

Laboratorium – Uzupełnienie Teoretyczne

Klonowanie kontrolerów domeny (Virtualized Domain Controller Cloning)

1. Wprowadzenie

Klonowanie kontrolerów domeny (Virtualized DC Cloning) to mechanizm wprowadzony w Windows Server 2012, umożliwiający szybkie tworzenie nowych kontrolerów domeny w środowiskach wirtualnych. Technologia ta wykorzystuje funkcję VM-GenerationID hypervisora, dzięki czemu proces jest bezpieczny i chroni przed błędami replikacji (np. USN rollback).

2. Wymagania wstępne

- Hypervisor musi obsługiwać VM-GenerationID (Hyper-V 2012+, VMware vSphere 6+)
- Kontroler domeny musi działać na Windows Server 2012 lub nowszym
- Emulator PDC FSMO musi być dostępny i działać na Windows Server 2012+
- Konto użytkownika musi posiadać uprawnienia administratora domeny
- Należy sprawdzić listę aplikacji niekompatybilnych przed klonowaniem

3. Proces klonowania krok po kroku

Etap 1 – Przygotowanie źródłowego kontrolera domeny:

1. Dodaj DC do grupy Cloneable Domain Controllers:

```
Add-ADGroupMember -Identity 'Cloneable Domain Controllers' -Members '<NazwaKomputera$>'
```

2. Sprawdź aplikacje niezgodne:

```
Get-ADDCCloningExcludedApplicationList -GenerateXml
```

3. Wygeneruj plik DCCloneConfig.xml:

```
New-ADDCCloneConfigFile -Static -CloneComputerName 'DC-CLONE01' -IPv4Address '10.10.10.21' -IPv4SubnetMask '255.255.255.0' -IPv4DefaultGateway '10.10.10.1' -IPv4DNSResolver '10.10.10.10' -SiteName 'Default-First-Site-Name'
```

4. Wyłącz maszynę źródłową (Stop-Computer) i wykonaj jej eksport lub kopiowanie.

Etap 2 – Utworzenie klona na Hyper-V lub VMware:

- W Hyper-V użyj Import-VM z opcją -Copy -GenerateNewId
- W VMware utwórz nową maszynę z kopii, upewniając się, że VM-GenerationID zostanie zmieniony
- Nie wykonuj klonowania działającego DC (hot clone)!

Etap 3 – Pierwsze uruchomienie kłona:

Po uruchomieniu sklonowany DC wykryje zmianę VM-GenerationID i automatycznie skonfiguruje się na podstawie pliku DCCloneConfig.xml, po czym stanie się nowym kontrolerem domeny w domenie.

4. Typowe problemy i diagnostyka

- Brak pliku DCCloneConfig.xml lub błędny plik → klon uruchomi się w DSRM
- VM-GenerationID nie zmienił się → brak klonowania, ryzyko błędów replikacji
- Brak PDC online → New-ADDCCloneConfigFile zakończy się błędem

5. Dobre praktyki

- Klonuj tylko wyłączone DC
- Używaj czystych DC z minimalną ilością aplikacji
- Testuj procedurę w środowisku laboratoryjnym
- Po zakończeniu usuń plik DCCloneConfig.xml z katalogu NTDS

6. Przykładowe polecenia PowerShell

```
Add-ADGroupMember -Identity 'Cloneable Domain Controllers' -Members 'DC1$'  
Get-ADDCCloneConfigExcludedApplicationList -GenerateXml  
New-ADDCCloneConfigFile -Static -CloneComputerName 'DC-CLONE01' -IPv4Address  
'10.10.10.21' -IPv4SubnetMask '255.255.255.0' -IPv4DefaultGateway '10.10.10.1' -  
IPv4DNSResolver '10.10.10.10' -SiteName 'SiteA'  
Stop-Computer  
Import-VM -Path 'C:\Export\DC01' -Copy -GenerateNewId
```

7. Źródła i dokumentacja

- Microsoft Docs: Virtualized Domain Controller Deployment and Configuration
- Microsoft Docs: New-ADDCCloneConfigFile
- VMware Docs: Virtualizing Active Directory Domain Services on vSphere