générateur de nombre aléatoire DSA FIPS 186-2 utilisant SHA-1 pour générer des clés de chiffrement.

Lorsqu'un KMA n'est pas configuré avec une carte SCA 6000, le chiffrement est effectué à l'aide du jeton dynamique PKCS#11 de la structure de chiffrement Solaris (SCF). La structure SCF est configurée dans le mode FIPS 140 conformément aux règles de sécurité Solaris FIPS 140-2 les plus récentes.

3.7.3. Chiffrement de clé AES

Oracle Key Manager utilise le chiffrement de clé AES (RFC 3994) avec des clés de chiffrement 256 bits pour protéger les clés symétriques pendant qu'elles sont créées, stockées sur le KMA, transmises aux agents ou dans des fichiers de transfert de clés.

3.7.4. Réplication de clés

Quand le premier KMA d'un cluster OKM est initialisé, il génère un pool de clés important. A mesure que des KMA supplémentaires sont ajoutés au cluster, les clés sont répliquées sur les nouveaux KMA et sont ensuite prêtes à être utilisées pour chiffrer des données. Chaque KMA ajouté au cluster génère un pool de clés et les réplique sur les KMA pairs dans le cluster. Tous les KMA génèrent de nouvelles clés si nécessaire afin de maintenir une taille de pool suffisante pour que les agents puissent à tout moment disposer de clés prêtes à l'emploi. Lorsqu'un agent a besoin d'une nouvelle clé, il contacte un KMA du cluster et lui demande une clé. Le KMA sort une clé du pool et l'assigne au groupe de clés par défaut de l'agent et à l'unité de données. Le KMA réplique ensuite ces mises à jour de la base de données sur les autres KMA du cluster à travers le réseau. Plus tard, l'agent pourra contacter un autre KMA du cluster pour récupérer cette clé. Les composants de clé sous forme de texte clair ne sont jamais transmis à travers le réseau.

3.7.5. Stratégies de sécurité FIPS 140-2 de Solaris

En décembre 2013, le NIST (National Institute of Standards and Technology) a octroyé le certificat de validation FIPS 140-2 de niveau 1 #2061 au module Oracle Solaris Kernel Cryptographic Framework de Solaris 11. En janvier 2014, le NIST a octroyé le certificat de validation FIPS 140-2 de niveau 1 #2076 à la structure cryptographique utilisateur d'Oracle Solaris avec SPARC T4 et SPARC T5. Le KMA Oracle Key Manager 3.1.0 est désormais basé sur le système Solaris 11.3 dont les tests de validation FIPS 140-2 ne sont pas terminés. La structure cryptographique de noyau Oracle Solaris d'un KMA Oracle Key Manager 3.1 .0 est configurée conformément à la *stratégie de sécurité de la structure cryptographique de noyau Oracle*. De la même manière, le KMA est configuré conformément à la *stratégie de sécurité de la structure cryptographique utilisateur d'Oracle Solaris avec SPARC T4 et*

SPARC T5. OKM adoptera des stratégies de sécurité Solaris plus récentes dès qu'elles seront disponibles.

3.7.6. Mises à niveau logicielles

Tous les lots de mise à niveau du logiciel KMA sont signés numériquement pour empêcher le chargement de logiciels non fiables à partir de sources non approuvées.

4

Chapitre 4. Points limite

OKM prend en charge plusieurs types de points limite de chiffrement. En voici la liste :

- Lecteurs de bande aptes au chiffrement
- Oracle Transparent Database Encryption (TDE) 11g ou version supérieure
- Oracle ZFS Storage Appliance
- Systèmes de fichiers ZFS Oracle Solaris 11

Par ailleurs, il existe des outils liés aux points limite pour les développeurs d'applications ou, dans le cas de PKCS#11, pour une utilisation avec la fonctionnalité TDE (Transparent Database Encryption) d'Oracle Database.

