Restore AD replication after time jumps and fast

Ing. Ondřej Ševeček | GOPAS a.s. |

MCSM:Directory2012 | MCM:Directory2008 | MVP:Enterprise Security | CEH: Certified Ethical Hacker | CHFI: Computer Hacking Forensic Investigator |

ondrej@sevecek.com | www.sevecek.com |

Motivation

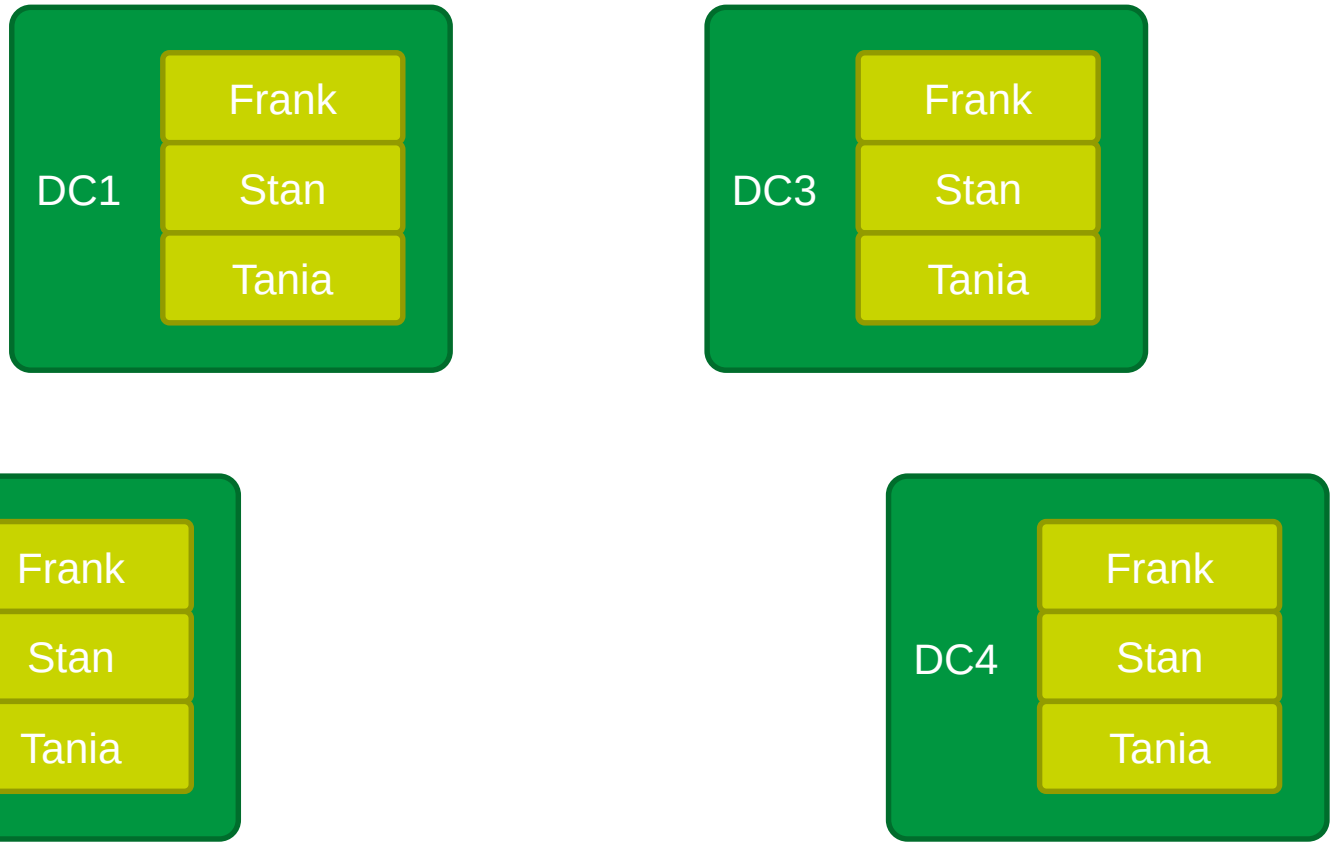
- Hardware does not always maintain its time well
- A single hardware-based DC may go out of sync
- Many virtualized DCs on a cloud may go out of sync simultaneously

- My own experience is 5 clouds in past 2 years

What happens

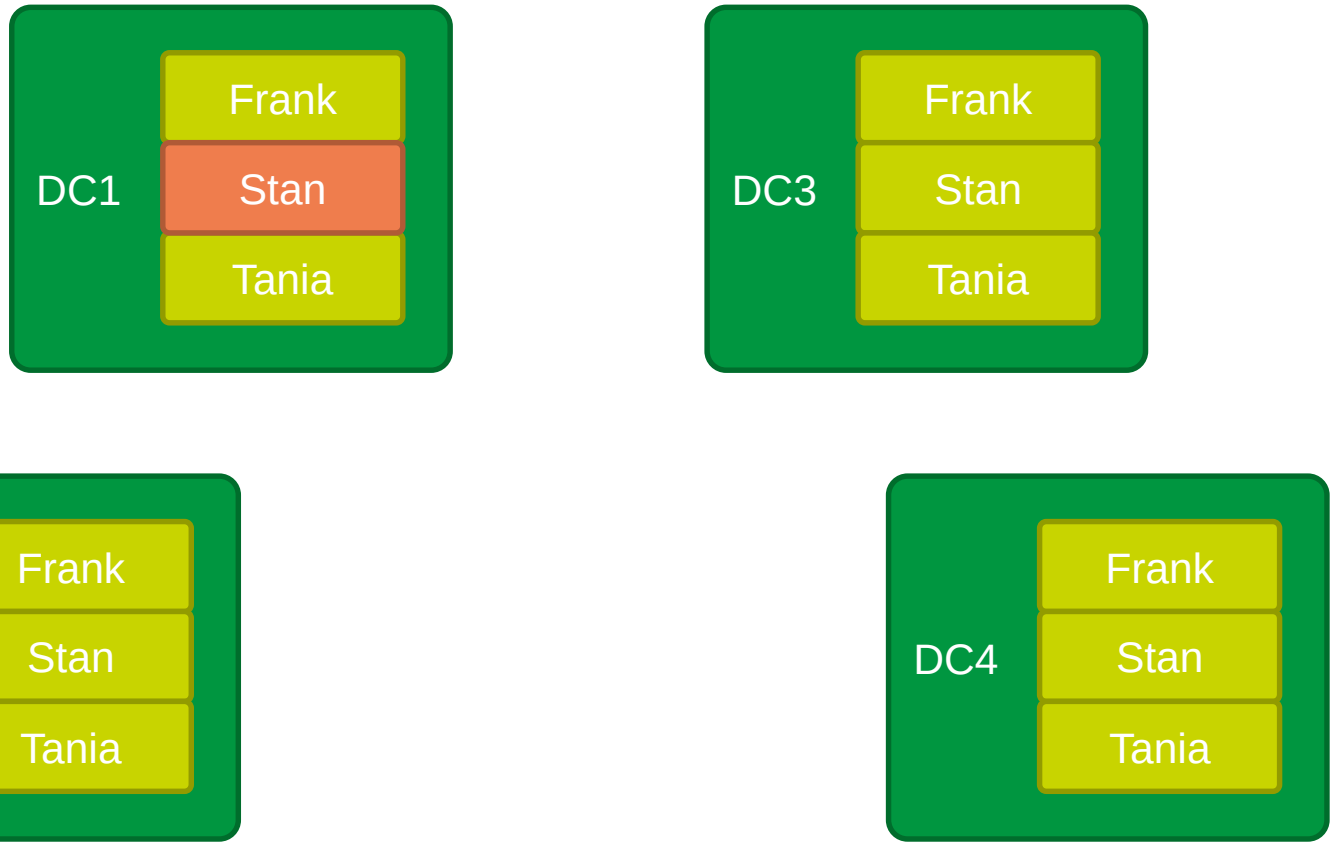
- Going over 60 days means DC account passwords are out of sync
  - Kerberos failures, NTLM works fine
  - reset passwords
- Going over 180 days (or tombstone lifetime)
  - remove lingering objects
  - restore replication

