Sessão 4: Serviços básicos de segurança

1) Configuração do servidor de log remoto

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

Nesta atividade iremos configurar um repositório de logs em um servidor da DMZ (*LinServer-G*), e enviar os logs dos demais servidores para esse concentrador. O objetivo desta atividade é fazer o aluno aplicar os conceitos de repositório de logs de uma rede e preparar o ambiente para os serviços seguintes, que serão configurados durante o curso.

1. Primeiro, vamos configurar o concentrador de logs. Acesse a máquina *LinServer-G* e instale o pacote `syslog-ng`.

   ```
   # hostname
   LinServer-A

   # apt-get install --no-install-recommends syslog-ng
   ```

2. Observe que na última linha do arquivo `/etc/syslog-ng/syslog-ng.conf` são incluídos arquivos com a extensão `.conf` localizados no diretório `/etc/syslog-ng/conf.d`:

   ```
   # tail -n1 /etc/syslog-ng/syslog-ng.conf
   @include "/etc/syslog-ng/conf.d/*.conf"
   ```

   Aproveitando-se desse fato, crie um novo arquivo com a extensão apropriada nesse diretório e configure o recebimento de logs remotos. Faça com que o `syslog-ng` escute por conexões na porta 514/UDP, e envie os arquivos de log de uma dado *host* para o arquivo `/var/log/$HOST.log`. Finalmente, reinicie o `syslog-ng`.

   Abaixo, mostramos o conteúdo do arquivo `/etc/syslog-ng/conf.d/rserver.conf`, que cumpre os objetivos especificados:

   ```
   source s_net { udp(); };
   destination d_rhost { file("/var/log/$HOST.log"); };
   log { source(s_net); destination(d_rhost); };
   ```

   Depois, basta reiniciar o serviço:

   ```
   # systemctl restart syslog-ng.service
   ```

3. Agora, na máquina *FWGW1-G*, instale o `syslog-ng` e configure-o como um cliente Syslog. Crie um arquivo de configuração na pasta `/etc/syslog-ng/conf.d` que envie todos os eventos de log locais

para a máquina *LinServer-G* na porta 514/UDP.

```
# hostname
FWGW1-A

# apt-get install --no-install-recommends syslog-ng
```

A seguir, temos o arquivo `/etc/syslog-ng/conf.d/rclient.conf`, que envia os logs locais para o servidor remoto:

```
destination d_rserver { udp("172.16.1.10" port(514)); };
log { source(s_src); destination(d_rserver); };
```

Finalmente, basta reiniciar o `syslog-ng`:

```
# systemctl restart syslog-ng.service
```

4. Usando o comando `logger`, teste seu ambiente.

   Na máquina *FWGW1-G*, crie um evento de log qualquer usando o comando `logger`:

   ```
   # hostname
   FWGW1-A

   # logger -p error Teste
   ```

   Observando a máquina *LinServer-G*, perceba que foi criado um novo arquivo `/var/log/172.16.G.1.log`. Verificando seu conteúdo, é possível constatar que, de fato, os logs remotos do *host FWGW1-G* estão sendo enviados para cá.

   ```
   # hostname
   LinServer-A

   # tail -n1 /var/log/172.16.1.1.log
   Aug 26 06:49:30 172.16.1.1 aluno: Teste
   ```

5. Agora, vamos configurar a máquina *WinServer-G* para enviar registros de eventos para o concentrador Syslog. Faça login como usuário `Administrator` e abra o *Group Policy Editor* digitando `gpedit.msc` no menu *Start* > *Run...*.

   Na ferramenta, acesse a seção *Computer Configuration* > *Windows Settings* > *Security Settings* > *Local Policies* > *Audit Policy* e habilite os seguintes eventos como "Sucesso" e "Falha":

   Tabela 1. Políticas de auditoria para o WinServer-G

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success
Audit privilege use	Failure
Audit process tracking	No Auditing
Audit system events	Success, Failure

A tela ficaria, portanto, desta forma:

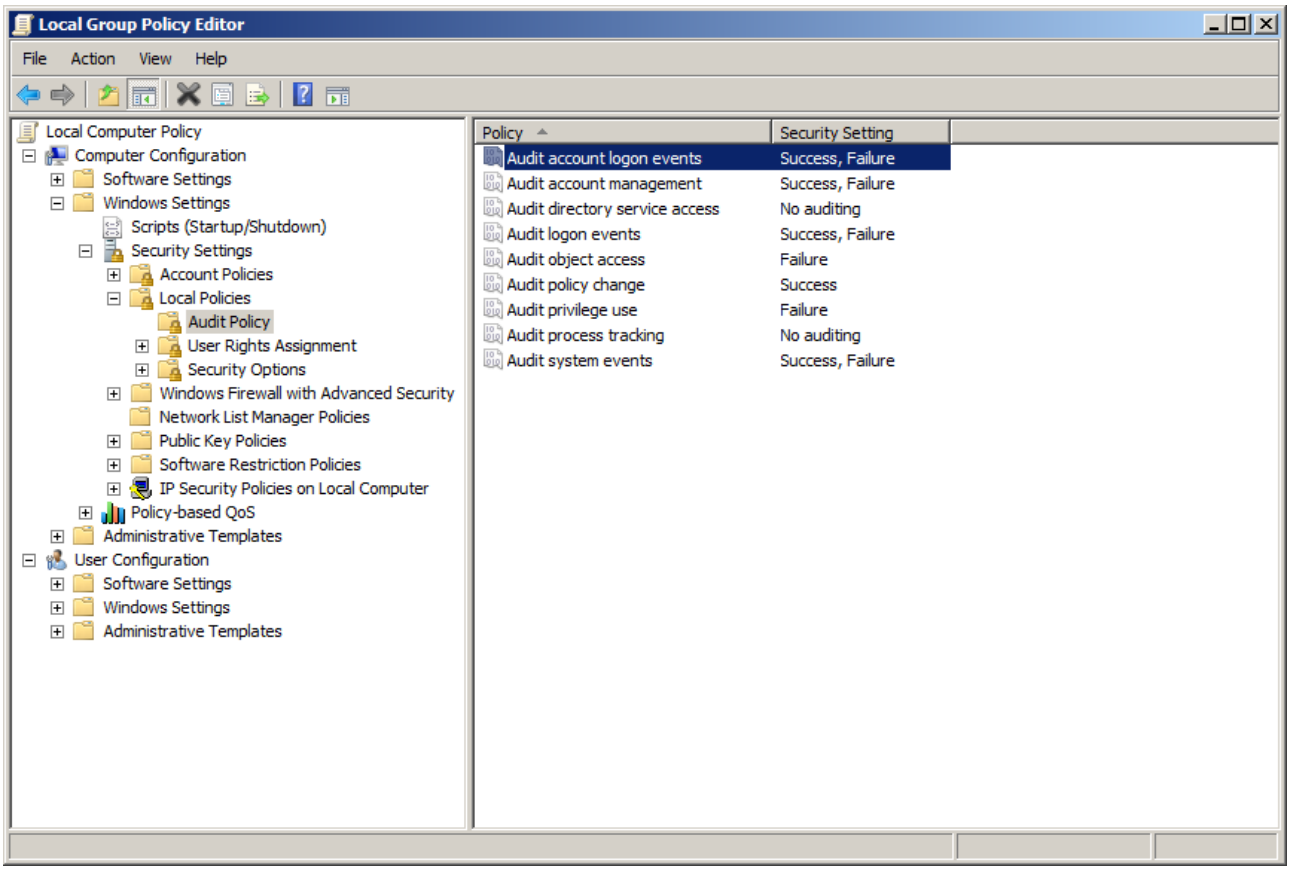

Figura 1. Tela de políticas de auditoria para o WinServer-G

6. O próximo passo é instalar o Snare, que permitirá envio dos registros de eventos do Windows para um servidor Syslog remoto. Faça o download em https://www.snaresolutions.com/products/snare-agents/open-source-agents/ ; será necessário cadastrar seu nome/email para receber o link de download. Alternativamente, solicite o instalador ao instrutor.

   Durante a instalação, responda todas as perguntas com as opções padrão, exceto:

   Tabela 2. Opções de instalação do Snare

Opção	Escolha
Snare Auditing	Yes
Service Account	Use System Account
Remote Control Interface	Enable Web Access (Password: rnpesr)

7. Após a instalação, abra o Snare. Clique em *Start* e digite "snare", escolhendo a opção `Snare for Windows (Open Source)`, como se segue:

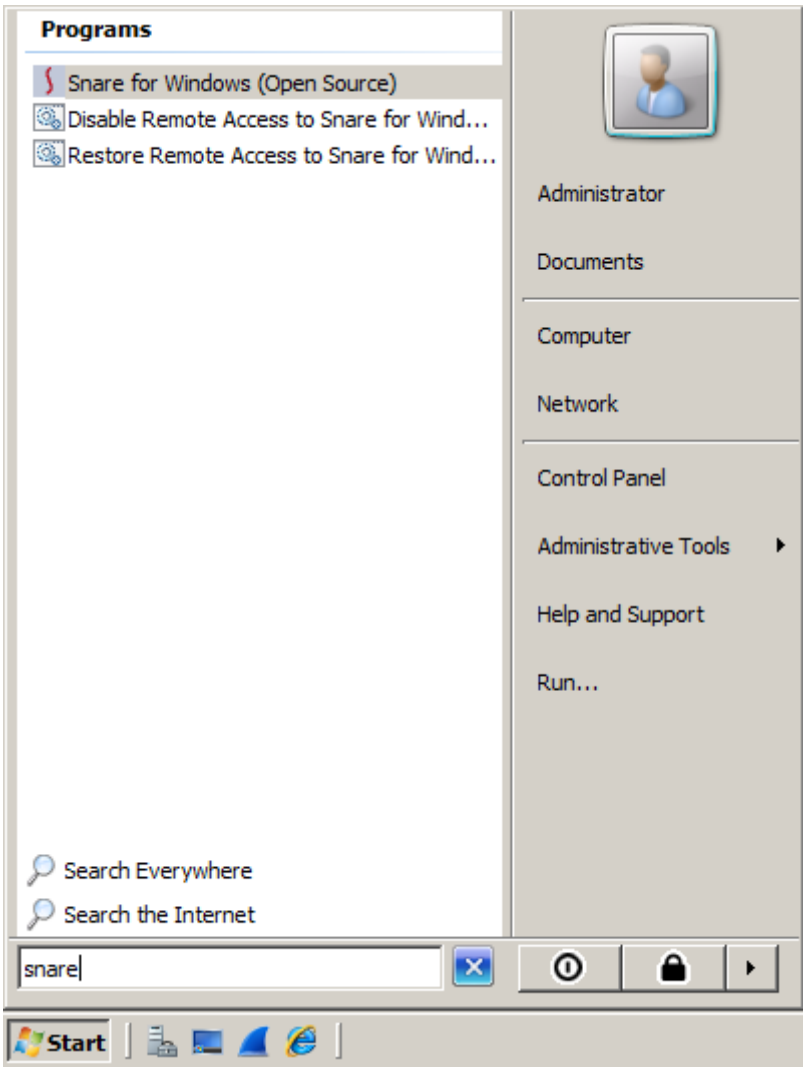

Figura 2. Inicialização do Snare

Irá ser lançada uma janela do navegador. Informe o usuário `snare`, e senha `rnpesr`, como se segue:

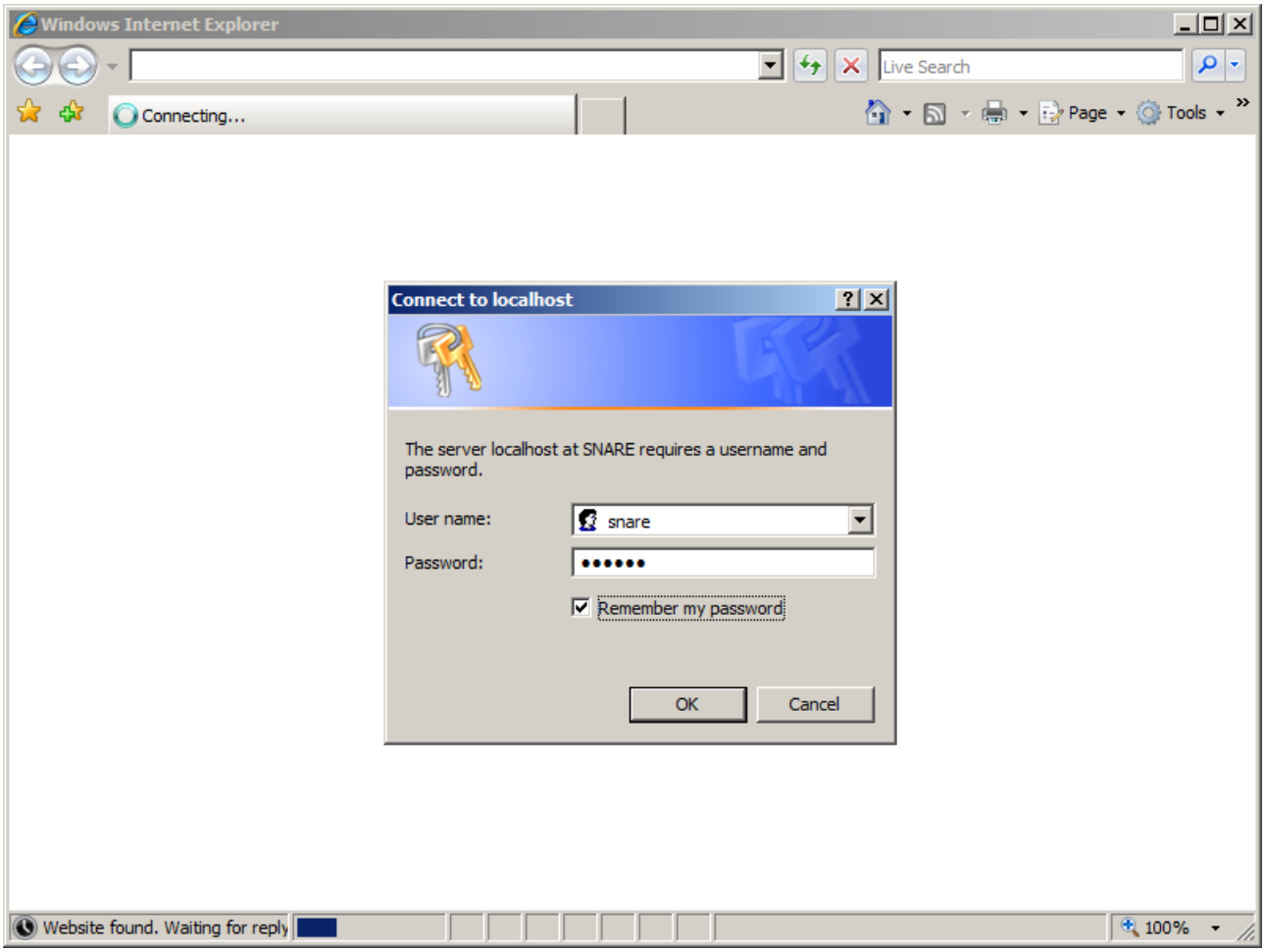

Figura 3. Login no Snare

Clique em *Network Configuration* — informe o IP da máquina *LinServer-G* no campo *Destination Snare Server address*, e a porta 514 no campo *Destination Port*, como se segue. Em seguida, clique em *Change Configuration*.

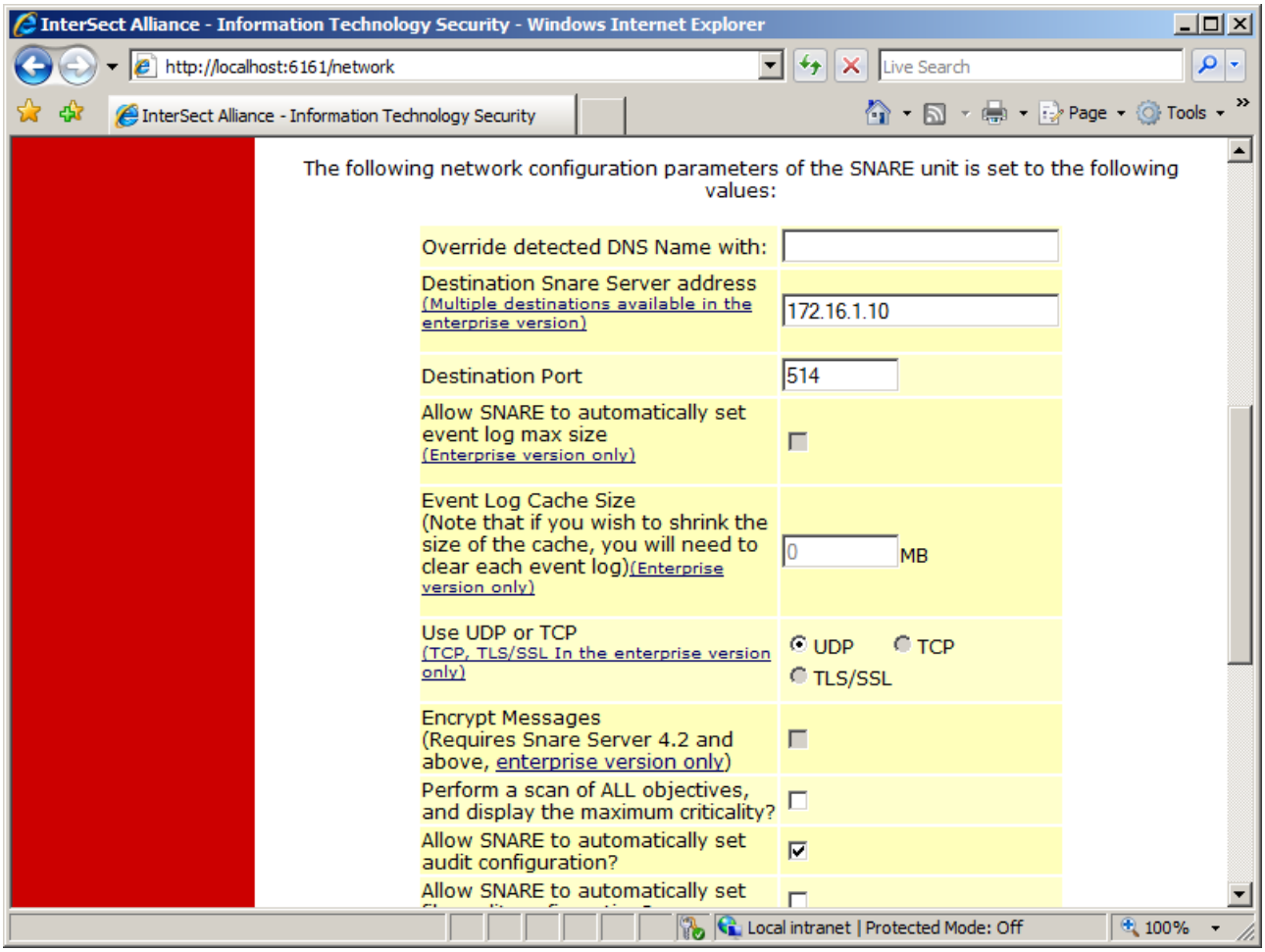

Figura 4. Configurações do Snare

Em seguida, clique em *Apply the Latest Audit Configuration* e depois em *Reload Settings*.

8. Faça logoff/logon no *WinServer-G* para gerar registros de eventos. Em seguida, volte à máquina *LinServer-G* e verifique que os logs estão de fato sendo enviados.

```
# hostname
LinServer-A

# grep Logoff /var/log/172.16.1.20.log
Aug 26 07:10:25 172.16.1.20 WinServer-A MSWinEventLog   1       Security        50
dom ago 26 08:10:23 2018  4647    Microsoft-Windows-Security-Auditing
WINSERVER-A\Administrator       N/A     Success Audit     WinServer-A     Logoff
User initiated logoff:    Subject:   Security ID:  S-1-5-21-1959434341-4039883546-
812769935-500   Account Name:  Administrator   Account Domain:  WINSERVER-A   Logon
ID:  0x16898    This event is generated when a logoff is initiated but the token
reference count is not zero and the logon session cannot be destroyed.  No further
user-initiated activity can occur.  This event can be interpreted as a logoff
event.  41
```

2) Configuração do servidor de hora

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

Nesta atividade vamos configurar o serviço de sincronismo de relógio em um servidor da rede (*LinServer-G*) e configurar os demais *hosts* da rede para sincronizar com o relógio desse servidor.

