CS-MARS ：Technotes故障排除

目录

简介

本文描述在Cisco安全监听、分析和答复系统(CS-MARS)的错误消息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据Cisco Secure火星版本4.2x/5.2x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

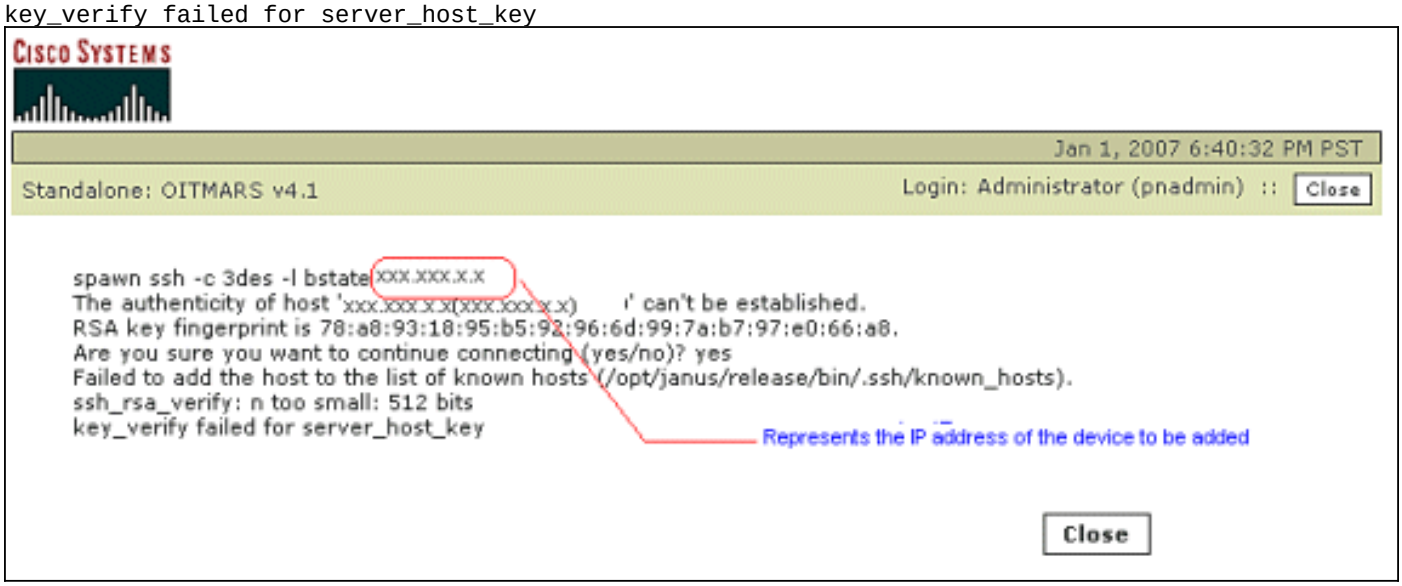
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

错误消息，当添加设备时

问题

当您尝试添加一个设备例如Cisco IOS路由器或交换机时，此错误消息在CS-MARS出现：

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



解决方案

请使用此解决方案为了解决问题。

此错误消息的原因归结于由路由器的512-bit密钥(设备)生成，但是MARS期待一1024位或更高的密钥。

为了解决此问题，调零密钥和生成在路由器的一1024位密钥：

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

警告： Cisco建议您使用被标记的密钥对而不是DEFAULT键对，因为调零DEFAULT键对可能导致VPN隧道终止。例如它能也影响依靠您的默认键的Certificate Authority (CA)数据，：

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

参考Cisco IOS安全命令参考欲知更多信息。

当设备被添加时，空白的上推屏幕出现

问题

当您尝试添加在CS-MARS时的一个设备，一空白的上推屏幕出现。只有当您使用Internet Explorer版本7浏览器时，这发生。

解决方案

这是与Internet Explorer版本7的一个已知问题，并且空白的上推屏幕没有在功能的任何影响。您能关闭空白屏幕和继续添加设备。避免空白的上推屏幕问题的Internet Explorer版本6或其他浏览器。

