Risolvi problemi di connettività dell'agente Cowork (Frontier) quando Umbrella è abilitato

Sommario

Problema

Quando Cisco Umbrella è stato abilitato, l'agente Cowork (Frontier) non stava funzionando correttamente sui notebook. Quando Cisco Umbrella era inattivo, l'agente funzionava come previsto. Gli utenti non sono stati in grado di utilizzare la funzionalità dell'agente Cowork quando Umbrella era attivo, e nessun registro blocchi era visibile in Cisco Umbrella quando gli utenti hanno riscontrato questo problema. Sono state fornite schermate di errore che mostrano gli errori dell'applicazione durante l'operazione Umbrella.

Ambiente

- Cisco Umbrella implementata su notebook aziendali
- Applicazione Cowork (Frontier) Agent
- Ispezione del traffico SSL/TLS abilitata in Cisco Umbrella
- Aggiunta certificato implementata nell'applicazione Cowork

Risoluzione

Il problema è stato risolto aggiungendo l'applicazione Cowork all'elenco Do Not Decrypt (DND) in Cisco Umbrella. Questa modifica alla configurazione consente all'agente Cowork di ignorare l'ispezione SSL/TLS e mantenere la connessione crittografata diretta ai server Cowork.

Passaggi per la configurazione dell'elenco DND

Passaggio 1: Accedere al dashboard di Cisco Umbrella e passare alla configurazione del criterio di decrittografia SSL.

Passaggio 2: Aggiungere domini e URL relativi alla rete all'elenco Non decrittografare per ignorare l'ispezione SSL per questa applicazione.

Passaggio 3: Applicare le modifiche ai criteri e attendere che la configurazione venga propagata a tutti gli endpoint.

Passaggio 4: Verificare la funzionalità dell'agente Cisco con Cisco Umbrella abilitato per verificare il corretto funzionamento.

Convalida

Dopo aver implementato la configurazione dell'elenco DND, l'applicazione Cowork funzionava normalmente con Cisco Umbrella abilitato. I test interni hanno confermato che il problema non si è verificato nuovamente nei giorni di monitoraggio e che tutti gli utenti sono stati in grado di accedere alle funzionalità di Cwork come previsto.

Causa

L'agente Cowork (Frontier) utilizza il pinning del certificato come meccanismo di sicurezza. Il blocco del certificato indica che l'applicazione è hardcoded per accettare e considerare attendibile solo il proprio certificato server specifico. Quando Cisco Umbrella intercetta il traffico e presenta il certificato Cisco anziché il certificato server originale, l'applicazione Cisco rileva la modifica, presume che la connessione non sia sicura e intenzionalmente interrompe la connessione per proteggere i dati. Si tratta del comportamento previsto per le applicazioni che implementano le misure di protezione di associazione dei certificati.

Contenuto correlato

- Crea elenco elementi non decrittografati valido per applicazioni Microsoft
- 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).