**Objetos do AD**

Toda a estrutura de uma rede baseada em Domínio terá como base **2 tipos de estrutura topológica**:  
  
**- A topologia da rede em si, ou seja, a configuração de protocolos. É a rede adotada pela empresa, sempre levando em conta a replicação dos dados pelo Active Directory;**  
  
**- A topologia Lógica que corresponde aos objetos existentes em todo Active Directory, organizando-os e definindo políticas específicas, delimitados de maneira lógica.**

|  |
| --- |
|  |
| Imagem, Technet |

**Objetos:**

**- Domain Controller:** servidor com AD instalado, encarregado da autenticação dos usuários, replicação dos dados entre outros DCs. Este servidor é responsável pela comunicação com outros domínios da rede.**IMPORTANTE**! Para haver um serviço de diretório, é necessário pelo menos um Domain Controller na rede.

**- Contas de Usuários:**  qualquer pesssoa que irá acessar o ambiente necessita de um usuário para verificação e autenticação de suas credenciais. De acordo com o que vimeos em aula, temos que ter  certeza de que os usuários que terão acesso aos recursos em sua rede nos horários, locais e meios acertados com a empresa. Tanto no AD do Windows 2000, Server 2003, 2008 e 2012, existe a possibilidade de garantir que as senhas serão complexas. No 2000, isso não vinha configurado por padrão, a partir do 2003 o usuário já vem como uma série restrições, chamadas de restrições básicas. O cadastro de um usuário não significa apenas completar os campos nome e sobrenome e ele é único na rede.

**Para reforçar:** uma conta de usuário é um objeto do Active Directory que permite o acesso através do logon a recursos configurados e permitidos pelo Administrador do sistema. As informações sobre as contas de usuários ficam armazenadas no Active Directory e nos servidores Controladores de Domínio que pertencem  a  rede.  Quando  um  usuário  se  loga  na  rede  baseada  em  Domínio,  suas  informações  são verificadas. Se o usuário e senha existirem e, a conta de usuário não estiver bloqueada, o logon será permitido e o perfil do objeto será carregado na área de trabalho da máquina cliente.

**- Grupos de Usuários:** um Grupo de Usuários é um objeto do Active Directory, é uma coleção de usuários.

Os grupos simplificam a administração porque o Administrador pode atribuir direitos em nível de grupo. Para

simplificar a administração de contas de usuários que têm necessidades semelhantes, basta dividi-los em

Grupos. Um Grupo é um nome, semelhante ao nome de usuário de uma conta, que pode ser usado para se

referir a um ou mais usuários. O uso de grupos é conveniente para permitir e controlar o acesso de usuários que realizam tarefas semelhantes. Sem os grupos seria necessário alterar as restrições de cada conta de usuário. Ao agrupar os usuários, você permite a todos eles os mesmos recursos ou restrições de uma vez só.

**\*Características de Operação com Grupos:**

**- Grupos são uma coleção de contas de usuários;**

**- Os membros de um grupo, herdam as permissões atribuídas ao grupo;**

**- Os usuários podem ser membros de vários grupos;**

**- Grupos podem ser membros de outros grupos;**

**- Contas de computadores podem ser membros de um grupo (novidade a partir do Windows Server 2003);**

**\*Tipos de Grupos:**

**- - Grupos de Segurança:** Normalmente utilizados para atribuir permissões de acesso aos recursos da rede. Por exemplo, ao criar um grupo Adm (que conterá todas as contas dos funcionários do departamento administrativo) o qual será utilizado para atribuir permissões de acesso a uma pasta compartilhada, deve-se criar este grupo como sendo do tipo Grupo de segurança. Um grupo de segurança também pode ser utilizado como um grupo de distribuição, embora essa não seja uma situação muito comum. Esses grupos, assim como as contas de usuários são armazenados no Banco de dados do Active Directory.

**- - Grupos  de  Distribuição:** São  utilizados  para  funções  não  relacionadas  com  segurança  (não relacionadas a atribuição de permissões). Normalmente são utilizados em conjunto com servidores de e-mail, tais como o Exchange Server 2003, para o envio de e-mail para um grupo de usuários. **Uma das utilizações típicas para um Grupo de distribuição é o envio de mensagens de e-mail para um grupo de usuários de uma só vez.  Não é possível utilizar grupos de distribuição para funções relacionadas com segurança.**

**\*Escopo de Grupos:**

O Escopo permite que o grupo seja utilizado de diferentes maneiras para a atribuição de permissões e visualização no Domínio e Sub Domínio. O escopo de um grupo, determina em que partes do Domínio ou de uma floresta de Domínios, o grupo é visível, ou seja, pode ser utilizado para receber permissões de acesso aos recursos da rede e quais tipos de objetos (grupos e usuários), podem ser inseridos como membros do grupo. Existem três escopos para grupos de usuários: Universal, Global e Local do domínio.

