

Deploying a Fault-Tolerant Microsoft Active Directory Environment

GSP118



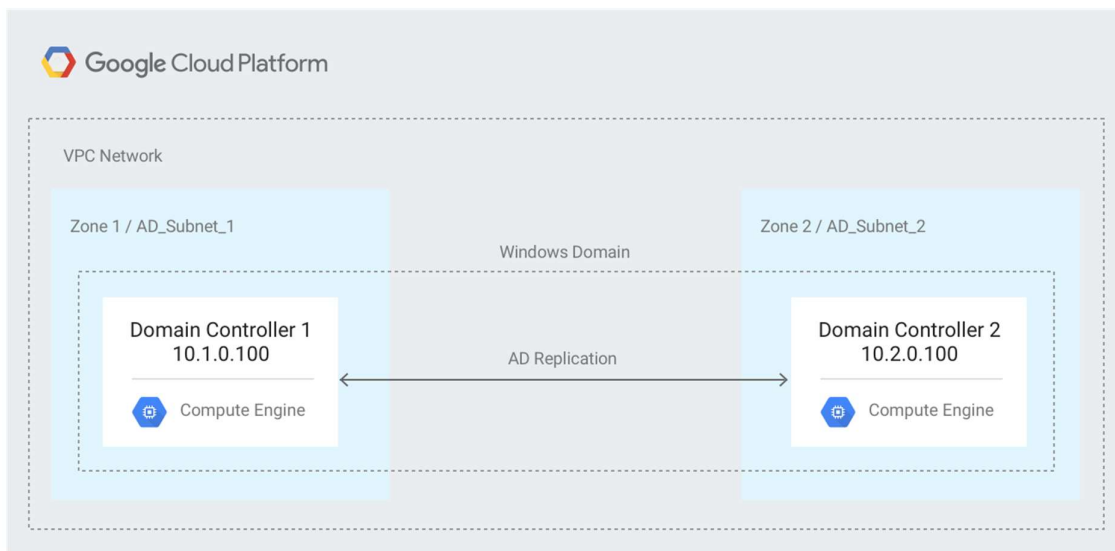
This lab is part of a series aimed at helping you deploy a highly available Windows architecture on Google Cloud with Microsoft Active Directory (AD), SQL Server, and Internet Information Services (IIS). In this lab you set up a redundant pair of Windows Domain Controllers (DC) with AD using a new Virtual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



Setup and Requirements

Before you click the Start Lab button

Read these instructions. Labs are timed and you cannot pause them. The timer, which starts when you click **Start Lab**, shows how long Google Cloud resources will be made available to you.

This Qwiklabs hands-on lab lets you do the lab activities yourself in a real cloud environment, not in a simulation or demo environment. It does so by giving you new, temporary credentials that you use to sign in and access Google Cloud for the duration of the lab.

What you need

To complete this lab, you need:

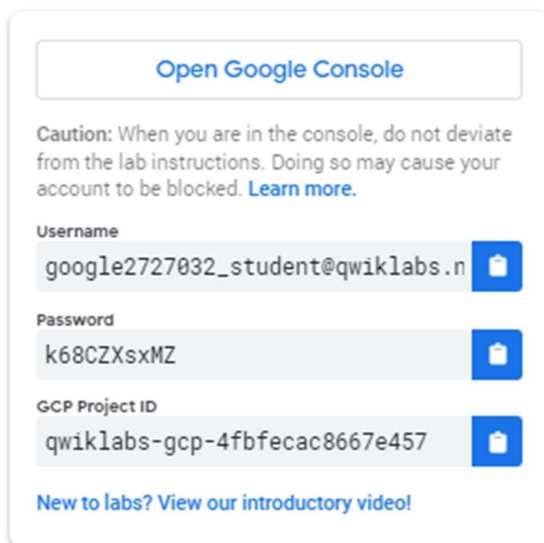
- Access to a standard internet browser (Chrome browser recommended).
- Time to complete the lab.

Note: If you already have your own personal Google Cloud account or project, do not use it for this lab.

Note: If you are using a Pixelbook, open an Incognito window to run this lab.

How to start your lab and sign in to the Google Cloud Console

1. Click the **Start Lab** button. If you need to pay for the lab, a pop-up opens for you to select your payment method. On the left is a panel populated with the temporary credentials that you must use for this lab.



