*53-1005047-01*
*22 May 2017*

# Brocade Virtual Traffic Manager: Compliance with the Security Technical Guidelines (STIG)

Supporting 17.2

BROCADE

## Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger Way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

# Contents

# Preface

Read this preface for an overview of the information provided in this guide. This preface includes the following sections:



## Document Conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Brocade technical documentation.

### Notes and Warnings

Note, important, and caution statements might be used in this document. They are listed in the order of increasing severity of potential hazards.

**Note:** A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

**Important:** An Important statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

**Caution:** A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

## Text Formatting Conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

| Format | Description |
|---|---|
| **bold text** | Identifies command names |
| | Identifies keywords and operands |
| | Identifies the names of user-manipulated GUI elements |
| | Identifies text to enter at the GUI |
| *italic text* | Identifies emphasis |
| | Identifies variables |
| | Identifies document titles |
| `Courier font` | Identifies CLI output |
| | Identifies command syntax examples |

## Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

| Convention | Description |
|---|---|
| **bold text** | Identifies command names, keywords, and command options. |
| *italic text* | Identifies a variable. |
| value | In Fibre Channel products, a fixed value provided as input to a command option is printed in plain text.<br>For example, **--show** WWN. |
| [ ] | Syntax components displayed within square brackets are optional.<br>Default responses to system prompts are enclosed in square brackets. |
| { x \| y \| z } | A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.<br>In Fibre Channel products, square brackets may be used instead for this purpose. |
| x \| y | A vertical bar separates mutually exclusive elements. |
| < > | Nonprinting characters, for example, passwords, are enclosed in angle brackets. |
| ... | Repeat the previous element, for example, member[member...]. |
| \ | Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash. |

# Brocade Resources

Visit the Brocade website to locate related documentation for your product and additional Brocade resources.

White papers, data sheets, and the most recent versions of Brocade software and hardware manuals are available at www.brocade.com. Product documentation for all supported releases is available to registered users at MyBrocade. Click the **Support** tab and select **Document Library** to access documentation on MyBrocade or www.brocade.com. You can locate documentation by product or by operating system.

Release notes are bundled with software downloads on MyBrocade. Links to software downloads are available on the MyBrocade landing page and in the Document Library.

# Document Feedback

Quality is our first concern at Brocade and we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. You can provide feedback in two ways:

- Through the online feedback form in the HTML documents posted on www.brocade.com.
- By sending your feedback to documentation@brocade.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

# Contacting Brocade Technical Support

As a Brocade customer, you can contact Brocade Technical Support 24x7 online, by telephone, or by e-mail. Brocade OEM customers contact their OEM/Solutions provider.

## Brocade Customers

For product support information and the latest information on contacting the Technical Assistance Center, go to www.brocade.com and select **Support**.

If you have purchased Brocade product support directly from Brocade, use one of the following methods to contact the Brocade Technical Assistance Center 24x7.

| Online | Telephone | E-mail |
|---|---|---|
| Preferred method of contact for nonurgent issues:<br>• Case management through the MyBrocade portal.<br>• Quick Access links to Knowledge Base, Community, Document Library, Software Downloads and Licensing tools. | Required for Sev 1-Critical and Sev 2-High issues:<br>• Continental US: 1-800-752-8061<br>• Europe, Middle East, Africa, and Asia Pacific: +800-AT FIBREE (+800 28 34 27 33)<br>• Toll-free numbers are available in many countries.<br>• For areas unable to access a toll free number: +1-408-333-6061 | support@brocade.com<br>Please include:<br>• Problem summary<br>• Serial number<br>• Installation details<br>• Environment description |

## Brocade OEM Customers

If you have purchased Brocade product support from a Brocade OEM/Solution Provider, contact your OEM/Solution Provider for all of your product support needs.

