排除Umbrella中活动搜索报告中缺少的Active Directory用户故障

目录

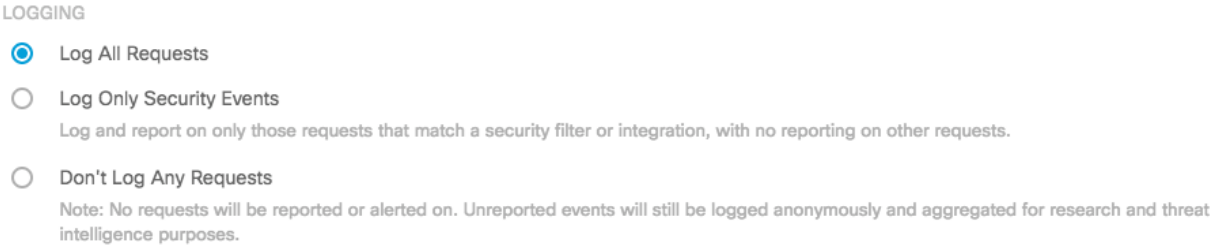
简介

本文档介绍Cisco Umbrella中的活动搜索报告。活动搜索报告是几乎实时的报告，其中包含用户正在执行的所有DNS查询。如果您已设置Cisco Umbrella Active Directory(AD)集成，您可能会看到您的AD用户填充您的活动搜索中的Identity列。但是，有时用户会从Identity列中丢失。

分辨率

如果您认为应该直接在“活动搜索”的“身份”列中看到AD用户，但是没有看到他们，或者看到了一些AD用户，但数量没有预期的多，请注意以下几点：

1. 站点和Active Directory
    - 检查所有AD组件，确保没有报告的错误或问题。如果您在任何组件上看到任何灰色、橙色或红色状态指示灯，请获取这些详细信息并打开支持通知单(umbrella-support@cisco.com)。
        - 来自受影响的用户（未显示在活动搜索中的用户）的诊断测试
        - 虚拟设备(VA)控制台的截图，其中扩展了任何错误消息
        - AD连接器审核日志
2. 日志记录设置
    - 在每个策略的Advanced Settings中，底部有一个关于记录量的部分。您可以将其设置为：
        - 记录所有请求
        - 仅记录安全事件
        - 不记录任何请求
    - 如果您的策略当前设置为“仅记录安全事件”，则可以解释为什么您看到的查询没有预期的多，或者某些用户根本没有结果。



3. 正确的策略优先级
    - 如果您的策略应用于网络身份在策略列表中比AD用户策略高，则网络身份策略可能会应用。这进而意味着，在活动搜索中，您将看到网络作为报告的身份。有关最佳实践和策略优先顺序，请查看Cisco Umbrella文档。

原因

活动搜索从哪里获取“身份”？

当DNS查询进入Umbrella时，假设您的AD集成按预期运行，此信息将在查询中传递：

- 内部 IP 地址
- AD身份哈希（用户、主机或两者）
- 出口IP
- 正在查询的域

AD身份散列由虚拟设备添加到查询，虚拟设备传递了该信息，并从AD连接器为登录事件提供了相应的内部IP地址。

然后，Cisco Umbrella使用此信息查找组织并确定应用哪个策略。如果您没有专门应用于AD用户的策略，但针对您的网络或站点有策略，则Cisco Umbrella会使用该身份应用策略。这意味着当在活动搜索中报告查询、标识和响应时，即触发所报告策略的标识。其他信息仍被标记在请求中，因此您仍然可以搜索AD用户并获取将网络报告为标识的活动。此外，如果将“活动搜索”数据导出到CSV文件，则会显示与该查询关联的所有身份信息。

Additional Information

如果您仍然没有看到任何AD用户，请与支持部门(umbrella-support@cisco.com)联系，并提供诊断测试结果，以及相关的AD连接器审核日志。

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）。