



## ISE-PIC 中的监控和故障排除服务

监控和故障排除服务是面向所有思科 ISE-PIC 运行时服务的综合身份解决方案，并使用以下组件：

- 监控 - 提供代表网络访问活动状态的有意义数据的实时展示。通过查看展示，您可以轻松地解释并影响操作条件。
- 故障排除 - 提供解决网络访问问题的情景指南。之后，您即可了解用户的问题并及时提供解决方案。
- 报告 - 提供一类标准报告，您可以用这些报告来分析趋势和监控系统性能以及网络活动。您可以用各种方式自定义这些报告，并可保存这些报告以供将来使用。您可以使用通配符以及“身份”、“终端 ID”和“节点”字段的多个值来搜索记录。

在本节中详细了解如何使用监控、故障排除和报告工具来管理 ISE-PIC。

- [实时会话，第 1 页](#)
- [可用报告，第 4 页](#)
- [思科 ISE-PIC 警报，第 7 页](#)
- [用于验证传入流量的 TCP Dump 实用工具，第 15 页](#)
- [日志记录机制，第 18 页](#)
- [Active Directory 故障排除，第 18 页](#)
- [获取其他故障排除信息，第 30 页](#)

## 实时会话

下表说明了 **实时会话 (Live Sessions)** 窗口中的字段，此窗口显示实时会话。从主菜单栏中，选择**实时会话 (Live Sessions)**。

表 1: 实时会话

字段名称	说明
启动时间 (Initiated)	显示启动会话时的时间戳。
已更新 (Updated)	显示会话上次由于任何更改而更新时的时间戳。

字段名称	说明
帐户会话时间 (Account Session Time)	显示用户会话的时间跨度（秒）。
会话状态 (Session Status)	显示终端设备的当前状态。
操作 (Action)	单击“操作”图标以打开 <b>操作 (Actions)</b> 弹出窗口。可以执行以下操作： <ul style="list-style-type: none"> <li>• 清除会话</li> <li>• 检查当前用户的会话状态</li> </ul>
终端 ID (Endpoint ID)	显示终端的唯一标识符，通常是 MAC 或 IP 地址。
身份 (Identity)	显示终端设备的用户名。
IP 地址 (IP Address)	显示终端设备的 IP 地址。
服务器 (Server)	指示已从中生成日志的 PIC 节点。
身份验证方式 (Auth Method)	显示 RADIUS 协议使用的身份验证方式，例如“密码身份验证协议” (Password Authentication Protocol)、 “质询握手身份验证协议” (Challenge Handshake Authentication Protocol)、 IEE 802.1x 或 dot1x 等等。
会话源 (Session Source)	指示它是 RADIUS 会话还是 PassiveID 会话。
用户域名 (User Domain Name)	显示用户的注册 DNS 名称。
用户 NetBIOS 名称 (User NetBIOS Name)	显示用户的 NetBIOS 名称。

字段名称	说明
提供程序 (Provider)	<p>终端活动获悉自不同的系统日志源。这些系统日志源称为提供程序。</p> <ul style="list-style-type: none"> <li>• Windows Management Instrumentation (WMI) - WMI 是一种 Windows 服务，用于提供通用接口和对象模型来访问有关操作系统、设备、应用和服务的管理信息。</li> <li>• 代理 - 代表客户端或另一个程序在客户端上运行的程序。</li> <li>• 系统日志 - 客户端发送活动消息的日志记录服务器。</li> <li>• REST - 客户端通过终端服务器进行身份验证。对于此系统日志源，将会显示“TS代理 ID”、“源端口开始时间”、“源端口结束时间”和“源第一个端口”值。</li> <li>• SPAN - 使用 SPAN 探测器发现的网络信息。</li> <li>• DHCP - DHCP 事件。</li> <li>• 终端</li> </ul> <p>从终端会话获悉来自不同提供程序的两个事件后，提供程序在实时会话页面中显示为逗号分隔值。</p>
MAC 地址 (MAC Address)	显示客户端的 MAC 地址。
终端检查时间 (Endpoint Check Time)	显示终端探测器上次检查终端的时间。
终端检查结果 (Endpoint Check Result)	<p>显示终端探测的结果。可能的值包括：</p> <ul style="list-style-type: none"> <li>• 无法接通</li> <li>• 用户退出</li> <li>• 活动用户</li> </ul>
起始源端口 (Source Port Start)	(仅为 REST 提供程序显示值) 显示端口范围内的第一个端口号。
结束源端口 (Source Port End)	(仅为 REST 提供程序显示值) 显示端口范围内的最后一个端口号。

字段名称	说明
源第一个端口 (Source First Port)	<p>(仅为 REST 提供程序显示值) 显示由终端服务器 (TS) 代理分配的第一个端口。</p> <p>终端服务器 (TS) 指允许多个终端在无需调制解调器或网络接口的情况下连接到其上的服务器或网络设备, 可实现多个终端到 LAN 网络的连接。多个终端可能会有相同的 IP 地址, 因此难以识别特定用户的 IP 地址。所以, 为了识别特定用户, 需在服务器上安装 TS 代理, 为每个用户分配一个端口范围。这有助于创建 IP 地址 - 端口 - 用户映射。</p>
TS 代理 ID (TS Agent ID)	(仅为 REST 提供程序显示值) 显示安装在终端上的终端服务器 (TS) 代理的唯一标识。
AD 用户解析的身份 (AD User Resolved Identities)	(仅为 AD 用户显示值) 显示匹配的潜在账户。
AD 用户解析的 DN (AD User Resolved DNs)	(仅为 AD 用户显示值) 显示 AD 用户的可分辨名称, 例如 CN=chris,CN=Users,DC=R1,DC=com

## 可用报告

下表按照报告类别分组列出系统预配置的报告。此外还提供对报告功能和日志记录类别的说明。

报告名称	说明	日志记录类别
<b>IDC 报告</b>		
AD Connector Operations	<p>“AD连接器操作”报告提供AD连接器所执行的操作的日志, 例如 ISE-PIC 服务器密码更新、Kerberos 票证管理、DNS 查询、DC 发现、LDAP 和 RPC 连接管理等。</p> <p>如果遇到某些 AD 故障, 您可以在此报告中查看详细信息以确定可能的原因。</p>	选择管理 ( <b>Administration</b> ) > 系统 ( <b>System</b> ) > 日志记录 ( <b>Logging</b> ) > 日志记录类别 ( <b>Logging Categories</b> ), 然后选择“AD 连接器” (AD Connector)。
Administrator Logins	管理员登录报告提供关于所有基于 GUI 的管理员登录事件以及成功的 CLI 登录事件的信息。	选择 <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> , 然后选择 <b>Administrative and Operational Audit</b> 。

报告名称	说明	日志记录类别
Change Configuration Audit	更改配置审核报告提供关于指定时间内配置更改的详细信息。如果需要对某个功能进行故障排除，此报告可以帮助您确定是不是最近的配置更改导致了问题。	选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择“管理和操作审核” (Administrative and Operational Audit)。
Current Active Sessions	您可以通过当前活动会话报告导出包含关于指定时间内哪些用户正在访问网络的详细信息的报告。  如果用户无法访问网络，您可以查看会话是否经过了身份验证或是否中断，或会话是否存在其他问题。	选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择以下日志记录类别：“记账” (Accounting) 和“RADIUS 记账” (RADIUS Accounting)。
Health Summary	运行状况摘要报告提供与控制面板类似的详细信息。但是，控制面板仅显示前 24 小时的数据，而您可以使用此报告查看更久之前的历史数据。  您可以评估这些数据，以查看数据中的一致模式。例如，您可能预计当大多数员工都开始工作时，CPU 使用率较高。如果您发现这些趋势存在不一致性，您可以确定潜在的问题。  CPU 使用率表列出不同 ISE-PIC 功能的 CPU 使用率的百分比。此表中提供 <b>show cpu usage</b> CLI 命令的输出，您可以将这些值与部署中的问题相关联，从而识别可能的原因。	选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择以下日志记录类别：“管理和操作审核” (Administrative and Operational Audit)、 “系统诊断” (System Diagnostics) 及“系统统计信息” (System Statistics)。
Operations Audit	“操作审核” 报告提供有关任何操作变更的详细信息，例如运行备份、注册思科 ISE-PIC 节点或重新启动应用。	选择管理 (Administration) > 系统 (System) > 日志记录 (Logging) > 日志记录类别 (Logging Categories)，然后选择“管理和操作审核” (Administrative and Operational Audit)。

