

# Hyper-V Remote Management Configuration Script

## Contents

- Hyper-V Remote Management Configuration Script..... 1
- Introduction ..... 3
- License..... 4
- Quick start guide ..... 4
- About..... 5
- Installation & Removal..... 5
- Hyper-V Release To Manufacturing (RTM) ..... 6
- Hyper-V Remote Management Configuration Steps ..... 7
- Server Usage ..... 8
  - Elevation requirements..... 8
  - Displaying the current server settings ..... 8
    - Server verification. .... 9
    - WMI Security..... 9
    - Authorization Manager Policy Store ..... 10
    - Distributed COM Users ..... 11
    - COM Security for Launch and Activation Permissions ..... 11
    - Firewall Settings (Hyper-V server rules)..... 12
    - Firewall Settings (Remote WMI) ..... 12
    - IP Configuration ..... 13
    - Latest version verification..... 13
    - Warnings and Errors summary ..... 14
  - Granting a user permission to remotely manage Hyper-V ..... 15
  - Removing user permissions for remotely manage Hyper-V ..... 16
  - Advanced parameters ..... 17
- Client Usage ..... 18
  - Elevation requirements..... 18
  - Display the current settings ..... 18
    - Basic information. .... 18
    - COM Security for Access Permissions ..... 19

ANONYMOUS LOGON remote access to Distributed COM .....	19
Firewall settings for Hyper-V Management Clients .....	20
Firewall exception for Microsoft Management Console (mmc.exe) .....	20
IP Configuration .....	21
Stored Credential summary .....	21
Warnings and Errors summary .....	22
Change ANONYMOUS LOGON remote access to Distributed COM setting .....	22
Change Windows Firewall settings for Hyper-V Management Clients .....	22
Additional Options .....	24
debug .....	24
noversioncheck .....	24
Troubleshooting.....	25
Future Enhancements.....	26

## Introduction

HVRemote was developed by [John Howard](#), Senior Program Manager in the Hyper-V team at Microsoft Corporation, November 2008. To contact me, follow the blog hyperlink above and use the email option. If you find a bug or want to suggest an improvement, please drop me an email or add a comment to the blog post announcing this tool. Of course, I'd love to hear from you if you find it useful.

HVRemote was developed to avoid the manual steps required for remote configuration as I documented in March 2008 on my blog, in these five parts: [1](#), [2](#), [3](#), [4](#) and [5](#). The official Microsoft documentation is at <http://technet.microsoft.com/en-us/library/cc794756.aspx>, which, at the time of writing, covers the domain joined scenario only.

Typically, without remote management configuration, you will get the error *"You do not have the required permission to complete this task. Contact the administrator of the authorization policy for the computer 'COMPUTERNAME'."*

Version	Date	Change History
0.1	10 <sup>th</sup> November 2008	First draft
0.2	14 <sup>th</sup> November 2008	Explaining additional capabilities added since 0.1
0.3	19 <sup>th</sup> November 2008	Clarifications, typo corrections and additional capabilities, largely based on feedback from <i>lots</i> of people. Thank you!  Script changes: <ul style="list-style-type: none"><li>- Check for elevation if needed</li><li>- Corrected error message if not elevated</li><li>- Outputs currently logged on user</li><li>- Checks for System Center Virtual Machine Manager</li><li>- Outputs Machine access permissions (client)</li><li>- Outputs Machine launch and activation perms (server)</li><li>- Graceful error handling if firewall disabled or not running</li><li>- Latest version check</li></ul>
0.4	7 <sup>th</sup> January 2009	More clarifications based on your feedback. Again, thank you!  Script changes: <ul style="list-style-type: none"><li>- Checks for problem (eg disabled) accounts on server side</li><li>- Displays a summary of warnings/errors at end</li><li>- Fixed a bug where hvremote on its own had no output</li><li>- Outputs IP Configuration (saves me keep asking)</li><li>- Outputs list of stored credentials in cmdkey</li><li>- Vista check for known unsupported SKUs</li><li>- Vista check for KB952627 being installed</li><li>- Fixed a problem a couple of users hit with ADs reference</li><li>- Fixed silly capitalization mistake</li><li>- Some really minor other fixes not worth enumerating.</li></ul>

## License

HVRemote and this document are licensed as described at <http://code.msdn.microsoft.com/HVRemote/Project/License.aspx>.

HVRemote and the associated documentation are provided “as-is”. You bear the risk of using it. No express warranties, guarantees or conditions are provided. It is not supported or endorsed by Microsoft Corporation and should be used at your own risk.

### Note

If your server is being managed by System Center Virtual Machine Manager 2008, you should not use this script. As of version 0.3 of the script, a check is made by the script.

