

Guia de Segurança do MiniCluster S7-2

ORACLE

Número do Item: E78274-02
Outubro de 2016

Número do Item: E78274-02

Copyright © 2016, Oracle e/ou suas empresas afiliadas. Todos os direitos reservados e de titularidade da Oracle Corporation. Proibida a reprodução total ou parcial.

Este programa de computador e sua documentação são fornecidos sob um contrato de licença que contém restrições sobre seu uso e divulgação, sendo também protegidos pela legislação de propriedade intelectual. Exceto em situações expressamente permitidas no contrato de licença ou por lei, não é permitido usar, reproduzir, traduzir, divulgar, modificar, licenciar, transmitir, distribuir, expor, executar, publicar ou exibir qualquer parte deste programa de computador e de sua documentação, de qualquer forma ou através de qualquer meio. Não é permitida a engenharia reversa, a desmontagem ou a descompilação deste programa de computador, exceto se exigido por lei para obter interoperabilidade.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. A Oracle Corporation não garante que tais informações estejam isentas de erros. Se você encontrar algum erro, por favor, nos envie uma descrição de tal problema por escrito.

Se este programa de computador, ou sua documentação, for entregue / distribuído(a) ao Governo dos Estados Unidos ou a qualquer outra parte que licencie os Programas em nome daquele Governo, a seguinte nota será aplicável:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este programa de computador foi desenvolvido para uso em diversas aplicações de gerenciamento de informações. Ele não foi desenvolvido nem projetado para uso em aplicações inerentemente perigosas, incluindo aquelas que possam criar risco de lesões físicas. Se utilizar este programa em aplicações perigosas, você será responsável por tomar todas e quaisquer medidas apropriadas em termos de segurança, backup e redundância para garantir o uso seguro de tais programas de computador. A Oracle Corporation e suas afiliadas se isentam de qualquer responsabilidade por quaisquer danos causados pela utilização deste programa de computador em aplicações perigosas.

Oracle e Java são marcas comerciais registradas da Oracle Corporation e/ou de suas empresas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários.

Intel e Intel Xeon são marcas comerciais ou marcas comerciais registradas da Intel Corporation. Todas as marcas comerciais SPARC são usadas sob licença e são marcas comerciais ou marcas comerciais registradas da SPARC International, Inc. AMD, Opteron, o logotipo da AMD e o logotipo do AMD Opteron são marcas comerciais ou marcas comerciais registradas da Advanced Micro Devices. UNIX é uma marca comercial registrada licenciada por meio do consórcio The Open Group.

Este programa ou equipamento e sua documentação podem oferecer acesso ou informações relativas a conteúdos, produtos e serviços de terceiros. A Oracle Corporation e suas empresas afiliadas não fornecem quaisquer garantias relacionadas a conteúdos, produtos e serviços de terceiros e estão isentas de quaisquer responsabilidades associadas a eles, a menos que isso tenha sido estabelecido entre você e a Oracle em um contrato vigente. A Oracle Corporation e suas empresas afiliadas não são responsáveis por quaisquer tipos de perdas, despesas ou danos incorridos em consequência do acesso ou da utilização de conteúdos, produtos ou serviços de terceiros, a menos que isso tenha sido estabelecido entre você e a Oracle em um contrato vigente.

Acessibilidade da Documentação

Para obter informações sobre o compromisso da Oracle com a acessibilidade, visite o Web site do Programa de Acessibilidade da Oracle em <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Acesso ao Oracle Support

Os clientes da Oracle que adquiriram serviços de suporte têm acesso a suporte eletrônico por meio do My Oracle Support. Para obter informações, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> caso tenha deficiência de audição.

Conteúdo

Usando Esta Documentação	7
Biblioteca de Documentação do Produto	7
Feedback	7
Noções Básicas dos Princípios de Segurança	9
Tarefas de Segurança Mínimas Necessárias	9
Princípios Básicos de Segurança	10
Máquinas Virtuais Seguras	11
Controle de Acesso	12
Proteção de Dados	13
Auditoria e Conformidade	14
Noções Básicas da Configuração de Segurança	17
Perfis de Segurança Incorporados	17
▼ Verificar o Perfil de Segurança de VM (CLI)	18
Protegendo os Dados	21
Proteção de Dados com a Criptografia de Conjuntos de Dados ZFS	21
▼ Exibir Chaves de Criptografia de Conjunto de Dados ZFS (BUI)	21
Serviço Secure Shell	22
▼ Alterar Chaves SSH (BUI)	22
Proteger a Comunicação com IPsec	24
▼ Configurar IPsec e IKE	25
Controlando o Acesso	27
▼ Alterar as Senhas root Padrão do Oracle ILOM	27
▼ Configurar Senhas do EEPROM	28
Provisionamento do Usuário	29
Processo de Aprovação de Usuários do MCMU	29
Controle de Acesso Baseado em Atribuição	30

Contas de Usuário	31
Políticas de Senha e Autenticação do Usuário	32
▼ Verificar as Atribuições dos Usuários do Oracle Solaris	33
Proteger contra Exclusão de VMs	33
▼ Verificar as Regras do Firewall Baseado em Host	33
▼ Verificar o Ambiente de Inicialização Verificada	35
▼ Restringir o Acesso ao Armazenamento Compartilhado	36
Relatórios de Auditoria e Conformidade	39
▼ Verificar as Políticas de Auditoria	39
▼ Revisar Logs de Auditoria	40
▼ Gerar Relatórios de Auditoria	41
▼ (Se Necessário) Ativar a Operação em Conformidade com o FIPS-140 (Oracle ILOM)	43
Conformidade com o FIPS-140-2 Nível 1	44
Avaliando a Conformidade com Segurança	47
Benchmarks de Conformidade com Segurança	47
▼ Programar um Benchmark de Conformidade com Segurança (BUI)	48
▼ Exibir Relatórios de Benchmark (BUI)	49
Noções Básicas dos Controles de Segurança do Servidor SPARC S7-2	53
Noções Básicas de Segurança de Hardware	53
Restrições de Acesso	53
Números de Série	54
Unidades de Disco Rígido	54
Restringindo o Acesso ao OpenBoot	55
▼ Acessar o Prompt do OpenBoot	55
▼ Verificar Falhas de Log-in	56
▼ Fornecer um Power-On Banner	56
Índice Remissivo	57

Usando Esta Documentação

- **Visão geral** - fornece informações sobre planejamento, configuração e manutenção de um ambiente seguro para sistemas do Oracle MiniCluster S7-2.
- **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/miniclusters7-2/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 do Oracle MiniCluster S7-2.

Os tópicos a seguir são tratados nesta seção:

- [“Tarefas de Segurança Mínimas Necessárias” \[9\]](#)
- [“Princípios Básicos de Segurança” \[10\]](#)
- [“Máquinas Virtuais Seguras” \[11\]](#)
- [“Controle de Acesso” \[12\]](#)
- [“Proteção de Dados” \[13\]](#)
- [“Auditoria e Conformidade” \[14\]](#)

Tarefas de Segurança Mínimas Necessárias

Como sistema integrado, o MiniCluster é configurado como um sistema altamente seguro de fábrica por padrão, fornecendo estas funcionalidades de segurança:

- Pré-configurado com controles de segurança totalmente automatizados para todas as máquinas virtuais (VMs).
- A criptografia é ativada por padrão, garantindo dados seguros em repouso e em trânsito.
- As VMs são configuradas automaticamente com um sistema operacional reforçado e minimizado com firewalls baseados em host.
- O controle de acesso requer acesso baseado em atribuição com o mínimo de privilégios.
- Todas as VMs usam armazenamento ZFS criptografado.
- Há um recurso de gerenciamento de chaves centralizado, que usa PKCS#11, e suporte para FIPS.
- O sistema inclui uma política de auditoria abrangente com logs de auditoria centralizados.
- O sistema e todas as VMs são configurados para um perfil de segurança PCI-DSS, CIS Equivalent ou DISA-STIG. Observação – O último perfil está em análise no momento. Só utilize o perfil DISA-STIG para uso experimental em ambientes que não são de produção.

- Há um painel de conformidade fácil de visualizar que dá suporte a benchmarks de conformidade fáceis de executar.

Logo após a instalação do MiniCluster, há duas tarefas necessárias para o administrador de segurança:

- Alterar a senha root do Oracle ILOM. Consulte [Alterar as Senhas root Padrão do Oracle ILOM \[27\]](#)

Além disso, ler as informações sobre segurança neste guia para entender e verificar as funcionalidades de segurança do MiniCluster.

Princípios Básicos de Segurança

O MiniCluster é uma plataforma de infraestrutura de nuvem segura para consolidação de aplicativos e bancos de dados e é adequada para fornecer serviços de computação dedicados em nuvem baseados em IaaS (infrastructure as a Service, Infraestrutura como um Serviço). Projetado como um sistema para vários fins, ele combina o poder de computação do processador SPARC S7 da Oracle, os recursos eficientes de virtualização do SPARC Solaris e o desempenho otimizado do banco de dados Oracle integrado com armazenamento dedicado. Além disso, é implantada uma rede 10 GbE que permite aos clientes acessar serviços em execução no MiniCluster. Por fim, outra rede 10 GbE fornece a via pela qual ocorre toda a intercomunicação entre o ambiente de máquina virtual nos servidores SPARC S7 e os aplicativos hospedados.

O processador SPARC S7 apresenta uma funcionalidade criptográfica assistida por hardware always-on que ajuda as entidades hospedadas pelo MiniCluster a proteger suas informações com proteção de dados de alto desempenho - em repouso, em uso e em trânsito. O processador também apresenta a funcionalidade Silicon Secured Memory, que detecta e impede ataques relacionados a corrompimentos de dados da memória e "scraping" de memória garantindo, desse modo, a integridade dos dados dos aplicativos.

