



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 |

GOPAS: info@gopas.cz | www.gopas.cz | www.facebook.com/P.S.GOPAS

Motivation

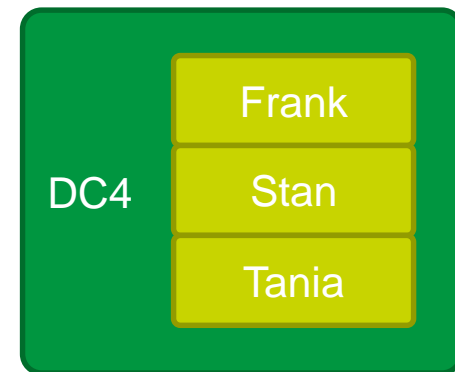
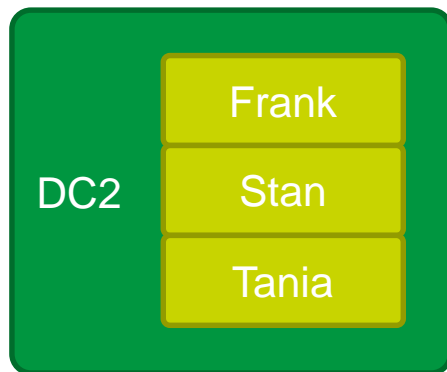
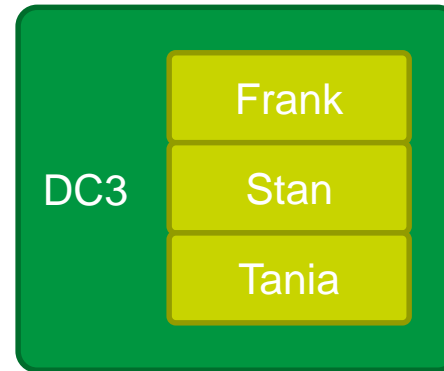
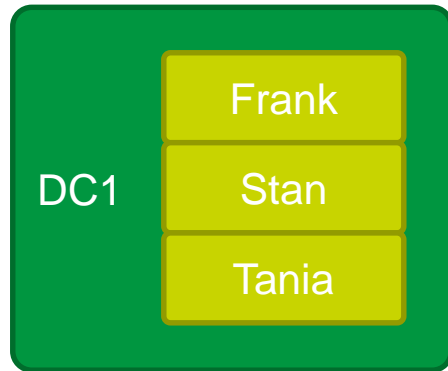
- Hardware does not always maintain its time well
- A single hardware-based DC may go out of sync
- Many **virtualized DCs** on a cloud may go out of sync simultaneously

- My own experience is 5 clouds in past 2 years

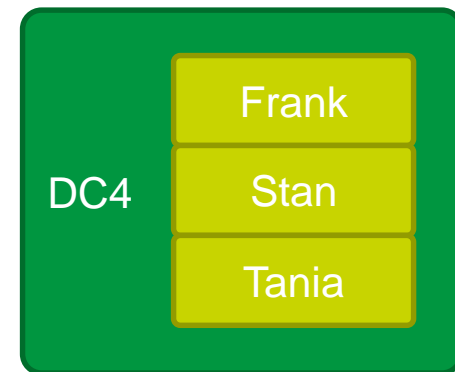
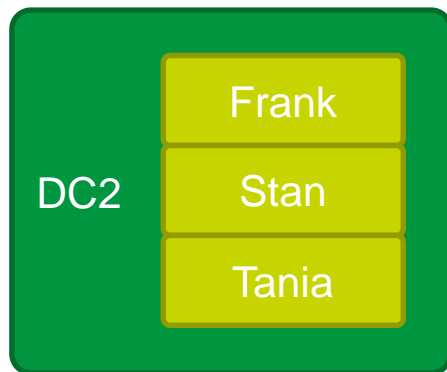
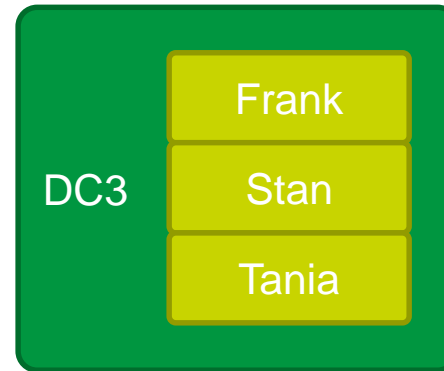
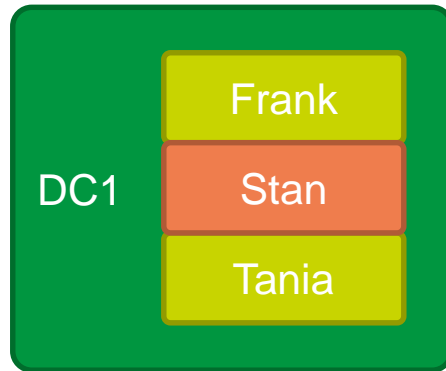
What happens

- 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

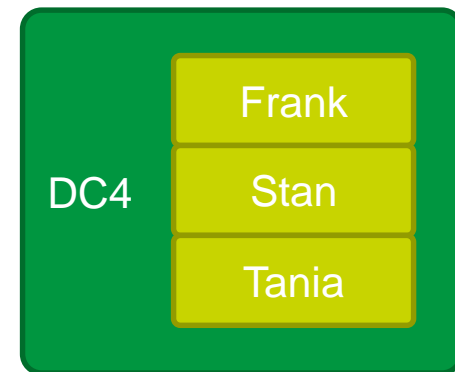
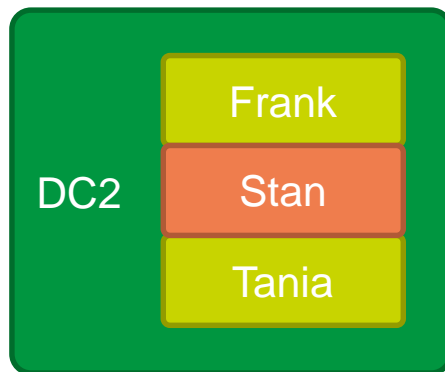
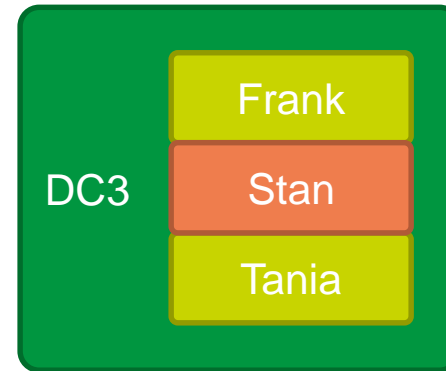
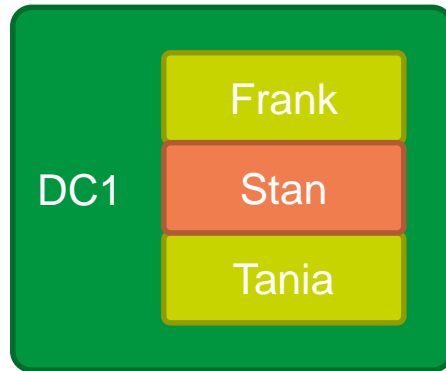
Normal AD deletion process: objects and tombstones



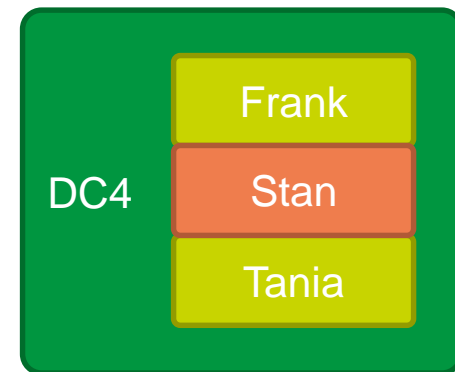
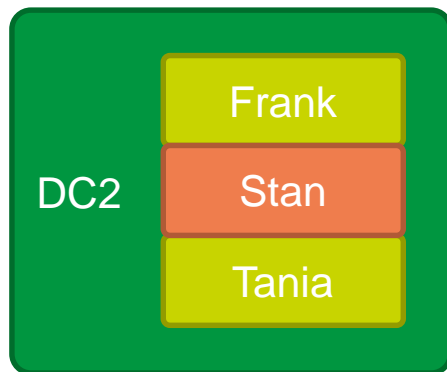
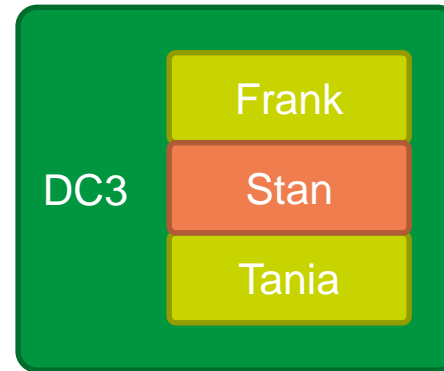
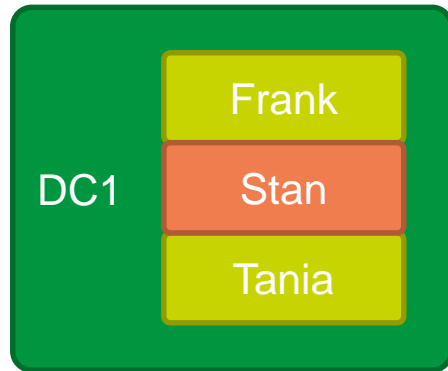
Normal AD deletion process: objects and tombstones



