Sessão 9: Configuração segura de servidores Windows

1) Configuração do controlador de domínio *Active Directory*

Esta atividade será realizada na máquina virtual *WinServer-G*.

Nesta atividade iremos instalar e configurar a *role Active Directory* na máquina *WinServer-G*, tornando-o um controlador de domínio primário (também conhecido como AD DC — *Active Directory Domain Controller*) para o domínio `domainG.esr.local`, sendo `G` a letra associada ao seu grupo. Para fazer isso, siga os passos abaixo:

1. Acesse a máquina *WinServer-G* como o usuário `Administrator`. Acesse *Start* > *Run...* e digite `dcpromo.exe`. Clique em *OK*. O Windows Server irá iniciar o processo de instalação dos binários do *Active Directory* na máquina e, ao final do processo, irá abrir o *wizard* de configuração como se segue:

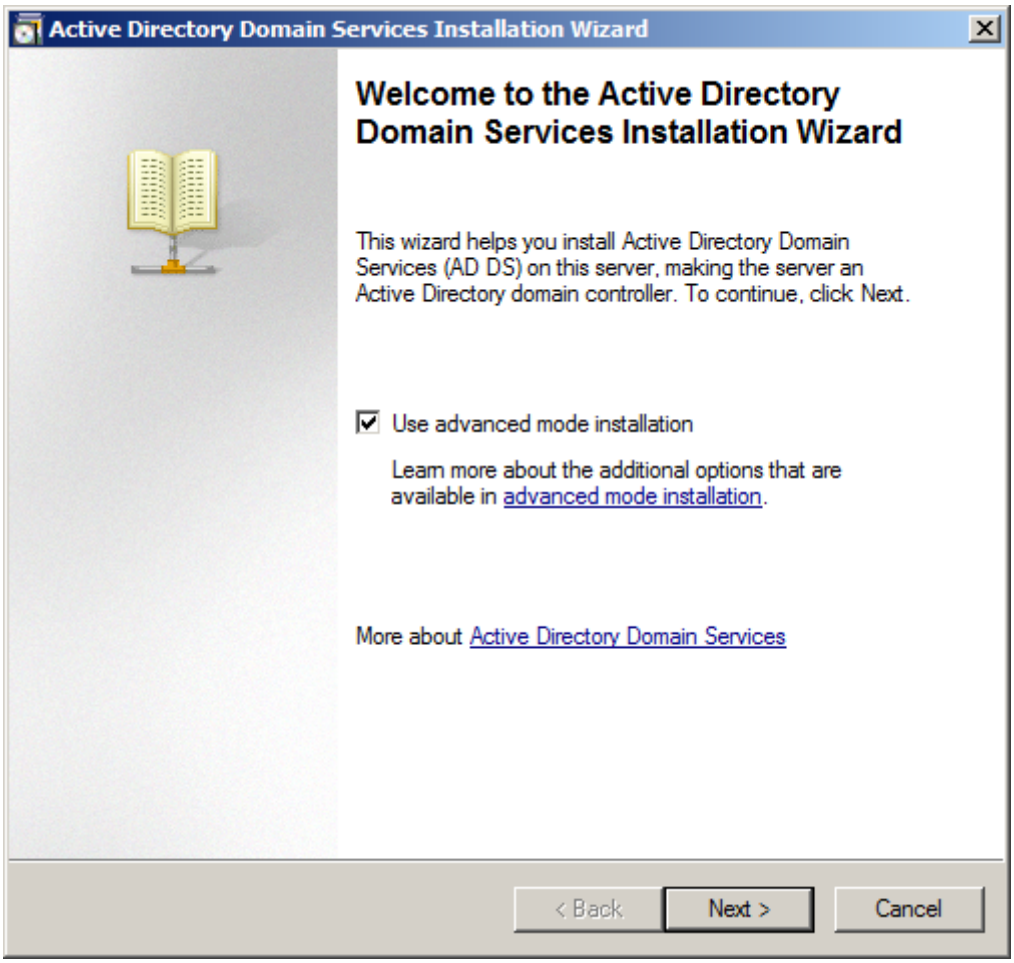

Figura 1. Tela inicial de configuração do AD DC

   Marque a opção *Use advanced mode installation* e clique em *Next*.

2. Na tela *Operating System Compatibility*, clique em *Next*.

3. Na tela *Choose a Deployment Configuration*, selecione *Create a new domain in a new forest*, como mostrado abaixo, e clique em *Next*.

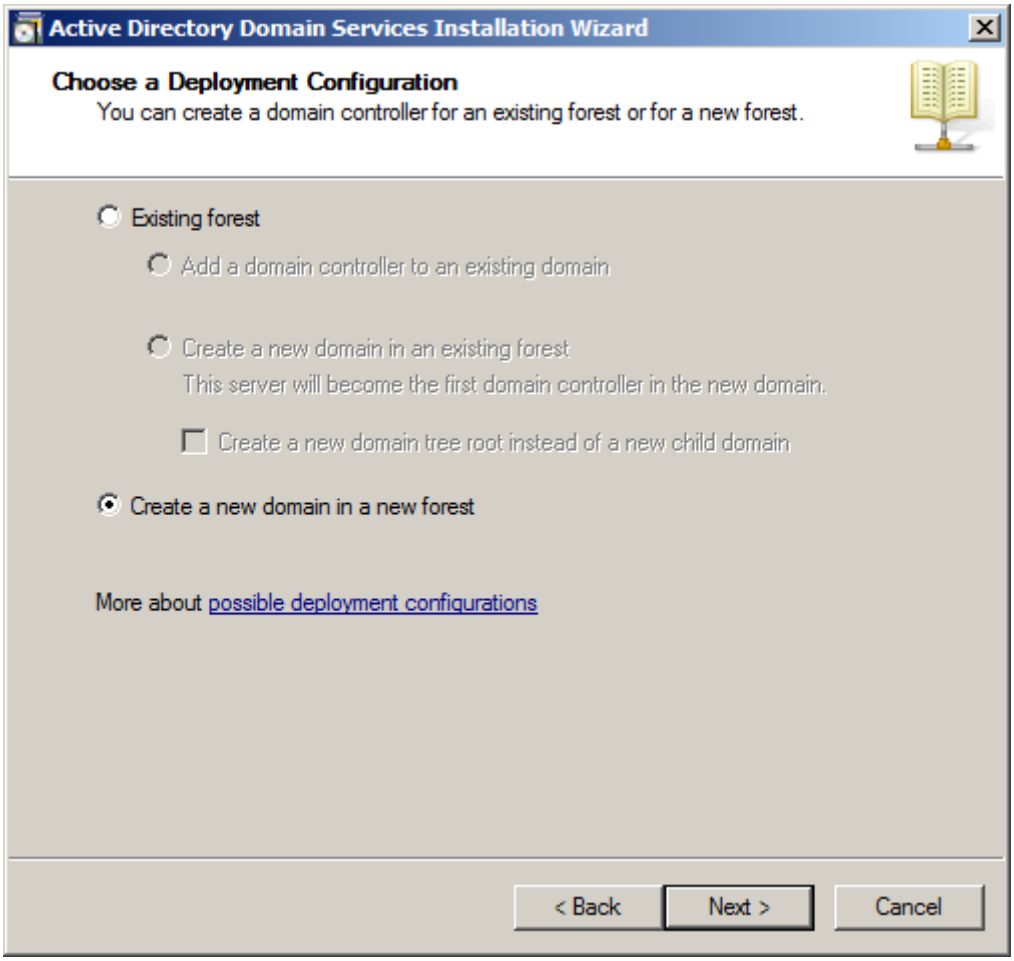

Figura 2. Escolha de tipo de instalação do AD DC

4. Na tela *Name the Forest Root Domain*, escolha o FQDN do seu domínio. Se estiver no grupo A, digite `domainA.esr.local`; no grupo B, digite `domainB.esr.local`. Verifique sua entrada de acordo com a imagem que se segue, e clique em *Next*.

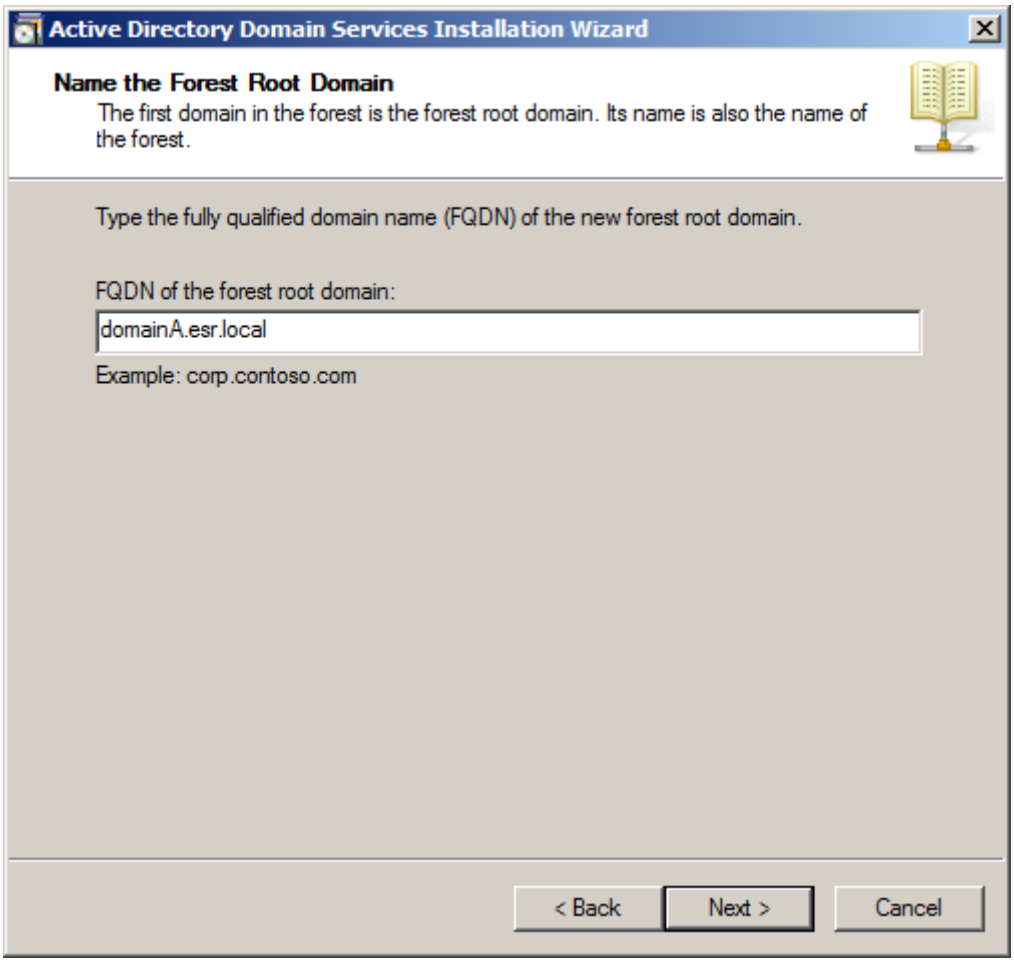

Figura 3. Escolha do FQDN do AD DC

5. Na tela subsequente, *Domain NetBIOS Name*, escolha `DOMAINA` ou `DOMAINB` (dependendo do seu grupo) e clique em *Next*.

6. Na página *Set Forest Functional Level*, selecione o nível funcional de floresta que acomoda os controladores de domínio a serem instalados em qualquer lugar da floresta. Como teremos somente controladores de domínio Windows 2008 Server e acima, utilizaremos o nível funcional `Windows 2008 Server`. Confira sua seleção de acordo com a imagem a seguir, e clique em *Next*.

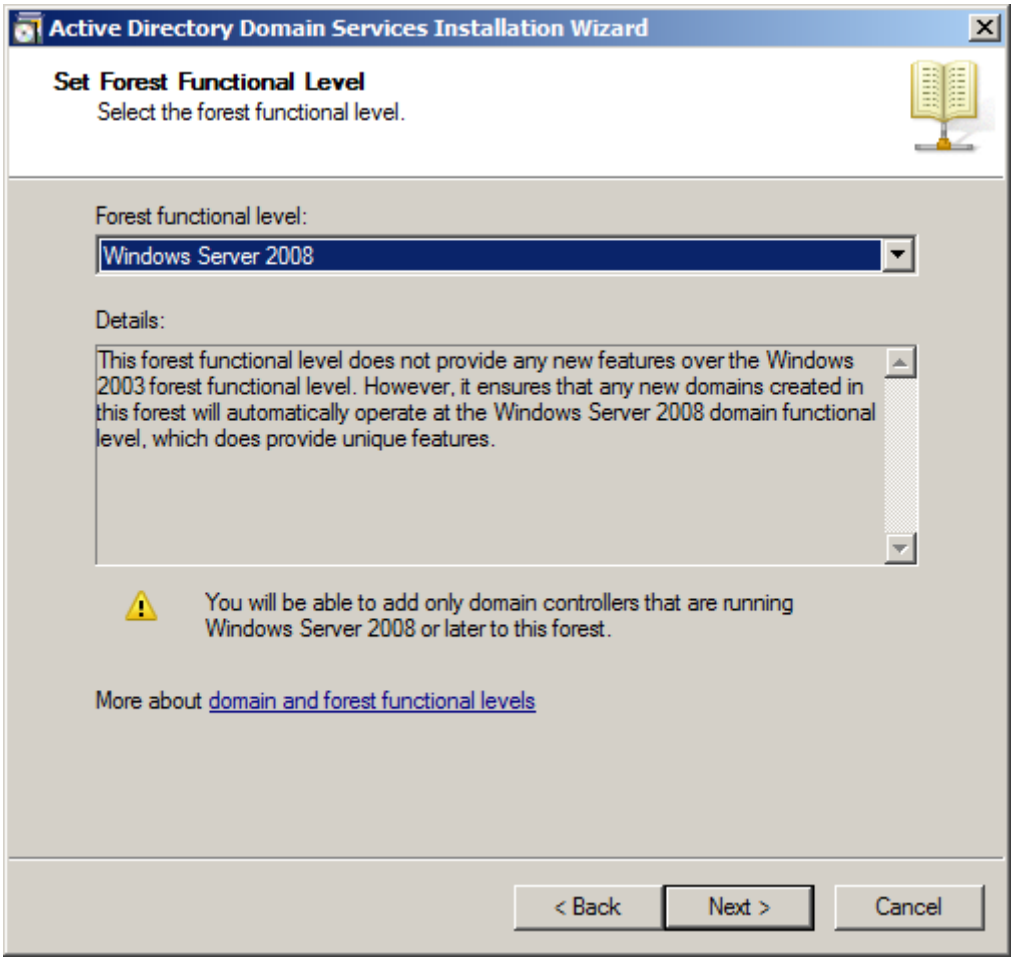

Figura 4. Escolha do nível funcional da floresta AD DC

7. Na tela *Additional Domain Controller Options*, mantenha a opção `DNS Server` marcada, indicando que a infraestrutura DNS da sua floresta deverá ser criada durante a instalação do AD DS. Em seguida, clique em *Next*.

   O sistema irá informar que uma delegação DNS para o servidor local (a máquina *WinServer-G*) não pode ser criada pois o servidor DNS autoritativo não está usando o servidor DNS do Windows, como se segue:

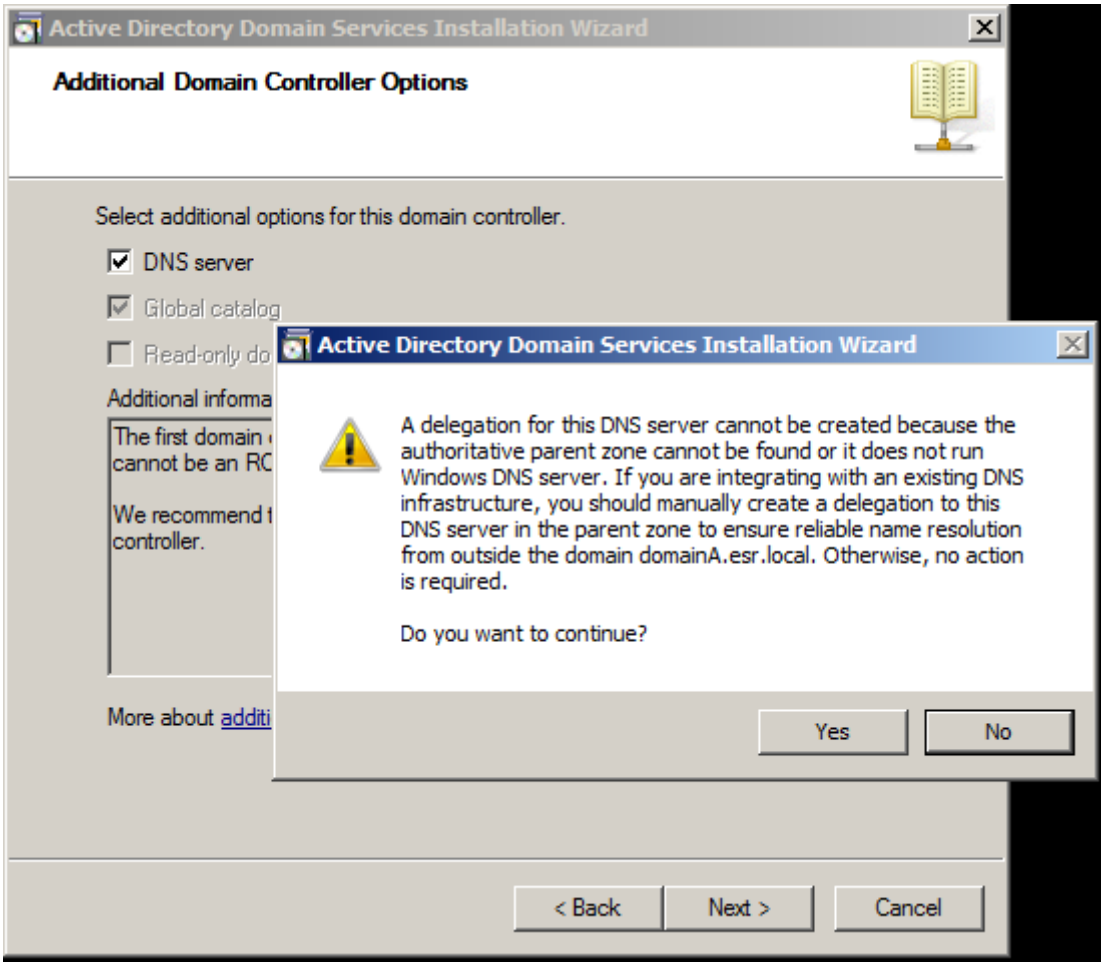

Figura 5. Erro na delegação DNS do AD DC

   Após ler a mensagem de aviso, clique em *Yes* para continuar.

8. Na tela *Location for Database, Log Files and SYSVOL*, mantenha os valores propostos pelo instalador e clique em *Next*.

9. Na tela *Directory Services Restore Mode Administrator Password*, defina uma senha para o modo de recuperação dos serviços de diretório do AD DC a ser usada em casos de falha. Para este exemplo, defina a senha como `rnpesr`, como mostrado abaixo. Em seguida, clique em *Next*.

