IDS 4.0/AIP-SSM/IPS 5.0及以上版本常见问题

目录

[简介](#)
[IDS 4.0](#)
[IPS 5.0及以上版本](#)
[相关信息](#)

简介

本文回答与Cisco安全入侵监测系统(常见问题)涉及的多数常见问题(IDS) 4.0，先进的检查和预防安全服务模块(AIP SSM)和思科入侵防御系统(IPS) 5.0及以上版本。

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

IDS 4.0

Q. 我安装IDS MC和SecMon在新的服务器，并且我当前想要对import all配置(用户，设备，等等)从旧有服务器到新的。我怎样做这个?

A. 执行此的简便的方法是启动您新的VMS服务器，然后发现有此的传感器新建的方框。

注意： 当您添加传感器时，请勿手工添加它。检查**发现设置**方框。

一旦传感器是已发现，请导入它到SecMon。所有配置在传感器保存。在您构件您新的服务器后，签名设置，过滤器，等等应该遇到。确保您更新IDS MC对最新的签名。

Q. IDS-4215接收`idsPackageMgr` 错误消息，当尝试升级IDS恢复分区时。需要执行什么解决此问题？

A. 这是制造问题。一些客户接收与一坏基本镜像(4.0)的IDS-4215s。完成下面这些步骤。

1. 下载恢复分区镜像(仅限注册用户)。
2. 通过CLI运用恢复分区镜像升级： `sensor#configure terminal sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/ IDS-4215-K9-r-1.1-a-4.1-1-S47.tar.pkg`
3. 一旦恢复分区镜像应用， 4215恢复对正常运行4.1(1) 4215基础。 `sensor(config)#recover application-partition`

Q. 当我从2位升级到3位信号时请成水平包，例如S100或以后，例如， 4.1(4)S99对4.1(4)S100， auto-update功能发生故障。如何解决此问题？

注意： Cisco VMS和CLI客户不遇到此问题。

问题的原因是使用的排序的逻辑，当文件名解析时。当应该是数字的时，它是一个字母数字排序。应急方案是使用CLI (或VM)升级到3位信号级别包，例如S100或以后。一旦这完成， auto-update开始再作用。参考Cisco Bug ID CSCef07999 (仅限注册用户)欲知更多信息。

Q. 什么执行""错误消息平均值？

A. 为了解决此问题，请使用默认密码(cisco)两次然后更改从配置模式的密码。IDS要求两次将被输入的默认密码。

例如：

```
login:cisco
Password:cisco
Enter current password:cisco
Enter new password: ***
Re-enter new password: ***
```

Q. 如何从交换机删除IDSM ？

A. 模块，在您禁用电源之后，应该删除。完成这些步骤：

1. 从传感器CLI，请发出**重置**powerdown命令。
2. 一旦传感器完成关闭，从交换机CLI，请勿发出Cisco IOS的**power enable模块**(module_number)命令或CatOS的**set module power down (module_number)**命令。
3. 按下刀片上的**关闭**按钮。
4. 关闭机箱电源。当状态灯显示一张美国钞票时，您能安全去除模块。

IPS 5.0及以上版本

Q. 我安排避开配置，但是我被迷惑关于如何配置在签名的阻塞。块主机和块连接有何区别？

A. 块主机阻塞从该源地址的所有信息包。块连接只阻塞根据源和目的IP/port的这一连接。PIX工作以有些不同的方式。对于自动避开，传感器发送来源IP、目的地IP、源端口和目的地端口。PIX阻塞起源于该IP地址的所有信息包。PIX用于其他信息从其连接表取消该一连接。如果连接未从连接表删除，则很可能，理论上，如果避开删除，在应用之后，然后原始连接也许没有计时。这允许攻击者继续在原始连接的攻击。连接的删除从表保证原始连接不可能用于继续攻击，在避开删除后。因为PIX不支持使用**shun命令**为了避开单个连接，传感器不能避开在PIX的一单个连接。不论提供，**shun命令的**PIX总是避开源地址其他联系人信息。

