Oracle® Key Manager 3

Guide de présentation et de planification

Version 3.0.2

E52229-02

Avril 2015

ORACLE®

Oracle® Key Manager 3

Guide de présentation et de planification

E52229-02

Table des matières

Liste des illustrations

Liste des tableaux

Préface

Ce guide présente Oracle Key Manager (OKM), en décrit la planification et identifie les exigences relatives à son implémentation.

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

Planification de l'installation

Référez-vous à la liste de vérification suivante pour planifier une installation OKM.

Passez en revue la présentation et les configurations d'OKM

- Chapitre 2, *Présentation d'OKM* .
- Chapitre 3, *Configurations d'OKM* .

Passez en revue les exigences des serveurs

- Passez en revue les spécifications KMA (Section 2.2.1, « KMA Server for OKM 3.0 »).
- Passez en revue les spécifications des racks KMA (Section 2.2.3, « Spécifications des racks »).
- Vérifiez que le site est conforme aux exigences en termes de température, d'humidité, de refroidissement et d'alimentation du serveur.
  - Pour les spécifications du serveur Sun Netra SPARC T4-1, voir :

    http://docs.oracle.com/cd/E23203_01/index.html
  - Vérifiez l'emplacement et les caractéristiques des coupe-circuits.
  - Pour l'option d'alimentation redondante, assurez-vous qu'un interrupteur d'alimentation APC supplémentaire est disponible.

Passez en revue les conditions requises pour le réseau

- Chapitre 4, *Mise en réseau d'OKM* .

Passez en revue les conditions requises pour les lecteurs de bande

- Chapitre 5, *Conditions requises pour le lecteur de bande*.

Planifiez les rôles utilisateur

- Section 2.8, « Rôles utilisateur ».

Préparez la livraison

- Assurez-vous que le personnel autorisé est disponible pour gérer et accepter la livraison. OKM Key Management Appliance (KMA) est considéré comme un matériel sûr.

- Assurez-vous qu'il existe un plan de mise au rebut ou de recyclage des matériaux d'emballage.

Commandez les composants

- Chapitre 6, *Commande* .

2

Présentation d'OKM

OKM assure la sécurité des données en chiffrant les données stockées (chiffrement basé sur périphérique). Cette solution crée, stocke et gère les clés de chiffrement. OKM prend en charge les systèmes ouverts et les plates-formes d'entreprise.

Les sections suivantes décrivent les concepts et les composants de la solution OKM.

2.1. Normes de chiffrement prises en charge

OKM repose sur les normes sectorielles suivantes :

- FIPS PUB 140-2, Security Requirements for Cryptographic ModulesFIPS PUB 46-3, Data Encryption StandardFIPS PUB 171, Key Management
- NIST 800-57 Part 1, Recommendations for Key Management
- IEEE 1619.1 Standard for Tape Encryption (texte complet) IEEE 1619.2 Standard for Disk Encryption (en cours d'élaboration) IEEE 1619.3 Standard for Key Management (en cours d'élaboration)
- Critères communs (CC)
- Techniques de sécurité ISO/IEC 1779
- Chiffrement CCM–AES-256
- Chiffrement symétrique
- Nonce
- Suite de chiffrement (TLS 1.0, RSA 2048 bits, SHA1, HMAC)

2.2. Key Management Appliance (KMA)

KMA est un serveur à sécurité renforcée qui assure l'authentification, le contrôle d'accès, des services d'allocation de clés et la gestion des clés du cycle de vie sur la base de stratégies. Le serveur KMA s'assure que tous les périphériques de stockage sont enregistrés et authentifiés et que toutes les créations, allocations et suppressions de clés de chiffrement sont conformes aux stratégies établies.

2.2.1. KMA Server for OKM 3.0

OKM 3.0 prend en charge Solaris 11 sur le serveur Netra SPARC T4-1. La version OKM de ce serveur inclut :

- Un processeur SPARC T4 4 coeurs à 2,85 GHz
- 32 Go de DRAM (quatre DIMM de 8 Go)
- Disque dur 2,5" SAS de 600 Go, 10 000 TPM
- 4 ports Gigabit Ethernet
- Alimentations électriques redondantes
- 5 emplacements de cartes PCIe Gen 2 (8 voies chacune)
- Lecteur de DVD (désactivé - non utilisé avec OKM)

Pour connaître les autres caractéristiques du serveur, notamment les exigences en termes d'environnement et d'alimentation, voir :

http://docs.oracle.com/cd/E23203_01/index.html

2.2.2. KMA Servers for OKM 2.x

OKM 2.x prend en charge Solaris 10 sous Sun Fire X2100 M2, X2200 M2 et X4170 M2.

Remarque:

Les KMA Sun Fire ne peuvent pas être mis à niveau vers OKM 3.0, mais peuvent communiquer avec les KMA OKM 3.0 qui se trouvent dans le même cluster. Les KMA OKM 3.0 peuvent rejoindre un cluster OKM 2.x existant à l'aide d'un KMA exécutant KMS 2.2 ou supérieur.

2.2.3. Spécifications des racks

Les KMA peuvent être installés dans les armoires ou les racks à quatre montants RETMA 19 pouces standard. Les racks à deux montants ne sont pas pris en charge.

Remarque:

La bibliothèque SL8500 peut accueillir quatre racks de 19 pouces. Pour plus d'informations, reportez-vous au *Guide d'assurance des systèmes StorageTek SL8500*.

Les rails coulissants sont compatibles avec les racks respectant les normes suivantes :

- Ouverture horizontale et insertion verticale d'unités conformes aux normes ANSI/EIA 310-D-1992 ou IEC 60927.
- Distance entre les plans de montage avant et arrière comprise entre 610 mm et 915 mm (24 à 36 pouces).
- Espace libre minimal devant la porte avant de l'armoire de 25,4 mm (1 pouce).
- Espace libre minimal derrière la porte arrière de l'armoire de 800 mm (31,5 pouces) pour intégrer la gestion des câbles ou de 700 mm (27,5 pouces) sans gestion des câbles.
- Espace libre minimal entre les supports structurels et les chemins de câbles et entre les plans avant et arrière de 456 mm (18 pouces).

2.2.4. Carte SCA6000

La carte Sun Cryptographic Accelerator (SCA6000) disponible en option est destinée à la prise en charge des fonctions administratives et de traitement cryptographique requises pour la conformité FIPS. Il s'agit d'un module de sécurité matérielle FIPS 140-2 de niveau 3.

2.3. Interface utilisateur graphique (GUI) d'OKM

Vous pouvez utiliser l'interface GUI d'OKM pour configurer et gérer OKM. Cette interface s'exécute sur une station de travail fournie par le client et communique avec les KMA sur un réseau IP. Vous n'avez pas besoin de droits d'administrateur (sous Windows) ou racine (sous Solaris) pour installer et exécuter l'interface GUI.

Plates-formes prises en charge

- Solaris 10 10/09 (mise à jour 8) x86
- Solaris 10 9/10 (mise à jour 9) SPARC
- Solaris 10 9/10 (mise à jour 9) x86
- Microsoft Windows 7 Professionnel
- Microsoft Windows 7 Entreprise
- Microsoft Windows Vista Professionnel
- Microsoft Windows XP Professionnel Version 2002
- Microsoft Windows XP Professionnel
- Microsoft Windows Server 2008 Version 6.0
- Microsoft Windows Server 2003 R2 édition Standard
- Microsoft Windows Server 2003

2.4. Interface CLI d'OKM

Deux utilitaires de l'interface de ligne de commande (CLI) prennent en charge un sous-ensemble de fonctions identiques à celles de l'interface GUI d'OKM. Ces utilitaires permettent d'automatiser différentes tâches, telles que la sauvegarde, l'exportation de clés et la création de rapports d'audit.

2.5. Cluster OKM

Un cluster est un ensemble complet de KMA dans un système. Tous les KMA se reconnaissent les uns les autres et répliquent mutuellement la totalité de leurs informations. Le cluster fournit des lecteurs de bande pouvant sélectionner des KMA pour extraire des composants de clés.

