WMI

CONFIGURAÇÃO

CONFIGURAÇÃO DO WMI

OBSOLETO

Utilize o tutorial abaixo para monitorar servidores e estações Windows:

https://wiki.monsta.com.br/books/wmi-configuracao/page/sonda-monitoramento-de-windows

---

Configuração básica de um usuário para acessar o serviço WMI em sistemas operacionais Windows.

Criar um usuário

> Este procedimento pode ser feito através da tela de gerenciamento de Usuários e Grupos.

Logado como administrador, no prompt de comando digite os comandos abaixo:

```
net user wmimonsta senha
monsta /addwmic useraccount where "Name='wmimonsta'" set PasswordExpires=FALSE
net localgroup “Usuários” wmimonsta /delete
net localgroup “Usuários de monitor de desempenho” wmimonsta /add
net localgroup "Distributed COM - Usuários" wmimonsta /add
net localgroup "Usuários de log de desempenho" wmimonsta /add
```

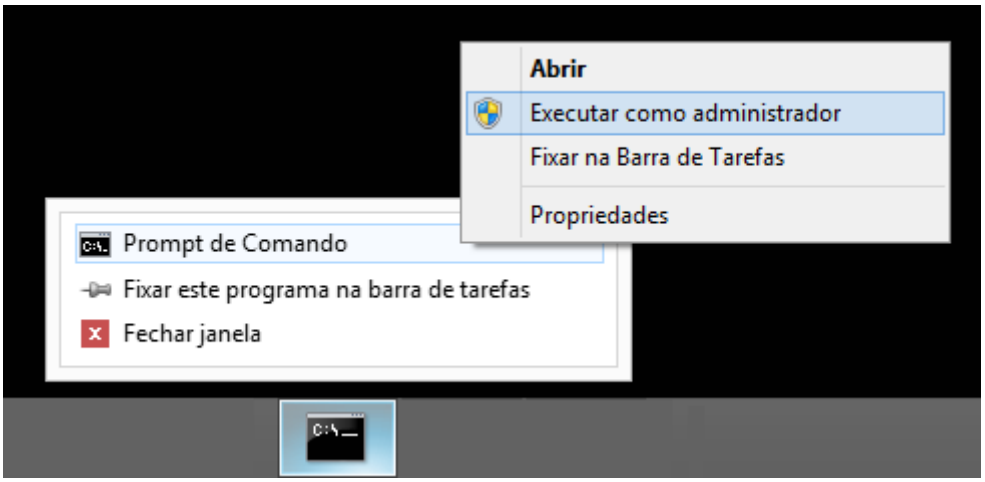
Estes comandos irão criar o usuário “wmimonsta”, remover o grupo “Usuários” e adicionar o grupo “Usuários de monitor de desempenho” para as pesquisas por WMI.

> Este grupo serve para Windows em português. Para outras línguas, consulte o nome do grupo correto.

No caso do seguinte erro ocorrer:

> Erro de Sistema 5.
> Acesso negado.

Abra o prompt de comando como usuário administrador, clicando com o botão direito sobre o ícone do Prompt de Comando
conforme figura ao lado e execute novamente os comandos deste tópico.