## Quick start

The 5 second guide for the most common configuration steps....:

1. Add a user rights to remotely access Hyper-V.

On the server, from an elevated command prompt, run:

```
cscript hvremote.wsf /add:domain\user (if machine is in a domain)     or  
cscript hvremote.wsf /add:user                     (if machine is in a workgroup)
```

2. Add a firewall exception for the Microsoft Management Console on the client if using Vista or Windows 7 client (not needed on Windows Server 2008 or Windows Server 2008 R2).

On the client, from an elevated command prompt, run:

```
cscript hvremote.wsf /mmc:enable
```

3. Allow anonymous DCOM access on the client if the client and server are both in workgroups, or the client and server are in *untrusted* domains (this is not needed for trusted domains or the same domain).

On the client, from an elevated command prompt, run:

```
cscript hvremote.wsf /anondcom:grant
```

4. Reboot server *and* client if this is the first time some reconfiguration has been done.

## About

HVRemote can configure both server and client remote management settings for Hyper-V. It is written in VBScript as this is a common scripting platform available on all SKUs where this script can run.

### Server support

- Windows Server 2008 with the Hyper-V role enabled (only available on x64 editions)
  - Both server Core and full installations
- Microsoft Hyper-V Server 2008.
- Windows Server 2008 R2 with the Hyper-V role enabled <sup>1</sup>

### Client support

- Windows Server 2008 x86 Full installations
- Windows Server 2008 x64 Full installations (both with and without the Hyper-V role enabled)
- Windows Vista SP1 Business, Enterprise and Ultimate SKUs
- Windows 7 Client (Business, Enterprise and Ultimate) <sup>1</sup>

Note that not all operating system SKUs support Hyper-V or the Hyper-V Remote Management tools. In particular, server SKUs “without Hyper-V” and web edition cannot run Hyper-V or the Hyper-V remote management tools.

The script is designed to be locale neutral, meaning that it will configure any language operating system instance. (I have verified on English and Japanese server installations, and I have reports of it working on German locales ☺). However, all text output is English only.

The script is designed to cover configuration of all combinations of workgroup and domain joined server and client. (Note that if client and server are in untrusted domains, from a configuration perspective, it is the same as workgroup to workgroup)

## Installation & Removal

Copy HVRemote.wsf to a location on the target machine. It is recommended to create a new sub-directory such as C:\HVRemote in which to store the script. There is no install program, and HVRemote does not appear listed as an installed program. To remove HVRemote, delete HVRemote.wsf.

---

<sup>1</sup> Windows Server 2008 R2 and Windows 7 are in development at the time of writing. As at “Beta” release, HVRemote works.

## Hyper-V Release To Manufacturing (RTM)

The Hyper-V role on the “Shiny Media” of Windows Server 2008 is beta code. Hyper-V RTM was released in [June 2008](#) and is available for free download on both Windows Update and the Microsoft Download Centre. Note that remote management is not fully functional in Hyper-V Beta. Hence, you *must* install the Hyper-V RTM update, [KB950050](#). For upgrade considerations from pre-release versions (Beta, RC0 and RC1) to RTM, see [KB949222](#).

Note - The remote management components, Hyper-V Manager and Virtual Machine Connection on the shiny media are also beta components and must be updated, even if the Hyper-V role is not enabled, or the SKU is not capable of running the Hyper-V role.

No update is required for [Microsoft Hyper-V Server 2008](#).

The remote management components for Vista SP1 are not present in-box and can be installed by downloading and installing [KB952627](#). Once installed, Hyper-V Manager will be present under Control Panel, Administrative Tools.

The remote management components for Windows Server 2008 can be installed without the Hyper-V role. If the Hyper-V role is enabled (non server core installations), the Hyper-V management tools are automatically installed. To install the management tools without the Hyper-V server role, run “ocsetup Microsoft-Hyper-V-Management-Clients”. Alternatively, they are available for installation under Remote System Administration Tools (RSAT) in Server Manager.

## Hyper-V Remote Management Configuration Steps

Server side configuration (i.e. the machine running the Hyper-V role) consists of the following steps:

- 1) WMI Security permissions to the root\cimv2 namespace
- 2) WMI Security permissions to the root\virtualization namespace
- 3) Permission to the Authorisation policy store
- 4) Windows Firewall configuration for Hyper-V rules
- 5) Distributed COM remote access permission
- 6) (Optional) Windows Firewall configuration for WMI administration rules
- 7) (Optional) Disable IPSec policy if connection from management clients would be blocked

Client side configuration (i.e. the machine running Hyper-V Manager and Virtual Machine Connection) consists of the following steps:

- 1) Windows Firewall configuration for Hyper-V Remote Management Client rules
- 2) (In some scenarios:) ANONYMOUS LOGON remote DCOM access (<sup>2</sup>)
- 3) (In some scenarios:) cmdkey for credentials. (<sup>3</sup>)
- 4) Windows firewall exceptions for management tools

---

<sup>2</sup> See section "Change ANONYMOUS LOGON remote access to Distributed COM setting" for a description of when this is needed

<sup>3</sup> This is needed if the client is in a domain but the server is in a workgroup. Note that hvremote does **NOT** have a capability to set this and it must be done manually from an **UNELEVATED** command line. See part 5 of the blog post series, or run hvremote /show from a domain joined client machine for more information. The syntax is "cmdkey /add:ServerComputerName /user:ServerComputerName\UserName /pass"

## Server Usage

Note: “/mode:server” can be omitted if the Hyper-V role is detected as HVRemote will assume you are performing a server operation. The script must be run from an elevated command prompt for all server operations.

