Caro leitor,

Esse material rico servirá de base para implementação da segurança do Active Directory em qualquer ambiente. Independente do tamanho.

Quando falamos de segurança, a grande maioria vai pensar apenas em Firewall, IPS, etc. Mas existe um recurso que é extremamente importante manter seguro.

Eu estou falando de um recurso que todo ambiente possui, que a maioria das aplicações utiliza e tem integrações. Mas que muitos acabam negligenciando a segurança. Estou falando do Active Directory.

Hoje não adianta muito ter o melhor Firewall, os melhores equipamentos de segurança e deixar o AD vulnerável.

Pois hoje a maioria das aplicações se integram ou utilizam o Active Directory para

autenticação. E uma vez que o Active Directory seja comprometido, praticamente todo o ambiente ficará vulnerável.

A verdade é que ou você cuida da segurança do Active Directory ou todo seu ambiente estará vulnerável.

E aqui vai um segredo que talvez você não saiba. Mas a implementação padrão do Active Directory precisa de algumas configurações adicionais para que o ambiente fique mais seguro.

O problema é que são poucos profissionais que conhecem essas configurações ou que não a implementam nos ambientes.

São configurações relativamente simples de implementar, mas que podem aumentar de forma significativa a segurança do ambiente.

Agora imagina só, os pontos que você irá ganhar com seu chefe, ao explicar que o

ambiente do Active Directory possui melhorias de segurança que você pode implementar. E uma dica, ele não precisa saber que é simples.

Além de configurações especificas para serem implementas pós instalação do Active Directory, existem algumas práticas de segurança, que em um primeiro momento podem parecer desnecessárias, mas eu vou te provar que são práticas que podem salvar a segurança do seu ambiente como um todo.

Está preparado para começar a aprender como deixar seu ambiente do Active Directory mais seguro?

Vamos lá!

Ingressar Máquinas no Domínio

Pode parecer algo desnecessário se preocupar com a questão de ingressar máquinas no

domínio. Porém você precisa entender que ao ingressar uma máquina no domínio essa máquina terá um canal seguro com o Active Directory.

Essa máquina irá guardar informações importantes do AD, como por exemplo o Ticket Kerberos.

E dentro do ticket kerberos terá todas as permissões do usuário e computador que fez o logon.

Em outras palavras, uma máquina não autorizada que seja ingressada no domínio, pode coletar informações que podem ser utilizadas contra ataques ao Active Directory.

A verdade é que o administrador do ambiente precisa saber se as máquinas ingressadas no domínio são confiáveis.

Agora você deve estar se perguntando...”mas o que tem haver tudo isso com ingressar

máquinas no domínio, pois somente a equipe de TI tem esse privilégio”.

É exatamente aqui que muitos por falta de conhecimentos cai do cavalo.

Por padrão qualquer usuário pode ingressar até 10 máquinas no domínio. Isso mesmo que você leu.

Eu estou falando que usuários sem privilegio algum, podem ingressar até 10 máquinas que podem ser máquinas não autorizadas no domínio do Active Directory.

E isso é padrão, ou seja, qualquer ambiente que é instalado o Active Directory, qualquer usuário pode ingressar até 10 máquinas no domínio.

Consegue enxergar o risco de segurança aqui?

A recomendação é que assim que você finalizar a instalação do Active Directory, a

primeira coisa que você faça é mudar essa configuração.

Você deve deixar o AD configurado para que apenas usuários autorizados (que tenha permissão) possam ingressar máquinas no domínio.