- OEM/Solution Providers are trained and certified by Brocade to support Brocade® products.
- Brocade provides backline support for issues that cannot be resolved by the OEM/Solution Provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information, contact Brocade or your OEM.
- For questions regarding service levels and response times, contact your OEM/Solution Provider.

# CHAPTER 1 About this Guide

This document describes the set-up procedure necessary to place Brocade Virtual Traffic Manager (the Traffic Manager) into a special locked-down state ready for compliance with the Security Technical Implementation Guidelines (STIG). This procedure consists of the high-level tasks listed below. Two are required and two are optional:

- (Required) Run the built-in lock-down script in order to secure the virtual appliance.

  For details about running the lock-down script, see Chapter 2, "Performing the Lock-down Procedure." .

- (Required) Configure the virtual appliance to comply with the STIG requirements.

  For details, see Chapter 3, "Configuring the Virtual Appliance for STIG Compliance." This chapter discusses the configuration key settings required, along with a brief description of their use.

- (Optional) Use the Maintenance CLI to manage and maintain the virtual appliance.

  The Maintenance CLI is an alternative control method that can be used instead of the Admin UI.

  For details, see Chapter 4, "Using the Maintenance CLI (Command-Line Interface)."

- (Optional) Review the information about the additional features associated with an STIG-compliance virtual appliance.

  For details about these features, see Chapter 5, "Additional Features."

## Additional STIG-ID Documentation

Where applicable, the relevant STIG-IDs are provided for reference. These are described in the following documents, available from:

http://iase.disa.mil/stigs/index.html

- UNIX Security Technical Implementation Guide (version 5, release 1)
- Web Server STIG (version 7, release 1)
- Application Security and Development STIG (version 3, release 2)

CHAPTER 2

# Performing the Lock-down Procedure

This chapter contains the instructions for performing the lock-down procedure. This chapter contains the following sections:



## Prerequisites

Before you begin, make sure that the server can connect to the virtual appliance by using SCP or SFTP. Then make sure you have the following items:

- The OVF edition of the Traffic Manager virtual appliance variant
- A valid customer account number
- An IP address for the virtual appliance
- A valid license

## Procedure

To put the virtual appliance in the locked-down state, complete the following procedure:

1. Import the OVF version of the Traffic Manager virtual appliance into VMware VSphere (or other compatible virtualization platform).
2. Using ssh, log in to the newly created virtual appliance using these credentials:

   Username: admin

   Password: admin
3. At the ssh prompt, run the following command to start the z-lock-down script.

```
/usr/lib/zeus-customisations/z-lock-down
```

4. Follow the on-screen instructions.

   The z-lock-down script creates a maintenance user ssh key-pair, disables password-based ssh access, and stores the key-pair and other information (including an archive copy of the maintenance tarball contents) in a maintenance details temporary directory. The location and name of this archive maintenance tarball is displayed.

---

**Caution:** Once you log out of the shell, the only way to gain root-level access to the virtual appliance is to use the credentials stored in the maintenance tarball.

Therefore, do not log out without first making a copy of the maintenance tarball. (Step 5).

Otherwise, you will need to run the z-lock-down script again.

---

   A signature key (that is, the Maintenance ID) is generated by the lock-down script. The lock-down script is a series of hexadecimal values separated by colons, and is the alphanumeric string appended to the name of the maintenance tarball (without the colons).

   For example, where the Maintenance ID is:

   aa:bb:cc:dd:ee:ff:00:11:22:33:44:55:66:77:88:99

   The maintenance tarball name becomes:

   support-report-aabbccddeeff00112233445566778899.tgz

   The Maintenance ID is displayed on the Diagnose > Technical Support page of the Admin UI and on the login banner of the Maintenance CLI. The Maintenance ID can also be found in the TSR (Technical Support Report), and is required by your support provider to identify the correct maintenance tarball created through this procedure.

5. Using the command **scp**, copy the maintenance tarball to a secure location outside of the virtual appliance.

6. Type **reboot** at the prompt to restart your virtual appliance. Restarting your virtual appliance ensures that any remaining temporary files are removed.