The basic server operations are to show the current settings, or to add or remove users or groups from Hyper-V remote access.

**To show the current settings:**                    hvremote [/mode:server] /show  
**To grant a user access:**                        hvremote [/mode:server] /add:domain\user  
**To remove a user access:**                    hvremote [/mode:server] /remove:domain\user

If the server is in a workgroup, you can use the alternate syntax for add and remove:

**To grant a user access:**                        hvremote [/mode:server] /add:user  
**To remove a user access:**                    hvremote [/mode:server] /remove:user

## Elevation requirements

All server operations must be run from an elevated command prompt. If you are running as a non-admin or from a “standard” command prompt, you will get the following message:

```
INFO: Computername is ADMINISTRATOR1
INFO: Computer is in workgroup WORKGROUP
INFO: Current user is ADMINISTRATOR1\user
INFO: Assuming /mode:server as the role is installed

*****
***** Must run from an elevated command prompt for all server operations
*****
```

## Displaying the current server settings

```
hvremote [/mode:server] /show
```

In /show mode, several sections of output are displayed. It may help to pipe the output to a text file and use notepad or another editor to examine the output.

### Tip

It is recommended that you use /show and save the output before any changes are made.

## Server verification.

Basic verification is that the server is running Hyper-V (by detecting the VMMS service) and that it is not running pre-release software.

```
INFO: Computername is ADMINISTRATOR1
INFO: Computer is in workgroup WORKGROUP
INFO: Current user is ADMINISTRATOR1\Administrator
INFO: Assuming /mode:server as the role is installed
INFO: This machine has the Hyper-U (v1) QFE installed <KB950050>
```

## WMI Security

This section is displayed once for the root\cimv2 namespace, and once for the root\virtualization namespace. The screenshot example below is for the root\cimv2 namespace

```
-----
DACL for WMI Namespace root\cimv2
Required for Hyper-U remote mangement: Allow, EnabAct, RemEnab, InheritAce
HURemote also sets NoPropInheritAce and ValidInheritFlags
-----
BUILTIN\Administrators    <$-1-5-32-544>
  Allow: Exec FullWrt PartWrt ProvWrt EnabAct RemEnab RdSec EdSec <393279>
  Flags: InheritAce InheritedAce ValidInheritFlags <18>
NT AUTHORITY\NETWORK SERVICE    <$-1-5-20>
  Allow: Exec ProvWrt EnabAct <19>
  Flags: InheritAce InheritedAce ValidInheritFlags <18>
NT AUTHORITY\LOCAL SERVICE    <$-1-5-19>
  Allow: Exec ProvWrt EnabAct <19>
  Flags: InheritAce InheritedAce ValidInheritFlags <18>
NT AUTHORITY\Authenticated Users    <$-1-5-11>
  Allow: Exec ProvWrt EnabAct <19>
  Flags: InheritAce InheritedAce ValidInheritFlags <18>
```

Each entry shows an ACE (Access Control Entry) for a user or group. To determine if a user has the minimum required access to the namespace for Hyper-V remote management, you are looking for the settings Allow, EnabAct, RemEnab and InheritAce. Note that HVRemote will automatically set NoPropInheritAce and ValidInheritFlags as in the example below.

```
ADMINISTRATOR1\user    <$-1-5-21-1233540721-2480008661-429491542-1000>
  Allow: EnabAct RemEnab <33>
  Flags: InheritAce NoPropInheritAce ValidInheritFlags <6>
```