Normal AD deletion process: objects and tombstones

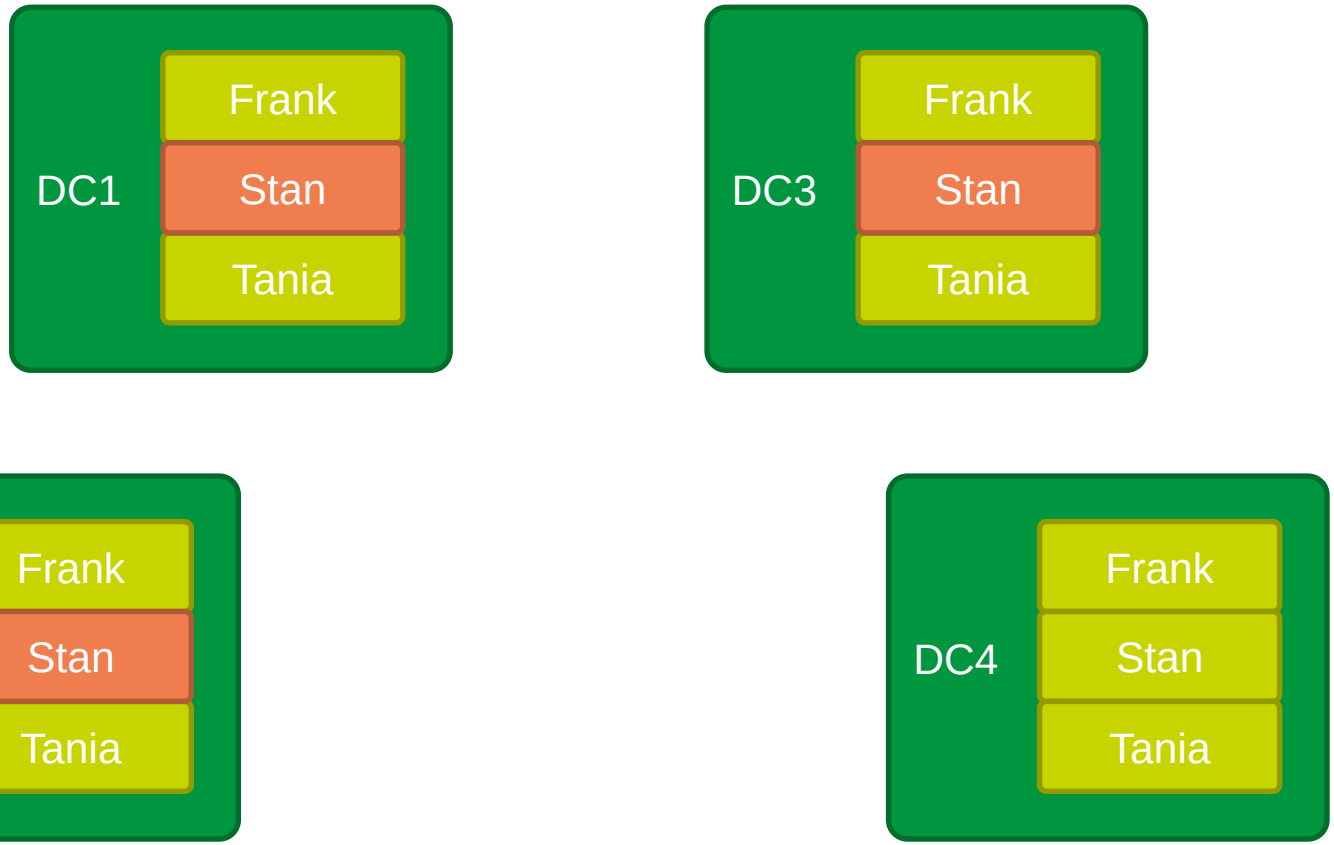


GOPAS

Normal AD deletion process: objects and tombstones

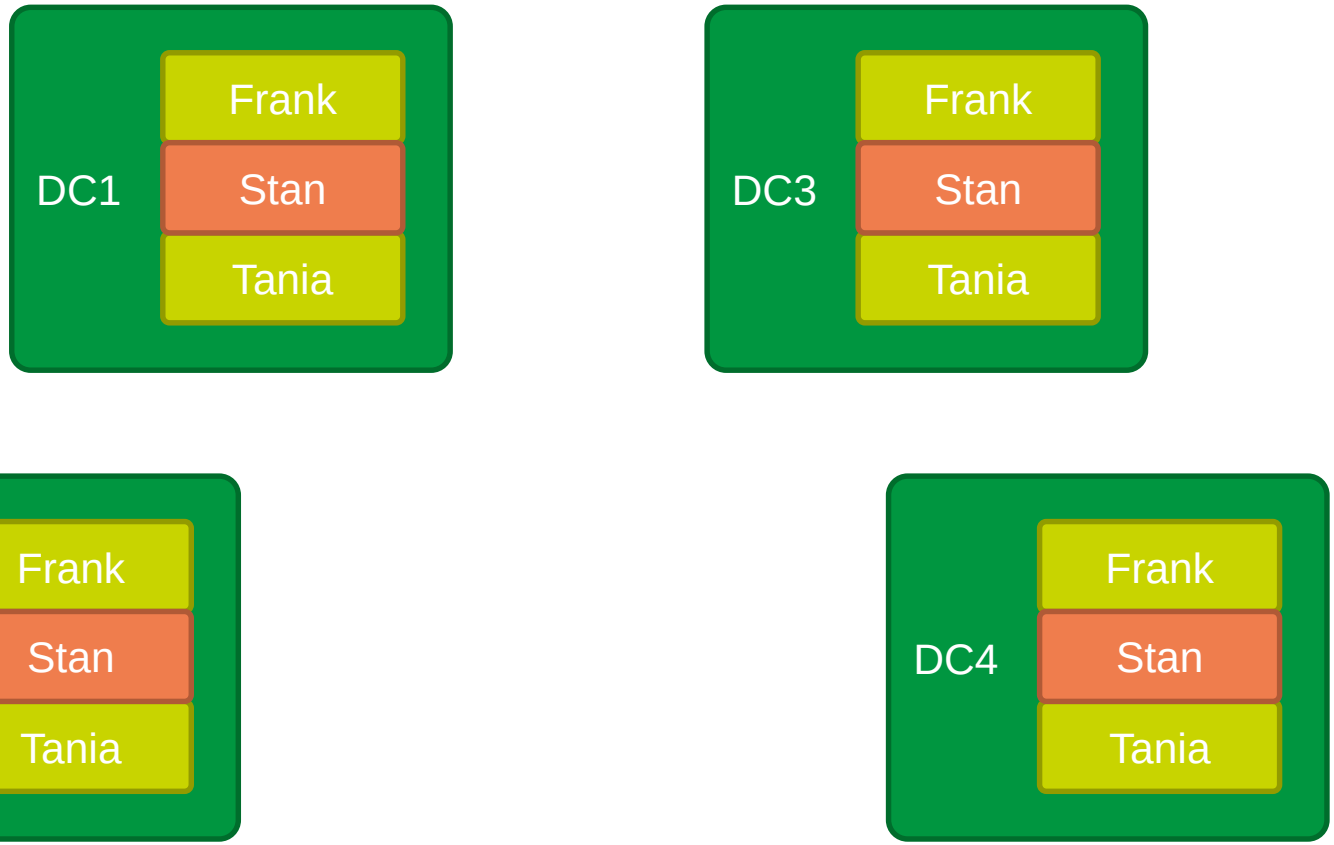


Normal AD deletion process: objects and tombstones



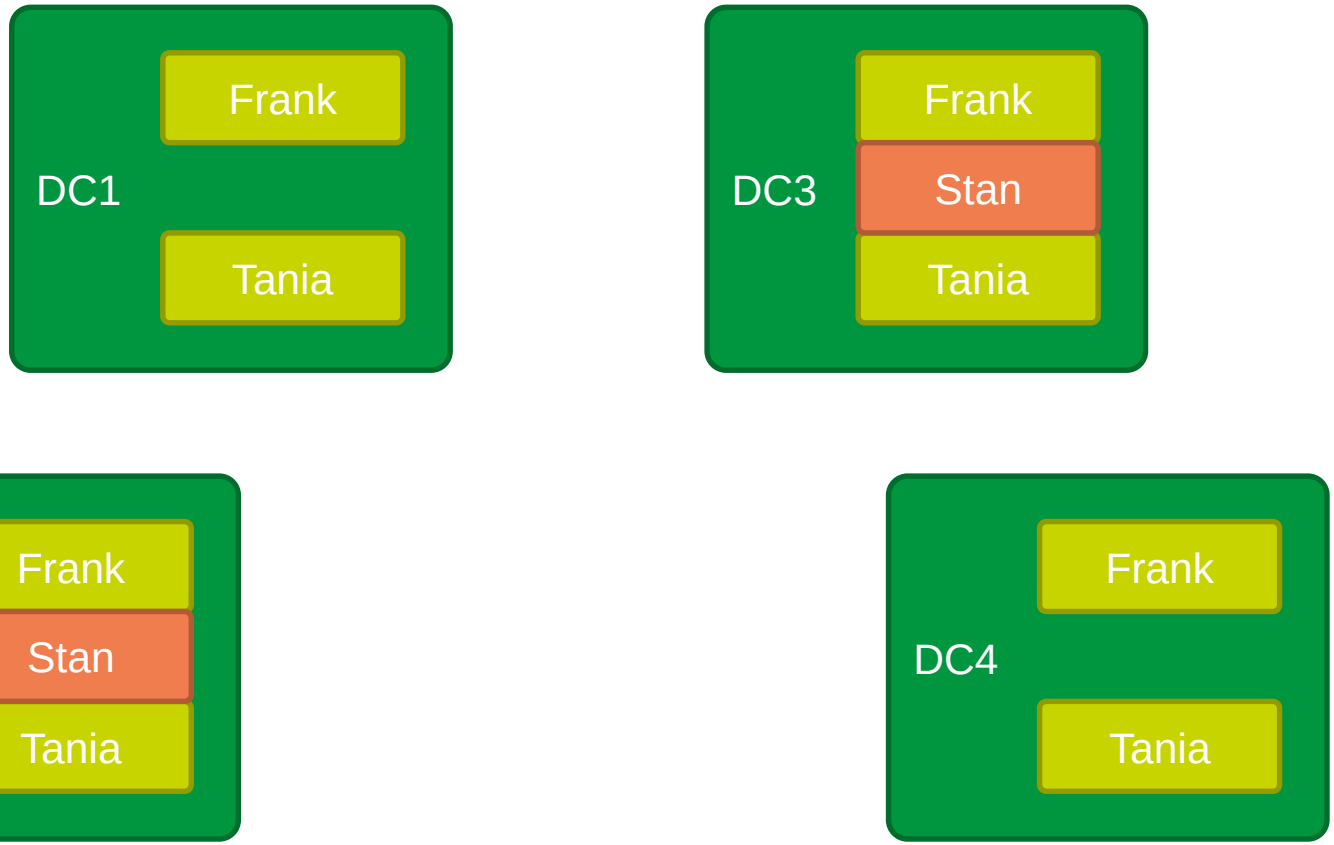
GOPAS

Normal AD deletion process: objects and tombstones

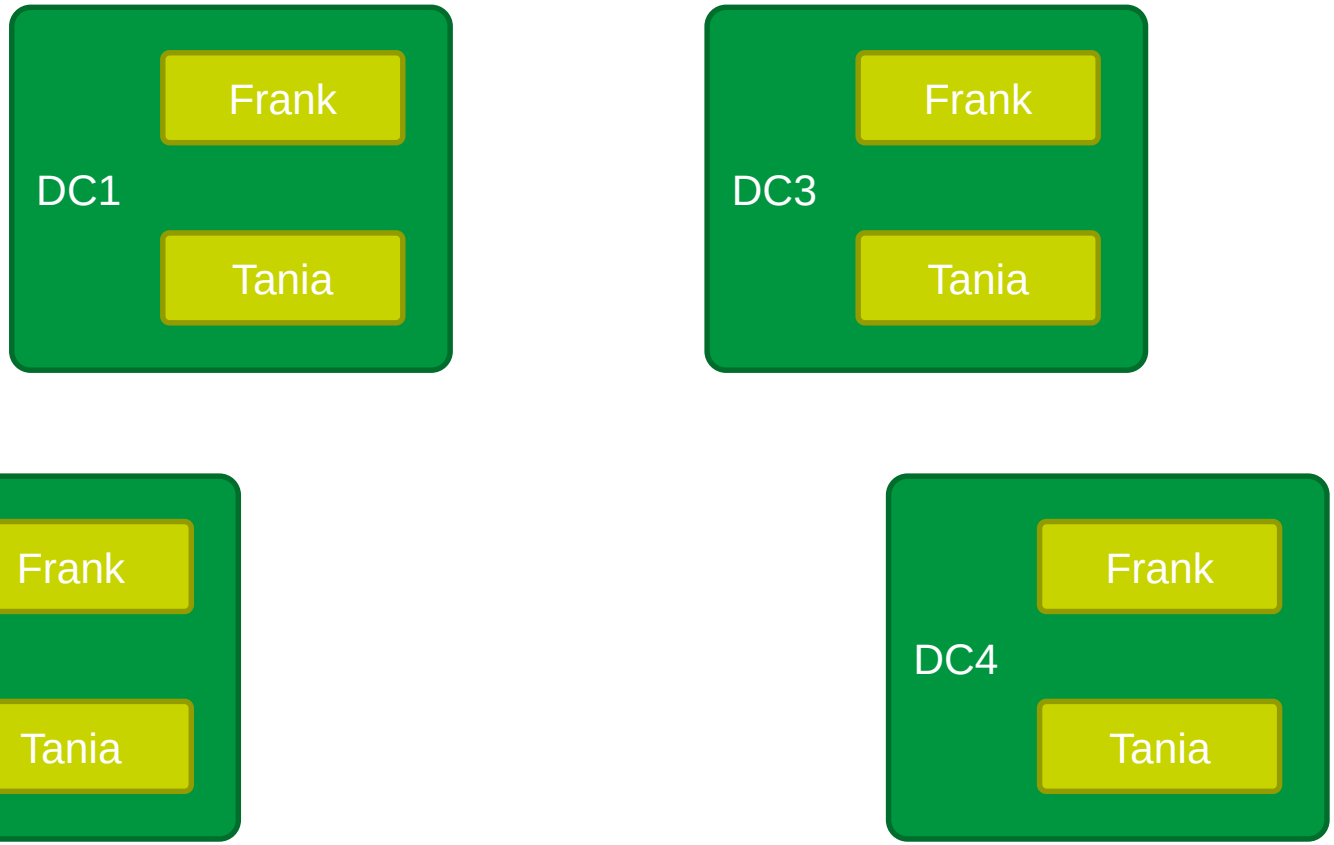


GOPAS

Normal AD deletion process: garbage collection 1/day

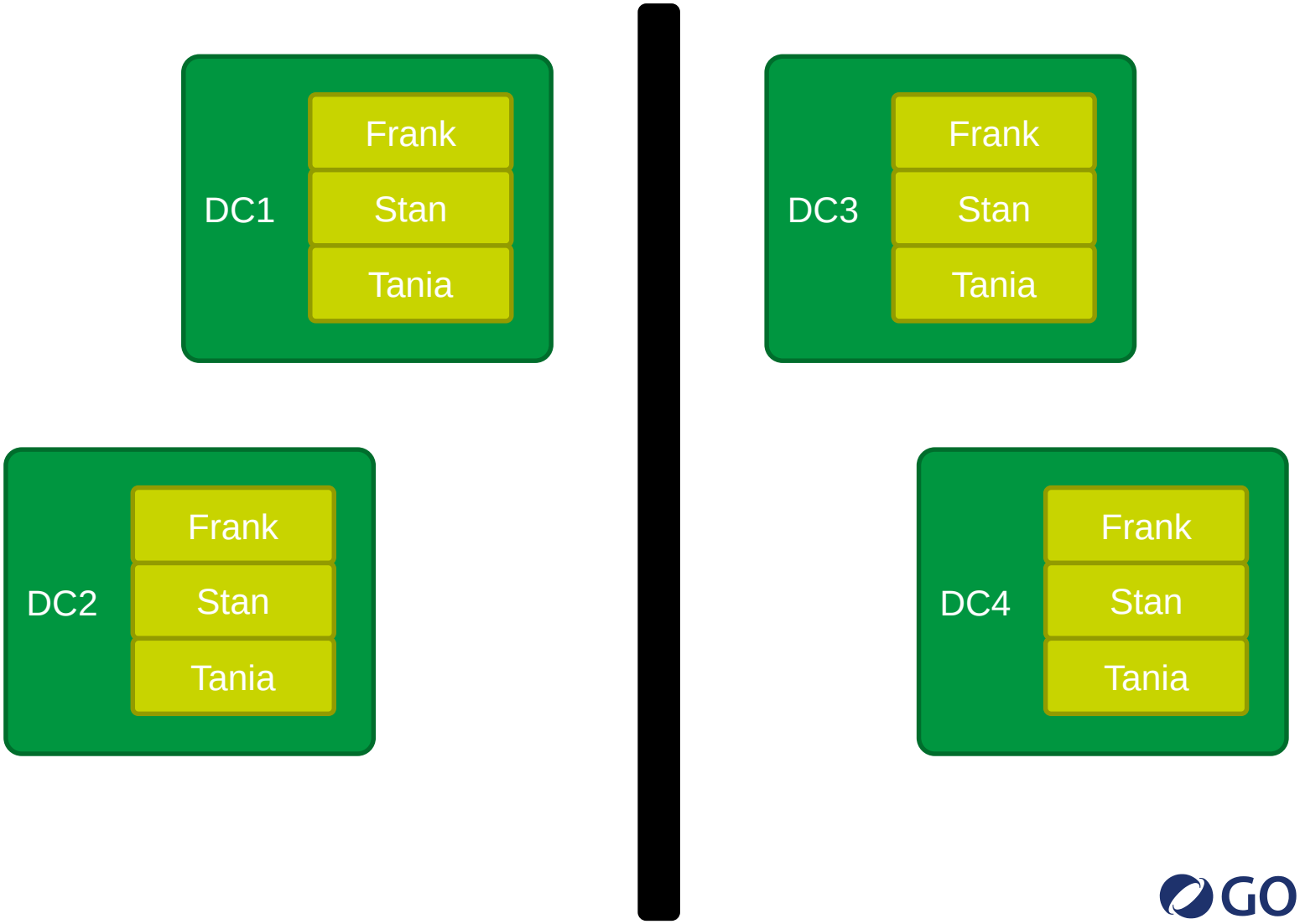


Normal AD deletion process: garbage collection 1/day



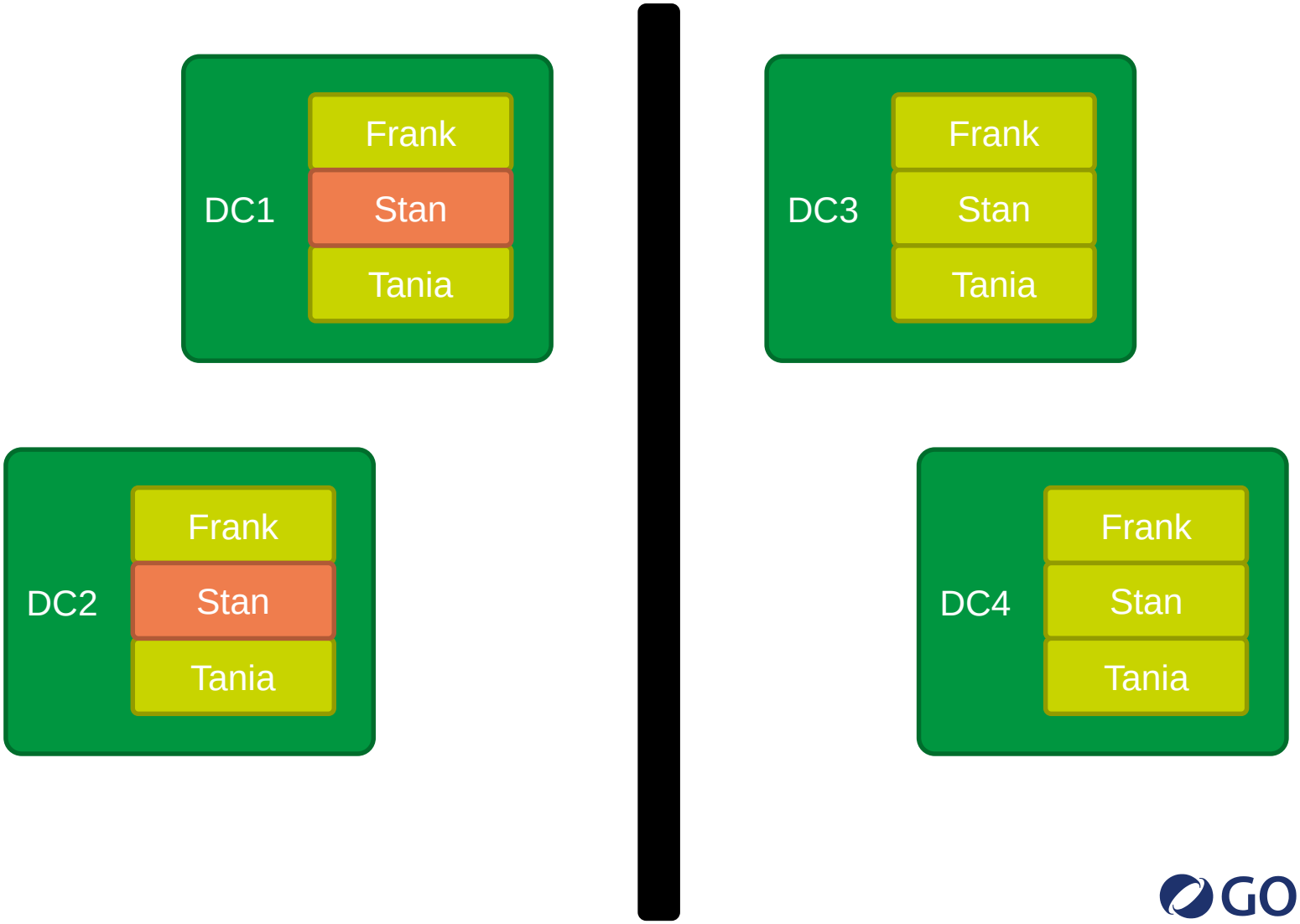
GOPAS