Q. 什么执行"Error:"错误消息平均值？

A. 此错误意味您的默认网关是不正确或意味着的一通用的错误消息IP、网络屏蔽或者默认网关不正确。消息的部分意味着在第一失败以后，先前配置应用并且失败。传感器发出**ifconfig，**并且**路由**发出命令，并且一个人或他们两个发生故障。

Q. 自动更新失效与"mainApp[343] Cid/E errSystemError httpresponse:500"错误消息。此错误消息是什么意思？

A. 此问题也许是自动更新功能，不运作，因为设置下载在一个均等小时。设法设置自动更新为随机

时间;一小偏移量八或晚上分钟能解决此问题。

一般来说，问题是解决和Error:http错误消息是的500被看到是否更改检索时间对一非每小时边界。

注意： IPS发生故障签名auto-update并且返回与此错误消息：

```
HTTP[1,110] name=errSystemError
```

请验证以下项目以解决此问题：

- 如果防火墙防止传感器到达的Cisco.com，请验证。
- 如果路由变为问题，请验证。
- 如果NAT在下行设备的，网关设备适当地配置请验证。
- 如果用户凭证正确，请验证。
- 更改更新开始时间对多的个小时。

Q. 什么执行"Error:execUpgradeSoftware AnalysisEngine"错误消息平均值？

A. 为了解决此问题，请设法重新加载传感器或再镜像传感器。

Q. 我如何解决错误消息Cid/W- DNSHTTPDNSHTTPDNS''？

A. 完成这些任务为了解决此问题：

- 禁用全局相关性。
- 添加代理/dns配置。

Q. 我如何解决IPS为全局相关性健康问题收到的这些错误："23Jan2010 15:50:39.831 38.001 collaborationApp[655] rep/E AHTTPTLSX.X.82.127:443 TLS"并且"collaborationApp[459] rep/E Aibrs/1.1/drop/default/1296529950URIIP"？

A. IPS无法到互联网由于端口问题，例如，在没有正确端口开放为互联网访问的路径或它的一防火墙可以是NAT问题。

全局相关性首先作用完全，传感器联系方式通过https update-manifests.ironport.com为了验证用户HTTP连接然后下载GC更新。传感器从HTTP的文件(updates.ironport.com)下载是全局相关性使用的名誉数据。https update-manifests.ironport.com应该总是解决到X.X.82.127地址，但是http updates.ironport.com **IP地址能更改**，取决于互联网您访问。因此您必须检查IP地址。如果URL过滤启用，请添加IPS管理接口IP的一例外在URL过滤，因此IPS能连接到互联网。

当有在一次上一个GC更新的损坏此错误出现：

```
collaborationApp[459] rep/E Aibrs/1.1/drop/default/1296529950URIIP
```

此问题可能被关闭GC服务然后打开它通常修改回到。在IDM，请选择**Configuration>策略>全局相关性>检查/名誉**，设置全局相关性检查(和**名誉过滤，**如果)对，应用更改，等待10分钟，打开功能，并且监控。

Q. AopenConnection badAddrStringIpAddrExceptionHTTPDNS错误消息在"名誉更新失败"类别接收。如何解决此问题？

A. 确认以下各项：

- 您必须有一个有效IPS许可证为了允许全局相关性功能作用。
- 您必须安排HTTP代理服务器或DNS服务器配置为了允许全局相关性功能作用。
- 由于全局相关性更新通过传感器管理接口出现，防火墙必须允许tcp 443/80和udp 53流量。
- 确保您的传感器支持全局相关性功能。如果不想要此，请禁用从IDM的全球协作功能：去 **Configuration>策略>全局相关性>检查/名誉**和集全局相关性检查(和名誉过滤，如果)。