## Authorization Manager Policy Store

```
-----
Contents of Authorization Store Policy
-----

Hyper-V Registry configuration:
- Store: msxml://C:\ProgramData\Microsoft\Windows\Hyper-V\InitialStore.xml
- Service Application: Hyper-V services

Application Name: Hyper-V services
Operation Count: 33

  100 - Read Service Configuration
  105 - Reconfigure Service
  200 - Create Virtual Switch
  205 - Delete Virtual Switch
  210 - Create Virtual Switch Port
  215 - Delete Virtual Switch Port
  220 - Connect Virtual Switch Port
  225 - Disconnect Virtual Switch Port
  230 - Create Internal Ethernet Port
  235 - Delete Internal Ethernet Port
  240 - Bind External Ethernet Port
  245 - Unbind External Ethernet Port
  250 - Change VLAN Configuration on Port
  255 - Modify Switch Settings
  260 - Modify Switch Port Settings
  265 - View Switches
  270 - View Switch Ports
  275 - View External Ethernet Ports
  280 - View Internal Ethernet Ports
  285 - View VLAN Settings
  290 - View LAN Endpoints
  295 - View Virtual Switch Management Service
  300 - Create Virtual Machine
  305 - Delete Virtual Machine
  310 - Change Virtual Machine Authorization Scope
  315 - Start Virtual Machine
  320 - Stop Virtual Machine
  325 - Pause and Restart Virtual Machine
  330 - Reconfigure Virtual Machine
  335 - View Virtual Machine Configuration
  340 - Allow Input to Virtual Machine
  345 - Allow Output from Virtual Machine
  350 - Modify Internal Ethernet Port

1 role assignment(s) were located

Role Assignment 'Administrator' (Targetted Role Assignment)
- All Hyper-V operations are selected
- There are 1 member(s) for this role assignment

- BUILTIN\Administrators (S-1-5-32-544)
```

Hyper-V includes an authorization store which, but default contains a single role assignment 'Administrator' which has access to all operations. HVRemote manipulates this role assignment when adding or removing users by default.

## Distributed COM Users

```
-----  
Contents of Group Distributed COM Users  
-----  
There are no members in Distributed COM Users
```

```
-----  
Contents of Group Distributed COM Users  
-----  
2 member(s) are in Distributed COM Users  
- WG\disabled          ****WARN: This account is disabled  
                      ****WARN: This account has an expired password  
- WG\John
```

Each user who needs remote access must be a member of the Distributed COM Users, or granted explicit permission. HVRemote manipulates the Distributed COM Users group rather than granting explicit permission on a per-user or per-group basis. Note that during this check, each user account is verified to ensure it is not locked out, disabled, or has an expired password.

## COM Security for Launch and Activation Permissions

```
-----  
DACL for COM Security Launch and Activation Permissions  
-----  
BUILTIN\Administrators    (&S-1-5-32-544)  
  Allow: LocalLaunch RemoteLaunch LocalActivation RemoteActivation <31>  
\Everyone                 (&S-1-1-0)  
  Allow: LocalLaunch LocalActivation <11>  
BUILTIN\Distributed COM Users (&S-1-5-32-562)  
  Allow: LocalLaunch RemoteLaunch LocalActivation RemoteActivation <31>  
BUILTIN\Performance Log Users (&S-1-5-32-559)  
  Allow: LocalLaunch RemoteLaunch LocalActivation RemoteActivation <31>
```

This section should be read in conjunction with the Distributed COM Users section above. Even if a user is not a member of Distributed COM Users, other groups such as “Performance Log Users” and “Administrators” have RemoteLaunch permissions in a default configuration. (This section is mostly for diagnosis information and to help me investigate when you report problems ☺)

## Firewall Settings (Hyper-V server rules)

If the Windows Firewall service has been stopped, or the firewall has been disabled, you will get an error near the top of the output similar to the following, and the firewall settings themselves will be skipped.

```
WARN: The Windows firewall is not active in one or more active profiles.  
Not all functionality of HVRemote will be available.  
Use 'netsh firewall set opmode enable' to turn it on!
```

### Firewall Settings for Hyper-U

Public Firewall Profile is active

```
Enabled: Hyper-U <SPL-TCP-In>  
Enabled: Hyper-U <RPC>  
Enabled: Hyper-U <RPC-EPMAP>  
Enabled: Hyper-U - WMI <ASync-In>  
Enabled: Hyper-U - WMI <TCP-Out>  
Enabled: Hyper-U - WMI <TCP-In>  
Enabled: Hyper-U - WMI <DCOM-In>
```

There are a set of seven Windows Firewall rules required for remote management connectivity. If you are running a third party firewall on the server, you must ensure the appropriate matching rules are configured.

## Firewall Settings (Remote WMI)

### Firewall Settings for Windows Management Instrumentation <WMI>

Public Firewall Profile is active

```
Disabled: Windows Management Instrumentation <ASync-In>  
Disabled: Windows Management Instrumentation <WMI-Out>  
Disabled: Windows Management Instrumentation <WMI-In>  
Disabled: Windows Management Instrumentation <DCOM-In>
```

Note: Above firewall settings are not required for Hyper-U Remote Management

These rules are not required for remote management of Hyper-V, but can assist, particularly in a Server Core environment (or Microsoft Hyper-V Server environment) to use GUI management tools for remote server management.