**- - Grupos  Universais:** podem ser  utilizados  em  qualquer  parte  de  um  Domínio  ou  da  árvore  de Domínios e podem conter como membros, grupos e usuários de quaisquer Domínios.  Pode ser membro de:

**- - Grupos locais** de qualquer Domínio ou grupos universais de qualquer Domínio. Pode receber permissões para

recursos localizados em qualquer Domínio;

**- - Grupos Globais:** Um grupo Global é “global” quanto aos locais onde ele pode receber permissões de acesso, ou seja, um grupo Global pode receber permissões de acesso em recursos (pastas compartilhadas, impressoras, etc) de qualquer domínio;

**- - Grupos de Domínio Local:** São grupos que somente podem receber permissões para os recursos do Domínio onde foram criados, porém podem ter como membros, grupos e usuários de outros Domínios;

|  |
| --- |
|  |
| Imagem, site Technet |

**Relembrando ....**

**Na instalação do Active Directory:**  
  
O Active Directory nada mais é do que uma base de dados que foi implementada pela Microsoft com a função de centralizar o gerenciamento e a segurança da rede.  
  
**Componentes da Instalação:**  
  
**1º - FQDN:** é o DNS de Domínio, é o nome qualificado do Domínio. Chamamos também de SPACENAME - espaço de nome, onde tudo será referenciado fazendo parte do limite administrativo.  
**2º - NetBIOS do Domínio:** responsável por oferecer suporte as versões antigas ou anteriores de sistemas operacionais.  
**3º - SAM - Security Accounts Manager:** é o BD do AD responsável pela autenticação de usuários da rede.  
**4º - Sysvol:** é um volume replicado, responsável pela replicação de arquivos públicos de Domínio.  
  
**Componentes de Gerenciamento dos objetos da rede - Usuários e Computadores do AD!**

|  |
| --- |
|  |
| Console Usuários e Computadores do AD |

|  |
| --- |
|  |
| Contas Builtin |

**- Builtin:** são  contas  criadas  automaticamente  após  a instalação  do  AD e possuem um conjunto de usuários e grupos com permissões e/ou restrições extremamente importantes para o gerenciamento da rede baseada em domínio.  
  
**\* Conta Administrador:** Esta conta pertence a diversos grupos do Domínio. O resultado prático é que a conta Administrador tem poderes totais em todos os computadores do Domínio, ou seja, é a conta com o mais alto nível de permissões no Domínio. Esta conta pertence, automaticamente, aos seguintes grupos: Administradores, Domain Admins (Admins. do Domínio), Domain Users (Usuários do Domínio), Enterprise Admins  (Administradores de empresa), Group Police Creator Owners  (Proprietários criadores de diretivas de grupo) e Schema Admins  (Administradores de esquemas). Como a conta Administrator é a conta com o maior níveis de permissões do domínio, algumas  recomendações adicionais de  segurança  são necessárias:  
**- Defina uma senha complexa para esta conta. Senha complexa significa uma senha com no mínimo 10 ou mais caracteres e que possua  requisitos de complexidade;**  
**- É recomendado que você renomeie a conta Administrador. Com  isso, se alguém quiser fazer o  logon como administrador, além da senha desta conta  terá  também que  tentar descobrir o novo nome. Ao  renomear a**  
**conta Administrador, você dificulta a vida de um hacker, ao fazer com que ele tenha que descobrir o nome e também a  senha.**  
**- É recomendado que o Administrador do Domínio  tenha  também uma conta de usuário comum, com permissões limitadas. Somente quando for necessário realizar tarefas administrativas é que este usuário deve fazer o logon como Administrador. Isso reduz a possibilidades de erros de operação, os quais podem ser desastrosos  se cometidos quando o usuário está  logado como Administrador do Domínio.**  
  
**\* Conta Convidado:** Esta conta é criada automaticamente e por padrão está bloqueada, ou seja, não está habilitada para ser usada para logon no Domínio. Esta conta normalmente é utilizada por pessoas de fora da empresa, que estão na empresa prestando um serviço específico ou participando de uma reunião e precisam, por algum motivo,  fazer o  logon na  rede. A conta Convidado pode  ter  senha em branco e por padrão  tem acesso bastante  limitado aos  recursos da  rede.  
  