报告名称	说明	日志记录类别
PassiveID	通过“被动 ID”报告，可以监控与域控制器的 WMI 连接的状态并收集与其相关的统计信息（例如接收的通知数量、每秒钟用户登录/注销的次数等）。	选择 <b>管理 (Administration)</b> > <b>系统 (System)</b> > <b>日志记录 (Logging)</b> > <b>日志记录类别 (Logging Categories)</b> ，然后选择“身份映射” (Identity Mapping)。
pxGrid Administrator Audit	<p>“pxGrid 管理员审核”报告提供 pxGrid 管理操作的详细信息，例如注册客户端、注销客户端、审批客户端、创建主题、删除主题、添加发布者/用户以及删除发布者/用户。</p> <p>每条记录都会注明在节点上执行相应操作的管理员名称。</p> <p>您可以根据管理员和消息条件过滤 pxGrid 管理员审核报告。</p>	-
System Diagnostic	<p>“系统诊断”报告提供有关 ISE-PIC 节点的状态的详细信息。如果 ISE-PIC 节点无法注册，可以查看此报告来对问题进行故障排除。</p> <p>此报告要求首先启用几个诊断日志记录类别。收集这些日志可能会对 ISE-PIC 性能产生不利影响。因此，默认情况下未启用这些类别。如果您启用这些类别，应使其启用持续时间刚好满足收集数据的要求即可。否则，30 分钟后系统会自动禁用这些类别。</p>	选择 <b>管理 (Administration)</b> > <b>日志记录 (Logging)</b> > <b>日志记录类别 (Logging Categories)</b> ，然后选择以下日志记录类别：“内部操作诊断” (Internal Operations Diagnostics)、 <b>“分布式管理” (Distributed Management)</b> 、 <b>“管理员身份验证” (Administrator Authentication)</b> 和 <b>“授权” (Authorization)</b> 。
User Change Password Audit	用户更改密码审核报告显示关于员工密码更改的验证信息。	选择 <b>管理 (Administration)</b> > <b>系统 (System)</b> > <b>日志记录 (Logging)</b> > <b>日志记录类别 (Logging Categories)</b> ，然后选择“管理和操作审核” (Administrative and Operational Audit)。

## 思科 ISE-PIC 警报

警报显示在“警报”(Alarms) Dashlet 中，通知您网络中的情况。有三种警报严重级别：严重、警告和信息。警报还会提供关于系统活动的信息，如数据清除事件。可以配置要接收系统活动通知的方式，或完全禁用警报。还可以为某些警报配置阈值。

大多数警报没有关联的计划，会在事件发生后立即发送。在任何给定时间点，系统只会保留最新的 15,000 个警报。

如果事件再次发生，则系统会在一个小时内抑制相同的警报。在事件再次发生期间，可能需要经过一个小时，警报才会再次出现，该取决于触发器。

下表列出了所有思科 ISE-PIC 警报、说明及其解决方法。

表 2: 思科 ISE-PIC 警报

警报名称	警报说明	警报解决方法
管理和操作审核管理		
部署升级失败	ISE PIC 节点升级失败。	检查故障节点的 ADE.log，以查找升级失败的原因并制定纠正措施。
升级捆绑包下载失败	ISE-PIC 节点升级捆绑包下载失败。	检查故障节点的 ADE.log，以查找升级失败的原因并制定纠正措施。
由于 CRL 查找到已吊销的证书，安全 LDAP 连接重新连接	CRL 检查结果是用于 LDAP 连接的证书已吊销。	检查 CRL 配置并检验它是否有效。检查 LDAP 服务器证书及其颁发机构证书是否已吊销。如果已吊销，颁发新证书并将其安装在 LDAP 服务器上。
由于 OCSP 查找到已吊销的证书，安全 LDAP 连接重新连接	OCSP 检查结果是用于 LDAP 连接的证书已吊销。	检查 OCSP 配置并检验它是否有效。检查 LDAP 服务器证书及其颁发机构证书是否已吊销。如果已吊销，颁发新证书并将其安装在 LDAP 服务器上。
由于 CRL 查找到已吊销的证书，安全系统日志连接重新连接	CRL 检查结果是用于系统日志连接的证书已吊销。	检查 CRL 配置并检验它是否有效。检查系统日志服务器证书及其颁发机构证书是否已吊销。如果已吊销，颁发新证书并将其安装在系统日志服务器上。

警报名称	警报说明	警报解决方法
由于 OCSP 查找到已吊销的证书，安全系统日志连接重新连接	OCSP 检查结果是用于系统日志连接的证书已吊销。	检查 OCSP 配置并检验它是否有效。检查系统日志服务器证书及其颁发机构证书是否已吊销。如果已吊销，颁发新证书并将其安装在系统日志服务器上。
管理员帐户已锁定/禁用	由于密码过期或登录尝试不正确，系统锁定或禁用管理员帐户。有关详细信息，请参阅管理员密码策略。	管理员密码可以由其他管理员使用 GUI 或 CLI 进行重置。
ERS 识别已弃用的 URL	ERS 识别已弃用的 URL	请求的 URL 已被弃用，建议避免使用它。
ERS 识别过时的 URL	ERS 识别过时的 URL	请求的 URL 已过时，建议使用更新的 URL。未来的版本不会删除此 URL。
ERS 请求“内容-类型”标头已过时	ERS 请求的内容类型报头已过时。	请求“内容-类型”标头中描述的资源版本已过时。这表明资源方案已被修改。可能已添加或删除一个或多个属性。为使用过时的方案解决这一问题，ERS 引擎将使用默认值。
ERS XML 输入有 XSS 或注入攻击的嫌疑	ERS XML 输入有 XSS 或注入攻击的嫌疑。	请检查您的 xml 输入。
备份失败	思科 ISE-PIC 备份操作失败。	检查思科 ISE-PIC 与存储库之间的网络连接性。确保： <ul style="list-style-type: none"> <li>• 用于存储库的凭证是正确的。</li> <li>• 存储库中有足够的磁盘空间。</li> <li>• 存储库用户具有写入权限。</li> </ul>
CA 服务器已关闭	CA 服务器已关闭。	检查以确保 CA 服务已启动并正在 CA 服务器上运行。
CA 服务器已启动	CA 服务器已启动。	通知管理员 CA 服务器已启动。



警报名称	警报说明	警报解决方法
证书到期	此证书即将到期。证书到期时，思科 ISE-PIC 可能无法与客户端建立安全通信。	更换证书。对于信任证书，请联系证书颁发机构 (CA)。对于 CA 签名的本地证书，请生成 CSR 并使 CA 创建新证书。对于自签名的本地证书，请使用思科 ISE-PIC 延长有效期。如果不再使用证书，可将其删除。
证书被吊销	管理员被吊销由内部 CA 颁发给终端的证书。	从头完成 ISE-PIC 流程以获得新证书。
证书调配初始化错误	证书调配初始化失败	在主题中找到多个具有相同 CN (CommonName) 属性值的证书，无法构建证书链。检查系统中的所有证书。
证书复制失败	到辅助节点的证书复制失败	证书在辅助节点上无效，或存在某些其他永久错误条件。检查辅助节点是否有预先存在的冲突证书。如果找到，请删除辅助节点上预先存在的证书，然后在主节点上导出新证书，删除证书，然后将其导入以重新尝试复制。
证书复制暂时失败	到辅助节点的证书复制暂时失败	由于网络故障等临时条件，证书未复制到辅助节点。系统将重试复制，直至成功。
证书已过期	此证书已过期。思科 ISE-PIC 可能无法与客户端建立安全通信。节点到节点通信可能也会受到影响。	更换证书。对于信任证书，请联系证书颁发机构 (CA)。对于 CA 签名的本地证书，请生成 CSR 并使 CA 创建新证书。对于自签名的本地证书，请使用思科 ISE-PIC 延长有效期。如果不再使用证书，可将其删除。
证书请求转发失败	证书请求转发失败。	确保传入的认证请求与发件人的属性相匹配。
配置已更改	思科 ISE 配置已更新。系统没有为任何用户和终端的配置更改触发此警报。	检查是否应存在配置更改。