1. Primeiro, vamos configurar o servidor de hora. Acesse a máquina *LinServer-G* e instale o pacote `ntp`.

```
# hostname
LinServer-A
```

```
# apt-get install --no-install-recommends ntp
```

2. Edite o arquivo `/etc/ntp.conf` e substitua o conteúdo das linhas 21-24 (que começam com a palavra-chave `server`) pelas que se seguem. Comente ou remova as linhas originais.

```
# nano /etc/ntp.conf
(...)
```

```
# grep '^server' /etc/ntp.conf
server a.ntp.br iburst
server b.ntp.br iburst
server c.ntp.br iburst
```

3. Para sincronizar o relógio de forma imediata, pare o serviço do `ntp`, rode o comando `ntpd -gq` e em seguida inicie o *daemon*. Verifique se a hora está corrigida.

```
# systemctl stop ntp
```

```
# ntpd -gq
ntpd: time slew +0.000090s
```

```
# date
Mon Sep  3 19:36:26 EDT 2018
```

```
# systemctl start ntp
```

4. Cheque se o `ntp` está funcionando, e se está escutando por conexões de rede na porta esperada. A seguir, iremos configurar os clientes NTP.

```
# ntpq -c pe
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*a.ntp.br        200.160.7.186    2 u   48   64   77   16.623   -0.352   0.229
 b.ntp.br        200.160.7.186    2 u   51   64   77   57.992   -1.086   0.239
 c.ntp.br        200.160.7.186    2 u   50   64   77   40.497   -2.432   0.281
```

```
# netstat -unlp | grep '^udp .*:123'
udp        0      0 172.16.1.10:123         0.0.0.0:*
11052/ntpd
udp        0      0 127.0.0.1:123           0.0.0.0:*
11052/ntpd
udp        0      0 0.0.0.0:123             0.0.0.0:*
11052/ntpd
```

5. Vamos configurar o cliente NTP Linux, na máquina *FWGW1-G*. Instale o pacote `ntp`; edite o arquivo `/etc/ntpd.conf` para consultar o servidor de hora *LinServer-G*; pare o serviço `ntp`, sincronize a hora imediatamente e reinicie-o.

```
# hostname
FWGW1-A
```

```
# apt-get install --no-install-recommends ntp
```

```
# nano /etc/ntp.conf
(...)
```

```
# grep '^server' /etc/ntp.conf
server 172.16.1.10 iburst
```

```
# systemctl stop ntp
```

```
# ntpd -gq
ntpd: time slew -0.000270s
```

```
# date
Mon Sep  3 19:44:04 EDT 2018
```

```
# systemctl start ntp
```

6. Finalmente, configure o cliente NTP na máquina *WinServer-G*. O Microsoft Windows possui uma forma simples de configurar o sincronismo de relógio com servidores de rede, desde de que não tenham o servidor de diretório *Microsoft Active Directory* como controlador de domínio, pois dessa forma o sincronismo é automático.

   Para a configuração do sincronismo automático do *host* Windows com o servidor de hora da rede, clique no relógio da barra de tarefas, e em seguida em *Change date and time settings...*; logo depois, navegue até a aba *Internet Time*.

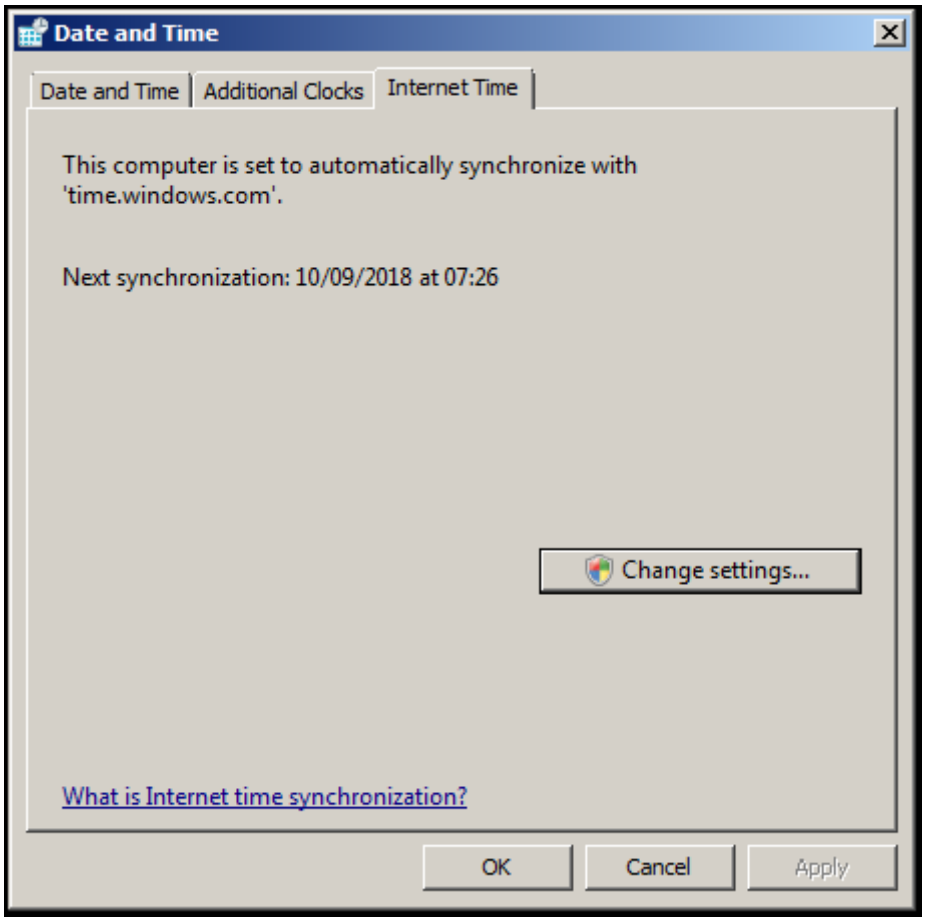

Figura 5. Aba Internet Time do relógio do Windows

   Clique em *Change Settings...*, e informe o IP da máquina *LinServer-G* no campo *Server*. Em seguida, clique em *Update now* (se ocorrer um erro, clique uma segunda vez), e o relógio do sistema deverá ser atualizado.

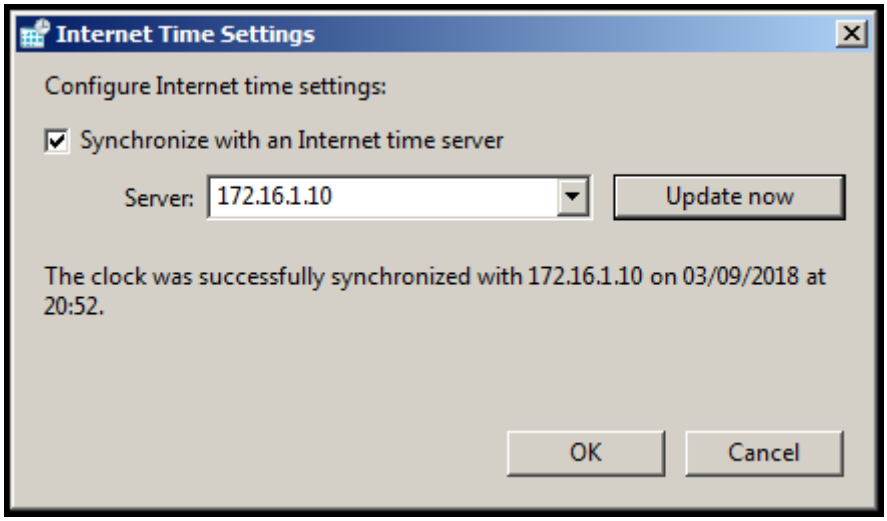

Figura 6. Modificando o servidor NTP do Windows

3) Monitoramento de serviços

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

Nesta atividade prática, o software Cacti será configurado para monitorar os recursos dos servidores da rede. O Cacti e os pacotes necessários para o correto funcionamento serão instalados na máquina *LinServer-G*. Serão configurados agentes SNMP nos servidores *WinServer-G* e *FWGW1-G* para que o Cacti possa monitorar os recursos desses hosts.

1. Primeiro, vamos instalar o Cacti. Acesse a máquina *LinServer-G* e instale o pacote `cacti`.
    - Quando perguntado sobre a senha para o usuário `root` do MySQL, informe `rnpesr123`.
    - Quando perguntado sobre o *web server* para o qual o Cacti deve ser autoconfigurado, escolha `apache2`.
    - Quando perguntado se a base de dados do Cacti deve ser configurada usando o `dbconfig-common`, responda *Yes*. Para a senha do usuário administrativo da base de dados e a senha do aplicativo Cacti no MySQL, informe `rnpesr123` para ambas as perguntas.

```
# hostname
LinServer-A
```

```
# apt-get install cacti
(...)
```

2. Em sua máquina física, acesse a URL `http://172.16.1.10/cacti` para concluir a instalação do Cacti.

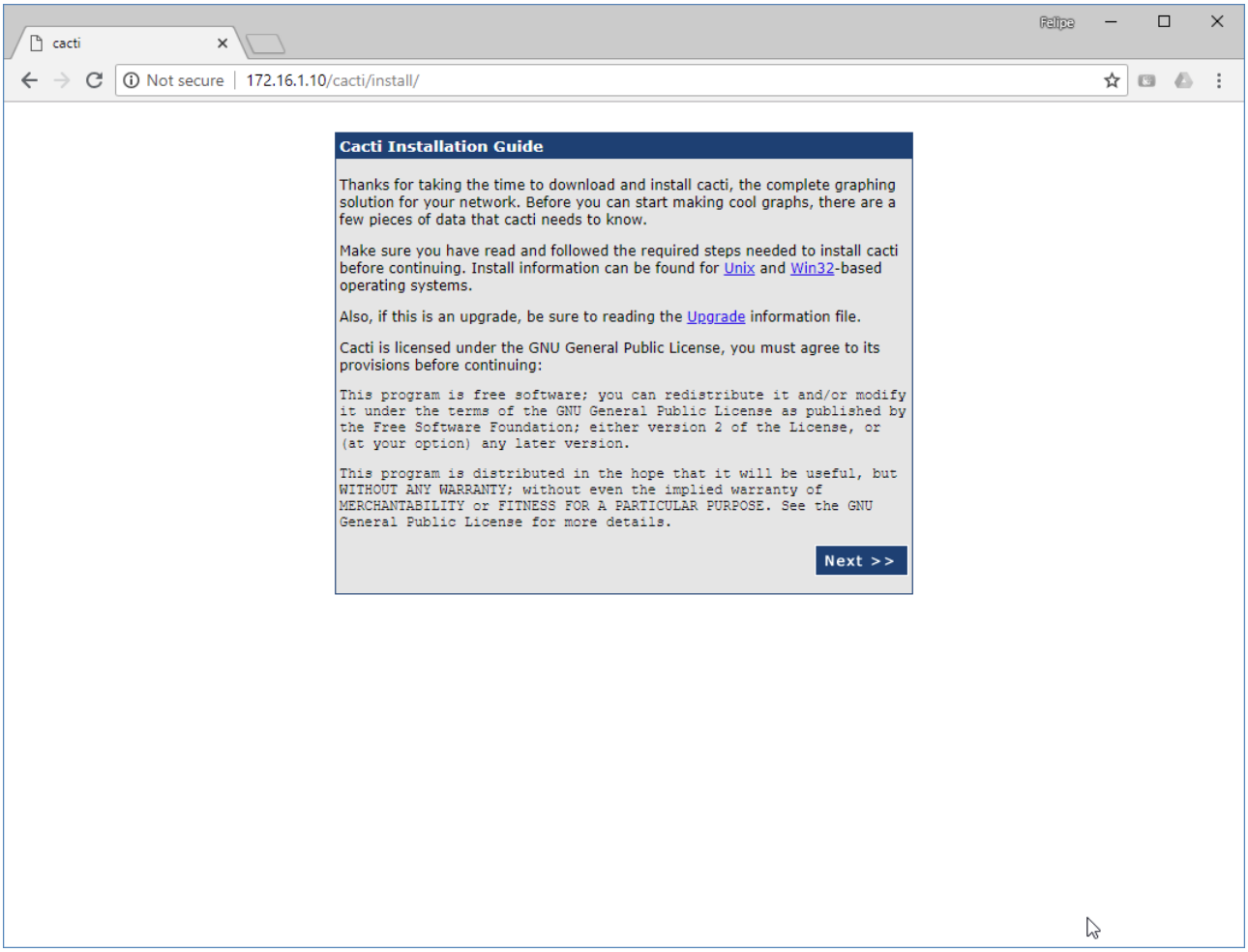

Figura 7. Tela inicial do Cacti

Clique em *Next*. Na tela seguinte, mantenha a escolha em *New Install* e clique em *Next*. Verifique que todos os valores na tela a seguir estão corretos (texto em verde com os dizeres `OK: FILE FOUND`), e clique em *Finish*.

