Configuración del comportamiento de DLP cerrado a fallos que bloquea las acciones del usuario durante la pérdida de conectividad a la nube

Contenido

Problema

Un usuario con el módulo de DLP para terminales (EDLP) instalado estaba experimentando un bloqueo al imprimir y copiar en recursos compartidos de archivos de red, a pesar de no estar incluido en ninguna regla de EDLP configurada. Todas las reglas de EDLP existentes se configuraron en modo MONITOR, con solo 3 usuarios específicos incluidos en dichas reglas. El usuario afectado se estaba encontrando con acciones de bloqueo inesperadas para las operaciones de impresión y las operaciones de copia de archivos compartidos, aunque no estaban destinadas a estar sujetas a la aplicación de EDLP.

Durante la resolución de problemas, se determinó que el bloqueo se producía cuando la conectividad de la nube de EDLP no estaba disponible, lo que provocaba que el sistema aplicara un comportamiento de fallo-cierre como mecanismo de reserva. Se denegó al usuario la impresión y el acceso al recurso compartido de red durante los períodos en los que el cliente EDLP no estableció la conectividad con el servicio en la nube para emitir veredictos de políticas.

Entorno

- Módulo Cisco Endpoint DLP versión 1.5.0.292
- Gestión del portal de Cisco Secure Access/Secure/Data Loss Prevention
- Varias reglas EDLP configuradas en modo MONITOR
- Canal compartido de red configurado con comportamiento de fallo-cierre
- Cambios en la resolución DNS que afectan a la conectividad de red del cliente

Resolución

La resolución implicaba comprender y explicar el comportamiento de cierre ante fallos de EDLP y su aplicación durante la pérdida de conectividad a la nube:

Análisis de causa raíz

El análisis del paquete DART y de los registros de EDLP reveló que EDLP aplicó una reserva de denegación porque el canal compartido de red se configuró como cerrado a fallos. En el momento de los incidentes de bloqueo, la conectividad de nube de EDLP no estaba disponible debido a los cambios de resolución de DNS en la red del cliente, lo que impedía al sistema obtener veredictos de políticas del servicio en la nube.

Explicación del comportamiento de fallo-cierre

La política de cierre por error se aplicó al sistema del usuario porque se instaló el módulo EDLP, independientemente de si la identidad del usuario se incluía en alguna regla EDLP específica. El estado fallo-apertura/fallo-cierre es una configuración global proporcionada en la configuración de la política DLP y la configuración de canal se aplica en función de esa configuración global.

Recuperación de conectividad

El problema se resolvió automáticamente una vez restaurada la estabilidad de DNS en la red del cliente, lo que permitió al cliente EDLP restablecer la conectividad con el servicio en la nube. No se requirió ninguna intervención manual una vez que se resolvió el problema de conectividad de red subyacente.

Condiciones que provocan el comportamiento de fallo-cierre

Estas condiciones pueden activar el comportamiento de cierre a fallos de EDLP:

- Problemas de resolución de DNS
- Interrupciones de red
- Cambio entre redes
- Cualquier condición que impida la conexión integral entre el cliente y el servicio en la nube

Causa

El comportamiento de bloqueo fue causado por la configuración de cierre por error de EDLP para el canal compartido de red. Cuando el cliente EDLP perdió la conectividad con el servicio en la nube debido a cambios en la resolución DNS, no puede obtener veredictos de políticas y, por lo tanto, aplicó el comportamiento de fallo-cierre configurado como mecanismo de reserva de seguridad. Esto ocurrió independientemente de si el usuario estaba incluido explícitamente en alguna regla EDLP, ya que la configuración de cierre por error se aplica globalmente a todos los sistemas con el módulo EDLP instalado cuando la conectividad en la nube no está disponible.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).