警报名称	警报说明	警报解决方法
CRL 检索失败	无法从服务器检索 CRL。如果指定的 CRL 不可用，就可能会出现这种情况。	确保下载 URL 正确且可用于服务。
DNS 解析失败	节点上的 DNS 解析失败。	检查是否可访问使用 <b>ip name-server</b> 命令配置的 DNS 服务器。  如果您收到的警报为“DNS Resolution failed for CNAME <hostname of the node>”，则确保为每个思科 ISE 节点创建 CNAME RR 以及 A 记录。
需要进行固件更新	需要在此主机上进行固件更新。	联系思科技术支持中心 (TAC) 获取固件更新
虚拟机资源不足	此主机上的虚拟机 (VM) 资源（如 CPU、RAM、磁盘空间或 IOPS）不足。	确保 VM 主机达到《思科 ISE 硬件安装指南》中指定的最低要求。
NTP 服务故障	此节点上的 NTP 服务已关闭。	这可能是因为 NTP 服务器与思科 ISE-PIC 节点之间存在较大的时间差异（超过 1000 秒）。确保 NTP 服务器正常工作并使用 <b>ntp server &lt;servername&gt;</b> CLI 命令重新启动 NTP 服务并修复时间差。
NTP 同步失败	在此节点配置上的所有 NTP 服务器均无法访问。	从 CLI 执行 <b>show ntp</b> 命令，进行故障排除。确保可从思科 ISE-PIC 访问 NTP 服务器。如果已配置 NTP 身份验证，请确保密钥 ID 和值与服务器的相匹配。
未安排配置备份	未安排思科 ISE-PIC 配置备份。	创建配置备份计划。
操作数据库清除失败	无法从操作数据库中清除较旧的数据。如果 M&T 节点繁忙，就可能会出现这种情况。	检查数据清除审核报告并确保 <b>used_space</b> 小于 <b>threshold_space</b> 。使用 CLI 登录到 M&T 节点，手动执行清除操作。

警报名称	警报说明	警报解决方法
复制失败	辅助节点无法使用复制的消息。	登录思科 ISE-PIC GUI 并从部署页面执行手动同步。取消注册并重新注册受影响的思科 ISE-PIC 节点。
恢复失败	思科 ISE-PIC 恢复操作失败。	确保思科 ISE-PIC 与存储库之间存在网络连接。确保用于存储库的凭证正确。确保备份文件未损坏。从 CLI 执行 <b>reset-config</b> 命令并恢复已知的最后一次有效备份。
补丁失败	服务器上的补丁进程失败。	在服务器上重新安装补丁进程。
补丁成功	服务器上的补丁进程成功。	-
复制已停止	ISE-PIC 节点无法从主节点复制配置数据。	登录思科 ISE-PIC GUI 以从部署页面执行手动同步，或取消注册并重新注册带必填字段的受影响思科 ISE-PIC 节点。
终端证书已过期	终端证书已由每天安排的作业标记为过期。	请重新注册终端设备，获取新的终端证书。
终端证书已清除	过期的终端证书已由每天安排的作业清除。	不需要采取行动 - 这是管理员发起的清理操作。
复制减慢错误	系统检测到复制减慢或停滞。	请验证节点是否可访问并是部署的一部分。
复制减慢信息	系统检测到复制减慢或停滞。	请验证节点是否可访问并是部署的一部分。
复制减慢警告	系统检测到复制减慢或停滞。	请验证节点是否可访问并是部署的一部分。
EST 服务已停止	EST 服务已停止。	确保 CA 和 EST 服务正常运行，且证书服务终端子 CA 证书链完整。
EST 服务已启动	EST 服务已启动。	通知管理员 EST 服务已启动。
Smart Call Home 通信故障	Smart Call Home 消息未成功发送。	确保思科 ISE-PIC 和思科系统之间存在网络连接。
遥测通信故障	遥测消息未成功发送。	确保思科 ISE 和思科系统之间存在网络连接。

警报名称	警报说明	警报解决方法
ISE 服务		
AD 连接器必须重新启动	AD 连接器意外停止，必须重新启动。	如果此问题仍然存在，请联系思科 TAC 寻求帮助。
Active Directory 林不可用	Active Directory 林 GC（全局目录）不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
身份验证域不可用	身份验证域不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
ID 映射。身份验证处于非活动状态	身份映射服务在过去 15 分钟未收集任何用户身份验证事件。	如果这是一个应进行用户身份验证的时间（例如，工作时间），则检查到 Active Directory 域控制器的连接。
配置的名称服务器已关闭	配置的名称服务器已关闭或不可用。	检查 DNS 配置和网络连接。
AD: 计算机 TGT 刷新失败	ISE-PIC 服务器 TGT（根凭证）刷新失败；它用于 AD 连接和服务。	检查思科 ISE-PIC 计算机帐户是否存在且有效。另请检查是否存在时钟偏差、复制、Kerberos 配置和/或网络错误。
AD: ISE 帐户密码更新失败	ISE-PIC 服务器未能更新其 AD 计算机帐户密码。	检查思科 ISE-PIC 计算机帐户密码是否未更改，计算机帐户是否未禁用或受限制。检查到 KDC 的连接。
所加入的域不可用	所加入的域不可用，无法用于身份验证、授权，以及组和属性检索。	检查 DNS 配置、Kerberos 配置、错误条件和网络连接性。
身份库不可用	思科 ISE-PIC 策略服务节点无法访问配置的身份库。	检查思科 ISE-PIC 与身份库之间的网络连接。
AD: ISE 计算机帐户没有获取组所需的权限。	思科 ISE-PIC 计算机帐户没有获取组所需的权限。	检查思科 ISE-PIC 计算机帐户是否有权获取 Active Directory 中的用户组。
系统运行状况		

警报名称	警报说明	警报解决方法
高磁盘 I/O 利用率	思科 ISE-PIC 系统遇到高磁盘 I/O 利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高磁盘空间利用率	思科 ISE-PIC 系统遇到高磁盘空间利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高平均负载	思科 ISE-PIC 系统遇到高平均负载。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高内存利用率	思科 ISE-PIC 系统遇到高内存利用率。	检查系统是否有足够的资源。检查系统的实际工作量，例如，身份验证数量、分析器活动等。添加额外服务器以分配负载。
高操作数据库使用率	思科 ISE-PIC 监控节点遇到的系统日志数据量高于预期数据量。	检查并缩小操作数据的清除配置窗口。
运行状态不可用	监控节点未收到思科 ISE-PIC 节点的运行状态。	确保思科 ISE-PIC 节点已启动并且正在运行。确保思科 ISE-PIC 节点能够与监控节点通信。
进程已关闭	其中一个思科 ISE-PIC 进程未运行。	重新启动思科 ISE-PIC 应用。
已达到 OCSP 事务阈值	已达到 OCSP 事务阈值。当内部 OCSP 服务达到较高流量时触发此警报。	请检查系统是否有足够的资源。
许可		
PIC 许可证已过期	思科 ISE-PIC 节点上安装的许可证已过期。	联系思科客户团队购买新许可证。
在 30 天内到期的 PIC 许可证	思科 ISE-PIC 节点上安装的许可证将在 30 天后到期。	请联系思科销售团队以延期 ISE-PIC 许可证。
在 60 天内到期的 PIC 许可证	思科 ISE-PIC 节点上安装的许可证将在 60 天后到期。	请联系思科销售团队以延期 ISE-PIC 许可证。
在 90 天内到期的 PIC 许可证	思科 ISE-PIC 节点上安装的许可证将在 90 天后到期。	请联系思科销售团队以延期 ISE-PIC 许可证。

警报名称	警报说明	警报解决方法
系统错误		
日志收集错误	思科 ISE-PIC 监控收集器进程无法留存从策略服务节点生成的审核日志。	这不会影响策略服务节点的实际功能。如需进一步解决问题，请联系 TAC。
计划的报告导出失败	无法将导出的报告（CSV 文件）复制到配置的存储库。	验证配置的存储库。如果存储库已删除，请重新添加存储库。如果存储库不可用或不可访问，请将其重新配置为有效存储库。

将用户或终端添加到思科 ISE-PIC 时，系统不会触发警报。

## 警报设置

下表说明了警报设置 (Alarm Settings) 窗口（设置 (Settings) > 警报设置 (Alarm Settings)）中的字段。

字段名称	说明
警报类型 (Alarm Type)	警报类型。
警报名称 (Alarm Name)	警报的名称。
说明 (Description)	警报说明。
建议的操作 (Suggested Actions)	触发警报时要执行的操作。
状态 (Status)	启用或禁用警报规则。
严重性 (Severity)	选择警报的严重性级别。有效的选项包括： <ul style="list-style-type: none"> <li>“严重” (Critical): 指示严重错误情况。</li> <li>“警告” (Warning): 指示正常但重要的情况。这是默认情况。</li> <li>“信息” (Info): 指示信息性的消息。</li> </ul>
发出系统日志消息 (Send Syslog Message)	为思科 ISE-PIC 生成的每个系统警报发送系统日志消息。
输入以逗号分隔的多个电子邮件 (Enter multiple e-mails separated with comma)	电子邮件地址和/或 ISE-PIC 管理员名称的列表。
电子邮件中的备注 (0 到 4000 个字符) (Notes in Email [0 to 4000 characters])	您希望与系统警报关联的自定义文本消息。

