了解和配置macOS服务ISE终端安全评估条件

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 确定要检查的服务名称
- （可选）检查服务的详细信息，以定义其是座席还是座席
- 选择要评估的服务运营商
- 已加载的服务
- 未加载的服务
- 已加载并运行
- 已加载退出代码
- 已加载并正在运行或使用退出代码
- 为此类条件配置要求和状态策略

验证

故障排除

- 证书不受信任
- 绕过Cisco安全客户端扫描
- 其他问题

简介

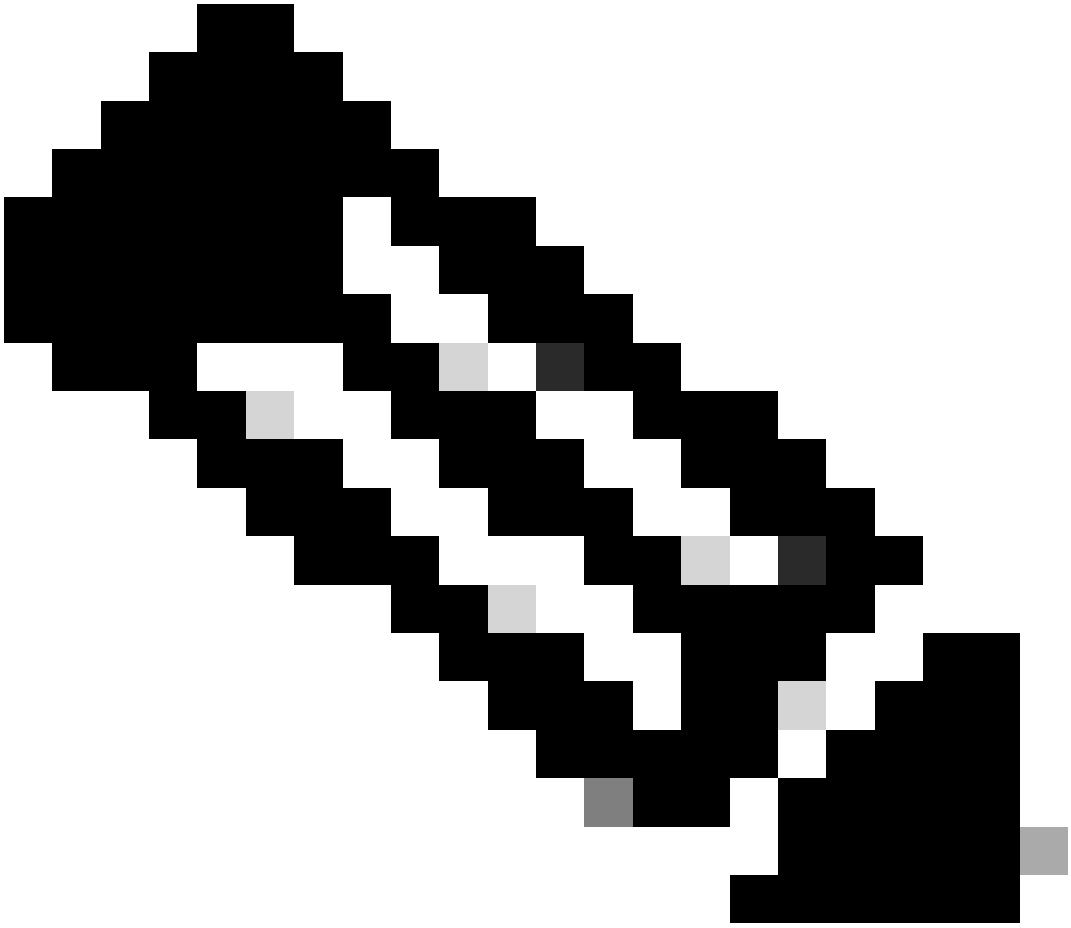
本文档介绍在思科ISE中配置macOS服务条件的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- MacOS基础知识。
- 了解ISE终端安全评估流程。



注意：本文档介绍macOS服务条件的配置。初始状态配置不在本文档中。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE 3.3补丁1
- 运行Sonoma 14.3.1的macoOS设备
- 思科安全客户端5.1.2.42
- 合规性模块版本4.3.3432.64000

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

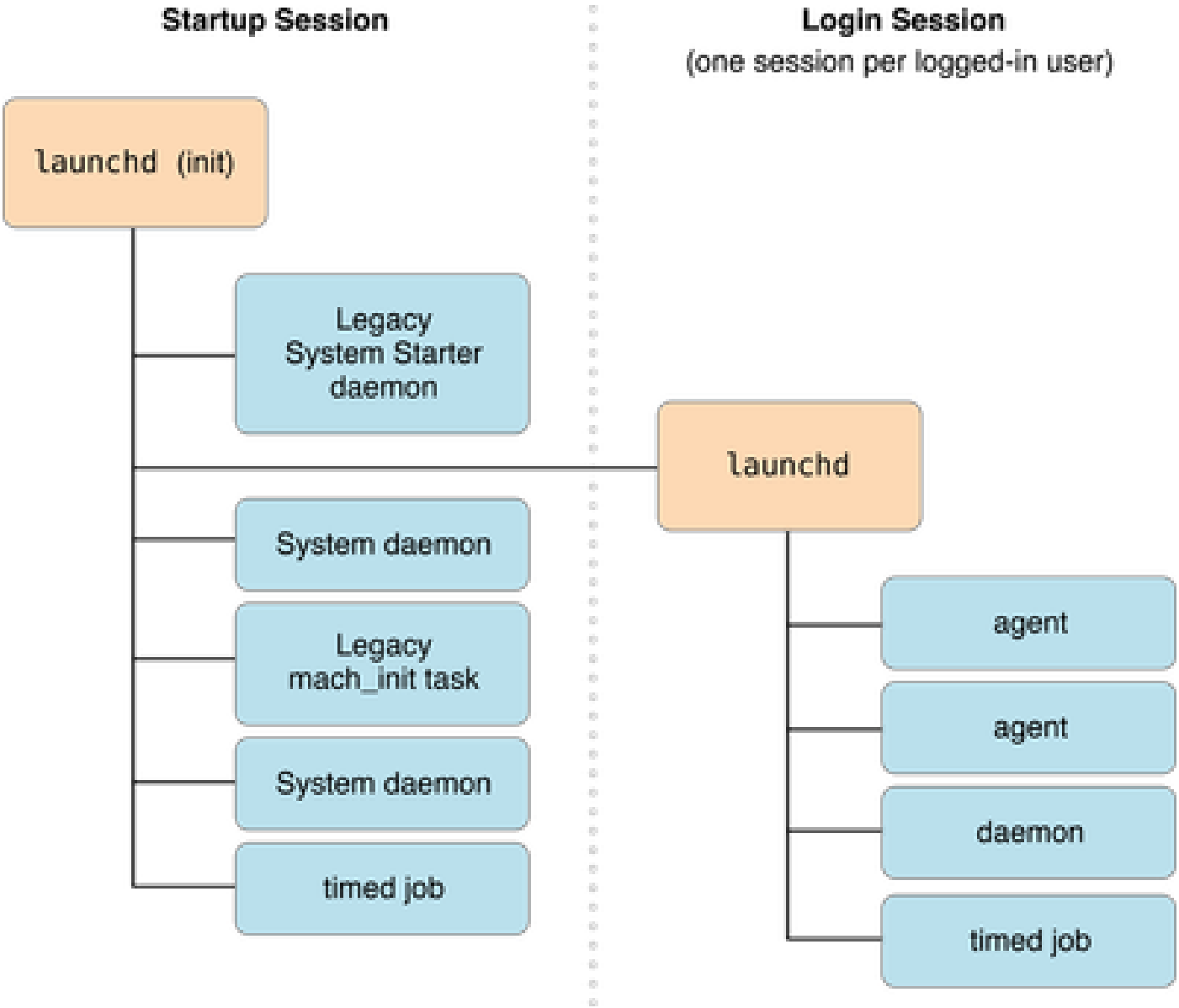
当必须使用用例检查服务是否已加载到macOS设备中时，macOS服务条件很有用，还可以检查服

务是否正在运行。macOS服务条件可以检查两种不同的服务类型：守护程序和代理。

后台守护程序是在后台作为整个系统的一部分运行的程序（也就是说，它不与特定用户关联）。守护程序无法显示任何GUI;更具体地说，它不允许连接到window服务器。Web服务器是守护程序的完美示例。

代理是代表特定用户在后台运行的进程。代理非常有用，因为它们可以执行守护程序无法执行的操作，例如可靠地访问用户的主目录或连接到windows服务器。日历监控程序是座席的一个很好的示例。

在下面的图表中，您可以看到如何根据设备启动和用户登录来加载每个设备：



有关守护程序和代理的更多信息，请参阅Apple文档

在以下位置可以找到您的macOS设备上可用的调试程序和代理：

位置	描述

~/库/启动代理	用户提供的每用户代理。
/Library/LaunchAgents	由管理员提供的每用户代理。
/Library/LaunchDaemons	由管理员提供的系统范围守护程序。
/System/Library/LaunchAgents	OS X每用户代理
/System/Library/LaunchDaemons	OS X系统范围守护程序

