Guia de Segurança do Oracle SuperCluster Série M7

Número do Item: E69655-01
Fevereiro de 2016

Conteúdo

Usando Esta Documentação

- **Visão geral** – fornece informações sobre planejamento, configuração e manutenção de um ambiente seguro para sistemas da série Oracle SuperCluster M7.
- **Público-alvo** – Técnicos, administradores de sistema e provedores de serviço autorizados
- **Conhecimento necessário** – experiência avançada com UNIX e administração de banco de dados.

Biblioteca de Documentação do Produto

A documentação e os recursos desse produto e dos produtos relacionados estão disponíveis em http://www.oracle.com/goto/sc-m7/docs.

Feedback

Forneça feedback sobre esta documentação em http://www.oracle.com/goto/docfeedback.

Noções Básicas dos Princípios de Segurança

Este guia fornece informações sobre planejamento, configuração e manutenção de um ambiente seguro para sistemas da série Oracle SuperCluster M7.

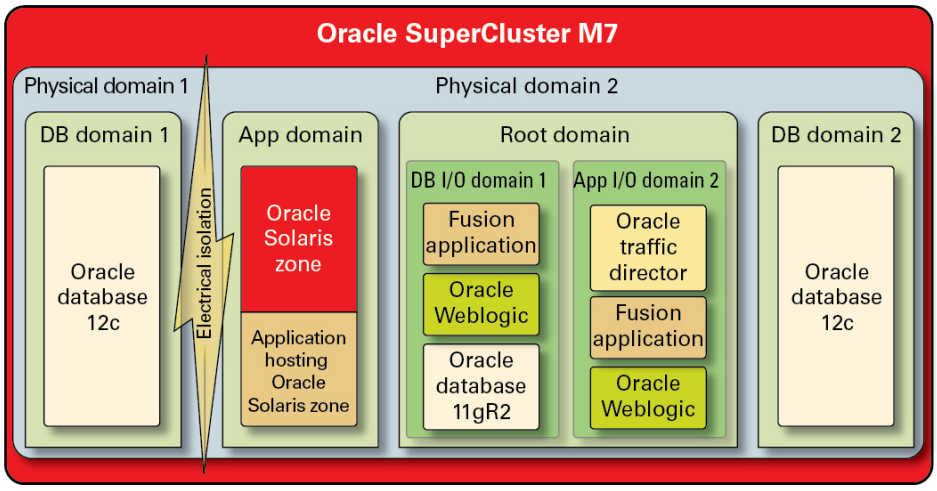
Os tópicos a seguir são tratados nesta seção:

Isolamento Seguro

O SuperCluster M7 dá suporte a uma variedade de estratégias de isolamento que provedores de nuvem podem selecionar com base em seus requisitos de segurança e controle. Essa flexibilidade permite que provedores de nuvem criem uma arquitetura multitenant personalizada e segura adequada para a sua empresa.

O SuperCluster M7 dá suporte a várias estratégias de isolamento de carga de trabalho, sendo que cada uma tem seu próprio conjunto de recursos. Embora seja possível usar cada estratégia de implementação de modo independente, elas também podem ser usadas juntas em uma abordagem híbrida permitindo que os provedores de nuvem implantem arquiteturas que possam equilibrar, com mais eficiência, suas necessidades de segurança, desempenho, disponibilidade, entre outras.

FIGURA 1 Isolamento Seguro com uma Configuração de Tenant Dinâmica



Os provedores de nuvem podem usar domínios físicos (também denominados PDomains) para situações nas quais seus hosts tenant estejam executando aplicativos e bancos de dados que devem ser isolados fisicamente de outras cargas de trabalho. Recursos físicos dedicados podem ser necessários para uma implantação devido à sua criticidade para a organização, o sigilo das informações que ela contém, as obrigações de conformidade ou simplesmente porque a carga de trabalho do banco de dados ou do aplicativo usará completamente os recursos de todo um sistema físico.

Para organizações que exijam o isolamento mediado por hipervisor, o Oracle VM Server para domínios SPARC, denominados domínios dedicados, são usados para criar ambientes virtuais que isolam instâncias de aplicativos e/ou banco de dados. Criado como parte da instalação do SuperCluster, cada domínio dedicado executa sua própria instância exclusiva do Oracle Solaris OS. O acesso a recursos físicos é mediado por hipervisores assistidos por hardware incorporados nos processadores SPARC.

Além disso, o SuperCluster permite criar domínios adicionais denominados domínios root, que tiram proveito da tecnologia de virtualização de E/S root única (SR-IOV). Os domínios root possuem um ou mais IB HCAs e 10 GbE NICs. Você pode optar por criar dinamicamente domínios adicionais, denominados domínios de E/S, sobre domínios root. O SuperCluster M7 inclui uma ferramenta baseada em navegador para criá-los e gerenciá-los.

No entanto, dentro de cada um desses domínios, os tenants de consumidor de nuvem podem aproveitar a tecnologia de Zonas do Oracle Solaris para criar ambientes isolados adicionais.

Usando zonas, é possível implantar instâncias individuais ou grupos de aplicativos ou bancos de dados em um ou mais contêineres virtualizados que são executados coletivamente em um único kernel OS. Essa abordagem leve da virtualização é usada para criar um limite de segurança mais forte ao redor dos serviços implantados.

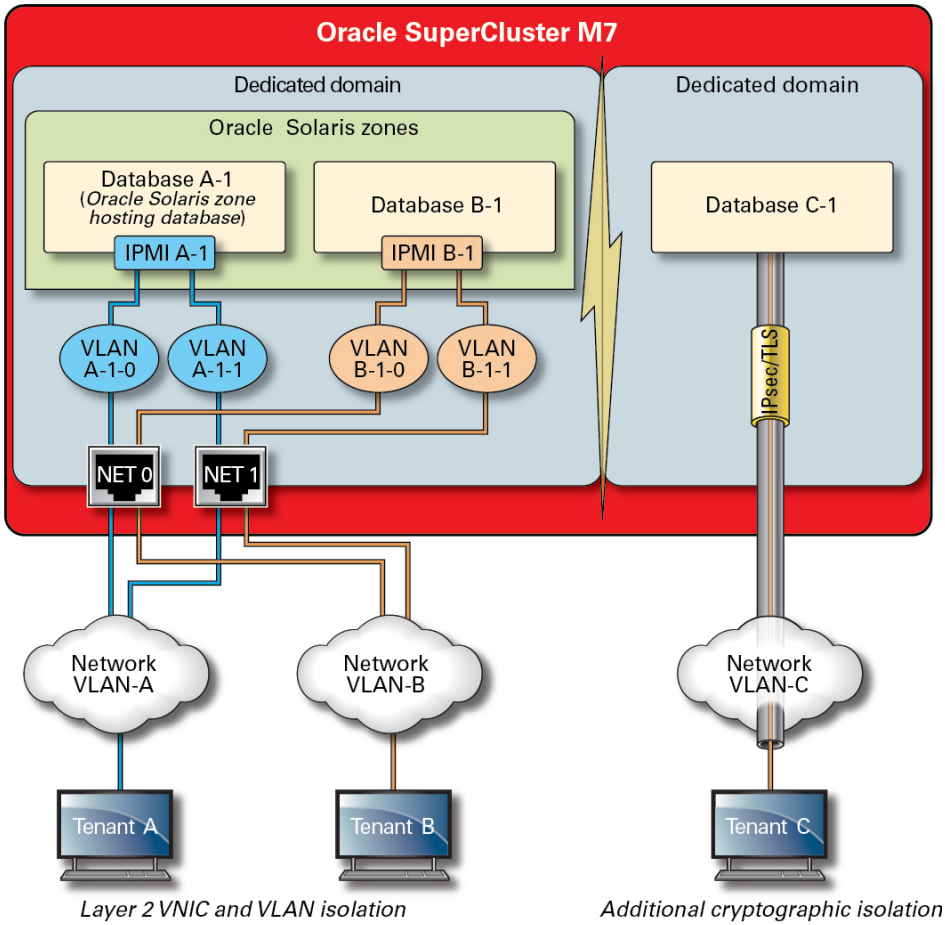
Os tenants que hospedam vários aplicativos e bancos de dados no SuperCluster também podem optar por empregar uma abordagem híbrida, usando uma combinação de estratégias de isolamento baseadas em Zonas do Oracle Solaris, domínios de E/S e domínios dedicados para criar arquiteturas flexíveis, mas resilientes, que se alinhem às suas necessidades de infraestrutura de nuvem. Com uma variedade de opções de virtualização, o SuperCluster permite aos tenants hospedados ser isolados de forma segura na camada de hardware e fornece Zonas do Oracle Solaris proporcionando maior segurança e isolamento no ambiente de tempo de execução.

Garantir que aplicativos individuais, bancos de dados, usuários e processos sejam isolados corretamente em seu sistema operacional host é uma boa primeira etapa. No entanto, é igualmente importante considerar as três redes primárias usadas no SuperCluster e como os recursos de isolamento de rede e comunicações que trafegam pela rede são protegidos:

- Rede de acesso ao 10 GbE Client
- Rede de serviço IB privado
- Rede de gerenciamento

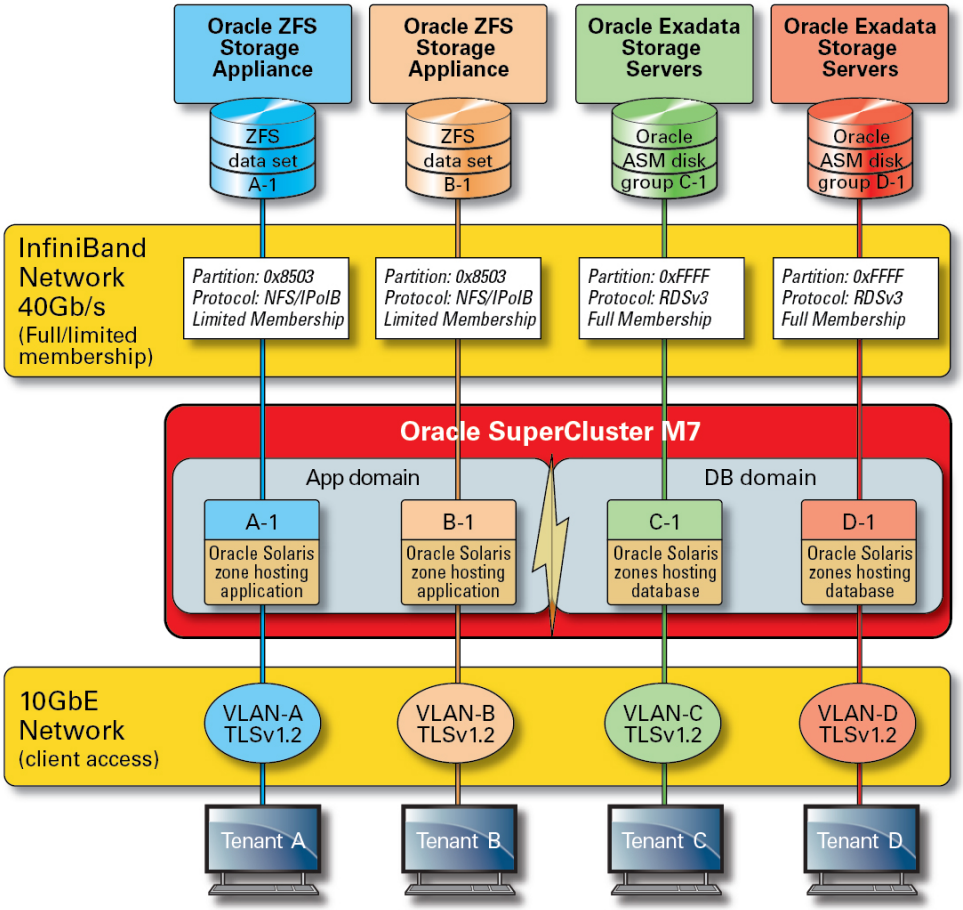
O tráfego da rede que flui pela rede de acesso do cliente do SuperCluster pode ser isolado com uma variedade de técnicas. Nesta figura, é mostrada uma configuração possível na qual quatro instâncias de banco de dados são configuradas para funcionar em três LANs virtuais distintas (VLANs). Ao configurar as interfaces de rede do SuperCluster para usar VLANs, é possível isolar o tráfego de rede entre os domínios dedicados do Oracle VM Server para SPARC e entre as Zonas do Oracle Solaris.

FIGURA 2 Isolamento de Rede Segura pela Rede de Acesso do Cliente



O SuperCluster inclui uma rede IB privada que é usada por instâncias de banco de dados para acessar as informações armazenadas nos servidores de armazenamento Exadata e no appliance de armazenamento de ZFS e para realizar as comunicações internas necessárias para cluster e alta disponibilidade. Esta ilustração mostra isolamento de rede segura no SuperCluster M7.

FIGURA 3 Isolamento de Rede Segura na Rede IB 40 Gbs



Por padrão, a rede SuperCluster IB é dividida em seis partições distintas durante a instalação e a configuração. Embora não seja possível alterar as partições padrão, a Oracle não dá suporte à criação e ao uso de partições dedicadas adicionais em situações em que é necessária maior segmentação da rede IB. Além disso, a rede IB dá suporte à noção de associação de partição completa e limitada. Membros limitados podem se comunicar apenas com membros integrais, enquanto estes podem se comunicar com todos os nós na partição. Os domínios de E/S de aplicativos e as Zonas do Oracle Solaris 11 podem ser configurados como membros limitados de suas respectivas partições IB garantindo que eles possam se comunicar apenas com o

appliance de armazenamento de ZFS, que é configurado como membro integral, e não com outros nós de associação limitada que possam existir na mesma partição.

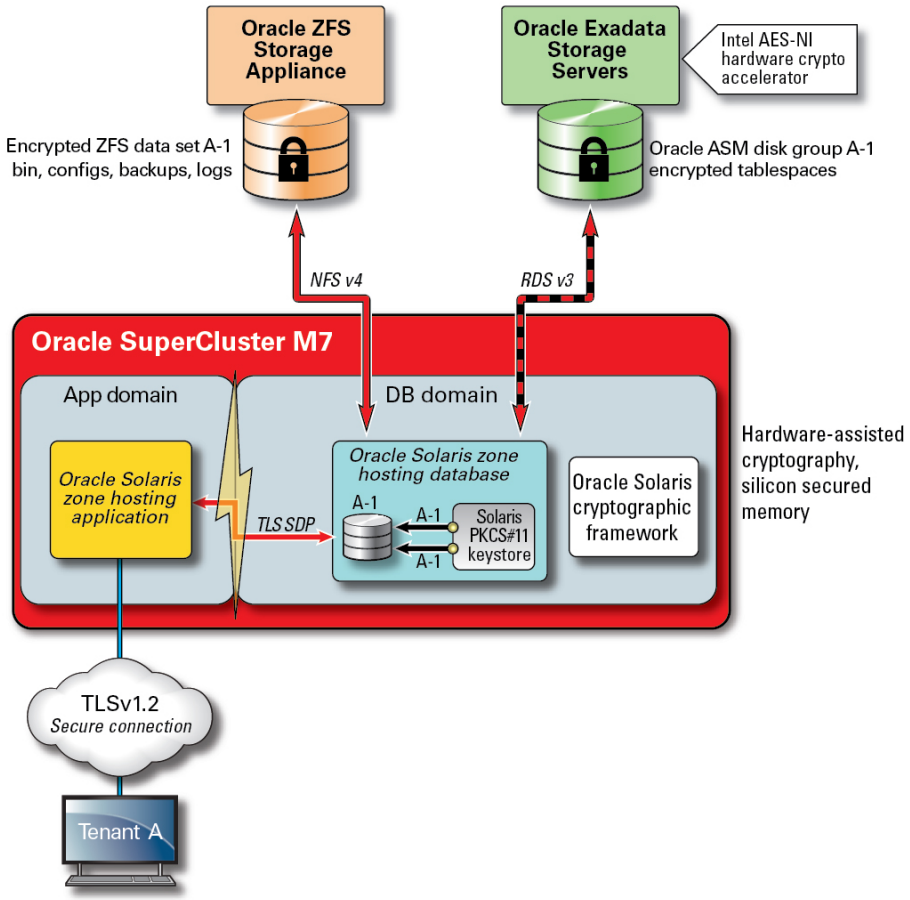
O SuperCluster também inclui uma rede de gerenciamento dedicada por meio da qual seus principais componentes podem ser gerenciados e monitorados. Essa estratégia mantém funções sensatas de gerenciamento e monitoramento isoladas dos caminhos da rede que são usados para processar solicitações de cliente. Ao manter as funções de gerenciamento isoladas a essa rede de gerenciamento, o SuperCluster pode reduzir ainda mais a superfície de ataque de rede que é exposta pelas redes de acesso do cliente e IB. É altamente recomendável que os provedores de nuvem sigam esta prática recomendada e isolem as funções de gerenciamento, monitoramento e funções relacionadas para que fiquem acessíveis apenas a partir da rede de gerenciamento.

Proteção de Dados

Para provedores de nuvem, a proteção de dados é a parte essencial de sua estratégia de segurança. Dada a importância das obrigações de privacidade e conformidade, as organizações que consideram arquiteturas multitenant devem considerar o uso de criptografia para proteger informações que transitam por seus bancos de dados. O uso de serviços criptográficos para proteção de dados é sistematicamente aplicado para garantir a confidencialidade e a integridade das informações ao transitarem pela rede e quando elas residem no disco.

O processador SPARC M7 no SuperCluster facilita a criptografia de alto desempenho e assistida por hardware para atender às necessidades de proteção de dados de ambientes de TI sensíveis em termos de segurança. O processador SPARC M7 também apresenta a tecnologia Silicon Secured Memory que garante a prevenção de ataques no nível de aplicativos mal-intencionados, como "memory scraping", corrompimento silencioso da memória, estouro de buffer e ataques relacionados.

FIGURA 4 Proteção de Dados Fornecida pela Aceleração Criptográfica Assistida por Hardware e Proteção contra Invasão de Memória



Para arquiteturas multitenant protegidas, nas quais a proteção de dados está presente em quase todos os aspectos da arquitetura, o SuperCluster e seu software de base permitem que as organizações cumpram seus objetivos de conformidade e segurança sem precisar sacrificar o desempenho. O SuperCluster tira proveito de instruções criptográficas baseadas em núcleo e recursos de Silicon Secured Memory, que são projetados em seu processador SPARC M7 para acelerar as operações criptográficas e garantir a proteção sem impacto no desempenho. Esses recursos produzem um desempenho criptográfico aperfeiçoado e fornecem verificação de

invasão de memória, além de melhorarem o desempenho geral porque é possível dedicar mais recursos de computação às cargas de trabalho de tenants.

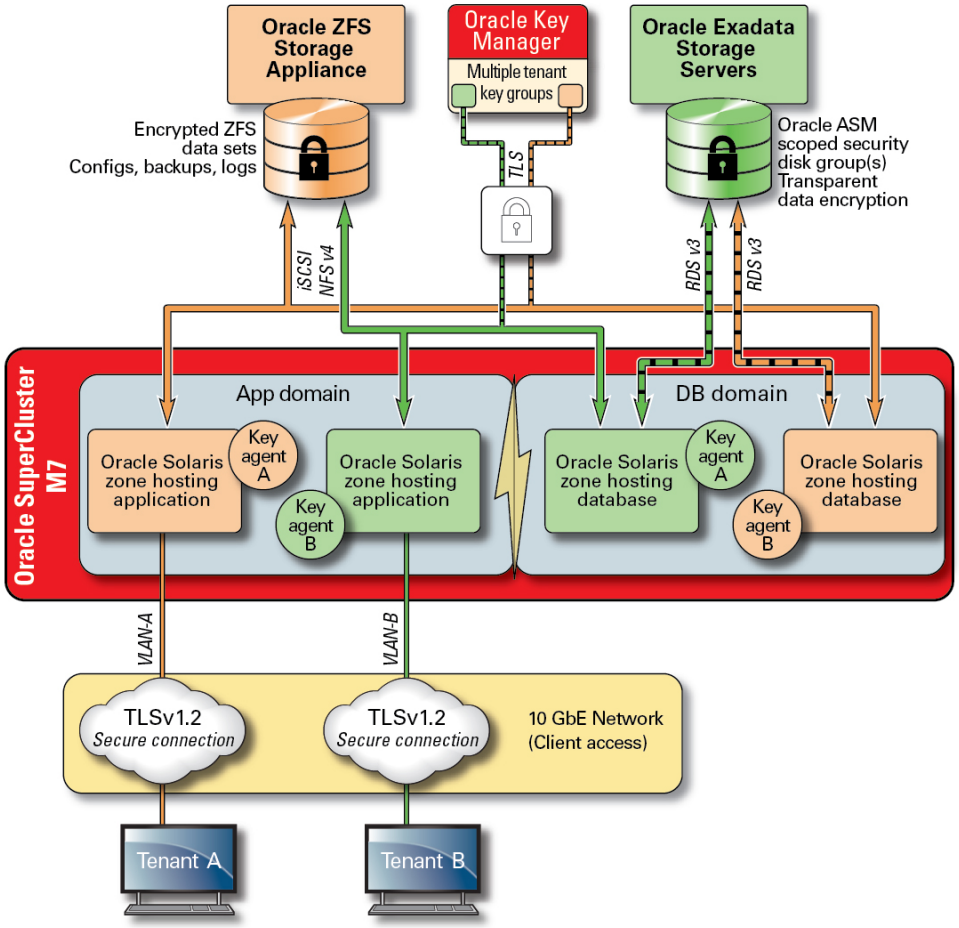
O processador SPARC habilita o suporte à aceleração criptográfica assistida por hardware para mais do que 16 algoritmos criptográficos padrão do setor. Juntos, esses algoritmos dão suporte às mais modernas necessidades criptográficas incluindo a criptografia de chaves públicas, a criptografia de chaves simétricas, a geração de números aleatórios, bem como o cálculo e a verificação de assinaturas digitais e resumos de mensagens. Além disso, no nível do sistema operacional, a aceleração criptográfica de hardware é ativada por padrão para a maioria dos serviços de núcleo incluindo Secure Shell, IPSec/IKE e conjuntos de dados ZFS criptografados.

O Oracle Database e o Oracle Fusion Middleware identificam automaticamente o Oracle Solaris OS e o processador SPARC usados pelo SuperCluster. Isso permite que o banco de dados e o middleware usem automaticamente os recursos de aceleração criptográfica de hardware da plataforma para operações de criptografia de espaço de tabela, TLS e WS-Security. Também permite que eles usem o recurso Silicon Secured Memory para garantir a proteção da memória e a integridade dos dados dos aplicativos sem precisar de configuração do usuário final. Para proteger a confidencialidade e a integridade de comunicações baseadas em IP, interzona, específicas de tenants, que trafegam pela rede IB, use IPSec (IP Security) e IKE (Internet Key Exchange).

