Imagen que contiene Diagrama

Descripción generada automáticamente

Indice

Contenido

[1](#_Toc170120867)

[Indice 2](#_Toc170120868)

[Deploying a Fault-Tolerant Microsoft Active Directory Environment 2](#_Toc170120869)

[**GSP118** 2](#_Toc170120870)

[Architecture 3](#_Toc170120871)

[**Task 1. Initializing common variables** 4](#_Toc170120872)

[**Task 2. Creating the network infrastructure** 5](#_Toc170120873)

[**Task 3. Creating the first domain controller** 8](#_Toc170120874)

[Copy and paste with the RDP client 10](#_Toc170120875)

[**Task 4. RDP into your instance** 11](#_Toc170120876)

[**Task 5. Creating the second domain controller** 21](#_Toc170120877)

[**Task 6. Testing the installation** 30](#_Toc170120878)

Deploying a Fault-Tolerant Microsoft Active Directory Environment

[Deploying a Fault-Tolerant Microsoft Active Directory Environment | Google Cloud Skills Boost](https://www.cloudskillsboost.google/focuses/1817?parent=catalog)

**GSP118**



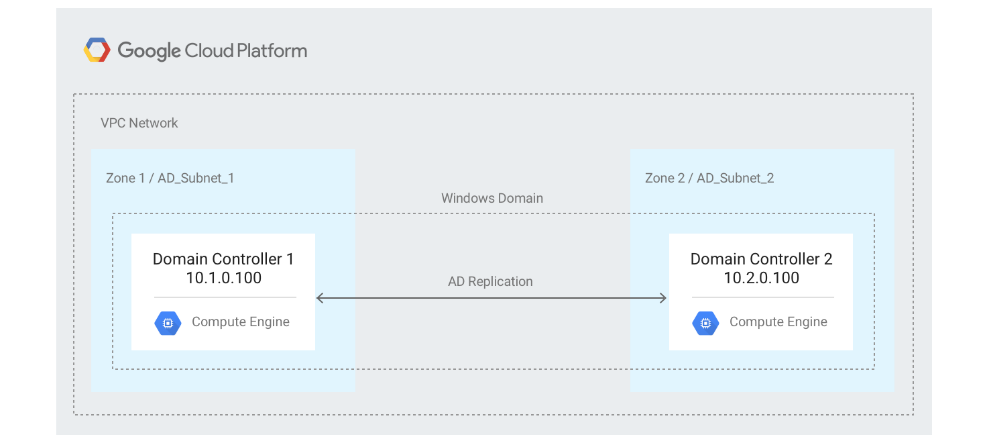
This lab is part of a series aimed at helping you deploy a highly available Windows architecture on Google Cloud with Microsoft Active Directory (AD), SQL Server, and Internet Information Services (IIS). In this lab you set up a redundant pair of Windows Domain Controllers (DC) with AD using a new Virtual Private Cloud (VPC) network and multiple subnets.

You can also use this lab to learn to set up an AD configuration for use in other architectures. Replicating a remote AD environment to the new Google Cloud-based AD environment will not be covered, although this is possible with Cloud VPN and additional AD configuration.

Objectives

* Create a custom mode VPC network with two subnets spanning two zones.
* Create Windows Server virtual instances and enable AD Domain Services.
* Configure a new domain with Active Directory.
* Join the new Windows Server instances to the new domain.
* Configure firewall rules to allow traffic to the virtual machines.
* Test the configuration.

Architecture



**Task 1. Initializing common variables**

You must define several variables that control where elements of the infrastructure are deployed.

1. Run the following script to define the environment variables for your project:

export region1="Region 1"

export region2="Region 2"

export zone\_1="Zone 1"

export zone\_2="Zone 2"

export vpc\_name=webappnet

export project\_id=$(gcloud config get-value project)

Captura de pantalla de computadora

Descripción generada automáticamente

1. Run the following to set the region to Region 1 :

gcloud config set compute/region ${region1}

1. Click **Authorize** when prompted.

Captura de pantalla de un celular con texto e imagen

Descripción generada automáticamente

**Task 2. Creating the network infrastructure**

After you've defined the infrastructure variables, create the network and subnets that AD will use.