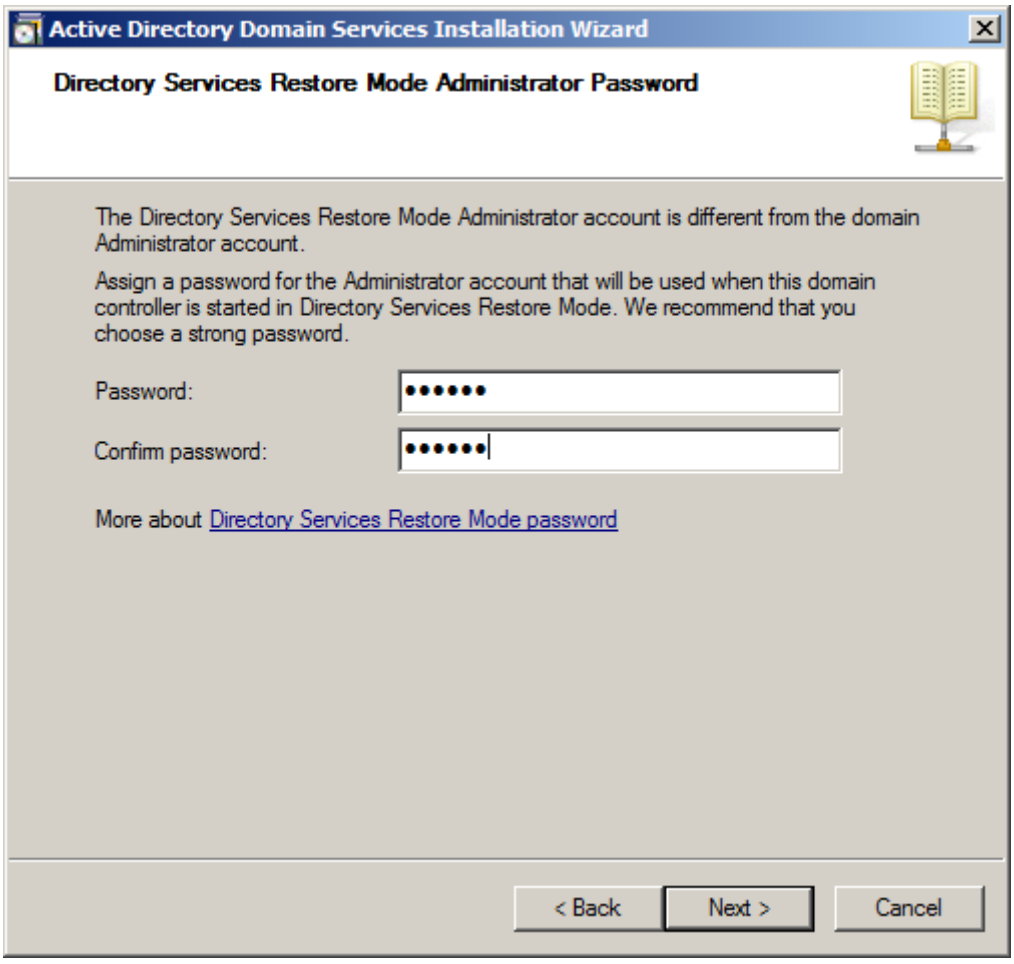

Figura 6. Definição da senha do modo de recuperação do AD DC

10. Na tela *Summary*, verifique se todas as opções definidas para o servidor do *Active Directory* estão corretas; em caso positivo, clique em *Next*.
11. Ao final do processo de instalação da *role* AD DC, reinicie a máquina *WinServer-G* para concluir o processo de instalação.

2) Configuração do firewall para o *Active Directory*

Esta atividade será realizada na máquina virtual *FWGW1-G*.

O próximo passo seria adicionar a máquina *WinClient-G* ao domínio mas, antes disso, temos que configurar a *chain* FORWARD do firewall *FWGW1-G* para permitir o repasse dos pacotes nas portas relevantes.

A base de documentação da Microsoft, acessível através do link (https://support.microsoft.com/en-us/help/832017#method1) lista um grande conjunto de portas a serem acessadas, como se segue:

- Para ambientes que utilizam exclusivamente versões do Windows anteriores ao Windows Server 2008 e Windows Vista, deve-se habilitar conectividade das portas 1025 a 5000.

- Para ambientes que utilizam apenas o Windows Server 2008 R2, Windows Server 2008, Windows 7 ou Windows Vista, deve-se habilitar conectividade das portas 49152 a 65535.
- Para ambientes que utilizam tanto versões modernas quanto antigas do Windows, deve-se habilitar ambas as faixas acima, 1025 a 5000 e 49152 a 65535.

Além dessas portas, a figura a seguir mostra também quais portas conhecidas devem ser liberadas pelo firewall para conectividade.

Application protocol	Protocol	Ports
Active Directory Web Services (ADWS)	TCP	9389
Active Directory Management Gateway Service	TCP	9389
Global Catalog	TCP	3269
Global Catalog	TCP	3268
ICMP		No port number
LDAP Server	TCP	389
LDAP Server	UDP	389
LDAP SSL	TCP	636
IPsec ISAKMP	UDP	500
NAT-T	UDP	4500
RPC	TCP	135
RPC randomly allocated high TCP ports[1]	TCP	1024 - 5000 49152 - 65535[2]
SMB	TCP	445

Figura 7. Portas conhecidas para liberação do AD no firewall

Considerando o grande número de portas em questão, iremos permitir a faixa completa de conexão entre as máquinas *WinServer-G* e *WinClient-G*, para facilitar a configuração neste laboratório.

1. Acesse a máquina *FWGW1-G* como usuário `root` e permita trânsito irrestrito de pacotes entre as máquinas *WinServer-G* e *WinClient-G*. Considere o sentido do fluxo de pacotes em suas regras.

```
# hostname ; whoami
FWGW1-A
root
```

```
# iptables -A FORWARD -s 10.1.1.10/32 -d 172.16.1.20/32 -j ACCEPT
```

3) Adição de clientes ao *Active Directory*

Esta atividade será realizada na máquina virtual *WinClient-G*.

1. Vamos, agora sim, adicionar a máquina *WinClient-G* ao domínio. Acesse-a como usuário `Aluno` e abra as configurações de rede. Acesse *Iniciar* e digite `ncpa.cpl`. Em seguida, clique com o botão direito em *Conexão Local* e navegue para *Propriedades* > *Protoloco TCP/IP Versão 4* > *Propriedades*. Altere o servidor DNS primário para o IP da máquina *WinServer-G*, como se segue:

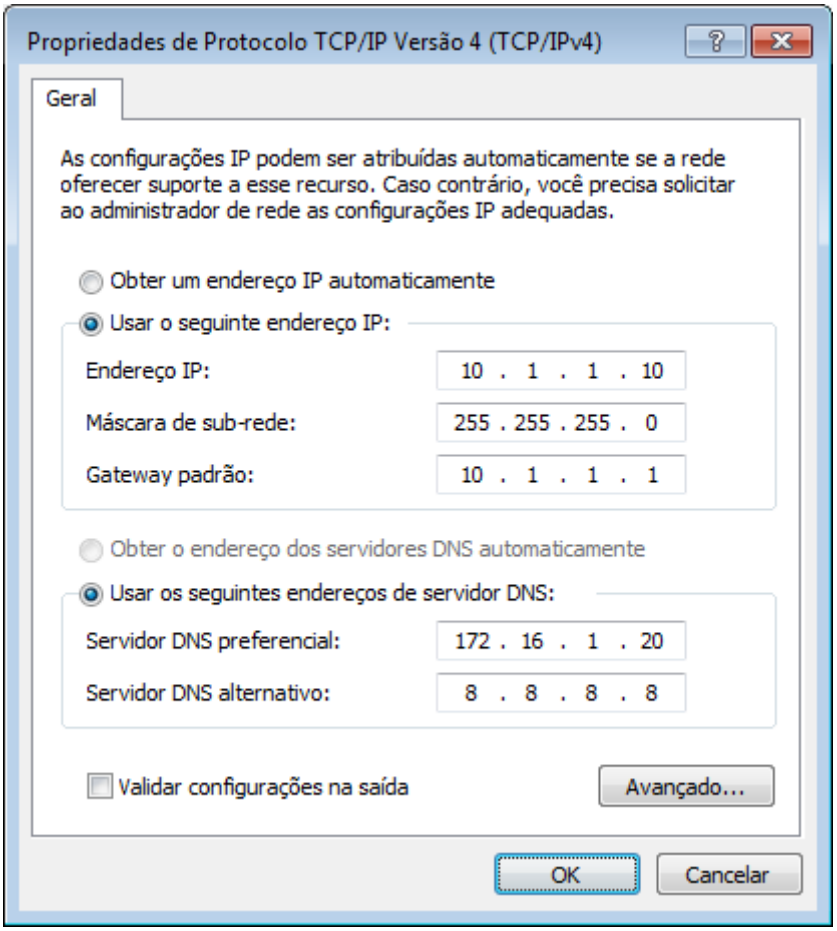

Figura 8. Configuração DNS do cliente AD

2. Agora, navegue para *Painel de Controle* > *Sistema e Segurança* > *Sistema* > *Alterar configurações*. Em seguida, clique no botão *Alterar...* para mudar o domínio da máquina local. Na caixa *Membro de*, marque o botão *Domínio* e digite o FQDN do domínio configurado no passo (4) da atividade (1) desta sessão, como se segue.

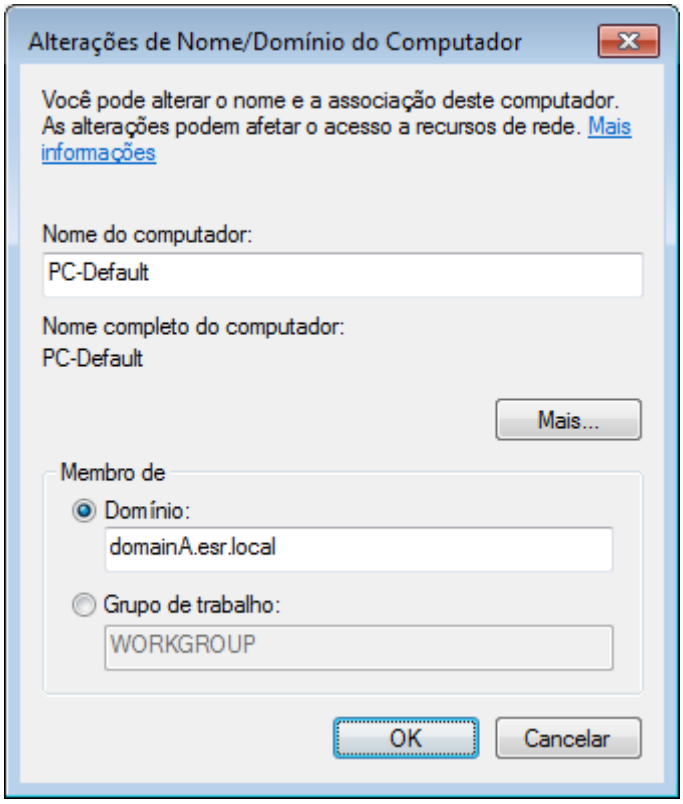

Figura 9. Inserindo o cliente AD no domínio

Clique em *OK*. O sistema irá exigir autenticação — você deve usar um usuário com permissões **administrativas** no AD DC, como o usuário `Administrator`. Informe, também, o domínio de autenticação do usuário. Trocando em miúdos, autentique-se como:

- Nome de usuário: `DOMAINA\Administrator`
- Senha: `rnpesr`

Após algum tempo de processamento, você deverá receber a mensagem *Bem vindo ao domínio domainG.esr.local*, como mostrado abaixo.

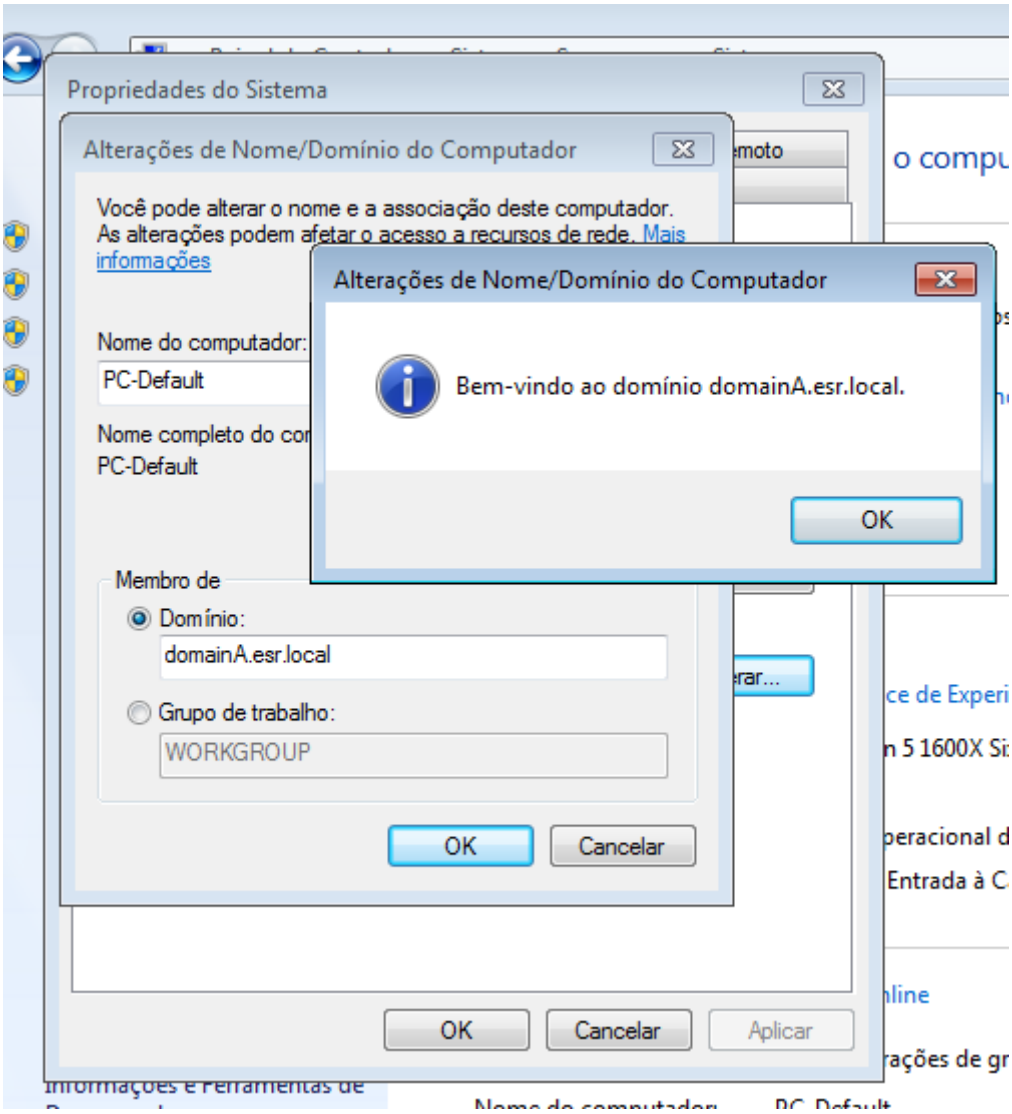

Figura 10. Inserção do cliente AD no domínio com sucesso

Reinicie a máquina *WinClient-G* para concluir o processo.

4) Adição de usuários ao *Active Directory*

Esta atividade será realizada nas máquinas virtuais *WinServer-G* e *WinClient-G*.

1. Vamos criar um usuário não-privilegiado para autenticar-se no domínio. Logue na máquina *WinServer-G* como um usuário administrativo (por exemplo, `DOMAINA\Administrator`), e execute *Start* > *Run...* > `dsa.msc`. Você deverá ver a tela do *Active Directory Users and Computers*, como se segue:

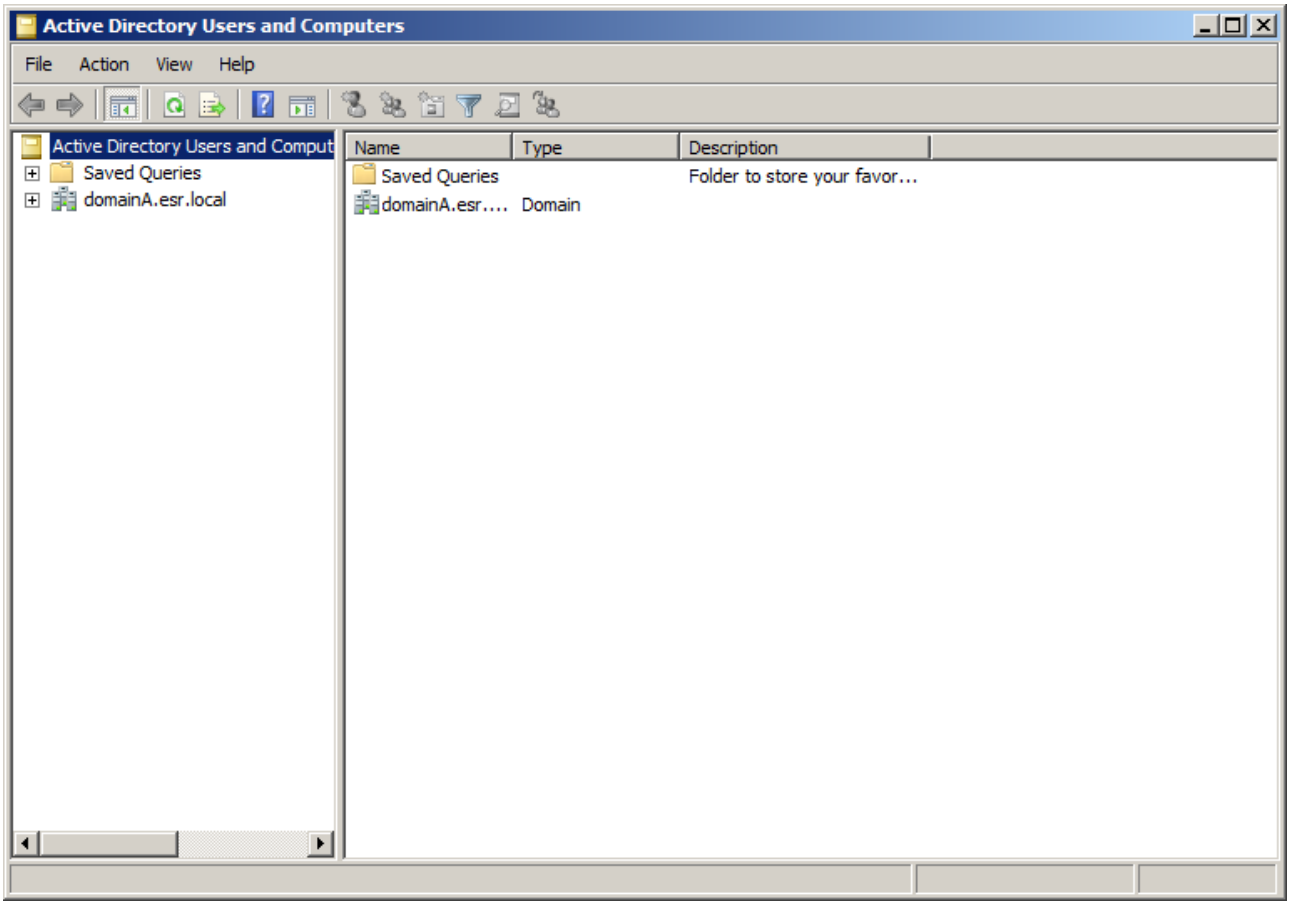

Figura 11. Interface de edição de usuários e máquinas do AD

2. Expanda a floresta `domainA.esr.local`, e observe as pastas *Builtin*, *Computers*, *Domain Controllers*, *ForeignSecurityPrincipals* e *Users*. Para visualizar os usuários e grupos existentes no domínio, clique sobre a pasta *Users*.

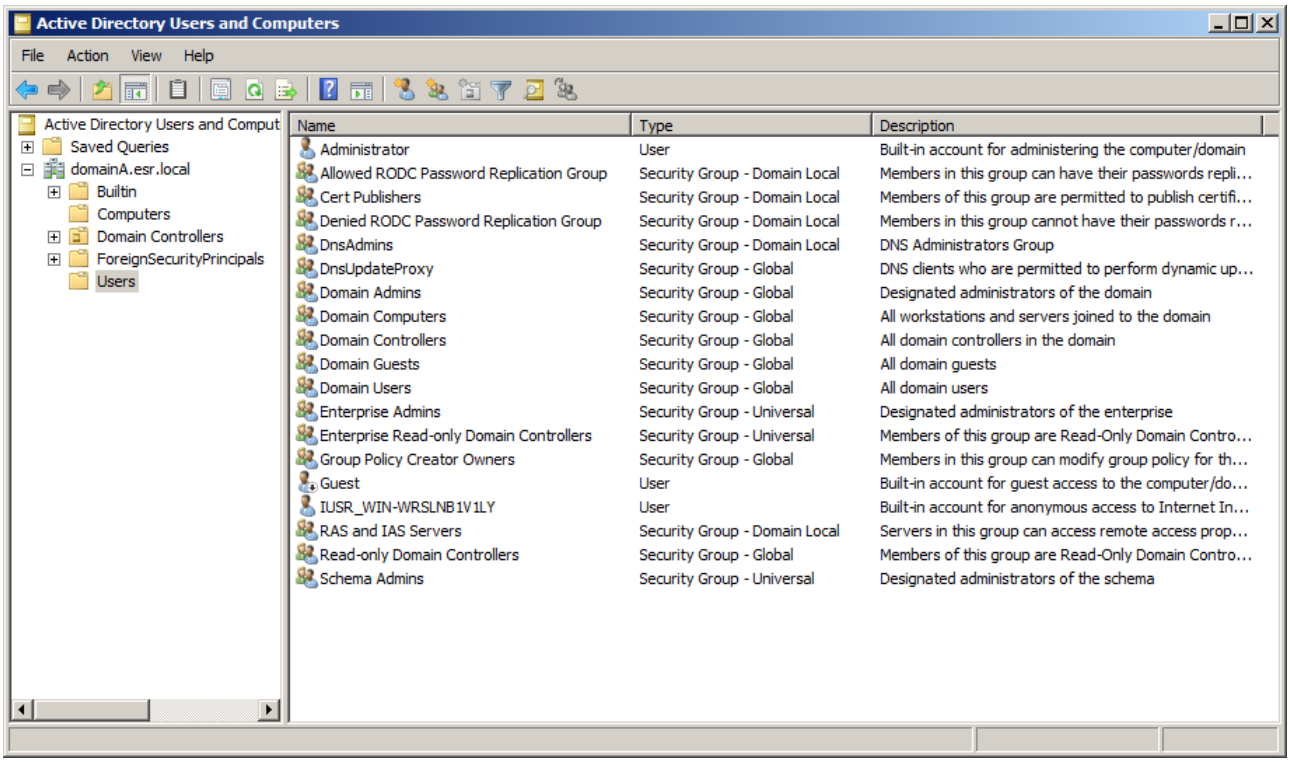

Figura 12. Visão de usuários e grupos existentes no AD

De igual forma, para ver os computadores adicionados ao AD, basta clicar sobre a pasta

Computers.