Qualquer discussão sobre criptografia seria incompleta se não discutíssemos como as chaves de criptografia são gerenciadas. A geração e o gerenciamento de chaves de criptografia, principalmente para grandes coleções de serviços, são tradicionalmente os maiores desafios para organizações, e os desafios ficam ainda mais significativos no caso de um ambiente multitenant baseado em nuvem. No SuperCluster, a criptografia de conjuntos de dados ZFS e a Criptografia de Dados Transparente do Oracle Database podem tirar proveito de um keystore Oracle Solaris PKCS#11 para proteger a chave mestra. Ao usar o keystore Oracle Solaris PKCS#11, a aceleração criptográfica assistida por hardware SPARC é ativada automaticamente para todas as operações de chave mestra. Isso permite ao SuperCluster melhorar significativamente o desempenho das operações de criptografia e descriptografia associadas à criptografia de conjuntos de dados ZFS, criptografia de espaço de tabela do Oracle Database, backups de bancos de dados criptografados (usando o Oracle Recovery Manager [Oracle RMAN]), exportações de banco de dados criptografados (usando o recurso Data Pump do Oracle Database) e redo logs (usando o Oracle Active Data Guard).

Os tenants que usam uma abordagem de carteira compartilhada podem tirar proveito do appliance de armazenamento de ZFS para criar um diretório que pode ser compartilhado em todos os nós de um cluster. O uso de um keystore centralizado e compartilhado pode ajudar os tenants a gerenciar, manter e girar melhor as chaves em arquiteturas de banco de dados clusterizadas, como o Oracle Real Application Clusters (Oracle RAC), porque as chaves serão sincronizadas em cada um dos nós do cluster.

FIGURA 5 Cenário de Proteção de Dados pelo Gerenciamento de Chaves Multitenant Usando o Oracle Key Manager



Para resolver complexidades e problemas de gerenciamento de chaves associados a vários hosts e aplicativos em um ambiente multitenant baseado em nuvem, use o Oracle Key Manager opcional como um appliance integrado à rede de gerenciamento. O Oracle Key Manager autoriza, protege e gerencia centralmente o acesso a chaves de criptografia usadas pelo Oracle Database, aplicativos do Oracle Fusion, Oracle Solaris e o appliance de armazenamento de ZFS. O Oracle Key Manager também dá suporte às unidades de fita de criptografia do StorageTek da Oracle. Ter o gerenciamento de chaves e política de criptografia no nível do conjunto de dados

ZFS (sistema de arquivos) fornece exclusão garantida de sistemas de arquivos de tenants por meio da destruição de chaves.

O Oracle Key Manager é um appliance de gerenciamento de chave completo que dá suporte a operações de gerenciamento de chaves de ciclo de vida e armazenamento de chaves confiável. Quando configurado com uma Placa PCIe Sun Crypto Accelerator 6000 PCIe adicional, o Oracle Key Manager oferece armazenamento de chaves certificado por FIPS 140-2 Nível 3 de chaves de criptografia AES de 256 bits, bem como geração de números aleatórios em conformidade com FIPS 186-2. No SuperCluster, todos os domínios de aplicativos e bancos de dados, inclusive suas zonas globais e não globais, podem ser configurados para usar o Oracle Key Manager para gerenciamento de chaves associadas a aplicativos, bancos de dados e conjuntos de dados ZFS criptografados. Na verdade, o Oracle Key Manager pode dar suporte a operações de gerenciamento de chaves associadas a instâncias de bancos de dados múltiplas e individuais, ao Oracle RAC, ao Oracle Active Data Guard, ao Oracle RMAN e ao recurso Data Pump do Oracle Database.

Por fim, a separação de obrigações, aplicada pelo Oracle Key Manager, permite a cada tenant manter o controle completo de suas chaves de criptografia com visibilidade consistente em qualquer operação de gerenciamento de chave. Dada a importância das chaves para a proteção das informações, é essencial que os tenants implementem os níveis necessários de controle de acesso baseado em funções e auditoria para garantir que as chaves permaneçam protegidas por toda a sua vida.

Informações Relacionadas

- “Oracle Key Manager” [126]

Controle de Acesso

Para organizações que adotaram uma estratégia de ambiente hospedado na nuvem, o controle de acesso é um dos desafios mais críticos a serem resolvidos. Os tenants devem ter certeza de que as informações armazenadas na estrutura compartilhada estão protegidas e disponíveis apenas para hosts, serviços, indivíduos, grupos e funções autorizados. Hosts, indivíduos e serviços autorizados devem ser ainda mais limitados, de acordo com o princípio de menor privilégio, de forma que eles tenham apenas os direitos e privilégios necessários para uma operação específica.

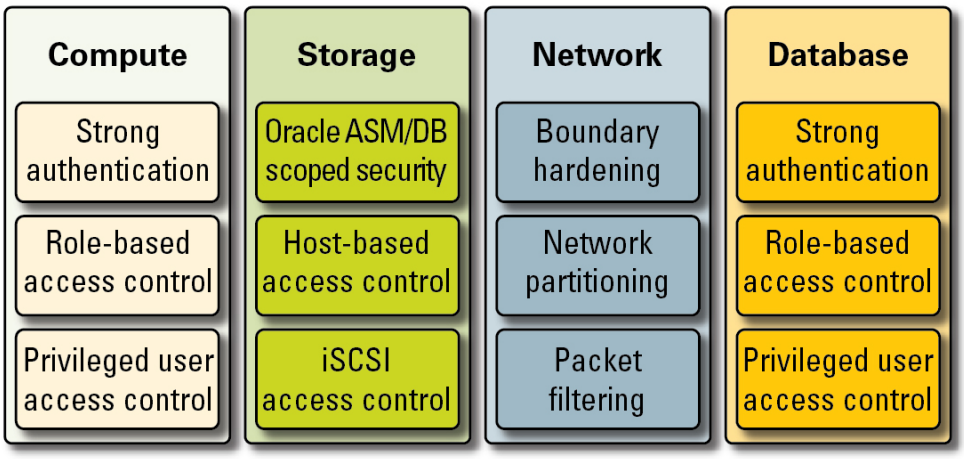
O SuperCluster facilita uma arquitetura de controle de acesso em camadas flexível que abrange cada camada da pilha e dá suporte a uma variedade de funções incluindo usuários finais, administradores de banco de dados e administradores de sistemas. Isso permite às organizações

definir políticas que protejam hosts, aplicativos e bancos de dados individualmente e proteger a infraestrutura de computação, armazenamento e rede subjacente na qual os serviços são executados.

Nas camadas de virtualização e sistema operacional, o controle de acesso começa com a redução do número de serviços expostos na rede. Isso ajuda a controlar o acesso aos consoles do Oracle VM Server para SPARC, domínios e zonas. Ao reduzir o número de pontos de entrada pelos quais os sistemas podem ser acessados, o número de políticas de controle de acesso também pode ser reduzido e mantido com mais facilidade durante a vida do sistema.

No Oracle Solaris OS, os controles de acesso são implementados usando uma combinação de permissões POSIX juntamente com o recurso de controle de acesso baseado em funções (RBAC) do Oracle Solaris. Igualmente importante é a capacidade de proteger os hosts, aplicativos, bancos de dados e serviços relacionados em execução no SuperCluster contra ataques baseados na rede. Para fazer isso, os tenants devem primeiro verificar se apenas serviços de rede aprovados estão em execução e ouvindo conexões de rede de entrada. Uma vez minimizada a superfície de ataques da rede, os tenants, em seguida, configuram os serviços restantes de modo que eles escutem conexões de entrada somente em redes e interfaces aprovadas. Essa prática simples ajudará a garantir que os protocolos de gerenciamento, como o Secure Shell, não sejam acessíveis de nenhum local além da rede de gerenciamento.

FIGURA 6 Resumo do Controle de Acesso de Ponta a Ponta



Além disso, os tenants também podem optar por implementar um firewall baseado em host, como o serviço IP Filter do Oracle Solaris. Os firewalls baseados em host são úteis porque

fornecem aos hosts uma forma mais rica em recursos de controlar o acesso a serviços de rede. Por exemplo, recurso Filtro de IP dá suporte à filtragem de pacotes com monitoração de estado e pode filtrar pacotes pelo endereço IP, porta, protocolo, interface de rede e direção do tráfego. Esses recursos são importantes para plataformas, como SuperCluster, que operam muitas interfaces de rede e dão suporte a uma variedade de comunicações de rede de entrada e saída.

No SuperCluster, o Filtro de IP pode ser configurado em um domínio do Oracle VM Server para SPARC ou operado de dentro de uma Zona do Oracle Solaris. Isso permite que a política de controle de acesso seja aplicada no mesmo contêiner de sistema operacional no qual os serviços de banco de dados são oferecidos. Em um cenário multitenant, a quantidade de atividades de rede de saída provavelmente será mínima e poderá facilmente ser categorizada de forma que seja possível criar uma política que limite as comunicações a interfaces de rede e destinos específicos. Todo o restante do tráfego seria negado e registrado como parte de uma política "de negação padrão" para bloquear comunicações não autorizadas, tanto de entrada quanto de saída.

A segurança de usuários finais da Oracle permite aos tenants integrar seus aplicativos e bancos de dados com seus serviços de gerenciamento de identidades existente a fim de dar suporte ao single sign-on (SSO) e ao gerenciamento centralizado de usuários e funções. Especificamente, a Segurança de Usuários Finais da Oracle ajuda a centralizar (1) o provisionamento e o desprovisionamento de usuários e administradores de banco de dados, (2) o gerenciamento e a redefinição de senhas de autoatendimento e (3) o gerenciamento de autorizações usando funções globais de banco de dados. As organizações que precisam de métodos de autenticação multifator, como Kerberos ou PKI, podem tirar proveito da Segurança Avançada da Oracle.

A tecnologia do Oracle Exadata Storage Server dá suporte a um conjunto predefinido de contas de usuário, cada uma com privilégios distintos. Os administradores que realizam a administração do Oracle Exadata Storage Server devem usar uma destas funções predefinidas para acessar o sistema. Por outro lado, o appliance de armazenamento de ZFS dá suporte à criação de contas administrativas locais e remotas, que podem dar suporte à atribuição individual de funções e privilégios.

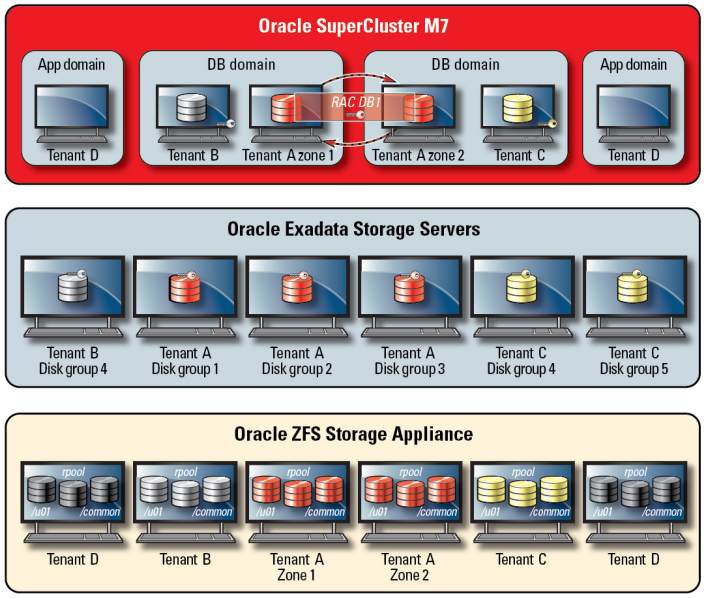
Por padrão, os Servidores de Armazenamento Oracle Exadata usados no SuperCluster são acessados pelos domínios de banco de dados usando o recurso Oracle Automatic Storage Management. Esse recurso permite aos provedores de nuvem criar grupos de discos distintos para cada tenant que sejam capazes de atender aos seus requisitos de capacidade, desempenho e disponibilidade. Em termos de controle de acesso, o Oracle Automatic Storage Management dá suporte a três modos de controle de acesso: segurança aberta, segurança no escopo do Oracle Automatic Storage Management e segurança no escopo do banco de dados.

Em um cenário multitenant, a segurança no escopo do banco de dados é recomendada porque oferece o nível mais refinado de controle de acesso. Nesse modo, é possível configurar grupos de discos de forma que eles só possam ser acessados por um banco de dados. Especificamente, isso significa que é possível limitar o acesso dos administradores de banco de dados e dos usuários apenas aos discos de grade que contêm informações para as quais eles tenham

privilégios de acesso. Em cenários de consolidação de banco de dados nos quais bancos individuais podem dar suporte a diferentes organizações ou tenants, é importante que cada tenant possa acessar e manipular somente seu próprio armazenamento. Especificamente, quando combinado com as estratégias de isolamento de bancos de dados e cargas de trabalho discutidas anteriormente, os tenants podem efetivamente compartimentar o acesso a bancos de dados individuais.

A segurança no escopo do banco de dados é uma ferramenta eficaz para limitar o acesso a discos de grade do Oracle ASM. Esta figura mostra a segurança no escopo do Oracle ASM juntamente com a segurança de ZFS. Em situações nas quais há grandes quantidades de instâncias do Oracle Database sendo implantadas na plataforma do SuperCluster, uma estratégia no escopo do Oracle ASM por tenant pode fazer mais sentido porque ela reduz significativamente o número de chaves que precisam ser criadas, atribuídas e gerenciadas. Além disso, como a segurança no escopo do banco de dados exige que grupos de discos separados sejam criados para cada banco de dados, essa abordagem também reduzirá significativamente o número de discos de grade separados que precisam ser criados em um Exadata Storage Server.

FIGURA 7 Segurança no Escopo do Oracle ASM por Tenant



O SuperCluster tira proveito da proteção de link de dados do Oracle Solaris, que procura impedir possíveis danos que possam ser causados por máquinas virtuais de tenant mal-

intencionadas na rede. Esse recurso integrado do Oracle Solaris oferece proteção contra as seguintes ameaças básicas: falsificação de endereços IP e MAC, bem como falsificação de quadros L2 (por exemplo, ataques de Bridge Protocol Data Unit). A proteção de link de dados do Oracle Solaris também pode ser aplicada individualmente a todas as zonas não globais do Oracle Solaris implantadas no ambiente multitenant.

Como os tenants individuais nunca devem exigir acesso no nível do host ou administrativo aos Exadata Storage Servers, é altamente recomendável que esse acesso seja restrito. Os Exadata Storage Servers devem ser configurados para impedir o acesso direto para zonas não globais de tenant e domínios de E/S de banco de dados permitindo, ao mesmo tempo, o acesso a partir dos domínios de banco de dados do SuperCluster (que são operados pelo provedor de nuvem). Isso garante que os Exadata Storage Servers possam ser gerenciados apenas de locais confiáveis na rede de gerenciamento.

Uma vez definida e implementada a configuração de segurança dos tenants, os provedores de serviços podem considerar a etapa adicional de configurar zonas não globais e globais específicas de tenants como ambientes imutáveis, de somente leitura. As zonas imutáveis criam um ambiente operacional resiliente de alta integridade no qual os tenants podem operar seus próprios serviços. Com base nos recursos de segurança inerentes do Oracle Solaris, as zonas imutáveis garantem que alguns (ou todos) os diretórios e arquivos do SO não possam ser alterados sem a intervenção do provedor de serviços em nuvem. A aplicação dessa postura somente leitura ajuda a prevenir alterações não autorizadas, promove procedimentos de gerenciamento de alterações mais fortes e impedem a injeção de malware baseado em kernel e baseado em usuário.

Monitoramento e Auditoria de Conformidade

O monitoramento e a geração de logs proativos em um ambiente de nuvem são muito importantes e, em muitos casos, ajudam a reduzir os ataques originários de lacunas de segurança e vulnerabilidades. Seja para relatório de conformidade ou resposta a incidentes, o monitoramento e a auditoria são funções essenciais para o provedor de nuvem, e as organizações de tenants devem aplicar uma política de auditoria e geração de logs bem definida a fim de obter maior visibilidade de seu ambiente de hospedagem. O grau em que o monitoramento e a auditoria são empregados, em geral, baseia-se no risco ou na natureza crítica do ambiente que está sendo protegido.

A arquitetura de nuvem do SuperCluster baseia-se no uso do subsistema de auditoria do Oracle Solaris para coletar, armazenar e processar informações de eventos de auditoria. Cada zona não global específica de tenant gerará registros de auditoria que são armazenados localmente em cada um dos domínios dedicados do SuperCluster (zona global). Essa abordagem garantirá que os tenants individuais não possam alterar suas políticas de auditoria, configurações ou

dados registrados porque essa responsabilidade pertence ao provedor de serviços em nuvem. A funcionalidade de auditoria do Oracle Solaris monitora todas as ações administrativas, invocações de comandos e até mesmo chamadas de sistema no nível do kernel individual em zonas de tenant e domínios. Esse recurso é altamente configurável e oferece políticas de auditoria por zona e até mesmo por usuário. Quando o sistema usa zonas de tenant, os registros de auditoria para cada zona podem ser armazenados na zona global para protegê-los contra manipulação. Os domínios dedicados e domínios de E/S também tiram proveito do recurso nativo de auditoria do Oracle Solaris para registrar ações e eventos associados a eventos de virtualização e administração de domínios.

Os Exadata Storage Servers e o appliance de armazenamento de ZFS dão suporte a auditoria de login, hardware e configuração. Isso permite às organizações determinar quem acessou um dispositivo e quais ações foram executadas. Embora não seja exposta diretamente para o usuário final, a auditoria do Oracle Solaris fornece o conteúdo subjacente para informações apresentadas pelo appliance de armazenamento de ZFS.

De modo semelhante, a auditoria do Exadata Storage Server é uma coleção rica de eventos de sistema que pode ser usada juntamente com as informações de alerta de hardware e configuração fornecidas pelo Software do Exadata Storage Server. Com o recurso Filtro de IP do Oracle Solaris, o provedor de nuvem pode registrar seletivamente as comunicações de rede de entrada e de saída, e a capacidade pode ser aplicada no nível do domínio e da zona não global. Isso ajuda as organizações a segmentar suas políticas de rede e verificar os registros de atividade. Opcionalmente, o Oracle Audit Vault e o appliance Database Firewall podem ser implantados para agregar e analisar, de forma segura, as informações de auditoria de uma variedade de bancos de dados Oracle e não Oracle, bem como as informações de auditoria do Oracle Solaris.

Por meio da integração com o Oracle Enterprise Manager, o SuperCluster também pode dar suporte a uma variedade de operações de autoatendimento em nuvem. Os provedores de nuvem podem definir pools de recursos, atribuir pools e cotas a tenants individuais, identificar e publicar catálogos de serviços e, por fim, dar suporte ao monitoramento e à geração de logs de recursos de aplicativos e bancos de dados.

Informações Relacionadas

- Auditoria para Conformidade [119]
- “Monitorando a Segurança” [129]

Práticas Recomendas de Recursos Adicionais para Segurança do SuperCluster

Para obter informações adicionais sobre segurança, arquitetura e práticas recomendadas referentes ao SuperCluster, consulte estes recursos:

- Oracle SuperCluster M7 - Princípios e Recursos de Segurança da Plataforma

  http://www.oracle.com/us/products/servers-storage/servers/sparc-enterprise/supercluster/supercluster-t4-4/ssc-security-pac-1716580.pdf
- Oracle SuperCluster M7 - Arquitetura de Nuvem Privada Segura

  http://www.oracle.com/technetwork/server-storage/engineered-systems/oracle-supercluster/documentation/supercluster-secure-multi-tenancy-2734706.pdf
- Proteção de Dados Completa no Oracle SuperCluster

  https://community.oracle.com/docs/DOC-918251
- Consolidação de Banco de Dados Segura no Oracle SuperCluster

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

  http://www.oracle.com/technetwork/server-storage/engineered-systems/sparc-supercluster/supercluster-pci-dss-compliance-2372543.pdf
- Oracle SuperCluster - Guia de Implementação Técnica de Segurança (STIG) Validação e Práticas Recomendadas

  http://www.oracle.com/technetwork/server-storage/hardware-solutions/stig-sparc-supercluster-1841833.pdf
- Guia do Desenvolvedor para Segurança do Oracle Solaris 11

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

  http://www.oracle.com/us/products/servers-storage/solaris/solaris11/solaris11-pci-dss-wp-1937938.pdf
- Início Rápido de Auditoria do Oracle Solaris 11

  http://www.oracle.com/technetwork/articles/servers-storage-admin/sol-audit-quick-start-1942928.html
- Diretrizes de Segurança do Oracle Solaris 11

  http://docs.oracle.com/cd/E53394_01/html/E54807/index.html
- Guia de Segurança do Oracle Database 12c Release 1 (12.1)

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

Revisando a Configuração de Segurança Padrão

Estes tópicos descrevem a configuração de segurança padrão para o SuperCluster M7.

Configurações de Segurança Padrão

O software SuperCluster M7 é instalado com muitas configurações de segurança padrão. Sempre que possível, use as configurações de segurança padrão:

- As políticas de senha reforçam uma complexidade mínima das senhas.
- As tentativas de login com falha causam um bloqueio após um número definido de tentativas com falha.
- Todas as contas de sistema padrão no sistema operacional fiam bloqueadas e com o login proibido.
- A capacidade limitada de usar o comando `su` é configurada.
- Protocolos e módulos desnecessários são desativados do kernel do sistema operacional.
- O carregador de inicialização é protegido por senha.
- Todos os serviços desnecessários do sistema são desativados, inclusive `inetd` (daemon do serviço de internet).
- O firewall de software é configurado nas células do armazenamento.
- Permissões de arquivo restritivas são definidas nos arquivos executáveis e de configuração relacionadas à segurança de chaves.
- As portas de escuta SSH são restritas a gerenciamento e redes privadas.
- O SSH é limitado ao protocolo v2.

- Mecanismos inseguros de autenticação de SSH são desativados.
- Criptografia específica é configurada.
- As chaves são separadas no sistema do tráfego de dados na rede.

Contas de Usuários e Senhas Padrão

Esta tabela lista as contas de usuário e senhas padrão para o SuperCluster M7. Instruções adicionais para alterar as senhas padrão são fornecidas em capítulos subsequentes de cada componente.

Componente	Nome do Usuário	Senha	Informações sobre Contas do Usuário e Senhas
Oracle ILOM em: ■ Servidores da série SPARC M7 ■ Exadata Storage Servers ■ Appliance de armazenamento de ZFS	■ `root`	`welcome1`	Consulte "Configuração e Manutenção" na coleção de documentação do Oracle ILOM em: `http://docs.oracle.com/cd/E24707_01/html/E24528`
Servidores da série SPARC M7	■ `root` ■ `oracle` ■ `grid`	`welcome1` `welcome1` `welcome1`	Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51] Consulte também estes recursos: ■ **Oracle Solaris 11** – Consulte a documentação de segurança do Oracle Solaris 11 em: `http://www.oracle.com/goto/Solaris11/docs` ■ **Oracle Solaris 10** – Consulte *Administração do Oracle Solaris: Administração Básica* em: `http://docs.oracle.com/cd/E26505_01`

Servidores de armazenamento Exadata	■ `root`
	■ `celladmin`
	■ `cellmonitor`
		`welcome1`
		`welcome`
		`welcome`
			Consulte Alterar Senhas do Servidor de Armazenamento [92].

Oracle ZFS Storage ZS3-ES	■ `root`	`welcome1`	Consulte Alterar a Senha `root` do Appliance de Armazenamento de ZFS [81]. Consulte também a seção "Usuários" no *Guia de Administração do Appliance de Armazenamento do Oracle ZFS* em: `http://www.oracle.com/goto/ZS3-ES/docs`
Switches de InfiniBand	■ `root` ■ `nm2user`	`welcome1` changeme	Consulte Alterar Senhas `root` e `nm2user` [109].