Por padrão, o MiniCluster é pré-configurado com mais do que 250 controles de segurança predefinidos que reduzem a superfície de ataque do sistema desativando serviços, portas e protocolos que não sejam absolutamente necessários e configurando os serviços expostos para aceitar apenas conexões confiáveis.

O sistema dá suporte a uma variedade de opções de configuração e implantação. Esta figura ilustra uma implantação típica que consolida o as cargas de trabalho do Oracle Database e dos aplicativos.

de segurança que define um conjunto abrangente de controles e políticas de segurança que são automaticamente aplicados durante o processo de instalação. O uso de pools ZFS e conjuntos de dados permite distribuição e isolamento adicionais do armazenamento em unidades mais granulares para máquinas virtuais e é possível ter suas próprias políticas de segurança.

Controle de Acesso

Para proteger os dados dos aplicativos, as cargas de trabalho e a infraestrutura subjacente na qual eles são executados, o MiniCluster oferece recursos de controle de acesso abrangentes, mas flexíveis, para usuários e administradores. O MiniCluster usa o Oracle Solaris para uma variedade de métodos de controle de acesso para usuários e aplicativos que acessam serviços do sistema. Embora pares tradicionais de nome de usuário e senha ainda sejam amplamente utilizados, métodos mais fortes de autenticação podem ser facilmente integrados usando a arquitetura PAM (Pluggable Authentication Modules, Módulos de autenticação plugáveis) do Oracle Solaris que permite o uso de LDAP, Kerberos e autenticação de chave pública. O ambiente de computação do MiniCluster é baseado em um recurso RBAC (Role-Based Access Control, Controle de acesso baseado em atribuição) que proporciona às organizações a flexibilidade de delegar acesso de usuário e administrativo de acordo com a necessidade. Eliminando a noção de um superusuário todo poderoso, o recurso RBAC do Oracle Solaris permite a separação de deveres e dá suporte à noção de atribuições administrativas, autorizações, privilégios refinados e perfis de direitos que coletivamente são usados para atribuir direitos a usuários e administradores. O RBAC é integrado com serviços básicos do Oracle Solaris incluindo o Oracle Solaris SMF (Service Management Facility) e as máquinas virtuais, para fornecer uma arquitetura consistente e dar suporte a todas as necessidades de controle de acesso no nível do sistema operacional. O MiniCluster utiliza o recurso RBAC do Oracle Solaris como base para sua arquitetura de controle de acesso permitindo às organizações gerenciar, controlar e auditar o acesso de gerenciamento de virtualização e sistema operacional de uma autoridade centralizada. Todas as operações críticas são executadas usando o princípio de separação de deveres embasado por um fluxo de trabalho de autorização de várias pessoas. O sistema exige que duas ou mais pessoas aprovelem cada operação sensível em termos de segurança. Coletivamente, esses recursos podem ser usados para fornecer um alto grau de garantia para a identidade dos usuários e seu processamento de operações de negócios críticas.

Todos os dispositivos no sistema do MiniCluster incluem a capacidade de limitar o acesso da rede a serviços usando métodos de arquitetura (por exemplo, isolamento da rede) ou usando filtragem de pacotes e/ou listas de controle de acesso para limitar a comunicação entre dispositivos físicos e virtuais, bem como os serviços expostos pelo sistema. O MiniCluster implanta uma postura segura por padrão pela qual nenhum serviço de rede, exceto o Secure Shell (SSH), está ativado para acessar o tráfego de rede de entrada. Outros serviços de rede ativados captam internamente solicitações no sistema operacional Oracle Solaris (máquina virtual ou zona). Isso garante que todos os serviços de rede sejam desativados por padrão ou sejam definidos para captar somente as comunicações do sistema local. As organizações têm a liberdade de personalizar essa configuração com base em seus requisitos. O MiniCluster é pré-

configurado com uma filtragem de pacotes de camada de transporte e rede (com estado) usando a funcionalidade Filtro de IP do Oracle Solaris. O Filtro de IP oferece uma grande variedade de recursos de rede baseados em host incluindo filtragem de pacotes com estado, conversão de endereços de rede e de endereços de porta.

Proteção de Dados

O processador SPARC S7 no MiniCluster 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", corrupção silenciosa da memória, estouro de buffer e ataques relacionados.

O processador SPARC ativa 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 sistema operacional Oracle Solaris e o processador SPARC usados pelo MiniCluster. 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 a funcionalidade Silicon Secured Memory para garantir a proteção da memória e a integridade dos dados dos aplicativos sem precisar de configuração do usuário final. O MiniCluster dá suporte ao uso de IPSec (IP Security), e o IKE (Internet Key Exchange) é recomendado para proteger a confiabilidade e a integridade das comunicações inter-VM e específica de VMs que fluem pelas redes pública e privada.

No MiniCluster, a criptografia de conjuntos de dados ZFS utiliza um keystore Oracle Solares PKCS#11 centralizado para proteger com segurança as chaves de encapsulamento. Ao usar o keystore Oracle Solaris PKCS#11, a aceleração criptográfica assistida por hardware SPARC é ativada automaticamente para todas as operações de criptografia de chave mestra. Isso permite à Oracle melhorar significativamente o desempenho das operações de criptografia e descriptografia associadas à criptografia de conjuntos de dados ZFS, Oracle Database TDE (Transparent Data Encryption, Criptografia de dados transparentes), criptografia de espaço de tabela, backups de bancos de dados criptografados (usando o Oracle Recovery Manager [Oracle RMAN]), exportações de banco de dados criptografados (usando a funcionalidade Data Pump do Oracle Database) e redo logs (usando o Oracle Active Data Guard). As máquinas virtuais do banco de dados podem usar uma abordagem de wallet compartilhada utilizando o keystore Oracle Solaris PKCS#11 ou criar um diretório no armazenamento de compartilhamento

ACFS de forma que a wallet possa ser compartilhada entre os bancos de dados que residem nas máquinas virtuais. O uso de um keystore centralizado e compartilhado em cada nó de computação permite ao sistema gerenciar, manter e rotear melhor as chaves do Oracle TDE em infraestruturas de banco de dados em cluster baseadas na infraestrutura Oracle Grid, porque as chaves são sincronizadas em cada nó do cluster. O MiniCluster também apresenta a exclusão segura de máquinas virtuais e conjuntos de dados ZFS associados fazendo com que a política de criptografia e o gerenciamento de chaves no nível desse conjunto de dados ZFS (sistema de arquivos/ZVOL) forneçam exclusão garantida por meio da destruição de chaves.

Auditoria e Conformidade

O MiniCluster baseia-se no uso do subsistema de auditoria do Oracle Solaris para coletar, armazenar e processar informações de eventos de auditoria. Cada máquina virtual (zona não global) gera registros de auditoria que são armazenados localmente em cada armazenamento de auditoria (zona global) do MiniCluster. Essa abordagem garante que as máquinas virtuais individuais não possam alterar suas políticas de auditoria, configurações nem 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 nas máquinas virtuais. Esse recurso é altamente configurável e oferece políticas de auditoria por zona e até mesmo por usuário. Quando configurados para usar máquina virtual, os registros de auditoria de cada máquina virtual podem ser armazenados na zona global para protegê-las contra adulteração. A zona global também aproveita o recurso nativo de auditoria do Oracle Solaris para registrar ações e eventos associados a eventos de virtualização e administração do MiniCluster.

O MiniCluster fornece ferramentas que avaliam e relatam a conformidade do ambiente de tempo de execução do Oracle Solaris que reside nas máquinas virtuais. Os utilitários de conformidade se baseiam na implementação do SCAP (Security Content Automation Protocol). O MiniCluster dá suporte a dois perfis de benchmark de conformidade de segurança:

- **Perfil de Segurança Padrão** – Um perfil CIS Equivalent (baseado no benchmark Centro de Segurança de Internet) que está mais alinhado com os requisitos de conformidade de segurança estabelecidos por regulamentos como HIPAA, FISMA, SOX, etc.
- **Perfil PCI-DSS** – o Padrão de Segurança de Dados do Setor de Cartão de Pagamento
- **Perfil DISA STIG** – O Defense Information System Agency - Security Technical Implementation Guidance Standard (padrão de orientação para implementação técnica de segurança da Agência de Sistemas de Informação de Defesa). Este perfil se baseia no Perfil de Segurança Padrão e acrescenta 75 controles de segurança, criptografia FIPS-140-2 e suporte para definição de senha do S. *Observação:* – Este perfil está em análise no momento. Só utilize este perfil para uso experimental em ambientes que não são de produção.

O administrador do MiniCluster pode executar o benchmark de conformidade sob demanda e verificar o ambiente para conformidade e anomalias. Essas ferramentas de criação de perfis mapeiam os controles de segurança aos requisitos de conformidade exigidos pelos padrões do setor. Os relatórios de conformidade associados podem reduzir o tempo e os custos significativos de auditoria.

A partir do MiniCluster v.1.1.18, o sistema inclui estes recursos de auditoria:

- **Função de Auditor** – Quando esta função é especificada para um usuário e o usuário pode acessar a página de análise do auditor na BUI do MCMU. O usuário não pode visualizar ou executar outras tarefas administrativas do MiniCluster.
- **Página de análise do auditor** – É uma página especial da BUI do MCMU que somente usuários com a função de auditor podem visualizar. A página fornece acesso ao status do pool de auditoria e permite gerar registros de auditoria para todas as atividades de usuário, por zona. Consulte [Gerar Relatórios de Auditoria \[41\]](#).

