Oracle® Key Manager 3

Guia de Segurança

Release 3.1

E52210-02

Abril de 2016

ORACLE®

Oracle® Key Manager 3
Guia de Segurança

E52210-02

Índice

Lista de Tabelas

Prefácio

Este documento descreve os recursos de segurança do Oracle Key Manager 3 (OKM 3).

Público-alvo

Este guia destina-se a todos os usuários dos recursos de segurança do OKM 3, bem como ao pessoal envolvido na instalação e na configuração seguras do produto.

Acessibilidade da Documentação

Para obter informações sobre o comprometimento da Oracle com a acessibilidade, visite o site do Oracle Accessibility Program em http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Acesso ao Oracle Support
Os clientes da Oracle que adquiriram serviços de suporte têm acesso a suporte eletrônico por meio do My Oracle Support. Para obter informações, visite http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info ou http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs se você for portador de deficiência auditiva.

1

Capítulo 1. Visão Geral

Esta seção oferece uma visão geral do produto e explica os princípios gerais da segurança de aplicativos.

1.1. Visão Geral do Produto

O Oracle Key Manager (OKM) cria, armazena e gerencia chaves de criptografia. Ele consiste nos seguintes componentes:

- KMA (Key Management Appliance) – Um compartimento protegido que oferece serviços de Gerenciamento do Ciclo de Vida de Chaves, autenticação, controle de acesso e provisionamento de chaves baseados em política. Como uma autoridade confiável para redes de armazenamento, o KMA garante que todos os dispositivos de armazenamento sejam registrados e autenticados, e que todas as operações de provisionamento e exclusão estejam de acordo com as políticas prescritas.
- GUI do Oracle Key Manager – Uma Interface Gráfica do Usuário que é executada em uma estação de trabalho e que se comunica com o KMA em uma rede IP para configurar e gerenciar o OKM. A GUI do Oracle Key Manager deve ser instalada em uma estação de trabalho fornecida pelo cliente.
- CLIs do Oracle Key Manager – Duas Interfaces de Linha de Comandos executadas em uma estação de trabalho e que se comunicam com o KMA em uma rede IP para automatizar operações administrativas executadas com frequência. As CLIs do Oracle Key Manager devem ser instaladas em uma estação de trabalho fornecida pelo cliente.
- Cluster do OKM – O conjunto completo de KMAs do sistema. Todos esses KMAs reconhecem uns aos outros e replicam as informações entre si.
- Agente – Um dispositivo ou software que executa a criptografia usando as chaves gerenciadas pelo Cluster do OKM. Uma unidade de fita de criptografia StorageTek é um exemplo de agente. Os agentes se comunicam com os KMAs usando o Protocolo de Agente KMS. A API de Agente é um conjunto de interfaces de software incorporadas no hardware ou no software do agente.

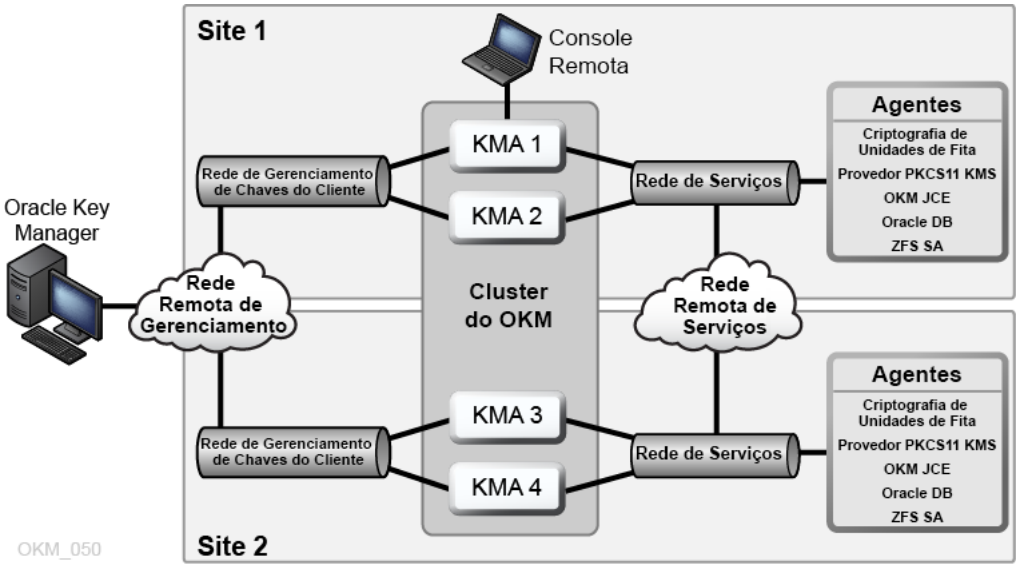
O OKM usa a rede TCP/IP para as conexões entre KMAs, Agentes e estações de trabalho em que a GUI e as CLIs do Oracle Key Manager estão sendo executadas. Para oferecer conexões de rede flexíveis, são fornecidas três interfaces em cada KMA:

- A conexão de gerenciamento – Destinada à conexão com a rede do cliente
- A conexão de serviço – Destinada à conexão com os agentes

- A conexão com o ILOM/ELOM – Destinada à conexão com o ILOM ou o ELOM no KMA

Veja o exemplo na seguinte imagem:

Figura 1.1.



1.2. Princípios Gerais de Segurança

Os princípios a seguir são essenciais para o uso seguro de qualquer aplicativo.

1.2.1. Mantenha o Software Atualizado

Um dos princípios da boa prática de segurança é manter todas as versões e patches do software atualizados. Os instaladores e os pacotes de atualização mais recentes do Oracle Key Manager estão disponíveis no site do My Oracle Support: `http://support.oracle.com`.

1.2.2. Restrinja o Acesso à Rede aos Serviços Críticos

Mantenha seus aplicativos de negócios atrás de um firewall. O firewall garante que o acesso a esses sistemas seja restrito a uma rota de rede conhecida, que pode ser monitorada e restringida, se necessário. Como alternativa, um roteador de firewall é usado no lugar de vários firewalls independentes.

