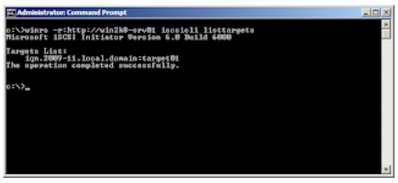
Настройка WinRM на Windows Server

Главная
Сетевые сервисы
Active Directory
RRAS
DNS
PKI
WSUS
DHCP
ISA / TMG
WMI
WINS
Cluster
IPv6
Другое

Бывают случаи, когда требуется выполнить какую-либо команду на сервере локально (например, сконфигурировать iSCSI Initiator). Подключаться для этого через Remote Desktop и запускать cmd - неудобно, использовать Telnet - небезопасно, ставить на сервер демона ssh - не... хочется...

Специально для таких случаев, Microsoft, начиная с Windows Server 2003 R2, снабдила администраторов новым средством управления - *Windows Remote Management (WinRM)*, позволяющим удаленно выполнять команды, используя стандартные средства ОС, и обеспечивая при этом должный уровень безопасности.

Вам даже не придется устанавливать дополнительных программ и компонентов - все, что называется, включено:

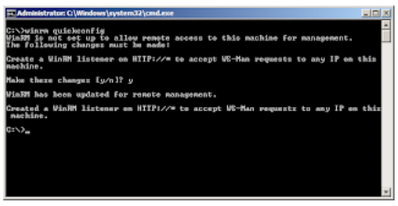


В качестве примера я рассмотрю процесс настройки WinRM на Windows Server 2008. Эта процедура никак не отличается от настройки *WinRM*, например, на Windows Vista или Hyper-V Server.

Проще всего WinRM настроить можно, используя режим быстрой конфигурации, набрав в CMD:

winrm quickconfig

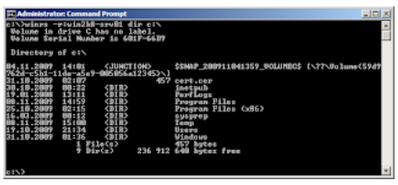
и ответив утвердительно ('**y**') на вопрос о создании нового объекта-listener'a, прослушающего порт TCP 80, и использующего протокол HTTP для коммуникаций между клиентом и сервером.



И все, сервером можно управлять удаленно, используя команду:

winrs -r:

,где - имя или IP адрес сервера, к которому осуществляется подключение;
- удаленная команда, которую требуется выполнить.



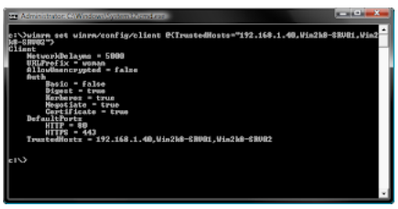
Если клиент и сервер не являются членами одного домена, вам потребуется дополнительно указать имя пользователя из-под которого будет запускаться команда и его пароль:

winrs -r: -u: -p:

, а заодно, как советует появившееся сообщение, добавить сервер в список доверенных узлов, либо использовать более надежный протокол для коммуникации (HTTPS).

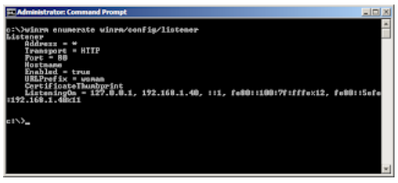
Для добавления узла в список надежных, выполните на клиенте, с которого планируете подключаться:

winrm set winrm/config/client @{TrustedHosts="[,]"}



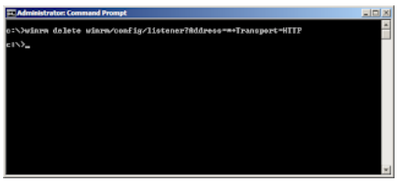
После настройки вы можете получить информацию о существующих listener'ах с помощью команды:

winrm enumerate winrm/config/listener



Удалить существующий listener можно следующим образом:

winrm delete winrm/config/listener?Address=*+Transport=HTTPS



Настройка WinRM с использованием HTTPS

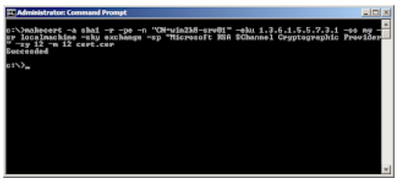
В ряде случаев вам может потребоваться создать надежный канал для безопасной пересылки команд между клиентом и сервером. Для этого можно использовать HTTPS.

