Лабораторная работа 8. Средства удаленного администрирования в ОС Windows.
Теоретический материал.

Средства удаленного администрирования - программы или функции операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или ЛВС и производить управление и администрирование удалённого компьютера в реальном времени. Программы удалённого администрирования предоставляют почти полный контроль над удалённым компьютером: они дают возможность удалённо управлять рабочим столом и всей операционной системой компьютера, возможность копирования или удаления файлов, установки и запуска приложений и т. д.

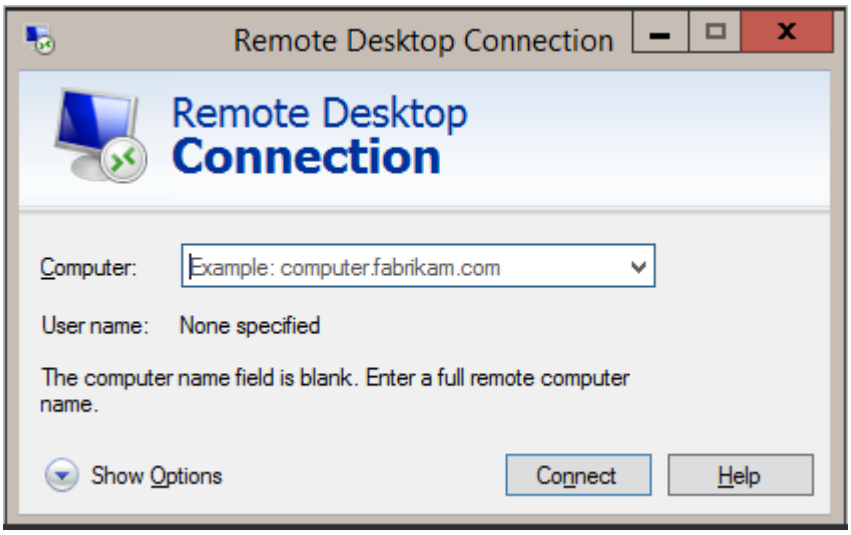
Существует множество реализаций программ удалённого администрирования. Все реализации различаются по интерфейсу и используемым протоколам. Отображаемый интерфейс может быть визуальным или консольным.

Для удаленного администрирования может применяться встроенное в современное ОС программное обеспечение, работающее по протоколам RDP, Telnet, SSH.

Широко известны также сторонние средства удаленного администрирования: VNC (UltraVNC, RealVNC), TeamViewer, Radmin, AnyDesk, DameWare, Ammyy Admin и др.

