Восстановление Active Directory из резервной копии

winitpro.ru/index.php/2019/10/31/vosstanovlenie-active-directory-backup

itpro

В этой статье мы покажем, как восстановить контроллер домена Active Directory из резервной копии System State (см. статью Резервное копирование Active Directory) и рассмотрим типы и принципы восстановления DC в AD.

При выходе из строя контроллера домена, даже если у вас актуальный бэкап, нужно выбрать сценарий восстановления, который вы будете использовать. Это зависит от того, есть ли у вас в сети другие исправные контроллеры домена, доступны ли они по сети с площадки со сломанным DC и цела ли база Active Directory на них.

Развертывание нового контроллера домена AD через репликацию

Если у вас развернуто несколько контроллеров домена (а это рекомендуемая конфигурация для Active Directory), вместо восстановления неисправного сервера с ролью DC из бэкапа, бывает проще развернуть на площадке новый контроллер домена.

Если размер базы ADDS небольшой и другой DC доступен по скоростному каналу, это намного быстрее, чем восстанавливать DC из бэкапа. Старый контроллер нужно просто удалить из AD (если на вышедшем из строя DC были запущены роли FSMO, нужно их предварительно передать на другой сервер).
После повышения сервера до DC, новый контроллера домена синхронизирует (реплицирует) базу данных ntds.dit, объекты GPO, содержимое папки SYSVOL и другие объекты AD с других DC, оставшихся доступными онлайн. Это самый простой способ восстановления работоспособности DC, который гарантирует что вы не внесете непоправимых изменений в AD.

Полномочное и неполномочное восстановление Active Directory

Есть два типа восстановления службы каталогов Active Directory Domain Services из резервной копии, в которых нужно четко разобраться перед началом восстановления:

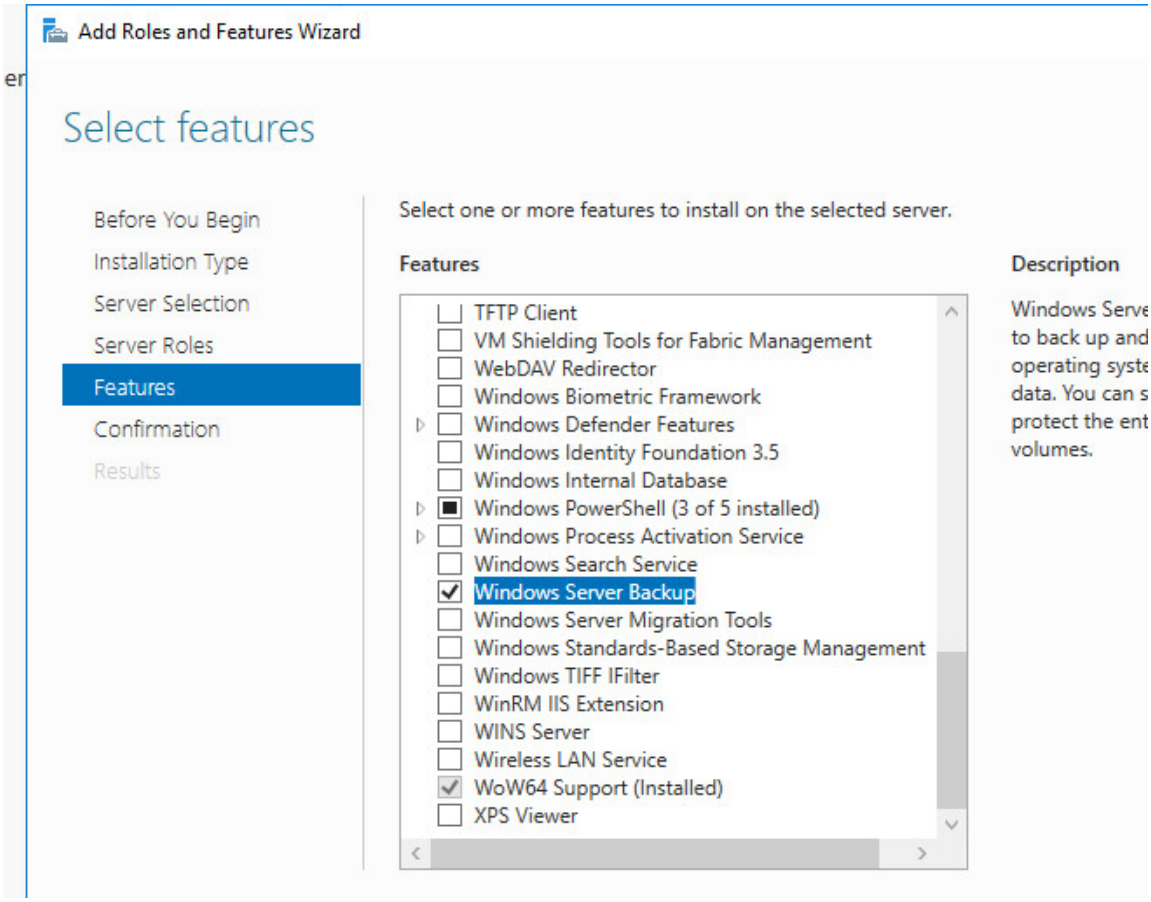
- **Authoritative Restore** (полномочное или авторитетно восстановление) – после восстановления объектов AD выполняется репликация с восстановленного DC на все остальные контроллеры в домене. Этот тип восстановления используется в сценариях, когда упал единственный DC или все DC одновременно (например, в результате атаки шифровальщика или вируса), или когда по домену реплицировалась поврежденная база NTDS.DIT. В этом режиме у всех восстановленных объектов AD значение USN (Update Sequence Number) увеличивается на 100000. Такие восстановленные объекты будут считаться более новыми другими DC, и будут реплицированы по домену. Полномочный способ восстановления нужно использовать очень аккуратно!!!
  При полномочном восстановлении вы потеряете все изменения в AD, произошедших с момента создания бэкапа (членство в группах AD, атрибуты Exchange и т.д.).
- **Non-Authoritative Restore** (неполномочное или не-авторитиативное восстановление) – способ используется при выходе из строя физического/виртуального сервера, на котором развернут DC. Восстановленный контроллер домена после развертывания из бэкапа сообщает другим DC, что он восстановлен из резервной копии и ему нужны последние изменения в AD (для DC создается новый DSA Invocation ID). Этот способ восстановления можно использовать на удаленных площадках, когда сложно сразу реплицировать большую базу AD по медленному WAN каналу; или когда на сервере имелись какие-то важные данные или приложения.