## What's Next?

Once you have completed this procedure, and you have the required maintenance tarball archive, your virtual appliance is now ready to be configured for STIG compliance. For detailed instructions, see Chapter 3, "Configuring the Virtual Appliance for STIG Compliance."

However, before you begin configuring the virtual appliance for STIG compliance, you need to let your support provider know that the virtual appliance is in lock-down state. See "Informing Your Support Provider" on page 8.

# Informing Your Support Provider

After completing the lock-down procedure, you must let your support provider know that the virtual appliance is in the lock-down state and that you have the required maintenance tarball. You let the support provider know this by opening a new Support case.

**Caution:** Do not send the maintenance tarball unless instructed to do so by an authorized support engineer.

Let your service provider know if your local security policy allows you to transfer the maintenance tarball off-site. Then complete one of the following procedures, as applicable:

### If Your Security Policy Allows You to Transfer the Maintenance Tarball

After receiving the support case, your support provider sends you an email with the instructions for performing a secure file transfer for the maintenance tarball.

**Note:** Please follow the instructions in the e-mail from your support provider and wait for an acknowledgment that your maintenance tarball has been successfully transferred. Do not delete your copy of the maintenance tarball without first receiving this acknowledgment.

### If Your Security Policy Does not Allow You to Transfer the Maintenance Tarball

If your security policy does not allow you to transfer the maintenance tarball to your support provider, store the maintenance tarball in a secure directory. You may end up storing the maintenance tarball for a long time before it is needed, so make sure your the long-term retrieval and backup processes in place are adequate.

Let your support provider know where the maintenance tarball is located. Provide as many details as possible, including the specific location, full file path, and contact information of the person/role responsible for the server or service storing the maintenance tarball. This level of detail helps the support provider locate the maintenance tarball later, if necessary.

If you have any questions or you need assistance, please contact your support provider.

CHAPTER 3

# Configuring the Virtual Appliance for STIG Compliance

This chapter contains information about configuring the Traffic Manager Virtual Appliance for STIG compliance. It lists the settings (accessible from the Admin UI) required and describes how the settings are used. This chapter contains the following sections:



## Login Banner Settings

These settings are configured in the Login and Security section of the System > Global Settings page.

| Setting | Function |
|---|---|
| login_banner | Sets the desired login banner (shown before login). (GEN000400, GEN000420) |
| banner_accept | Set to yes if users should explicitly accept the terms of the login banner before logging in. |
| post_login_banner | Sets the desired post_login_banner (shown after a successful login). |
| uipage_banner | Set a banner that will be displayed on all pages of the UI. (V-6146 APP3270) |

# Login Security Settings

These settings are configured in the Login and Security section of the System > Global Settings page.

| Setting | Function |
|---|---|
| max_login_attempts | The number of sequential failed login attempts that will cause a user account to be suspended. Avalue of 0 disables this feature. Default:0<br>STIG: Set to: 3 (GEN000460) |
| max_login_external | Whether the Traffic Manager tracks externally-authenticated (LDAP, RADIUS or TACACS+) users, such that they are suspended from accessing the Admin UI, or the SOAP and REST APIs, after the max_login_attempts limit is breached. Default: No<br>STIG: Set this to Yes unless the external service implements its own login suspension for failed passwords. |
| max_login_suspension_time | The number of minutes for which users who have exceeded the max_login_attempts limit should be suspended. Default: 15<br>STIG: Set to 15 (default) (GEN000460) |
| login_delay | The delay, in seconds, after a failed login before another login attempt can be made. Default: 4<br>STIG: Set to 4 (GEN000480) |
| bootloader_password | Enables or disables bootloader password protection.<br>Note: On a Traffic Manager Virtual Appliance, this only sets the bootloader password used for choosing between different versions of the Traffic Manager software. Even if the bootloader password is not set, a vendor-only password prevents access to the recovery shell.<br>STIG: Enable and set password (LNX00140) |

