IPS MC传感器版本信息是过时的

目录

简介 先决条件 要求 使用的组件 规则 背景信息 问题 解决方案 删除传感器子组 从传感器组中删除传感器 创建传感器子组 将传感器添加到传感器组 验证 使用进度查看器 查看设备统计信息 相关信息

<u>简介</u>

本文档介绍如何向IPS MC层次结构添加组和传感器以及如何执行其他任务,如如何使用进度查看器 (用于后台任务的状态和确认)以及如何查看设备统计信息。

使用IPS传感器管理中心(IPS MC)在IDS上安装签名。成功更新签名后,更新的签名信息不会显示在 IPS MC中,但会显示在IDS的**show version**命令输出中。

<u>先决条件</u>

<u>要求</u>

本文档没有任何特定的要求。

<u>使用的组件</u>

本文档不限于特定的软件和硬件版本。

<u>规则</u>

有关文档规则的详细信息,请参阅 Cisco 技术提示规则。



IPS MC作为Web服务器在Windows 2000和Solaris 8(Sun 2.8)平台上运行。使用您选择的Web浏览 器作为Web客户端,以使用CiscoWorks界面登录IPS MC。通过CiscoWorks登录后,您可以查看 IPS MC接口。

在安装IPS MC之前,必须安装CiscoWorks Common Services。

在启动IPS MC之前,先启动CiscoWorks Common Services。

- Windows操作系统上带Service Pack 1的Microsoft® Internet Explorer 6.0
- Windows操作系统上的Netscape® Navigator 7.1

IPS MC使用组和传感器的层次结构。组可以包含传感器、其他组或传感器和组的组合。启动IPS MC时,始终至少有一个活动定义的组。这是全局组。IPS MC层次结构可以包含许多级别的组和传 感器,类似于Windows 2000中包含许多级别的文件夹和文件的文件夹。

组和传感器的IPS MC层次结构允许您一次配置多个传感器,因为传感器可以从其父组获取设置。如 果父级将这些设置定义为强制设置,则传感器必须从父组获取设置。子项无法覆盖此类设置的值。

问题

使用IPS MC升级签名后,IPS MC中的版本信息(如签名版本)将显示为过期。

<u>解决方案</u>

解决方法是删除并重新安装传感器。完成本文档中介绍的步骤以删除和添加传感器。

从Devices(设备)选项卡,您可以控制要使用IPS MC管理的传感器。可以添加和删除传感器和传 感器组。但是,不能删除全局组。如果已在其他位置建立设置,可以将其应用于从Devices选项卡设 置的传感器和组。有关如何执行特定任务的分步步骤,请参阅以下各节:

- 删除传感器子组
- 从传感器组中删除传感器
- 创建传感器子组
- 将传感器添加到传感器组

<u>删除传感器子组</u>

可以从任何传感器组(包括全局组)中删除任何子组。"全局"组是您无法删除的唯一组。

要删除传感器组,请完成以下步骤:

1. 选择**Devices > Sensor Group**。出现"Sensor Group(传感器组)"窗口。

⊡ 🔁 illustrations
Create Subgroup Edit Delete

- 在树中,选择要删除的组。注意:如果您选择删除传感器组,IPS MC不会要求您确认您的选择。
- 3. 单击删除。Sensor Group窗口再次出现,您刚删除的组不会显示在其父组下。

<u>从传感器组中删除传感器</u>

可以从任何传感器组(包括Global组)中删除传感器。

要从传感器组中删除传感器,请完成以下步骤:

1. 选择**Devices > Sensor**。出现"Sensor(传感器)"窗口。

Sensor					
All	Selection				
800	Global				
¢⊡•	Austin				
	Fourex				
	fivex				
	East				
·	West				
		Odd	Pe Import	Peboot	Belete
Research		Aud	Re-import	Rebuut	Delete

