StorageTek Virtual Storage Manager GUI

Security Guide

Release 1.0

E61471-01

April 2015

ORACLE

StorageTek Virtual Storage Manager GUI Security Guide Release 1.0

E61471-01

Primary Author: VSM Development

Contributing Author:

Contributor:

Contents

Preface

This document describes the security features of Oracle's StorageTek Virtual Storage Manager GUI.

Audience

This guide is intended for anyone involved with using security features and secure installation and configuration of VSM GUI.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

1

Overview

This section gives an overview of StorageTek Virtual Storage Manager (VSM) GUI and explains the general principles of its security.

Product Overview

StorageTek VSM GUI is an Oracle software product that provides customers with virtual tape control and reporting, to efficiently and proactively monitor and manage their data center's virtual tape operations.

VSM GUI supports Enterprise MVS Virtual Storage Manager (VSM) tape customers. VSM GUI supports customers with all supported generations of VSM products.

Security

Physical

It is required VSM GUI is installed on a virtual machine on a customer's Oracle VM or VMware server within an organization's data center. Physical access to the server would be dictated by the Customer company policy.

Network

It is required VSM GUI be added or configured to a Customer internal firewall protected network. This network needs TCP/IP access to all instances of SMC HTTP server that report on virtual tape resources.

User Access

The VSM GUI Application access is controlled by username and password authentication. User name and password authentication are performed by configuring the application to the user's LDAP service.

General Security Principles

The following principles are fundamental to using any product securely.

Keep Software Up To Date

One of the principles of good security practice is to keep all software versions and patches up to date. Throughout this document, we assume software levels of:

VSM GUI Release 1.0; May 2015

Note: VSM GUI supports ELS7.1 and ELS7.2, and requires latest maintenance updates to be applied.

Restrict Network Access

Keep the VSM GUI host server behind a data center firewall. The firewall provides assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation. Check this document every release for revisions. Specific security concerns may also be addressed in release notes as well.

2

Secure Installation

This section outlines the planning process for a secure installation and describes several recommended deployment topologies for the systems. The VSM GUI User Guide 1.0 covers installation, configuration, and administration in detail.

Understand Your Environment

To better understand security needs, the following questions must be asked:

Which resources need to be protected?

For VSM GUI the host server and the associated network must be protected from unauthorized access

From whom are the resources being protected?

VSM GUI must be protected from everyone on the Internet, external users, and unauthorized internal users.

What will happen if the protections on strategic resources fail?

As VSM GUI is a virtual storage resource monitoring and usage application, unauthorized access to VSM GUI can affect VSM resources availability. The state of a resource can be affected, but the data residing on the storage resources will not be affected.

Installing StorageTek VSM GUI

VSM GUI should only be installed on systems that are within the same protected (firewalled) network infrastructure as the monitored virtual resources (that is, VTCS and HSC). Customer access controls should be enforced on the systems where VSM GUI is installed to assure restricted access to the application.

Refer to the *VSM GUI User Guide* for installation instructions.

Post Installation Configuration

There are no post-installation configuration security changes. The configuration is set by the customer during installation.

Assign the user (admin) password

The customer administration account password is set by the customer during the installation.

Enforce password management

Customer Corporate password management rules such as password length, history, and complexity must be applied to the administrator password.

3

Security Features

This section outlines the specific security mechanisms offered by the product.

The VSM GUI application provides user with encrypted password roles to protect itself. This is not the only line of security to protect the application. The application should be in a physically secured data center that also has a secured network that allows access only to authorized users

A

Secure Deployment Checklist

The following security checklist includes guidelines that help secure the library:

1. Enforce password management.
2. Enforce access controls.
3. Restrict network access.
   a. A firewall should be implemented.
   b. The firewall must not be compromised.
   c. System access should be monitored.
   d. Network IP addresses should be checked.
4. Contact Oracle Security Products if you come across vulnerabilities in VSM GUI.

B

References

VSM GUI User Guide