**\* Conta de Usuário de sistema - Power user:** É aquele usuário interativo que recebe permissões especiais de operação na rede baseada em Domínio. Por exemplo, se o administrador de domínio necessita de usuários assessores para operar na rede, podemos criar usuários normais e atribuir permissões específicas. Estes usuários podem pertencer a um dos grupos das contas Builtin.  
  
**\* Conta de Usuário interativo - usuário restrito:** É o usuário normal criado e configurado no Active Directory. Tipo de user que já vem com algumas restrições básicas, tais como:  
- sem acesso a configurações de rede;  
- não cria e não acessa compartilhamento;  
- painel de controle restrito;  
- regedit e demais edições de registros estão bloqueados;  
- cmd bloqueado;  
  
  
**- Computers:** exibe a lista de  estações de trabalho que pertencem a rede.

|  |
| --- |
|  |
| Domain Controllers |

**- Domain  Controllers** (Controladores  de  Domínio):  é  exibido  a  lista  de  computadores Controladores de Domínios.  
 **- ForeignSecurityPrincipals e Managed Service Accounts:** são exibidos a lista de relações de confiança relacionadas a políticas de segurança criadas manualmente pelo Administrador de Domínio.

|  |
| --- |
|  |
| Users |

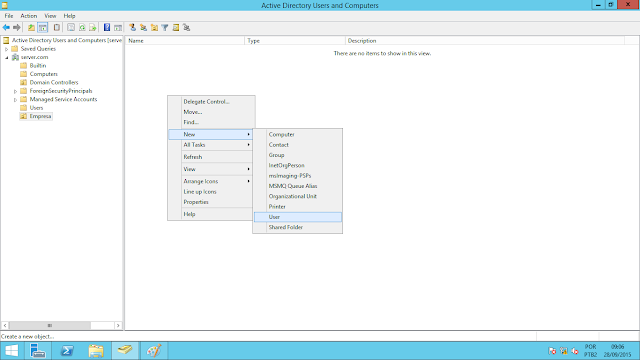
**- Users (usuários):** é exibida a lista de contas criadas automaticamente após a instalação do Active Directory  
  
  
**Trabalhando com os Objetos do AD e sua hierarquia!**  
  
Primeiro, a hierarquia dos objetos que iremos trabalhar é:  
  
**DC**  
**UO**  
**Grupos**  
**Computadores**  
**Usuários**  
 **Como criar uma Unidade Organizacional?**  
1) Acesse Usuários e Computadores do Active Directory;  
2) Selecione o nome do Domínio;  
  
3) Clique com o botão direito do mouse, Novo/Unidade Organizacional;

|  |
| --- |
|  |
| Passo um |

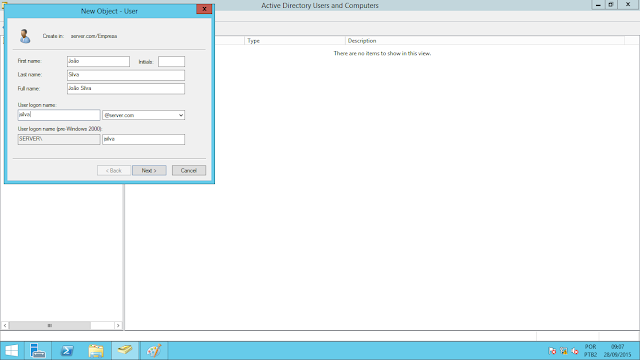
|  |
| --- |
|  |
| Passo dois |

|  |
| --- |
|  |
| Passo Três |

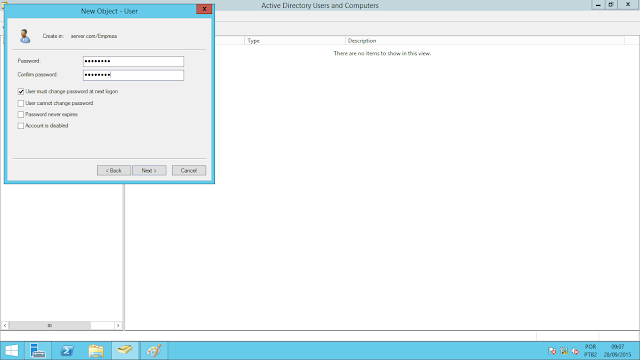
**Como criar um usuário?**  
  
Neste exemplo, vamos criar dentro da UO que acabamos de fazer!