1. In Cloud Shell, run the following command to create the VPC network:

gcloud compute networks create ${vpc\_name} \

--description "VPC network to deploy Active Directory" \

--subnet-mode custom

Una captura de pantalla de una computadora

Descripción generada automáticamente con confianza media

1. The following warning can be ignored. You'll create firewall rules in later steps.

**Note:**Instances on this network will not be reachable until firewall rules are created.

1. Add two subnets to the VPC network:

gcloud compute networks subnets create private-ad-zone-1 \

--network ${vpc\_name} \

--range 10.1.0.0/24 \

--region ${region1}

Texto

Descripción generada automáticamente

gcloud compute networks subnets create private-ad-zone-2 \

--network ${vpc\_name} \

--range 10.2.0.0/24 \

--region ${region2}

Texto

Descripción generada automáticamente

1. Create an internal firewall rule to allow traffic between subnets:

gcloud compute firewall-rules create allow-internal-ports-private-ad \

--network ${vpc\_name} \

--allow tcp:1-65535,udp:1-65535,icmp \

--source-ranges 10.1.0.0/24,10.2.0.0/24

**Note:**In a production environment, it's a best practice to secure all the ports that your systems are not actively using and to secure access to your machines using a [bastion host](https://cloud.google.com/solutions/connecting-securely#bastion).

Texto

Descripción generada automáticamente

1. Create a firewall rule to allow an RDP connection on port 3389 from any location:

gcloud compute firewall-rules create allow-rdp \

--network ${vpc\_name} \

--allow tcp:3389 \

--source-ranges 0.0.0.0/0

Texto

Descripción generada automáticamente

Click *Check my progress* to verify the objective.

|  |
| --- |
| Creating the network infrastructure  Check my progress |

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

**Task 3. Creating the first domain controller**

Next you'll create a domain controller that has the following properties:

* Name: ad-dc1
* IP Address: 10.1.0.100

1. Create a Compute Engine instance of Windows Server 2016 to use as the first domain controller:

gcloud compute instances create ad-dc1 --machine-type e2-standard-2 \

--boot-disk-type pd-ssd \

--boot-disk-size 50GB \

--image-family windows-2016 --image-project windows-cloud \

--network ${vpc\_name} \

--zone ${zone\_1} --subnet private-ad-zone-1 \

--private-network-ip=10.1.0.100

**Note:**In a production environment you can increase the boot disk size based on your expected needs.

Texto

Descripción generada automáticamente

Click *Check my progress* to verify the objective.

|  |
| --- |
| Creating the first domain controller  Check my progress |

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Wait approximately one minute, and then create a password for ad-dc1 by running the following command. Save the ip-address, username and password returned in Cloud Shell and label it for Domain Controller 1, they will be used in later steps:

gcloud compute reset-windows-password ad-dc1 --zone ${zone\_1} --quiet --user=admin

**Note:**If the instance is not ready to accept the request, you'll receive the following error message:

ERROR: (gcloud.compute.reset-windows-password) The instance may not be ready for use. This can occur if the instance was recently created or if the instance is not running Windows. Please wait a few minutes and try again.

If so, just retry the command.

**Con esto conseguimos que nos devuelva la dirección IP, el nombre de usuario y contraseña del Controlador de dominio 1**

Texto

Descripción generada automáticamente

Copy and paste with the RDP client

Once you are securely logged into your instance, you may find yourself copying and pasting commands from the lab manual.

To paste, hold the **CTRL-V** keys (if you are a Mac user, using **CMND-V** will not work.) If you are in a Powershell window, be sure that you have clicked into the window or else the paste shortcut won't work.

If you are pasting into putty, **right click**.

**Task 4. RDP into your instance**

Use RDP to connect to the domain controller instance with the credentials you created in the previous step.

1. From the **Navigation menu**, go to **Compute Engine** > **VM Instances**.
2. Click ad-dc1 to open the VM instance Details page for the first AD machine.