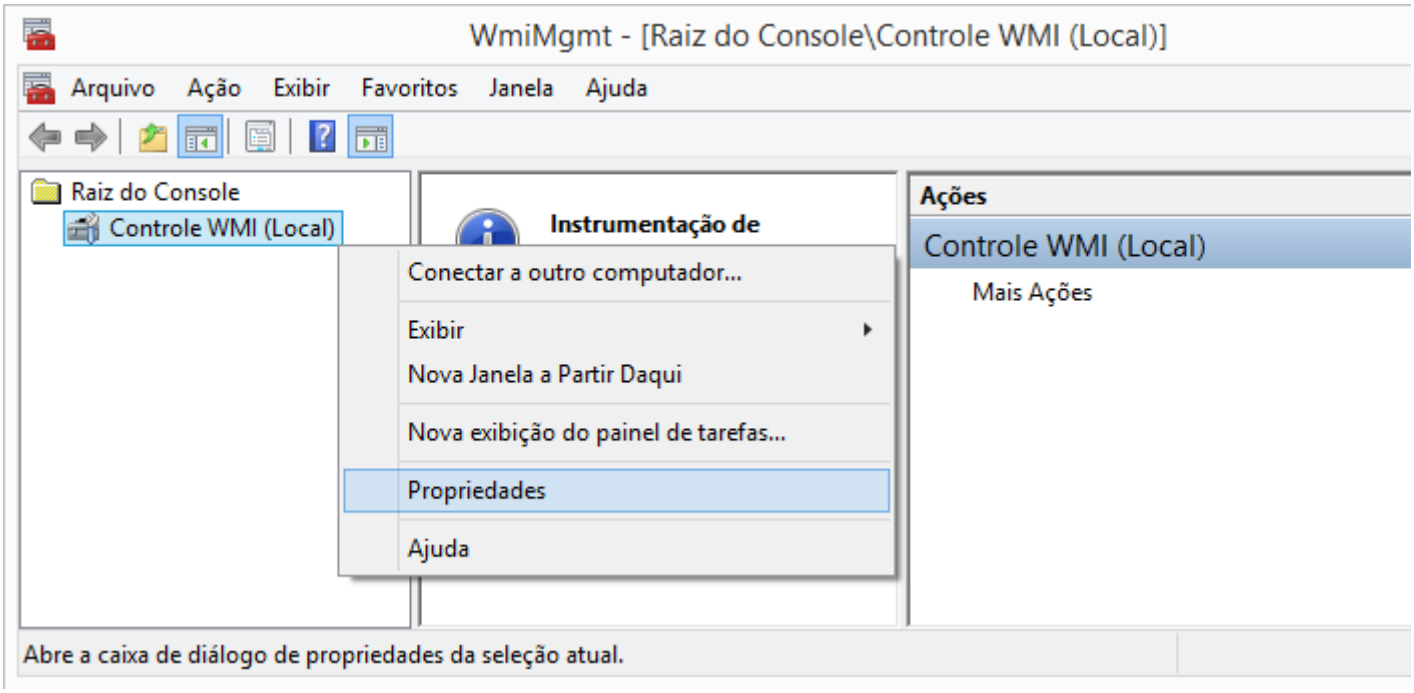


Configurando as permissões no WMI

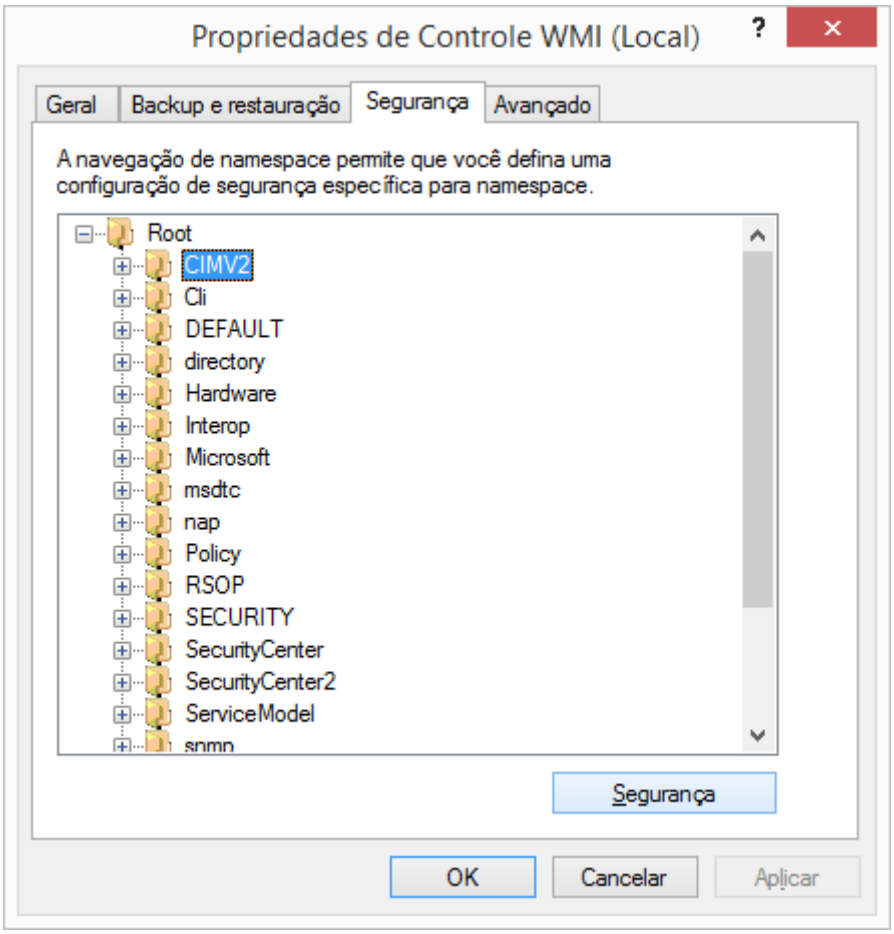
Logado como administrador, no prompt de comando digite:

```
wmimgmt.msc
```

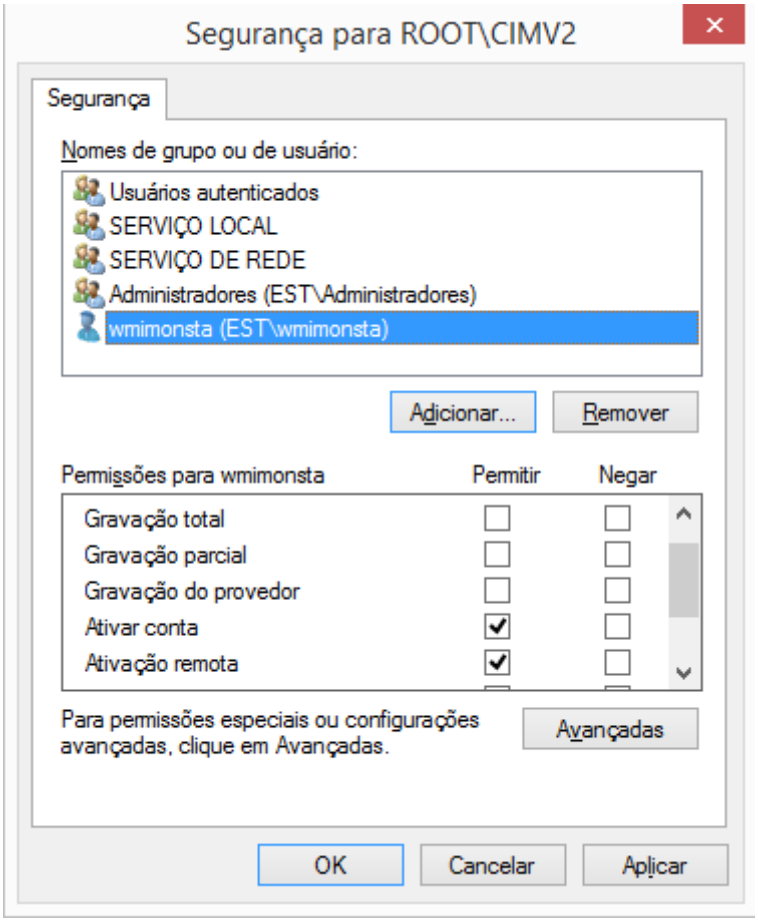
A seguinte tela será mostrada:



• Expanda o item “Raiz do Console”;
• Clique com o botão direito sobreo item “Controle WMI (Local)”;
• Selecione “Propriedades”;



• Selecione a aba “Segurança”
• Expanda o item “Root”
• Selecione o item “CIMV2”;
• Clique no botão “Segurança”;



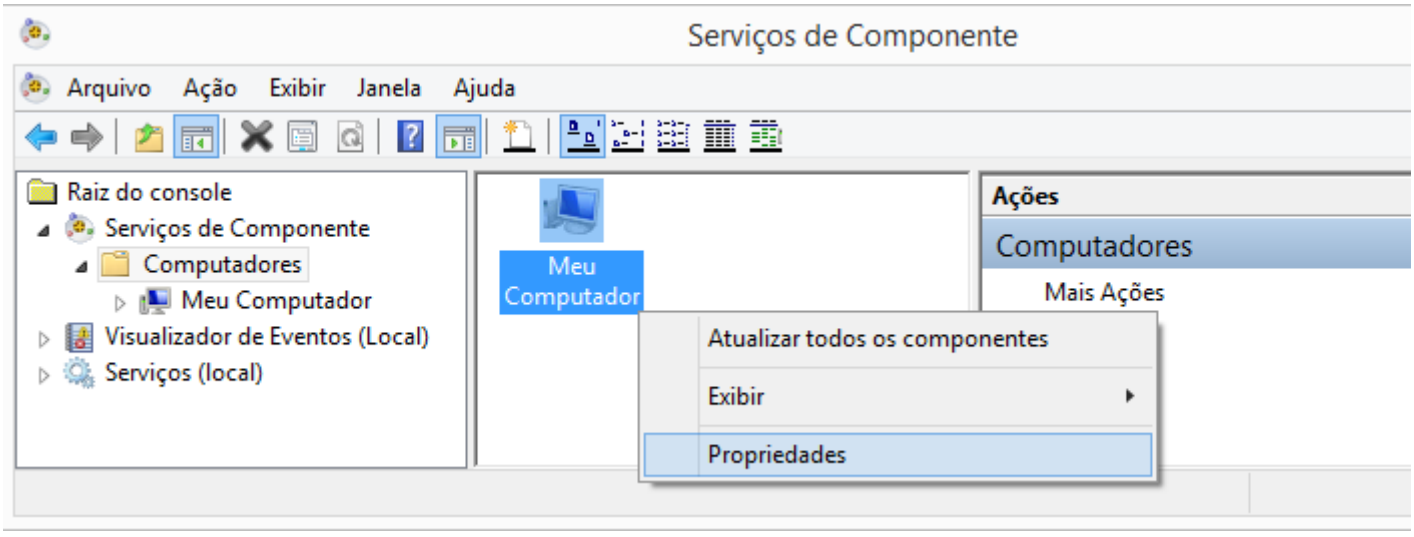
- Adicione o usuário“wmimonsta”;
- Marque o item “Ativar conta”;
- Marque o item “Ativação remota”;
- Clique no botão “Ok”;
- Clique no botão “Ok”;
- Feche a janela do Wmimgmt.