Noções Básicas da Configuração de Segurança

Estes tópicos descrevem os controles de segurança do MiniCluster:

- [“Perfis de Segurança Incorporados” \[17\]](#)
- [Verificar o Perfil de Segurança de VM \(CLI\) \[18\]](#)

Perfis de Segurança Incorporados

A inicialização do MiniCluster é realizada usando a BUI do MCMU ou o CLI. Durante a inicialização, o MCMU requer que o instalador escolha um destes perfis de segurança:

- **Perfil de Segurança Padrão** – cumpre os requisitos comparáveis e equivalentes aos benchmarks estabelecidos pelas avaliações do Center for Internet Security (CIS) e das Security Technical Implementation Guidelines (STIG).
- **Perfil PCI-DSS** – cumpre o Payment Card Industry Data Security Standard (PCI DSS) definido pelo Payment Card Industry Security Standards Council.
- **Perfil DISA STIG** – O Defense Information System Agency - Security Technical Implementation Guidance Standard (padrão de orientação para implementação técnica de segurança da Agência de Sistemas de Informação de Defesa). Este perfil se baseia no Perfil de Segurança Padrão e acrescenta 75 controles de segurança, criptografia FIPS-140-2 e suporte para definição de senha do eeprom. *Observação:* – Este perfil está em análise no momento. Só utilize este perfil para uso experimental em ambientes que não são de produção.

Com base na política selecionada, o MCMU configura a zona global e as zonas não globais com mais do que 250 controles de segurança.

Após a inicialização, como as máquinas virtuais são criadas, o MCMU exige a seleção de um dos perfis de segurança para cada máquina virtual. Com base em seus requisitos de segurança, você pode ter uma mistura de perfis de segurança nas máquinas virtuais.

▼ Verificar o Perfil de Segurança de VM (CLI)

Use este procedimento para verificar ou identificar o perfil de segurança que está configurado para as zonas e as máquinas virtuais.

Observação - Para executar este procedimento, é necessário acessar o sistema com uma conta de usuário que tenha a atribuição `root`.

Observação - Para identificar o perfil de segurança atribuído à zona global, na BUI do MCMU, exiba Configuração do Sistema -> Resumo da Entrada do Usuário. O perfil de segurança é exibido na parte inferior da página.

1. Efetue log-in na zona global como `mcinstall`.

Para obter detalhes sobre como acessar o sistema, consulte o *Oracle MiniCluster S7-2 Administration Guide*.

2. Assuma a atribuição `root`.

Exemplo:

```
# su root
```

3. Determine o nome do arquivo de log para a VM em questão.

Neste exemplo, há um arquivo de log para cada VM:

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

4. Exiba os arquivos de log de verificação.

Exiba as últimas linhas do arquivo de log: Se (PCI-DSS) for exibido, o perfil de segurança da VM será PCI-DSS. Se nenhum perfil for listado, o perfil de segurança do VM será CIS Equivalent.

- Exemplo das últimas 22 linhas de uma VM com um perfil PCI-DSS:

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

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

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

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

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

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

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

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

■ Exemplo das últimas 22 linhas de uma VM com um perfil CIS Equivalent:

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

```
Checking if NDP routing daemon is disabled:  
Passed/Configured
```

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

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

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

```
Checking if GDM is enabled:  
Failed/Not Configured
```

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

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


Protegendo os Dados

Estes tópicos descrevem as tecnologias de proteção de dados do MiniCluster:

- [“Proteção de Dados com a Criptografia de Conjuntos de Dados ZFS” \[21\]](#)
- [Exibir Chaves de Criptografia de Conjunto de Dados ZFS \(BUI\) \[21\]](#)
- [“Serviço Secure Shell” \[22\]](#)
- [Alterar Chaves SSH \(BUI\) \[22\]](#)
- [“Proteger a Comunicação com IPsec” \[24\]](#)
- [Configurar IPsec e IKE \[25\]](#)

Proteção de Dados com a Criptografia de Conjuntos de Dados ZFS

No MiniCluster, a proteção de dados em repouso é automaticamente configurada usando a criptografia de conjuntos de dados ZFS. A criptografia é configurada da seguinte forma:

- Todos os conjuntos de dados ZFS são criptografados em máquinas virtuais que incluem os sistemas de arquivos swap e root.
- Todos os conjuntos de dados ZFS são criptografados na zona global, com exceção dos sistemas de arquivos swap e root.

Você pode verificar a configuração de criptografia exibindo as chaves de criptografia. Consulte [Exibir Chaves de Criptografia de Conjunto de Dados ZFS \(BUI\) \[21\]](#).

▼ Exibir Chaves de Criptografia de Conjunto de Dados ZFS (BUI)

Use este procedimento para exibir detalhes de chaves de criptografia.

1. **Acesse a BUI do MCMU.**

Para obter detalhes sobre como acessar a BUI do MCMU, consulte o *Oracle MiniCluster S7-2 Administration Guide*.

2. **No painel de navegação, selecione Configurações do Sistema -> Segurança.**
Clique em um nó para exibir os detalhes.

Encryption Key Information
Encryption keys for all virtual machines and attached volumes

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

Serviço Secure Shell

O MiniCluster requer o uso do protocolo de rede SSH para permitir a você efetuar log-in de forma segura nos nós de computação do MiniCluster (zonas globais) e nas instâncias de máquina virtual (zonas não globais).

Quando um usuário efetua log-in pela primeira vez usando SSH, o sistema gera automaticamente um novo par de chaves SSH para o usuário.

▼ Alterar Chaves SSH (BUI)

Use este procedimento para alterar as chaves SSH para uma zona ou uma VM com uma destas configurações:

- Insira uma nova chave para autorizar SSH sem senha – exige que você informe o nome de usuário e o nome da máquina da VM, bem como a chave pública RSA.
- Gerar automaticamente novas chaves para VMs

Observação - Para executar este procedimento usando o MCMU CLI, consulte o *Oracle MiniCluster S7-2 Administration Guide*.

1. **Acesse a BUI do MCMU.**
2. **No painel de navegação, selecione Configurações do Sistema -> Segurança.**

The screenshot displays the MCMU BUI interface for managing encryption keys. It is divided into two main sections: "Encryption Key Information" and "Modify SSH Keys".

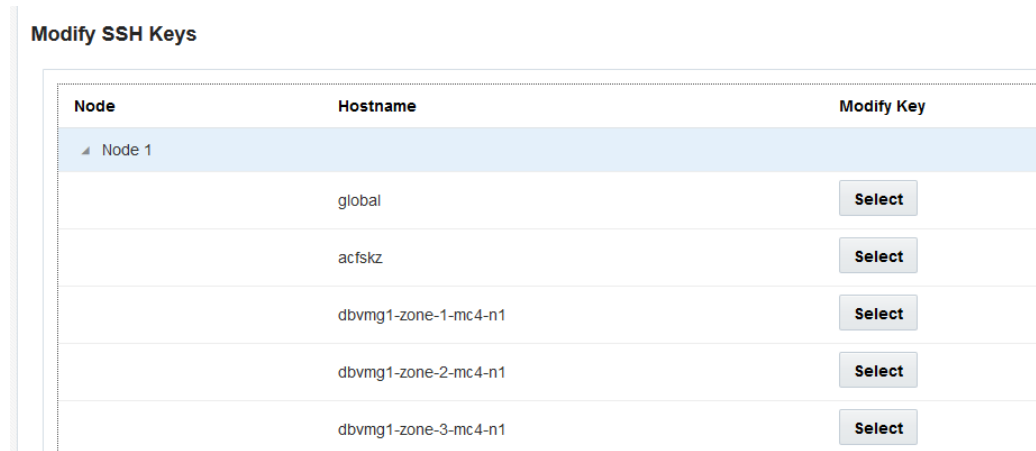
Encryption Key Information
Encryption keys for all virtual machines and attached volumes

Node	VM Name	ZFS Pool	Key Label	Encryption Key	Encryption Status	Key Source	Creation Date
▶ Node 1							
▶ Node 2							

Modify SSH Keys

Node	Hostname	Modify Key
▶ Node 1		
▶ Node 2		

3. No painel **Modificar Chaves SSH**, clique em um nó para expandir a exibição.



Node	Hostname	Modify Key
Node 1		
	global	Select
	acfskz	Select
	dbvmg1-zone-1-mc4-n1	Select
	dbvmg1-zone-2-mc4-n1	Select
	dbvmg1-zone-3-mc4-n1	Select

4. Para a VM que você planeja alterar, clique em **Selecionar**.
5. **Selecione uma opção no menu drop-down e clique em Avançar.**
Estas são as opções:
 - Inserir Nova Chave para Autorizar SSH sem Senha
 - Gerar Automaticamente Novas Chaves para Máquinas
6. **Clique em Avançar.**
7. **Se você selecionou autorizar SSH sem senha, forneça estas informações e clique em Avançar.**
 - Nome de usuário da máquina
 - Nome de host da máquina
 - Chave pública RSA da máquina
8. **Clique em Configurar SSH.**
A alteração é aplicada.

Proteger a Comunicação com IPsec

O uso de IPsec (IP Security) e IKE (Internet Key Exchange) é recomendado para proteger a confidencialidade e a integridade das comunicações baseadas em IP inter-zona e do tráfego

NFS que flui pela rede. O IPsec é recomendado porque ele dá suporte a autenticação de pares no nível da rede, autenticação da origem de dados, confidencialidade e integridade dos dados e proteção contra reprodução. Quando usados na plataforma Oracle MiniCluster, IPsec e IKE podem aproveitar automaticamente a aceleração de criptografia assistida por hardware minimizando, dessa forma, o impacto no desempenho usando criptografia para proteger informações confidenciais que fluem por esse canal de rede.

▼ Configurar IPsec e IKE

Para ser possível configurar o IPsec, os nomes de host específicos e/ou endereços IP usados entre pares de comunicação devem ser definidos.

Para o exemplo neste procedimento, os endereços IP 10.1.1.1 e 10.1.1.2 são usados para designar duas zonas não globais Solaris operadas por um único tenant. A comunicação entre esses dois endereços será protegida pelo IPsec. O exemplo é da perspectiva de uma zona não global associada ao endereço IP 10.1.1.1.

Use as seguintes etapas para configurar e usar IPsec e IKE entre um par de zonas não globais designadas (máquinas virtuais):

1. Defina a política de segurança IPsec.

Defina a política de segurança que será aplicada entre o par de zonas em comunicação.