Q. 我如何解决“openConnection IPS为全局相关性健康问题收到的IpAddrException badAddrString”错误？

A. 如果使用全局相关性(GC)那么请确保名字解析工作，例如， DNS可及的。并且请检查是否有防火墙阻塞端口53。否则，如果希望摆脱此消息，您能关闭GC功能。

Q. 如何解决我收到的MySQL错误消息的当我启动从浏览器时的IME ？

A. 此问题通常出现，当客户尝试运行在不支持的操作系统的IME，例如Windows 7。

Q. 我如何解决“88-nsmc-c1IDM Cisco Inc. Category JNLPfileJAR”“在应用程序的启动期间，IDM收到，发生的idmx.x.x.x:443”错误？

A. 清除浏览器缓存为了解决此问题。

Q. 如果使用GUI，在IPS的不对称模式是否是可配置？

A. 在版本6.0，使用CLI是可配置仅和不可用在GUI在IPS的不对称模式。但是，在版本6.1此功能也是可用的在GUI。

Q. 如何解决延时问题用IPS传感器？

A. 为了解决此问题，请启动处理不对称的模式为了允许有流的传感器同步状态和为不要求两个方向的那些引擎维护检查。使用此配置：

```
IPS_Sensor#configure terminal IPS_Sensor(config)#service analysis-engine IPS_Sensor(config-ana)#virtual-sensor vs0 IPS_Sensor(config-ana-vir)#inline-TCP-evasion-protection-mode asymmetric
```

延时问题发生，当拒绝操作线型并且丢弃数据包为在VS0的每个签名启用。启用所有签名将导致延迟， IPS检查通过通过每一的数据包。启用根据网络流量运输流量要求的仅特定签名为了解决延时问题是好的。

Q. AIP-SSM是否帮助阻塞Skype ？

A. PIX/ASA不能阻塞skype流量。Skype有能力协商动态端口和使用加密流量。对于加密数据流，由于没有要查找的模式，因此几乎检测不到它。

您可能最终使用思科IPS (入侵防御系统) /AIP-SSM。它有一些签名，这些签名可以检测连接到 Skype 服务器以同步其版本的 Windows Skype 客户端。这通常在客户端启动连接时执行。当传感器获得最初的 Skype 连接时，您可以找到使用该服务的人员，并阻止从他们的 IP 地址启动的所有连接。

Q. 为什么感觉的接口或频繁地去IPS的故障状态？

A. 在签名更新和重新配置期间，处理数据包的sensorApp终止，处理在更新的新的签名。网络驱动器检测sensorApp终止了并且拉其中任一从缓冲区的新建的数据包。因此网络驱动器做不同的事，取决于配置和传感器型号：

混乱接口—，一旦sensorApp开始再，监控它带来链路下来在接口，并且带来链路备份。

轴向接口或轴向VLAN对—它取决于旁路设置：

- **旁路自动**—驱动程序保持链路上并且开始通过传递数据包，不用分析。一旦sensorApp开始再，监控它然后恢复回到发送数据包通过sensorApp。
- **绕过**驱动程序带来链路下来在接口，是相同的正如在混杂模式，并且带来他们备份，一旦sensorApp开始再监控。

因此，如果传感器app不请求从缓冲区的数据包，可能发生，因为没有配置的接口处理数据包，然后驱动程序能在放置接口。

当感觉的接口摆动时，这些日志被看到：

```
28Jun2011 09:03:09.483 6050.885 interface[409] Cid/W errWarning Inline
    databypass has started.
28Jun2011 09:03:13.639 4.156 interface[409] Cid/W errWarning Inline databypass
    has stopped.
28Jun2011 09:19:23.922 970.283 interface[409] Cid/W errWarning Inline databypass
    has started.
28Jun2011 09:19:27.486 3.564 interface[409] Cid/W errWarning Inline databypass
    has stopped.
```

Q. IDS或入侵防御系统(IPS)传感器是否维护密码历史记录？

A. 不，传感器不维护密码历史记录。密码在任何时间不看得见。

Q. IDS或入侵防御系统(IPS)传感器是否支持系统日志服务器发送日志？

A. 不能。

Q. 什么是存储在IPS的事件最大限制？

A. 一旦30 MB限制达到，传感器的本地事件存储仅30 MB并且开始覆盖。此限制是不可配置的。

Q. 如何写入签名检测foto [a-z] \ .zip文件在任何流入或传出电子邮件？

A. 请使用STRING.TCP为了写入检测附件的签名。寻找事类似于此：

```
Engine STRING.TCP
Enabled True
Severity informational
AlarmThrottle Summarize
CapturePacket False
Direction ToService
MinHits 1
Protocol =TCP
RegexString [Ff][Ii][Ll][Ee][Nn][Aa][Mm][Ee][=]["][Ff][Oo]
            [Tt][Oo][a-zA-Z][.][Zz][Ii][Pp]["]
```

```
ResetAfterIdle 15
ServicePorts 25
StorageKey =STREAM
```

