

Como eu crio os grupos de política de acesso que combinam grupos do diretório ativo?

Índice

[Pergunta](#)

Pergunta

Como eu crio os grupos de política de acesso que combinam grupos do diretório ativo (AD)?

A primeira etapa é configurar um reino da autenticação (reino do gerenciador de LAN de NT (NTLM)) e uma identidade que use o reino da autenticação.

-
1. Crie um reino NTLM na ferramenta de segurança da Web (WSA) sob a **rede > a autenticação**.
 2. Uma vez que você tem seu reino NTLM configurado, escolha o **gerenciador de segurança > as identidades da Web**, a seguir clique-os **adicionam a identidade**.
 3. Siga estas etapas para criar uma identidade: Nome: Authentic.Id Introduza acima: 1 Defina membros pela autenticação: *name* > do reino <NTLM Esquema: **Use básico ou NTLMSSP** ou **use NTLMSSP** Deixe todos ajustes restantes como o padrão.
Se você quer à autenticação de teste contra clientes selecionados, o uso **define membros pela sub-rede** e especifica o IP do cliente de pedido. Isto permite que o WSA peça a autenticação para estes clientes selecionados somente. Clique em Submit.

Neste momento você deve somente ter duas identidades, **Authentic.Id** e **política global da identidade**, com a autenticação permitida na **identidade Authentic.Id**.

A próxima etapa é usar a identidade **Authentic.Id** e criar as políticas de acesso baseadas nesta identidade. Você pode especificar grupos exigidos ou usuários AD nas políticas de acesso.

-
1. Escolha **GUI > gerenciador de segurança > políticas de acesso da Web**.
 2. O clique **adiciona a política**.
 3. Siga estas etapas para criar uma política de acesso: Nome da política: Sales.Policy Introduza acima da política: 1 Política da identidade: Authentic.Id - **Specify autorizou grupos e usuários** Dê entrada com os nomes do grupo manualmente, ou o clique **refresca o diretório** para obter a lista de usuários que existem em seu AD. Uma vez que você selecionou os usuários, o clique **adiciona**. O clique **submete-se** quando feito.

Se você precisa de criar uma outra política de acesso, o clique **adiciona a política** e cria uma outra política de acesso para o grupo novo AD.

Você não deve criar identidades novas para o mesmo reino da autenticação. Reutilize a

identidade existente (Authentic.Id) e crie políticas de acesso novas para grupos diferentes AD, enquanto a identidade não está limitada às **portas de proxy, categorias URL, agentes de usuário, ou defina membros pela sub-rede.**

Para políticas do acesso múltiplo usando grupos diferentes AD, a instalação deve olhar como esta:

Identidade

“Authentic.Id”

“Política global da identidade”

Política de acesso

“Sales.Policy” que usa “Authentic.Id”

“Support.Policy” que usa “Authentic.Id”

“Manager.Policy” que usa “Authentic.Id”

“Admin.Policy” que usa “Authentic.Id”

“Política global” que usa “tudo”