Top Issues for the Cisco Security Monitoring, Analysis, and Response System

Last Updated: July 23, 2009

This document identifies common issues and customer questions about the Cisco Security Monitoring, Analysis, and Response System (MARS). It also provides pointers to newly documented topics as they become available, focusing more on the topic rather than a version-specific compendium. While the content identified in this document is presumably targeted to the latest release, many configuration operations apply to earlier releases as well. For device support by release, refer to the Supported and Interoperable Devices and Software list:

http://www.cisco.com/en/US/products/ps6241/products_device_support_tables_list.html

Getting Started

This section identifies topics that assist in getting your MARS Appliance up and running.

Hardware Installation Overview

The following topic provides a quick overview of the tasks you must perform to install the appliance in a rack.

- Installation Quick Reference

Initial Hardware Configuration Checklist

The following topic identifies the process required to deploy and initially configure the appliance, bringing it online within your network.

- Checklist for Initial Configuration

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Client Configuration

The following topic identifies proper client configuration so that you can access the MARS HTML interface.

- Web Browser Client Requirements

Task Flow Overview

The following topic outlines the expected flow for configuring the appliance and the reporting and mitigation devices that it monitors. Review this document after the appliance is installed and running on the network.

- STM Task Flow Overview

Device Configuration

This section organizes topics that address configuration of the reporting devices.

Adding CheckPoint Devices as Reporting Devices

The following topic presents the task flow and procedures for configuring CheckPoint devices in MARS.

- Check Point Devices

Getting Logs from Windows Hosts

The following topic includes detailed procedures for pulling events from Windows hosts, as well as updated information on configuring SNARE agents. It discusses advantages and disadvantages of these two methods.

- Microsoft Windows Hosts

Note It is possible to represent a Windows XP-based host. To do so, select the Windows 2003 option when defining the host details in the MARS user interface. Also, if you intend to pull logs from a Windows XP Home Edition host, you must enable RPC on the host.

NetFlow Configuration Update

The following topic explains how to configure NetFlow for Cisco Routers and Switches and how MARS uses this information to detect anomalies in network traffic.

- Understanding NetFlow Anomaly Detection

ACS Configuration and Appliance Support

The following topics explain how to configure the Cisco ACS server, how to configure a relay host to support the Cisco ACS Solution Engine, how to download, install, and configure the pnLog agent, and how to configure MARS to receive the logs forwarded by the pnLog agent.

- Supporting Cisco Secure ACS Server
- Supporting Cisco Secure ACS Solution Engine
- Install and Configure the PN Log Agent

Deleting, Re-adding, Renaming a Device

The following topic explains how to delete a device so that you can add a new reporting device with the same IP address.

- Delete a Device

Global Controller Configuration

The following topic highlights the key tasks to perform to configure a Global Controller to communicate with one or more Local Controllers, and provides the expected order of those tasks.

- Configuring the Global Controller

Appliance Maintenance

These topics address the maintenance and recovery of the MARS Appliance.

Upgrade Package Download Changes

MARS Appliance releases 6.0.1/6.0.2/6.0.3 contain a feature that automatically populated the availablity of software updates and simplified their downloading from the MARS GUI. Due to recent infrastructure changes, that feature no longer operates.

Downloading new upgrade packages must now be accomplished by a more manual method.

Upgrade images and supporting software are found on the CCO software download pages dedicated to MARS. You can access these pages at the following URLs, assuming you have a valid CCO account and that you have registered your SMARTnet contract number for your MARS Appliance.

Top-level page:

http://www.cisco.com/go/mars/

Click the **Download Software** link in the Support box on the right side of the MARS product home page.

Result: The Download Software page loads.

From this top-level page, you can select one of the following options:

- CS-MARS IPS Signature Updates Archives

- CS-MARS IPS Signature Updates
- CS-MARS Patches and Utilities (supplementary files)
- CS-MARS Recovery Software
- CS-MARS Upgrade Packages

If you are upgrading from a release earlier than those posted on CCO, please contact Cisco support for information on obtaining the required images. Do not attempt to skip releases along the upgrade path.

For information on obtaining a CCO account, see the following URL:

http://www.cisco.com/en/US/applicat/cdcrgstr/applications_overview.html

NFS Server Configuration

Configuring NFS servers on Linux and Windows servers requires specific, detailed information. This section discusses the file format expected on the NFS server and new procedures for configuring Windows servers. It also includes some key syntax changes in the Linux configuration example and removes references to Solaris support. We are currently discovering the information required to configure NFS on Solaris, at which time we will release updated documentation with a configuration example.