- Un cluster peut contenir deux[1] KMA au minimum et 20 KMA au maximum.
- Les nouvelles clés générées sur n'importe quel site sont répliquées sur tous les KMA du cluster.
- Toutes les modifications administratives sont propagées à tous les autres KMA du cluster.
- Prenez en compte la taille du cluster lors de la conception du système, afin d'assurer une disponibilité optimale.
- Plusieurs KMA peuvent être inclus dans un cluster sur un réseau étendu dédié, privé ou local.
- Tout KMA inclus dans un cluster peut offrir des services à tout agent sur le réseau.
- N'importe quel KMA peut être utilisé pour les fonctions d'administration.

Remarque:

Les KMA d'un cluster ne reconnaissent pas les KMA des autres clusters.

2.5.1. Comment les lecteurs de bande utilisent les KMA d'un cluster

Les lecteurs de bande extraient les clés à partir du cluster de KMA à travers la détection, l'équilibrage de charge et le basculement.

2.5.1.1. Détection

Les lecteurs de bande (agents) envoient une demande de découverte de cluster à un KMA. Le KMA qui reçoit la demande de détection de cluster fournit les informations suivantes pour chaque KMA :

- Adresses IP (IPv4 et IPv6)
- Nom du site
- ID du KMA
- Nom du KMA
- Version du KMA (permet de déterminer la prise en charge FIPS pour les lecteurs de bande pris en charge)
- Etat du KMA :
  - Réponse : indique si le KMA répond sur le réseau

[1]Une exception peut être définie pour l'approbation des services techniques, des services professionnels et des services d'assistance.

- Verrouillé : indique si le KMA est actuellement verrouillé

Les lecteurs de bande extraient régulièrement ces informations dans le cadre d'une opération de bande (lorsque le lecteur de bande est actif) et les demandent toujours lors de l'inscription et à chaque fois que le lecteur est en chargement initial (IPL).

Lorsqu'un lecteur détecte un nouvel état de réponse pour un KMA, il met à jour les informations du cluster en conséquence.

2.5.1.2. Equilibrage de charge

Au cours des opérations normales du lecteur de bande, les lecteurs utilisent leur tableau local d'informations de cluster pour sélectionner un KMA pour l'extraction de clés.

Le lecteur utilise un algorithme pour sélectionner un KMA sur le même site que le lecteur. Si tous les KMA d'un site sont verrouillés ou ne répondent pas, le lecteur de bande tente alors d'accéder à un KMA d'un autre site. Si les KMA d'autres sites sont inaccessibles, la tentative d'extraction des clés finira par expirer, entraînant alors un basculement.

2.5.1.3. Basculement

La capacité des lecteurs de bande à basculer vers des sites distants peut améliorer la fiabilité et la disponibilité des lecteurs lorsque les KMA locaux sont indisponibles ou lents à répondre (comme en cas d'expiration du délai d'attente en raison d'importantes charges de travail).

Dans tous les cas où un lecteur de bande ne peut pas communiquer avec l'un des KMA d'un cluster, le lecteur en question utilise un algorithme pour sélectionner un KMA pour une tentative de basculement. Lors de la sélection, les informations du lecteur concernant l'état du cluster sont à nouveau utilisées.

Les lecteurs de bande tente d'effectuer un basculement jusqu'à trois fois avant d'abandonner et de renvoyer une erreur à l'application de bande hôte.

Remarque:

Parfois, un lecteur peut sélectionner un KMA qui ne répond pas pendant une tentative de basculement si tous les autres KMA ne répondent pas. Toutefois, les informations concernant le cluster pouvant être obsolètes, il est possible que le KMA soit en réalité en ligne et qu'il réponde.

2.6. Agents

Les agents sont des extrémités de chiffrement qui utilisent des clés cryptographiques pour chiffrer et déchiffrer les données. Les agents sont des périphériques (des lecteurs de bande, par exemple) qui sont authentifiés auprès d'OKM et obtiennent les composants de clés via une session "sécurisée" (TLS). Les agents communiquent avec les KMA via l'API de l'agent. (L'API de l'agent est un ensemble d'interfaces logicielles incorporées dans le matériel ou le logiciel de l'agent.) Par défaut, les agents sont servis par les KMA locaux, si ceux-ci sont disponibles.

- Les agents de lecteurs de bande ne doivent pas se trouver sur des réseaux publics.
- Les agents doivent rester connectés au réseau dans l'éventualité où une clé de chiffrement serait nécessaire. Connectez les agents de lecteurs de bande aux KMA sur un réseau de service privé.
- Les KMA et les agents peuvent être "regroupés" logiquement pour créer un site, sur lequel les agents font référence aux KMA sur le site auxquels ils sont affectés.

2.7. Unités de données, clés, stratégies de clés et groupes de clés

Unités de données
Les unités de données représentent des données chiffrées par des agents. Pour les lecteurs de bande, une unité de données est une cartouche de bande.

Clés
Les clés correspondent aux valeurs de clés réelles (composant de clé) et à leurs métadonnées associées.

Stratégies de clés
Les stratégies de clés définissent les paramètres régissant les clés. Cela comprend les paramètres de cycle de vie (tels que la période de chiffrement et la durée de validité) et les paramètres d'exportation/importation (importation autorisée, exportation autorisée, par exemple).

Groupes de clés
Les groupes de clés associent des clés et des stratégies de clés. Chaque groupe de clés dispose d'une stratégie de clés et est affecté à des agents. Les agents peuvent extraire uniquement les clés attribuées à l'un des groupes de clés autorisés de l'agent en question. Les agents disposent également d'un groupe de clés par défaut. Lorsqu'un agent crée une clé (et l'attribue à une unité de données), la clé est placée dans le groupe de clés par défaut de l'agent.

Remarque:

Pour que le système fonctionne, vous devez définir au moins une stratégie de clés et un groupe de clés (attribué comme le groupe de clé attribué) pour tous les agents.

2.8. Rôles utilisateur

OKM a un ensemble prédéfini de rôles utilisateur :

Responsable de la sécurité
Effectue la configuration et la gestion des OKM.

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
Effectue les opérations de sauvegarde.

Auditeur
Peut afficher les pistes d'audit du système.

Membre du quorum
Examine et approuve les opérations en attente du quorum.

Pour plus d'informations sur les rôles utilisateur, notamment la liste des opérations que chaque rôle peut effectuer, reportez-vous au *Guide d'administration* d'OKM.

Remarque:

Vous pouvez utiliser une feuille de saisie pour simplifier la planification des rôles utilisateur, 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.

2.9. Intégration d'IBM ICSF

IBM Integrated Cryptography Service Facility (ICSF) est une solution de chiffrement dans laquelle un fichier de clés externe se trouve dans un mainframe IBM et est accessible via un protocole TLS/XML. Reportez-vous au document *OKM-ICSF Integration Guide* pour plus d'informations.

3

Configurations d'OKM

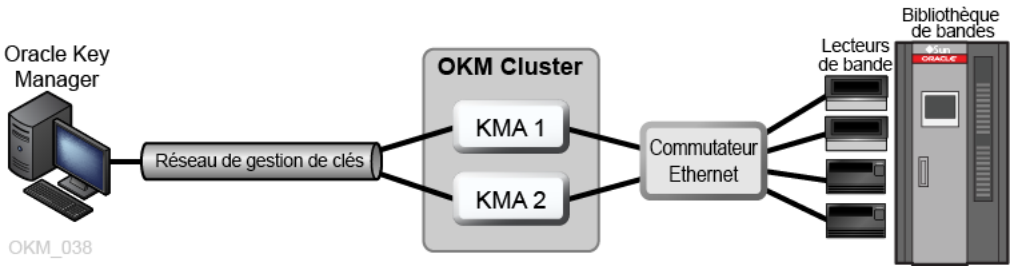
Les exemples suivants illustrent des configurations d'OKM :

- Site unique
- Site double
- Sites doubles avec récupération après sinistre
- Sites doubles avec base de données Oracle
- Sites multiples avec bibliothèque partitionnée

3.1. Site unique

La Figure 3.1, « Configuration de site unique » illustre un site unique comportant deux KMA dans un cluster. Le réseau de service inclut plusieurs lecteurs de bande (agents).