Componente	Nome do Usuário	Senha	Informações sobre Contas do Usuário e Senhas
			Consulte também "Controlando o Chassi" na *Coleção de Documentos HTML do Sun Datacenter InfiniBand Switch 36 para Firmware Versão 2.1* em: `http://docs.oracle.com/cd/E36265_01`
InfiniBand Oracle ILOM	■ `ilom-admin` ■ `ilom-operator`	ilom-admin ilom-operator	Consulte Alterar Senhas de Chaves de IB (Oracle ILOM) [110]. Consulte também a documentação de InfiniBand em: `http://docs.oracle.com/cd/E36265_01`
Chave de gerenciamento de Ethernet	■ `admin`	`welcome1`	Consulte Alterar a Senha da Chave de Ethernet [117]
Ferramenta de Criação do Oracle I/O Domain	■ `admin`	welcome1	Consulte o *Guia de Administração do Oracle I/O Domain* disponível em: `http://www.oracle.com/goto/sc-m7/docs`.
Oracle Engineered Systems Hardware Manager	■ `admin` ■ serviço	welcome1 welcome1	Consulte o *Guia do Proprietário do Oracle SuperCluster Série M7: Administração* disponível em: `http://www.oracle.com/goto/sc-m7/docs`.

Observação - Quando a senha `root` ou `admin` para esse componente é alterada, ela também deve ser alterada no Oracle Engineered Systems Hardware Manager. Consulte o *Guia do Proprietário do Oracle SuperCluster Série M7: Administração* para obter instruções. Consulte também “Senhas Conhecidas pelo Oracle Engineered Systems Hardware Manager” [29]

Senhas Conhecidas pelo Oracle Engineered Systems Hardware Manager

O Oracle Engineered Systems Hardware Manager deve ser configurado com as contas e senhas dos componentes nesta tabela.

Observação - O Oracle Engineered Systems Hardware Manager não precisa conhecer as senhas para nenhum domínio ou zona lógica.

Componente	Conta
Todos os Oracle ILOMs	`root`
Sistema operacional dos servidores de armazenamento Exadata	`root`

Componente	Conta
Sistema operacional dos controladores de armazenamento de ZFS	`root`
Switches de IB	`root`
Chave de gerenciamento de Ethernet	`admin`
PDUs	`admin`

Para obter mais informações sobre o Oracle Engineered Systems Hardware Manager, consulte "Oracle Engineered Systems Hardware Manager" [127] e o *Guia de Administração do Oracle SuperCluster Série M7* em `http://www.oracle.com/goto/sc-m7/docs`.

Protegendo o Hardware

Estas seções descrevem as diretrizes de segurança para proteger o hardware:

Restrições de Acesso

- Instale os sistemas da série Oracle SuperCluster M7 e equipamento relacionado em uma sala trancada, de acesso restrito.
- Tranque as portas do rack, a menos que seja necessário fazer manutenção em componentes dentro do rack. Esse procedimento restringe o acesso a dispositivos hot-pluggable ou hot-swappable e a portas USB, portas de rede e consoles do sistema.
- Guarde unidades substituíveis no campo (FRUs) e unidade substituíveis pelo cliente (CRUs) sobressalentes em um armário trancado. Restrinja o acesso ao gabinete trancado a pessoas autorizadas.
- Periodicamente, verifique o status e a integridade dos bloqueios no rack e no gabinete de peças sobressalentes para protegê-los ou para detectar falsificação ou portas deixadas acidentalmente destravadas.
- Guarde as chaves do gabinete em um local seguro com acesso limitado.
- Restrinja o acesso aos consoles USB. Dispositivos como controladores de sistema, PDUs (unidades de distribuição de energia) e switches de rede podem ter conexões USB, as quais fornecem um acesso mais fácil do que conexões SSH. Restringir o acesso físico é um método mais seguro de acessar um componente, já que ele não é suscetível a ataques baseados na rede.

Números de Série

- Registre os números de série dos componentes nos sistemas da série SuperCluster M7.
- Faça uma marca de segurança em todos os itens relevantes de hardware, do computador, como peças de reposição. Use canetas especiais ultravioletas ou etiquetas em alto-relevo.
- Mantenha registros das chaves e licenças de ativação de hardware e licenças em um local seguro que seja facilmente acessível para o gerente do sistema em emergências do sistema. Os documentos impressos podem ser sua única prova de propriedade.
- Armazene com segurança todas as folhas de informações que forem fornecidas com o sistema.

Unidades de Disco

Discos rígidos e unidades de estado sólido são geralmente usados para armazenar informações confidenciais. Para proteger essas informações contra a divulgação não autorizada, esvazie as unidades antes de reutilizá-las, descontinuá-las ou descartá-las.

- Use ferramentas de limpeza de disco como o comando `format`(`1M`) do Oracle Solaris para apagar completamente todos os dados da unidade.
- É recomendado que as organizações consultem suas políticas de proteção de dados para determinar o método mais apropriado de limpeza dos discos rígidos.
- Se necessário, utilize o Serviço de Retenção de Dispositivos e de Dados do Cliente da Oracle. Consulte este documento: `http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf`

Cuidado - Talvez um software de limpeza de disco não consiga excluir alguns dados em unidades modernas, devido à maneira como gerenciam o acesso aos dados.

OBP

Por padrão, a série SPARC M7 OBP não é protegida por senha. Você pode aumentar a segurança do sistema restringindo o acesso ao OBP executando estas ações:

- Implemente a proteção por senha.
- Verifique falhas de login do OBP.

- Forneça um banner de ativação do OBP.

Recursos de Hardware Adicionais

Todos os princípios de segurança que são destacados no *Guia de Segurança de Servidores do Sistema da Série SPARC M7* são aplicáveis aos servidores SPARC M7 no SuperCluster. Esse guia de segurança está disponível em: http://www.oracle.com/goto/M7/docs

Protegendo o Oracle ILOM

O Oracle ILOM fornece hardware e software de processador de serviço avançados que são usados para gerenciar e monitorar os componentes do Oracle SuperCluster incluindo os servidores de computação, servidores de armazenamento, appliance de armazenamento de ZFS e chaves de IB.

O Oracle ILOM permite a você gerenciar e monitorar ativamente os servidores e dispositivos subjacentes independentemente do estado do sistema operacional, fornecendo um recurso de gerenciamento "lights out" confiável.

Para proteger completamente o Oracle ILOM no SuperCluster M7, você deve aplicar configurações de segurança a todos os componentes ativados do Oracle ILOM individualmente. Esses componentes têm o Oracle ILOM:

- Servidores de computação
- Servidores de armazenamento
- Appliance de armazenamento de ZFS
- Switches de IB

Execute estas tarefas para proteger o Oracle ILOM:

▼ Fazer login na CLI do Oracle ILOM

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

Neste exemplo, substitua *ILOM_SP_ipaddress* pelo Endereço IP do Oracle ILOM para o componente que você deseja acessar:

- Servidores de computação
- Servidores de armazenamento
- Appliance de armazenamento de ZFS
- Switches de IB

Os endereços IP para a sua configuração estão listados no Resumo de Implantação fornecido pelo pessoal da Oracle.

```
% ssh root@ILOM_SP__ipaddress
```

2. **Digite a senha root do Oracle ILOM.**

   Consulte "Contas e Senhas Padrão (Oracle ILOM)" [38].

▼ Determinar a Versão do Oracle ILOM

Para aproveitar os recursos mais recentes, os recursos e os aprimoramentos de segurança, atualize o software do Oracle ILOM para a versão compatível mais recente.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Exiba a versão do Oracle ILOM.**

   Neste exemplo, a versão do software Oracle ILOM é 3.2.4.1.b.

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

Observação - Para atualizar a versão do software Oracle ILOM em qualquer um dos componentes do SuperCluster, instale o SuperCluster Quarterly Full Stack Download Patch mais recente disponível no My Oracle Support em `https://support.oracle.com`.

Observação - Os sistemas projetados pela, como o SuperCluster, são restritos em relação a quais versões do Oracle ILOM podem ser usadas e como essas versões são atualizadas. Para obter mais detalhes, entre em contato com o representante da Oracle.

(Se necessário) Ativar a Operação em Conformidade com FIPS-140 (Oracle ILOM)

O uso de criptografia validada FIPS 140 é exibido por clientes do Governo Federal dos EUA.

Por padrão, o Oracle ILOM não funciona com criptografia validada FIPS 140. No entanto, o uso de criptografia validada FIPS 140 pode ser ativada, se necessário.

Alguns recursos do Oracle ILOM não estão disponíveis quando configurados para operação em conformidade com FIPS 140. Uma lista desses recursos está disponível no *Guia de Segurança do Oracle ILOM* na seção intitulada "Recursos Sem Suporte Quando o Modo FIPS Está Ativado" (consulte “Recursos Adicionais do Oracle ILOM” [50]).

Consulte também “Conformidade com FIPS-140-2 Nível 1” [122].

Cuidado - Esta tarefa requer a redefinição do Oracle ILOM. Uma redefinição resulta na perda de todas as definições configuradas pelo usuário. Para esse motivo, é necessário ativar a operação em conformidade com FIPS 140 antes de alterações adicionais específicas do local feitas no Oracle ILOM. Para sistemas nos quais alterações específicas do local tenham sido feitas, faça backup da configuração do Oracle ILOM para que seja possível restaurá-la após a redefinição do Oracle ILOM. Caso contrário, essas alterações serão perdidas.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Determine se o Oracle ILOM está configurado para operação em conformidade com FIPS 140.**

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

   O modo de conformidade com FIPS no Oracle ILOM é representado pelas propriedades `state` e `status`. A propriedade `state` representa o modo configurado no Oracle ILOM e a propriedade `status` representa o modo operacional no Oracle ILOM. Quando a propriedade `state` do FIPS é alterada, a alteração não afeta o modo operacional (propriedade `status` do FIPS), até a próxima reinicialização do Oracle ILOM.

3. **Ative a operação em conformidade com FIPS 140.**

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

4. **Reinicie o processador de serviços do Oracle ILOM.**

   O Oracle ILOM SP deve ser reiniciado para que as alterações entrem em vigor.

```
-> reset /SP
```

Contas e Senhas Padrão (Oracle ILOM)

Conta	Tipo	Senha Padrão	Descrição
`root`	administrador	`welcome1`	Essa é a conta padrão que é fornecida e ativada para esse componente. Essa conta é usada para executar a configuração inicial e permitir a criação de contas administrativas adicionais não compartilhadas. Para fins de segurança, altere a senha padrão.

Serviços de Rede Exposta Padrão (Oracle ILOM)

Essa tabela lista os serviços de rede padrão que são expostos pelo Oracle ILOM.

Para obter informações adicionais sobre esses serviços, consulte o *Guia de Segurança do Oracle ILOM* (consulte “Recursos Adicionais do Oracle ILOM” [50]).

Nome do Serviço	Protocolo	Porta	Descrição
SSH	TCP	22	Usado pelo serviço Secure Shell integrado para permitir o acesso administrativo à CLI do Oracle ILOM.
HTTP (BUI)	TCP	80	Usado pelo serviço HTTP integrado para permitir o acesso administrativo ao Oracle ILOM usando uma interface de navegador. Embora a TCP/80 geralmente seja usada para acesso de texto não criptografado, por padrão, o Oracle ILOM redireciona automaticamente as solicitações de entrada para a versão protegida desse serviço em execução na TCP/443.
NTP	UDP	123	Usado pelo serviço Network Time Protocol (NTP) integrado (somente cliente) usado para sincronizar o relógio do sistema local com uma ou mais fontes de tempo externas.
SNMP	UDP	161	Usado pelo serviço SNMP integrado a fim de fornecer uma interface de gerenciamento para monitorar a integridade do Oracle ILOM e monitorar as notificações de interceptação recebidas.
HTTPS (BUI)	TCP	443	Usado pelo serviço HTTPS integrado para permitir o acesso administrativo ao Oracle ILOM por um canal (SSL/TLS) criptografado usando uma interface de navegador.
IPMI	TCP	623	Usado pelo serviço Intelligence Platform Management Interface (IPMI) integrado para fornecer uma interface de computador para várias funções de monitoramento e gerenciamento. Esse serviço não deve

Nome do Serviço	Protocolo	Porta	Descrição
			ser desativado porque ele é usado pelo Oracle Enterprise Manager Ops Center para coletar dados de inventário de hardware, descrições de FRU, informações de sensor de hardware e informações de status de componentes de hardware.
KVMS Remoto	TCP	5120 5121 5123 5555 5556 7578 7579	Coletivamente, as portas KVMS remotas fornecem um conjunto de protocolos que fornecem recursos de armazenamento, teclado, vídeo e mouse que podem ser usados com o Oracle Integrated Lights Out Manager.
ServiceTag	TCP	6481	Usado pelo serviço Oracle ServiceTag. Esse é um protocolo de descoberta da Oracle usado para identificar servidores e facilitar solicitações de serviço. Esse serviço é usado por produtos, como o Oracle Enterprise Manager Ops Center, para descobrir o software Oracle ILOM e integrar com outras soluções de serviço automático da Oracle.
WS-Man sobre o HTTPS	TCP	8888	Usado pelo serviço WS-Man integrado para fornecer uma interface de serviços Web baseados em padrões que é usada para gerenciar o Oracle ILOM pelo protocolo HTTPS. Desativar esse serviço impede que o Oracle ILOM seja gerenciado usando esse protocolo. Esse serviço não é mais incluído a partir do Oracle ILOM versão 3.2.
WS-Man sobre o HTTP	TCP	8889	Essa porta é usada pelo serviço WS-Man integrado para fornecer uma interface de serviços Web baseados em padrões que é usada para gerenciar o Oracle ILOM pelo protocolo HTTPS. Desativar esse serviço impedirá que o Oracle ILOM seja gerenciado usando esse protocolo. Esse serviço não é mais incluído a partir do Oracle ILOM versão 3.2.
Single Sign-On	TCP	11626	Essa porta é usada pelo recurso Single Sign-On que reduz o número de vezes que um usuário deve inserir um nome e senha de usuário. Desativar esse serviço impede a execução do KVMS sem precisar fornecer novamente a senha.

Protegendo a Configuração de Segurança do Oracle ILOM

Estes tópicos descrevem como proteger o Oracle ILOM por meio de várias configurações.

▼ Desativar Serviços Desnecessários (Oracle ILOM)

Desative todos os serviços que não sejam necessários para dar suporte aos requisitos operacionais e de gerenciamento da plataforma.

Por padrão, o Oracle ILOM emprega uma configuração de rede protegida por padrão pela qual serviços não essenciais já são desativados. No entanto, com base em seus requisitos e políticas de segurança, pode ser necessário desativar serviços adicionais.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Determine a lista de serviços compatíveis com o Oracle ILOM.**

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

3. **Determine se um determinado serviço está ativado.**

   Substitua *servicename* pelo nome do serviço identificado em Passo 2.

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

   Embora a maioria dos serviços reconheça e use o parâmetro `servicestate` para registrar se o serviço está ativado ou desativado, há alguns serviços, como `servicetag`, `ssh`, `sso` e `wsman`, que usam um parâmetro denominado `state`. Independente do parâmetro real usado, um serviço estará ativado se o parâmetro `servicestate` ou `state`retornar um valor de `enabled`, conforme mostrado nestes exemplos:

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

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

4. **Para desativar um serviço que não seja necessário, defina seu estado como `disabled`.**

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

5. **Determine se algum destes serviços precisa ser desativado.**
Dependendo das ferramentas e métodos usados, estes serviços poderão ser desativados se não forem necessários ou não estiverem sendo usados:

- **Para uma Interface administrativa de navegador (HTTP, HTTPS), digite:**

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

- **Para o serviço de teclado, vídeo e mouse (KVMS), digite:**

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

- **Para o gerenciamento de serviços Web (WS-Man sobre HTTP/HTTPS) - (Oracle ILOM versão 3.1 e posterior), digite:**:

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

- **Para serviços Single-Sign On (SSO), digite:**

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

▼ Configurar o Redirecionamento HTTP para HTTPS (Oracle ILOM)

Por padrão, o Oracle ILOM é configurado para redirecionar solicitações HTTP de entrada para o serviço HTTPS para garantir que todas as comunicações baseadas em navegador sejam criptografadas entre o Oracle ILOM e o administrador.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**
Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Verifique se o redirecionamento seguro está ativado.**

```
-> show /SP/services/http secureredirect
```

```
/SP/services/https
Properties:
secureredirect = enabled
```

3. **Se o padrão tiver sido alterado, você poderá ativar o redirecionamento seguro.**

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

4. **Verifique a configuração repetindo Passo 2.**

Desativar Protocolos Não Aprovados

Use estes tópicos para desativar protocolos não aprovados:

- Desativar o Protocolo SSLv2 para HTTPS [42]
- Desativar o Protocolo SSLv3 para HTTPS [42]

▼ Desativar o Protocolo SSLv2 para HTTPS

Por padrão, o protocolo SSLv2 é desativado para o serviço HTTPS.

Para fins de segurança, é muito importante que o SSLv2 seja desativado.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**
Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Determine se o protocolo SSLv2 está desativado para o serviço HTTP.**

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

3. **Se o serviço for ativado, desative o protocolo SSLv2.**

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

4. **Verifique a configuração repetindo Passo 2.**

▼ Desativar o Protocolo SSLv3 para HTTPS

Por padrão, o protocolo SSLv3 é desativado para o serviço HTTPS.

Para fins de segurança, desative o protocolo SSLv3.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Determine se o protocolo SSLv3 está desativado para o serviço HTTP.**

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

3. **Desative o protocolo SSLv3.**

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

4. **Verifique a configuração repetindo Passo 2.**

Desativar Protocolos TLS Não Aprovados para HTTPS

Por padrão, os protocolos TLSv1.0, TLSv1.1 e TLSv1.2 são ativados para o serviço HTTPS.

Você pode desativar uma ou mais versões do protocolo TLS que não cumpram suas políticas de segurança.

Para fins de segurança, use TLSv1.2, a menos que seja necessário suporte para versões anteriores do protocolo TLS.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Determine a lista de versões do protocolo TLS que estão ativadas para o serviço HTTPS.**

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

3. **Desative o TLSv1.0.**

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

4. **Desative o TLSv1.1.**

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

5. **Verifique a configuração repetindo Passo 2.**

Desativar Criptografia SSL Fraca e Média para HTTPS

Por padrão, o Oracle ILOM desativa o uso de criptografia fraca e média para o serviço HTTPS.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**
   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Determine se as criptografias fraca e média estão desativadas.**

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

3. **Se o padrão tiver sido alterado, será possível desativar o uso de criptografias fraca e média.**

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

4. **Verifique a configuração repetindo Passo 2.**

Desativar Protocolos SNMP Não Aprovados (Oracle ILOM)

Por padrão, somente o protocolo SNMPv3 é desativado para o serviço SNMP que é usado para monitorar e gerenciar o Oracle ILOM. Garanta que as versões anteriores do protocolo SNMP permaneçam desativadas, a menos que seja necessário ativá-las.

Alguns produtos da Oracle e de terceiros estão limitados em seu suporte para versões mais recentes do protocolo SNMP. Consulte a documentação do produto associada aos componentes para confirmar seu suporte para versões específicas do protocolo SNMP. Garanta que o Oracle ILOM esteja configurado para dar suporte a quaisquer versões do protocolo necessárias por esses componentes.

Observação - A versão 3 do protocolo SNMP introduziu o suporte para o Modelo de Segurança Baseado em Usuário (USM). Essa funcionalidade substitui as strings de comunicação SNMP tradicionais pelas contas de usuário reais que podem ser configuradas com permissões específicas, protocolos de autenticação e privacidade e senhas. Por padrão, o Oracle ILOM não inclui nenhuma conta USM. Configure contas SNMPv3 USM com base em seus próprios requisitos de implantação, gerenciamento e monitoramento.

---

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Determine o status de cada protocolo SNMP.**

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

3. **Se necessário, desative SNMPv1 e SNMPv2c.**

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

4. **Verifique a configuração repetindo Passo 2.**

▼ Configurar Strings de Comunidade SNMP v1 e v2c (Oracle ILOM)

Essa tarefa só será aplicável se SNMP v1 ou SNMPv2c estiver ativado e configurado para uso.

Para o SNMP funcionar corretamente, um cliente e um servidor devem concordar em relação à string de comunidade que é usada para autenticar o acesso. Dessa forma, ao alterar as strings de comunidade SNMP, garanta que a nova string seja configurada no Oracle ILOM e para todos os componentes que tentarem se conectar com o Oracle ILOM usando o protocolo SNMP.

Como o SNMP, geralmente, é usado para monitorar a integridade do dispositivo, é importante que as strings da comunidade SNMP padrão usadas pelo dispositivo sejam substituídas por valores definidos pelo cliente.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Crie uma nova string de comunidade SNMP.**

   Neste exemplo, substitua estes itens na linha de comando:

   - *string* – Substitua por um valor definido pelo cliente que esteja em conformidade com os requisitos do Departamento de Defesa dos EUA relativos à composição de strings da comunidade SNMP.
   - *access* – Substitua por `ro` ou `rw`, dependendo se é uma string de acesso somente leitura ou leitura e gravação.

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

   Uma vez criadas as novas strings da comunidade, as strings padrão devem ser removidas.

3. **Remova as strings da comunidade SNMP padrão.**

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

4. **Verifique as strings de comunidade SNMP**

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

▼ Substituir Certificados Autoassinados Padrão (Oracle ILOM)

O Oracle ILOM usa certificados autoassinados para permitir o uso predefinido dos protocolos SSL e TLS. Sempre que possível, substitua certificados autoassinados por certificados aprovados para uso em seu ambiente e assinados por uma autoridade certificadora reconhecida.

O Oracle ILOM dá suporte a uma variedade de métodos que podem ser usados para acessar o certificado digital e a chave privada incluindo HTTPS, HTTP, SCP, FTP, TFTP, e à cola das informações diretamente em uma interface de navegador Web. Para obter mais informações,

consulte o *Guia de Configuração e Manutenção do Oracle ILOM* (consulte "Recursos Adicionais do Oracle ILOM" [50]).

1. **Determine se o Oracle ILOM está usando um certificado autoassinado padrão.**

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

2. **Instale o certificado de sua organização.**

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

Configurar o Tempo Limite de Inatividade da Interface de Navegador Administrativa

O Oracle ILOM dá suporte à capacidade de desconectar e fazer logoff de sessões administrativas que permanecerem inativas por mais do que um intervalo predefinido de minutos. Por padrão, o tempo da sessão de interface do navegador se esgota após 15 minutos.

Os parâmetros de tempo limite de sessão associados aos serviços HTTPS e HTTP são definidos e gerenciados de modo independente. Certifique-se de definir o parâmetro `sessiontimeout` associado a cada serviço.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Verifique o parâmetro de tempo limite de inatividade associado ao serviço HTTPS.**

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

3. **Defina o parâmetro de tempo limite de inatividade.**

   Substitua *n* por um valor especificado em minutos.

