SCHEMA

Schema

- O Schema contém a definição para todos os objetos do Active Directory. Quando você cria um novo objeto, as informações fornecidas são validadas com base nas definições contidas no Schema, antes que o objeto seja salvo na base de dados do Active Directory.

- Por exemplo, se você preencheu um atributo do tipo número, com valores de texto, o Active Directory não irá gravar o objeto no Active Directory e uma mensagem de erro será exibida.

Schema

- O Schema é feito de **objetos**, **classes** e **atributos**. O Schema definido por padrão com o Active Directory, contém um número de classes e atributos, os quais atendem as necessidades da maioria das empresas. Porém o Schema pode ser modificado, o Administrador pode modificar as classes existentes ou adicionar novas classes ou atributos.

- Qualquer alteração no Schema deve ser **cuidadosamente planejada**, pois alterações feitas no Schema afetam toda a árvore de domínios. Todos os domínios de uma árvore tem que utilizar o mesmo Schema, ou seja, não podem ser utilizados diferentes esquemas para os diferentes domínios de uma árvore de domínios.

Como os objetos do Active Directory são definidos no Schema:

- No Schema, uma classe de objetos representa uma categoria de objetos do Active Directory, como por exemplo contas de usuários, contas de computadores, impressoras ou pastas compartilhadas publicadas no Active Directory e assim por diante.

- Na definição de cada classe de objetos do Active Directory, está contida uma lista de atributos que podem ser utilizadas para descrever um objeto da referida classe. Por exemplo, um objeto usuário contém atributos tais como: nome, senha, validade da conta, descrição, etc.

- Quando um novo usuário é criado no Active Directory, o usuário torna-se uma nova instância da classe User do Schema e as informações que você digita sobre o usuário, tornam-se instâncias dos atributos definidos na classe user.

Como o Schema é armazenado no Active Directory:

- Cada floresta pode conter um único Schema, ou seja, o Schema tem que ser único ao longo de todos os domínios de uma floresta. O Schema é armazenado nas partições de schema do Active Directory.

- A partição de schema do Active Directory, bem como a partição de definição do Active Directory, são replicadas para todos os DCs da floresta.

- Porém um único DC controla a estrutura do Schema, DC este conhecido como Schema Master. Ou seja, somente no DC configurado como Schema Master é que o Administrador poderá fazer alterações no Schema.

Cache do Schema:

- Cada DC mantém uma cópia do Schema na memória do servidor (bem como uma cópia em disco), para melhorar a performance das operações relacionadas ao Schema, tais como validação de novos objetos.

- A versão armazenada no Cache do servidor é automaticamente atualizada (em intervalos de tempos definidos) cada vez que o Schema é atualizado (o que não ocorre como freqüência, na verdade é muito raro fazer alterações no Schema).

Quem tem autorização para modificar o Schema:

- A definição do Schema é protegida por permissões de acesso. Por padrão, somente membos do grupo Schema Admins (Administradores de esquemas) tem permissão de leitura no Schema.

- Para que um administrador possa alterar o Schema (operação conhecida como estender o Schema), a sua conta deve fazer parte do grupo Schema Admins (Administradores de esquemas) .

Quem tem autorização para modificar o Schema:

- Por padrão somente a conta Administrator (Administrador) do domínio root (em uma árvore de domínios) faz parte do grupo Schema Admins (Administradores de esquemas).

- Evidentemente que o acesso a este grupo deve ser rigorosamente limitado, pois ao adicionar um usuário a este grupo, você dá ao usuário permissões para alterar o Schema.

- Alterações indevidas (ou má intencionadas) no Schema podem simplesmente paralisar toda a rede, em situações mais graves, fazendo que todos os servidores tenham que ser reinstalados, causando possíveis perdas de dados, enfim: um verdadeiro desastre.

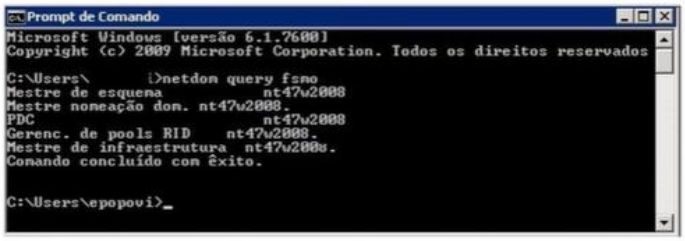
Quem tem autorização para modificar o Schema:

- Para alterar o Schema você deve ter acesso ao servidor que atua como Schema Master. O Schema Master normalmente é o primeiro DC instalado no domínio root, embora esta função possa ser delegada a qualquer outro DC do domínio.