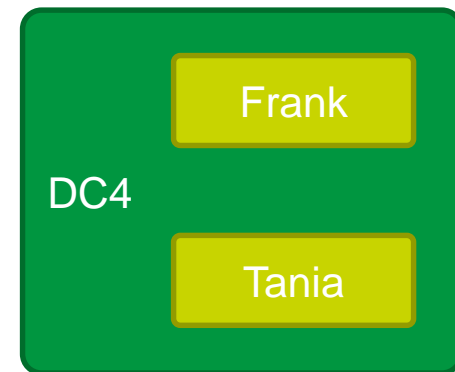
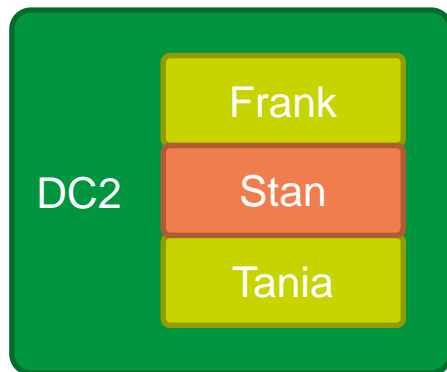
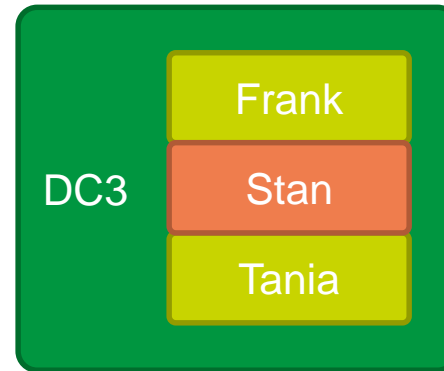
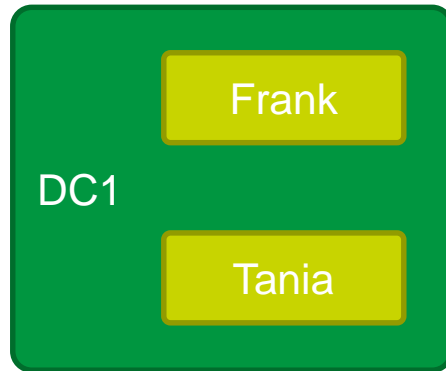
Normal AD deletion process: objects and tombstones



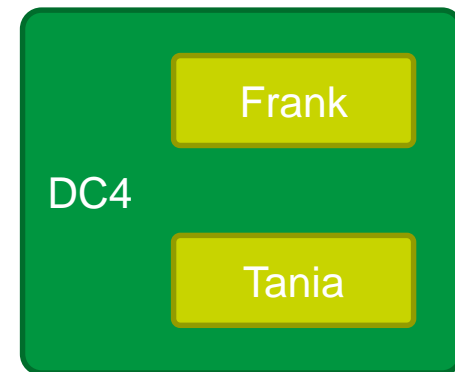
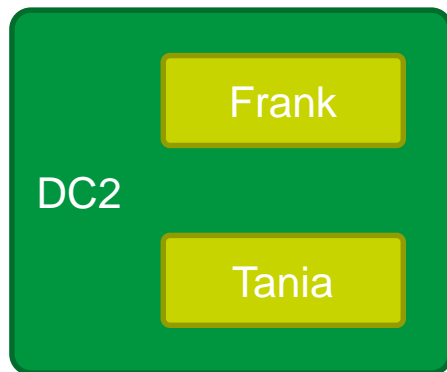
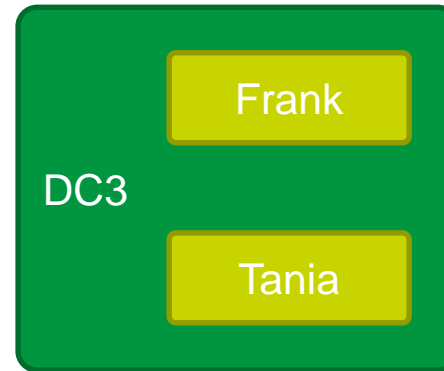
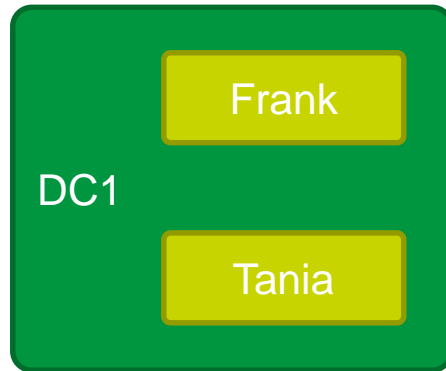
Normal AD deletion process: objects and tombstones



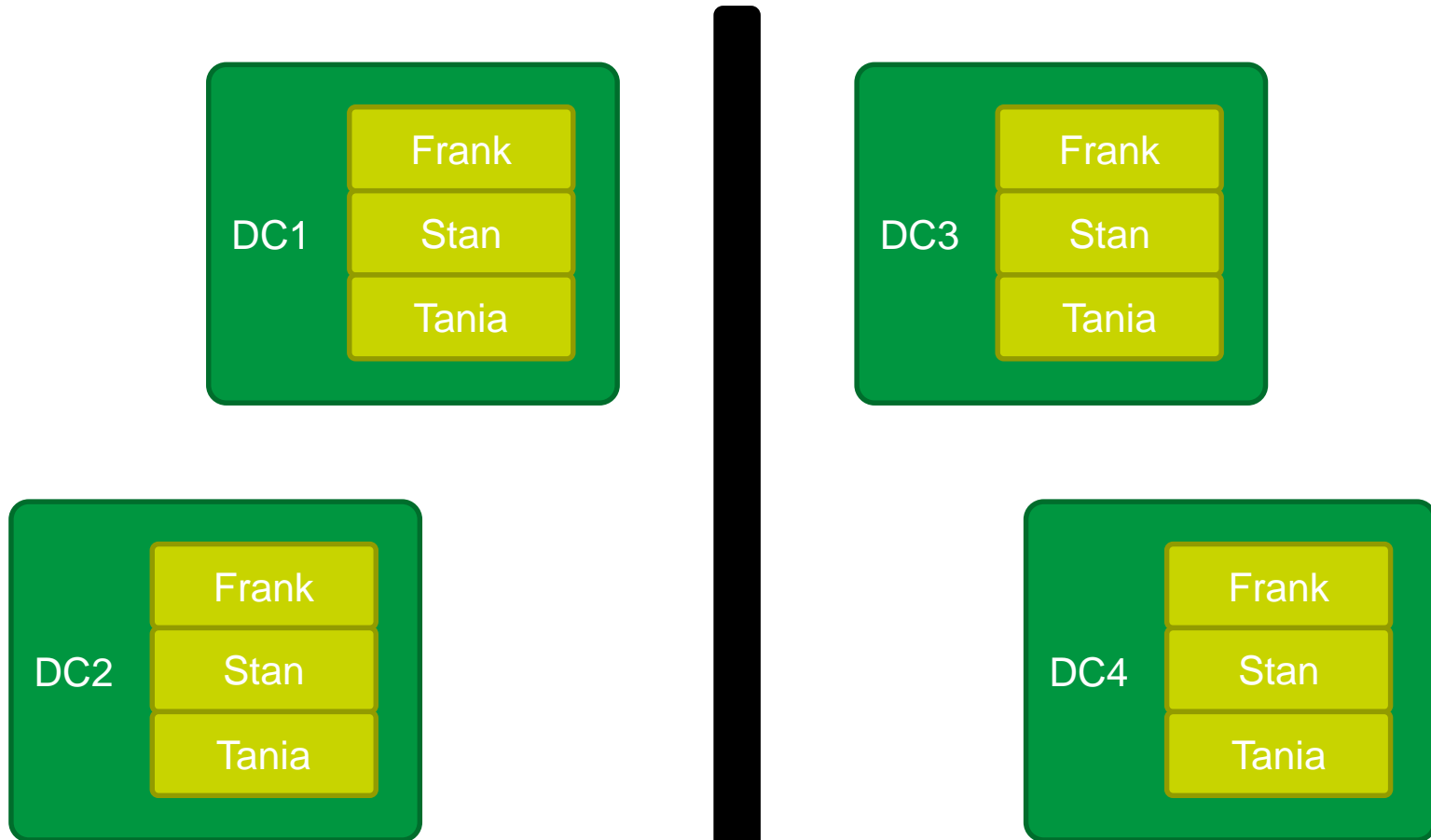
Normal AD deletion process: garbage collection 1/day