- 2. 在树中,选择要删除的传感器。
- 3. 单击删除。系统将显示一个对话框,要求您确认删除。
- 4. Click OK.Sensor(传感器)窗口刷新,显示传感器已删除。

Are Here: • Devices > Sen	sor Actions & Notifications:	🢵 📑 🜔 🎎 🚊 🛛
	Sensor	
	All Selection	Instructions This page allows yo to Add, Delete or Re- Import sensors. To Delete or Re-Import select items in the tr and then click Delete Re-Import. To Add, click Add at you will then enter a wizard that will guid you through the process. Help

创建传感器子组

可以向任何传感器组添加子组,其中包括Global组。

要创建传感器子组,请完成以下步骤:

1. 选择Devices > Sensor Group。出现"Sensor Group(传感器组)"窗口。

	⊟ 🔄 Global			
		Create Subgroup	Edit	Delete
2				
۷.	在例下,透开安问关亦加了纽约传感相纽的口标。			
З	单 击" ብ 建 子 归 "			
3. ⊿	单击" 创建子组 "。 左祖夕宫段山,输入贾汤加的乙组的夕称,单 共"默 礼	(佶"(佶田公佶) 畄	土"凵仴信	■判讼署
3. 4.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 " 然后从关联团表框中选择组的名称	\值"(使用父值) 。单	击 "从组复	夏制设置
3. 4.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK 系统将显示Sonsor Group窗口并显示你添加	∖值"(使用父值) 。单 [∶] □的 佐 咸哭곷细	击" 从组复	夏制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK .系统将显示Sensor Group窗口并显示您添加	值"(使用父值) 。单□ □的传感器子组。	击"从组复	夏制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK .系统将显示Sensor Group窗口并显示您添加 <mark>同全 Glubal</mark>	∖值"(使用父值) 。单 □的传感器子组。	击" 从组复	〔 制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK .系统将显示Sensor Group窗口并显示您添加 Click illustrations	∖值"(使用父值) 。单 □的传感器子组。	击" 从组 复	〔 制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK .系统将显示Sensor Group窗口并显示您添加 Click OK .系统将显示Sensor Group窗口并显示您添加	∖值"(使用父值) 。单 □的传感器子组。	击" 从组复	〔 制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK .系统将显示Sensor Group窗口并显示您添加	∖值"(使用父值) 。单 □的传感器子组。	击" 从组复	【制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK .系统将显示Sensor Group窗口并显示您添加 Click OK .系统将显示Sensor Group窗口并显示您添加	∖值"(使用父值) 。单 □的传感器子组。	击" 从组复	〔 制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK .系统将显示Sensor Group窗口并显示您添加	值"(使用父值) 。单 的传感器子组。	击" 从组 复	〔 制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK.系统将显示Sensor Group窗口并显示您添加 Click July Clubal	∖值"(使用父值) 。单 □的传感器子组。	击" 从组 复	€制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK .系统将显示Sensor Group窗口并显示您添加	∖值"(使用父值) 。单 □的传感器子组。	击"从组复	〔 制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK.系统将显示Sensor Group窗口并显示您添加	值"(使用父值) 。单 的传感器子组。	击"从组复	€制设置
 3. 4. 5. 	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK.系统将显示Sensor Group窗口并显示您添加 Click OK.系统将显示Sensor Group窗口并显示您添加	\值"(使用父值) 。单 口的传感器子组。	击"从组复	2制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK.系统将显示Sensor Group窗口并显示您添加	\值"(使用父值) 。单 口的传感器子组。	击"从组复	2制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK.系统将显示Sensor Group窗口并显示您添加 Click Julial	【值"(使用父值) 。单 四的传感器子组。	击"从组复	2制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK.系统将显示Sensor Group窗口并显示您添加 Click OK.系统将显示Sensor Group窗口并显示您添加	\值"(使用父值) 。单 口的传感器子组。	击"从组复	2制设置
3. 4. 5.	单击" 创建子组 "。 在组名字段中,输入要添加的子组的名称。单击 "默认 ",然后从关联列表框中选择组的名称。 Click OK.系统将显示Sensor Group窗口并显示您添加 Click OK.系统将显示Sensor Group窗口并显示您添加	、值"(使用父值)。单 如的传感器子组。 Crcate Subgroup	击"从组复	E制设置