## IP Configuration

This section is simply the output of ipconfig /all. The reason I include this is because it's one of those things I always ask for when diagnosing issues.

```
-----
IP Configuration
-----

Windows IP Configuration

Host Name . . . . . : wg
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : .com

Ethernet adapter Local Area Connection 3:

Connection-specific DNS Suffix . . : .com
Description . . . . . : Microsoft Virtual Machine Bus Network Adapter
Physical Address. . . . . : 00-15-5D-C8-41-26
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::dc37:5797:8df0:7b73%16 (Preferred)
IPv4 Address. . . . . : 192.168.200.57 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, January 06, 2009 7:24:46 PM
Lease Expires . . . . . : Thursday, January 08, 2009 7:24:49 PM
Default Gateway . . . . . : 192.168.200.254
DHCP Server . . . . . : 192.168.200.201
DNS Servers . . . . . : 192.168.200.202
                          192.168.200.201
                          192.168.200.200
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection* 8:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : .com
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

## Latest version verification

As of version 0.3, HVRemote has a built in capability to determine if there is a later version of HVRemote available. You must have Internet connectivity for this check to be made. You can use the /noversioncheck option to turn off latest version verification. If you have an out-of-date version, a message will be displayed.

```
***** There is a newer version of HVRemote available *****
Latest Version: 0.
Release Date: 1/2/2008
Location: http://code.msdn.microsoft.com/HVRemote/url
```

## Warnings and Errors summary

This section has been introduced as it has been noticed that it's hard to spot warnings and errors in a relatively verbose output.

```
-----  
2 warning(s) or error(s) were found in the configuration. Review the  
detailed output above to determine whether you need to take further action.  
Summary is below.  
  
1: Found a disabled user account  
2: Found an account with an expired password  
  
-----
```

## Granting a user permission to remotely manage Hyper-V

```
hvremote [/mode:server] /add:domain\user           (Domain or workgroup)
hvremote [/mode:server] /add:user                 (Workgroup only)
```

Note that instead of user, a group name can be specified (both Local and Domain based groups). If the group name contains spaces, use double-quotes around the parameter such as:

```
hvremote /mode:server /add:"domain\group name with spaces"
```

In /add mode, several sections of output are displayed. Note that if a user already has permission to an item, a warning message will be output, but the script will continue to configure the other settings.

```
INFO: Computername is ADMINISTRATOR1
INFO: Computer is in workgroup WORKGROUP
INFO: Current user is ADMINISTRATOR1\Administrator
INFO: Assuming /mode:server as the role is installed
INFO: This machine has the Hyper-U (v1) QFE installed (KB950050)

Adding user or group to root\cimv2 namespace...
INFO: DACL with user or group ACE built
OK: Security update applied to root\cimv2 namespace
INFO: root\cimv2 namespace permissions updated OK

Adding user or group to root\virtualization namespace...
INFO: DACL with user or group ACE built
OK: Security update applied to root\virtualization namespace
INFO: root\virtualization namespace permissions updated OK

Adding user to Distributed COM Users...
INFO: user added to Distributed COM Users OK

Adding user to AZMan role Administrator

NOTE: If this is the first time you have used HURemote
to add a user for remote configuration, it may be necessary
to restart this machine. See documentation for further
information.
```

## Note

You may need to reboot the server if this is the first time a user has been added, especially in the case where connections have already been attempted by a client. After client configuration, if the client cannot connect, it is strongly recommended that you reboot both the server AND the client as the first step in troubleshooting to release all pre-existing connections.

## Removing user permissions for remotely manage Hyper-V

```
hvrename [/mode:server] /remove:domain\user      (Domain or workgroup)
hvrename [/mode:server] /remove:user             (Workgroup only)
```

Note that instead of user, a group name can be specified (both Local and Domain based groups). If the group name contains spaces, use double-quotes around the parameter such as:

```
hvrename [/mode:server] /remove:"domain\group name with spaces"
```

In /remove mode, several sections of output are displayed. Note that if a user does not previously have permission to an item, a warning message will be output, but the script will continue to configure the other settings.

```
Removing user or group from root\cimv2 namespace...
INFO: DACL without user or group ACE in it built
OK: Security update applied to root\cimv2 namespace
INFO: root\cimv2 namespace permissions updated OK

Removing user or group from root\virtualization namespace...
INFO: DACL without user or group ACE in it built
OK: Security update applied to root\virtualization namespace
INFO: root\virtualization namespace permissions updated OK

Removing user from Distributed COM Users...
INFO: user removed from Distributed COM Users OK

