

Просмотр и анализ логов RDP подключений в Windows

<http://winitpro.ru/index.php/2018/09/25/analizing-rdp-logs-windows-terminal-rds/>

В этой статье мы рассмотрим, особенности аудита / анализа логов RDP подключений в Windows. Как правило, описанные методы могут пригодиться при расследовании различных инцидентов на терминальных / RDS серверах Windows, когда от системного администратора требуется предоставить информацию: какие пользователи входили на RDS сервер, когда авторизовался и завершил сеанс конкретный пользователь, откуда / с какого устройства (имя или IP адрес) подключался RDP-пользователь. Я думаю, эта информация будет полезна как для администраторов корпоративных RDS ферм, так и владельцам RDP серверов в интернете (Windows VPS как оказалось довольно популярны).

Статья применима при исследовании RDP логов как в Windows Server 2008 R2, 2012/R2, 2016, так и в соответствующих десктопных версиях Windows (Windows 7, 8.1, 10).

Как и другие события, логи RDP подключения в Windows хранятся в журналах событий. Откройте консоль журнала событий (Event Viewer). Есть несколько различных журналов, в которых можно найти информацию, касающуюся RDP подключения.

В журналах Windows содержится большое количество информации, но быстро найти нужное событие бывает довольно сложно. Когда пользователь удаленно подключается к RDS серверу или удаленному столу (RDP) в журналах Windows генерируется много событий. Мы рассмотрим журналы и события на основных этапах RDP подключения, которые могут быть интересны администратору:

1. Network Connection
2. Authentication
3. Logon
4. Session Disconnect/Reconnect
5. Logoff

1. **Network Connection:** – установление сетевого подключения к серверу от RDP клиента пользователя. Событие с EventID – **1149 (Remote Desktop Services: User authentication succeeded)**. Наличие этого события не свидетельствует об успешной аутентификации пользователя. Этот журнал находится в разделе Applications and Services Logs -> Microsoft -> Windows -> **Terminal-Services-RemoteConnectionManager** -> Operational. Включите фильтр по данному событию (ПКМ по журналу-> Filter Current Log -> **EventId 1149**).

The screenshot shows the Windows Event Viewer interface. On the left, the tree view is expanded to 'Terminal-Services-RemoteConnectionManager' > 'Operational'. The main pane displays a list of events with the following columns: Level, Date and time, Source, Event ID, and Task Category. The events are as follows:

Level	Date and time	Source	Event ID	Task Category
Information	24.09.2018 16:18:33	Termin...	1149	None
Information	24.09.2018 16:18:27	Termin...	261	None
Information	24.09.2018 16:17:57	Termin...	261	None
Information	24.09.2018 16:16:55	Termin...	261	None
Information	24.09.2018 16:04:32	Termin...	1149	None
Information	24.09.2018 16:04:31	Termin...	261	None

Overlaid on the bottom right is the 'Filter Current Log' dialog box. It has a 'Filter' tab and an 'XML' sub-tab. The 'Logged' dropdown is set to 'Any time'. Under 'Event level', the 'Information' checkbox is selected. Under 'By log', the 'Event logs' dropdown is set to 'Microsoft-Windows-TerminalServices-Remote...'. The 'Event sources' dropdown is empty. At the bottom, there is a text input field containing '1149' and a 'Task category' dropdown.

В результате у вас получится список с историей всех сетевых RDP подключений к данному серверу. Как вы видите, в логах указывается имя пользователя, домен (используется NLA аутентификация, [при отключенном NLA](#) текст события выглядит иначе) и IP адрес компьютера, с которого осуществляется RDP подключение.

The screenshot shows the Windows Event Viewer interface. On the left, a tree view displays the 'TerminalServices-RemoteConnectionManager' log. The main pane shows a list of events filtered by 'Log: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational;'. One event is selected and its details are shown in a separate window.