Neste exemplo, todas as comunicações entre 10.1.1.1 e 10.1.1.2 serão criptografadas:

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

2. Armazene a política no arquivo `/etc/inet/ipsecinit.conf`.

3. Verifique se a política IPsec está sintaticamente correta.

Exemplo:

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

4. Configure o serviço IKE (Internet Key Exchange).

Configure o serviço seguindo as configurações de host e algoritmos no arquivo `/etc/inet/ike/config`.

```
{ label "ipsec"
local_id_type ip
remote_addr 10.1.1.2
p1_xform { auth_method preshared oakley_group 5
auth_alg sha256 encr_alg aes } }
```

5. Configure a chave pré-compartilhada.

Para ser possível configurar o IPsec, é necessário compartilhar o material de chaves com os dois nós pares para que eles possam ser autenticados entre si.

A implementação do Oracle Solaris IKE dá suporte a uma variedade de tipos de chave que incluem chaves pré-compartilhadas e certificados. Para simplificar, este exemplo usa chaves pré-compartilhadas que são armazenadas no arquivo `/etc/inet/secret/ike.preshared`. No entanto, as organizações que buscam usar formas mais fortes de autenticação pode seguir esse procedimento.

Edite o arquivo `/etc/inet/secret/ike.preshared` e forneça as informações de chave pré-compartilhada. Por exemplo:

```
{
localidtype IP
localid 10.1.1.1
remoteid type IP
key "This is an ASCII phrAz, use str0ng p@sswords"
}
```

6. Ative os serviços IPsec e IKE nos dois pares.

Os serviços devem ser ativados nos pares de comunicação para que a comunicação criptografada seja possível.

Exemplo:

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

Controlando o Acesso

Estes tópicos abrangem as funcionalidades de controle de acesso disponíveis no MiniCluster:

- [Alterar as Senhas root Padrão do Oracle ILOM \[27\]](#)
- [Configurar Senhas do EEPROM \[28\]](#)
- [“Provisionamento do Usuário” \[29\]](#)
- [“Processo de Aprovação de Usuários do MCMU” \[29\]](#)
- [“Controle de Acesso Baseado em Atribuição ” \[30\]](#)
- [“Contas de Usuário” \[31\]](#)
- [“Políticas de Senha e Autenticação do Usuário” \[32\]](#)
- [Verificar as Atribuições dos Usuários do Oracle Solaris \[33\]](#)
- [“Proteger contra Exclusão de VMs” \[33\]](#)
- [Verificar as Regras do Firewall Baseado em Host \[33\]](#)
- [Verificar o Ambiente de Inicialização Verificada \[35\]](#)
- [Restringir o Acesso ao Armazenamento Compartilhado \[36\]](#)

▼ Alterar as Senhas root Padrão do Oracle ILOM

O sistema é fornecido com senhas padrão atribuídas às contas root do Oracle ILOM nos dois nós. Isso permite que o processo de instalação seja executado com uma conta de acesso inicial previsível. Logo após a instalação, altere as senhas padrão para garantir a segurança ideal.

1. Efetue log-in no Oracle ILOM no nó 1 como root.

Use o comando `ssh` para se conectar ao Oracle ILOM.

Para obter os nomes de host do Oracle ILOM, na BUI do utilitário, selecione Configurações do Sistema -> Informações do Sistema. Os nomes de host são indicados na coluna ILOM.

Sintaxe:

```
% ssh root@node1_ILOM_hostname_or_IPaddress
```

Informe a senha root padrão do Oracle ILOM: `welcome1`

2. Altere a senha root do Oracle ILOM.

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

Enter new password again: *****

3. **Repita as etapas para alterar a senha root do Oracle ILOM no nó 2.**
4. **Atualize o Oracle Engineered Systems Hardware Manager com as novas senhas.**
Consulte [“Update Component Passwords” in Oracle MiniCluster S7-2 Administration Guide.](#)

▼ Configurar Senhas do EEPROM

Cada nó de MiniCluster tem um EEPROM (às vezes chamado de PROM do OpenBoot), que é o firmware de baixo nível que contém alguns drivers e parâmetros de configuração capazes de facilitar a inicialização do sistema. Por padrão, o recurso de senha do EEPROM está desativado.

Em ambientes seguros, use este procedimento para ativar o recurso de senha e definir uma senha. A senha é ativada automaticamente e aplicada a ambos os nós.

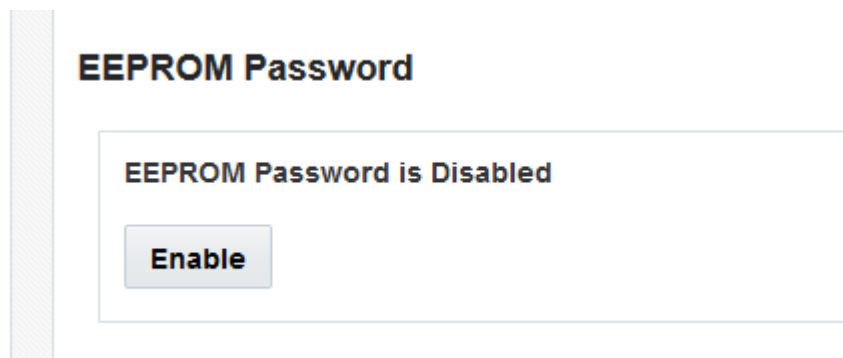
Este procedimento substitui métodos mais antigos em que a senha é definida no prompt `ok` do OpenBoot ou no Oracle Solaris com o comando `eprom`.



Cuidado - É importante lembrar a senha. Se você esquecê-la, precisará pedir ao serviço de suporte para tornar o sistema inicializável novamente.

Observação - Este procedimento descreve como definir as senhas usando a BUI do MCMU. Outra opção é usar o comando `mcmu security -e`.

1. **Efetue log-in no MCMU como um administrador primário (`mcinstall`, por exemplo).**
2. **No painel de navegação, selecione Configurações do Sistema -> Segurança.**



3. **Execute uma destas ações:**

- Para ativar e definir a senha – Clique em Ativar, digite a senha duas vezes e clique em Definir Senha.
- Para desativar o recurso – Clique em Desativar e depois em Confirmar.
- Para alterar uma senha existente – Altere a senha, digite a nova senha duas vezes e clique em Atualizar.

Provisionamento do Usuário

Durante a instalação do MiniCluster, o processo solicita criar e registrar o primeiro usuário do MCMU denominado `mcinstall`. As informações demográficas do usuário, incluindo o endereço de e-mail e o telefone, são coletadas. O usuário `mcinstall` é a conta do primeiro administrador principal. No primeiro log-in do `mcinstall`, o utilitário solicita que o `mcinstall` crie uma nova senha de acordo com as políticas de senha do Oracle Solaris associadas ao perfil de segurança.

Durante o registro do usuário `mcinstall`, é solicitado que você especifique uma pessoa para atuar como o supervisor do MCMU. O supervisor só será identificado por um nome e um endereço de e-mail. O supervisor não é um usuário do MCMU e não tem credenciais de log-in.

O supervisor e os usuários `mcinstall` estão associados a nomes de pessoas reais e endereços de e-mail válidos.

Quando novos usuários do MCMU são provisionados, é aplicada a cada conta de usuário uma atribuição de administrador principal ou secundário (consulte “[Controle de Acesso Baseado em Atribuição](#)” [30]). Antes de a nova conta ser ativada, o usuário `mcinstall` e o supervisor devem aprovar a nova conta de usuário por meio de uma URL que eles recebem por e-mail (consulte “[Processo de Aprovação de Usuários do MCMU](#)” [29]). No primeiro log-in, o usuário é forçado a definir uma senha em conformidade com as políticas de senha do MCMU. Consulte “[Políticas de Senha e Autenticação do Usuário](#)” [32].

Processo de Aprovação de Usuários do MCMU

Todas as contas de usuários do MCMU requerem a aprovação de duas pessoas, ou seja, do supervisor e do administrador principal do MCMU. O processo funciona da seguinte forma:

1. O provável usuário (ou um administrador do MCMU em seu nome) acessa a página de registro do MCMU e fornece estes detalhes obrigatórios:
 - Nome do usuário do MCMU
 - Endereço de e-mail
 - Nome completo

- Telefone
 - Atribuição do MCMU
2. O MCMU envia ao supervisor e ao administrador principal do MCMU um e-mail solicitando aprovação ou recusa. O e-mail inclui um URL para a funcionalidade de aprovação/recusa do MCMU e um identificador de chave exclusivo.
 3. Quando o supervisor e o administrador principal aprovam a conta, ela é ativada, e o MCMU envia ao novo usuário um e-mail confirmando a ativação da conta. O usuário recebe uma conta do MCMU que pode ser acessada por meio da BUI do MCMU ou do CLI. O usuário também recebe uma conta de usuário do Oracle Solaris. Se o usuário existir em um LDAP corporativo, e o MiniCluster estiver configurado com um cliente LDAP, o usuário só poderá usar o LDAP para a conta do Oracle Solaris.

Todos os usuários registrados são armazenados no repositório do MCMU. Um administrador do MCMU pode verificar os usuários, incluindo suas atribuições e o supervisor visualizando Configurações do Sistema do MCMU -> Contas de Usuários. Exemplo:

User Accounts

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

os tópicos subsequentes nesta seção descrevem como executar estas tarefas.

Controle de Acesso Baseado em Atribuição

Não há usuário `root` no MiniCluster. Em vez disso, `root` é uma atribuição destinada aos usuários do MCMU que são registrados como administradores principais.

Ao criar um usuário do MCMU, você designa para ele uma destas atribuições:

- **Administrador principal (atribuição `root`)** – a atribuição `root` define os direitos e os privilégios dos administradores principais do sistema do MiniCluster incluindo todos os seus nós de computação, redes, banco de dados e armazenamento. Os usuários com a atribuição `root` podem executar toda a instalação e todas as operações administrativas

críticas sem restrições. Como administradores principais, eles podem delegar operações e aprovar a inclusão e a exclusão de usuários, inclusive de novos administradores principais e secundários. O usuário precisa efetuar log-in com suas próprias credenciais. Todas as ações e as operações executadas são registradas e auditadas com base no identificador do usuário, não da atribuição.