# Password Restriction Settings

These settings are configured in the Password Security Settings section of the System > Users > Local Users > Password Policy page.

| Setting | Function |
|---|---|
| password_security | Sets various password security settings. For STIG compliance, set to "default," which uses the following settings:<br>min_password_length: 8 (GEN000580)<br>min_alpha_chars: 2 (GEN000600)<br>min_uppercase_chars: 1 (GEN000600)<br>min_numeric_chars: 1 (GEN000620)<br>min_special_chars: 1 (GEN000640)<br>allow_consecutive_chars: No (GEN000680)<br>Alternatively, choose "custom" to set individual values for these items. |
| password_reuse_after | Sets the number of times passwords must be changed before the same password can be set again.<br>STIG: set to 10 (GEN000800) |
| password_changes_per_day | Sets the maximum number of password changes per day.<br>STIG: set to 1 (GEN000540) |

## Password Expiration Time Setting

The password expiration time is set by permission group, from System > Users > Groups > {admin, Demo, Guest, Monitoring}.

| Setting | Function |
|---|---|
| password_expire_time | Sets the number of days after which members of a group must change their passwords. If set to 0 (default), members are never required to change their passwords.<br>STIG: Set to 90 for all four default groups, and any new groups (GEN000720) |

CHAPTER 4

# Using the Maintenance CLI (Command-Line Interface)

You typically administer the Traffic Manager Virtual Appliance using the Web-based Admin UI. However, you can also administer the appliance using the Maintenance CLI. This chapter provides an overview of the Maintenance CLI commands, along with the command syntax and usage guidelines for the Maintenance CLI commands. This chapter contains the following sections:



## Maintenance CLI Overview

The Maintenance CLI allows you to access the command subsystem and perform various maintenance operations. To access the command subsystem, log in to the virtual appliance using an SSH client.

### Maintenance CLI Help System

The Maintenance CLI is a limited shell, with a number of useful commands. Typing **help** at the system prompt provides a list of the available commands. Typing **help** <*command*> provides help for the specific command.

The hostname (the appliance to which you are connected) appears before the system prompt. In the example below, stm1 is the hostname.

```
Last login: Tue Jan 25 08:43:48 2011 from 10.100.1.86
-------------------------------------------------------------
Brocade Virtual Traffic Manager Maintenance CLI
Type 'help' for information on available commands.
-------------------------------------------------------------
Maintenance ID: aa:bb:cc:dd:ee:ff:11:22:33:44:55:66:77:88:99:00
-------------------------------------------------------------
stm1 >
```

# Maintenance CLI Commands

The Maintenance CLI commands are grouped into two broad categories; commands used to gather support information (such as traces, TCP dumps, and networking information) and commands used to restore access to the Web-based Admin UI on a virtual appliance if the network connection fails.

The following table lists each of the Maintenance CLI commands, the command description, usage guidelines, and command syntax.

| Command | Description and Syntax |
|---|---|
| delete-file | Deletes a support file or log file from the disk.<br>Note the following points about using this command:<br>• To see all the files that can be deleted, use the **list-files** command. For more information about the **list-files** command, see "list-files" on page 18.<br>• Deleting error files clears the event log and you will be asked to confirm this action.<br>• Audit log files cannot be deleted.<br>• Wildcard characters can be used to delete multiple files.<br>Command Syntax:<br>**delete-file** <*filename*><br>Arguments:<br>• filename: The support file or log to delete.<br>Aliases: rm |
| exit | Logs you out of the Maintenance CLI and terminates your session.<br>Aliases: Logout, quit |
| firewall-clear | Clears all internal firewall settings (rules) on the Traffic Manager. Use this command only if the firewall settings prevent contact with the virtual appliance.<br>To see the current firewall rules, use the **info** command with the firewall subcommand. For more information about the **info** command, see "info" on page 17. |