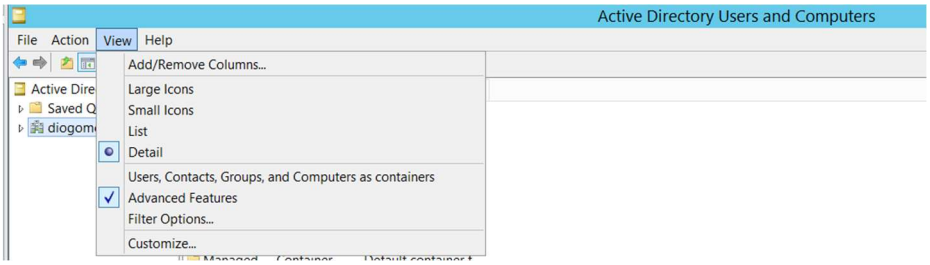
Existe um atributo no Active Directory que é o responsável por essa configuração. Esse atributo é o “ms-DS-MachineAccountQuota”.

O valor padrão desse atributo é “10” o que permite que qualquer usuário possa ingressar até 10 máquinas no domínio.

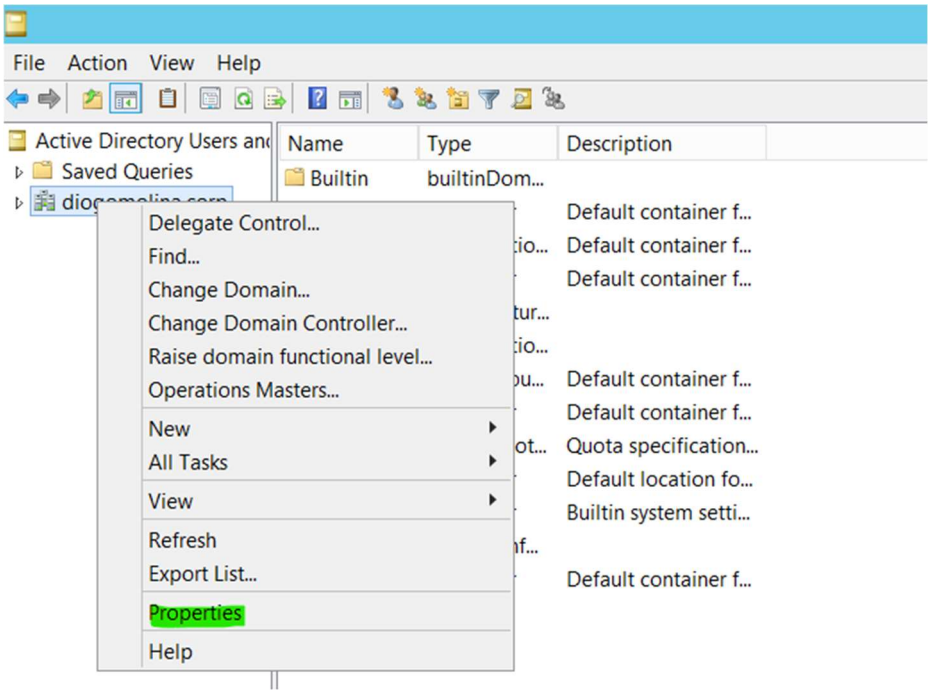
A recomendação é que esse atributo tem o valor de “0”. Com isso usuários sem privilégios não poderão ingressar máquinas no domínio.

