Aplique políticas para contas locais no Ative Diretory Umbrella

Contents

Introdução

Dispositivo virtual de guarda-chuva e identificação de conta local

- Recomendações para o Umbrella Virtual Appliance

Política de Conta Local e de Cliente de Roaming de Guarda-Chuva

- Recomendações para o cliente de roaming Umbrella

Introdução

Este documento descreve o comportamento de política esperado ao sincronizar produtos no local do Umbrella com o Ative Diretory e contas de usuário locais.

Dispositivo virtual de guarda-chuva e identificação de conta local

O Umbrella Virtual Appliance recebe informações de logon do Ative Diretory dos Controladores de Domínio do Windows. Ele armazena em cache e identifica os usuários do Ative Diretory com base em seus endereços IP de origem.

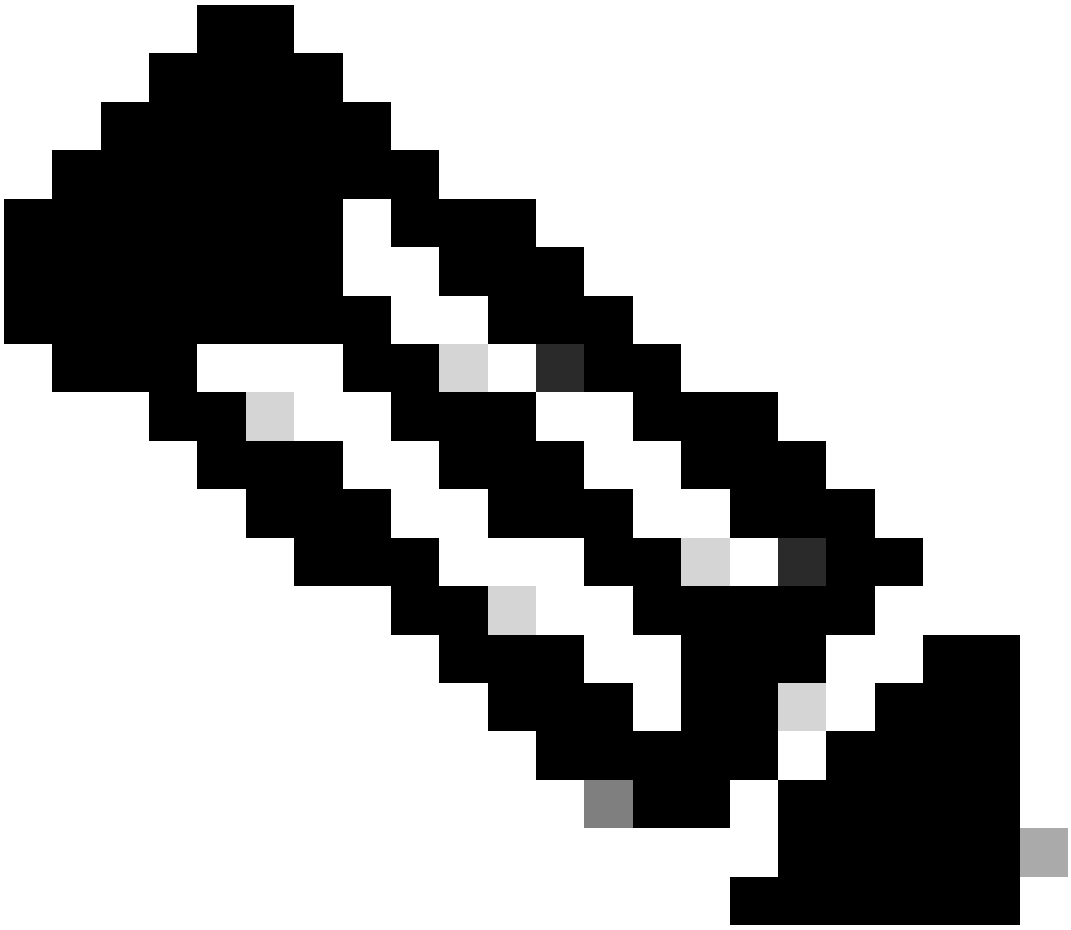
- O controlador de domínio não rastreia logons de usuários locais, portanto esses usuários não podem ser identificados diretamente pelo dispositivo virtual.
- Se um usuário do Ative Diretory fez logon recentemente de um endereço IP, a identidade armazenada em cache ainda poderá ser usada com base em nosso cache. O Virtual Appliance não tem como saber se o usuário do AD foi substituído por uma conta local.
- Se nenhum usuário armazenado em cache estiver presente, o Virtual Appliance usará uma identidade padrão (não AD). A identidade disparada pode ser:
  - Nome do site de guarda-chuva (por exemplo, Site Padrão)
  - Rede interna (endereço IP interno)
  - Rede (endereço IP externo)

Recomendações para o Umbrella Virtual Appliance

- Restrinja o acesso a contas e senhas locais.
- Crie uma política separada para o nome do site do Umbrella (por exemplo, Site Padrão). Atribua a esta diretiva uma prioridade mais baixa do que a diretiva de usuário padrão do Ative Diretory. Essa política mais restritiva se aplica quando nenhum usuário do AD é detectado.
- Se você precisar de políticas diferentes para contas de usuários locais, considere a

implantação do Umbrella Roaming Client.

Política de Conta Local e de Cliente de Roaming de Guarda-Chuva



Note: Para usar a integração do Ative Diretory com o cliente de roaming, navegue para Identidades > Computadores de roaming e habilite a configuração Habilitar a aplicação da diretiva de usuário e de grupo do Ative Diretory.

O cliente de roaming detecta os usuários conectados no Registro do Windows, permitindo a identificação dos usuários do Ative Diretory pelo GUID exclusivo do AD.

- O cliente de roaming não pode identificar nomes de usuário locais para fins de política.
- Quando um usuário do AD é detectado, a identidade do usuário do AD se aplica à

imposição de política, incluindo usuários do AD conectados com credenciais em cache fora da rede.
- Se nenhum usuário do AD for detectado (por exemplo, quando um usuário local estiver conectado), a identidade do Computador Móvel será usada para imposição de política.

Recomendações para o cliente de roaming Umbrella

- Restrinja o acesso a contas e senhas locais.
- Crie uma política separada paraComputadores emRoaming com uma prioridade mais baixa do que a sua política de Usuário do AD padrão. Esta política se aplica a computadores em roaming que não ingressaram no domínio ou são usados por usuários locais.

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.