

CS–MARS: Troubleshooting Technotes

Document ID: 99790

Introduction

Prerequisites

Requirements

Components Used

Conventions

Problem: Error Message When Adding a Device

Solution

Problem: Blank Pop–up Screen Appears While Device is Added

Solution

Problem: MARS Drops Rules

Solution

Problem: CSM MARS Integration Cross Launch Issue

Solution

Problem: NFS Archiving Not Working

Solution

Problem: Oracle Database Corrupted

Solution

Problem: Unable to Add Device with a Seed File

Solution

Problem: System Rule: Inactive CS–MARS Reporting Device

Solution

Problem: Error Within Export of the Device Configuration

Solution

Problem: Unable to Reset the Password in CS–MARS

Solution

Problem: Local Controller does not Sync Properly with Global Controller

Solution

Problem: Error When Importing the Configuration from Version 4.3.6 to 6.0.2 in CS–MARS

Solution

Problem: Configuration Import Fails from Version 6.0.1(2990) to Mainline Release 6.0.3(3188) in CS–MARS

Solution

Problem: Unable to Configure Email Alerts on MARS for all Severity Level RED Rules

Solution

Problem: MARS Auto Signature Update Feature does not Work

Solution

Problem: Unable to Configure MARS for NetFlow

Solution

Problem: CS–MARS Reports Multiple Destinations as Port 0

Solution

Problem: CS–MARS has Events that Report Source as 0.0.0.0 Port 0

Solution

Problem: program aborted due to: ORA–01033: Oracle initializing or shutdown in progress.

Solution

Problem: Unable to Back up Only the Configuration in CS–MARS

Solution

Problem: Upgrade the Software with DVD

Solution

Problem: Unable to Run the raidstatus Command

Solution

Problem: Unknown Reporting Device IP

Solution

Problem: Error While Downloading the Update Package on CS-MARS

Solution

Related Information

Introduction

This document describes the error messages in the Cisco Security Monitoring, Analysis, and Response System (CS-MARS).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Secure MARS Version 4.2x/5.2x.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Problem: Error Message When Adding a Device

This error message appears in CS-MARS when you try to add a device such as a Cisco IOS router or switch:

```
ssh_rsa_verify: n too small: 512 bits
key_verify failed for server_host_key
```



Solution

Use this solution in order to resolve the problem.

The cause for this error message is due to a 512-bit key that is generated by a router (device), but MARS expects a 1024-bit or higher key.

In order to resolve this issue, zeroize the key and generate a 1024-bit key in the router:

```
Router#config terminal
Router(config)#crypto key zeroize rsa
Router(config)#crypto key generate rsa general-keys modulus 1024
```



Warning: Cisco recommends that you use labeled key pairs instead of the default key pairs because the zeroizing of the default key pairs can lead to VPN tunnel termination. It can also affect the Certificate Authority (CA) data that relies on your default keys, for example:

```
Router(config)#crypto key generate rsa general-keys label sshkey modulus 1024 exportable
Router(config)#ip ssh rsa keypair-name sshkey
```

Refer to the Cisco IOS Security Command Reference for more information.

Problem: Blank Pop-up Screen Appears While Device is Added

When you try to add a device in the CS-MARS, a blank pop-up screen appears. This occurs only when you use the Internet Explorer version 7 browser.

Solution

This is a known issue with Internet Explorer version 7, and the blank pop-up screen does not have any impact on the functionality. You can close the blank screen and continue to add devices. Internet Explorer version 6 or any other browser to avoid the blank pop-up screen issue.

Problem: MARS Drops Rules

After you upgrade from version 6.0.2 to 6.0.3, it appears that drop rules are ignored.

Solution

Update your MARS with the patch release 6.0.3 (3188) (csmars-6.0.3.3190-customerpatch.zip) in order to correct the potential issues with drop rules.

Problem: CSM MARS Integration Cross Launch Issue

An internal error has occurred. Please close all the browser windows and ensure that the specific device is added and submitted in Cisco Security Manager (CSM)

Solution

The problem occurs when the alerts that are generated from the firewalls use names, not IP addresses, and the CSM MARS integration does not support firewall alerts that use names.

In order to resolve this issue, issue the **no names** command on the firewall to enable the cross launch feature for all firewall alerts.

Problem: NFS Archiving Not Working

You might receive the "Invalid remote IP or path" error while NFS archives.

Solution

In order to resolve the issue, change the privilege level on the window server or re-start the services.

Refer to Configure the NFS Server on Windows for more information about how to configure NFS. Refer to Enable Logging of NFS Events for more information about how to enable logging.

Problem: Oracle Database Corrupted

You might receive this error message if your Oracle database is corrupted:

Program aborted due to: ORA-01034: ORACLE not available

ORA-27101: shared memory realm does not exist

Linux Error: 2: No such file or directory

Solution

In order to resolve this issue, re-image the MARS appliance. For more information on how to re-image MARS, refer to Re-Imaging a Local Controller.