将传感器添加到传感器组

您可以将传感器添加到任何传感器组,其中包括Global组。"添加传感器向导"将引导您完成此过程。 添加传感器有三种方法:

- 创建默认设备
- •从现有传感器导入配置
- •导入.csv或.xml格式的传感器列表

本文档提供手动添加传感器的步骤的详细信息。"添加传感器向导"中提供了另外两种方法:

- 导入存在的传感器
- •从列表中添加多个传感器

<u>导入存在的传感器</u>

要导入存在的传感器,请完成以下步骤:

- 1. 选择**从设备导**入配置(请参阅<u>Manually Add a Sensor to a Sensor Group(手动将传感器添加到</u> <u>传感器组)过程中的</u>步骤3)。
- 2. 确定要添加的传感器。
- 3. 确认显示的摘要信息。

从列表添加多个传感器

要从列表中添加多个传感器,请完成以下步骤:

- 1. 按照安装期间复制到IPS MC安装目录的示例文件所示的方式,以.csv或.xml格式准备传感器列 表。**注意:**示例.csv格式和.xml格式文件位于:InstallDirectory\MDC\etc\ids\ and are named MultipleAddDevices-format.csv和MultipleAddDevices-format.xml。
- 选择Add Multiple devices(添加多个设备)(请参<u>阅Manually Add a Sensor to a Sensor</u> Group(手动将传感器添加到传感器组))。
- 3. 确定列表的格式(.csv或.xml)。
- 4. 指定列表。
- 5. 确认显示的摘要信息。

<u>手动将传感器添加到传感器组</u>

要手动将传感器添加到传感器组,请完成以下步骤:

1. 选择**Devices > Sensor**。出现"Sensor(传感器)"窗口。

Are Here: • Devices > Sensor		Actions & Notifications: 🧏) 🖆 🖒 🧶 🛎
	All Selection		Instructions This page allows you to Add, Delete or Re- Import sensors. To Delete or Re-Impor select items in the tre and then click Delete of Re-Import. To Add, click Add and you will then enter a wizard that will guide you through the process. Help

2. 单击 Add。"添加传感器向导"打开并显示"选择类型"窗口。

You Are Here:		Actions & Notifications:	Sa 🖻
Mode: ADDING 1. Select Type 2	Select Type		Ins Select want sens impor from multig
	Add type C Import configuration from device C create default configuration		Help
	C Add multiple devices		

- 3. 选择**创建默认配置。注:本**节前面部分显示了替代方法选择、从设备导入配置和添加多个设备 的摘要。
- 4. 单击 Next。系统将显示Select Sensor Group(选择传感器组)窗口。

ou Are Here: • Devices > Sensor		Actions & Notifications:	- 🐘 📑	🌔 🤼 💈	
Moster Approx	Select Sensor Group				
Moud: Muulins			Inst	ructions	
2 Select Group			The se	ensor will be	
3. Enter Sensor			added	to the group	
Information	Select Sensor Group	selecti	selected on this page.		
4. Summary					
			Help		
	Cr _ Austin				
	- Step 2 of 4 -			HI HI	
		Back Next > Finit	sh.	Cancel	

- 5. 选择要向其添加传感器的组。
- 6. 单击 Next。系统将显示Enter Sensor Information(输入传感器信息)窗口。注意:"输入传感器信息"窗口因传感器类型而异。显示的窗口反映了上次添加的传感器类型。