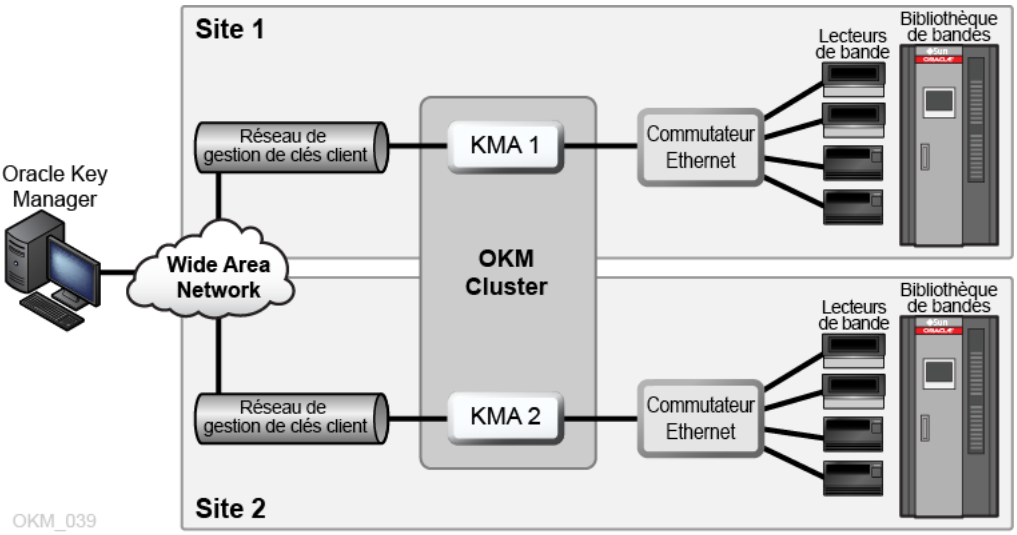
Figure 3.1. Configuration de site unique



3.2. Site double

Dans la Figure 3.2, « Configuration de site double », chaque site comprend un KMA. Les KMA sont gérés sur un réseau étendu et les deux KMA appartiennent au même cluster OKM. Dans cette configuration, Oracle recommande des sites dispersés entre différentes régions géographiques.

Figure 3.2. Configuration de site double



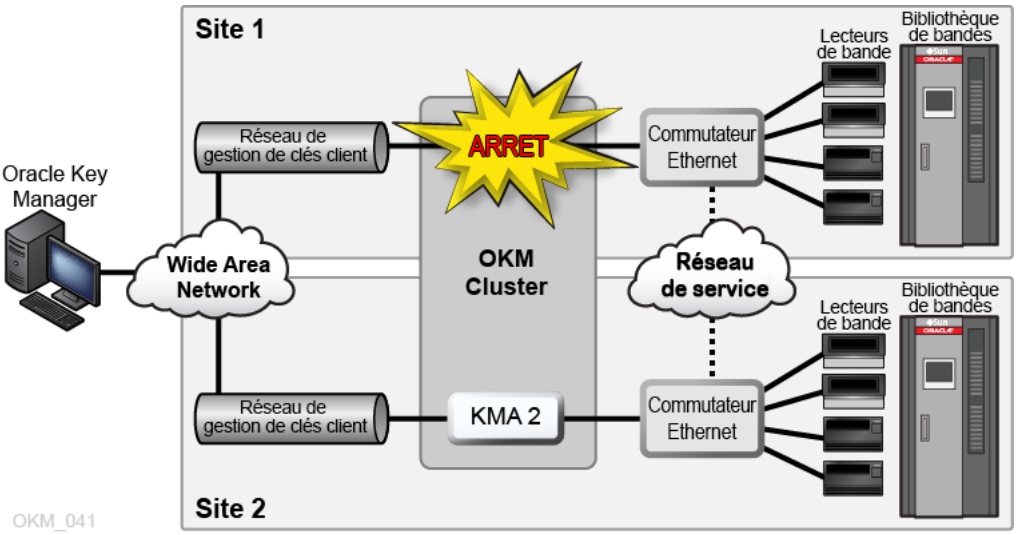
3.3. Sites doubles avec récupération après sinistre

Pour réduire le risque qu'un sinistre détruise l'intégralité du cluster, il est recommandé que ce dernier s'étende sur plusieurs sites géographiques distincts.

Dans la Figure 3.3, « Configuration de la récupération après sinistre », il existe deux réseaux étendus : un réseau pour la gestion et l'autre pour les services. L'interface GUI d'OKM communique avec les deux KMA du cluster, tandis que Le réseau étendu de service permet à l'un ou l'autre KMA de communiquer avec les agents.

Pour plus d'informations sur la récupération après sinistre, reportez-vous au document *Disaster Recovery Reference Guide*.

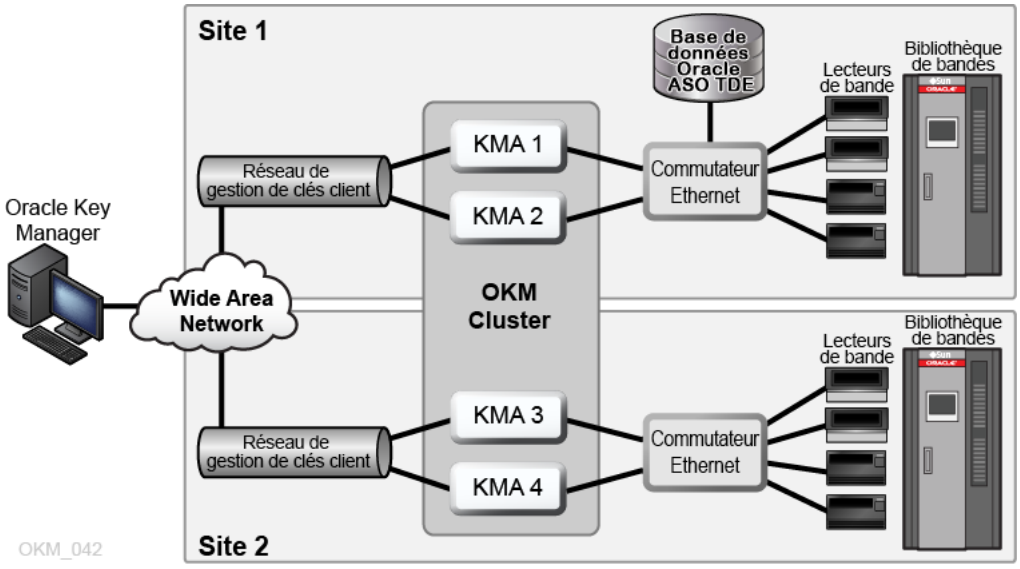
Figure 3.3. Configuration de la récupération après sinistre



3.4. Sites doubles avec base de données Oracle

Dans la Figure 3.4, « Exemple de base de données », quatre KMA d'un cluster prennent en charge les bibliothèques de bandes automatisées et une base de données Oracle avec la solution de cryptage transparent des données d'Oracle Advanced Security (TDE). Pour plus d'informations, reportez-vous au *Guide d'administration* d'OKM.

