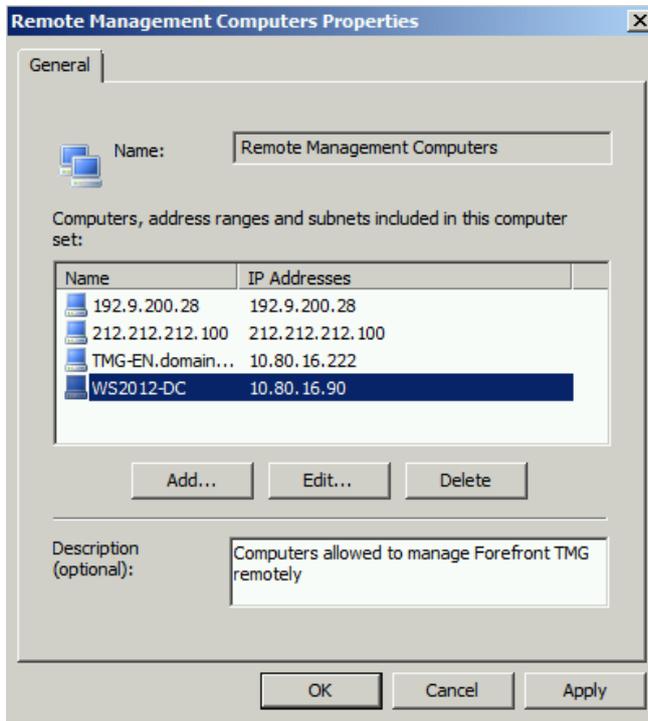


Allow Windows Remote Access to Forefront TMG

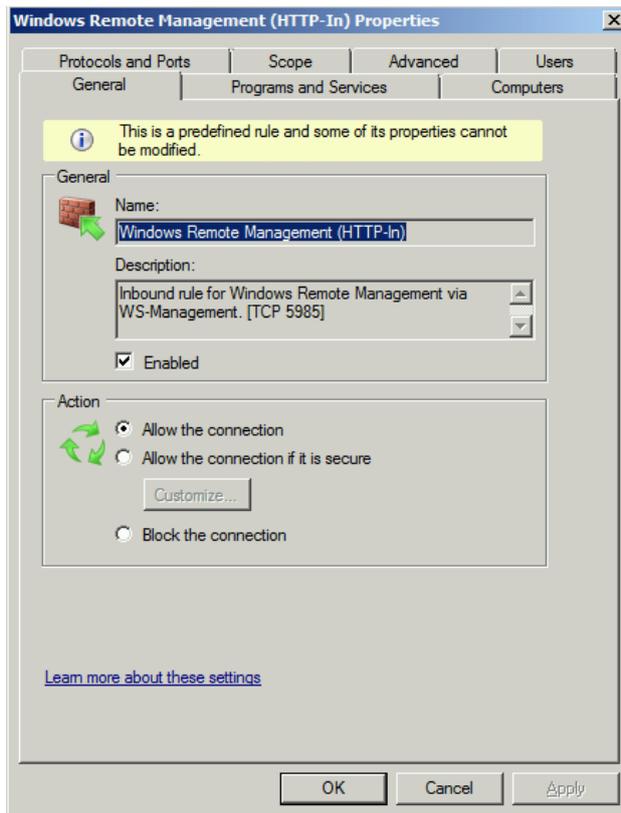
Add the machine from where you want to remote control the TMG Server to the Remote Management Computers System Policy in Forefront TMG