- Em todo o diretório existe um único servidor no qual existe uma cópia do Schema habilitada para alterações. Este servidor é conhecido como Schema Master e normalmente é o primeiro DC instalado no domínio root de uma árvore de domínios.

Identificação do Ambiente AD

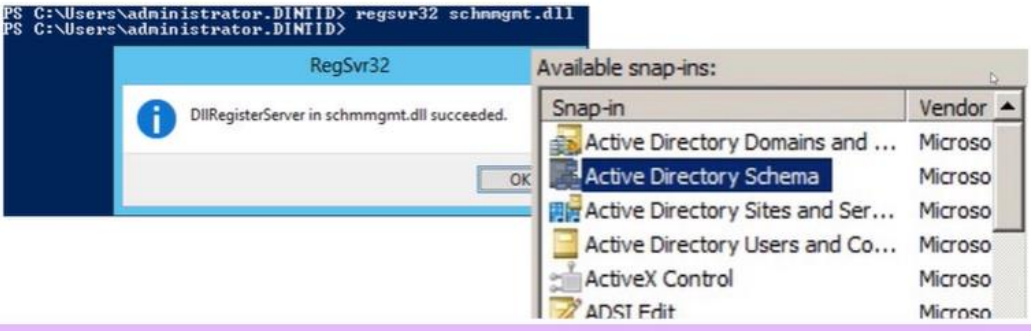
- **Schema Master**
- Para localizar o servidor que possui o Schema master digite o comando ***netdom query fsmo*** pelo prompt.



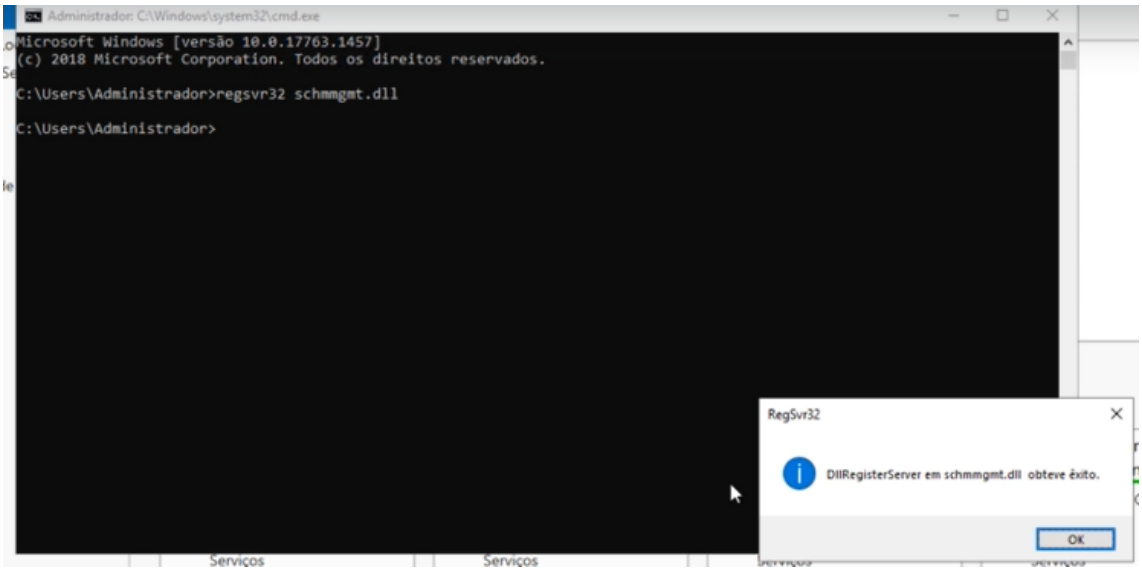
Obs: Este comando não funciona no Windows 2000 e Windows 2003. Para que funcione, instale o Support Tools for Windows, disponível no site da Microsoft e na pasta Tools do CD de instalação do Windows.