1.2.3. Siga o Princípio do Privilégio Mínimo

O princípio do privilégio mínimo indica que os usuários devem receber o menor número possível de privilégios para executar suas tarefas. A concessão muito ambiciosa de responsabilidades, atribuições, concessões etc. com frequência deixa o sistema sujeito a

abusos, especialmente no início do ciclo de vida de uma organização, quando há escassez de pessoal e o trabalho precisa ser realizado com rapidez. Os privilégios do usuário devem ser revistos periodicamente a fim de determinar a relevância para as responsabilidades do cargo atual.

1.2.4. Monitore a Atividade do Sistema

A segurança do sistema é apoiada em três pilares: bons protocolos de segurança, configuração adequada do sistema e monitoramento do sistema. As operações de auditoria e análise de registros de auditoria atendem a esse terceiro requisito. Cada componente de um sistema tem algum grau de capacidade de monitoramento. Siga as dicas fornecidas neste documento e monitore regularmente os registros de auditoria.

1.2.5. Mantenha-se Atualizado com as Informações Mais Recentes sobre Segurança

A Oracle aprimora continuamente seu software e a documentação relacionada. Verifique anualmente as revisões no site My Oracle Support.

2

Capítulo 2. Instalação e Configuração Seguras

Esta seção destaca o processo de planejamento de uma instalação segura e descreve várias topologias de implantação recomendadas para os sistemas.

2.1. Compreenda o Seu Ambiente

Para entender melhor as suas necessidades de segurança, responda as seguintes perguntas:

2.1.1. Quais recursos estou protegendo?

Muitos recursos do ambiente de produção podem ser protegidos. Considere os recursos que deseja proteger ao decidir o nível de segurança a ser fornecido.

Normalmente, o principal recurso a ser protegido são os dados. Outros recursos são descritos aqui, pois estão associados ao gerenciamento e à proteção dos dados. Algumas das preocupações relacionadas a essa proteção incluem a perda de dados (ou seja, a indisponibilidade dos dados) e o comprometimento ou a divulgação de dados para partes não autorizadas.

Geralmente, chaves criptográficas são usadas para proteger os dados contra divulgação não autorizada. Portanto, esse é outro recurso que deve ser protegido. O gerenciamento de chaves altamente confiável é essencial para manter a alta disponibilidade dos dados. Outra camada de recursos que precisa ser protegida são os ativos contidos no próprio Cluster do Oracle Key Manager, incluindo os KMAs (Key Management Appliances).

2.1.2. Estou protegendo os recursos contra o acesso de quem?

Esses recursos devem ser protegidos contra o acesso de todas as pessoas não autorizadas a acessá-los. Eles devem ser protegidos fisicamente. Considere quais dos seus funcionários devem ter acesso a esses recursos. Em seguida, identifique quais tipos de operações cada funcionário poderá executar no ambiente do Oracle Key Manager.

2.1.3. O que acontecerá se as proteções dos recursos estratégicos falharem?

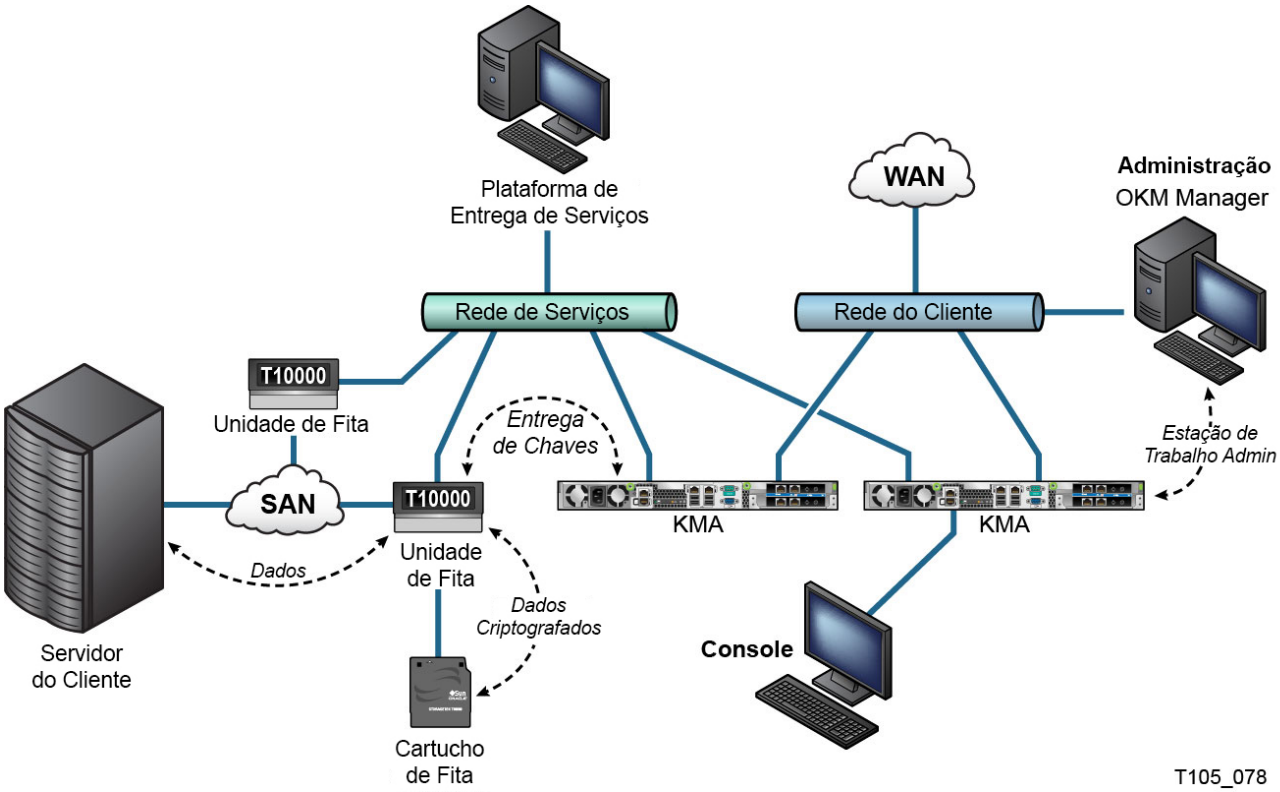
Em alguns casos, uma falha no esquema de segurança é facilmente detectada e considerada nada mais do que uma inconveniência. Em outros casos, uma falha poderá causar danos a

empresas ou a clientes individuais que utilizam os recursos. Compreender as ramificações de segurança dos recursos vai ajudar você a protegê-los de forma adequada.