## 添加自定义报警

思科 ISE-PIC 包含 5 个默认警报类型，例如“配置更改” (Configuration Changed)、“高磁盘 I/O 利用率” (High Disk I/O Utilization)、“高磁盘空间利用率” (High Disk Space Utilization)、“高内存利用率” (High Memory Utilization) 和“ISE 身份验证处于非活动状态” (ISE Authentication Inactivity)。思科定义的系统警报列在“警报设置” (Alarm Settings) 页面 (“设置” (Settings) > “警报设置” (Alarm Settings))。您只能编辑系统报警。

除现有系统报警外，您还可以添加、编辑或删除现有报警类型下的自定义报警。

对于每种报警类型，您最多可以创建 5 个报警，而且报警总数限制为 200。

要添加报警，请按以下步骤操作：

---

**步骤 1** 选择设置 (Settings) > 警报设置 (Alarm Settings)。

**步骤 2** 在报警配置 (Alarm Configuration) 选项卡中，单击添加 (Add)。

**步骤 3** 输入必要的详细信息。请参阅[警报设置](#)部分了解详细信息。

根据警报类型，“警报配置” (Alarm Configuration) 页面会显示其他属性。例如，对于“配置更改” (Configuration Changed) 警报，将显示“对象名称” (Object Name)、“对象类型” (Object Type) 和“管理员名称” (Admin Name) 字段。您可以为规定不同条件的相同报警添加多个实例。

**步骤 4** 单击提交 (Submit)。

---

## 用于验证传入流量的 TCP Dump 实用工具

TCP 转储实用工具嗅探数据包，可以使用此实用工具验证预计数据包是否已到达节点。例如，当报告中没有显示传入身份验证或日志时，您可能会怀疑没有传入流量或传入流量无法到达思科 ISE。在这种情况下，您可以运行此工具进行验证。

可以配置 TCP 转储选项，然后从网络流量收集数据以帮助您对网络问题进行故障排除。

## 使用 TCP Dump 监控网络流量

“TCP 转储” (TCP Dump) 窗口列出了您创建的 TCP 转储进程文件。可以创建不同文件以用于不同目的，根据需要运行这些文件，然后在不需要这些文件时将其删除。

您可以通过指定大小、文件数量以及进程运行时间来控制收集的数据。如果进程在时间限制之前完成，并且文件小于最大大小，并且您启用了多个文件，则进程会继续并创建另一个转储文件。

可以对更多接口运行 TCP 转储，包括绑定接口。



---

**注释** 不再提供人可读格式选项，转储文件始终为原始格式。

---

支持与存储库的 IPv6 连接。

### 开始之前

**TCP 转储 (TCP Dump)** 窗口页面中的**网络接口 (Network Interface)** 下拉列表仅显示已配置 IPv4 或 IPv6 地址的网络接口卡 (NIC)。在 VMware 中，默认情况下将连接所有 NIC，因此，所有 NIC 均具有 IPv6 地址，并显示在**网络接口 (Network Interface)** 下拉列表中。

**步骤 1** 从**主机名称 (Host Name)** 下拉列表中选择 TCP Dump 实用工具的源。

**步骤 2** 从**网络接口 (Network Interface)** 下拉列表中选择要监控的接口。

**步骤 3** 在**过滤器 (Filter)** 字段中，输入要对其进行过滤的布尔表达式。

系统支持以下标准 TCP 转储过滤器表达式：

- ip host 10.77.122.123
- ip host ISE123
- ip host 10.77.122.123 and not 10.77.122.119

**步骤 4** 输入此 TCP 转储进程的**文件名 (File Name)**。

**步骤 5** 从**存储库 (Repository)** 下拉列表中选择用于存储 TCP 转储日志文件的存储库。

**步骤 6** 从**文件大小 (File Size)** 下拉列表中选择最大文件大小。

如果转储超出此文件大小，则一个新文件将打开以继续转储。转储可通过新文件继续的次数受限制为**(Limit to)** 设置的限制。

**步骤 7** 限制为**(Limit to)** 选项用于限制转储可扩展到的文件数。

**步骤 8** **时间限制 (Time Limit)** 选项可用于配置转储在运行多长时间后结束。

**步骤 9** 单击开**(On)** 或关**(Off)**，设置**混合模式 (Promiscuous Mode)**。默认值为开**(On)**。

混合模式为默认嗅探模式，在此模式下，网络接口将所有流量都传输到系统的 CPU。我们建议将该选项设置为 On。



**注释** 思科 ISE 不支持大于 1500 MTU 的帧（巨帧）。

## 保存 TCP Dump 文件

### 开始之前

您应按照[使用 TCP Dump 文件监控网络流量](#)一节中所描述的内容成功完成任务。





**注释** 还可以通过思科 ISE CLI 访问 TCP 转储。有关详细信息，请参阅思科身份服务引擎 *CLI* 参考指南。

**步骤 1** 从格式 (**Format**) 下拉列表中选择选项。默认设置为人可读 (**Human Readable**)。

**步骤 2** 单击下载 (**Download**)，导航至所需位置，并单击保存 (**Save**)。

**步骤 3** (可选) 若要清除以前的转储文件而无需保存，请单击删除 (**Delete**)。

## TCP Dump 设置

下表介绍 **tcpdump** 实用工具页面上的字段，此页面监控网络接口上的数据包内容，并对网络上出现的问题进行故障排除。此页面的导航路径为：**故障排除 (Troubleshoot)**。

表 3: *TCP Dump* 设置

选项	使用指南
状态 (Status)	<ul style="list-style-type: none"> <li>• Stopped - tcpdump 实用工具不在运行</li> <li>• Start - 单击以启动监控网络的 tcpdump 实用工具。</li> <li>• Stop - 单击以停止 tcpdump 实用工具</li> </ul>
主机名 (Host Name)	从下拉列表选择要监控的主机的名称。
网络接口 (Network Interface)	从下拉列表选择要监控的网络接口。 <b>注释</b> 您必须配置使用 IPv4 或 IPv6 地址的所有网络接口卡 (NIC)，使其显示于思科 ISE Admin 门户中。
混杂模式 (Promiscuous Mode)	<ul style="list-style-type: none"> <li>• On - 单击以打开混杂模式 (默认设置)。</li> <li>• Off - 单击以关闭混杂模式。</li> </ul> 混杂模式是默认的数据包嗅探模式。我们建议您将其设置为 On。在此模式下，网络接口会将所有流量传递到系统的 CPU。

选项	使用指南
过滤器 (Filter)	输入用于筛选的布尔表达式。支持的标准 tcpdump 过滤器表达式： ip host 10.77.122.123 ip host 10.77.122.123 and not 10.177.122.119 ip host ISE123
格式 (Format)	选择 tcpdump 文件的格式。
转储文件 (Dump File)	显示最后一个转储文件上的数据，例如以下数据： Last created on Wed Apr 27 20:42:38 UTC 2011 by admin  File size: 3,744 bytes Format: Raw Packet Data Host Name: Positron Network Interface: GigabitEthernet 0 Promiscuous Mode: On  <ul style="list-style-type: none"> <li>• Download - 单击以下载最新的转储文件。</li> <li>• Delete - 单击以删除最新的转储文件。</li> </ul>

## 日志记录机制

### 思科 ISE-PIC 日志记录机制

#### 配置系统日志清除设置

使用此流程可设置本地日志存储期，并可在一定时间后删除本地日志。

## Active Directory 故障排除

### 将 Active Directory 与思科 ISE-PIC 集成的前提条件

本节介绍配置 Active Directory 以与思科 ISE-PIC 集成所需的手动步骤。但是，在大多数情况下，可以启用思科 ISE-PIC 来自动配置 Active Directory。以下是将 Active Directory 与思科 ISE-PIC 集成的前提条件。

- 确保您拥有对 AD 域配置进行更改所需的 Active Directory 域管理员凭证。

- 使用网络时间协议 (NTP) 服务器设置来同步思科 ISE-PIC 服务器和 Active Directory 之间的时间。您可以从思科 ISE-PIC CLI 配置 NTP 设置。
- 您必须在思科 ISE-PIC 加入到的域中具有至少一个可由思科 ISE-PIC 运行并访问的全局目录服务器。