Você verá a tela de login do Cacti. Entre com o usuário `admin` e senha `admin`; quando solicitada mudança de senha, escolha `rnpesr` em ambos os campos e clique em *Save*. Você deverá acessar a tela principal de configuração do Cacti.

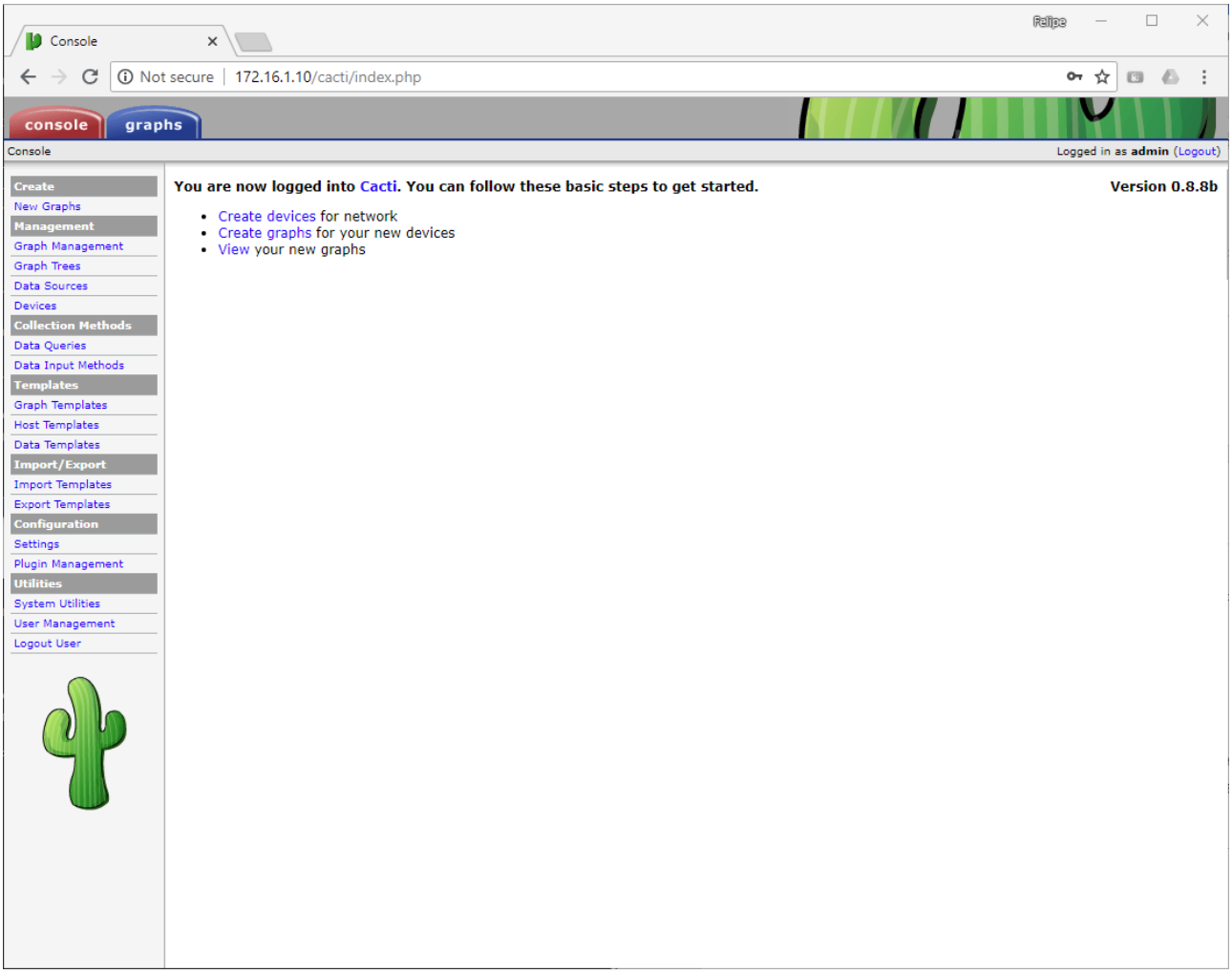

Figura 8. Console do Cacti

3. Vamos instalar o agente SNMP na máquina *FWGW1-G*. Instale o pacote `snmpd`.

```
# hostname
FWGW1-A
```

```
# apt-get install --no-install-recommends snmpd
```

4. Edite o arquivo `/etc/snmp/snmpd.conf`, comente a linha `agentAddress udp:127.0.0.1:161` e descomente a linha `agentAddress udp:161,udp6:[::1]:161`. Em seguida, reinicie o `snmpd` e verifique que ele está escutando na porta apropriada.

```
# vi /etc/snmp/snmpd.conf
(...)
```

```
# grep '^#*agentAddress' /etc/snmp/snmpd.conf
#agentAddress  udp:127.0.0.1:161
agentAddress udp:161,udp6:[::1]:161
```

```
# systemctl restart snmpd
```

```
# netstat -unlp | grep '^udp .*:161'
udp        0      0 0.0.0.0:161             0.0.0.0:*
12527/snmpd
```

5. Lembre-se que a *chain* INPUT da tabela *filter* do firewall *FWGW1-G* não está configurada para permitir conexões nessa porta. Corrija o problema e salve as modificações no arquivo `/etc/iptables/rules.v4`.

```
# iptables -A INPUT -s 172.16.1.10/32 -p udp -m udp --dport 161 -m state --state
NEW,ESTABLISHED -j ACCEPT
```

```
# iptables-save > /etc/iptables/rules.v4
```

6. Agora, vamos instalar o agente SNMP na máquina *WinServer-G*. Acesse como usuário *Administrator* e, dentro do *Server Manager*, clique com o botão direito em *Features* > *Add Features*. Desça a barra de rolagem, selecione a caixa *SNMP Services* e prossiga com o assistente.

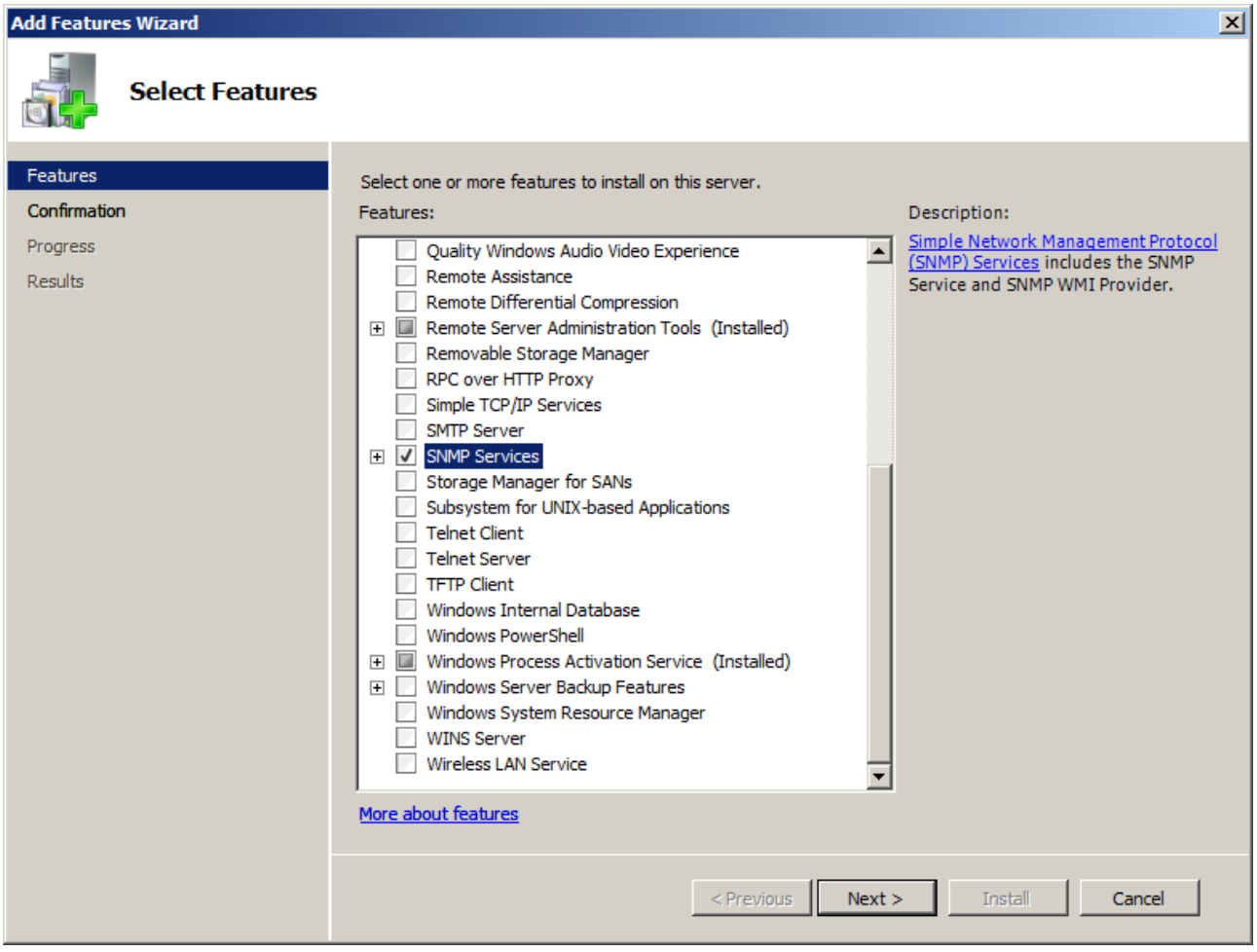

Figura 9. Instalação da feature SNMP

7. Abra o gestor de serviços do Windows, via menu *Start* > *Run...* > `services.msc`. Encontre o serviço *SNMP Service* e clique com o botão direto > *Properties*.