Восстановление контроллера домена AD из system state бэкапа

Предположим, что в домене имелся только один DC, который стал недоступен вследствие выхода из строя физического сервера. У вас есть относительно свежий бэкап System State старого контроллера домена, и вы хотите восстановить Active Directory на новом сервере в режиме полномочного восстановления.

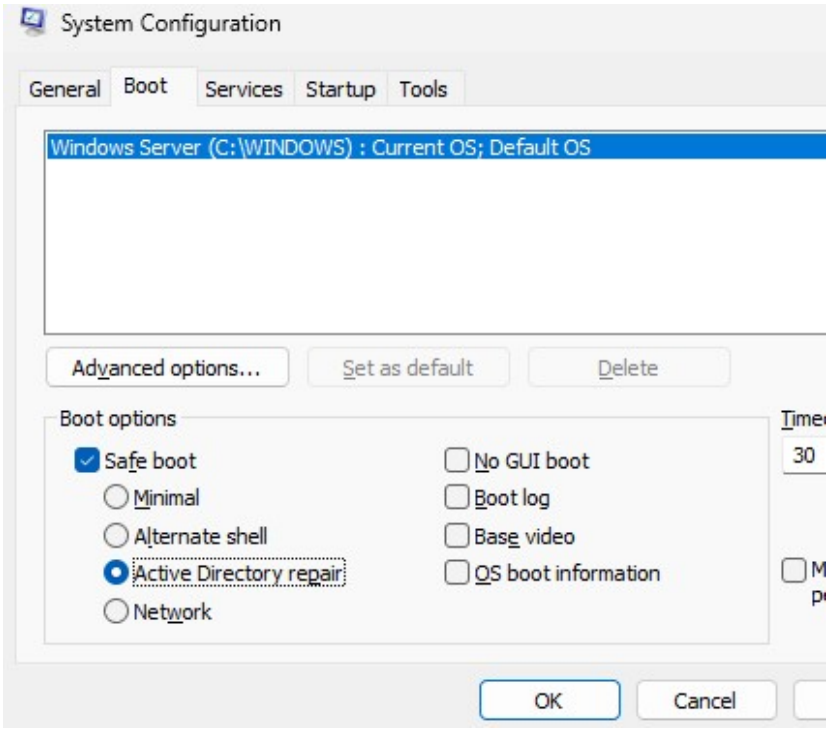
Подготовьте новый сервер (физический или виртуальный) для развертывания DC из бэкапа:

- На новом сервере должна быть установлена та же самая версия Windows Server, что на неисправном DC
- Выполните чистую установку Windows Server. Не нужно пока задавать ему имя компьютера (hostname) старого DC и IP адрес.
- Установите роль **Active Directory Domain Services** (не настраивая ее) и компонент **Windows Server Backup**. Можно установить эти компоненты из Server Manager или с помощью PowerShell: `Install-WindowsFeature -Name AD-Domain-Services, Windows-Server-Backup`

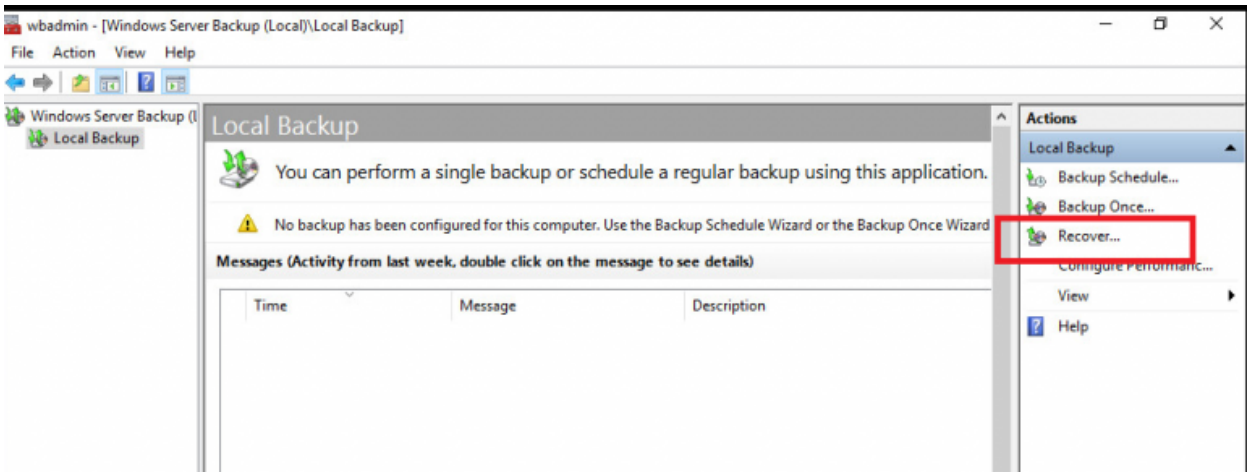


Чтобы приступить к восстановлению Active Directory, нужно загрузить сервер в режиме восстановления служб каталогов **DSRM** (Directory Services Restore Mode). Для этого запустите `msconfig` и на вкладе **Boot** выберите Safe Boot -> **Active Directory repair**. Или выполните команды:

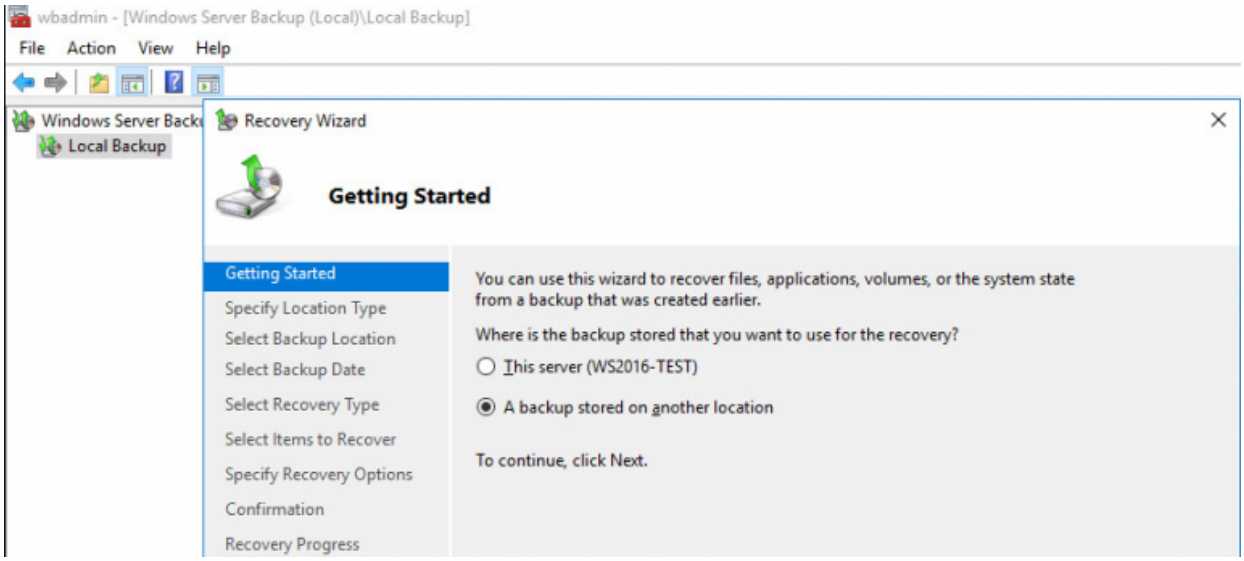
```
bcdedit /set safeboot dsrepair
shutdown /r /t 0
```



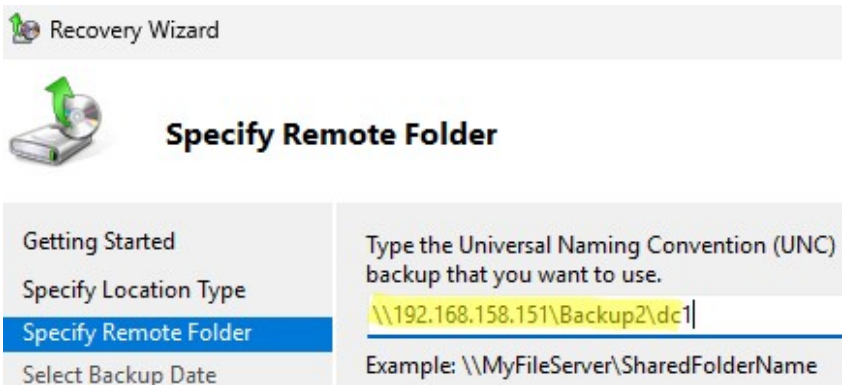
После перезагрузки сервер перейдет в безопасный режим DSRM. Запустите консоль управления Windows Server Backup (`wbadmin.msc`) и в правом меню выберите **Recover**.



В мастере восстановления выберите, что резервная копия хранится в другом месте (A backup stored on another location).