[](https://3.bp.blogspot.com/-WazSEklsxxU/VgmykymQ-4I/AAAAAAAADYQ/dgRZJvCHCA0/s1600/8.png)

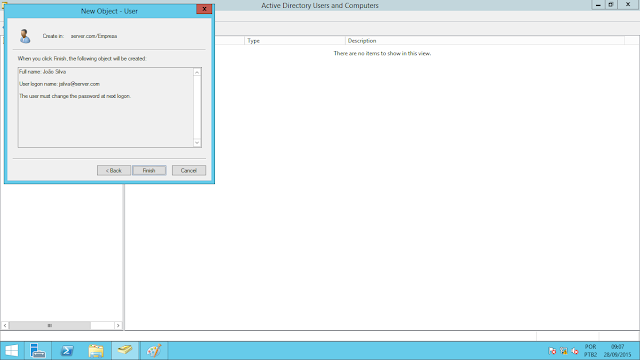
Aqui, criamos o usuário por meio do meno de contexto, dentro da UO criada!

[](https://1.bp.blogspot.com/-oPADMrHd2vw/VgmylGpbeII/AAAAAAAADYY/xIgpzbit3MM/s1600/9.png)

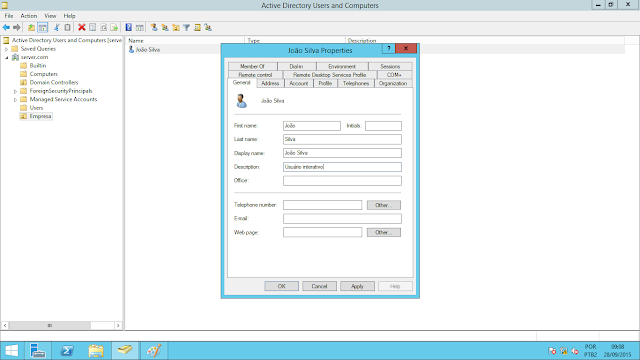
Nesta parte digitamos todas as informações do objeto user. O nome de logon é único, não podemos ter nomes de logo iguais!! Aqui observamos que há o nome do user com todo o sufixo de DNS, que é reconhecido  a partir do Windows Server 2000 e o nome do NetBIOS, para sistemas operacionais mais antigos e envolve também o PDC - que falamos em aula.

[](https://2.bp.blogspot.com/-6gLUSi361ko/VgmyjTZliCI/AAAAAAAADXg/-u3Yb_C2UgE/s1600/10.png)

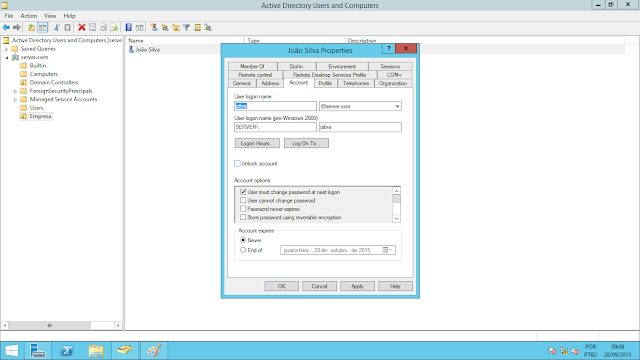
Cadastramos a senha e definimos as propriedades dela, ou seja, se o user precisa alterar a senha no próximo logo, se o user não pode alterar a senha, se a senha nunca expira e se a conta está desativada!

[](https://3.bp.blogspot.com/-bNiQMm5n_O0/VgmyjRg_QeI/AAAAAAAADXk/EGuiZANLPzs/s1600/11.png)

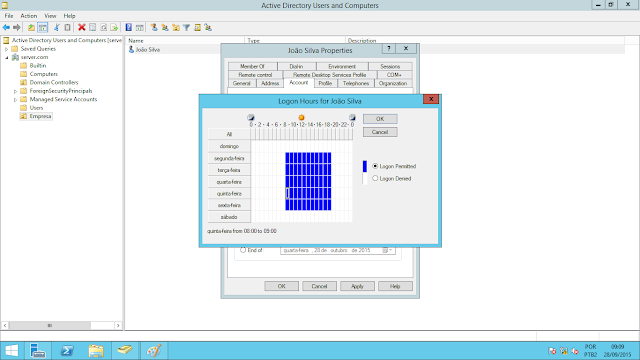
Um pequeno relatório do nosso objeto criado!