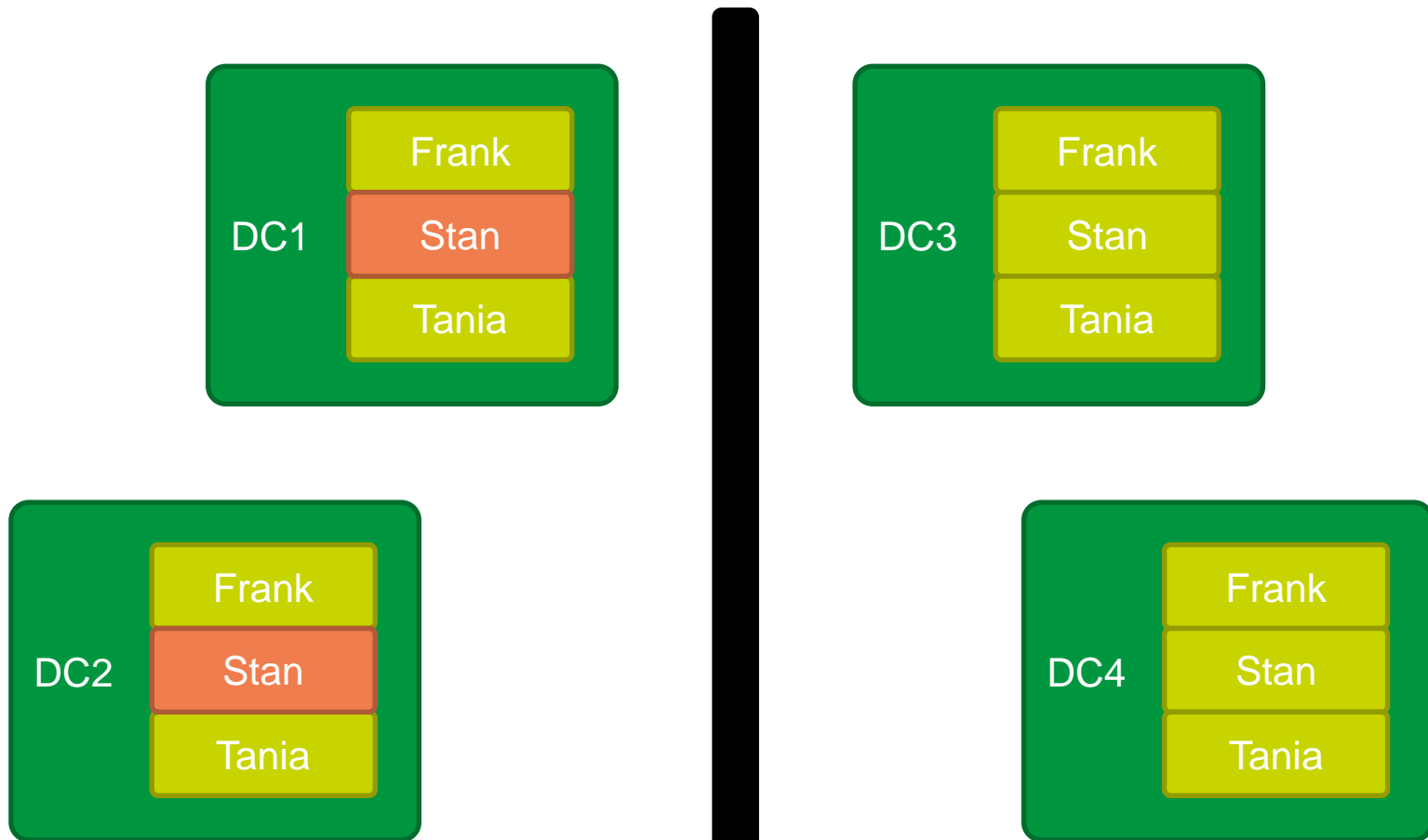
Normal AD deletion process: garbage collection 1/day