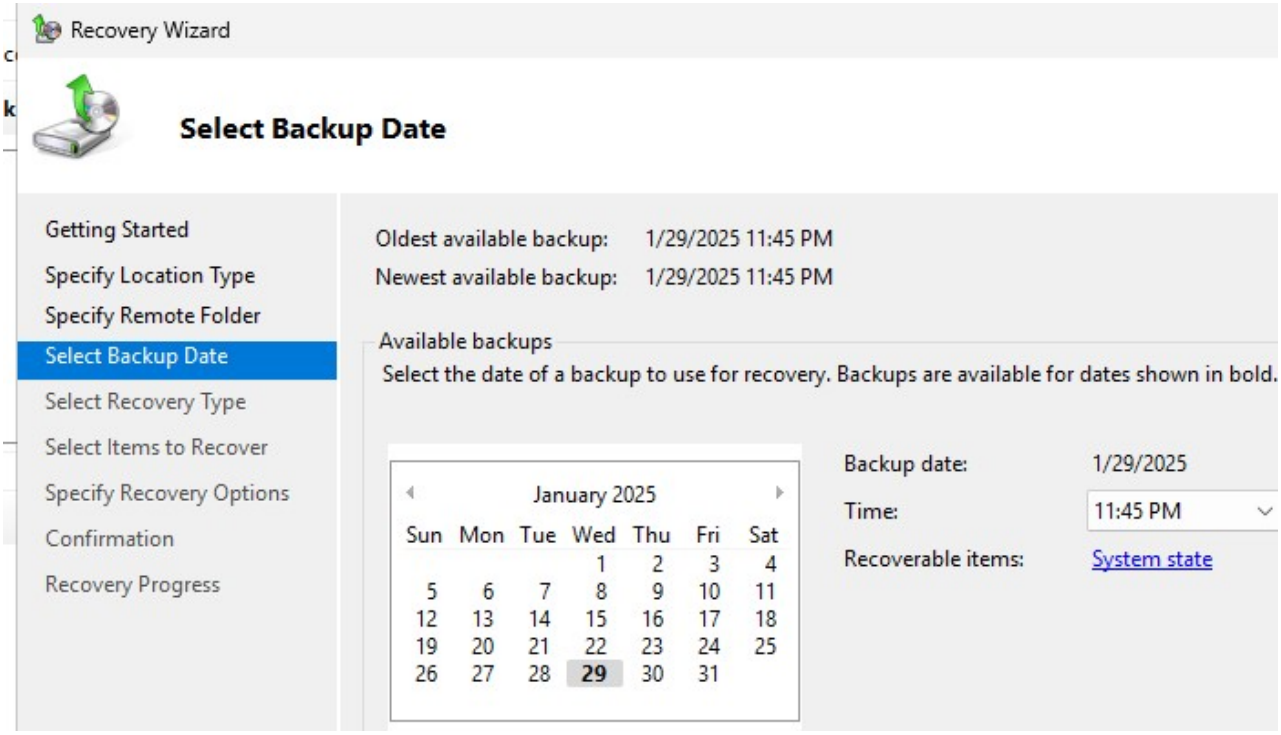
Выберите диск, на котором находится резервная копия DC, или укажите UNC путь к сетевой папке, содержащей **WindowsImageBackup**. Например `\\FileServer1\Backup\DC1` .



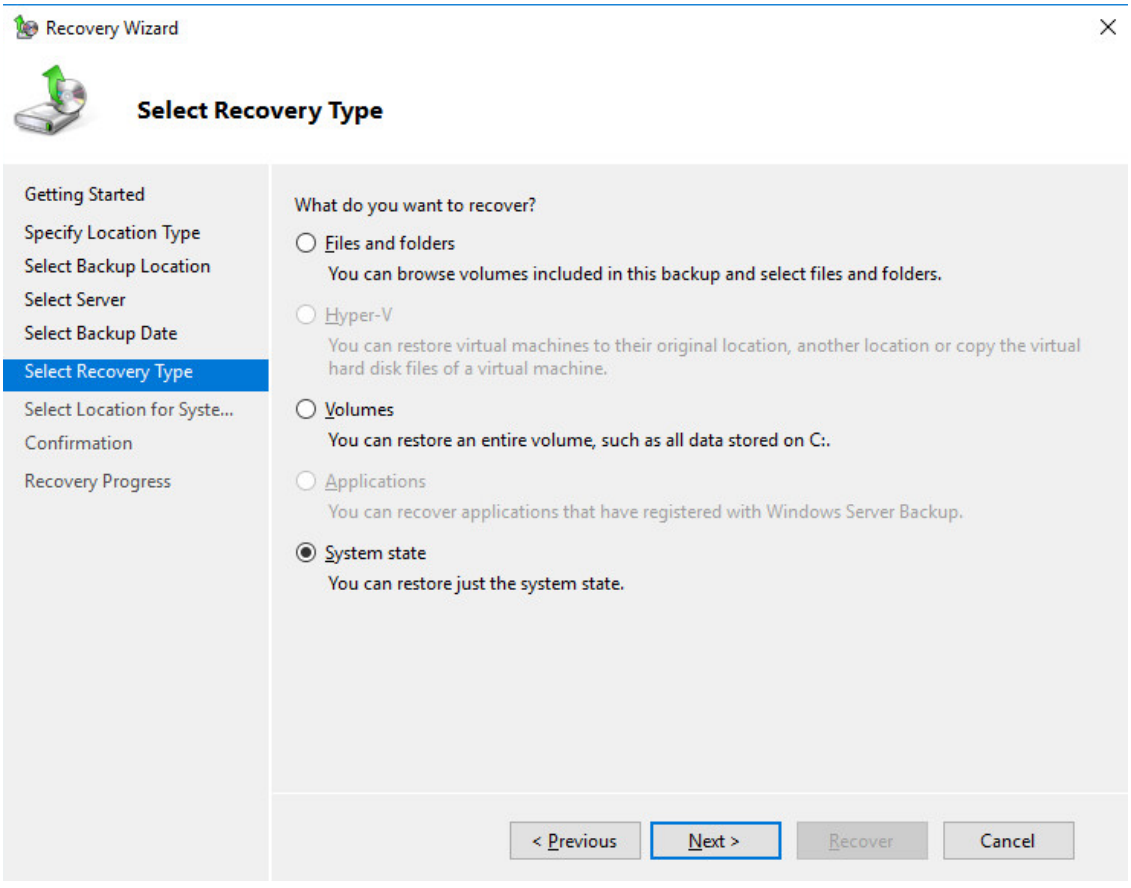
Если вы хотите использовать для восстановления резервную копию с локального диска, нужно поместить каталог WindowsImageBackup в корень диска. Проверить

наличие резервных копий на диске с помощью команды:
`wbadmin get versions -backupTarget:D:`

Выберите дату, на которую нужно восстановить резервную копию.