Level	Date and Time	Source	Event ID	Task C...
Information	24.09.2018 16:18:33	Termin...	1149	None
Information	24.09.2018 16:04:32	Termin...	1149	None
Information	24.09.2018 15:29:03	Termin...	1149	None
Information	24.09.2018 15:20:48	Termin...	1149	None
Information	24.09.2018 15:06:33	Termin...	1149	None
Information	24.09.2018 14:45:26	Termin...	1149	None
Information	24.09.2018 13:06:31	Termin...	1149	None
Information	24.09.2018 11:56:22	Termin...	1149	None

Event 1149, TerminalServices-RemoteConnectionManager

General Details

Remote Desktop Services: User authentication succeeded:

User: otnikov
 Domain: CORP
 Source Network Address: 10. 1.55

Log Name: Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
 Source: TerminalServices-RemoteCo Logged: 24.09.2018 15:20:48
 Event ID: 1149 Task Category: None
 Level: Information Keywords:
 User: NETWORK SERVICE Computer: ts-cc

2. Authentication: – успешная или неуспешная аутентификация пользователя на сервере. Журнал Windows -> Security. Соответственно нас могут интересовать события с **EventID – 4624** (успешная аутентификация — An account was successfully logged on) или **4625** (ошибка аутентификации — An account failed to log on). Обратите внимание на значение LogonType в событии. При входе через терминальную службу RDP — **LogonType = 10**. Если **LogonType = 7**, значит выполнено переподключение к уже имеющейся RDP сессии.

The screenshot shows the Windows Event Viewer with the 'Security' log selected. A specific event (ID 4624) is highlighted, and its properties are displayed in a detailed window.

Computer Management

Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 2 569

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

Account Domain: CORP
 Logon ID: 0x3E7

Logon Type: 10

Impersonation Level: Impersonation

New Logon:
 Security ID: CORP\...
 Account Name: ...
 Account Domain: CORP
 Logon ID: 0x5E50F261
 Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
 Process ID: 0x1468
 Process Name: C:\Windows\System32\winlogon.exe

Network Information:
 Workstation Name: ...
 Source Network Address: 10. ...

Log Name: Security
 Source: Microsoft Windows security Logged: 24.09.2018 16:18:39
 Event ID: 4624 Task Category: Logon

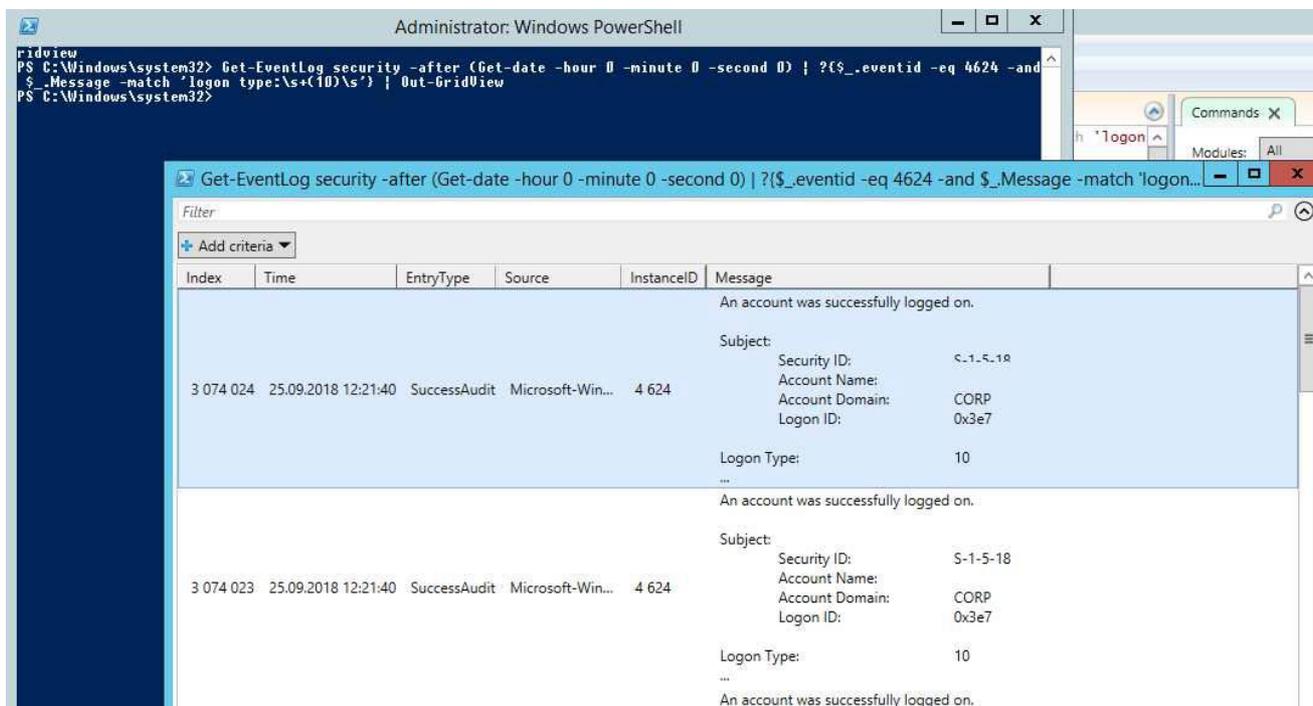
При этом имя пользователя содержится в описании события в поле **Account Name**, имя компьютера в **Workstation Name**, а имя пользователя в **Source Network Address**.