Interfaz de usuario gráfica, Texto, Aplicación, Word

Descripción generada automáticamente

1. Click **RDP** to open an RDP session to this instance.

* Depending on the system you are using you may need to install a third party RDP client or install the Chrome RDP plug-in in order to connect.
* Connect using the ip-address, username and password you saved when you set the local windows user account password.
* If you download the RDP file to connect you will need to change the username used to make the connection to the username you saved in the previous section.

**On Windows systems:**

1. Download and then open the RDP file.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click **Connect**. The connection will fail as the default username is incorrect.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Si intentaramos iniciar session con estas credenciales nos daría error ya que no es el nombre de usuario ni contraseña correcto.**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Click **More Choices**.
2. Click **Use a different account**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Enter the username and password you saved at the beginning of this section and then click **OK** to log in.

**Usamos las credenciales correctas, sacadas anteriormente en cloud shell.**

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. When you see a security warning dialog stating that the identity of the remote computer cannot be verified click **Yes**.
2. When the initial RDP connection to the Windows machine opens click **Yes** to make this machine discoverable.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Open a PowerShell terminal as Administrator. (Click in the search box on the task-bar, type "PowerShell", and then with Windows PowerShell selected, press **Shift-Ctrl-Enter**.)

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. When prompted to allow this application to make changes to your device click **Yes**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Set the Windows credentials for the Administrator account:

net user Administrator \*

1. You're prompted to create a password. Use a strong password, and store the password in safe location for future use. Even though this is a lab, you must follow the password creation rules.

Interfaz de usuario gráfica

Descripción generada automáticamente

The Administrator account will become a domain admin account after you've created the [AD forest](https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx) with it.

1. Enable the account:

net user Administrator /active:yes

Texto

Descripción generada automáticamente

1. Install Active Directory Domain Services, including Management Tools:

Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Texto

Descripción generada automáticamente

1. Set the following PowerShell variables:

$DomainName = "example-gcp.com"

$DomainMode = "7"

$ForestMode = "7"

$DatabasePath = "C:\Windows\NTDS"

$SysvolPath = "C:\Windows\SYSVOL"

$LogPath = "C:\Logs"

Texto

Descripción generada automáticamente

1. Install the new Active Directory forest configuration in Windows Server 2016 mode:

Install-ADDSForest -CreateDnsDelegation:$false `

-DatabasePath $DatabasePath `

-LogPath $LogPath `

-SysvolPath $SysvolPath `

-DomainName $DomainName `

-DomainMode $DomainMode `

-ForestMode $ForestMode `

-InstallDNS:$true `

-NoRebootOnCompletion:$true `

-Force:$true

1. When you're prompted, enter a Safe Mode Administrator password. Store the password in a safe location for future use.
2. Dismiss the following warnings. Each warning will appear two times, once during prerequisites verification and a second time during the installation process.

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

WARNING: Windows Server 2016 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.

Learn more about this setting from Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

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: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "example-gcp.com".

Otherwise, no action is required.

1. Restart the virtual machine:

Restart-Computer

This will disconnect your RDP session. The machine will now take about a minute to restart.

1. Once it has restarted use RDP to connect to the domain controller ad-dc1 with the Administrator credentials you defined during the AD forest installation.
   * Remember to add the domain name as a prefix, as in EXAMPLE-GCP\Administrator.
   * The initial log-in to the domain may take a few minutes as services such as group policies are initialized for the first time.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Note:**If you are using the Chrome RDP client, you might receive the following warning about the certificate. Follow the instructions to connect:

WARNING Someone could be trying to intercept your communication. To connect anyway select Chrome RDP Options, select the Certificates tab, select the :3389 certificate listing and press the Delete Certificate button.

If you are using a built in Windows RDP client or a third party RDP client you will have to confirm that you accept the new certificate in order to connect.

1. Open a PowerShell terminal as Administrator and set the following variables:

$DNS1 = "10.2.0.100"

$DNS2 = "127.0.0.1"

$LocalStaticIp = "10.1.0.100"

$DefaultGateway = "10.1.0.1"

Texto

Descripción generada automáticamente

1. Set the IP address and default gateway:

netsh interface ip set address name=Ethernet static `

$LocalStaticIp 255.255.255.0 $DefaultGateway 1

Texto

Descripción generada automáticamente

**Note:** RDP might lose connectivity for a few seconds or require you to reconnect.

1. Configure the primary DNS server:

netsh interface ip set dns Ethernet static $DNS1

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

1. DNS server ad-dc2 will be available only after the second domain controller is deployed, so you can ignore the following error message:

The configured DNS server is incorrect or does not exist.

