Создание и использование gMSA для запуска сервера 1С

Введение

Group Managed Service Account (gMSA) — это специальный тип сервисной учетной записи в Active Directory, который позволяет автоматически управлять паролем и использовать её для запуска служб без необходимости вручную вводить и обновлять пароль. Данная статья описывает процесс создания и настройки gMSA для запуска сервера 1С.

Шаг 1. Создание корневого ключа KDS на контроллере домена

На контроллере домена создаём корневой ключ службы распространения ключей (Key Distribution Service, KDS):

powershell

```
Add-KdsRootKey –EffectiveImmediately
```

> **Важно:** Ключ начинает работать через 10 часов. Для тестовых целей можно ускорить процесс:
>
> powershell
>
> ```
> # For single-DC test environments only
> Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)
> ```

Шаг 2. Проверка создания корневого ключа KDS

Проверяем, что корневой ключ KDS успешно создан:

powershell

```
Get-KdsRootKey
Test-KdsRootKey -KeyId (Get-KdsRootKey).KeyId
```

Шаг 3. Создание группы для серверов

Создаём глобальную группу безопасности, в которую будут входить серверы, имеющие право использовать gMSA:

powershell

```
New-ADGroup MySQLServers -path 'OU=SQLServers,dc=example,DC=local' -GroupScope Global -
PassThru –Verbose
```

Шаг 4. Добавление серверов в группу

Добавляем в созданную группу серверы, которые смогут использовать gMSA:

powershell

```
Add-AdGroupMember -Identity MySQLServers -Members SQLServ1$, SQLServ2$, SQLServ3$
```

> **Примечание:** Имена компьютеров указываются со знаком `$` на конце.

Шаг 5. Создание групповой управляемой сервисной учетной записи

(gMSA)

Создаём gMSA для группы `MySQLServers`:

powershell

```
New-ADServiceAccount -name gmsaSrv1c -DNSHostName gmsaSrv1c.example.local -
PrincipalsAllowedToRetrieveManagedPassword MySQLServers –verbose
```

Шаг 6. Перезапуск серверов

Перезапускаем серверы, на которых планируется использовать gMSA. Это необходимо для того, чтобы серверы получили актуальный состав групп и членство в `MySQLServers`.

Шаг 7. Установка модуля PowerShell для Active Directory

На каждом сервере, где будет использоваться gMSA, устанавливаем модуль PowerShell для работы с Active Directory:

powershell

```
Add-WindowsFeature RSAT-AD-PowerShell
```

Шаг 8. Установка учетной записи gMSA на сервере

На каждом сервере устанавливаем учетную запись gMSA:

powershell

```
Install-ADServiceAccount -Identity gmsaSrv1c
```

Шаг 9. Проверка корректности установки gMSA

Проверяем, что gMSA успешно установлена и готова к использованию:

powershell

```
Test-ADServiceAccount gmsaSrv1c
```

Дополнительные команды

Изменение периодичности смены пароля

По умолчанию пароль gMSA меняется каждые 30 дней. Изменить интервал можно командой:

powershell

```
Set-ADServiceAccount gmsaSrv1c -ManagedPasswordIntervalInDays 60
```

Получение времени последней смены пароля

powershell

```
Get-ADServiceAccount -Identity gmsaSrv1c -Properties passwordlastset
```

Настройка запуска службы 1С из-под gMSA

Для запуска службы из-под сервисной учетной записи gMSA необходимо:

1. Открыть свойства нужной службы.
2. Перейти на вкладку **Log on** (Вход в систему).
3. Выбрать пункт **This account** (С учетной записью).
4. Указать имя сервисной учетной записи **со знаком** `$` **на конце** (например, `gmsaSrv1c$`), **без указания пароля**.
5. Перезапустить службу.

> **Важно:** Для корректной работы сервера 1С необходимо предоставить полные права учетной записи gMSA на каталог `SRVINFO`.

Примечание

Использовать gMSA напрямую, например, на NAS Synology, не получится. Однако можно включить учетную запись gMSA в глобальную группу безопасности и назначать разрешения на NAS уже для этой группы.

Версия #6
Admin создал 2026-09-10 12:24:34 UTC
Admin обновил 2026-09-10 12:52:52 UTC