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

4. **Verifique o parâmetro de tempo limite de inatividade associado ao serviço HTTP.**

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

5. **Defina o parâmetro de tempo limite de inatividade.**

   Substitua *n* por um valor especificado em minutos.

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

6. **Verifique a configuração repetindo Passo 2 e Passo 4.**

Configurar o Tempo Limite da Interface Administrativa (CLI do Oracle ILOM)

O Oracle ILOM dá suporte à capacidade de desconectar e fazer logoff de sessões de CLI administrativas que permanecerem inativas por mais do que um intervalo predefinido de minutos.

Por padrão, a CLI SSH CLI não tem valor de tempo limite especificado e, consequentemente, os usuários administrativos que acessam esse serviço permanecem conectados indefinidamente.

Para fins de segurança, defina esse parâmetro para estabelecer a correspondência entre o valor associado e a interface do usuário do navegador. Pode ser 15 minutos ou algum outro valor.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Verifique o parâmetro de tempo limite de inatividade associado à CLI.**

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

3. **Defina o parâmetro de tempo limite de inatividade.**

   Substitua *n* por um valor especificado em minutos.

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

4. **Verifique a configuração repetindo Passo 2.**

▼ Configurar Banners de Aviso de Login (Oracle ILOM)

O Oracle ILOM dá suporte à capacidade de exibir mensagens específicas do cliente antes e depois que um administrador se conecta ao dispositivo.

A mensagem de conexão do Oracle ILOM é exibida antes da autenticação, enquanto a mensagem de login é exibida após a autenticação.

Opcionalmente, você pode configurar o Oracle ILOM para exigir a aceitação da mensagem de login antes de o acesso ser concedido a funções do Oracle ILOM. As mensagens de conexão e login e o requisito de aceitação opcional são implementados nas interfaces de acesso de linha de comando e navegador.

O Oracle ILOM dá suporte a mensagens de conexão e login com 1.000 caracteres no máximo.

1. **Na rede de gerenciamento, faça login no Oracle ILOM.**

   Consulte Fazer login na CLI do Oracle ILOM [35]

2. **Determine se mensagens de conexão e login serão configuradas.**

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

3. **Defina uma mensagem de conexão ou login.**

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

4. **Determine se a aceitação da mensagem de login será ativada.**

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

5. **(Opcional) Aplique a aceitação da mensagem de login.**

Cuidado - Exigir a aceitação da mensagem de login pode inibir a operação correta de processos de gerenciamento automatizados que usam SSH, porque eles podem não conseguir responder à solicitação de aceitação ou não estar configurados para isso. Como resultado, essas conexões podem demorar ou expirar porque o Oracle ILOM não permitirá o uso da CLI até o requisito de aceitação da mensagem ser cumprido.

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

6. **Verifique a configuração repetindo Passo 2 e Passo 4.**

Recursos Adicionais do Oracle ILOM

Para obter mais informações sobre procedimentos de segurança e administração do Oracle ILOM, consulte a biblioteca de documentação do Oracle ILOM correspondente à versão em execução no SuperCluster M7:

- Guia de Segurança do *Oracle ILOM - Releases 3.0, 3.1 e 3.2 do Firmware*:

  http://docs.oracle.com/cd/E37444_01/html/E37451
- Oracle Integrated Lights Out Manager Versão 3.2.*x*:

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

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

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

Protegendo os Servidores de Computação

Um ou dois servidores SPARC M7 (servidores de computação) estão instalados no SuperCluster M7. Cada servidor de computação está dividido em duas partições de hardware (dois PDomains). Cada PDomian inclui metade dos processadores, memória e slots de expansão PCIe possíveis no chassi. Os dois PDomains funcionam como um servidor separado dentro do mesmo chassi. Um par redundante de módulos de processador de serviço (SPMs) gerencia cada partição.

É necessário proteger cada PDomain.

Esta seção fornece um conjunto de controles de segurança para os servidores de computação.

▼ Fazer Login em um Servidor de Computação e Alterar a Senha Padrão

Para acessar um único PDomain por meio do Oracle ILOM, é necessário fazer login no SPM ativo que controla esse PDomain. Você pode ligar, reinicializar ou gerenciar uma partição enquanto a outra continua a funcionar normalmente.

Há uma variedade de métodos que você pode usar para fazer login no servidor de computação SuperCluster. O método descrito nesta tarefa envolve fazer login na CLI do Oracle ILOM no SPM do servidor de computação. Esse método permite acessar o servidor em qualquer um destes estados:

- Modo de ativação Standby
- Sistema ligado, mas o host não está funcionando
- O sistema operacional está sendo inicializado
- Totalmente ligado, e o sistema operacional está funcionando

1. **Na rede de gerenciamento, faça login usando o comando `ssh`.**

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

2. **Quando solicitado, informe a senha.**

   A senha padrão de fábrica `root` é `welcome1`.

   Se for solicitada a alteração da senha, altere-a.

   Nesse momento, você pode executar qualquer tarefa de segurança apropriada no Oracle ILOM, no servidor de computação.

3. **Se você quiser acessar o console do host do servidor de computação, inicie o console.**

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

Serial console started.  To stop, type #.

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

Observação - Você não verá o PDomain se o host estiver em execução.

Observação - Para voltar para o prompt do Oracle ILOM, digite os caracteres de escape (`#.` são os caracteres padrão).

4. **Se necessário, assuma uma função de superusuário.**

   Use o comando `su` para mudar para um usuário que esteja configurado com a função `root`.

Contas e Senhas Padrão (Servidores de Computação)

Conta	Senha Padrão	Descrição
`root`	`welcome1`	O Oracle ILOM requer que a senha padrão seja alterada imediatamente após o primeiro login bem-sucedido.
`oracle`	`welcome1`	
`grid`	`welcome1`	

▼ Determinar a Versão do Software SuperCluster

1. **Faça login em um dos servidores de computação e acesse o console do host.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Digite este comando.**

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

Na saída, os números anexados a `ssc` representam a versão do software.
Para atualizar a versão do software SuperCluster, instale o SuperCluster Quarterly Full Stack Download Patch mais recente disponível no My Oracle Support em `https://support.oracle.com`.

Observação - No caso do SuperCluster, restrições adicionais podem limitar as versões do software que podem ser usadas e como elas são atualizadas. Nessas situações, entre em contato com o representante da Oracle.

▼ Configurar o Serviço Secure Shell

A execução dessa tarefa ajuda a aumentar a segurança do Secure Shell implantado no Oracle SuperCluster.

O arquivo `/etc/ssh/sshd_config` é um arquivo de configuração no âmbito do sistema no qual você configura os parâmetros para o serviço Secure Shell.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Edite o arquivo `/etc/ssh/sshd_config`.**

3. **Configure o parâmetro `ListenAddress` para garantir que apenas as conexões que se originarem da rede de acesso do cliente do SuperCluster sejam aceitas.**
   Garanta que o endereço IP `ListenAddress` seja definido na rede do cliente.
   Isso garante que conexões do Secure Shell não possam ser iniciadas com êxito entre componentes pelas redes IB ou de gerenciamento.

4. **Reveja outros parâmetros `sshd_config` e defina-os de acordo com os requisitos do local.**
   Essas configurações protegem o serviço Secure Shell:

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

5. **Salve o arquivo `sshd_config`.**

6. **Reinicie o serviço.**
   Você deve reiniciar o serviço para que as alterações tenham efeito.

```
# svcadm restart ssh
```

▼ Verificar se `root` é uma Função

Por padrão, o Oracle Solaris é configurado para que `root` seja uma função e não uma conta de usuário. Além disso, a configuração do SuperCluster não permite logins de usuário `root` anônimos. Em vez disso, todos os usuários devem fazer login como usuários regulares antes de assumir a função root. Todas as operações de administração do SuperCluster devem ser executadas usando `root` como função.

1. **Faça login em um dos servidores de computação e acesse o console do host.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Verifique se os atributos `root` estão definidos como `type=role`.**

```
# grep root /etc/user_attr
```

```
root::::type=role
```

3. **(Opcional) Atribua a qualquer usuário regular a função `root`.**

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

Serviços de Rede Expostos Padrão (Servidores de Computação)

Essa tabela lista os serviços de rede padrão que são expostos nos servidores de computação.

Nome do Serviço	Protocolo	Porta	Descrição
SSH	TCP	22	Usado pelo serviço Secure Shell integrado para permitir o acesso administrativo aos servidores de computação usando uma CLI.
HTTP (BUI)	TCP	80	Usado pelo serviço HTTP integrado para permitir o acesso administrativo aos servidores de computação usando uma interface de navegador.
HTTPS (BUI)	TCP	443	Usado pelo serviço HTTPS integrado para permitir o acesso administrativo aos servidores por um canal (SSL/TLS) criptografado usando uma interface de navegador.
SNMP	UDP	161	Usado pelo serviço SNMP integrado a fim de fornecer uma interface de gerenciamento para monitorar a integridade dos servidores de computação e as notificações de interceptação recebidas.

Protegendo a Configuração de Segurança do Servidor de Computação

Estes tópicos descrevem como configurar os servidores de computação com segurança.

Ativar o Serviço `intrd`

O serviço do balanceador de interrupção (`intrd`) monitora as atribuições entre interrupções e CPUs para garantir o desempenho ideal. Consulte a página man `intrd(1M)` para obter detalhes.

Esse serviço funciona apenas na zona global.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51].

2. **Inicie o serviço.**

```
# svcadm enable intrd
```

Desativar Serviços Desnecessários (Servidores de Computação)

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Desative o monitor de status NFS se o sistema não for um servidor ou cliente NFS.**

   Esse serviço interage com `lockd(1M)` para fornecer as funções de falha e recuperação para os serviços de bloqueio em NFS.

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

3. **Desative o serviço de gerenciador de bloqueio NFS se não estiver usando NFS ou estiver usando NFSv4.**

   O gerenciador de bloqueio NFS dá suporte às operações de bloqueio de registros em arquivos NFS em NFSv2 e NFSv3.

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

4. **Se o sistema não estiver montando arquivos, você poderá desativar o serviço do cliente de NFS ou desinstalar seu pacote.**

   O serviço do cliente de NFS não será necessário se o sistema estiver montando arquivos de um servidor NFS. Para obter mais informações, consulte a página man `mount_nfs(1M)`.

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

5. **Desative o serviço de servidor NFS em um sistema que não seja um servidor de arquivos NFS.**

   O serviço de servidor NFS lida com solicitações do sistema de arquivos cliente no NFS versões 2, 3 e 4. Se esse sistema não for um servidor NFS, desative o serviço.

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

6. **Se você não estiver usando FedFS para registros DNS SRV ou encaminhamentos baseados em LDAP, desative o serviço.**

   O serviço do cliente do sistema de arquivos federados (FedFS) gerencia padrões e informações de conexão para servidores LDAP que armazenam informações do FedFS.

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

7. **Desative o serviço `rquota`.**

   O servidor de cotas `remote` retorna cotas para um usuário de um sistema de arquivos local que é montado em NFS. Os resultados são usados por `quota(1M)` para exibir cotas de usuário para sistemas de arquivos remotos. O daemon `rquotad(1M)` normalmente é invocado pelo `inetd(1M)`. O daemon fornece informações sobre a rede para usuários potencialmente mal-intencionados.

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

8. **Desative o serviço `cbd`.**

   O serviço `cbd` gerencia pontos de extremidade de comunicação para o protocolo NFS Versão 4. O daemon `nfs4cbd(1M)` é executado no cliente do NFS Versão 4 e cria uma porta ouvinte para callbacks.

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

9. **Desative o serviço `mapid` se você não estiver usando NFSv4.**

   O serviço de daemon de mapeamento de IDs de grupos e usuários NFS é mapeado de e para os atributos de identificação `owner` e `owner_group` do NFS versão 4 e números UID e GID locais usados pelo servidor e cliente do NFS versão 4.

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

10. **Desative o serviço `ftp`.**

    O serviço FTP fornece um serviço de transferência de arquivos não criptografados e usa autenticação de texto simples. Use o programa de cópia segura `scp(1)` em vez de `ftp`, porque ele fornece autenticação criptografada e transferência de arquivos.

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

11. **Desative o serviço de gerenciador de volumes remoto.**

    O gerenciador de volumes removível é um gerenciador com reconhecimento de HAL que pode montar e desmontar automaticamente mídia removível e armazenamento hot-pluggable. Os usuários podem importar programas mal-intencionados ou transferir dados confidenciais para fora do sistema. Consulte a página man `mvolmgr(1M)` para obter detalhes.

    Esse serviço funciona apenas na zona global.

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

12. **Desative o serviço `smserver`.**

    O serviço `smserver` é usado para acessar dispositivos de mídia removíveis.

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

13. **Especifique `pam_deny.so.1` como o módulo da pilha de autenticação para os serviços `r-protocol` no diretório `/etc/pam.d`.**

    Por padrão, serviços legados, como `r-protocols`, `rlogin(1)` e `rsh(1)`, não estão instalados. No entanto, esses serviços são definidos em `/etc/pam.d`. Se você remover as definições de serviço

de `/etc/pam.d`, os serviços usarão os outros serviços (SSH, por exemplo) caso os serviços legados estejam ativados.

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

14. Edite o arquivo `/etc/default/keyserv` para alterar o valor de `ENABLE_NOBODY_KEYS` para `NO`.

O serviço `keyserv` não pode usar a chave de usuário `nobody`. O valor de `ENABLE_NOBODY_KEYS` é `YES` por padrão.

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

15. Adicione usuários ao arquivo `ftpusers` para restringir o acesso ao `ftp`.

As transferências de arquivos para o FTP não devem estar disponíveis para todos os usuários e devem exigir que os usuários qualificados forneçam seus nomes e senhas. Em geral, os usuários do sistema devem ser proibidos de usar o FTP. Essa verificação examina se as contas do sistema estão incluídas no arquivo `/etc/ftpd/ftpusers`, para que elas não possam usar o FTP.

O arquivo `/etc/ftpd/ftpusers` é usado para proibir os usuários de usar o serviço FTP. No mínimo, inclua todos os usuários do sistema, como `root`, `bin`, `adm`, etc.

```
# pfedit /etc/ftpd/ftpusers
....
root
daemon
bin
...
```

16. Defina uma máscara de criação de arquivos padrão forte para os arquivos criados pelo servidor FTP.

O servidor FTP não usa necessariamente a máscara de criação do sistema de arquivos do usuário. A definição da máscara de FTP garante que os arquivos transmitidos pelo FTP usem uma máscara de criação de arquivos forte.

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

17. Desative as respostas para as consultas de topologia da rede.

É importante desativar as respostas para as solicitações de eco. As solicitações ICMP são gerenciadas usando o comando `ipadm`.

Essas configurações impedem a disseminação das informações sobre a topologia de rede.

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

18. **Desative as mensagens de redirecionamento ICMP.**

    Os roteadores usam mensagens de redirecionamento ICMP para informar hosts sobre rotas mais diretas para um destino. Uma mensagem de redirecionamento ICMP ilícito pode resultar em um ataque a intermediários.

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

19. **Desative `mesg(1)` para impedir o acesso de `talk(1)` e `write(1)` a terminais remotos.**

    ```
    # mesg -n
    ```

20. **(Opcional) Reveja e desative a escuta de serviços desnecessária na rede.**

    Por padrão, `ssh(1)` é o único serviço de rede que pode enviar e receber pacotes de rede.

    ```
    # svcadm disable FMRI_of_unneeded_service
    ```

▼ Ativar a Hospedagem Múltipla Estrita

Para sistemas que são gateways de outros domínios, como um firewall ou um nó VPN, ative a hospedagem múltipla estrita. A propriedade `hostmodel` controla o comportamento de envio e de recebimento de pacotes IP em um sistema de hospedagem múltipla. Defina a hospedagem múltipla estrita como `1` para que os pacotes não sejam aceitos em outra interface. O valor padrão é `0`.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Defina a hospedagem múltipla estrita como `1`.**

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

Ativar ASLR

Observação - Não ative a ASLR em Domínios de Banco de Dados nem em Zonas de Banco de Dados.

O Oracle Solaris marca muitos binários de usuário para ativar a randomização do layout do espaço de endereço (ASLR). A ASLR randomiza o endereço inicial das partes chave de um espaço de endereço. Esse mecanismo de defesa de segurança pode fazer com que os ataques de Return Oriented Programming (ROP) falhem ao tentar explorar vulnerabilidades do software. As zonas herdam esse layout randomizado para seus processos. Como o uso da ASLR pode não ser ideal para todos os binários, a ASLR é configurável no nível da zona e do binário.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Ativar ASLR**

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

Configurar Conexões TCP

A definição do máximo de conexões TCP meio aberta como 4096 por endereço IP por porta ajuda a defender contra ataques de negação de serviço de inundação SYN. A definição do número máximo de conexões de entrada em fila TCP no mínimo como 1024 ajuda a evitar determinados ataques de negação de serviço (DDoS) distribuídos.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Defina o máximo de conexões TCP de entrada em fila e meio abertas.**

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

Definir Logs de Histórico e Políticas de Senha para Conformidade com PCI

O parâmetro `HISTORY` no arquivo `/etc/default/passwd` impede que os usuários utilizem senhas semelhantes com o valor `HISTORY`.

Se `MINWEEKS` for definido como `3` e `HISTORY` for definido como `10`, não será possível reutilizar as senhas por 10 meses.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Edite o arquivo `/etc/default/passwd` e defina os parâmetros de senha.**

```
# pfedit /etc/default/passwd
. . .
#Compliance to the PCI-DSS benchmark is 10
#HISTORY=0
HISTORY=10
MINDIFF=4
MINDIGIT=1
MINUPPER=1
MINWEEKS=3
MAXWEEKS=13
```

3. **Edite o arquivo `/etc/default/login` para incluir esses parâmetros.**

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

Garantir que os Diretórios Base do Usuário Tenham Permissões Apropriadas

Os diretórios base devem ser graváveis e pesquisáveis por seus proprietários. Em geral, outros usuários não têm direitos para modificar esses arquivos nem adicionar arquivos ao diretório base do usuário. Para garantir que esse seja o caso, defina permissões no diretório do usuário.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Defina permissões no diretório de um usuário.**

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

Ativar o Firewall de Filtro de IP

O Filtro de IP é um firewall baseado em host que fornece filtragem de pacotes com estado e conversão de endereços de rede (NAT). A filtragem de pacotes fornece proteção básica contra ataques baseados em rede. O Filtro de IP também inclui filtragem de pacotes sem informações de estado e pode criar e gerenciar pools de endereços.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Ative o Firewall de Filtro de IP.**

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

Garantir que os Serviços de Nome Só Usem Arquivos Locais

O SO usa vários bancos de dados de informações sobre hosts, `ipnodes`, usuários (`passwd(4)`, `shadow(4)`, `user_attr(4)`) e `groups`. Os dados para esses itens vêm de uma variedade de fontes. Nomes e endereços de host, por exemplo, podem ser encontrados em `/etc/hosts`, NIS, LDAP, DNS ou Multicast DNS. Os sistemas em ambientes restritos serão mais seguros se apenas entradas de arquivos locais forem usadas para esses itens.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Configure serviços de nome para usar apenas arquivos locais.**

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

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

Ativar os Serviços Sendmail e NTP

O serviço sendmail deverá estar em execução, caso contrário, emails importantes do sistema para `root` não serão entregues.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Ative o sendmail.**

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

3. **Se necessário, instale o serviço NTP.**

   O serviço `ntp` deverá ser instalado em todos os sistemas em que a segurança e a conformidade forem desejadas.

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

4. **Configure o serviço NTP como um cliente e ative o serviço.**

   O daemon Network Time Protocol deve ser ativado e configurado corretamente como um cliente. O arquivo `/etc/inet/ntp.conf` deve incluir, pelo menos, uma definição de servidor. O arquivo também deve conter a linha `restrict default ignore` para impedir que o cliente também aja como um servidor.

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

Desativar o GSS (Exceto se o Kerberos for Usado)

O serviço de segurança genérico (`gss`) gerencia a geração e a validação de tokens de segurança da Generic Security Service Application Program Interface (GSS-API). O daemon `gssd (1M)`funciona entre o kernel `rpc` e a GSS-API.

Observação - O Kerberos usa esse serviço. Desative o serviço `rpc/gss` se o Kerberos não estiver configurado e em uso.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Ative `rpc/gss`.**

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

3. **Defina um limite de tamanho para `/tmpfs`.**

   Por padrão, o tamanho do sistema de arquivos `tmpfs` não tem limite. Para evitar um impacto negativo no desempenho, limite o tamanho de cada montagem `tmpfs`. Para obter mais informações, consulte as páginas man `mount_tmpfs(1M)` e `vfstab(4)`.

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

4. **Reinicialize o servidor de computação.**

```
# reboot
```

Definir o Sticky Bit para Arquivos Graváveis

O sticky bit em um diretório impede que os arquivos em um diretório gravável sejam excluídos ou movidos por alguém que não seja o proprietário do arquivo ou a função `root`. Isso é útil em diretórios que são comuns a muitos usuários, como o diretório `/tmp`.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Defina o sticky bit em `/tmp` e todos os outros arquivos graváveis.**

```
# chmod 1777 /tmp
```

Proteger Despejos de Núcleo

Os despejos de núcleo podem conter dados confidenciais. As proteções podem incluir permissões de arquivo e eventos de registro de despejo de núcleo. Consulte as páginas man `coreadm(1m)` and `chmod(1M)`.

Use o comando `coreadm` para visualizar e definir a configuração atual.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Exiba a configuração atual.**

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

3. **Configure os arquivos de núcleo e proteja o diretório de despejo de núcleo.**

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

4. **Verifique as permissões.**

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

5. **Defina as permissões corretamente no diretório.**

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

Reforçar Pilhas Não Executáveis

A ativação de pilhas não executáveis é uma técnica muito útil para impedir certos tipos de ataques de estouro de buffer. Quando o Oracle Solaris `nxstack` for ativado, o segmento de

memória da pilha de processos será marcado como não executável. Essa extensão defende contra ataques que se baseiam em injetar código mal-intencionado e executá-lo na pilha.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Ativar `nxstack`.**

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

3. **Verifique a configuração.**

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

Ativar Espaço de Troca Criptografado

Criptografe o espaço de troca, seja um volume ZFS ou um dispositivo bruto. A criptografia garante que todos os dados confidenciais, tais como senhas do usuário, sejam protegidos se o sistema precisar mudar essas páginas de disco.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Edite o arquivo `/etc/vfstab` e defina `swap` como `encrypted`.**

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

3. **Crie e inicialize um keystore PKCS #11.**

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

4. **Gere uma chave simétrica e armazene-a em um keystore PKCS #11.**

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

Ativar Auditoria

Certifique-se de que os logs de auditoria capturem todas as ações administrativas incluindo comandos com argumentos.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Configure o recurso de auditoria.**

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

Ativar Proteção de Link de Dados (Falsificação) em Zonas Globais

A proteção de link de dados do Oracle Solaris previne os possíveis danos que podem ser causados por VMs guest mal-intencionadas na rede.