2.2. Topologias de Implantação Recomendadas

A figura a seguir mostra uma implantação típica de uma solução do Oracle Key Manager.

Figura 2.1. Implantação Típica de uma Solução do OKM



2.3. Instalando um KMA (Key Management Appliance)

Esta seção descreve como instalar e configurar um KMA (Key Management Appliance) do OKM com segurança.

Os KMAs são fabricados como appliances protegidos que já dispõem da funcionalidade do Oracle Key Manager.

A instalação e a configuração de KMAs em um Cluster do OKM envolvem as seguintes etapas:

1. Instale cada KMA em um rack.
2. Para cada KMA, proteja o respectivo ILOM.

3. Configure o primeiro KMA no Cluster do OKM.
4. Adicione outros KMAs ao Cluster do OKM.

Mais informações sobre como planejar a implantação de um Cluster do OKM são fornecidas no OKM *Overview and Planning Guide*.

2.3.1. Instalando um KMA em um Rack

Um Engenheiro de Suporte ao Cliente da Oracle instala um KMA em um rack de acordo com os procedimentos descritos no *Oracle Key Manager Installation and Service Manual*. O pessoal de suporte ao cliente da Oracle poderá consultar esse manual para obter informações mais detalhadas.

2.3.2. Protegendo o ILOM de um KMA

Os KMAs do Oracle Key Manager são fabricados com o firmware mais recente do ILOM. O ILOM de um KMA deve ser protegido por um Engenheiro de Suporte ao Cliente da Oracle ou pelo cliente. O ILOM também deverá ser protegido após o upgrade do respectivo firmware.

A proteção do ILOM consiste em configurar definições específicas do ILOM a fim de impedir alterações que possam comprometer a segurança. Para obter instruções, consulte "ILOM Security Hardening" no apêndice Service Processor Procedures do OKM *Administration Guide*.

2.3.3. Configurando o Primeiro KMA em um Cluster do OKM

Antes de configurar o primeiro KMA, primeiro identifique as credenciais de divisão de chaves, bem como os IDs de usuário e as frases-senhas a serem definidos neste Cluster do OKM. Você pode usar uma planilha para este objetivo, como a encontrada no OKM *Installation and Service Manual* (apenas para uso interno) — solicite ao seu representante de suporte da Oracle.

Forneça essas credenciais de divisão de chaves, os IDs de usuário e as frases-senhas ao pessoal adequado. Consulte o tópico "Proteção por Quorum." mais adiante nesta documentação para obter mais informações.

Observação:

Guarde e proteja essas credenciais de divisão de chaves, bem como os IDs de usuário e as frases-senhas!

Abra um Web browser, inicie a Console Remota e, em seguida, inicie o utilitário QuickStart do OKM nessa console. Para inicializar o Cluster do OKM nesse KMA, siga o procedimento Initialize Cluster descrito no *Oracle Key Manager Administration Guide* incluído nas bibliotecas de documentação do Oracle Key Manager.

As credenciais de divisão de chaves e um usuário com privilégios de Oficial de Segurança são definidos durante este procedimento. Uma vez concluído o procedimento QuickStart, o usuário com privilégios de Oficial de Segurança deverá fazer log-in no KMA e definir outros usuários do OKM.

2.3.4. Considerações sobre a Definição de Credenciais de Divisão de Chaves

A definição de um menor número de frases-senhas e IDs de usuário de divisão de chaves, bem como de um limite mais baixo, é mais conveniente, porém menos segura. A definição de um maior número de frases-senhas e IDs de usuário de divisão de chaves, bem como de um limite mais alto, é menos conveniente, porém mais segura.

2.3.5. Considerações sobre a Definição de Usuários Adicionais do OKM

A definição de um menor número de usuários do OKM, alguns dos quais com várias atribuições designadas, é mais conveniente, porém menos segura. A definição de mais usuários do OKM, a maioria dos quais com apenas uma atribuição designada, é menos conveniente, porém mais segura, uma vez que facilita o rastreamento das operações executadas por determinado usuário do OKM.

2.3.6. Adicionando Outros KMAs ao Cluster do OKM

Abra um Web browser, inicie a Console Remota e, em seguida, inicie o utilitário QuickStart do OKM nessa console. Para adicionar esse KMA ao Cluster do OKM, siga o procedimento Join Cluster descrito no *Oracle Key Manager Administration Guide* em:

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

2.3.7. Considerações sobre a Adição de Outros KMAs

O Oracle Key Manager oferece a opção de Desbloqueio Autônomo para cada KMA. Essa opção é definida durante o procedimento QuickStart para o primeiro e os demais KMAs de um Cluster e pode ser modificada pelo Oficial de Segurança posteriormente.

Se a opção Desbloqueio Autônomo estiver ativada, o KMA desbloqueará a si mesmo automaticamente durante a inicialização e será capaz de fornecer as chaves sem exigir a aprovação do quorum. Se essa opção estiver desativada, o KMA permanecerá bloqueado durante a inicialização e não fornecerá as chaves até que o Oficial de Segurança envie uma solicitação de desbloqueio e um quorum a aprove.