3. Para adicionar um novo usuário, clique com o botão direito sobre a pasta *Users*, e em seguida *New* > *User*. Crie um usuário com os seguintes dados:

   - *First name*: Indiana
   - *Last name*: Jones
   - *Initials*: IJ
   - *Full name*: Henry Walton Jones Jr.
   - *User logon name*: `indyjones@domainA.esr.local`
   - *User logon name (pre-Windows 2000)*: `DOMAINA\indyjones`

   Preenchidos os dados, clique em *Next*.

4. Na tela de definição de senha, devemos escolher uma senha suficientemente complexa para que o AD não a invalide. Uma senha como `RnpEsr!123` é uma boa escolha. Logo abaixo, mantenha marcada a caixa *User must change password at next logon*, e todas as demais desmarcadas. Clique em *Next*.
5. Na tela de confirmação dos dados, verifique que tudo está correto como mostrado a seguir, e clique em *Finish*.

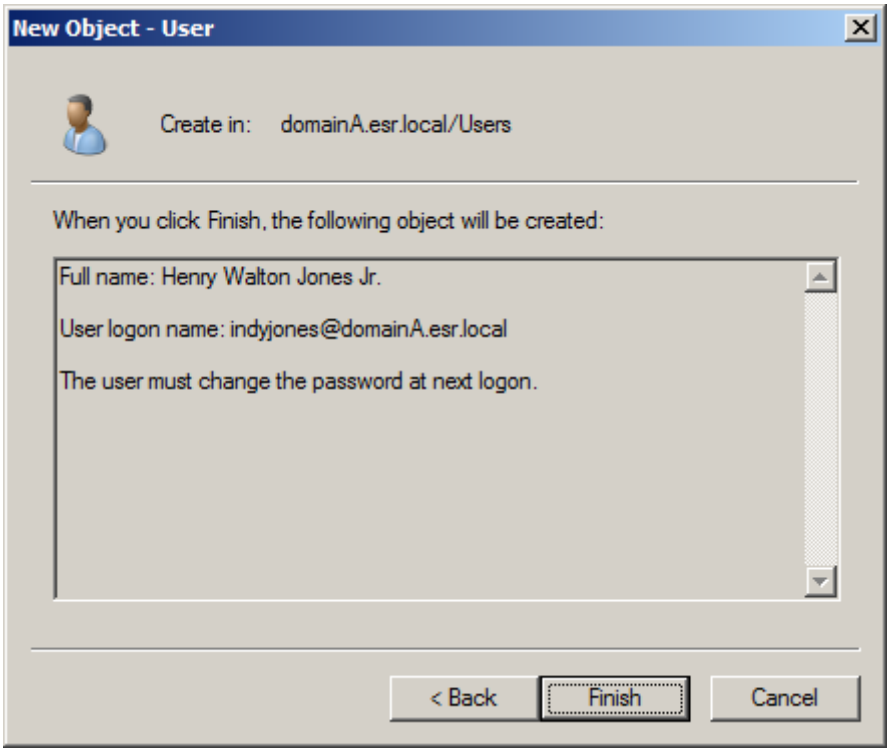

Figura 13. Confirmação de adição de usuário ao AD

6. De volta à máquina *WinClient-G*, tente logar com o usuário `indyjones` recém-criado. Clique no botão *Trocar Usuário* > *Outro Usuário* e digite os dados inseridos nos passos (3) e (4). Observe que o logon será feito no domínio `DOMAINA`, como objetivado.

Figura 14. Logon inicial no AD

Imediatamente, o AD reporta que a senha deve ser alterada no primeiro logon — isso faz sentido, pois mantivemos a caixa *User must change password at next logon* marcada quando da criação do usuário no passo (4). Escolha uma nova senha, diferente da primeira e igualmente complexa (sugestão: `Seg2@rnp!`), e confirme o logon.

Finalmente, verifique que você está de fato logado na máquina como o usuário do domínio.

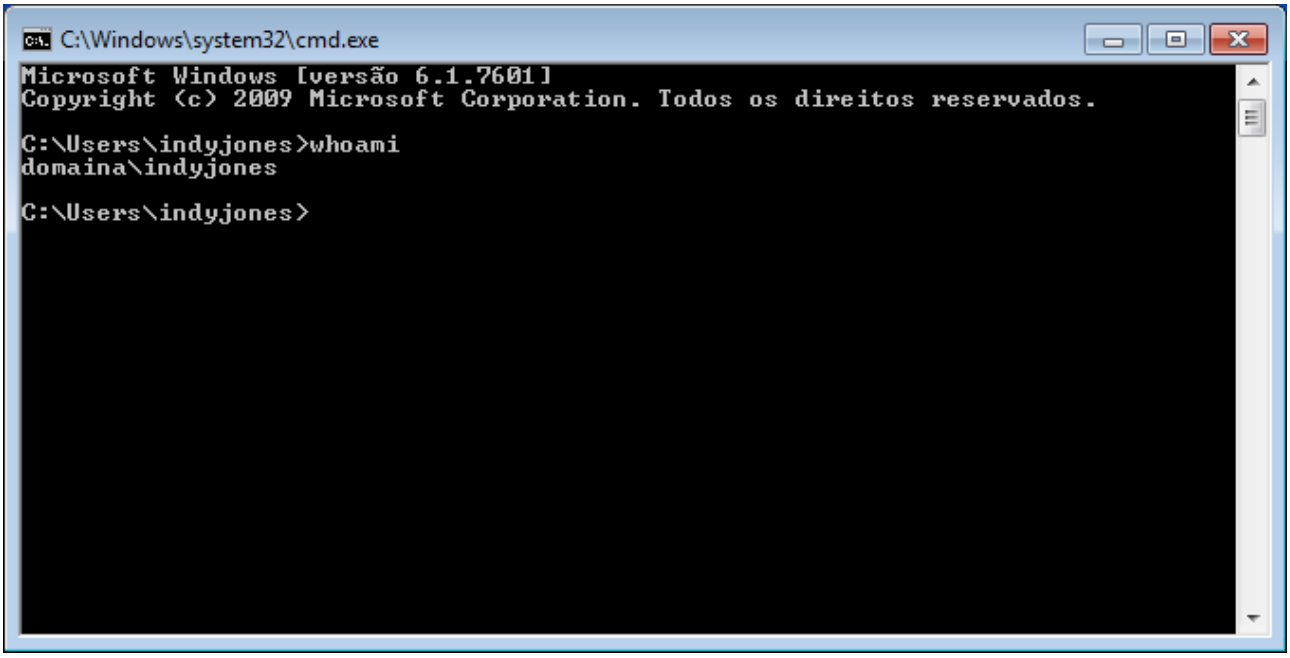

Figura 15. Verificação de logon no AD

5) Distribuição de configurações via GPOs

Esta atividade será realizada nas máquinas virtuais *FWGW1-G*, *WinServer-G* e *WinClient-G*.

Iremos agora usar GPOs (*Group Policy Objects*) para fazer configurações centralizadas de máquinas clientes do domínio. De fato, iremos usar as GPOs para resolver um problema que já tivemos anteriormente neste curso: a adição de certificados de ACs para *man-in-the-middle*, especificamente o do Squid *SslBump Peek and Splice* (sessão 7, atividade 2).

1. Primeiro, acesse a máquina *FWGW1-G* como usuário `root` e volte a executar o Squid em modo de interceptação de tráfego SSL, como fizemos anteriormente. Caso as regras de firewall não estejam mais ativas, reinsira-as e execute o Squid:

```
# hostname ; whoami
FWGW1-A
root
```

```
# iptables -t nat -A PREROUTING -i eth2 -o eth0 -p tcp -m tcp --dport 80 -j
REDIRECT --to-port 8080
# iptables -t nat -A PREROUTING -i eth2 -o eth0 -p tcp -m tcp --dport 443 -j
REDIRECT --to-port 8443
# iptables -A INPUT -s 10.1.1.0/24 -p tcp -m tcp -m multiport --dports 8080,8443 -j
ACCEPT
```

```
# /usr/local/sbin/squid -f /usr/local/etc/squid.conf
```

2. Na máquina *WinClient-G*, tente acessar um website via HTTPS para testar se a interceptação está ativa. No exemplo abaixo, estamos acessando o https://facebook.com ; note que o certificado é identificado como inválido (como esperado), e emitido pela CA da máquina `fwgw1-g.esr.rnp.br`:

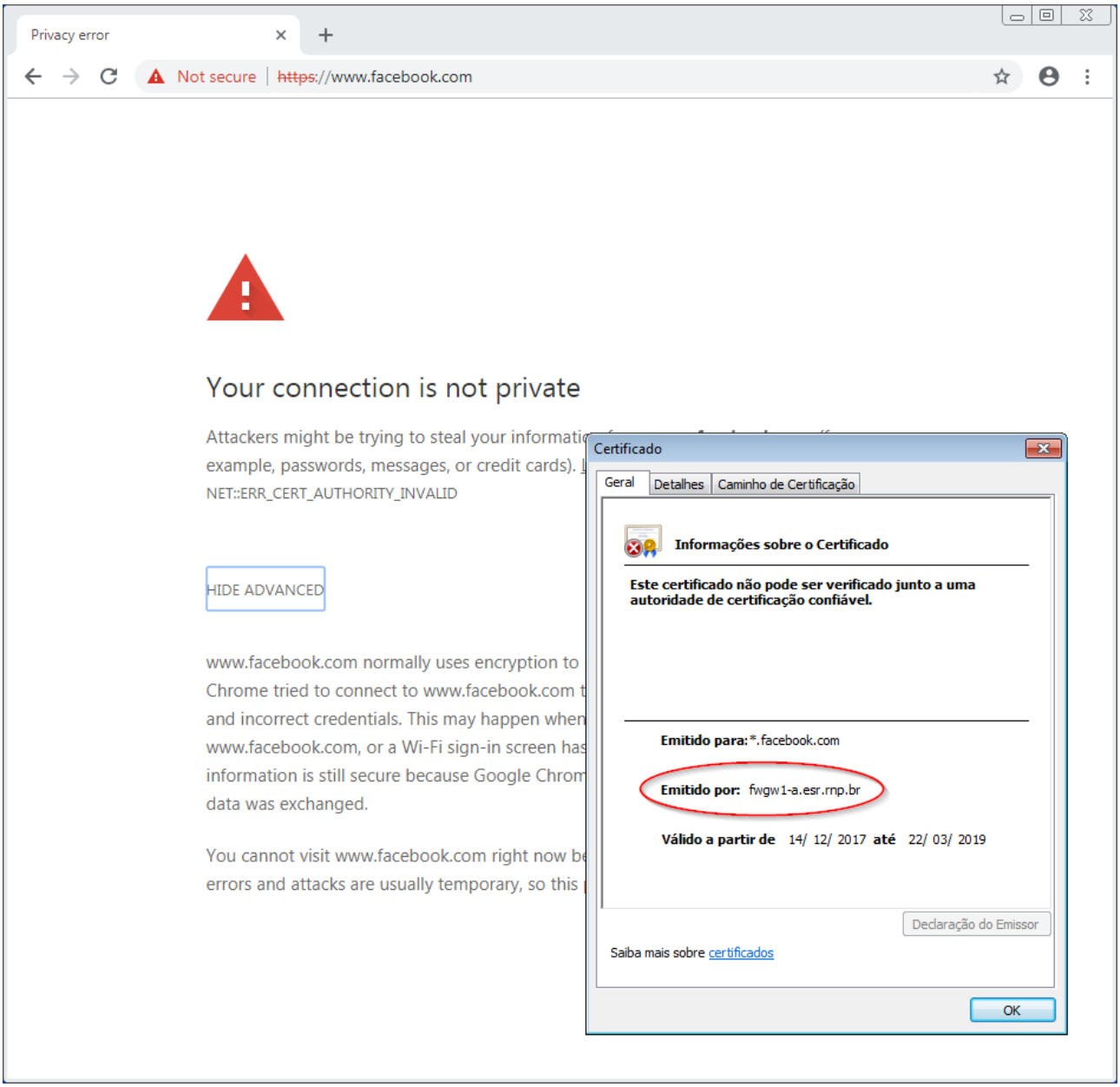

Figura 16. Detecção de certificado forjado não-confiável na máquina WinClient-G

3. Para resolver o problema, vamos adicionar o certificado do Squid instalado na máquina *FWGW1-G* à base de certificados raiz confiáveis, como fizemos anteriormente. Mas, ao invés de fazer isso manualmente, vamos usar o AD e as GPOs para realizar essa tarefa. Copie o certificado localizado em `/usr/local/etc/ssl/public.crt` (na máquina *FWGW1-G*) para o *Desktop* da máquina *WinServer-G* — use o programa `WinSCP` ou a pasta compartilhada pelo Virtualbox, como preferir.

   Ao final do processo, você deverá ter a chave pública da CA do Squid disponível na máquina *WinServer-G*, como mostrado abaixo.

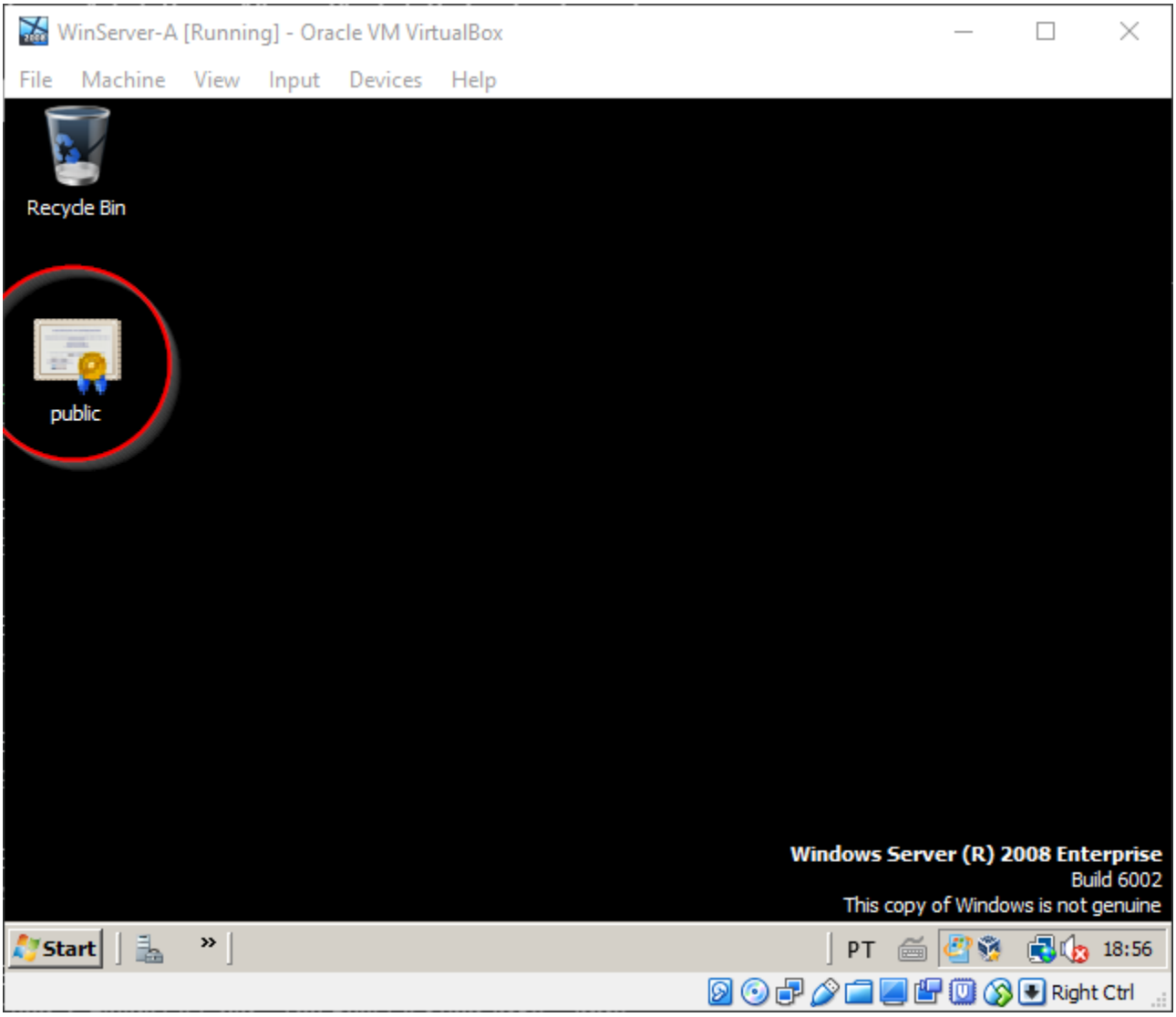

Figura 17. Cópia do certificado da CA do Squid para a máquina WinServer-G

4. Vamos criar uma política para distribuição do certificado copiado. Execute *Start* > *Run...* > `gpmc.msc`. Você deverá ver a tela do *Group Policy Management*, como se segue:

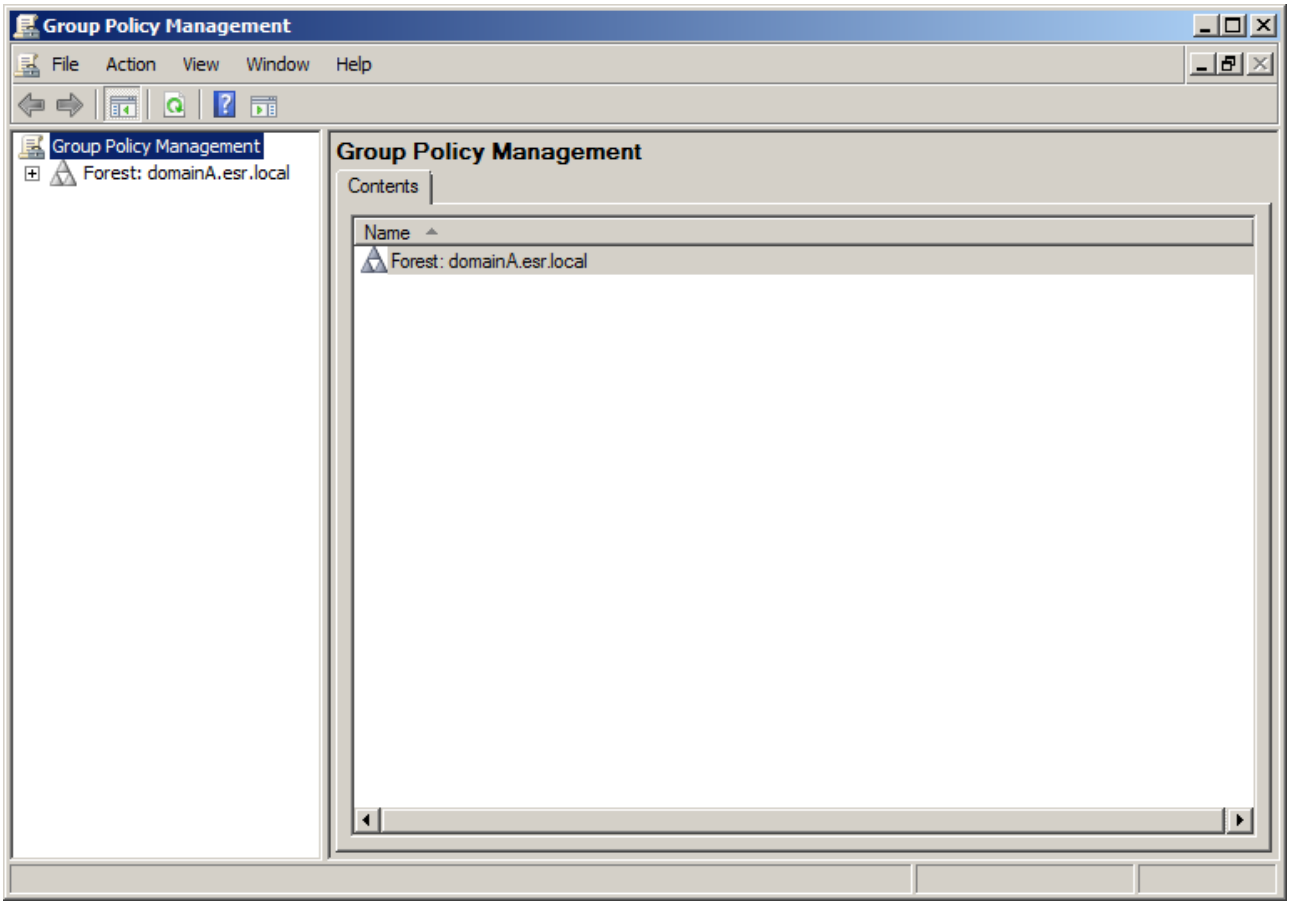

Figura 18. Ferramenta para gestão de políticas no AD

5. Expanda a floresta `domainA.esr.local`, e em seguida *Domains*. Clique com o botão direito no domínio `domainA.esr.local`, e em seguida em *Create a GPO in this domain, and Link it here...*. Para o nome da GPO, digite *squidcert*, e em seguida clique em *OK*. Uma nova política deve surgir na lista do painel direito, como mostrado abaixo:

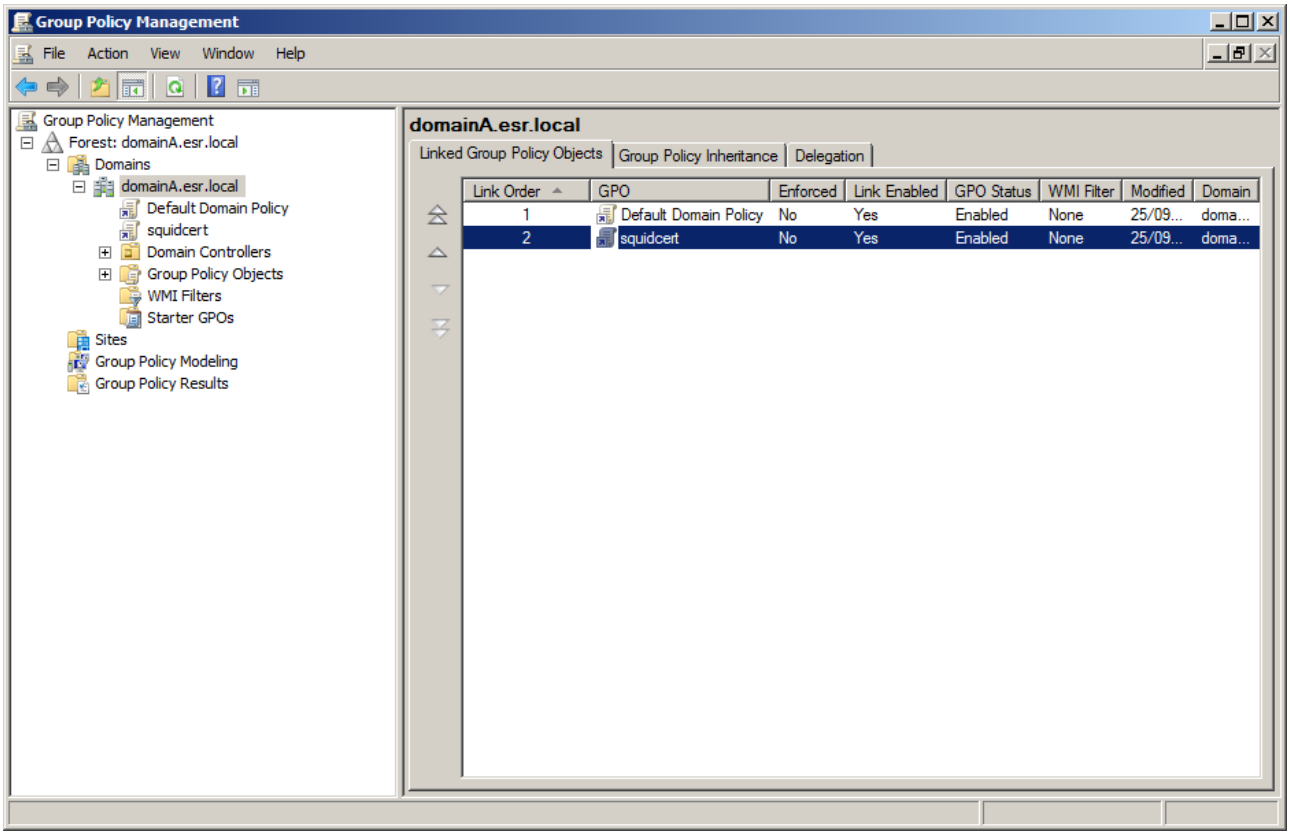

Figura 19. Criação de nova GPO

6. Clique com o botão direito na política *squidcert*, e em seguida em *Edit*. Surgirá uma nova janela para edição de políticas, idêntica à invocada pelo *snap-in* `gpedit.msc`. Navegue para *Computer Configuration* > *Policies* > *Windows Settings* > *Security Settings* > *Public Key Policies*, clique com o botão direito em *Trusted Root Certification Authorities*, como mostrado abaixo. Em seguida, clique em *Import*.

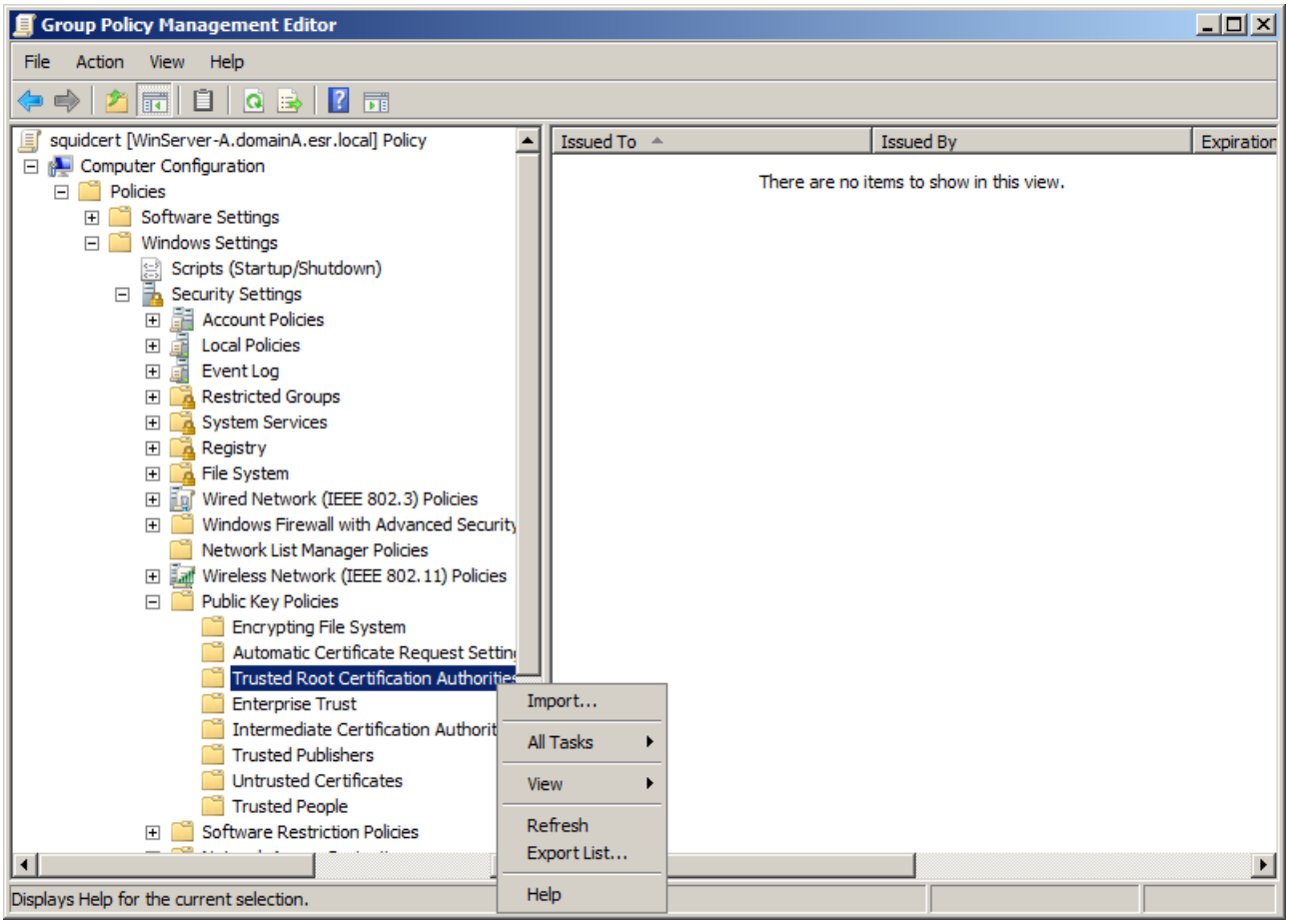

Figura 20. Navegando na tela de edição de políticas

7. Será aberta uma tela de adição de certificado idêntica à que usamos na sessão 7. Aponte o certificado do Squid baixado no passo (3) desta atividade, e confirme todas as janelas de adição do certificado. Ao final, você deverá vê-lo adicionado ao *Trusted Root Certification Authorities* da GPO, como mostrado a seguir.

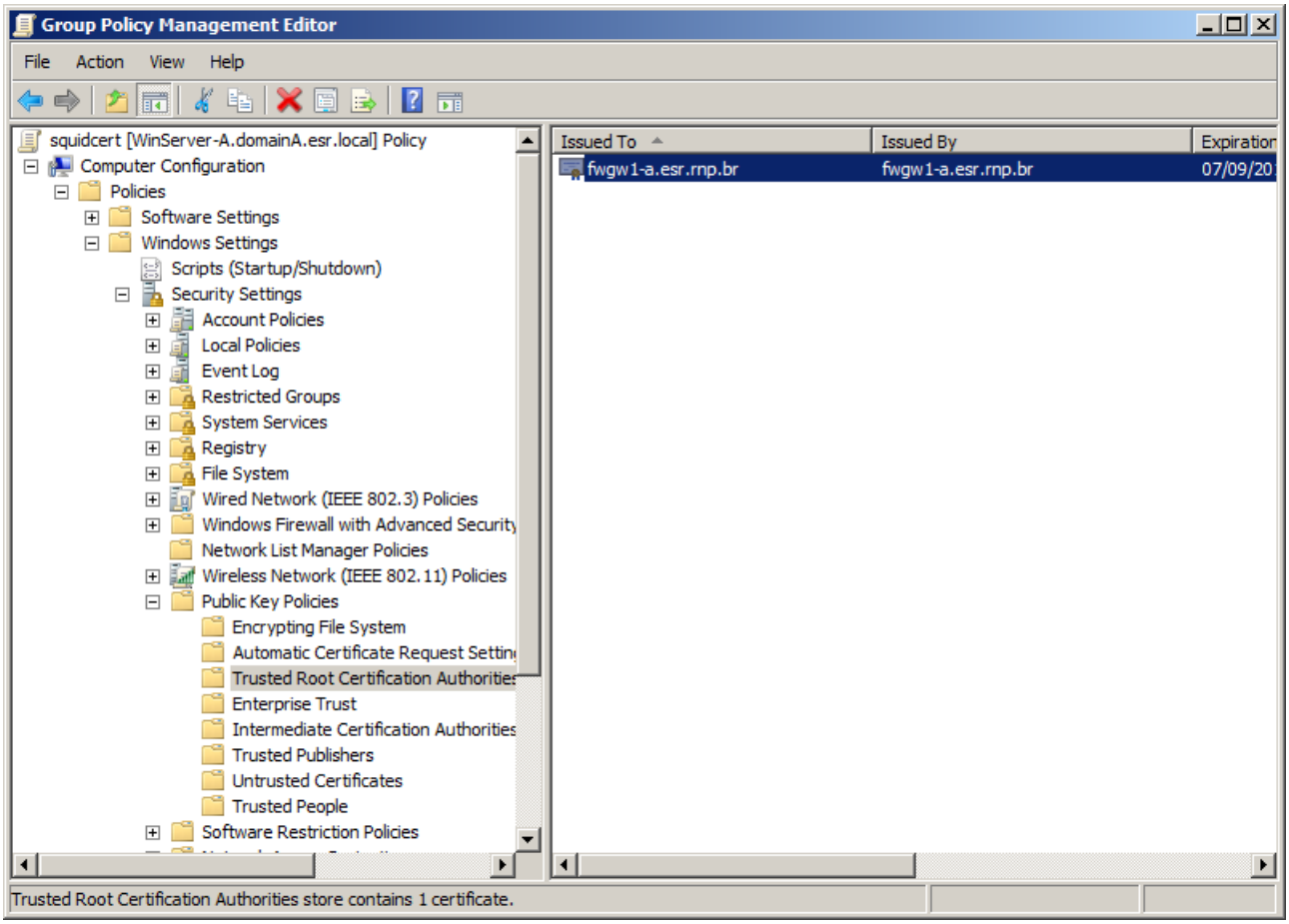

Figura 21. Certificado do Squid adicionado à GPO

8. Tudo pronto! Feche a janela do *Group Policy Management Editor* e do *Group Policy Management*, e volte à máquina *WinClient-G*. Segundo a *knowledge base* da Microsoft (https://msdn.microsoft.com/en-us/library/ms813077.aspx), as GPOs são atualizadas de 90 em 90 minutos, com *offsets* aleatórios de 30 minutos. Como não queremos esperar tudo isso para verificar nossa configuração, abra (novamente, na máquina *WinClient-G*) uma janela do *prompt* de comando e digite `gpupdate /force` para atualizar as GPOs imediatamente:

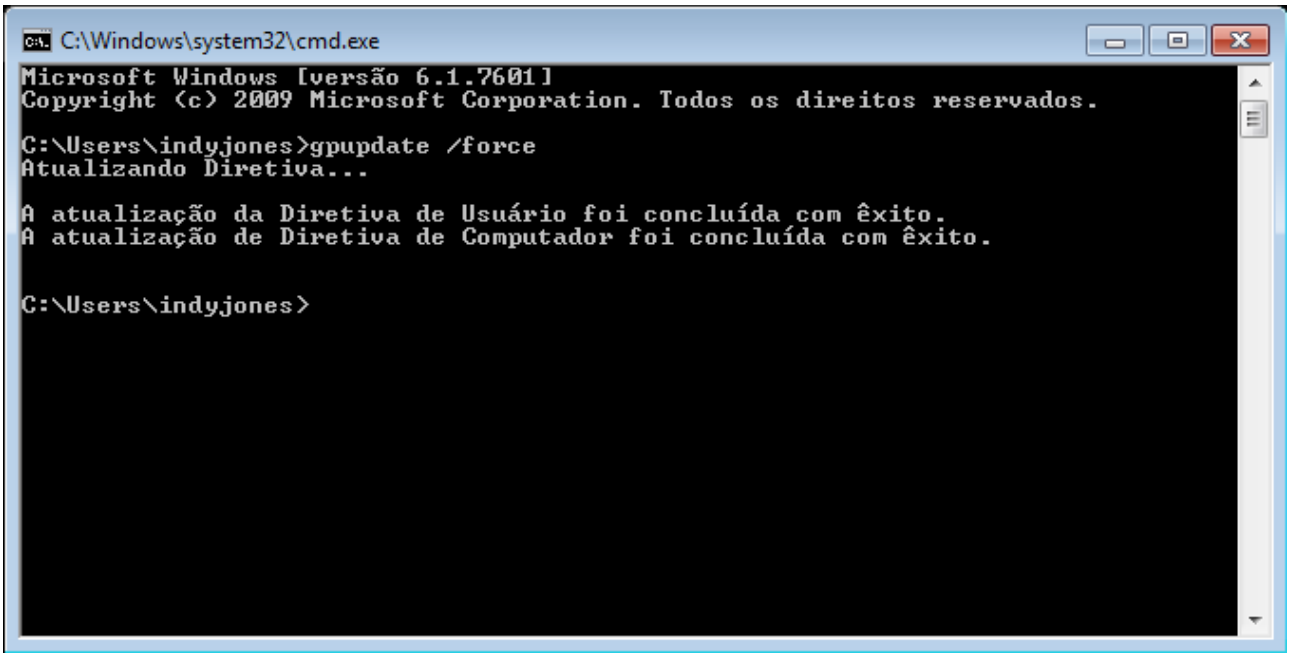

Figura 22. Forçando atualização de GPOs imediatamente

9. Abra o navegador e tente acessar um website em HTTPS, como o https://facebook.com que havia sido acessado anteriormente. Note que, agora, o navegador reporta o certificado forjado pela CA do Squid como confiável.