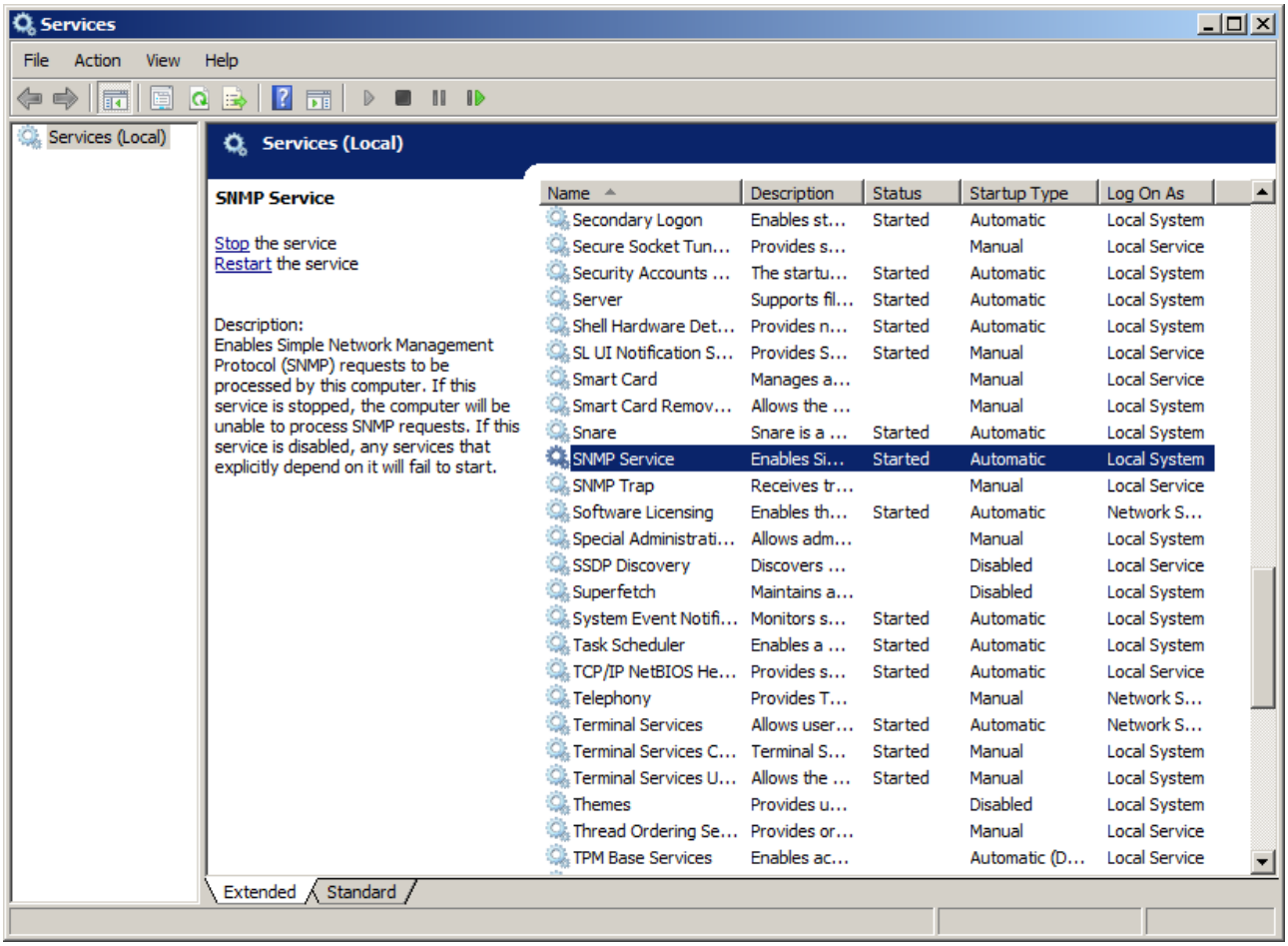

Figura 10. Propriedades do serviço SNMP

Na aba *Security*, caixa *Accepted community names*, clique em *Add...* e adicione a comunidade `public` com permissões *READ ONLY*. Logo abaixo, na caixa *Accept SNMP packets from these hosts*, clique em *Add...* e adicione o IP da máquina *LinServer-G*. Sua janela deverá ficar assim:

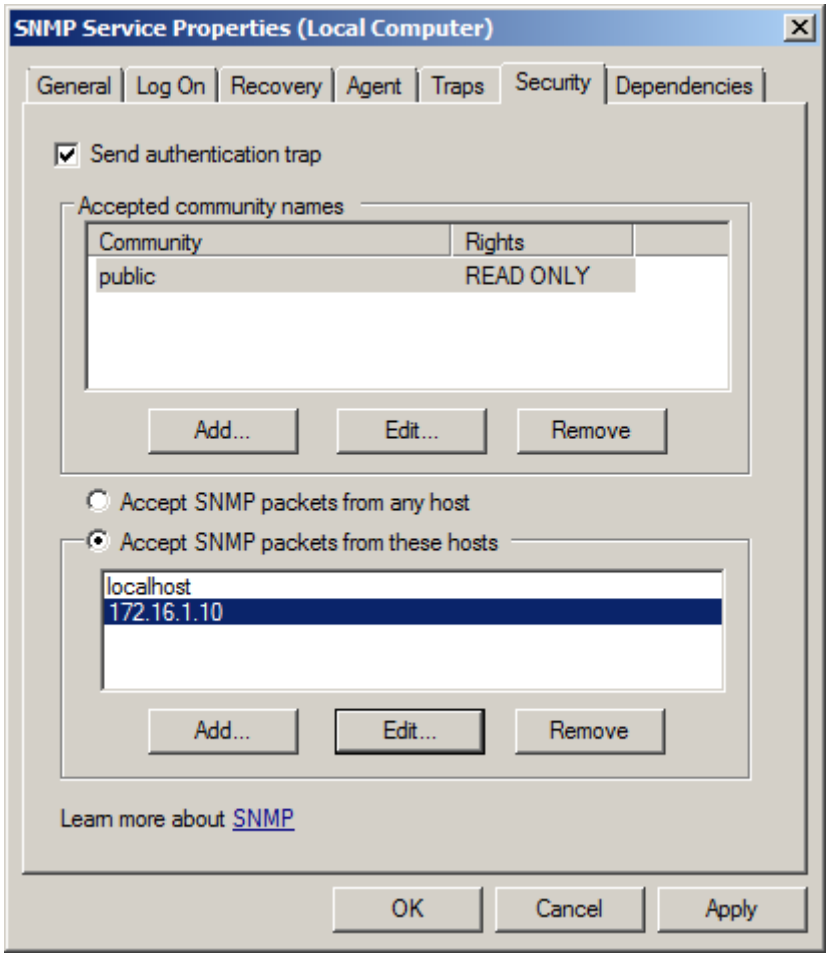

Figura 11. Configurações do serviço SNMP

Finalmente, clique com o botão direito no serviço *SNMP Service* e em seguida em *Restart*.

8. De volta à console do Cacti, no navegador da sua máquina física acessando a URL `http://172.16.1.10/cacti`, vamos adicionar os dois servidores configurados. No menu à esquerda, clique em *Devices*, e em seguida na palavra *Add* no canto superior direto da nova janela.

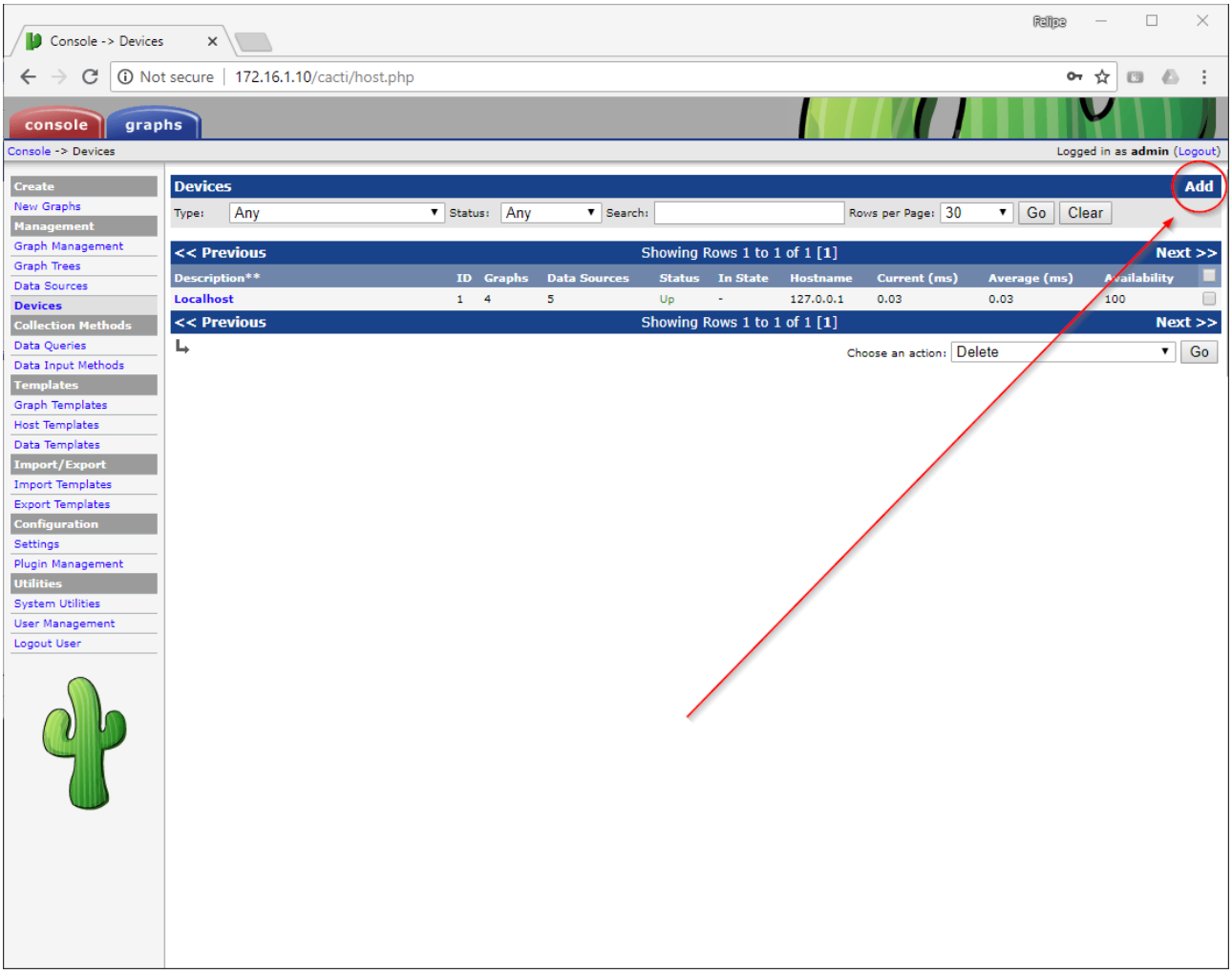

Figura 12. Adicionando device no Cacti, parte 1

Na nova janela, informe o nome da máquina *FWGW1-G* no campo *Description*, seu IP exposto à DMZ no campo *Hostname*, e escolha a opção *Local Linux Machine* no campo *Host Template*. Verifique se sua janela está como se segue, e clique em *Create*.