Configurando as permissões DCOM

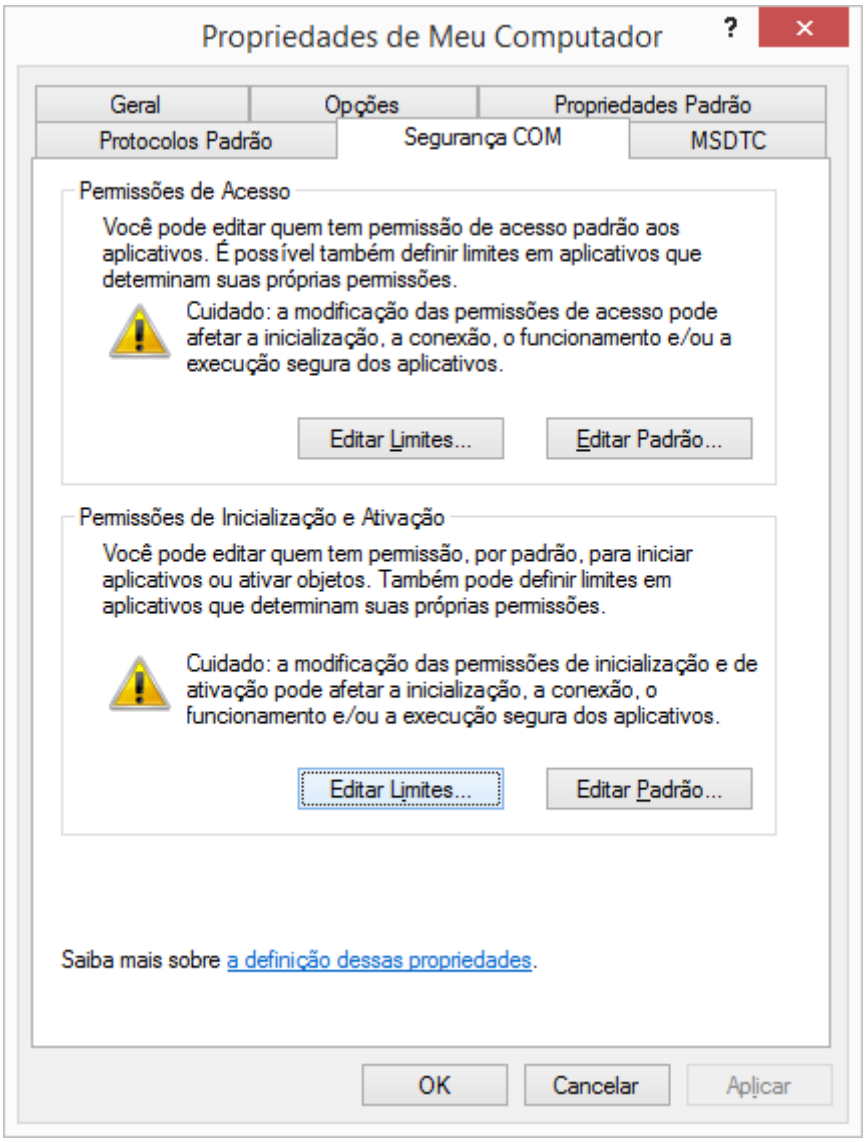
Logado como administrador, no prompt de comando digite:

```
dcomcnfg
```

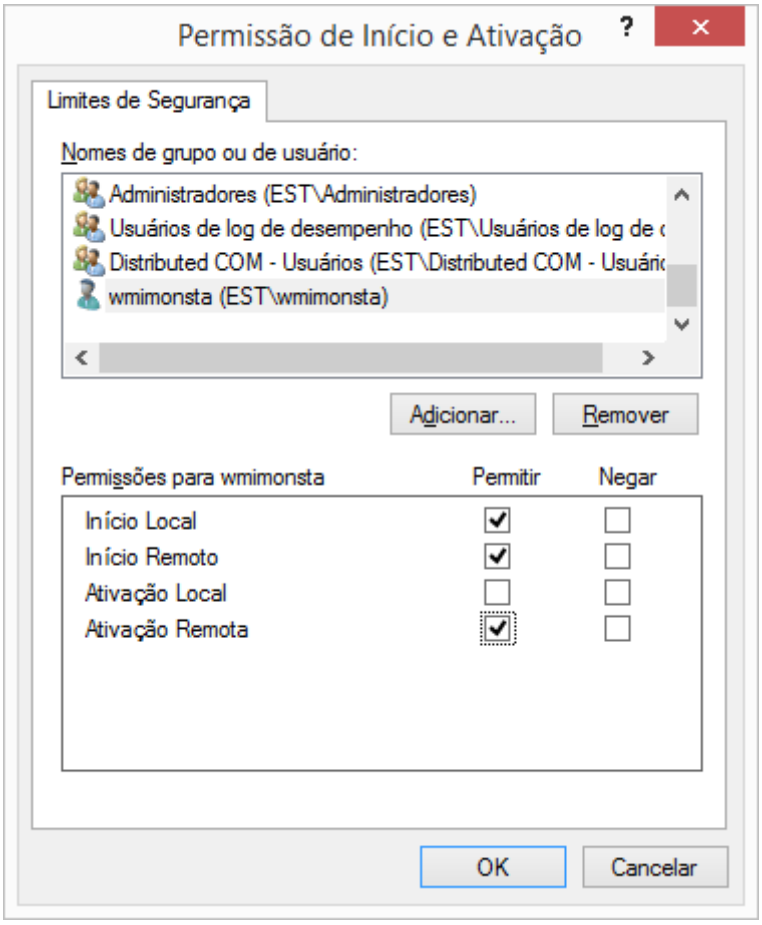
A seguinte tela será mostrada:



• Expanda o item “Raiz do Console”;
• Expanda o item “Serviços de Componente”;
• Expanda o item “Computadores”;
• Clique com o botão direito sobre o item “Meu Computador” e selecione “Propriedades”;



• Selecione a aba “Segurança COM”;
• Clique no botão “Editar Limites...” em Permissões de Inicialização e Ativação;



- Adicione o usuário wmimonsta;
- Marque as opções:
  - x Início Local
  - x Início Remoto
  - x Ativação Remota
- Clique no botão “Ok”
- Clique no botão “Ok”
- Feche a janela dos “Serviços de Componente”.

