```
Set-AzureSubscription “Pay-As-You-Go” -CurrentStorageAccount
portalvhdsxgwgzn2ml54p5

# Set custom variables

$vmName = "CONTOSODC5"
$serviceName = "contosodc5"
$ipAddress = "10.0.0.8"
$firstDC = $false
$domainadmin = "contosodc1admin@ad.contoso.com"

# Set static variables

$compName = $serviceName + ".cloudapp.net"
$passwordsec = convertto-securestring "Passw0rd!" -asplaintext -force
$password = "Passw0rd!"
$username = $vmName + "admin"
$vnetName = "CONTOSO"
$subNet = "Subnet-1"
$location = "North Europe"

# Check availability of IP address and cloud service name

$IPtest = Test-AzureStaticVnetIP -VNetName $vnetName -IPAddress
$ipAddress
$cservices = Test-AzureName -service -name $serviceName

If(($cservices -eq $true) -or ($IPtest.IsAvailable -eq $false)) {
If ($cservices -eq $true) {
Write-Host "The cloud service name already exists" -foregroundcolor
yellow -backgroundcolor red }
If ($IPtest.IsAvailable -eq $false) {
Write-Host "The IP address is not available" -foregroundcolor yellow -
backgroundcolor red }
throw "An error occurred"
}

# Get the name of the latest image
$images = Get-AzureVMImage | where { $_.ImageFamily -eq “Windows
Server 2012 R2 Datacenter” } | Sort-Object -Descending -Property
PublishedDate

# Create a new VM with a static IP address
$newVM = New-AzureVMConfig -Name $vmName -InstanceSize “Medium” -
ImageName $images[0].ImageName -DiskLabel "OS" | Add-
AzureProvisioningConfig -Windows -Password $password -AdminUsername
$username -DisableAutomaticUpdates | Set-AzureSubnet -SubnetNames
$subNet | Set-AzureStaticVNetIP -IPAddress $ipAddress

New-AzureVM -ServiceName $serviceName -VMs $newVM -VNetName $vnetName
```

```
-Location $location -WaitForBoot

# Attach data disk for AD NTDS files

$myVM = Get-AzureVM -ServiceName $serviceName -Name $vmName
$myVM | Add-AzureDataDisk -CreateNew -DiskSizeInGB 120 -DiskLabel
"NTDS" -LUN 0 | Update-AzureVM

# Install the cert for the VM locally

$WinRMCertificateThumbprint = ($myVM | Select-Object -ExpandProperty
VM).DefaultWinRMCertificateThumbprint
(Get-AzureCertificate -ServiceName $serviceName -Thumbprint
$WinRMCertificateThumbprint -ThumbprintAlgorithm SHA1).Data | Out-File
"${env:TEMP}\cert.tmp"

$X509Object = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2
"$env:TEMP\cert.tmp"
$X509Store = New-Object
System.Security.Cryptography.X509Certificates.X509Store "Root",
"LocalMachine"
$X509Store.Open([System.Security.Cryptography.X509Certificates.OpenFla
gs]::ReadWrite)
$X509Store.Add($X509Object)
$X509Store.Close()

Remove-Item "$env:TEMP\cert.tmp"

# Get the port for PowerShell remoting

$ports = $myVM | Get-AzureEndpoint | where { $_.Name -eq
“WinRmHTTPs” }
$powerPort = $ports[0].port


# Create new PowerShell Remoting session

$cred = new-object -typename System.Management.Automation.PSCredential
-argumentlist $username,$passwordsec

$s = New-PSSession -ComputerName $compName -port $powerPort -
Credential $cred -UseSSL

# Initialize, partition and format disk

Invoke-Command -Session $s -ScriptBlock {

Get-Disk | where partitionstyle -eq 'raw' | Initialize-Disk -
PartitionStyle MBR -PassThru | New-Partition -AssignDriveLetter -
```

```
UseMaximumSize | Format-Volume -FileSystem NTFS -NewFileSystemLabel
"NTDS" -Confirm:$false

# Set AD install paths
$drive = get-volume | where { $_.FileSystemLabel -eq “NTDS” }
$NTDSpath = $drive.driveletter + ":\Windows\NTDS"
$SYSVOLpath = $drive.driveletter + ":\Windows\SYSVOL"

}

# Pass the $password variable to the remote machine, install the AD
Directory Services 'bits' and install the first DC in the forest

If ($firstDC -eq $true) {

Invoke-Command -Session $s -ArgumentList @($passwordsec) -ScriptBlock
{

Param (
$passwordsec )

write-host "Installing the first DC in the domain"
Install-WindowsFeature –Name AD-Domain-Services -
includemanagementtools
Install-ADDSForest -DatabasePath $NTDSpath -LogPath $NTDSpath -
SysvolPath $SYSVOLpath -DomainName "ad.contoso.com" -InstallDns -Force
-Confirm:$false -SafeModeAdministratorPassword $passwordsec

}

}

else

{

Invoke-Command -Session $s -ArgumentList @($passwordsec, $domainadmin)
-ScriptBlock {

Param (
$passwordsec, $domainadmin )

# Set domain admin credentials
$cred = new-object -typename System.Management.Automation.PSCredential
-argumentlist $domainadmin,$passwordsec

write-host "Installing additional domain controller"
Install-WindowsFeature –Name AD-Domain-Services -
includemanagementtools
Install-ADDSDomainController -Credential $cred -DatabasePath $NTDSpath
```

```
-LogPath $NTDSpath -SysvolPath $SYSVOLpath -DomainName
"ad.contoso.com" -InstallDns -Force -Confirm:$false -SiteName
"Default-First-Site-Name" -SafeModeAdministratorPassword $passwordsec

}

}

# Display the RDP connection string
$rdpPort = $myVM | Get-AzureEndpoint | where { $_.Name -eq “RDP” }
$rdpString = $servicename + ".cloudapp.net:" + $rdpPort.Port
write-host "Make a Remote Desktop connection to the VM using the URL
below:" -foregroundcolor yellow -backgroundcolor red
write-host $rdpString
```