CS−MARS: Troubleshooting Technotes

Document ID: 99790

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Error Message when Adding a Device
Problem
Solution
Blank Pop−up Screen Appears While Device is Added
Problem
Solution
MARS Drops Rules
Problem
Solution
CSM MARS Integration Cross Launch Issue
Problem
Solution
NFS Archiving Not Working
Problem
Solution
Oracle Database Corrupted
Problem
Solution
Unable to Add Device with a Seed File
Problem
Solution
Unable to Connect to Device
Problem
Solution
Error when Pulling Logs from Windows
Problem
Solution
System Rule: Inactive CS−MARS Reporting Device
Problem
Solution
Error Within Export of the Device Configuration
Problem
Solution
Unable to Reset the Password in CS−MARS
Problem
Solution
Local Controller Does Not Sync Properly with Global Controller
Problem
Solution
Error when Importing the Configuration from Version 4.3.6 to 6.0.2 in CS−MARS
Problem

Solution
Error when Importing the Configuration from CS−MARS Version 6.0.4
Problem
Solution
Error: Configuration error: host name does not match janus.conf::janusBoxName.
Problem
Solution

Configuration Import Fails from Version 6.0.1(2990) to Mainline Release 6.0.3(3188) in CS−MARS
Problem
Solution
Unable to Configure Email Alerts on MARS for all Severity Level RED Rules
Problem
Solution
MARS Auto Signature Update Feature Does Not Work
Problem
Solution
Unknown Device Event Type
Problem
Solution
Unable to Configure MARS for NetFlow
Problem
Solution
CS−MARS Reports Multiple Destinations as Port 0
Problem
Solution
CS−MARS Events Report Source as 0.0.0.0 Port 0
Problem
Solution
program aborted due to: ORA−01033: Oracle initializing or shutdown in progress.
Problem
Solution
Unable to Back Up Only the Configuration in CS−MARS
Problem
Solution
Upgrade the Software with DVD
Problem
Solution
Unable to Run the raidstatus Command
Problem
Solution
Unknown Reporting Device IP
Problem
Solution
Error Received when Downloading the Update Package on CS−MARS
Problem
Solution
Unable to Add an FWSM in CS−MARS
Problem
Solution
NTLMv2 Does Not Work with CS−MARS
Problem
Solution
CS−MARS Crashes with the "kernel panic 5" Console Message

Problem
Solution
Error on CS−MARS During Boot Up
Problem
Solution
Error on CS−MARS During Device Upgrade
Problem
Solution
MARS GUI Navigation is Slow After Upgrade From 5.x to 6.0(4)
Problem
Solution
Reports do not Export to Other Applications
Problem
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

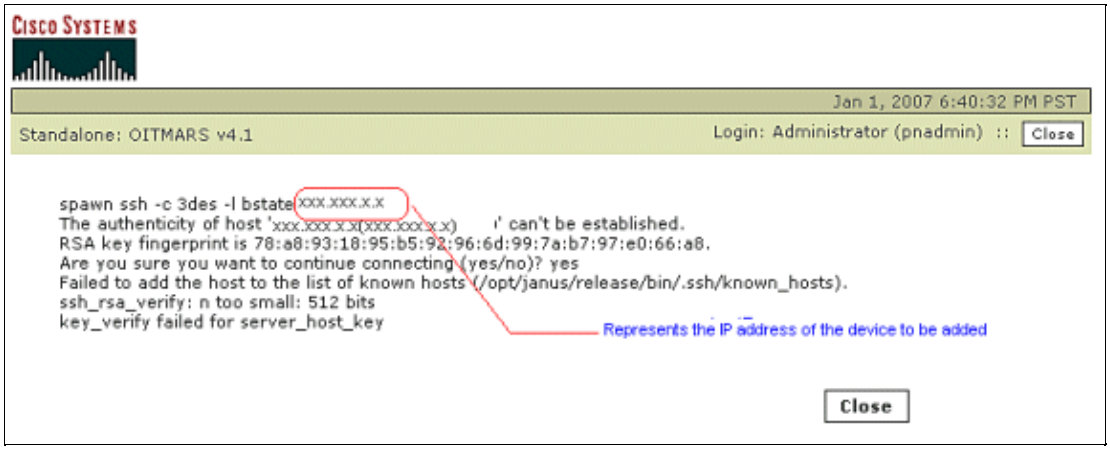
Refer to Cisco Technical Tips Conventions for more information on document conventions.