Para garantir a segurança máxima, a Oracle não aconselha ativar o desbloqueio autônomo. Para obter mais informações sobre a opção Desbloqueio Autônomo, consulte o *Oracle Key Manager Version 2.x Security and Authentication White Paper* em:

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

2.3.8. Características dos KMAs Protegidos

Conforme mencionado anteriormente, os KMAs são fabricados como appliances protegidos que já dispõem da funcionalidade do Oracle Key Manager. Como appliances protegidos, eles têm as seguintes características:

- Os pacotes Solaris desnecessários não são incluídos na imagem do Solaris. Por exemplo, os utilitários e os serviços ftp e telnet não aparecem nessa imagem.
- Os KMAs não produzem arquivos de núcleo.
- O utilitário de log-in padrão do Solaris(1) foi substituído pela Console do OKM. Portanto, os usuários não podem fazer log-in na console do Solaris.
- Por padrão, o serviço ssh permanece desativado. Para fins de suporte ao cliente, o usuário com privilégios de Oficial de Segurança poderá ativar esse serviço e definir uma conta de suporte por um período limitado. Essa conta, que tem acesso e permissões limitados, é a única disponível. A auditoria do Solaris rastreia os comandos chamados pela conta de suporte.
- A conta raiz está desativada e foi configurada como uma atribuição.
- Os KMAs não dispõem de uma unidade de DVD.
- As portas USB estão desativadas.
- As portas de rede não utilizadas estão fechadas.
- As pilhas não executáveis estão ativadas.
- A randomização de lookup do espaço de endereço está configurada.
- Os heaps não executáveis estão ativados.
- A criptografia ZFS é usada na segurança de sistemas de arquivos confidenciais.
- O Solaris está configurado para ter conformidade com o benchmark SCAP PCI-DSS.
- Os serviços SMF desnecessários estão desativados.
- O Oracle Solaris Verified Boot pode ser configurado em KMAs baseados no SPARC T7-1 para proteger o processo de inicialização do sistema contra danos nos módulos de kernel, contra a inserção de kits raiz ou contra outros programas mal-intencionados.
- Os KMAs mais recentes baseados em servidores SPARC T7-1 e Netra SPARC T4-1 são invioláveis (falha do ILOM) quando a porta do chassis é acessada enquanto o equipamento está ligado.
- O firmware do ILOM 3.2 agora tem a certificação FIPS 140-2 Nível 1 e pode ser configurado no modo FIPS.
- A BART (Basic Audit and Report Tool) é executada periodicamente para ajudar na auditoria de dados. Esses relatórios são incluídos nos dumps de sistema do OKM.
- O Solaris Cryptographic Security Framework está configurado de acordo com as políticas de segurança FIPS 140-2 Nível 1 (documentadas para o Solaris 11.1) com ou sem a presença de um Módulo de Segurança de Hardware.

2.4. Conexões de TCP/IP e o KMA

Se existir um firewall entre as entidades (OKM Manager, agentes e outros KMAs no mesmo cluster) e o KMA, o firewall deverá permitir que a entidade estabeleça conexões TCP/IP com o KMA nas seguintes portas:

- A comunicação entre o OKM Manager e KMAs requer as portas 3331, 3332, 3333, 3335.
- A comunicação entre Agentes e KMAs requer as portas 3331, 3332, 3334, 3335.
- A comunicação entre KMAs requer as portas 3331, 3332, 3336.

Observação:

Para usuários que configuram seus KMAs com o objetivo de usar endereços IPv6, configure firewalls de borda baseados no IPv4 para eliminar todos os pacotes de saída IPv4 do protocolo 41 e configure pacotes da porta UDP 3544 para impedir que os hosts da Internet usem tráfego tunelado IPv6 sobre IPv4 para acessar hosts internos.

Consulte a documentação da configuração do seu firewall para obter detalhes. Tabela 2.1, “Conexões de Porta KMA ” lista as portas que os KMAs utilizam explicitamente ou as portas nas quais os KMAs fornecem serviços.

Tabela 2.1. Conexões de Porta KMA

Número da Porta	Protocolo	Direção	Descrição
22	TCP	Listener	SSH (somente quando o Suporte Técnico está ativado)
123	TCP/UDP	Listener	NTP
3331	TCP	Listener	OKM CA Service
3332	TCP	Listener	OKM Certificate Service
3333	TCP	Listener	OKM Management Service
3334	TCP	Listener	OKM Agent Service
3335	TCP	Listener	OKM Discovery Service
3336	TCP	Listener	OKM Replication Service

Tabela 2.2, “Outros Serviços ” mostra outros serviços com listener em portas que possivelmente não são utilizadas.

Tabela 2.2. Outros Serviços

Número da Porta	Protocolo	Direção	Descrição
53	TCP/UDP	Conexão	DNS (somente quando o KMA está configurado para usar DNS)
68	UDP	Conexão	DHCP (somente quando o KMA está configurado para usar DNS)
111	TCP/UDP	Listener	RPC (KMAs respondem a consultas rpcinfo). Esta porta permanece aberta para solicitações externas somente no KMS 2.1 ou em versões anteriores

Número da Porta	Protocolo	Direção	Descrição
161	UDP	Conexão	SNMP (somente quando Gerenciadores de SNMP estiverem definidos)
161	UDP	Listener	SNMP (somente quando o Hardware Management Pack está ativado)
514	TCP	Conexão	Syslog remoto (somente quando servidores syslog remotos estão definidos e configurados para usar TCP decriptografado)
546	UDP	Conexão	DHCPv6 (somente quando o KMA está configurado para usar DHCP e IPv6)
4045	TCP/UDP	Listener	Daemon de bloqueio NFS (KMS 2.0 somente)
6514	NetBios sobre TCP	Conexão	Syslog remoto (somente quando servidores syslog remotos estão definidos e configurados para usar TLS)

Observação:

A porta 443 deve estar aberta para permitir que os clientes acessem a interface Web do Processador de Serviços e a Console do OKM por meio do firewall. Consulte o *Oracle Key Manager Installation and Service Manual* (somente para uso interno) para ver as portas ELOM e ILOM.