Figure 3.4. Exemple de base de données



3.5. Sites multiples avec bibliothèque partitionnée

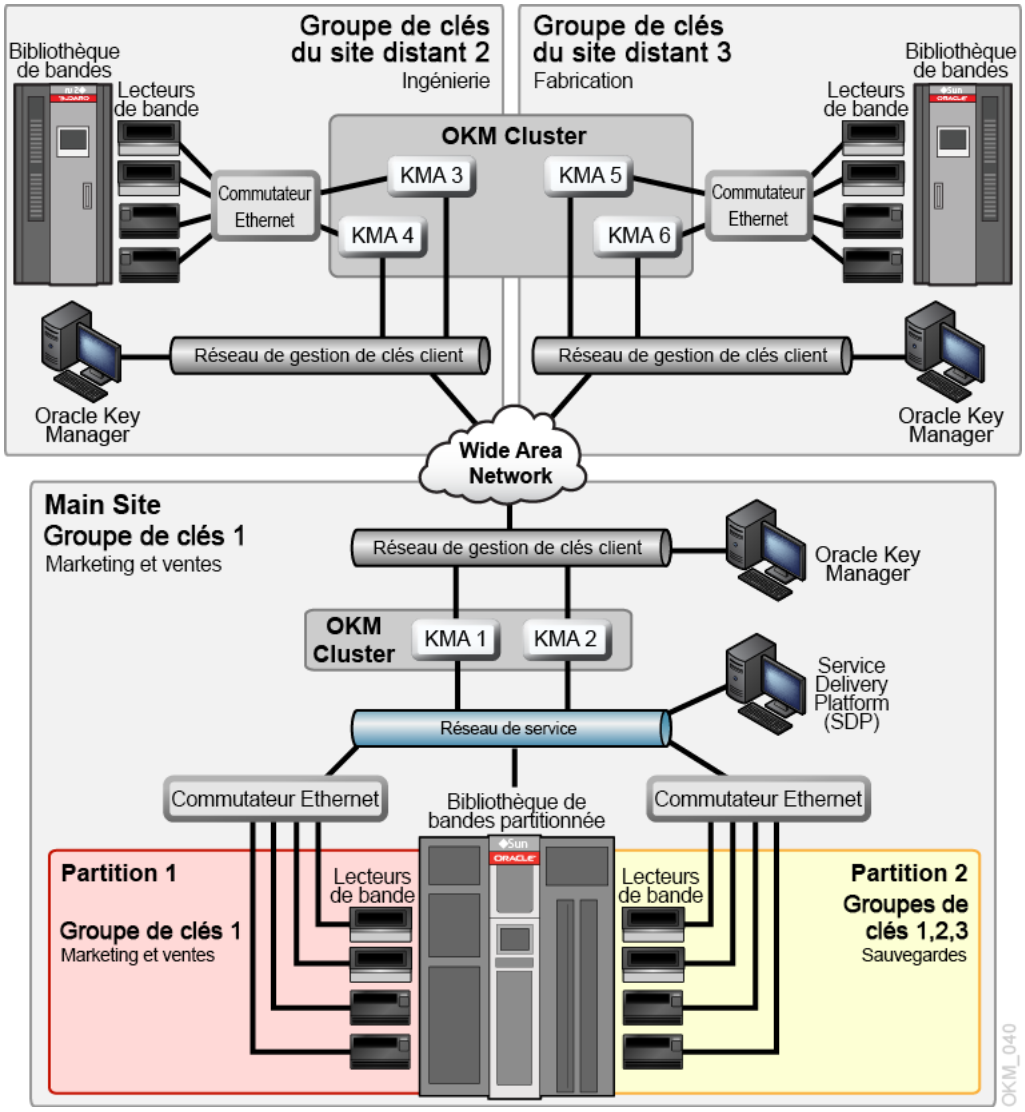
Lorsque vous utilisez des lecteurs de bande aptes au chiffrement, les partitions peuvent ajouter une couche de sécurité des données. Les partitions peuvent :

- Limiter l'accès aux lecteurs de bande et aux cartouches de données ;
- séparer différents groupes de clés de chiffrement ;
- isoler des clients comme des centres de service ;
- être dédiés à des tâches spécifiques ;
- offrir à de nombreux services, de nombreuses organisations et sociétés un accès à des ressources de bibliothèques de taille adéquate.

La Figure 3.5, « Configuration à plusieurs sites » illustre deux sites distants et un site local (principal) dans un cluster OKM unique. Le site principal contient une bibliothèque partitionnée avec des groupes de clés spécifiques, qui offre des solutions de sauvegarde pour tous les KMA (1 à 6) et les médias du cluster OKM.

Pour plus d'informations sur le partitionnement, reportez-vous à la documentation relative à votre bibliothèque.

Figure 3.5. Configuration à plusieurs sites



4

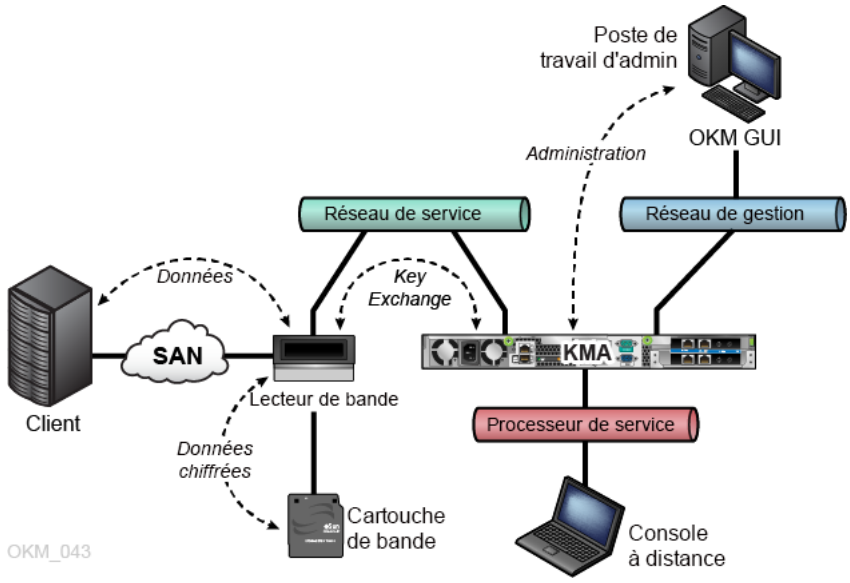
Mise en réseau d'OKM

4.1. Présentation du réseau

OKM utilise un réseau TCP/IP (double pile IPv4 et IPv6[1]) pour les connexions entre les KMA, les agents et les stations de travail. Chaque KMA dispose de connexions réseau pour :

- Réseau de gestion
- Réseau de service
- Processeur de service

Figure 4.1. Connexions réseau OKM



[1]Toutes les applications n'utilisent pas Ipv6 (par exemple, DNS). En conséquence, IPv4 est toujours requis.

4.1.1. Réseau de gestion

Le réseau de gestion connecte le KMA à l'interface GUI d'OKM et à d'autres KMA du cluster pour la réplication entre homologues. Le réseau de gestion peut être local, distant ou une combinaison des deux. Les clients doivent fournir le réseau de gestion. Utilisez une connexion Ethernet gigabit afin d'assurer une réplication et des performances optimales.

Pour plus de sécurité et afin d'isoler le trafic LAN, vous pouvez envisager d'utiliser des réseaux locaux virtuels (VLAN) pour la connexion au réseau de gestion.

4.1.2. Réseau de service

Le réseau de service connecte les KMA aux agents. Il isole les extractions de clés des autres trafics sur le réseau.

Les interfaces du réseau de service du KMA peuvent, si vous le souhaitez, être regroupées (voir Section 4.2.2, « Groupement de ports de service de KMA »).

4.1.3. Processeur de service

La connexion au processeur de service permet d'accéder au gestionnaire ILOM (Integrated Lights Out Manager) sur les serveurs Netra SPARC T4-1 ou au gestionnaire ELOM (Embedded Lights Out Manager) sur les serveurs Sun Fire. Votre représentant du support technique Oracle accède aux gestionnaires ILOM/ELOM pour la configuration initiale des KMA.

Le protocole STP doit être arrêté ou désactivé sur le réseau du processeur de service (ELOM ou ILOM).

4.2. Commutateurs gérés

Oracle recommande l'utilisation d'un commutateur géré pour la connexion des KMA à des lecteurs de bande sur des réseaux de service privés. Un connecteur géré fournit la connectivité aux connecteurs de lecteurs de bande non gérés et aux routeurs de réseaux étendus.

Les commutateurs gérés améliorent la facilité de maintenance grâce aux diagnostics améliorés des commutateurs et au dépannage du réseau de service, et ils peuvent réduire les points de défaillance sur ce dernier grâce à l'utilisation de connexions redondantes et du protocole STP.

4.2.1. Modèles de commutateurs gérés pris en charge

Oracle fournit des conseils, teste et recommande les configurations pour ce qui suit :

- Commutateur 3COM 4500G 24 ports (3CR17761-91)
- Extreme Networks Summit X150-24t

- Brocade ICX 6430

4.2.2. Groupement de ports de service de KMA

Vous pouvez regrouper les interfaces Ethernet physiques en une seule interface virtuelle. Le regroupement de ces ports renforce la disponibilité ; ainsi, si une défaillance se produit au niveau d'un port, l'autre maintient la connectivité.

Vérifiez que la configuration des ports de commutateurs Ethernet est correcte. Les ports de commutateurs doivent être définis de manière à négocier automatiquement la vitesse gigabit et le mode duplex intégral.

Pour obtenir les instructions de configuration de l'agrégation des ports de service, votre représentant du support technique Oracle peut consulter le *Manuel d'installation et d'entretien d'OKM* (réservé un usage interne).