火星丢包规则

问题

在您从版本6.0.2到6.0.3后升级，看来丢弃规则忽略。

解决方案

更新您的火星用补丁程序版本6.0.3 (3188) (csmars-6.0.3.3190-customerpatch.zip)为了修改与丢弃规则的潜在问题。

CSM毁损集成—发怒启动问题

问题

您将收到以下错误消息：`Cisco Security Manager (CSM)`

解决方案

此问题发生，当从防火墙生成的警报使用名称、IP地址和不是CSM火星集成不支持使用名称的防火墙警报。

为了解决此问题，请发出**no names命令**在防火墙启用所有防火墙警报的发怒启动功能。

归档不工作的NFS

问题

您也许收到“无效远程IP或路径”错误，当NFS存档时。

解决方案

为了解决问题，请改变在Windows服务器的权限级别或重新启动服务。

参考请配置在Windows的NFS服务器关于如何配置NFS的更多信息。如何的更多信息参考NFS事件启用日志关于对启用日志。

损坏的Oracle数据库

问题

如果您的Oracle数据库是损坏的，您也许收到此错误消息：

程序中止的由于：ORA-01034 ：不可用的ORACLE

ORA-27101 ：共享内存领域不存在

Linux Error:2 ：No Such File or Directory

解决方案

为了解决此问题，请再镜像火星设备。关于如何再镜像火星的更多信息，参考再镜像LocalDirector。

无法添加设备用种子文件

问题

当您尝试添加一个设备用在CS-MARS时的一个种子文件，此错误消息出现：

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

解决方案

这发生，当种子文件在逗号分隔的值(CSV)时格式没有保存。您必须保存种子文件作为一个真的CSV文件。请勿保存文件作为Microsoft Excel文件(.xls文件);当上载种子数据时，火星不能编译Microsoft Excel被格式化的.xls文件和暂停。以一个真的逗号分隔的值文件的形式， CS-MARS需要此数据。参考请添加多个报告和缓解设备使用种子文件关于如何设置种子文件的更多信息。

无法连接到设备

问题

当您无法访问从火星时的一3550交换机您也许收到此错误：

```
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
```

解决方案

如果在SSH密钥的模数设置在交换机设到512，此错误出现;值应该更加高。

错误，当拉从Windows时的日志

问题

当您请求从后端的日志，您也许收到此错误：`3075656624:winpull 10.1.1.52`

解决方案

当用于的获知的Windows帐户请求事件日志没有火星帐户的权利在服务器，此错误出现。

系统规则：非激活CS-MARS报告的设备

问题

Mars报告此规则：

系统规则：*非激活CS-MARS报告的设备。并且没有接收Syslog。*

解决方案

此规则检测未在过去小时内报告一个事件的报告的设备。对于话多设备，例如防火墙和IDS，此错误能指示连通性问题或一个问题用设备。此规则必须是包括仅话多网络基础设施设备的scoped下来。

在设备配置的出口的内错误

问题

当您设法导出设备配置时，进程似乎运行，但是没有在SFTP服务器的配置文件，该一个空的文件夹创建的进程。您也许也接收*Error:失败保存文件到远程主机*消息。

解决方案

检查您使用的帐户访问写访问。思科建议您使用在Windows的Cygwin SFTP服务器。

Cisco安全毁损支持SFTP服务器作为存储介质存档或迁移从4.x的数据到6.0.1。关于如何配置Cygwin和OpenSSH的信息在Windows，参考请配置在Windows的Cygwin SFTP服务器。它瞄准在Windows XP的Cygwin SFTP服务器。

无法重置在CS-MARS的密码

问题

您无法重置在CS-MARS的密码。

解决方案

请使用*pnadmin*作为用户名和密码。如果这不工作，重置在火星传感器的密码的唯一方法是使用恢复DVD，基本上再镜像设备。在您使用恢复CD/DVD前，请确保您安排您的许可证密钥写入下来。参考恢复丢失的管理密码关于如何重置在CS-MARS的密码的更多信息。

