StorageTek Virtual Storage Manager GUI

Guia de Segurança

E79973-01

Julho de 2016

ORACLE

StorageTek Virtual Storage Manager GUI
Guia de Segurança

E79973-01

Índice

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.

1

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.

2

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.

3

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