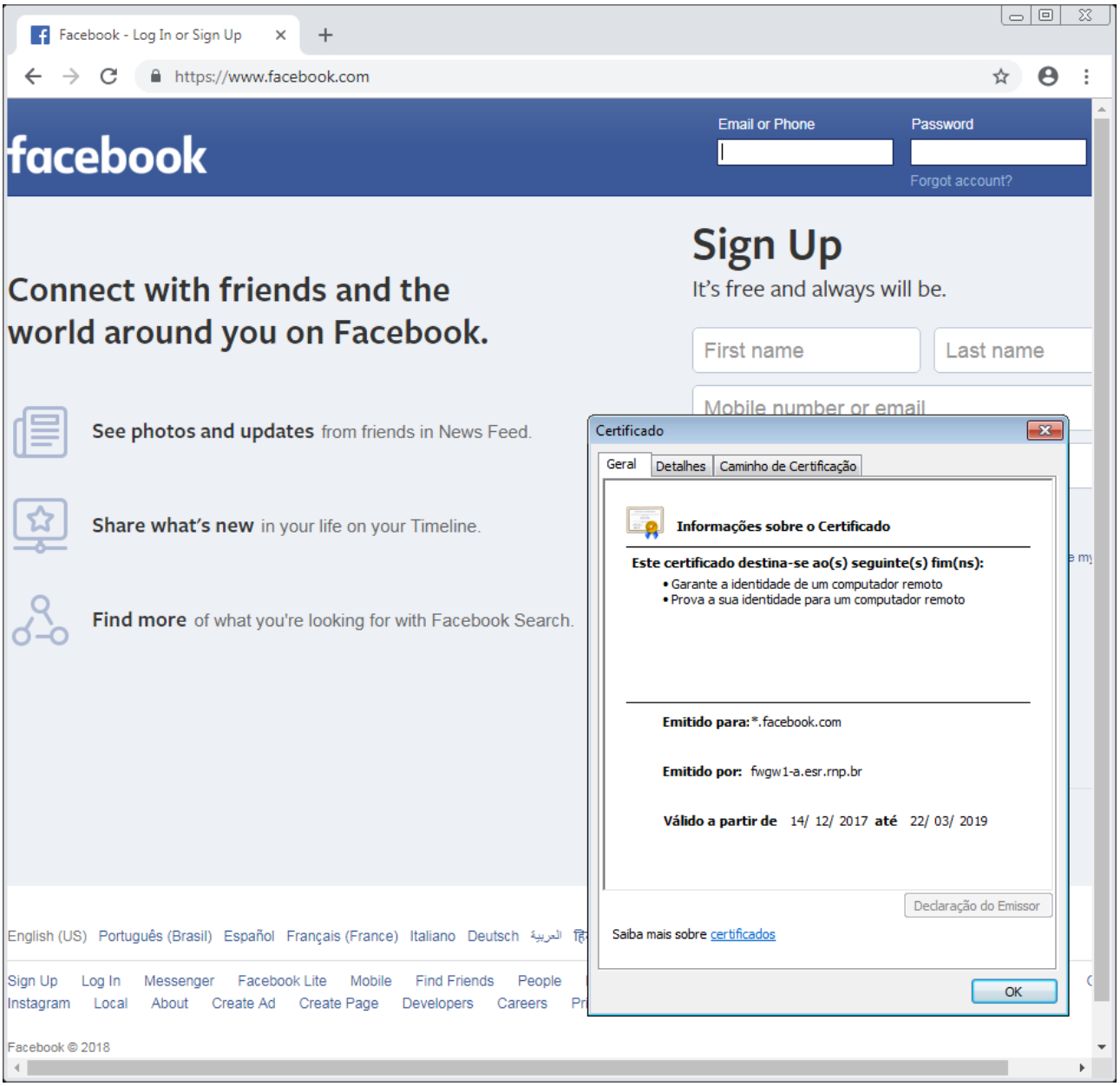

Figura 23. Detecção de certificado da CA do Squid como confiável

10. De fato, verificando a lista de certificados raiz confiáveis do sistema, o da máquina *FWGW1-G* consta da lista.

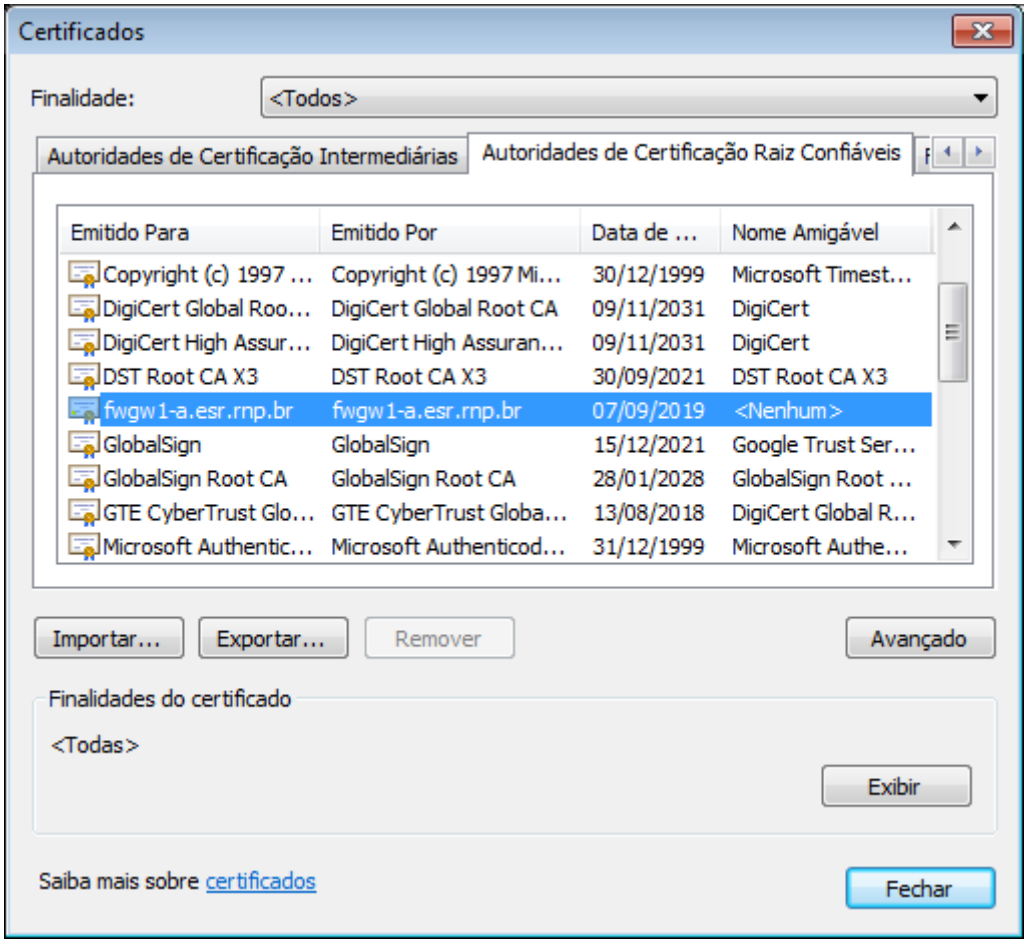

Figura 24. Certificado da CA do Squid adicionado à lista de certificadoras raiz confiáveis

Com efeito, nossa configuração via GPO funcionou corretamente — em um cenário com dezenas de clientes Windows, ou mesmo centenas, você poderia usar um esquema de configuração como este para distribuir o certificado do seu *proxy* de forma imediata.

6) Instalação e configuração do WSUS

Esta atividade será realizada na máquina virtual *WinServer-G*.

1. Acesse a máquina *WinServer-G* como um usuário administrativo (por exemplo, `DOMAINA\Administrator`) e verifique que todos as atualizações de segurança da Microsoft estão aplicadas. Execute *Start* > *Windows Update* e verifique que o servidor está totalmente atualizado, como mostrado abaixo.

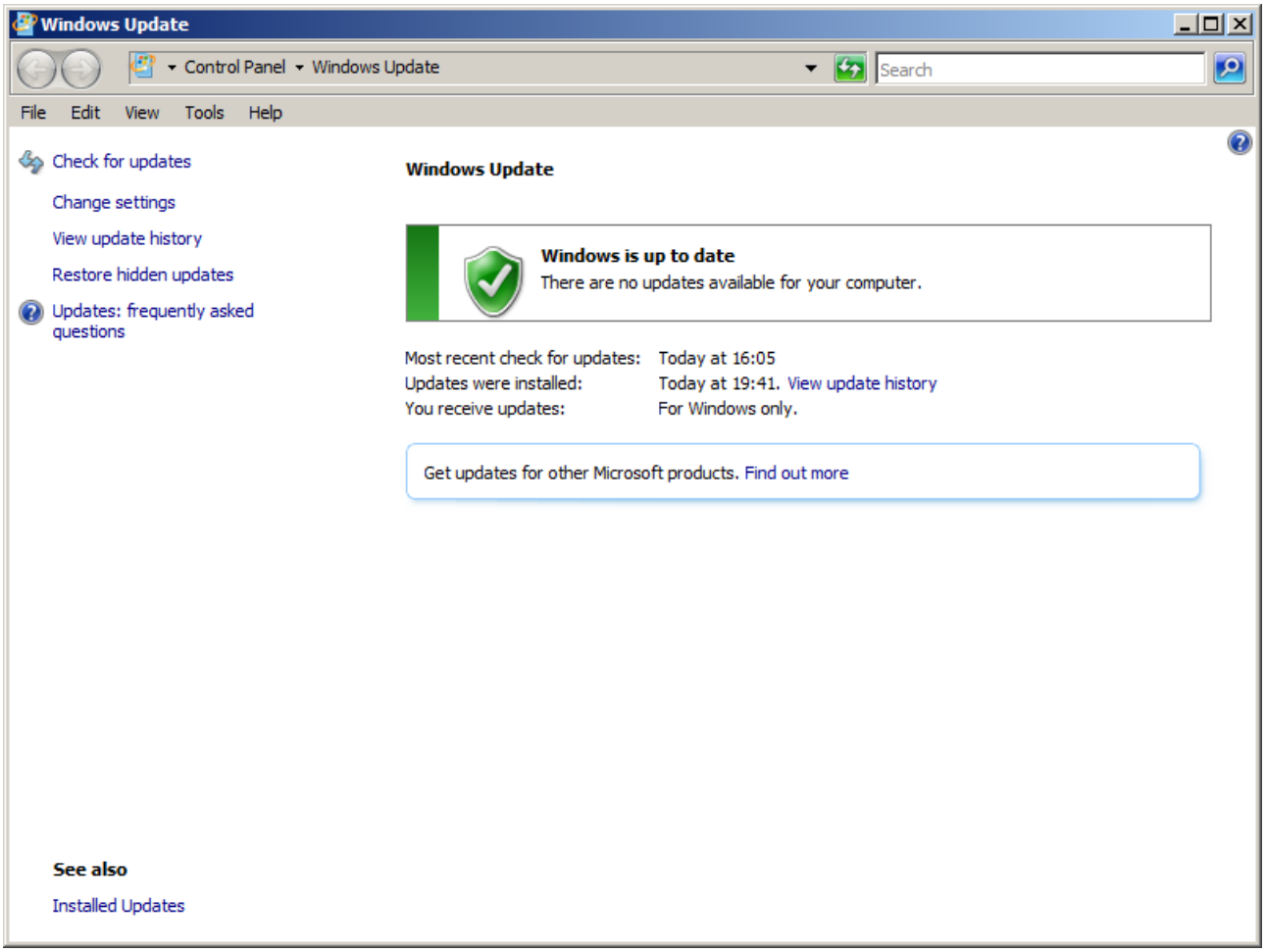

Figura 25. Máquina WinServer-G atualizada

2. Ainda na máquina *WinServer-G*, abra o *Server Manager* e em seguida navegue para *Roles* > *Web Server (IIS)* > *Add Role Services*. Nos serviços abaixo, marque as caixas que se seguem:

    - *Application Development* (aceitando a instalação da dependência *Windows Process Activation Service* > *.NET Environment*):
        - *ASP .NET*
        - *ISAPI Extensions*
        - *ISAPI Filters*
        - *.NET Extensibility*
    - *Performance*:
        - *Dynamic Content Compression*
    - *Security*:
        - *Windows Authentication*

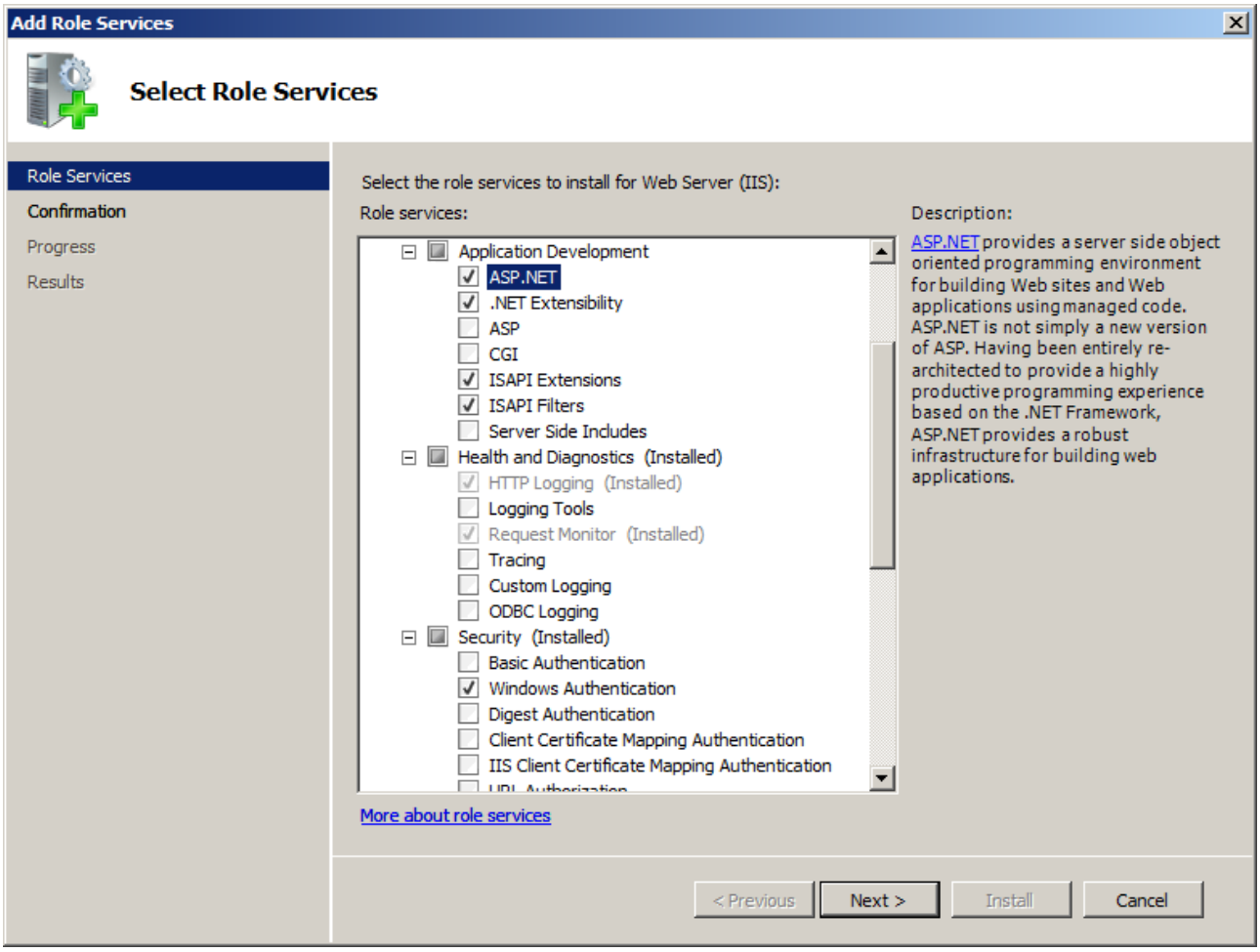

Figura 26. Instalação das dependências do WSUS

Confirme que suas seleções estão corretas e clique em *Next*, e em seguida em *Install*.

3. A seguir, desligue a máquina *WinServer-G*. Iremos adicionar um novo disco para instalação do WSUS no Virtualbox — o procedimento é bastante similar ao que fizemos para a instalação do Nessus na sessão 8.

   Na console administrativa do Virtualbox, selecione a máquina *WinServer-G* e navegue para *Settings* > *Storage* > *SATA Controller* > *Add hard disk*. Na nova tela, selecione *Create new disk*, formato VDI, *Dynamically allocated* e aloque um espaço de 20 GB para o disco, com nome `wsus`. Finalmente, clique em *Create*.

   Ao final do processo, ligue novamente a máquina *WinServer-G*, e faça login como `DOMAINA\Administrator`.

4. Execute *Start* > *Run...* > `diskmgmt.msc`. Imediatamente, o sistema detectará o novo disco e irá sugerir sua inicialização, como mostrado a seguir:

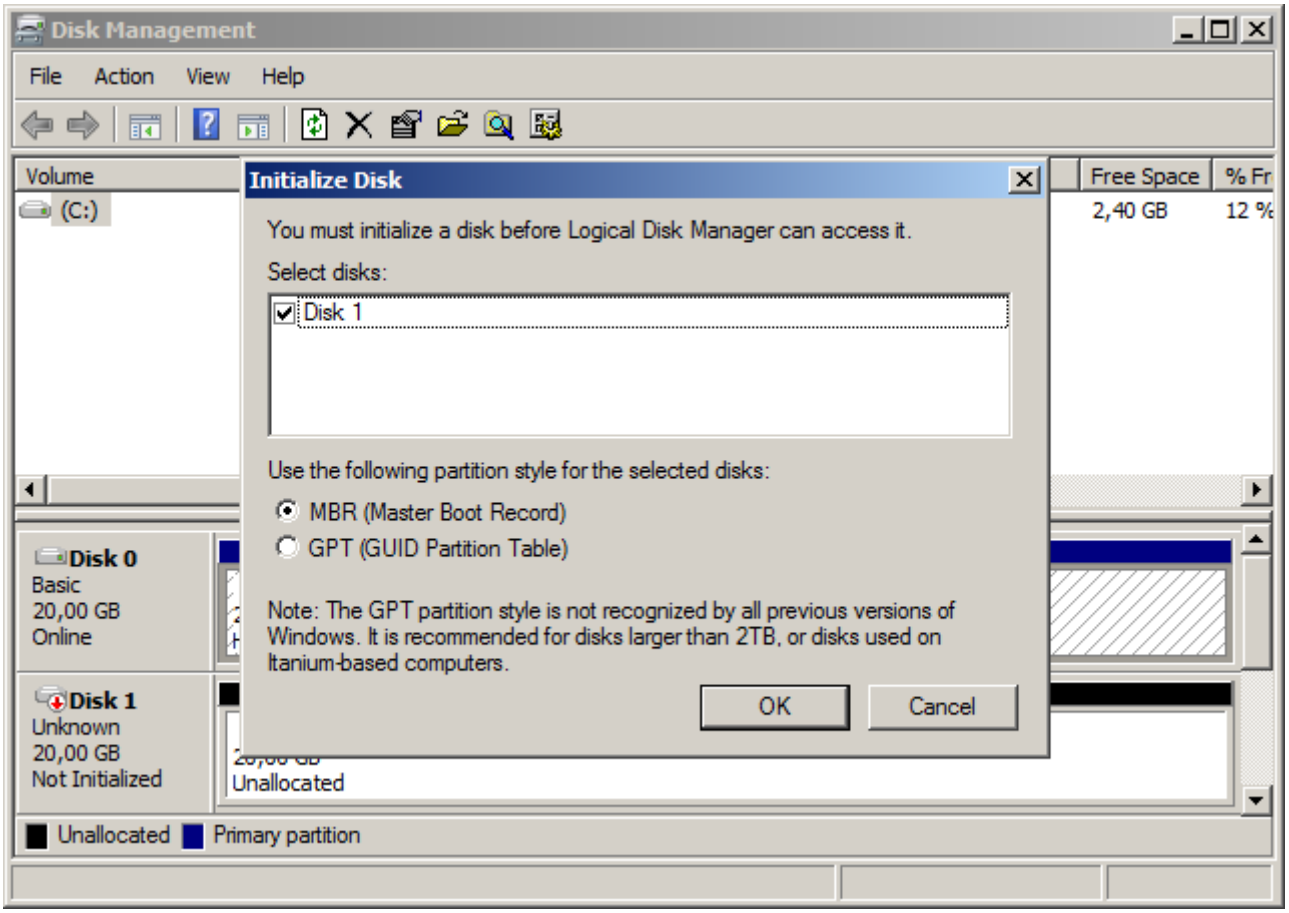

Figura 27. Inicialização do disco para o WSUS

Mantenha marcada a caixa *MBR (Master Boot Record)* e clique em *OK*. Em seguida, clique com o botão direito no novo disco (o nome dele deve ser *Disk 1*), e selecione *New Simple Volume...*.

Na nova janela, clique em *Next*. Na tela *Specify Volume Size*, mantenha o valor máximo de 20477 MB e clique em *Next*. Em *Assign Drive Letter or Path*, mantenha marcada a caixa *Assign the following drive letter* e escolha uma letra não-utilizada do sistema, como `K:` por exemplo.

Em *Format Partition*, mantenha marcada a caixa *Format this volume with the following settings* e escolha:

- *File system*: NTFS
- *Allocation unit size*: *Default*
- *Volume label*: WSUS
- *Perform a quick format*: marcada
- *Enable file and folder compression*: desmarcada

Clique em *Next*. Na tela seguinte, verifique que todas as opções de formatação do volume estão corretas, como se segue:

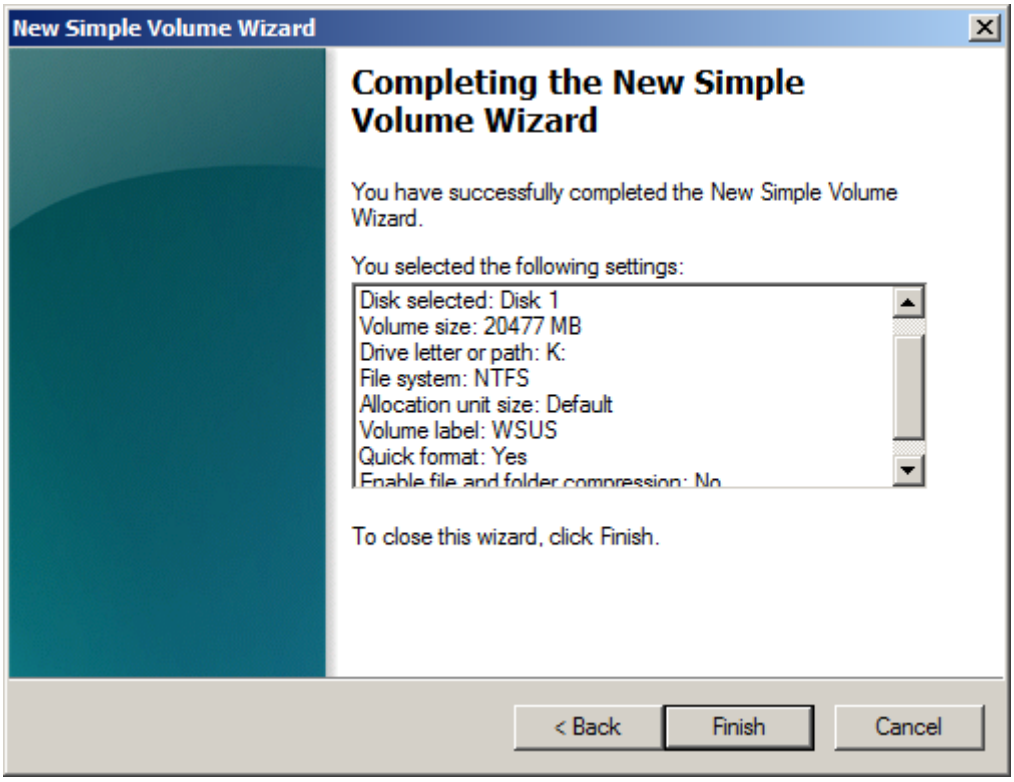

Figura 28. Formatação do volume para o WSUS

Clique em *Finish*. Ao final do processo, feche a janela do *Disk Management* e verifique que o novo volume `K:`, com *label* `WSUS`, está disponível no *Windows Explorer*.

5. Agora, baixe o pacote do *Windows Server Update Services* 3.0 SP2, disponível em https://www.microsoft.com/en-us/download/details.aspx?id=5216 , e inicie sua instalação.