## 执行各种操作所需的 Active Directory 帐户权限

加入操作	退出操作	思科 ISE-PIC 机器帐户
<p>加入操作需要以下帐户权限：</p> <ul style="list-style-type: none"> <li>• 搜索 Active Directory（以查看思科 ISE-PIC 机器帐户是否存在）</li> <li>• 将思科 ISE-PIC 机器帐户创建到域（如果机器帐户尚不存在）</li> <li>• 在新机器帐户上设置属性（例如，思科 ISE-PIC 机器帐户密码、SPN、dnsHostname）</li> </ul>	<p>退出操作需要以下帐户权限：</p> <ul style="list-style-type: none"> <li>• 搜索 Active Directory（以查看思科 ISE-PIC 机器帐户是否存在）</li> <li>• 从域中删除思科 ISE-PIC 机器帐户</li> </ul> <p>如果执行强制退出（在没有密码的情况下退出），则不会从域中删除计算机帐户。</p>	<p>用于传达到 Active Directory 连接的思科 ISE-PIC 机器帐户需要以下权限：</p> <ul style="list-style-type: none"> <li>• 更改密码</li> <li>• 读取与已联系的用户和机器对应的用户和机器对象。</li> <li>• 查询 Active Directory 以获取信息（例如，受信任域和替代 UPN 后缀等）</li> <li>• 读取 tokenGroups 属性</li> </ul> <p>可以在 Active Directory 中预创建机器帐户。如果 SAM 名称与思科 ISE-PIC 设备主机名匹配，则应在加入操作期间找到该名称并重复使用。</p> <p>如果具有多个加入操作，则会在思科 ISE-PIC 中维护多个机器帐户，每个加入操作对应一个帐户。</p>



**注释** 用于加入或退出操作的凭证不存储在思科 ISE-PIC 中。仅存储新创建的思科 ISE-PIC 机器帐户凭证。

Microsoft Active Directory 中的网络访问权限：限制允许远程调用 SAM 的客户端安全策略已修改。因此，思科 ISE 可能无法每 15 天更新一次其机器帐户密码。如果机器帐户密码未更新，思科 ISE 不会再通过 Microsoft Active Directory 对用户进行身份验证。您将在思科 ISE 控制板上收到 **AD: ISE 密码更新失败 (AD: ISE password update failed)** 警报，以通知您此事件。

安全策略可使用户枚举本地安全帐户管理器 (SAM) 数据库和 Microsoft Active Directory 中的用户和组。要确保思科 ISE 可更新其机器帐户密码，请检查 Microsoft Active Directory 中的配置是否正确。有关受影响的 Windows 操作系统和 Windows Server 版本的详细信息，包括这对您的网络意味着什么、可能需要哪些更改，请参阅：

<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls>

## 必须开放用于通信的网络端口

协议	端口（远程-本地）	目标	备注
DNS (TCP/UDP)	随机数大于或等于 49152	DNS 服务器/AD 域控制器	-
MSRPC	445	域控制器	-
Kerberos (TCP/UDP)	88	域控制器	MS AD/KDC
LDAP (TCP/UDP)	389	域控制器	-
LDAP (GC)	3268	全局目录服务器	-
NTP	123	NTP 服务器/域控制器	-
IPC	80	对于辅助 ISE-PIC 节点	—

## 支持 ISE-PIC 的 Active Directory 要求

ISE-PIC 使用 Active Directory 域控制器生成的 Active Directory 登录审核事件来收集用户登录信息。必须正确配置 Active Directory 服务器，才能使 ISE 用户能够连接和获取用户登录信息。以下各部分说明如何配置 Active Directory 域控制器（Active Directory 端的配置）以支持 ISE-PIC。

要配置 Active Directory 域控制器（Active Directory 端的配置）以支持，请按照以下步骤操作：



**注释** 必须配置所有域中的所有域控制器。

1. 从 ISE-PIC 设置 Active Directory 加入点和域控制器。请参阅[添加 Active Directory 加入点并将思科 ISE-PIC 节点加入到该加入点](#)和 [#unique\\_35](#)。
2. 根据域控制器配置 WMI。请参阅[#unique\\_36](#)。
3. 从 Active Directory 执行以下步骤：
  - 为被动身份服务配置 Active Directory，第 21 页
4. （可选）使用以下步骤在 Active Directory 上对 ISE 执行的自动配置进行故障排除：
  - 为域管理员组中的 Microsoft Active Directory 用户设置权限，第 24 页
  - 不在域管理员组中的 Microsoft Active Directory 用户的权限，第 24 页
  - 在域控制器上使用 DCOM 的权限，第 25 页
  - 设置访问 WMI Root 和 CIMv2 命名空间的权限，第 27 页

- 授权访问 AD 域控制器上的安全事件日志，第 28 页

## 为被动身份服务 配置 Active Directory

ISE-PIC Active Directory 域控制器生成的 Active Directory 登录审核事件来收集用户登录信息。ISE-PIC 连接到 Active Directory 并获取用户登录信息。

应从 Active Directory 域控制器执行以下步骤：

### 步骤 1 确保相关 Microsoft 补丁安装在 Active Directory 域控制器上。

- 需要以下 Windows Server 2008 补丁：

- <http://support.microsoft.com/kb/958124>

此补丁可修复 Microsoft WMI 中的内存泄漏，这会阻止 ISE 与域控制器建立成功连接。

- <http://support.microsoft.com/kb/973995>

此补丁修复 Microsoft 的 WMI 中的不同的内存泄漏，该泄漏偶尔阻止 Active Directory 域控制器将必要的用户登录事件写入至域控制器的安全日志。

- Windows Server 2008 R2 需要以下补丁（除非安装 SP1）：

- <http://support.microsoft.com/kb/981314>

此补丁修复 Microsoft 的 WMI 中的内存泄漏，该泄漏偶尔阻止 Active Directory 域控制器将必要的用户登录活动事件写入至域控制器的安全日志。

- <http://support.microsoft.com/kb/2617858>

此补丁修复 Windows Server 2008 R2 中的启动或登录过程意外缓慢。

- 需要以下链接中列出的 Windows 平台 WMI 相关问题补丁：

- <http://support.microsoft.com/kb/2591403>

这些热修复与 WMI 服务及其相关组件的操作和功能相关。

### 步骤 2 确保 Active Directory 在 Windows 安全日志中记录用户登录事件。

验证“审核策略” (Audit Policy) 设置（“组策略管理” [Group Policy Management] 设置的一部分）支持成功登录在 Windows 安全日志中生成必要事件（这是 Windows 默认设置，但是，您必须明确保证此设置正确）。

### 步骤 3 您必须拥有具备足够权限的 Active Directory 用户才能将 ISE-PIC 连接到 Active Directory。以下说明显示如何为管理域组用户或无管理域组用户定义权限：

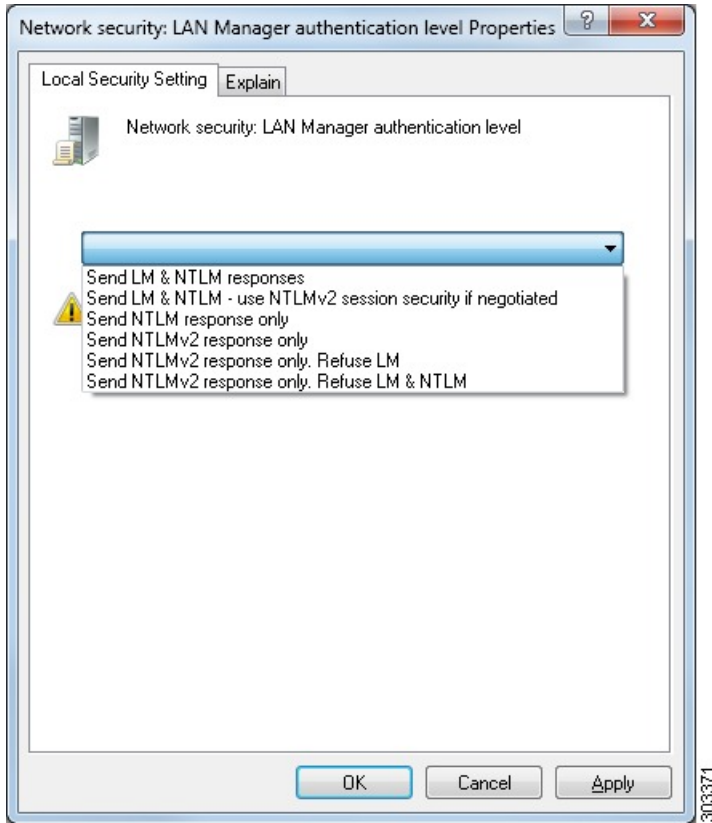
- Active Directory 用户为域管理员组成员时需要的权限
- Active Directory 用户不是域管理员组成员时需要的权限