Q. 如何配置FTP客户端超时？

A. 发出以下命令：

```
configure terminal
service host
networkParams
ftpTimeout 300 <timeout is in seconds>
```

Q. 如何转换开始时间和结束时间在iplog状态对可读的格式？

A. 此输出是当前时间的十进制表示法从UNIX epoc。在UNIX日期/时间计算器站点请使用一个UNIX epoc计算器例如查找的 那个。请进入前10个位，因为此计算器是粒状对仅秒钟，并且IDS存储纳秒。这意味着剥去最后九个位。从一开始时间在此输出中，`1084798479 =200451712:54:39 (GMT)`是什么您接收。

从CLI，回车iplog**状态**为了收到此输出：

```
"
Log ID:             138343946
IP Address:         xxx.xxx.xxx.xxx
Group:              0
Status:             completed
Start Time: 1084798479512524000 End Time: 1084798510136582000 Bytes Captured: 2833 Packets
Captured: 14 "
```

Q. “IOExceptiojava.security.cert.CertificateExpiredException”错误消息。这如何可以是解决的？

A. 如此示例所显示，为了解决此错误消息，请登陆到AIP-SSM并且发出**tls生成KEY** in命令特权EXEC模式：

```
sensor#tls generate-key
```

注意： 使用命令**tls生成KEY的**此解决方法也解决的AIP-SSM问题能连接到IME。

Q. “IOExceptio IME IME”错误消息出现，当我添加在IME时的IPS。此问题如何可以是解决的？

A. 为了解决此错误消息，请选择**控制面板>管理工具>** Services并且重新启动IME服务。

Q. 当我添加IPS传感器到IME时，不/[IOException - connect timed out]错误消息接收。此问题如何可以是解决的？

A. 这指示IME和IPS传感器之间的残破的通信。确保没有阻塞SDEE的软件。

Q. IME“()”错误消息。此问题如何可以是解决的？

A. 为了解决此错误消息，请验证使用正确IP地址的那，当您添加在IME的IPS并且检查在IME计算机运行，能阻塞连接的所有软件防火墙时。

Q. IDS或入侵防御系统(IPS)传感器能否发送电子邮件告警？

A. IDS传感器没有能力独自地发送电子邮件告警。安全监视器，当使用与IDS有能力发送电子邮件通知，当事件规则由传感器时触发。

参考请配置电子邮件通知关于如何配置与安全监视器的电子邮件通知的更多信息。

Cisco IPS Manager Express (IME)可以配置传送电子邮件通知消息(警报)，当事件规则由思科IPS传感器时触发。参考的IPS 6.X和以后：电子邮件通知使用IME配置示例欲知更多信息。

Q. 错误：:`mainApp (getVersion)`当我设法连接到我的传感器，错误消息出现。此问题如何可以是解决的？

A. 重新启动传感器为了解决此问题。

Q. `regexesConsider`错误消息出现调整在我的传感器的签名。此问题如何可以是解决的？

A. 退休不是在使用中的为了解决此问题并且应该减少客户签名数量与regexes的签名。并且，没有推荐使用*和+在regexes的元字符。

Q. 延迟问题为什么出现在思科入侵防御系统(IPS)传感器？此问题如何可以是解决的？

A. 延时问题能发生由于不对称路由。设法禁用签名1330为了解决此问题。

Q. 禁用SSHv1和留给仅SSHv2启用在思科入侵防御系统(IPS)是否是可能的传感器？

A. 目前，不可能禁用 SSHv1 并仅启用 SSHv2。SSHv1 和 SSHv2 一起启用，无法单独禁用。

Q. `=/usr/cids/idsRoot/var115000 KB110443 KB`当我升级传感器对版本4.1(5)，消息出现。此问题如何可以是解决的？

A. 此错误消息发生由于在传感器的内存不足。

完成这些任务为了解决此问题：

1. 登录服务帐户并且变为根
2. 取消以下目录如下所示：
```
# rm -rf /usr/cids/idsRoot/var/updates/files/S69
# rm -rf /usr/cids/idsRoot/var/updates/files/common
# rm /usr/cids/idsRoot/var/virtualSensor/*
# rm /usr/cids/idsRoot/var/.tmp/*
```
3. 现在请设法升级传感器。参考Cisco Bug ID CSCsb81288 (仅限注册用户)欲知更多信息。