4.2.3. Mise en miroir de ports

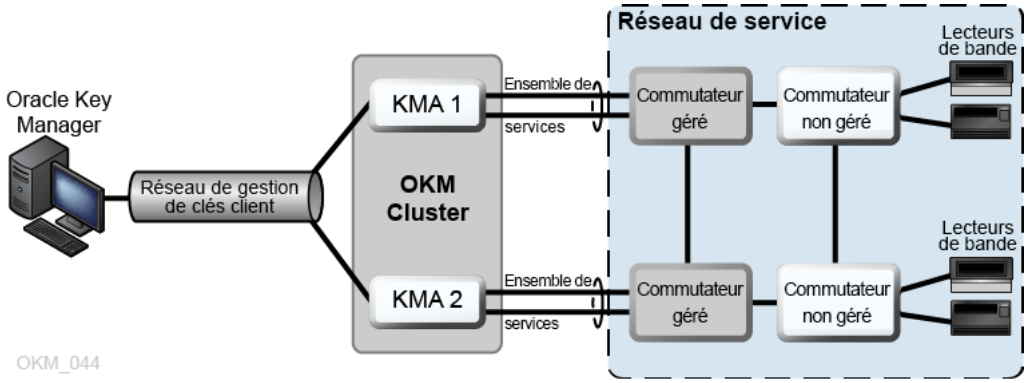
Vous pouvez mettre en miroir des ports pour utiliser un analyseur de réseau sur le réseau de service. Les ports peuvent être mis en miroir sur les commutateurs Brocade ICX 6430. Pour obtenir les instructions de configuration, votre représentant du support technique Oracle peut consulter le *Manuel d'installation et d'entretien d'OKM* (réservé à un usage interne).

4.2.4. Exemple de configuration de commutateur géré

Dans Figure 4.2, « Configuration de commutateur géré » :

- Si un KMA ou un commutateur géré est défaillant, les lecteurs disposent toujours d'un chemin de communication avec l'autre KMA.
- Les commutateurs gérés sont connectés à des commutateurs non gérés contenant des chemins redondants nécessitant une configuration STP. (Les commutateurs gérés doivent être activés pour le protocole STP lorsque le câblage comprend la fonction de redondance.)
- Les interfaces du réseau de service sont regroupées dans une interface virtuelle unique (voir Section 4.2.2, « Groupement de ports de service de KMA »).

Figure 4.2. Configuration de commutateur géré



4.3. Configuration de routage réseau

La configuration de routage d'un KMA a des conséquences sur les réponses aux demandes de détection de lecteurs de bande. Des erreurs dans la configuration du routage peuvent entraîner la fourniture d'informations incorrectes concernant les clusters aux lecteurs de bande. Les lecteurs peuvent, par exemple, tenter de communiquer avec des KMA auxquels ils ne peuvent pas accéder sur le réseau.

Lors de la planification du réseau OKM, observez les consignes suivantes :

- Utilisez l'option de menu du réseau de la console KMA pour configurer un itinéraire entre des sites. Ne configurez pas un itinéraire par défaut.

  Remarque:

  Oracle ne recommande pas de commencer avec une topologie de réseau de service multi-site.

- Lors de la planification d'un réseau de service multi-site, déterminez le schéma d'adressage du sous-réseau des lecteurs et des ports de service KMA. Vous devez éviter les adresses réseau en double et l'utilisation de réseaux 172.18.18.x (convention commune).
- L'utilisation de paramètres de passerelle par défaut peut affecter les performances de basculement. Consultez un ingénieur réseau pour planifier la fonction de basculement.

4.4. Exigences relatives aux pare-feu SDP

La plate-forme SDP (Service Delivery Platform) consiste en une appliance intelligente et un réseau dédié. Elle contrôle les bibliothèques de bande Oracle et les lecteurs T-series. SDP fournit un diagnostic à distance en recueillant les événements relatifs aux périphériques et en avertissant le service d'assistance technique Oracle en cas de problème.

Il doit y avoir un pare-feu entre les périphériques connectés à un KMA et SDP. Le pare-feu partitionne le réseau de service en deux : le réseau de service contrôlé par Oracle et le réseau de service contrôlé par le client. Le pare-feu du client permet à SDP de n'accéder qu'aux périphériques qu'il peut contrôler.

Important:

Configurez le pare-feu de sorte que SDP puisse contrôler les lecteurs de bande dans la partie du réseau de service contrôlée par le client.

Dans Figure 4.3, « Exemple de connectivité SDP » :

- Le pare-feu du client est connecté au Port 2 de l'appliance SDP.

  L'interface du réseau du client désigne la connexion entre les périphériques de stockage SDP et Oracle connectés au réseau local de votre centre opérationnel, qui est associé à votre réseau. Ces périphériques comprennent les lecteurs de bande et les commutateurs connectés aux KMA.
- L'interface du réseau de service Oracle est connectée au Port 1 de l'appliance SDP.

L'interface du réseau de service Oracle désigne la connexion entre l'unité de site SDP et les périphériques de stockage.

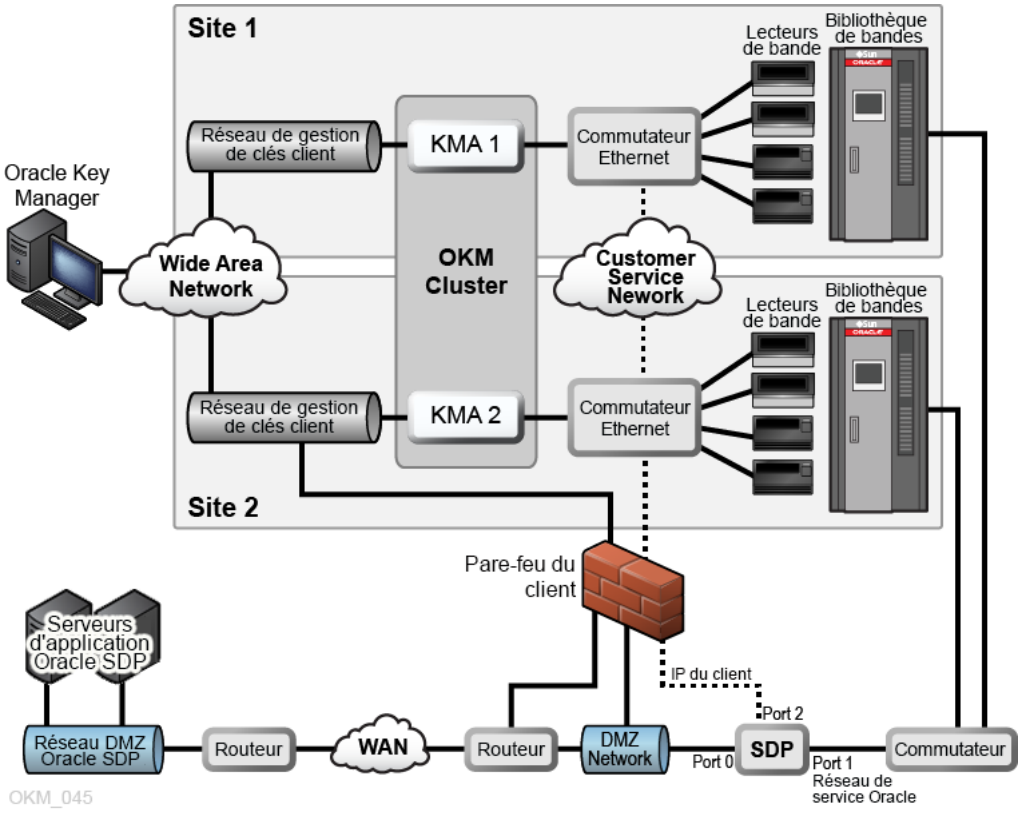
- La zone démilitarisée (DMZ) désigne l'architecture de réseau sécurisée de SDP qui sécurise le trafic réseau entre l'unité de site SDP et le réseau Oracle (Port 0).

Remarque:

Le personnel de maintenance Oracle doit assurer le fonctionnement de l'équipement dans les deux partitions du réseau de service et s'accorder avec les ingénieurs SDP pour la planification et la configuration.

Pour plus informations, reportez-vous au *Livre blanc de la sécurité pour Service Delivery Platform*.