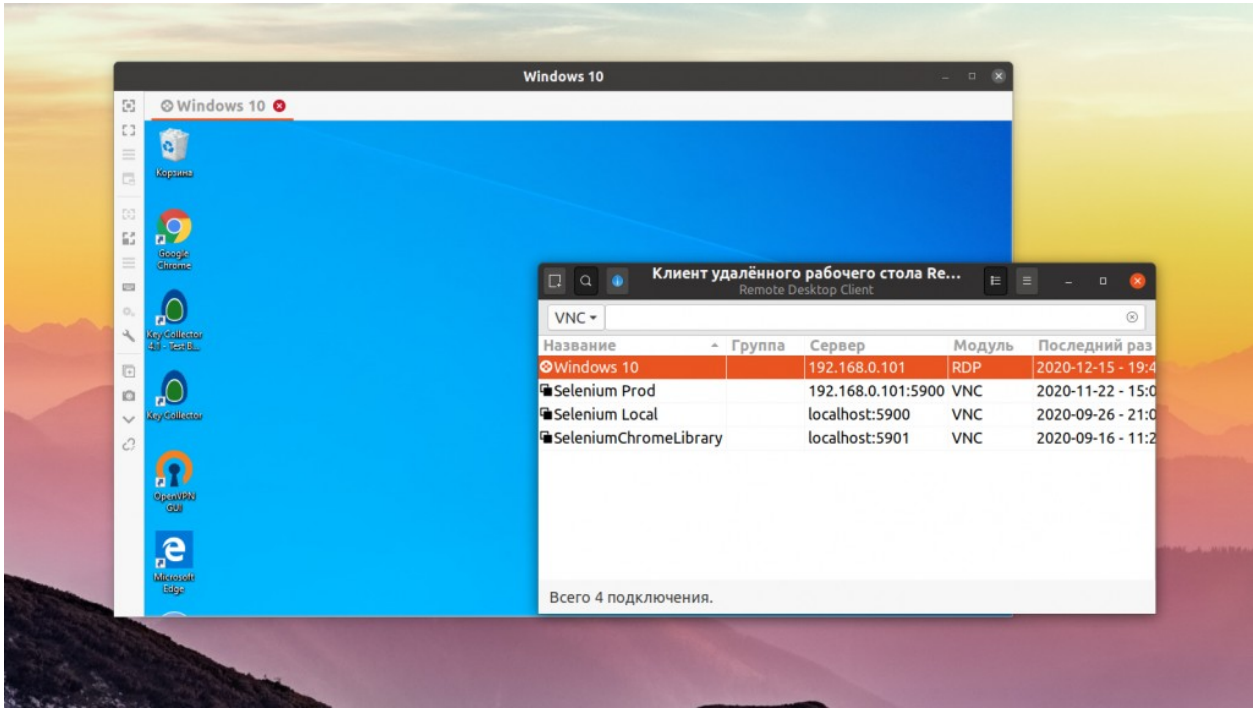
RDP

К самым популярным средствам администрирования в среде ОС Windows можно отнести компонент системы — Remote Desktop Services с клиентом Remote Desktop Connection (подключение к удаленному рабочему столу), которой работает по протоколу RDP (Remote Desktop Protocol).



Клиент RDP при подключении предоставляет графический интерфейс для управления удаленным компьютером.

Для ОС на базе Linux существуют как клиенты RDP – например, Remmina, FreeRDP, rdesktop и др., так и серверы RDP – например, XRDP.



Telnet

Telnet — сетевой протокол для реализации текстового терминального интерфейса по сети, а также утилита, реализующая клиентскую часть протокола.

Огромное количество сетевых устройств поддерживает удаленное управление при помощи данного протокола. Клиенты и серверы Telnet

функционируют в том числе на ОС семейства Microsoft Windows, а также на базе Linux.

В протоколе не предусмотрено использование ни шифрования, ни проверки подлинности данных. Поэтому он уязвим для любого вида атак, к которым уязвим его транспорт, то есть протокол TCP. Поэтому в качестве замены Telnet в настоящее время, как правило, применяется протокол SSH.

SSH

SSH – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Схож по функциональности с протоколами Telnet и rlogin, но, в отличие от них, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

SSH-сервер обычно прослушивает соединения на TCP-порту 22.