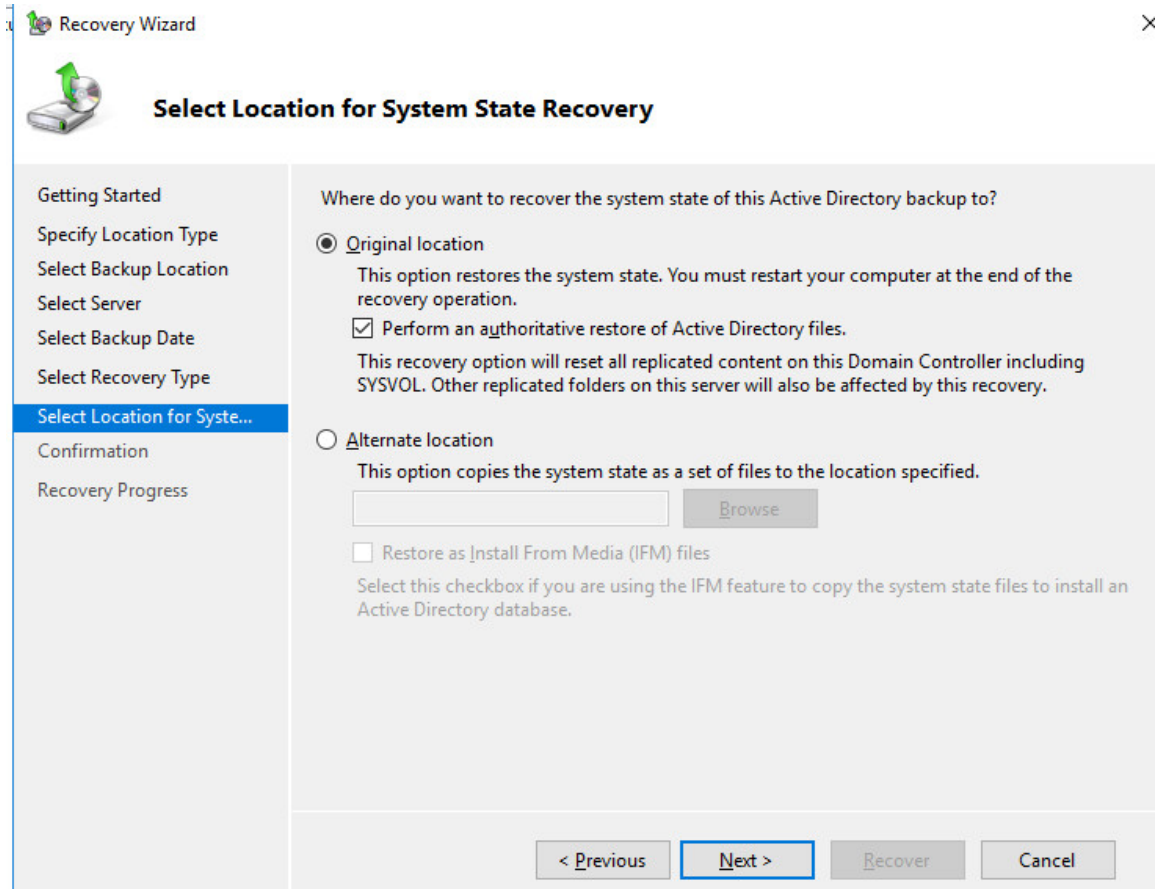


Укажите, что вы восстанавливаете состояние **System State.**

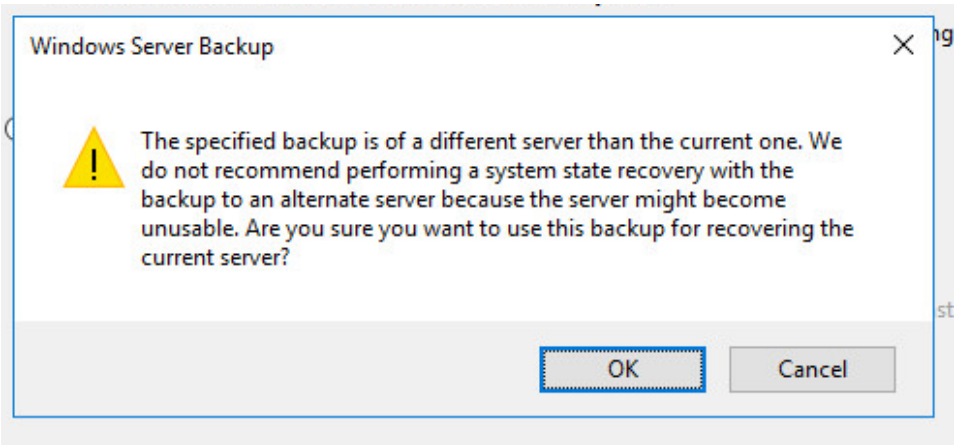


Выберите для восстановления «Исходное размещение» (Original location) и обязательно установите галочку «**Выполнить заслуживающее доверия восстановление файлов Active Directory» (Perform an authoritative restore of Active Directory files**). (напоминаю что мы рассматриваем сценарий авторитативного восстановления AD, когда в сети единственный DC, других исправных контроллеров домена нет!!).

