*Статья базы знаний*

# #108 Просмотр и анализ логов RDP подключений в

Windows

Описание

**Просмотр и анализ логов RDP подключений в Windows**

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.

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).

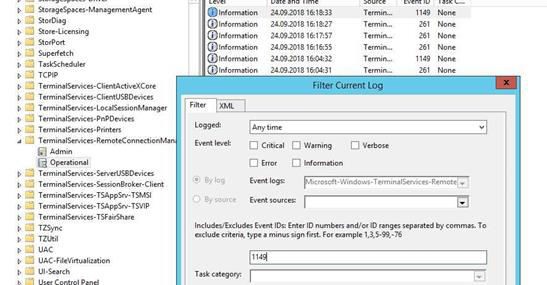
Как и другие события, логи RDP подключения в Windows хранятся в журналах событий. Откройте консоль журнала событий (Event Viewer). Есть несколько различных журналов, в которых можно найти информацию, касающуюся RDP подключения.

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:

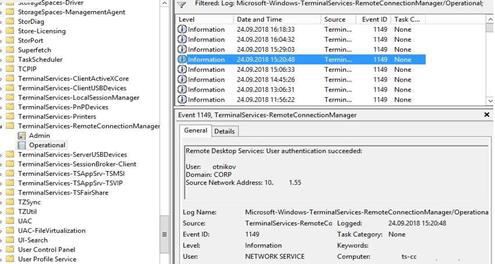
## Network Connection

1. **Authentication**
2. **Logon**
3. **Session Disconnect/Reconnect**
4. **Logoff**
5. **Network Connection:** – установление сетевого подключение 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** ->

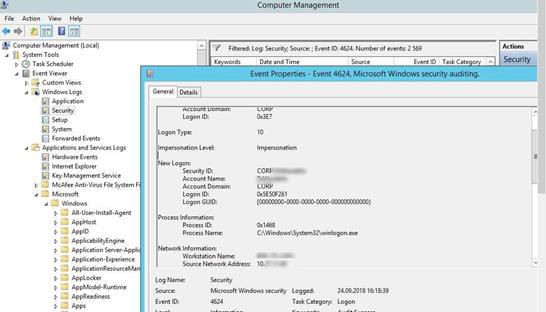
Operational. Включите фильтр по данному событию (ПКМ по журналу-> Filter Current Log -> **EventId 1149**).



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.



1. **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.

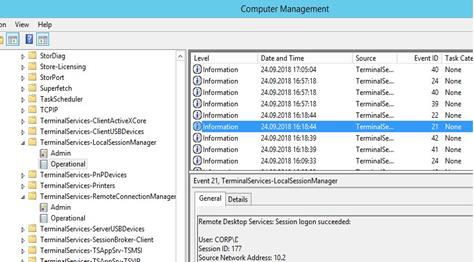


При этом имя пользователя содержится в описании события в поле **Account Name**, имя компьютера в

**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).

1. **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).

1. **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.

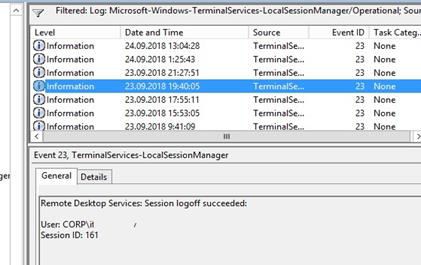
Событие с EventID – **4778** в журнале Windows -> Security (A session was reconnected to a Window Station).

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.

1. **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).



# Решение Обходной путь Файлы

*Опубликовал: Конаков Андрей Андреевич Дата публикации: 24.05.2023 13:14 Раздел базы знаний: Технические статьи Тип статьи: Помощь в работе*