A ativação da configuração da revisão de rastreamento melhora o desempenho da rede ativando o tráfego de rede do ambiente virtual para ser isolado do tráfego maior que é recebido ou enviado pelo sistema host. A proteção de link previne os danos que possam ser causados por VMs guest potencialmente mal-intencionadas na rede. O recurso oferece proteção contra estas ameaças básicas:

- Falsificação de IP e MAC
- Falsificação de quadro L2, como ataques de Bridge Protocol Data Unit (BPDU)

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**
   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Defina a proteção de link.**

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

3. **Confirme a configuração.**

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

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

4. **Defina os IPs permitidos no link.**

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

Ativar Proteção de Link de Dados (Falsificação) em Zonas Não Globais

A proteção de link de dados do Oracle Solaris também pode ser aplicada individualmente a todas as zonas não globais do Oracle Solaris implantadas no ambiente do SuperCluster.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Reforce a proteção de link de dados em uma interface de rede específica usando o comando `zonecfg(1M)`.**

   Garanta que a lista de endereços IP permitidos esteja precisa e completa. A lista deve incluir todos os endereços IP virtuais usados pelo Oracle Solaris IPMP, Oracle Real Application Clusters, etc. Observe também que as alterações feitas na configuração de zona não global do SuperCluster só entram em vigor quando a zona não global é reiniciada.

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

Criar Conjuntos de Dados ZFS Criptografados

As organizações que exigem proteção *data-at-rest* podem optar por intensificar a proteção de aplicativos implantados em zonas e informações usando conjuntos de dados ZFS

criptografados. Para garantir que cada zona não global possa ser iniciada sem intervenção do administrador, os conjuntos de dados ZFS criptografados são configurados para acessar chaves de criptografia ZFS que são armazenadas localmente no aplicativo individual ou no domínio de aplicativos.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Crie chaves de criptografia ZFS.**

   Uma forma simples de criar a chave necessária é usar comandos semelhantes a estes:

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

3. **Crie o conjunto de dados ZFS criptografados.**

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

4. **Criptografe os conjuntos de dados comuns e u01.**

   Essa mesma abordagem pode ser usada para criptografar os conjuntos de dados comuns e u01 usando a mesma chave (específica do SuperCluster) ou uma chave exclusiva por conjunto de dados dependendo das políticas e requisitos específicos do local. Neste exemplo, o conjunto de dados comuns é criado com a mesma chave que foi criada em Passo 3. Observe que os parâmetros de configuração ZFS adicionais, como compactação, também podem ser definidos durante a criação desses conjuntos de dados adicionais.

```
# zfs create -o compression=on -o encryption=aes-256-ccm -o \
keysource=raw,file:///zfs_pool_name/zfskeystore/zone_name.key \zfs_pool_name/u01
```

▼ (Opcional) Definir uma Frase Secreta para Acesso ao Armazenamento de Chaves

A tarefa anterior,Criar Conjuntos de Dados ZFS Criptografados [69], usa um arquivo de chaves (bruto) localmente definido que deve ser armazenado diretamente em um sistema de arquivos. Outra técnica de armazenamento de chaves aproveita um keystore PKCS#11

protegido por frase secreta denominado *Sun Software PKCS#11 Softtoken*. Para usar esse método, execute esta tarefa.

O keystore PKCS#11 deve ser desbloqueado manualmente antes de a chave ser disponibilizada para ZFS. Por fim, isso significa que a intervenção administrativa manual é necessária para montar o conjunto de dados ZFS criptografado (e iniciar a zona não global se a zona também estiver usando um conjunto de dados ZFS criptografado). Para obter mais informações sobre outras estratégias de armazenamento de chaves, consulte a página manual `zfs_encrypt(1M)`.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Defina um PIN (frase secreta) que será necessária para acessar o keystore.**

   O PIN padrão associado a um novo keystore PKCS#11 é `changeme`. Use essa frase secreta no primeiro prompt neste exemplo.

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

3. **Defina uma variável de ambiente `${SOFTTOKEN}` para armazenar a chave em outro local.**

   O material de chave usado pelo PKCS#11 Softtoken é armazenado por padrão no diretório `/var/user/ ${USERNAME}/pkcs11_softtoken`. A variável de ambiente `${SOFTTOKEN}` pode ser definida para armazenar o material de chave em outro local. Você pode usar essa capacidade para ativar o armazenamento específico do SuperCluster para esse material de chave protegido por frase secreta.

```
# export SOFTTOKEN=/<zfs_pool_name>/zfskeystore
# pktool setpin keystore=pkcs11
Enter token passphrase:
Create new passphrase:
Re-enter new passphrase:
```

4. **Crie uma chave.**

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

5. **Crie o conjunto de dados ZFS criptografado, referenciando a chave criada na etapa anterior.**

```
# zfs create -o encryption=aes-256-ccm -o keysource=raw,pkcs11:
object=<zone_name>_rpool zfs_pool_name/zone_name
```

```
Enter PKCS#11 token PIN for 'zfs_pool_name/zone_name':
```

Criar Zonas Globais Imutáveis

A proteção contra alterações com imutabilidade permite que zonas globais e não globais criem um ambiente operacional de alta integridade e resiliente dentro do qual os servidores de computação SuperCluster operam seus próprios serviços. Com base nos recursos de segurança inerentes das zonas globais e não globais do Oracle Solaris, as zonas imutáveis garantem que (alguns ou todos) os diretórios e arquivos do SO não possam ser alterados (sem a intervenção do administrador). A aplicação dessa postura somente leitura ajuda a prevenir alterações não autorizadas, promove procedimentos de gerenciamento de alterações mais fortes e impedem a injeção de malware baseado em kernel e usuário.

Observação - Uma vez configurada uma zona imutável, não é possível atualizá-la de outro meio que não seja pelo login de Caminho Confiável ou quando o sistema é reiniciado no modo gravável por `reboot -- -w`.

Embora sempre seja necessário confirmar se o software aplicativo funciona conforme o esperado em um ambiente imutável, lembre-se de que as instâncias do Oracle Database e os clusters Oracle RAC são verificados para funcionar corretamente em zonas não globais imutáveis do Oracle Solaris.

1. **Faça login na zonal global do Oracle Solaris (Domínio Dedicado, Domínio Raiz ou Domínio de E/S) como superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Modifique a configuração de zona global do Oracle Solaris definindo a propriedade `file-mac-profile`.**

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

3. **Reinicie a zona global do Oracle Solaris para as alterações entrarem em vigor. Faça login no domínio por meio do console do ILOM.**

4. **Inicie o console do caminho confiável da zona global imutável.**

   Ao configurar a zona global imutável, é importante inserir o login do console usando uma destas sequências de quebra:

   - **Console gráfico** – F1-A

- **Console serial** – <Break> ou a sequência de quebra alternativa (CR~ Ctrl-b)

```
trusted path console login:
```

5. **Faça login na zona global do Domínio de E/S e suponha que a função `root` execute todas as atualizações específicas do sistema, em seguida, reinicie o sistema para restaurar o modo somente leitura.**

```
# reboot
```

Configurar Zonas Não Globais Imutáveis

Para configurar uma zona não global do Oracle Solaris para ser imutável, execute esta tarefa.

Observação - O Oracle Solaris 11 OS dá suporte a configurações de zona imutável adicionais além das identificadas nesta tarefa (configuração fixa). Para obter mais informações sobre essas opções, consulte a página manual `zonecfg(1M)`. No entanto, somente a opção de configuração fixa foi testada como parte da arquitetura do SuperCluster.

Cuidado - Não é possível adicionar, modificar nem excluir contas e senhas de usuários de zonas caso a imutabilidade das zonas não globais do Oracle Solaris esteja ativada, conforme descrito nesta tarefa. No entanto, esse problema pode ser resolvido implantando um diretório LDAP para conter informações específicas de zonas, como usuários, funções, grupos, perfis de direitos, etc.

Cuidado - A funcionalidade de zonas imutáveis do Oracle Solaris é limitada aos conjuntos de dados ZFS implementados por padrão em uma zona não global do Oracle Solaris. Sistemas de arquivos, pools ou conjuntos de dados adicionais não estão sujeitos à política de zona imutável, embora o acesso a esses elementos de arquivo possa ser controlado por outros meios, como o uso de montagens de loopback somente leitura.

1. **Faça login em um dos servidores de computação e acesse o console do host como um superusuário.**

   Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Garanta que a zona não global do Oracle Solaris seja desligada.**

   Se esse comando retornar um valor, a zona não global do Oracle Solaris estará em execução e você deverá desligá-la.

Observação - Embora seja possível parar a zona com o comando `zoneadm(1M)`, siga os procedimentos de desligamento apropriados, estabelecidos por sua organização para evitar a possibilidade de interrupção de serviços e perda de dados.

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

3. **Ajuste a configuração de zona global do Oracle Solaris definindo a propriedade de configuração de zona `file-mac-profile`.**

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

4. **Se necessário, desative a configuração imutável de zonas não globais.**

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

5. **Reinicie a zona global do Oracle Solaris para as alterações entrarem em vigor.**

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

Ativar Inicialização Verificada Segura (CLI do Oracle ILOM)

Use essa tarefa para ativar a inicialização verificada segura por meio da CLI do Oracle ILOM. Como alternativa, você pode usar a interface Web do Oracle ILOM. Consulte “Inicialização Verificada Segura (Interface Web do Oracle ILOM)” [76].

Inicialização verificada refere-se à verificação de módulos de objeto antes da execução usando assinaturas digitais. O Oracle Solaris protege contra o carregamento de módulos kernel invasores. A inicialização verificada aumenta a segurança e a robustez do Oracle Solaris verificando os módulos kernel antes da execução.

Se ativada, a inicialização verificada do Oracle Solaris verificará a assinatura de fábrica em um módulo kernel antes de carregá-lo e executá-lo. Essa verificação detecta modificações acidentais ou mal-intencionadas de um módulo. A ação executada é configurável e, quando ativada, imprimirá uma mensagem de aviso e continuará a carregar e executar o módulo ou falhará e não o carregará.

1. **Acesse o Oracle ILOM no servidor de computação.**

Consulte Fazer Login em um Servidor de Computação e Alterar a Senha Padrão [51]

2. **Ative a inicialização verificada.**

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

3. **Acesse e exiba o certificado fornecido pela Oracle.**

Um arquivo de certificado de inicialização verificada pré-instalado, `/etc/certs/ORCLS11SE`, é fornecido como parte do Oracle ILOM.

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

4. **Inicie o carregamento do certificado.**

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

5. **Copie o conteúdo do arquivo `/etc/certs/ORCLS11SE` e cole no console do Oracle ILOM.**

Pressione Ctrl-z para salvar e processar informações.

Pressione Ctrl-c para sair e descartar as alterações.

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

6. **Verifique o certificado.**

```
-> show /HOST/verified_boot/user_certs/1/
/HOST/verified_boot/user_certs/1
Targets:
Properties:
clear_action = (Cannot show property)
issuer = /C=US/O=Oracle Corporation/OU=VeriSign Trust Network/OU=Class 2 Managed PKI
 Individual
Subscriber CA/CN=Object Signing CA
load_uri = (Cannot show property)
subject = /O=Oracle Corporation/OU=Corporate Object Signing/OU=Solaris Signed Execution/
CN=Solaris 11
```

```
valid_from = Mar 1 00:00:00 2012 GMT
valid_until = Mar 1 23:59:59 2015 GMT
Commands:
cd
load
reset
show
->
```

7. **Verifique se o parâmetro OBP `use-nvram` está definido como `false`.**

   Ao usar a inicialização verificada, o parâmetro `use-nvram` do OBP deve ser definido como `false`. Isso impede que o OBP seja modificado para desativar o recurso de inicialização verificada. O valor padrão é false. Faça login no Oracle Solaris e digite:

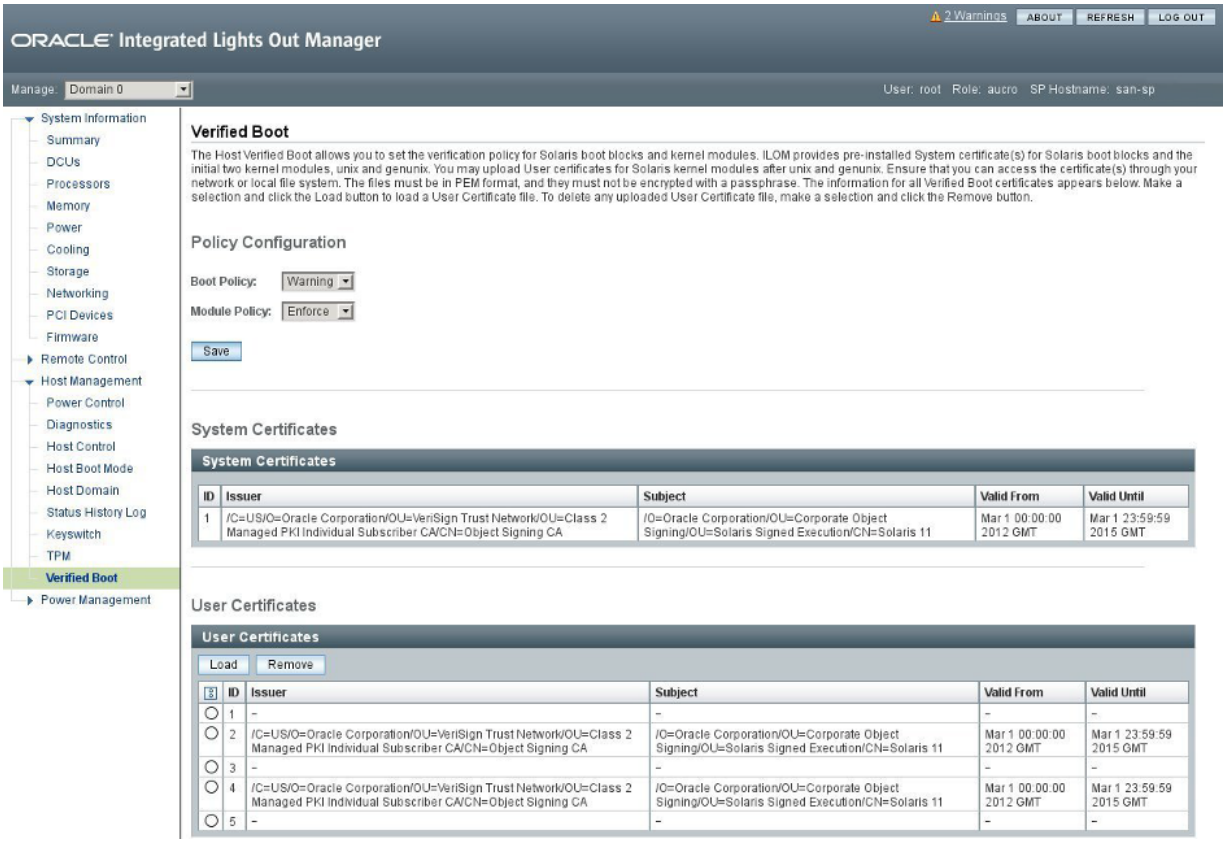
```
$ /usr/sbin/eeprom/eeprom use-nvramrc?

use-nvramrc?=false
```

Inicialização Verificada Segura (Interface Web do Oracle ILOM)

A interface Web do Oracle ILOM também dá suporte à definição das variáveis da política de inicialização verificada e o gerenciamento de arquivos de certificado fornecendo a mesma funcionalidade que a CLI. Navegue para o link Inicialização Verificada no menu de navegação Gerenciamento de Host.

Por exemplo:



Recursos Adicionais do Servidor de Computação

Para obter os guias de segurança do Oracle Solaris OS e do Oracle Solaris Cluster, consulte a biblioteca de documentação correspondente à sua versão do sistema operacional. As bibliotecas estão disponíveis em `http:/docs.oracle.com/en/operating-systems`.

Para obter informações de segurança do Oracle VM Server para SPARC, consulte o guia de segurança em `http://docs.oracle.com/cd/E62357_01`.

Para obter informações de segurança sobre o hardware do servidor de computação, consulte o guia de segurança em `http://docs.oracle.com/cd/E55211_01`.

Protegendo o Appliance de Armazenamento de ZFS

O appliance de armazenamento de ZFS é um dos componentes do SuperCluster para dar suporte à consolidação de armazenamento em uma variedade de cargas de trabalho exigentes, incluindo business intelligence, data warehousing, virtualização, desenvolvimento e teste e proteção de dados.

O appliance de armazenamento de ZFS inclui dois controladores de armazenamento de ZFS redundantes. É necessário proteger os dois controladores.

Estas seções descrevem as diretrizes e recursos de segurança do appliance de armazenamento de ZFS:

▼ Fazer Login no Appliance de Armazenamento de ZFS

Para executar as tarefas de segurança nesta seção, faça login no appliance de armazenamento de ZFS pela rede de gerenciamento.

Esta tarefa descreve como fazer login usando a CLI. Para obter instruções equivalentes para fazer login na interface Web do Oracle ILOM, consulte o *Guia de Administração do Appliance de Armazenamento de ZFS Oracle* Consulte “Recursos Adicionais do Appliance de Armazenamento de ZFS” [89].

1. **Em sua rede de armazenamento, use SSH para estabelecer conexão com o appliance de armazenamento de ZFS.**

   Se você não tiver configurado outros usuários para administrar o appliance, faça login como `root`.

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

2. **Se necessário, acesse a ajuda da CLI.**

   O comando `help` fornece ajuda específica do contexto. Ajuda sobre um tópico específico está disponível especificando o tópico como um argumento para `help`. Os tópicos disponíveis são exibidos completando com tab o comando de ajuda ou digitando `help topics`.

Determinar a Versão do Software do Appliance de Armazenamento de ZFS

Use este procedimento para determinar a versão de software no appliance de armazenamento de ZFS.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Exiba a versão de software.**

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

   Neste exemplo, a versão do software do appliance de armazenamento de ZFS é `2013.06.05.2.10`.

   Para atualizar a versão do software do appliance de armazenamento de ZFS, instale o SuperCluster Quarterly Full Stack Download Patch mais recente disponível no My Oracle Support em `https://support.oracle.com`.

Observação - No caso do SuperCluster, restrições adicionais podem limitar as versões do software de appliance de armazenamento de ZFS que podem ser usadas e como elas são atualizadas. Nessas situações, entre em contato com o representante da Oracle.

Alterar a Senha root do Appliance de Armazenamento de ZFS

O próprio appliance de armazenamento de ZFS não é pré-configurado com uma senha root padrão. A configuração inicial do appliance de armazenamento de ZFS é executada por meio de uma sessão de console a partir de seu Oracle ILOM incorporado. A senha root do appliance é definida durante sua sessão de configuração inicial.

Quando você inicialmente acessa o console do appliance, uma tela de configuração da interface do shell é exibida. Verifique as informações na tela e digite os valores necessários. A senha root do appliance de armazenamento de ZFS é definida durante esse processo.

Observação - O Oracle ILOM para o appliance tem uma conta root e senha de welcome1 padrão. Consulte Protegendo o Oracle ILOM [35].

Assim que você tiver uma conta root, você poderá alterar a senha a qualquer momento conforme descrito nesta tarefa.

Observação - Quando uma senha é alterada para qualquer componente do SuperCluster gerenciado pelo Oracle Engineered Systems Hardware Manager (como o sistema operacional do controlador de armazenamento de AFS), também é necessário atualizar a senha no Oracle Engineered Systems Hardware Manager. Para obter detalhes, consulte o *Guia de Administração do Oracle SuperCluster Série M7*.

---

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Altere a senha root.**

   Neste exemplo, substitua a *senha* por uma que cumpra as políticas de complexidade de senhas do Departamento de Defesa dos EUA.

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

Para obter mais informações sobre a instalação e a configuração iniciais do appliance de armazenamento de ZFS, consulte o *Guia de Instalação do Appliance de Armazenamento de ZFS da Oracle*. Consulte “Recursos Adicionais do Appliance de Armazenamento de ZFS” [89].

Serviços de Rede Expostos Padrão (Appliance de Armazenamento de ZFS)

Esta tabela lista os serviços de rede padrão que são expostos pelo appliance de armazenamento de ZFS.

Serviço	Protocolo	Porta	Descrição
SSH	TCP	22	Usada pelo serviço Secure Shell para permitir o acesso administrativo ao appliance de armazenamento de ZFS usando uma CLI.
PORTMAP	TCP/UDP	111	Usada pelo daemon de mapeamento de porta Remote Procedure Call (RPC) (conhecido como `rpcbind` ou `portmap`). Esse serviço é necessário para dar suporte ao NFS versão 3.
NTP	UDP	123	Usada pelo serviço Network Time Protocol (NTP) integrado (somente cliente) para sincronizar o relógio do sistema local com uma ou mais fontes de tempo externas.
HTTPS (BUI)	TCP	215	Usada pelo serviço HTTPS integrado para permitir o acesso administrativo ao appliance de armazenamento de ZFS por um canal (SSL/TLS) criptografado usando uma interface de navegador.
Replicação Remota	TCP	216	Usada pelo serviço de replicação de dados remota integrada. A replicação de dados remota duplica e sincroniza projetos e compartilha-os entre os appliances de armazenamento de ZFS por um canal (SSL/TLS) criptografado.
NFS	TCP/UDP	2049 4045 vários	Usada pelo serviço de sistema de arquivos de rede (NFS). O NFS fornece o serviço de compartilhamento de arquivos de rede. O número real de portas depende de qual versão do protocolo NFS é usada. O NFS versão3 baseia-se no daemon de mapeamento de portas RPC (listado acima) e portas dinamicamente alocadas para fornecer montagem, status, cota e serviços relacionados. No entanto, o NFS verão 4 baseia-se somente no TCP/2049. O serviço de bloqueio de NFS usa TCP/4045.
iSCSI / iSNS	TCP	3260	Usada pelo serviço iSCSI que fornece um protocolo de sistema de rede de armazenamento baseado em IP para recursos de vínculo de armazenamento de dados. O appliance de armazenamento de ZFS pode ser configurado para compartilhar dispositivos iSCSI (denominados LUNs) com clientes em rede.
Service Tags	TCP	6481	Usada pelo serviço Oracle ServiceTag. Esse é um protocolo de descoberta da Oracle usado para identificar servidores e facilitar solicitações de serviço. Esse serviço é usado por produtos, como o Oracle Enterprise Manager Ops Center, para descobrir software de appliance de armazenamento de ZFS e integrar com outras soluções de serviço automático da Oracle.
NDMP	TCP	10000	Usada pelo serviço Network Data Management Protocol (NDMP) que permite ao appliance de armazenamento de ZFS participar de backups coordenados remotamente.

O appliance de armazenamento de ZFS também dá suporte a uma variedade de outros serviços que são desativados incluindo, por padrão, `HTTP`, `FTP`, `SFTP`, `TFTP`, `WebDAV`, etc. Portas de rede adicionais poderão ser expostas se esses serviços forem ativados após a instalação.

Protegendo a Configuração de Segurança do Appliance de Armazenamento de ZFS

Estes tópicos descrevem como proteger a configuração de segurança do appliance de armazenamento de ZFS:

▼ Implementar a Proteção da Configuração de Segurança do Oracle ILOM

O appliance de armazenamento de ZFS inclui um Oracle ILOM incorporado como parte do produto. Como com outras implementações do Oracle ILOM, há alterações de configuração relevantes de segurança que podem ser implementadas para melhorar a configuração de segurança padrão do dispositivo.

