**GRT-5279 Automation Logic – Remove Lingering Objects from DC**

**Objective:**

|  |  |
| --- | --- |
| 1 | Collect event ID 1988 |
| 2 | Evaluate the information from 1988 and display the result with server name and other details |
| 3 | Evaluate the strict replication status |
| 4 | Remove lingering objects if option is selected. |
| 5 | Push the replication and gather the health status |

**UI Needed:**

1. Generate the number of lingering objects using advisory mode $advisorymode
2. Remove lingering objects $Removalmode (to be run from server generating event ID 1988)
3. Get the present number of lingering object from divergent or corrupt replication partner
4. Get the number of lingering object removed from divergent or corrupt replication partner
5. Set the ADWS Service to automatic
6. Start the ADWS Service.

**Automatic Steps:-**

1. Check the system’s Windows NT kernel version.

*(Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion").CurrentVersion*

1. If the kernel version is equal to OR greater than 6.1, continue to next step.
2. If the kernel version is less than 6.1, exit with error: Legacy OS found.
3. Check if current machine is domain controller

If current machine is not a DC then exit stating “This machine is not a domain controller, exiting the script.”

1. Check the status of ADWS Service if the same is not running then exit stating “could not proceed further as ADWS Service is not running please select “set the ADWS Service to automatic” and “start the ADWS Service” to proceed further.“
2. If the ADWS Service is running but set to manual then continue stating “ADWS Service is set to manual startup type but running and if you want to set the same to Automatic then select “set the ADWS Service to automatic””
3. Check the status of ADWS Service if the same is not present then exit stating “could not continue further as the ADWS Service is not present “
4. Option to be given to start the ADWS Service if set to Automatic and another option to be given to set automatic if Service is set to Manual or Disabled.
5. Check if NTDS and Netlogon Services are running and if the same are not in running state then exit stating “$ServiceName Service is not running, cannot proceed further.”
6. Run repadmin /showreps and if there are no issues in replication then exit stating “Did not find any errors in replication, cannot proceed further” and exit with requiredinfo.
7. Check the number of DC’s in the FOREST if there is single forest and single DC then exit stating “Only one domain with single DC found in the domain” exit after showing the requiredinfo.
8. Proceed further only if $getAdvisoryResult -eq false if $getAdvisoryResult –eq $true then **skip to point number 17 and 18**
9. Check if there is any event ID 1988 present in directory Services logs if there are no 1988 events then exit stating message, write-output “Did not find any 1988 event ID’s for lingering object issues.”
10. If the 1988 event found in Directory Services logs then state write-output like “There are 10 event ID 1988 present in last 24 hours and last event ID occurred at $time with below description”

$Descriptionoflast1988

1. Evaluate the 1988 event ID as below.

Log Name: Directory Service

Source: Microsoft-Windows-ActiveDirectory\_DomainService

Date: 2/7/2008 8:20:11 AM

Event ID: 1988

Task Category: Replication

Level: Error

Keywords: Classic

User: ANONYMOUS LOGON

Computer: DC5.contoso.com

Description:

Active Directory Domain Services Replication encountered the existence of objects in the following partition that have been deleted from the local domain controllers (DCs) Active Directory Domain Services database. Not all direct

or transitive replication partners replicated in the deletion before the tombstone lifetime number of days passed. 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 servers

in other domains in the forest are known as "lingering objects".

This event is being logged because the source DC contains a lingering object which does not exist on the local DCs Active Directory Domain Services database. This replication attempt has been blocked.

The best solution to this problem is to identify and remove all

Lingering objects in the forest.