| Command | Description and Syntax |
|---|---|
| info | Displays system information based on a specified subcommand.<br>Command Syntax:<br>**info** <*subcommand*><br>Argument:<br>subcommand: Specify one of the following:<br>– arp<br>– disk<br>– firewall<br>– interfaces<br>– maintenance-id<br>– memory<br>– nat<br>– net-devices<br>– net-stats<br>– ports<br>– processes<br>– routes<br>– sockets<br>– version |
| install-package | Installs (uploads) a package into the uploads directory. This command displays information about the package and requests confirmation before proceeding with the installation.<br>Use the **help scp** command for more information on uploading files.<br>Command Syntax:<br>**install-package** <*package*><br>Argument:<br>package: The package to be installed. The package must be uploaded to the uploads directory. |

| Command | Description and Syntax |
|---|---|
| list-files | Lists available files (and file sizes) that can be accessed by the Maintenance CLI. The following files are included in the list:<br>• errors: Event logs<br>• audit: Audit logs<br>• tmp/*: Temporary files<br>• statd/*: Historical activity logs<br>• vservers*: Virtual server request logs<br>• maintenance/*: Files created by the Maintenance CLI<br>• uploads/*: Files uploaded using the **scp** command<br>• discoveryagent/*: SteelHead discovery agent support data<br>Note the following points:<br>• To view the files, use the **view-file** command.<br>• To delete the files, use the **delete-file** command.<br>• To download the files, use the **scp** command. For more details about the **scp** command, use the **help scp** command.<br>Command Syntax:<br>**list-files**<br>Aliases: ls |
| network-configure | Sets up the IP address and the netmask of the primary Ethernet interface.<br>(Optional) This command allows you to specify an alternative network interface (rather than the default primary) or gateway IP. Specifying an alternative network interface clears the existing configuration for the interface. Therefore, specify an alternative network interface only if the network settings disable the connection to the appliance.<br>**Caution:** If you are using the Maintenance CLI over SSH, this command may terminate your session.<br>Command Syntax:<br>**network-configure** <*ip*> <*netmask*> [<*interface*>] [<*gateway*>]<br>Arguments<br>• IP: The IP address to use.<br>• netmask: The netmask to use.<br>• interface: (Optional) The interface to setup. If not specified, the interface is assumed to be your primary network interface, usually eth0.<br>gateway: (Optional) The IP address of the default gateway of the interface. |
| reboot | Reboots (restarts) the Traffic Manager Virtual Appliance and logs you out of the Admin UI. |
| reset-to-factory-defaults | Resets all configuration settings to the factory defaults.<br>**Caution:** By running this command, all system and traffic management configuration is lost, and the system is rebooted. Therefore, when using this command you are asked to confirm the action. |

| Command | Description and Syntax |
|---|---|
| restart | Restarts one component or all components. The components are the Traffic Manager service, the Admin UI, the REST API service, and the hardserver.<br>Note the following points about using this command:<br>• By default, all components (except the hardserver) are restarted, unless you specify a particular component.<br>• The hardserver is a background process that handles communications with an nShield HSM device. Under normal circumstances, you should never need to restart the hardserver unless communications have been disrupted or if instructed to do so by your support provider.<br>For more details, see your nCipher documentation.<br>Command Syntax:<br>**restart** [<*component*>]<br>Argument:<br>• component: (Optional) The component to restart. Valid entries are all, traffic_manager, ui, rest_api, and hardserver. All is the default value.<br>**Note:** The default value (all) does not include the hardserver. |
| rollback-delete | Completely deletes an archived minor revision of the Traffic Manager software.<br>Note the following points about using this command:<br>• You cannot restore this revision after you have deleted it.<br>• This command lets you delete only minor revisions of the full version currently in use. For example, if this appliance is running version 10.0, you will only be able to delete minor 'r' revisions installed for version 10.0.<br>• To remove 'r' revisions for other versions, first perform a full-version rollback. For details of this procedure, see the *Brocade Virtual Traffic Manager: Virtual Appliance Installation and Getting Started Guide*.<br>Command Syntax:<br>**rollback-delete** <*revision*><br>Argument:<br>• revision: The revision to be deleted. |
| rollback-list | Lists all previously installed revisions of the current Traffic Manager software version.<br>Command Syntax:<br>**rollback-list** |
| rollback-to | Performs a roll-back of the Traffic Manager software to the desired revision.<br>Note the following points about using this command:<br>• This command lets you roll back to only a minor revision of the presently installed full version. For example, if this appliance is running version 10.0, you will only be able to roll back to minor 'r' revisions installed for version 10.0.<br>• To roll back to 'r' revisions for other versions, first perform a full-version rollback. For details of this procedure, see the *Brocade Virtual Traffic Manager: Virtual Appliance Installation and Getting Started Guide*.<br>Command Syntax:<br>**rollback-to** <*revision*><br>Argument:<br>revision: The revision to be deleted. |