- **Proteja a interface do Oracle ILOM do appliance de armazenamento de ZFS executando os procedimentos em Protegendo o Oracle ILOM [35].**

▼ Desativar Serviços Desnecessários (Appliance de Armazenamento de ZFS)

Desative todos os serviços que não sejam necessários para dar suporte aos requisitos operacionais e de gerenciamento da plataforma.

Por padrão, o appliance de armazenamento de ZFS emprega uma configuração de *rede protegida por padrão* pela qual serviços não essenciais já são desativados. No entanto, com

base em seus requisitos e políticas de segurança, pode ser necessário ativar ou desativar serviços adicionais.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Exiba a lista de serviços compatíveis com o appliance de armazenamento de ZFS.**

   ```
   hostname:> configuration services
   ```

3. **Determine se um determinado serviço está ativado.**

   Substitua *servicename* pelo nome de um serviço identificado em Passo 2.

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

   Um serviço será ativado se seu parâmetro de estado retornar um valor de `enabled`. Por exemplo:

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

4. **Desative um serviço que não seja mais necessário.**

   Defina o estado do serviço como desativado. Por exemplo:

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

▼ Desativar Roteamento Dinâmico

O appliance de armazenamento de ZFS está configurado para executar o protocolo de roteamento dinâmico por padrão.

Antes de desativar o serviço de rotamento dinâmico, garanta que o appliance de armazenamento de ZFS esteja diretamente conectado a qualquer rede com a qual ele deva ser comunicar ou que tenha sido configurado para usar o roteamento dinâmico ou uma rota padrão. Essa etapa é necessária para garantir que não haja perda de conectividade assim que o roteamento dinâmico seja desativado.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Desativar o roteamento dinâmico.**

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

3. **Para determinar se o roteamento dinâmico está ativado, digite:**

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

▼ Restringir o Acesso root Remoto Usando Secure Shell

Por padrão, o appliance de armazenamento de ZFS permite o acesso administrativo à conta root usando o serviço Secure Shell (SSH).

Execute esse procedimento para desativar o acesso root remoto usando SSH.

Depois de fazer essa alteração na configuração, a conta root não pode mais acessar o sistema usando SSH. No entanto, a conta root pode acessar esse sistema usando a interface administrativa HTTPS.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Desative o acesso root remoto.**

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

3. **Verifique se a conta root não pode mais acessar o sistema usando SSH.**

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

4. **Se o acesso administrativo SSH for necessário, crie, pelo menos, uma conta que não seja root.**

   Para obter instruções, consulte o *Guia de Administração do Appliance de Armazenamento de ZFS* correspondente à release em execução no appliance de armazenamento de ZFS. Consulte "Recursos Adicionais do Appliance de Armazenamento de ZFS" [89].

Configurar o Tempo Limite de Inatividade da Interface Administrativa (HTTPSN)

O appliance de armazenamento de ZFS dá suporte à capacidade de desconectar e fazer logoff de sessões administrativas que permanecerem inativas por um intervalo predefinido de minutos. Por padrão, o tempo da sessão de interface do navegador (HTTPS) se esgota após 15 minutos.

Observação - Nenhum parâmetro equivalente aplica um tempo limite de inatividade na linha de comando SSH da interface de armazenamento de ZFS.

Execute esse procedimento para definir o parâmetro de tempo limite de inatividade como um valor personalizado.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Exiba o parâmetro de tempo limite de inatividade atual associado à interface de navegador.**

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

3. **Configure o parâmetro de tempo limite.**

   O valor `session_timeout` está especificado em minutos (10 minutos nesse exemplo).

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

4. **Verifique o parâmetro de tempo limite repetindo Passo 2.**

Desativar Protocolos SNMP Não Aprovados

Por padrão, SNMPv1 e SNMPv2c são ativados no appliance de armazenamento de ZFS. O appliance de armazenamento de ZFS dá suporte a SNMPv1/v2c em todas as versões compatíveis do produto. A partir da versão 2013.1.2, o appliance de armazenamento de ZFS também dá suporte ao SNMPv3.

Observação - A versão 3 do protocolo SNMP introduziu o suporte para o Modelo de Segurança Baseado em Usuário (USM). Essa funcionalidade substitui as strings de comunicação SNMP tradicionais pelas contas de usuário reais que podem ser configuradas com permissões específicas, protocolos de autenticação e privacidade e senhas. Por padrão, o appliance de armazenamento de ZFS não inclui um nome de usuário nem uma senha para a conta USM integrada (somente leitura). Para fins de segurança, configure as credenciais e os protocolos USM com base em requisitos de implantação, gerenciamento e monitoramento.

Certifique-se de que versões mais antigas ou não usadas do protocolo SNMP esteja desativadas, a menos que elas sejam necessárias.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Determine qual versão do protocolo SNMP é usada pelo dispositivo.**

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

3. **Ative o uso de SNMPv3 (se disponível).**

   O uso de SNMPv1/v2c e SNMPv3 é mutuamente exclusivo, portanto, ao ativar o SNMPv3, o SNMPv1/v2c são desativados.

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

4. **Verifique a versão do SNMP.**

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

▼ Configurar Strings de Comunidade SNMP

Execute esta tarefa apenas se o appliance de armazenamento de ZFS estiver configurado para usar SNMPv1 ou v2.

Como o SNMP, geralmente, é usado para monitorar a integridade do dispositivo, é importante que as strings de comunidade de SNMP padrão usadas pelo dispositivo sejam alteradas por um valor definido pelo cliente.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Altere a string de comunidade de SNMP.**

   Neste exemplo, substitua *string* por um valor que esteja em conformidade com os requisitos do Departamento de Defesa dos EUA relativos à composição de strings de comunidade de SNMP.

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

3. **Verifique a string de comunidade de SNMP.**

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

Configurar Redes de SNMP Autorizadas

Execute esta tarefa apenas se o appliance de armazenamento de ZFS estiver configurado para usar SNMPv1 ou v2.

Para minimizar a divulgação da configuração do sistema, consultas SNMP só devem ser aceitas de fontes de host ou rede aprovadas.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Configure o parâmetro de rede autorizada SNMP.**

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

3. **Verifique o valor do parâmetro de rede autorizada SNMP.**

   Neste exemplo, a definição do parâmetro de rede como `127.0.0.1/8` bloqueia efetivamente todas as consultas SNMP baseadas em rede. Esse valor deve ser ajustado conforme necessário para determinar redes e hosts aprovados.

   Um valor de `0.0.0.0/0` permite consultas de qualquer local de rede.

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

▼ Restringir o Acesso à Rede de Gerenciamento

Além desses procedimentos de proteção de segurança, as interfaces de armazenamento expostas pelo appliance de armazenamento de ZFS devem ser implantadas em uma rede de gerenciamento isolada dedicada. Essa etapa ajuda a proteger o appliance de armazenamento de ZFS contra tráfego de rede não autorizado ou não intencional. Você deve controlar rigorosamente o acesso à rede de armazenamento concedendo-o apenas aos administradores que precisam desse nível de acesso.

Além disso, o appliance de armazenamento de ZFS pode ser configurado para ativar ou desativar o acesso administrativo (gerenciamento) em interfaces de rede específicas. Essa alteração pode ser implementada usando esse procedimento.

1. **Faça login no appliance de armazenamento de ZFS.**

   Consulte Fazer Login no Appliance de Armazenamento de ZFS [79].

2. **Configure as interfaces de rede de gerenciamento**

   Neste exemplo, substitua o valor *interface* pelo nome da interface de rede real para a qual essa configuração será aplicada.

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

Recursos Adicionais do Appliance de Armazenamento de ZFS

Para obter diretrizes de segurança adicionais para o appliance de armazenamento de ZFS, consulte o guia de segurança correspondente à release em execução no appliance de armazenamento de ZFS. Consulte Determinar a Versão do Software do Appliance de Armazenamento de ZFS [80].

Estes guias fornecem informações adicionais sobre os recursos e as opções de segurança do produto:

- *Guia de Segurança de Release do Appliance de Armazenamento de ZFS da Oracle* (Release 2013.1.4.0)

  http://docs.oracle.com//cd/E56047_01
- *Guia de Segurança de Release do Appliance de Armazenamento de ZFS da Oracle* (Release 2013.1.3.0)

http://docs.oracle.com/cd/E56021_01

- *Guia de Segurança de Release do Appliance de Armazenamento de ZFS da Oracle* (Release 2013.1.2.0)

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

Protegendo os Servidores de Armazenamento Exadata

Os servidores de armazenamento Exadata (servidores de armazenamento) são os elementos básicos do armazenamento do SuperCluster. Cada servidor de armazenamento é fornecido pré-instalado e integrado como parte do SuperCluster M7 com todos os seus componentes de software, armazenamento e computação necessários.

Observação - Você só pode fazer alterações na configuração por meio da aplicação de métodos, patches ou atualizações aprovadas. O software de servidor de armazenamento não pode ser alterado de nenhuma outra forma.

O SuperCluster M7 tem, no mínimo, três servidores de armazenamento. Os servidores de armazenamento adicionais podem ser instalados no principal rack do SuperCluster e em racks de expansão opcionais. Você deve proteger cada servidor de armazenamento individual.

Estes tópicos descrevem como proteger os servidores de armazenamento.

▼ Fazer Login no Sistema Operacional do Servidor de Armazenamento

- **Na rede de gerenciamento, faça login em um dos servidores de armazenamento como `celladmin`.**

Para a senha padrão, consulte “Contas e Senhas Padrão” [92].

```
# ssh celladmin@Storage_Server_IP_address
```

Contas e Senhas Padrão

Esta tabela lista as contas e senhas padrão do servidor de armazenamento.

Nome da Conta	Tipo	Senha Padrão	Descrição
`root`	Administrador	`welcome1`	Usado para acessar o sistema operacional do servidor de armazenamento para executar ações administrativas gerais e atualizar o software do servidor de armazenamento.
`celladmin`	Administrador de célula	`welcome`	Usado para executar a instalação e a configuração do servidor de armazenamento. Além disso, todos os serviços de armazenamento na plataforma funcionam com essa conta.
`cellmonitor`	Monitor	`welcome`	Usado somente para fins de monitoramento. Essa conta tira proveito de um shell restrito para garantir que a configuração e os objetos que residem no servidor de armazenamento não possam ser modificados a partir dessa conta.

▼ Alterar Senhas do Servidor de Armazenamento

Para obter uma lista de contas e senhas padrão, consulte “Contas e Senhas Padrão” [92].

Observação - Quando uma senha é alterada para qualquer componente do SuperCluster gerenciado pelo Oracle Engineered Systems Hardware Manager (como o sistema operacional do servidor de armazenamento Exadata), também é necessário atualizar a senha no Oracle Engineered Systems Hardware Manager. Para obter detalhes, consulte o *Guia de Administração do Oracle SuperCluster Série M7*.

1. **Faça login no servidor de armazenamento como `celladmin`.**

   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Altere uma senha padrão usando um destes métodos.**

   - **Altere a senha para uma conta no servidor no qual você está fazendo login.**

     ```
     # passwd account_name
     ```

- **Altere a senha de uma conta em todos os servidores de armazenamento.**
  O `cell_group` é um arquivo de texto simples que lista os nomes de host de todos os servidores de armazenamento (um por linha).
  Neste exemplo, substitua estes itens de linha de comando:
  - *new_password* – substitua pela nova senha que está em conformidade com as políticas do local.
  - *account_name* – substitua pelo nome da conta do Oracle Linux.

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

Determinar a Versão de Software do Servidor de Armazenamento Exadata

1. **Faça login em um dos servidores de armazenamento.**
   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Digite este comando.**
   Neste exemplo a versão do software do servidor de armazenamento é 12.1.2.1.1.150316.2.

```
# imageinfo -ver
12.1.2.1.1.150316.2
```

   Para atualizar a versão do software, instale o SuperCluster Quarterly Full Stack Download Patch mais recente disponível no My Oracle Support em `https://support.oracle.com`.

Observação - No caso do SuperCluster, restrições adicionais podem limitar as versões do software que podem ser usadas e como elas são atualizadas. Nessas situações, entre em contato com o representante da Oracle.

Serviços de Rede Expostos Padrão (Servidores de Computação)

Nome do Serviço	Protocolo	Porta	Descrição
SSH	TCP	22	Usado pelo serviço Secure Shell que é integrado ao software de servidor de armazenamento para fornecer acesso administrativo ao sistema usando uma CLI.

Nome do Serviço	Protocolo	Porta	Descrição
			Por padrão, o servidor do Secure Shell é configurado para responder a solicitações de conexão somente nas redes de gerenciamento (NET 0) e IB (BONDIB0).

O servidor de armazenamento também se comunica com os Domínios do Oracle Database no SuperCluster usando o protocolo Reliable Datagram Sockets (RDSv3) por interfaces RDMA. Essa comunicação ponto a ponto não usa TCP/IP e é limitada à partição de rede IB interna na qual os Domínios do Oracle Database no SuperCluster e servidores de armazenamento residem.

Protegendo a Configuração de Segurança do Servidor de Armazenamento

Observação - O servidor de armazenamento inclui um Oracle ILOM incorporado como parte do produto. Como com outras implementações do Oracle ILOM, há alterações de configuração relevantes de segurança que podem ser implementadas para melhorar a configuração de segurança padrão do dispositivo. Para obter mais informações, consulte Protegendo o Oracle ILOM [35].

Estes tópicos descrevem como proteger a segurança dos servidores de armazenamento:

Restrições de Configuração de Segurança

O utilitário host_access_control é o único método permitido e compatível para implementar as alterações na configuração de segurança nos servidores de armazenamento. Você não tem permissão para fazer alterações manuais na configuração desses dispositivos de acordo com a notificação 1068804.1 do Oracle Support. Além disso, antes de usar essa ferramenta, você precisa primeiro obter uma aprovação explícita do Oracle SuperCluster Support para alterar a configuração de segurança de seus servidores de armazenamento. Para solicitar essa aprovação, abra uma solicitação de serviço com o Oracle Support.

O comando host_access_control, disponível a partir do software Exadata versão 11.2.3.3.0, é usado para implementar um conjunto limitado de configurações de acesso e segurança:

- Restringindo o acesso root remoto.
- Restringindo o acesso da rede a determinadas contas.
- Implementando políticas de complexidade e validade de senhas.
- Implementando banners de aviso de login.
- Definindo políticas de tempo limite de sessão e bloqueio de contas.

▼ Exibir as Configurações de Segurança Disponíveis com host_access_control

Para o que está disponível no utilitário host_access_control, execute estas etapas.

1. **Faça login no sistema operacional do servidor de armazenamento.**

   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **(Opcional) Exiba a ajuda host_access_control para obter detalhes.**

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

Configurar uma Senha do Carregador de Inicialização do Sistema

Você pode configurar os servidores de armazenamento para solicitar uma senha do carregador de inicialização do sistema sempre que um administrador tentar acessar o editor do carregador de inicialização (GRUB) ou a interface de comando.

1. **Faça login no servidor de armazenamento como `celladmin`.**
   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Configure uma senha do carregador de inicialização do sistema.**

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

3. **Verifique a configuração.**
   Se o comando retornar um valor semelhante a este exemplo, uma senha de carregador de inicialização será instalada.

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

Desativar o Acesso ao Console do Sistema Oracle ILOM

Cada servidor de armazenamento inclui um Oracle ILOM incorporado para permitir o monitoramento e o gerenciamento remotos. O Oracle ILOM também pode ser usado para fornecer acesso remoto ao console do sistema de servidor de armazenamento.

Execute este procedimento se quiser desativar o acesso ao servidor de armazenamento por meio do Oracle ILOM.

1. **Faça login no servidor de armazenamento como `celladmin`.**
   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Desative o acesso ao console do sistema Oracle ILOM.**

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

3. **Verifique a configuração.**

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

Restringir o Acesso root Remoto Usando SSH

Por padrão, o usuário root tem permissão para acessar remotamente cada servidor de armazenamento.

1. **Faça login no servidor de armazenamento como celladmin.**
Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Desative o acesso root remoto por meio do SSH.**

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

3. **Verifique a configuração.**

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

Configurar o Bloqueio de Contas do Sistema

Por padrão, os servidores de armazenamento são configurados para bloquear contas do sistema após cinco tentativas de autenticação com falha consecutivas.

Para alterar esse limite, execute este procedimento.

1. **Faça login no servidor de armazenamento como celladmin.**
Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Altere o limite.**
Para cumprir os requisitos de segurança do Departamento de Defesa dos EUA, especifique um valor de 3. Se necessário, substitua esse valor por um que esteja em conformidade com a política do local.

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

3. **Verifique a configuração.**

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

Configurar Regras de Complexidade de Senhas

Por padrão, os servidores de armazenamento não implementam restrições significativas que regem a complexidade das senhas das contas do sistema.

1. **Faça login no servidor de armazenamento como `celladmin`.**
   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Defina uma política de complexidade de senhas.**
   Sintaxe:

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

Substitua *N0,N1,N2,N3,N4* por um conjunto de cinco valores separados por vírgula. Esses cinco valores definem coletivamente a política real de complexidade de senhas do sistema. Estes são os valores (também listados na página man `passwdqc.conf(5)`):

- *N0* –Usado para senhas que consistem em apenas uma classe de caractere (dígitos, caracteres de letra minúscula, caracteres de letra maiúscula e caracteres especiais). Em geral, esse parâmetro é definido como `disabled` porque senhas simples não são seguras.
- *N1* – Usado para senhas que consistem em duas classes de caracteres que não atendem aos requisitos para uma frase secreta. Para que essa regra seja aplicada, a senha deverá ter, no mínimo, N1 caracteres.
- *N2* – Usado para senhas que consistem em uma frase secreta. Para que essa regra seja aplicada, a senha deverá ter, pelo menos, N2 caracteres e deve cumprir o requisito de frase secreta.
- *N3* – Usado para senhas que consistem em, pelo menos, três classes de caracteres. Para que essa regra seja aplicada, a senha deverá ter, pelo menos, N3 caracteres.
- *N4* – Usado para senhas que consistem em, pelo menos, quatro classes de caracteres. Para que essa regra seja aplicada, a senha deverá ter, pelo menos, *N4* caracteres.

Para cumprir os requisitos de segurança do Departamento de Defensa dos EUA, defina os parâmetros *N0,N1,N2,N3,N4* como `disabled,disabled,disabled,disabled,15`. Isso garante que as únicas senhas que sejam aceitas consistam em, pelo menos, quatro classes de caracteres (letra maiúscula, letra minúscula, numérico e especial) e tenham, pelo menos, 15 caracteres.

Observação - Letras maiúsculas no início da senha e dígitos no final da senha não são contados ao calcular o número de classes de caracteres.

Por exemplo, para definir a complexidade das senhas que cumpra os requisitos do Departamento de Defesa dos EUA, digite:

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

3. **Verifique o status atual desta configuração.**

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

Configurar uma Política de Histórico de Senhas

Por padrão, os servidores de armazenamento definem uma política de histórico de senhas que impede os usuários de reutilizarem as 10 (dez) últimas senhas.

1. **Faça login no servidor de armazenamento como `celladmin`.**
   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Exiba a configuração atual.**

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

3. **Altere o histórico de senhas.**
   Para cumprir os requisitos de segurança e PCI-DSS do Departamento de Segurança dos EUA, defina a política de histórico de senhas como `5`. Isso garante que uma conta não possa reutilizar nenhuma das cinco senhas anteriores atribuídas a ela. Se necessário, substitua esse valor por um que esteja em conformidade com as políticas do local.

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

4. **Para verificar a configuração, repita Passo 2.**

Configurar um Atraso de Bloqueio de Autenticação com Falha

Por padrão, os servidores de armazenamento implementam uma política em que uma conta do sistema é bloqueada por 10 minutos após qualquer tentativa de autenticação com falha.

Para alterar esse limite, execute este procedimento.

1. **Faça login no servidor de armazenamento como `celladmin`.**

   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Exiba a configuração atual.**

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

3. **Altere o limite.**

   Para cumprir os requisitos de segurança do Departamento de Defesa dos EUA, defina o valor como 4 (segundos). Se necessário, substitua esse valor por um que esteja em conformidade com as políticas do local.

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

4. **Para verificar a configuração, repita Passo 2.**

▼ Configurar Políticas de Controle de Validade de Senhas

Os servidores de armazenamento dão suporte a uma variedade de controles de validade de senhas, inclusive parâmetros para controlar o número máximo de dias que uma senha é usada, o número mínimo de dias entre alterações de senhas e o número de dias antes da expiração da senha em que um usuário é alertado.

Para cumprir os requisitos de segurança e PCI-DSS do Departamento de Segurança dos EUA, use os valores do Departamento de Segurança dos EUA nesta tabela:

Política	Valor Padrão da Oracle	Valor DOD
Vida útil máxima da senha	90 dias	60 dias
Vida útil mínima da senha	1 dia	1 dia
Tamanho mínimo da senha	8 caracteres	15 caracteres
Advertência para expiração de senha	7 dias	7 dias

Para alterar qualquer um desses parâmetros, execute este procedimento.

1. **Faça login no servidor de armazenamento como `celladmin`.**
   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Exiba as configurações atuais.**

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

3. **Configure essas políticas de acordo com as políticas de senha do local.**

   - **Para alterar o parâmetro de vida útil máxima de senhas, digite:**

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

   - **Para alterar o parâmetro de vida útil mínima de senhas, digite:**

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

   - **Para alterar o parâmetro de tamanho mínimo de senhas, digite:**

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

   - **Para alterar o parâmetro de advertência de expiração da senha, digite:**

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

4. **Para verificar as configurações, repita Passo 2.**

Configurar o Tempo Limite de Inatividade da Interface Administrativa (Shell de Login)

O servidor de armazenamento dá suporte à capacidade de encerrar sessões administrativas que ficam inativas por mais do que um intervalo de segundos predefinido.

Para definir o tempo limite de inatividade da interface administrativa para um shell de login da conta de sistema, execute este procedimento.

1. **Faça login no servidor de armazenamento como `celladmin`.**
   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Exiba a configuração atual.**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep Shell
```

3. **Defina o tempo limite de inatividade da interface administrativa.**

   Para cumprir os requisitos de segurança e PCI-DSS do Departamento de Defesa dos EUA, especifique um valor de `900` (segundos). Se necessário, substitua esse valor por um que esteja em conformidade com a política do local.

```
# /opt/oracle.cellos/host_access_control idle-timeout --shell 900
```

4. **Para verificar a configuração, repita Passo 2.**

Configurar o Tempo Limite de Inatividade da Interface Administrativa (Shell de Login)

O servidor de armazenamento dá suporte à capacidade de encerrar sessões SSH administrativas que ficam inativas por mais do que um intervalo de segundos predefinido.

Para definir o tempo limite de inatividade da interface administrativa para uma sessão SSH, execute este procedimento.

1. **Faça login no servidor de armazenamento como `celladmin`.**

   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Exiba a configuração atual.**

```
# /opt/oracle.cellos/host_access_control idle-timeout --status | grep SSH
```

3. **Defina o tempo limite de inatividade da interface administrativa para uma sessão SSH.**

   Para cumprir os requisitos de segurança do Departamento de Defesa dos EUA, especifique um valor de `900` (segundos). Se necessário, substitua esse valor por um que esteja em conformidade com a política do local.