LocalDirector不用全局控制器适当地同步

问题

LocalDirector (LC)与全局控制器(GC)不适当地同步。

解决方案

确保LC和GC有同一个签名。LC和GC必须有同一个签名为了他们同步，不用任何问题。

错误，当导入从版本4.3.6到6.0.2的配置在CS-MARS时

问题

您也许接收`111`错误，当您导入从版本4.3.6到6.0.2的一配置在CS-MARS。

解决方案

配置可以从CS-MARS版本4.3.6导入到仅版本6.0.1;它不可能导入到6.0.2。为了解决此问题，请导入从4.3.6的配置到6.0.1然后再镜像CS-MARS到6.0.2。

错误，当导入从CS-MARS版本6.0.4时的配置

问题

您也许接收`Error:4.3.15.x.x`错误，当您导入从版本4.x到6.0.4的一配置在CS-MARS。

解决方案

配置可以从CS-MARS版本4.x导入到仅版本6.0.1;它不可能导入到6.0.2。为了解决此问题，请导入从4.x的配置到6.0.1然后再镜像CS-MARS到6.0.4。

参考迁移从Cisco安全火星4.x的数据到6.0.X关于CS-MARS的迁移的更多信息。

Error:配置错误：主机名不匹配janus.conf ： ：janusBoxName。

问题

在您升级CS-MARS后，您也许收到此错误：

```
Error:janus.conf  janusBoxName
```

解决方案

此错误归结于Cisco Bug ID CSCsh82939 (仅限注册用户)。为了避免此问题今后它是推荐更改主机名到运行在新的默认“主机名”的原始主机名pnrestore在重新镜像以后和在pnrestore前，

配置导入从版本6.0.1(2990)失效到在CS-MARS的主线版本6.0.3(3188)

问题

当您导入从版本6.0.1到6.0.3的一配置在CS-MARS时，您也许收到此错误：

```
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
```

解决方案

如果使用**pnexp，**并且**pnimp**发出命令，配置被备份了并且仅恢复对同一个火星版本。唯一的例外从版本4.x移植到版本6.0.1;此步骤不为移植工作从版本6.0.1到版本6.0.3。

您必须再再镜像与原始6.0.1版本的火星(的版本您以前运行**pnexp**命令)，恢复与**pnimp的**配置，然后完成两连续的升级用pnupgrade工具：6.0.1到6.0.2然后6.0.2到6.0.3。

注意： 数据从一个大模式恢复到CS-MARS一个小模式不支持。例如，您不能恢复从Mars 100的数据到火星50。

无法配置在火星的电子邮件告警所有严重级别RED的规定

问题

您无法配置在火星的电子邮件告警所有严重级别RED规则的。

解决方案

配置所有严重级别RED规则的电子邮件告警在一个步骤是不可能的。您必须配置根据每规则基本类型的电子邮件告警。创建海关规则(规则>Add)，为除了严重性的所有参数然后选择其中**任一**。对于严重性参数，请选择**RED**，并且设置操作发电子邮件配置在火星的电子邮件告警所有严重级别RED规则的。参考配置规则发送一提醒的操作欲知更多信息。

欲知更多信息，参考Cisco Bug ID CSCse89349 (仅限注册用户)。

火星自动签名更新功能不运作

问题

如果使用一个代理或代理/缓存服务器为了访问互联网，在火星的自动签名更新功能不运作。在自动签名更新期间，您也许收到此错误消息：URL

解决方案

如果使用一个代理或代理/缓存服务器访问互联网，火星无法下载动态IPS签名更新。如果使用一个代理/缓存服务器，您能手工下载从此URL的签名更新文件：http://www.cisco.com/cgi-bin/tablebuild.pl/mars-ips-sigup (仅限注册用户)。关于自动签名更新的更多信息参考的IPS签名动态更新设置在火星。