Q. 我收到`mainApp[396] cplane/E- accept()-1`错误消息在ASA日志中。如何才能解决此错误？

A. `mainApp[396] cplane/E- accept()-1`错误消息表明Web服务器不能读文件和失败的accept()程序，产生文件描述符，当TLS连接存在时。但是此文件为正常行为不是需要的。这是无害的。

Q. 我如何解决tls/W errTransport WebSession sessionTask TLS错误消息？

A. 此错误消息表明证书不再是有效在模块。完成这些步骤以解决问题：

1. 重新生成从CLI的证书：登陆对传感器line命令。发出**tls生成**命令，并且按回车。注释显示的指纹。
2. 请求新证书对IME ：打开IME并且找出在列表的传感器名称在主页。用鼠标右键单击传感器，并且单击**编辑**。当您到达编辑设备屏幕时，请点击OK键。绕过关于的所有警告能获取传感器时间。您用新的安全证书(您生成)的那个将提示。检查确保指纹匹配，并且点击**是**。在几秒钟之后，传感器在事件状态应该显示“再连接”。

Q. 当我尝试登陆到IPS时，我收到此错误消息：errSystemError ctsensorAPP.450 clientpipe。 如何解决此问题？

A. 为了解决此错误，请使用**reset命令**为了重新启动IPS。

Q. 在AIP-SSM的时间与在思科可适应安全工具(ASA)的时间有所不同。此问题如何可以是解决的？

A. 为了解决此问题，请使用Ntp server同步在思科可适应安全Appliance(ASA)和AIP-SSM的时间。

参考配置在IPS传感器的NTP欲知更多信息。

Q. 如何能应用在AIP-SSM的多个虚拟传感器？

A. 因为AIP-SSM只有一个接口，在AIP-SSM的虚拟传感器不可能每个接口应用。当您创建多个虚拟传感器时，您只必须分配此接口到一个虚拟传感器。您不需要指派其他虚拟传感器的一个接口。

在您创建虚拟传感器后，您必须映射他们到可适应安全工具的(ASA)安全上下文使用分配**IPS**命令。您能映射许多安全上下文到许多虚拟传感器。参考*分配的虚拟传感器对*配置AIP-SSM的*可适应安全工具上下文*部分欲知更多信息。

Q. 什么是AIP-SSM支持的虚拟传感器最大？

A. 可以支持四个虚拟传感器最大。

Q. 如果我使用然后SSH是否是或IDM为了登陆到IPS它可能配置IPS 4240/IDSM/IDSM2为了验证管理用户RADIUS/TACACS+服务器？

A. 对TACACS+服务器不是可能的，但是RADIUS从IPS 7.0.(4)E4版本支持。参考版本注释的*新和更改的信息*和*限制和限制*部分思科入侵防御系统的7.0(4)E4欲知更多信息。并且，参考IPS 7.X ：用户登录验证使用ACS 5.X作为配置示例的RADIUS服务器配置示例。

Q. 什么是已到期许可证影响在IPS funcationality ？

A. 一个已到期许可证有在传感器的唯一的影响是制止签名更新。

Q. IPS签名更新是否有在服务或网络连通性的影响？

A. 不能。IPS签名更新没有在服务或网络连通性的一影响。

Q. 什么是我需要为IPS模块输入自动地更新与最新的签名的确切的URL ？

A. 要求的链路允许IPS模块自动地更新与最新的签名是：https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl。

您必须使用您的思科用户ID和密码完成IPS模块的更新。

注意： 在代码6.x系列中，不支持从Cisco.com的自动更新。您必须手工下载签名文件和适用于他们传感器。有在6.x代码的一个auto-update功能;然而，这从签名文件必须手工下载的本地文件服务器是仅可能的。