Configurando o Firewall do Windows

Logado como administrador, no prompt de comando digite os comandos abaixo:

```
netsh advfirewall firewall add rule dir=in name="DCOM"
program=%systemroot%\system32\svchost.exe service=rpcss action=allow protocol=TCP
localport=135
netsh advfirewall firewall add rule dir=in name ="WMI"
program=%systemroot%\system32\svchost.exe service=winmgmt action = allow protocol=TCP
localport=any
netsh advfirewall firewall add rule dir=in name ="UnsecApp"
program=%systemroot%\system32\wbem\unsecapp.exe action=allow
netsh advfirewall firewall add rule dir=out name ="WMI_Saída"
program=%systemroot%\system32\svchost.exe service=winmgmt action=allow protocol=TCP
```

```
localport=any
netsh advfirewall firewall add rule name=”ICMP Allow incoming V4 echo
request”protocol=icmpv4:8,any dir=in action=allow
```

Configurando permissões de acesso ao Service Control Manager

Logado como administrador, no prompt de comando digite o comando abaixo:

```
sc sdset SCMANAGER
D:(A;;CCLCRPRC;;;AU)(A;;CCLCRPWPRC;;;SY)(A;;KA;;;BA)S:(AU;FA;KA;;;WD)(AU;OIIOFA;GA;;;WD)
```

Agora faz-se necessário desabilitar o UAC (User Account Control) no registro do Windows para que todos os serviços possam ser listados para contas que não sejam administrador. Para fazer isso, siga o procedimento abaixo:

• Execute o regedit com permissões de administrador:

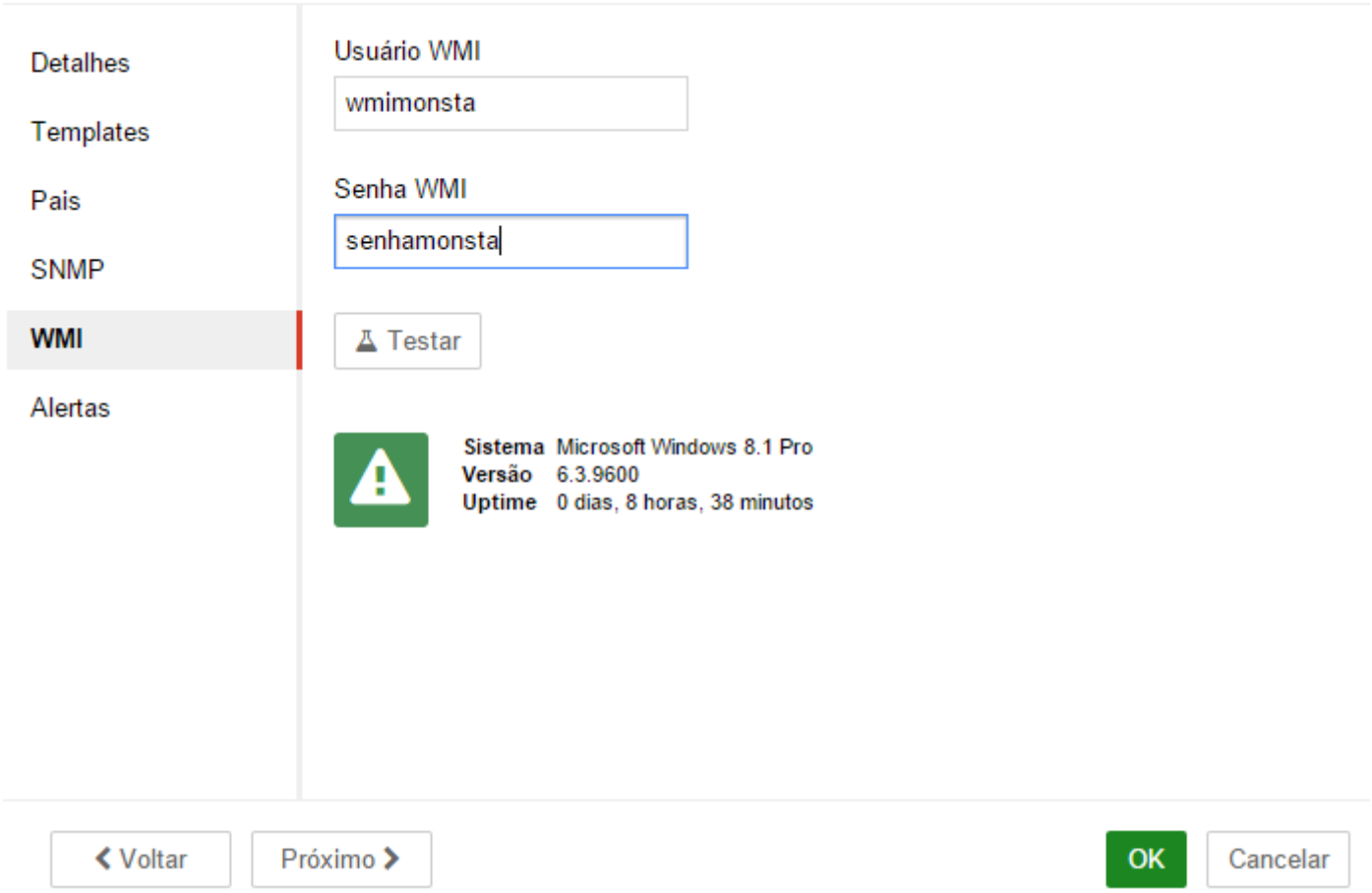
> Atenção: Alterações incorretas no registro do windows pode fazer seu computador não iniciar mais. Para sua segurança, faça um backup do registro antes de modificá-lo.

```
regedit
```

• Acesse a estrutura HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
• Localize ou crie a chave “LocalAccountTokenFilterPolicy” com o tipo DWORD e modifique o valor para 1.