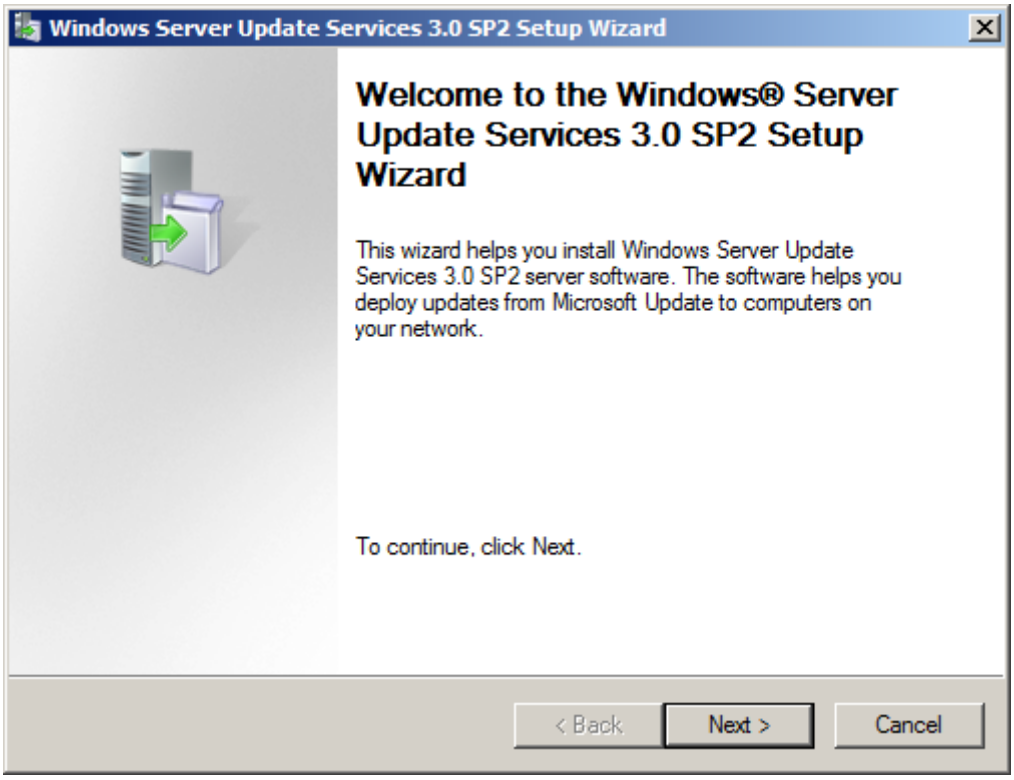

Figura 29. Instalação do WSUS

6. Na tela *Installation Mode Selection*, marque *Full server installation including Administration*

Console e clique em *Next*.

7. Em *License Agreement*, marque a caixa *I accept the terms of the License agreement* e clique em *Next*.
8. Na tela *Required Components to use administration UI*, clique em *Next*. Iremos instalar essa dependência a seguir.
9. Em *Select Update Source*, mantenha a caixa *Store updates locally* marcada, com o valor `K:\WSUS`, como se segue. Clique em *Next*.

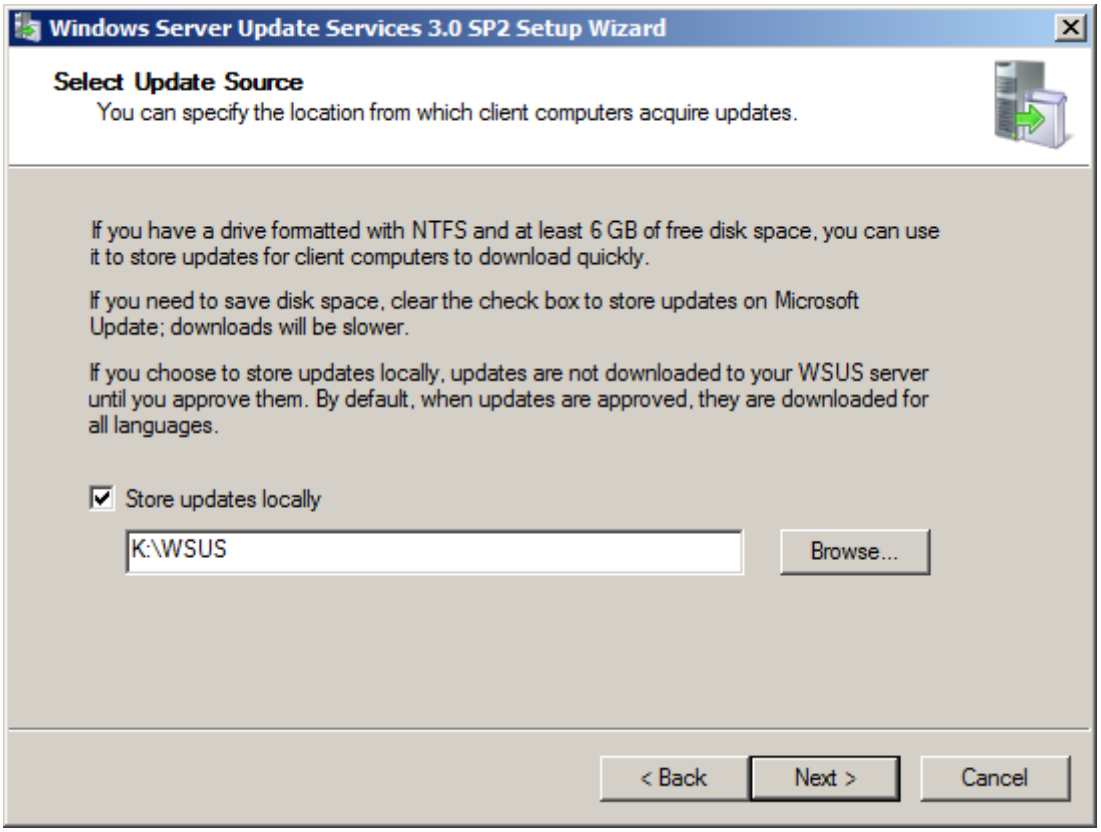

Figura 30. Pasta de download dos arquivos de update do WSUS

10. Na tela *Database Options*, mantenha marcada a caixa *Install Windows Internal Database on this computer* com o valor `K:\WSUS`, e clique em *Next*.
11. Em *Web Site Selection*, mantenha marcada a caixa *Use the existing IIS Default Web site (recommended)* e clique em *Next*.
12. Na tela *Ready to Install Windows Server Update Services 3.0 SP2*, verifique as opções de instalação como mostrado a seguir. Se tudo estiver correto, clique em *Next*.

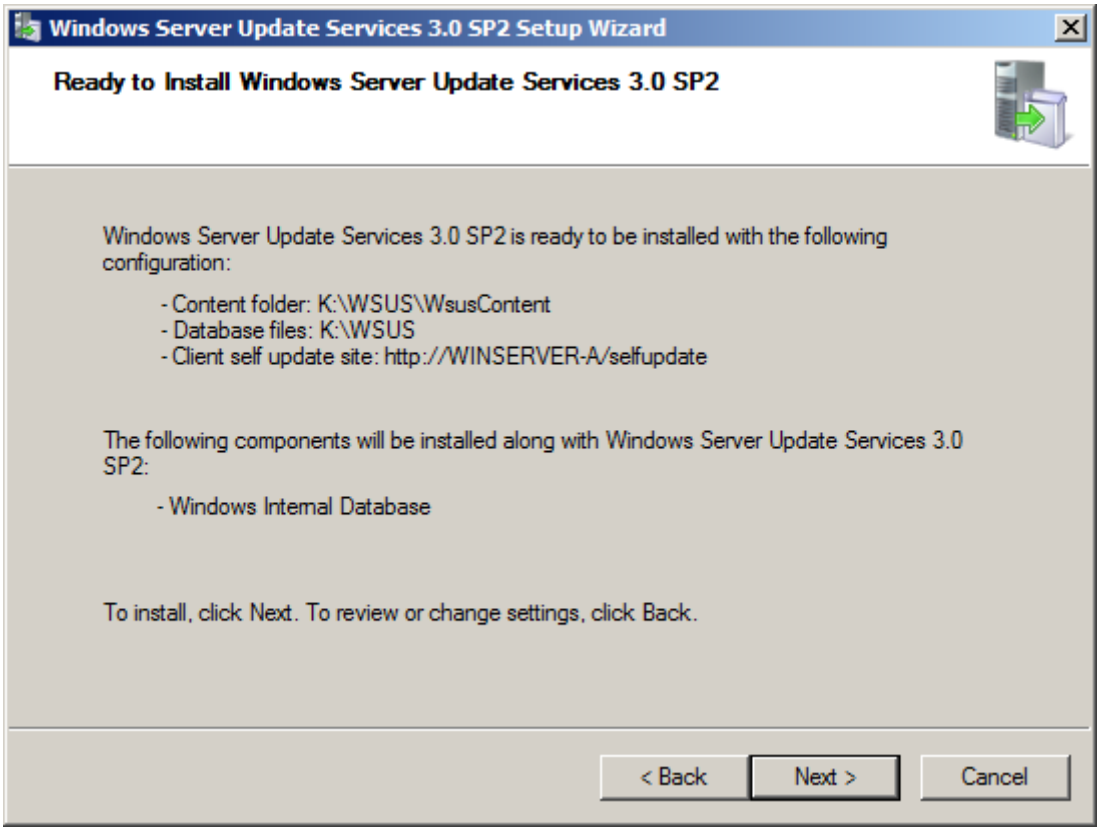

Figura 31. Revisão das opções de instalação do WSUS

Aguarde o processo de instalação do WSUS. Ao final, clique em *Finish*.

13. Após a instalação será aberto o *Windows Server Update Services Configuration Wizard*, como mostrado abaixo. Clique em *Next*.

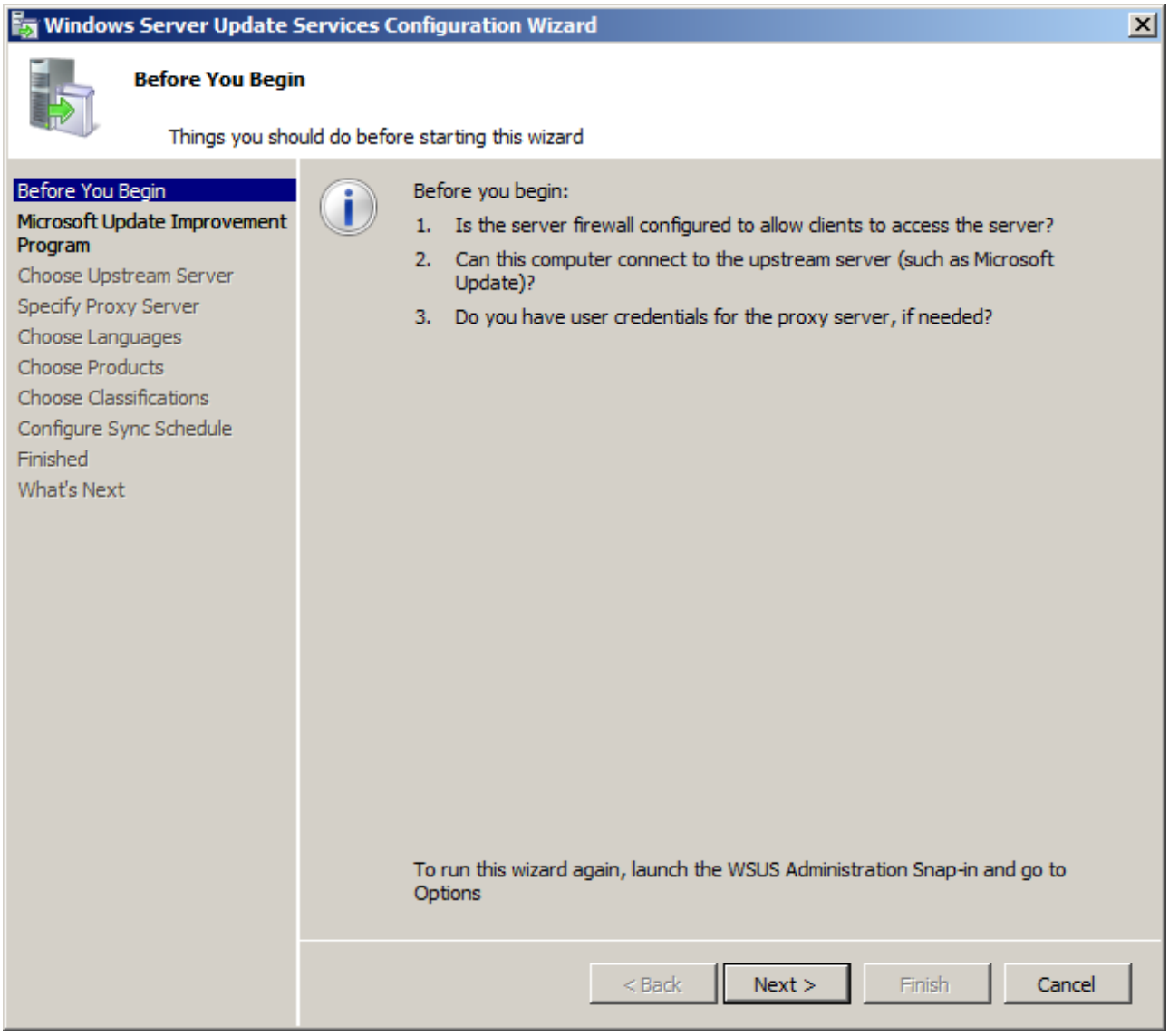

Figura 32. Configuração do WSUS

14. Na tela *Join the Microsoft Update Improvement Program*, desmarque a caixa *Yes, I would like to join the Microsoft Update Improvement Program* e clique em *Next*.
15. Em *Choose Upstream Server*, mantenha marcada a caixa *Synchronize from Microsoft Update* e clique em *Next*.
16. Na tela *Specify Proxy Server*, apenas clique em *Next*.
17. Em *Connect to Upstream Server*, clique no botão *Start Connecting*. O configurar irá conectar-se à Microsoft para fazer o download de tipos de atualizações disponíveis, produtos que podem ser atualizados e linguagens disponíveis. Esse processo pode demorar alguns minutos.

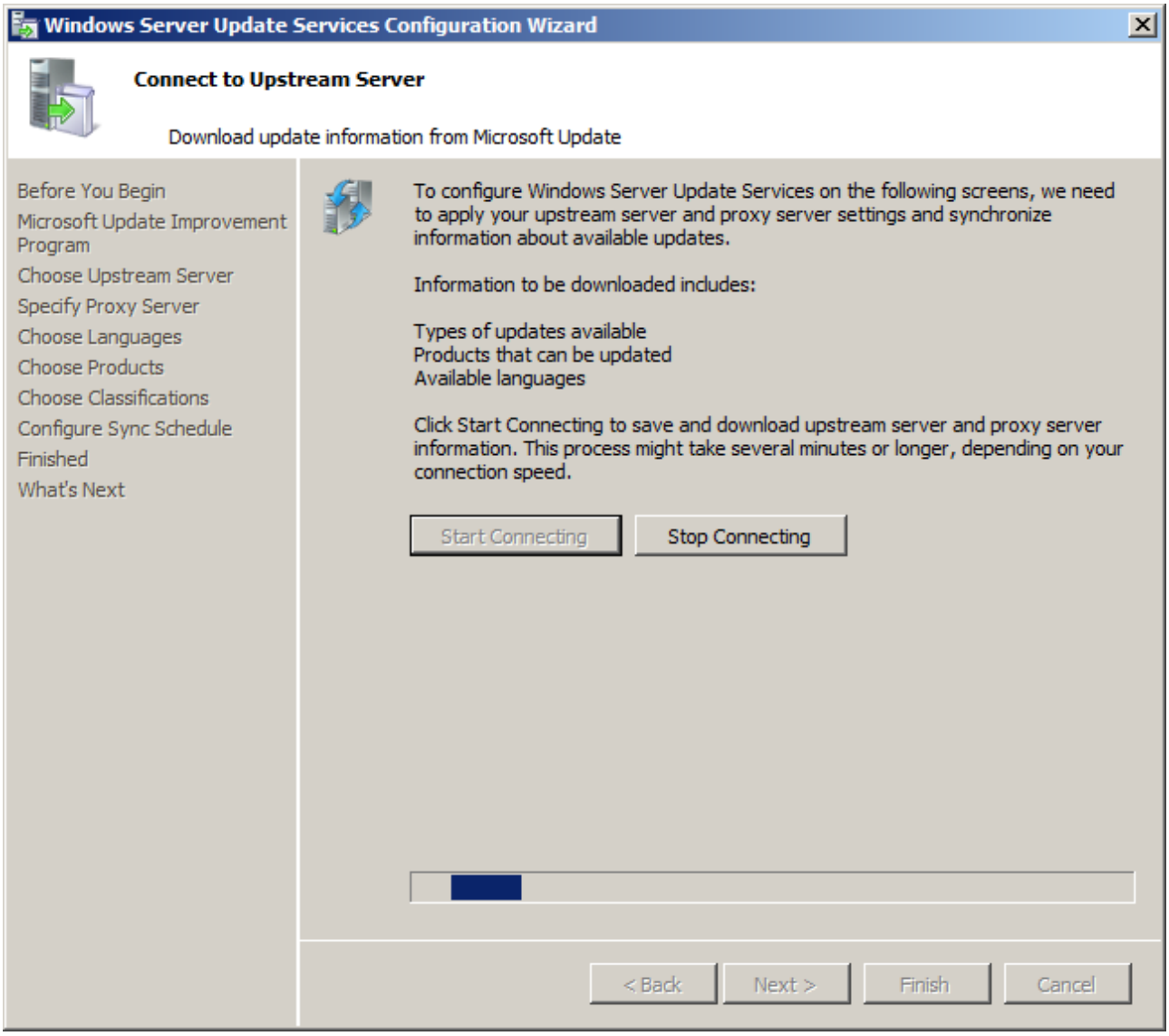

Figura 33. Atualização da base de updates do WSUS

Ao final do procedimento, clique em *Next*.

18. Iremos fazer o download de atualizações para a máquina *WinServer-G* (Windows Server 2008 x86, idioma Inglês-EUA) e *WinClient-G* (Windows 7 x64, idioma Português-Brasil). Assim, na tela *Choose languages*, marque a caixa *Download updates only in these languages* e marque os idiomas *English* e *Portuguese (Brazil)*. Clique em *Next*.
19. Em *Choose Products*, desmarque todas as atualizações do Office e do Windows. Pontualmente, marque apenas as caixas *Windows* > *Windows 7* e *Windows* > *Windows Server 2008*, como mostrado a seguir. Clique em *Next*.

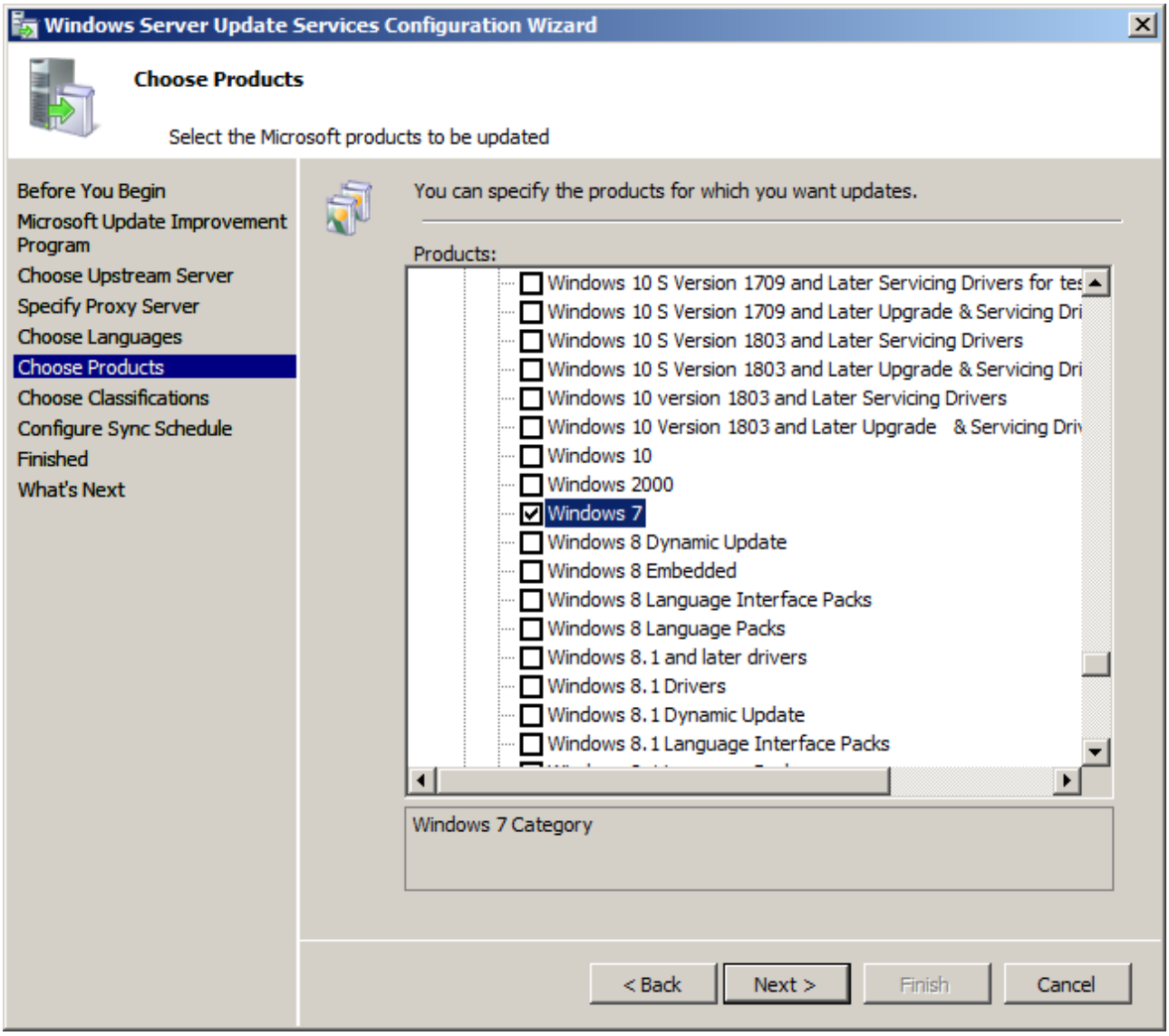

Figura 34. Escolha de produtos para download de atualizações

20. Na tela *Choose Classifications*, marque as caixas *Critical Updates*, *Definition Updates*, *Security Updates* e *Service Packs*. Clique em *Next*.

