Examine o fluxo de integração do Ative Diretory Umbrella

Contents

Introdução

Este documento descreve o fluxo de comunicação entre os componentes operacionais em uma integração do Cisco Umbrella Ative Diretory (AD).

Informações de Apoio

Entender o fluxo de comunicação do Ative Diretory pode ajudar a solucionar problemas e garantir um ambiente configurado corretamente antes da implantação.

Fluxo de comunicação com implementação abrangente do Ative Diretory

Quando o script do Conector AD é executado em um Controlador de Domínio (DC)

O script do Windows faz uma conexão única do Controlador de Domínio (DC) com a nuvem na porta TCP/443 usando HTTPS para registrar o DC no painel. Esse registro permite que o conector reconheça o DC. Uma chamada é feita para **https://api.opendns.com** com parâmetros específicos. Quando o script registra o DC com êxito, ele é exibido no painel.

Às vezes, os problemas podem estar relacionados a Atualizações do certificado raiz no Windows. Para determinar isso rapidamente, navegue até o Internet Explorer e aponte o navegador para: https://api.opendns.com/v2/OnPrem.Asset. Esta ação imprime uma mensagem como **1005 Chave de API ausente.** Se erros ou avisos de certificado aparecerem nessa página, verifique se a última Atualização de Certificados Raiz da Microsoft está instalada.

Como o Conector AD se Comunica

O conector AD se comunica com o serviço Umbrella Cloud ou um Virtual Appliance da seguinte maneira:

- Conector para nuvem

  O conector carrega todos os dados do Ative Diretory (AD) a cada cinco minutos se ocorrerem alterações, usando uma conexão HTTPS na porta 443 TCP. Somente informações sobre grupos, usuários e computadores são carregadas. Nenhuma senha é carregada e todas as informações do usuário são misturadas localmente, tornando os dados exclusivos.

- Conector para dispositivos virtuais

  O conector envia constantemente eventos do AD para os dispositivos virtuais usando a porta 443 TCP (não criptografada). Esta é uma comunicação unidirecional; os dispositivos não se comunicam de volta aos conectores. Um pré-requisito obrigatório é que o conector e o Virtual Appliance (VA) comuniquem-se através de uma rede confiável.

- Conector para controladores de domínio

  O conector se comunica com todos os controladores de domínio localizados no mesmo local usando as portas 389 TCP e 3268 TCP/UDP para sincronização LDAP. O conector também se comunica com os controladores de domínio usando WMI/RPC. A porta TCP 135 é a porta padrão para RPC e WMI. A WMI também usa uma porta atribuída aleatoriamente entre 1024 TCP e 65535 TCP para Windows 2003 e versões mais antigas, ou entre 49152 TCP e 65535 TCP para Windows 2008 e versões mais recentes. A partir da versão 1.1.24, o conector também se comunica com o controlador de domínio usando LDAPS (LDAP sobre SSL) sobre as portas 636 TCP e 3269 TCP.

Se forem observados problemas de comunicação, verifique se há algum proxy de aplicativo da Camada 7 que possa estar bloqueando ou descartando dados. Um caso comum é o recurso de inspeção em dispositivos Cisco que atuam em protocolos como DNS, HTTP ou HTTPS. Para obter mais informações, consulte nossa documentação sobre Aplicação da Inspeção do Protocolo da Camada de Aplicação.

Dispositivos virtuais (VA) para a nuvem

Os dispositivos virtuais frequentemente se comunicam na porta 443 TCP para **api.opendns.com**, bem como para 53 TCP/UDP para consultas DNS ou sondas, e 22, 25, 53, 80, 443 ou 4766 TCP para estabelecer o túnel de suporte. Os dispositivos virtuais se comunicam com a nuvem usando as portas 53 UDP/TCP, 443 TCP, 123 TCP e 80 TCP. Eles recebem dados dos conectores na porta TCP 443 (não uma conexão HTTPS), mas não exigem comunicação de volta para eles.

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.