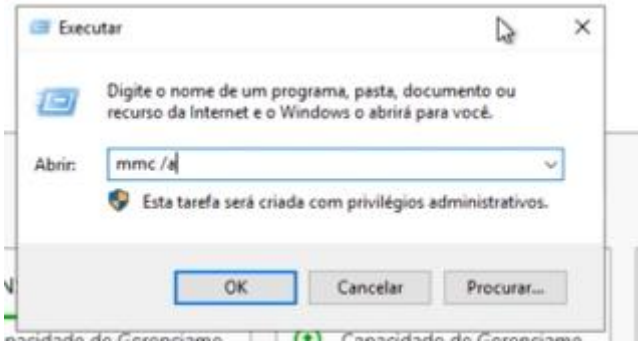
schmmgmt.msc

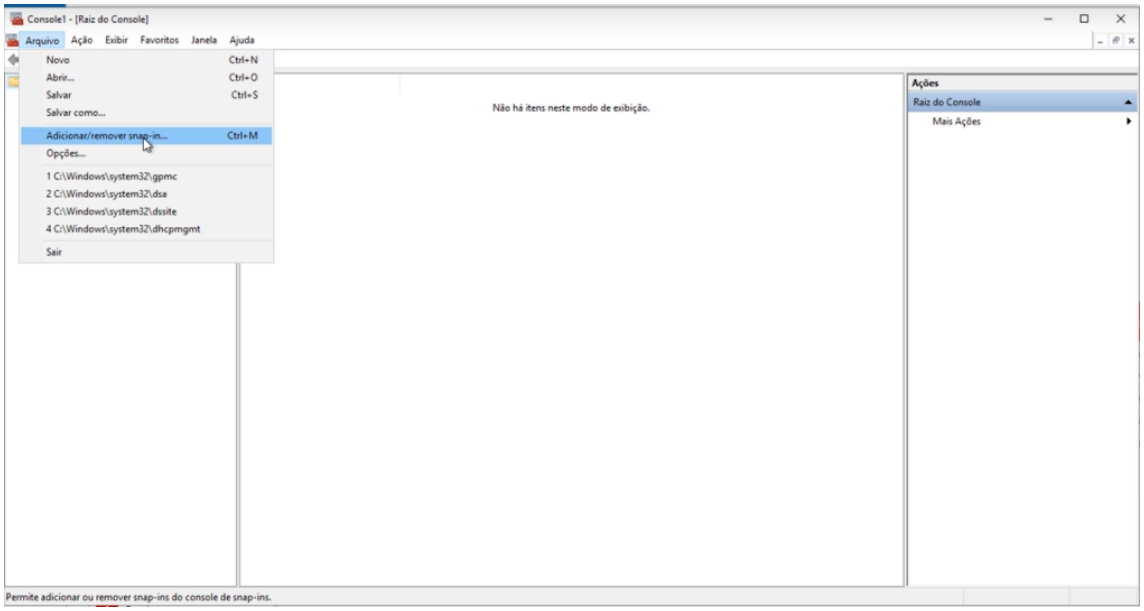
Abra o prommpt de comando e digite **regsvr32 schmmgmt.dll**