21. Em *Set Sync Schedule* é possível agendar a atualização periódica e automática da base de atualizações a partir do site da Microsoft. Já que neste laboratório estamos configurando apenas um ambiente de testes, mantenha a caixa *Synchronize manually* marcada e clique em *Next*.

22. Na tela *Finished*, desmarque a caixa *Launch the Windows Server Update Services Administration Console* e mantenha marcada a caixa *Begin initial synchronization*. Clique em *Finish*.

23. Para visualizar os relatórios do WSUS, faça o download do *Microsoft Report Viewer 2008 Redistributable* em https://www.microsoft.com/en-us/download/details.aspx?id=6576 , e instale-o. Aceite todas as opções padrão do instalador.

24. Abra a console de configuração do *Windows Server Update Services* — abra o menu *Start* e pesquise pelo termo `update` para encontrar o programa. Você deverá ver a tela abaixo:

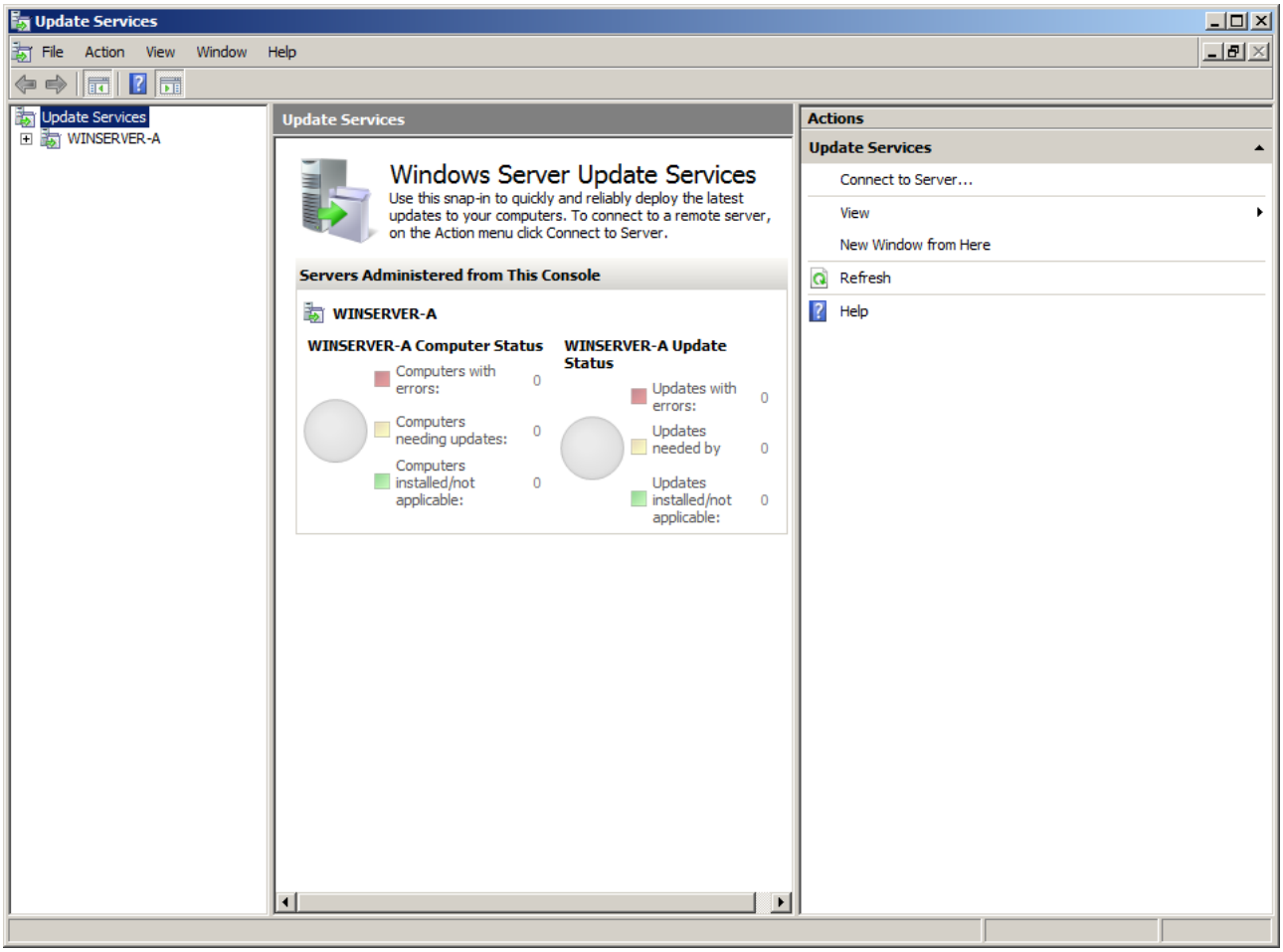

Figura 35. Console administrativa do WSUS

Para verificar o estado da sincronização iniciada no passo (22), navegue para *WINSERVER-G* > *Synchronizations*. Ao final da sincronização você deverá ver o processo concluído com sucesso, como se segue:

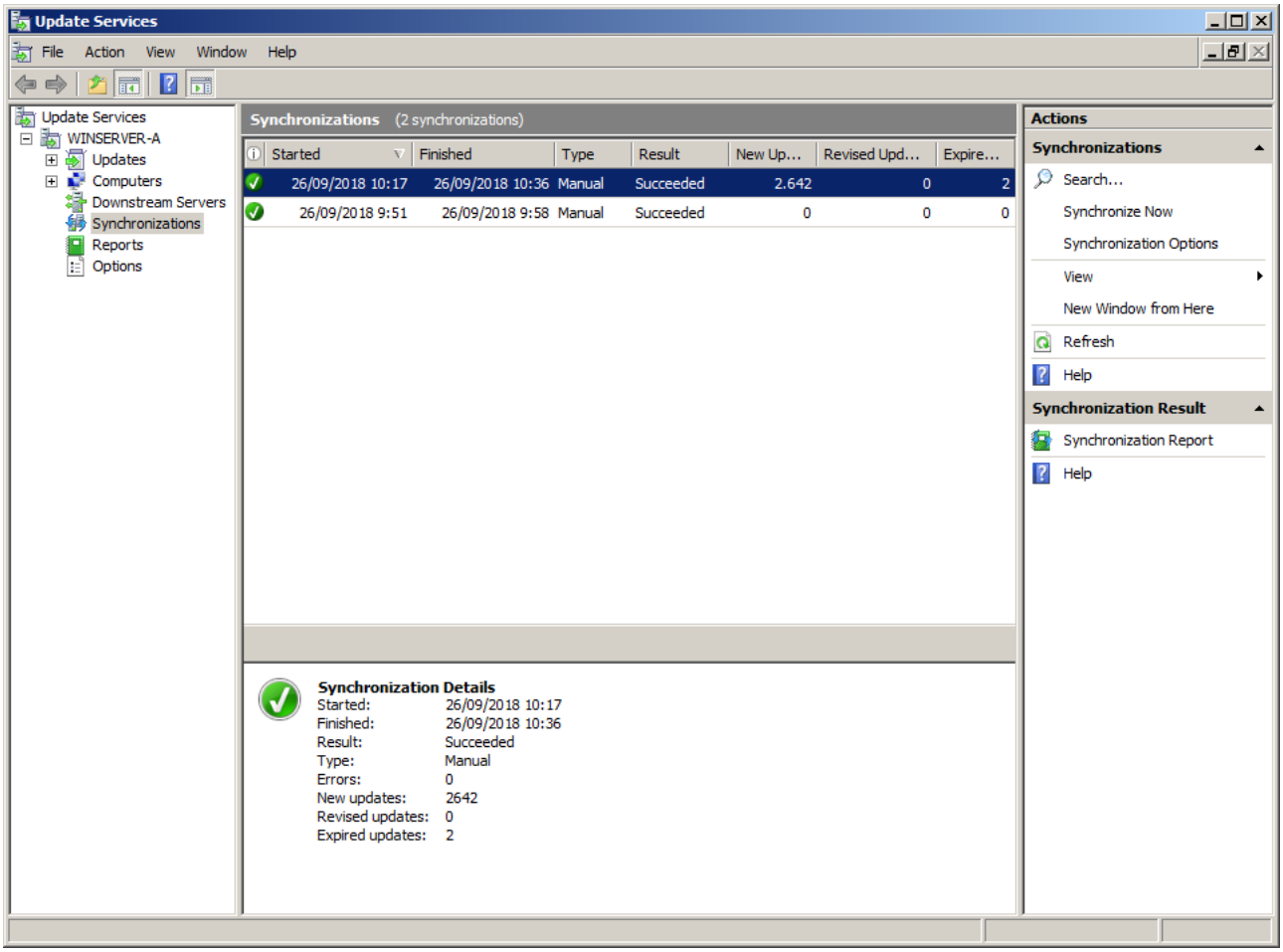

Figura 36. Sincronização do WSUS realizada com sucesso

Finalmente, feche a console de configuração do *Windows Server Update Services*.

25. Antes de utilizar plenamento o WSUS, é necessário atualizar novamente sua máquina *WinServer-G* usando o *Windows Update*. A atualização KB2720211 (https://support.microsoft.com/en-us/help/2720211/), de 8/6/2011, é necessária para atualização dos canais de comunicação do WSUS com os clientes de atualização.

    Ao final da atualização, reinicie a máquina *WinServer-G* para concluir o processo.

7) Configuração de clientes no WSUS

Esta atividade será realizada nas máquinas virtuais *WinServer-G* e *WinClient-G*.

1. Vamos criar uma política para atualização automática de clientes a partir de nosso servidor WSUS. Execute *Start* > *Run...* > `gpmc.msc`. Você deverá ver a tela do *Group Policy Management*, como na atividade (5).

    Expanda a floresta `domainA.esr.local`, e em seguida *Domains*. Clique com o botão direito no domínio `domainA.esr.local`, e em seguida em *Create a GPO in this domain, and Link it here...*. Para o nome da GPO, digite *wsus*, e em seguida clique em *OK*. Uma nova política deve surgir na lista do painel direito, como mostrado abaixo:

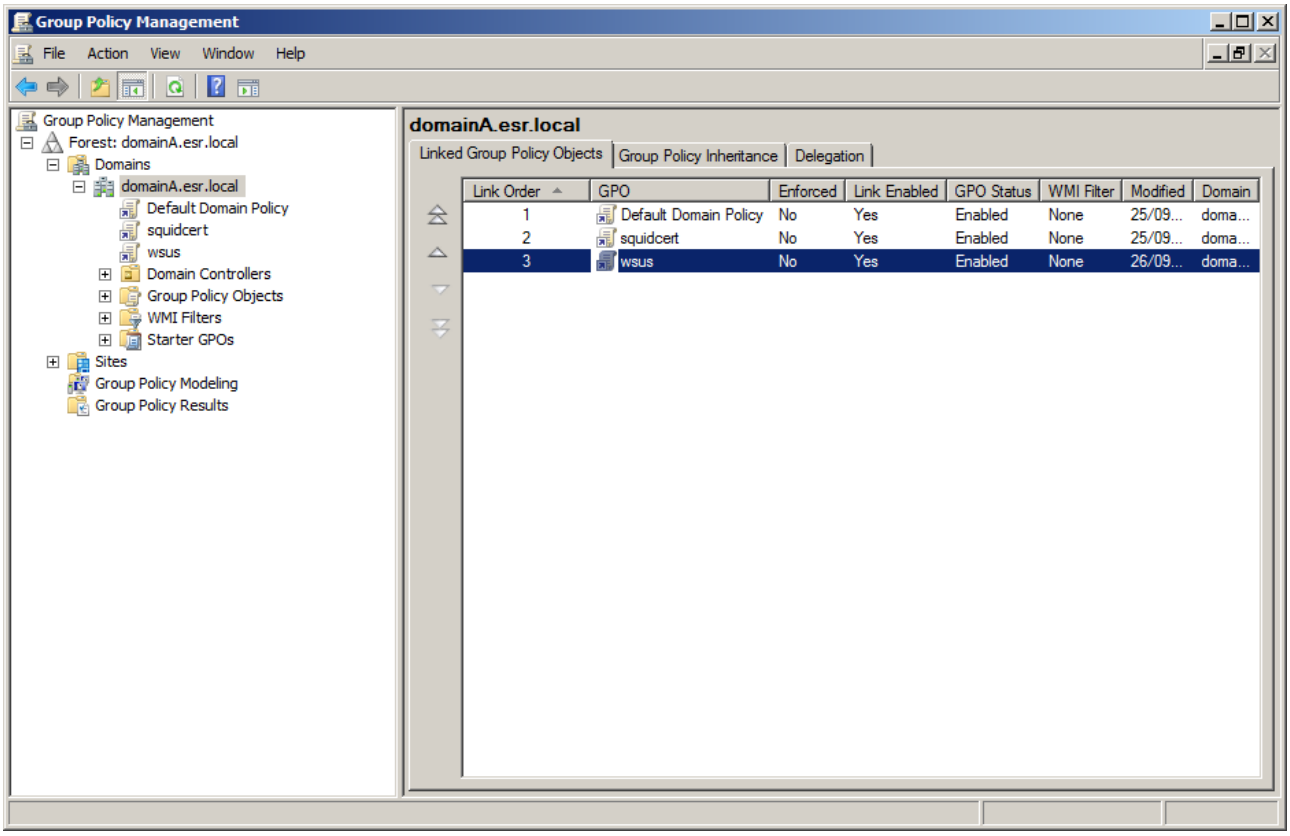

Figura 37. Criação de política para o WSUS

2. Clique com o botão direito sobre a política *wsus*, e em seguida em *Edit*. Navegue para *Computer Configuration* > *Policies* > *Administrative Templates* > *Windows Components* > *Windows Update*. Em seguida, clique duas vezes sobre a diretiva de configuração *Configure Automatic Updates*.

   Marque a caixa *Enabled*, e em seguida escolha:

   - *Configure automatic updating*: *3 - Auto download and notify for install*
   - *Scheduled install day*: *0 - Every day*
   - *Scheduled install time*: *03:00*

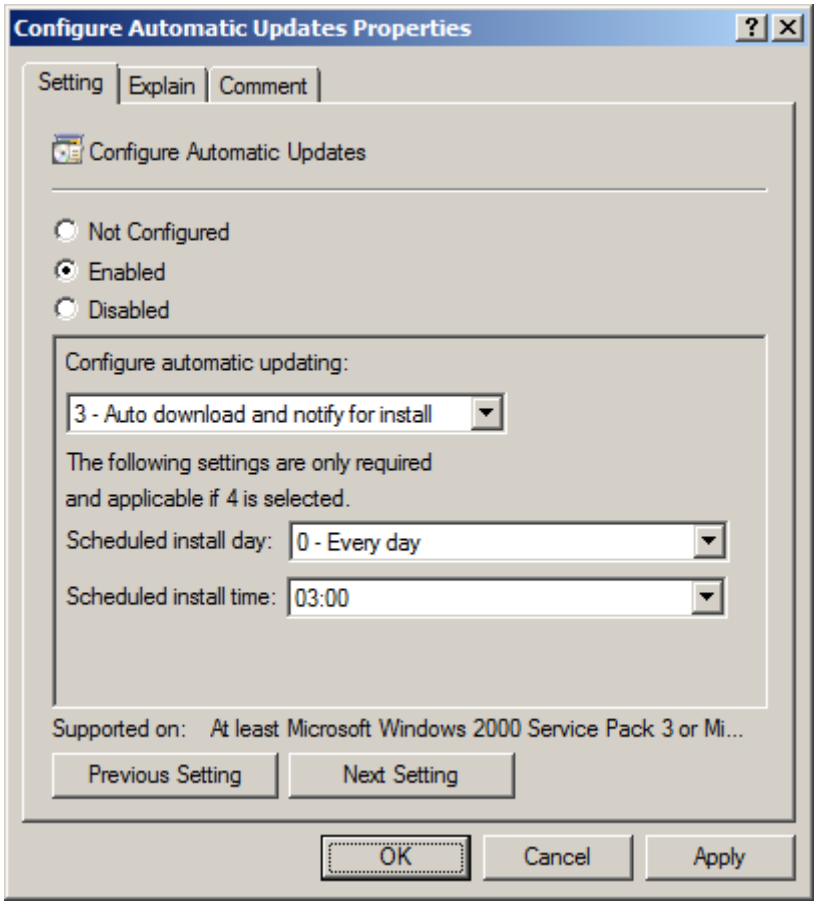

Figura 38. Configuração de atualizações automáticas via GPO

Clique em *OK*.

3. De volta à tela de edição de GPOs, clique duas vezes sobre a diretiva de configuração *Specify intranet Microsoft update service location*.

   Marque a caixa *Enabled*, e em seguida escolha:

   - *Set the intranet update service for detecting updates*: `http://172.16.1.20`
   - *Set the intranet statistics server*: `http://172.16.1.20`

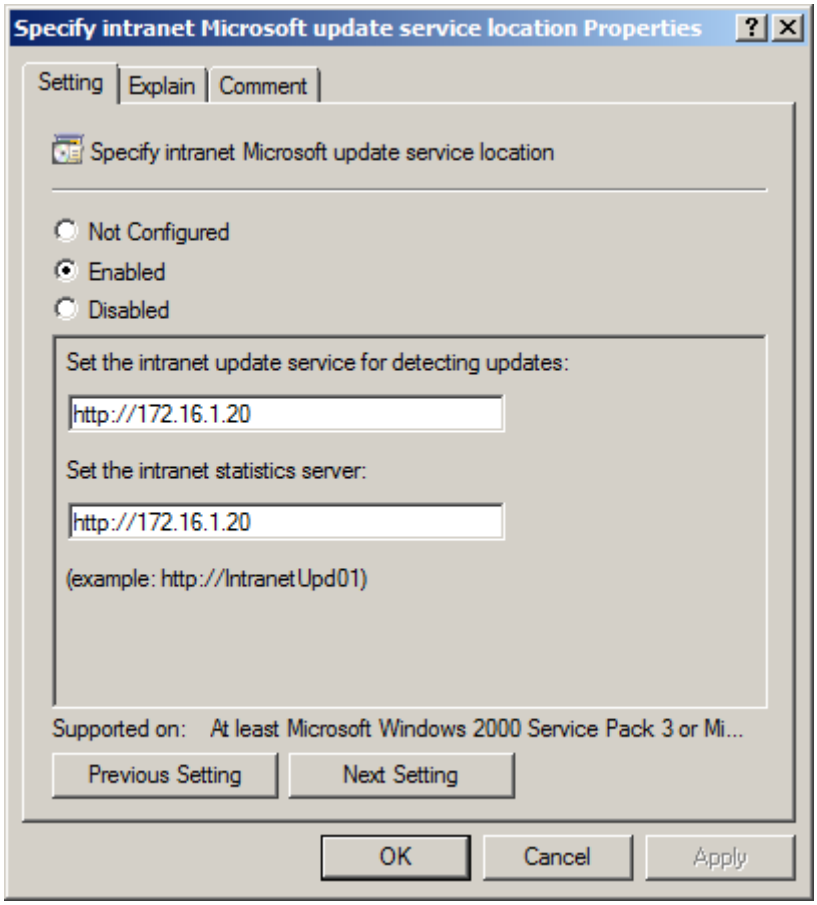

Figura 39. Configuração de servidor remoto para download de atualizações

Clique em *OK*.