Testar o usuário e senha no Monsta

Acesse o Monsta, clique no ícone para editar o dispositivo, clique na aba WMI e teste o usuário e senha criados para essa funcionalidade conforme tela abaixo:



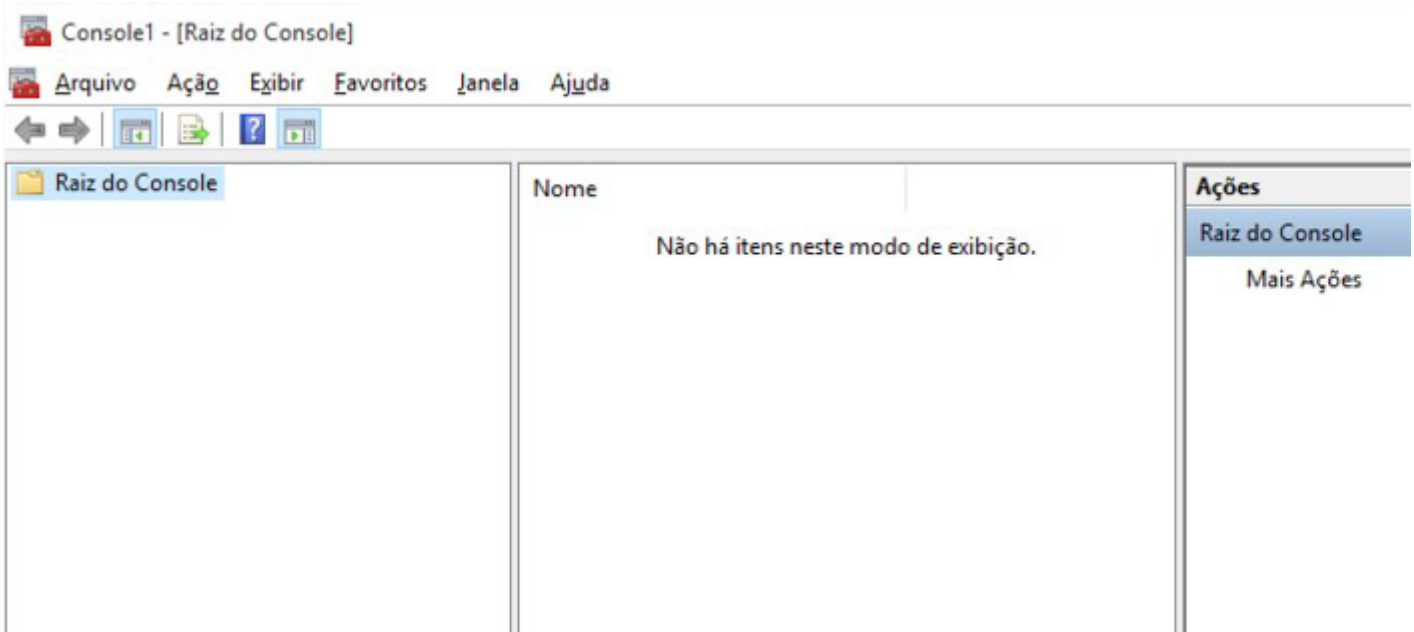
Configurações adicionais para WMI com Active Directory

Nos servidores onde o usuário wmimonsta foi criado dentro do domínio do Active Directory, as configurações abaixo são necessárias para cada servidor/estação que se deseja monitorar.

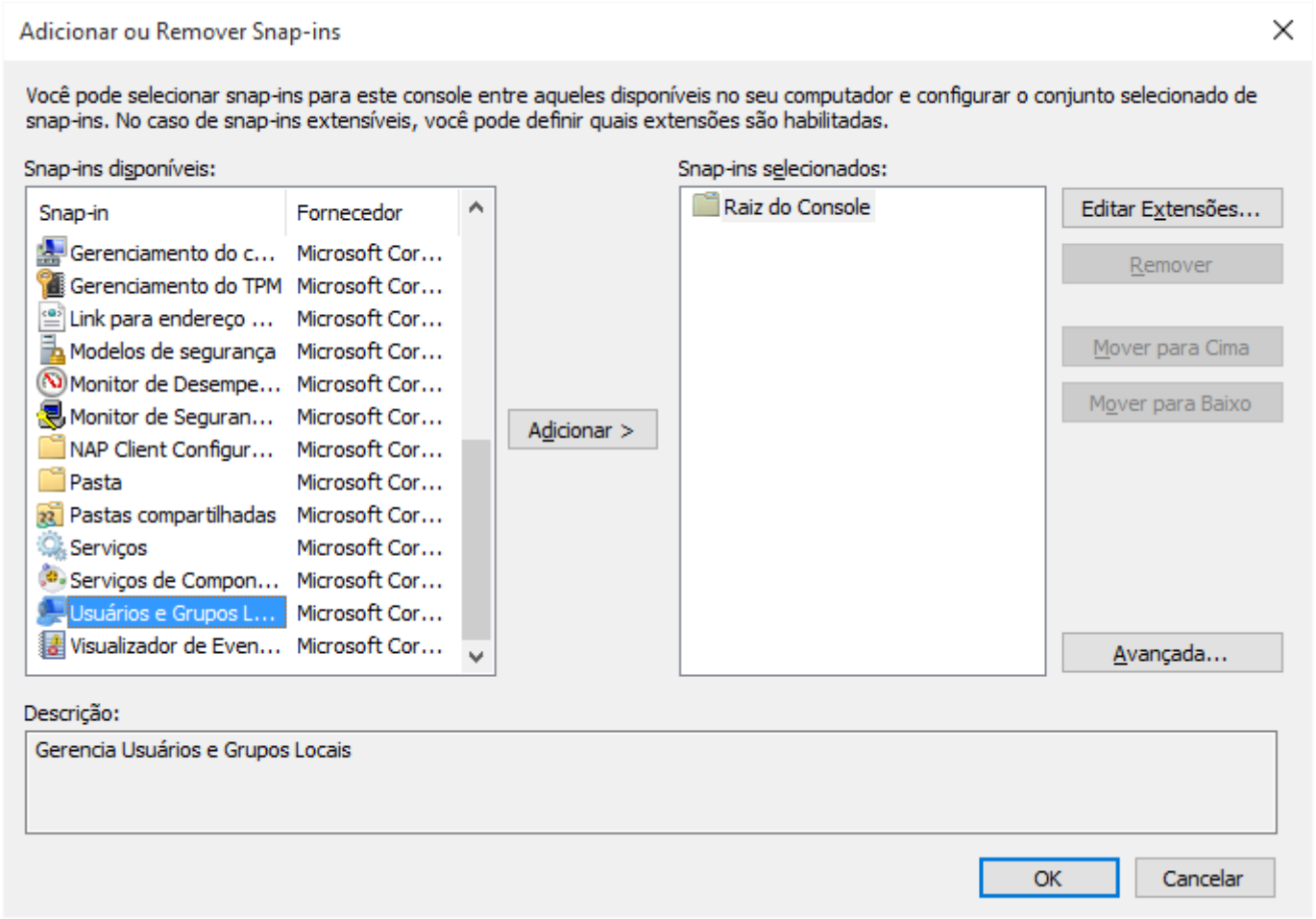
No(s) servidor(es) controlador(es) de domínio, adicione o grupo “Admins do Domínio” para o usuário wmimonsta criado no domínio. Nos demais servidores/estações, logado como Administrador, no prompt de comando digite:

```
mmc
```