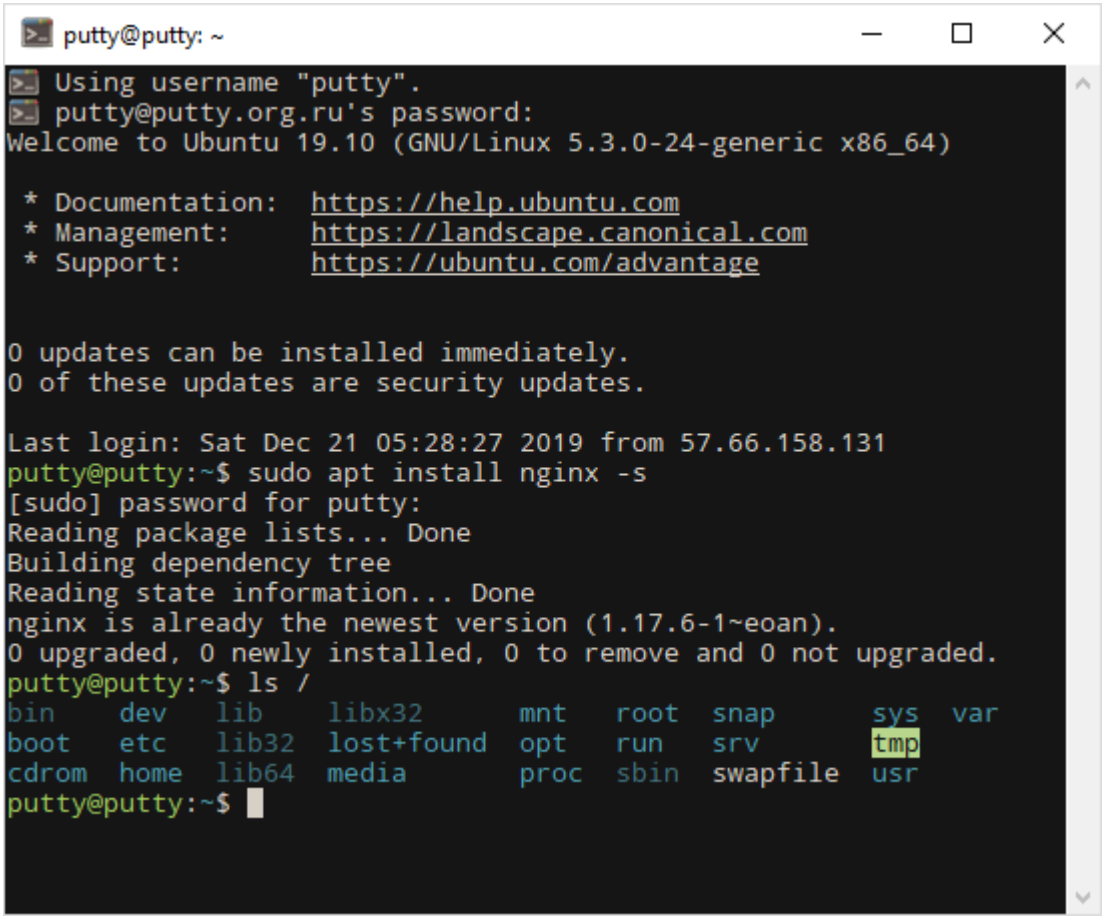
Для аутентификации сервера в SSH используется протокол аутентификации сторон на основе алгоритмов электронно-цифровой подписи RSA или DSA, но допускается также аутентификация при помощи пароля (режим обратной совместимости с Telnet) и даже ip-адреса хоста (режим обратной совместимости с rlogin).

1. Аутентификация по паролю наиболее распространена. При каждом подключении подобно https вырабатывается общий секретный ключ для шифрования трафика.

2. При аутентификации по ключевой паре предварительно генерируется пара открытого и закрытого ключей для определённого пользователя. На машине, с которой требуется произвести подключение, хранится закрытый ключ, а на удалённой машине — открытый. Эти файлы не передаются при аутентификации, система лишь проверяет, что владелец открытого ключа также владеет и закрытым. При данном подходе, как правило, настраивается автоматический вход от имени конкретного пользователя в ОС.

3. Аутентификация по ip-адресу небезопасна, эту возможность чаще всего отключают.

Помимо нативных клиентов SSH и Telnet в современных ОС, для подключения и удаленного управления по данным протоколам широкое распространение получила программа-клиент PuTTy.



VNC

Virtual Network Computing (VNC) — система удалённого доступа к рабочему столу компьютера, использующая протокол RFB (англ. Remote FrameBuffer, удалённый кадровый буфер). Управление осуществляется путём передачи нажатий клавиш на клавиатуре и движений мыши с одного компьютера на другой и ретрансляции содержимого экрана через компьютерную сеть.

Система VNC платформонезависима: VNC-клиент, называемый VNC viewer, запущенный на одной операционной системе, может подключаться к VNC-серверу, работающему на любой другой ОС. Существуют реализации клиентской и серверной части для большинства операционных систем. К одному VNC-серверу одновременно могут подключаться множественные клиенты.

RFB (англ. remote framebuffer) — простой клиент-серверный сетевой протокол прикладного уровня для удалённого доступа к графическому рабочему столу компьютера, используемый в VNC. Так как он работает на уровне кадрового буфера, то его можно применять для графических оконных

систем, например Windows, X Window System (UNIX), Quartz Compositor (macOS).