Однако, для создания listener'а с поддержкой HTTPS вам потребуется цифровой сертификат, который можно запросить у доверенного Центра Сертификации, либо воспользоваться различными утилитами по созданию самоподписанных (самозаверенных) сертификатов, например, Makecert, входящей в состав Windows SDK. Скачать Makecert отдельно можно отсюда.

Для создания самоподписанного серитификата выполните следующую команду:

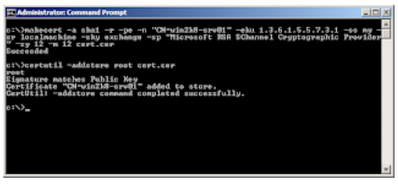
makecert -a sha1 -r -pe -n "CN=" -eku 1.3.6.1.5.5.7.3.1 -ss my -sr localmachine -sky Exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12 -m 12

, где соответствует имени, которое будет использовать клиент при подключении к серверу;
- путь к файлу, куда будет сохранен сертификат с открытым ключем.



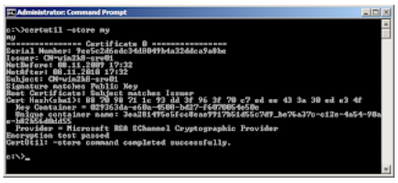
Сертификат с закрытым ключем будет создан и помещен в хранилище сертификатов локального компьютера. Добавьте его к доверенным корневым сертификатам:

certutil -addstore root cert.cer



Теперь просмотрите хранилище сертификатов, найдите там требуемый сертификат и запишите его Thumbprint (Cert Hash):

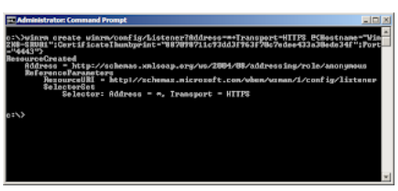
certutil -store my



Наконец, можно приступать к созданию HTTPS listener. Введите команду:

winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="";CertificateThumbprint="";Port=""}

,где - имя, которое указывается при обращении к серверу
- Thumbprint, который вы узнали на предыдущем шаге (без пробелов).
- порт, на который будет подключаться клиент (TCP 443 по-умолчанию).

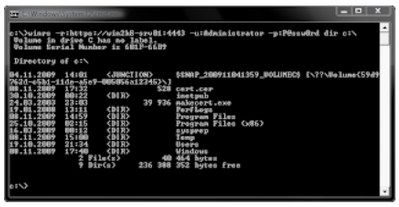


Если на сервере включен брандмауэр Windows, не забудьте добавить правило:

netsh advfirewall firewall add rule name="allow WinRM on 4443" protocol=TCP dir=in localport=4443 action=allow

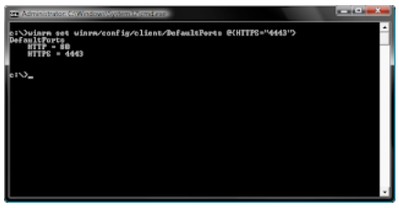
При использовании самоподписанных сертификатов, вам придется добавить его к доверенным корневым сертификатам на клиенте.

После выполнения всех шагов, вы, наконец, получите возможность удаленного выполнения команд:



Обратите внимание, что в случае использования нестандартного порта, вам потребуется специально его указать. Чтобы не делать этого каждый раз, вы можете изменить стандартный порт, который клиент использует при подключении по HTTPS, с помощью команды:

winrm set winrm/config/client/DefaultPorts @{HTTPS="4443"}



Заключение

Как видите, настройка Windows Remote Management достаточно проста в классических ситуациях (с использованием единого домена и CA), однако, при небольшом отклонении от данного шаблона могут обнаружиться несколько подводных камней. К WinRM привыкнуть можно достаточно быстро, особенно, если вы частенько пользуетесь консолью для настройки системы.

source: http://blog.vmpress.org/2009/11/winrm-windows-server-2008.html