可以使用以下命令从macOS终端检查每个类别的列表：

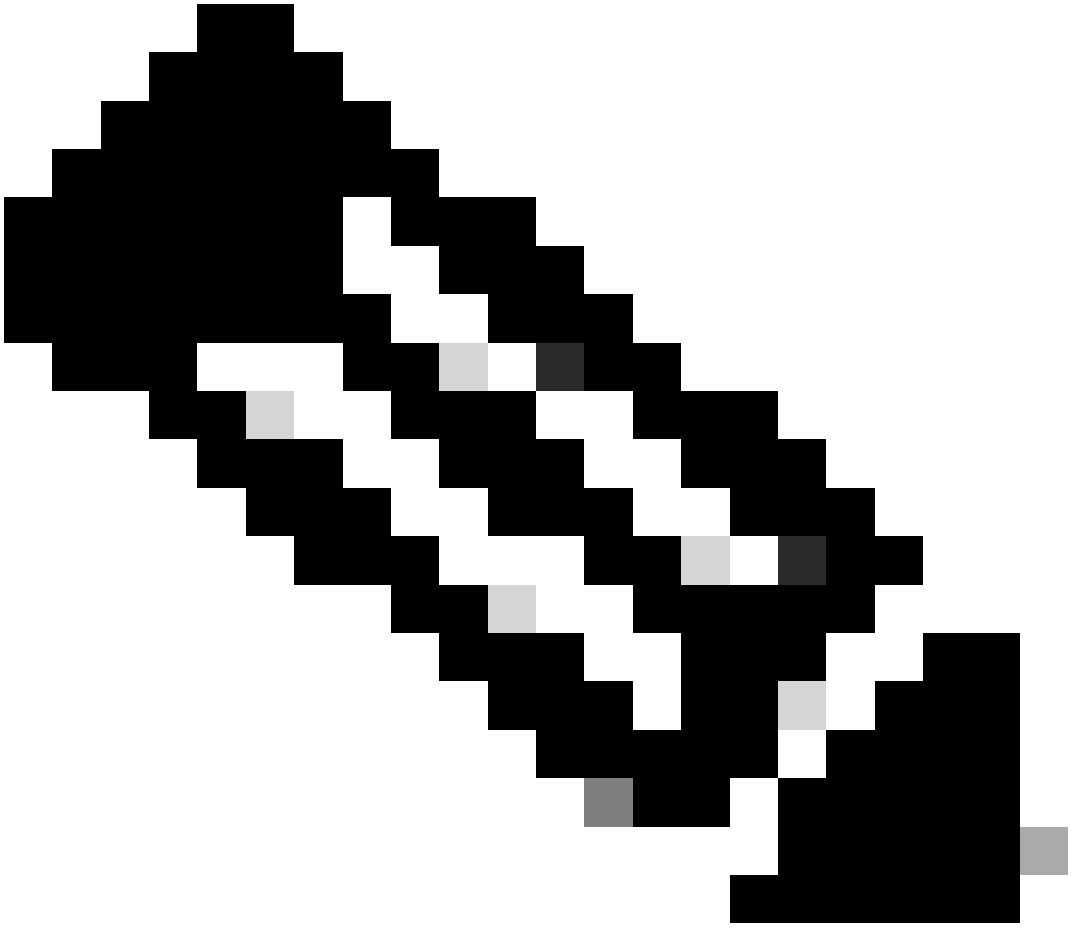
ls -ltr ~/Library/LaunchAgent
ls -ltr /Library/LaunchAgent
ls -ltr /Library/LaunchDaemons
ls -ltr /System/Library/LaunchAgents
ls -ltr /System/Library/LaunchDaemons

前面的位置可以显示macOS设备上可用的所有守护程序和代理，但并非所有守护程序和代理都已加载或运行。

配置

使用以下步骤可以配置macOS服务条件：

1.确定要检查的服务名称。
2.（可选）检查服务的详细信息，以定义其是座席还是管理员。
3.选择要评估的服务运营商。
4.为此类条件配置要求和状况策略。



注意：服务安全评估条件需要提升的权限才能工作，因此，必须确保ISE PSN受思科安全客户端（以前称为AnyConnect）信任 — 参考指南

确定要检查的服务名称

ISE终端安全评估合规性模块能够检查已加载、正在运行和已加载的服务，以及正在使用退出代码运行的服务。

要检查已加载的服务，请使用sudo launchctl dumpstate命令。

要检查已加载且具有退出代码的服务，请使用命令sudo launchctl list。

前面的命令可以突然显示许多信息，而只需使用这些命令来显示实际的服务名称：

要仅检查已加载的服务名称，请使用以下命令：

```
sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||'
```

要仅检查已加载的服务名称和退出代码，请使用以下命令：

sudo launchctl list | awk“{if(NR>1)print $3}”

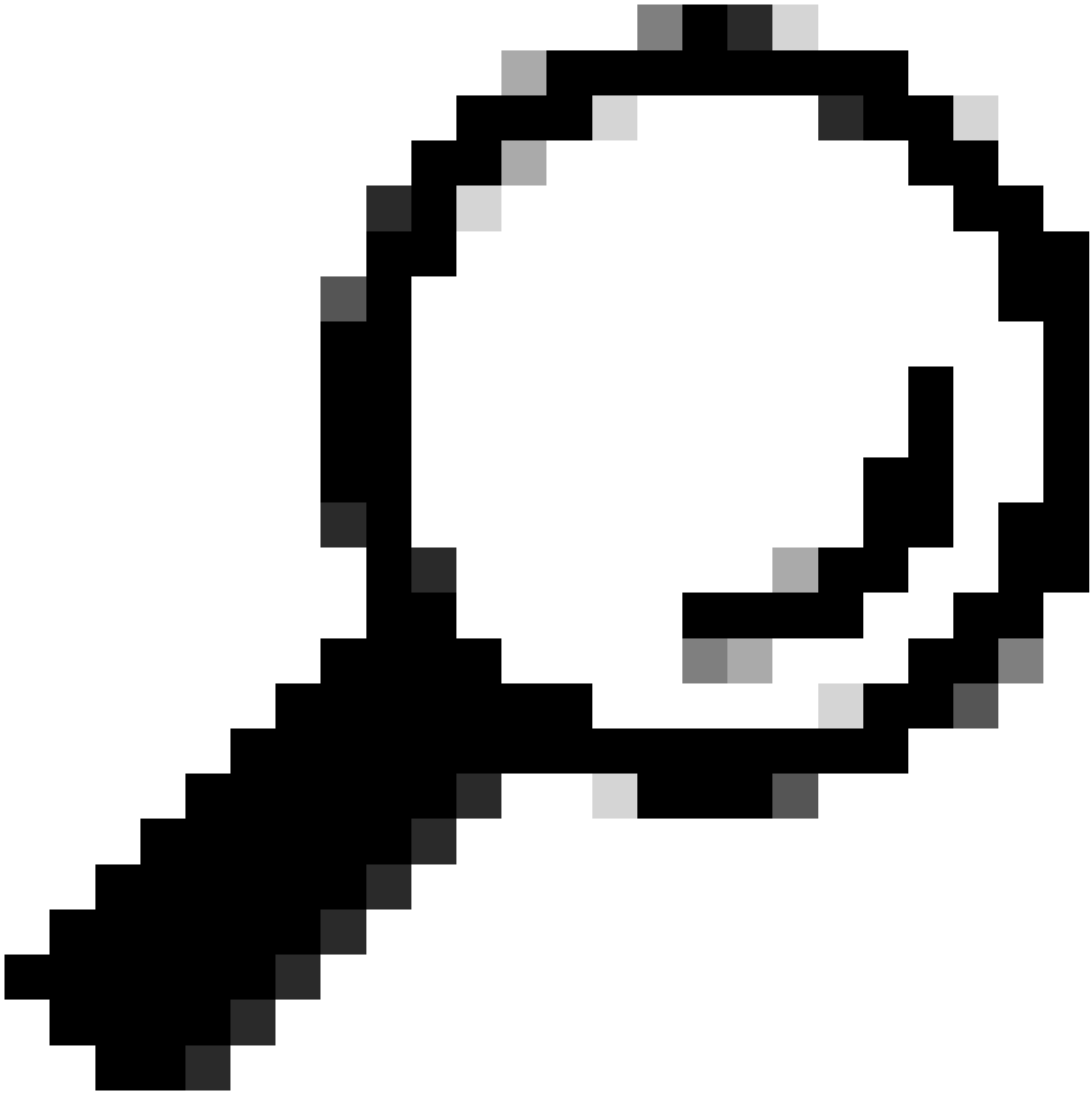
这些命令显示了许多信息，因此建议您在每个命令末尾使用另一个grep过滤器来查找要查找的服务。
例如，如果您正在查找供应商特定的服务，则可以在和处使用关键字作为过滤器。

对于思科服务，命令如下所示：

sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||' | grep -i cisco
sudo launchctl list | awk“{if(NR>1)print $3}” | grep -i cisco

（可选）检查服务的详细信息，以定义其是座席还是座席

在此条件配置的第二部分，您需要检查您的服务是守护程序类型还是代理类型。



提示：此步骤是可选的，因为ISE允许您为守护程序或用户代理选择选项，所以您可以只选择该选项并跳过此部分。

如果要在此情况下进行细化，可以通过以下操作检查类型：

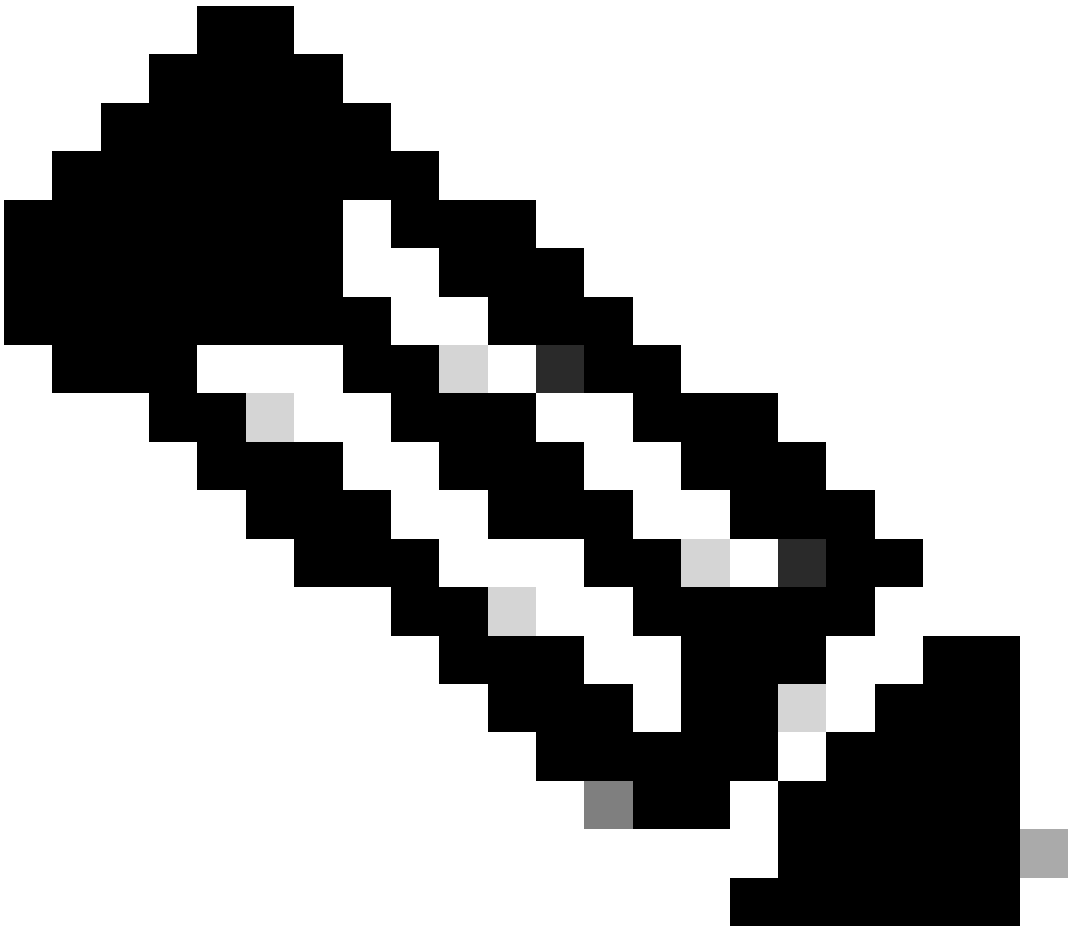
1. 首先，使用命令sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)"检查服务的完整launchctl名称 | grep -aiE "\/.*= {" | sed 's|.*/||;s| = {$||' | grep -i {您的服务名}

