Assignment 3:  
Domain Controller Roles, Backups and Recovery

*Kyle Walker*

*NETW2500*

*10/17/2024*

Table of Contents

[Task 1: 2](#_Toc180252588)

[Question 1: 2](#_Toc180252589)

[PDCtranscriptA3.txt: 3](#_Toc180252590)

[Read-Only Domain Controller Screenshots: 6](#_Toc180252591)

[C:\RODCtranscriptA3.txt: 6](#_Toc180252592)

[RODC Password Replication Policy Screenshot: 8](#_Toc180252593)

[Task 2: 8](#_Toc180252594)

[RODC Connection Information Screenshot: 9](#_Toc180252595)

[Replication Settings Screenshot: 9](#_Toc180252596)

[Task 5: 10](#_Toc180252597)

[Question 1: 10](#_Toc180252598)

[Question 2: 10](#_Toc180252599)

[Documentation and Backups: 10](#_Toc180252600)

[Bibliography 12](#_Toc180252601)

# Task 1:

Question 1: **What is your Forest and Domain function levels identified in your commands. What are function levels and why are they set as recorded in your report?**

Functional levels determine what kind of ADDS functionalities your server will be capable of while also displaying which version of Windows Server can be run on the domain controller. In our case, the Forest and Domain both have the Windows Server 2016 functional level, so it can operate under Windows Server 2016, 2019, 2022 and the newest 2025 if needed. (Microsoft, n.d.)

## PDCtranscriptA3.txt:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Windows PowerShell transcript start

Start time: 20241017184931

Username: kaw\Administrator

RunAs User: kaw\Administrator

Configuration Name:

Machine: DC01A1C20 (Microsoft Windows NT 10.0.20348.0)

Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noExit -Command Invoke-SConfigLogon

Process ID: 368

PSVersion: 5.1.20348.2760

PSEdition: Desktop

PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.20348.2760

BuildVersion: 10.0.20348.2760

CLRVersion: 4.0.30319.42000

WSManStackVersion: 3.0

PSRemotingProtocolVersion: 2.3

SerializationVersion: 1.1.0.1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Transcript started, output file is C:\PDCtranscriptA3.txt

PS C:\Users\Administrator> Import-Module ActiveDirectory

PS C:\Users\Administrator> cd c:

PS C:\Users\Administrator> cd c:\

PS C:\> ls

Directory: C:\

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 5/8/2021 5:15 AM PerfLogs

d-r--- 9/16/2024 12:11 PM Program Files

d----- 5/8/2021 6:34 AM Program Files (x86)

d-r--- 9/25/2024 1:48 PM Users

d----- 10/17/2024 6:47 PM Windows

-a---- 9/17/2024 11:57 AM 424 DCPromoScript.txt

-a---- 9/24/2024 12:18 PM 4698 HistoryLog.txt

-a---- 10/17/2024 6:49 PM 0 PDCtranscriptA3.txt

PS C:\> mkdir Reports

Directory: C:\

Mode LastWriteTime Length Name

---- ------------- ------ ----

d----- 10/17/2024 6:51 PM Reports

PS C:\> cd ./Reports

PS C:\Reports> Get-ADForest >> ./FLReport.txt

>> ParameterBinding(Out-File): name="InputObject"; value="kaw.netw2500.ca"

PS C:\Reports> Get-ADDomain >> ./FLReport.txt

>> ParameterBinding(Out-File): name="InputObject"; value="DC=kaw,DC=netw2500,DC=ca"

PS C:\Reports> notepad .\FLReport.txt

PS C:\Reports> notepad .\FLReport.txt

PS C:\Reports> Add-ADDSReadOnlyDomainControllerAccount -DomainControllerAccountName "RODC01A1U30" -DomainName "kaw.netw2500.ca" -SiteName Default-First-Site-Name -DelegatedAdministratorAccountName "RemoteOff\_gp"

WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

WARNING: Windows Server 2022 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

Message Context RebootRequired Status

------- ------- -------------- ------

Operation completed successfully DCPromo.General.1 False Success

PS C:\Reports> Stop-Transcript

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Windows PowerShell transcript end

End time: 20241017191412

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## Read-Only Domain Controller Screenshots:

A close up of a white background

Description automatically generated

*Before DC Role*

A close up of a computer

Description automatically generated

*After DC Role*

## C:\RODCtranscriptA3.txt:

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Windows PowerShell transcript start

Start time: 20241017152544

Username: RODC01A1U30\Administrator

RunAs User: RODC01A1U30\Administrator

Configuration Name:

Machine: RODC01A1U30 (Microsoft Windows NT 10.0.17763.0)

Host Application: powershell.exe

Process ID: 3796

PSVersion: 5.1.17763.6414

PSEdition: Desktop

PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17763.6414

BuildVersion: 10.0.17763.6414

CLRVersion: 4.0.30319.42000

WSManStackVersion: 3.0

PSRemotingProtocolVersion: 2.3

SerializationVersion: 1.1.0.1

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Transcript started, output file is C:\RODCtranscriptA3.txt

PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Success Restart Needed Exit Code Feature Result

------- -------------- --------- --------------

True No Success {Active Directory Domain Services, Group P...

PS C:\Users\Administrator> Install-ADDSDomainController -DomainName "kaw.netw2500.ca" -UseExistingAccount -Credential (Get-Credential) -NoRebootOnCompletion:$true

The target server will be configured as a domain controller. The server needs to be restarted manually when this operation is complete.

Do you want to continue with this operation?

&Yes Yes to &All &No No to A&ll &Suspend

Y

WARNING: This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

WARNING: This computer has at least one physical network adapter that does not have static IP address(es) assigned to its IP Properties. If both IPv4 and IPv6 are enabled for a network adapter, both IPv4 and IPv6 static IP addresses should be assigned to both IPv4 and IPv6 Properties of the physical network adapter. Such static IP address(es) assignment should be done to all the physical network adapters for reliable Domain Name System (DNS) operation.

Message Context RebootRequired Status

------- ------- -------------- ------

You must restart this computer to complete the operation... DCPromo.General.2 True Success

PS C:\Users\Administrator> Stop-Transcript

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Windows PowerShell transcript end

End time: 20241017152930

## RODC Password Replication Policy Screenshot:

A screenshot of a computer

Description automatically generated

# Task 2:

## RODC Connection Information Screenshot:

A screenshot of a computer

Description automatically generated

## Replication Settings Screenshot:

A screenshot of a computer screen

Description automatically generated

# Task 5:

## Question 1:

**What is a System State Backup and what is included in a System State Backup?**

A System State Backup is a backup that only holds the systems core OS files. It includes the Domain members, domain controllers, computers that run cluster services and computers that run certificate services. (Microsoft, n.d.)

**What is a Bare Metal Backup?**

A bare metal backup consists of ALL of the files on a machine, including the System State backup. This includes the User data a System State backup would not include. Bare metal meaning a computer with nothing installed on it at all, the idea is a bare metal backup can take a computer with nothing and restore it back to working order. (Microsoft, n.d.)

## Question 2:

**What are Volume Shadow Copies (VSS)?**

VSS is a feature within Windows that helps backup information while the applications may still be in use, like a Snapshot in VMWare (although our systems are turned off when we use this feature). VSS uses 3 main components, the requesters, the writers and the providers. These can come in many different forms, but essentially, the requester is the function or program that asks VSS for the backup, the writer points the data to the right spot and ensures data consistency, while the provider creates the shadow copies on the storage volumes. (Microsoft, n.d.)

# Documentation and Backups:

A screenshot of a computer

Description automatically generated

*DC01 Gold Copy*

A screenshot of a computer

Description automatically generated

*SD01 Gold Copy*

A screenshot of a computer

Description automatically generated

*MS01 Gold Copy*

# Bibliography

Microsoft. (n.d.). *Active Directory Domain Services functional levels*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels

Microsoft. (n.d.). *learn.microsoft.com*. Retrieved from Back up system state and bare metal: https://learn.microsoft.com/en-us/system-center/dpm/back-up-system-state-and-bare-metal?view=sc-dpm-2022&tabs=RestoreBMR

Microsoft. (n.d.). *Volume Shadow Copy Service (VSS)*. Retrieved from learn.microsoft.com: https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service