Problemen met Azure Virtual Desktop Connectivity oplossen

Inhoud

uitgifte

Azure Virtual Desktop (AVD)-verbindingen mislukken wanneer gebruikers toegang krijgen tot AVD vanuit het kantoornetwerk met Cisco Secure Access ingeschakeld. Dit specifieke gedrag werd waargenomen:

- AVD werkt prima wanneer het wordt benaderd via een persoonlijk netwerk met Secure Access uitgeschakeld.
- AVD werkt prima wanneer het wordt benaderd vanuit het kantoornetwerk zonder beveiligde toegang.
- AVD werkt niet wanneer deze wordt geopend vanaf een netwerk met Secure Access ingeschakeld.

Deze connectiviteitsstoring heeft gevolgen voor de toegang van gebruikers tot hun virtuele desktops en heeft gevolgen voor de bedrijfsactiviteiten van de productie. Analyse van pakketvastlegging toonde bidirectioneel verkeer aan in zowel werkende als niet-werkende scenario's zonder TCP-resets of andere netwerkniveau-indicatoren dat Secure Access de AVD-verbinding beëindigde.

milieu

- Cisco Secure Access met Zero Trust Network Access (ZTNA) ingeschakeld
- ZTNA-profiel geconfigureerd om ZTA te gebruiken voor alle internetbestemmingen
- Implementatie van Azure Virtual Desktop (AVD) via Microsoft-eindpunten
- Office-netwerkomgeving met Secure Access-client geïmplementeerd

- Gebruikers die toegang hebben tot AVD via zowel kantoornetwerken als persoonlijke netwerken

resolutie

Het probleem is opgelost door Microsoft AVD-gerelateerde domeinen toe te voegen aan de ZTA-uitzonderingenlijst, waardoor de Secure Access-client ZTNA voor AVD-verkeer kan omzeilen.

diagnostische analyse

Gezamenlijke analyse van het oplossen van problemen bepaalde dat het ZTNA-profiel was geconfigureerd om ZTA te gebruiken voor alle internetbestemmingen, waardoor Secure Access het continue WebSocket-verkeer van AVD via de Secure Access-cloudproxy kon routeren. Dit gedrag leidde tot sessiedaling omdat Azure Virtual Desktop complex, continu verkeer (WebSockets) gebruikt om desktopsessies in realtime te streamen, en cloudproxy's zijn ontworpen om standaard webpagina's te inspecteren in plaats van streamingprotocollen te verwerken.

Configuratiewijziging

Deze Microsoft AVD-gerelateerde domeinen zijn toegevoegd aan de ZTA-uitzonderingenlijst:

```
*.wvd.microsoft.com
*.core.windows.net
*.servicebus.windows.net
*.events.data.microsoft.com
```

Door deze domeinen toe te voegen aan de lijst met ZTA-uitzonderingen, werd de Secure Access-client geïnstrueerd om AVD-specifiek verkeer volledig te negeren. Hierdoor kan AVD-verkeer rechtstreeks naar Microsoft gaan en de ZTNA-proxy volledig omzeilen, wat precies is wat Microsoft nodig heeft om AVD goed te laten functioneren.

validering

Na toepassing van de ZTA Exceptions-configuratie werd AVD-connectiviteit gerapporteerd als normaal functionerend tijdens de monitoringsperiode. Gebruikers konden vanaf het kantoornetwerk met Secure Access toegang krijgen tot hun virtuele desktops.

Oorzaak

De hoofdoorzaak was de ZTNA-profielconfiguratie die al het internetgebonden verkeer onderschepte, inclusief Azure Virtual Desktop-verbindingen. Toen AVD's WebSocket-verkeer via de Secure Access-cloudproxy werd geleid voor inspectie, veroorzaakte dit verbindingsdalingen omdat de proxy niet was ontworpen om het continue streaming-karakter van AVD-sessies aan te kunnen. AVD vereist directe connectiviteit met Microsoft-eindpunten om stabiele desktopstreamingsessies te behouden.

Gerelateerde inhoud

- Microsoft Azure Virtual Desktop vereiste FQDN-eindpunten
- Problemen oplossen en basisinformatie verzamelen voor Cisco Secure Access
- 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.