**步骤 4** ISE-PIC 使用的 Active Directory 用户可以通过 NT LAN Manager (NTLM) v1 或 v2 进行身份验证。您需要验证 Active Directory NTLM 设置是否与 ISE-PIC NTLM 设置一致，以确保 ISE-PIC 和 Active Directory 域控制器之间的连接成功进行身份验证。下表显示所有 Microsoft NTLM 选项及支持哪些 ISE-PIC NTLM 操作。如果 ISE-PIC 设置为 NTLMv2，则支持所述的全部六个选项。如果 ISE-PIC 设置为支持 NTLMv1，则仅支持前五个选项。

表 4: 基于 ISE-PIC 和 AD NTLM 版本的受支持身份验证类型

ISE-PIC NTLM 设置选项 / Active Directory (AD) NTLM 设置选项 NTLMv1 NTLMv2	NTLMv1	NTLMv2
发送 LM & NTLM 响应	允许连接	允许连接
发送 LM & NTLM - 如果有协商，使用 NTLMv2 会话安全	允许连接	允许连接
仅发送 NTLM 响应	允许连接	允许连接
仅发送 NTLMv2 响应	允许连接	允许连接
仅发送 NTLMv2 响应。拒绝 LM	允许连接	允许连接
仅发送 NTLMv2 响应。拒绝 LM & NTLM	拒绝连接	允许连接

图 1: MS NTLM 身份验证类型选项



**步骤 5** 确保您已创建一个防火墙规则允许流量去往 Active Directory 域控制器中的 `dllhost.exe`。

您可以关闭防火墙，或者允许在特定 IP（ISE-PIC IP 地址）访问以下端口：

- TCP 135: 通用 RPC 端口。在执行异步 RPC 呼叫时，侦听此端口的服务告知客户端为此请求服务的组件使用哪个端口。
- UDP 137: Netbios 名称解析
- UDP 138: Netbios 数据报服务
- TCP 139: Netbios 会话服务
- TCP 445: SMB

可以动态分配更高的端口，也可以手动进行配置。我们建议您添加 `%SystemRoot%\System32\dllhost.exe` 作为目标。此程序可动态管理端口。

所有防火墙规则均可分配到特定 IP (ISE-PIC IP)。

## 为域管理员组中的 Microsoft Active Directory 用户设置权限

默认情况下，对于 Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2，域管理员组对 Windows 操作系统中的某些注册表项没有完全控制权限。Microsoft Active Directory 管理员必须给予 Microsoft Active Directory 用户对以下注册表项的完全控制权限：

- **HKEY\_CLASSES\_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

以下 Microsoft Active Directory 版本不需要对注册表进行更改：

- Windows 2003
- Windows 2003R2
- Windows 2008

要授予完全控制权限，Microsoft Active Directory 管理员必须首先获得注册表项的所有权：

**步骤 1** 右键单击注册表项图标，然后选择所有者 (Owner) 选项卡。

**步骤 2** 单击 **Permissions** (权限)。

**步骤 3** 单击高级 (Advanced)。

## 不在域管理员组中的 Microsoft Active Directory 用户的权限

对于 Windows Server 2012 R2，授予 Microsoft AD 用户对以下注册表项的完全控制权限：

- HKEY\_CLASSES\_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

在 Windows PowerShell 中使用以下命令来检查是否提供了对注册表项的完整权限：

- ```
get-acl -path "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list
```
- ```
get-acl -path "hkmlm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" | format-list
```

当 Microsoft AD 用户不在域管理员组，但在域用户组中时，还需要以下权限：

- 添加注册表项以允许 ISE-PIC 连接到域控制器。
- [在域控制器上使用 DCOM 的权限，第 25 页](#)
- [设置访问 WMI Root 和 CIMv2 命名空间的权限，第 27 页](#)

只有以下 Active Directory 版本要求具有这些权限：



- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

### 添加注册表项以允许ISE-PIC 连接到域控制器

必须手动将一些注册表项添加到域控制器，以允许ISE-PIC以域用户身份进行连接，并检索登录身份验证事件。域控制器或该域中的任何其他机器都不需要代理。

以下注册脚本显示了要添加的密钥。您可以将其复制并粘贴到一个文本文件，并另存为扩展名为 .reg 的文件，然后双击该文件进行注册更改。要添加注册密钥，用户必须是根密钥的所有者。

