思科 ISE 系统日志简介

思科 ISE 消息目录

思科身份识别服务引擎(ISE)提供用于审核、故障管理和故障排除的日志记录机制。日志记录机制可以帮助您识别所部署的服务中的故障情况并有效地对相应问题进行故障排除。它还以一致的方式从监控和故障排除主要节点提供日志记录输出。

在思科 ISE 中，系统在称为日志记录目标的位置收集系统日志。目标是指收集和存储日志的服务器的 IP 地址。您可以在本地生成和存储日志，也可以使用 FTP 工具将日志传输至外部服务器。

可以使用思科 ISE 控制板的“消息目录”(Message Catalog) 页面查看所有可能的日志消息和说明。依次选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。

系统将显示“日志消息目录”(Log Message Catalog) 页面，您可以在此查看所有显示在日志文件中可能的日志消息。此页面中可用的数据仅用于显示。如果使用的是思科 ISE 2.3 及更高版本，请选择**导出 (Export)** 以 CSV 文件形式导出所有系统日志消息。

本地存储系统日志消息格式

思科 ISE 日志消息以如下系统日志消息格式发送至本地存储：

timestamp sequence_num msg_ode msg_sev msg_class msg_text attr =value

字段	说明
timestamp	依据源思科 ISE 节点的本地时钟的消息生成的日期，格式如下： *YYYY- MM-DD hh:mm:ss:xxx +/-zh:zm*。 可能的值包括： • YYYY = 年份的数字表示。 • MM = 月份的数值表示。对于单个数的月份（1 月至 9 月），此数值前加零。 • DD=每月的日期数字表示。对于单个数的日期（每月 1 号至 9 号），此数值前加零。 • hh = 一天的整点 - 此值范围为 00 至 23。 • mm = 整点后面的分钟数 - 此值范围为 00 至 59。 • ss = 分钟数后的秒数 - 此值范围为 00 至 59。 • xxx = 秒数后面的毫秒数 - 此值范围为 000 至 999。 • +/-zh:zm = 与思科 ISE 服务器时区的时区偏移，其中 zh 是偏移小时数，zm 是偏移小时的分钟数，所有时区偏移值前面都有一个正号或负号，表示偏移的方向。例如，+02:00 表示某个思科 ISE 节点上在时间戳指示的时间生成的消息比思科 ISE 服务器时区早两个小时。
sequence_num	每条消息的全局计数器。如果一条消息发送至本地存储库，下一条消息发送至系统日志服务器目标，则该计数器数值增加 2。可能的值为 0000000001 至 999999999。
msg_ode	日志记录类别中定义的消息代码。
msg_sev	日志消息的消息严重性级别。请查看 **Administration** > **System** > **Logging** > **Logging Categories**。
msg_class	消息类，是具有相同上下文的一系列消息的标识。
msg_text	英文说明性文本消息。

字段	说明
attr=value	属性 - 值对的集合，提供关于所记录事件的详细信息。每对之间用逗号 (,) 隔开。 属性名称如思科 ISE 字典所定义。 Response direction AttributesSet 的值与一个名称为 Response 的属性放在一起并用花括号 “{} ” 括起来。此外，Response 内的属性-值对用分号分隔。 例如，Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00;}

远程系统日志消息格式

思科 ISE 日志消息采用此系统日志消息信头格式发送到远程系统日志服务器，此格式位于本地存储库系统日志消息格式之前：

pri_num Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

字段	说明
pri_num	消息的优先级值；消息的易度值和严重性值的组合。优先级值 =（易度值*8）+ 严重性值。请参阅适用于您的版本的相关《思科 ISE 管理员指南》，以设置消息代码的安全级别。 设备代码的有效选项包括： • LOCAL0（代码 = 16） • LOCAL1（代码 = 17） • LOCAL2（代码 = 18） • LOCAL3（代码 = 19） • LOCAL4（代码 = 20） • LOCAL5（代码 = 21） • LOCAL6（代码 = 22；默认值） • LOCAL7（代码 = 23）

字段	说明
time	基于原始思科 ISE 服务器本地时钟的消息生成日期，格式为 Mmm DD hh:mm:ss。 可能的值包括： • Mmm = 月份表示 - Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec。 • DD=每月的日期数字表示。对于一位数的日期（1 至 9），数字前面留有一个空格。 • hh = 一天的整点 - 此值范围为 00 至 23。 • mm = 整点后面的分钟数 - 此值范围为 00 至 59。 • ss = 分钟数后的秒数 - 此值范围为 00 至 59。 某些设备会发送以 -/+hhmm 格式指定时区的消息，其中 - 和 + 用于标识思科 ISE 服务器时区的方向偏移量，hh 是偏移小时数，mm 是偏移小时的分钟数。例如，+02:00 表示某个思科 ISE 节点上在时间戳指示的时间生成的消息比思科 ISE 服务器时区早两个小时。
xx:xx:xx:xx/host_name	原始思科 ISE 节点的 IP 地址或主机名。
cat_name	CSCOxxx 字符串之后的日志记录类别名称。
msg_id	唯一消息 ID；1 至 4294967295。消息 ID 随着每个新消息递增 1。每次重新启动应用时，消息 ID 会从 1 重新开始。
total_seg	日志消息中的分段总数。长消息划分为多个分段。 **注释** *total_seg* 取决于远程日志记录目标页面中的 Maximum Length 设置。请参阅“远程日志记录目标设置”。
seg_num	消息中的分段的序列号。使用此号码可确定正在查看的消息的分段。

日志消息数据或负载与本地存储系统日志消息格式相同。远程系统日志服务器目标使用设备代码名称进行标识，范围为 LOCAL0 到 LOCAL7（LOCAL6 是默认日志记录位置）。您分配给远程系统日志服务器的日志消息被发送至 Linux 系统日志的默认位置 (/var/log/messages)，但是您可以在服务器上配置不同位置。