Source DC (Transport-specific network address):

4a8717eb-8e58-456c-995a-c92e4add7e8e.\_msdcs.contoso.com

Object:

CN=InternalApps,CN=Users,DC=contoso,DC=com

Object GUID:

a21aa6d9-7e8a-4a8f-bebf-c3e38d0b733a

UI to be developed in a way that

If $advisorymode is $true and $removalmode is $false

1. We need to run below 5 commands for individual directory partitions to gather the state of lingering objects in advisory mode

repadmin /removelingeringobjects Destination\_domain\_controller Source\_domain\_controller\_GUID

Directory\_partition /advisory\_mode

So if the 1988 event ID triggered on DC2 with GUID 1df57db8-dfd5-4295-8acb-8b27e9927552 and Source under event ID 1988 is showing as 352001e1-2b91-4b53-8f69-964f7a93fc79 .\_msdcs.domain.local

Then the commands would be similar to below

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

dc=domain,dc=local /advisory\_mode

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

cn=configuration,dc=domain,dc=local /advisory\_mode

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

DC=domainDNSZones,dc=domain,dc=local /advisory\_mode

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

dc=forestdnszones,dc=domain,dc=local /advisory\_mode

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

CN=Schema,CN=Configuration,DC=domain,DC=local/advisory\_mode

Refer <https://support.microsoft.com/en-us/help/870695/outdated-active-directory-objects-generate-event-id-1988-in-windows-se> for more information and understanding.

1. We need to grab the **Source DC (Transport-specific network address):**  andget the hostname of the same

$srcdc =(Test-Connection -count 1 "1df57db8-dfd5-4295-8acb-8b27e9927552.\_msdcs.domain.local").\_\_SERVER

1. Grab the current hostname name and find the GUID of the same and run below command

$thisDC=$env:COMPUTERNAME

$site= nltest /dsgetsite

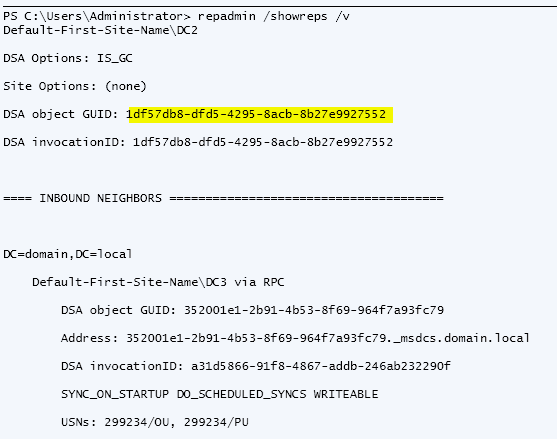
$sitename=($site -replace "The command completed successfully", "")

$sitename

$GUID=Get-ADObject "CN=NTDS Settings,CN=$thisDC,CN=Servers,CN=$sitename,CN=Sites,CN=Configuration,DC=domain,DC=local" |select ObjectGUID

$healthyGUID=$GUID.objectGUID.GUID

You may also find the GUID of DC using repadmin /showrepl /v



Above are two different method to get the GUID of the DC however please prefer the more precise way to capture details

Once the command has been completed successfully we need to write-output “Command has been completed successfully and to find the list of lingering objects, please select “Get the lingering object advisory result” ($getAdvisoryResult)and run the script from the source of lingering object and as per event it is $Sourceoflingeringobjects ” 4a8717eb-8e58-456c-995a-c92e4add7e8e.\_msdcs.contoso.com.

1. DC3 is the source DC which was mentioned in the event log as *Source DC (Transport-specific network address):*
2. Collect event ID 1942 under Directory service log and print the last five occurrence time and description.

If $advisorymode is $false and $removalmode is $true

1. If the $removelingeringobject is $true then we need to run the same commands without /advisory\_mode

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

dc=domain,dc=local

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

cn=configuration,dc=domain,dc=local

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

DC=domainDNSZones,dc=domain,dc=local

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

dc=forestdnszones,dc=domain,dc=local

repadmin /removelingeringobjects DC3 1df57db8-dfd5-4295-8acb-8b27e9927552

CN=Schema,CN=Configuration,DC=domain,DC=local

1. Once $removelingeringobject part is executed script should ask the tech to run below check in point number 20 on DC3.
2. Collect event ID 1939 under Directory service log and print the last five occurrence time and description.