4.1. Fournisseur de service KMS Linux PKCS#11

Un fournisseur de service KMS Linux PKCS#11 est disponible pour les clients qui souhaitent communiquer avec OKM à l'aide de PKCS#11. Un administrateur peut télécharger le fournisseur de service KMS Linux PKCS#11 sur le site Web My Oracle Support et l'installer sur un serveur Oracle Enterprise Linux. Le fournisseur de service KMS Linux PKCS#11 possède les mêmes caractéristiques de sécurité que d'autres agents et s'authentifie de la même manière auprès des appareils Oracle Key Manager. Il stocke un fichier journal et des informations de profil dans un répertoire `/var/opt/kms/username`. L'utilisateur et/ou l'administrateur doit gérer ce fichier journal manuellement ou en utilisant un utilitaire tel que logrotate. Le contrôle d'accès au répertoire `/var/opt/kms/username` doit être limité par des autorisations appropriées. Dans le répertoire de profils, les informations d'authentification de l'agent sont conservées dans un fichier PKCS#12. Ce fichier PKCS#12 est sécurisé par un mot de passe. Pour plus d'informations à propos du fournisseur de service KMS Linux PKCS#11, reportez-vous au *Guide d'administration d'Oracle Key Manager* inclus dans les bibliothèques de documentation d'Oracle Key Manager à l'adresse suivante :

`http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#mainframeswncs`

4.2. Fournisseur de service KMS PKCS#11 pour Solaris

Un fournisseur de service KMS PKCS#11 analogue est disponible avec Solaris 10 et Solaris 11.

4.3. Fournisseur de service KMS JCE

Un fournisseur JCE (Java Cryptographic Environment) est disponible pour les développeurs qui souhaitent implémenter des applications client Java capables d'obtenir des clés auprès d'OKM. Ce produit a été intégré à divers produits Oracle et peut être obtenu à partir d'OTN (Oracle Technology Network).

4.4. Plug-in OKM pour Oracle Enterprise Manager

Le plug-in Oracle Key Manager (OKM) pour Oracle Enterprise Manager (OEM) Cloud Control fournit des fonctionnalités de surveillance pour les clusters OKM. Chaque KMA appartenant à un cluster est surveillé par ce plug-in. Un guide de sécurité est fourni pour cet outil.

5

Chapitre 5. Syslog distant

Oracle Key Manager prend en charge le système syslog distant. Les KMA peuvent être configurés pour envoyer des messages au format RFC 3164 ou RFC 5424 à un serveur syslog distant via le protocole TCP non chiffré ou via TLS (Transport Layer Security). Notez que la RFC 5425 décrit l'utilisation de TLS pour fournir une connexion sécurisée destinée au transport des messages syslog au format de message RFC 5424.

Un responsable de la sécurité peut configurer un KMA pour qu'il envoie des messages via le protocole TCP non chiffré ou via TLS. Il est plus sûr d'utiliser TLS pour authentifier et chiffrer les communications entre le KMA et un serveur syslog distant. Le KMA authentifie le serveur syslog distant en demandant son certificat et sa clé publique. Le serveur syslog distant peut éventuellement être configuré pour utiliser l'authentification mutuelle. L'authentification mutuelle garantit que le serveur syslog distant accepte uniquement les messages provenant de clients autorisés (tels que des KMA). Lorsqu'il est configuré pour utiliser l'authentification mutuelle, le serveur syslog distant demande un certificat au KMA afin de vérifier l'identité de ce dernier.

6

Chapitre 6. Hardware Management Pack

Oracle Key Manager prend en charge Oracle Hardware Management Pack (HMP) sur les KMA SPARC T7-1, Netra SPARC T4-1 et Sun Fire X4170 M2. Le produit HMP s'inscrit dans le cadre de la gestion de système unique (SSM) Oracle au même titre qu'ILOM. Un agent de sécurité peut activer HMP sur un KMA pour utiliser un agent de gestion dans Solaris afin de permettre la surveillance in-band du KMA sur SNMP. Le logiciel HMP est préinstallé mais désactivé avec la configuration d'agent SNMP. Par conséquent, le port d'écoute de l'agent SNMP n'est pas ouvert tant que HMP n'est pas activé. HMP est désactivé par défaut.

L'activation de HMP apporte les avantages suivants :

- Notification d'événements en cas de problèmes matériels avant que ces derniers n'apparaissent en tant que notifications SNMP propres à Oracle Key Manager ou en tant que panne du KMA.
- Possibilité d'activer HMP sur certains KMA pris en charge d'un cluster OKM ou sur tous.
- Possibilité d'utiliser des opérations SNMP Get en lecture seule vers les bases MIB du service SNMP du KMA, notamment MIB-II, SUN-HW-MONITORING-MIB et SUN-STORAGE-MIB.
- Intégration d'Oracle Red Stack avec Oracle Enterprise Manager via des receivelets et des fetchlets SNMP.