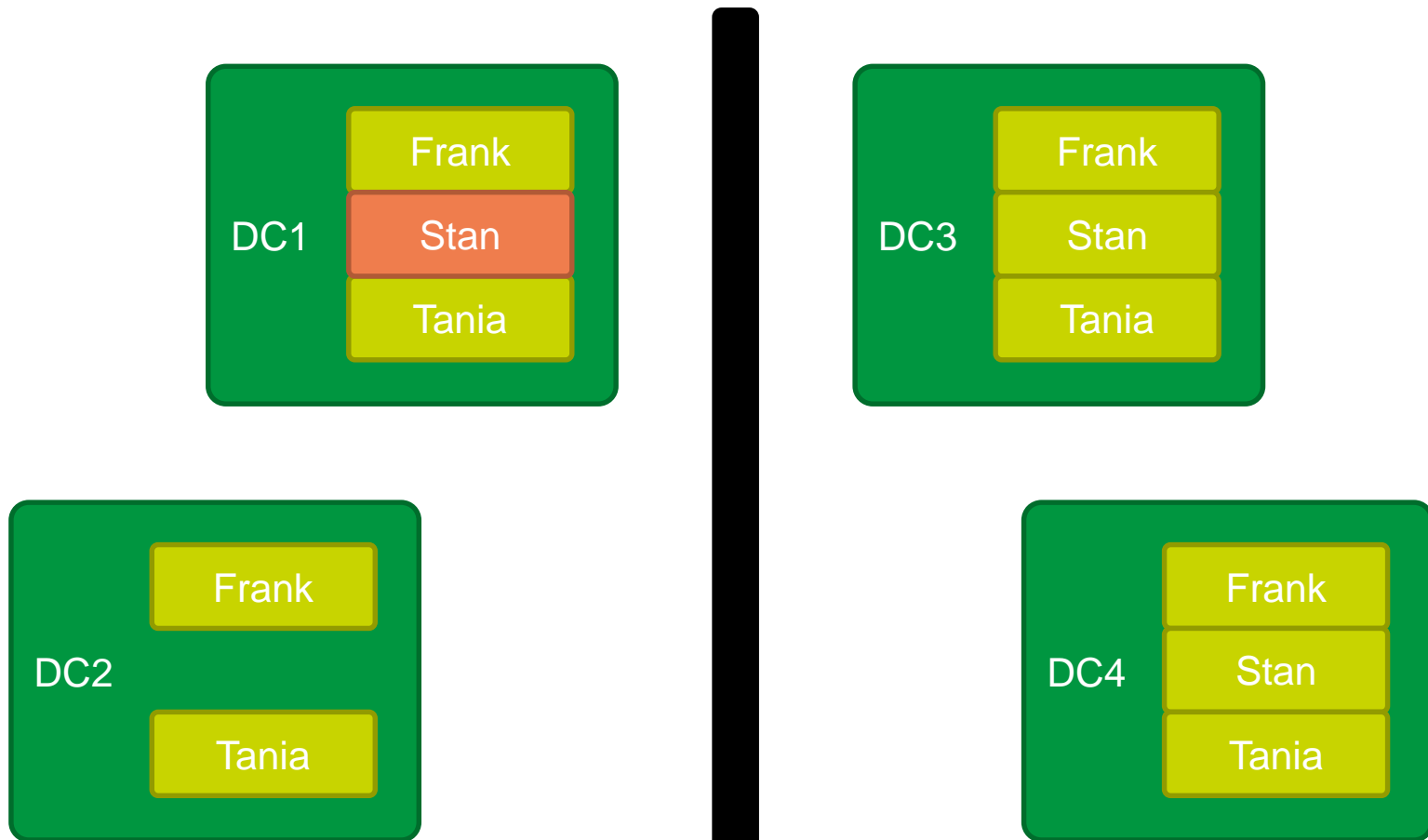
Lingering objects: how they arise



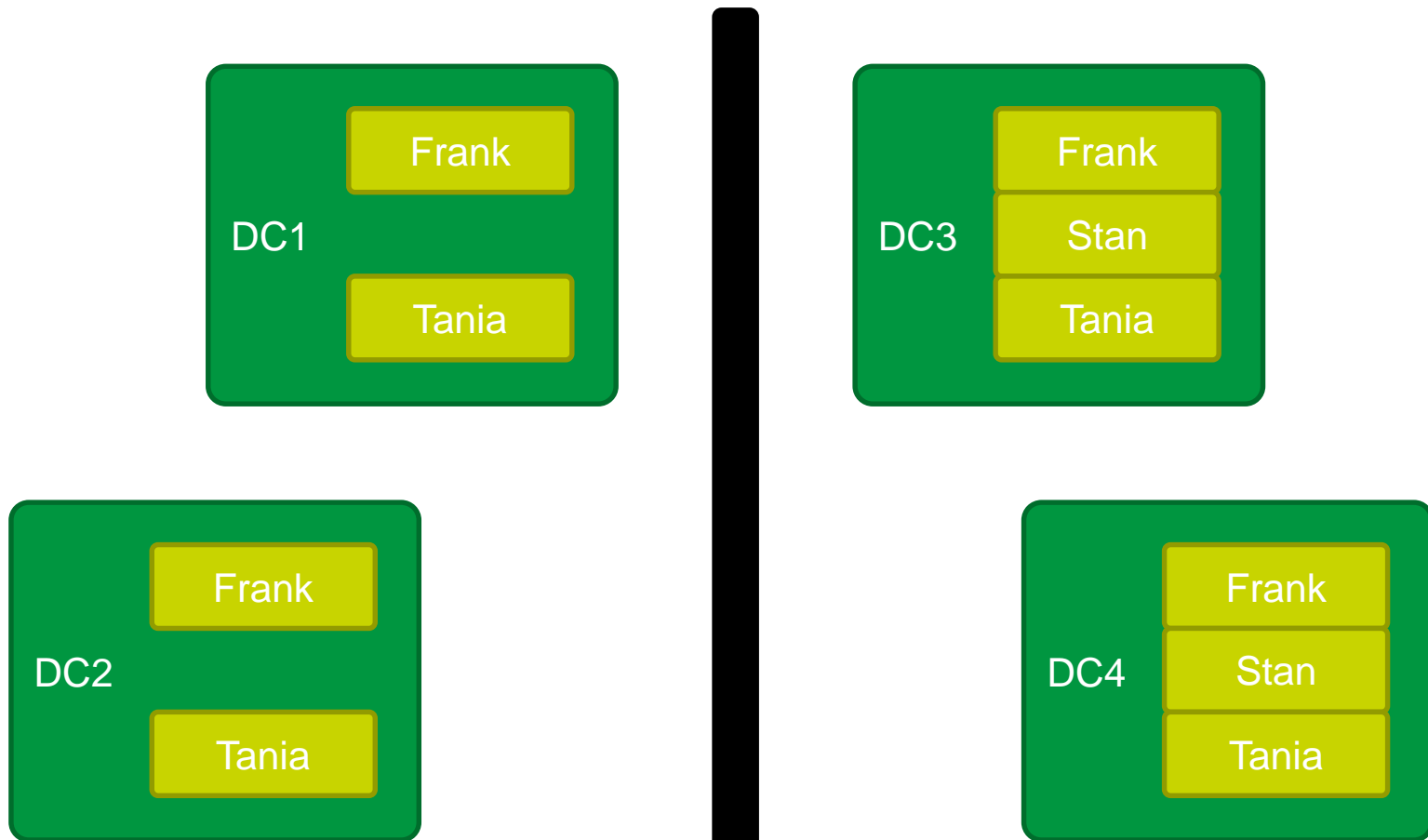
Lingering objects: how they arise



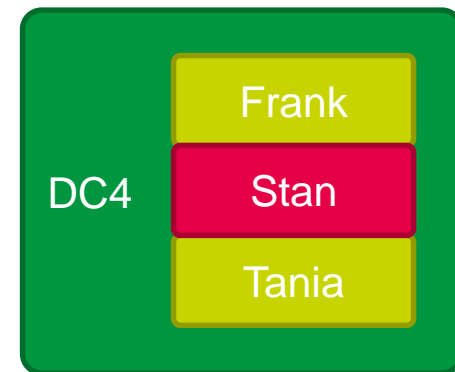
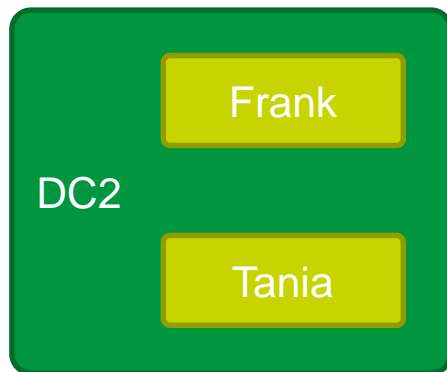
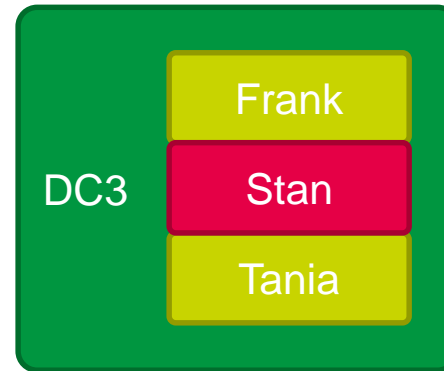
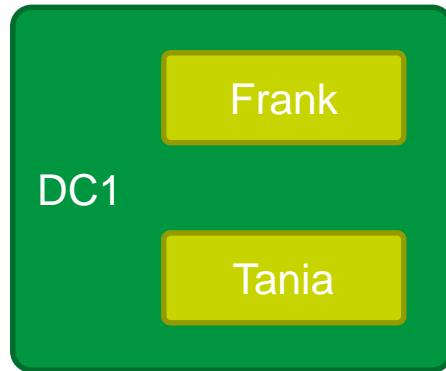
Lingering objects: how they arise after garbage collection



Lingering objects: how they arise after garbage collection



Lingering objects: what would happen after tombstone lifetime

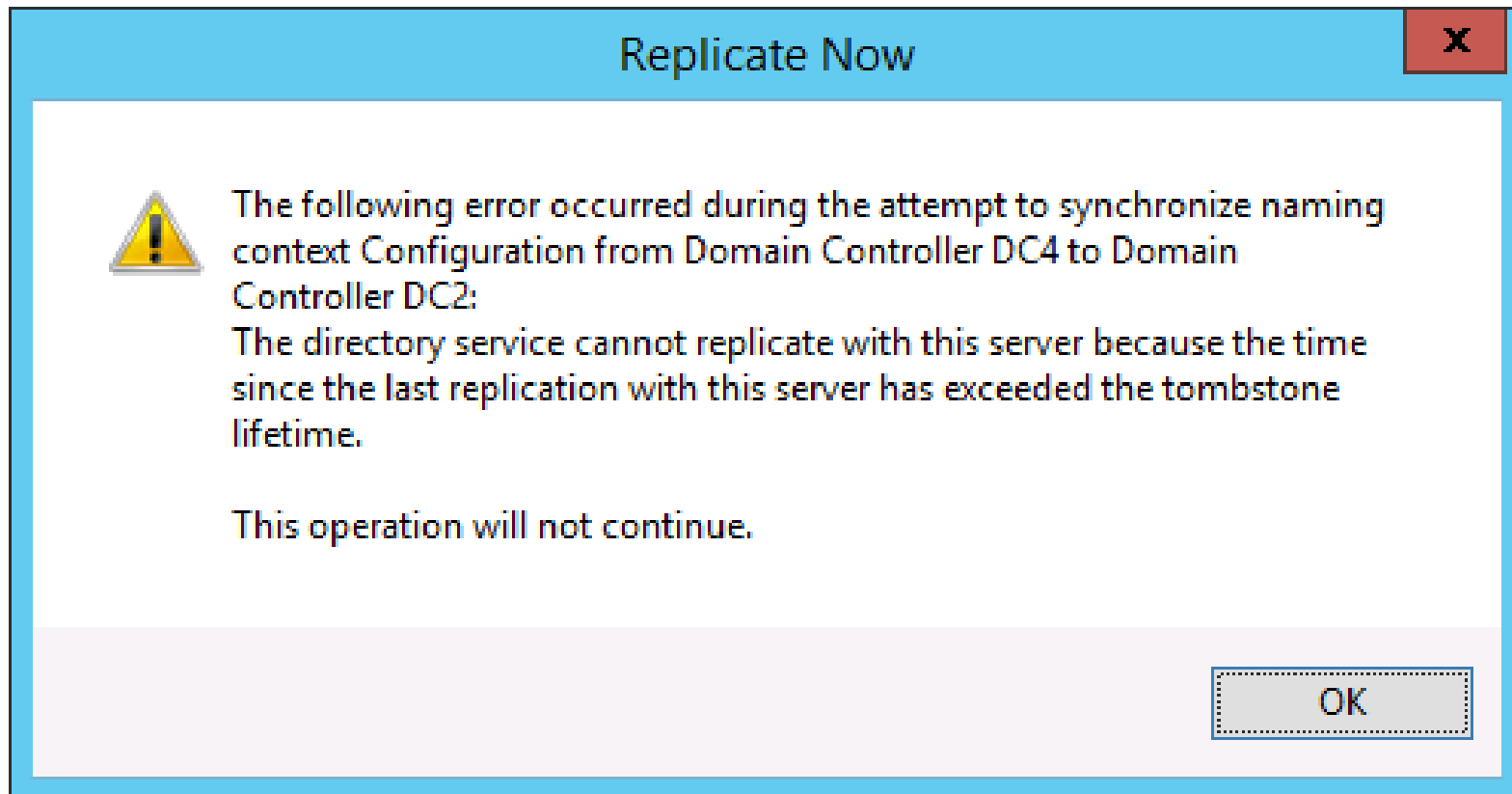


Symptoms

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

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.

Event Properties - Event 2042, ActiveDirectory_DomainService

General Details

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. Replication has been stopped with this source.

The reason that replication is not allowed to continue is that the two DCs may contain lingering objects. Objects that have been deleted and garbage collected from an Active Directory Domain Services partition but still exist in the writable partitions of other DCs in the same domain, or read-only partitions of global catalog

Log Name: Directory Service

Source: ActiveDirectory_DomainServ Logged: 26. 7. 2017 8:53:42

Event ID: 2042 Task Category: Replication

Level: Error Keywords: Classic

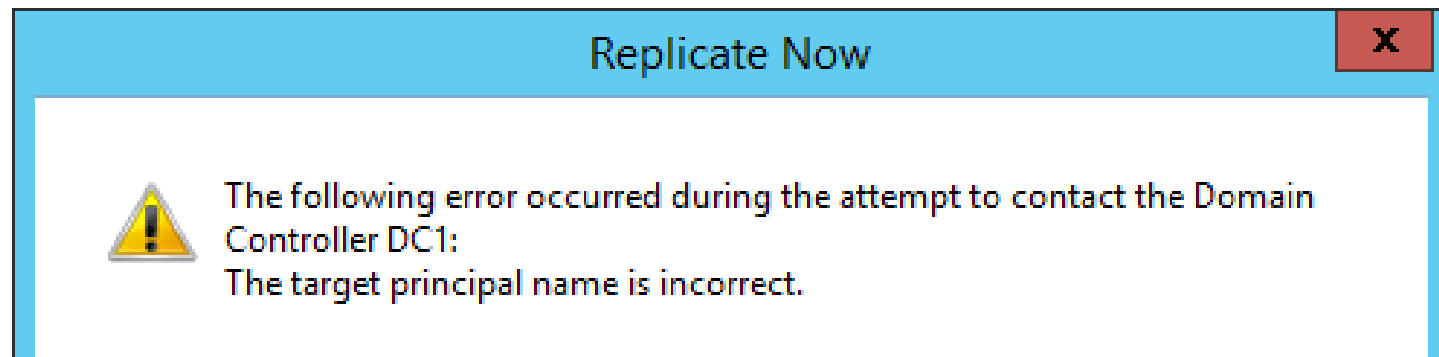
User: ANONYMOUS LOGON Computer: DC5.GOPAS.virtual