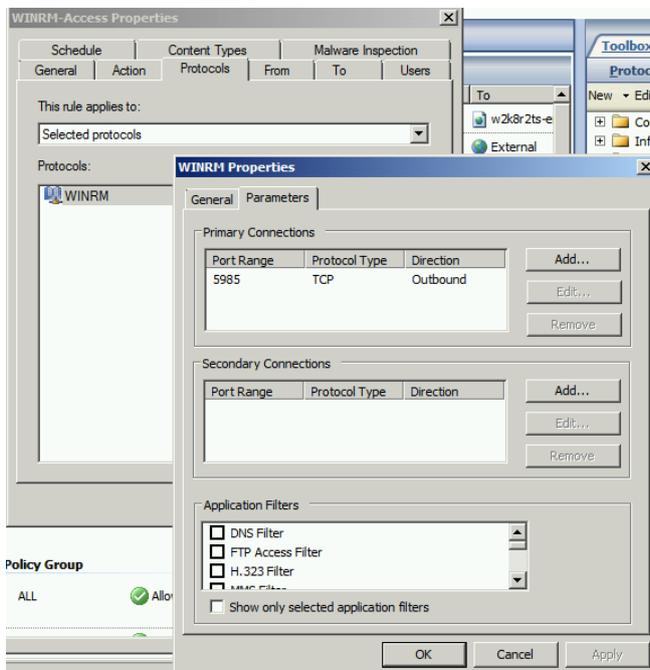
Configure TMG Server to accept WS-MAN request for the WinRM Listener

```
Administrator: Command Prompt
C:\Users\administrator.WIN2012>winrm quickconfig
WinRM is not set up to receive requests on this machine.
The following changes must be made:
Start the WinRM service.
Make these changes [y/n]? y
WinRM has been updated to receive requests.
WinRM service started.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:
Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this
machine.
Enable the WinRM firewall exception.
Make these changes [y/n]? y
WinRM has been updated for remote management.
Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this
machine.
WinRM firewall exception enabled.
C:\Users\administrator.WIN2012>
```

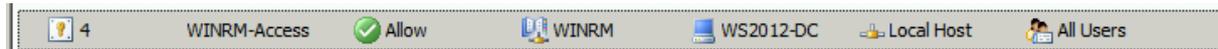
A Windows Firewall rule will be created in the Windows Personal Firewall



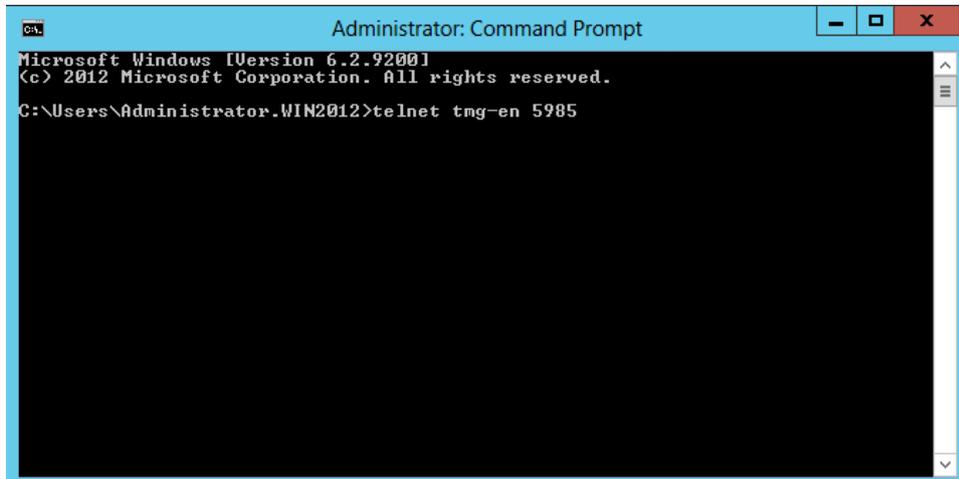
Because Forefront TMG takes control over the Windows Firewall with WFP we must create a protocol definition for WINRM (default port 5985 TCP Outbound)



