Risoluzione dei problemi di connettività di Azure Virtual Desktop

Sommario

Problema

Le connessioni di Azure Virtual Desktop (AVD) hanno esito negativo quando gli utenti accedono ad AVD dalla rete aziendale con Cisco Secure Access abilitato. Questo comportamento specifico è stato osservato:

- AVD funziona correttamente se l'accesso avviene da una rete personale con l'opzione Accesso sicuro disabilitata.
- AVD funziona correttamente se si accede dalla rete aziendale senza accesso protetto.
- AVD non funziona quando si accede da una rete con accesso protetto abilitato.

Questo problema di connettività influisce sulla capacità degli utenti di accedere ai desktop virtuali e sulle attività aziendali di produzione. L'analisi dell'acquisizione dei pacchetti ha mostrato il traffico bidirezionale in scenari lavorativi e non operativi senza reimpostazioni TCP o altri indicatori a livello di rete che indicavano che Secure Access stava terminando la connessione AVD.

Ambiente

- Cisco Secure Access con ZTNA (Zero Trust Network Access) abilitato
- Profilo ZTNA configurato per utilizzare ZTA per tutte le destinazioni Internet
- Distribuzione di Azure Virtual Desktop (AVD) a cui si accede tramite gli endpoint Microsoft
- Ambiente di rete di Office con client Secure Access distribuito
- Utenti che accedono ad AVD sia da reti aziendali che personali

Risoluzione

Il problema è stato risolto aggiungendo domini relativi a Microsoft AVD all'elenco delle eccezioni ZTA, consentendo al client Secure Access di ignorare ZTNA per il traffico AVD.

Analisi diagnostica

L'analisi congiunta della risoluzione dei problemi ha determinato che il profilo ZTNA era configurato per utilizzare ZTA per tutte le destinazioni Internet, il che ha causato la distribuzione da parte di Secure Access del traffico WebSocket continuo di AVD attraverso il proxy del cloud Secure Access. Questo comportamento ha determinato interruzioni di sessione perché Azure Virtual Desktop utilizza traffico continuo e complesso (WebSockets) per trasmettere in streaming le sessioni desktop in tempo reale e i proxy cloud sono progettati per ispezionare le pagine Web standard anziché gestire i protocolli di streaming.

Modifica della configurazione

I seguenti domini correlati a Microsoft AVD sono stati aggiunti all'elenco delle eccezioni ZTA:

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

Aggiungendo questi domini all'elenco delle eccezioni ZTA, al client Secure Access è stato chiesto di ignorare completamente il traffico specifico di AVD. In questo modo il traffico AVD viene indirizzato direttamente a Microsoft, ignorando completamente il proxy ZTNA, che è esattamente ciò che Microsoft richiede per il corretto funzionamento di AVD.

Convalida

Dopo l'applicazione della configurazione delle eccezioni ZTA, la connettività AVD è stata segnalata come funzionante normalmente durante il periodo di monitoraggio. Gli utenti sono stati

in grado di accedere ai desktop virtuali dalla rete aziendale con l'accesso protetto abilitato.

Causa

La causa principale è stata la configurazione del profilo ZTNA che ha intercettato tutto il traffico associato a Internet, incluse le connessioni di desktop virtuale di Azure. Quando il traffico WebSocket di AVD è stato instradato attraverso il proxy cloud Secure Access per l'ispezione, ha causato interruzioni di connessione perché il proxy non è stato progettato per gestire la natura di flusso continuo delle sessioni AVD. AVD richiede una connettività diretta agli endpoint Microsoft per mantenere stabili le sessioni di streaming desktop.

Contenuto correlato

- Endpoint FQDN necessari per il desktop virtuale di Microsoft Azure
- Risoluzione dei problemi e raccolta di informazioni di base per Cisco Secure Access
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).