

# Como impedir múltiplos logons em uma rede com Active Directory

Por Marcelo Ramos e Tiago Souza

Data de criação: 27/05/2009

## Resumo

Este documento apresenta uma forma alternativa a softwares de mercado para controle de logon de usuário. Explicamos como limitar o logon em uma rede que utiliza Active Directory e Group Policies.

# Como impedir múltiplos logons em uma rede com Active Directory

## Directory

### 1. Introdução

O processo que vamos descrever aborda como impedir que o usuário possa se logar em mais de uma estação de trabalho com o mesmo login de rede do domínio.

Não se trata do recurso do Active Directory (Fig1) onde podemos limitar o login a uma ou mais estações, pois nesse caso o bloqueio fica limitado a uma lista pré-definida de máquinas (Fig2). A grande desvantagem é que caso seja necessária a troca de máquinas, geraria trabalho manual para o administrador de rede, que teria que alterar a lista a cada vez que isso acontecesse.

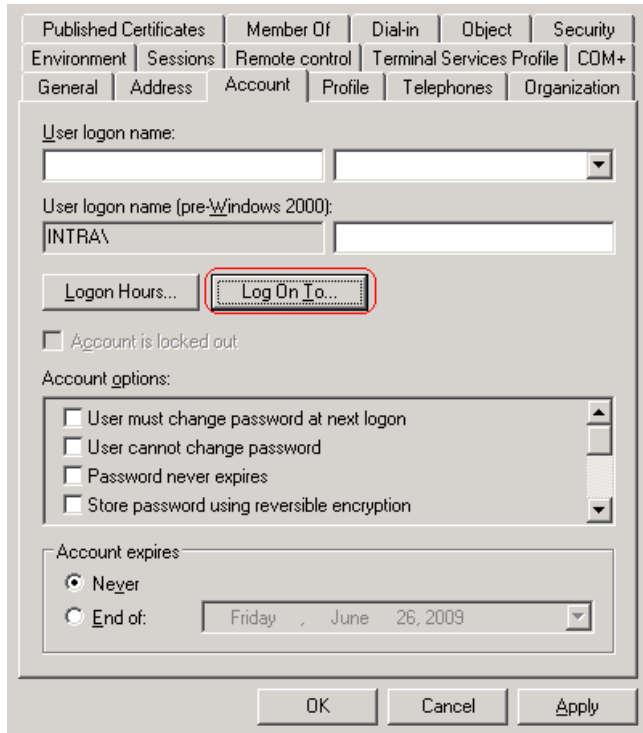


Fig1 – Propriedade de Account do Active Directory

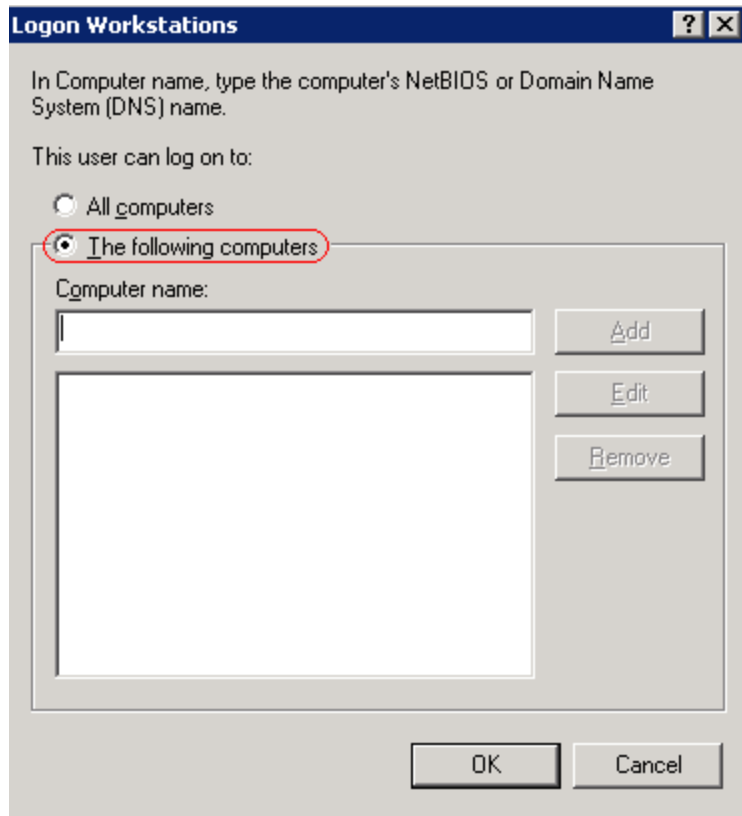


Fig2 – Lista com computadores

Esse documento tem como finalidade explicar como limitar mais de um login em qualquer máquina da rede de forma automática, não havendo necessidade de associar determinada máquina a um usuário específico. Para isso vamos utilizar o Active Directory, GPOs (Group Policy Objects), Scripts de Logon e Logoff e banco de dados SQL Express.