Figure 4.3. Exemple de connectivité SDP



5

Conditions requises pour le lecteur de bande

5.1. Lecteurs de bande pris en charge

Les lecteurs de bande suivants prennent en charge le chiffrement :

- StorageTek T10000A
- StorageTek T10000B
- StorageTek T10000C
- StorageTek T10000D
- StorageTek T9840D
- HP LTO-4 (requiert une carte HP Dione)
- HP LTO-5 et 6
- IBM LTO-4, 5 et 6 (tous requièrent une carte IBM Belisarius)

5.2. Lecteurs de bande conformes à la norme FIPS

Tableau 5.1. Lecteurs de bande conformes à la norme FIPS 140-2

Lecteur de bande	Niveau FIPS 140-2
T10000A	1
T10000B	2
T10000C	1
T10000D	1
T9840D	1
LTO4 (HP et IBM)	Aucun plan pour FIPS
LTO5 (HP et IBM)	Aucun plan pour FIPS
LTO6 (HP et IBM)	Aucun plan pour FIPS

Remarque:

Seuls les lecteurs LTO peuvent être validés FIPS, mais pas nécessairement dans certaines applications de chiffrement.

Les niveaux de sécurité FIPS 140-2 pour les lecteurs de bande mentionnés précédemment comprennent :

- Niveau 1 : niveau élémentaire des critères de production.
- Niveau 2 : critères supplémentaires concernant les dispositifs de sécurité anti-violation et l'authentification basée sur des rôles. Conçu sur une plate-forme d'exploitation validée. Cette sélection fournit un niveau de sécurité plus élevé pour les KMA et les lecteurs de bande.

5.3. Comportement de chiffrement des lecteurs de bande T-Series

Tableau 5.2. Comportement de chiffrement des lecteurs de bande T-Series

Type de lecteur de bande	Bandes non chiffrées	Bandes chiffrées
Non inscrit pour le chiffrement	• Entièrement compatible • Lecture, écriture et ajout	• Lecture, écriture ou ajout impossibles • Possibilité de réécriture à partir du début de la bande (BOT)
Inscrit pour le chiffrement	• Fonction de lecture uniquement • Ajout impossible • Possibilité de réécriture à partir du début de la bande (BOT)	• Entièrement compatible • Lecture avec les clés appropriées • Ecriture avec la clé d'écriture actuelle

5.4. Comportement de chiffrement des lecteurs LTO

Remarque:

Seuls les médias LTO-4 (LTO-4 et LTO-4 WORM) prennent en charge le chiffrement sur les lecteurs de bande LTO-4.

Tableau 5.3. Comportement de chiffrement pour lecteur LTO-4 non inscrit pour le chiffrement

Comportement du lecteur	Fonctionnalité
Lecture des données non chiffrées LTO-4	OK sans chiffrement
Lecture des données chiffrées LTO-4	Erreur
Ecriture LTO-4 à partir de BOT	OK sans chiffrement
Lecture de bande LTO-3	OK sans chiffrement
Ajout/écriture LTO-4 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-4 aux données non chiffrées (lecture sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-4 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement

Comportement du lecteur	Fonctionnalité
Ajout/écriture LTO-4 aux données chiffrées (lecture sur EOD, puis écriture)	Erreur

Tableau 5.4. Comportement de chiffrement pour lecteur LTO-4 inscrit pour le chiffrement

Comportement du lecteur	Fonctionnalité
Lecture des données non chiffrées LTO-4	OK sans chiffrement
Lecture des données chiffrées LTO-4	OK avec chiffrement si la clé appropriée est disponible
Ecriture LTO-4 à partir de BOT	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-4 aux données chiffrées	OK avec chiffrement si la clé appropriée est disponible
Ecriture de bande LTO-3	HP : OK sans chiffrement[1] IBM : Erreur
Lecture de bande LTO-3	OK sans chiffrement
Ajout/écriture LTO-4 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[2] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-4 aux données non chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[2] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-4 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-4 aux données chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible. IBM : OK avec chiffrement si la clé appropriée est disponible, mais avec la clé de lecture antérieure[3]

[1]Les lecteurs HP écriront sur les bandes en mode sans chiffrement. Le format LTO-3 ne prend pas en charge le chiffrement, ce qui peut être considéré comme une faille de sécurité puisque les lecteurs HP LTO-4/LTO-5 peuvent écrire des données non chiffrées simplement via l'insertion d'une cartouche LTO-3.

[2]Ce cas de figure permet d'ajouter des données chiffrées après des données non chiffrées, ce qui présente un avantage opérationnel puisque cela permet d'utiliser des bandes préétiquetées avec des données non chiffrées dans des lecteurs LTO HP dans l'environnement de chiffrement sans devoir les réétiqueter.

[3]Dans ce cas, les lecteurs IBM écriront des données chiffrées, mais utiliseront la même clé que celle utilisée pour la lecture des données chiffrées antérieures sur la bande. Le lecteur ne demandera pas de nouvelle clé à OKM lors de l'émission de la commande d'écriture et ignorera la stratégie d'expiration de clé définie par OKM.

Tableau 5.5. Comportement de chiffrement pour lecteur LTO-5 non inscrit pour le chiffrement

Comportement du lecteur	Fonctionnalité
Lecture de données non chiffrées LTO-5	OK sans chiffrement
Lecture de données chiffrées LTO-5	Erreur

Comportement du lecteur	Fonctionnalité
Ecriture LTO-5 à partir de BOT	OK sans chiffrement
Lecture des données non chiffrées LTO-4	OK sans chiffrement
Lecture des données chiffrées LTO-4	Erreur
Ecriture LTO-4 à partir de BOT	OK sans chiffrement
Lecture LTO-3	OK sans chiffrement
Ajout/écriture LTO-5 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-5 aux données non chiffrées (lecture sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-5 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO5 aux données chiffrées (lecture sur EOD, puis écriture)	Erreur
Ajout/écriture LTO-4 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-4 aux données non chiffrées (lecture sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-4 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-4 aux données chiffrées (lecture sur EOD, puis écriture)	Erreur

Tableau 5.6. Comportement de chiffrement pour lecteur LTO-5 inscrit pour le chiffrement

Comportement du lecteur	Fonctionnalité
Lecture de données non chiffrées LTO-5	OK sans chiffrement
Lecture de données chiffrées LTO-5	OK avec chiffrement si la clé appropriée est disponible
Ecriture LTO-5 à partir de BOT	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-5 aux données chiffrées	OK avec chiffrement si la clé appropriée est disponible
Lecture des données non chiffrées LTO-4	OK sans chiffrement
Lecture des données chiffrées LTO-4	OK avec chiffrement si la clé appropriée est disponible
Ecriture LTO-4 à partir de BOT	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-4 aux données chiffrées	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-5 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[1] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-5 aux données non chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[1] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.

Comportement du lecteur	Fonctionnalité
Ajout/écriture LTO-5 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO5 aux données chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible. IBM : OK avec chiffrement si la clé appropriée est disponible, mais avec la clé de lecture antérieure[2]
Ajout/écriture LTO-4 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[1] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-4 aux données non chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[1] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-4 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-4 aux données chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible. IBM : OK avec chiffrement si la clé appropriée est disponible, mais avec la clé de lecture antérieure[2]
Lecture de données non chiffrées LTO-3	OK sans chiffrement

[1]Ce cas de figure permet d'ajouter des données chiffrées après des données non chiffrées, ce qui présente un avantage opérationnel puisque cela permet d'utiliser des bandes préétiquetées avec des données non chiffrées dans des lecteurs LTO HP dans l'environnement de chiffrement sans devoir les réétiqueter.

[2]Dans ce cas, les lecteurs IBM écriront des données chiffrées, mais utiliseront la même clé que celle utilisée pour la lecture des données chiffrées antérieures sur la bande. Le lecteur ne demandera pas de nouvelle clé à OKM lors de l'émission de la commande d'écriture et ignorera la stratégie d'expiration de clé définie par OKM.