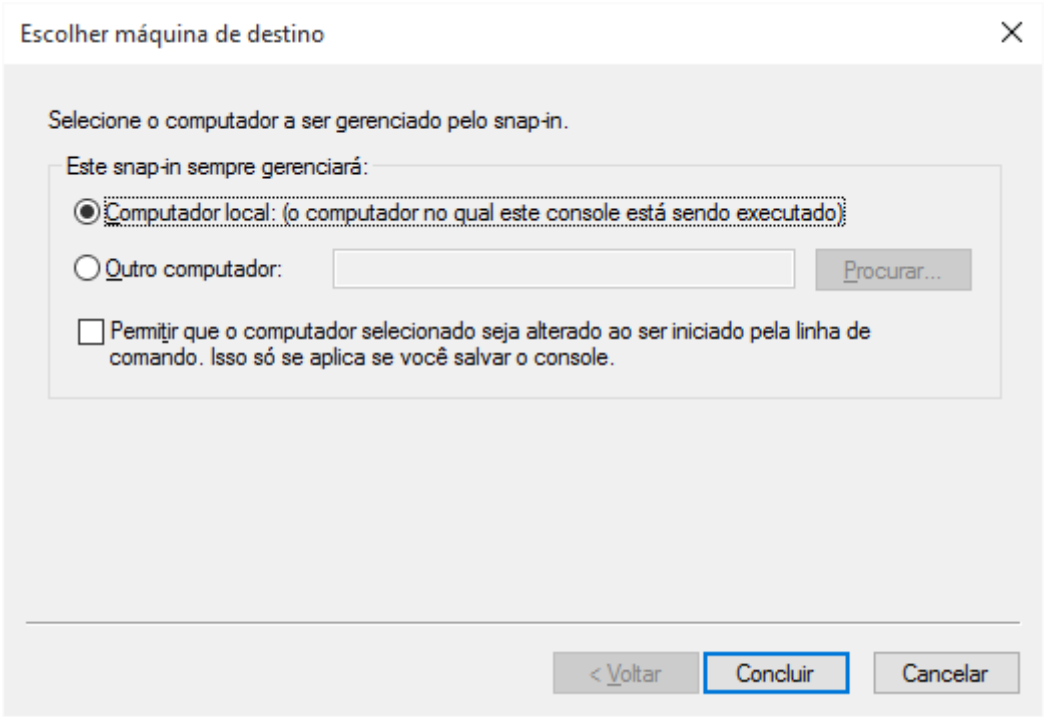
A seguinte tela será mostrada:



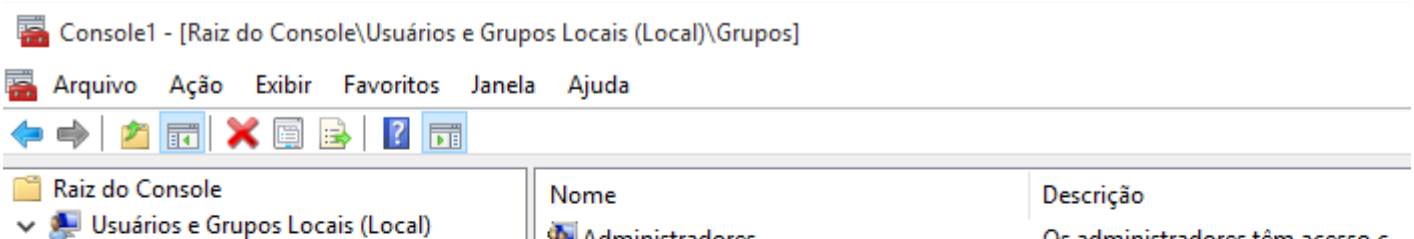
• Clique no menu “Arquivo” e selecione a opção “Adicionar/remover snap-in...”;



• Na aba “Snap-in disponíveis” selecione “Usuários e Grupos Locais”;• Clique no botão “Adicionar”;



