Resolver Problemas de Conectividade do Agente de Cooperação (Fronteira) quando o Umbrella estiver Habilitado

Contents

Problema

O agente Cowork (Frontier) não estava funcionando corretamente em laptops quando o Cisco Umbrella foi habilitado. Quando o Cisco Umbrella estava inativo, o agente funcionava conforme o esperado. Os usuários não puderam usar a funcionalidade de agente de trabalho conjunto quando o Umbrella estava ativo e nenhum log de bloco estava visível no Cisco Umbrella quando os usuários experimentaram esse problema. Capturas de tela de erro foram fornecidas, mostrando as falhas do aplicativo durante a operação do Umbrella.

Ambiente

- Cisco Umbrella implantado em laptops empresariais
- Aplicativo de agente de trabalho (fronteira)
- Inspeção de tráfego SSL/TLS ativada no Cisco Umbrella
- Fixação de certificado implementada no aplicativo Cowork

Resolução

O problema foi resolvido adicionando-se o aplicativo Cowork à lista Do Not Decrypt (DND) no Cisco Umbrella. Esta alteração de configuração permite que o agente de Trabalho em Grupo ignore a inspeção de SSL/TLS e mantenha sua conexão criptografada direta com os servidores de Trabalho em Grupo.

Etapas para configurar a lista DND

Passo 1: Acesse o painel do Cisco Umbrella e navegue até a configuração da política de decodificação de SSL.

Passo 2: Adicione domínios relacionados a colegas e URLs à lista Não descriptografar para ignorar a inspeção SSL deste aplicativo.

Passo 3: Aplique as alterações de política e aguarde até que a configuração seja propagada para todos os endpoints.

Passo 4: Teste a funcionalidade do agente Cowork com o Cisco Umbrella habilitado para verificar a operação apropriada.

Validação

Depois de implementar a configuração da lista de DNS, o aplicativo Cowork funcionou normalmente com o Cisco Umbrella ativado. Testes internos confirmaram que o problema não ocorreu novamente durante vários dias de monitoramento e todos os usuários puderam acessar a funcionalidade do Cowork conforme esperado.

Causa

O agente de Trabalho (Fronteira) usa a fixação de certificado como um mecanismo de segurança. Fixação de certificado significa que o aplicativo é codificado para aceitar e confiar apenas em seu próprio certificado de servidor específico. Quando o Cisco Umbrella intercepta o tráfego e apresenta o certificado da Cisco em vez do certificado original do servidor, o aplicativo Cowork detecta essa alteração, presume que a conexão não é segura e intencionalmente descarta a conexão para proteger os dados. Esse é o comportamento esperado para aplicativos que implementam medidas de segurança de fixação de certificado.

Conteúdo relacionado

- Criar Lista Não Descriptografar Efetiva para Aplicativos Microsoft
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.