Gardez à l'esprit les considérations suivantes lorsque vous décidez d'activer HMP sur un KMA. Une fois activé, HMP lance les opérations suivantes :

- Exploitation de tous les gestionnaires SNMP v2c configurés dans le cluster Oracle Key Manager et activés. Le protocole SNMP v2c est dépourvu des améliorations de sécurité introduites dans la version SNMP v3.
- Activation d'un agent de gestion SNMP sur le KMA, ce qui permet l'accès réseau en lecture seule aux informations de MIB SNMP sur le KMA considéré.
- Les risques en matière de sécurité identifiés dans le *Guide de sécurité d'Oracle Hardware Management Pack (HMP)* (`http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf`) sont atténués de diverses façons :
  - "Les produits de gestion système permettent d'obtenir un environnement root amorçable" - La sécurisation des KMA désactive l'accès de root aux utilisateurs du système. SNMP est configuré pour l'accès en lecture seule. Les opérations SNMP Put sont donc rejetées.
  - "Les produits de gestion système comprennent des outils puissants pouvant uniquement être exécutés à l'aide de privilèges d'administrateur ou de privilèges root" - L'accès de

root aux KMA est désactivé. Les utilisateurs du système ne peuvent donc pas exécuter ces outils.

Annexe A. Liste de contrôle du déploiement sécurisé

La liste de contrôle de sécurité suivante inclut les directives permettant de sécuriser votre système de gestion des clés :

1. Installez chaque KMA dans un environnement physiquement sécurisé.
2. Sécurisez le BIOS ou la PROM OpenBoot sur chaque KMA.
3. Sécurisez Lights Out Manager sur chaque KMA.
4. Définissez la configuration de scission de clé pour ce cluster Oracle Key Manager.
5. Définissez le paramètre de déverrouillage autonome pour chaque KMA, le cas échéant.
6. Définissez les utilisateurs Oracle Key Manager et leurs rôles.
7. Pratiquez le principe du moindre privilège.
   a. Attribuez uniquement les rôles nécessaires à chaque utilisateur Oracle Key Manager.
8. Surveillez l'activité sur le cluster Oracle Key Manager.
   a. Recherchez s'il y a des erreurs, plus particulièrement des violations de sécurité, qui sont consignées dans le journal d'audit d'Oracle Key Manager.
9. Sauvegardez la sécurité principale quand la configuration de scission de clé est initialement définie et quand elle est modifiée.
10. Effectuez régulièrement des sauvegardes d'Oracle Key Manager.
11. Stockez les fichiers de sauvegarde de sécurité principale et les fichiers de sauvegarde d'Oracle Key Manager dans un emplacement sécurisé.

Annexe B

Annexe B. Références

- Documentation client d'Oracle Key Manager

  http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#crypto
- *Oracle Enterprise Manager System Monitoring Plug-in for Oracle Key Manager Security Guide*
- *Manuel d'installation et d'entretien d'Oracle Key Manager* (réservé à un usage interne)
- *Présentation d'Oracle Key Manager*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf
- *Oracle Key Manager Version 3.0 Security and Authentication White Paper* (livre blanc sur la sécurité et l'authentification d'Oracle Key Manager version 3.0)

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/okm-security-auth-300497.pdf
- Documentation d'Oracle Integrated Lights Out Manager (ILOM)

  http://docs.oracle.com/cd/E37444_01/
- Documentation sur les serveurs SPARC T7-1 https://docs.oracle.com/cd/E54976_01/
- Documentation sur les serveurs Netra SPARC T4-1

  http://docs.oracle.com/cd/E23203_01/
- Documentation sur Oracle Hardware Management Pack
  - Bibliothèque de documentation d'Oracle Hardware Management Pack

    http://docs.oracle.com/cd/E20451_01/
  - Gestion de système autonome Oracle

    http://www.oracle.com/technetwork/server-storage/servermgmt/overview/index.html
- Documentation NIST :
  - *Publication spéciale 800-60 Volume I Revision 1 du National Institute of Standards and Technology*

http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf

- Documentation sur les stratégies de sécurité pour les produits Oracle :
  - *Oracle Solaris Kernel Cryptographic Framework Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2061.pdf
  - *Oracle Solaris Kernel Cryptographic Framework with SPARC T4 and T5 Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2060.pdf
  - *Sun Cryptographic Accelerator 6000 FIPS 140-2 Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Oracle StorageTek T10000D Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Oracle StorageTek T10000C Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Oracle StorageTek T10000B Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Oracle StorageTek T10000A Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Oracle StorageTek T9480D Tape Drive Security Policy*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- Certificats de validation FIPS pour les produits Oracle :
  - SCA (Sun Cryptographic Accelerator) 6000 - Certificat #1026 (expiré)

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1026.pdf