配置DLP失效关闭行为，阻止云连接丢失期间的用户操作

目录

问题

安装了终端DLP(EDLP)模块的用户遇到阻止打印和复制到网络文件共享的问题，尽管未包括在任何已配置的EDLP规则中。所有现有EDLP规则均在MONITOR模式下配置，这些规则中仅包含3个特定用户。受影响的用户遇到针对打印操作和文件共享复制操作的意外阻止操作，即使这些操作不打算接受EDLP实施。

在故障排除期间，确定当EDLP云连接不可用时发生了阻塞，导致系统应用故障关闭行为作为回退机制。在EDLP客户端未建立与云服务的连接以进行策略裁决期间，用户遇到打印和网络共享访问被拒绝的情况。

环境

- 思科终端DLP模块版本1.5.0.292
- 思科安全访问/安全/防数据丢失门户管理
- 在监控模式下配置多个EDLP规则
- 配置了失效关闭行为的网络共享信道
- 影响客户端网络连接的DNS解析更改

分辨率

解决方案涉及了解和解释EDLP失效关闭行为及其在云连接丢失期间的应用：

根本原因分析

对DART捆绑包和EDLP日志的分析显示，EDLP应用了拒绝回退，因为网络共享通道被配置为失效关闭。发生阻止事件时，由于客户端网络上的DNS解析更改，EDLP云连接不可用，导致系统无法从云服务获取策略判定。

失效关闭行为解释

因为安装了EDLP模块，所以故障关闭策略已应用到用户的系统，无论用户身份是否包括在任何特定EDLP规则中。失效开放/失效关闭状态是在DLP策略配置中调配的全局设置，信道配置根据该全局设置应用。

连接恢复

在客户端网络上恢复DNS稳定性后，问题会自动解决，从而允许EDLP客户端重新建立与云服务的连接。一旦基本网络连接问题得到解决，就无需手动干预。

导致故障关闭行为的条件

以下条件可以触发EDLP失效关闭行为：

- DNS解析问题
- 网络故障
- 在网络之间切换
- 任何阻止客户端与云服务之间端到端连接的条件

原因

阻止行为是由网络共享信道的EDLP的故障关闭配置引起的。当EDLP客户端由于DNS解析更改而失去与云服务的连接时，它无法获得策略判决，因此将配置的故障关闭行为作为安全回退机制实施。无论用户是否明确包括在任何EDLP规则中，都会发生这种情况，因为失败关闭设置全局应用于云连接不可用时安装了EDLP模块的所有系统。

相关内容

- 思科技术支持和下载

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）。