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "
```

确保 DllSurrogate 注册表项的值包含两个空格。如果手动更新注册表，必须仅包含两个空格，不包含引号。手动更新注册表时，请确保 AppID、DllSurrogate 及其值中不包含引号。

如前一步脚本所示，保留所有空行，包括文件末尾的空行。

在 Windows 命令提示符下使用以下命令，以确认注册表项是否已创建并包含正确值：

- reg query "HKEY\_CLASSES\_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e
- reg query HKEY\_CLASSES\_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e
- reg query HKEY\_CLASSES\_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f " " /e

### 在域控制器上使用 DCOM 的权限

用于ISE-PIC被动身份服务的 Microsoft Active Directory 用户必须具有在域控制器服务器上使用 DCOM 的权限。通过 **dcomcnfg** 命令行工具配置权限。

**步骤 1** 从命令行运行 **dcomcnfg** 工具。

步骤 2 扩展组件服务 (Component Services)。

步骤 3 扩展计算机 (Computers) > 我的计算机 (My Computer)。

步骤 4 从菜单栏中选择操作 (Action)，单击属性 (Properties)，然后单击 COM 安全性 (COM Security)。

步骤 5 思科 ISE 用于访问和启动的帐户必须具有允许权限。将 Microsoft Active Directory 用户添加至所有四个选项（访问权限 (Access Permissions) 和启动并激活权限 (Launch and Activation Permissions) 的编辑限制设置 (Edit Limits) 和编辑默认设置 (Edit Default)）。

步骤 6 对于访问权限 (Access Permissions) 和启动并激活权限 (Launch and Activation Permissions)，允许所有本地和远程访问。

图 2: 访问权限的本地和远程访问

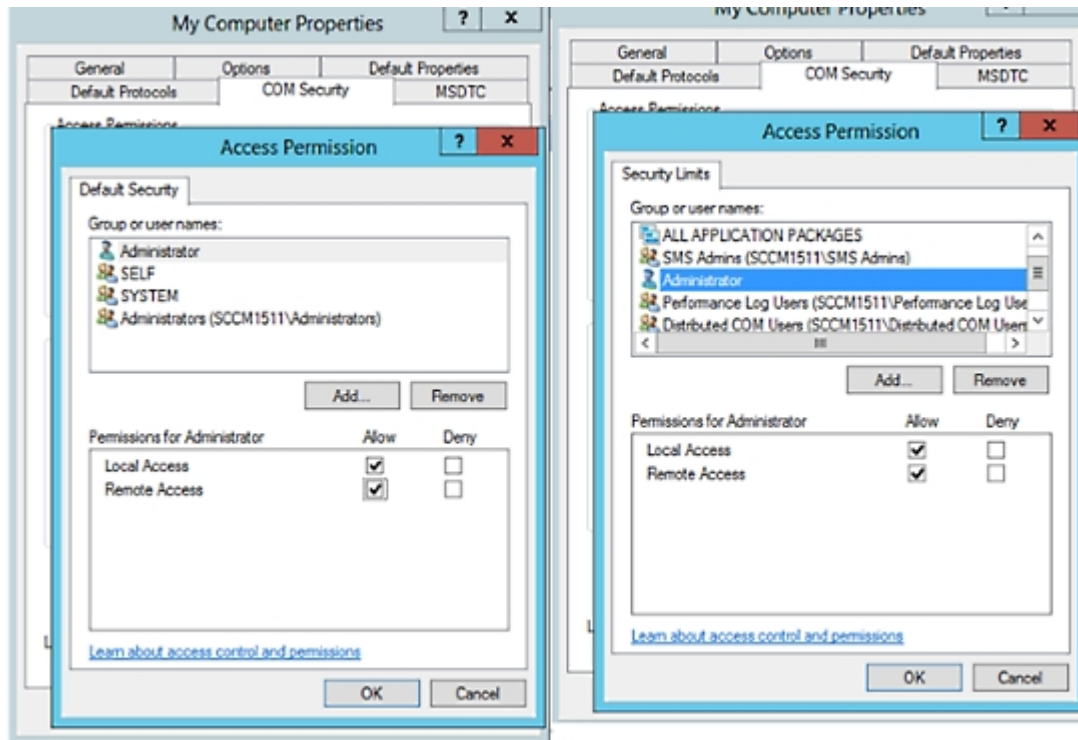
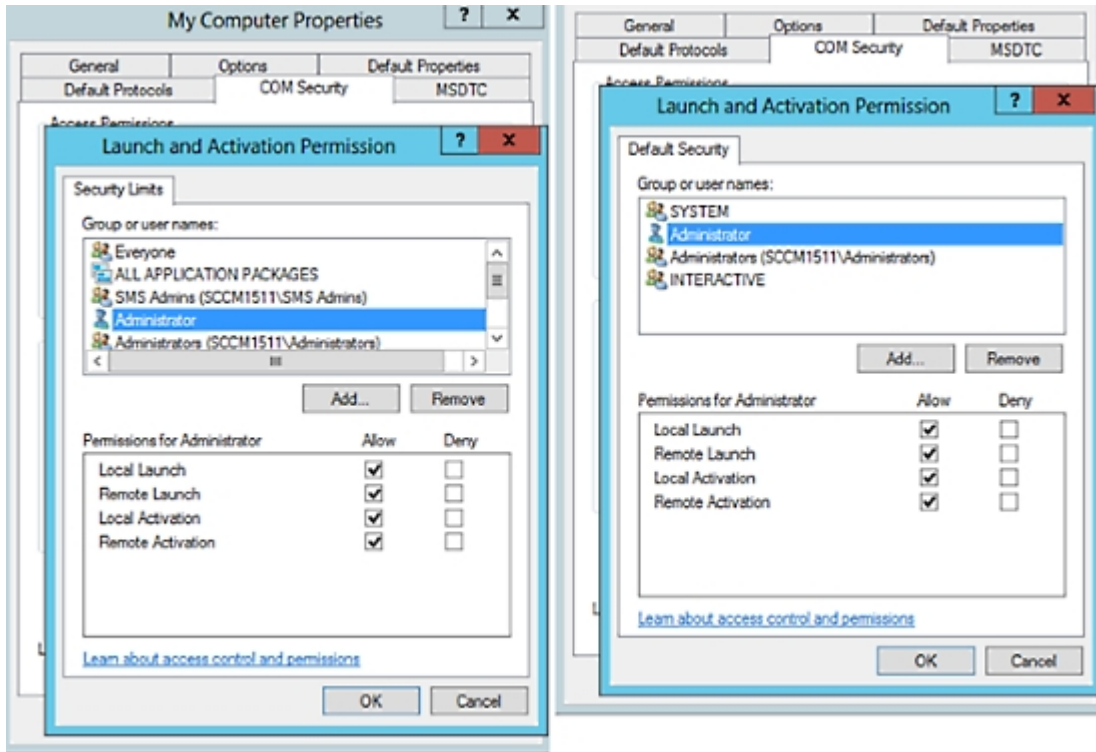


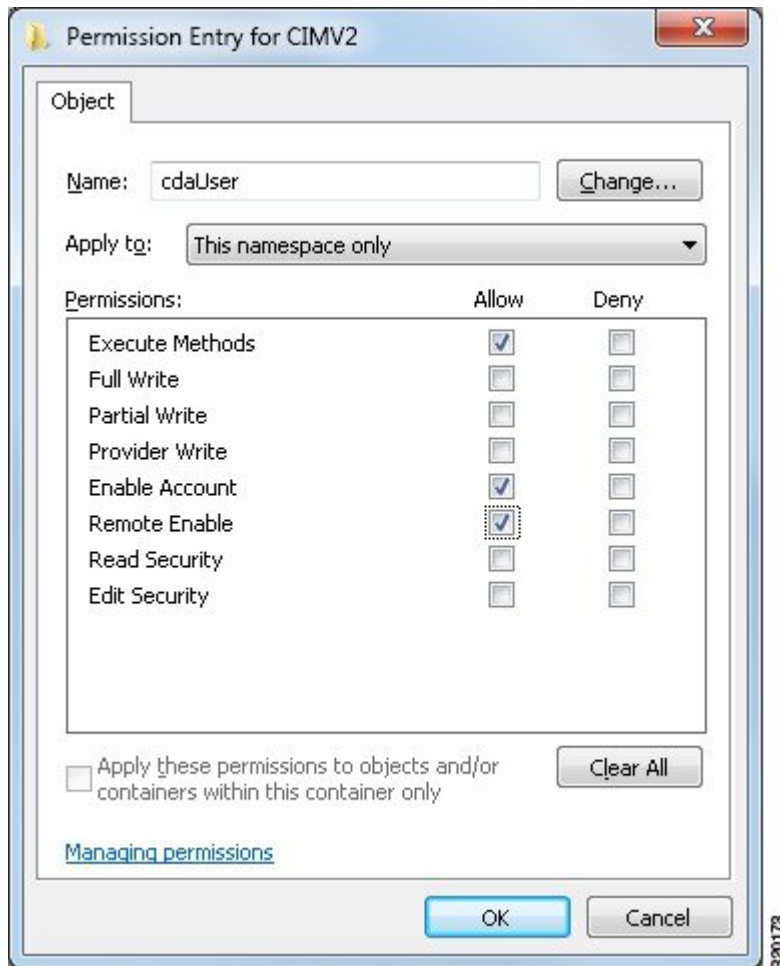
图 3: 启动和激活权限的本地和远程访问



### 设置访问 WMI Root 和 CIMv2 命名空间的权限

默认情况下，Microsoft Active Directory 用户没有对“执行方法” (Execute Methods) 和“远程启用” (Remote Enable) 的权限。您可以使用 `wimgmt.msc` MMC 控制台授予访问权限。

- 步骤 1 选择开始 (Start) > 运行 (Run)，然后输入 `wimgmt.msc`。
- 步骤 2 右键单击 WMI 控制 (WMI Control) 并单击属性 (Properties)。
- 步骤 3 在安全 (Security) 选项卡下，展开根 (Root) 并选择 CIMV2。
- 步骤 4 单击安全 (Security)。
- 步骤 5 添加 Active Directory 用户，并按如下所示配置所需的权限。



## 授权访问 AD 域控制器上的安全事件日志

在 Windows 2008 及更高版本上，您可以通过将 ISE-PIC ID 映射用户添加到名为“事件日志读取器”的组中来授予对 AD 域控制器日志的访问权限。

在 Windows 所有旧版本上，您必须编辑一个注册表项，如下所示。

**步骤 1** 要委托访问至安全事件日志，请查找该帐户的 SID。

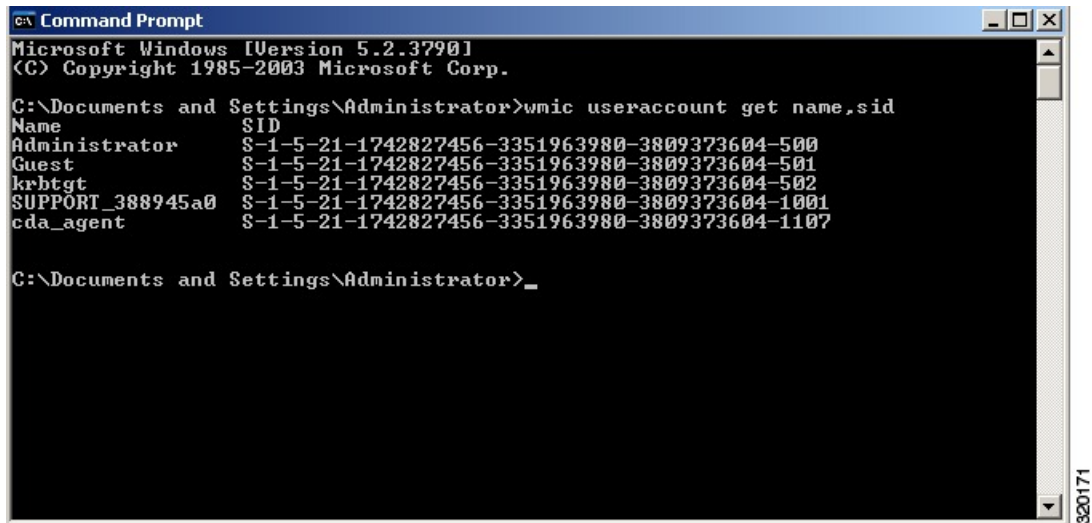
**步骤 2** 在命令行处使用以下命令，列出所有 SID 帐户，也如下图所示。

```
wmic useraccount get name,sid
```

您可以使用用于特定用户名和域的以下命令：

```
wmic useraccount where name="iseUser" get domain,name,sid
```

图 4: 列出所有 SID 帐户