| Command | Description and Syntax |
|---|---|
| shutdown | Shuts down the Traffic Manager Virtual Appliance and logs you out of the Admin UI. |
| start | Starts one component or all components. The components are the Traffic Manager service, the Admin UI, the REST API service, and the hardserver.<br>Note the following points about using this command:<br>• By default, all components (except the hardserver) are started, unless you specify a particular component.<br>• The hardserver is a background process that handles communications with an nShield HSM device. Under normal circumstances, you should never need to send commands the hardserver unless instructed to do so by your support provider.<br>For more details, see your nCipher documentation.<br>Command Syntax:<br>**start** [<*component*>]<br>Argument:<br>• component: (Optional) The component to start. Valid entries are all, traffic_manager, ui, rest_api, and hardserver. All is the default value.<br>**Note:** The default value (all) does not include the hardserver. |
| stop | Stops one component or all components. The components are the Traffic Manager service, the Admin UI, the REST API service, and the hardserver.<br>Note the following points about using this command:<br>• By default, all components (except the hardserver) are stopped, unless you specify a particular component.<br>• The hardserver is a background process that handles communications with an nShield HSM device. Under normal circumstances, you should never need to send commands the hardserver unless instructed to do so by your support provider.<br>For more details, see your nCipher documentation.<br>Command Syntax:<br>**stop** [<*component*>]<br>Argument:<br>• component: (Optional) The component to stop. Valid entries are all, traffic_manager, ui, rest_api, and hardserver. All is the default value.<br>**Note:** The default value (all) does not include the hardserver. |
| support-report | Generates a support report tarball file (.tgz) and places it in the support files directory.<br>The report tarball file can then be downloaded by using the Support Files page in the Admin UI or by using the **scp** command from a remote client.<br>For more details about the **scp** command, use the **help scp** command. |

| Command | Description and Syntax |
|---|---|
| tcpdump | Captures packet information passing through the Traffic Manager virtual appliance. This command outputs information about the packet capture to the stdout directory and to disk.<br>To access the file on disk, use the Diagnose > Support Files page of the Admin UI.<br>To stop the command, type **Ctrl+C**.<br>Command Syntax:<br>**tcpdump** <*interface*> <*mode*> <*additional*><br>Arguments:<br>• interface: The interface to listen on, or "any" to listen on all interfaces. Valid entries are any, eth0, or lo.<br>• modes: The type of output to generate. Valid entries are text (which prints text information on the packet) or raw (which prints raw binary data).<br>• additional: Allows you to specify additional parameters and filters, using the same arguments as the **tcpdump** command. |
| trace | Traces a Traffic Manager process. This command sends the trace information to the standard output choices and to disk. To access the file on disk, use the Diagnose > Support Files page of the Admin UI. For more information about the Support Files page, see Chapter 5, "Additional Features."<br>**Caution:** Use this command only if requested to do so by your support provider.<br>To stop the command, type **Ctrl+C**.<br>Command Syntax:<br>**trace** <*process*> <*additional*><br>Arguments<br>• process: Type of process to trace (as requested by your support provider). Valid entries are children, child, parent, eventd, flipper, admin, monitor, and sysd.<br>• additional: Additional flags to use when tracing a Traffic Manager process, using the same valid entries as the process argument. |
| view-file | Enables viewing of a support file or log file from a disk. This command allows you to view text files only.<br>To view all available files, use the **list-files** command. For more information about the **list-files** command, see "list-files" on page 18.<br>Command Syntax:<br>**view-file** <*filename*> [*lines*]<br>Arguments<br>• filename: The support file or log file to view.<br>• lines: (Optional) The number of lines of the file to display.<br>Aliases: cat |