Tabela 2.3, “Portas ELOM/ILOM ” lista as portas ELOM/ILOM do KMA. Essas portas serão ativadas se o acesso ao ELOM/ILOM for necessário a partir de fora do firewall; caso contrário, eles não precisarão ser ativados para o endereço IP do ELOM/ILOM:

Tabela 2.3. Portas ELOM/ILOM

Número da Porta	Protocolo	Direção	Descrição
22	TCP	Listener	SSH (para interface de linha de comandos ELOM/ILOM)
53	TCP/UDP	Conexão	DNS (somente necessário quando o DNS está configurado)
68	UDP	Conexão	Se o DHCP for obrigatório para o ELOM/ILOM. **Observação**: A documentação para DHCP e ELOM/ILOM não está disponível; no entanto, é suportada.

80	TCP	Listener	HTTP (para a interface Web do ELOM/ILOM)
			
			Se o HTTP for necessário; caso contrário, os usuários poderão ver instruções sobre como estabelecer conexão com a console remota em:
			
			ELOM:
			
			`http://docs.oracle.com/cd/E19121-01/sf.x2100m2/819-6588-14/819-6588-14.pdf`
			
			ILOM:
			
			`http://docs.oracle.com/cd/E19860-01/index.html`

161	UDP	Listener /Conexão	SNMPv3 (configurável; esta é a porta padrão)
443	TCP /TLS	Listener	Embedded/Integrated Lights Out Manager

Número da Porta	Protocolo	Direção	Descrição
			Web Services DMTF (Desktop Management Task Force) para WS-Man (Management Protocol) sobre TLS (Transport Layer Security)
623	UDP	Listener	IPMI (Intelligent Platform Management Interface)

3

Capítulo 3. Funcionalidades de Segurança

Esta seção descreve os mecanismos específicos de segurança oferecidos pelo produto.

3.1. Ameaças Potenciais

Estas são as principais preocupações dos clientes que têm agentes habilitados para criptografia:

- Divulgação de informações, violando a política
- Perda ou destruição de dados
- Atraso inaceitável na restauração de dados em caso de uma falha catastrófica (por exemplo, em um site de continuidade de negócios)
- Modificação de dados não detectada.

3.2. Objetivos das Funcionalidades de Segurança

O objetivo das funcionalidades de segurança do Oracle Key Manager são:

- Proteger os dados criptografados contra divulgação.
- Minimizar a exposição a ataques.
- Oferecer um nível de confiabilidade e disponibilidade suficientemente alto.

3.3. O Modelo de Segurança

Esta seção do guia de segurança deve apresentar uma visão geral de alto nível das ameaças que o sistema deve combater e de como as funcionalidades de segurança individuais são combinadas para impedir os ataques.

As funcionalidades de segurança que oferecem essas proteções são:

- Autenticação – Garante o acesso somente de indivíduos autorizados ao sistema e aos dados
- Autorização – Controla o acesso aos privilégios e aos dados do sistema; esse controle baseia-se na autenticação para garantir que os indivíduos tenham somente o acesso apropriado
- Auditoria – Permite que os administradores detectem tentativas de violação do mecanismo de autenticação e tentativas ou violações bem-sucedidas do controle de acesso.

Para obter mais informações sobre a segurança e a autenticação do Oracle Key Manager, consulte o *Oracle Key Manager Version 2.x Security and Authentication White Paper* em:

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

3.4. Autenticação

A arquitetura do Oracle Key Manager permite a autenticação mútua entre todos os elementos do sistema: entre KMA e KMA, entre agente e KMA e entre GUI ou CLI do Oracle Key Manager e KMA para operações do usuário.

Cada elemento (por exemplo, um novo agente de criptografia) é inscrito no sistema por meio da criação de um ID e de uma frase-senha no OKM, os quais são inseridos no elemento a ser adicionado. Por exemplo, quando uma unidade de fita é adicionada ao sistema, o agente e o KMA executam automaticamente um protocolo de desafio/resposta baseado na frase-senha compartilhada. Como resultado, o agente obtém o certificado da Autoridade de Certificação (CA) raiz, bem como um novo par de chaves e um certificado assinado. Após obter o certificado da CA raiz, o certificado de agente e o par de chaves, o agente poderá executar o protocolo TLS (Transport Layer Security) para todas as comunicações subsequentes com os KMAs. Todos os certificados são certificados X.509.

O OKM se comporta com uma autoridade de certificação raiz para gerar um certificado raiz que os KMAs, por sua vez, utilizam para derivar (autoassinar) os certificados usados pelos agentes, pelos usuários e pelos novos KMAs.

3.5. Controle de Acesso

Estes são os tipos de controle de acesso:

- Controle de Acesso Baseado em Atribuição e Usuários
- Proteção por Quorum.

3.5.1. Controle de Acesso Baseado em Atribuição e Usuários

O Oracle Key Manager permite definir vários usuários, cada um com um ID de usuário e uma frase-senha. Cada usuário tem uma ou mais atribuições predefinidas. Essas atribuições determinam quais operações o usuário tem permissão de executar em um sistema Oracle Key Manager. As atribuições são:

- Oficial de Segurança – Executa a configuração e o gerenciamento do Oracle Key Manager
- Operador – Executa a configuração de agentes e as operações diárias
- Oficial de Conformidade – Define os Grupos de Chaves e controla o acesso dos agentes a esses grupos
- Operador de Backup – Executa operações de backup

- Auditor – Exibe as trilhas de auditoria do sistema
- Membro do Quorum – Exibe e aprova operações pendentes do quorum

Um Oficial de Segurança é definido durante o processo QuickStart, que configura um KMA em um Cluster do OKM. Posteriormente, um usuário deverá fazer log-in no Cluster como Oficial de Segurança utilizando a GUI do Oracle Key Manager para definir outros usuários. O Oficial de Segurança poderá designar várias atribuições a determinado usuário, bem como designar uma atribuição específica a vários usuários.