Error Message when Adding a Device

Problem

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.

Blank Pop−up Screen Appears While Device is Added

Problem

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.

MARS Drops Rules

Problem

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.

CSM MARS Integration Cross Launch Issue

Problem

You receive this error message: `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

This 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.

NFS Archiving Not Working

Problem

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.

Oracle Database Corrupted

Problem

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.

Unable to Add Device with a Seed File

Problem

When you try to add a device with a seed file in the CS−MARS, this error message appears:

```
Status: Errors occured while retrieving csv file from ftp server.
```

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.

Unable to Connect to Device

Problem

You might receive this error when you are unable to access a 3550 switch from MARS:

```
spawn ssh −c 3des −l marssys 10.15.110.16
The authenticity of host '10.15.110.16 (10.15.110.16)' can't be established.
RSA key fingerprint is ca:d6:ca:2c:ea:09:d6:2c:e2:78:d5:97:b6:f6:de:a5.
Are you sure you want to continue connecting (yes/no)? yes
Failed to add the host to the list of known hosts
(/opt/janus/release/bin/.ssh/known_hosts).
ssh_rsa_verify: n too small: 512 bits
key_verify failed for server_host_key
```

Solution

This error occurs if the modulus setting on the ssh key in the switch is set to 512; the value should be higher.

Error when Pulling Logs from Windows

Problem

When you pull logs from the backend, you might receive this error: `Thread 3075656624:winpull: repeated error pulling from 10.1.1.52, look in backend log for full info of the error`

Solution

This error occurs when the learned windows account used to pull event logs does not have the rights for the MARS account on the server.

System Rule: Inactive CS−MARS Reporting Device

Problem

Mars reports this rule:

System Rule: *Inactive CS−MARS Reporting Device. And did not receive syslogs.*

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.

Error Within Export of the Device Configuration

Problem

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.

Unable to Reset the Password in CS−MARS

Problem

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.

Local Controller Does Not Sync Properly with Global Controller

Problem

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.

Error when Importing the Configuration from Version 4.3.6 to 6.0.2 in CS−MARS

Problem

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.

Error when Importing the Configuration from CS−MARS Version 6.0.4

Problem

You might receive the `Error: no configuration archive found. This tool only supports importing configuration archive generated by 4.3.1 release or later with the exception of 5.x.x releases.` error when you import a configuration from version 4.x to 6.0.4 in CS−MARS.

Solution

The configuration can be imported from the CS−MARS version 4.x 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.x to 6.0.1 and then re−image CS−MARS to 6.0.4.

Refer to Migrating Data from Cisco Security MARS 4.x to 6.0.X for more information on migration of CS−MARS.

Error: Configuration error: host name does not match janus.conf::janusBoxName.

Problem

You might receive this error after you upgrade CS−MARS:

```
Error: Configuration error: host name does not match
janus.conf::janusBoxName. Please contact Cisco for support.
```

Solution

This error is due to the Cisco bug ID CSCsh82939 (registered customers only) . In order to avoid this issue in future it is recommend to change the hostname to the original hostname instead running pnrestore on new default "hostname" both after the re−image and before the pnrestore,

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

Problem

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.

Note: Data restore from a larger model to a smaller model of CS−MARS is not supported. For example, you cannot restore data from Mars 100 to MARS 50.

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

Problem

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) .

MARS Auto Signature Update Feature Does Not Work

Problem

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. You might receive this error message during auto signature update: `unable to connect to the server, please check the URL,User name and password`

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.