例如，对于命令sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed's/.\{3\}$/' | grep -i com.cisco.secureclient.iseposture，输出为：gui/501/com.cisco.secureclient.iseposture。

2.使用命令sudo launchctl print{ Your launchctl service name } | grep -i 'type = Launch'检查服务类型

按照示例，对于命令sudo launchctl print gui/501/com.cisco.secureclient.iseposture | grep -i 'type = Launch'，输出为： type = LaunchAgent。

这意味着服务类型为Agent，否则将显示为type = LaunchDaemon。



注意：如果信息为空，请在ISE中选择Daemon Or User Agent选项作为服务类型设置。

选择要评估的服务运营商

ISE允许您选择5个不同的服务运营商：

- 已加载
- 未加载
- 已加载并运行
- 已加载退出代码
- 已加载并正在运行或使用退出代码

已加载的服务

在使用以下两个命令时列出的所有服务是否都包含在内：

```
sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed
's|.*/||;s| = {$||'
sudo launchctl list | awk“{if(NR>1)print $3}”
```

未加载的服务

是定义了其属性列表(plist)但尚未加载的所有服务，还是甚至没有定义属性列表(plist)因而根本无法加载的服务。

这些服务不易识别，当您需要检查特定服务是否不应存在于macOS设备时，最常用于使用案例。例如，如果要阻止在macOS设备上加载缩放服务，可以将us.zoom.ZoomDaemon作为该服务的值，这样可以确保缩放未运行或根本没有安装。

有些服务无法卸载，并且已定义其属性列表。
例如，使用此命令，您可以看到dhcp6d plist已定义：

```
ls -ltr /System/Library/LaunchDaemons | grep com.apple.dhcp6d.plist
```

检查服务列表，可以看到未加载的项：

```
sudo grep -B 10 -A 10 -E "^\s*state = " << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed
's|.*/||;s| = {$||' | grep -i com.apple.dhcp6d
sudo launchctl list | awk“{if(NR>1)print $3}” | grep -i com.apple.dhcp6d
```

如果将该值设置为com.apple.dhcp6d，则macOS设备是合规的，因为即使定义了服务列表，也不会加载服务。

已加载并运行

并非所有服务都在运行，每个服务都有多种状态，如正在运行、未运行、等待、退出、未初始化等。
要检查正在运行的所有服务，请使用以下命令：

```
sudo grep -B 10 -A 10 -E "^\s*state = running" << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed
's|.*/||;s| = {$||'
```

使用上述命令列出的服务命中Loaded & Running service operator条件。

已加载退出代码

某些服务可能会以预期或意外的退出代码终止，此类服务可以通过命令列出：

sudo grep -B 10 -A 10 "state = e" << "$(launchctl dumpstate)" | grep -aiE "\/.*= {" | sed's/.\{3\}$/'

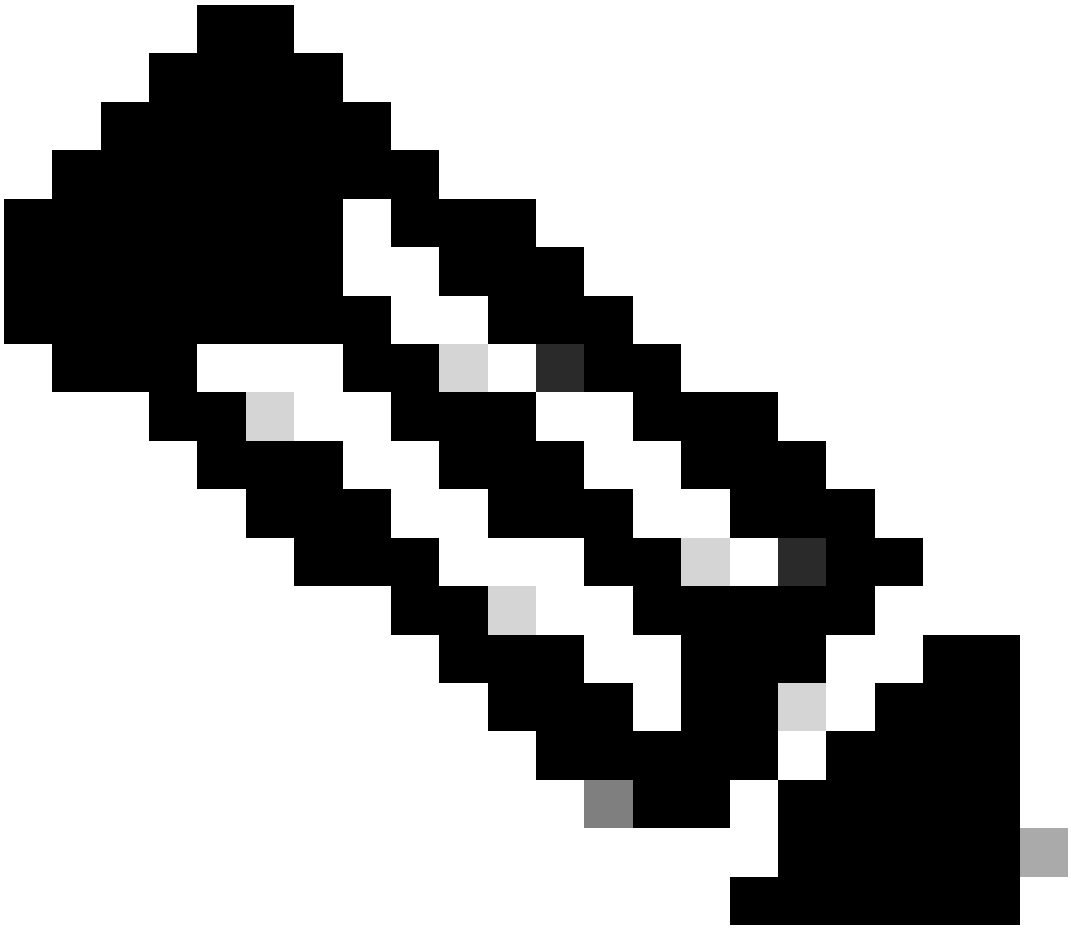
要了解其退出代码，您可以选择任何服务并使用命令：

sudo launchctl print {您的launchctl service name } | grep -i '最后一个退出代码'

例如：

sudo launchctl print gui/501/com.apple.mdmclient.agent | grep -i '最后一个退出代码'