Q. IPS传感器是否易受攻击对X11端口转发会话劫持漏洞？

A. 不能。它不易受攻击对于这些原因：

- 传感器没有X11库。所以没有劫机的会话。
- X11端口转发没有在SSH配置里启用。
- IPv6没有被编译到传感器内核。这要求为了利用漏洞。

Q. 当ASA显示大量警告和攻击日志时， AIP-SSM为什么不显示任何日志？

A. 这发生，因为，当ASA阻塞某事时，没有通过对重复的检查的IPS。所以，您看不到重复项注册ASA和IPS。

Q. 在用户部署S518签名集后，“invalidValue EditngXL TCP”错误消息发生。为什么？

A. 这是完整错误消息：

```
evError: eventId=1284051856322985135 vendor=Cisco severity=warning
  originator:
    hostId: vbintestids03
    appName: sensorApp
    appInstanceId: 700
  time: offset=-240 timeZone=GMT-05:00 1286305251136551000
errorMessage: name=errWarning invalidValue:Editing string-xl-tcp
sig 21619 has NO effect
```

因为硬件，不支持字符串XL TCP或字符串TCP XL引擎此问题出来。欲了解更详细的信息，参考IPS引擎E4版本注释。

Q. 当我自动地更新在ASA-SSM-10的签名与自动更新功能时，我收到此错误消息：status=true。如何能解决此问题？

A. 此输出表示完整错误消息：

```
autoUpgradeServerCheck:
    uri: https://XX.XX.XX.XX//cgi-bin/front.x/ida/locator/locator.pl
    packageFileName:
    result: No installable auto update package found on server  status=true
```

此错误生成，并且签名不自动地更新，因为在S479以后的签名定义更新要求E4引擎。为了解决此，您需要手工升级传感器到7.0(2)E4。

注意： 传感器不能自动地升级到E4，因为要求7.0(2)和传感器的重新启动。

Q. 在IPS 5.0的自动更新feauture NIDS模块的不工作。如何能解决此问题？

A. 此输出表示完整错误消息：

```
autoUpgradeServerCheck:
    uri: ftp://hfcu-inet01@192.168.1.12//ips-update/
    packageFileName:
    result: No installable auto update package found on server  status=true
```

此问题出现由于与FTP服务器的一个不正确的目录列表样式。为了解决此，交换机到从现有MS-DOS样式目录列表的UNIX类型目录列表。

为了修改目录列表设置，请选择**启动>** Program Files >Administrative**工具**为了打开Internet Services Manager。然后请去Home Directory选项并且更改目录列表样式从MS-DOS到UNIX。

Q. IPS-4255接收SensorApp TcpRootNode失效： ：在升级期间的expireNow()错误消息。如何解决此问题？

A. 此问题归结于分析引擎的失败和寻址在Cisco Bug ID CSCtb39179 (仅限注册用户)。升级传感器对版本7.0(4)E4为了调整此问题。

Q. 当我尝试执行许可证更新，在I purchanse新准许设备报告此错误后：**"update license""errExpiredLicense-The"**如何能解决此问题？

A. 当接收的许可证文件无效，此问题出现。要得到有效许可证文件，请登陆对Cisco.com作为注册用户，并且下载适当的许可证文件。一旦得到有效许可证文件，请安装它在您的传感器。

如果安装新的许可证文件和您仍然请收到错误，也许有一个问题用现有无效的许可证文件。为了解决此问题，请完成这些步骤删除现有无效的许可证文件：

1. 登陆对服务帐户通过键入您的服务帐户用户名。如果没有一个服务帐户，打开IPS line命令，输入配置模式，并且输入此命令**用户名***命名***权限服务口令***密码*
```
ciscoasa# session 1
Opening command session with slot 1.

Connected to slot 1. Escape character sequence is 'CTRL-^X'.
login:
Password:

IPS#
IPS#conf t
IPS(config)# username name privilege service password password
```
2. 一旦登陆对您的服务帐户，请输入**su命令**为了去根源(使用密码和服务帐户一样)。
3. 删除在/usr/cids/idsRoot/shared/目录的文件。**注意：** 请勿删除host.conf文件。输入**cd /usr/cids/idsRoot/shared/**命令为了去共享目录。输入**ls命令**为了查看在目录的文件。输入**rm** *file_name*命令为了删除文件。**注意：** 请勿删除host.conf文件。
4. 输入**/etc/init.d/cids重新启动**命令重新启动传感器。
5. 安装新的许可证。