The screenshot shows a panel with the following content:

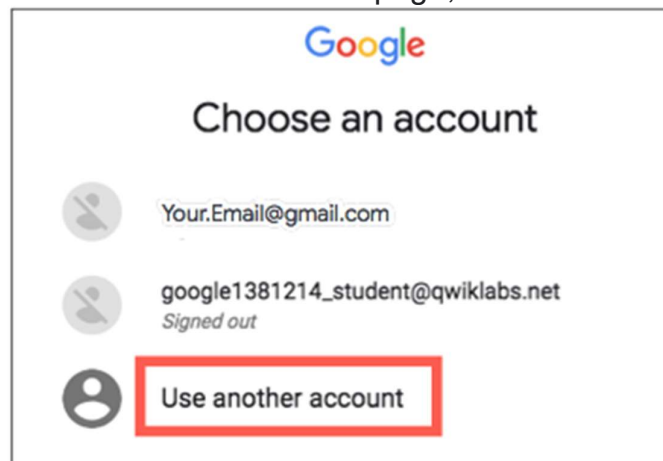
- A button at the top labeled "Open Google Console".
- A caution message: "Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more.](#)"
- Three input fields, each with a copy icon to its right:
 - Username: google2727032_student@qwiklabs.n
 - Password: k68CZXsxMZ
 - GCP Project ID: qwiklabs-gcp-4fbfecac8667e457
- A link at the bottom: "New to labs? View our introductory video!"

2. Copy the username, and then click **Open Google Console**. The lab spins up resources, and then opens another tab that shows the **Sign in** page.



Tip: Open the tabs in separate windows, side-by-side.

If you see the **Choose an account** page, click **Use Another**



Account.

3. In the **Sign in** page, paste the username that you copied from the Connection Details panel. Then copy and paste the password.

Important: You must use the credentials from the Connection Details panel. Do not use your Qwiklabs credentials. If you have your own Google Cloud account, do not use it for this lab (avoids incurring charges).

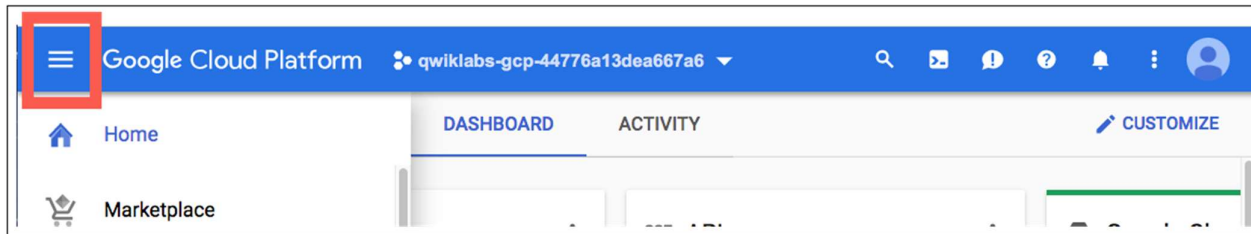
4. Click through the subsequent pages:

- Accept the terms and conditions.
- Do not add recovery options or two-factor authentication (because this is a temporary account).
- Do not sign up for free trials.

After a few moments, the Cloud Console opens in this tab.

Note: You can view the menu with a list of Google Cloud Products and Services by clicking the **Navigation menu** at the top-

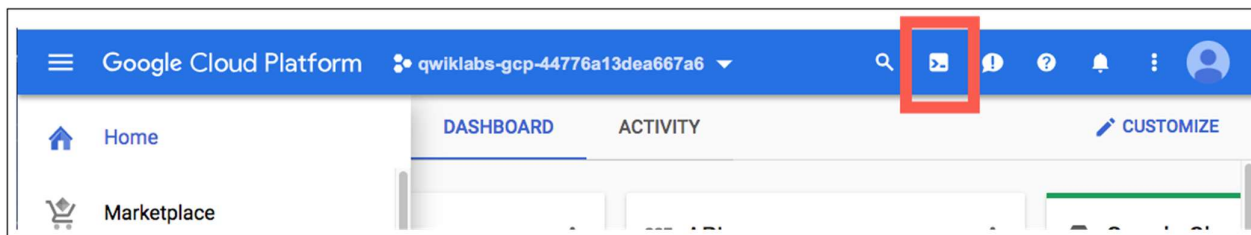
left.