- **Administrador secundário (atribuição `mcadmin`)** – esta atribuição define os direitos e os privilégios dos administradores secundários dos domínios e das zonas não globais do MiniCluster. Por padrão, esta função permite apenas um acesso somente para leitura ao MCMU. Todas as ações e as operações executadas são registradas e auditadas com base no identificador do usuário, não da atribuição.
- **Administrador tenant (atribuição `tadmin`)** – esta atribuição define os direitos e os privilégios do administrador de uma VM do MiniCluster. A atribuição define os direitos e os privilégios de um administrador de VM envolvido com operações administrativas diárias que dão suporte a instalações e implantação de aplicativos. Todas as ações são auditadas com base no identificador do usuário, não da atribuição.
- **Auditor (função `auditor`)** – Somente usuários com esta função têm acesso à página de análise de auditoria da BUI do MCMU, na qual é possível ver o status do pool de auditoria e gerar relatórios de atividade de usuários. Somente usuários com esta função podem acessar a página de análise de auditoria. Auditores não podem acessar o MCMU (exceto a página de auditoria), nem efetuar log-in em VMs ou zonas do kernel.

Contas de Usuário

O MiniCluster inclui as contas de usuários indicadas nesta tabela.

Usuário	Senha	Atribuição	Descrição
<code>mcinstall</code>	A senha é configurada durante a instalação. É possível redefini-la e alterá-la por meio do MCMU.	<code>root</code>	<p>O processo de instalação exige que você crie <code>mcinstall</code> como administrador primário do MCMU e crie uma senha. Esta conta deve ser o administrador primário do MCMU.</p> <p>Essa conta de usuário é usada para estas atividades:</p> <ul style="list-style-type: none"> ■ Executando a inicialização do sistema no momento da instalação executando <code>installmc</code>. ■ Administrando o sistema, incluindo VMs que utilizam a BUI do MCMU e a CLI <code>mcmu</code>. ■ Para assumir a atribuição <code>root</code> (<code>su</code> para <code>root</code>) nas VMs dos aplicativos, na zona global e nas zonas de kernel para privilégios de superusuário.
<i>Supervisor do MCMU</i> – nome de conta determinado na instalação	Não Aplicável	Não Aplicável	<p>No software MiniCluster, o usuário supervisor é apenas um nome de usuário e um endereço de e-mail. Não é uma credencial de log-in. Você pode usar essa conta para fornecer um segundo nível no processo de aprovação de usuários do MCMU.</p> <p>Esse usuário recebe um e-mail toda vez que um novo usuário do MCMU é criado. O novo usuário deve ser aprovado pelo supervisor e pelo administrador principal para a conta do usuário ser ativada.</p>

Usuário	Senha	Atribuição	Descrição
			Você pode usar essa conta para fornecer uma segunda camada no processo de aprovação de usuários do MCMU. Para isso, defina como supervisor uma pessoa que não seja o administrador principal.
(Opcional) <i>Administrador tenant</i> – Nome de conta determinado no registro do usuário	Determinado no log-in inicial.	tadmin	Este usuário pode executar todas as atividades pós-instalação apenas em VMs. Este usuário não pode acessar as zonas globais ou do kernel e não pode executar a CLI ou a BUI do MCMU.
(Opcional) <i>Administrador secundário</i> – nome da conta determinado no registro do usuário	Determinado no log-in inicial.	mcadmin	Quando um usuário do MCMU é criado e atribuído como administrador secundário e tem acesso somente para leitura a zonas não globais.
oracle	A senha é a mesma que mcinstall.	root	Essa conta de usuário é usada para estas atividades: <ul style="list-style-type: none"> ■ Usada como a conta de log-in inicial nas VMs de bancos de dados, na qual você pode configurar as VMs dos bancos de dados com um banco de dados, dados e outras contas, conforme necessário. ■ Para assumir a atribuição root (su para root) em VMs de banco de dados para privilégios de superusuário.

A senha padrão do MCMU usada no primeiro log-in é `welcome1`. Uma vez fornecida a senha `welcome1`, o utilitário força o usuário a criar uma nova senha que siga as políticas. Consulte [“Políticas de Senha e Autenticação do Usuário” \[32\]](#).

Todas as ações executadas por todos os usuários do MCMU são registradas com base no identificador do usuário. Para obter informações sobre relatórios de auditoria, consulte [Relatórios de Auditoria e Conformidade \[39\]](#).

Observação - As contas dos usuários do MCMU não são usadas nas atividades rotineiras do sistema, como uso dos aplicativos e dos bancos de dados. Essas contas de usuários são gerenciadas por meio do Oracle Solaris, do aplicativo, do banco de dados nas VMs e por meio dos serviços de nome do seu local.

Políticas de Senha e Autenticação do Usuário

Todos os usuários provisionados no MiniCluster recebem uma atribuição com políticas de senha rigorosas e uma criptografia de senhas que é reforçada pelo perfil de segurança.

A política de segurança padrão estabelece estes requisitos de senha do MCMU:

- Deve conter no mínimo 14 caracteres

- Deve ter no mínimo um caractere numérico
- Deve ter no mínimo um caractere alfabético maiúsculo
- Deve ser diferente da senha anterior em pelo menos 3 caracteres
- Não deve coincidir com as 10 senhas anteriores

Todos os usuários efetuam log-in em sua conta do Oracle Solaris usando apenas a própria senha.

▼ Verificar as Atribuições dos Usuários do Oracle Solaris

1. **Efetue log-in na zona global do MiniCluster e assuma a atribuição root.**
Para obter mais detalhes, consulte o *Oracle MiniCluster S7-2 Administration Guide*.

2. **Verifique a lista de atribuições disponíveis.**

```
# logins -r
```

3. **Verifique a atribuição e a senha do usuário necessários para autenticação:**

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

Proteger contra Exclusão de VMs

Somente o administrador principal do MCMU pode excluir VMs e grupos de VMs. Quando um componente de VM é excluído, as chaves correspondentes são excluídas automaticamente, e um e-mail é enviado ao administrador principal.

Para verificar essa funcionalidade, antes de excluir um componente de VM, faça log-in na BUI do MCMU como o administrador principal e exiba as chaves de criptografia (Definições do Sistema -> Segurança). Exclua o componente de VM e exiba as chaves novamente. A VM e o rótulo de chave associada do componente excluído não são mais exibidos.

▼ Verificar as Regras do Firewall Baseado em Host

Todos os ambientes de computação, inclusive as zonas globais, zonas de kernel e zonas não globais, são configurados automaticamente com firewalls IPFilter. Nenhum manual é necessário.

Para verificar os IPFilters em uso, execute estas etapas.

1. Efetue log-in na zona global no nó 1 como mcinstall e assumo a atribuição root.

Para obter instruções sobre como efetuar log-in no Oracle ILOM, consulte o *Oracle MiniCluster S7-2 Administration Guide*.

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

2. Verifique a configuração de IPFilter.

Garanta que as regras no arquivo /etc/ipf/ipf.conf correspondam à seguinte saída de tela.

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

3. Verifique se os serviços IPF estão on-line.

```
# svcs | grep svc:/network/ipfilter:default
online          22:13:55 svc:/network/ipfilter:default
# ipfstat -v
bad packets:           in 0    out 0
  IPv6 packets:       in 0 out 0
  input packets:      blocked 2767 passed 884831 nomatch 884798 counted 0 short 0
output packets:       blocked 0 passed 596143 nomatch 595516 counted 0 short 0
  input packets logged: blocked 0 passed 0
output packets logged: blocked 0 passed 0
  packets logged:     input 0 output 0
  log failures:       input 0 output 0
fragment state(in):   kept 0  lost 0  not fragmented 0
fragment reassembly(in): bad v6 hdr 0    bad v6 ehdr 0  failed reassembly 0
fragment state(out):  kept 0  lost 0  not fragmented 0
packet state(in):     kept 0  lost 0
```

```

packet state(out):      kept 0  lost 0
ICMP replies: 0        TCP RSTs sent: 0
Invalid source(in):    0
Result cache hits(in): 0        (out): 0
IN Pullups succeeded: 0        failed: 3462
OUT Pullups succeeded: 0        failed: 0
Fastroute successes: 0        failures: 0
TCP cksum fails(in): 0        (out): 0
IPF Ticks: 92894
Packet log flags set: (0)
                    none

```

4. **Garanta que seus bancos de dados e aplicativos estejam acessíveis sem alterar as regras de firewall.**

▼ Verificar o Ambiente de Inicialização Verificada

O Oracle Solaris Verified Boot é uma funcionalidade de integridade anti-malware que reduz o risco de entrada de componentes críticos de inicialização e kernel mal-intencionados ou modificados acidentalmente. Essa funcionalidade verifica as assinaturas de criptografia assinadas de fábrica do firmware, do sistema de inicialização e do kernel.

Por padrão, as zonas globais do MiniCluster são configuradas com o Oracle Solaris Verified Boot. Se quiser verificar se o sistema está configurado com inicialização verificada, execute estas etapas.

1. **Efetue log-in no Oracle ILOM em um dos nós.**

Para obter instruções sobre como efetuar log-in no Oracle ILOM, consulte o *Oracle MiniCluster S7-2 Administration Guide*.

2. **Verifique a configuração de inicialização verificada no Oracle ILOM.**

Garanta que a `boot_policy` esteja definida como `warning`.

```

-> show /HOST/verified_boot

/HOST/verified_boot
Targets:
  system_certs
  user_certs

Properties:
  boot_policy = warning

Commands:
  cd
  show

```

3. **Verifique a configuração de política verificada.**

Garanta que a `module_policy` esteja definida como `enforce`.

```

-> show /HOST/verified_boot module_policy

```

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

4. Inicie o console de host para acessar a zona global.

Efetue log-in como mcinstall.