# CHAPTER 5 Additional Features

This chapter describes the additional features and functionality available on the STIG-compliant Traffic Manager Virtual Appliance. An optional task when setting up the virtual appliance is to review and become familiar with these additional features and use them, as applicable.

This chapter contains the following sections:



## The Role of the Audit User and Audit Group

STIG-compliant Traffic Manager Virtual Appliances include a dedicated audit user and audit group.

The audit user cannot be modified or removed, can only view Audit/Event log pages, and is the only user allowed to remove qualifying audit log archive files (that is, files that are older than the preset minimum retention age of five years).

Archived audit logs are maintained on the Diagnose > Audit Log > Audit Archive page of the Admin UI.

To maintain a secure audit trail, no other user (including the members of the admin group) can remove audit logs. Additionally, only the audit user can change his or her password. The audit group provides the preconfigured set of access privileges for the audit user. The audit group cannot be modified or removed, and no other users can be added to the group.

For more information about audit logging, including rotation, archiving and deletion, see the *Brocade Virtual Traffic Manager: User's Guide*.

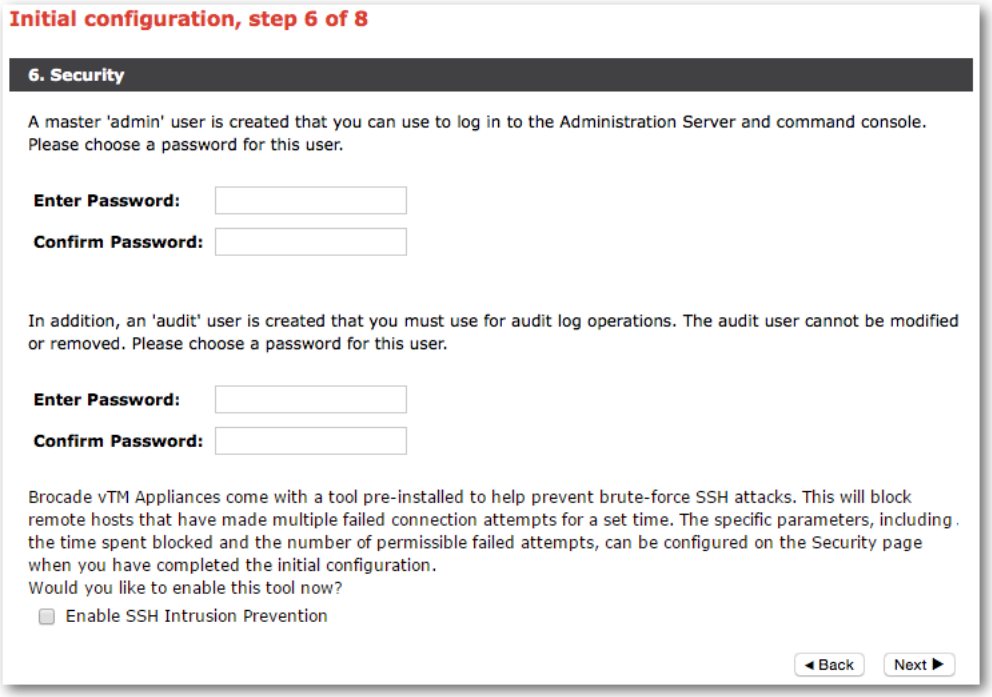
### Setting the Admin User and Audit User Password

You set the audit user password when you use the Initial Configuration Wizard.