[](https://4.bp.blogspot.com/-1pNA1vpwIwc/VgmyjVt03LI/AAAAAAAADXo/MiZddtw971I/s1600/12.png)

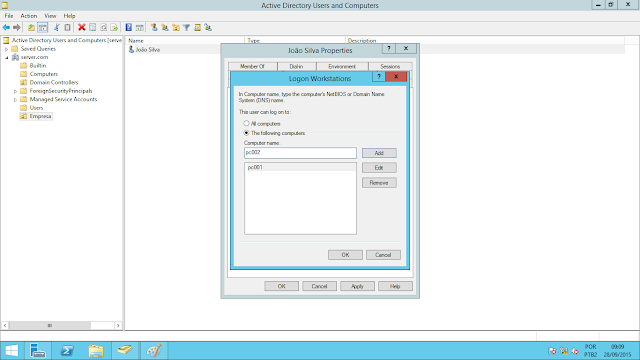
Propriedades do user. No geral, podemos cadastrar todas as informações pertinentes do user, é importante colocarmos a descrição, pois ela ajudará na documentação e organização da nossa rede. Há também a guia de endereços! Vale lembrar que os dados cadastrados aqui variam de acordo com a política de segurança da empresa para qual estamos configurando uma rede baseada em domínio!

[](https://2.bp.blogspot.com/-2ygy0WVH3hk/Vgmyj0KJ2aI/AAAAAAAADXw/wa5zt_nRwxw/s1600/13.png)

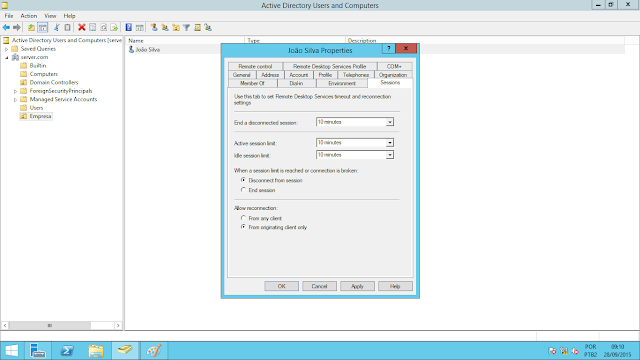
Nesta aba, podemos configurar a alteração dos nomes de logon ...

[](https://3.bp.blogspot.com/--SdsMy1jXyM/VgmykHY8PWI/AAAAAAAADYA/TmrirSF5KPE/s1600/14.png)

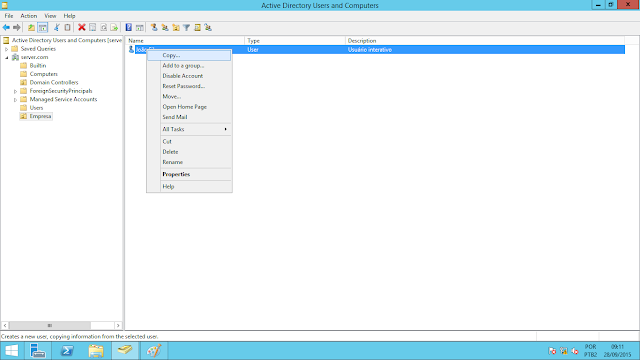
o horário de logon ....

[](https://3.bp.blogspot.com/-NBknBo6QeKI/VgmykFFGflI/AAAAAAAADX8/JXTJwrrP0BQ/s1600/15.png)

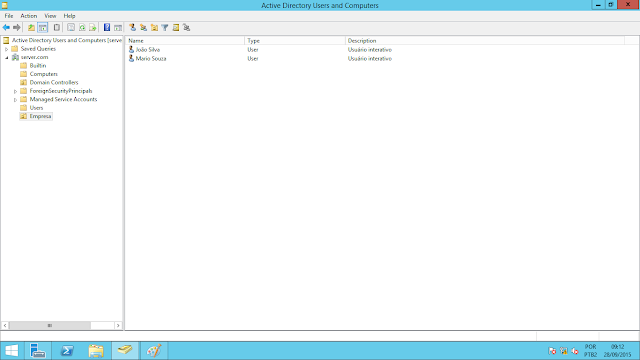
os computadores da rede em que o user poderá se logar!