You Are Here: Oevices Sensor			Actions & Notifications:
Mode: ADDING	Enter Sensor Information		
 ✓ 1. Select Type ✓ 2. Select Group 	ID Address	44 55 66 77	_
3, Enter Sensor Information	NAT Address:		-
4. Summary	Sensor Name:	West	-
	User ID:*	cisco	-
	Password: (or pass phrase if using existing SSH keys): *	•••••	
	Port	443	
	Enable TLS:	v	
	Version	5.1(0.5)S179.0 -	
	Anti-virus Version:	∨1.0 ▼	
	Comment		×
	NAT Address to MC		
	Note: * - Required Field Step 3 of 4 -	< Ba	nck Next > Finis

7. 提供输入传感器信息窗口所需的信息。注:星号(*)表示必填字段。从"版本"列表框中选择要添加的传感器的版本号。"输入传感器信息"窗口显示您选择的传感器类型和版本的字段。输入传感器的IP地址。输入传感器的NAT地址(如果有)。输入传感器名称。输入主机与传感器之间安全外壳(SSH)通信的用户ID和密码。注意:如果使用现有的SSH密钥,请在Password字段中输入密码短语。在端口(Port)字段中,查看默认值并根据需要进行更改。如果要启用TLS,请选中启用TLS复选框。从"版本"列表框中,选择要添加的传感器的版本号。从Anti-virus Version列表框中,根据需要选择要添加的传感器的防病毒版本号。注意:仅在使用此类版本时,才会显示防病毒版本列表框。输入注释(可选)。输入主机ID,通常是传感器IP地址的最后一个二进制八位数。根据需要,输入NAT地址到MC。单击 Next。系统将显示Sensor Information(传感器信息)窗口,其中包含Add Sensor Summary(添加传感器摘要)表信息。



- 8. 查看显示的传感器摘要信息。注意:如有必要,可单击"上一步"以返回并更改显示的信息。
- 9. 单击 完成。系统将显示Sensor(传感器)窗口,其中更新了您添加的传感器的记录。

All	Selection			
	lobal Austin Fourex Sis			
	ivex East West			

<u>验证</u>

使用进度查看器

对于每个传感器,进度查看器显示将配置部署到传感器、签名更新和从Cisco.com下载到IPS MC服 务器的状态和完成百分比。

要使用进度查看器,请完成以下步骤:

- 1. 选择"**设备">"进度查看器**"。"查看进度任务"窗口出现在当前浏览器窗口中。
- 2. 单击"查看进度任务"页底部的"新建窗口",以在新窗口中打开进度查看器。注意:您还可以单击路径栏中的进度查看器图标,以便在新窗口中直接打开进度查看器。
- 在"进度查看器"表中选择背景任务,然后单击"显示消息"以查看背景任务的消息。背景任务的 消息将显示在新浏览器窗口中。
- 4. 选择项目, 然后单击"删除"以从"进度查看器"表中删除消息。
- 5. 单击Refresh以刷新Progress Viewer表。
- 6. 选中**启用刷新率**复选框并从下拉列表中选择时间间隔以自动刷新页面。

<u>查看设备统计信息</u>

您可以查看IPS MC安装中设备的统计信息。统计信息不会实时更新。相反,它在请求信息时显示设 备组件的快照。

要显示设备的统计信息,请完成以下步骤:

- 1. 选择Devices > Statistics。
- 在对象选择器中,选择要查看其统计信息的设备。所选设备的组件列在"选择要查看的组件"标题下。
- 3. 从"选择要查看的组件"列表中选择设备组件。您可以从以下组件中选择统计信息:分析引擎身份验证被拒绝的攻击者事件服务器事件存储主机接口(仅5.x设备)记录器网络访问通知控制器SDEE服务器事务服务器交易来源版本/许可证虚拟传感器Web Server
- 4. 单击 View。报告将显示在新的浏览器窗口中。

相关信息

- Cisco IPS 4200系列传感器 故障排除技术说明
- <u>技术支持和文档 Cisco Systems</u>