Integrar o Ative Diretory usando VA ou CSC

Contents

Introdução

Este documento descreve dois métodos de integração do Ative Diretory (AD) com o Umbrella: Virtual Appliance (VA) ou Cisco Secure Client (CSC).

Pré-requisitos

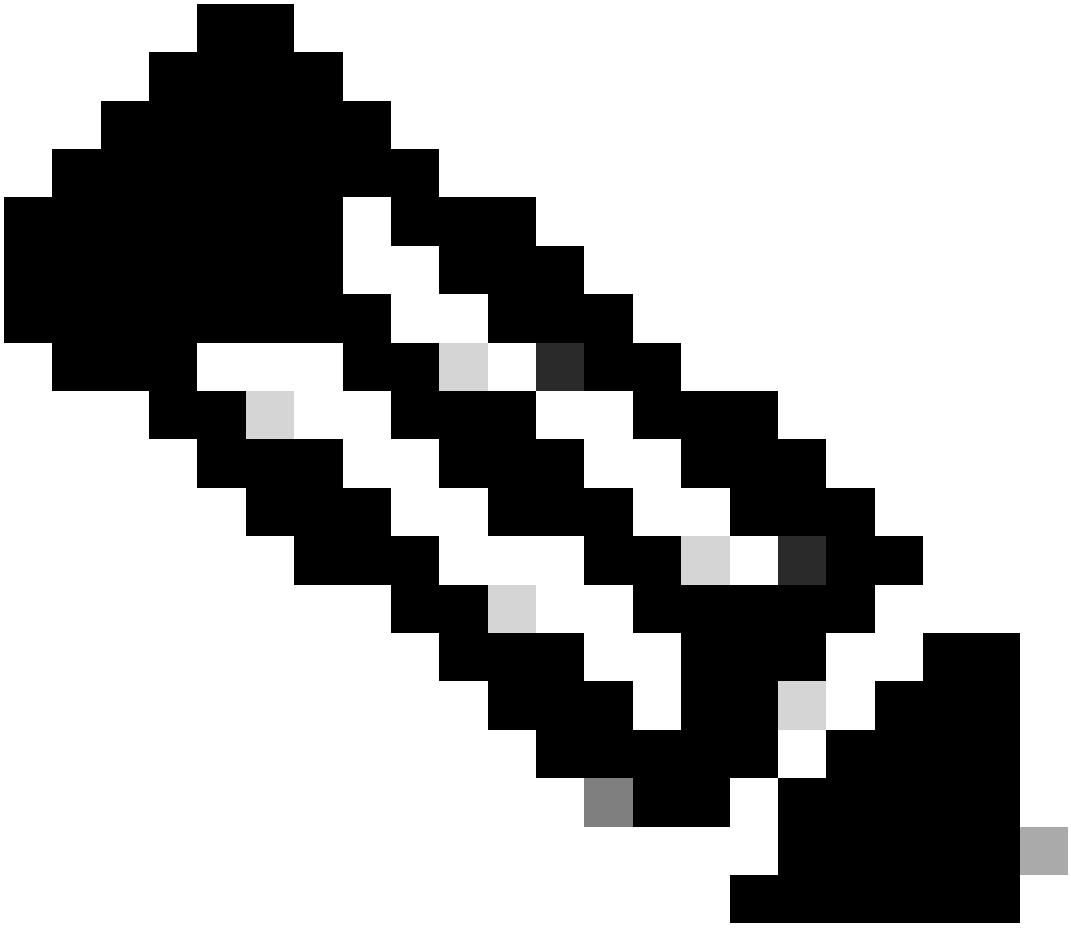
Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conector AD: Sincroniza a árvore do AD de um único domínio do Ative Diretory com o painel. Para a implementação do VA, ele também sincroniza ativamente os eventos de logon dos DCs no mesmo site do Umbrella com os VAs. A árvore do AD para a organização é sincronizada com a nuvem do Umbrella pelo Conector do AD, extraindo esses dados do DC registrado. Atualizações de árvore são detectadas e a nuvem Umbrella é atualizada dentro de várias horas.
- Controlador de Domínio (Servidor AD): Os DCs são registrados no painel de controle por meio do script de configuração de registro .wsf, conforme baixado do painel de controle. Isso adiciona seu nome, domínio e IP interno ao Painel para informar ao Conector com quais IPs tentar sincronizar. Se você não conseguir executar o script, o registro manual também será possível. Entre em contato com o Umbrella Support para obter mais informações e suporte.
- Dispositivo virtual: O encaminhador DNS do Umbrella on premise. Aplica a identidade do AD

(opcional) na rede, bem como IPs internos em relatórios. Isso aciona todos os clientes de roaming atrás dele para desabilitar a proteção de DNS e adiar para o modo "Por trás da proteção de VA".

- Cisco Secure Client: O serviço de software no local Umbrella que fornece criptografia DNS, bem como identificação de usuário para Windows e macOS. Também vem como um módulo AnyConnect.