未知设备事件类型

问题

在更高的签名更新期间， CS-MARS报告此错误：

解决方案

CS-MARS比传感器有一次更高的签名更新;在解析的问题不应该出现。然而，如果传感器比CS-MARS有一次更高的签名更新， CS-MARS也许生成*未知设备事件类型*错误，因为CS-MARS不能直接地解析更新的签名;原始事件数据存在。应该有性能影响到CS-MARS外部潜在不伦不类的事件消息。

注意： 自定义签名分类作为“未知设备在CS-MARS的事件类型”事件;然而，签名查找作用正如所料。

无法配置Netflow的火星

问题

在您配置Netflow的后，火星您遇到问题。

解决方案

是支持监听网络流量的思科技术和所有基本Cisco IOS镜像支持Netflow。火星收集从报告的设备发送的Netflow，并且提供多种级别功能(从属您是否存储它对数据库)。如果存储， Netflow可以被查询，并且您能有报告、规则和事件它的。参考了解Netflow异常情况检测关于如何配置Netflow的火星和如何的更多信息Netflow工作。并且配置的Netflow安全事件记录日志(NSEL)参考的Taskflow欲了解更详细的信息在火星在Netflow配置。

CS-MARS报告多个目的地作为Port0

问题

CS-MARS报告多个目的地作为端口0。目的地端口是0，并且有时目的IP地址是0.0.0.0。

解决方案

因为报告的设备一些事件类型报告多个目的地目的端口或IP地址，这是预计的CS-MARS行为。火星统一此信息到单个值(0)。如果关注数据报告对触发此行为的火星，您能运行*所有匹配的事件原始*消息类型查询触发此行为为了发现信息报告对火星，包括多个指定端口或IP地址的一个或很多报告的设备。与原始事件的所有匹配的事件原始消息显示事件ID、事件类型、时间、报告的设备和原始消息字段。

CS-MARS事件报告来源作为0.0.0.0 Port0

问题

CS-MARS有报告来源作为0.0.0.0端口0的一些事件事件。

解决方案

在CS-MARS， IP地址0.0.0.0意味着没有此字段的信息。这是在CS-MARS内使用的规则。`0.0.0.0` IP地址和港和`0`在两个案件分别出现：

1. 在Syslog未指定的那些
2. 有多个值的那些(2或更多IP或端口)

程序中止的由于：ORA-01033 ：Oracle正在初始化或进展中的关闭。

问题

当您设法开始或终止与**pnstart**或**pnstop** at命令的服务在CS-MARS的CLI此错误出现：

```
ORA-01033 Oracle
```

此错误消息表明数据库失败了。

解决方案

如果再镜像配置导入，跟随的CS-MARS此错误可以是解决的。

无法备份在CS-MARS的仅配置

问题

没有在CS-MARS的数据您无法备份设备配置。

解决方案

您能存档从火星设备的数据和使用该数据恢复操作系统(OS)、系统配置设置、动态数据(事件数据)，或者完整系统。设备到/从有网络文件系统协议的一个外部连接网络的存储系统存档并且恢复数据。在您归档所有数据和设备配置后，请恢复仅设备配置信息，以便仅设备配置恢复。参考配置并且执行设备数据备份关于在CS-MARS的设备数据备份的更多信息。

升级与DVD的软件

问题

您无法升级与DVD的镜像在CS-MARS。

解决方案

CS-MARS不认可DVD作为恢复镜像。为了解决问题，请烧录CD以**4x速度**。参考下载和烧录恢复DVD关于与DVD的工具软件升级的更多信息在CS-MARS。

无法运行raidstatus命令

问题

您无法运行**raidstatus** in命令CS-MARS。

解决方案

CS-MARS不支持**raidstatus** in命令低端的型号- 20或50。仅对于型号100， 100E和200是支持的此命令。

未知报告的设备IP

问题

设备报告作为在火星系统的*未知报告的设备IP*。

解决方案

此问题归结于CS-MARS标记事件数据，因为接收根据来自的源IP地址，在方面然后执行查找匹配源IP地址到已配置的报告的设备)的其配置(。如果没有找到匹配，设备被标记作为“未知报告的设备IP”，意味着用户未配置火星认可火星的所有需求能能解析/了解事件数据，例如运行IP地址和软件版本/代码的设备类型。

