

诊断数据的集从在Linux运行的FireAMP连接器的

目录

[简介](#)

[生成诊断文件](#)

[调试模式](#)

[请使用AMP控制台](#)

[启动调试模式](#)

[禁用调试模式](#)

[请使用Line命令](#)

[启动调试模式](#)

[禁用调试模式](#)

[相关信息](#)

简介

本文描述步骤生成从在Linux运行的FireAMP连接器的诊断文件。如果遇到一个技术问题用在Linux运行的FireAMP连接器，思科技术支持工程师也许要分析日志消息可用在诊断文件。

生成诊断文件

使用使用此命令，您能生成诊断文件直接地从Linux命令行界面(CLI)：

```
/opt/cisco/amp/bin/ampsupport
```

这创建在您的桌面的一个.7z文件。您能提供此文件给Cisco技术支持中心(TAC)为进一步分析。

调试模式

FireAMP连接器的调试模式提供另外的冗余给记录日志。它准许更多见解到一问题用连接器。此部分描述如何启动在FireAMP连接器的调试模式。

警告：应该启用调试模式，只有当思科要求此数据。如果启动最长时间的调试模式，非常迅速填满磁盘空间并且也许防止支持诊断文件采集**连接器**日志由于额外的文件大小。

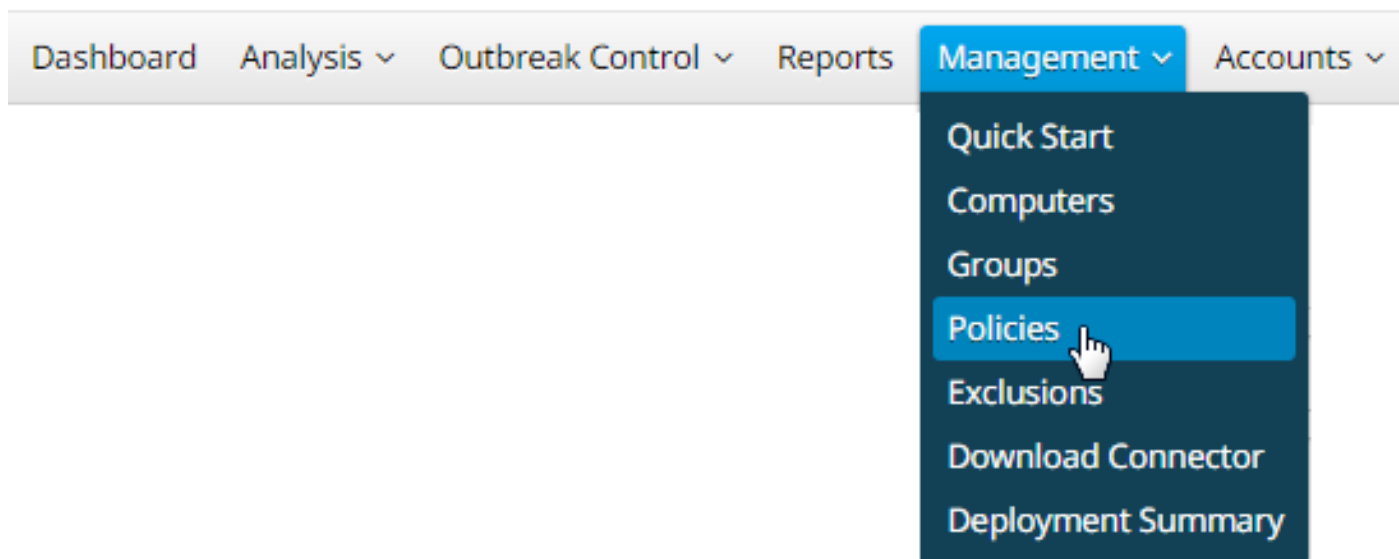
请使用AMP控制台

启动调试模式

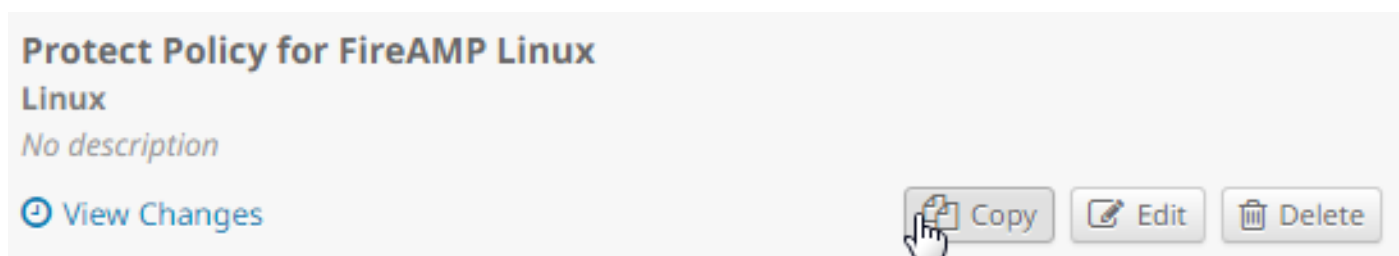
您能启动在当前策略的调试模式与步骤5 - 7或者创建在调试模式的一项新的策略与所有这些步骤：