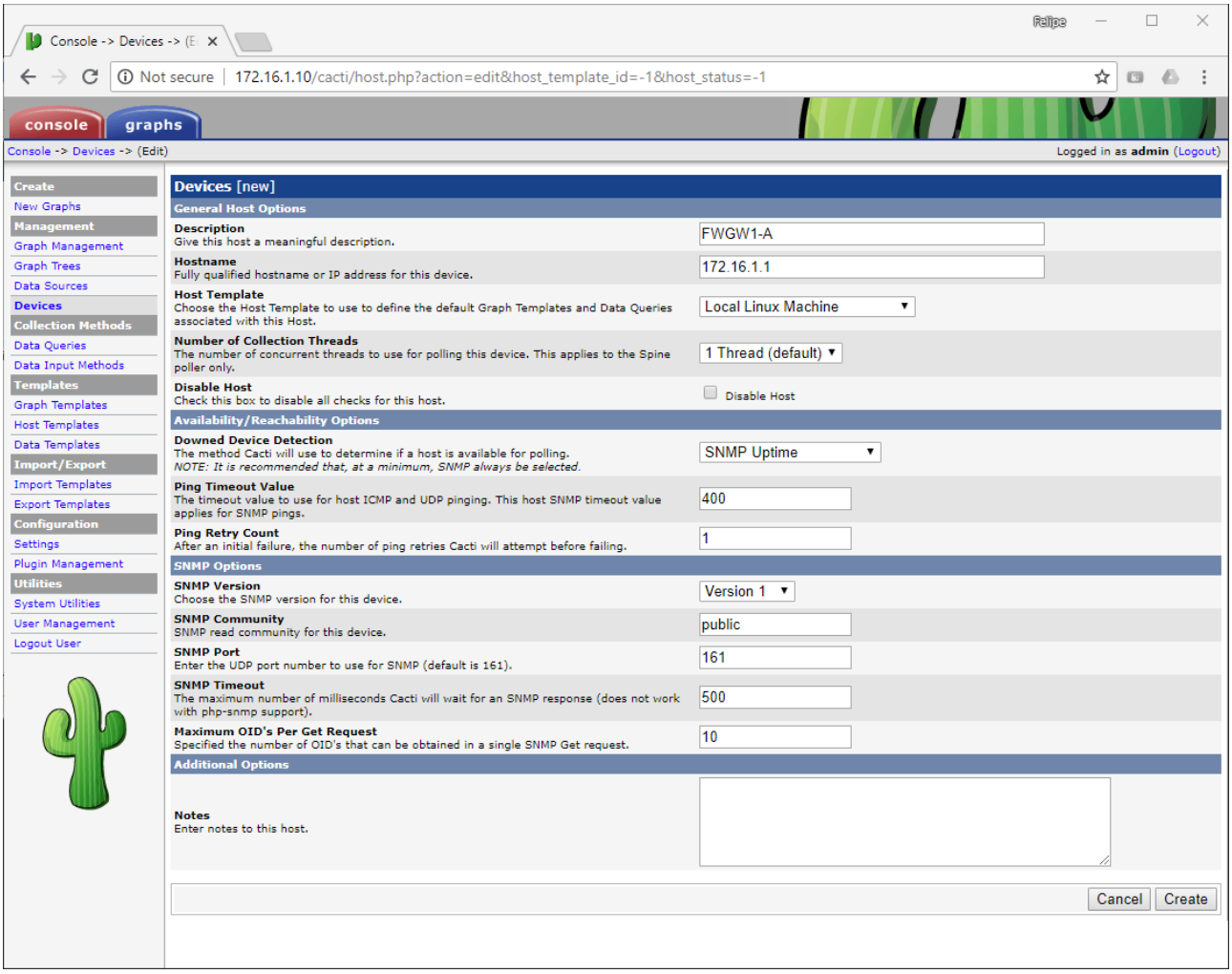

Figura 13. Adicionando device no Cacti, parte 2

Verifique que as informações SNMP do *host FWGW1-G* figuram corretamente na seção *SNMP Information* no topo da tela. Em seguida, clique em *Create Graphs for this Host*.

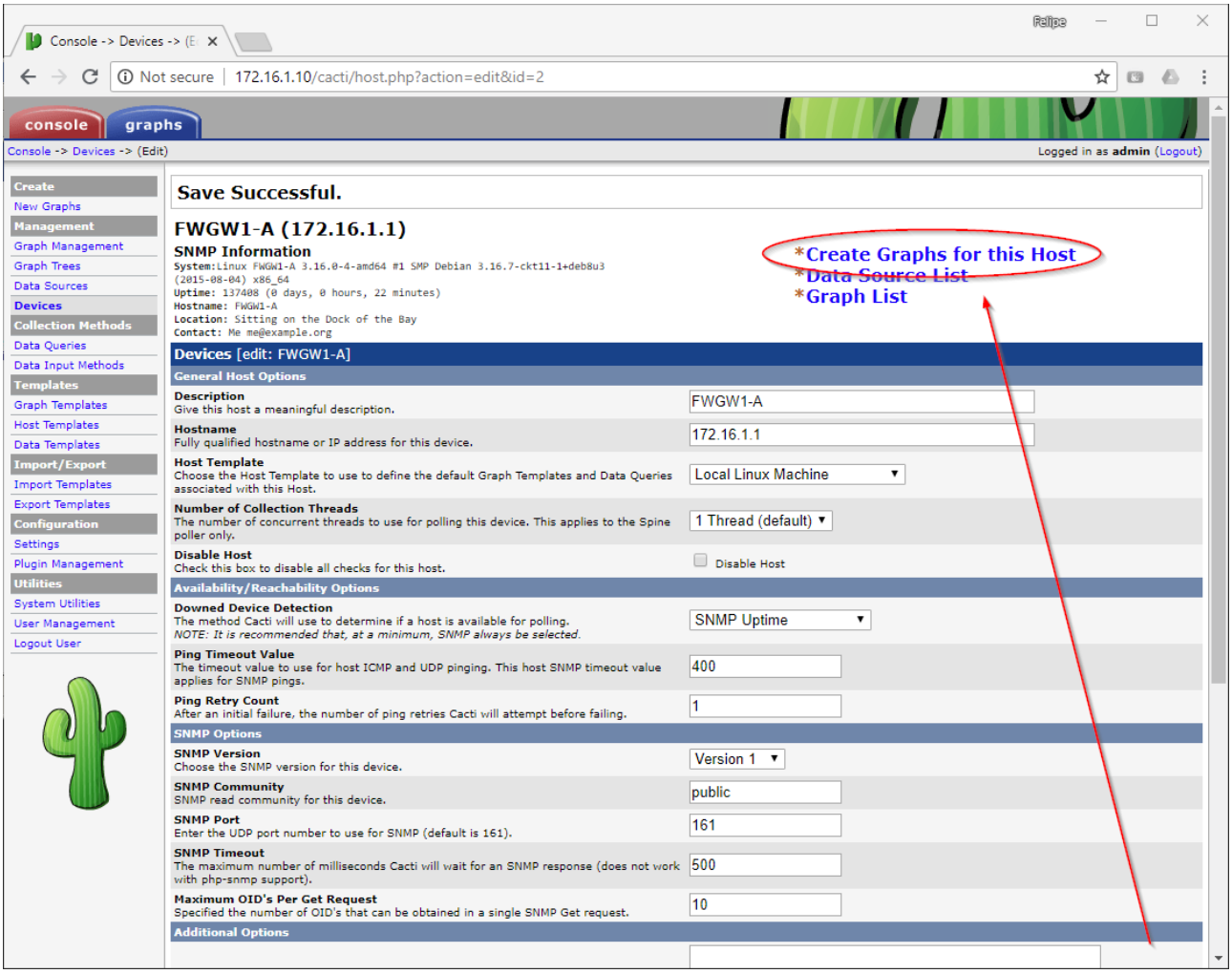

Figura 14. Adicionando gráficos no Cacti, parte 1

Na nova janela, selecione todos os *Graph Templates* e *Data Queries* disponíveis e clique em *Create*. Na janela que se segue, clique novamente em *Create*.

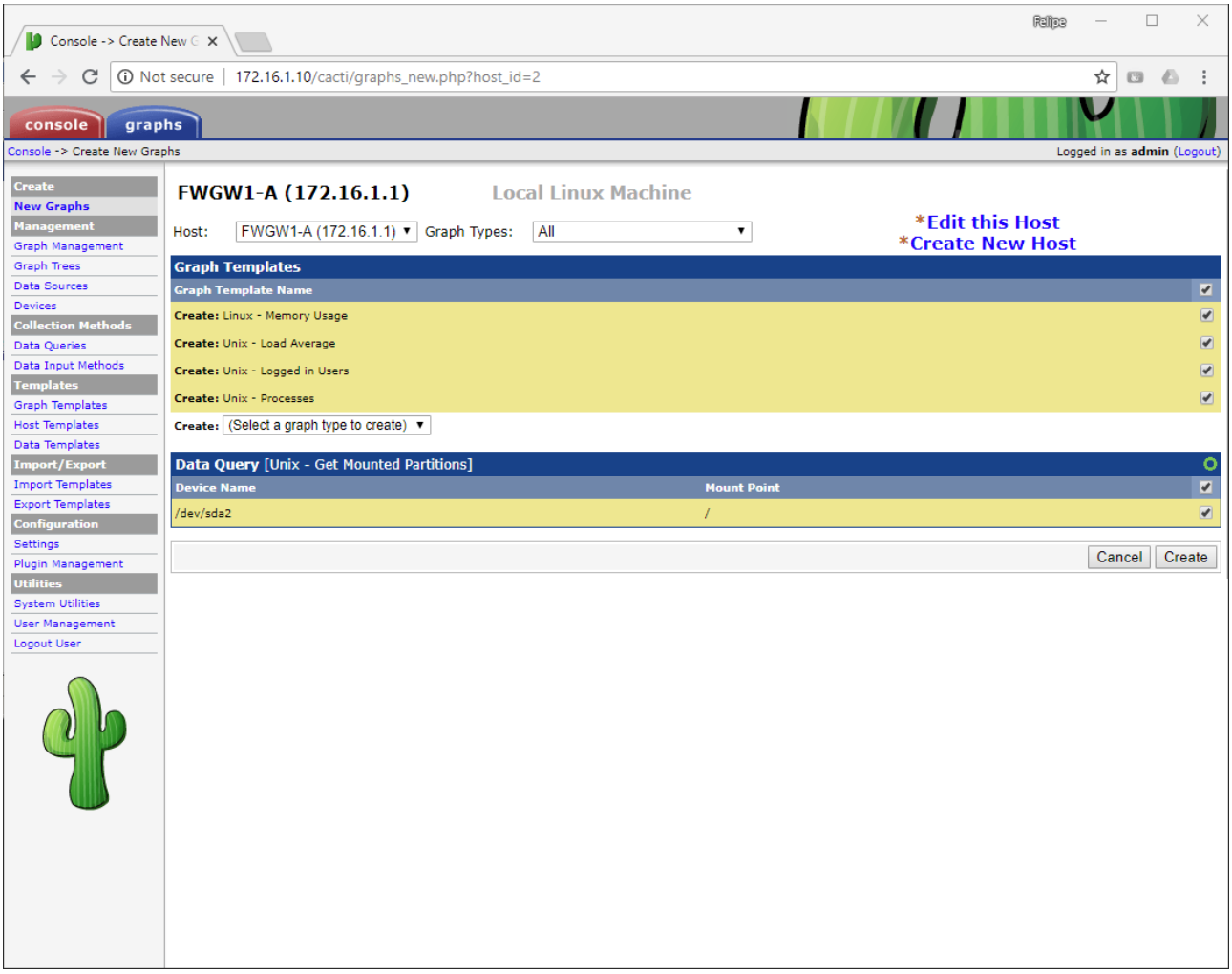

Figura 15. Adicionando gráficos no Cacti, parte 2

Agora, o passo final é adicionar os gráficos a uma árvore de gráficos. No menu à esquerda, clique em *Graph Trees*, e em seguida em *Default Tree*.