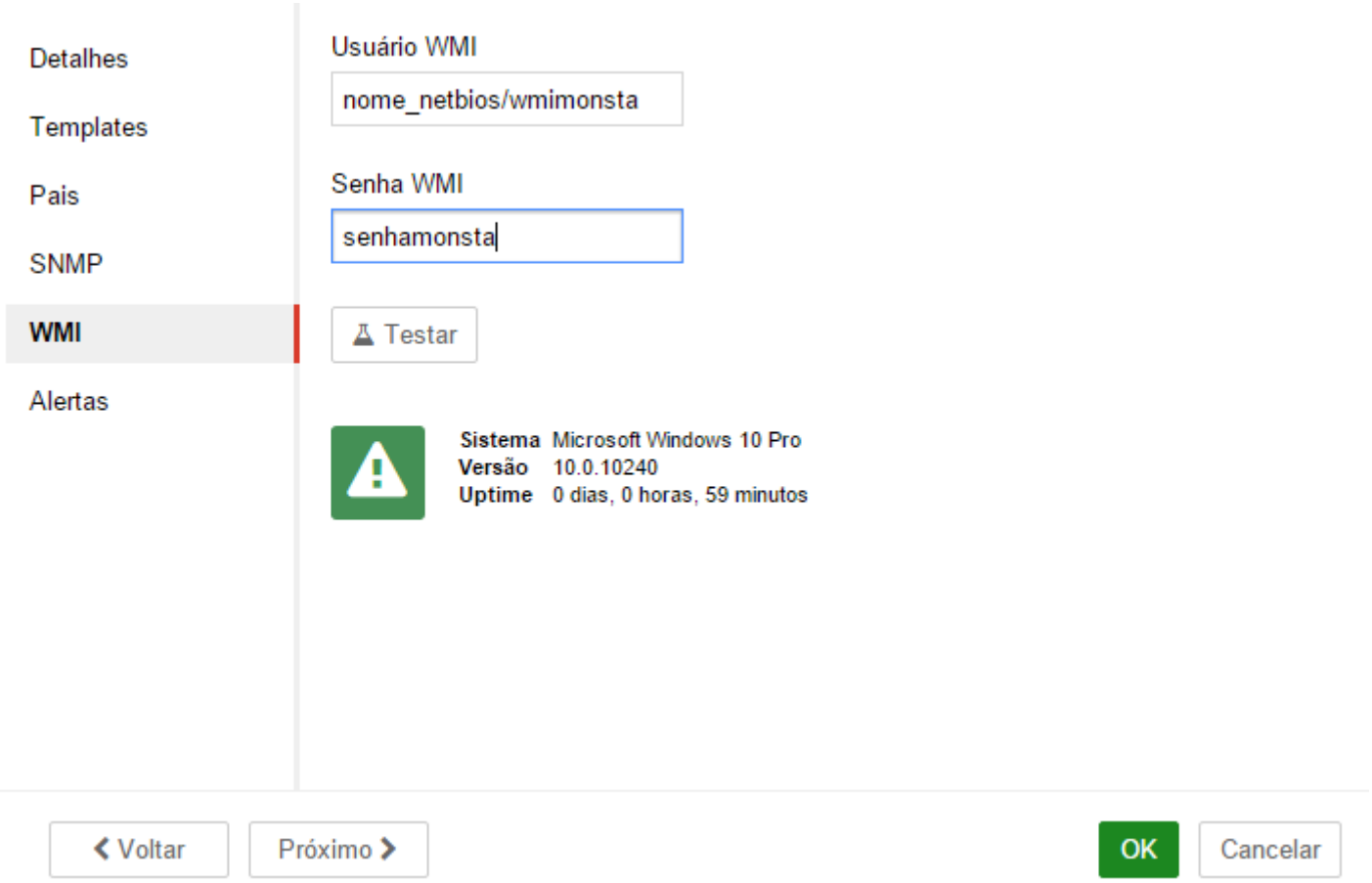
• Selecione a opção do Computador Local e clique no botão “Concluir”;
• Clique no botão “Ok”;



• Expanda o item “Usuários e Grupos”;
• Clique em “Grupos”;
• Clique com o botão direito no grupo “Usuários de monitor de desempenho” e selecione “Propriedades”;
• Adicione o usuário wmimonsta criado no domínio e clique no botão “Ok”;

Configurar usuário e a senha para acesso ao WMI no Monsta

• No Monsta, edite o dispositivo que irá utilizar o recurso de WMI;



• Selecione a aba “WMI”;
• No campo “Usuário WMI”, informe o nome Netbios do servidor/estação monitorado seguido pelo usuário, conforme figura ao lado;
• No campo “Senha WMI” informe a senha do usuário wmimonsta;
• Clique no botão “Testar” e verifique se o Monsta consegue se comunicar com o dispositivo;
• Clique em Ok.

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

SONDA - MONITORAMENTO WINDOWS

A sonda coletora do Monsta é um software utilizado para interagir com os sistemas operacionais Windows pela plataforma de monitoramento Monsta. Seu intuito é coletar métricas de WMI através da API disponibilizada pela própria Microsoft e também interagir através dos programas disponibilizados por linha de comando ou Power Shell.

Habilitar o coletor WMI no Monsta

Acesse com um usuário root o servidor Linux onde o Monsta está instalado e execute os comandos abaixo:

```
yum install -y wget
cd /opt/monsta/bin
mv wmic wmic.backup
wget https://www.monsta.com.br/monsta/download/wmic --no-check-certificate
chmod ugo+x /opt/monsta/bin/wmic
```

Instalação da Sonda

- Baixe o programa da sonda no sistema operacional Windows que deseja monitorar;

DOWNLOAD

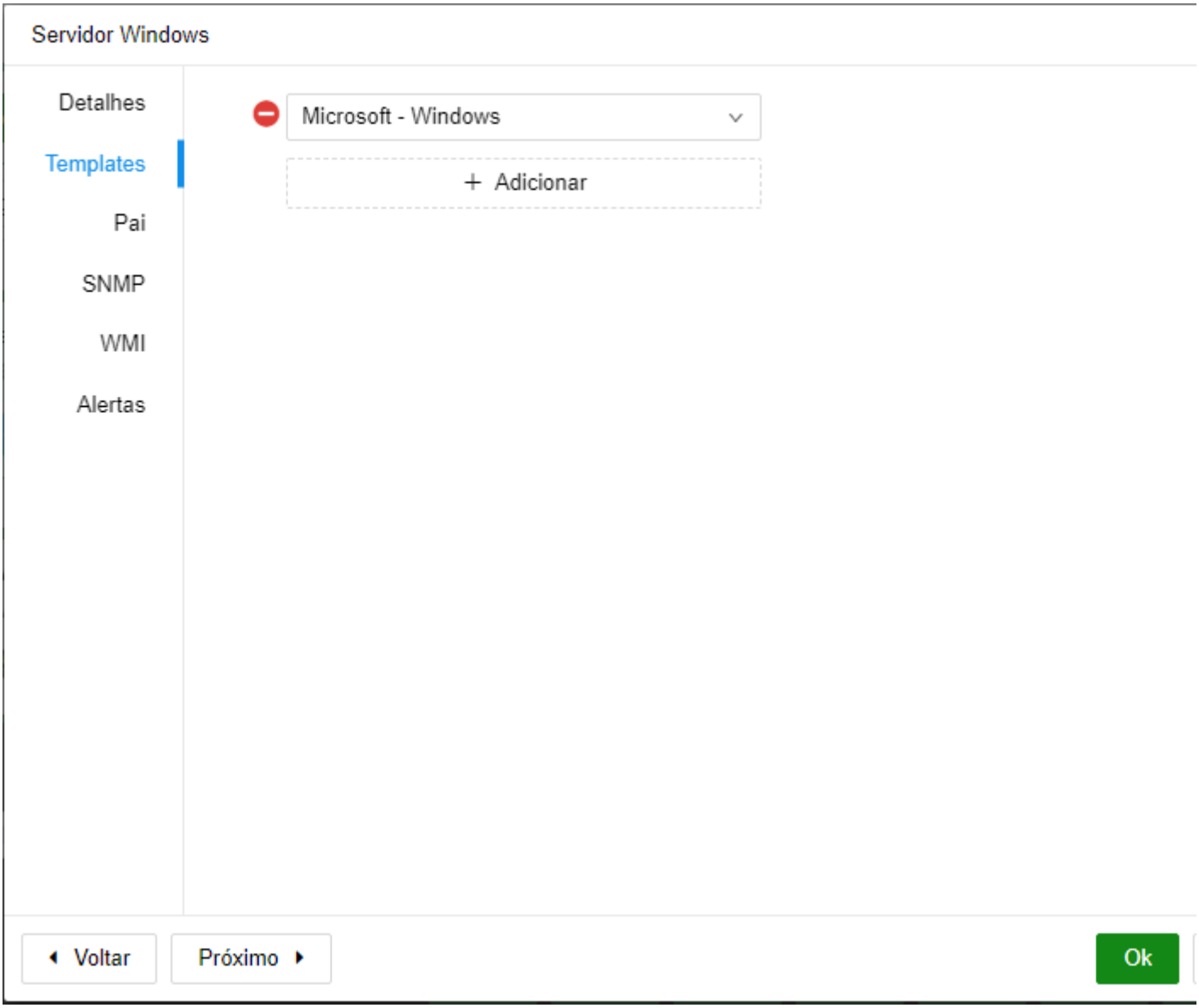
https://www.monsta.com.br/monsta/download/MonstaProbe.exe (64bits)