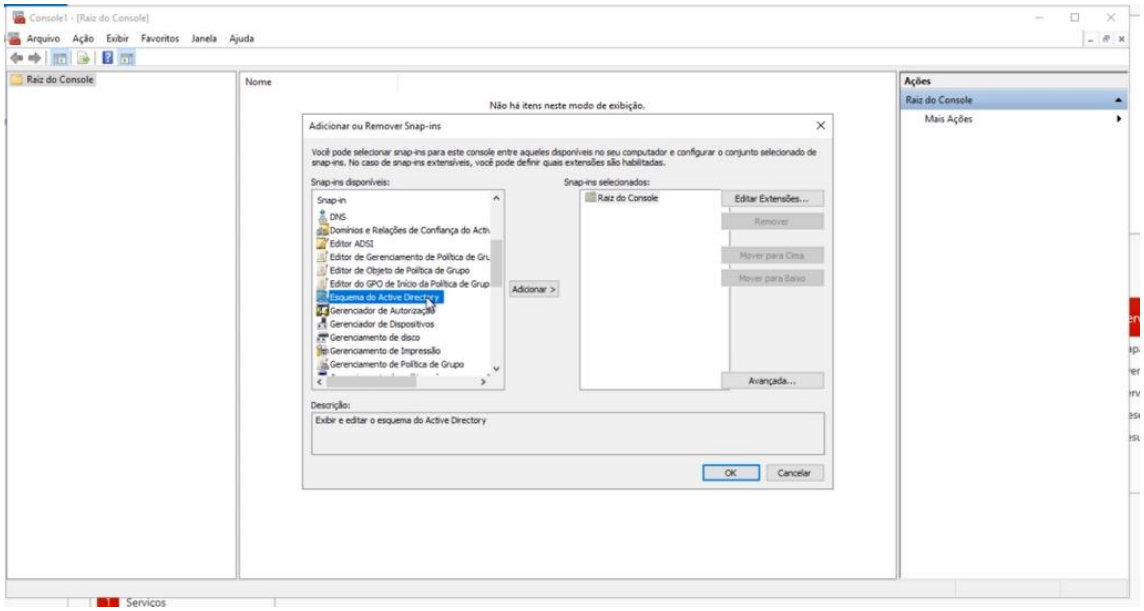


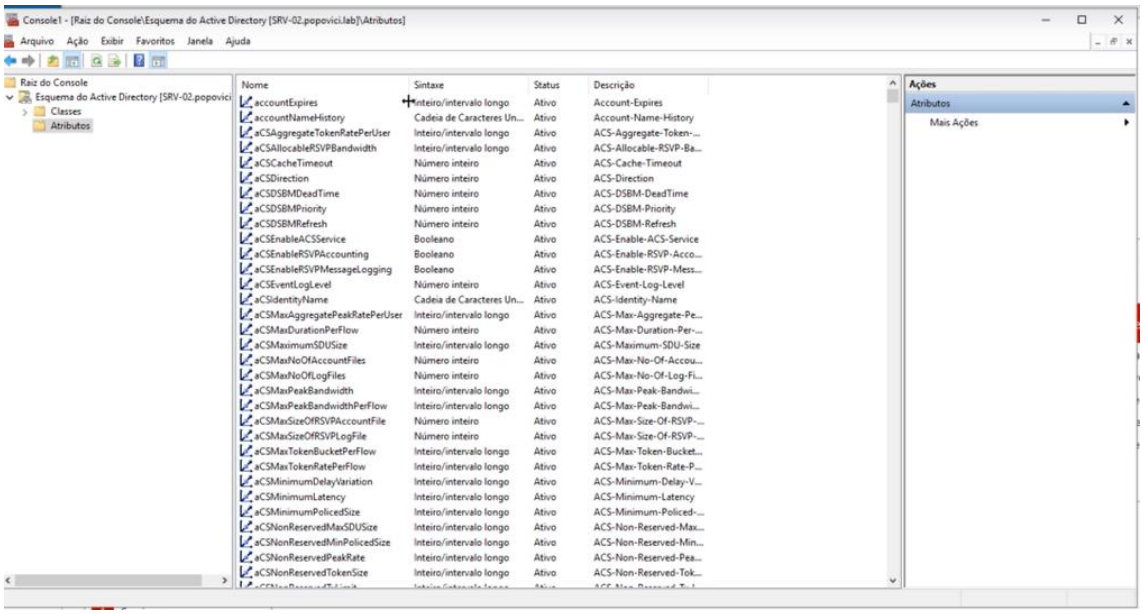
Registrando a schmmgmt.dll




Executar
Digite o nome de um programa, pasta, documento ou recurso da Internet e o Windows o abrirá para você.
Abrir:
mmc /a
Esta tarefa será criada com privilégios administrativos.
OK
Cancelar
Procurar...


Console1 - [Raiz do Console]
Arquivo Ação Exibir Favoritos Janela Ajuda
Novo Ctrl+N
Abrir... Ctrl+O
Salvar Ctrl+S
Salvar como...
Adicionar/remover snap-in... Ctrl+M
Opções...
1 C:\Windows\system32\gpmc
2 C:\Windows\system32\dsa
3 C:\Windows\system32\dssite
4 C:\Windows\system32\dhcpmgmt
Sair
Não há itens neste modo de exibição.
Ações
Raiz do Console
Mais Ações
Permite adicionar ou remover snap-ins do console de snap-ins.