Примеры программного обеспечения, использующего VNC для организации удаленного администрирования: UltraVNC, TightVNC, RealVNC и др. В качестве клиента VNC могут также использоваться Remmina, Vinagre и др.

Средства удаленного администрирования сервера (RSAT)

Для удалённого управления сервером из-под Windows 10 используются средства удалённого администрирования сервера, в которые входят:

- диспетчер сервера;
- оснастки консоли управления (MMC);
- консоли;
- командлеты и поставщики Windows PowerShell;
- программы командной строки для управления ролями и компонентами в Windows Server.

Начиная с обновления Windows 10 за октябрь 2018 г., средства удалённого администрирования входят в состав набора компонентов по запросу непосредственно в Windows 10.

Эти средства используются для управления определенными технологиями на компьютерах Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, а в ограниченных случаях — Windows Server 2012 или Windows Server 2008 R2.

Доступны следующие инструменты администрирования:

- RSAT: Active Directory Domain Services and Lightweight Directory Services Tools
- RSAT: BitLocker Drive Encryption Administration Utilities
- RSAT: Active Directory Certificate Services Tools
- RSAT: DHCP Server Tools
- RSAT: DNS Server Tools
- RSAT: Failover Clustering Tools
- RSAT: File Services Tools

- RSAT: Group Policy Management Tools
- RSAT: IP Address Management (IPAM) Client
- RSAT: Data Center Bridging LLDP Tools
- RSAT: Network Controller Management Tools
- RSAT: Network Load Balancing Tools
- RSAT: Remote Access Management Tools
- RSAT: Remote Desktop Services Tools
- RSAT: Server Manager
- RSAT: Shielded VM Tools
- RSAT: Storage Migration Service Management Tools
- RSAT: Storage Replica Module for Windows PowerShell
- RSAT: System Insights Module for Windows PowerShell
- RSAT: Volume Activation Tools
- RSAT: Windows Server Update Services Tools

Windows Admin Center

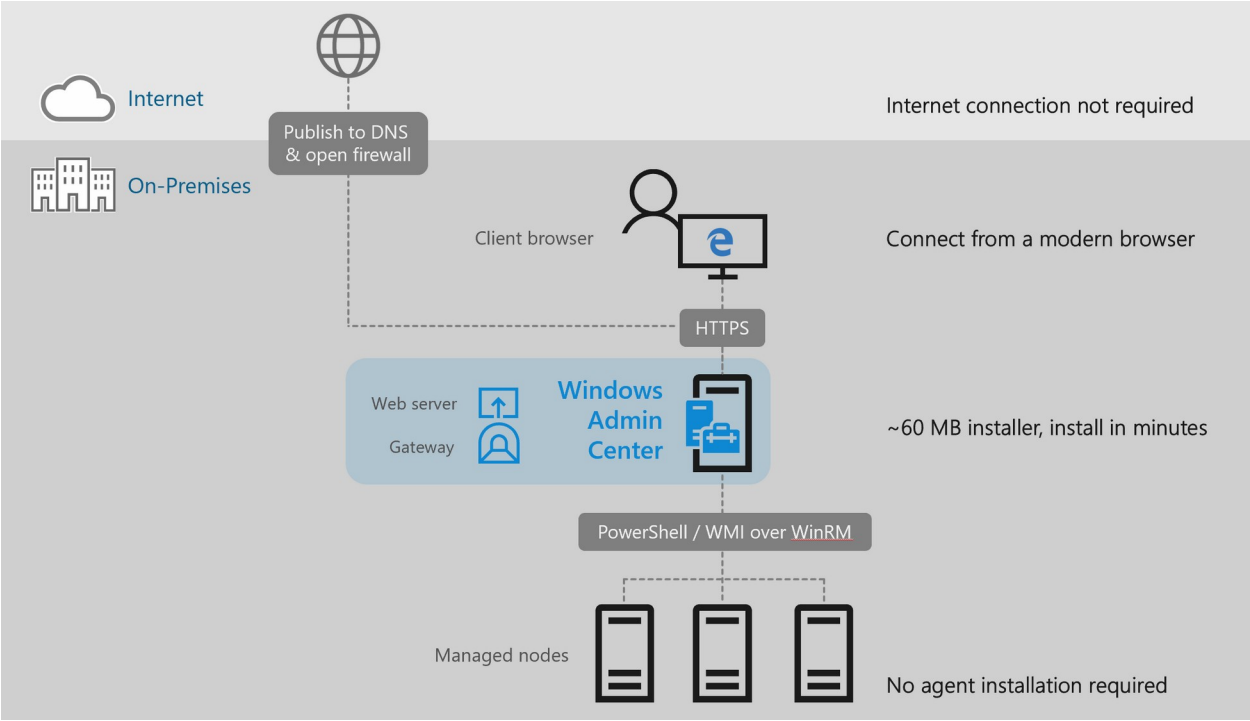
Windows Admin Center представляет собой локально развертываемое браузерное приложение для управления серверами, кластерами, гиперконвергентной инфраструктурой Windows, а также ПК с Windows 10.