- Configuring and Performing Appliance Data Backups

Backup and Restore

Archiving and restoring data is an important operation. While there isn't documentation specific to this operation, we can piece it together from the backup and recovery procedures.

Backup

- Configuring and Performing Appliance Data Backups

Restore CLI

- pnrestore

Restore Overview

- Restoring Archived Data after Re-Imaging a MARS Appliance

Restore Guidelines

- Guidelines for Restoring

Upgrade vs. Re-image

Customers who are running versions that are two or more releases behind the current release are often puzzled by the incremental upgrade path. The question arises, “Why can't I just back up, re-image the appliance, and then restore the data on the newer image?” Several potential issues prevent this from being a valid solution. First, only the configuration data can be backed up completely. Event data is backed up only from the point at which you enable backup. In other words, if you have 8 days of data and you turned on archiving on day 6, the only data that is archived is the last two days. Second, the database table structures can change between releases, which means the restore operation might result

in restoring an older database table into a newer table structure, which can cause database corruption and data loss. The database table migrations are addressed by the upgrade process, which is one reason why upgrades can take so long. The upgrade process converts all old data to the new structure.

So when does it make sense to re-image rather than upgrade? The answer is simple, when you do not want to preserve any configuration and event data. In this case, you start with a clean system, and re-imaging can be much faster than following a multi-path upgrade.

Upgrade

- Checklist for Upgrading the Appliance Software

Re-image

- Recovery Management

View and Query Archived Data

When you archive data in MARS, you are really backing up that data. That data is backed up using a compressed format that can only be accessed manually by uncompressing the file and analyzing the raw message logs. You can pull raw message logs from the archive without configuring a second appliance. This log format is detailed, ordered according to message timestamp, and unable to be queried using the sophisticated query features found in MARS. However, once uncompressed, the logs are in ASCII, which allows you to search these logs using `grep' or custom scripts developed on an administrative computer.

If you prefer the powerful query options found in MARS, you must configure a secondary appliance that is dedicated to reviewing archived logs. In other words, you can query across the archived data using scripts and string matching, but you cannot define a query as you would in MARS unless you restore that data to an appliance. If you need to manipulate data in this fashion, we recommend purchasing a model that is the same or larger than the model that is archiving the data. You must restore the data range in which you are interested, and then perform the query as you normally would. Issues arise when you restore the configuration data, such as conflicting devices on the network. Therefore, we recommend that you restore this data on an isolated network that can access the NFS backup server.

Raw Message Logs

- Retrieving Raw Messages

Restore an Archived Image

- Restoring Archived Data after Re-Imaging a MARS Appliance

Secondary Server Guidance

- Configuring a Standby or Secondary MARS Appliance

Restore Guidelines

- Guidelines for Restoring

Raw Message vs. Archive File Message Formats

The data that is returned from raw message is simply the audit message provided by the reporting device. The archive file includes the raw message and the system data required to correlate that message with the session, device type, five tuple (source IP, destination IP, protocol, source port, and destination port), and all other data points. The raw message is just the message as sent by the reporting device, such as a syslog message.

Password Recovery

Recovering a lost password does not come without costs. However, this issue is seen primarily for appliances that have changed hands or have been inactive for some time. The answer to this problem is to re-image the appliance, thereby restoring the original factory default password. This approach resets both the pnadmin password and the user-provided portion of the expert mode password to the factory installed defaults.

We recommend downloading the latest ISO image and re-imaging with that ISO image. For more information, see:

- Recovering a Lost Administrative Password

Issues and Discussion

The topics in this section are ones that frequent mailing lists and bulletin boards regarding MARS.

Standby Servers

The concept of high-availability is one that most enterprise-level customers consider important. While MARS does not support automatic failover to a second appliance, you can configure a standby or “hot swap” server that shares the configuration and event data of the primary appliance. We discuss the expected configuration in the following sections of the *Install and Setup Guide for Cisco Security Monitoring, Analysis, and Response System*:

- Configuring a Standby or Secondary MARS Appliance
- Guidelines for Restoring

License Keys

One of the most common asked questions is that of locating a lost license key. For MARS Appliance models sold running release 3.4.3 and later (post May 2005), the license key is included on the chassis of the actual appliance. For more information on locating your license key on the chassis, see Locating the License Key (Gen2 appliances), or Locating the License Key (Gen1 appliances).

In June 2009, the Disk on Module (DOM) memory device in all CS-MARS 25R, 25, and 55 models was updated, which created a condition in some MARS appliances where the Cisco-supplied license key would not be accepted when the appliance was installing or running a software version prior to Release 6.0.3.