其输出为：最后一个退出代码= 0

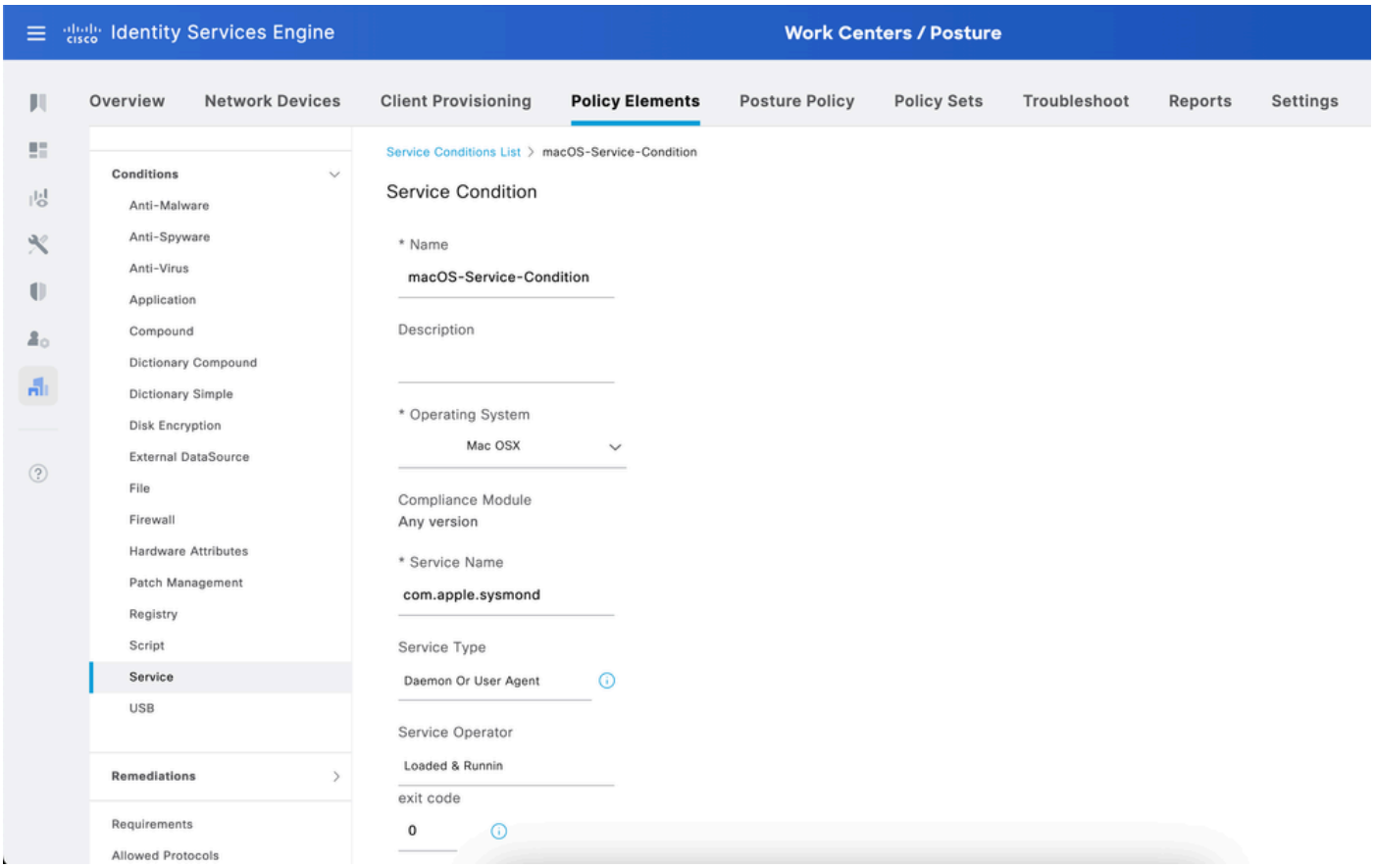


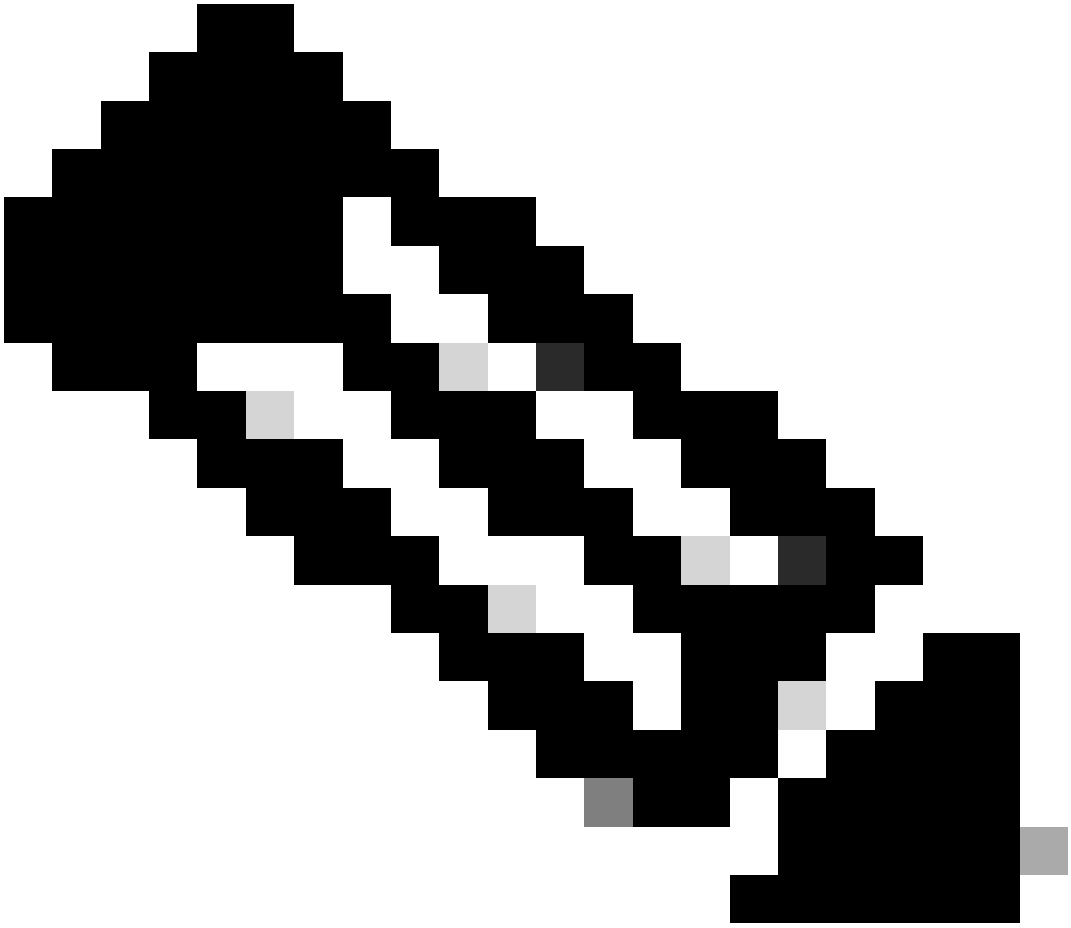
> 注意：在这里，退出代码0通常表示服务正确完成了一切。如果计算机与作为退出代码的0不匹配，则表示服务未执行预期操作。

已加载并正在运行或使用退出代码

当服务为Loaded & Running或Loaded with exit code时，最后一个选项起作用。

下图显示了macOS服务条件的示例。

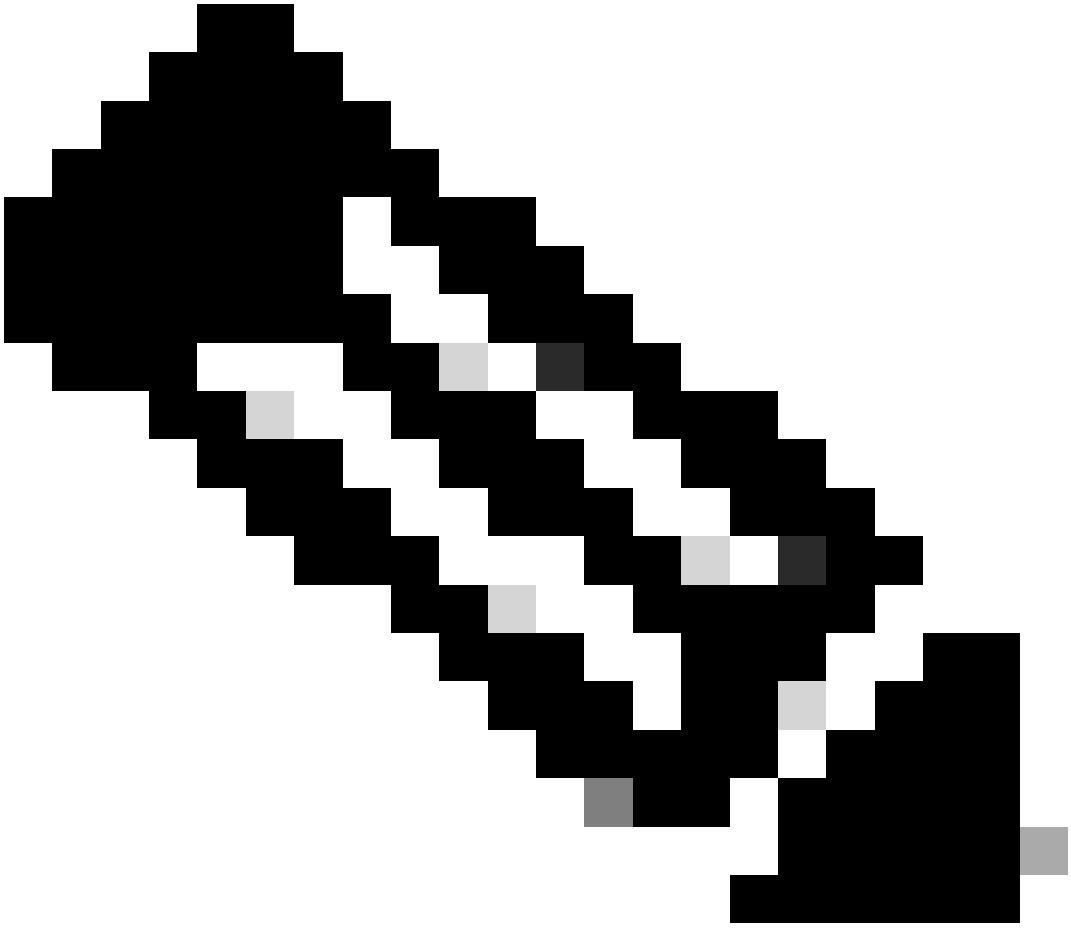




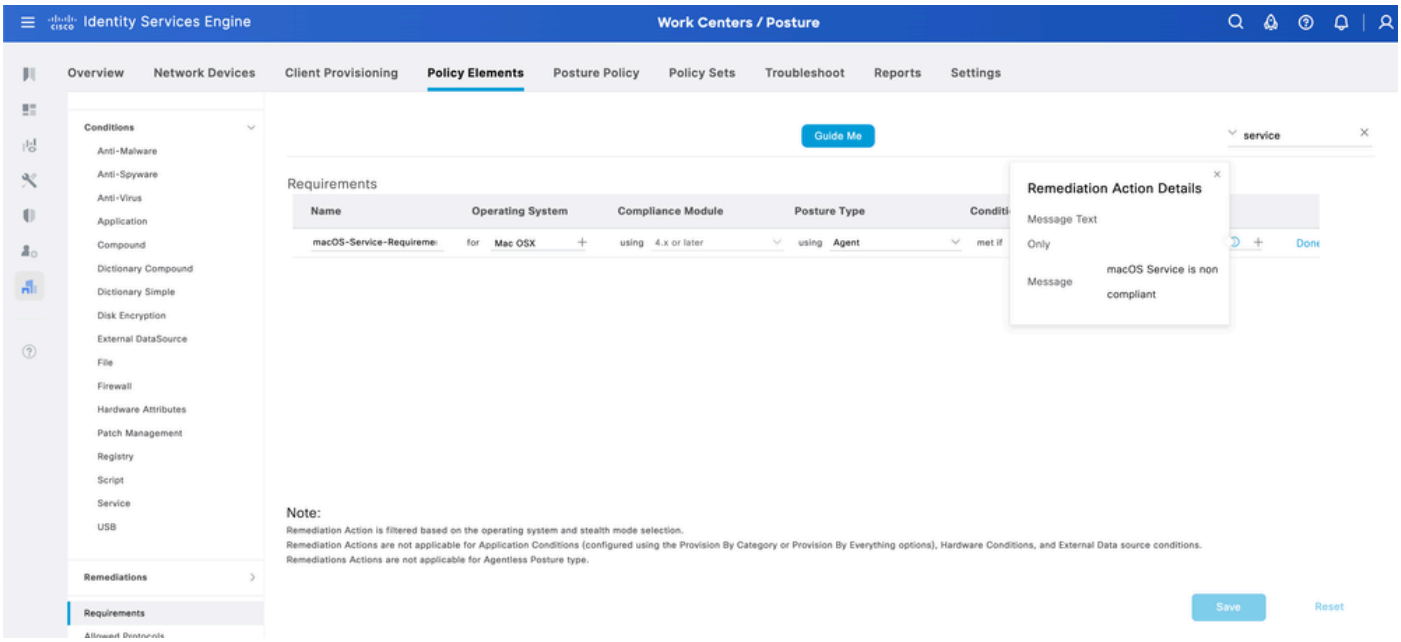
注意：目前，仅支持确切的服务名称。服务名称中有支持通配符的增强请求，Cisco bug ID CSCwf01373