Problem: Unable to Add Device with a Seed File

When you try to add a device with a seed file in the CS-MARS, an error message appears.

Solution

This occurs when the seed file is not saved in the comma separated value (CSV) format. You must save the seed file as a true CSV file. Do not save the file as a Microsoft Excel file (.xls file); MARS cannot interpret a Microsoft Excel formatted .xls file and will hang while it uploads the seed data. CS-MARS needs this data in the form of a true comma-separated value file. Refer to Add Multiple Reporting and Mitigation Devices Using a Seed File for more information on how to set up a seed file.

Problem: System Rule: Inactive CS-MARS Reporting Device

Mars reports this rule:

System Rule: *Inactive CS-MARS Reporting Device. And did not receive syslog.*

Solution

This rule detects reporting devices that have not reported an event in the past hour. For chatty devices, such as firewalls and IDS, this error can indicate connectivity issues or an issue with the device itself. This rule must be scoped down to include only chatty network infrastructure devices.

Problem: Error Within Export of the Device Configuration

When you try to export the device configuration, the process seems to run, but there is no configuration file on the SFTP server, just an empty folder that the process created. You might also receive the *Error: failed to save file to the remote host* message.

Solution

Check that the account you use has write access. Cisco recommends that you use the Cygwin SFTP Server on Windows.

The Cisco Security MARS supports SFTP servers as a storage medium to archive or to migrate data from 4.x to 6.0.1. Refer to *Configure the Cygwin SFTP Server on Windows* for information on how to configure the Cygwin and OpenSSH on Windows. It targets the Cygwin SFTP server on Windows XP.

Problem: Unable to Reset the Password in CS-MARS

You are unable to reset the password in CS-MARS.

Solution

Use *pnadmin* as the user name and password. If this does not work, the only way to reset the password on a MARS sensor is to use the recovery DVD, which basically reimages the appliance. Make sure you have your license key written down before you use the recovery CD/DVD. Refer to *Recovering a Lost Administrative Password* for more information on how to reset the password on CS-MARS.

Problem: Local Controller does not Sync Properly with Global Controller

The Local Controller (LC) does not synchronize properly with the Global Controller (GC).

Solution

Make sure that both the LC and GC have the same signature. The LC and GC must have the same signature in order for them to synchronize without any issues.

Problem: Error When Importing the Configuration from Version 4.3.6 to 6.0.2 in CS-MARS

You might receive the `Configuration import failed with error code: 111` error when you import a configuration from version 4.3.6 to 6.0.2 in CS-MARS.

Solution

The configuration can be imported from the CS-MARS version 4.3.6 to version 6.0.1 only; it cannot be imported to 6.0.2. In order to resolve this issue, import the configuration from 4.3.6 to 6.0.1 and then re-image CS-MARS to 6.0.2.

Problem: Configuration Import Fails from Version 6.0.1(2990) to Mainline Release 6.0.3(3188) in CS-MARS

You might receive this error when you import a configuration from version 6.0.1 to 6.0.3 in CS-MARS:

```
File gen_or_06_0_13.sql missing from schema.  
Configuration import failed with error code: 1  
Configrestore failed!  
Error: failed to import config data
```

Solution

If you use the **pnexp** and **pnimp** commands, the configuration is backed up and restored only to the same MARS version. The only exception is migrating from version 4.x to version 6.0.1; this procedure does not work for migrating from version 6.0.1 to version 6.0.3.

You must reimage MARS with the original 6.0.1 version again (the version from which you previously ran the **pnexp** command), restore configuration with **pnimp**, and then complete two sequential upgrades with the **pnupgrade** utility: 6.0.1 to 6.0.2 and then 6.0.2 to 6.0.3.

Problem: Unable to Configure Email Alerts on MARS for all Severity Level RED Rules

You are unable to configure email alerts on MARS for all severity level RED rules.

Solution

It is not possible to configure email alerts for all severity level RED rules in one step. You must configure email alerts on a per-rule basis. Create a custom rule (Rules > Add), and then choose **any** for all parameters except severity. For the severity parameter, choose **RED**, and set an action to email to configure email alerts on MARS for all severity level RED rules. Refer to Configure a Rule to Send an Alert Action for more information.

For more information, refer to Cisco bug ID CSCse89349 (registered customers only) .

Problem: MARS Auto Signature Update Feature does not Work

The auto signature update feature in MARS does not work if you use a proxy or proxy/caching server in order to access the Internet.

Solution

MARS is unable to download dynamic IPS signature updates if you use a proxy or proxy/caching server to

access the Internet. If you use a proxy/caching server, you can manually download the signature update files from this URL: <http://www.cisco.com/cgi-bin/tablebuild.pl/mars-ips-sigup> (registered customers only) . Refer to IPS Signature Dynamic Update Settings for more information about auto signature updates in MARS.