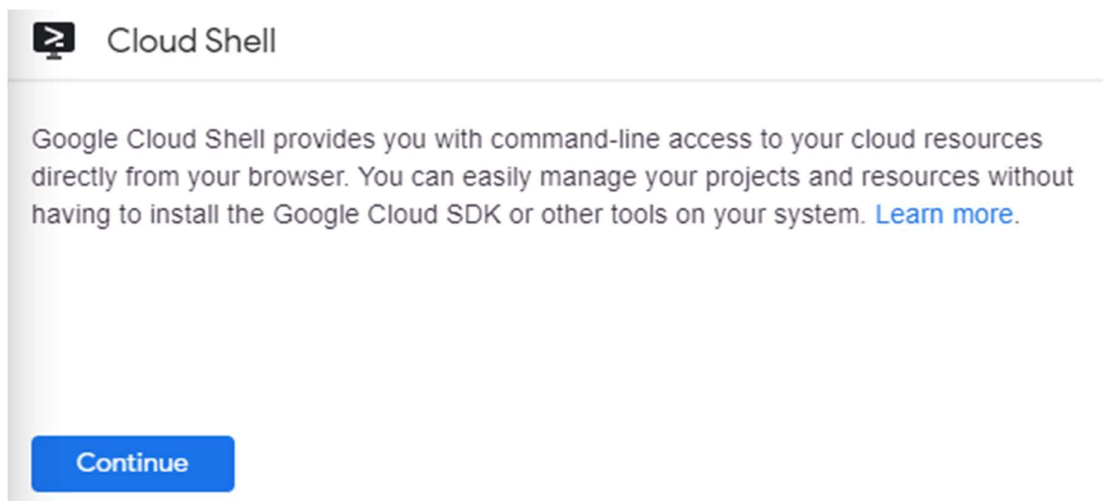
Activate Cloud Shell

Cloud Shell is a virtual machine that is loaded with development tools. It offers a persistent 5GB home directory and runs on the Google Cloud. Cloud Shell provides command-line access to your Google Cloud resources.

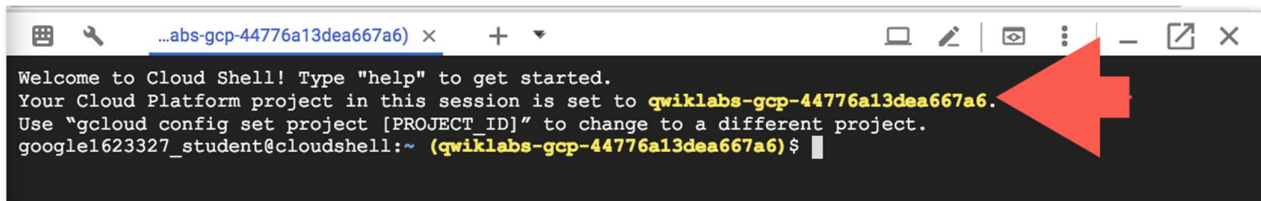
In the Cloud Console, in the top right toolbar, click the **Activate Cloud Shell** button.



Click **Continue**.



It takes a few moments to provision and connect to the environment. When you are connected, you are already authenticated, and the project is set to your *PROJECT_ID*. For example:



```
...abs-gcp-44776a13dea667a6) x + ▾
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to qwiklabs-gcp-44776a13dea667a6.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
google1623327_student@cloudshell:~ (qwiklabs-gcp-44776a13dea667a6) $
```

`gcloud` is the command-line tool for Google Cloud. It comes pre-installed on Cloud Shell and supports tab-completion.

You can list the active account name with this command:

```
gcloud auth list
```

(Output)

```
Credentialed accounts:
- <myaccount>@<mydomain>.com (active)
```

(Example output)

```
Credentialed accounts:
- google1623327_student@qwiklabs.net
```

You can list the project ID with this command:

```
gcloud config list project
```

(Output)

```
[core]
project = <project ID>
```

(Example output)

```
[core]
project = qwiklabs-gcp-44776a13dea667a6
```

For full documentation of `gcloud` see the [gcloud command-line tool overview](#).

Initializing common variables

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

Run the following script:

```
export region1=us-central1
export region2=us-east1
export zone_1=${region1}-b
export zone_2=${region2}-c
export vpc_name=webappnet
export project_id=$(gcloud config get-value project)

gcloud config set compute/region ${region1}
```

The script sets the region to `us-central1`. If you make any changes to the script, make sure that the zone values reference the region you specify.

Creating the network infrastructure

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

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
```

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

```
Instances on this network will not be reachable until firewall rules
are created.
```

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}

gcloud compute networks subnets create private-ad-zone-2 \
  --network ${vpc_name} \
  --range 10.2.0.0/24 \
  --region ${region2}
```

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](#).