Como zerar o atributo

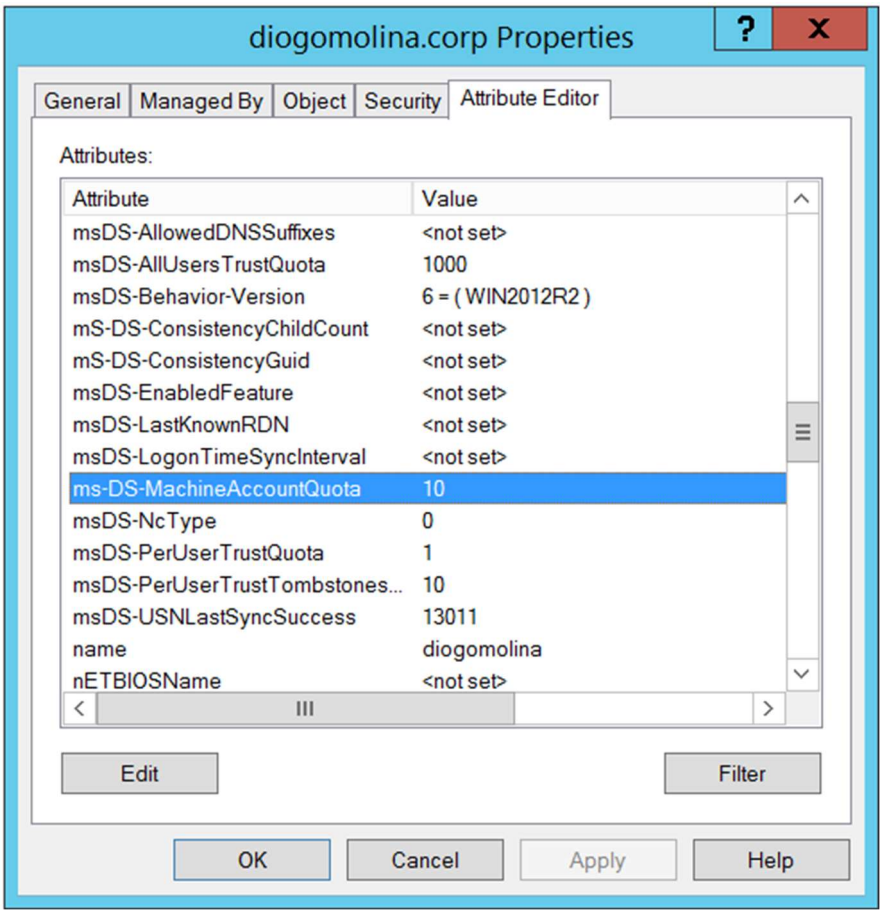
Para configurar o atributo você deve abrir a ferramenta Usuários e Computadores do Active Directory, ir no menu superior “view” e selecionar a opção “Advanced Features”.



Depois vá até o domínio e selecione propriedades.



Vá até a aba “Attribute Editor” e procure pelo atributo “ms-DS-MachineAccountQuota”.



É só clicar em “edit” e selecionar o valor “0”.

Agora eu preciso que você preste muita atenção.

A partir do momento que você zerar esse atributo, por padrão somente membros do grupo “Domain Admins” poderão ingressar máquinas no domínio.

Mas geralmente não são os administradores do ambiente que ingressam as máquinas no domínio. Geralmente é uma atividade do Service Desk, Help Desk.

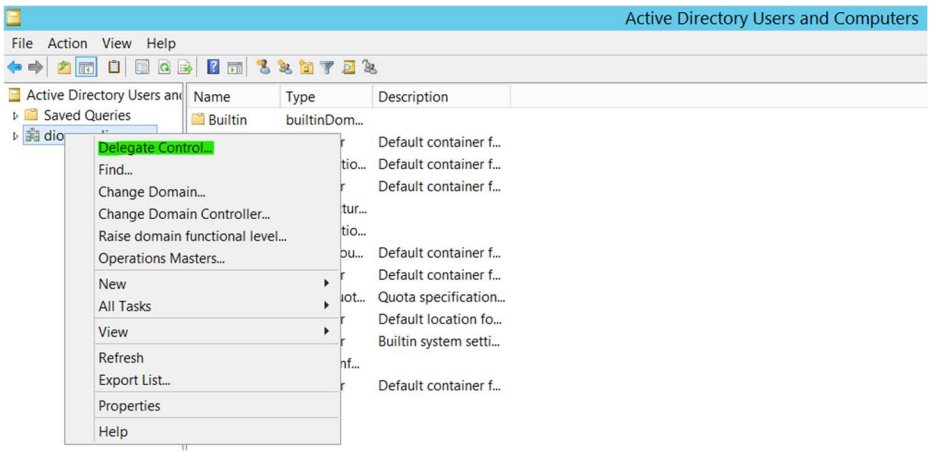
E você não deve de forma alguma colocar esses usuários como membros do grupo “Domain Admins” pois os membros desse grupo poderá gerenciar todo o domínio, inclusive remove-lo.