Lingering objects: how they arise

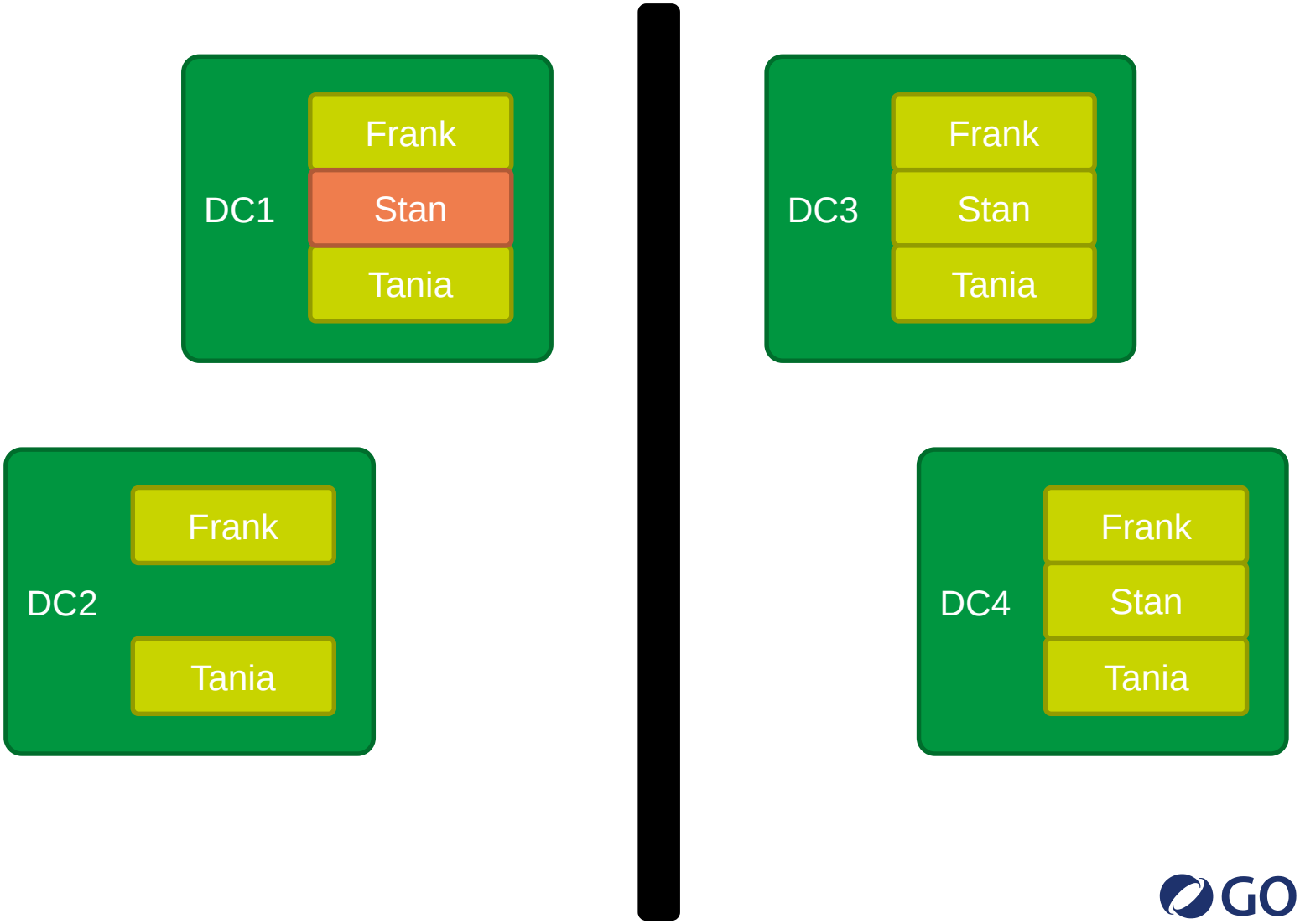


GOPAS

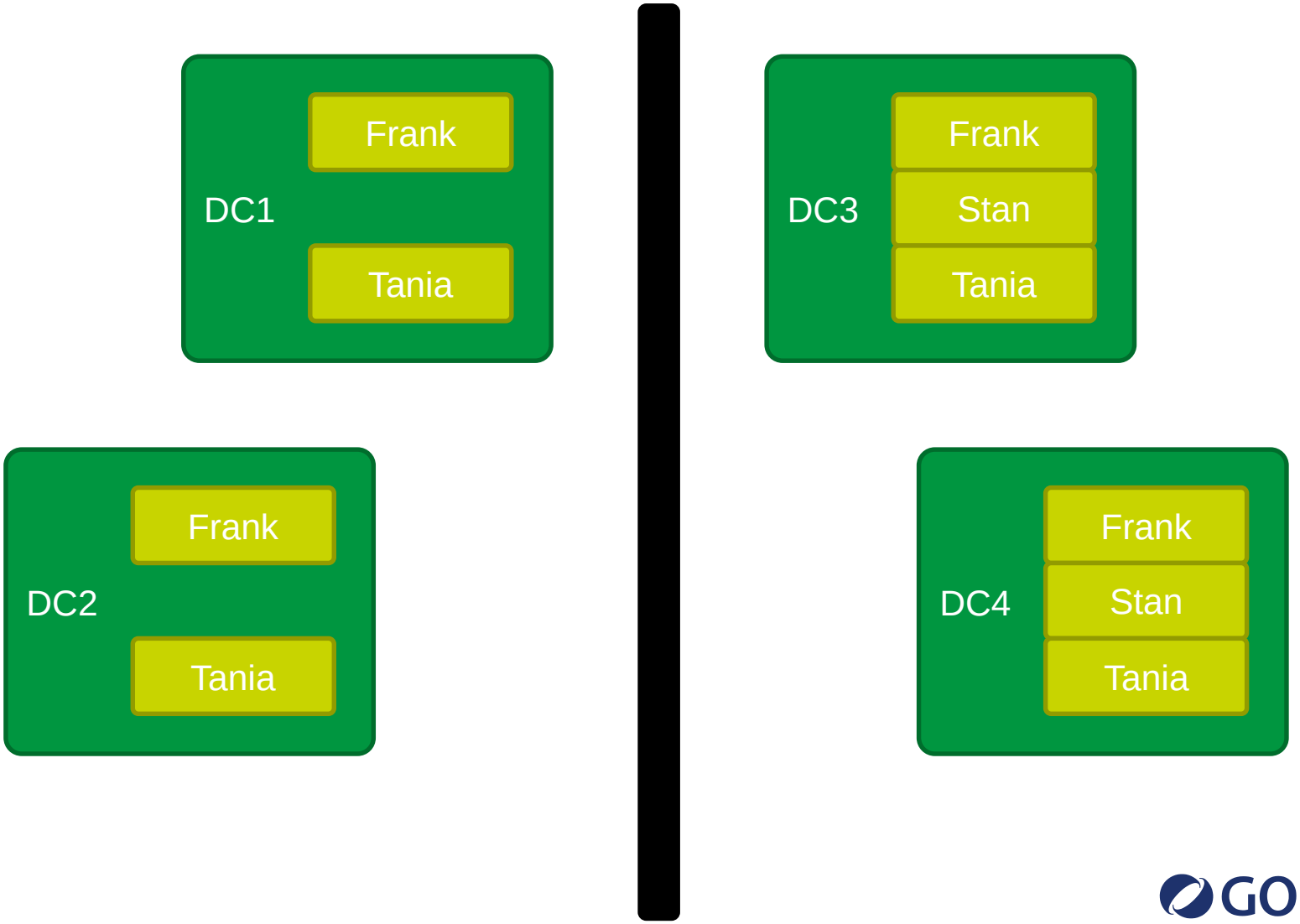
Lingering objects: how they arise



Lingering objects: how they arise after garbage collection

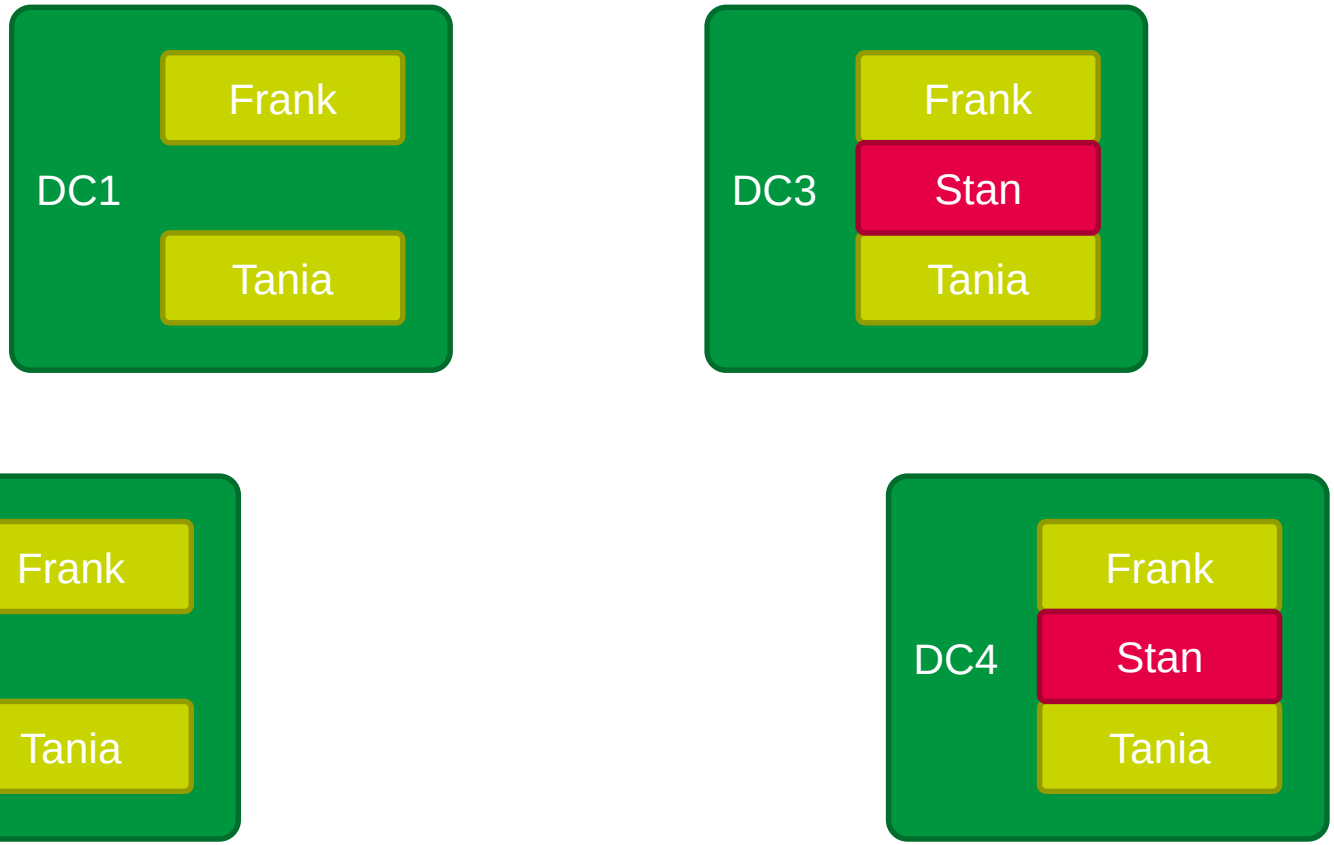


Lingering objects: how they arise after garbage collection



GOPAS

Lingering objects: what would happen after tombstone lifetime



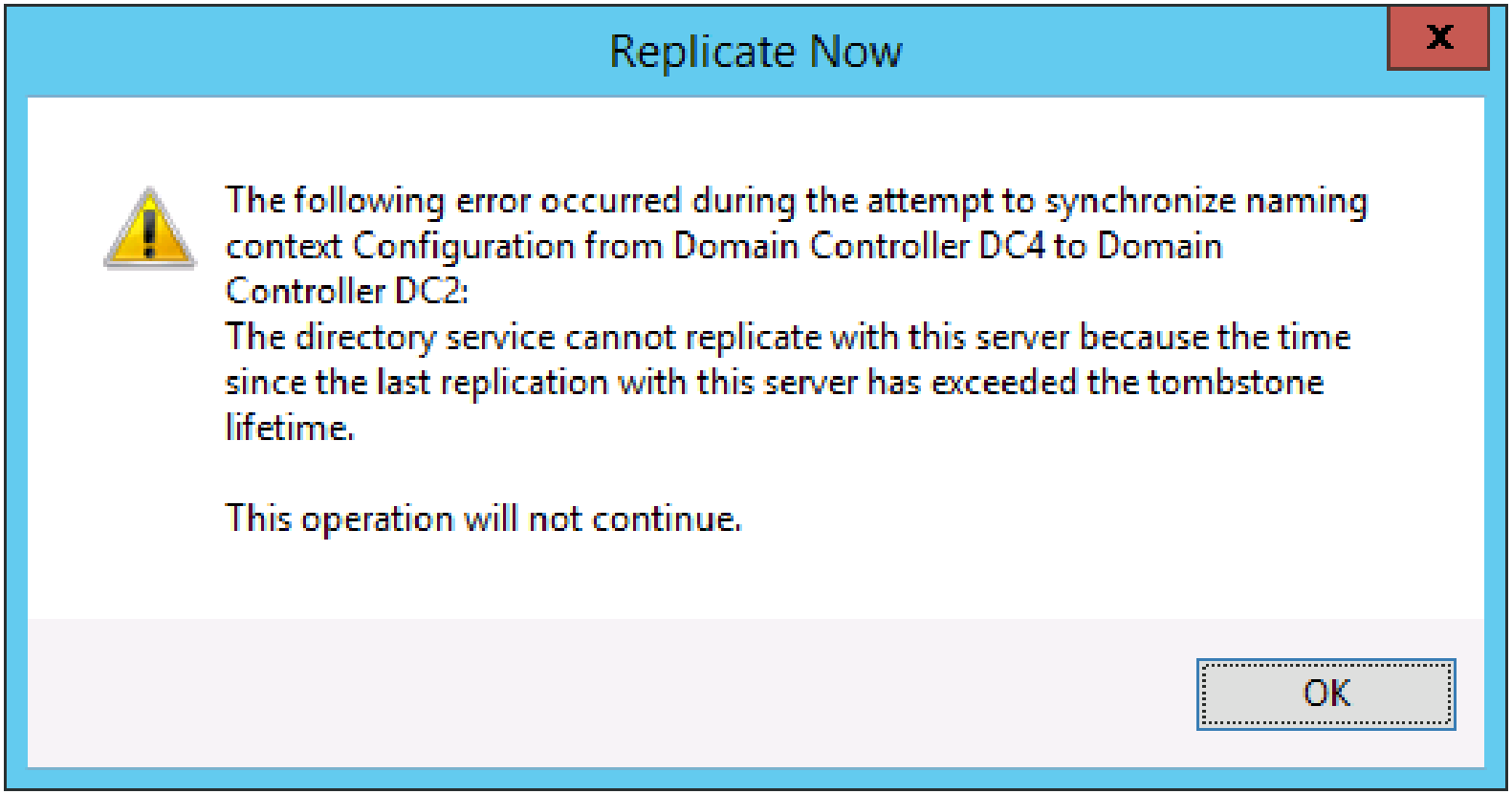
Symptoms

How to restore AD replication after a time jump as fast as possible

GOPAS

Tombstone lifetime exceeded