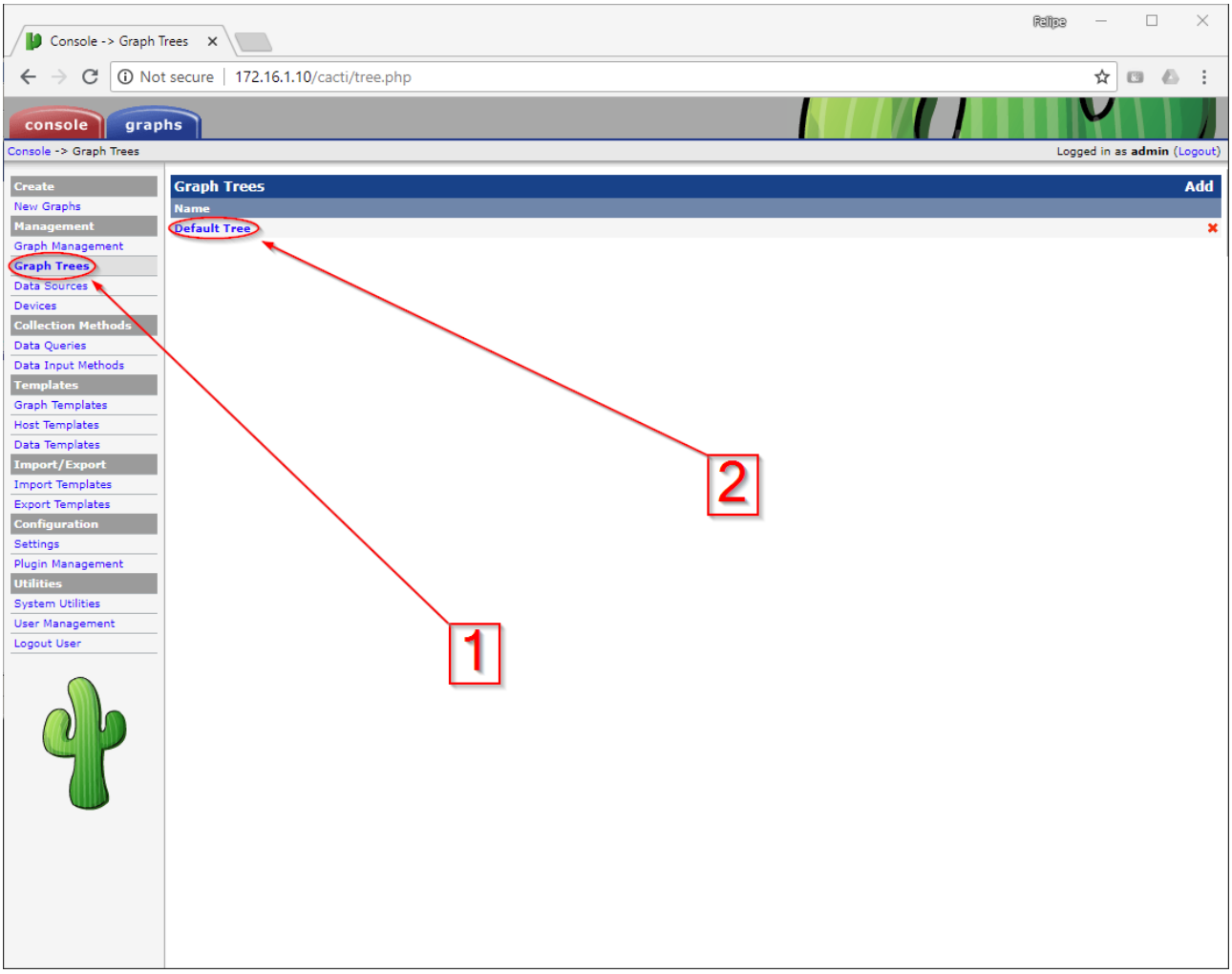

Figura 16. Adicionando gráficos a árvores no Cacti, parte 1

Na nova janela, em *Tree Items*, clique em *Add*.

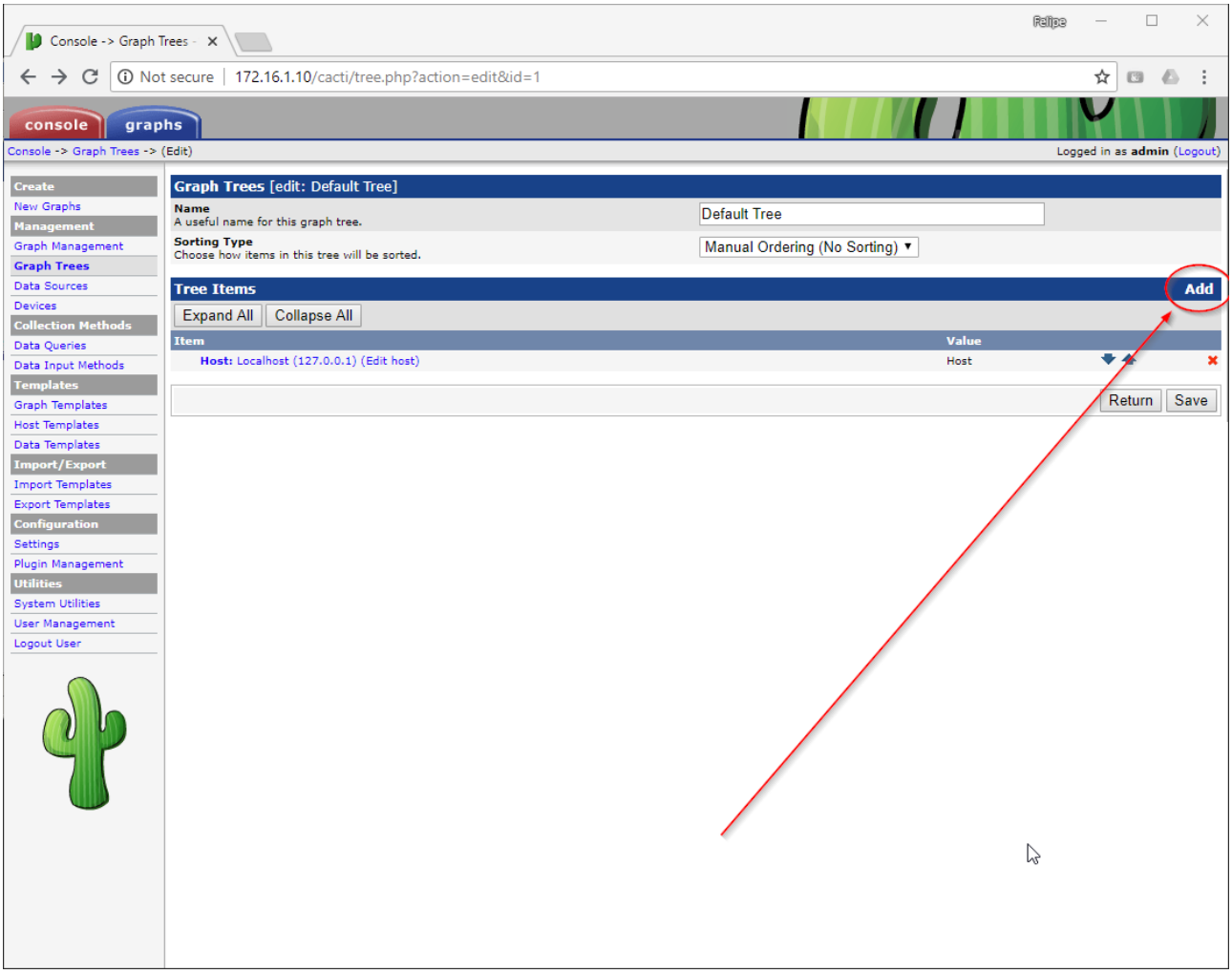

Figura 17. Adicionando gráficos a árvores no Cacti, parte 2

Na nova janela, em *Tree Item Type*, altere o valor para *Host*. Novas opções irão surgir. Em *Host*, selecione a máquina *FWGW1-G*, e depois clique em *Create*.