Unknown Device Event Type

Problem

CS−MARS reports this error during higher signature update: `Unknown Device Event Type`

Solution

CS−MARS has a higher signature update than the sensors; no issue in parsing should arise. However, if the sensor has a higher signature update than CS−MARS, CS−MARS might generate an *Unknown Device Event Type* error as the CS−MARS cannot directly parse the newer signatures; raw event data will still be present. There should be performance impact to CS−MARS outside potentially non−descript event messages.

Note: Custom signatures are categorized as "Unknown Device Event Type" events in CS−MARS; however, signature look−up functions as expected.

Unable to Configure MARS for NetFlow

Problem

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.

CS−MARS Reports Multiple Destinations as Port 0

Problem

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.

CS−MARS Events Report Source as 0.0.0.0 Port 0

Problem

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)

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

Problem

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.
```

This error message indicates that the database has crashed.

Solution

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

Unable to Back Up Only the Configuration in CS−MARS

Problem

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.

Upgrade the Software with DVD

Problem

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.

Unable to Run the raidstatus Command

Problem

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.

Unknown Reporting Device IP

Problem

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.

Error Received when Downloading the Update Package on CS−MARS

Problem

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)*.

Unable to Add an FWSM in CS−MARS

Problem

You are unable to add an FWSM in CS−MARS.

Solution

Before you can add an FWSM module in a switch, you must add and configure the base module (the Cisco switch) in MARS. Refer to Configuring Cisco Firewall Devices for more information.

NTLMv2 Does Not Work with CS−MARS

Problem

You are unable to use NTLMv2 with CS−MARS.

Solution

NTLMv2 is not supported on CS−MARS; therefore, you are unable to use NTLMv2 with CS−MARS.

CS−MARS Crashes with the "kernel panic 5" Console Message

Problem

CS−MARS crashes with the `kernel panic 5` message on the console. The message includes this information: `CET Fatal ./csips Thread 62385072:Exiting the process as OUT_OF_MEMORY returned by CURL. superV will restart the process.`

Solution

Usually, this issue is seen together with a high memory usage on the CS−MARS appliance. Running a command to show system inventory information can trigger this issue. For more information, refer to Cisco bug ID CSCsm40349 (registered customers only) .

Error on CS−MARS During Boot Up

Problem

You might receive this error when CS−MARS boots up:

```
/dev/hda2 UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY.
```

Solution

Re−image the CS−MARS device in order to resolve this issue. You can also try to run **fsck** manually before you re−image the device.

Refer to Re−Imaging a Local Controller for more information on how to re−image the CS−MARS device.

Error on CS−MARS During Device Upgrade

Problem

You might receive this error when you upgrade csmars−6.0.2.2102.30 to csmars−6.0.3.3188.32:

```
[Error][check_dependency/541]: minimal allowed version(6.0.2.3102.31) >
current version(6.0.2.3102.30)
```

Solution

This error might occur if the data version was not properly updated during a previous version upgrade.

In order to resolve this issue, perform the upgrade to 6.0.2 from the CLI. The software version upgrade is skipped, but the data version upgrade is performed. You can then upgrade to version 6.0.3.

Verify your current version with the **version** CLI command

Refer to Upgrade from the CLI for more information on how to upgrade the CS−MARS device.

MARS GUI Navigation is Slow After Upgrade From 5.x to 6.0(4)

Problem

You might experience performance issues with the MARS GUI after you upgrade from 5.3.1 to 6.0.

Solution

Upgrade to version 6.0.6 in order to resolve this issue.

Reports do not Export to Other Applications

Problem

You are not able to export reports from MARS in a presentable format, such as PowerPoint, PDF, Word, or Excel.

Solution

CS−MARS does include functionality to export reports to other applications. CS−MARS supports only these two types of formats for reports:

- Comma−separated values (CSV)
- HTML

Note: If you chose to view the report as a CSV file, you need to save the file to your computer, and open the CSV file in a third−party application. For more information, refer to Operations on Existing Reports.

Related Information

- **Cisco Security Monitoring, Analysis and Response System − Compatibility Information**
- **Troubleshooting CS−MARS fsck issues**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 13, 2009 Document ID: 99790