为此类条件配置要求和状态策略

配置完条件后，您需要创建此类条件的要求，并为此要求使用Message Test Only选项。
导航到ISE > Work Centers > Posture > Requirements创建它。

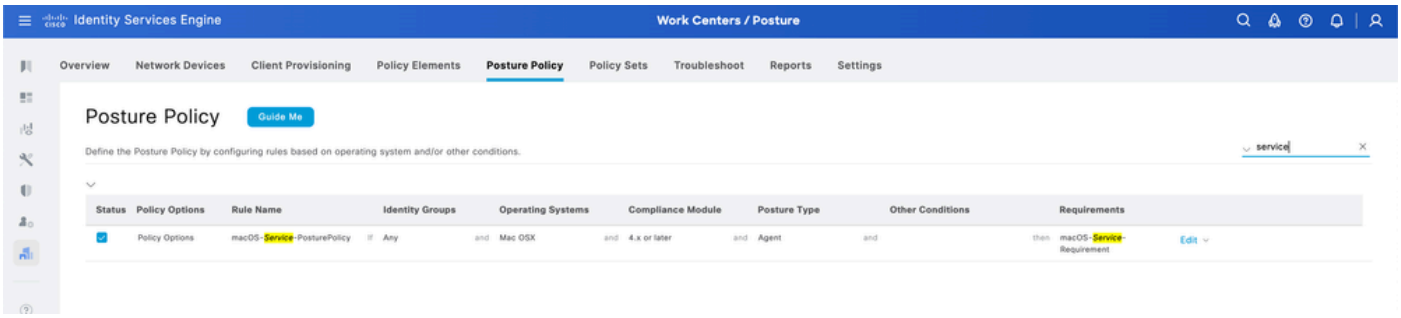


注意：服务条件没有补救选项。



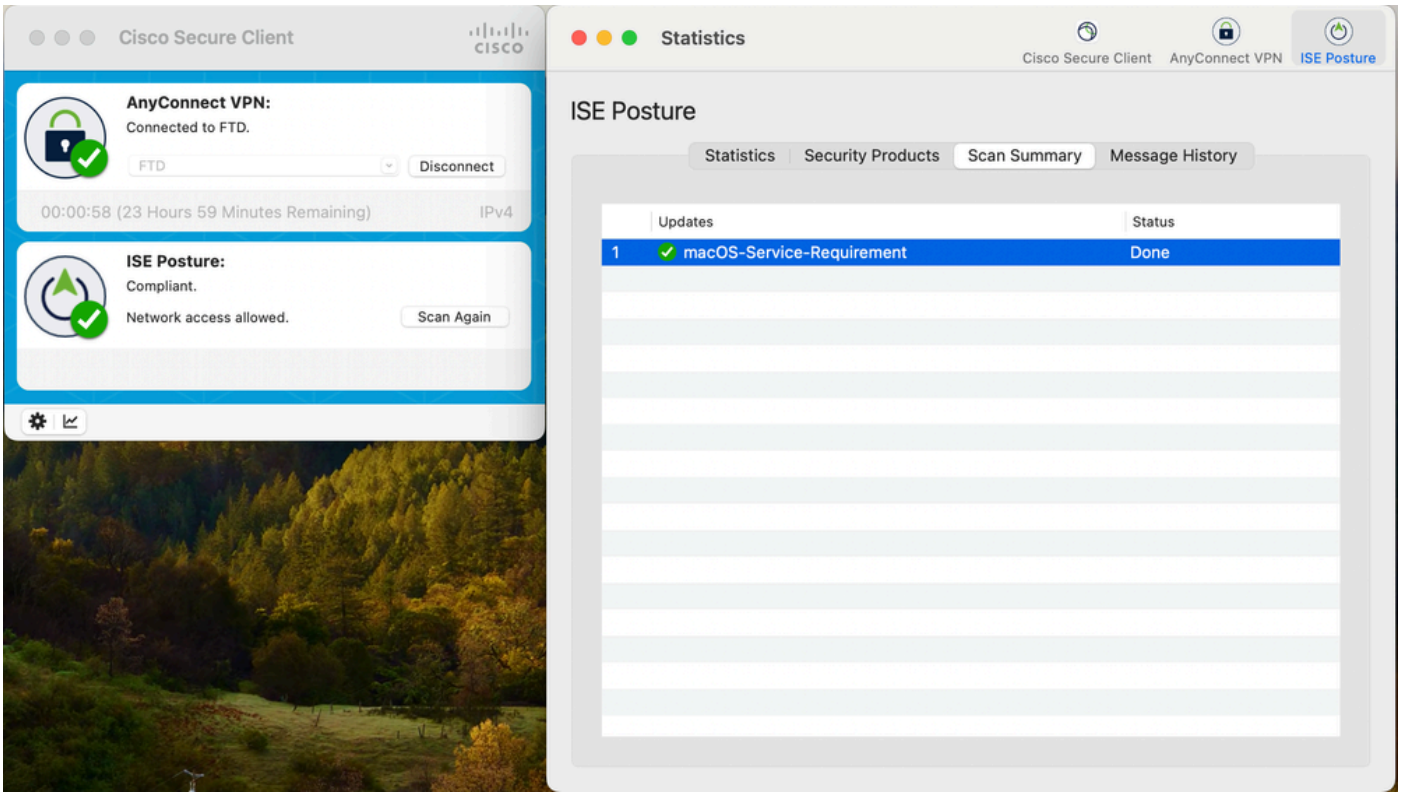
完成此操作后，最后一步是配置使用创建要求的终端安全评估策略。
导航到ISE > Work Centers > Posture > Posture Policy以创建策略。

启用新策略，根据需要命名它，然后选择刚创建的要求。

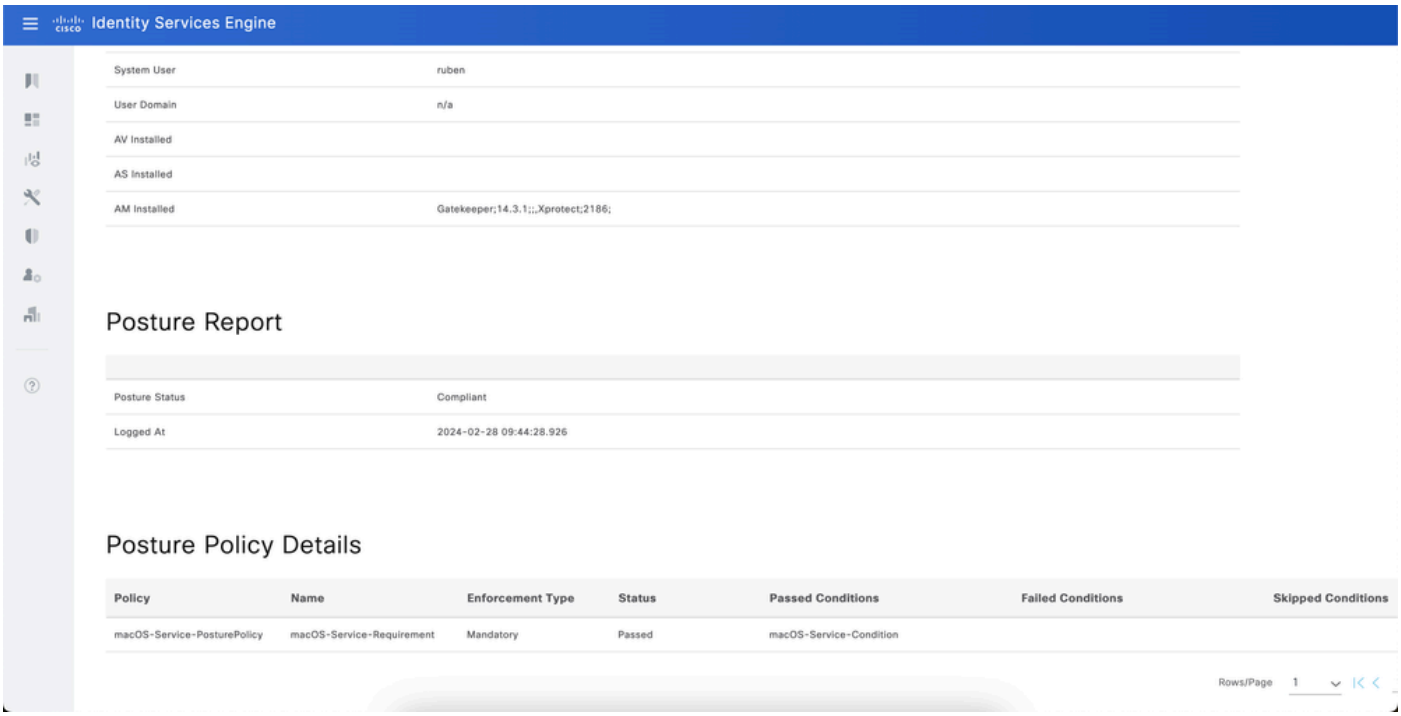


验证

您可以从Cisco安全客户端GUI本身验证macOS状态条件通过或失败。



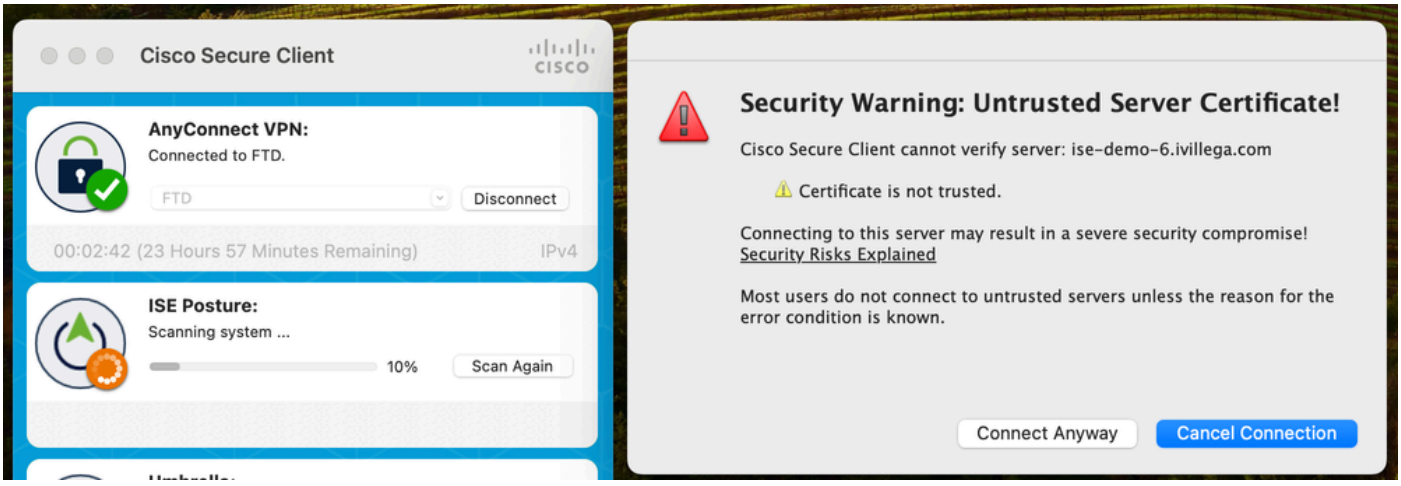
此外，您还可以从ISE > Operations > Reports > Reports > Endpoints and Users > Posture Assessment by Endpoint检查ISE终端安全评估。