OpCode: Info

More Information: [Event Log Online Help](#)

DC account passwords out of sync

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



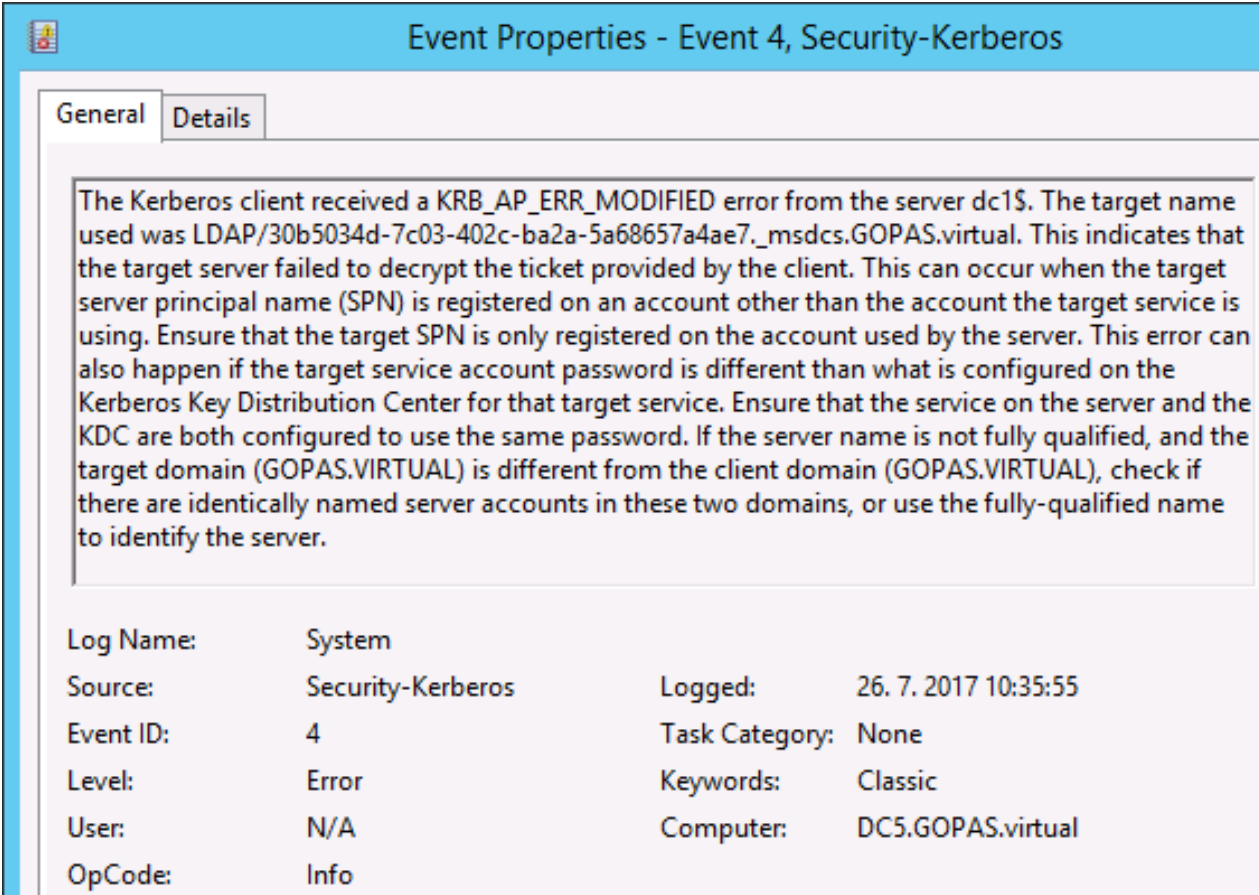
```
Administrator: C:\Windows\system32\cmd.exe
C:\>
C:\>repladmin /replsummary
Replication Summary Start Time: 2016-11-26 10:02:29

Beginning data collection for replication summary, this may take awhile:
.....

Source DSA          largest delta      fails/total %%   error
DC1                 01h:25m:24s      0 / 11   0
DC2                 01h:25m:24s      0 / 6    0
DC3                 01h:25m:29s      0 / 18   0
DC4                 01h:25m:29s      0 / 13   0
DC5                 01h:25m:17s      5 / 5   100 (2148074274) The target principal name is incorrect.
```

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.



The Kerberos client received a KRB_AP_ERR_MODIFIED error from the server dc1\$. The target name used was LDAP/30b5034d-7c03-402c-ba2a-5a68657a4ae7._msdcs.GOPAS.virtual. This indicates that the target server failed to decrypt the ticket provided by the client. This can occur when the target server principal name (SPN) is registered on an account other than the account the target service is using. Ensure that the target SPN is only registered on the account used by the server. This error can also happen if the target service account password is different than what is configured on the Kerberos Key Distribution Center for that target service. Ensure that the service on the server and the KDC are both configured to use the same password. If the server name is not fully qualified, and the target domain (GOPAS.VIRTUAL) is different from the client domain (GOPAS.VIRTUAL), check if there are identically named server accounts in these two domains, or use the fully-qualified name to identify the server.

Log Name:	System	Logged:	26. 7. 2017 10:35:55
Source:	Security-Kerberos	Task Category:	None
Event ID:	4	Keywords:	Classic
Level:	Error	Computer:	DC5.GOPAS.virtual
User:	N/A		
OpCode:	Info		

Repair notes

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

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

Phase 1

Prepare and populate a recovery DNS server

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

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

The screenshot displays the DNS Manager console with the 'gopas.virtual' zone selected in the left-hand tree. The 'gopas.virtual Properties' dialog box is open, showing the 'Start of Authority (SOA)' tab. The 'Type' is set to 'Primary' and 'Dynamic updates' is set to 'Nonsecure and secure'. A warning icon is present at the bottom of the dialog.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], rr.gopas.cz., hostmast...
(same as parent folder)	Name Server (NS)	rr.gopas.cz.

gopas.virtual Properties

Name Servers | WINS | Zone Transfers

General | Start of Authority (SOA)

Status: Running

Type: Primary

Replication: Not an Active Directory-integrated zone

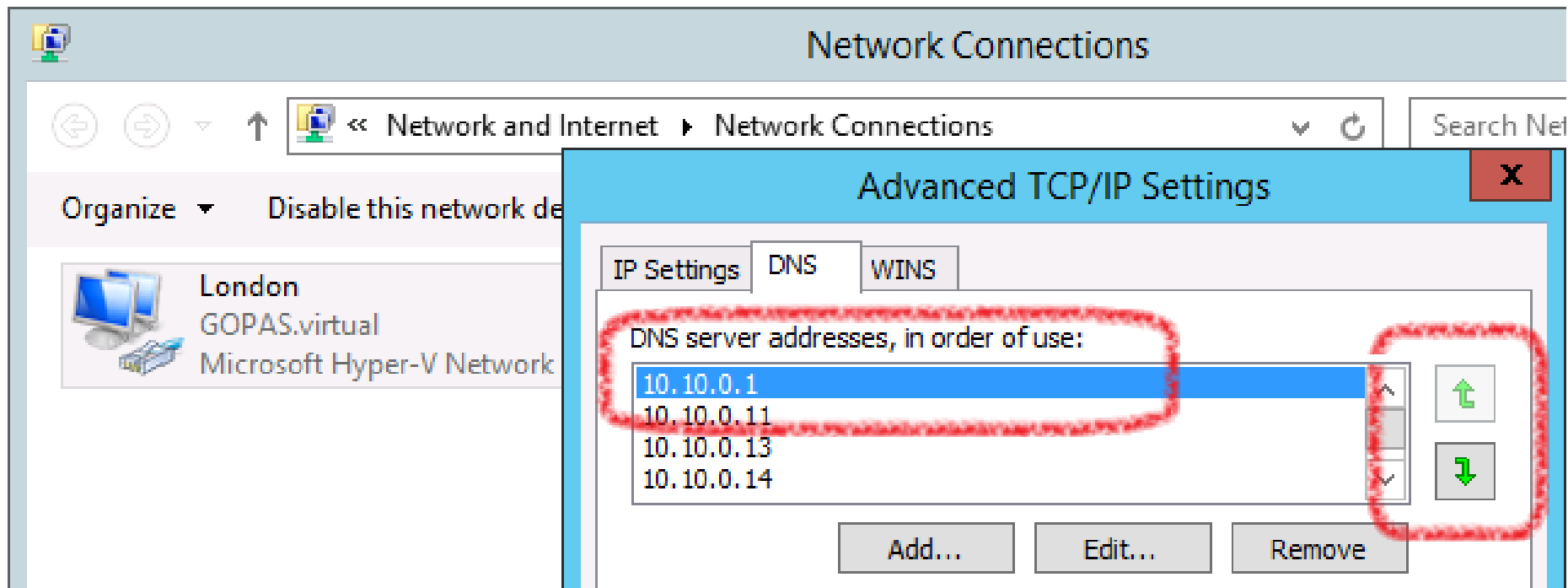
Zone file name:
gopas.virtual.dns

Dynamic updates: Nonsecure and secure

Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.