Step 6 of the Initial Configuration Wizard allows you to set the password for both the admin and audit users. Enter and then confirm the Admin and Audit user passwords in the fields shown.

The Traffic Manager also contains the option to enable SSH Intrusion Detection to help prevent brute-force SSH attacks on your virtual appliance. Brocade strongly recommends you enable this option.

**Figure 5-1. Entering Your System Security Settings**



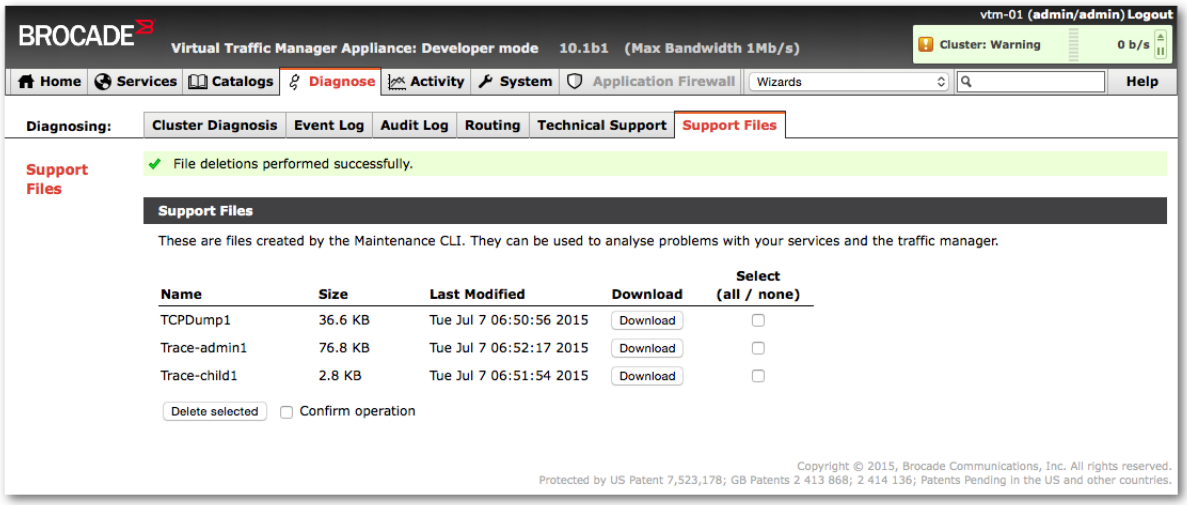

## Features on the Diagnose Page

The Diagnose page contains two tabs with functionality that can be used for troubleshooting system errors on the Traffic Manager Virtual Appliance: the Support Files tab, and the Technical Support tab.

## Support Files Tab

The Support Files tab lists TCP dumps and trace files created by the Maintenance CLI. These files can be used to analyze and troubleshoot virtual appliance system performance issues.

**Figure 5-2. The Support Files Tab**




## Technical Support Tab

Use the functionality of the Technical Support tab to generate the Technical Support Report.

The Technical Support Report includes system traces and TCP dumps. These system traces and TCP dumps provide detailed process data that your support provider can use to troubleshoot system performance issues. Your support provider can often diagnose the cause of any encountered system performance issues by analyzing various system logs and settings appearing in the Technical Support Report.

The process data is stored in files that you can download using the Diagnose > Support Files page of the Admin UI.

---

**Note:** You can also use the Maintenance CLI to generate system traces and TCP dumps. For more information about the Maintenance CLI, see "Using the Maintenance CLI (Command-Line Interface)" on page 15.

---