## 2. Pré-requisitos

- Active Directory com domínio previamente configurado
- Estações Windows 2000 ou superior
- SQL Express (ferramenta gratuita, podendo ser instalada no mesmo servidor que hospeda o Active Directory. Em nosso exemplo trabalhamos com a versão 2005)
- GPMC (Group Policy Management Console – ferramenta gratuita para edição de políticas de grupo)

### 3. Scripts de Logon, Logoff e SQL

Para baixar os scripts de Logon, Logoff e SQL, clique no link abaixo. Os scripts estão comentados para facilitar o entendimento.

[Scripts.Zip](#)

Nos scripts login.vbs e logoff.vbs, onde aparece a string de conexão com o banco de dados, será preciso trocar os \*\*\* pelos dados reais de seu ambiente.

#### String de Conexão

```
"Provider=SQLOLEDB.1; Password=***;Persist Security Info=True;User ID=***;Initial  
Catalog=LOGON;Data Source=***"
```

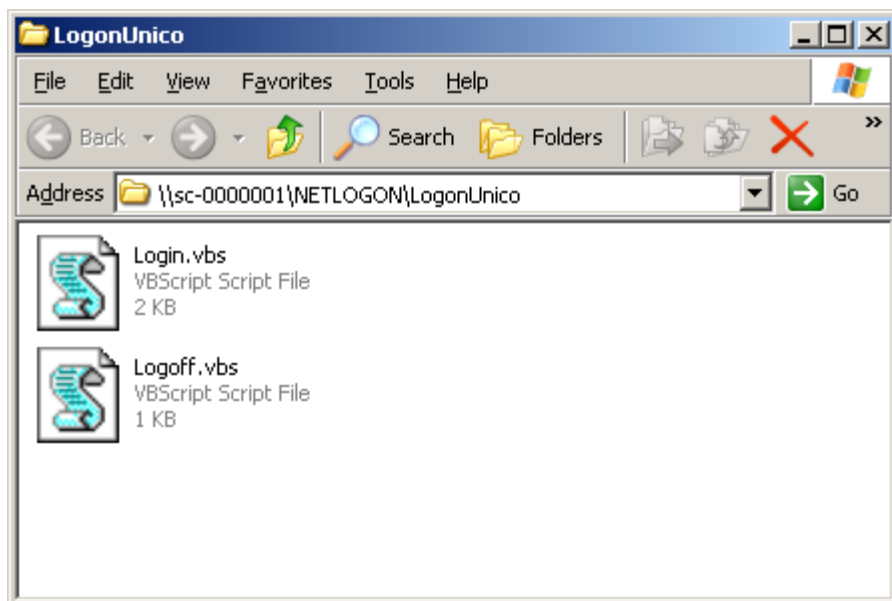
User ID = Usuário com permissão no banco de dados

Password = Senha do usuário configurado no campo User ID

Data Source = Nome do servidor ( Geralmente MAQUINA\SQLEXPRESS onde MAQUINA é o nome do servidor onde foi instalado o SQL Express )