Para obter mais informações sobre as operações permitidas por cada atribuição e como o Oficial de Segurança cria usuários e designa atribuições a eles, consulte o *Oracle Key Manager Administration Guide* incluído nas bibliotecas de documentação do Oracle Key Manager em:

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

Esse controle de acesso baseado em atribuição suporta as atribuições operacionais do NIST (National Institute of Standards and Technology) SP (Special Publication) 800-60 para segregação de funções operacionais.

3.5.2. Proteção por Quorum.

Algumas operações são extremamente críticas e exigem um maior nível de segurança. Exemplos dessas operações incluem a adição de um KMA a um Cluster do OKM, o desbloqueio de um KMA, a criação de usuários e a adição de atribuições a usuários. Para implementar essa segurança, o sistema usa um conjunto de credenciais de divisão de chaves, além do acesso baseado em atribuição descrito anteriormente.

As credenciais de divisão de chaves consistem em um conjunto de pares de ID de usuário e frase-senha, juntamente com o número mínimo desses pares necessário para que o sistema permita que certas operações sejam concluídas. Essas credenciais também são denominadas "o quorum" e o número mínimo é chamado "o limite do quorum".

O Oracle Key Manager permite até 10 pares de ID de usuário/frase-senha de divisão de chaves e um limite a ser definido. Eles são definidos durante o processo QuickStart quando o primeiro KMA é configurado em um Cluster do OKM. Os IDs de usuário e as frases-senhas de divisão de chaves são diferentes dos utilizados para fazer log-in no sistema. Quando o usuário tentar executar uma operação que exige a aprovação do quorum, o limite definido de usuários e frases-senhas de divisão de chaves deve aprovar essa operação para que o sistema a execute.

3.6. Auditorias

Cada KMA registra os eventos de auditoria referentes às operações que ele executa, incluindo os emitidos por agentes, usuários e KMAs correspondentes no Cluster do OKM. Os KMAs

também registram eventos de auditoria sempre que ocorre falha na autenticação de um agente, usuário ou KMA correspondente. Os eventos de auditoria que indicam uma violação de segurança são anotados. Uma falha na autenticação é um exemplo de evento de auditoria que indica uma violação de segurança. Se Agentes SNMP forem identificados no Cluster do OKM, os KMAs também enviarão SNMP INFORMs a esses agentes SNMP caso encontrem uma violação de segurança. Se o Syslog Remoto tiver sido configurado, o KMA também encaminhará essas mensagens de auditoria aos servidores configurados. Consulte Capítulo 5, *Syslog Remoto* .

Para que possam exibir os eventos de auditoria, os usuários devem fazer log-in de maneira adequada no Cluster do OKM e ter uma atribuição designada a eles.

Os KMAs gerenciam os respectivos eventos de auditoria. Os KMAs removem os eventos de auditoria mais antigos com base nos termos e nos limites (contagens) de retenção. O Oficial de Segurança poderá modificar esses termos e limites conforme necessário.

3.7. Outras Funcionalidades de Segurança

O Oracle Key Manager fornece outras funcionalidades de segurança. Para obter mais informações sobre essas e outras funcionalidades do OKM, consulte o documento *Oracle Key Manager Overview* em:

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

3.7.1. Comunicação Segura

O protocolo de comunicação entre um agente e um KMA, um usuário e um KMA, e um KMA e um KMA correspondente é o mesmo. Em cada um desses casos, o sistema usa a frase-senha da entidade que inicia a comunicação para executar um protocolo de desafio/resposta. Se a execução for bem-sucedida, a entidade receberá um certificado e a chave privada correspondente. Esse certificado e a chave privada podem estabelecer um canal TLS (Transport Layer Security) (soquetes seguros). A autenticação mútua é executada; cada extremidade de uma conexão autentica a outra. Os KMAs a partir da versão OKM 3.1 em diante, sempre utilizarão o TLS 1.2 para seu tráfego de replicação correspondente.

3.7.2. Módulo de Segurança de Hardware

Os KMAs têm um Módulo de Segurança de Hardware disponível, que é encomendado separadamente. Esse Módulo de Segurança de Hardware – uma placa SCA (Sun Cryptographic Accelerator) 6000 – foi certificado pelo FIPS 140-2 Nível 3 e fornece chaves de criptografia AES (Advanced Encryption Standard) de 256 bits (este certificado expirou em 12/31/2015 e não está sendo atualizado; um HSM alternativo será fornecido em uma release subsequente). A placa SCA 6000 suporta o modo de operação FIPS 140-2 Nível 3, e o OKM sempre a utiliza dessa maneira. Quando o Cluster do OKM opera no modo compatível com

FIPS, as chaves de criptografia não ultrapassam o limite criptográfico da placa SCA 6000 em um formato não encapsulado. A placa SCA 6000 usa o gerador de números aleatórios aprovado pelo FIPS, conforme especificado no FIPS 186-2 DSA Random Number Generator usando o SHA-1 para geração das chaves de criptografia.

Quando um KMA não é configurado com uma placa SCA 6000, a criptografia é executada com o token de software SCF (Solaris Cryptographic Framework) PKCS#11. O SCF é configurado no modo FIPS 140 de acordo com as políticas de segurança Solaris FIPS 140-2 publicadas mais recentemente.

3.7.3. Encapsulamento de Chaves AES

O Oracle Key Manager usa o Encapsulamento de Chaves AES (RFC 3994) com chaves de criptografia de 256 bits para proteger as chaves simétricas quando elas são criadas, armazenadas no KMA, transmitidas para agentes ou nos arquivos de transferência de chaves.