Обратите внимание на значение поля **TargetLogonID** – это уникальный идентификатор сессии пользователя с помощью которого можно отслеживать дальнейшую активность данного пользователя. Однако при отключении

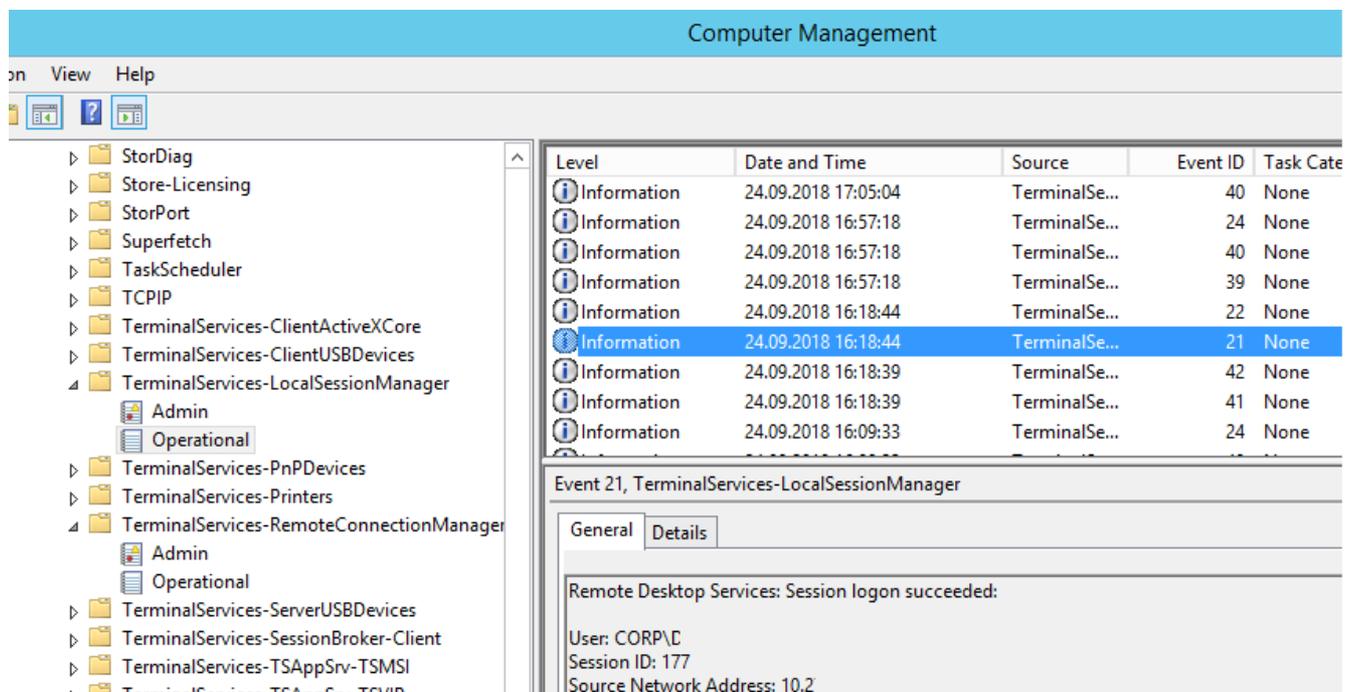
от RDP сессии (disconnect) и повторного переподключения в сессию, пользователю будет выдан новый TargetLogonID (хотя RDP сессия осталась той же самой).

Вы можете получить список событий успешных авторизаций по RDP (событие с EventID – 4624) с помощью такой команды PowerShell.

```
Get-EventLog security -after (Get-date -hour 0 -minute 0 -second 0) | ?{$_eventid -eq 4624 -and $_.Message -match 'logon type:\s+(10)\s'} | Out-GridView
```



- 3. Logon:** – RDP вход в систему, событие появляющееся после успешной аутентификации пользователя. Событие с EventID – 21 (Remote Desktop Services: Session logon succeeded). Этот журнал находится в разделе Applications and Services Logs -> Microsoft -> Windows -> TerminalServices-LocalSessionManager -> Operational. Как вы видите здесь можно узнать идентификатор RDP сессии для пользователя — Session ID.