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

Serial console started. To stop, type #.

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

5. Verifique a zona global em busca de evidências de que o sistema foi inicializado em uma configuração de inicialização verificada.

Verifique no arquivo messages a string NOTICE: Verified boot enabled; policy=warning.

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

▼ Restringir o Acesso ao Armazenamento Compartilhado

O MiniCluster inclui um array de armazenamento com uma combinação de SSDs e HDS. Os HDDs podem ser configurados para fornecer armazenamento compartilhado às VMs.

O MiniCluster inclui um recurso de isolamento de armazenamento compartilhado – Um switch de alternância que facilita o isolamento de armazenamento compartilhado aplicado apenas a zonas globais e do kernel. Isso ajuda a isolar um ambiente de grupo de VMs habilitado para conformidade e segurança em relação ao compartilhamento de arquivos com as zonas globais e do kernel. Isso garante que os grupos de VM não estão mais associados a montagens de NFS e que os serviços NFS estão desativados.

Para ambientes altamente seguros, não ative o armazenamento compartilhado para VMs de banco de dados e de aplicativos. Se o armazenamento compartilhado for ativado, o sistema de arquivos deverá estar acessível para as VMs como somente leitura. Para obter instruções sobre como ativar ou desativar o armazenamento compartilhado, consulte o *Oracle MiniCluster S7-2 Administration Guide*, disponível em: http://docs.oracle.com/cd/E69469_01.

O diretório /sharedstore é o ponto de montagem para o armazenamento compartilhado:

- **Com base em suas necessidades de segurança, configure o armazenamento compartilhado com estas recomendações em mente:**

- Garanta que o armazenamento compartilhado não esteja disponível para VMs de banco de dados e de aplicativos ou que esteja no modo somente leitura.
- Em implantações de produção, verifique se as zonas do kernel não podem ser acessadas por redes públicas ou diretamente para acesso do cliente. O acesso direto e o uso de serviços de armazenamento compartilhado em redes públicas ou acesso do cliente devem ser encerrados. Se as máquinas virtuais necessitarem de acesso ao sistema de arquivos /sharedstore por meio de NFS, verifique se ele é facilitado por canais IPSEC/IKE.

Relatórios de Auditoria e Conformidade

Estes tópicos descrevem os recursos de relatórios de auditoria e conformidade disponíveis no MiniCluster:

- [Verificar as Políticas de Auditoria \[39\]](#)
- [Revisar Logs de Auditoria \[40\]](#)
- [Gerar Relatórios de Auditoria \[41\]](#)
- [\(Se Necessário\) Ativar a Operação em Conformidade com o FIPS-140 \(Oracle ILOM\) \[43\]](#)
- [“Conformidade com o FIPS-140-2 Nível 1” \[44\]](#)

▼ Verificar as Políticas de Auditoria

A política de auditoria é configurada durante a instalação das zonas globais e não globais na seleção de um perfil de conformidade (CIS Equivalent padrão ou PCI-DSS).

Para verificar se as políticas de auditoria estão ativadas, execute estas etapas.

1. Faça log-in na zona global como `mcinstall` e assuma a atribuição `root`.

Para obter instruções sobre como fazer log-in no Oracle ILOM, consulte o *Oracle MiniCluster S7-2 Administration Guide*.

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

2. Verifique se o serviço de auditoria está on-line.

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

3. Verifique se o serviço de auditoria está ativo.

```
# auditconfig -getplugin audit_binfile
```

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

4. Verifique as políticas de auditoria ativas.

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

5. Verifique se todas as atribuições foram capturadas pela política de auditoria cusa.

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

▼ Revisar Logs de Auditoria

1. Faça log-in na zona global como mcinstall e assumo a atribuição root.

Para obter instruções sobre como fazer log-in no Oracle ILOM, consulte o *Oracle MiniCluster S7-2 Administration Guide*.

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

2. Use o comando auditreduce conforme mostrado.

Esta é a sintaxe para visualizar os logs de auditoria:

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

# cd /var/share/audit
#
# ls
20160628051437.not_terminated.mc4-n1
#
# auditreduce -z dbvmg1-zone-1-mc4-n1 20160628051437.not_terminated.mc4-n1 | praudit -s
file,2016-06-27 22:58:53.000 -07:00,
header,127,2,AUE_zone_state,,mc4-n1.us.oracle.com,2016-06-27 22:58:53.354 -07:00
subject,mcinstall,root,root,root,root,26272,415120213,9462 65558 mc4-n1.us.oracle.com
text,boot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
header,88,2,AUE_zone_state,na,mc4-n1.us.oracle.com,2016-06-27 23:02:30.767 -07:00
text,reboot
zone,dbvmg1-zone-1-mc4-n1
return,success,0
zone,global
file,2016-06-27 23:02:30.000 -07:00,
```


▼ Gerar Relatórios de Auditoria

Use este procedimento para gerar relatórios de auditoria para um nó ou para zonas globais e VMs individuais.

- 1. Efetue log-in no MCMU como usuário que recebeu a função de Auditor.**
Para obter informações sobre usuários e funções do MCMU, consulte o *Guia de Administração do MiniCluster S7-2*, disponível em: http://docs.oracle.com/cd/E69469_01.
- 2. No painel de navegação, selecione Configurações do Sistema -> Segurança.**
A página Análise de Auditoria será exibida.

Observação - Somente usuários do MCMU que tenham a função de auditor podem exibir esta página.

The screenshot shows the Oracle MiniCluster Configuration Utility interface. At the top, it says "ORACLE MiniCluster Configuration Utility" and "English mc1auditor". The main content area is titled "Welcome to the Minicluster Audit Review!".

Audit Pool Status

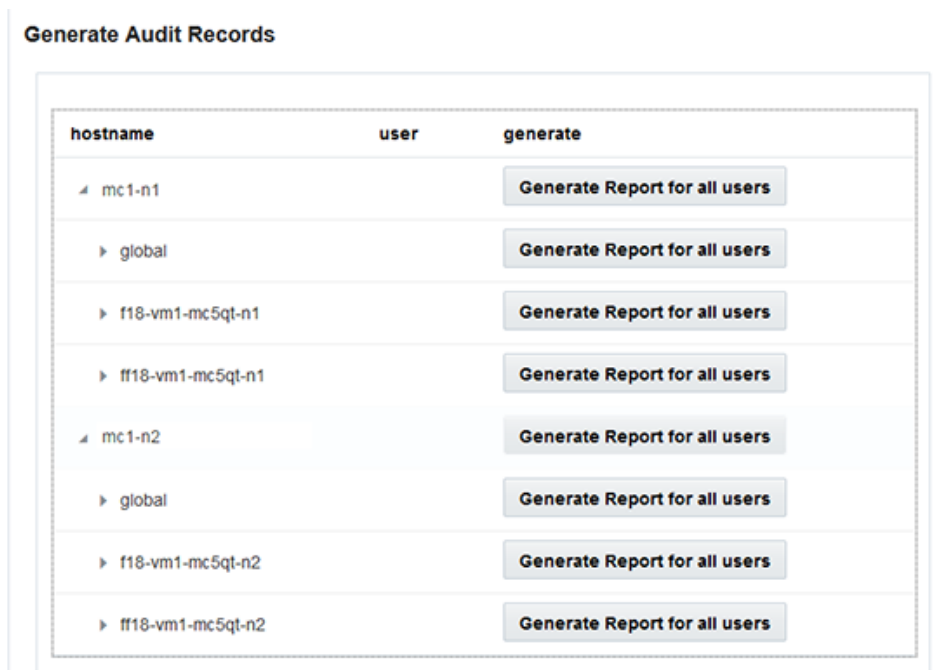
hostname	used	available
mc1-n1	12M	708G
mc1-n2	6.5M	709G

Generate Audit Records

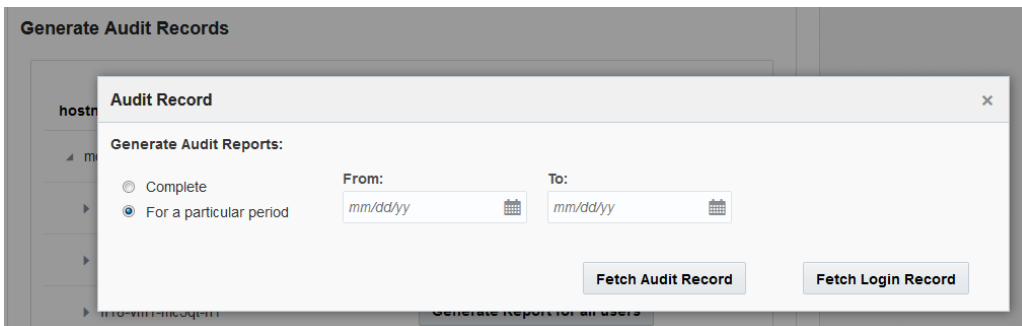
hostname	user	generate
mc1-n1		Generate Report for all users
global		Generate Report for all users
azg1-vm1-mc1-n1		Generate Report for all users
mc1-n2		Generate Report for all users
global		Generate Report for all users

- 3. Consulte a seção Status do Pool de Auditoria.**
Esta seção relaciona a quantidade de espaço usado e disponível para pools de auditoria em cada nó.
- 4. Para gerar um relatório para o nó inteiro, clique no botão Gerar relativo a um dos nós e vá para Passo 6.**
Outra opção é gerar um relatório para uma zona ou uma VM específica. Consulte [Passo 5](#).
- 5. Para gerar um relatório para uma zona global ou uma VM específica, execute estas etapas.**

- a. Clique no triângulo ao lado do nó para expandir a view.



- b. Na zona global ou na VM, clique em Gerar Relatórios para todos os usuários.
6. Na caixa de diálogo Registro de Auditoria, configurar os parâmetros do registro de auditoria.



Estas são as opções:

- **Completo** – Selecione se você deseja um relatório que inclua todos os registros de auditoria.
- **Para um determinado período** – Selecione se você deseja especificar um período de tempo específico e insira as datas de início e término.

7. **Clique em um dos botões Obter.**

Estas são as opções:

- **Obter Registro de Auditoria** – Gera um registro de auditoria completo.
- **Obter Registro de Log-in** – Gera atividades de usuário como log-ins, log-outs e ações do usuário.

8. **Clique no botão Clique Aqui e selecione o arquivo XML para download.**

O arquivo XML pode ser importado para aplicativos de análise de auditoria como o Oracle Audit Vault.

9. **Clique em Fechar.**

▼ (Se Necessário) Ativar a Operação em Conformidade com o FIPS-140 (Oracle ILOM)

O uso de criptografia validada FIPS 140 é exigido 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 ativado, se necessário.

Algumas funcionalidades do Oracle ILOM não estão disponíveis quando configuradas para operação em conformidade com o FIPS 140. Uma lista dessas funcionalidades é encontrada no *Guia de Segurança do Oracle ILOM* na seção intitulada "Funcionalidades Não Suportadas Quando o Modo FIPS Está Ativado".

Consulte também [“Conformidade com o FIPS-140-2 Nível 1” \[44\]](#).



Cuidado - Esta tarefa requer a redefinição do Oracle ILOM. Uma redefinição resulta na perda de todas as definições configuradas pelo usuário. Por esse motivo, é necessário ativar a operação em conformidade com o 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, efetue log-in no Oracle ILOM.**

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

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

O modo de conformidade com o 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 o 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
```