Windows Admin Center — это продукт эволюции встроенных средств управления, таких как Диспетчер серверов и MMC.

Windows Admin Center запускается в браузере и управляет Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, Windows 10, Azure Stack HCI и другими версиями через шлюз Windows Admin Center, установленный в Windows Server или присоединенной к домену Windows 10. Шлюз управляет серверами с помощью удаленной оболочки PowerShell и WMI через WinRM. Шлюз входит в состав Windows Admin Center в одном облегченном MSI-пакете, который можно загрузить.

При публикации в DNS и предоставлении доступа через соответствующие корпоративные брандмауэры шлюз Windows Admin Center позволяет

безопасно подключиться к серверам и управлять ими из любого места с помощью Microsoft Edge или Google Chrome.

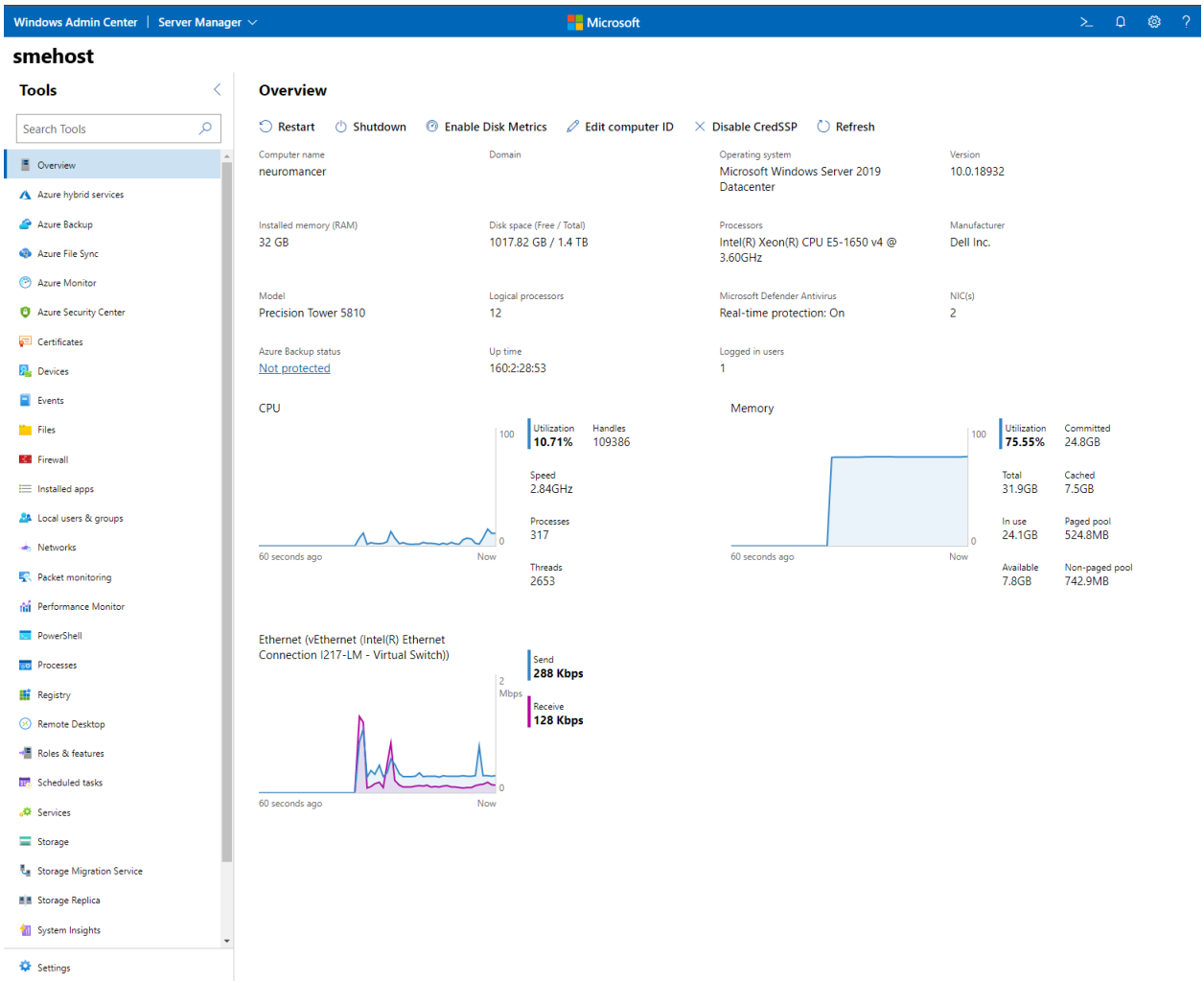


Несмотря на то, что платформа Windows Admin Center поддерживает управление множеством распространенных сценариев, она не является полноценной заменой для всех традиционных средств консоли управления (MMC).

В состав диспетчера управления серверами в Windows Admin Center входят следующие основные возможности:

- отображение ресурсов и их использования;
- управление сертификатами
- управление устройствами;
- просмотр событий
- проводник
- управление брандмауэром
- управление установленными приложениями;
- настройка локальных пользователей и групп;
- параметры сети

- просмотр и завершение процессов, а также создание дампов процессов;
- изменение реестра;
- управление запланированными задачами;
- управление службами Windows;
- включение и отключение ролей и компонентов;
- управление виртуальными машинами Hyper-V и виртуальными коммутаторами;
- управление хранилищем;
- управление репликой хранилища;
- управление обновлениями Windows;
- консоль PowerShell;
- подключение к удаленному рабочему столу



Windows Admin Center также предоставляет следующие решения:

- Управление компьютером — предоставляет набор функции диспетчера серверов для управления клиентскими компьютерами с Windows 10.
- Диспетчер отказоустойчивого кластера — поддержка непрерывного управления отказоустойчивыми кластерами и ресурсами кластера.
- Диспетчер гиперконвергентных кластеров — совершенно новые возможности, разработанные специально для работы с локальными дисковыми пространствами и Hyper-V. В его состав входит информационная панель с диаграммами и оповещениями для мониторинга.