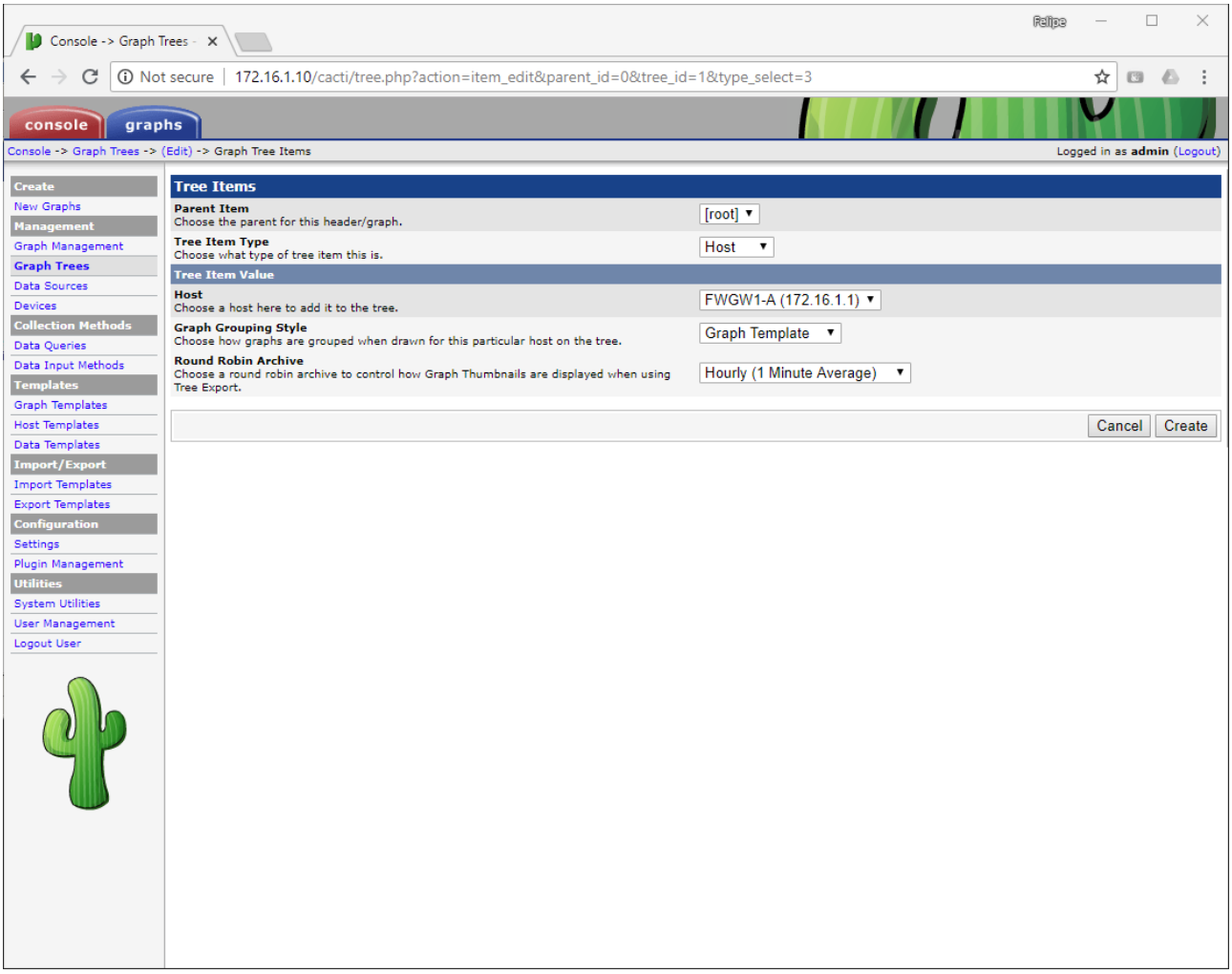

Figura 18. Adicionando gráficos a árvores no Cacti, parte 3

Para visualizar os gráficos recém-criados, no menu superior acesse *graphs*, expanda a *Default Tree* e clique no *host FWGW1-G*. Pode demorar algum tempo para que os gráficos sejam populados.

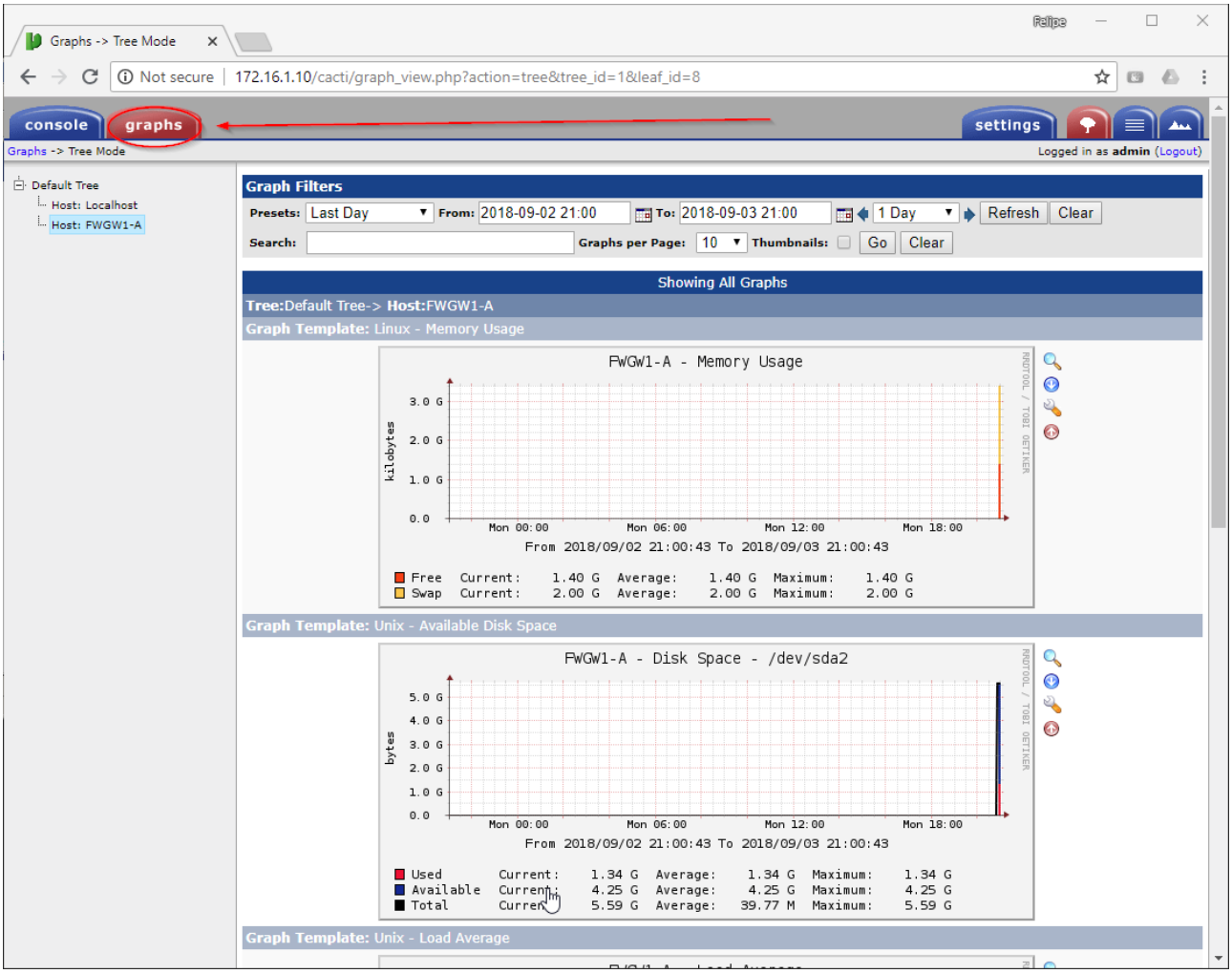

Figura 19. Visualizando gráficos no Cacti, máquina FWGW1-G

9. Faça o mesmo procedimento realizado no passo (8), mas agora com a máquina *WinServer-G*. A única diferença é que você irá apontar o IP da máquina *WinServer-G* no campo *Hostname*, e o *Host Template* como sendo *Windows 2000/XP Host*. Ao final do processo, os gráficos deverão ficar visíveis como se segue.

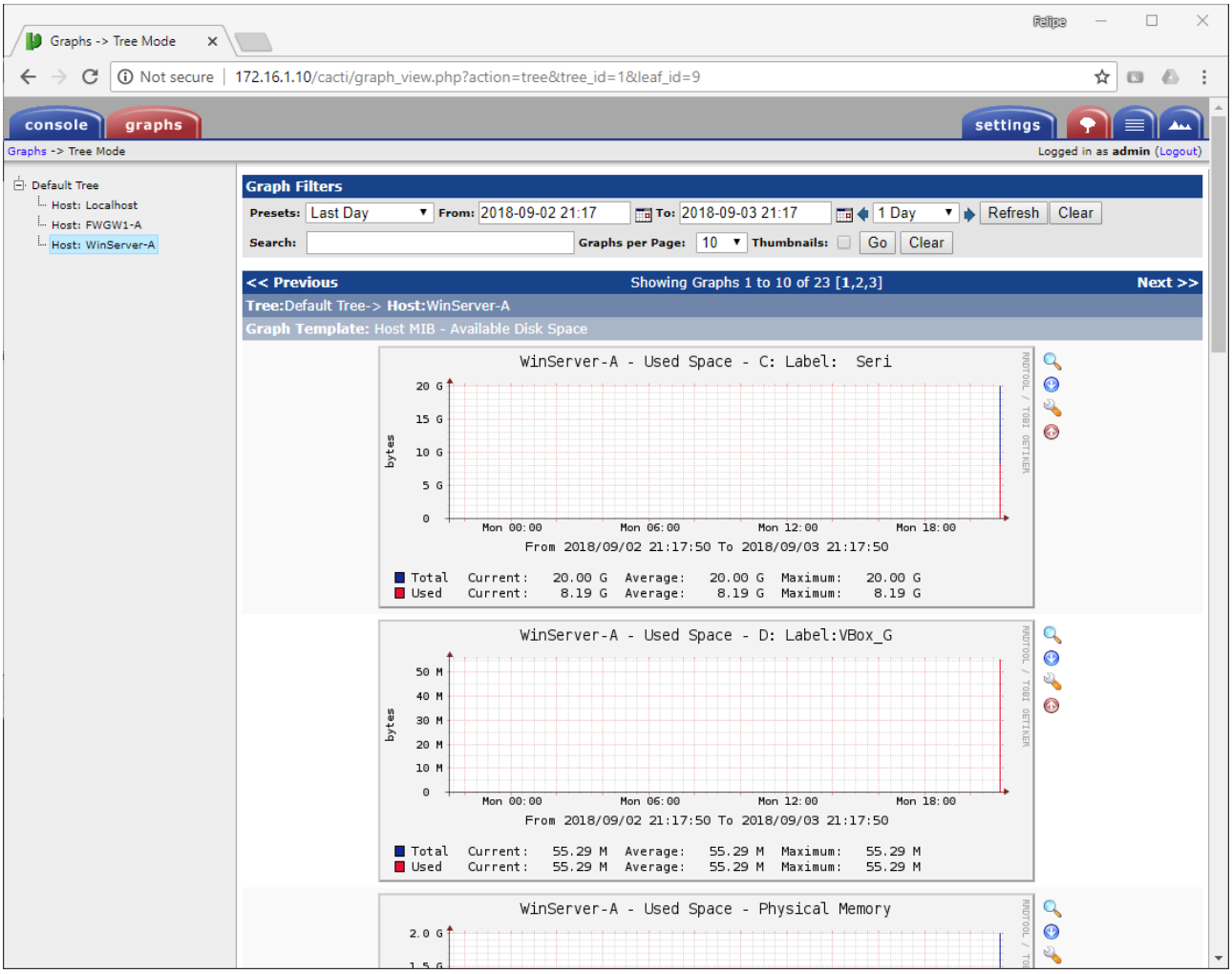

Figura 20. Visualizando gráficos no Cacti, máquina WinServer-G