

Домен на базе Microsoft Windows - полезные вещи

Серверы

- Управление всеми серверами - только через один или несколько management-серверов, имеющих все консоли управления, необходимые оснастки и ПО. Управление напрямую с рабочих станций ИТ-сотрудников заблокировано
- На каждом сервере обязательно работают:
 - Firewall с настроенными правилами
 - UAC (если только его отключение не требует установленное ПО и сервисы)
 - Windows Update
 - Антивирус (если это не снижает функционал сервера)

Рабочие станции

- Пользователи работают на рабочих станциях (VDI) с минимальными правами
- Обязательная настройка Software Restriction Policies (SRP) или AppLocker. Две стратегии: «Разрешить запуск исполняемых файлов на компьютере только из определенных папок» (самый надежный метод, но требует длительного периода отладки и выявления нужного ПО, которое не работает в такой конфигурации) или «Запрет запуска исполняемых файлов из пользовательских каталогов» - выбираем подходящую для наших нужд.
- Вся рабочая информация и документы хранится на сетевых ресурсах для централизованной раздачи прав, так же удобно для резервного копирования
- На ПК пользователей принудительно включить и настроить VSS (Volume Shadow Copy) - очень помогает любителям хранить все на рабочем столе от шифровальщиков

Учетные записи (УЗ)

- Самый крутой администратор работает на своей рабочей станции с такой же бесправной доменной учеткой как и все другие пользователи. Работа с серверами и сервисами - под отдельной учеткой.
- Каждый день скриптом блокируются УЗ пользователей, более NN дней не входивших в систему. После блокировки такие записи переносятся в OU=Disabled
- Каждый день скриптом блокируются и переносятся в отключенные пользовательские компы, которые не входили в систему более NN дней

Файловый доступ

- Построение файловых ресурсов - на основе DFS, видимость для пользователей согласно ролевой модели с использованием ABE (Access-Based Enumeration / Перечисление на основании доступа)
- Раздача прав только на логическую единицу «каталог», никаких индивидуальных прав на

отельные файлы

- Права раздаются только группам пользователей

From:

<https://wiki.rtzra.ru/> - **RTzRa's hive**

Permanent link:

<https://wiki.rtzra.ru/software/windows/windows-domain-concepts>

Last update: **2019/02/12 17:42**