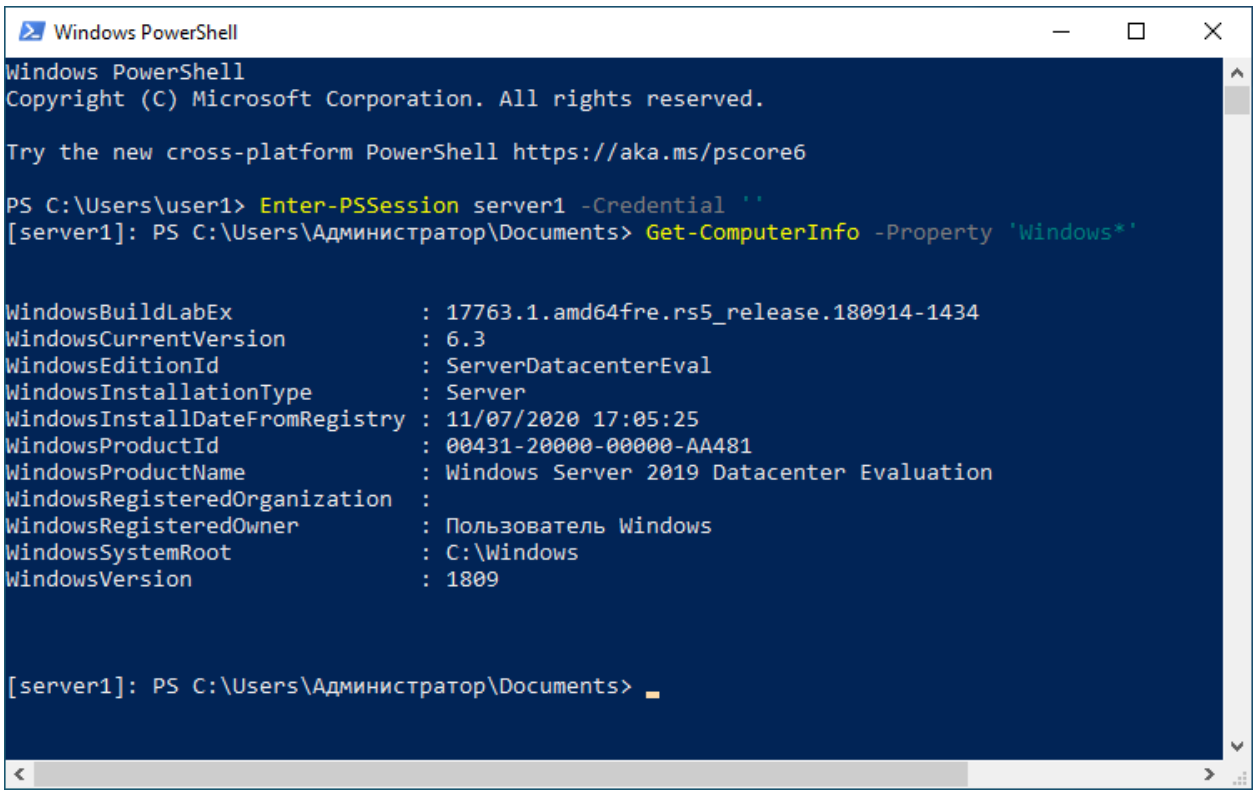
Windows Admin Center является дополнением к средствам удаленного администрирования сервера (RSAT) и не заменяет их, потому что роли, такие как Active Directory, DHCP, DNS и IIS, пока еще не обладают эквивалентными возможностями управления, доступными в Windows Admin Center.

PowerShell

PowerShell — это кроссплатформенное решение для автоматизации задач, которое включает оболочку командной строки, скриптовый язык и платформу управления конфигурацией. PowerShell поддерживается в Windows, Linux и macOS.

В отличие от оболочек, которые только принимают и возвращают текст, PowerShell принимает и возвращает объекты .NET. Это решение предлагает следующие возможности:

- журнал командной строки;
- заполнение нажатием клавиши TAB и подстановка команд;
- поддержка псевдонимов команд и параметров;
- создание конвейера для объединения команд;
- система справки в консоли, похожая на страницы man в Unix.



В качестве скриптового языка PowerShell обычно используется для автоматизации процессов управления системами. Это решение также часто используется для создания, тестирования и развертывания решений в средах CI/CD. В основе PowerShell лежит среда CLR .NET. Все входные и выходные данные являются объектами .NET. Отсутствует необходимость анализировать текстовые выходные данные для извлечения информации из них. Скриптовый язык PowerShell предлагает следующие возможности:

- расширяемость с использованием функций, классов, скриптов и модулей;
- расширяемая система форматирования для удобного вывода;
- расширяемая система типов для создания динамических типов;
- встроенная поддержка распространенных форматов данных, таких как CSV, JSON и XML.

Список источников:

1. https://ru.wikipedia.org/wiki/Программы_удалённого_администрирования

2. https://ru.wikipedia.org/wiki/SSH

3. https://ru.wikipedia.org/wiki/Virtual_Network_Computing

4. https://docs.microsoft.com/ru-ru/windows-server/remote/remote-server-administration-tools

5. https://docs.microsoft.com/ru-ru/windows-server/manage/windows-admin-center/overview

6. https://docs.microsoft.com/ru-ru/powershell/scripting/overview?view=powershell-7.1