Событие с EventID – 21 (Remote Desktop Services: Shell start notification received) означает успешный запуск оболочки Explorer (появление окна рабочего стола в RDP сессии).

- 4. Session Disconnect/Reconnect** – события отключения / переподключения к сессии имеют разные коды в зависимости от того, что вызвало отключение пользователя (отключение по неактивности, выбор пункта Disconnect в сессии, завершение RDP сессии другим пользователем или администратором и т.д.). Эти события находятся в разделе журналов Applications and Services Logs -> Microsoft -> Windows ->

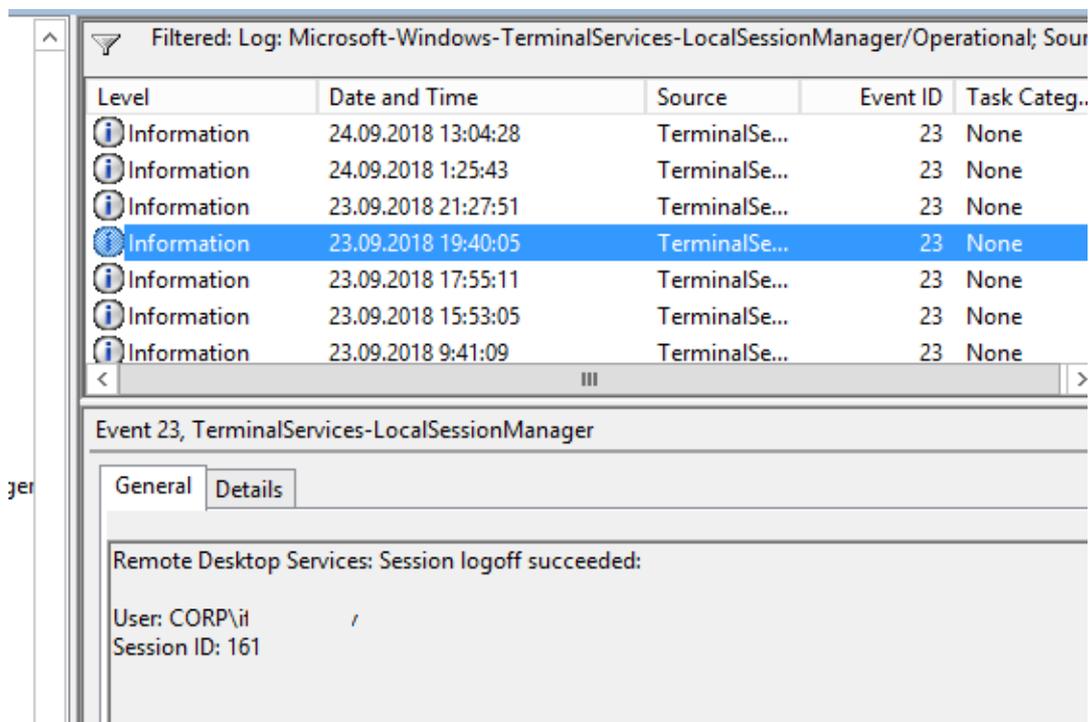
TerminalServices-LocalSessionManager -> Operational. Рассмотрим RDP события, которые могут быть интересными:

- **EventID – 24** (Remote Desktop Services: Session has been disconnected) – пользователь отключился от RDP сессии.
- **EventID – 25** (Remote Desktop Services: Session reconnection succeeded) – пользователь переподключился к своей имеющейся RDP сессии на сервере.
- **EventID – 39** (Session <A> has been disconnected by session) – пользователь сам отключился от своей RDP сессии, выбрав соответствующий пункт меню (а не просто закрыл окно RDP клиента). Если идентификаторы сессий разные, значит пользователя отключил другой пользователь (или администратор).
- **EventID – 40** (Session <A> has been disconnected, reason code). Здесь нужно смотреть на код причины отключения в событии. Например:
 - **reason code 0** (No additional information is available)– обычно говорит о том, что пользователь просто закрыл окно RDP клиента.
 - **reason code 5** (The client’s connection was replaced by another connection) – пользователь переподключился к своей старой сессии.
 - **reason code 11** (User activity has initiated the disconnect) – пользователь сам нажал на кнопку Disconnect в меню.

Событие с EventID – **4778** в журнале Windows -> Security (A session was reconnected to a Window Station). Пользователь переподключился к RDP сессии (пользователю выдается новый LogonID).