4. Feche as janelas de configuração das GPOs. Como anteriormente, sabemos que as GPOs são atualizadas de 90 em 90 minutos, com *offsets* aleatórios de 30 minutos — para não aguardar esse intervalos, acesse a máquina *WinClient-G*, abra uma janela do *prompt* de comando e digite `gpupdate /force` para atualizar as GPOs imediatamente. Para iniciar o contato imediato da máquina com o servidor WSUS, digite `wuauclt.exe /detectnow`.

   Feito isso, abra o *Windows Update* e verifique se há novas atualizações para a máquina *WinClient-G*:

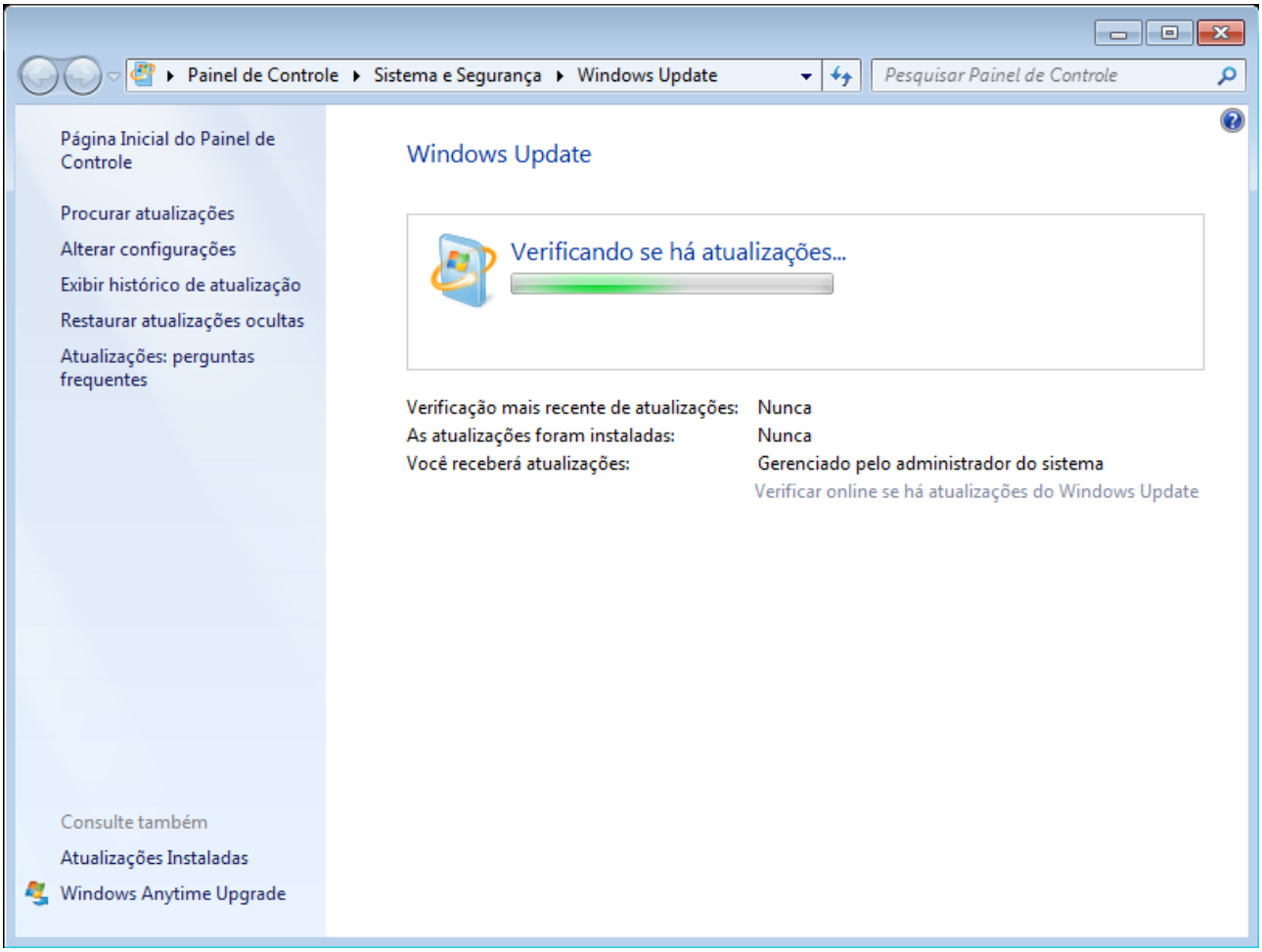

Figura 40. WinClient-G verificando se existem novas atualizações

Ao final do processo, a máquina irá reportar-se como atualizada. Isso é parcialmente verdade, como veremos a seguir.

5. De volta à máquina *WinServer-G*, abra a console de configuração do *Windows Server Update Services* e navegue para *WINSERVER-G* > *Computers* > *All Computers*. O estado de atualização da máquina *WinClient-A* será mostrado num gráfico no centro da tela, como na imagem a seguir:

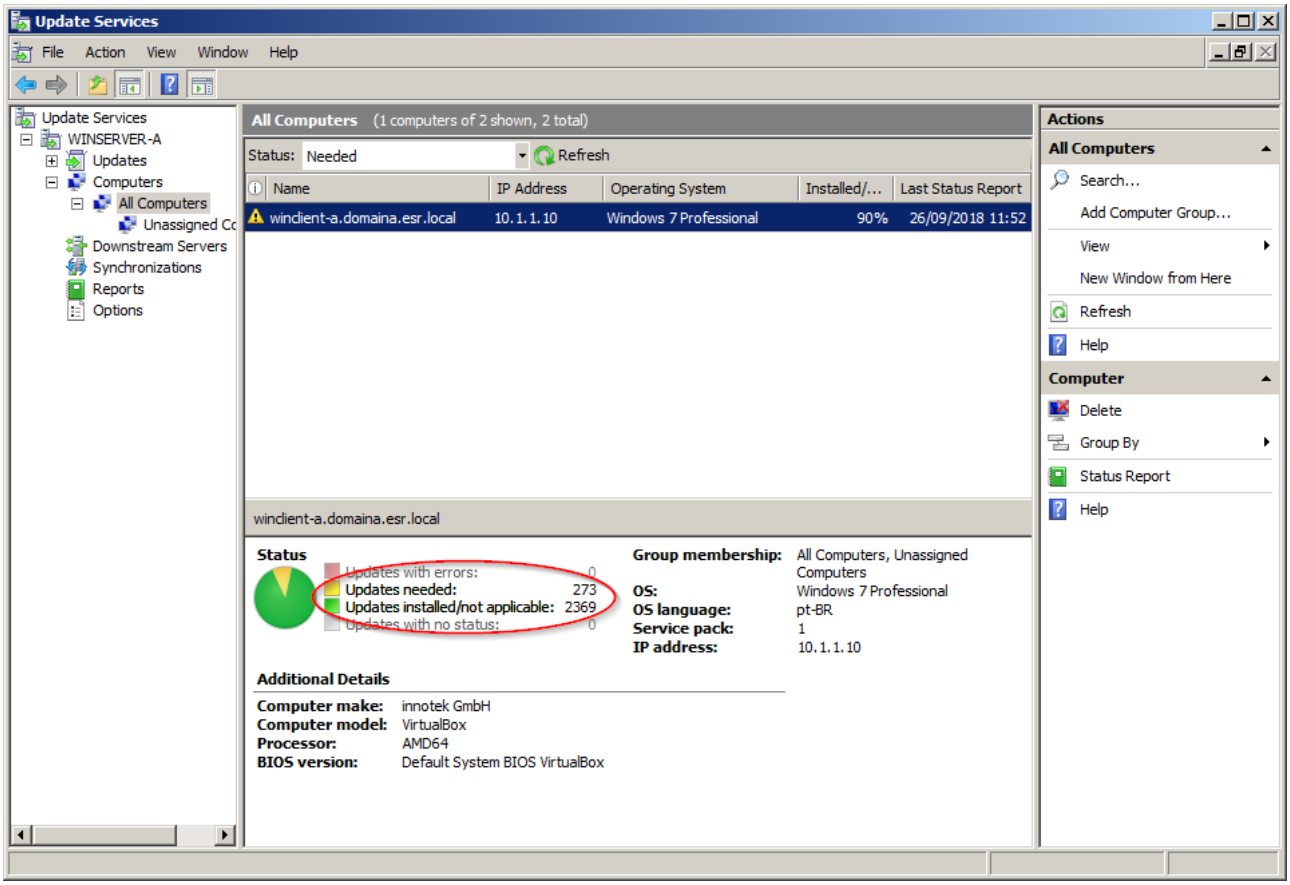

Figura 41. Status de atualização da máquina WinClient-G

Observe que a máquina *WinClient-G* possui 2369 atualizações realizadas e 273 ainda não aplicadas, e com o *service pack* 1 instalado. No WSUS, a gestão de atualizações é feita de forma centralizada pelo administrador — pode-se agrupar máquinas em grupos de trabalho, e habilitar/desabilitar atualizações pontualmente para essas máquinas e grupos. Para gerenciar a aprovação de atualizações, navegue para *WINSERVER-A* > *Updates* > *All Updates*. Ajuste o filtro para condição *Unapproved* e estado *Failed or Needed*, e clique em *Refresh*. Você deverá ver algo semelhante a tela a seguir:

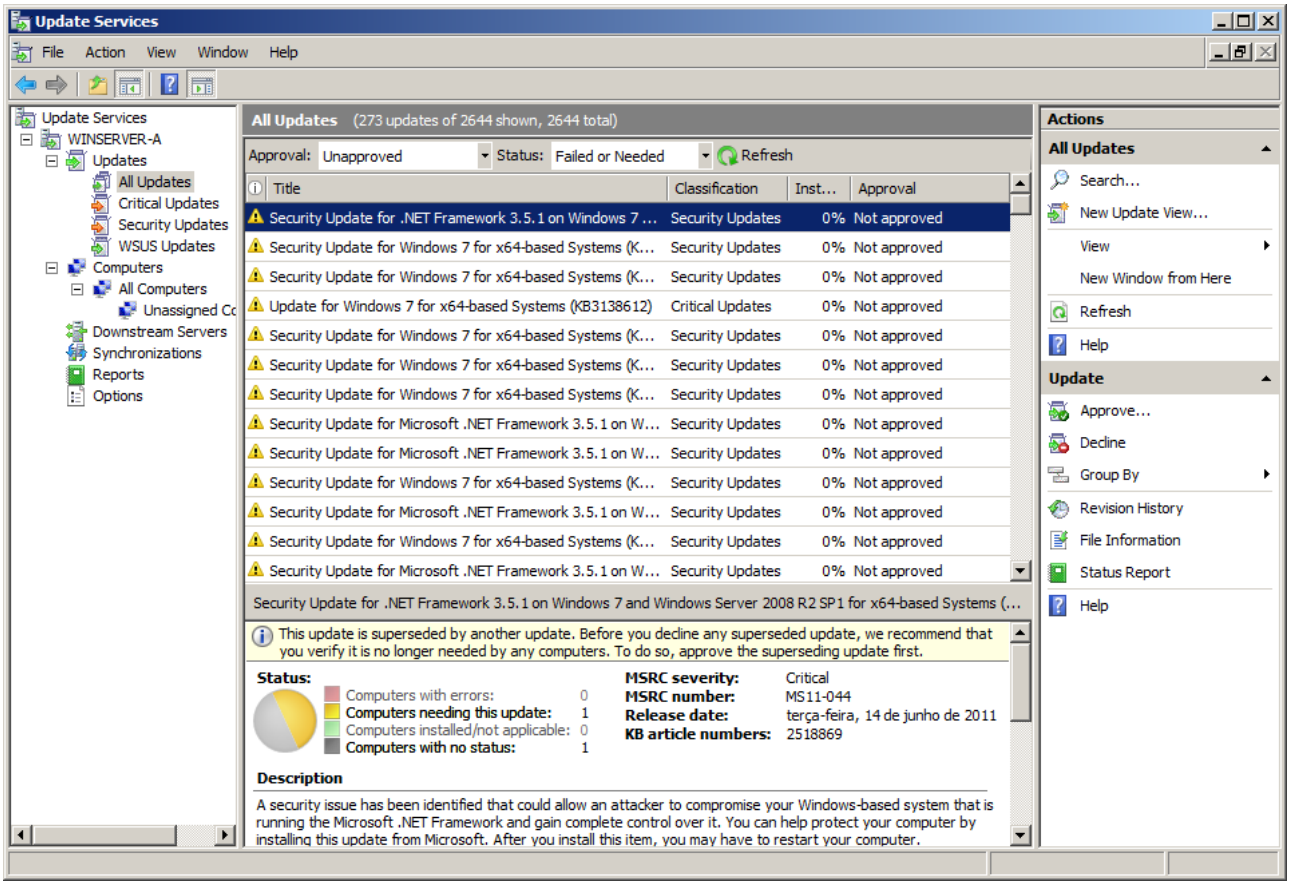

Figura 42. Aprovação de atualizações no WSUS, parte 1

Aprove todas as atualizações. Selecione-as usando SHIFT e no painel direito, clique em *Actions* > *Update* > *Approve...*. Na nova janela, clique no quadrado à esquerda de *All Computers* e marque *Approved for Install*; faça o mesmo para o grupo abaixo, *Unassigned Computers*, e clique em *OK*. O WSUS iniciará o processo de aprovação das atualizações, como mostrado abaixo:

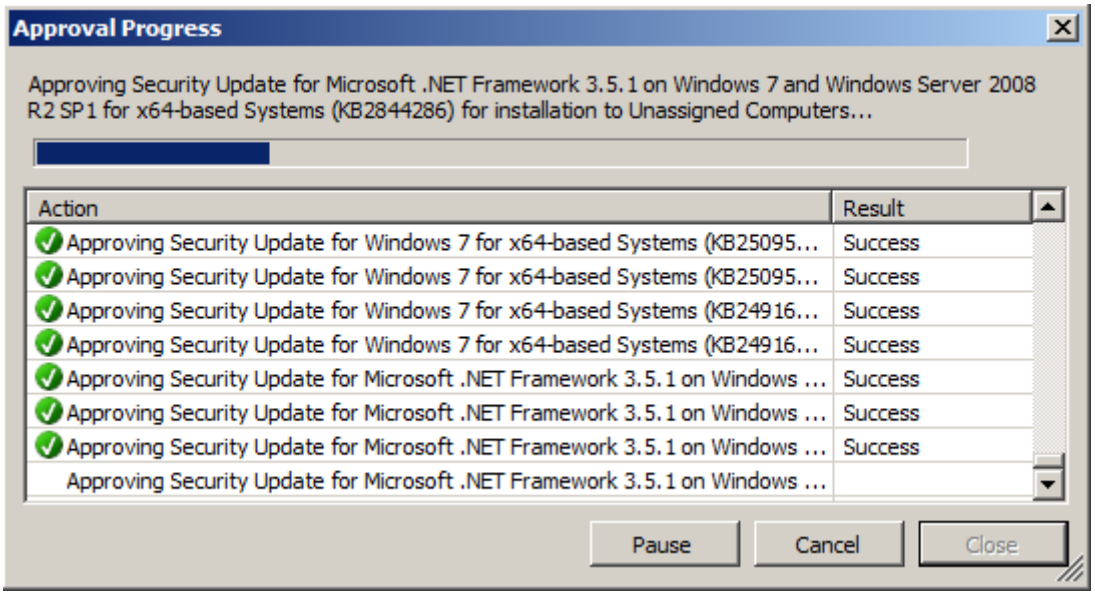

Figura 43. Aprovação de atualizações no WSUS, parte 2

Ao final do processo, clique em *Close*.

6. De volta à máquina *WinClient-G*, verifique novamente por atualizações usando o *Windows Update*. Normalmente, não seria necessário realizar este passo — já configuramos o download e

notificação automática de atualizações no passo (2) desta atividade. Mas, para não termos que esperar até 3 da manhã, vamos acelerar o processo. Após a verificação, note que novas atualizações surgem como disponíveis na interface:

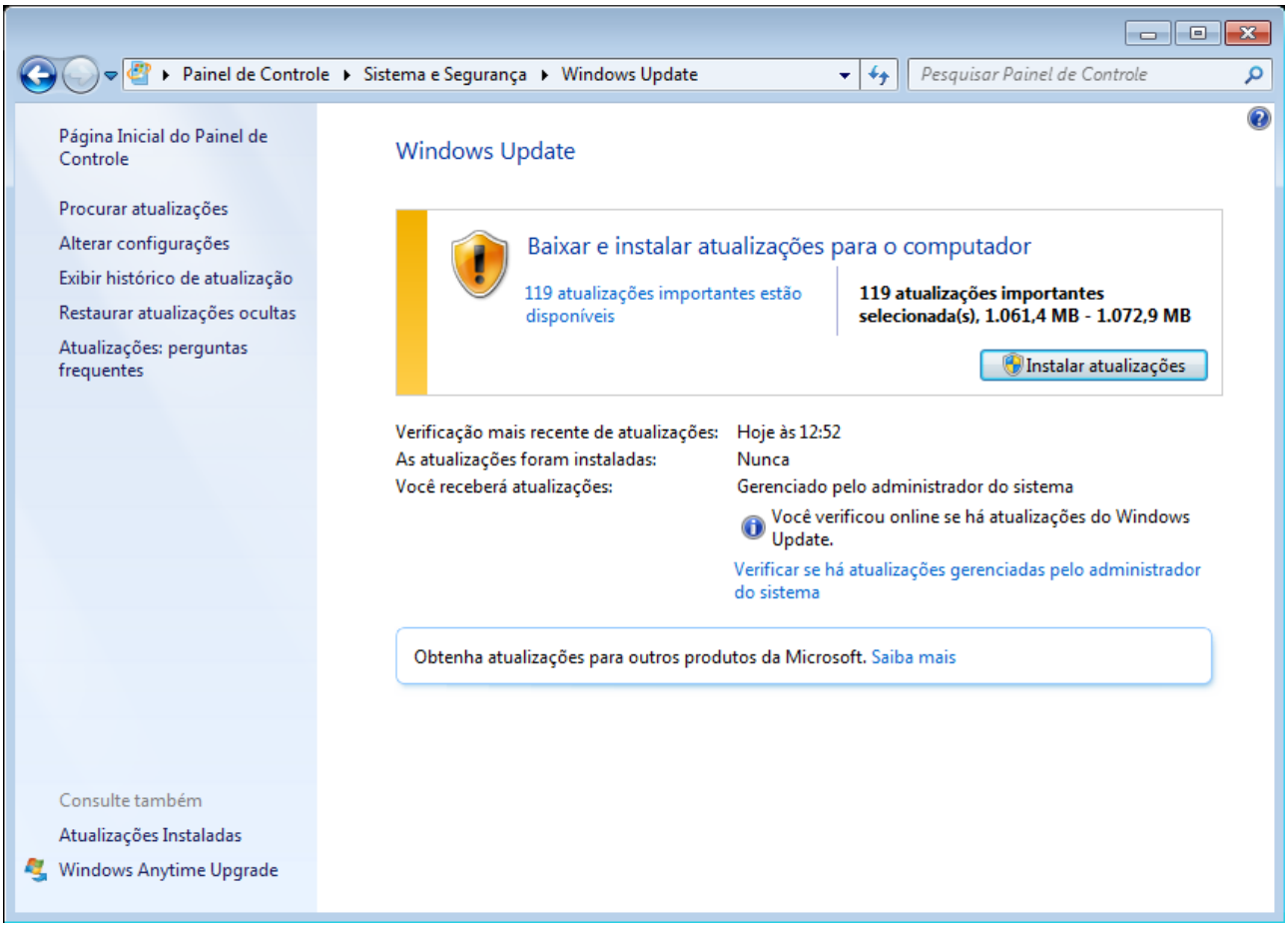

Figura 44. Novas atualizações aprovadas pelo WSUS disponibilizadas

Um vez aprovadas na console administrativa do WSUS, as atualizações podem ser instaladas nas máquinas cliente. Assim, o administrador pode controlar de forma granular quais atualizações distribuir, para quais máquinas, e quando deseja que elas sejam instaladas, tornando o processo de gestão de segurança do parque computacional muito mais eficiente.