- The directory service cannot replicate with this server because the time since the last replication with this server has exceeded the tombstone lifetime

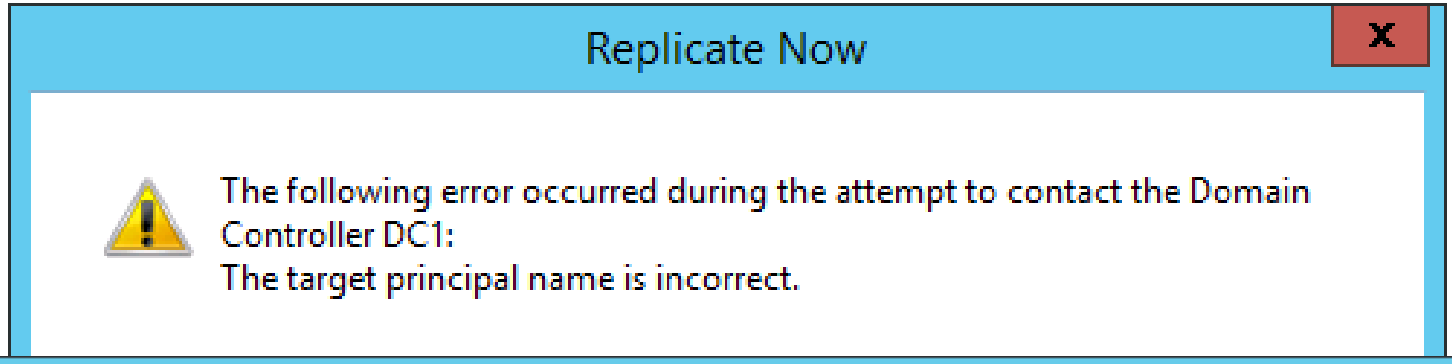


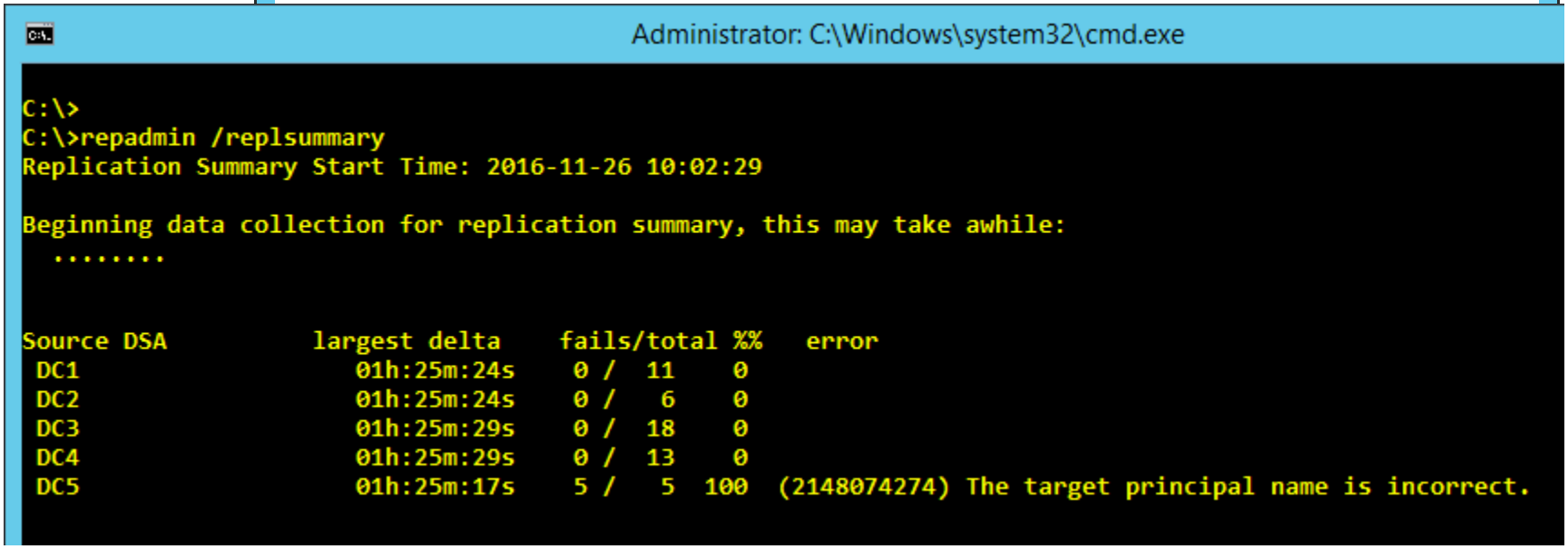
Tombstone lifetime exceeded (Event Id 2042)

- It has been too long since this machine last replicated with the named source machine. The time between replications with this source has exceeded the tombstone lifetime.

DC account passwords out of sync

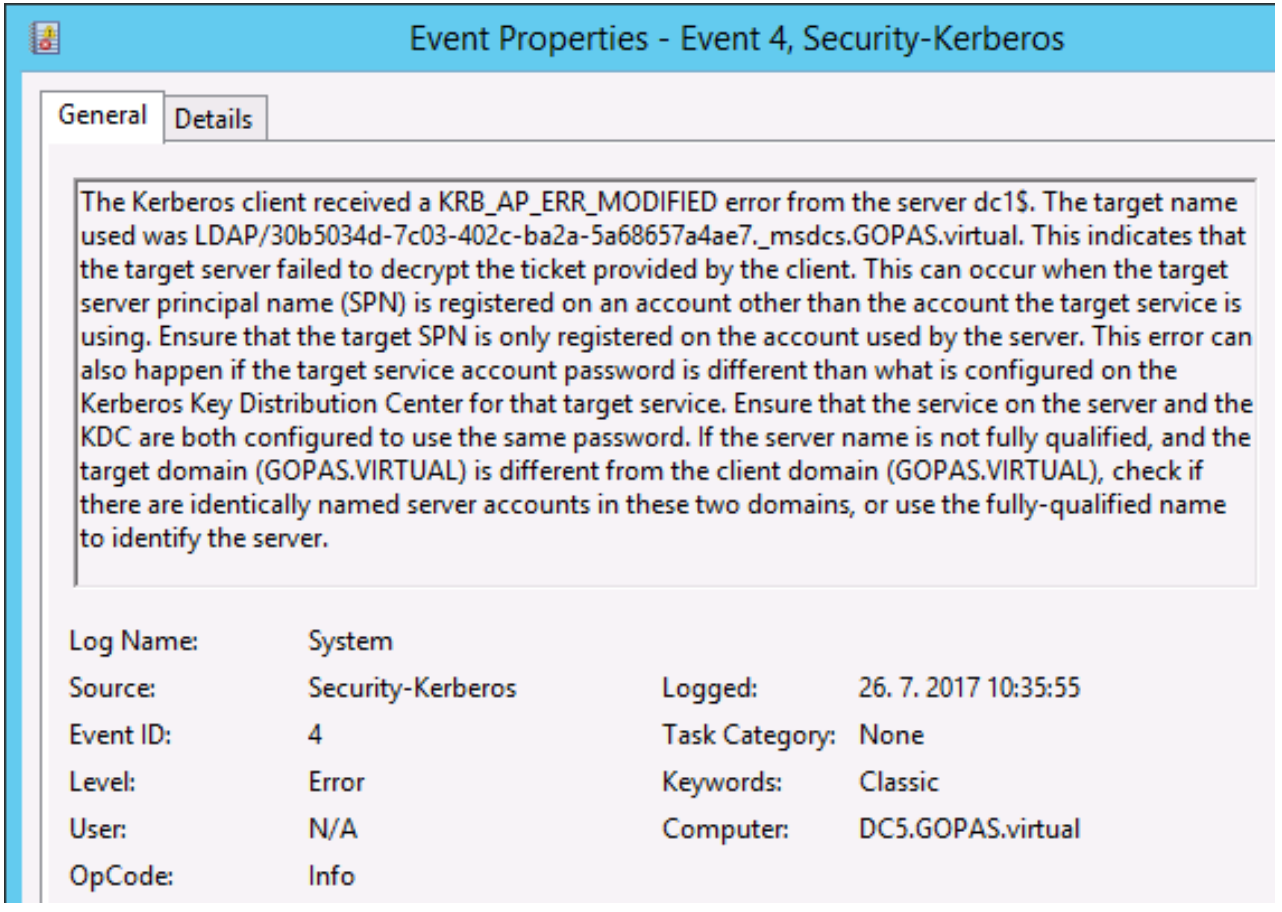
- Kerberos error: The target principal name is incorrect
- error: 2148074274 = 0x80090322 = SEC_E_WRONG_PRINCIPAL