Conformidade com o FIPS-140-2 Nível 1

Os aplicativos criptográficos hospedados no MiniCluster baseiam-se na funcionalidade Cryptographic Framework do Oracle Solaris, que está validado em relação à conformidade com o FIPS 140-2 Nível 1. O Oracle Solaris Cryptographic Framework é o armazenamento criptográfico central para o Oracle Solaris e fornece dois módulos validados pelo FIPS 140 que dão suporte aos processos no nível do kernel e no espaço do usuário. Esses módulos de biblioteca fornecem funções de criptografia, decriptografia, 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 o 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 o FIPS 140. Quando executados em modos em conformidade com o FIPS 140, o Oracle Solaris e o OpenSSL, que são provedores do FIPS 140-2, reforçam o uso de algoritmos criptográficos validados para o FIPS 140.

Consulte também [\(Se Necessário\) Ativar a Operação em Conformidade com o FIPS-140 \(Oracle ILOM\) \[43\]](#).

Essa tabela lista algoritmos aprovados pelo FIPS compatíveis com o Oracle Solaris no MiniCluster.

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: modos 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 o FIPS 140-2 Nível 1.

- A funcionalidade 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, decryptografia, hash, geração e verificação de assinaturas, geração e verificação de certificados e autenticação de mensagens para aplicativos. Os aplicativos de nível de usuário chamados nesses módulos são executados no modo FIPS 140, como, 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 consomem 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 *Using a FIPS 140 Enabled System in Oracle Solaris 11.2*, disponível abaixo do título Securing the Oracle Solaris 11 Operating System em: http://docs.oracle.com/cd/E36784_01.

Avaliando a Conformidade com Segurança

Estes tópicos descrevem a funcionalidade de benchmark de segurança do MiniCluster:

- [“Benchmarks de Conformidade com Segurança” \[47\]](#)
- [Programar um Benchmark de Conformidade com Segurança \(BUI\) \[48\]](#)
- [Exibir Relatórios de Benchmark \(BUI\) \[49\]](#)

Benchmarks de Conformidade com Segurança

Quando o sistema é instalado, um perfil de segurança (PCI-DSS, CIS Equivalent e DISA-STiG) é selecionado e o sistema é configurado automaticamente para atender a esse perfil de segurança. Para garantir que o sistema continue a funcionar de acordo com os perfis de segurança, o MCMU fornece o meio para executar benchmarks de segurança e acesso aos relatórios de benchmark. Você pode administrar os benchmarks usando o MCMU BUI e o CLI.

A execução de benchmarks de segurança fornece estes benefícios:

- Permite avaliar o estado de segurança atual do banco de dados e das VMs dos aplicativos.
- Os testes de conformidade com segurança dão suporte a PCI-DSS, CIS Equivalent (padrão) e DISA-STiG, com base no nível de segurança configurado durante a instalação.
- Os testes de conformidade com segurança são executados automaticamente quando o sistema é inicializado e podem ser executados sob demanda ou em intervalos programados.
- Disponíveis somente para os administradores principais do MCMU, pontuações e relatórios de conformidade são facilmente acessados no MCMU BUI.
- Os relatórios de conformidade fornecem recomendações de reparo.

Observação - O perfil DISA-STIG está em análise no momento. Só utilize este perfil para uso experimental em ambientes que não são de produção.

▼ Programar um Benchmark de Conformidade com Segurança (BUI)

Use este procedimento para programar um benchmark de segurança usando a BUI do MCMU. Para usar o MCMU CLI, consulte o *Oracle MiniCluster S7-2 Administration Guide* para obter instruções.

1. **Efetue log-in na BUI do MCMU como um administrador principal.**
Consulte o *Oracle MiniCluster S7-2 Administration Guide* para obter instruções.

2. **Na Página inicial, role para o painel Informações de Conformidade.**

3. **Clique em um nó para expandir seus detalhes.**

Todas as zonas e VMs foram configuradas com um perfil de segurança (CIS Equivalent ou PCI-DSS). Ao programar um benchmark, selecione um que corresponda ao perfil de segurança do componente.

Compliance Information
Assess and Report Compliance for the virtual machines in the system

Update Reports

Node	Hostname	Benchmark Type	Compliance Score	Date & Time	Remarks	View Repo
Node 1						
	global	pci-dss			No Reports Found	
	global	cis.equivalent			No Reports Found	
	dbvmg1-zone-1-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-1-mc4-n1	cis.equivalent			No Reports Found	
	dbvmg1-zone-2-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-2-mc4-n1	cis.equivalent			No Reports Found	
	dbvmg1-zone-3-mc4-n1	pci-dss			No Reports Found	
	dbvmg1-zone-3-mc4-n1	cis.equivalent			No Reports Found	

4. **Role para a direita e clique em um botão Programar para uma das VMs.**

A página Programar execução de conformidade é exibida.

5. **Especifique a hora e a frequência e, em seguida, clique em Iniciar.**

Após a execução do teste de conformidade com segurança no horário programado, leia o relatório. Consulte [Exibir Relatórios de Benchmark \(BUI\) \[49\]](#).

▼ Exibir Relatórios de Benchmark (BUI)

Estes são os resultados de conformidade aceitáveis:

	CIS Equivalent	PCI-DSS
Zonas globais	aprox. 88%	aprox. 88%
VMs	aprox. 90%	aprox. 93%

Estas são as falhas de teste de conformidade conhecidas devido a problemas no Oracle Solaris:

- Integridade do pacote (core os, rad-python)
- GDM
- Daemon de roteamento
- Endereços de loopback SSH – a mitigação não corrige o problema.
- Os serviços de nomenclatura não reconhecem o DNS
- Cliente LDAP

Estas são as falhas de teste de conformidade conhecidas devido a problemas de configuração solicitada pelo cliente do MiniCluster:

- Serviços do cliente NFS – os serviços selecionados precisam estar disponíveis.
- Configuração da senha eeprom – uma configuração opcional

- 1. Efetue log-in na BUI do MCMU.**
- 2. Na Página inicial, role para o painel Informações de Conformidade.**
- 3. Clique em Atualizar Relatórios.**
O processo de atualização leva cerca de um minuto para ser concluído.
- 4. Expanda a exibição do nó e identifique o relatório de conformidade.**

3-1-mc4-n1	cis.equivalent	89.83/100	2016-06-20,14:21	-	View Report
------------	----------------	-----------	------------------	---	-----------------------------

- 5. Role para a direita e clique em Exibir Relatório.**
O relatório de benchmark é exibido.

Em Visão Geral da Regra, você pode selecionar quais tipos de teste exibir com base em seus resultados. Você também pode especificar uma string de pesquisa no campo de pesquisa.

ORACLE SOLARIS Compliance Report

Oracle Solaris Security Policy

with profile **Solaris Recommended Security Policy**

Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.

Evaluation Characteristics

Target machine	appvmg1-zone-1-mc4-n1
Benchmark Title	Oracle Solaris Security Policy
Benchmark Version	1.13749
Benchmark Description	Oracle Solaris Compliance baseline and recommended settings for general purpose operating systems installations.
Profile ID	Recommended
Started at	2016-06-20T14:21:21
Finished at	2016-06-20T14:22:10
Performed by	

CPE Platforms

- cpe:/o:oracle:solaris:11

Addresses

Compliance and Scoring

The target system did not satisfy the conditions of 11 rules! Please review rule results and consider applying remediation.

Rule results

174 passed

11 failed

Severity of failed rules

1 other

4 low

5 medium

1 high

- Com base no relatório, você pode verificar os controles de segurança, as pontuações de conformidade, as anormalidades e os procedimentos de reparo.
- Clique no nome de um teste para obter detalhes e as informações sobre reparos recomendados.

Observação - Você pode exibir todos os detalhes de todos os testes clicando em **Mostrar todos os Detalhes dos Resultados** na parte inferior do relatório.

Rule ID	OSC-54005
Result	fail
Time	2016-06-20T14:21:46
Severity	high
Identifiers and References	
Description	Run 'pkg verify' to check that all installed Oracle Solaris software matches the packaging database and that ownership, permissions and content are correct.