Событие с EventID **4799** в журнале Windows -> Security (A session was disconnected from a Window Station). Отключение от RDP сеанса.

5. **Logoff:** – выход пользователя из системы. При этом в журнале Applications and Services Logs -> Microsoft -> Windows -> TerminalServices-LocalSessionManager -> Operational фиксируется событие с EventID **23** (Remote Desktop Services: Session logoff succeeded).



При этом в журнале Security нужно смотреть событие с **EventID – 4634** (An account was logged off).

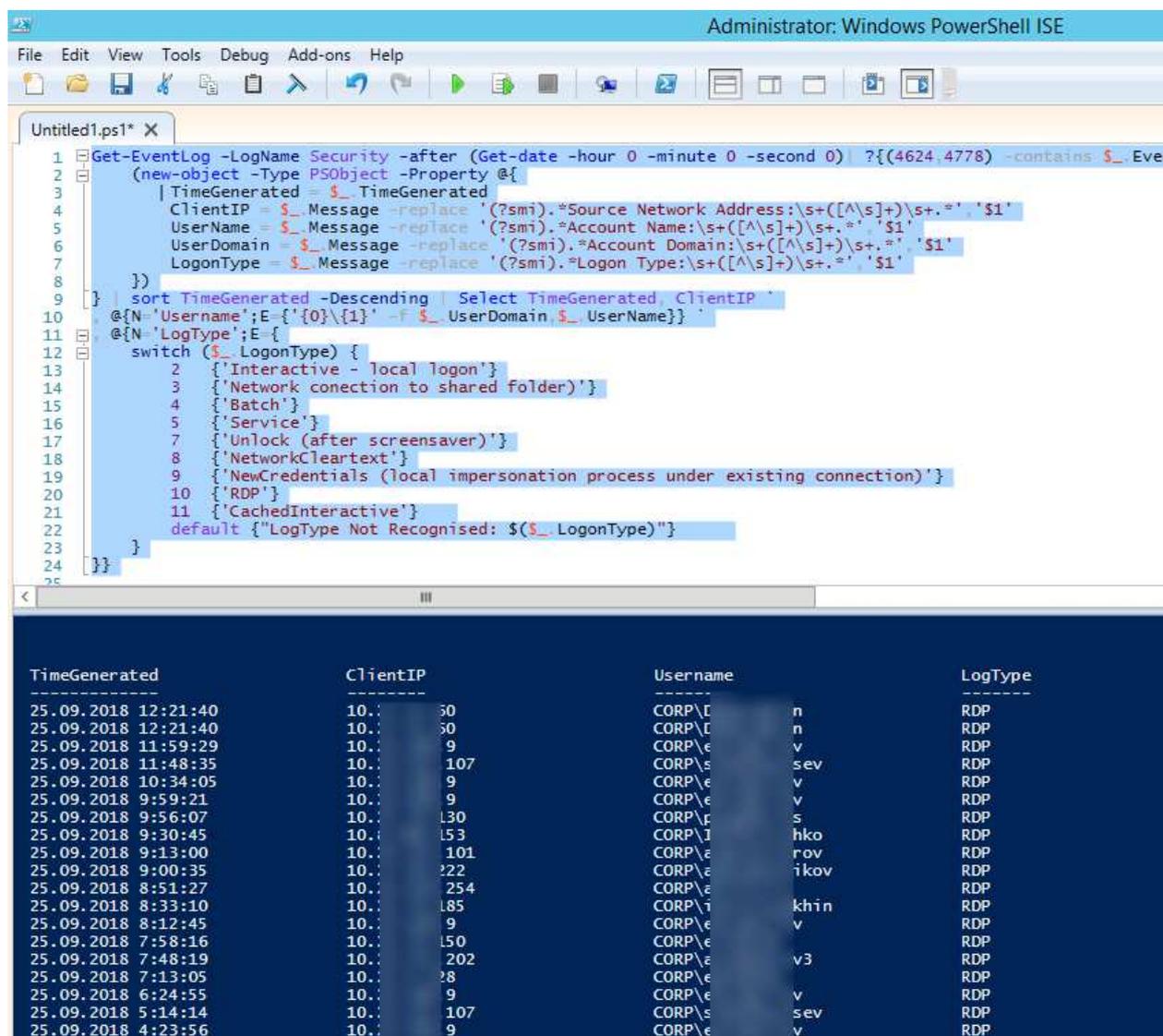
Событие с **EventID – 9009** (The Desktop Window Manager has exited with code (<X>)) в журнале System говорит о том, что пользователь инициировал завершение RDP сессии, и окно и графический shell пользователя был завершен.