### 4. Compartilhando os Scripts

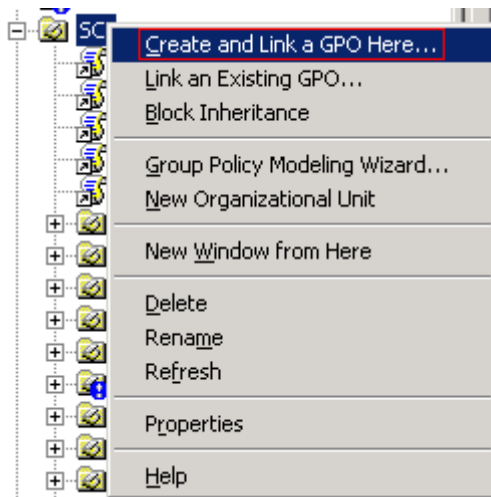
Vamos trabalhar com dois vbscripts, um de Logon e outro de Logoff. Eles devem ficar em um local da rede que o usuário tenha acesso de execução, para isso sugerimos manter o padrão do Active Directory e utilizar o NETLOGON para esse fim.



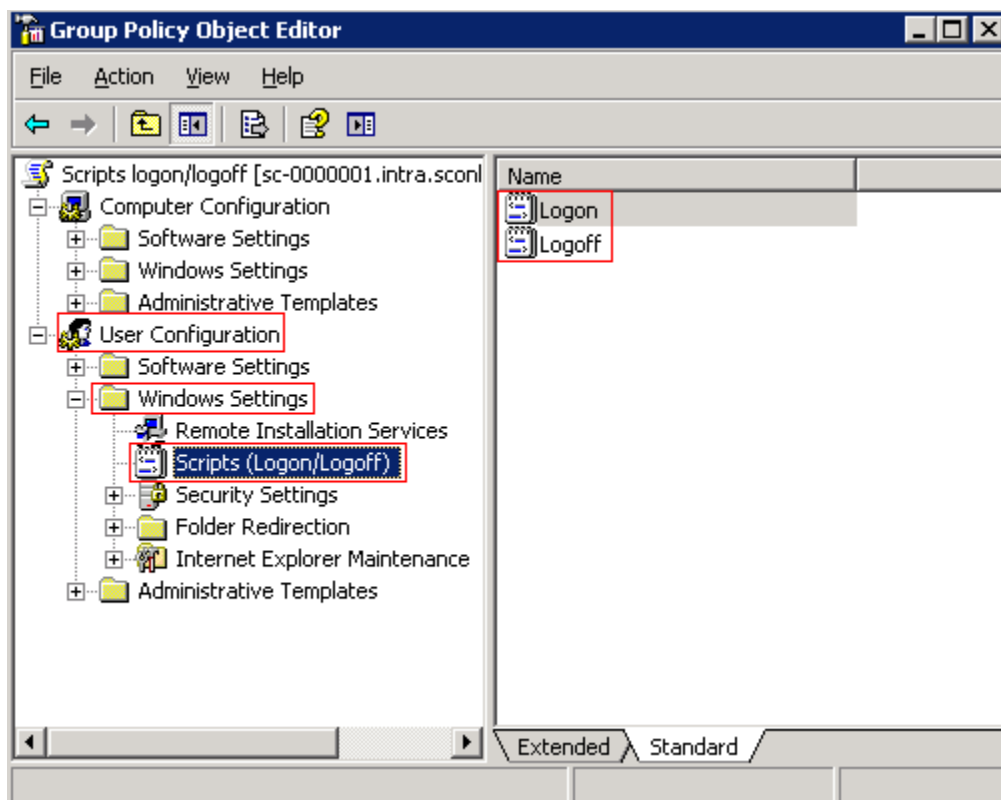
## 5. Criação das GPOs

Vamos iniciar pela criação das GPOs com os scripts de Logon e Logoff. Para realizar este procedimento iremos utilizar o console de edição de políticas GPMC (Group Policy Management Console).