Removing user from AZMan role Administrator
```

## Advanced parameters

```
hvremote /mode:server Operation [Options]
```

HVRemote supports a number of advanced operations and options. Generally, the options are to limit what settings are changed when adding and removing users, or showing the current settings.

By default, items 1 through 5 from Referring to the numbering in the “Hyper-V Remote Management Configuration Steps” above, Items 1 through 5 are set by HVRemote. Item 6 is not set unless explicit requested as a separate operation.

<b>Do not update the cimv2 namespace</b>	/ns:virtualization	(1)
<b>Do not update the virtualization namespace</b>	/ns:cimv2	(2)
<b>Do not update either namespace</b>	/ns:none	(1) and (2)
<b>Do not update the authorization store</b>	/NoAZMan	(3)
<b>Alternate Role Assignment in AZMan</b>	/RoleAssign:<assignment>	(3)
<b>Do not update Windows Firewall for Hyper-V</b>	/FirewallHyperVMgmt:None	(4)
<b>Disable the Windows Firewall for Hyper-V</b>	/FirewallHyperVMgmt:Disable	(4)
<b>Do not add user to Distributed COM Users</b>	/NoDCOM	(5)

Example:

```
Hvremote /mode:server /add:domain\user /ns:cimv2
```

- Grants remote access to domain\user *except* in the virtualization namespace
- *Does* add user to security permissions to the root\cimv2 namespace (1)
- **Does not** user to security permissions to the root\virtualization namespace (2)
- *Does* add user administrator access to AZMan (3)
- *Does* open Windows Firewall for Hyper-V rule group (4)
- *Does* add user to the Distributed COM Users Group (6)

*This will **NOT** be a total Hyper-V remote management configuration as the user will not be granted security permissions to the root\virtualization namespace.*

## Client Usage

Note: “/mode:client” can be omitted if the Hyper-V role is not detected as HVRemote will assume you are performing a client operation. To perform any changes to client configuration, the script must be run from an elevated command prompt. Administrators can use the /show option from a non-elevated command prompt.

### Elevation requirements

All client operations except /show must be run from an elevated command prompt. If you are running as a non-admin or from a “standard” command prompt, you will get the following message if elevation is required:

```
INFO: Computername is CLIENT
INFO: Computer is in workgroup WORKGROUP
INFO: Current user is CLIENT\admin
INFO: Assuming /mode:client as the Hyper-U role is not installed

*****
***** All client operations which change the configuration must be run
***** from an elevated command prompt.
*****
```

### Display the current settings

```
hvremote [/mode:client] /show
```

In /show mode, several sections of output are displayed. It may help to pipe the output to a text file and use notepad or another editor to examine the output.

#### Tip

It is recommended that you use /show and save the output before any changes are made.

### Basic information.

Basic information shows the computer name, the domain membership and the mode if it was determined that the machine is not running the Hyper-V role and client mode has been assumed. At this stage, for Windows Vista, KB952627 is verified as is the SKU of Windows Vista being used (not all SKUs support remote management)

```
INFO: Computername is CLIENT
INFO: Computer is in workgroup WORKGROUP
INFO: Current user is CLIENT\admin
INFO: Assuming /mode:client as the Hyper-U role is not installed
INFO: This machine has Hyper-U Management Client installed (KB952627)
```

## COM Security for Access Permissions

```
-----  
DACL for COM Security Access Permissions  
-----  
\Everyone      (S-1-1-0)  
    Allow: LocalLaunch RemoteLaunch <?>  
NT AUTHORITY\ANONYMOUS LOGON  (S-1-5-7)  
    Allow: LocalLaunch RemoteLaunch <?>  
BUILTIN\Distributed COM Users  (S-1-5-32-562)  
    Allow: LocalLaunch RemoteLaunch <?>  
BUILTIN\Performance Log Users  (S-1-5-32-559)  
    Allow: LocalLaunch RemoteLaunch <?>
```

This section should be read in conjunction with the ANONYMOUS LOGON remote access to Distributed COM section below. (This section is almost entirely for diagnosis information and to help me investigate when you report problems ☺)

### ANONYMOUS LOGON remote access to Distributed COM

This section shows the current setting for ANONYMOUS LOGON. Note the warning which is displayed if the permission has been granted.

```
-----  
ANONYMOUS LOGON Machine DCOM Access  
-----  
ANONYMOUS LOGON does not have remote access
```

Or

```
-----  
ANONYMOUS LOGON Machine DCOM Access  
-----  
WARN: ANONYMOUS LOGON does have remote access  
  
This setting should only be enabled if required as security on this  
machine has been lowered. It is needed if you need to manage Hyper-U  
on a remote server which is either in an an untrusted domain from this  
machine, or both machines are in a workgroup.  
  
Use hvremote /Mode:Client /AnonDCOM:Revoke to turn off
```

## Firewall settings for Hyper-V Management Clients

If the Windows Firewall service has been stopped, or the firewall has been disabled, you will get an error near the top of the output similar to the following, and the firewall settings themselves will be skipped.