[](https://4.bp.blogspot.com/-zOcWrxK5jIg/VgmykSBb5FI/AAAAAAAADYE/LDFDMiy0eyc/s1600/16.png)

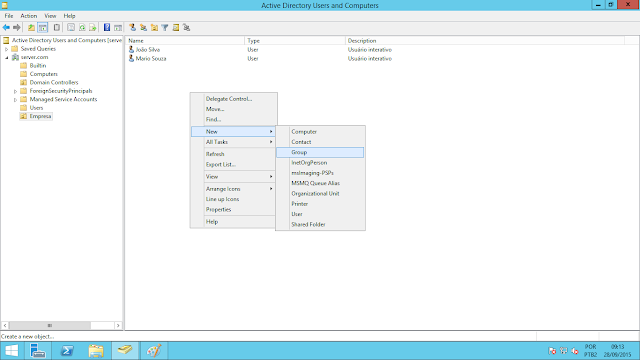
Na aba seção, há uma configuração muito importante! Esta configuração nos permite definir como ficará a seção logada do usuário se ele deixar seu sistema ocioso, bem como, se vamos liberar para que o usuário possa se logar simultaneamente em mais de uma estação de trabalho!

[](https://1.bp.blogspot.com/-EjsK3SeJwhk/Vgmyko_w1BI/AAAAAAAADYM/b5d8g9G6YYA/s1600/17.png)

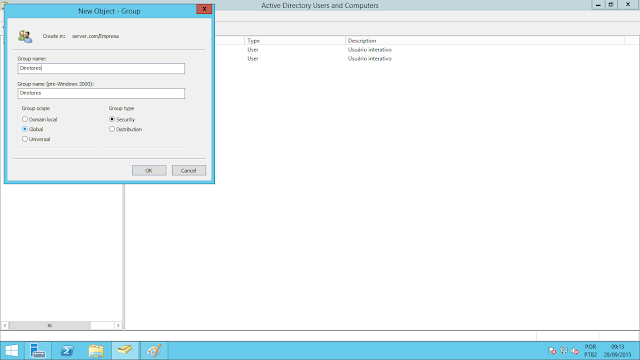
Aqui, o comando que copia usuários. É muito útil quando queremos criar vários users utilizando as mesmas restrições de horário e local de fazer logon

[](https://1.bp.blogspot.com/-wJ41wGFKQAU/VgqhkrPf-0I/AAAAAAAADZM/bb6GehLuq7M/s1600/19.png)

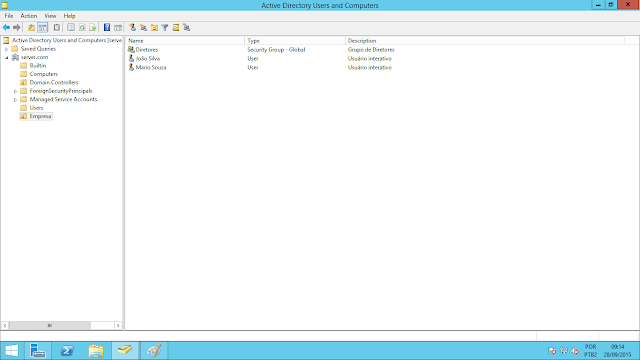
Aqui vemos o usuário "original" e o usuário copiado, mas lembre-se! Nome completo, nome de logon, senha, configurações de sessão, e tempo ocioso, são configurações únicas.

[](https://2.bp.blogspot.com/-qyGVTCuKV-g/Vgqhk8v2iZI/AAAAAAAADZU/Ex-MBWi4tmI/s1600/20.png)

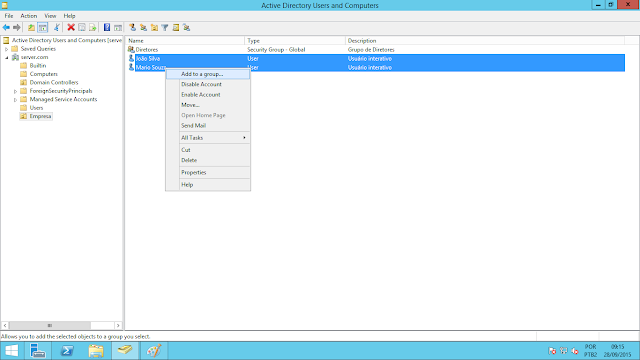
Aqui, criando grupos!

