**Выполнение консольных команд на удаленных компьютерах по сети**

2010-02-08, 01:01 / [Argon](http://argon.pro/blog/author/admin/)

В данной статье рассмотрены способы выполнения консольных команд на уделенных компьютерах сети, в качестве примеров даются некоторые очень полезные для системных администраторов команды.

Я использую 2 средства удаленного выполнения консольных команд: [PsExec](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#ch1) и [WinRM](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#ch2), у каждого из них есть свои преимущества.

**PsExec**

Одним из отличных решений поставленной в заголовке задачи является использование программы [PsExec](http://argon.pro/goto/technet.microsoft.com/ru-ru/sysinternals/bb897553.aspx) от великого [Марка Руссиновича](http://argon.pro/goto/technet.microsoft.com/ru-ru/sysinternals/default.aspx).

Программа работает по клиент-серверному принципу: на локальной машине выполняется клиент, который посылает команды серверу на удаленном компьютере. Особенностью этой программы является то, что серверная часть устанавливается автоматически непосредственно перед выполнением команды, а затем удаляется. Таким образом для выполнения команд на удаленных машинах достаточно иметь на них административные права.

Если PsExec запускается от имени администратора, который входит в тот же домен, что и удаленны компьютер, то никаких учетных данных даже вводить не нужно. В противном случае, их можно указать в командной строке, либо PsExec сама их запросит. PsExec работает на ОС начиная с Windows 2000 и заканчивая 64-битным Windows Server 2008 R2.

Очень полезными в PsExec являются следующие возможности:

* **Выполнение команды на группе компьютеров**. Пример: следующая команда позволяет принудительно применить самые свежие групповые политики:  
  psexec @group.txt gpupdate /force
* **Выполнение команд от имени системной учетной записи**. Пример: следующая команда заставит удаленную систему принудительно проверить обновления:  
  psexec \\computer -s wuauclt /detectnow
* **Копирование выполняемой программы на удаленный компьютер перед выполнением**. Пример: следующая команда позволит обновить членство данного компьютера в группе безопасности Active Directory (токен доступа) без перезагрузки:  
  psexec \\computer -c -s [klist.exe](http://argon.pro/goto/www.microsoft.com/downloads/details.aspx?FamilyID=1581e6e7-7e64-4a2d-8aba-73e909d2a7dc) purge

Трудно переоценить пользу этой программы, если использовать скрипты и возможности консольных команд, встроенных в Windows.

**Windows Remote Management**

Изначально это была серверная технология для удаленного управления оборудованием, которая появилась в Windows Server 2003 R2 как часть компонента Hardware Management, но недавно Microsoft выпустили пакет Windows Management Framework, который включает в себя PowerShell 2.0 и WinRM 2.0 и устанавливается на клиентские ОС как обновление. Подробности можно прочитать в статье [KB968929](http://argon.pro/goto/support.microsoft.com/kb/968929).

Прелесть WinRM заключается в простоте развертывания в доменной среде через WSUS в качестве факультативного обновления ОС и мощи, которую даёт совместное с PowerShell применение.

Использование WinRM происходит через 2 команды.

**winrm.cmd** служит для конфигурирования настроек и диагностики клиента и сервера WinRM.

Для того, чтобы сервер WinRM начал принимать команды, должна быть запущена служба Windows Remote Management и произведена её начальная конфигурация. Используйте команду

winrm quickconfig на локальной машине, либо финт ушами  
psexec -s \\servername winrm quickconfig по сети, используя PsExec от имени системной учетной записи.

Будет предложено автоматически запускать службу WinRM и разрешить уделенные подключения, соглашайтесь ;)

Чтобы успешно подключаться к WinRM серверу (имеется в виду серверная часть, принимающая команды), не входящему в тот же домен, что и ваш клиентский компьютер, необходимо на клиенте этот целевой сервер добавить в «доверенный список» следующей командой:

winrm set winrm/config/client @{TrustedHosts="servername"}, где вместо servername можно указать IP-адрес, либо \* (звёздочку).

Для пользователей Windows Vista и Windows 7, работающим не от имени встроенного администратора (обычно так и бывает), нужно выполнить следующую команду

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG\_DWORD /d 1 /f

По умолчанию, установлено ограничение на 5 одновременных соединений WinRM от клиента, для увеличения этого числа выполните команду

winrm s winrm/config/winrs @{MaxShellsPerUser="X"}

**winrs.exe** — клиент для отправки запросов к серверной части. Пример: следующая команда принудительно перезагрузит удаленную систему…

winrs -r:servername shutdown /r /t 0

В доменной среде при отправке команд используются учетные данные запустившего пользователя. Для посыла команд от имени другого пользователя используются ключи -u:user -p:pass. Пример: следующая команда очистит локальный кэш DNS-имён на удаленной системе

winrs -r:servername -u:user -p:pass ipconfig /flushdns

|  |  |
| --- | --- |
| **Рубрика** | [Tips and Tricks](http://argon.pro/blog/topics/exp/tips-and-tricks/) |
| **Метки** | [windows client](http://argon.pro/blog/tags/windows-client/), [windows server](http://argon.pro/blog/tags/windows-server/), [автоматизация](http://argon.pro/blog/tags/avtomatizatsiya/), [удаленное администрирование, remote administration](http://argon.pro/blog/tags/remote-admin/) |
| **Опубликовано** | 2010-02-08, 1:01; обновлено 2011-01-09, 17:02 |
| **Комментарии** | [Комментарии (10) »](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comments) |
|  | [Ссылка на запись](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/) | [Обратная ссылка](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/trackback/) | [RSS комментариев](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/feed/) |

**Комментарии (10)**

Тойво Глумов

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-88) от 2010-03-01, 19:07

«Прелесть WinRM заключается в прост-а-те развертывания в доменной» – думаю, стоит поправить опечатку.

Argon

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-89) от 2010-03-01, 19:27

Спасибо за полезный комментарии, среди моря лести спамеров.

gavrosh

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-1157) от 2010-06-17, 14:15

А централизованного механизма развёртывания WinRM в домене никакого нет? а то ведь опухнешь на всех клиентах настраивать(

gavrosh

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-1158) от 2010-06-17, 14:18

и ещё вопрос, может глупый), а чем телнет плох?

Argon

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-1159) от 2010-06-17, 14:26

Конечно есть, через WSUS распространяете последний .Net Framework, разрешаете в групповых политиках запрашивать опциональные обновления, после этого клиенты у WSUS-а спросят WinRM 2.0, его и одобряем. Вот WinRM и установлен на всех компах.

А телнет немного для другого сделан.

gavrosh

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-1160) от 2010-06-17, 14:40

т.е. теоретически я говорю через групповую политику – Служба WinRM включись, и оно работает, так?

Argon

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-1161) от 2010-06-17, 14:52

Да, все можно сделать через ГП, но могут быть тонкости.

gavrosh

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-1163) от 2010-06-17, 16:24

Здорово, спасибо за материал)

lamer

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-3820) от 2011-03-03, 15:40

к сожалению, с правами юзера этим пользоваться нельзя… а очень хотелось бы выполнить на удаленном компе какую-нибудь команду не будучи администратором, а будучи простым пользователем

Argon

[# Комментарий](http://argon.pro/blog/2010/02/execute-shell-commands-on-remote-computers/#comment-3827) от 2011-03-03, 18:50

Верно, ведь удаленное выполнение команд — это очень мощная функция, которая не должна быть доступна пользователям, не имеющим на это прав.

Однако, psexec имеет ключ «-l», который позволяет имитировать исполнение команды от имени пользователя без прав администратора на целевой системе.