Ниже представлен небольшой PowerShell, который выгружает из журналов терминального RDS сервера историю всех RDP подключений за текущий день. В полученной таблице указано время подключения, IP адрес клиента и имя RDP пользователя (при необходимости вы можете включить в отчет другие типы входов).

```

Get-EventLog -LogName Security -after (Get-date -hour 0 -minute 0 -second 0) | ?{(4624,4778) -contains
$_.EventID -and $_.Message -match 'logon type:\s+(\d+)\s'} | %{
(new-object -Type PSObject -Property @{
TimeGenerated = $_.TimeGenerated
ClientIP = $_.Message -replace '(?smi).*Source Network Address:\s+([\s])\s+.*','$1'
UserName = $_.Message -replace '(?smi).*Account Name:\s+([\s])\s+.*','$1'
UserDomain = $_.Message -replace '(?smi).*Account Domain:\s+([\s])\s+.*','$1'
LogonType = $_.Message -replace '(?smi).*Logon Type:\s+([\s])\s+.*','$1'
})
} | sort TimeGenerated -Descending | Select TimeGenerated, ClientIP `
, @{{N='Username';E='{0}\{1}' -f $_.UserDomain,$_ .UserName}} `
, @{{N='LogType';E={
switch ($_.LogonType) {
2 {'Interactive - local logon'}
3 {'Network connection to shared folder'}}
4 {'Batch'}}
5 {'Service'}}
7 {'Unlock (after screensaver)'}
8 {'NetworkCleartext'}}
9 {'NewCredentials (local impersonation process under existing connection)'}
10 {'RDP'}}
11 {'CachedInteractive'}}
default {"LogType Not Recognised: $($_.LogonType)"}
}
}}

```



Иногда бывает удобно с логами в таблице Excel, в этом случае вы можете выгрузить любой журнал Windows в текстовый файл и импортировать в Excel. Экспорт журнала можно выполнить из консоли Event Viewer (конечно, при условии что логи не очищены) или через командную строку:

```
WEVTUtil query-events Security > c:\ps\security_log.txt
```

Или так:

```
get-winevent -logname "Microsoft-Windows-TerminalServices-LocalSessionManager/Operational" | Export-Csv c:\ps\rdp-log.txt -Encoding UTF8
```

Список текущих RDP сессий на сервере можно вывести командой:

`qwinsta`

Команда возвращает как идентификатор сессии (ID), имя пользователя (USERNAME) и состояние (Active/Disconnect). Эту команду удобно использовать, когда нужно определить ID RDP сессии пользователя при [теневоом подключении](#).

```
PS C:\Windows\system32> qwinsta
SESSIONNAME      USERNAME          ID  STATE  TYPE      DEVICE
-----
services         0                Disc
console          1                Conn
rdp-tcp#29       ██████████       156 Active
rdp-tcp#78       ██████████       157 Active
                 ██████████       158 Disc
                 ██████████       159 Disc
                 ██████████       160 Disc
                 ██████████       161 Disc
                 ██████████       163 Disc
rdp-tcp#63       ██████████       167 Active
rdp-tcp#37       ██████████       172 Active
                 ██████████       174 Disc
                 ██████████       176 Disc
>rdp-tcp#62       ██████████       177 Active
rdp-tcp          ██████████       65536 Listen
PS C:\Windows\system32>
```

Список запущенных процессов в конкретной RDP сессии (указывается ID сессии):

`qprocess /id:157`

```
Select Administrator: Windows Po
PS C:\Windows\system32> qprocess /id:157
USERNAME      SESSIONNAME      ID  PID  IMAGE
-----
(unknown)     rdp-tcp#78       157 10324  csrss.exe
system        rdp-tcp#78       157 5632  winlogon.exe
(unknown)     rdp-tcp#78       157 7228  dwm.exe
(unknown)     rdp-tcp#78       157 8940  taskhostex.exe
(unknown)     rdp-tcp#78       157 7564  rdpclip.exe
(unknown)     rdp-tcp#78       157 6288  rdpinit.exe
(unknown)     rdp-tcp#78       157 4764  rdpshell.exe
(unknown)     rdp-tcp#78       157 7012  r.exe
system        rdp-tcp#78       157 6776  logonui.exe
PS C:\Windows\system32>
```

На RDP-клиенте логи не такие информационные, основное чем часто пользуются информация об [истории RDP подключений](#) в реестре.