DC account password out of sync (Event Id 4)

- The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server. The target name used was LDAP/._msdcs. This indicates that the target server failed to decrypt the ticket provided by the client.



Repair notes

How to restore AD replication after a time jump as fast as possible

GOPAS

Reparation process

- Correct the clock first!
- Reset DC machine account passwords
  - netdom resetpwd
- Remove lingering objects
- Enable replication and replicate
  - Allow Replication with Divergent and Corrupt Partner = 1
- Return the registry value back to default value
  - Allow Replication with Divergent and Corrupt Partner = 0

Blockers

- AD cannot replicate
- Many DNS servers on different DCs cause deadlocks
  - AD requires DNS
  - DNS requires AD

Do not!

- Do not restart any DC
  - or you will wait ages
- Do not restart any DC
  - if it is not GC, you may not log on again
- Do not demote any DC
  - you may have a lot of changes not yet replicated out
  - such as user/computer passwords

Phase 0

Correct the clock!

How to restore AD replication after a time jump as fast as possible

GOPAS

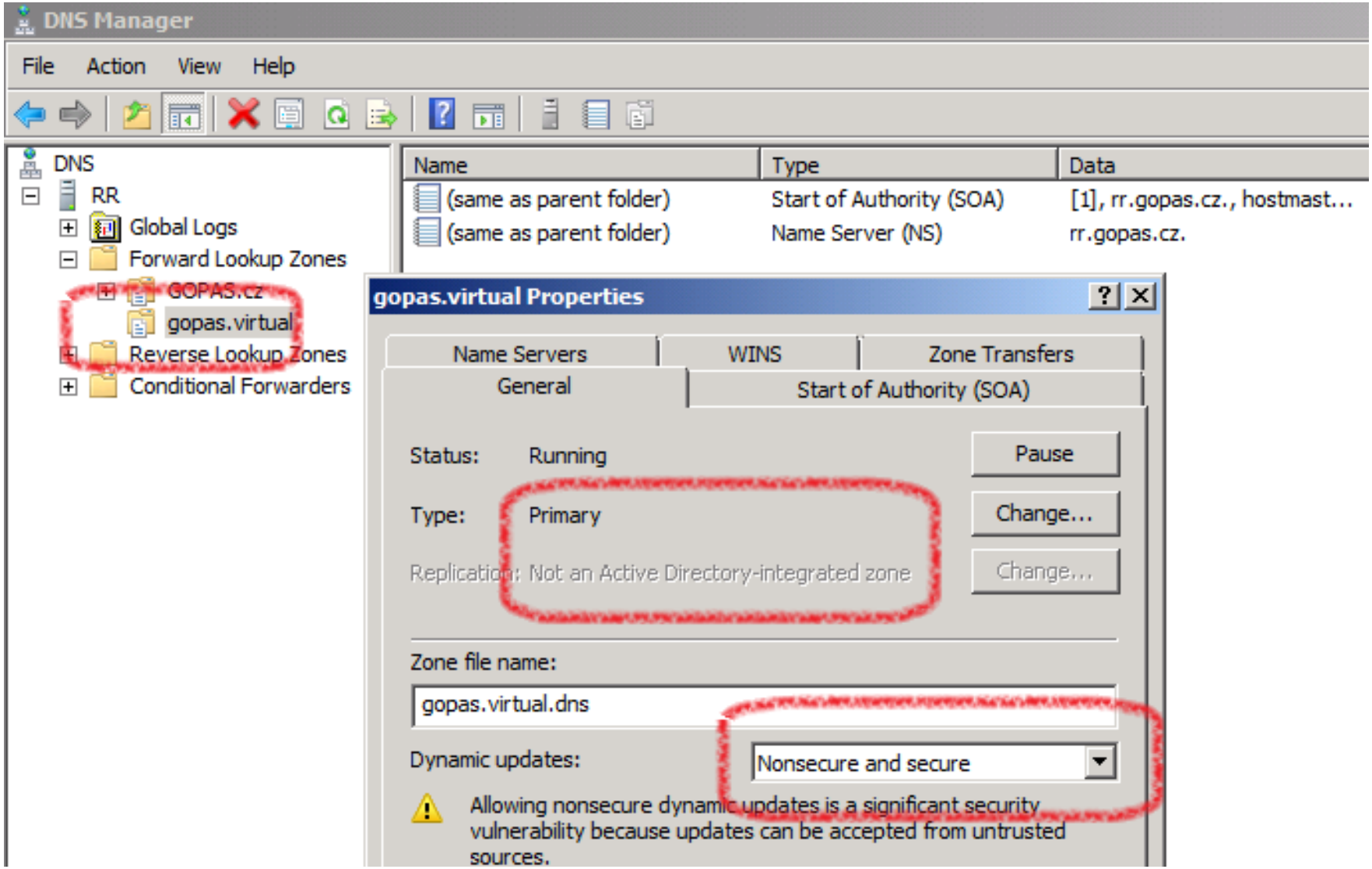
Phase 1

Prepare and populate a recovery DNS server

How to restore AD replication after a time jump as fast as possible

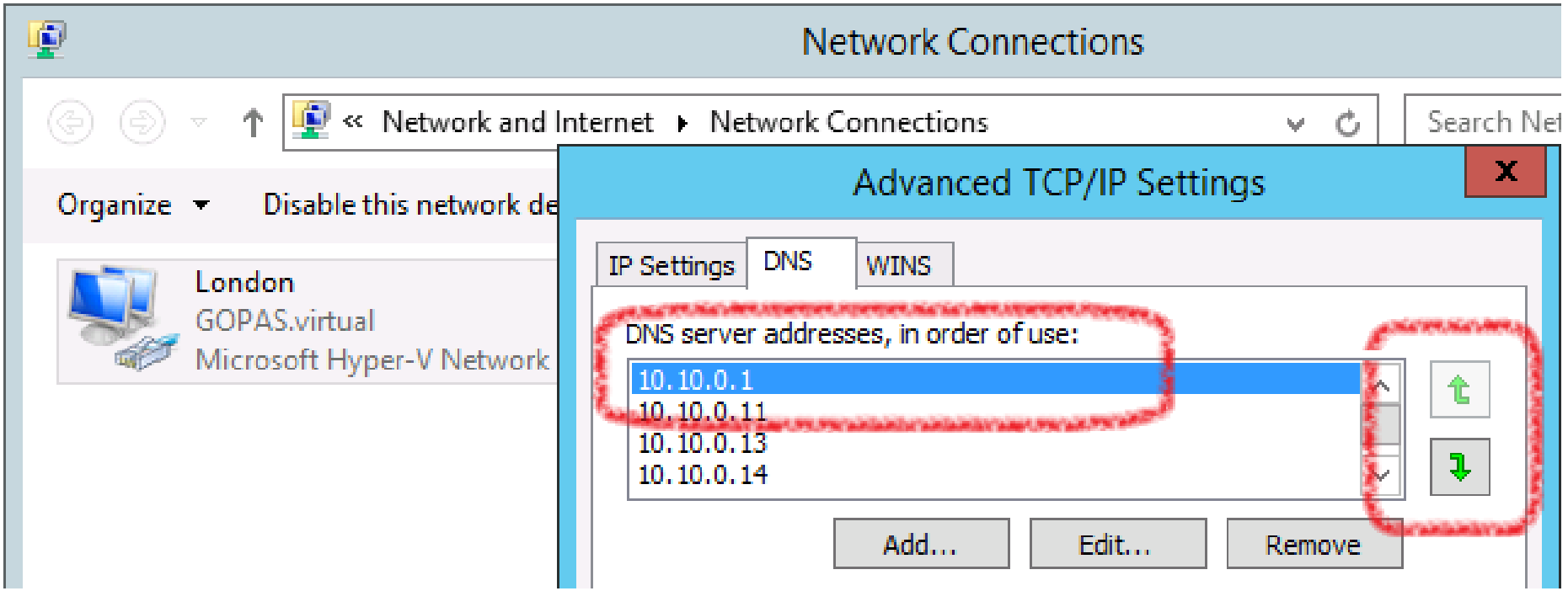
GOPAS

Step 1: Create a temporary single separate non-DC DNS server with dynamic updates enabled



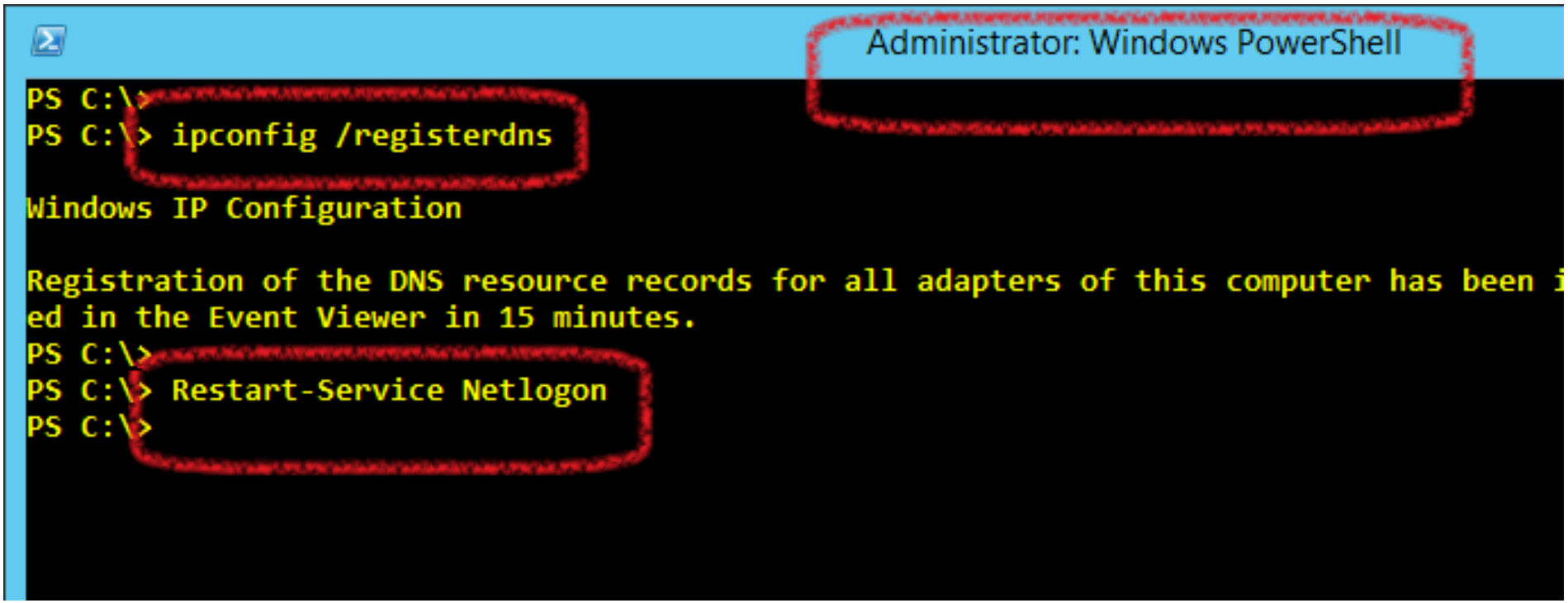
Step 2: reconfigure all the DCs to use the temporary DNS server as resolver and to update their DC locator DNS records

- Just make it the first in the list
- Do not need to remove the others
- Leave local AD DNS servers running for clients

