

StorageTek Virtual Storage Manager GUI

Guia de Segurança

E79973-01

Julho de 2016

StorageTek Virtual Storage Manager GUI

Guia de Segurança

E79973-01

Copyright © 2016, Oracle e/ou suas empresas afiliadas. Todos os direitos reservados.

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, envie-nos 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 da SPARC são usadas sob licença e são marcas comerciais registradas da SPARC International, Inc. AMD, Opteron, a logomarca da AMD e a logomarca da AMD Opteron são marcas comerciais ou marcas comerciais registradas da Advanced Micro Devices. UNIX é uma marca comercial registrada do The Open Group.

Este programa ou hardware 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.

Índice

Prefácio	5
Público-alvo	5
Acessibilidade da Documentação	5
1. Visão Geral	7
Visão Geral do Produto	7
Segurança	7
Princípios Gerais de Segurança	7
Manter o Software Atualizado	7
Restringir o Acesso à Rede	8
Manter-se Atualizado com as Informações Mais Recentes de Segurança	8
2. Instalação Segura	9
Compreender seu Ambiente	9
Quais recursos precisam ser protegidos?	9
De quem os recursos precisam ser protegidos?	9
O que acontecerá se houver falha na proteção dos recursos estratégicos?	9
Instalação do StorageTek VSM GUI	9
Configuração Pós-Instalação	10
Atribuir a senha (admin) do usuário	10
Impor o gerenciamento de senhas	10
3. Recursos de Segurança	11
A. Lista de Verificação para uma Implantação Segura	13
B. Referências	15

Prefácio

Este documento descreve os recursos de segurança do StorageTek Virtual Storage Manager GUI da Oracle.

Público-alvo

Este guia destina-se a todos os envolvidos no uso dos recursos de segurança e na instalação e configuração seguras do VSM GUI.

Acessibilidade da Documentação

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

Acesso ao Oracle Support

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

Capítulo 1. Visão Geral

Esta seção fornece uma visão geral do StorageTek Virtual Storage Manager (VSM) GUI e explica os princípios gerais de sua segurança.

Visão Geral do Produto

O StorageTek VSM GUI é um software da Oracle que fornece aos clientes controle e geração de relatórios de fitas virtuais para um monitoramento e gerenciamento eficientes das operações em fita virtual do centro de dados.

O VSM GUI é compatível com clientes de fitas Enterprise MVS Virtual Storage Manager (VSM). O VSM GUI é compatível com clientes de todas as gerações de produtos VSM com suporte.

Segurança

Física

É necessário instalar o VSM GUI em uma máquina virtual no servidor Oracle VM ou VMware do cliente dentro do centro de dados da organização. O acesso físico ao servidor seria controlado pela política da empresa do cliente.

Rede

É necessário que o VSM GUI seja adicionado ou configurado em uma rede interna protegida por firewall do cliente. Essa rede precisa de acesso TCP/IP a todas as instâncias do servidor SMC HTTP que interagem com os recursos da fita virtual.

Acesso do Usuário

O acesso ao aplicativo VSM GUI é controlado pela autenticação do nome do usuário e da senha. A autenticação do nome de usuário e da senha é executada pela configuração do aplicativo para o serviço LDAP do usuário.

Princípios Gerais de Segurança

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

Manter o Software Atualizado

Um dos princípios da boa prática de segurança é manter todas as versões e patches do software atualizados. Em todo o documento, pressupomos estes níveis de software:

VSM GUI Versão 1.1; Julho de 2016

Nota:

O VSM GUI é compatível com ELS7, 1 ELS 7.2 e ELS 7.3 requer que as atualizações mais recentes de manutenção sejam aplicadas.

Restringir o Acesso à Rede

Mantenha o servidor host do VSM GUI protegido por um firewall de centro de dados. O firewall garante que o acesso a esses sistemas seja restrito à rota de rede conhecida, a qual pode ser monitorada e restringida, se necessário. Como alternativa, um roteador de firewall substitui vários firewalls independentes.

Manter-se Atualizado com as Informações Mais Recentes de Segurança

A Oracle aprimora continuamente seu software e documentações relacionadas. Verifique se há revisões em cada versão deste documento. Questões de segurança específicas também podem ser citadas nas notas de versão.

Capítulo 2. Instalação Segura

Esta seção destaca o processo de planejamento para uma instalação segura e descreve várias topologias de implantação recomendadas para os sistemas. O Guia do Usuário do VSM GUI 1.0 aborda em detalhes as etapas de instalação, configuração e administração.

Compreender seu Ambiente

Para melhor compreender as necessidades de segurança, as seguintes perguntas devem ser feitas:

Quais recursos precisam ser protegidos?

Para o VSM GUI, o servidor host e a rede associada deverão ser protegidos contra o acesso não autorizado

De quem os recursos precisam ser protegidos?

O VSM GUI deverá ser protegido de todos na Internet, de usuários externos e internos não autorizados.

O que acontecerá se houver falha na proteção dos recursos estratégicos?

Como o VSM GUI é um aplicativo de utilização e monitoramento dos recursos de armazenamento virtual, o acesso não autorizado ao VSM GUI pode afetar a disponibilidade de recursos do VSM. O estado de um recurso pode ser afetado, mas os dados contidos nos recursos de armazenamento não serão afetados.

Instalação do StorageTek VSM GUI

O VSM GUI só deve ser instalado em sistemas que estejam dentro da mesma infraestrutura de rede protegida (com firewall) que os recursos virtuais monitorados (ou seja, VTCS e HSC). Os controles de acesso do cliente devem ser impostos nos sistemas onde o VSM GUI está instalado para garantir o acesso restrito ao aplicativo.

Consulte o *Guia do Usuário do VSM GUI* para obter instruções de instalação.

Configuração Pós-Instalação

Não há alterações de segurança na configuração pós-instalação. A configuração é definida pelo cliente durante a instalação.

Atribuir a senha (admin) do usuário

A senha da conta de administração do cliente é definida pelo cliente durante a instalação.

Impor o gerenciamento de senhas

Regras de gerenciamento de senhas corporativas do cliente, como tamanho, histórico e complexidade , devem ser aplicadas à senha do administrador.

Capítulo 3. Recursos de Segurança

Esta seção descreve os mecanismos de segurança específicos oferecidos pelo produto. O aplicativo VSM GUI oferece ao usuário funções de senha criptografadas para proteção. Esta não é a única linha de segurança para proteger o aplicativo. O aplicativo deve estar em um centro de dados fisicamente seguro que também tenha uma rede segura, a qual permite acesso somente aos usuários autorizados.

Apêndice A

Apêndice A. Lista de Verificação para uma Implantação Segura

A seguinte lista de verificação de segurança inclui diretrizes que ajudam a proteger a biblioteca:

1. Impor o gerenciamento de senhas.
2. Impor controles de acesso.
3. Restringir o acesso à rede.
 - a. Um firewall deve ser implementado.
 - b. O firewall não deve ser comprometido.
 - c. O acesso ao sistema deve ser monitorado.
 - d. Os endereços IP da rede devem ser verificados.
4. Entre em contato com a equipe do Oracle Security Products caso encontre vulnerabilidades no VSM GUI.

Apêndice B

Apêndice B. Referências

Guia do Usuário do VSM GUI

