DLP Fail-Closed Behavior (DLP) configureren om acties van gebruikers te blokkeren tijdens het verlies van connectiviteit in de cloud

Inhoud

uitgifte

Een gebruiker met de geïnstalleerde Endpoint DLP-module (EDLP) ondervond blokkering van afdrukken en kopiëren naar gedeelde netwerkbestanden, ondanks dat deze niet was opgenomen in geconfigureerde EDLP-regels. Alle bestaande EDLP-regels zijn in de MONITORMODUS geconfigureerd en slechts 3 specifieke gebruikers zijn in die regels opgenomen. De betrokken gebruiker ondervond onverwachte blokacties voor afdrukbewerkingen en bestands-share-kopieerbewerkingen, hoewel deze niet bedoeld waren om te worden onderworpen aan EDLP-handhaving.

Tijdens het oplossen van problemen werd vastgesteld dat de blokkering plaatsvond wanneer EDLP-cloudconnectiviteit niet beschikbaar was, waardoor het systeem failclosed gedrag toepaste als een fallback-mechanisme. De gebruiker heeft tijdens perioden waarin de EDLP-client geen verbinding met de cloudservice tot stand bracht voor beleidsbeslissingen, het afdrukken en delen van netwerktoegang geweigerd.

milieu

- Cisco Endpoint DLP-module versie 1.5.0.292
- Cisco Secure Access/Secure/Data Loss Prevention Portal Management
- Meerdere EDLP-regels geconfigureerd in MONITORMODUS
- Netwerkdeelkanaal geconfigureerd met niet-gesloten gedrag
- Wijzigingen in DNS-resolutie die van invloed zijn op de netwerkconnectiviteit van de client

resolutie

De resolutie betrof het begrijpen en verklaren van het door een storing-gesloten gedrag van de EDLP en de toepassing ervan tijdens het verlies van connectiviteit in de cloud:

analyse van de grondoorzaak

Analyse van de DART-bundel en EDLP-logs toonde aan dat EDLP een fallback van de weigering toepaste omdat het kanaal voor netwerkdeling was geconfigureerd als failclosed. Ten tijde van de blokkeringsincidenten was de EDLP-cloudconnectiviteit niet beschikbaar vanwege wijzigingen in de DNS-resolutie op het clientnetwerk, waardoor het systeem geen beleidsbeslissingen van de cloudservice kon krijgen.

Uitleg over mislukt gesloten gedrag

Het failclosed-beleid is toegepast op het systeem van de gebruiker omdat de EDLP-module is geïnstalleerd, ongeacht of de identiteit van de gebruiker is opgenomen in een specifieke EDLP-regel. De status fail-open/fail-closed is een algemene instelling die is ingesteld in de DLP-beleidsconfiguratie en de kanaalconfiguratie wordt toegepast op basis van die algemene instelling.

Connectiviteitsherstel

Het probleem is automatisch opgelost zodra de DNS-stabiliteit op het clientnetwerk is hersteld, waardoor de EDLP-client opnieuw verbinding met de cloudservice kan maken. Er was geen handmatige interventie vereist zodra het onderliggende probleem met de netwerkconnectiviteit was opgelost.

Aandoeningen die faalgesloten gedrag veroorzaken

Deze voorwaarden kunnen leiden tot niet-gesloten gedragingen in het kader van de EDLP:

- Problemen met DNS-oplossing
- Netwerkuitval
- Schakelen tussen netwerken
- Elke voorwaarde die end-to-end verbinding tussen de client en de cloudservice voorkomt

Oorzaak

Het blokkeringsgedrag werd veroorzaakt door de failclosed-configuratie van EDLP voor het netwerkdeelkanaal. Wanneer de EDLP-client de connectiviteit met de cloudservice heeft verloren als gevolg van wijzigingen in de DNS-resolutie, kan deze geen beleidsbeslissingen verkrijgen en daarom het geconfigureerde failclosed-gedrag afdwingen als een beveiligingsfallback-mechanisme. Dit gebeurde ongeacht of de gebruiker expliciet was opgenomen in een van de EDLP-regels, omdat de instelling voor mislukte sluiting wereldwijd van toepassing is op alle systemen met de EDLP-module die is geïnstalleerd wanneer er geen cloudconnectiviteit beschikbaar is.

Gerelateerde inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.