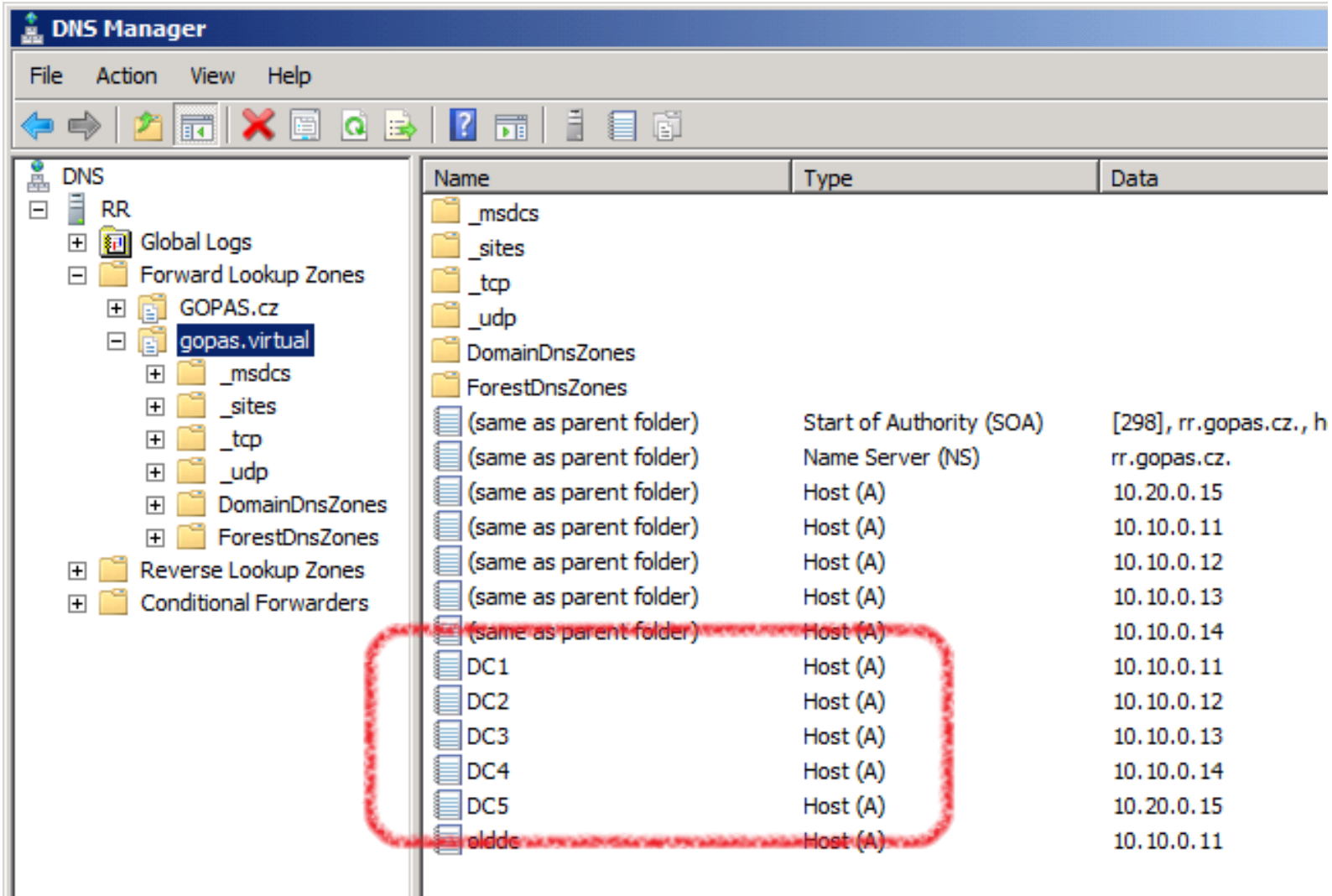


Step 3: force dynamic DNS registration and Netlogon DC locator DNS record re-registration on all DCs

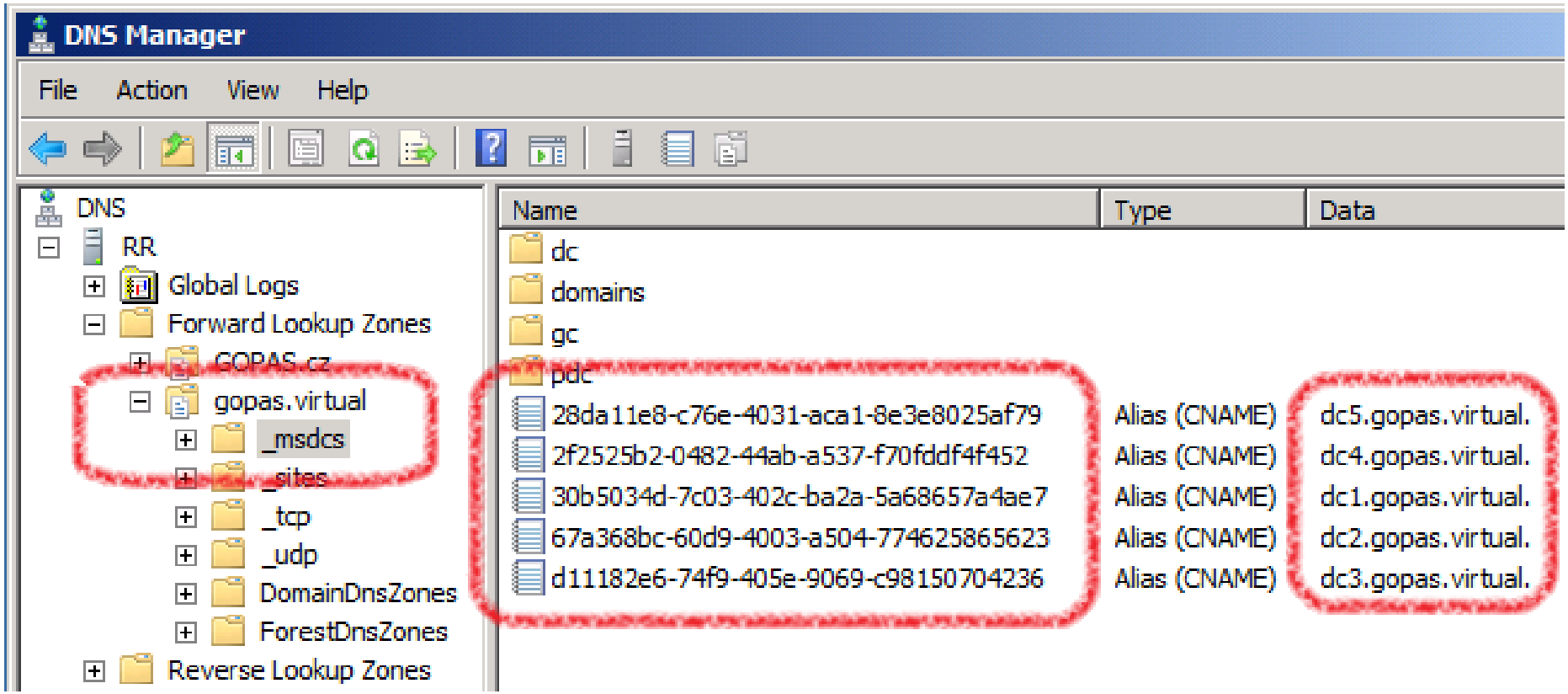
```
ipconfig /registerdns
Restart-Service Netlogon
```



Step 4: verify that DNS A records have been updated well in the recovery DNS server



Step 5: verify that the DC locator DNS records necessary for replication have been updated well in the _msdcs zone of recovery DNS server



GOPAS

Phase 2

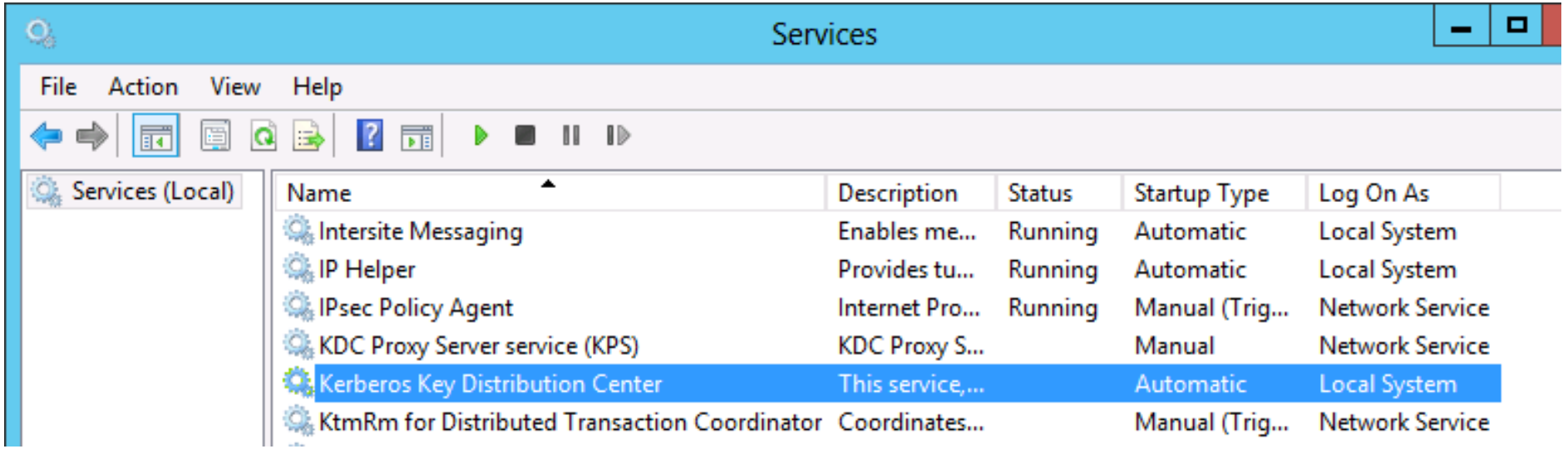
Stop all KDCs except for one "recovery KDC"

How to restore AD replication after a time jump as fast as possible

GOPAS

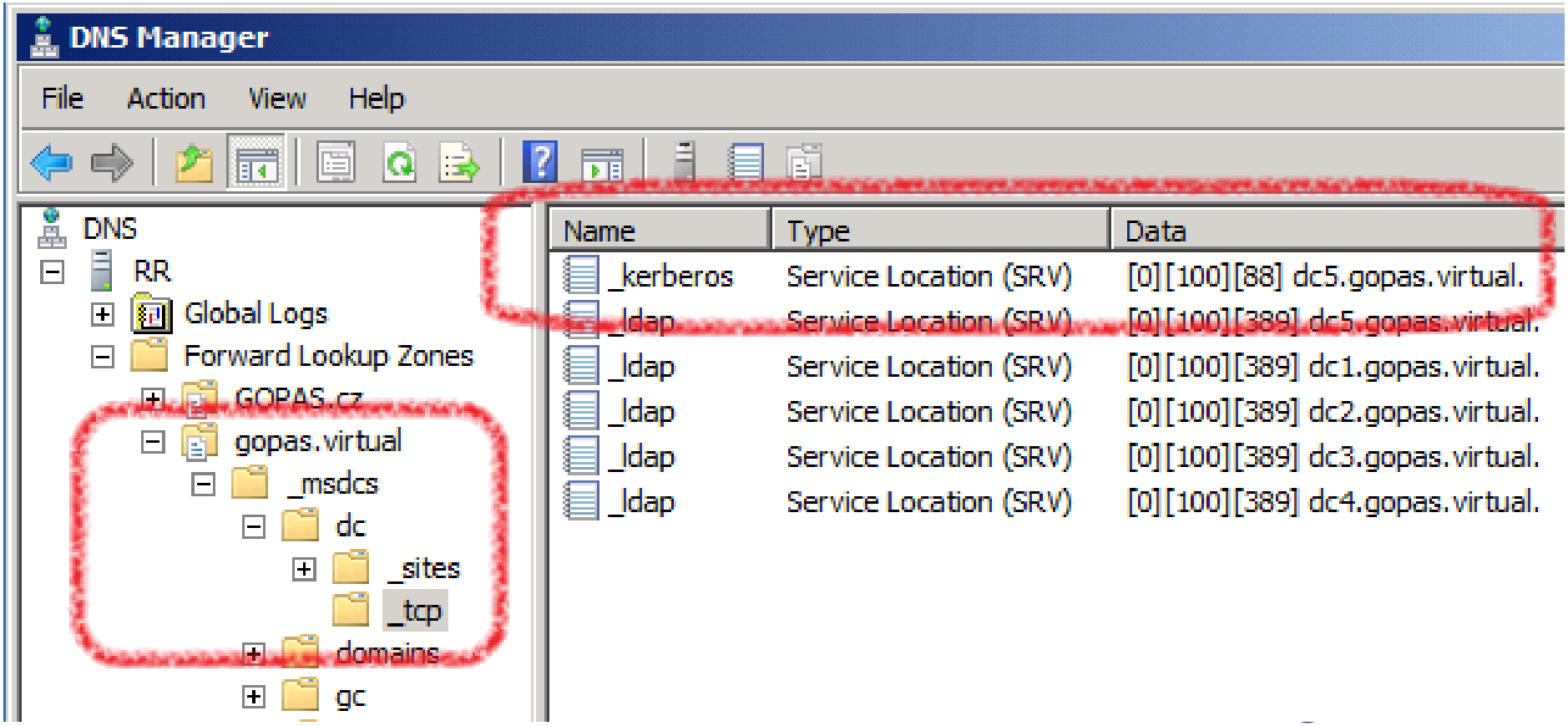
Step 6: select a single DC as recovery KDC and stop KDC services on all other DCs

```
Stop-Service KDC
```