步骤1.登录FireAMP控制台。

步骤2.选择Management>策略。



步骤3.找出应用到终端设备或计算机的策略并且点击“Copy”。



第四步：在您点击“Copy”后，与复制的策略的FireAMP控制台更新。



步骤5.单击编辑然后单击管理功能。

< Edit Policy: Copy of Protect Policy for FireAMP Linux

Policy for Linux

Name	<input type="text" value="Copy of Protect Policy for FireAMP Linux"/>
Description	<input type="text"/>

CUSTOM DETECTIONS

Simple	<input type="text" value="Quick SCD"/>
Advanced	<input type="text" value="None"/>

APPLICATION CONTROL

Blocking	<input type="text" value="None"/>
Whitelisting	<input type="text" value="Custom Whitelist"/>

NETWORK

IP Blacklists & Whitelists	<input type="button" value="Edit"/>
----------------------------	-------------------------------------

Exclusions

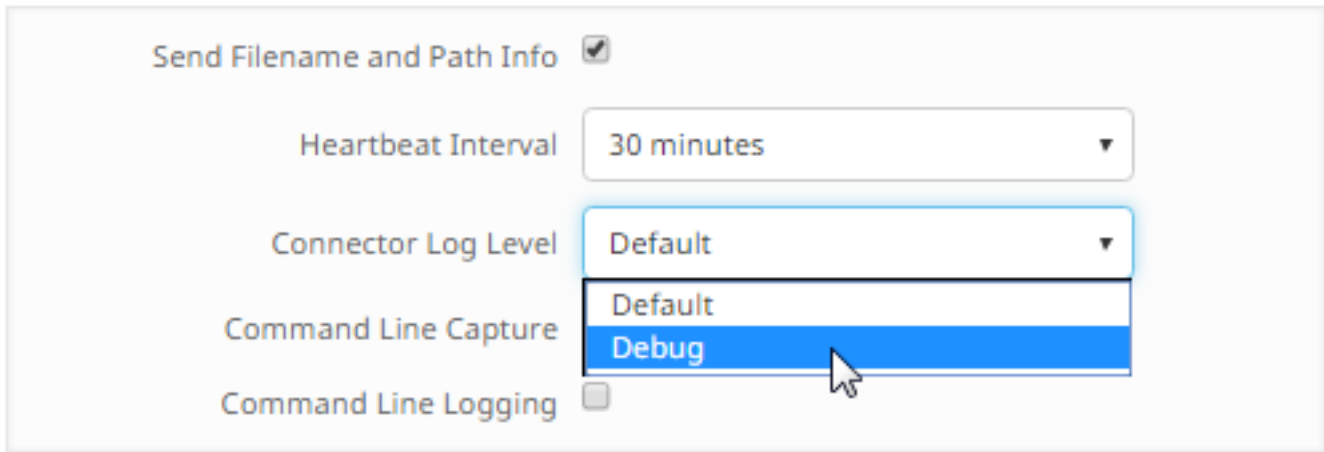
General | File | Network

Administrative Features

Send Filename and Path Info	<input checked="" type="checkbox"/>
Heartbeat Interval	<input type="text" value="30 minutes"/>
Connector Log Level	<input type="text" value="Default"/>
Command Line Capture	<input checked="" type="checkbox"/>
Command Line Logging	<input type="checkbox"/>

第六步：对于连接器日志级别，请选择从下拉列表的调试。

Administrative Features



Send Filename and Path Info

Heartbeat Interval 30 minutes ▼

Connector Log Level Default ▼

Command Line Capture

Command Line Logging

步骤7. 点击**更新策略**为了保存更改。

步骤 8在您更新策略后，您需要更改您的组包括您要生成调试信息的终端设备。

禁用调试模式

要禁用调试模式，请通过步骤和一样您完成启动调试模式，但是更改级连接器的日志默认。

请使用Line命令

启动调试模式

如果遇到对门户的任何连通性问题，并且要启动调试模式，请运行这些on命令CLI：

```
/opt/cisco/amp/bin/ampcli  
ampcli>debuglevel 1
```

这是输出：

```
ampcli>debuglevel 1  
Daemon now logging at 'info' level until next policy update
```

禁用调试模式

要禁用调试模式，请使用这些命令：

```
/opt/cisco/amp/bin/ampcli  
ampcli>debuglevel 0 Daemon now logging at 'notice' level until next policy update
```

相关信息

- [诊断数据的集从—FireAMP连接器运行的Windows](#)
- [诊断数据的集从—FireAMP连接器运行的Mac OS](#)
- [技术支持和文档 - Cisco Systems](#)