```
# /opt/oracle.cellos/host_access_control idle-timeout --client 900
```

4. **Para verificar a configuração, repita Passo 2.**

▼ Configurar um Banner de Aviso de Login (Servidor de Armazenamento)

O servidor de armazenamento dá suporte à capacidade de exibir mensagens específicas do cliente antes que um usuário faça a autenticação bem-sucedida no sistema.

Para definir um banner de aviso de login pré-autenticação, execute este procedimento.

1. **Faça login no servidor de armazenamento como `celladmin`.**

   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Determine a configuração atual.**

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

3. **Crie um arquivo de texto que contenha a mensagem do banner de aviso de login aprovado.**

4. **Defina um banner de aviso de login de pré-autenticação.**

   Para cumprir os requisitos de segurança do Departamento de Defesa dos EUA, substitua *filename* pelo caminho e nome de um arquivo que contenha a mensagem do banner de aviso de login aprovado.

   ```
   # /opt/oracle.cellos/host_access_control banner --file filename
   ```

5. **Para verificar a configuração, repita Passo 2.**

Limitando o Acesso à Rede Remota

É possível limitar o acesso à rede remota de entrada aos servidores de armazenamento implementando um conjunto de regras de filtragem. Você também pode refinar o acesso à rede definindo um conjunto de regras personalizadas.

Use estes procedimentos para limitar o acesso remoto.

- “Isolamento da Rede de Gerenciamento do Servidor de Armazenamento” [104]
- Limitando o Acesso à Rede Remota [104]

Isolamento da Rede de Gerenciamento do Servidor de Armazenamento

O servidor de armazenamento é implantado em uma rede de gerenciamento dedicada e isolada. Isso ajuda a proteger o servidor de armazenamento contra tráfego de rede não autorizado ou não intencional. O acesso à rede de gerenciamento deve ser estritamente controlado com acesso concedido apenas aos administradores que precisem desse nível de acesso.

▼ Limitando o Acesso à Rede Remota

Há várias formas de limitar o acesso à rede remota nos servidores de armazenamento. Você pode restringir o acesso à rede de entrada ao servidor de armazenamento implementando um conjunto de regras de filtragem de cima para baixo que defina o acesso por conta de usuário e origem. Também é possível definir um conjunto de regras personalizadas para permitir ou negar acesso de acordo com os requisitos do Departamento de Defesa dos EUA e PCI-DSS.

Cuidado - Ao implementar políticas que não sejam padrão, tenha cuidado para garantir que o acesso ao sistema não seja interrompido. Ao adicionar novas regras individuais, as alterações entram em vigor imediatamente.

Para implementar um conjunto de regras, executa este procedimento.

1. **Faça login no servidor de armazenamento como `celladmin`.**

   Consulte Fazer Login no Sistema Operacional do Servidor de Armazenamento [91].

2. **Examine o conjunto de regras ativo.**

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

3. **Exporte o conjunto de regras atual para um arquivo e salve-o como uma cópia de backup.**

   Este comando exporta o conjunto de regras para um arquivo de texto ASCII:

   ```
   # /opt/oracle.cellos/host_access_control access-export --file filename
   ```

4. **Configure o conjunto de regras executando um ou mais destes comandos com base no método que você deseja usar para criar o conjunto de regras:**

- **Para implementar um conjunto de regras aberto que remova restrições de rede de entrada, digite:**

```
# /opt/oracle.cellos/host_access_control access --open
```

- **Para implementar um conjunto de regras fechado que só permita o acesso de entrada usando SSH, digite:**

```
# /opt/oracle.cellos/host_access_control access --close
```

- **Para modificar o conjunto de regras existente, digite:**

  Exporte o conjunto de regras atual para um arquivo de texto ASCII:

```
# /opt/oracle.cellos/host_access_control access-export --file filename
```

  Use um editor para editar o arquivo de texto para configurar o conjunto de regras.

  Importe o conjunto de regras para o arquivo de texto, substituindo o conjunto existente:

```
# /opt/oracle.cellos/host_access_control access-import --file filename
```

- **Para adicionar regras específicas individualmente:**

  Este método inclui permitir e negar acesso com base nestes parâmetros:

  - **Username** – os valores válidos incluem a palavra-chave `all` ou um ou mais nomes de usuário de contas locais válidas.
  - **Origem** – os valores válidos incluem a palavra-chave `all` ou entradas individuais que descrevam a origem do acesso do sistema incluindo console, console virtual, Oracle ILOM, endereço IP, endereço de rede, nome do host ou domínio DNS.

  Neste exemplo, o acesso ao servidor de armazenamento é concedido ao usuário `celladmin` quando a conexão é iniciada a partir do host `trusted.example.org` ou de qualquer host dentro do domínio `.trusted.domain.com`.

```
# /opt/oracle.cellos/host_access_control access --add --user celladmin \
--origins trustedhost.example.org,.trusted.domain.com
```

Recursos Adicionais do Servidor de Armazenamento

Consulte o Guia de Segurança da Máquina de Banco de Dados Exadata em http://docs.oracle.com/cd/E50790_01/welcome.html.

Protegendo as Chaves de IB e Ethernet

O Oracle Sun Data Center InfiniBand Switch 36 que é usado pelo SuperCluster fornece a base da rede para um painel traseiro de alto desempenho, altamente dimensionável e totalmente redundante em todos os componentes internos.

As chaves de IB se conectam aos servidores de computação, células de armazenamento e o appliance de armazenamento de ZFS. As chaves de IB compreendem um Oracle ILOM incorporado para fornecer recursos avançados de monitoramento e gerenciamento. Especificamente, o Oracle ILOM permite o monitoramento e controle de usuários, hardware, serviços, protocolos e outros parâmetros de configuração.

O SuperCluster M7 tem um mínimo de duas chaves de IB, com chaves de IB adicionais instaladas conforme necessário para configurações maiores. Você deve proteger cada chave de BI individual.

Estes tópicos descrevem como proteger as chaves de IB no SuperCluster M7:

▼ Fazer Login em uma Chave de IB

Esta tarefa descreve como fazer login na interface do Oracle ILOM na chave, na qual a maioria das tarefas administrativas é executada.

- **Na rede de gerenciamento, faça login no Oracle ILOM na chave de IB como `ilom-admin`.**

  Para senhas padrão, consulte "Contas e Senhas Padrão (Chave de IB)" [108].

```
% ssh ilom-admin@IB_Switch_ILOM_IPaddress
->
```

▼ Determinar a Versão de Firmware da Chave de IB

Para aproveitar os recursos, capacidades e aprimoramentos de segurança mais recentes, verifique se a chave de IB está atualizada com a versão mais recente e com suporte do firmware.

1. **Faça login em uma chave de IB como `ilom-admin`.**

   Consulte Fazer Login em uma Chave de IB [107].

2. **Exiba a versão do firmware.**

   Neste exemplo, o firmware da chave de IB é `2.1.5-1`.

```
-> version
SP firmware 2.1.5-1
SP firmware build number: 47111
SP firmware date: Sat Aug 24 16:59:14 IST 2013
SP filesystem version: 0.1.22
```

Para atualizar a versão do software, instale o SuperCluster Quarterly Full Stack Download Patch mais recente disponível no My Oracle Support em `https://support.oracle.com`.

Observação - Para o SuperCluster M7, restrições adicionais podem limitar as versões do software da chave de IB que podem ser usadas. As restrições também ditam como o firmware é atualizado. Nessas situações, entre em contato com o representante da Oracle.

Contas e Senhas Padrão (Chave de IB)

Nome da Conta	Tipo	Senha Padrão	Descrição
`root`	Administrador	`welcome1`	Usado para acessar o sistema operacional da chave de IB. Essa conta, geralmente, não é usada em favor de `ilom-admin`, `ilom-operator` nem contas definidas pelo cliente.

Nome da Conta	Tipo	Senha Padrão	Descrição
ilom-admin	Administrador	ilom-admin	Usado para executar funções administrativas no software Oracle ILOM incorporado, executar atualizações de software, configurar usuários e serviços e executar funções de gerenciamento de diagnóstico e fabric de chave de IB.
ilom-operator	Operador	ilom-operator	Usado apenas para funções de diagnóstico de fabric de IB e monitoramento do Oracle ILOM.
nm2user	Somente leitura	changeme	Essa conta tem privilégios somente leitura na interface administrativa da linha de comando da chave de IB. Essa conta, geralmente, é usada pelo Oracle Enterprise Manager para dar suporte ao monitoramento do hardware e do software da chave.

▼ Alterar Senhas root e nm2user

A chave de IB mantém contas do sistema em dois locais. As contas root e nm2user são configuradas e expostas pelo sistema operacional da chave. Adicionar, remover ou alterar as contas não têm suporte nessa camada, mas você deve alterar as senhas padrão.

Para outras contas e senhas, consulte Alterar Senhas de Chaves de IB (Oracle ILOM) [110].

A chave de IB não tem a capacidade de definir nem reforçar a complexidade, a validade, o histórico de senhas nem outras regras. É necessário garantir que as senhas atribuídas cumpram os requisitos de complexidade de senhas do Departamento de Defesa dos EUA e os processos sejam implementados para garantir que as senhas sejam atualizadas de acordo com a política do Departamento de Defesa dos EUA.

Para obter mais informações sobre gerenciamento de contas de chaves de IB, inclusive como criar novas contas, atribuir permissões às contas existentes ou remover contas, consulte o *Guia de Segurança do Hardware do Oracle Sun Data Center InfiniBand Switch 36* e o *Suplemento do Oracle Integrated Lights Out Manager para o Oracle Sun Data Center InfiniBand Switch 36*. Consulte "Recursos Adicionais da Chave de IB" [116].

Observação - Quando uma senha é alterada para qualquer componente do SuperCluster gerenciado pelo Oracle Engineered Systems Hardware Manager (como as chaves de IB), também é necessário atualizar a senha no Oracle Engineered Systems Hardware Manager. Para obter detalhes, consulte o *Guia de Administração do Oracle SuperCluster Série M7*.

---

1. Faça login na chave de IB como root.

```
# ssh root@IB_Switch_IP_address
```

Para senhas padrão, consulte "Contas e Senhas Padrão (Chave de IB)" [108].

2. **Altere a senha `root`.**

```
$ passwd root
```

3. **Altere a senha `nm2user`.**

```
$ passwd nm2user
```

▼ Alterar Senhas de Chaves de IB (Oracle ILOM)

A chave de IB mantém contas do sistema em dois locais. Esta seção descreve como alterar senhas na interface do Oracle ILOM da chave de IB. Para as outras contas e senhas, consulte Alterar Senhas `root` e `nm2user` [109].

As contas de chaves de IB padrão e todas as contas definidas pelo cliente são gerenciadas por meio do Oracle ILOM incorporado nas chaves de IB.

Para visualizar as contas e alterar as senhas, execute este procedimento.

1. **Faça login em uma chave de IB como `ilom-admin`.**

   Consulte Fazer Login em uma Chave de IB [107].

   Para senhas padrão, consulte “Contas e Senhas Padrão (Chave de IB)” [108].

2. **Visualize as contas configuradas do Oracle ILOM na chave de IB.**

```
-> show /SP/users
```

3. **Altere a senha da conta `ilom-admin`.**

```
-> set /SP/users/ilom-admin password=password
```

Isolamento da Rede de Chave de IB

A interface de gerenciamento da chave de IB é implantada em uma rede de gerenciamento isolada e dedicada. Isso protege a chave de IB contra tráfego de rede não autorizado ou não intencional.

O acesso a essa rede de gerenciamento deve ser estritamente controlado com acesso concedido apenas aos administradores que precisem desse nível de acesso.

Serviços de Rede Exposta Padrão (Chave de IB)

Nome do Serviço	Protocolo	Porta	Descrição
SSH	TCP	22	Usado pelo serviço Secure Shell integrado para permitir o acesso administrativo à chave de IB usando uma CLI.
HTTP (BUI)	TCP	80	Usado pelo serviço HTTP integrado para permitir o acesso administrativo à chave de IB usando uma interface de navegador. Embora a TCP/80 geralmente seja usada para acesso de texto não criptografado, por padrão, a chave de IB redireciona automaticamente as solicitações de entrada para a versão protegida desse serviço em execução na TCP/443.
NTP	UDP	123	Usado pelo serviço Network Time Protocol (NTP) integrado (somente cliente) usado para sincronizar o relógio do sistema local com uma ou mais fontes de tempo externas.
SNMP	UDP	161	Usado pelo serviço SNMP integrado a fim de fornecer uma interface de gerenciamento para monitorar a integridade da chave de IB e monitorar as notificações de interceptação recebidas.
HTTPS (BUI)	TCP	443	Usado pelo serviço HTTPS integrado para permitir o acesso administrativo à chave de IB por um canal (SSL/TLS) criptografado usando uma interface de navegador.
IPMI	TCP	623	Usado pelo serviço Intelligence Platform Management Interface (IPMI) integrado para fornecer uma interface de computador para várias funções de monitoramento e gerenciamento. Não desative esse serviço porque ele é usado pelo Oracle Enterprise Manager Ops Center para coletar dados de inventário de hardware, descrições de unidades substituíveis em campo, informações de sensor de hardware e informações de status de componentes de hardware.
ServiceTag	TCP	6481	Usado pelo serviço Oracle ServiceTag. Esse é um protocolo de descoberta da Oracle usado para identificar servidores e facilitar solicitações de serviço. Esse serviço é usado por produtos, como o Oracle Enterprise Manager Ops Center, para descobrir software de chave de IB e integrar com outras soluções de serviço automático da Oracle.

Protegendo a Configuração da Chave de IB

Estes tópicos descrevem como proteger a chave de IB por meio de várias configurações de segurança.

▼ Desativar Serviços Desnecessários (Chave de IB)

Desative todos os serviços que não sejam necessários para dar suporte aos requisitos operacionais e de gerenciamento da plataforma. Por padrão, a chave de IB emprega uma configuração de rede protegida por padrão pela qual serviços não essenciais já são desativados. No entanto, com base em requisitos e políticas de segurança do cliente, pode ser necessário desativar serviços adicionais.

1. **Faça login em uma chave de IB como `ilom-admin`.**

   Consulte Fazer Login em uma Chave de IB [107].

2. **Determine a lista de serviços compatíveis com a chave de IB.**

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

3. **Determine se um determinado serviço está ativado.**

   Substitua *servicename* pelo nome de um serviço de Passo 2.

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

   Embora a maioria dos serviços reconheça e use o parâmetro `servicestate` para registrar se o serviço está ativado ou desativado, há alguns serviços, como `servicetag`, `ssh`, `sso` e `wsman`, que usam um parâmetro denominado `state`. Independente do parâmetro real usado, um serviço estará ativado se o parâmetro de estado retornar um valor de `enabled`, conforme mostrado nestes exemplos:

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

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

4. **Para desativar um serviço que não seja mais necessário, defina seu estado como `disabled`.**

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

5. **Determine se algum destes serviços precisa ser desativado.**

   Dependendo das ferramentas e métodos usados, os serviços de navegador HTTP e HTTPS poderão ser desativados se não forem necessários ou não estiverem sendo usados. Tipo:

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

- Interface Administrativa do Navegador (HTTP, HTTPS):
  - -> **set /SP/services/http servicestate=disabled**
  - -> **set /SP/services/http secureredirect=disabled**
  - -> **set /SP/services/https servicestate=disabled**

▼ Configurar o Redirecionamento HTTP para HTTPS (Chave de IB)

Por padrão, a chave de IB é configurada para redirecionar solicitações HTTP de entrada para o serviço HTTPS para garantir que todas as comunicações baseadas em navegador sejam criptografadas entre a chave e o administrador.

1. **Faça login em uma chave de IB como `ilom-admin`.**

   Consulte Fazer Login em uma Chave de IB [107].

2. **Verifique se o redirecionamento seguro está ativado.**

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

3. **Se o padrão tiver sido alterado, você poderá ativar o redirecionamento seguro.**

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

▼ Desativar Protocolos SNMP Não Aprovados (Chave de IB)

Por padrão, SNMPv1, SNMPv2c e SNMPv3 são todos ativados para o serviço SNMP que é usado para monitorar e gerenciar a chave de IB. Garanta que as versões anteriores do protocolo SNMP permaneçam desativadas, a menos que seja necessário ativá-las.

Observação - A versão 3 do protocolo SNMP introduziu o suporte para o Modelo de Segurança Baseado em Usuário (USM). Essa funcionalidade substitui as strings de comunicação SNMP tradicionais pelas contas de usuário reais que podem ser configuradas com permissões específicas, protocolos de autenticação e privacidade e senhas. Por padrão, a chave de IB não inclui nenhuma conta USM. Configure contas SNMPv3 USM com base em seus próprios requisitos de implantação, gerenciamento e monitoramento.

1. **Faça login em uma chave de IB como `ilom-admin`.**

   Consulte Fazer Login em uma Chave de IB [107].

2. **Determine o status de cada protocolo SNMP.**

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

3. **Se necessário, desative SNMPv1 e SNMPv2c.**

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

▼ Configurar Strings de Comunidade SNMP (Chave de IB)

Essa tarefa só será aplicável se SNMP v1 ou SNMPv2c estiver ativado e configurado para uso.

Como o SNMP, geralmente, é usado para monitorar a integridade do dispositivo, é importante que as strings da comunidade SNMP padrão usadas pelo dispositivo sejam substituídas por valores definidos pelo cliente.

1. **Faça login em uma chave de IB como `ilom-admin`.**

   Consulte Fazer Login em uma Chave de IB [107].

2. **Crie uma nova string da comunidade SNMP.**

   Neste exemplo, substitua estes itens na linha de comando:

- *string* – Substitua por um valor definido pelo cliente que esteja em conformidade com os requisitos do Departamento de Defesa dos EUA relativos à composição de strings da comunidade SNMP.
- *access* – Substitua por `ro` ou `rw`, dependendo se é uma string de acesso somente leitura ou leitura e gravação.

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

Uma vez criadas as novas strings da comunidade, as strings padrão devem ser removidas.

3. **Remova as strings da comunidade SNMP padrão.**

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

4. **Verifique as strings de comunidade SNMP**

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

Substituir Certificados Autoassinados Padrão (Chave de IB)

As chaves de IB usam certificados autoassinados para permitir o uso predefinido do protocolo HTTPS. Como prática recomendada, substitua certificados autoassinados por certificados aprovados para uso em seu ambiente e assinados por uma autoridade certificadora reconhecida.

A chave de IB dá suporte a uma variedade de métodos que podem ser usados para acessar o certificado SSL/TLS e a chave privada incluindo HTTPS, HTTP, SCP, FTP, TFTP, e à cola das informações diretamente em uma interface de navegador Web. Para obter mais informações, consulte o *documento Suplemento do Oracle Integrated Lights Out Manager para o Oracle Sun Data Center InfiniBand Switch 36*. Consulte “Recursos Adicionais da Chave de IB” [116].

1. **Faça login em uma chave de IB como `ilom-admin`.**

   Consulte Fazer Login em uma Chave de IB [107].

2. **Determine se a chave de IB está usando um certificado autoassinado padrão.**

```
-> show /SP/services/https/ssl cert_status
/SP/services/https/ssl
Properties:
```

```
cert_status = Using Default (No custom certificate or private key loaded)
```

3. **Instale o certificado de sua organização.**

```
-> load -source URI /SP/services/https/ssl/custom_cert
-> load -source URI /SP/services/https/ssl/custom_key
```

Configurar o Tempo Limite da Sessão de CLI Administrativa (Chave de IB)

As chaves de IB dão suporte à capacidade de desconectar e fazer logoff de sessões de CLI administrativas que permanecerem inativas por mais do que um intervalo predefinido de minutos.

Por padrão, o tempo limite da CLI é de 15 minutos.

1. **Faça login em uma chave de IB como `ilom-admin`.**

   Consulte Fazer Login em uma Chave de IB [107].

2. **Verifique o parâmetro de tempo limite de inatividade associado à CLI.**

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

3. **Defina o parâmetro de tempo limite de inatividade.**

   Substitua *n* por um valor especificado em minutos.

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

Recursos Adicionais da Chave de IB

Para obter mais informações sobre procedimentos de segurança e administração de chaves de IB, consulte a biblioteca de documentação do Sun Datacenter InfiniBand Switch 36 em http://docs.oracle.com/cd/E36265_01.

Alterar a Senha da Chave de Ethernet

Observação - Quando uma senha é alterada para qualquer componente do SuperCluster gerenciado pelo Oracle Engineered Systems Hardware Manager (como a chave de Ethernet), também é necessário atualizar a senha no Oracle Engineered Systems Hardware Manager. Para obter detalhes, consulte o *Guia de Administração do Oracle SuperCluster Série M7*.

1. **Conecte um cabo serial do console da chave de Ethernet a um laptop ou dispositivo similar.**

   A velocidade padrão da porta serial é 9600 baud, 8 bits, sem paridade, 1 bit de parada e sem handshake.

```
sscsw-adm0 con0 is now available
Press RETURN to get started.
```

2. **Coloque a chave no modo de ativação.**

```
sscsw-adm0> enable
```

3. **Defina a senha.**

```
sscsw-adm0# configure terminal
Enter configuration commands,one per line.End with CNTL/Z.
sscsw-adm0(config)# enable password *******
sscsw-adm0(config)# enable secret *******
sscsw-adm0(config)# end
sscsw-adm0# write memory
*Apr 24 14:25:05.893:%SYS-5-CONFIG_I:Configured from console by
console
Building configuration...
Compressed configuration from 2502 bytes to 1085 bytes [OK ]
```

4. **Salve a configuração.**

```
sscsw-adm0# copy running-config startup-config
```

5. **Saia da sessão.**

```
sscsw-adm0# exit
```

6. **Desconecte o laptop da chave de Ethernet.**

Auditoria para Conformidade

Use o utilitário de conformidade do Oracle Solaris para avaliar e gerar relatório da conformidade de um sistema com um benchmark conhecido.

O comando `de conformidade` do Oracle Solaris mapeia os requisitos de um benchmark em relação ao código, arquivo ou saída de comando que verifica a conformidade com um requisito específico. O Oracle SuperCluster atualmente dá suporte a dois perfis de benchmark de conformidade de segurança:

- **Recomendado** – perfil baseado no benchmark Center of Internet Security.
- **PCI-DSS** – perfil que verifica os requisitos de conformidade Payment Card Industry Data Security Standard (PCI DSS).

Essa ferramentas de criação de perfil mapeiam os controles de segurança aos requisitos de conformidade, e os relatórios de conformidade resultantes podem reduzir o tempo de auditoria significativo. Além disso, um recurso de conformidade fornece guias que contêm a lógica para cada verificação de segurança e as etapas para corrigir uma verificação com falha. Os guias podem ser úteis para treinamento e como diretrizes para testes futuros. Por padrão, os guias para cada perfil de segurança são criados na instalação. O administrador do SuperCluster Solaris pode adicionar ou alterar um benchmark e criar um novo guia.

Estes tópicos descrevem como executar relatórios de conformidade e a conformidade com FIPS-140:

- Gerar uma Avaliação de Conformidade [119]
- (Opcional) Executar Relatórios de Conformidade com uma Tarefa `cron` [122]
- “Conformidade com FIPS-140-2 Nível 1” [122]

▼ Gerar uma Avaliação de Conformidade

Para executar esta tarefa, você deve receber o perfil de direitos Software Installation para adicionar pacotes ao sistema. Você deve receber direitos administrativos para a maioria dos comandos de conformidade.

1. **Instale o pacote de conformidade.**

```
# pkg install compliance
```

A seguinte mensagem indica que o pacote foi instalado:

```
No updates necessary for this image.
```

Para obter mais informações, consulte a página man `pkg(1)`.

Observação - Instale o pacote em todas as zonas onde você pretende executar testes de conformidade.

---

2. **Liste os benchmarks disponíveis, os perfis e todas as avaliações anteriores.**

Neste exemplo, há dois benchmarks.

- **`pci-dss`** – inclui um perfil denominado `Solaris_PCI-DSS`
- **`solaris`** – inclui dois perfis denominados `Baseliine` e `Recommended`

```
# compliance list -p
Benchmarks:
pci-dss: Solaris_PCI-DSS
solaris: Baseline, Recommended
Assessments:
No assessments available
```

3. **Gere uma avaliação de conformidade.**

Execute o comando `compliance` com esta sintaxe:

`avaliação de conformidade -b` *benchmark* `-p` *perfil*

`-b`	Especifica um benchmark específico. Se não estiver especificado, o padrão do valor será `solaris`.
`-p`	Especifica o perfil. O nome do perfil faz distinção de maiúsculas e minúsculas. Se não estiver especificado, o padrão do valor será o primeiro perfil.

Exemplos:

- Usando o perfil `Recommended`.