GOPAS

Step 7: verify that the DC locator DNS records of _kerberos._tcp.dc._msdcs used by KDC service disappeared from zone of the recovery DNS server



Phase 3

Reset all DC machine passwords against the "recovery KDC"

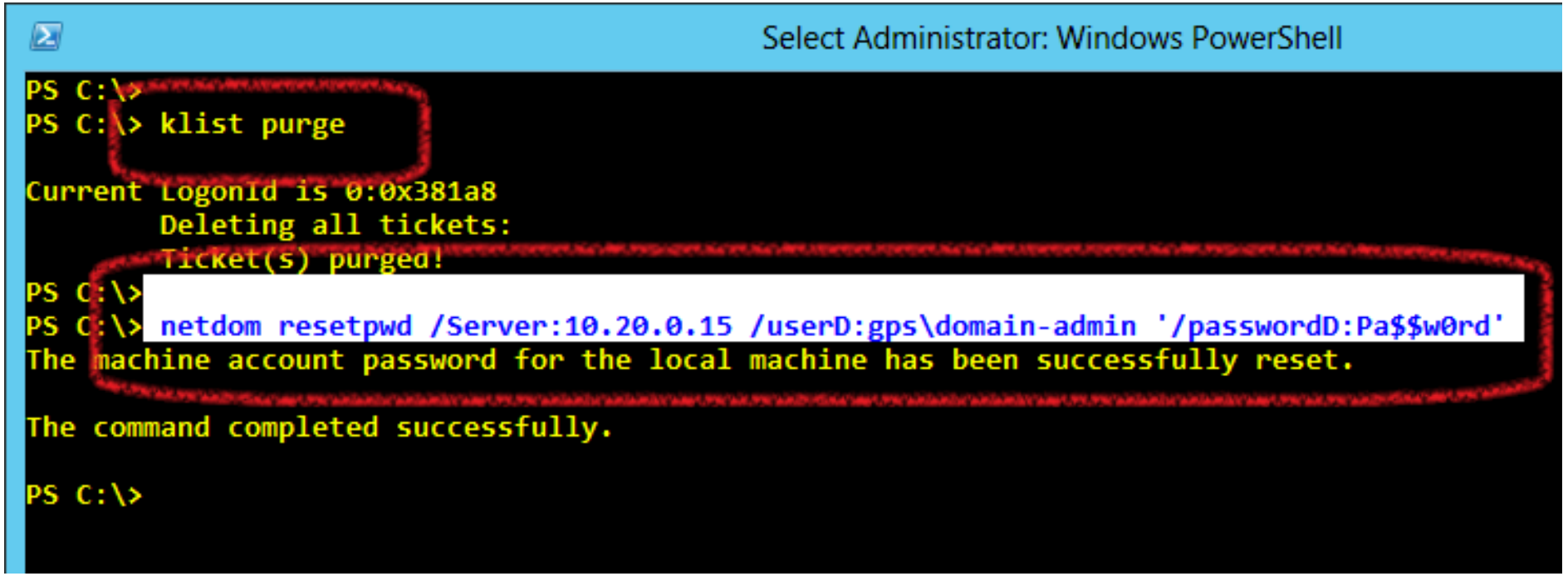
How to restore AD replication after a time jump as fast as possible

GOPAS

Step 8: reset local machine account passwords on all DCs against the IP address of the recovery KDC (using NTLM instead of Kerberos)

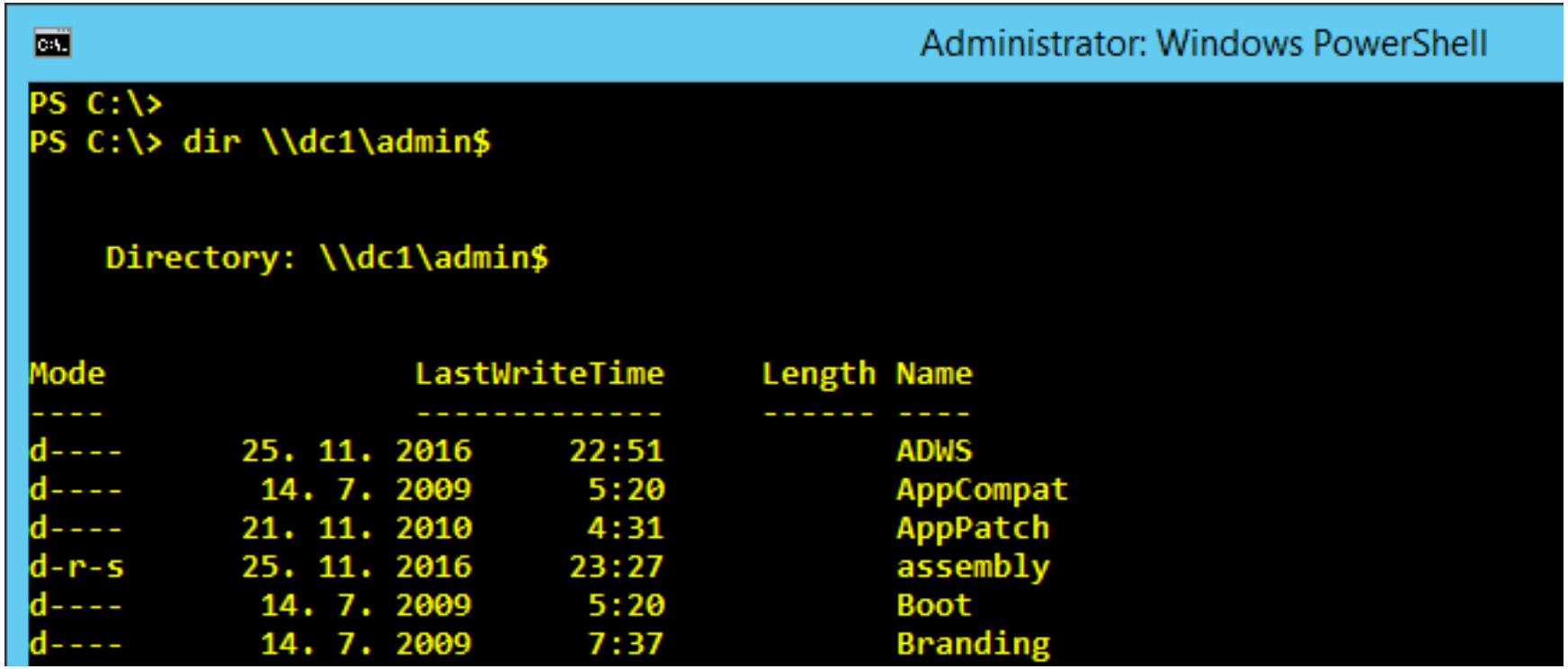
```
klist purge
netdom RESETPWD /Server:10.20.0.15 /userD:gps\domain-admin
'/passwordD:Pa$$w0rd'

# Note: in PowerShell use apostrophes to enclose any special characters
```



Step 9: verify that the Kerberos authentication works again

```
dir \\dc1\admin$
gwmi Win32_OperatingSystem -Computer dc2
```



Phase 4

Verify and remove all lingering objects from all partitions

How to restore AD replication after a time jump as fast as possible

GOPAS

Step 10: run repadmin /removelingeringobjects among every two DCs and for every directory partition

```
[string[]] $dcNames = dsquery server -forest -o rdn | % { $_.Trim('"') }

[string[]] $dcGuids = dsquery server -forest | % { dsquery * $_ -filter
"(objectClass=nTDSDSA)" -attr objectGUID -l } | % { $_.Trim('{}') }

[string[]] $partitions = dsquery partition | % { $_.Trim('"') }

foreach ($onePartition in $partitions) {

  for ($iDC = 0; $iDC -lt $dcNames.Length; $iDC ++) {

    for ($iGuid = 0; $iGuid -lt $dcGuids.Length; $iGuid ++) {

      if ($iDC -ne $iGuid) {

        Write-Host ('{0} : {1} : {2}' -f $dcNames[$iDC], $dcGuids[$iGuid], $onePartition)
        # Note: ignore the failures if the partition is not hosted on the target DC
        repadmin /removelingeringobjects $dcNames[$iDC] $dcGuids[$iGuid] $onePartition
      }
} } }
```