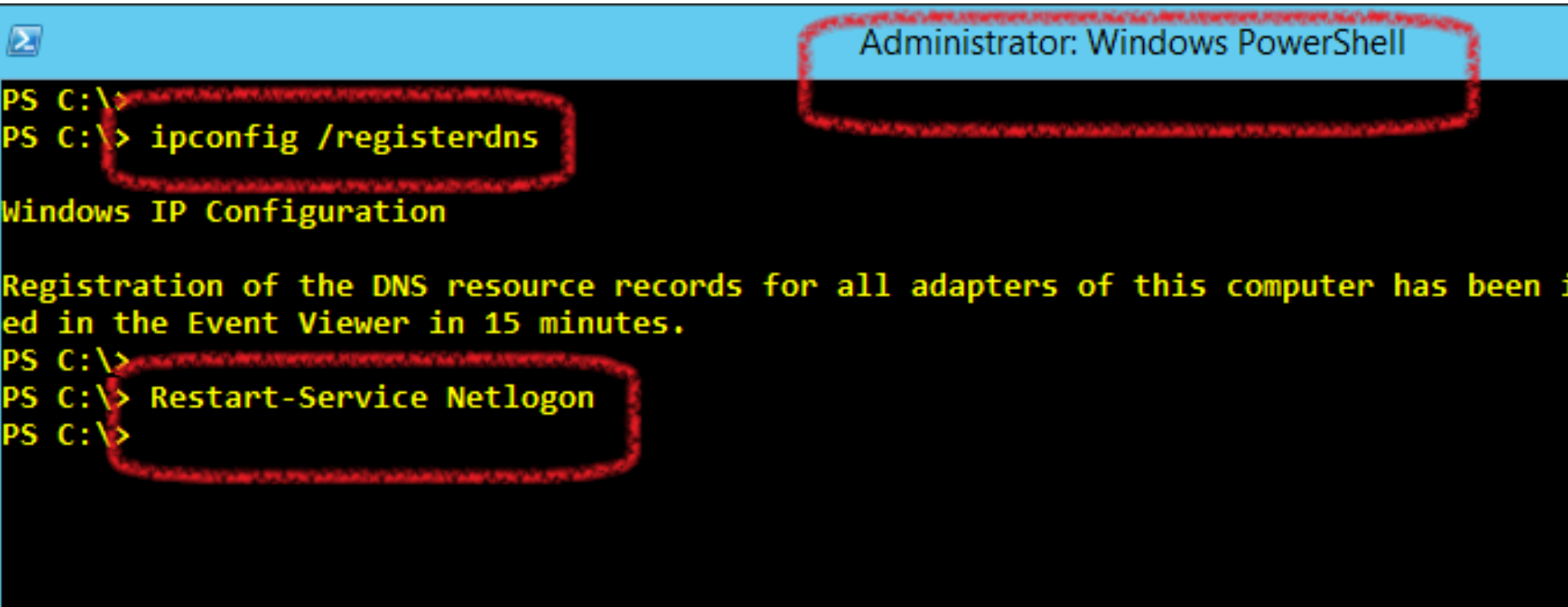
Step 2: reconfigure **all the DCs** to use the temporary DNS server as resolver and to update their DC locator DNS records

- 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
```



The screenshot shows a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal output is as follows:

```
PS C:\>  
PS C:\> ipconfig /registerdns  
Windows IP Configuration  
  
Registration of the DNS resource records for all adapters of this computer has been i  
ed in the Event Viewer in 15 minutes.  
PS C:\>  
PS C:\> Restart-Service Netlogon  
PS C:\>
```

Red dashed boxes highlight the command prompt and the command itself in the first instance, the "Windows IP Configuration" section, and the command prompt and command in the second instance.

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

The screenshot shows the DNS Manager console with the following structure:

- DNS
 - RR
 - Global Logs
 - Forward Lookup Zones
 - GOPAS.cz
 - gopas.virtual**
 - _msdcs
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - Reverse Lookup Zones
 - Conditional Forwarders

Name	Type	Data
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(same as parent folder)	Start of Authority (SOA)	[298], rr.gopas.cz., h
(same as parent folder)	Name Server (NS)	rr.gopas.cz.
(same as parent folder)	Host (A)	10.20.0.15
(same as parent folder)	Host (A)	10.10.0.11
(same as parent folder)	Host (A)	10.10.0.12
(same as parent folder)	Host (A)	10.10.0.13
(same as parent folder)	Host (A)	10.10.0.14
(same as parent folder)	Host (A)	10.10.0.14
DC1	Host (A)	10.10.0.11
DC2	Host (A)	10.10.0.12
DC3	Host (A)	10.10.0.13
DC4	Host (A)	10.10.0.14
DC5	Host (A)	10.20.0.15
olddc	Host (A)	10.10.0.11

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

The screenshot shows the DNS Manager console with the following structure:

- DNS
 - RR
 - Global Logs
 - Forward Lookup Zones
 - GOPAS.cz
 - gopas.virtual** (highlighted)
 - _msdcs** (highlighted)
 - dc
 - domains
 - gc
 - pdcc** (highlighted)
 - 28da11e8-c76e-4031-aca1-8e3e8025af79 (Alias (CNAME) -> dc5.gopas.virtual)
 - 2f2525b2-0482-44ab-a537-f70fddf4f452 (Alias (CNAME) -> dc4.gopas.virtual)
 - 30b5034d-7c03-402c-ba2a-5a68657a4ae7 (Alias (CNAME) -> dc1.gopas.virtual)
 - 67a368bc-60d9-4003-a504-774625865623 (Alias (CNAME) -> dc2.gopas.virtual)
 - d11182e6-74f9-405e-9069-c98150704236 (Alias (CNAME) -> dc3.gopas.virtual)
 - _sites
 - _tcp
 - _udp
 - DomainDnsZones
 - ForestDnsZones
 - Reverse Lookup Zones

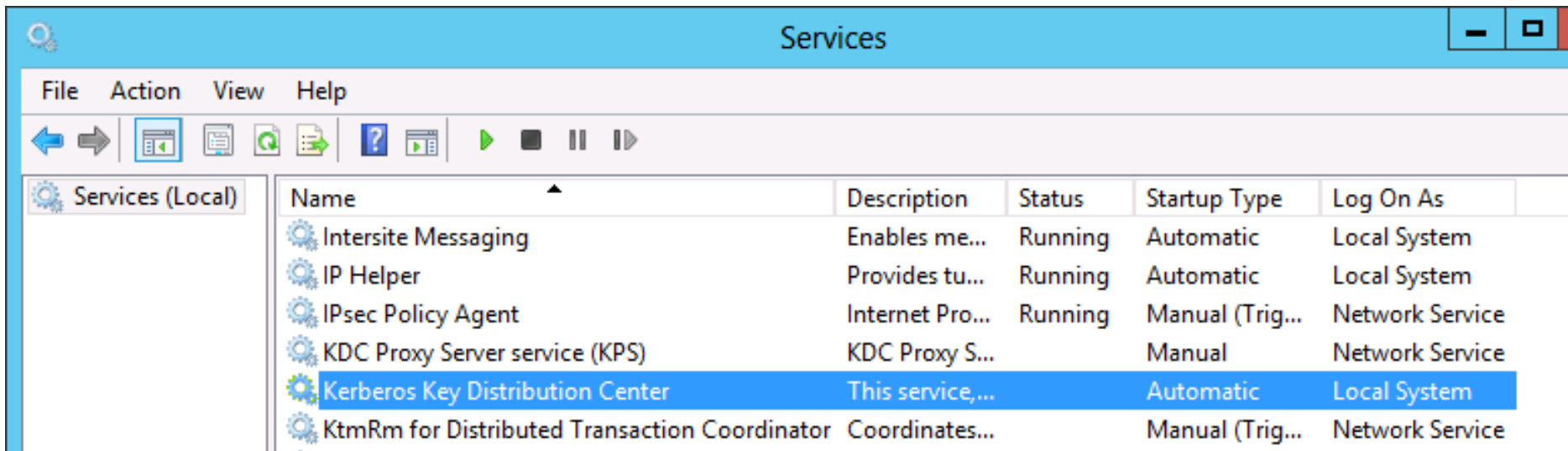
Phase 2

Stop all KDCs except for one "recovery KDC"

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

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

Stop-Service KDC



Phase 3

Reset all DC machine passwords against the "recovery KDC"

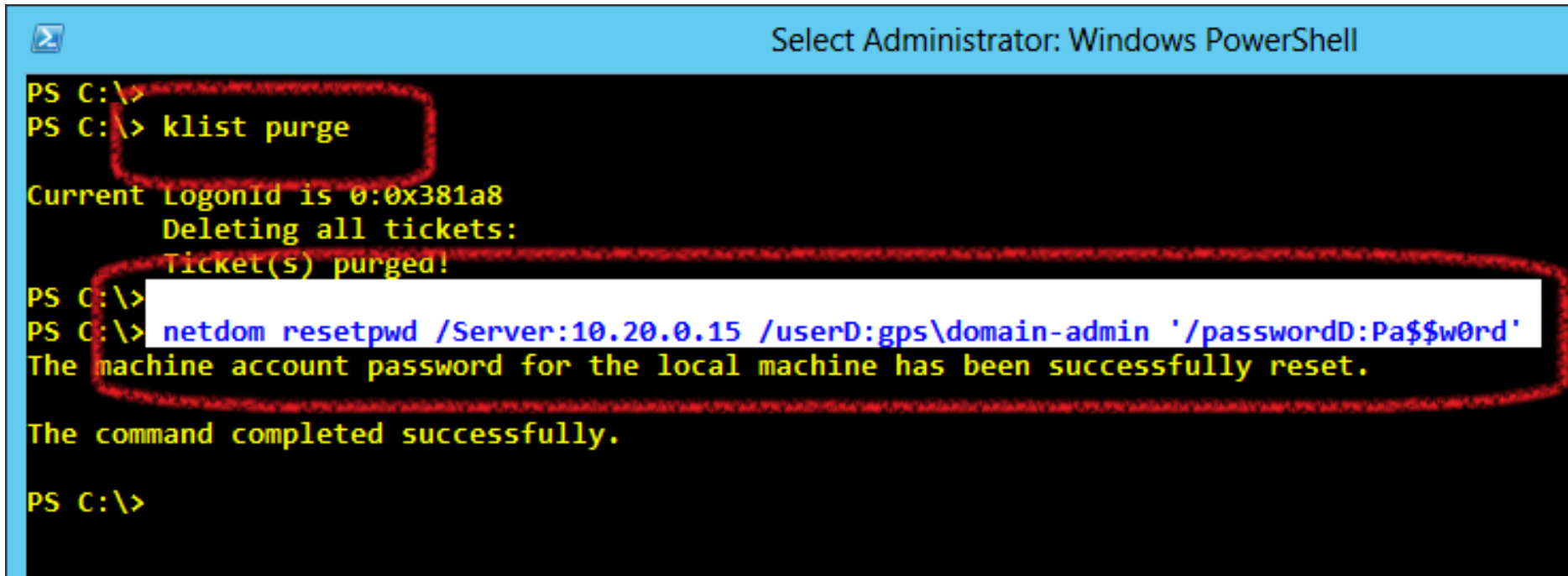
How to restore AD replication after a time jump as fast as possible

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