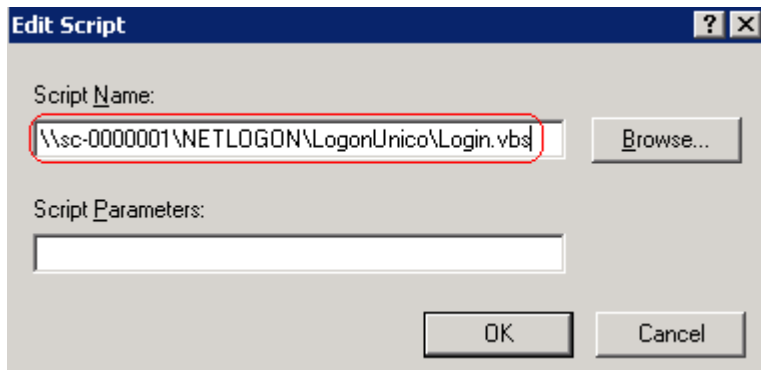
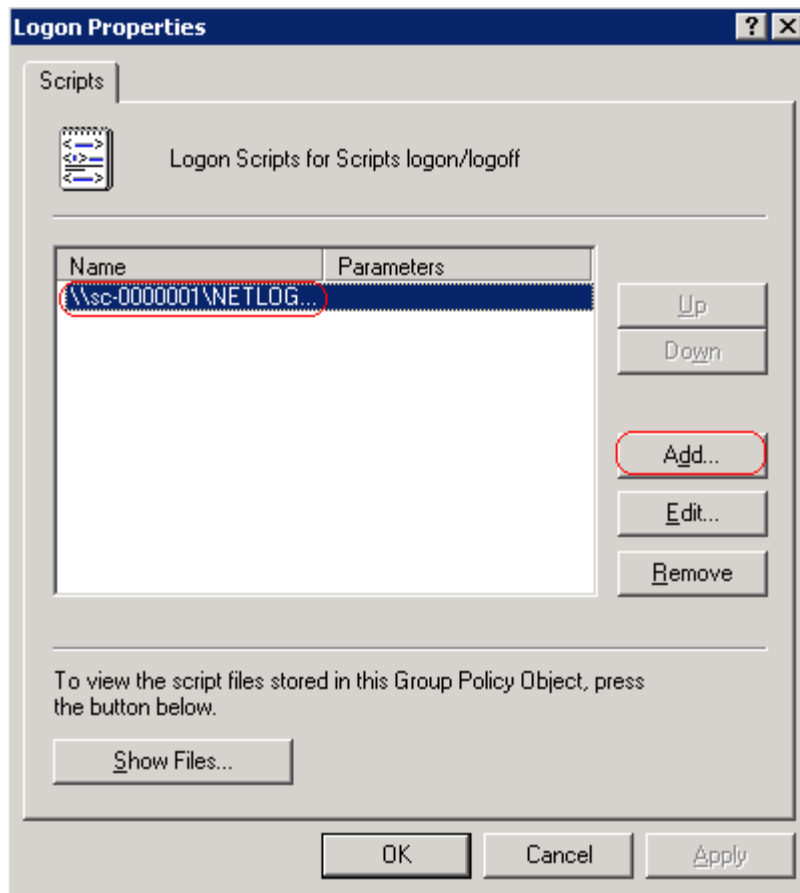
- 1 – Vamos abrir o GPMC para criarmos e editarmos nossa policie de scripts de **logon** e **logoff**. Clique em **start > run >** e digite **“gpmc.msc”** (sem as aspas)
- 2 – Vamos escolher em qual Unidade Organizacional vamos linkar a policy, clicamos com o botão direito em cima dela e selecionamos a opção **“Create and Link a GPO Here...”**



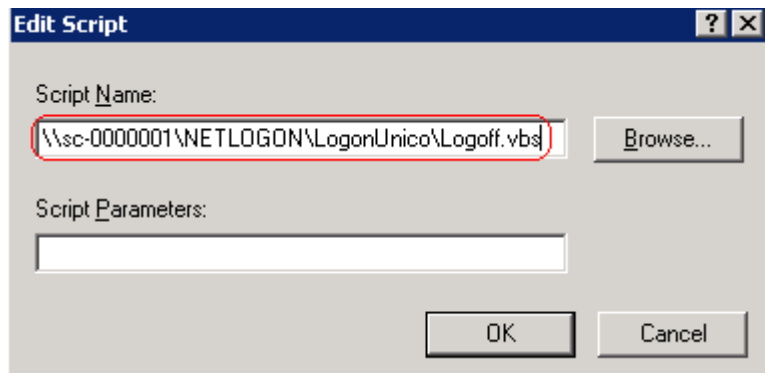
3 – Com o editor de políticas aberto vamos expandir: **User Configuration > Windows Settings > selecionar Scripts (Logon/Logoff)**