Если эта опция отключена, будет выполнено non-authoritative восстановление.



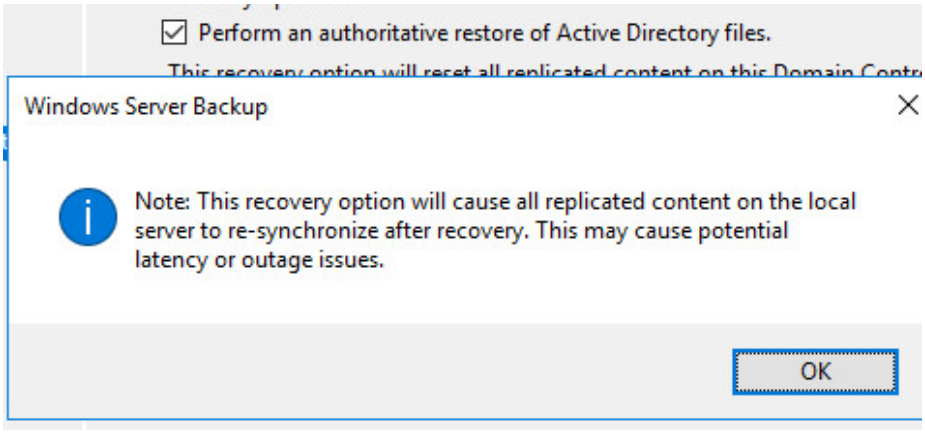
Система покажет предупреждение, что эта резервная копия другого сервера, и что при восстановлении на другом сервере может не завестись. Продолжаем.



Согласитесь с еще одним предупреждением:

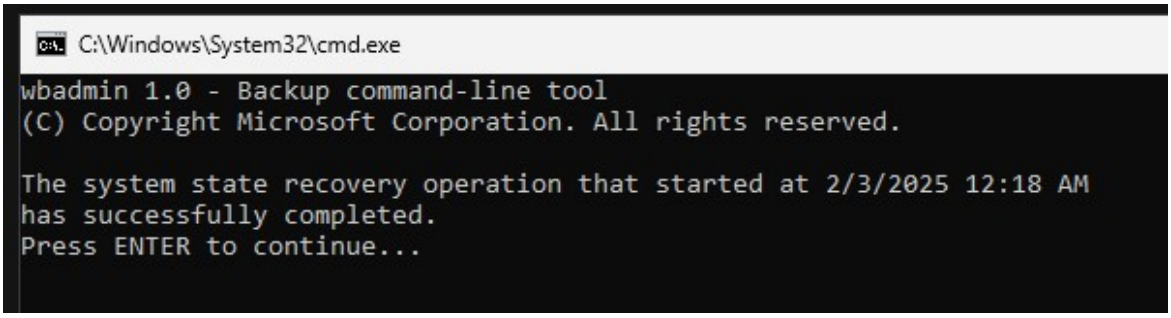
```
Windows Server Backup

Note: This recovery option will cause replicated content on the local server to re-
synchronize after recovery. This may cause potential latency or outage issues.
```



После этого запустится процесс восстановления контроллера домена AD на новом сервере. По завершении сервер потребует перезагрузку (имя нового сервера будет автоматически изменено на имя DC в бэкапе).

После перезагрузки, войдите на сервер с локальной учтённой записью администратора DSRM. Указав имя пользователя в формате `.\administrator`



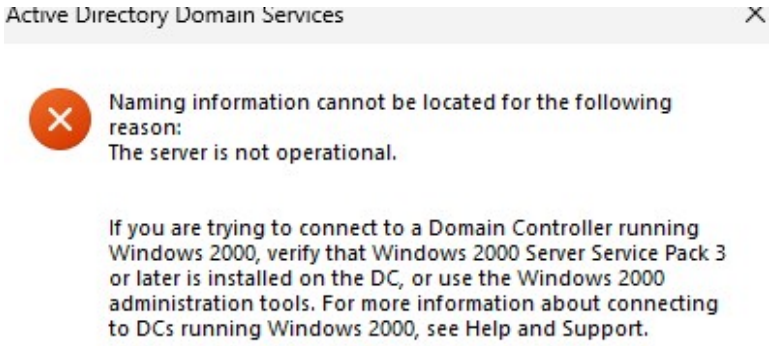
Теперь можно загрузить DC в обычном режиме, отключив загрузку DSRM из `msconfig` или командой:

```
bcdedit /deletevalue safeboot
```

Авторизуйтесь на сервере под учетной записью с правами администратора домена. (если не знаете пароль администратора домена, его можно сбросить).