```
# compliance assess -b solaris -p Recommended
```

O comando cria um diretório em `/var/share/compliance/assessments` que contém a avaliação em três arquivos: um arquivo de log, um arquivo XML e um arquivo HTML.

- Usando o perfil PCI-DSS:

```
# compliance assess -b pci-dss
```

Observação - O benchmark `pci-dss` só tem um perfil, então, a opção de perfil (`-p`) não é necessária na linha de comando.

4. **Verifique se os arquivos de conformidade foram criados.**

```
# cd /var/share/compliance/assessments/filename_timestamp
# ls
recommended.html
recommended.txt
recommended.xml
```

Observação - Se você executar o mesmo comando `compliance` de novo, os arquivos não serão substituídos. Você deve remover os arquivos antes de reutilizar um diretório de avaliações.

5. **(Opcional) Crie um relatório personalizado.**

   É possível executar relatórios personalizados repetidamente. No entanto, você só pode executar a avaliação uma única vez no diretório original.

   Neste exemplo, a opção `-s` é usada para selecionar quais tipos de resultado devem aparecer no relatório.

   Por padrão, todos os tipos de resultado aparecem no relatório, exceto `notselected` ou `notapplicable`. Os tipos de resultado são especificados como uma lista separada por vírgula para exibição além do padrão. Os tipos de resultado individuais podem ser suprimidos precedendo-os com um `-`, enquanto começar a lista com `=` especifica exatamente quais tipos de resultado devem ser incluídos. Os tipos de resultado são: `pass`, `fixed`, `notchecked`, `notapplicable`, `notselected`, `informational`, `unknown`, `error` ou `fail`.

```
# compliance report -s -pass,fail,notselected
/var/share/compliance/assessments/filename_timestamp/report_A.html
```

   Esse comando cria um relatório que contém itens não selecionados ou com falha no formato HTML. O relatório é executado na avaliação mais recente.

6. **Visualize o relatório completo.**

   É possível visualizar o arquivo de log em um editor de texto, visualizar o arquivo HTML em um navegador ou o arquivo XML em um visualizador XML. Por exemplo, para visualizar o relatório HTML personalizado na etapa anterior, digite a seguinte entrada no navegador:

```
file:///var/share/compliance/assessments/filename_timestamp/report_A.html
```

7. **Corrija as falhas para que sua política de segurança possa avançar.**

   Se a correção incluir a reinicialização do sistema, reinicialize o sistema antes de executar a avaliação novamente.

8. **Repita a avaliação até não haver mais falhas.**

▼ (Opcional) Executar Relatórios de Conformidade com uma Tarefa `cron`

- **Como superusuário, utilize o comando `crontab -e` para adicionar a entrada apropriada ao arquivo `crontab`.**

  Essa lista fornece exemplos de entradas `crontab`:

  - Executa avaliações de conformidade diárias às 2h30.

    ```
    30 2 * * * /usr/bin/compliance assess -b solaris -p Baseline
    ```

  - Executa avaliações de conformidade semanais à 1h15 aos domingos

    ```
    15 1 * * 0 /usr/bin/compliance assess -b solaris -p Recommended
    ```

  - Executa avaliações mensais no primeiro dia do mês, às 4h,

    ```
    0 4 1 * * /usr/bin/compliance assess -b pci-dss
    ```

  - Executa avaliações na primeira segunda-feira do mês, às 3h45,

    ```
    45 3 1,2,3,4,5,6,7 * 1 /usr/bin/compliance assess
    ```

Conformidade com FIPS-140-2 Nível 1

Os aplicativos criptográficos hospedados no SuperCluster baseiam-se no recurso Cryptographic Framework do Oracle Solaris, que está validado em relação à conformidade com FIPS 140-2 Nível 1. O Oracle Solaris Cryptographic Framework é o armazenamento criptográfico central para o Oracle Solaris e fornece dois módulos validados pela FIPS 140 que dão suporte aos processos no nível do kernel e no espaço do usuário. Esses módulos de biblioteca fornecem funções de criptografia, descriptografia, hash, geração e verificação de assinaturas, geração e verificação de certificados e autenticação de mensagens para aplicativos. Os aplicativos no nível do usuário que chamam esses módulos são executados no modo FIPS 140.

Além do Oracle Solaris Cryptographic Framework, o módulo de objeto OpenSSL fornecido com o Oracle Solaris é validado em relação à conformidade com FIPS 140-2 Nível 1, que dá suporte à criptografia para aplicativos baseados nos protocolos Secure Shell e TLS. O fornecedor de serviço em nuvem pode optar por ativar os hosts tenant com modos em conformidade com FIPS 140. Quando executados em modos em conformidade com FIPS 140, o Oracle Solaris e o OpenSSL, que são provedores de FIPS 140-2, reforçam o uso de algoritmos criptográficos validados para FIPS 140.

Consulte também (Se necessário) Ativar a Operação em Conformidade com FIPS-140 (Oracle ILOM) [37].

Essa tabela lista algoritmos aprovados pela FIPS compatíveis com Oracle Solaris em SuperCluster M7.

Chave ou CSP	Número da Certidão	
	v1.0	**v1.1**
Chave Simétrica		
AES: modos ECB, CBC, CFB-128, CCM, GMAC, GCM e CTR para chaves de 128, 192 e 256 bits	#2311	#2574
AES: modo XTS para chaves de 256 e 512 bits	#2311	#2574
TripleDES: modo CBC e ECB para opção de criação de chaves 1	#1458	#1560
Chave Assimétrica		
Geração/verificação de assinatura RSA PKCS#1.5: 1024, 2048 bits (com SHA-1, SHA-256, SHA-384, SHA-512)	#1194	#1321
Geração/verificação de assinatura ECDSA: P-192, -224, -256, -384, -521; K-163, -233, -283, -409, -571; B-163, -233, -283, -409, -571	#376	#446
Padrão de Hash Seguro (SHS)		
SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	#1425	#1596
Autenticação de Mensagem Baseada em Hash (de Chave)		
HMAC SHA-1, HMAC SHA-224, HMAC SHA-256, HMAC SHA-384, HMAC SHA-512	#1425	#1596
Geradores de Números Aleatórios		
Gerador de Números Aleatórios swrand FIPS 186-2	#1154	#1222
Gerador de Números Aleatórios n2rng FIPS 186-2	#1152	#1226

O Oracle Solaris oferece dois provedores de algoritmos criptográficos que são validados para FIPS 140-2 Nível 1.

- O recurso Cryptographic Framework do Oracle Solaris é o armazenamento criptográfico central em um sistema Oracle Solaris e fornece dois módulos FIPS 140. O módulo userland fornece criptografia para aplicativos que são executados no espaço do usuário, e o módulo kernel fornece criptografia para processos no nível do kernel. Esses módulos de biblioteca fornecem funções de criptografia, descriptografia, hash, geração e verificação de assinaturas, geração e verificação de certificados e autenticação de mensagens para aplicativos. Os aplicativos de nível de usuário que são chamados nesses módulos são executados no modo FIPS 140, por exemplo, o comando `passwd` e IKEv2. Consumidores do nível do kernel, por exemplo, Kerberos e IPsec, usam APIs proprietárias para chamar o kernel Cryptographic Framework.
- O módulo de objeto OpenSSL fornece criptografia para aplicativos Web e SSH. O OpenSSL é o kit de ferramentas de código aberto para os protocolos Secure Sockets Layer (SSL) e Transport Layer Security (TLS) e fornece uma biblioteca de criptografia. No Oracle Solaris, SSH e o Apache Web Server são consumidores do módulo OpenSSL FIPS 140. O Oracle Solaris é fornecido com uma versão FIPS 140 do OpenSSL com Oracle Solaris 11.2 que está disponível para todos os consumidores, mas a versão fornecida com o Oracle Solaris

11.1 está disponível apenas para Solaris SSH. Como os módulos do provedor de FIPS 140-2 usam muitos recursos da CPU, eles não são ativados por padrão. Como administrador, você é responsável por ativar os provedores no modo FIPS 140 e configurar os consumidores.

Para obter mais informações sobre ativação dos provedores de FIPS-140 no Oracle Solaris, consulte o documento intitulado *Usando um Sistema Ativado para FIPS 140 no Oracle Solaris 11.2*, disponível abaixo do título Protegendo o Sistema Operacional Oracle Solaris 11 em: `http://docs.oracle.com/cd/E36784_01`.

Mantendo os Sistemas SuperCluster M7 Seguros

Estes tópicos descrevem os recursos do SuperCluster série M7 que você pode usar para manter a segurança durante toda a vida útil do sistema:

Gerenciando a Segurança do SuperCluster

O SuperCluster M7 aproveita os recursos de gerenciamento de uma variedade de produtos, entre eles, Oracle ILOM, Oracle Enterprise Manager Ops Center, Oracle Enterprise Manager e Identity Management Suite da Oracle. Estas seções descrevem os detalhes:

Oracle ILOM para Gerenciamento Seguro

Oracle ILOM é um processador de serviço incorporado em muitos componentes do SuperCluster M7. Use o Oracle ILOM para executar estas atividade de gerenciamento fora de banda:

- Fornecer acesso seguro para executar gerenciamento integral seguro dos componentes do SuperCluster. O acesso inclui acesso baseado na Web protegido por SSL, acesso à linha de comandos usando o Secure Shell e protocolos IPMI v2.0 e SNMPv3.
- Separar requisitos operacionais usando um modelo RBAC. Atribuir usuários individuais a funções específicas que limitem as funções que eles podem executar.
- Fornecer um registro de auditoria de todos os logons e alterações de configuração. Cada entrada do log de auditoria lista o usuário que está executando a ação e um registro de data e hora. Esse recurso permite detectar uma atividade ou alterações não autorizadas e reatribui essas ações a usuários específicos.

Para obter mais informações, consulte a documentação do Oracle Integrated Lights Out Manager em: http://docs.oracle.com/en/hardware/?tab=4

Oracle Identity Management Suite

O Oracle Identity Management Suite gerencia o ciclo de vida integral das entidades e contas dos usuários em uma organização. A suíte inclui suporte para single sign-on, controle de acesso baseado na Web, segurança de serviços Web, administração de identidade, autenticação forte e governança de identidade e acesso.

O Oracle Identity Management pode fornecer um único ponto para gerenciamento de identidade e acesso não apenas para aplicativos e exercícios executados no Oracle SuperCluster, mas também para a infraestrutura subjacente e serviços que a gerenciam.

Para obter mais informações, consulte a documentação do Oracle Identity Management em:

http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html

Oracle Key Manager

O Oracle Key Manager é um sistema de gerenciamento de chaves completo (KMS) que simplifica o gerenciamento e o monitoramento das chaves de criptografia que protegem informações em repouso.

O Oracle Key Manager dá suporte para ambientes de nível empresarial com uma arquitetura altamente dimensionável e disponível que pode gerenciar milhares e dispositivos e milhões de chaves. Esse recurso funciona em um ambiente operacional protegido, reforça o controle de acesso e a separação de funções para operações de gerenciamento e monitoramento de chaves

e, opcionalmente, dá suporte ao armazenamento seguro de chaves na placa PCIe Sun Crypto Accelerator 6000 da Oracle, um módulo de segurança de hardware com classificação 140-2 FIPS.

No contexto do SuperCluster, o Oracle Key Manager pode autorizar, proteger e gerenciar o acesso a chaves de criptografia usadas por unidades de fita de criptografia Oracle StorageTek, bancos de dados Oracle criptografados com criptografia de dados transparente e sistemas de arquivos ZFS criptografados disponíveis no sistema operacional Oracle Solaris 11.

Para obter mais informações, consulte a documentação do Oracle Key Manager em:

http://docs.oracle.com/cd/E26076_02

Oracle Engineered Systems Hardware Manager

O Oracle Engineered Systems Hardware Manager é uma ferramenta de gerenciamento de hardware de nível de rack baseado em BUI a ser usada por pessoal do Oracle Service. Para obter detalhes, consulte o *Guia do Proprietário do Oracle SuperCluster Série M7: Administração*.

O Oracle Engineered Systems Hardware Manager inclui dois conjuntos de informações de autenticação:

- **Senhas dos componentes do SuperCluster M7**

  O Oracle Engineered Systems Hardware Manager mantém um armazenamento seguro de senhas para todas as contas de fábrica de todo o hardware do SuperCluster M7. O software usa essas senhas para gerenciar os componentes do SuperCluster M7.

  Quando uma dessas senhas for alterada, você deverá atualizar o aplicativo Oracle Engineered Systems Hardware Manager com as novas senhas.
- **Autenticação Local**

  O Oracle Engineered Systems Hardware Manager tem duas contas de usuário locais. Uma conta é usada por clientes para ajustar o Oracle Engineered Systems Hardware Manager para que seu ambiente gerencie a conta de serviço. A outra conta é usada pelo pessoal do Oracle Service para configurar, dar suporte e fazer manutenção do hardware do SuperCluster M7.

O Oracle Engineered Systems Hardware Manager fornece os recursos de gerenciamento locais a seguir.

- **Política de Senhas** – A capacidade de configurar as senhas do aplicativo de acordo com as suas políticas corporativas garante que as senhas sigam seus padrões corporativos.

Observação - Consulte o funcionário de Segurança Corporativa para obter as senhas da política de senhas.

- **Certificados** – O Oracle Engineered Systems Hardware Manager usa certificados para proteger a comunicação entre os servidores de computação e o servidor do Oracle Engineered Systems Hardware Manager e o BUI. Esses certificados são criados automaticamente durante a instalação e são exclusivos para cada instância do SuperCluster, no entanto, eles podem ser substituídos por chaves e certificados fornecidos pelo cliente.
- **Portas** – As portas de sistema de rede usadas pelo Oracle Engineered Systems Hardware Manager podem ser configuradas caso haja conflitos com a sua política corporativa. As portas 8001 a 8004 são usadas.

Para obter instruções sobre configuração, consulte o *Guia do Proprietário do Oracle SuperCluster Série M7: Administração*.

Oracle Enterprise Manager

A suíte do Oracle Enterprise Manager é uma solução de gerenciamento em nuvem completa e integrada que se concentra no gerenciamento do ciclo de vida de aplicativos, middleware, bancos de dados e infraestrutura física e virtual (usando o Oracle Enterprise Manager Ops Center). O Oracle Enterprise Manager fornece estas tecnologias de gerenciamento:

- Dá suporte ao monitoramento detalhado, notificação de eventos, aplicação de patches, gerenciamento de alterações, configuração contínua, gerenciamento de conformidade e geração de relatórios para o aplicativo, middleware e banco de dados.
- Permite manter, de modo seguro e central, as configuração de segurança, bem como as políticas de controle e auditoria de grupos de bancos de dados. O acesso a essas funções pode ser limitado a indivíduos autorizados garantindo que o acesso de gerenciamento dê suporte para requisitos de conformidade para separação de obrigações, privilégios mínimos e responsabilidade.
- Dá suporte à autenticação forte usando uma variedade de métodos, controles de acesso refinado e auditoria completa garantindo que o gerenciamento do ambiente do SuperCluster possa ser realizado de forma segura.

Para obter mais informações, consulte a documentação do Oracle Enterprise Manager em: `http://www.oracle.com/technetwork/oem/grid-control/documentation/oem-091904.html`

Oracle Enterprise Manager Ops Center (Opcional)

O Oracle Enterprise Manager Ops Center é uma tecnologia opcional que você pode usar para gerenciar alguns aspectos de segurança do Oracle SuperCluster.

Parte da suíte do Oracle Enterprise Manager, o Oracle Enterprise Manager Ops Center é uma solução de gerenciamento de hardware convergido que fornece uma única interface de gerenciamento para servidores, sistemas operacionais, firmware, máquinas virtuais, zonas e fabrics de rede.

Você pode usar o Oracle Enterprise Manager Ops Center para atribuir acesso administrativo a coleções de sistemas físicos e virtuais, monitorar a atividade do administrador, detectar falhas, bem como configurar e gerenciar alertas. O Oracle Enterprise Manager Ops Center dá suporte a uma variedade de relatórios que permitem comparar sistemas com linhas de base de configuração, níveis de patch e vulnerabilidades de segurança conhecidos.

Para obter mais informações, consulte a documentação do Oracle Enterprise Manager em: `http://docs.oracle.com/cd/E27363_01/index.htm`

Observação - Para versões anteriores do Oracle Enterprise Manager Ops Center, o software Ops Center foi instalado e executado no sistema do SuperCluster. A partir do Oracle Enterprise Manager Ops Center 12c Release 2 (12.2.0.0.0), o software Ops Center deve ser instalado e executado em um sistema fora do SuperCluster.

Monitorando a Segurança

Seja para geração de relatórios de conformidade ou resposta a incidentes, monitoramento e auditoria são funções essenciais que você deve usar para obter maior visibilidade no ambiente de TI. O grau em que o monitoramento e a auditoria são empregados, em geral, baseia-se no risco ou na natureza crítica do ambiente.

Os sistemas SuperCluster série M7 fornecem recursos completos de monitoramento e auditoria nas camadas de servidor, rede e banco de dados garantindo que as informações possam ser disponibilizadas em apoio aos requisitos de auditoria e conformidade.

Estas seções descrevem o monitoramento e a auditoria de carga de trabalho e banco de dados:

- “Monitoramento de Carga de Trabalho” [130]
- “Monitoramento e Auditoria da Atividade do Banco de Dados” [130]

Monitoramento de Carga de Trabalho

O sistema operacional Oracle Solaris tem um recurso de auditoria abrangente que pode monitorar ações administrativas, invocações de linha de comando e mesmo chamadas do sistema no nível do kernel individual. Esse recurso é altamente configurável e oferece políticas de auditoria por zona e até mesmo por usuário.

Quando o sistema está configurado para usar o Oracle Solaris Zones, os registros de auditoria para cada zona podem ser armazenados na zona global para protegê-los contra manipulação.

A auditoria do Oracle Solaris oferece a capacidade de enviar registros de auditoria para pontos de coleta remotos usando o recurso de log do sistema (`syslog`). Muitos serviços de prevenção e detecção de invasões podem usar os registros de auditoria do Oracle Solaris como uma entrada adicional para análise e geração de relatórios.

O Oracle VM Server for SPARC aproveita o recurso nativo de auditoria do Oracle Solaris para registrar ações e eventos associados a eventos de virtualização e administração de domínios.

Para obter mais informações, consulte a seção Monitorando e Mantendo a Segurança do Oracle Solaris nas Diretrizes de Segurança do Oracle Solaris em:

`http://docs.oracle.com/cd/E26502_01`

Monitoramento e Auditoria da Atividade do Banco de Dados

O suporte da auditoria refinada do Oracle Database permite estabelecer políticas que determinam de forma seletiva quando são gerados relatórios de auditoria. Esse recurso ajuda você a se concentrar em outras atividades do banco de dados e reduz a carga que, geralmente, está associada a atividades de auditoria.

O Oracle Audit Vault and Database Firewall centraliza o gerenciamento das configurações de auditoria do banco de dados e automatiza a consolidação dos dados de auditoria em um repositório seguro. Este software inclui a geração de relatórios incorporada para monitorar uma grande variedade de atividades incluindo atividade de usuários privilegiados e alterações em estruturas de banco de dados. Os relatórios gerados pelo Oracle Audit Vault and Database Firewall proporcionam visibilidade de várias atividades de aplicativos e banco de dados

administrativo e fornecem informações detalhadas para dar suporte à responsabilidade das ações.

O Oracle Audit Vault and Database Firewall permite a detecção proativa e o alerta de atividades que podem indicar tentativas de acesso não autorizado ou abuso de privilégios do sistema. Esses alertas podem incluir eventos e condições do sistema e definidos pelo usuário, como a criação de contas de usuários privilegiados ou a modificação de tabelas que contêm informações confidenciais.

O Oracle Audit Vault and Database Firewall Remote Monitor pode fornecer monitoramento de segurança do banco de dados em tempo real. Esse recurso consulta as conexões de banco de dados para detectar tráfego mal-intencionado, como desvio de aplicativos, atividade não autorizada, injeção de SQL e outras ameaças. Usando uma abordagem SQL precisa, baseada em gramática, este software ajuda você a rapidamente identificar atividade suspeita no banco de dados.

Para obter mais informações, consulte a documentação do Oracle Audit Vault and Database Firewall em: http://docs.oracle.com/cd/E37100_01/index.htm

Monitoramento de Rede

Depois que as redes são configuradas com base nos princípios de segurança, são necessárias revisões e manutenções regulares.

Siga estas diretrizes para garantir a segurança do acesso local e remoto ao seu sistema:

- Verifique possíveis incidentes nos logs e arquive-os de acordo com a política de segurança de sua organização.
- Realize análises periódicas da rede de acesso ao cliente para garantir que as configurações do host e do Oracle ILOM permaneçam intactas.

Para obter mais informações, consulte os guias de segurança do Oracle Solaris OS:

- Oracle Solaris 11 OS – http://www.oracle.com/goto/Solaris11/docs
- Oracle Solaris 10 OS – http://www.oracle.com/goto/Solaris10/docs

Atualização do Software e do Firmware

Atualizações do sistema do SuperCluster série M7 são fornecidas no QFSDP. A instalação do QFSDP atualiza todos os componentes simultaneamente. Essa prática garante que todos os

componentes continuem em execução em uma combinação de versões de software que foram totalmente testadas juntas pela Oracle.

Obtenha o QFSDP mais recente do My Oracle Support em: `http://support.oracle.com`

Para obter detalhes sobre o software e firmware compatíveis, consulte as *Notas do Produto do Oracle SuperCluster M7 Series*. Instruções para acessar as Notas do Produto estão disponíveis no MOS nota 1605591.1.

Observação - Somente atualize ou aplique patches a componentes individuais isoladamente para manutenção reativa de acordo com a orientação do suporte da Oracle.

Índice

C

D

E

F

G

R

S