```

c:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>wmic useraccount get name,sid
Name                SID
Administrator      S-1-5-21-1742827456-3351963980-3809373604-500
Guest                S-1-5-21-1742827456-3351963980-3809373604-501
krbtgt              S-1-5-21-1742827456-3351963980-3809373604-502
SUPPORT_388945a0    S-1-5-21-1742827456-3351963980-3809373604-1001
cda_agent           S-1-5-21-1742827456-3351963980-3809373604-1107

C:\Documents and Settings\Administrator>_

```

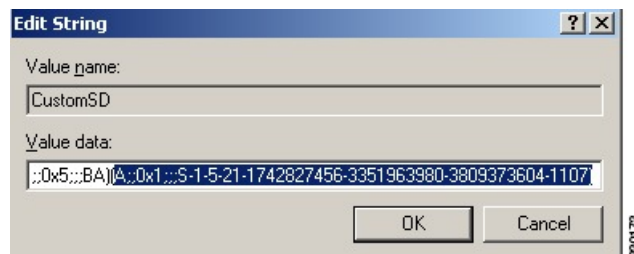
步骤 3 查找 SID，打开“注册表编辑器” (Registry Editor)，并对以下位置进行浏览：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog
```

步骤 4 单击安全 (Security)，然后双击 CustomSD。

例如，要允许读访问 ise\_agent 帐户 (SID - S-1-5-21-1742827456-3351963980-3809373604-1107)，请输入 (A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)。

图 5: 编辑 CustomSD 字符串



步骤 5 重启域控制器上的 WMI 服务。您可以通过以下两种方式重启 WMI 服务：

a) 在 CLI 处运行以下命令：

```
net stop winmgmt
```

```
net start winmgmt
```

b) 运行 Services.msc，打开 Windows 服务管理工具。在 Windows 服务管理窗口中，找到 Windows 管理规范 (Windows Management Instrumentation) 服务，右键单击，然后选择重启 (Restart)。

## 获取其他故障排除信息

通过思科 ISE-PIC，可以从管理员门户下载支持和故障排除信息。可以使用支持捆绑包为思科技术支持中心 (TAC) 准备诊断信息来对思科 ISE-PIC 的问题进行故障排除。



**注释** 支持捆绑包和调试日志为 TAC 提供高级故障排除信息，并且难以解释。可以使用思科 ISE-PIC 提供的各种报告和故障排除工具对在网络中面临的问题进行诊断和故障排除。

## 思科 ISE-PIC 支持捆绑包

您可以配置日志，使其成为支持捆绑包的一部分。例如，您可以配置来自特定服务的日志，使其成为调试日志的一部分。此外，您还可以根据日期过滤日志。

您可以下载的日志分类如下：

- 完整配置数据库：包含可读 XML 格式的思科 ISE-PIC 配置数据库。当您尝试解决问题时，可以将此数据库配置导入另一个思科 ISE 节点，以便重新创建场景。
- 调试日志：捕获引导程序、应用配置、运行时、部署、公共密钥基础设施 (PKI) 信息以及监控和报告。  
  
调试日志为特定的思科 ISE 组件提供故障排除信息。要启用调试日志，请参阅第 11 章日志记录。如果不启用调试日志，所有信息消息 (INFO) 将包含在支持捆绑包中。有关详细信息，请参阅 [思科 ISE-PIC 调试日志，第 32 页](#)。
- 本地日志：包含来自思科 ISE 上运行的各种进程的系统日志消息。
- 核心文件 - 包含有助于识别突发事件的原因的重要信息。这些日志在应用发生崩溃并且包含大量转储时创建。
- 监控和报告日志：包含关于警报和报告的信息。
- 系统日志 - 包含思科应用部署引擎 (ADE) 相关信息。
- 策略配置：包含在思科 ISE 中配置的可读格式的策略。

使用 **backup-logs** 命令可以从思科 ISE CLI 下载这些日志。有关详细信息，请参阅思科身份服务引擎 CLI 参考指南。

如果选择从 Admin 门户下载这些日志，您可以执行以下操作：

- 根据日志类型（例如调试日志或系统日志），仅下载日志子集。
- 对于所选日志类型，仅下载最新的  $n$  个文件。此选项允许您控制支持捆绑包的大小以及下载所需的时间。

监控日志提供关于监控、报告和故障排除功能的信息。有关下载日志的详细信息，请参阅 [下载思科 ISE-PIC 日志文件。](#)，第 31 页。

## 支持捆绑包

您可以将支持捆绑包以简单 tar.gpg 文件的形式下载至您的本地计算机。支持捆绑包将按照 ise-support-bundle\_ise-support-bundle-mm-dd-yyyy--hh-mm.tar.gpg 的格式用日期和时间戳命名。浏览器会提示您将支持捆绑包保存至适当的位置。您可以提取支持捆绑包的内容并查看 README.TXT 文件，此文件介绍该支持捆绑包的内容，以及在支持捆绑包包含 ISE 数据库内容的情况下如何导入 ISE 数据库内容。

## 下载思科 ISE-PIC 日志文件。

在对网络中的问题进行故障排除时，可以下载思科 ISE-PIC 日志文件，以查找更多信息。您也可以下载包含 ADE-OS 和其他日志文件的系统日志来排除安装和升级方面的问题。

### 开始之前

- 应已配置调试日志和调试日志级别。

---

**步骤 1** 选择 **管理 (Administration)** > **日志记录 (Logging)** > **下载日志 (Download Logs)** > **设备节点列表 (Appliance Node List)**。

**步骤 2** 单击要从其下载支持捆绑包的节点。

**步骤 3** 在 **支持捆绑包 (Support Bundle)** 选项卡中，选择要填充在您的支持捆绑包中的参数。

如果您将所有日志包含在内，则您的支持捆绑包会非常大，下载会需要较长时间。要优化下载流程，请选择只下载最新的  $n$  个文件。

**步骤 4** 输入生成支持捆绑包的**起始日期 (From)** 和**结束日期 (To)**。

**步骤 5** 选择以下其中一个选项：

- **公共密钥加密 (Public Key Encryption)**：如果您想要向思科 TAC 提供支持捆绑包以进行故障排除，请选择此选项。
- **共享密钥加密 (Shared Key Encryption)**：如果您希望在现场排除故障，请选择此选项。如果选择此选项，您必须输入支持捆绑包的加密密钥。

**步骤 6** 单击 **创建支持捆绑包 (Create Support Bundle)**。

**步骤 7** 单击 **下载 (Download)** 以下载新创建的支持捆绑包。

支持捆绑包是下载到正在运行您的应用浏览器的客户端系统的一个 tar.gpg 文件。

---

### 下一步做什么

下载特定组件的调试日志。

## 思科 ISE-PIC 调试日志

调试日志为各种思科 ISE-PIC 组件提供故障排除信息。调试日志包含过去 30 天生成的紧急和警告警报以及在过去 7 天生成的信息警报。报告问题时，可能会要求您启用并发送这些调试日志，以便诊断和解决问题。



**注释** 启用具有高负载的调试日志（例如监控调试日志）会生成有关高负载的警报。

## 获取调试日志

**步骤 1** 配置您希望获取调试日志的组件。

**步骤 2** 下载调试日志。

## 思科 ISE-PIC 组件和相应的调试日志

**注释** 以下列表是 ISE 中可用组件的完整列表。表格中列出的某些组件可能与 ISE-PIC 不相关。

表 5: 组件和相应的调试日志

组件	调试日志
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log



组件	调试日志
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
anc	ise-psc.log
anc	ise-psc.log
ers	ise-psc.log
guest	ise-psc.log
Guest Access Admin	guest.log
Guest Access	guest.log
MyDevices	guest.log
Portal	guest.log
Portal-Session-Manager	guest.log
Portal-web-action	guest.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log

组件	调试日志
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

## 下载调试日志

**步骤 1** 选择 **管理 (Administration)** > **日志记录 (Logging)** > **下载日志 (Download Logs)**。

**步骤 2** 在“设备节点” (Appliance node) 列表中，单击您希望下载调试日志的节点。

**步骤 3** 单击调试日志 (**Debug Logs**) 选项卡。

系统会显示调试日志类型和调试日志的列表。此列表显示的内容取决于您的调试日志配置。

**步骤 4** 单击您希望下载的日志文件并将其保存到正在运行客户端浏览器的系统中。

您可以根据需要重复此过程下载其他日志文件。可以从**调试日志 (Debug Logs)** 页面下载以下额外的调试日志：

- isebootstrap.log: 提供引导日志消息
- monit.log: 提供监视程序消息
- pki.log: 提供第三方加密库日志
- iseLocalStorage.log: 提供本地存储文件相关日志
- ad\_agent.log: 提供 Microsoft Active Directory 第三方库日志
- catalina.log: 提供第三方日志