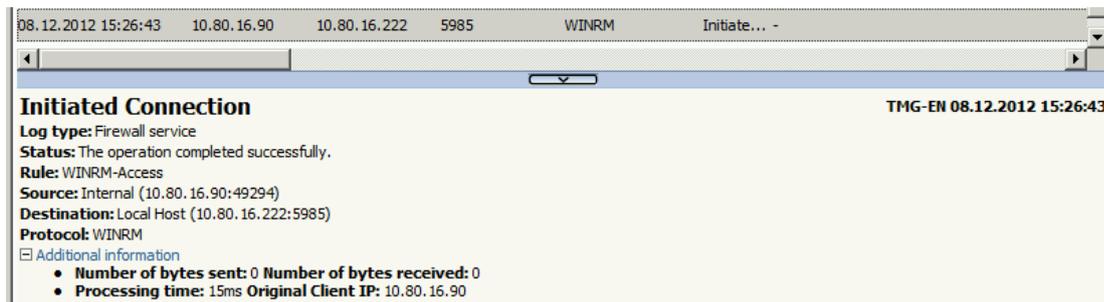
We also have to create a Firewall Policy rule which allows the Computer (my DC for this article) to allow WINRM access to the TMG Server (LOCALHOST).



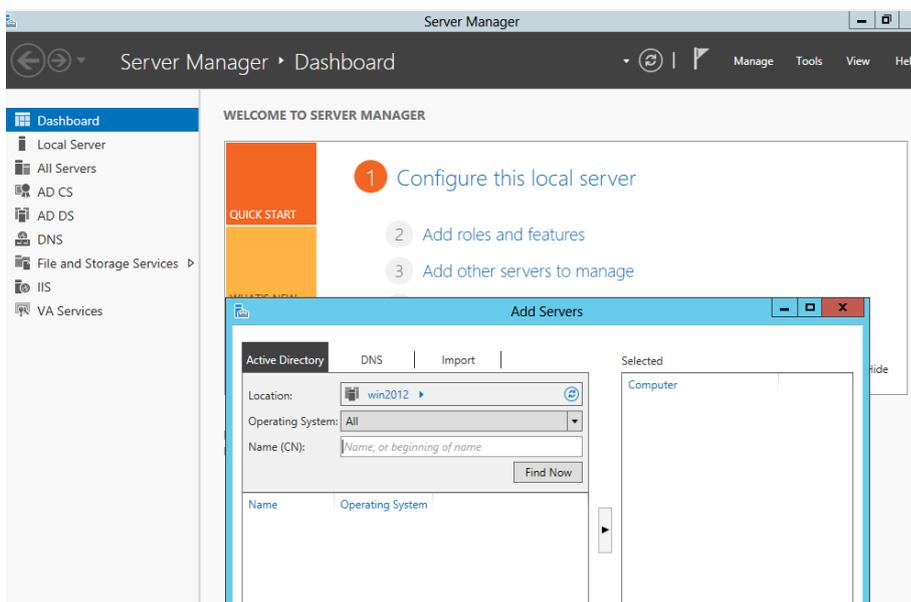
Test the connection to port 5985 with Telnet