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
```

Click *Check my progress* to verify the objective.

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

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

```
gcloud compute instances create ad-dc1 --machine-type n1-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.

Click *Check my progress* to verify the objective.

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.

Copy and pasting with the RDP client

Once you are securely logged in to 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 in to the window or else the paste shortcut won't work.

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

RDP into your instance

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

In the Google Cloud console, go to **Compute Engine > VM Instances**.

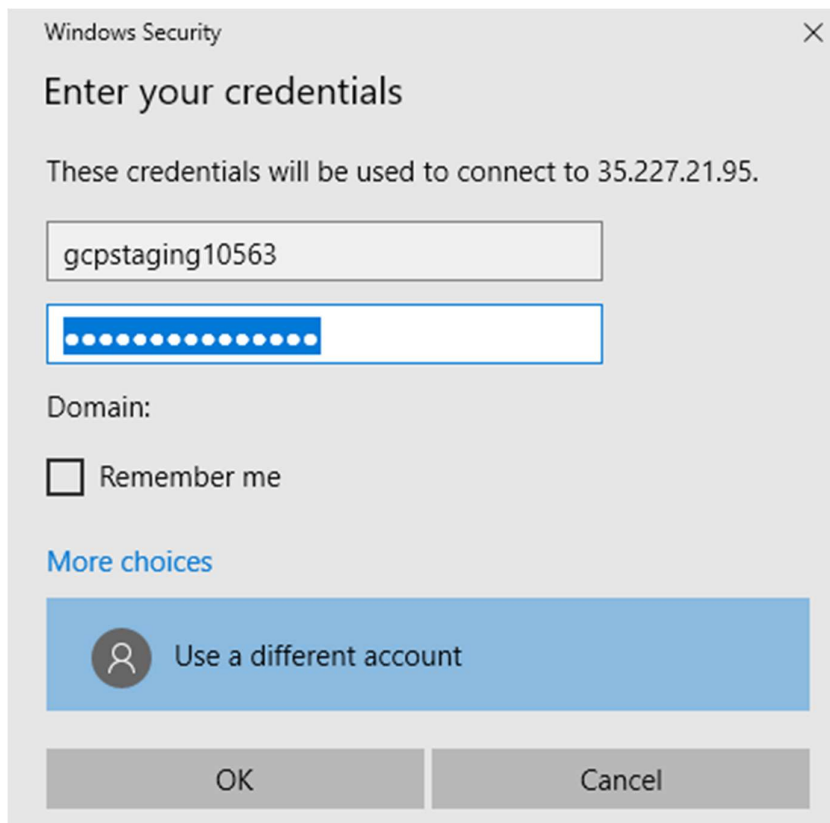
Click `ad-dc1` to open the VM instance Details page for the first AD machine.

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.
2. Click **Connect**. The connection will fail as the default username is incorrect.
3. Click **More Choices**.
4. Click **Use a different account**.
5. Enter the username and password you saved at the beginning of this section and then click **OK** to log in.



6. When you see a security warning dialog stating that the identity of the remote computer cannot be verified click **Yes**.

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

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**.)

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

Set the Windows credentials for the Administrator account:

```
net user Administrator *
```

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.

The Administrator account will become a domain admin account after you've created the [AD forest](#) with it.

Enable the account:

```
net user Administrator /active:yes
```

Install Active Directory Domain Services, including Management Tools:

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

Set the following PowerShell variables:

```
$DomainName = "example-gcp.com"
$DomainMode = "7"
$ForestMode = "7"
$DatabasePath = "C:\Windows\NTDS"
$SysvolPath = "C:\Windows\SYSVOL"
$LogPath = "C:\Logs"
```

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
```

When you're prompted, enter a Safe Mode Administrator password. Store the password in a safe location for future use.

Dismiss the following warnings. Each warning will appear two times, 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: 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.
```

Restart the virtual machine:

```
Restart-Computer
```

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

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.

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"
```

Set the IP address and default gateway:

```
netsh interface ip set address name=Ethernet static `
    $LocalStaticIp 255.255.255.0 $DefaultGateway 1
```

Note: RDP might lose connectivity for a few seconds or require you to reconnect. Configure the primary DNS server:

```
netsh interface ip set dns Ethernet static $DNS1
```

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.

Configure the secondary DNS server:

```
netsh interface ip add dns Ethernet $DNS2 index=2
```

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.

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

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=us-east1
export zone_2=${region2}-c
export vpc_name=webappnet
export project_id=$(gcloud config get-value project)
gcloud config set compute/region ${region2}
```

Copy the script into your Cloud Shell window and run it.