SCE stdout

```
The following packages showed errors
pkg://solaris/system/core-os          ERROR
pkg://solaris/system/management/rad/client/rad-python  ERROR
Run 'pkg verify' to determine the nature of the errors.
```

Remediation description:

'pkg verify' has produced errors. Rerun the command and evaluate the errors. As appropriate, based on errors found, you should run 'pkg fix <package-fmri>' See the pkg(1) man page.

Remediation script:

```
# pkg verify
followed by
# pkg fix <package-fmri>
```

Service svc:/system/pkg is enabled in global zone | medium | pass

Noções Básicas dos Controles de Segurança do Servidor SPARC S7-2

Estes tópicos descrevem os controles de segurança para o hardware e o ambiente OpenBoot.

- [“Noções Básicas de Segurança de Hardware” \[53\]](#)
- [“Restringindo o Acesso ao OpenBoot” \[55\]](#)

Noções Básicas de Segurança de Hardware

O isolamento físico e o controle do acesso compõem a base da arquitetura de segurança. Garantir que o servidor físico esteja instalado em um ambiente seguro o protege contra o acesso não autorizado. Da mesma forma, registrar todos os números de série ajuda a impedir roubo, revenda ou risco à cadeia de fornecimento (ou seja, injeção de componentes falsificados ou comprometidos na cadeia de fornecimento da sua organização).

Estas seções fornecem diretrizes gerais sobre segurança do hardware para o MiniCluster.

- [“Restrições de Acesso” \[53\]](#)
- [“Números de Série” \[54\]](#)
- [“Unidades de Disco Rígido” \[54\]](#)

Restrições de Acesso

- Instale os servidores e equipamentos relacionados em um local trancado e com acesso restrito.
- Se o equipamento for instalado em um rack com uma porta com trava, só destranque a porta do rack durante a manutenção dos componentes no rack. O travamento das portas também restringe o acesso aos dispositivos hot-plug ou hot-swap.
- Guarde FRUs (unidades substituíveis no campo) e CRUs (unidade substituíveis pelo cliente) sobressalentes em um gabinete fechado. 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. O acesso físico é um método mais seguro de acessar um componente já que ele não é suscetível a ataques baseados na rede.
- Conecte a console a um KVM externo para permitir o acesso remoto à console. Em geral, os dispositivos KVM suportam autenticação de dois fatores, controle de acesso centralizado e auditoria. Para obter mais informações sobre as diretrizes de segurança e as práticas recomendadas para KVM, consulte a documentação que acompanha o dispositivo KVM.

Números de Série

- Mantenha um registro dos números de série de todo o equipamento de hardware.
- Faça uma marca de segurança em todos os itens relevantes de hardware, do computador, como peças de reposição. Use canetas ultravioleta especiais ou rótulos.
- Mantenha as chaves e as licenças de ativação de hardware em um local seguro que seja facilmente acessível para o gerente do sistema em emergências de segurança. Os documentos impressos talvez sejam o seu único comprovante de propriedade.

Os leitores de identificação por radiofrequência (RFID) sem fio podem simplificar ainda mais o rastreamento de ativo. Um white paper da Oracle, *How to Track Your Oracle Sun System Assets by Using RFID*, está disponível em:

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

Unidades de Disco Rígido

Discos rígidos são geralmente usados para armazenar informações confidenciais. Para proteger essas informações contra a divulgação não autorizada, os discos rígidos devem ser limpos antes de serem reutilizados, descontinuados ou descartados.

- Use ferramentas de limpeza de disco como o comando `format (1M)` do Oracle Solaris para apagar completamente todos os dados do disco rígido.
- 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

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

Restringindo o Acesso ao OpenBoot

Estes tópicos descrevem como restringir o acesso ao prompt do OpenBoot.

Para obter instruções sobre como configurar uma senha do OpenBoot, consulte [Configurar Senhas do EEPROM \[28\]](#).

- [Acessar o Prompt do OpenBoot \[55\]](#)
- [Verificar Falhas de Log-in \[56\]](#)
- [Fornecer um Power-On Banner \[56\]](#)

Para obter informações sobre como definir as variáveis de segurança do OpenBoot, consulte a documentação do OpenBoot em:

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

▼ Acessar o Prompt do OpenBoot

Este procedimento descreve como acessar o prompt do OpenBoot nos nós de computação do MiniCluster a fim de configurar os controles de segurança.

É necessário encerrar o sistema para atingir o prompt do OpenBoot. Siga os procedimentos adequados para encerrar as VMs de forma limpa, conforme descrito no *Oracle MiniCluster S7-2 Administration Guide*.

1. Efetue log-in no Oracle ILOM em um nó e emita esse comando.

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

Efetue log-in no console de host como o usuário `mcinstall` e `su` para `root`.

2. Assim que todas as VMs forem encerradas, como a atribuição `root`, suspenda a zona global.

```
# init 0
.
.
.
{0} ok
```

▼ Verificar Falhas de Log-in

1. **Determine se alguém tentou e não conseguiu acessar o ambiente do OpenBoot usando o parâmetro `security-#badlogins`, como no exemplo a seguir.**

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

Se esse comando retornar um valor maior que 0, isso indica que foi registrada uma falha na tentativa de acessar o ambiente do OpenBoot.

2. **Redefina o parâmetro digitando este comando.**

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

▼ Fornecer um Power-On Banner

Embora este não seja um controle direto de prevenção ou detecção, um banner pode ser usado para esses motivos:

- Transmitir propriedade.
 - Avisar os usuários a respeito do uso aceitável do servidor.
 - Indicar que o acesso ou modificações no parâmetro OpenBoot estão restritos ao pessoal autorizado.
- **Use os comandos a seguir para ativar uma mensagem de advertência personalizada.**

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

A mensagem do banner pode ter até 68 caracteres. São aceitos todos os caracteres que podem ser impressos.

Índice

A

- aceleração criptográfica, 13
- acessando o prompt do OpenBoot, 55
- alterando chaves SSH, 22
- ambientes de inicialização verificada, verificando, 35
- analisando logs de auditoria, 40
- armazenamento compartilhado, restringindo o acesso, 36
- arquivos de log de verificação, 18
- ativando operação em conformidade com o FIPS-140 (Oracle ILOM), 43
- atribuições de contas de usuários, 30
- atribuições para contas de usuários do MCMU, 30
- auditoria e conformidade, 14
- autenticação de mensagens baseadas em hash, 44

B

- banner, fornecendo, 56
- benchmarks de conformidade
 - visão geral, 47

C

- chaves assimétricas, 44
- chaves simétricas, 44
- chaves SSH, alterando, 22
- comunicação segura com IPsec, 24
- configurando
 - IPsec e IKE, 25
 - senhas do EEPROM, 28
- conformidade e auditoria, 14
- conta de administrador primário, 31
- conta de administrador secundário, 31
- conta de administrador tenant, 31
- conta de supervisor, 31

- contas de usuário, 31
- contas de usuário do MCMU, 31
- controle de acesso, 12
- criptografia, 13, 21
- Criptografia de conjunto de dados ZFS, 21

E

- EEPROM, configurando uma senha, 28
- estratégias, segurança, 10
- exclusão segura de VMs, 33
- exibindo
 - informações do sistema de segurança (BUI), 21
 - relatórios de benchmark de segurança (BUI), 49
- exigido de tarefas de segurança, 9

F

- FIPS-140
 - algoritmos aprovados, 44
 - conformidade de Nível 1, 44
 - operação em conformidade (Oracle ILOM),
 - ativando, 43
- fornecendo um banner de ativação, 56
- funções de usuário do Oracle Solaris, verificando, 33

G

- geradores de números aleatórios, 44
- gerando relatórios de auditoria, 41

H

- hardware
 - números de série, 54

restrições de acesso, 53

I

IKE, configurando, 25

IPsec, 24

IPsec, configurando, 25

L

log-ins do OBP, verificando falhas, 56

logs de auditoria, analisando, 40

M

máquinas virtuais seguras, 11

mcinstall conta de usuário, 31

mínimo exigido de tarefas de segurança, 9

N

números de série, 54

O

OpenBoot

acessando, 55

configurando uma senha, 28

restringindo o acesso ao OpenBoot, 55

Oracle ILOM, alterando a senha raiz, 27

P

padrão de hash seguro, 44

perfil de segurança padrão, 17

perfil PCI-DSS, 17

perfil STIG DISA, 17

perfis de segurança

verificando, 18

perfis, segurança, 17

PKCS #11, 13

políticas de auditoria, verificando, 39

princípios, segurança, 9, 10

privilégios, 30

programando benchmarks de segurança, 48

proteção de dados, 13

proteção de dados com criptografia de conjunto de dados ZFS, 21

protegendo dados, 21

protocolo de rede SSH, 22

provisionando usuários, 29

R

raiz, alterando a senha

, 27

regras de firewall, verificando, 33

relatórios de auditoria, gerando, 41

restrições de acesso para hardware, 53

restringindo o acesso a armazenamento compartilhado, 36

S

segurança

alterando senhas no Oracle ILOM, 27

benchmarks de conformidade, 47

benchmarks de conformidade, programando (BUI), 48

exibindo informações (BUI), 21

exibindo relatórios de benchmark (BUI), 49

perfis, 17

princípios, 9, 10

segurança de hardware, noções básicas, 53

seguras, máquinas virtuais, 11

senhas

alterando no Oracle ILOM, 27

padrão para MCMU, 31

políticas, 32

serviço de shell seguro, 22

T

tarefas de segurança, mínimo exigido, 9

U

unidades de disco rígido, 54

usuários
 processo de aprovação, 29
 provisionando, 29
usuários do MCMU
 processo de aprovação, 29

V

verificando
 ambientes de inicialização verificada, 35
 funções de usuário do Oracle Solaris, 33
 perfis de segurança, 18
 políticas de auditoria, 39
 regras de firewall baseado em host, 33
verificando falhas nos log-ins do OBP, 56
visão geral
 contas de usuário do MCMU, 31
 processo de aprovação de usuários, 29
VMs, exclusão segura, 33