Talvez agora você esteja perguntando... Certo, e como vou fazer para que os responsáveis por ingressar máquinas no domínio consigam executar essa atividade sem pertencer ao grupo “Domain Admins”?

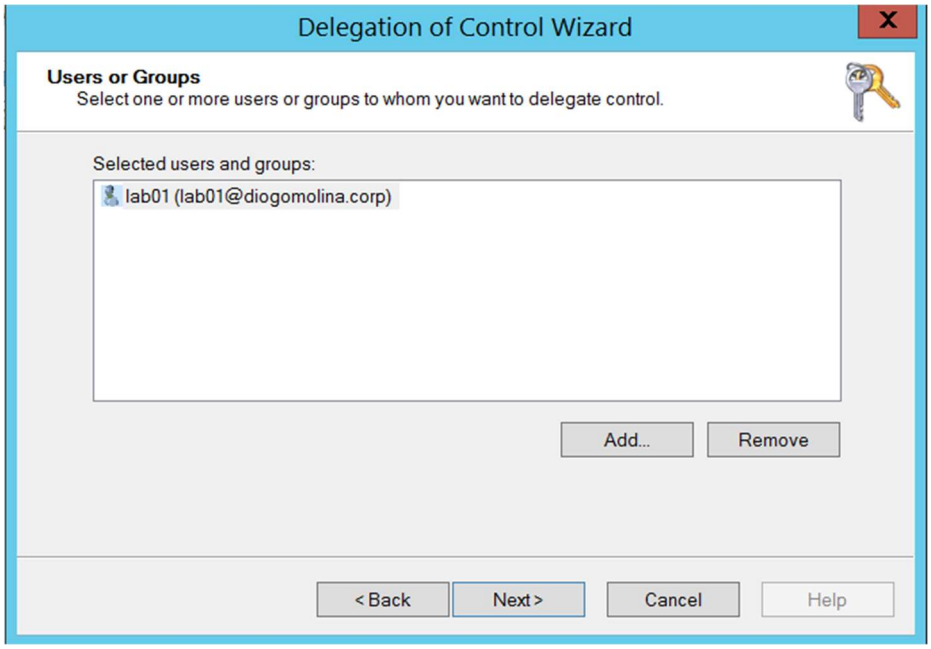
Aqui entra o recurso de Delegação. Nós podemos delegar atividades especificas para grupos ou usuários específicos. Entre essas atividades, está a atividade de ingressar máquinas no domínio.

Delegando Permissão Para Ingressar Máquinas no Domínio

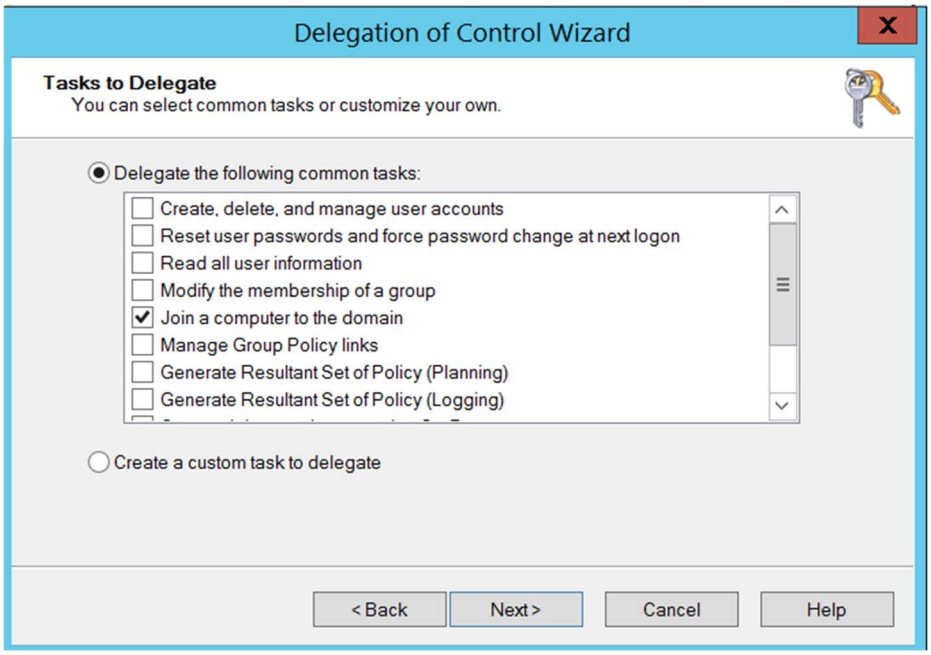
Na ferramenta Usuários e Computadores do Active Directory vá no domínio e selecione “Delegate Control”.