```
WARN: The Windows firewall is not active in one or more active profiles.  
Not all functionality of HVRemote will be available.  
Use 'netsh firewall set opmode enable' to turn it on!
```

There are four rules (all in one rule group) which must be enabled for remote management to operate

```
-----  
Firewall Settings for Hyper-V Management Clients  
-----  
  
Public Firewall Profile is active  
  
Enabled: Hyper-V Management Clients - WMI <Async-In>  
Enabled: Hyper-V Management Clients - WMI <TCP-Out>  
Enabled: Hyper-V Management Clients - WMI <TCP-In>  
Enabled: Hyper-V Management Clients - WMI <DCOM-In>
```

## Firewall exception for Microsoft Management Console (mmc.exe)

The Microsoft Management Console should have a firewall exception for remote management to operate. Note that there are two rules in the exception: One for UDP and one for TCP.

```
-----  
Windows Firewall exception rule(s) for mmc.exe  
-----  
  
Public Firewall Profile is active  
  
Enabled: Microsoft Management Console <HVRemote.wsf Created> <UDP>  
Enabled: Microsoft Management Console <HVRemote.wsf Created> <TCP>
```

Or

```
-----  
Windows Firewall exception rule(s) for mmc.exe  
-----  
  
Public Firewall Profile is active  
  
WARN: No MMC exception rules were found. These rules are needed  
for Hyper-V remote management. To add these rules, run:  
  
hvremote.wsf /Mode:Client /MMC:Enable
```

## IP Configuration

This section is simply the output of `ipconfig /all`. The reason I include this is because it's one of those things I always ask for when diagnosing issues.

```
IP Configuration
-----
Windows IP Configuration

Host Name . . . . . : client
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : . com

Ethernet adapter Local Area Connection 2:

Connection-specific DNS Suffix . . : . com
Description . . . . . : microsoft Virtual Machine Bus Network Adapter
Physical Address. . . . . : 00-15-5D-C8-41-25
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::4921:cdb6:ae1e:a14c%11(Preferred)
IPv4 Address. . . . . : 192.168.200.55(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, January 06, 2009 6:25:38 PM
Lease Expires . . . . . : Thursday, January 08, 2009 6:25:38 PM
Default Gateway . . . . . : 192.168.200.254
DHCP Server . . . . . : 192.168.200.201
DNS Servers . . . . . : 192.168.200.202
                          192.168.200.201
                          192.168.200.200
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Local Area Connection* 6:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . : . com
Description . . . . . : isatap.
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
```

## Stored Credential summary

This section is simply the output of `cmdkey /list`. The reason I include this is because it's one of those things I always ask for when diagnosing issues.

```
Stored Credentials
-----
Currently stored credentials:
* NONE *
```

## Warnings and Errors summary

This section has been introduced as it has been noticed that it's hard to spot warnings and errors in a relatively verbose output.

```
-----  
1 warning(s) or error(s) were found in the configuration. Review the  
detailed output above to determine whether you need to take further action.  
Summary is below.  
1: FW MMC Exception rule is missing  
-----
```

## Change ANONYMOUS LOGON remote access to Distributed COM setting

```
hvremote [/mode:client] /AnonDCOM:grant  
hvremote [/mode:client] /AnonDCOM:revoke
```

```
INFO: Computername is UISTA  
INFO: Computer is in workgroup WORKGROUP  
INFO: Assuming /mode:client as the Hyper-U role is not installed  
  
INFO: Obtaining current Machine Access Restriction...  
INFO: Examining security descriptor  
INFO: Granted Remote DCOM Access to Anonymous Logon  
WARN: See documentation for security implications
```

Note that granting ANONYMOUS LOGON remote access to Distributed DCOM lowers the security settings of the client machine. It should only be enabled if necessary. In particular, it is **NOT** required when both the server and client are domain joined, and they are either in the same or trusted domains.

This setting will be needed in untrusted domains, or workgroup environments. The reason is that Hyper-V Manager gets asynchronous callbacks from the server for certain WMI events. In those configurations, the server does not have authentication credentials to contact the client.

## Change Windows Firewall settings for Hyper-V Management Clients

If the Windows Firewall service has been stopped, or the firewall has been disabled, you will get an error near the top of the output similar to the following, and this function will not be available.

```
WARN: The Windows firewall is not active in one or more active profiles.  
Not all functionality of HVRemote will be available.  
Use 'netsh firewall set opmode enable' to turn it on!
```

```
hvremote [/mode:client] /FirewallHyperVClient:Enable  
hvremote [/mode:client] /FirewallHyperVClient:Disable
```

These four firewall rules must be enabled for remote management to operate correctly.

```
INFO: Computername is VISTA
INFO: Computer is in workgroup WORKGROUP
INFO: Assuming /mode:client as the Hyper-U role is not installed
INFO: Enabled firewall rule Hyper-U Management Clients - WMI (Async-In)
INFO: Enabled firewall rule Hyper-U Management Clients - WMI (TCP-Out)
INFO: Enabled firewall rule Hyper-U Management Clients - WMI (TCP-In)
INFO: Enabled firewall rule Hyper-U Management Clients - WMI (DCOM-In)
INFO: 4 firewall rule(s) updated
```

 **Note**

After client configuration, you may need to reboot the client if it has been reconfigured and you had pre-existing connection attempts to the server. After client configuration, if the client cannot connect, it is strongly recommended that you reboot both the client AND the server as the first step in troubleshooting to release all pre-existing connections.

## Additional Options

### **/debug**

HVRemote supports a /debug option which is especially useful to me if you are reporting a bug or issue (please use the /verbose option and attach all output). It can be combined with any client or server operation.