Console1 - [Raiz do Console]
Arquivo Ação Exibir Favoritos Janela Ajuda
Raiz do Console
Nome
Não há itens neste modo de exibição.
Ações
Raiz do Console
Mais Ações
Adicionar ou Remover Snap-ins
Você pode selecionar snap-ins para este console entre aqueles disponíveis no seu computador e configurar o conjunto selecionado de snap-ins. No caso de snap-ins extensíveis, você pode definir quais extensões são habilitadas.
Snap-ins disponíveis:
Snap-in
DNS
Domínios e Relações de Confiança do Acti
Editor ADSI
Editor de Gerenciamento de Política de Gru
Editor de Objeto de Política de Grupo
Editor do GPO de Início da Política de Grup
Esquema do Active Directory
Gerenciador de Autorizações
Gerenciador de Dispositivos
Gerenciamento de disco
Gerenciamento de Impressão
Gerenciamento de Política de Grupo
Adicionar >
Snap-ins selecionados:
Raiz do Console
Editar Extensões...
Remover
Mover para Cima
Mover para Baixo
Avançada...
Descrição:
Exibir e editar o esquema do Active Directory
OK
Cancelar
Serviços


Console1 - [Raiz do Console\Esquema do Active Directory [SRV-02.popovici.lab]\Atributos]
Arquivo Ação Exibir Favoritos Janela Ajuda
Raiz do Console
Esquema do Active Directory [SRV-02.popovici
Classes
Atributos
Nome Sintaxe Status Descrição
accountExpires Inteiro/intervalo longo Ativo Account-Expires
accountNameHistory Cadeia de Caracteres Un... Ativo Account-Name-History
aCSAggregateTokenRatePerUser Inteiro/intervalo longo Ativo ACS-Aggregate-Token-...
aCSAllocableRSVPBandwidth Inteiro/intervalo longo Ativo ACS-Allocable-RSVP-Ba...
aCSCacheTimeout Número inteiro Ativo ACS-Cache-Timeout
aCSDirection Número inteiro Ativo ACS-Direction
aCSDSBMDeadTime Número inteiro Ativo ACS-DSBM-DeadTime
aCSDSBMPriority Número inteiro Ativo ACS-DSBM-Priority
aCSDSBMRefresh Número inteiro Ativo ACS-DSBM-Refresh
aCSEnableACSService Booleano Ativo ACS-Enable-ACS-Service
aCSEnableRSVPAccounting Booleano Ativo ACS-Enable-RSVP-Acco...
aCSEnableRSVPMessageLogging Booleano Ativo ACS-Enable-RSVP-Mess...
aCSEventLogLevel Número inteiro Ativo ACS-Event-Log-Level
aCSIdentityName Cadeia de Caracteres Un... Ativo ACS-Identity-Name
aCSMaxAggregatePeakRatePerUser Inteiro/intervalo longo Ativo ACS-Max-Aggregate-Pe...
aCSMaxDurationPerFlow Número inteiro Ativo ACS-Max-Duration-Per-...
aCSMaximumSDUSize Inteiro/intervalo longo Ativo ACS-Maximum-SDU-Size
aCSMaxNoOfAccountFiles Número inteiro Ativo ACS-Max-No-Of-Accou...
aCSMaxNoOfLogFiles Número inteiro Ativo ACS-Max-No-Of-Log-Fi...
aCSMaxPeakBandwidth Inteiro/intervalo longo Ativo ACS-Max-Peak-Bandwi...
aCSMaxPeakBandwidthPerFlow Inteiro/intervalo longo Ativo ACS-Max-Peak-Bandwi...
aCSMaxSizeOfRSVPAccountFile Número inteiro Ativo ACS-Max-Size-Of-RSVP-...
aCSMaxSizeOfRSVPLogFile Número inteiro Ativo ACS-Max-Size-Of-RSVP-...
aCSMaxTokenBucketPerFlow Inteiro/intervalo longo Ativo ACS-Max-Token-Bucket...
aCSMaxTokenRatePerFlow Inteiro/intervalo longo Ativo ACS-Max-Token-Rate-P...
aCSMinimumDelayVariation Inteiro/intervalo longo Ativo ACS-Minimum-Delay-V...
aCSMinimumLatency Inteiro/intervalo longo Ativo ACS-Minimum-Latency
aCSMinimumPolicedSize Inteiro/intervalo longo Ativo ACS-Minimum-Policed-...
aCSNonReservedMaxSDUSize Inteiro/intervalo longo Ativo ACS-Non-Reserved-Max...
aCSNonReservedMinPolicedSize Inteiro/intervalo longo Ativo ACS-Non-Reserved-Min...
aCSNonReservedPeakRate Inteiro/intervalo longo Ativo ACS-Non-Reserved-Pea...
aCSNonReservedTokenSize Inteiro/intervalo longo Ativo ACS-Non-Reserved-Tok...
Ações
Atributos
Mais Ações