Problem: Unable to Configure MARS for NetFlow

You encounter issues after you configure MARS for NetFlow.

Solution

NetFlow is a Cisco technology that supports monitoring network traffic and is supported on all basic Cisco IOS images. MARS collects the NetFlow that is sent from the reporting device, and it provides various levels of functionality (dependent upon whether you store it to the database). If stored, NetFlow can be queried, and you can have reports, rules, and incidents for it. Refer to Understanding NetFlow Anomaly Detection for more information on how to configure MARS for NetFlow and how NetFlow works. Also refer to Taskflow for Configuring NetFlow Security Event Logging (NSEL) on MARS for more details on NetFlow configuration.

Problem: CS-MARS Reports Multiple Destinations as Port 0

CS-MARS reports multiple destinations as port 0. The destination port is 0, and sometimes the destination IP address is 0.0.0.0.

Solution

This is expected CS-MARS behavior since some event types of reporting devices report multiple destination ports or IP addresses. MARS simply consolidates this information into a single value (0). If you are concerned about the data reported to MARS that triggered this behavior, you can run an *All Matching Events Raw Messages* type query against one or more of the reporting devices that triggered this behavior in order to see the information that was reported to MARS, which includes the multiple designation ports or IP addresses. All Matching Events Raw Messages with raw events displays Event ID, Event Type, Time, Reporting Device, and Raw Message fields.

Problem: CS-MARS has Events that Report Source as 0.0.0.0 Port 0

CS-MARS has some events events that report the source as 0.0.0.0 port 0.

Solution

In CS-MARS, the IP address 0 . 0 . 0 . 0 means that there is no information for this field. This is a convention used within CS-MARS. IP addresses and ports of 0 . 0 . 0 . 0 and 0 respectively show up in two cases:

1. Those that were not specified in the syslog
2. Those that have multiple values (2 or more IPs or ports)

Problem: program aborted due to: ORA-01033: Oracle initializing or shutdown in progress.

This error occurs when you try to start or stop the service with the **pnstart** or **pnstop** commands at the CLI in CS-MARS: program aborted due to: ORA-01033: Oracle initializing or

shutdown in progress.

Solution

This error can be resolved if you re-image the CS-MARS followed by the configuration import.

Problem: Unable to Back up Only the Configuration in CS-MARS

You are unable to back up the device configuration without data in CS-MARS.

Solution

You can archive data from a MARS appliance and use that data to restore the operating system (OS), system configuration settings, dynamic data (event data), or the complete system. The appliance archives and restores data to and from an external network-attached storage (NAS) system with the network file system (NFS) protocol. After you archive all data and device configurations, restore only the device configuration information so that only the device configuration is restored. Refer to *Configuring and Performing Appliance Data Backups* for more information on appliance data backup in CS-MARS.

Problem: Upgrade the Software with DVD

You are unable to upgrade the image with DVD in CS-MARS.

Solution

CS-MARS does not recognize the DVD as a recovery image. In order to resolve the issue, burn the CD at **4x speed**. Refer to *Downloading and Burning a Recovery DVD* for more information on appliance software upgrade with DVD in CS-MARS.

Problem: Unable to Run the raidstatus Command

You are unable to run the **raidstatus** command in CS-MARS.

Solution

CS-MARS does not support the **raidstatus** command in the lower-end models – 20 or 50. Only for models 100, 100E, and 200 is this command supported.

Problem: Unknown Reporting Device IP

Devices report as *Unknown Reporting Device IP* in the MARS system.

Solution

This problem is due to CS-MARS tags event data since it is received based on the source IP address from which it came, and then it performs a lookup in its configuration (which matches the source IP address to a configured reporting device). If no match is found, the device is tagged as "Unknown Reporting Device IP," which means that the user has not configured MARS to recognize all requirements for MARS to be able to parse/understand event data, such as the type of device of the IP address and the version of software/code it

runs.

In order to verify, note the IP address or addresses in question, and navigate to **ADMIN > System Setup > Security and Monitor Devices page** in the MARS GUI. Verify that the same IP address or addresses are not listed. Once verified, add a proper reporting device (and every other network device that shows as *Unknown*) in order to correct this issue.

Problem: Error While Downloading the Update Package on CS-MARS

You might receive this error when you download the update package on CS-MARS:

```
Cisco.com Package List\n An error occurred while accessing Cisco.com: An error occurred accessing Cisco.com. Error Code: ERR_INTERNAL
```

Solution

This error occurs when full outbound access to *origin-www.cisco.com* (via *HTTPS/443*) and *software-sj.cisco.com* (via *HTTP/80*) is not configured on the firewall. In order to resolve this issue, make sure the firewall (if present) is configured in order to allow full outbound access to *origin-www.cisco.com* (via *HTTPS/443*) and *software-sj.cisco.com* (via *HTTP/80*).

Related Information

- [Cisco Security Monitoring, Analysis and Response System – Compatibility Information](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 13, 2009

Document ID: 99790
