配置DLP失效關閉行為阻止雲連線丟失期間的使用者操作

目錄

問題

安裝了終端DLP(EDLP)模組的使用者在列印和複製到網路檔案共用時遇到阻塞，儘管未包括在任何已配置的EDLP規則中。所有現有的EDLP規則均在MONITOR模式下配置，這些規則中僅包含3個特定使用者。受影響的使用者遇到列印操作和檔案共用複製操作的意外塊操作，即使這些操作不打算接受EDLP實施。

在故障排除過程中，確定當EDLP雲連線不可用時發生了阻塞，導致系統應用故障關閉行為作為回退機制。在EDLP客戶端未建立到雲服務的連線以進行策略裁決期間，使用者遇到列印和網路共用訪問被拒絕的情況。

環境

- 思科終端DLP模組版本1.5.0.292
- 思科安全訪問/安全/資料丟失防護門戶管理
- 在MONITOR模式下配置多個EDLP規則
- 配置了失效關閉行為的網路共用通道
- 影響客戶端網路連線的DNS解析更改

解析

解決方案涉及瞭解和解釋EDLP失效關閉行為及其在雲連線丟失期間的應用：

根本原因分析

對DART捆綁包和EDLP日誌的分析顯示，EDLP應用了拒絕回退，因為網路共用通道被配置為失效關閉。發生阻止事件時，由於客戶端網路上的DNS解析更改，EDLP雲連線不可用，導致系統無法從雲服務獲取策略裁決。

失效關閉行為說明

因為安裝了EDLP模組，所以將失效關閉策略應用到使用者的系統，而不管使用者身份是否包含在任何特定EDLP規則中。失效開放/失效關閉狀態是在DLP策略配置中調配的全域性設定，並根據該全域性設定應用通道配置。

連線恢復

在客戶端網路上恢復DNS穩定性後，問題會自動解決，從而允許EDLP客戶端重新建立與雲服務的連線。解決底層網路連線問題後，無需手動干預。

導致失效關閉行為的條件

以下條件可能會觸發EDLP失效關閉行為：

- DNS解析問題
- 網路中斷
- 網路間交換
- 任何阻止客戶端和雲服務之間端到端連線的條件

原因

阻塞行為是由EDLP的網路共用通道的失效關閉配置引起的。當EDLP客戶端由於DNS解析更改而失去與雲服務的連線時，它無法獲得策略判決，因此將配置的故障關閉行為作為安全回退機制實施。無論使用者是否明確包括在任何EDLP規則中，都會發生這種情況，因為失效關閉設定全域性應用於雲連線不可用時安裝了EDLP模組的所有系統。

相關內容

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。