Selecione os grupos ou usuários que você deseja delegar a permissão.



Em tarefas selecione a atividade “Join a computer to the domain”.



Clique em next e depois finish. E pronto o usuário ou grupo que você selecionou terá a permissão de ingressar quantas máquinas precisar no domínio.

E o mais importante, a permissão é somente para ingressar máquinas no domínio, nada além disso.

Agora sim, você tem um ambiente mais seguro, onde somente pessoas autorizadas

tem a permissão de ingressar máquinas no domínio.

Você pode validar como está essa configuração no seu ambiente, e caso esteja com a configuração padrão, você pode explicar para o seu chefe porque essa configuração padrão não é recomendada e planejar a configuração recomentada.

E ganhar alguns pontos com a chefia.

Existem outras configurações e recomendações que irão manter seu ambiente do Active Directory mais seguro.

E iremos falar delas agora.

Super Lotação do Grupo Domain Admins

Existe um erro muito comum em boa parte dos ambientes com Active Directory, que é uma

quantidade grande de usuários que fazem parte do grupo Domain Admins.

Antes de falarmos dessa recomendação é necessário você entender algumas coisas.

Primeiro que os membros desse grupo têm os privilégios mais altos em todos os recursos do Active Directory.

Em outras palavras, eles podem gerenciar, alterar, remover qualquer recurso/componente do Active Directory.

E tem um problema que agrava ainda mais esse cenário. Em muitas empresas essa conta que pertence a esse grupo, é utilizada para logar em estações de trabalho, na utilização do dia a dia.

Isso é um risco para a segurança do Active Directory sem precedentes.

Pois se uma estação de trabalho onde o usuário que pertence ao grupo Domain Admins logou for comprometida, por um vírus por exemplo, as credencias do usuário pode ser comprometida. E estamos falando de uma credencial que tem total privilégio no AD.

Consegue ver o baita problema que isso irá trazer para todo o ambiente.

Por isso que eu reforço, não adianta ter os melhores Firewalls, os melhores equipamentos de segurança, se você não projete o Active Directory.

O grupo Domain Admins deve ter a menor quantidade de usuários possíveis. Esse grupo deve ter como membros somente usuários que precisam do privilégio de administração completa no Active Directory.

O que poucos sabem, é que a maioria das atividades administrativas do Active Directory,

podem ser executadas sem o usuário pertencer ao grupo Domain Admins.

Como vimos na parte de delegar acesso para grupos e usuários ingressarem máquinas no domínio, existem várias outras atividades que podem ser delegadas.

Por exemplo, criar e gerenciar usuários, reset de senhas, criar e gerenciar grupos, etc.

São poucas atividades que realmente será necessário pertencer ao grupo Domain Admins para que possam ser executadas.

Existe uma recomendação da própria Microsoft, que fala para manter esse grupo vazio, e só utiliza-lo quando for executar alguma atividade que dependa dos privilégios desse grupo.

Nesse caso quando for executar a atividade, adiciona o usuário que irá executar no grupo e

depois que a atividade for concluída remove-se o usuário do grupo.

Para falar a verdade, são poucas empresas que seguem essa recomendação. Mas é importante ao menos deixar somente usuários bem específicos dentro desses grupos.