A workaround to this problem is posted at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/troubleshooting/tshot25_55_603.html

Tiny URL: http://tiny.cc/pNEZ9

Topology Discovery

In MARS, topology discovery has several responsibilities:

- Automatically discover reporting devices and mitigation devices.
- Discover and populate the network topology for use in the Layer 3 topology graphs on the Network Summary page.
- Pull event data periodically from specific types of reporting devices, including Qualys QualysGuard, eEye REM, FoundStone FoundScan, and Check Point log servers.

However, it is important to understand how the actual discovery process works. The following topics discuss each of the responsibilities and provide more detail on how the discovery process works:

- Adding Reporting and Mitigation Devices Using Automatic Topology Discovery
- Configuring Layer 3 Topology Discovery
- Scheduling Topology Updates

Syslog Forwarding

The MARS Appliance does not support direct syslog forwarding; it cannot relay syslog events that it receives from reporting devices to other syslog servers for further processing. However, you can configure inspection rules so that when parsed events fire a rule, then a syslog notification is generated and sent to any syslog servers you have identified. For information on defining this type of notification method, see Setting Alerts and Sending Alerts and Notifications.

Event Timestamps and Processing

To understand event timestamps, let's clarify our terminology:

- *MARS time* is the time on the MARS Appliance
- *device time* is the time on the reporting device when an event was generated

The MARS system processes events from multiple reporting devices. Various methods are used to obtain events from those devices, including syslog, SNMP traps, SDEE/RDEP, SNARE agent, pulling from Windows hosts, and pnLog agent. Broadly, we can separate these methods into two categories:

- **Passively received events.** The reporting device publish events to MARS Appliance, which simply listens on standard ports for any and all events. The methods used to passively receive events include syslog, SNMP traps, SNARE agent, and pnLog agent.
- **Actively pulled events.** The MARS Appliance actively contacts the reporting device, according to a predefined schedule, and pulls the event logs and data from the reporting device. The methods used to actively pull events include SDEE/RDEP, Windows pulling, and Oracle pulling.

How MARS processes the events and which timestamp is used varies based on the category:

- **Processing passively received events.** The MARS Appliance takes the MARS time at the instant it is processing the event and timestamps the event. This is the only time MARS attaches to the event. So, in a session, the event with the earliest time is used to denote the start of the session. There is no separate concept of a session time versus incident time.
- **Processing actively pulled events.** MARS extracts the device time from the data in the logs and assigns that time to the events. This method has the following restriction: if the device time is older or newer than 3,600 seconds relative to the MARS time, the MARS time is applied to the event. This occurs primarily when either the pulling interval is too long or when the time on the devices are not synchronized with the MARS Appliance, and it is done to ensure that customers are able to see events in a timely manner.

  As an example, consider the case where a customer has a MARS Appliance pulling events from an IPS device using SDEE. MARS uses the time on the IPS device assuming it is within the 3600 second window. However, if the time on the IPS device is not synchronized with the MARS Appliance and, for example, it is 5 minutes ahead of MARS, when the customer performs a query for events occurring in the last 10 minutes, the most current events will not appear. The customer would need to query for 10 minutes in the future to see the most current events.

In both cases, once a timestamp has been applied to an event, MARS uses that timestamp for all queries and reports. If MARS time is applied in either category and the original event included the device time, the device time for each event is embedded in the raw message. However, it is not used by MARS for queries and reports. You can determine the device time by delving into the details of the raw message via queries, reports, and raw message retrieval.

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available based on category.

Table 1 Product Documentation

Document Category	Available Formats
Documentation Road Maps	• On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/products_documentation_roadmaps_list.html
Quick Install and Release Notes	• On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/prod_release_notes_list.html
Install and Setup Guide	• On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/prod_installation_guides_list.html
Hardware Installation Guide	• On Cisco.com at this URL: http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/hardware/installation/guide/hig_mars_6x.html

Table 1 Product Documentation (continued)

Document Category	Available Formats
User Guides	• On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/products_user_guide_list.html
Device Configuration Guide	• On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/products_installation_and_configuration_guides_list.html
Command Reference	• On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/prod_command_reference_list.html
Supported Devices and Software Versions Tables	• On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/products_device_support_tables_list.html
Regulatory, Compliance, and Safety Information	• On Cisco.com at this URL: http://www.cisco.com/en/US/products/ps6241/prod_installation_guides_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Product Documentation" section.