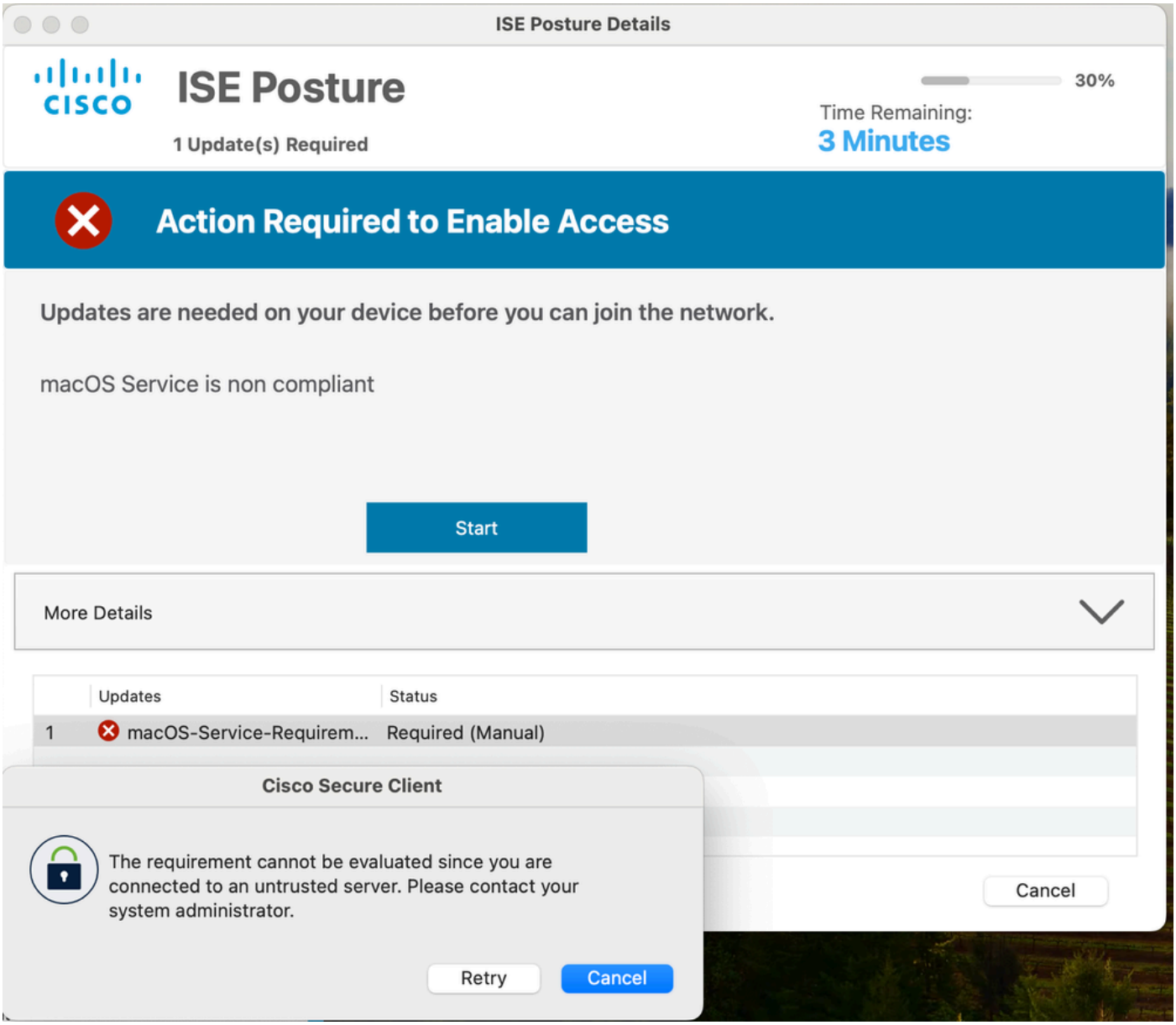
故障排除

配置此macOS服务状态条件时可能遇到的常见问题包括：

证书不受信任



如前所述，服务条件需要提升权限。状况扫描进程的证书必须受服务器信任。
否则会遇到如下错误：

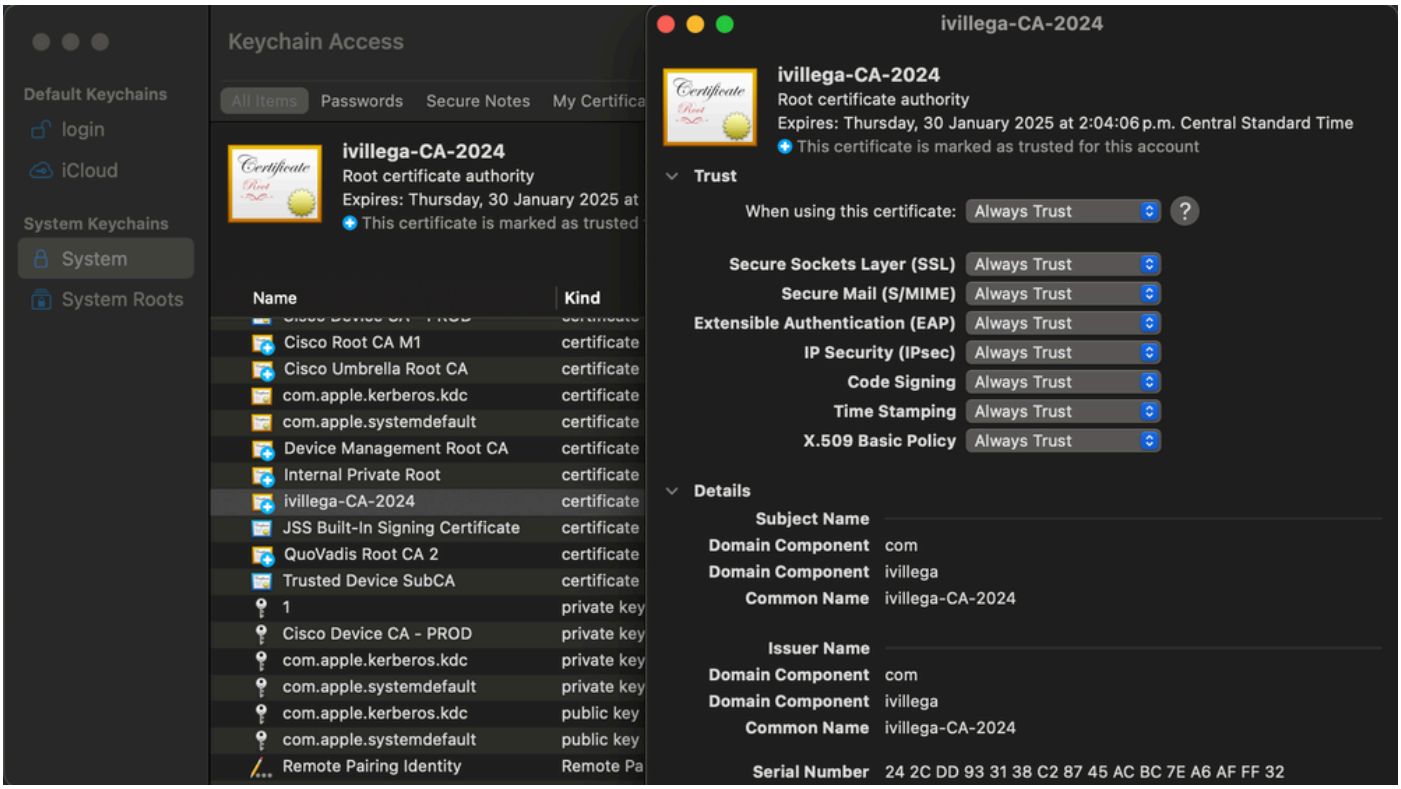


ISE终端安全评估模块通过IP地址或完全限定域名(FQDN)发现PSN服务器。 最佳实践是让安全评估配置文件通过FQDN发现ISE节点，因此Admin和Portal(Client Provisioning Portal)证书应该在CN字段或SAN字段中包含FQDN。您也可以为此使用通配符证书，此流支持通配符证书。

由于系统安全，CN字段在将来不可信。在SAN字段中包括通配符条目或FQDN作为最佳实践。

如果通过IP地址而不是FQDN发现ISE PSN，则要求节点的IP地址包含在与管理员和门户使用相关的证书的CN字段或SAN字段中。

ISE终端安全评估模块信任ISE服务器提供的证书。如果其CA在macOS Keychain access的系统证书存储中，则此CA应将When using this certificate设置为Always Trust。



您可能会遇到以下错误行为：即使正确加载了证书，并且满足所有CN和SAN要求，macOS系统仍不信任证书。在这种情况下，请打开Keychain access应用程序，导航到System certificate store选项卡，然后从该选项卡中删除CA证书。

然后，导航到macOS终端应用程序并执行以下命令：sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain

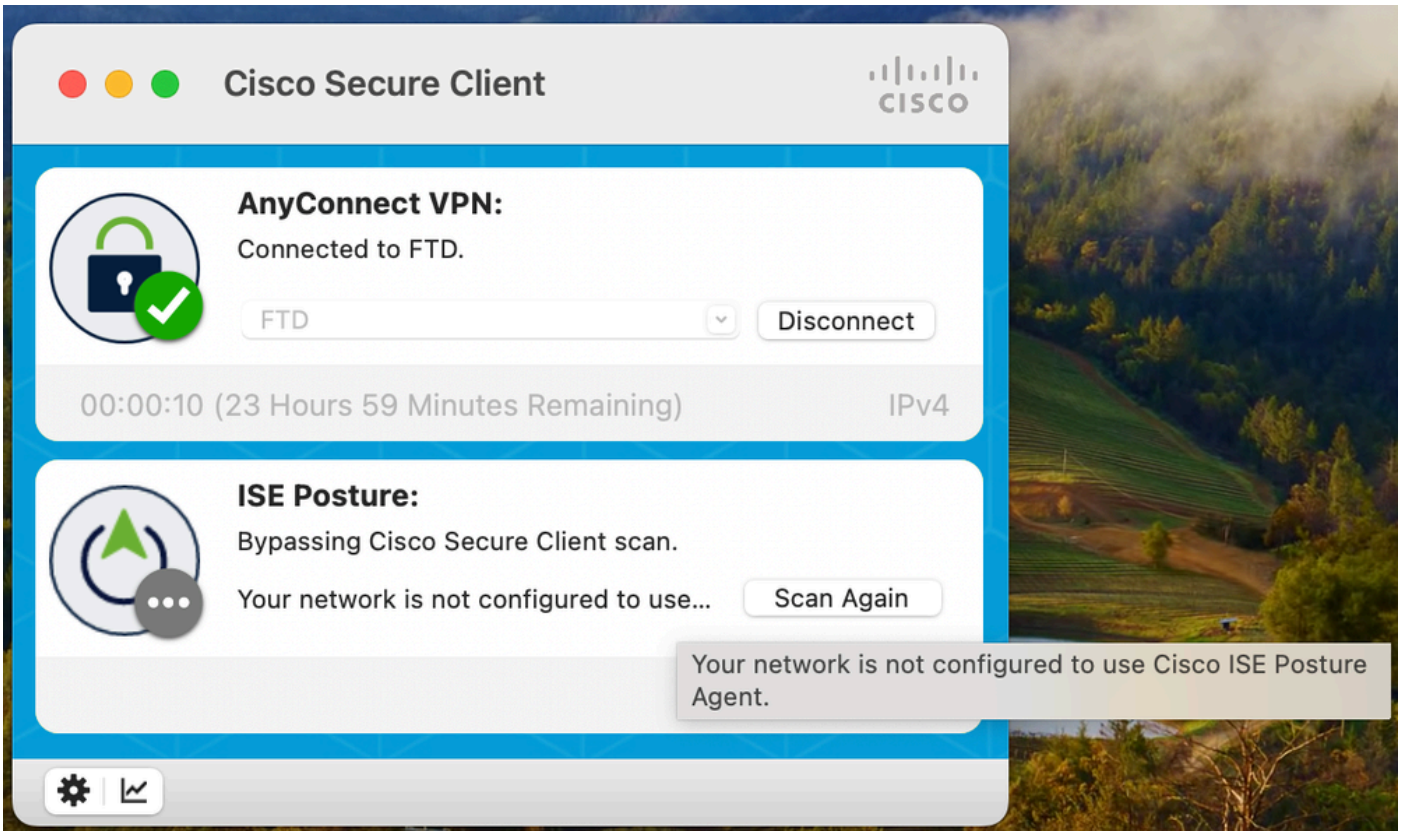
{CA证书的路径}

例如，如果您的证书在桌面中，则命令为：sudo /usr/bin/security add-trusted-cert -r trustRoot -d -k /Library/Keychains/System.keychain /Users/JohnDoe/Downloads/CA_certificate.crt

执行命令后，请重新启动计算机并重试。

绕过Cisco安全客户端扫描

您还可能遇到错误消息“Bypassing Cisco Secure Client Scan”和“Your network is not configured to use Cisco ISE Posture Agent”：



出现此消息是因为在ISE > Work Centers > Posture > Client Provisioning > Client Provisioning Policies的Client Provisioning中未配置配置文件。
即使您可能会看到Mac OSX操作系统的情况，但这并不意味着您涵盖的是所有macOS版本。

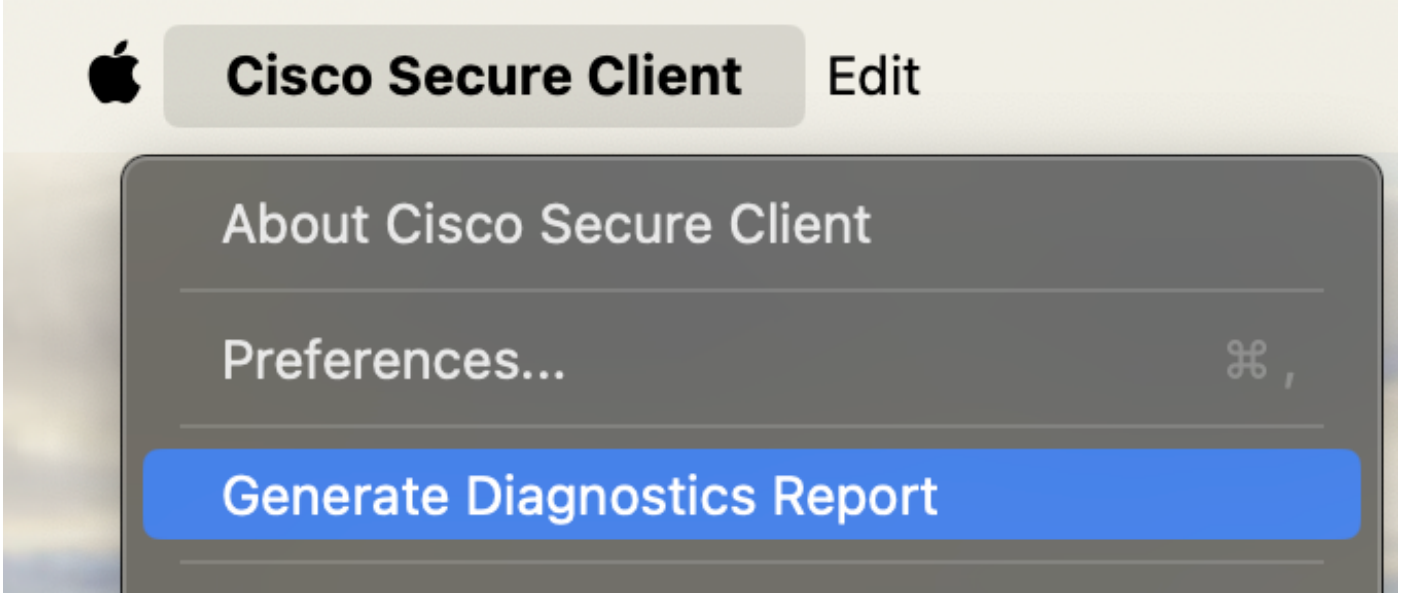
默认情况下，ISE不包含最新的macOS版本，例如Sequoia(15.6.x)，以避免此类消息，确保该状态已更新。

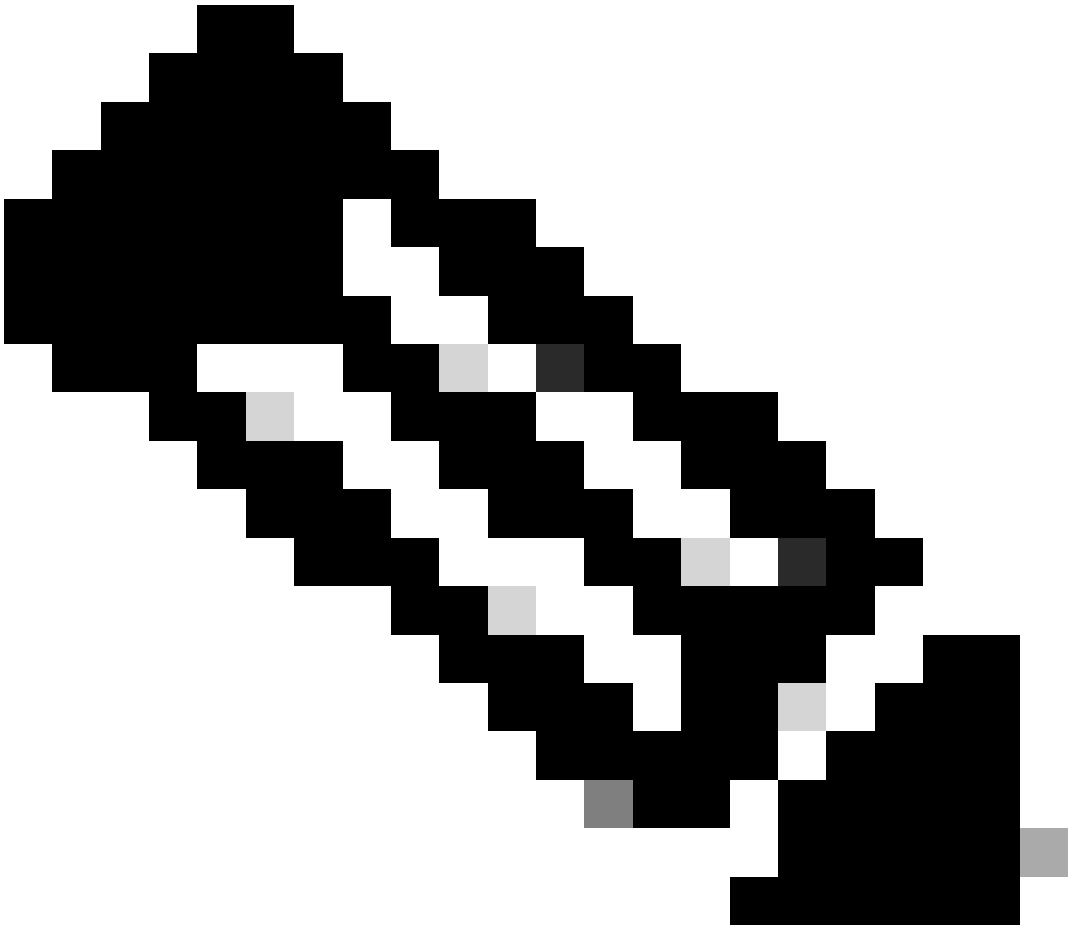
您必须从ISE > Work Centers > Posture > Settings > Software Updates > Posture Updates更新安全评估源。