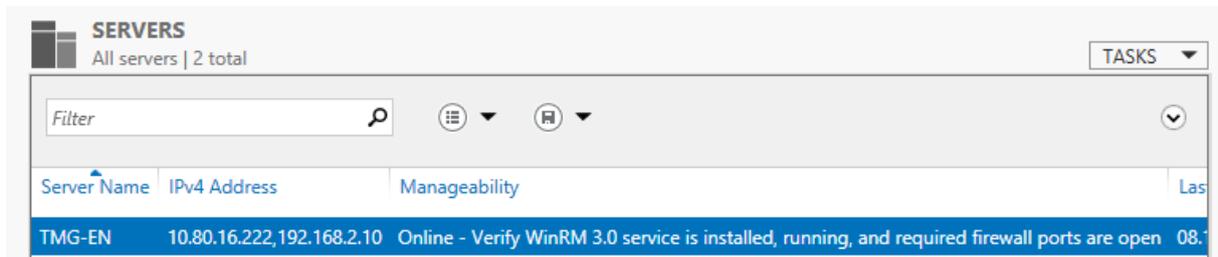
Test successful



Add TMG Server to Server Manager in Windows Server 2012

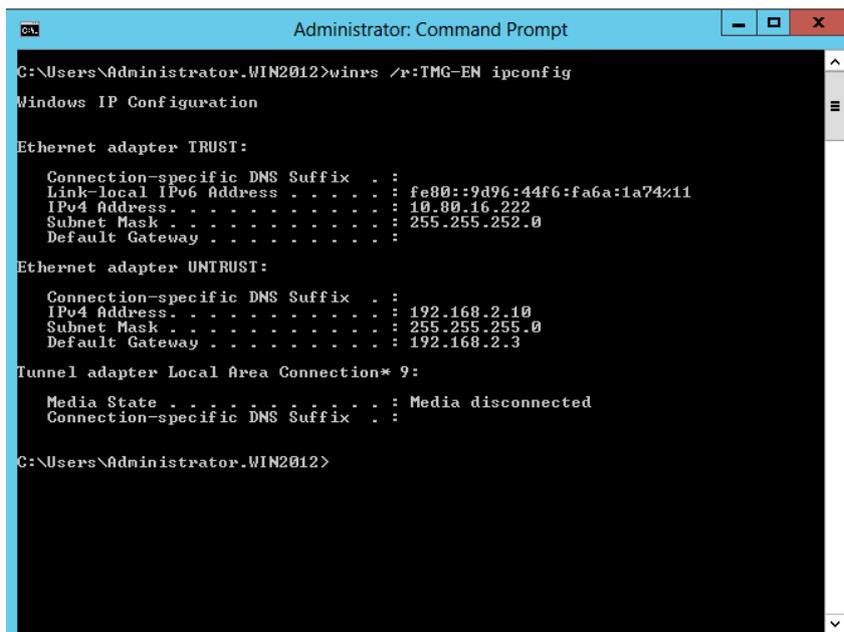


Test connectivity



Server Name	IPv4 Address	Manageability
TMG-EN	10.80.16.222, 192.168.2.10	Online - Verify WinRM 3.0 service is installed, running, and required firewall ports are open 08:...

Test a Remote connection with WINRS



```
C:\Users\Administrator.WIN2012>winrs /r:TMG-EN ipconfig
Windows IP Configuration

Ethernet adapter TRUST:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::9d96:44f6:fa6a:1a74%11
    IPv4 Address. . . . . : 10.80.16.222
    Subnet Mask . . . . . : 255.255.252.0
    Default Gateway . . . . . : 

Ethernet adapter UNTRUST:

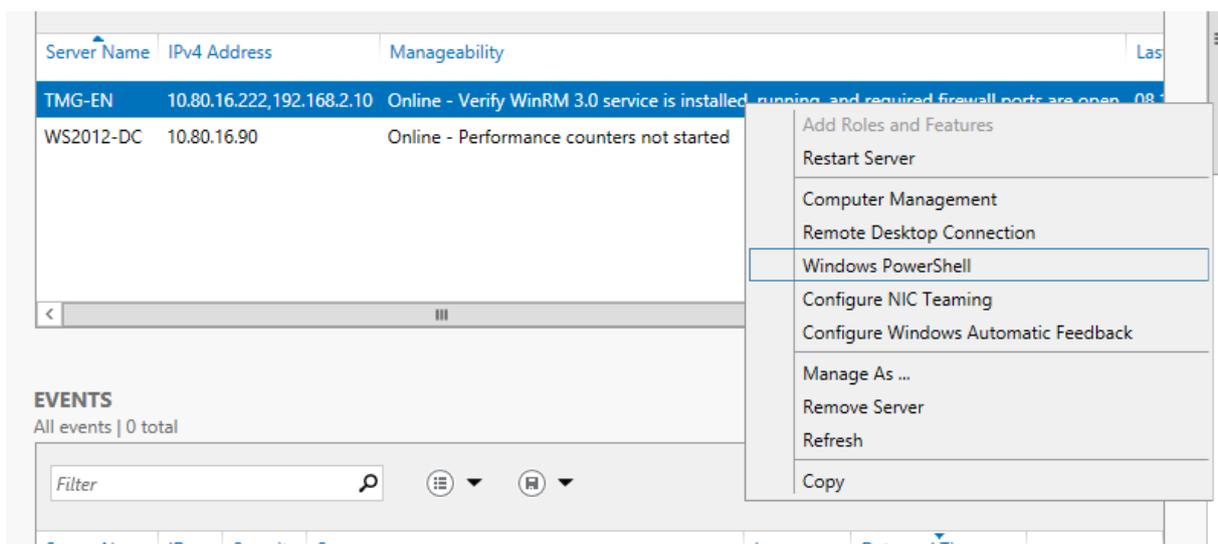
    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 192.168.2.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.3

Tunnel adapter Local Area Connection* 9:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Administrator.WIN2012>
```