4 – Vamos iniciar dando um duplo clique em **Logon**. A janela de configuração irá se abrir e vamos clicar em **Add** e passar o caminho do compartilhamento criado no NETLOGON, no nosso exemplo **\\SC-0000001\NETLOGON\LogonUnico\Logon.vbs**



5 – Vamos agora abrir o **Logoff** e fazer o mesmo procedimento, só que agora buscando o script de logoff no mesmo compartilhamento **\\SC-0000001\NETLOGON\LogonUnico\Logoff.vbs**



6 – Pronto, a política já está criada. Podemos forçar sua execução com o comando “gpupdate /force”.

## 6. SQL Express

O controle dos usuários logados é feito através de um registro incluído no banco de dados assim que ele efetua o logon (login.vbs).

Será necessário:

- Instalar o SQL Express
- Criar um banco de dados e nomeá-lo como **LOGON**
- Criar a tabela **USUARIOS** ( LogonUnico.sql )

Banco e ferramentas de administração podem ser encontrados nos links abaixo:

- **SQL Server 2005 Express Edition**  
[http://download.microsoft.com/download/F/4/E/F4EE8AE2-4979-47F0-A931-791B2B7DCFA2/SQLEXP32\\_PT6.EXE](http://download.microsoft.com/download/F/4/E/F4EE8AE2-4979-47F0-A931-791B2B7DCFA2/SQLEXP32_PT6.EXE)
- **SQL Server Management Studio Express -**  
<http://go.microsoft.com/fwlink/?linkid=65110>
- **SQL Server 2005 Express Edition with Advanced Services** <http://go.microsoft.com/fwlink/?linkid=65109>

## 7. Resolução de problemas

O único problema encontrado foi nas sessões de terminal services. Quando há queda ou congelamento da sessão não é executado o logoff que por sua vez não limpa o registro do usuário na base.

Para limpar o registro manualmente execute no SQL um dos seguintes comandos:

```
/* DELETANDO REGISTRO POR USUARIO */
```

```
DECLARE @USUARIO VARCHAR(30)
```

```
SET @USUARIO = 'USUARIO' -- COLOQUE O NOME DO USUARIO AQUI
```

```
DELETE FROM DBO.USUARIOS WHERE USUARIO = @USUARIO
```

```
/* DELETANDO REGISTRO POR MAQUINA */
```

```
DECLARE @MAQUINA VARCHAR(30)
```

```
SET @MAQUINA = 'MAQUINA' -- COLOQUE O NOME DA MAQUINA AQUI
```

```
DELETE FROM DBO.USUARIOS WHERE MAQUINA = @MAQUINA
```

```
/* DELETANDO TODOS OS REGISTROS */
```

```
DELETE FROM DBO.USUARIOS
```

## 8. Conclusão

O procedimento adotado nesse documento é uma alternativa **simples** aos softwares de mercado, pagos ou não, como LimitLogin da própria Microsoft. Não existe ferramenta de monitoria, ficando a manutenção e melhoria do processo por conta de cada administrador.

## **Autores:**

*Tiago Vieira Ferreira de Souza é idealizador do site Portal Tecnologia, atua desde 2004 como Administrador de Redes, com foco em tecnologias Microsot. Formado em Tecnologia em Redes de Computadores, MCP Windows Server 2003, MCTS Windows Vista.*

*Site: <http://www.portaltecnologia.net/>*

*E-mail: [contato@tiagosouza.net](mailto:contato@tiagosouza.net)*

*Marcelo Ramos Borges de Oliveira é MCP na plataforma .NET desde 2007, atua a aproximadamente 10 anos no mercado de TI. Atualmente é Gerente de TI em empresa de médio porte com foco em Desenvolvimento Web.*

*Site: <http://www.marceloramos.net/Blog>*

*E-mail: [mramos.oliveira@gmail.com](mailto:mramos.oliveira@gmail.com)*