As vezes vemos ambientes onde o grupo Domain Admins possui centenas de usuários. E certamente apenas 1% realmente precisariam desses privilégios para executar suas atividades.

Quer deixar seu ambiente do Active Directory mais seguro... reduza ao máximo os membros desse grupo.

Proteção dos Domain Controllers

Ou você protege os Domain Controller ou senta e veja seu ambiente se autodestruir.

Existe um documento da própria Microsoft que fala que se um Domain Controller for comprometido existe a possibilidade de 99% de chance do seu ambiente inteiro estar comprometido.

Eu sei que isso parece forte demais, mas precisamos analisar os fatos.

Hoje a maioria das aplicações ou são integradas ao Active Directory, ou fazem autenticação no AD.

Estou falando inclusive dos recursos e equipamentos de segurança.

E esses recursos e equipamentos trocam informações de autenticação com o Domain Controller. E um Domain Controller que foi comprometido, poderá ter essas informações extraídas.

Por isso a Microsoft faz essa afirmação tão forte. Poque hoje nos ambientes, tudo gira em torno do Active Directory.

Quando falamos da segurança do AD, um dos pontos mais importes são os Domain Controller. Que são as máquinas que possuem o banco de dados do AD, os serviços de autenticação.

Só que novamente vemos com certa frequência ambientes que não levam a segurança dos Domain Controller a sério.

Primeiro ponto é que quem tem acesso a logar no Domain Controller terá acesso aos serviços, configurações, banco de dados do Active Directory.

E uma pessoa mal-intencionada que consegue acessar o Domain Controller pode comprometer um ambiente inteiro.

Uma parte que poucos se preocupam, mas é extremamente importante, é a proteção física do Domain Controller.

Seja uma máquina virtual ou o Servidor físico. Pois alguém mal-intencionado com os discos ondem ficam as informações do AD, como banco de dados, pode extrair informações importantes do ambiente.

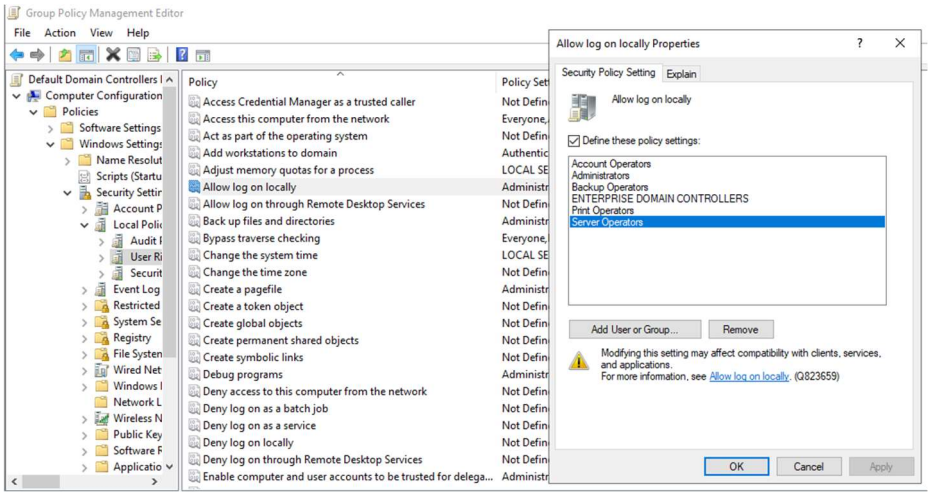
Existem o RODC que é um Domain Controller Somente Leitura que ajuda a endereçar esse problema.

Principalmente em filiais onde não é possível garantir a segurança física dos Servidores. Como o RODC é somente leitura, uma vez comprometido, as informações contidas serão extremamente restritas. Mantendo o restante do ambiente seguro.

Porém para os Domain Controller, não basta apenas garantir a segurança física. É necessário

limitar ao máximo os usuários que possuem privilégios de fazer o logon em DC.

Por padrão o acesso aos DC´s são limitados pela GPO “Default Domain Controller Policy”.



