

Сервисные операции

Сервисные операции для ресурсов Windows

Сервисные операции для ресурсов Windows выполняются от имени доменной или локальной учётной записи:

- Проверка соединения с ресурсом
- Синхронизация локальных учётных записей
- Проверка пароля локальных учётных записей
- Изменение пароля локальных учётных записей
- Получение данных о ОС
- Получение списка групп безопасности

Настройка доменной учётной записи в качестве сервисной

1. Выполните вход на ресурс.
2. Запустите оснастку **Управление компьютером** (Computer management)
3. Перейдите в раздел **Служебные программы** (System tools) - **Локальные пользователи** (Local Users and Groups) - **Группы** (Groups)
4. Откройте контекстное меню группы **Администраторы** (Administrators)
5. Выберите пункт **Свойства** (Properties)
6. Нажмите **Добавить** (Add)
7. Выберите доменную учётную запись, которая будет использоваться в роли сервисной для ресурса и нажмите **Ок**

Настройка локальной учётной записи в качестве сервисной

Если в качестве сервисной учётной записи будет использоваться локальный встроенный (built-in) администратор, то дополнительная настройка не требуется. Если в качестве сервисной учётной записи будет использоваться не встроенная локальная учётная запись администратора, то необходимо:

1. Выполните вход на ресурс.
2. Запустите оснастку **Управление компьютером** (Computer management)
3. Перейдите в раздел **Служебные программы** (System tools) - **Локальные пользователи** (Local Users and Groups) - **Группы** (Groups)
4. Откройте контекстное меню группы **Администраторы** (Administrators)
5. Выберите пункт **Свойства** (Properties)
6. Нажмите **Добавить** (Add)
7. Выберите локальную учётную запись, которая будет использоваться в роли сервисной для ресурса и нажмите **Ок**
8. Запустите **Редактор реестра** (RegEdit)
9. Раскройте ветку
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
10. Откройте контекстное меню раздела **System**
11. Выберите пункт **Создать** (Create) - **Параметр DWORD 32** (DWORD (32-bit) Value)
12. Введите название параметра - **LocalAccountTokenFilterPolicy**
13. Откройте контекстное меню параметра **LocalAccountTokenFilterPolicy**
14. Выберите пункт **Изменить** (Modify) и установите **Значение:** (Value data:) равное **1**

Настройка реестра необходима из-за ограничений удалённого управления WinRM для всех локальных учётных записей, кроме встроенного (built-in) администратора.

Настройка Indeed PAM Core для выполнения сервисных операций от имени локальных учётных за ресурса

Сервисные операции выполняются при помощи WinRM, для использования локальных учётных записей ресурса в качестве сервисных необходимо добавить ресурс в список доверенных **TrustedHosts** на сервере Indeed PAM Core.

Настройка TrustedHosts

1. Выполните вход на сервер Indeed PAM Core
2. Откройте **Командную строку** (CMD) от имени администратора
3. Выполните команду

```
C:\>winrm s winrm/config/client @{TrustedHosts="Resource1.domain.local, Resource2.domain.local"}
```

Указанные ресурсы будут добавлены в список доверенных.

При добавлении новых ресурсов в список доверенных необходимо указывать добавленные ранее ресурсы и новые, так как новое значение перезаписывает старое.

```
@{TrustedHosts="Resource1.domain.local, Resource2.domain.local, Resource3.domain.local"}
```

Сервисные операции в Active Directory

Настройка сервисной учётной записи

1. Запустите оснастку **Active Directory - пользователи и компьютеры** (Active Directory Users and Computers).
2. Откройте контекстное меню контейнера или подразделения.
3. Выберите пункт **Создать** (Create) - **Пользователь** (User)
4. Укажите имя, например, **IPAMADServiceOps**
5. Заполните обязательные поля и завершите создание учётной записи.
6. Откройте контекстное меню контейнера, подразделения или корня домена.
7. Выберите пункт **Свойства** (Properties)
8. Перейдите на вкладку **Безопасность** (Security)
9. Нажмите **Добавить** (Add)
10. Выберите учётную запись **IPAMADServiceOps** и нажмите **Ок**
11. Нажмите **Дополнительно** (Advanced)
12. Выберите учётную запись **IPAMADServiceOps** и нажмите **Изменить** (Edit)
13. Установите для поля **Применяется к:** (Applies to:) значение **Дочерние объекты: Пользователь** (Descendant User objects)
14. В разделе **Разрешения:** (Permissions:) отметьте **Сброс пароля** (Reset password)
15. Сохраните внесённые изменения

Сервисные операции для ресурсов *nix

Сервисные операции для ресурсов *nix выполняются от имени локальной сервисной учётной записи:

- Проверка соединения с ресурсом
- Поиск учётных локальных записей доступа
- Проверка пароля локальных учётных записей доступа
- Изменение пароля локальных учётных записей доступа
- Получение данных о ОС
- Получение списка групп безопасности

Создание и настройка сервисной учётной записи

1. Выполните вход на ресурс
2. Запустите **Терминал** (Terminal)
3. Создайте пользователя, например, **IPAMService**

```
adduser IPAMService
```

4. Добавьте пользователя в группу **SUDO**

```
usermod -aG sudo IPAMService
```

Настройка группы привилегированных учётных записей

Автоматический поиск и добавление учётных записей доступа в Indeed PAM выполняется на основании их права на выполнение команды SUDO. Для предоставления прав на выполнение команды SUDO необходимо внести изменения в файл **/etc/sudoers**