Note: Os pré-requisitos diferem significativamente entre as duas implementações. Consulte a implementação específica para obter todos os pré-requisitos.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

Overview

Este artigo esclarece e explora os dois métodos diferentes de integração do Ative Diretory com o Umbrella Dashboard. Atualmente, os usuários do AD podem ser aplicados à política e aos relatórios por meio dos dispositivos virtuais Umbrella ou do Cisco Secure Client.

Implementação segura do cliente

Requisitos

- Um conector AD
- Um DC no painel
- O usuário do OpenDNS_Connector deve ter permissão de Controlador de Domínio Somente Leitura.
- Versões mínimas do Secure Client para o cliente autônomo (Módulo AnyConnect):
  - Windows: 2.1.0 (4.5.01044)
  - OSX: 2.0.39 (4.5.02033)

Como funciona

- O usuário do AD conectado no momento é determinado diretamente no computador local pelo cliente móvel que lê o registro local.
- Suporta um máximo de um usuário conectado simultaneamente na estação de trabalho.
- Dois usuários simultâneos podem fazer com que nenhum usuário do AD seja aplicado.
- O GUID de usuário do AD e o IP interno são anexados via EDNS0 no proxy DNS do cliente móvel à consulta DNS enviada aos resolvedores do Umbrella, identificando exclusivamente o usuário do AD.
- Todas as políticas são aplicadas no lado do resolvedor.
- Nenhum conector ativo é necessário. No entanto, o usuário do AD e o aplicativo de política de grupo podem refletir a sincronização de árvore do AD bem-sucedida mais recente.

Onde funciona

- Qualquer rede globalmente.
- Não funciona por trás de um dispositivo virtual Umbrella, pois a camada DNS está desabilitada para adiar para os VAs locais.

Limitações

- Exige um agente de ponto de extremidade ativo e habilitado na estação de trabalho.
- Não oferece suporte a SOs de servidor.
- Não é possível aplicar a política com base no IP da rede interna.
- Não é possível aplicar a política ou os relatórios para Computador do AD (use o nome de

host móvel).

O conector ainda pode tentar receber eventos de login do AD de um DC registrado. Isso pode resultar em um erro de Painel que não é relevante para a integração do AD baseada em cliente de roaming. Para remover erros com permissões relacionadas a receber eventos de logon sem receber nenhum evento, desabilite a auditoria de eventos de logon (se não for usada de outra forma) pelo contrário das instruções de auditoria daqui.

Implementação de dispositivo virtual

Requisitos

- Dois VAs por local da Umbrella
- Um conector AD (redundante, um segundo opcional) por local Umbrella
- Cada DC (que não é um DC somente leitura) deve ser registrado no Painel.
- O usuário do OpenDNS_Connector deve ter o conjunto completo de permissões de pré-requisito.
- Os eventos de logon devem ser habilitados para registrar logs de eventos de segurança 4624 em todos os DCs. Consulte as dicas completas de solução de problemas.

Como funciona

- Os VAs recebem mapeamentos de usuário do AD com base nos logs de eventos de logon de segurança dos DCs do Windows.
- Cada logon de estação de trabalho é registrado no log de eventos de segurança do DC do servidor de logon como um evento de logon exclusivo, com o nome de usuário do AD ou o nome do computador do AD e o IP interno da estação de trabalho.
- O conector analisa esses eventos em tempo real por meio de uma assinatura WMI e sincroniza esses eventos com cada VA no site do Umbrella via TCP 443.
- O VA cria um mapeamento de usuário ao vivo entre o IP interno de um usuário/computador do AD e o nome de usuário do usuário/computador do AD.
- O VA tem visibilidade apenas no IP de origem interno de uma consulta DNS e utiliza o arquivo de mapeamento mencionado anteriormente criado pelos eventos sincronizados com o conector. O VA não tem visibilidade direta de quem está conectado atualmente em uma máquina. Isso anexa o GUID de usuário do AD e o IP interno via EDNS0 à consulta DNS enviada aos resolvedores de Umbrella pelo VA, identificando exclusivamente o usuário do AD.
- O hash do computador do AD é aplicado da mesma forma.
- Todas as políticas são aplicadas no lado do resolvedor.
- Um conector deve ser funcional e ativo na organização para receber um usuário do AD, e os eventos de logon devem ser atuais.
- O usuário deve ser o último usuário do AD a se autenticar nesta máquina, conforme visto nos logs de eventos.

Onde funciona

Na rede corporativa local onde todo o DNS é apontado para um dispositivo virtual Umbrella pertencente ao mesmo site Umbrella que o DC ao qual o usuário se autenticou.

Limitações

- O computador não pode apontar para um VA pertencente a um domínio do AD ou site de guarda-chuva diferente (grandes implantações em vários domínios não podem ver o aplicativo do AD fora de sua rede base).
- Implantações grandes podem exigir subdivisão em locais Umbrella com VAs separados.
- As exceções de usuário do AD podem ser necessárias para usuários do AD de serviço.
- Existe um throughput máximo de eventos de login por segundo para o conector mencionado anteriormente que pode atrasar a aplicação do usuário. Este é um fator de latência de rede e número de VAs.

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.