Use Cloud Shell to create the second domain controller instance::

```
gcloud compute instances create ad-dc2 --machine-type n1-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
```

Click *Check my progress* to verify the objective.

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
```

The username is the Qwiklabs student account username you used to log in to this lab. You will need to use the username and password to RDP into the Windows instance you created. Save the IP address, username and password, label them for Domain Controller 2.

Open the Google Cloud console.

Open **Compute Engine > VM Instances**.

Click **ad-dc2** to open the VM instance Details page for the second ad machine.

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.

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

Open a PowerShell terminal as Administrator. (Click **Start**, type **PowerShell**, and then press **Shift-Ctrl-Enter**.)

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

Install Active Directory Domain Services, including Management Tools:

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

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"
```

Configure the primary DNS server:

```
netsh interface ip set dns Ethernet static $DNS1
```

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

```
netsh interface ip add dns Ethernet $DNS2 index=2
```

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.
```

Set the IP address and default gateway:

```
netsh interface ip set address name=Ethernet static `
    $LocalStaticIp 255.255.255.0 $DefaultGateway 1
```

Note: RDP might lose connectivity for a few seconds or require you to reconnect. 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++) {
```

```

nlttest /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"
}
}

```

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

```

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-Google Cloud\Administrator.

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

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.

```

Restart the virtual machine:

```
Restart-Computer
```


Testing the installation

Wait 5-10 minutes to make sure that both domain controllers are operational and are replicating information.

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-Google Cloud\Administrator.

Once you are connected to the RDP session open a PowerShell console as Administrator if one is not already running.

Test that replication is working by running the following command in the PowerShell console.

```
repadmin /replsum
```

Note: For more information read about [replication and topology management in AD](#). The output should resemble the following, with no errors or failures.

```
PS C:\Users\administrator> repadmin /replsum
Replication Summary Start Time: 2017-09-08 20:15:55

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

Source DSA          largest delta    fails/total %%   error
AD-DC1              11m:11s        0 / 5           0
AD-DC2              10m:06s        0 / 5           0

Destination DSA     largest delta    fails/total %%   error
AD-DC1              10m:06s        0 / 5           0
AD-DC2              11m:11s        0 / 5           0
```

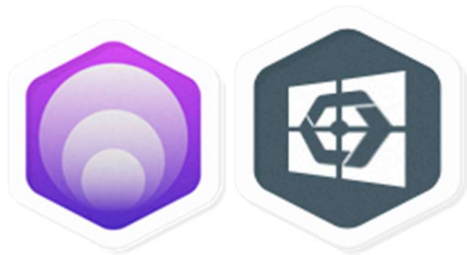
If the domain controller is not available, you receive a message that resembles the following:

```
Beginning data collection for replication summary, this may take awhile:
....
Source DSA          largest delta    fails/total %%   error
Destination DSA     largest delta    fails/total %%   error
```

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

Congratulations!

You have now successfully configured a Fault-Tolerant Microsoft Active Directory Environment.



Finish Your Quest

This self-paced lab is part of the Qwiklabs [Google Cloud Solutions I: Scaling Your Infrastructure](#) and [Windows on Google Cloud](#) Quests. A Quest is a series of related labs that form a learning path. Completing this Quest earns you the badge above, to recognize your achievement. You can make your badge (or badges) public and link to them in your online resume or social media account. Enroll in a Quest and get immediate completion credit if you've taken this lab. See [other available Qwiklabs Quests](#).

Take Your Next Lab

Continue your Quest with [Deploying Memcached on Container Engine](#), or check out these suggestions:

- [Running Dedicated Game Servers in Google Container Engine](#)

Next Steps / Learn More

Here are some follow-up steps :

- Review [Best Practices for Enterprise Organizations](#).

Google Cloud Training & Certification

...helps you make the most of Google Cloud technologies. [Our classes](#) include technical skills and best practices to help you get up to speed quickly and continue your learning

journey. We offer fundamental to advanced level training, with on-demand, live, and virtual options to suit your busy schedule. [Certifications](#) help you validate and prove your skill and expertise in Google Cloud technologies.

Manual Last Updated January 19, 2021

Lab Last Tested December 2, 2020

Copyright 2021 Google LLC All rights reserved. Google and the Google logo are trademarks of Google LLC. All other company and product names may be trademarks of the respective companies with which they are associated.