Configuration du comportement de fermeture en cas d'échec DLP bloquant les actions des utilisateurs pendant la perte de connectivité du cloud

Table des matières

Problème

Un utilisateur avec le module EDLP (Endpoint DLP) installé ne pouvait pas imprimer et copier sur des partages de fichiers réseau, bien qu'il n'ait pas été inclus dans les règles EDLP configurées. Toutes les règles EDLP existantes ont été configurées en mode MONITOR avec seulement 3 utilisateurs spécifiques inclus dans ces règles. L'utilisateur affecté a rencontré des actions de blocage inattendues pour les opérations d'impression et de copie de partage de fichiers, même s'il n'était pas prévu qu'elles soient soumises à l'application EDLP.

Au cours du dépannage, il a été déterminé que le blocage s'était produit lorsque la connectivité au cloud EDLP était indisponible, ce qui a amené le système à appliquer un comportement de fermeture en cas de panne comme mécanisme de secours. L'utilisateur a subi un refus d'impression et d'accès au partage réseau pendant les périodes où le client EDLP n'a pas établi de connectivité au service cloud pour les verdicts de stratégie.

Environnement

- Module Cisco Endpoint DLP version 1.5.0.292
- Gestion du portail Cisco Secure Access/Secure/Data Loss Prevention
- Plusieurs règles EDLP configurées en mode MONITOR
- Canal de partage réseau configuré avec un comportement de fermeture en cas de panne
- Modifications de résolution DNS affectant la connectivité réseau du client

Résolution

La résolution impliquait la compréhension et l'explication du comportement de fermeture en cas de panne EDLP et de son application en cas de perte de connectivité du cloud :

Analyse de la cause première

L'analyse de l'ensemble DART et des journaux EDLP a révélé qu'EDLP a appliqué un refus de secours parce que le canal de partage réseau a été configuré comme fermé en cas de panne. Au moment des incidents de blocage, la connectivité cloud EDLP était indisponible en raison des modifications apportées à la résolution DNS sur le réseau client, empêchant ainsi le système d'obtenir des verdicts de stratégie du service cloud.

Explication Du Comportement De Fermeture Automatique

La stratégie de fermeture en cas d'échec a été appliquée au système de l'utilisateur car le module EDLP a été installé, que l'identité de l'utilisateur ait été incluse ou non dans une règle EDLP spécifique. L'état fail-open/fail-closed est un paramètre global provisionné dans la configuration de la stratégie DLP, et la configuration du canal est appliquée en fonction de ce paramètre global.

Récupération de connectivité

Le problème a été résolu automatiquement une fois la stabilité DNS restaurée sur le réseau client, ce qui a permis au client EDLP de rétablir la connectivité au service cloud. Aucune intervention manuelle n'a été requise une fois le problème de connectivité réseau sous-jacent résolu.

Conditions Provoquant Un Comportement De Fermeture Automatique

Ces conditions peuvent déclencher un comportement de fermeture en cas de panne EDLP :

- Problèmes de résolution DNS

- Pannes réseau
- Commutation entre les réseaux
- Toute condition empêchant une connexion de bout en bout entre le client et le service cloud

Motif

Le comportement de blocage a été provoqué par la configuration de fermeture en cas de panne d'EDLP pour le canal de partage réseau. Lorsque le client EDLP a perdu la connectivité au service cloud en raison des modifications apportées à la résolution DNS, il ne peut pas obtenir de verdicts de stratégie et, par conséquent, a appliqué le comportement de fermeture en cas d'échec configuré comme mécanisme de secours de sécurité. Cela s'est produit indépendamment du fait que l'utilisateur ait été explicitement inclus dans les règles EDLP, car le paramètre de fermeture en cas de panne s'applique globalement à tous les systèmes sur lesquels le module EDLP est installé lorsque la connectivité au cloud n'est pas disponible.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.