```
klint 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



The screenshot shows a Windows PowerShell terminal window titled "Select Administrator: Windows PowerShell". The terminal output is as follows:

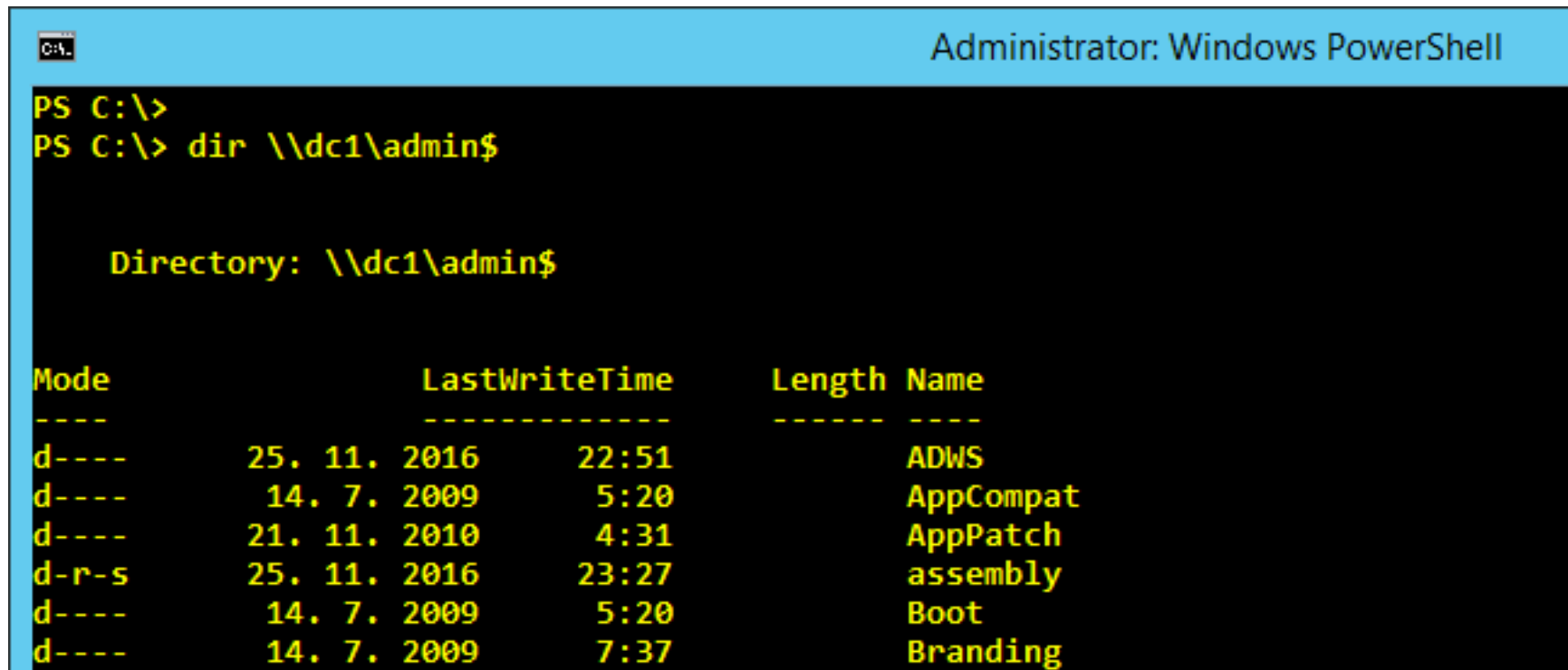
```
PS C:\>  
PS C:\> klist purge  
  
Current LogonId is 0:0x381a8  
Deleting all tickets:  
Ticket(s) purged!  
  
PS C:\>  
PS C:\> netdom resetpwd /Server:10.20.0.15 /userD:gps\domain-admin '/passwordD:Pa$$w0rd'  
The machine account password for the local machine has been successfully reset.  
  
The command completed successfully.  
  
PS C:\>
```

Red dashed boxes highlight the `klint purge` command and the `netdom resetpwd` command and its output.

Step 9: verify that the Kerberos authentication works again

```
dir \\dc1\admin$
```

```
gwmi Win32_OperatingSystem -Computer dc2
```



The screenshot shows a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The user is at the C:\ prompt and has entered the command `dir \\dc1\admin$`. The output shows a directory listing for `\\dc1\admin$` with columns for Mode, LastWriteTime, Length, and Name. The directory contains several subdirectories: ADWS, AppCompat, AppPatch, assembly, Boot, and Branding.

```
PS C:\>
PS C:\> dir \\dc1\admin$

Directory: \\dc1\admin$

Mode                LastWriteTime         Length Name
----                -
d----             25. 11. 2016         22:51 ADWS
d----             14. 7. 2009           5:20 AppCompat
d----             21. 11. 2010           4:31 AppPatch
d-r-s             25. 11. 2016         23:27 assembly
d----             14. 7. 2009           5:20 Boot
d----             14. 7. 2009           7:37 Branding
```

Phase 4

Verify and remove all lingering objects from all partitions

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

Step 10: run repadmin /removelingerobjects 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 /removelingerobjects $dcNames[$iDC] $dcGuids[$iGuid] $onePartition
            }
        }
    }
}
```

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
```

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

The screenshot shows the Active Directory Sites and Services console. The left pane displays a tree view of the directory structure, including Sites, Inter-Site Transports, Subnets, and various sites like Berlin, Budapest, London, Paris, Prague, Roma, and Vienna. The right pane shows a table of connection objects. Two objects are selected, and a context menu is open over them, highlighting the 'Replicate Now' option.