**Note:**You'll configure the DNS servers after the AD forest installation. Installing the forest overwrites the post-installation values with the IP addresses of the domain controllers ad-dc1 and ad-dc2. You'll set up the ad-dc2 domain controller later in this lab.

1. Configure the secondary DNS server:

netsh interface ip add dns Ethernet $DNS2 index=2

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

1. The DNS server entry for this domain controller, ad-dc1, should be second in the list in order to prevent AD from frequently losing connection with the other controller. Use the second domain controller, ad-dc2, as the primary DNS server.

You'll create the ad-dc2 domain controller in the next section. If you don't follow this pattern, the following errors appear under **Server Manager** > **Active Directory Domain Services**:

The DFS Replication service failed to update configuration in Active

Directory Domain Services. The service will retry this operation

periodically.

You might see errors on the ad-dc1 server before both servers are fully configured. You can ignore these errors.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

**Task 5. Creating the second domain controller**

Next you'll create a domain controller that has the following properties:

* Name: ad-dc2
* IP Address: 10.2.0.100

1. If your Cloud Shell window has expired, open a new Cloud Shell instance and reset the variables you set earlier. To do that, edit the following script to specify the project ID and region you used earlier:

export region2="Region 2"

export zone\_2="Zone 2"

export vpc\_name=webappnet

export project\_id=$(gcloud config get-value project)

gcloud config set compute/region ${region2}

Texto

Descripción generada automáticamente

1. Copy the script into your Cloud Shell window and run it.
2. Use Cloud Shell to create the second domain controller instance:

gcloud compute instances create ad-dc2 --machine-type e2-standard-2 \

--boot-disk-size 50GB \

--boot-disk-type pd-ssd \

--image-family windows-2016 --image-project windows-cloud \

--can-ip-forward \

--network ${vpc\_name} \

--zone ${zone\_2} \

--subnet private-ad-zone-2 \

--private-network-ip=10.2.0.100

Texto

Descripción generada automáticamente

Click *Check my progress* to verify the objective.

|  |
| --- |
| Creating the second domain controller  Check my progress |

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

1. Wait approximately one minute, and then create a password for the Windows instance ad-dc2:

gcloud compute reset-windows-password ad-dc2 --zone ${zone\_2} --quiet --user=admin

**Con este commando conseguimos la dirección IP, el nombre de usuario y la contraseña del controlador de dominio 2 recientemente creado.**

Texto

Descripción generada automáticamente

1. You will need to use the username and password to RDP into the Windows instance you created. Save the IP address, username and password, and label them for Domain Controller 2.
2. On the Google Cloud console.
3. Open **Compute Engine** > **VM Instances**.
4. Click **ad-dc2** to open the VM instance Details page for the second ad machine.
5. Click **RDP** to open an RDP session to this instance.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

**Note:**Depending on the system you are using you may need to install a third party RDP client or install the Chrome RDP plug-in in order to connect.

If you download the RDP file to connect you will need to change the username used to make the connection to the username you saved in the previous section.

If you are using a third party RDP client connect using the ip-address, username and password you saved when you set the local windows user account password.

1. When the initial connection to the Windows machine opens, click **Yes** to make this machine discoverable.

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza baja

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. Open a PowerShell terminal as Administrator. (Click **Start**, type **PowerShell**, and then press **Shift-Ctrl-Enter**.)
2. When prompted to allow this application to make changes to your device click **Yes**.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

1. Install Active Directory Domain Services, including Management Tools:

Install-WindowsFeature -Name AD-Domain-Services -IncludeManagementTools

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

1. Set the following PowerShell variables:

$DomainName = "example-gcp.com"

$DNS1 = "10.1.0.100"

$DNS2 = "127.0.0.1"

$LocalStaticIp = "10.2.0.100"