可以直接从ISE在线更新，也可以通过可从安全评估离线站点下载的zip文件脱机更新

其他问题

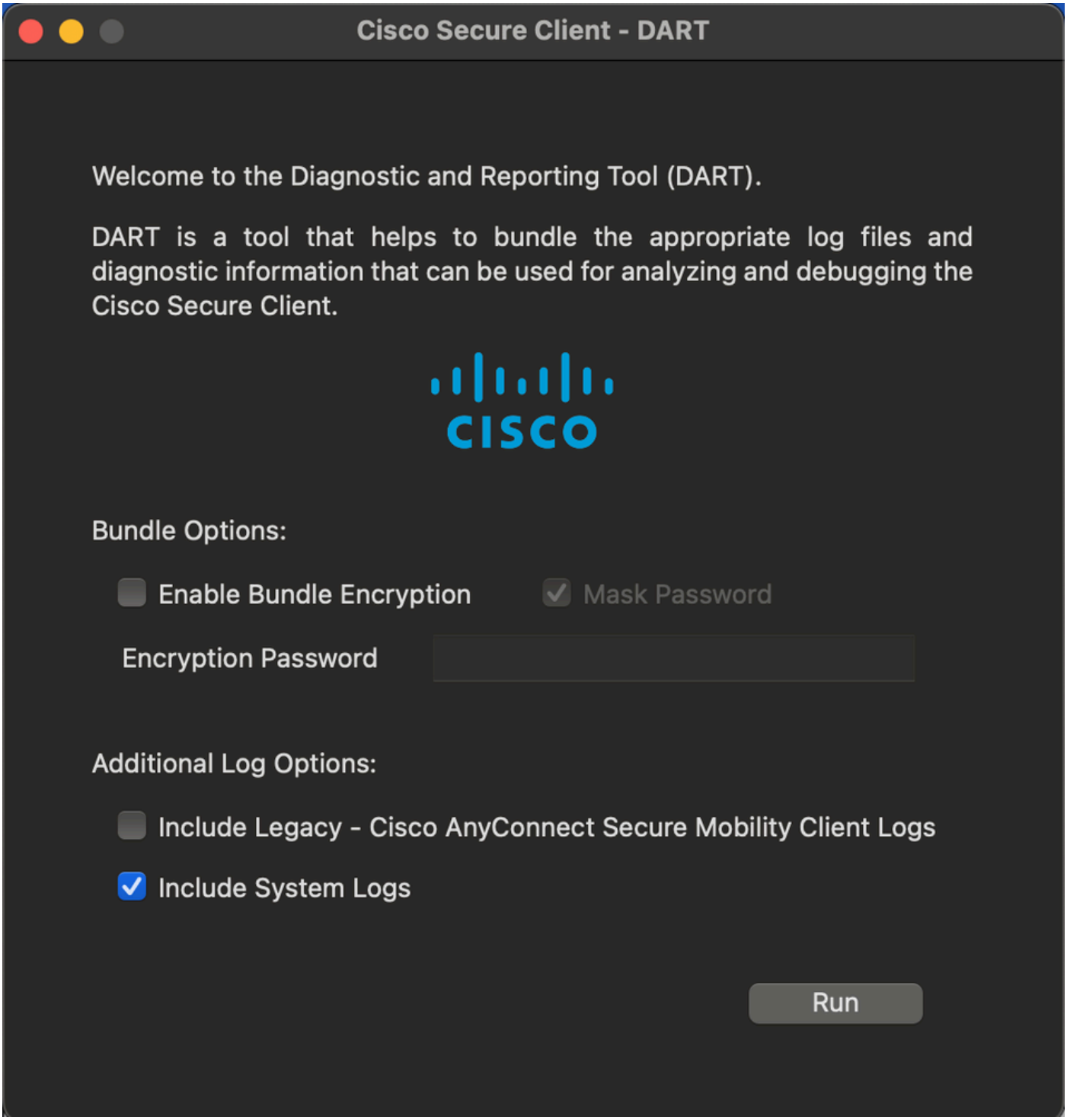
如果您想要了解详细信息，可以从状态化的macOS设备收集DART捆绑包。为此，您必须安装DART模块，然后，在Cisco Secure Client应用程序处于活动状态时，导航到Menu栏，然后单击Cisco Secure Client，然后在Generate Diagnostics Reports中单击。



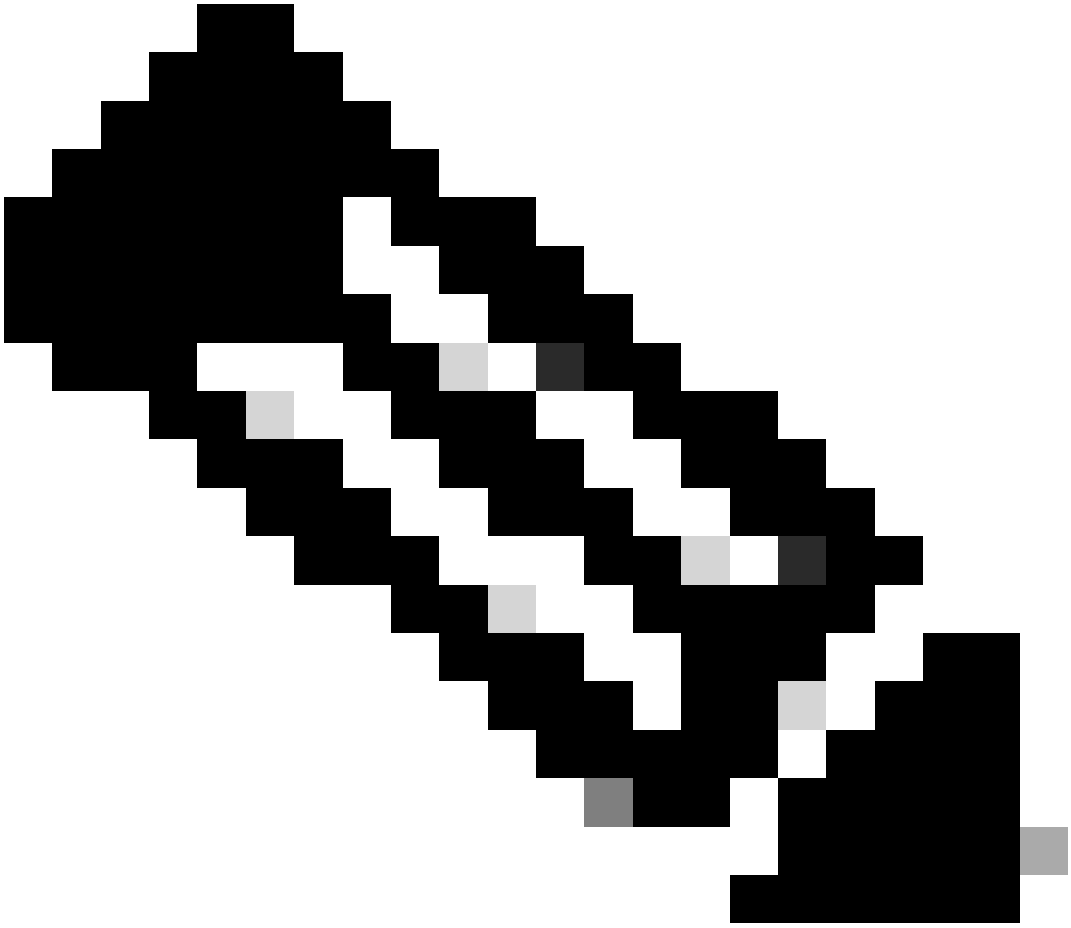


注意：在生成DART捆绑包时，必须启用Include System Logs选项，否则DART捆绑包不会

包含ISE终端安全评估模块信息。



由于安全原因，某些日志可能已被加密且不可见，但在DART捆绑包的unified_log.log中，您可能会看到类似的日志，如下所示：



注意：此日志示例适用于本文档中配置的macOS服务条件。

```
[Tue Feb 27 10:30:58.576 2024][csc_iseposture]Function: createCheckXMLString Thread Id: 0x4A9FD7C0 File
```

```
macOS-Service-Condition
```

```
3
```

303

com.apple.sysmond

running

0

)
[Tue Feb 27 10:30:58.576 2024][csc_iseagent]Function: processPostureData Thread Id: 0x4A9FD7C0 File: Au

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

[Tue Feb 27 10:30:58.576 2024][csc_iseagent]Function: SMP_initCheck Thread Id: 0x4A9FD7C0 File: SMNavPo

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

",isElevationAllowed:1,nRemediationTimeLeft:0}
[Tue Feb 27 10:30:58.646 2024][csc_eliseposture]Function: createCheckXMLString Thread Id: 0x4A9FD7C0 Fi

macOS-Service-Condition

3

303

```
        com.apple.sysmond

         running

         0

)
[Tue Feb 27 10:30:58.646 2024][csc_eliseposture]Function: doCheck Thread Id: 0x4A9FD7C0 File: Rqmt.cpp
[Tue Feb 27 10:30:58.658 2024][csc_eliseposture]Function: doCheck Thread Id: 0x4A9FD7C0 File: CheckSvc.
[Tue Feb 27 10:30:58.658 2024][csc_eliseposture]Function: completeCheck Thread Id: 0x4A9FD7C0 File: Rqm
```

此外，您还可以在对终端进行身份验证和状态的ISE PSN节点中，在调试日志级别设置posture组件。

您可以从ISE > Operations > Troubleshoot > Debug Wizard > Debug Log Configuration配置此日志级别。单击PSN Hostname并将Posture component 日志级别从INFO更改为DEBUG。

使用与macOS服务条件相同的示例，您可以在ise-psc.log中看到类似的日志：

```
2024-02-27 10:30:58.658 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-1][[]] cisco.cpm.posture.runtime.Pos

         ISE: 3.3.0.430

         ISE: 2.x
```

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

2024-02-27 10:30:58.659 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-1][[]] cisco.cpm.posture.util.Status

ISE: 3.3.0.430

ISE: 2.x

0

30

macOS-Service-Requirement

macOS Service is non compliant

3

0

3

macOS-Service-Condition

3

303

com.apple.sysmond

running

0

(macOS-Service-Condition)

]

2024-02-27 10:31:06.044 DEBUG [https-jsse-nio-10.4.21.59-8443-exec-8][[]] cisco.cpm.posture.util.AgentU

如果问题仍然存在，请向思科团队提交TAC通知单。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。