Em alguns ambientes nós recomendamos que essa restrição seja ainda maior. Por exemplo deixar somente membros do grupo “Domain Admin” com a permissão de fazer logon nos DC´s.

Essa restrição é importante pois os usuários com permissão para fazer o logon nos DC´s,

terão acesso ao banco de dados e serviços do Active Directory, e se esse usuário com esses privilégios for comprometido, todo o ambiente ficará em risco.

Protegendo grupos administrativos locais

Um outro ponto importante que envolve a segurança não só do Active Directory, mas do ambiente como um todo é a proteção dos grupos administrativos locais.

Uma coisa que você precisa entender é que quanto mais privilégios uma conta tiver, maiores serão os impactos caso a conta seja comprometida.

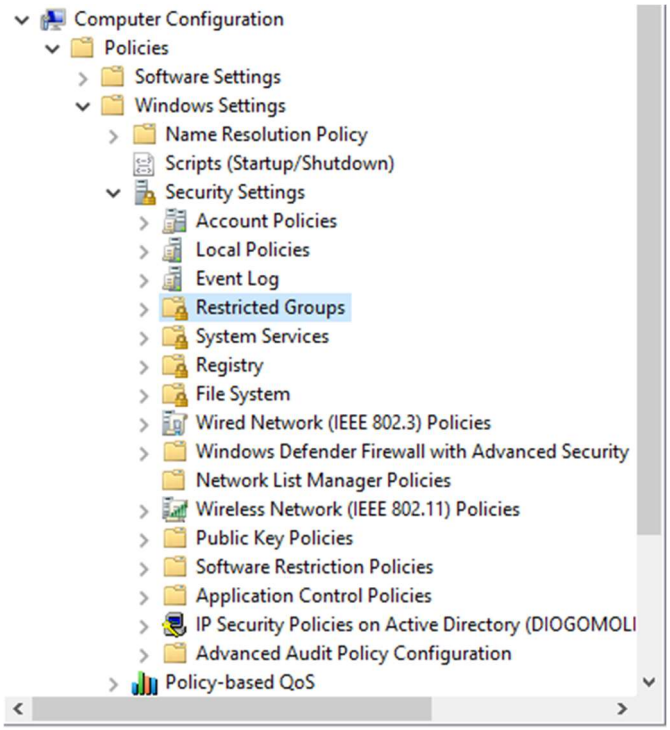
Por isso é recomendado que somente usuários autorizados sejam membros de grupos administrativos, inclusive os locais.

O problema é que é muito comum os grupos de administração locais de Servidores e Estações de trabalho terem uma quantidade grande de usuários. E na maioria das vezes sem necessidade.

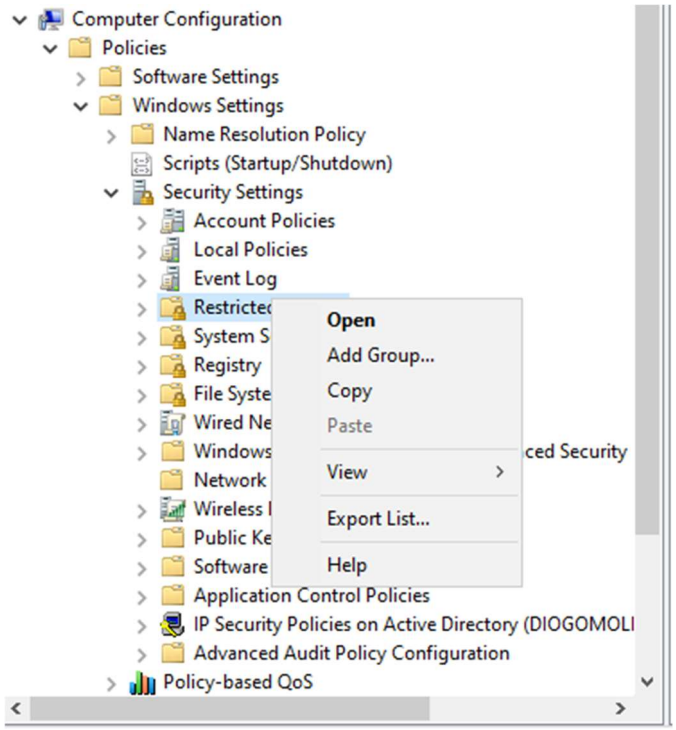
Mas ao mesmo tempo, fazer essa administração pode ser muito complicada, pois estamos falando de grupos locais.