为了验证，注释有问题的IP地址或的地址和导航对**ADMIN >System设置> Security和监控设备页**在火星GUI。验证同样IP地址或地址不是列出的。一旦验证，请添加适当的报告的设备(和显示作为*未知*)的其他网络设备为了修改此问题。

接收的错误，当下载在CS-MARS的更新包

问题

当您下载在CS-MARS时的更新包您也许收到此错误：

```
Cisco.com\nCisco.comCisco.com:ERR_INTERNAL
```

解决方案

此错误出现，当对*origin-www.cisco.com的*全双工出局访问*(通过HTTPS/443)*，并且*software-sj.cisco.com (通过HTTP/80)*在防火墙没有配置。为了解决此问题，请确保防火墙(若有)配置为了允许对*origin-www.cisco.com (通过HTTPS/443)*和*software-sj.cisco.com的*全双工出局访问*(通过HTTP/80)*。

无法添加在CS-MARS的FWSM

问题

您是无法添加每在CS-MARS的FWSM。

解决方案

在您能添加在交换机前的一个FWSM模块，您必须添加和配置基本模块(Cisco交换机)在火星。参考配置Cisco防火墙设备欲知更多信息。

NTLMv2不与CS-MARS一起使用

问题

您无法以CS-MARS使用NTLMv2。

解决方案

CS-MARS不支持NTLMv2;因此，您无法以CS-MARS使用NTLMv2。

CS-MARS失败与"内核紧急5"控制台信息

问题

CS-MARS失败与在控制台的5消息。消息包括此信息：`CET./csips62385072:Exiting OUT_OF_MEMORY superV`

解决方案

通常，此问题与在CS-MARS设备的一高端内存使用情况一起被看到。运行命令到show system库存信息能触发此问题。欲知更多信息，参考Cisco Bug ID CSCsm40349 (仅限注册用户)。

在CS-MARS的错误在期间启动

问题

当CS-MARS启动时，您也许收到此错误：

```
/dev/hda2;RAN fsck
```

解决方案

再镜像CS-MARS设备为了解决此问题。在您再镜像设备前，您能也设法手工运行**fsck**。

参考再镜像LocalDirector关于如何再镜像CS-MARS设备的更多信息。

在CS-MARS的错误在设备升级期间

问题

当您升级csmars-6.0.2.2102.30对csmars-6.0.3.3188.32时，您也许收到此错误：

```
[Error][check_dependency/541] version(6.0.2.3102.31) >version(6.0.2.3102.30)
```

解决方案

在以前版本升级期间，如果数据版本未适当地更新此错误也许出现。

为了解决此问题，请执行升级到6.0.2从CLI。软件版本升级被跳过，但是数据版本升级被执行。您能然后升级到版本6.0.3。

验证您的与CLI命令的**版本的**当前版本

参考从CLI的升级关于如何升级CS-MARS设备的更多信息。

火星GUI定位在从5.x的升级以后是慢到6.0(4)

问题

在您升级从5.3.1到6.0后，您也许遇到与火星GUI的性能问题。

解决方案

对版本6.0.6的升级为了解决此问题。

报告不导出对其他应用程序

问题

您不能导出从火星的报告在一个象样的格式，例如PowerPoint、PDF、词或者Excel。

解决方案

CS-MARS包括功能导出报告到其他应用程序。CS-MARS支持格式的仅这两种类型报告的：

- 逗号分隔的值 (CSV)
- HTML

注意： 如果选择观看报告作为CSV文件，您需要保存文件到您的计算机和打开在第三方应用的CSV文件。欲知更多信息，在存在的参考的操作报告。

相关信息

- **思科安全检测、分析及响应系统-兼容性信息**
- **排除故障CS-MARS fsck问题**
- **技术支持和文档 - Cisco Systems**