- Logado com um usuário administrador, execute o instalador "MonstaProbe.exe" (consulte "Opções" para maiores informações);
- Configure os parâmetros de porta e senha que serão solicitados durante a instalação.

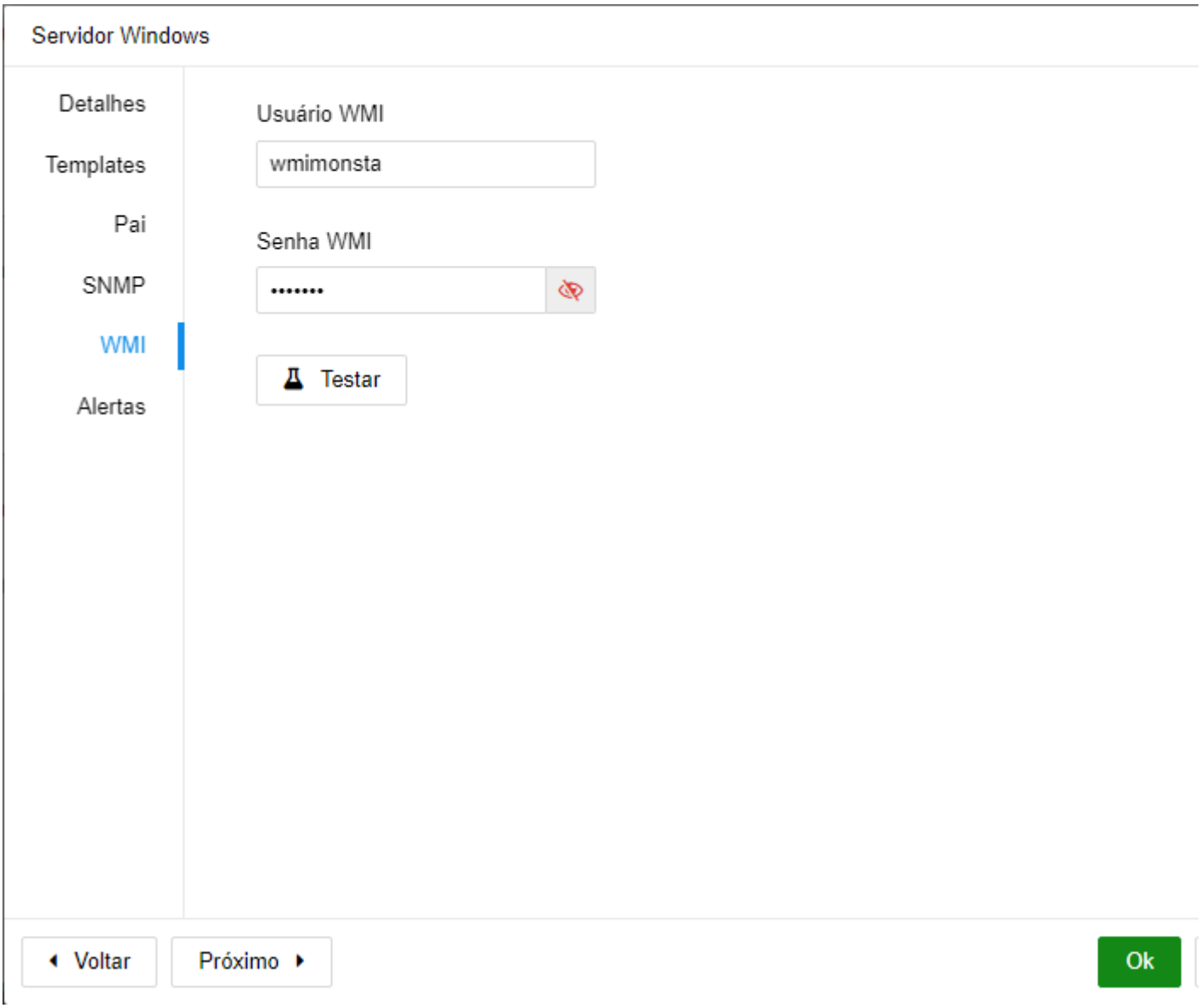
> **port:** É a porta que será utilizada pela sonda para o Monsta conectar. O padrão é 7744 (TCP).
> **password:** É a senha de autenticação para a sonda no computador instalado. O padrão é monsta@dm.

Configuração no Monsta

Dentro do Monsta, ao criar um dispositivo, apenas configure-o para utilizar os templates da Microsoft.



E preencha o campo "Usuário WMI" com qualquer informação (ele será descartado futuramente) e o campo "Senha WMI" com a senha informada na instalação da sonda.



Após criar o dispositivo você já pode utilizar os monitores disponíveis do template.

Opções

O instalador MonstaProbe.exe aceita opções na linha de comando. Você pode utilizá-las para automatizar a instalação em uma rede através de uma GPO, sem necessidade de interação com a interface gráfica.

--agree	Aceita o termo de uso da sonda coletora.
--port	Informa a porta a ser utilizada pela sonda coletora. Se não for informada, o padrão será 7744 (TCP).
--passwd	Atribui a senha a ser utilizada pela sonda coletora. A senha padrão será *monsta@dm* caso não seja informada.

EXEMPLO:
c:\> MonstaProbe.exe --agree --port 1234 --passwd senha

Contato

Monsta Tecnologia Ltda

Site: http://www.monsta.com.br

Downloads: http://www.monsta.com.br/download.html

E-mail: contato@monsta.com.br

MONSTA
MONITORAMENTO DE REDES