[](https://3.bp.blogspot.com/-95ZO-NqZ5-k/VgqhkWyUD7I/AAAAAAAADZE/Z-PdlldngCk/s1600/21.png)

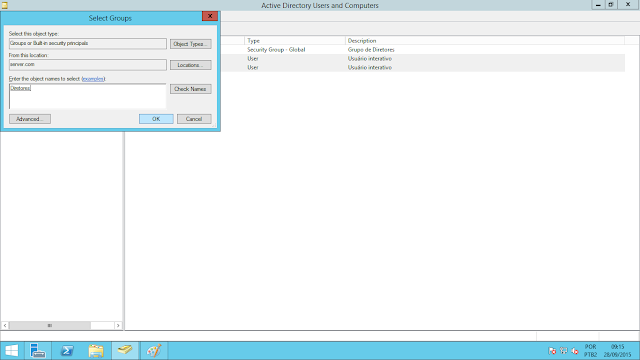
Nome, escopo e tipo de grupo (definição acima)

[](https://4.bp.blogspot.com/-qTx1lA4yWas/VgqhlYYAOcI/AAAAAAAADZY/jDU5WCVEv-U/s1600/22.png)

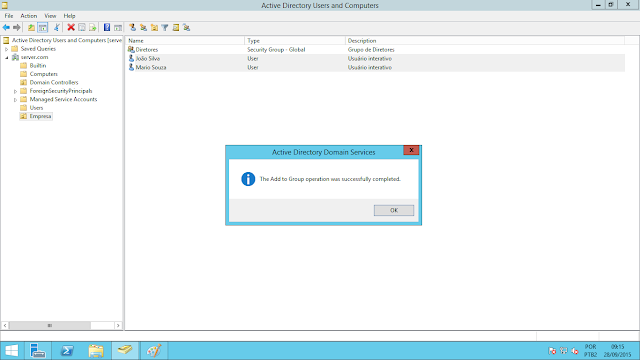
Visualização do grupo e usuários no recipiente Empresa

[](https://4.bp.blogspot.com/-Tgv-85SFLqQ/VgqhlwNTOtI/AAAAAAAADZk/sPQLrWTfmGc/s1600/23.png)

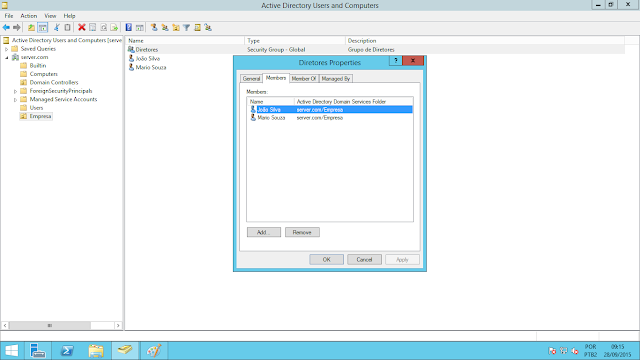
Aqui estamos adicionando os usuários no grupo. Uma dica, podemos selecionar todos eles, clicar com o botão direito do mouse e adicionar ao Grupo. Também podemos ir no objeto grupo, na guia Membros e localizarmos os usuários para adicionar. Particularmente, acho mais prático assim, mas cada um usa da forma como acha melhor :)

[](https://1.bp.blogspot.com/-vgZ__YBlyf4/VgqhmlanSJI/AAAAAAAADZs/6JYMH1lr7YY/s1600/24.png)

Nesta etapa, usamos o localizador para buscar o nome do grupo que queremos adicionar os usuários.

[](https://3.bp.blogspot.com/-f3oSkMV3s7c/VgqhnDOPhMI/AAAAAAAADZ0/LnRzrey7W6o/s1600/25.png)

Mensagem de confirmação da adição dos usuários

[](https://3.bp.blogspot.com/-orMPiIYClCM/VgqhnkCRv1I/AAAAAAAADZ4/GJmmaaU3FZs/s1600/26.png)

Verificação dos usuários pertencentes ao grupo!