3.7.4. Replicação de Chaves

Quando o primeiro KMA de um Cluster do OKM é inicializado, o KMA gera um grande pool de chaves. Quando outros KMAs são adicionados ao Cluster, as chaves são replicadas para os novos KMAs e podem ser usadas para criptografar dados. Cada KMA adicionado ao Cluster gera um pool de chaves e replica-os para os KMAs correspondentes no Cluster. Todos os KMAs gerarão novas chaves, conforme necessário, para manter o tamanho do pool de chaves de forma que haja sempre chaves prontas disponíveis para os agentes. Quando um agente necessita de uma nova chave, ele entra em contato com um KMA do Cluster e a solicita. O KMA extrai uma chave pronta de seu pool de chaves e a atribui ao grupo de chaves padrão do agente e à unidade de dados. Em seguida, o KMA replica essas atualizações do banco de dados na rede para os demais KMAs do Cluster. Posteriormente, o agente poderá entrar em contato com outro KMA do Cluster para recuperar a chave. Nenhum material de chaves com texto não criptografado é transmitido pela rede em momento algum.

3.7.5. Políticas de Segurança Solaris FIPS 140-2

Em dezembro de 2013, o NIST (National Institute of Standards and Technology) premiou o módulo Oracle Solaris Kernel Cryptographic Framework do Solaris 11 com o certificado de validação número 2061 do padrão FIPS 140-2 Nível 1. Em janeiro de 2014, o NIST (National Institute of Standards and Technology) premiou o módulo Oracle Solaris Kernel Cryptographic Framework baseado nos processadores SPARC T4 e SPARC T5 com o certificado de validação número 2076 do padrão FIPS 140-2 Nível 1. O KMA do Oracle Key Manager 3.1.0 agora se baseia no Solaris 11.3, que ainda está passando pelos testes de validação do FIPS 140-2. O Oracle Solaris Kernel Cryptographic Framework em um KMA do Oracle Key Manager está configurado de acordo com a *Política de Segurança do Oracle Kernel Cryptographic Framework*. Da mesma forma, o KMA também está configurado com a *Política de Segurança do Oracle Solaris Userland Cryptographic Framework baseado nos processadores SPARC T4 e SPARC T5*. O OKM será atualizado com as políticas de segurança mais recentes do Solaris, à medida que elas forem disponibilizadas.

3.7.6. Upgrades de Software

Todos os bundles de upgrade de software do KMA são assinados digitalmente para impedir o carregamento de softwares mal-intencionados de origens não aprovadas.

4

Capítulo 4. Pontos Finais

O OKM suporta uma grande variedade de pontos finais de criptografia. Estes são os pontos finais suportados:

- Unidades de fita com capacidade de criptografia
- Oracle Transparent Database Encryption (TDE) 11g e versões mais recentes
- Oracle ZFS Storage Appliance
- Sistemas de arquivos ZFS do Oracle Solaris 11

Além disso, as ferramentas de pontos finais estão disponíveis para desenvolvedores de aplicativos ou, no caso do PKCS#11, para uso com a TDE (Transparent Database Encryption) do Oracle Database.

4.1. Provedor Linux PKCS#11 KMS

Um provedor Linux PKCS#11 KMS está disponível para os clientes que desejam se comunicar com o OKM utilizando o PKCS#11. O administrador pode fazer download do provedor Linux PKCS#11 KMS no site My Oracle Support e instalá-lo em um servidor Oracle Enterprise Linux. O provedor Linux PKCS#11 KMS tem as mesmas características de segurança que outros agentes e autentica-se da mesma forma que eles nos appliances do Oracle Key Manager. Esse provedor armazena um arquivo de log e informações de perfil no diretório `/var/opt/kms/username`. O usuário e/ou o administrador devem gerenciar esse arquivo de log manualmente ou com um utilitário como logrotate. O controle de acesso ao diretório `/var/opt/kms/username` deve ser restringido por meio das permissões adequadas. No diretório de perfil, as credenciais de autenticação do agente são mantidas em um arquivo PKCS#12. O arquivo PKCS#12 é protegido com uma senha. Para obter mais informações sobre o provedor Linux PKCS#11 KMS, consulte o *Oracle Key Manager Administration Guide* incluído nas bibliotecas de documentação do Oracle Key Manager em:

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

4.2. Provedor PKCS#11 KMS para Solaris

Um provedor PKCS#11 KMS análogo está disponível com o Solaris 10 e o Solaris 11.

4.3. Provedor JCE KMS

Um provedor JCE (Java Cryptographic Environment) está disponível para os desenvolvedores que desejam implementar aplicativos clientes Java que podem obter chaves do OKM. Este produto foi integrado com diversos produtos Oracle e está disponível no site Oracle Technology Network.

4.4. Plug-in do OKM para Oracle Enterprise Manager

O plug-in de appliance do OKM (Oracle Key Manager) para o OEM (Oracle Enterprise Manager) Cloud Control fornece funcionalidades de monitoramento para clusters do OKM. Cada KMA pertencente a um cluster é monitorado pelo plug-in. Um guia de segurança é fornecido para esta ferramenta.

5

Capítulo 5. Syslog Remoto

O Oracle Key Manager suporta syslog remoto. Os KMAs podem ser configurados para enviar mensagens nos formatos RFC 3164 ou RFC 5424 a um servidor syslog remoto por meio de TCP não criptografado ou de TLS (Transport Layer Security). Observe que a RFC 5425 descreve o uso do TLS para fornecer uma conexão segura ao transporte de mensagens de syslog no formato de mensagem RFC 5424.

Um Oficial de Segurança pode configurar um KMA para enviar mensagens por meio de TCP não criptografado ou de TLS. É mais seguro usar o TLS para autenticar e para criptografar a comunicação entre o KMA e o servidor syslog remoto. O KMA autentica o servidor syslog remoto solicitando certificado e chave pública. Opcionalmente, o servidor syslog remoto pode ser configurado para usar autenticação mútua. A autenticação mútua garante que o servidor syslog remoto só aceite mensagens de clientes autorizadas (tais como KMAs). Quando configurado para usar a autenticação mútua, o servidor syslog remoto solicita um certificado do KMA para verificar a identidade do KMA.