```
/debug:standard
```

```
/debug:verbose
```

### **/noverversioncheck**

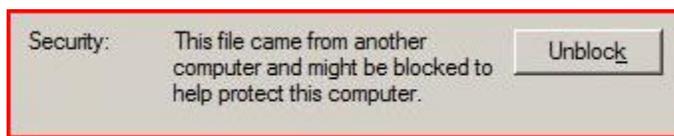
As of version 0.3 of HVRemote, HVRemote checks to see if you are running the latest version. If you are on a network which has no Internet connectivity, or you do not wish to perform this option, add the following option to the command line. It can be combined with any client or server operation.

```
/noverversioncheck
```

## Troubleshooting

This is a quick summary of the most common issues that have been reported is remote management does not appear to work after running HVRemote.

1. “Access Denied” when running HVRemote. This is a Windows security mechanism. On the machine where you downloaded HVRemote, in Windows Explorer, right-click on the file and select properties. On the general tab at the bottom of the page, there will be a message saying “Security: This file came from another computer and might be blocked to help protect this computer”. To the right of that is an Unblock button. You need to click that to allow HVRemote to work. To the best of my knowledge, you hit this when using Firefox to download HVRemote, but not when using Internet Explorer.



2. DNS. This is the number one reason why remote management fails. It is vitally important that the client can locate the server by name, **and** that the server can locate the client by name. Try doing an “nslookup <othermachinename>” on each machine or “ping <othermachinename> - 4”. It should return the IP Address of the other machine as seen when running “ipconfig”. If it doesn’t find the correct IP address, or doesn’t find the other machine at all, fix DNS, or consider editing /windows/system32/drivers/etc/hosts to hard-code an entry for the other machine as needed. But if editing the hosts file, be wary of possible changes should you also be using DHCP in your environment.
3. Depending on whether pre-existing connections are open before configuration was made, it may be that you need to reboot both the server and client. Always try this, especially after the first time you run the /add: command on the server or re-configure the client settings.
4. Client does not receive event notifications. For example, at the end of the new virtual machine wizard, the new VM is not listed unless you hit refresh in Hyper-V Manager. This is usually because you haven’t turned on hvremote /mode:client /AnonDCOM:grant on the client. Note the security implications above, and whether the domain/workgroup scenario you are in requires this configuration. Note also that if the server is Windows Server 2008 and is domain joined, and the client is workgroup, you will see this regardless of the client setting. This is a bug we are working on resolving in Windows Server 2008 R2, and possibly in SP2.
5. If you are trying to connect to a workgroup server from a client machine which has IPSec policy applied, you cannot connect to the server. It could be IPSec policy on the client blocking inbound connections (the server calls back to the client). Try “net stop bfe” on the client from an elevated command prompt. Work with your network administrator to determine if there are

exception IP address ranges, and what the implications of stopping this service are.

6. Remote management works on a wired connection, but not over a VPN. See 1 above and <http://blogs.technet.com/jhoward/archive/2008/08/07/hyper-v-why-does-hyper-v-manager-not-always-work-over-vpn-connection-access-denied-or-rpc-server-unavailable-errors.aspx>
7. Remote connectivity works, but at the end of the new virtual machine wizard, or when using the new virtual hard disk wizard, you get a failure about permission denied “The system failed to create <path>.vhd with error ‘General access denied error. (0x80070005)’”. If you are a standard user, not an administrator on the server, you will not have permissions to create VHDs in all directories. You should logon to the server as an administrator and create an appropriate directory for the user to create VHDs in.
8. Domain client to workgroup server: You must run the cmdkey operation to specify credentials as an additional step. See earlier in this document for more information.
9. Other firewall software is installed on either the client or the server, or a firewall is present between the client and the server. If you have followed all other troubleshooting steps, try disabling software firewalls to determine if that is the cause.

## Future Enhancements

HVRemote is a work in progress. It performs most of the major needs for Hyper-V remote management configuration though ☺

This section is a summary of things which I believe could be useful, are already in the pipeline for a future version, or are areas where there is still work for improvement:

- Client mode option to verify connectivity to the server
- Detection of IPSec policy enforced. This is as inbound connections may be blocked if the client and server are not in the same domain.
- Have a backup and restore function
- When adding an ACE to a DACL, no check is made for a Deny ACE in place
- Make server configuration run remotely. There are lots of places currently where it will only work on the Hyper-V enabled machine.