Tableau 5.7. Comportement de chiffrement pour lecteur LTO-6 non inscrit pour le chiffrement

Comportement du lecteur	Fonctionnalité
Lecture de données non chiffrées LTO-6	OK sans chiffrement
Lecture de données chiffrées LTO-6	Erreur
Ecriture LTO-6 à partir de BOT	OK sans chiffrement
Lecture de données non chiffrées LTO-5	OK sans chiffrement
Lecture de données chiffrées LTO-5	Erreur
Ecriture LTO-5 à partir de BOT	OK sans chiffrement
Lecture des données non chiffrées LTO-4	OK sans chiffrement
Ajout/écriture LTO-6 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-6 aux données non chiffrées (lecture sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-6 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement

Comportement du lecteur	Fonctionnalité
Ajout/écriture LTO-6 aux données chiffrées (lecture sur EOD, puis écriture)	Erreur
Ajout/écriture LTO-5 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-5 aux données non chiffrées (lecture sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO-5 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK sans chiffrement
Ajout/écriture LTO5 aux données chiffrées (lecture sur EOD, puis écriture)	Erreur

Tableau 5.8. Comportement de chiffrement pour lecteur LTO-6 inscrit pour le chiffrement

Comportement du lecteur	Fonctionnalité
Lecture de données non chiffrées LTO-6	OK sans chiffrement
Lecture de données chiffrées LTO-6	Erreur
Ecriture LTO-6 à partir de BOT	OK sans chiffrement
Lecture de données non chiffrées LTO-6	OK sans chiffrement
Lecture de données chiffrées LTO-6	OK avec chiffrement si la clé appropriée est disponible
Ecriture LTO-6 à partir de BOT	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-6 aux données chiffrées	OK avec chiffrement si la clé appropriée est disponible
Lecture de données non chiffrées LTO-5	OK sans chiffrement
Lecture de données chiffrées LTO-5	OK avec chiffrement si la clé appropriée est disponible
Ecriture LTO-5 à partir de BOT	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-5 aux données chiffrées	OK avec chiffrement si la clé appropriée est disponible
Lecture des données non chiffrées LTO-4	OK sans chiffrement
Lecture des données chiffrées LTO-4	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-6 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[1] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-6 aux données non chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[1] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-6 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO-6 aux données chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible.

Comportement du lecteur	Fonctionnalité
	IBM : OK avec chiffrement si la clé appropriée est disponible, mais avec la clé de lecture antérieure[2]
Ajout/écriture LTO-5 aux données non chiffrées (libération d'espace sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[1] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-5 aux données non chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible[1] IBM : Erreur. Il n'est pas permis de mélanger des données chiffrées et non chiffrées sur une même bande.
Ajout/écriture LTO-5 aux données chiffrées (libération d'espace sur EOD, puis écriture)	OK avec chiffrement si la clé appropriée est disponible
Ajout/écriture LTO5 aux données chiffrées (lecture sur EOD, puis écriture)	HP : OK avec chiffrement si la clé appropriée est disponible. IBM : OK avec chiffrement si la clé appropriée est disponible, mais avec la clé de lecture antérieure[2]

[1]Ce cas de figure permet d'ajouter des données chiffrées après des données non chiffrées, ce qui présente un avantage opérationnel puisque cela permet d'utiliser les bandes préétiquetées avec des données non chiffrées dans un lecteur LTO HP dans l'environnement de chiffrement sans devoir les réétiqueter.

[2]Dans ce cas, les lecteurs IBM écriront des données chiffrées, mais utiliseront la même clé que celle utilisée pour la lecture des données chiffrées antérieures sur la bande. Le lecteur ne demandera pas de nouvelle clé à OKM lors de l'émission de la commande d'écriture et ignorera la stratégie d'expiration de clé définie par OKM.

5.5. Préparation des lecteurs de bande pour le chiffrement

Pour inscrire les lecteurs de bande pour le chiffrement, demandez l'aide de votre représentant du support technique Oracle et référez-vous au *Guide d'administration* d'OKM. Avant leur inscription, certains lecteurs nécessitent une préparation. Pour plus d'informations, les représentants du support technique Oracle peuvent se référer au *Manuel d'installation et d'entretien* d'OKM (réservé à un usage interne).

Préparation des données de lecteurs de bande T-Series

Les lecteurs T10000C et T10000D exécutant les versions 1.57.30x (T10000C) ou 4.06 .106 (T10000D) du microprogramme, et des versions supérieures, ne nécessitent pas de clés d'activation du chiffrement. Pour les lecteurs et les versions de microprogramme antérieurs, le représentant du support technique Oracle doit demander une clé de licence pour le chiffrement de chaque lecteur.

Préparation des lecteurs de bande LTO

Aucune activation ou donnée de lecteur n'est requise pour les lecteurs de bande LTO. La seule préparation consiste à vérifier que vous disposez des informations pour associer les adresses IP et les noms d'agents aux lecteurs de bande dans le gestionnaire OKM.

5.6. Configuration de microprogramme requise

Le Tableau 5.9, « Compatibilités des microprogrammes » décrit la configuration minimale requise du microprogramme pour chaque lecteur de bande.

Les produits de gestion de bibliothèque suivants sont pris en charge :

- ACSLS - 7.1 et 7.1.1 avec PUT0701 ou 7.2 et 7.3
- HSC - 6.1 et 6.2
- VSM - 6.1 ou 6.2 (comprend VTCS et VTSS)
- Modèles VTL - 1.0 ou 2.0.

Mise à jour du microprogramme

Les niveaux du microprogrammé indiqués peuvent être modifiés. Pour accéder à la dernière version du microprogramme :

1. Accédez à My Oracle Support à l'adresse suivante : `http://support.oracle.com` et connectez-vous.
2. Cliquez sur l'onglet **Patches & mises à jour**.
3. Cliquez sur **Produit ou famille (avancé).**
4. Dans le champ **Commencez à écrire...**, saisissez les informations relatives au produit (par exemple, "Oracle Key Manager"), puis cliquez sur **Rechercher** pour afficher le dernier microprogramme pour chaque version.

Tableau 5.9. Compatibilités des microprogrammes

Lecteurs de bande	SL8500	SL3000	Lxxx	9310/9311	SL500	SL150
T10000A FC	L–3.11c D–1.37.113	L–FRS_2.00 D–1.37.113	L–3.17.03 D–1.37.113	L–4.4.08 D–137113	S/O	S/O
T10000A FICON	L–3.11c D–1.37.114	L–FRS_2.00 D–1.37.114	L–3.17.03 D–1.37.114	L–4.4.08 D–137114	S/O	S/O
T10000B FC	L–3.98b D–1.38.x09	L–FRS_2.00 D–1.38.x07	L–3.17.03 D–1.38.x07	S/O	S/O	S/O
T10000B FICON	L–3.98b D–1.38.x09	L–FRS_2.00 D–1.38.x09	L–3.17.03 D–1.38.x09	S/O	S/O	S/O
T10000C FC	L–FRS_7.0.0 D–1.53.316	L–FRS_3.0.0 D–1.53.316	S/O	S/O	S/O	S/O
T10000C FICON	L–FRS_7.0.0 D–1.53.316	L–FRS_3.0.0 D–1.53.316	S/O	S/O	S/O	S/O
T10000D FC	L–FRS_8.0.5 (lecteur 3590 non pris en charge)	L–FRS_3.62 (lecteur 3590 non pris en charge)	S/O	S/O	S/O	S/O

Lecteurs de bande	SL8500	SL3000	Lxxx	9310/9311	SL500	SL150
	D–4.06.107 FC/ FCoE	D–4.06.107 FC/ FCoE				
T10000D FICON	L–FRS_8.0.5 (lecteur 3590 non pris en charge) D–4.07.xxx	L–FRS_3.62 (lecteur 3590 non pris en charge) D–4.07.xxx	S/O	S/O	S/O	S/O
T10000D FCoE	L_FRS_8.3.0 D–4.06.106	L_FRS_4.xx D_4.06.106	S/O	S/O	S/O	S/O
T9840D FC	L–3.98 D–1.42.x07	L–FRS_2.00 D–1.42.x07	L–3.17.03 D–142x07	L–4.4.08 D–142x07	S/O	S/O
T9840D FICON & ESCON	L–3.98 D–142x07	L–FRS_2.00 D–142x07	L–3.17.03 D–142x07	L–4.4.08 D–142x07	S/O	S/O
HP LTO-4	L–3.98B D–H64S FC S/O pour SCSI	L–2.05 D–H64S FC S/O pour SCSI	S/O	S/O	L–1300 D–H64S FC D–B63S SCSI	S/O
HP LTO-5	D–I5BS FC S/O pour SAS	D–I5BS FC S/O pour SAS	S/O	S/O	D–I5BS FC D–X5AS SAS	L–1.80 D–Y5BS FC
HP LTO-6	D– J2AS FC S/O pour SAS	D– J2AS FC S/O pour SAS	S/O	S/O	D– J2AS FC S/O pour SAS	L–1.80 D–Z55S SAS D–22CS FC D–329S SAS
HP LTO-4	L–FRS_4.70 D–BBH4 FC S/O pour SCSI	L–FRS_2.30 D–BBH4 FC S/O pour SCSI	S/O	S/O	L–1373 D– BBH4 FC D– BBH4 SCSI	S/O
IBM LTO-5	D–BBNH FC	D–BBNH FC	S/O	S/O	L–1373 D–BBNH FC	S/O
IBM LTO-6	L–8.01 D–CT94 FC	L–4.0 D–CT94 FC	S/O	S/O	L–1483 D–BBNH FC S/O pour FC	S/O