На данный момент служба ADDS еще не работает. При попытке запустить оснастку ADUC, появится ошибка:

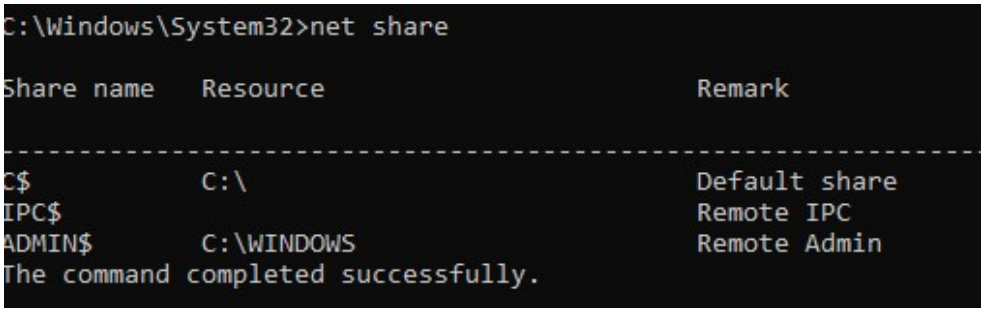
```
Active Directory Domain Services
Naming information cannot be located for the following reason:
The server is not operational.
```



Выводит список опубликованных общих папок на сервере командой:

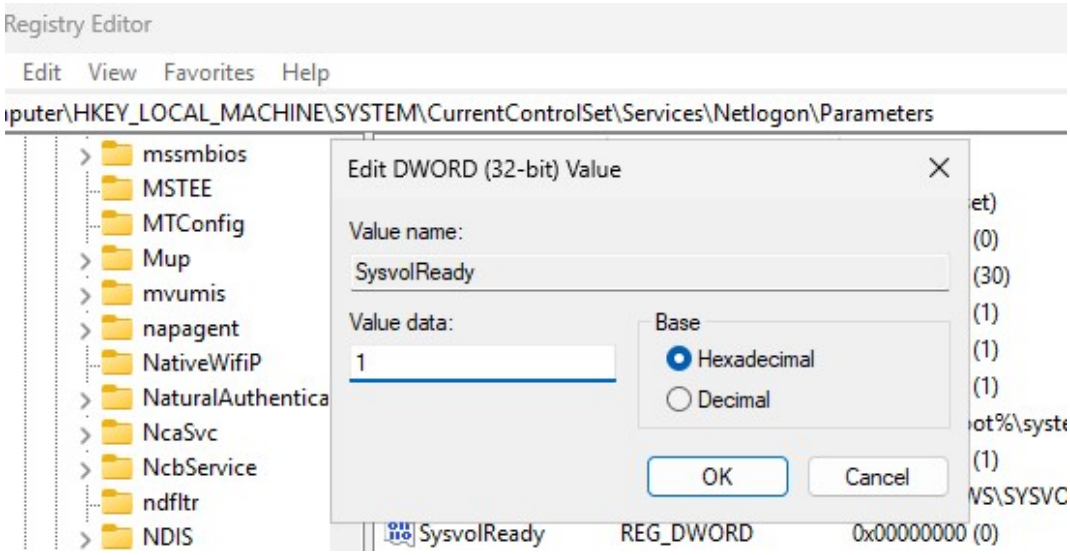
```
net share
```

Как вы видите, отсутствуют сетевые сетевых папки SYSVOL и NETLOGON.

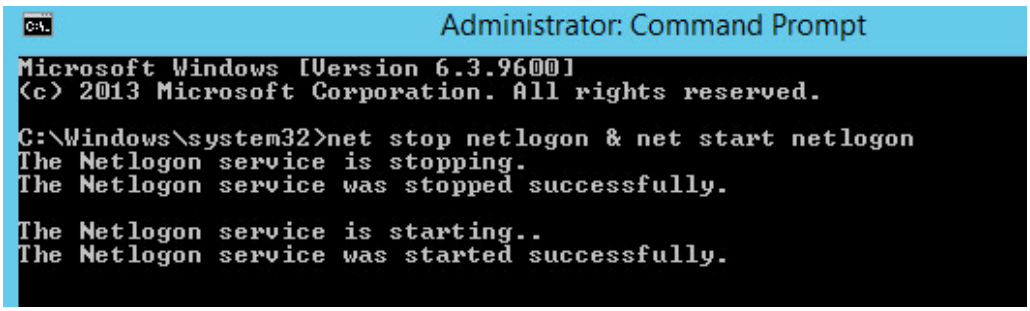


Чтобы исправить ошибку:

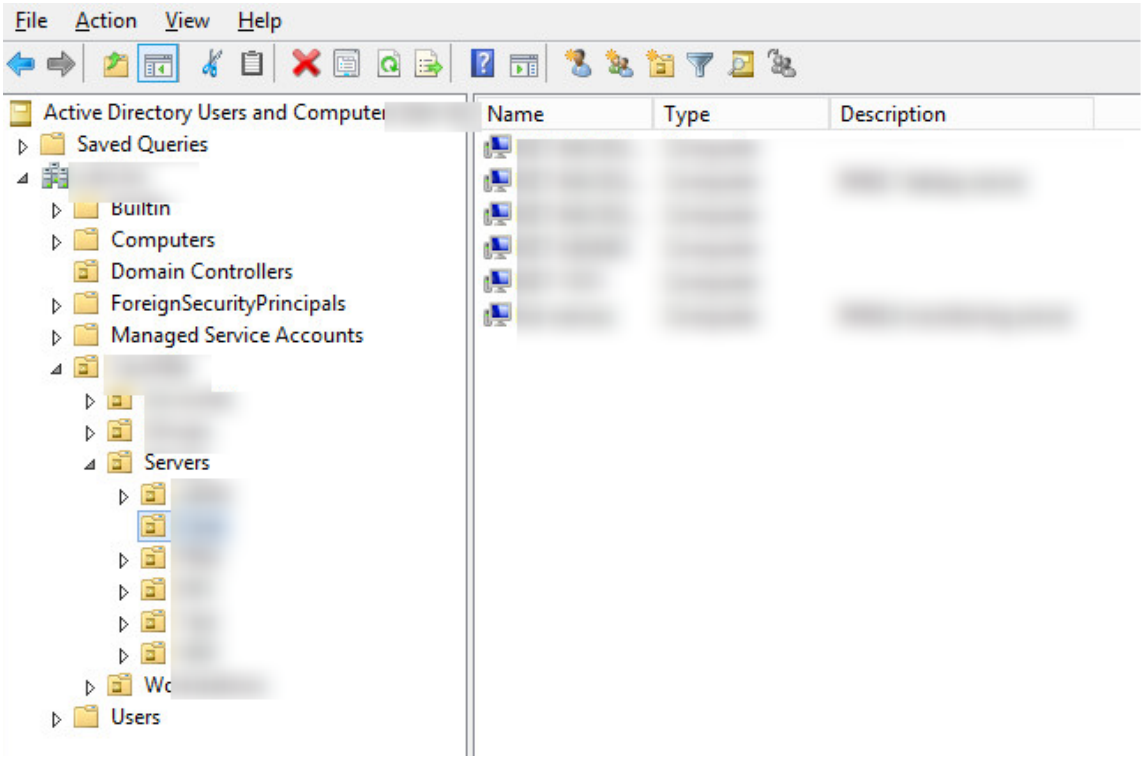
1. Запустите regedit.exe;
2. Перейдите в ветку **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters**
3. Измените значение параметра SysvolReady с 0 на **1**;



4. Потом перезапустите службу NetLogon: `net stop netlogon & net start netlogon`



Попробуйте открыть консоль ADUC еще раз. Вы должны увидеть структуру вашего домена.



Итак, вы успешно восстановили свой контроллер домен AD в режиме **Authoritative Restore.** Теперь все объекты в Active Directory будут автоматически реплицированы на другие контроллеры домена.

Восстановление отдельных объектов в Active Directory

Если вы случайно удалили какой-то объект в AD, не обязательно восстанавливать его из резервной копии. В Active Directory можно настроить корзину AD, из которой в течении 180 дней (значение по умолчанию для tombstoneLifetime) можно восстановить удаленный объект домена с помощью командлета `Restore-ADObject` или из оснастки Active Directory Administrative Center.

Если время захоронения уже просрочено, или ActiveDirectory RecycleBin не включена, вы можете восстановить отдельные объекты AD в режиме авторитетного восстановления. Для этого **в режиме DSRM** после восстановления DC из бэкапа нужно воспользоваться утилитой `ntdsutil` .

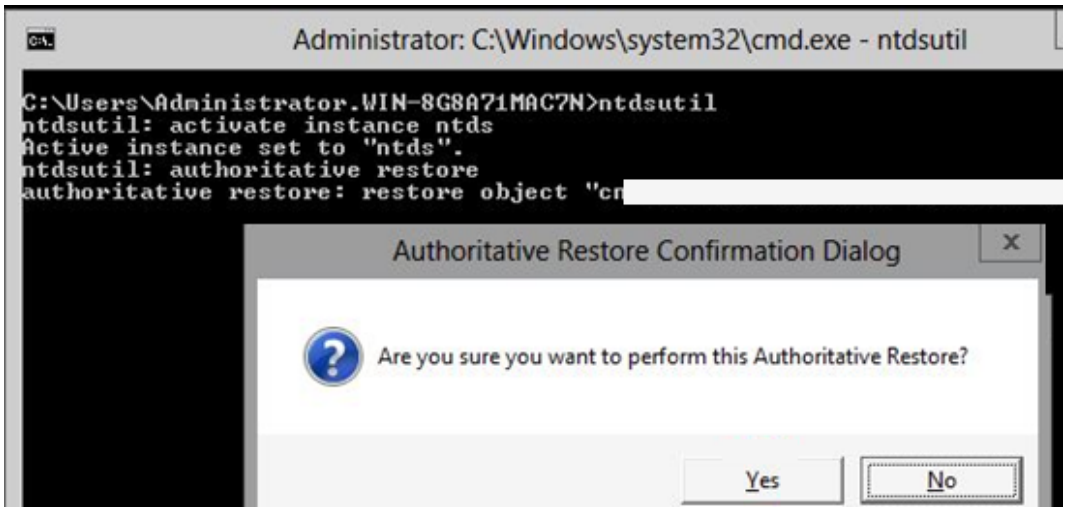
1. Выведите список доступных резервных копий: `wbadmin get versions`
2. Запустите восстановление выбранной резервной копии: `wbadmin start systemstaterecovery -version:[your_version]`
3. Подтвердите восстановление DC (в не-авторитативном режиме);
4. После перезагрузки запустите: `ntdsutil`
5. `activate instance ntds`
6. `authoritative restore`

Укажите полный путь к объекту, который нужно восстановить. Можно восстановить OU целиком:

```
restore subtree "OU=Users,DC=winitpro,DC=ru"
```

Или один объект:

```
restore object "cn=Test,OU=Users,DC=winitpro,DC=ru"
```



Данная команда запретит репликацию указанных объектов с других контроллеров домена и увеличит USN объекта на 100000.

Выйдите из ntdsutil: `quit`

Загрузите контроллер домена в обычном режиме и убедитесь, что удаленный объект AD был восстановлен.