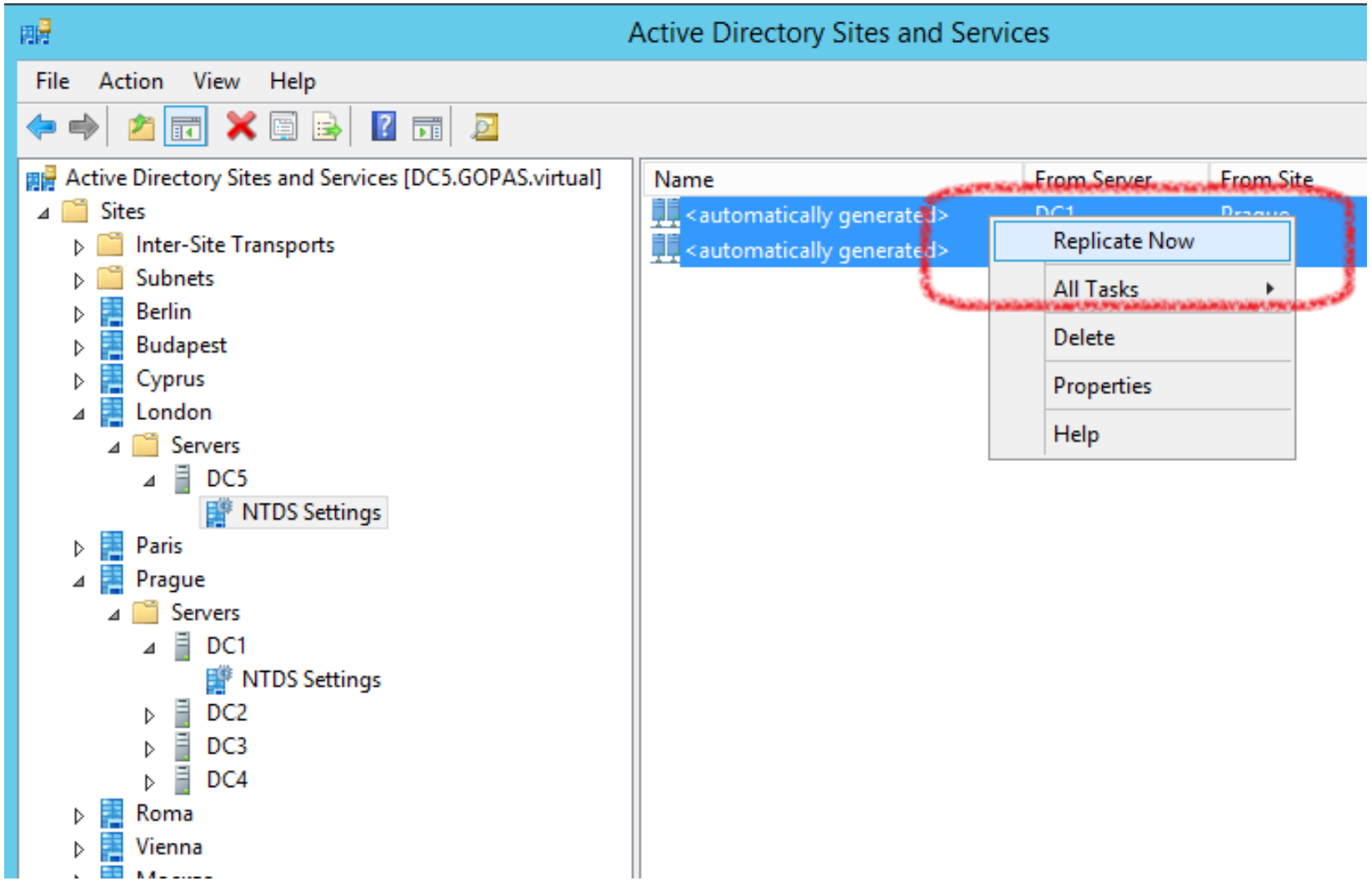
GOPAS

Step 11: enable replication again on all DCs

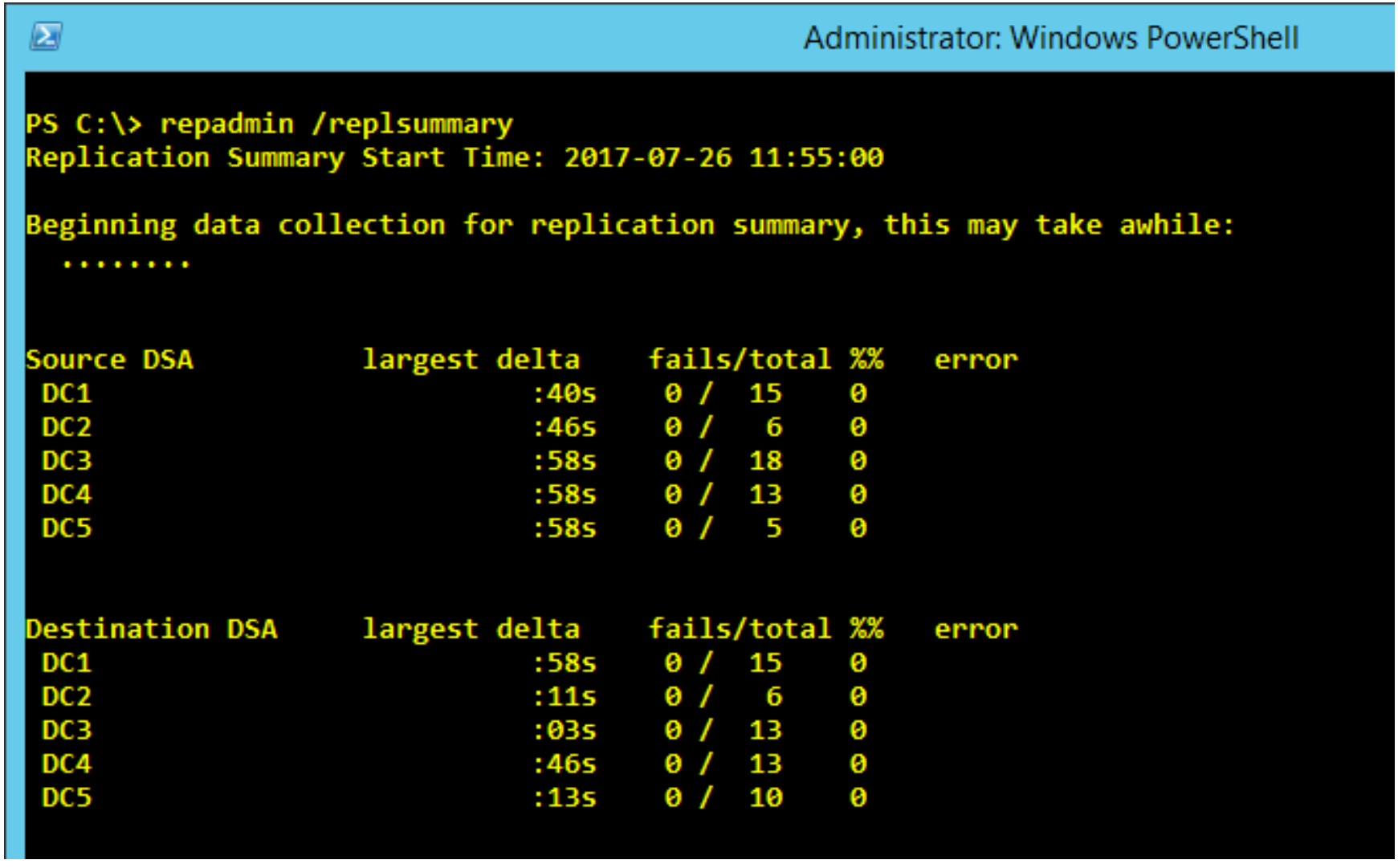
```
sp HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters `
   -Name 'Allow Replication with Divergent and Corrupt Partner' `
   -Value 1 `
   -Type Dword
```

GOPAS

Step 12: invoke replication of all connection objects for all DCs



Step 14: verify the overall replication health with repadmin /replsummary



Phase 5

Cleaning up and restoring normal operations

How to restore AD replication after a time jump as fast as possible

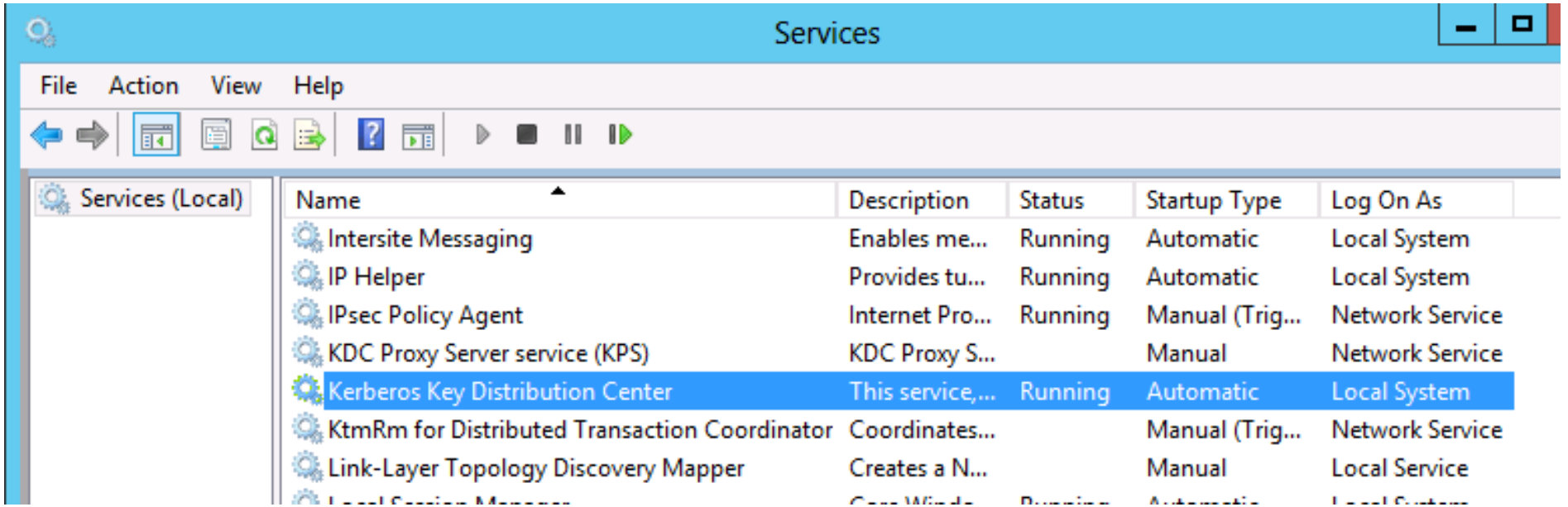
GOPAS

Step 15: disable the replication with divergent and corrupt partner back again on all DCs

```
sp HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters `
   -Name 'Allow Replication with Divergent and Corrupt Partner' `
   -Value 0 `
   -Type Dword
```

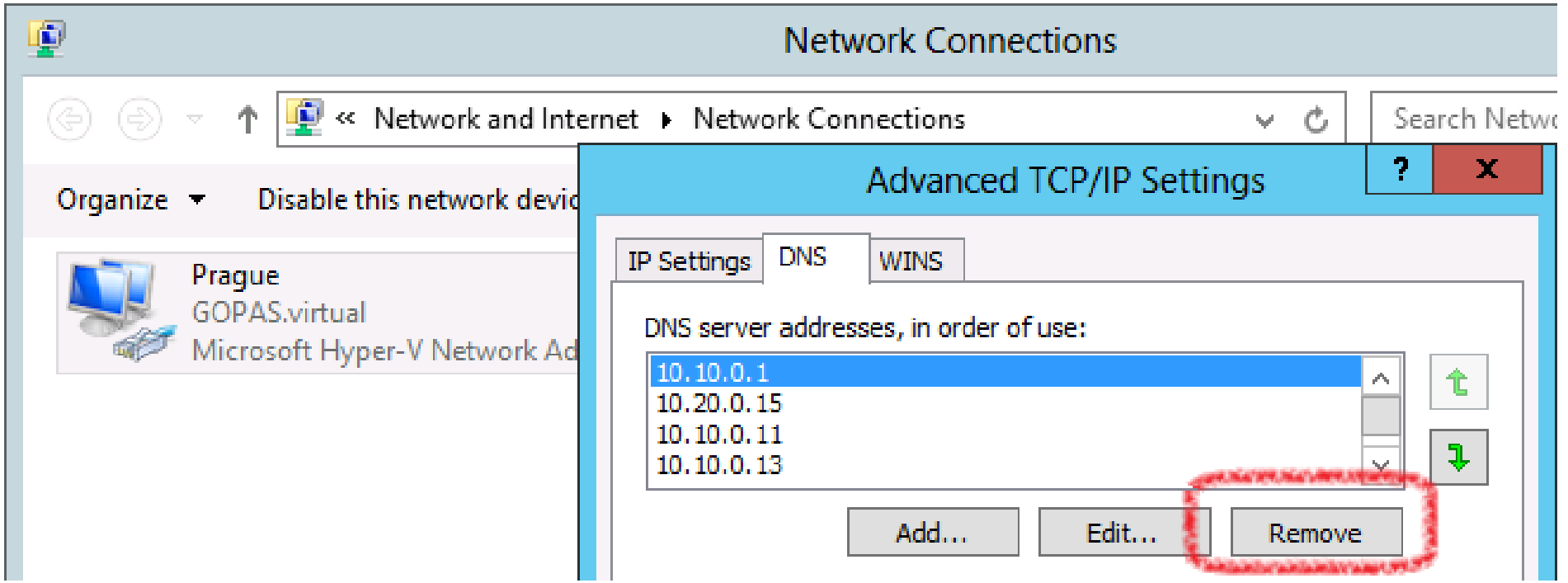
Step 16: start KDC service back on all DCs

```
Start-Service KDC
```



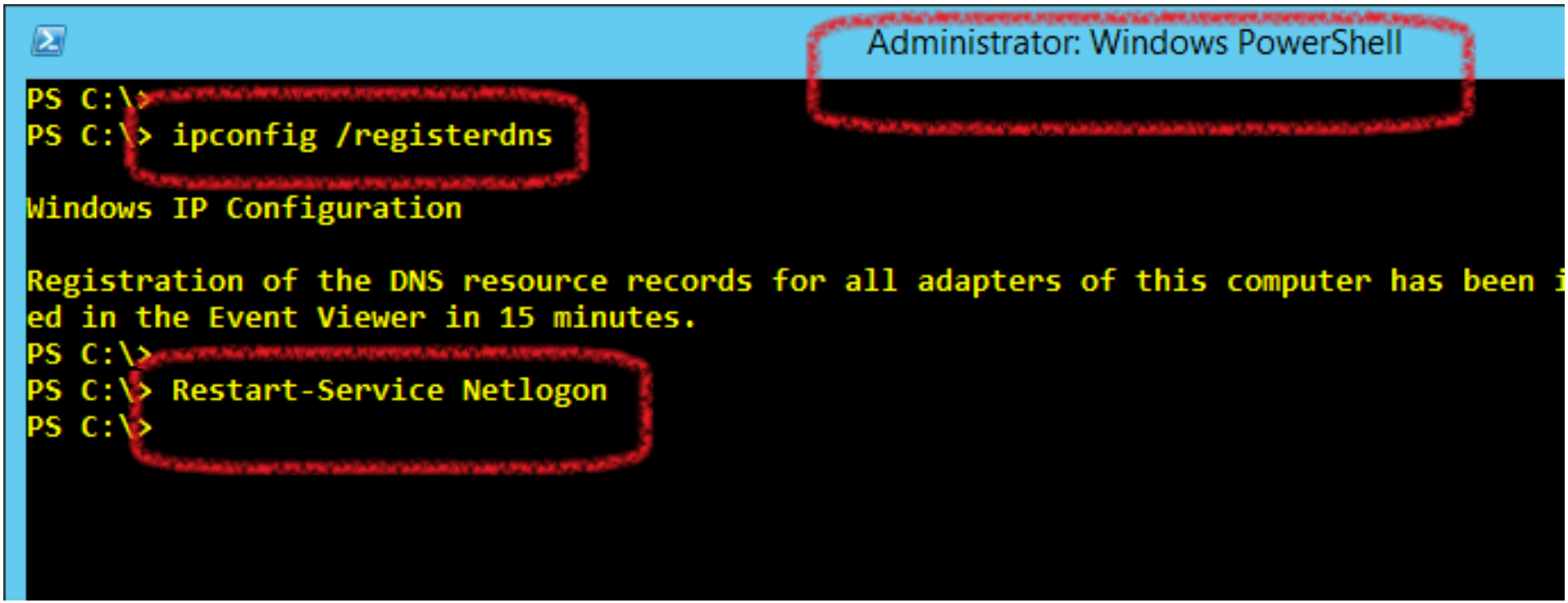
GOPAS

Step 17: remove the recovery DNS server from configuration of all DCs



Step 18: force dynamic DNS registration and Netlogon DC locator DNS record re-registration on all DCs again

```
ipconfig /registerdns
Restart-Service Netlogon
```



Crucial steps recap

- Do not restart DCs
- Correct the time
- Install separate recovery DNS on non-DC
- Stop all KDCs except for one recovery KDC
- Reset the machine passwords to the recovery KCC
- Remove lingering objects
- Enable replication

Thank you

- My training in GOPAS

- GOC166 - Advanced ADFS
- GOC167 - Troubleshooting Remote Access, VPN and DirectAccess
- GOC169 - ISO/IEC 2700x in Windows environment
- GOC171 - Active Directory Troubleshooting
- GOC172 - Kerberos Troubleshooting
- GOC173 - Enterprise PKI Deployment
- GOC175 - Advanced Windows Security
- GOC174 - SharePoint Troubleshooting

GOPAS