6

Capítulo 6. Hardware Management Pack

O Oracle Key Manager suporta o Oracle HPM (Hardware Management Pack) em KMAs SPARC T7-1, Netra SPARC T4-1 e Sun Fire X4170 M2. O produto HMP é membro do Oracle Single System Management, juntamente com o ILOM. Um Oficial de Segurança pode permitir que o HMP em um KMA utilize um agente de gerenciamento no Solaris para possibilitar o monitoramento in-band do KMA sobre SNMP. O software do HMP é pré-instalado, mas permanece desativado com a configuração de agente SNMP. Consequentemente, a porta de listener do agente SNMP não é aberta até que o HMP seja ativado. Por padrão, o HMP permanece desativado.

A ativação do HMP oferece o seguinte:

- Notificações de eventos para problemas de hardware, antes de eles serem exibidos como notificações SNMP específicas do Oracle Key Manager ou como uma interrupção do KMA.
- Capacidade de ativar o HMP nos KMAs suportados em um cluster do OKM.
- Capacidade de usar operações SNMP Get para MIBS SNMP no KMA, incluindo MIB-II, SUN-HW-MONITORING-MIB e SUN-STORAGE-MIB.
- Integração do Oracle Red Stack com o Oracle Enterprise Manager por meio de Receivelets SNMP e Fetchlets SNMP.

Você deverá manter as considerações de segurança a seguir em mente ao optar por ativar o HMP em um KMA. Quando ativado, o HMP:

- Utiliza quaisquer Gerenciadores de protocolo SNMP v2c ativados no cluster do Oracle Key Manager. O protocolo SNMP v2c não tem os aperfeiçoamentos de segurança presentes no protocolo SNMP v3.
- Ativa um agente de gerenciamento SNMP no KMA, permitindo um acesso de rede somente para leitura a informações de MIB neste KMA.
- Os riscos de segurança identificados no *Oracle Hardware Management Pack (HMP) Security Guide* (`http://docs.oracle.com/cd/E20451_01/pdf/E27799.pdf`) são mitigados por:
  - "É possível usar produtos de gerenciamento de sistemas para obter um ambiente root inicializável"- A proteção de KMAs desativa o acesso raiz a usuários do sistema. O SNMP é configurado para acesso somente de leitura. Portanto, as operações SNMP Put são rejeitadas.

- "Os produtos de gerenciamento de sistemas incluem ferramentas avançadas que exigem privilégios de administrador ou root para serem executadas" - o acesso root a KMAs permanece desativado. Portanto, os usuários do sistema não podem executar essas ferramentas.

Apêndice A

Apêndice A. Lista de Verificação para uma Implantação Segura

A seguinte lista de verificação de segurança contém diretrizes que ajudam a proteger o seu sistema de gerenciamento de chaves:

1. Instale cada KMA em um ambiente fisicamente seguro.
2. Proteja o OpenBoot PROM ou BIOS em cada KMA.
3. Proteja o Lights Out Manager em cada KMA.
4. Defina a configuração de divisão de chaves para este Cluster do Oracle Key Manager.
5. Defina a opção de desbloqueio autônomo para cada KMA conforme apropriado.
6. Defina os usuários do Oracle Key Manager e as respectivas atribuições associadas.
7. Siga o princípio do privilégio mínimo
   a. Conceda a cada usuário do Oracle Key Manager somente as atribuições necessárias.
8. Monitore a atividade do Cluster do Oracle Key Manager.
   a. Investigue todos os erros, especialmente as Violações de Segurança, registrados no log de auditoria do Oracle Key Manager.
9. Faça backup da segurança básica quando a configuração da divisão de chaves for definida inicialmente e sempre que ela for modificada.
10. Faça backups do Oracle Key Manager regularmente.
11. Armazene os arquivos de backup da segurança básica e os arquivos de backup do Oracle Key Manager em um local seguro.

Apêndice B

Apêndice B. Referências

- Documentação do cliente do 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*
- *Oracle Key Manager Installation and Service Manual* (somente para uso interno) para ver as portas ELOM e ILOM.
- *Visão Geral do Oracle Key Manager*

  http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o10-013-st-ckm-solution-4-187263.pdf
- *Oracle Key Manager Version 2.X Security and Authentication White Paper*

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

  http://docs.oracle.com/cd/E37444_01/
- Documentação do Servidor SPARC T7-1 https://docs.oracle.com/cd/E54976_01/
- Documentação do Servidor Netra SPARC T4-1

  http://docs.oracle.com/cd/E23203_01/
- Documentação do Oracle Hardware Management Pack
  - Biblioteca de documentação do Oracle Hardware Management Pack

    http://docs.oracle.com/cd/E20451_01/
  - Oracle Single System Management

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

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

- Documentação da política de segurança para produtos Oracle:
  - *Política de Segurança do Oracle Solaris Kernel Cryptographic Framework*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2061.pdf
  - *Política de Segurança do Oracle Solaris Kernel Cryptographic Framework com SPARC T4 e T5*

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

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1050.pdf
  - *Política de Segurança de Unidade de Fita Oracle StorageTek T10000D*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2254.pdf
  - *Política de Segurança de Unidade de Fita Oracle StorageTek T10000C*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1561.pdf
  - *Política de Segurança da Unidade de Fita Oracle StorageTek T10000B*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1156.pdf
  - *Política de Segurança da Unidade de Fita Oracle StorageTek T10000A*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1157.pdf
  - *Política de Segurança da Unidade de Fita Oracle StorageTek T9480D*

    http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1288.pdf
- Certificados de validação FIPS para produtos Oracle:
  - Sun Crypto Accelerator 6000 - Certificado #1026 (Expirado)

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