Légende :

- L – Niveau du microprogramme de bibliothèque
- D – Niveau du microprogramme de lecteur
- FC – Fibre Channel
- FCoE – Fibre Channel over Ethernet

- SPS – microprogramme spécial, approbation nécessaire
- S/O – Sans objet Non pris en charge.

5.7. Configuration requise pour Virtual Operator Panel

Le Tableau 5.10, « Version minimale de VOP » indique la version minimale d'Oracle Virtual Operator Panel (VOP) requise pour chaque type de lecteur.

Remarque:

Si vous utilisez Multi-Drive Virtual Operator Panel (MD-VOP), la version 1.1 ou supérieure est requise.

Tableau 5.10. Version minimale de VOP

Lecteur de bande	Version minimale de VOP
T10000A, B, C, D	1.0.18
T9840D	1.0.12
HP LTO-4	1.0.12
HP LTO-5	1.0.16
HP LTO-6	1.0.18
HP LTO-4	1.0.14
IBM LTO-5	1.0.16
IBM LTO-6	1.0.18

6

Commande

6.1. Serveur KMA

Tableau 6.1. Numéros de commande du serveur KMA

N° de commande	Description
7105795	Netra SPARC T4-1 Server personnalisé pour OKM
375-3424-06	Carte Sun Cryptographic Accelerator (SCA6000)

6.2. Kit d'accessoire de commutateur

Tableau 6.2. Numéros de commande du kit d'accessoire de commutateur

N° de commande	Description
7104584	Kit d'accessoire de commutateur (SAK). Inclut un commutateur géré 24 ports, ainsi que les câbles et le matériel de fixation correspondants.

6.3. Câbles Ethernet

Tableau 6.3. Numéros de commande des câbles Ethernet

N° de commande	Description
CABLE10187033-Z-N	Câble Ethernet CAT5e 8’
CABLE10187034-Z-N	Câble Ethernet CAT5e 35’
CABLE10187037-Z-N	Câble Ethernet CAT5e 55’

6.4. Câbles d'alimentation

Tableau 6.4. Références des câbles d'alimentation

Câble d'alimentation ATO	Equivalent PTO	Description	Ampères	Tension	Câble
333A-25-10-AR	X312F-N	Câble d'alimentation, Argentine, 2,5 m, IRAM2073, 10 A, C13	10	250	180-1999-02

Câble d'alimentation ATO	Equivalent PTO	Description	Ampères	Tension	Câble
333A-25-10-AU	X386L-N	Câble d'alimentation, Australie, 2,5 m, SA3112, 10 A, C13	10	250	180-1998-02
333A-25-10-BR	X333A-25-10-BR-N	Câble d'alimentation, Brésil, 2,5 m, NBR14136, 10 A, C13	10	250	180-2296-01
333A-25-10-CH	X314L-N	Câble d'alimentation, Suisse, 2,5 m, SEV1011, 10 A, C13	10	250	180-1994-02
333A-25-10-CN	X328L	Câble d'alimentation, Chine, 2,5 m, GB2099, 10 A, C13	10	250	180-1982-02
333A-25-10-DK	X383L-N	Câble d'alimentation, Danemark, 2,5 m, DEMKO107, 10 A, C13	10	250	180-1995-02
333A-25-10-EURO	X312L-N	Câble d'alimentation, Europe, 2,5 m, CEE7/ VII, 10 A, C13	10	250	180-1993-02
333A-25-10-IL	X333A-25-10-IL-N	Câble d'alimentation, Israël, 2,5 m, SI-32, 10 A, C13	10	250	180-2130-02
333A-25-10-IN	X333A-25-10-IN-N	Câble d'alimentation, Inde, 2,5 m, IS1293, 10 A, C13	10	250	180-2449-01
333A-25-10-IT	X384L-N	Câble d'alimentation, Italie, 2,5 m, CEI23, 10 A, C13	10	250	180-1996-02
333A-25-10-KR	X312G-N	Câble d'alimentation, Corée, 2,5 m, KSC8305, 10 A, C13	10	250	180-1662-03
333A-25-10-TW	X332A-N	Câble d'alimentation, Taïwan, 2,5 m, CNS10917, 10 A, C13	10	125	180-2121-02
333A-25-10-UK	X317L-N	Câble d'alimentation, Royaume-Uni, 2,5 m, BS1363A, 10 A, C13	10	250	180-1997-02
333A-25-10-ZA	X333A-25-10-ZA-N	Câble d'alimentation, Afrique du Sud, 2,5 m, SANS164, 10 A, C13	10	250	180-2298-01
333A-25-15-JP	X333A-25-15-JP-N	Câble d'alimentation, Japon, 2,5 m, PSE5-15, 15 A, C13	15	125	180-2243-01
333A-25-15-NEMA	X311L	Câble d'alimentation, Afrique du Nord/Asie, 2,5 m, 5-15P, 15 A, C13	15	125	180-1097-02
333A-25-15-TW	X333A-25-15-TW-N	Câble d'alimentation, Taïwan, 2,5 m, CNS10917, 15 A, C13	15	125	180-2333-01
333F-20-10-NEMA	X320A-N	Câble d'alimentation, Afrique du Nord/Asie, 2,0 m, 6-15P, 10 A, C13	10	250	180-2164-01
333F-25-15-JP	X333F-25-15-JP-N	Câble d'alimentation, Japon, 2,5 m, PSE6-15, 15 A, C13	15	250	180-2244-01
333J-40-15-NEMA	X336L	Câble d'alimentation, Afrique du Nord/Asie, 4,0 m, L6-20P, 15 A, C13	15	250	180-2070-01
333R-40-10-309	X332T	Câble d'alimentation, INTL, 4,0 m, IEC309-IP44, 10 A, C13	10	250	180-2071-01

Tableau 6.5. Références des cordons d'alimentation de racks non Oracle

Câble d'alimentation ATO	Equivalent PTO	Description	Ampères	Tension	Câble
333V-20-15-C14	X333V-20-15-C14-N	Câble d'alimentation, Jmpr, droit, 2,0 m, C14, 15 A, C13	15	250	180-2442-01
333V-30-15-C14	X333V-30-15-C14-N	Câble d'alimentation, Jmpr, droit, 3,0 m, C14, 15 A, C13	15	250	180-2443-01

Tableau 6.6. Références des cordons d'alimentation de racks Oracle (NGR).

Câble d'alimentation ATO	Equivalent PTO	Description	Ampères	Tension	Câble
333W-10-13-C14RA	X9237-1-A-N	Câble d'alimentation, Jmpr, 1,0 m, C14RA, 13 A, C13	13	250	180-2082-01
333W-25-13-C14RA	X9238-1-A-N	Câble d'alimentation, Jmpr, 2,5 m, C14RA, 13 A, C13	13	250	180-2085-01

Tableau 6.7. Références des câbles d'alimentation Oracle Rack II (Redwood)

Câble d'alimentation ATO	Equivalent PTO	Description	Ampères	Tension	Câble
SR-JUMP-1MC13	XSR-JUMP-1MC13-N	Câble d'alimentation, Jmpr, SR2, 1,0 m, C14RA, 13 A, C13	13	250	180-2379-01
SR-JUMP-2MC13	XSR-JUMP-2MC13-N	Câble d'alimentation, Jmpr, SR2, 2,0 m, C14RA, 13 A, C13	13	250	180-2380-01