Configurar o comportamento de fechamento com falha do DLP que bloqueia as ações do usuário durante a perda de conectividade de nuvem

Contents

Problema

Um usuário com o módulo EDLP (DLP de endpoint) instalado estava com bloqueio de impressão e cópia para compartilhamentos de arquivos de rede, apesar de não estar incluído em nenhuma regra EDLP configurada. Todas as regras EDLP existentes foram configuradas no modo MONITOR com apenas 3 usuários específicos incluídos nessas regras. O usuário afetado estava encontrando ações de bloqueio inesperadas para operações de impressão e de cópia de compartilhamento de arquivos, mesmo que elas não estivessem sujeitas à aplicação de EDLP.

Durante a solução de problemas, foi determinado que o bloqueio ocorreu quando a conectividade de nuvem EDLP não estava disponível, fazendo com que o sistema aplicasse o comportamento de fechamento com falha como um mecanismo de fallback. O usuário teve uma negação de acesso à impressão e ao compartilhamento de rede durante os períodos em que o cliente EDLP não estabeleceu conectividade com o serviço de nuvem para vereditos de política.

Ambiente

- Módulo Cisco Endpoint DLP versão 1.5.0.292
- Gerenciamento do portal Cisco Secure Access/Secure/Data Loss Prevention
- Várias regras EDLP configuradas no modo MONITOR
- Canal de compartilhamento de rede configurado com comportamento fail-closed
- Alterações de resolução DNS que afetam a conectividade de rede do cliente

Resolução

A resolução envolvia compreender e explicar o comportamento de EDLP com falha fechada e sua aplicação durante a perda de conectividade de nuvem:

Análise da causa raiz

A análise do pacote DART e dos logs EDLP revelou que o EDLP aplicou um fallback de negação porque o canal de compartilhamento de rede foi configurado como fail-closed. No momento dos incidentes de bloqueio, a conectividade de nuvem EDLP estava indisponível devido a alterações na resolução de DNS na rede do cliente, impedindo que o sistema obtivesse vereditos de política do serviço de nuvem.

Explicação do comportamento de fechamento com falha

A política de fechamento com falha foi aplicada ao sistema do usuário porque o módulo EDLP foi instalado, independentemente da identidade do usuário ter sido incluída em qualquer regra EDLP específica. O estado fail-open/fail-closed é uma configuração global fornecida na configuração de Política DLP e a configuração de canal é aplicada com base nessa configuração global.

Recuperação de conectividade

O problema foi resolvido automaticamente quando a estabilidade do DNS foi restaurada na rede do cliente, permitindo que o cliente EDLP restabelecesse a conectividade com o serviço de nuvem. Não foi necessária nenhuma intervenção manual depois que o problema de conectividade de rede subjacente foi resolvido.

Condições que causam o comportamento de fechamento com falha

Essas condições podem acionar o comportamento de fechamento com falha do EDLP:

- Problemas de resolução DNS
- Interrupções de rede
- Comutação entre redes
- Qualquer condição que impeça a conexão de ponta a ponta entre o cliente e o serviço de nuvem

Causa

O comportamento de bloqueio foi causado pela configuração fail-closed do EDLP para o canal de compartilhamento de rede. Quando o cliente EDLP perdeu conectividade com o serviço de nuvem devido a alterações na resolução DNS, ele não pode obter vereditos de política e, portanto, aplica o comportamento de fechamento com falha configurado como um mecanismo de fallback de segurança. Isso ocorreu independentemente de o usuário ter sido explicitamente incluído em alguma regra EDLP, pois a configuração de fechamento com falha se aplica globalmente a todos os sistemas com o módulo EDLP instalado quando a conectividade de nuvem não está disponível.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.