$DefaultGateway = "10.2.0.1"

$DatabasePath = "C:\Windows\NTDS"

$SysvolPath = "C:\Windows\SYSVOL"

$LogPath = "C:\Logs"

Texto

Descripción generada automáticamente

1. Configure the primary DNS server:

netsh interface ip set dns Ethernet static $DNS1

Texto

Descripción generada automáticamente

1. Configure the second server so that it acts as its own secondary DNS server:

netsh interface ip add dns Ethernet $DNS2 index=2

Imagen que contiene Interfaz de usuario gráfica

Descripción generada automáticamente

The ad-dc2 DNS server will be available only after ad-dc2 is joined to the domain as a domain controller. Because the server hasn't been joined yet, you see the following message, but you can ignore it:

The configured DNS server is incorrect or does not exist.

1. Set the IP address and default gateway:

netsh interface ip set address name=Ethernet static `

$LocalStaticIp 255.255.255.0 $DefaultGateway 1

Texto

Descripción generada automáticamente

**Note:** RDP might lose connectivity for a few seconds or require you to reconnect.

1. Run the following PowerShell script, which will let you know when the first domain controller becomes operational. Wait until you see the Domain controller is reachable message.

$DomainIsReady=$False

For ($i=0; $i -le 30; $i++) {

nltest /dsgetdc:example-gcp.com

if($LASTEXITCODE -ne 0) {

Write-Host "Domain not ready, wait 1 more minute, then retry"

Start-Sleep -s 60

}

else {

$DomainIsReady=$True

Write-Host "Domain controller is reachable"

break

}

}

if($DomainIsReady -eq $False) {

Write-Host "Domain not ready. Check if it was deployed ok"

}

Texto

Descripción generada automáticamente

1. Set the following PowerShell variable again:

$DomainName = "example-gcp.com"



1. Add the virtual machine to the forest as a second domain controller:

Install-ADDSDomainController `

-Credential (Get-Credential "EXAMPLE-GCP\Administrator") `

-CreateDnsDelegation:$false `

-DatabasePath $DatabasePath `

-DomainName $DomainName `

-InstallDns:$true `

-LogPath $LogPath `

-SysvolPath $SysvolPath `

-NoGlobalCatalog:$false `

-SiteName 'Default-First-Site-Name' `

-NoRebootOnCompletion:$true `

-Force:$true

1. When you're prompted to provide a password for the Administrator account, use the Administrator credentials you defined during AD forest installation. Add the domain name as a prefix, as in EXAMPLE-GCP\Administrator.

Captura de pantalla de un celular

Descripción generada automáticamente

1. When you're prompted to enter a Safe Mode Administrator password, use the same password you used for the first domain controller.

Texto

Descripción generada automáticamente

1. Ignore the following warnings. Each warning appears twice: once during prerequisites verification, and a second time during the installation process.

WARNING: Windows Server 2016 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: A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "example-gcp.com". Otherwise, no action is required.

1. Restart the virtual machine:

Restart-Computer

**Task 6. Testing the installation**

1. Wait 5-10 minutes to make sure that both domain controllers are operational and are replicating information.
2. Using RDP, re-connect to the first domain controller instance using the Administrator credentials you defined during the first domain controller installation. Add the domain name as a prefix, as in EXAMPLE-GCP\Administrator.

Accedemos con el controlador de dominio\Administrador con su correspondiente contraseña.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

1. Once you are connected to the RDP session open a PowerShell console as Administrator if one is not already running.
2. Test that replication is working by running the following command in the PowerShell console:

repadmin /replsum

**Note:**Learn more about replication and topology management in AD from the [Replication and Metadata documentation](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/powershell/advanced-active-directory-replication-and-topology-management-using-windows-powershell--level-200-#BKMK_Repl).

1. The output should resemble the following, with no errors or failures.
2. If the domain controller is not available, you receive a message that resembles the following:

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

....

Source DSA largest delta fails/total %% error

Destination DSA largest delta fails/total %% error

1. If you receive this message, wait a couple of minutes and then retry the repadmin /replsum command.

Esto puede tardar de 5 a 10 minutos