归档Cisco Bug寻址此行为。欲知更多信息，参考CSCtg76339 (仅限注册用户)。

Q. 什么执行**errorMessage IpLog 1712041197name=ErrLimitExceeded**错误消息平均值？如何解决此问题？

A. 此错误由在IP记录日志的过量的数据包造成。禁用IP操作日志功能为了解决此问题。IP记录日志为只排除故障含义;思科建议您不为所有签名启用它。

Q. 当我更新传感器从s550到s551时，我收到此错误：“signatureDefinition”"sig0"。如何能解决此问题？

A. 签名23899.0的修改导致此问题。参考Cisco Bug ID CSCtn84552 (仅限注册用户)欲知更多信息。

Q. 我收到在传感器的此错误：Error:autoUpdatecisco.comHTTP。如何能解决此问题？

A. 检查是否有URL过滤、内容过滤或者阻塞从发生的autoUpdate的代理服务器存在。确保autoUpdate没有阻塞并且验证提供的用户凭证正确。

Q. 我收到在以版本6.2(3)E4运行的IPS传感器的此XML错误消息：errorMessage IPSXML() XML‘*’。如何能解决此问题？

A. 此行为由Cisco Bug ID CSCsq50873 (仅限注册用户)寻址。这是表面问题，并且不创建除了接收的超出数量的任何运营开销日志。临时应急方案是删除在传感器的NTP相关的配置。永久解决方案，对此bug修复的版本的升级。

Q. IME工作站为什么建立对被管理的服务器的不变联系尽管客户端关门？

A. IME功能作为两Windows服务和GUI客户端。当客户端关闭时，两Windows服务(Cisco IPS Manager Express和MySQL IME)在本地MySQL数据库继续从被管理的传感器运行和收集事件和存储他们;这允许历史报告发生。

IME客户端应该打开单个SDEE订阅到被管理的传感器，并且重新使用随后的事件检索活动的此订阅。从IME工作站的不变连接被管理的传感器的是预料之中的行为。

Q. 能使用AIP-SSM模块， SPAN目标？

A. 不能。不可能使用AIP-SSM模块，因为SPAN目标，用于只监控流经ASA接口的流量。

Q. 在IPS升级到E3引擎后，高CPU使用情况为什么被观察？

A. 使用E3引擎更新， IPS使用一种不同的算法管理其空闲时间并且度过数据包的更多时间?能减少延迟。这增加检查导致在CPU使用情况的一个相应增加。正确方式测量在E3的CPU是没有由CPU使用情况，然而由显示正确CPU利用率的**信息包负载百分比**。

Q. 为什么间歇地是健康状态LED启用的RED在IPS设备？

A. 这能发生由于在远程maanagement站点的一不正确证书，运行软件例如CS-MARS， CSM、IEV、VMS-IDS/IPSMC等等为了解决此问题，完成这些步骤：

1. 应用在远程管理站点的传感器的TLS证书。
2. 配置一个有效DNS服务器。

Q. IPS如何从延迟HTTP数据流被终止，当横断其接口时？

A. 配置传感器工作在不对称模式将解决问题。为了放置传感器在不对称模式保护，请完成这些步骤：

1. 去**Configuration>策略> IPS策略**。
2. 双击**虚拟传感器**。
3. 去**提前选项**。
4. 下面请规范化模式，选择**不对称模式保护**。
5. 单击 **Ok**。
6. 重新启动单元为了更改能生效。

相关信息

- Cisco Secure入侵防御系统支持页面
- AIP-SSM故障排除
- 安全产品的问题信息通告（Field Notice）(包括CiscoSecure Intrusion Detection)
- 技术支持和文档 - Cisco Systems