Felizmente existe uma opção de automatizar o gerenciamento desses grupos locais.

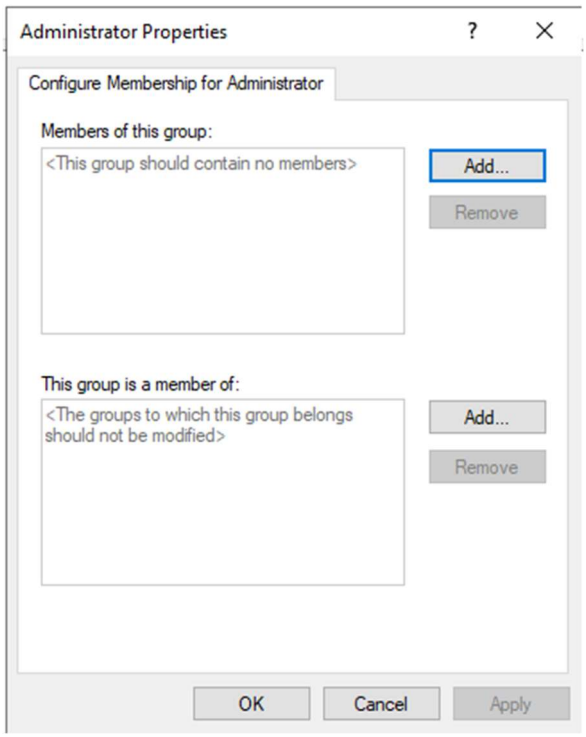
Conseguimos isso através das GPO.



Em “Restricted Groups” clique em “Add Group”



É só informar o nome do grupo local e os membros.



Se for adicionado outro usuário que não esteja configurado na GPO, o usuário será automaticamente removido. Os usuários que serão mantidos como membro do grupo, serão somente os usuários que estão definidos na GPO.

Os recursos que nós vimos nesse material não são complicados de implementar, mas irão

aumentar significativamente a segurança dos ambientes.

O mais importante é lembrar que quanto mais permissões uma conta possuir, mais vulnerável ficará um ambiente caso a conta seja comprometida.

Por isso a importância de liberar apenas poucas contas com privilégios administrativos.

Existem outros recursos mais avançados de segurança do Active Directory, principalmente para ambientes maiores.

Base line de segurança para proteger o Active Directory das principais vulnerabilidades.

Se você quer aprender esses recursos mais avançados, para manter qualquer ambiente, independente do tamanho longe de vulnerabilidades...

Seu próximo passo é a minha Imersão Base Line de Segurança do Active Directory.

Nessa Imersão você vai aprender como deixar seu ambiente do Active Directory realmente seguro.

Você irá aprender tudo na prática e passo a passo.

Depois dessa Imersão você terá todo conhecimento necessário para implementar ambientes seguros com Active Directory.

Ambientes totalmente protegidos contra os principais tipos de ataques contra o serviço do Active Directory.

Não vale a pena correr o risco de subir um ambiente com Active Directory vulnerável. Pois como vimos nesse material, o comprometimento de uma vulnerabilidade do Active Directory, pode deixar todo o ambiente comprometido.

Com os conhecimentos que você irá adquirir nessa Imersão de Segurança do Active Directory, você irá praticamente zerar os riscos de vulnerabilidades no Active Directory.

Para saber os detalhes e garantir sua vaga na Imersão Base Line de Segurança do Active Directory...

Você pode mandar uma mensagem para minha equipe no WhatsApp.

Link para falar com a equipe no WhatsApp