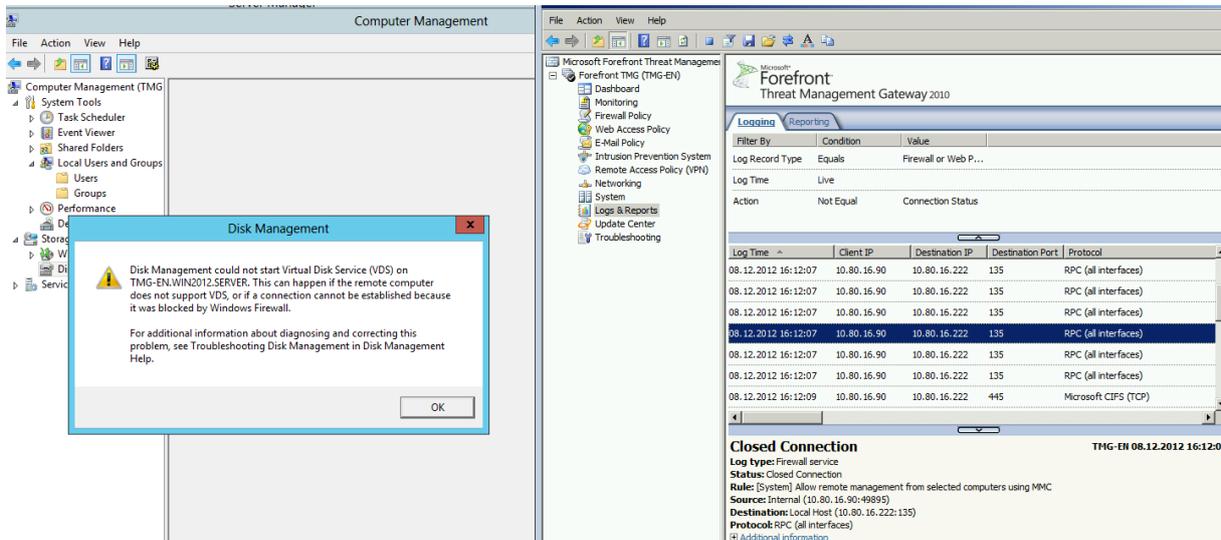
Remote Management of the TMG Server



Server Name	IPv4 Address	Manageability
TMG-EN	10.80.16.222, 192.168.2.10	Online - Verify WinRM 3.0 service is installed, running, and required firewall ports are open 08:...
WS2012-DC	10.80.16.90	Online - Performance counters not started

- Add Roles and Features
- Restart Server
- Computer Management
- Remote Desktop Connection
- Windows PowerShell
- Configure NIC Teaming
- Configure Windows Automatic Feedback
- Manage As ...
- Remove Server
- Refresh
- Copy

Remote Management works with the classic exceptions for example for remote Disk Management where the RPC filter of TMG blocks the requests



If we disable the RPC-Filter in TMG we will be able to connect to Disk Management for example