Name	From Server	From Site
<automatically generated>	DC1	Prague
<automatically generated>		

Context Menu Options:

- Replicate Now
- All Tasks
- Delete
- Properties
- Help

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

```
Administrator: Windows PowerShell

PS C:\> repadmin /replsummary
Replication Summary Start Time: 2017-07-26 11:55:00

Beginning data collection for replication summary, this may take awhile:
.....

Source DSA          largest delta      fails/total  %  error
DC1                  :40s              0 / 15      0
DC2                  :46s              0 / 6       0
DC3                  :58s              0 / 18      0
DC4                  :58s              0 / 13      0
DC5                  :58s              0 / 5       0

Destination DSA     largest delta      fails/total  %  error
DC1                  :58s              0 / 15      0
DC2                  :11s              0 / 6       0
DC3                  :03s              0 / 13      0
DC4                  :46s              0 / 13      0
DC5                  :13s              0 / 10      0
```

Phase 5

Cleaning up and restoring normal operations

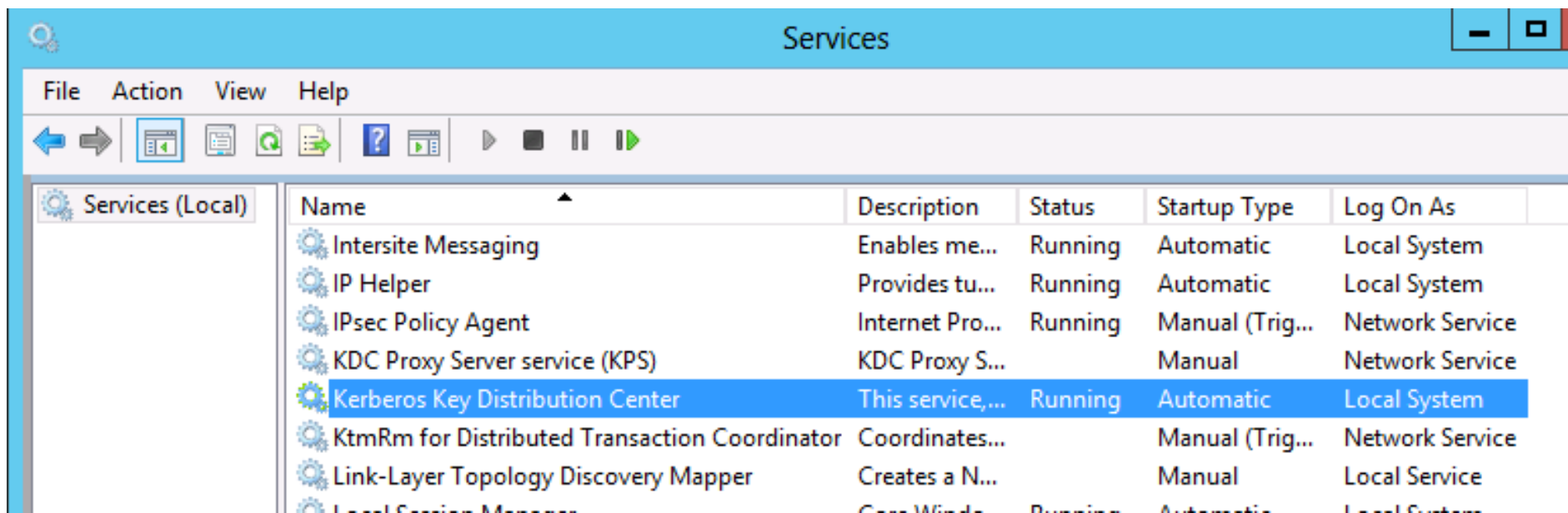
How to restore AD replication after a time jump as fast as possible

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

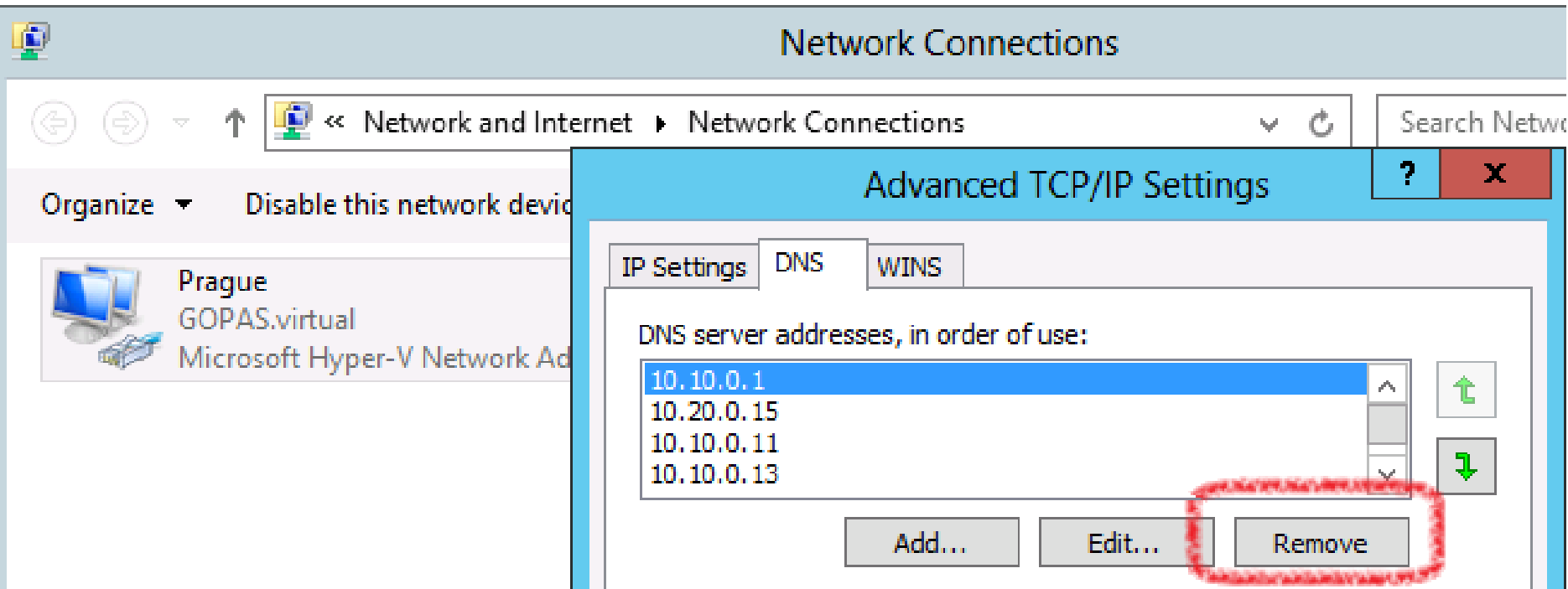
```
sp HKLM:\SYSTEM\CurrentControlSet\Services\NTDS\Parameters `
  -Name 'Allow Replication with Divergent and Corrupt Partner' `
  -Value 0 `
  -Type Dword
```

Step 16: start KDC service back on all DCs

Start-Service KDC

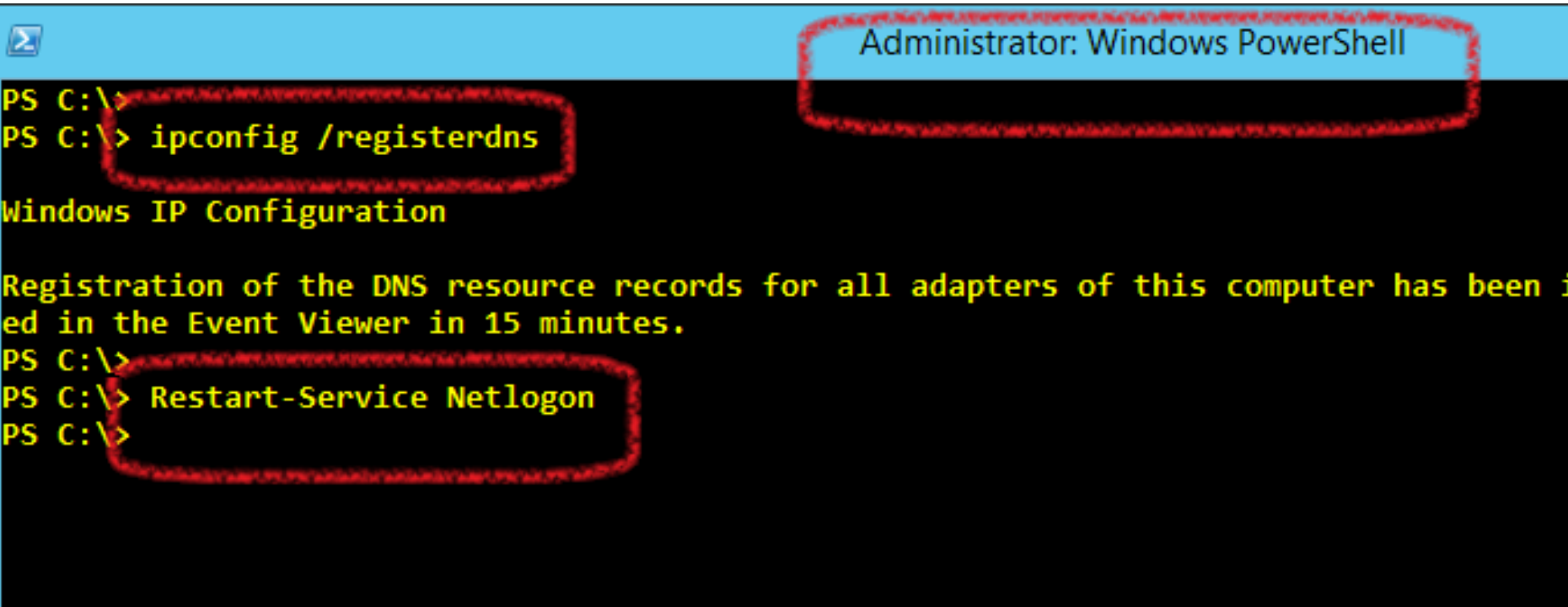


Step 17: remove the recovery DNS server from configuration of all DCs



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

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



The screenshot shows a Windows PowerShell terminal window titled "Administrator: Windows PowerShell". The terminal output is as follows:

```
PS C:\>  
PS C:\> ipconfig /registerdns  
Windows IP Configuration  
  
Registration of the DNS resource records for all adapters of this computer has been i  
ed in the Event Viewer in 15 minutes.  
PS C:\>  
PS C:\> Restart-Service Netlogon  
PS C:\>
```

Red dashed boxes highlight the command prompt and the command input for `ipconfig /registerdns`, the output message "Registration of the DNS resource records for all adapters of this computer has been i ed in the Event Viewer in 15 minutes.", and the command input for `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