ACLXRAY Lab deployment instructions

# What will be deployed to Azure IaaS

The deployment will create:

* VNET
* 2 Subnets
* 2 Network Security Groups
* Storage Account
* 4 VM
* Shutdown schedule for each VM
* Two forests
* File server attached to each forest
* Users in each forest
* Groups and memberships, including cross forest
* ACLs on OUs, folders and files
* Four accounts with SID history entries

# Deployment diagram



Deploying lab

## What you need

* Access to Azure Subscriotion with contributor role and ability to create and configure virtual networks.
* Following powershell modules.
  + Az
  + PSDscResources
  + ActiveDirectoryDsc
  + [VSCode editor](https://code.visualstudio.com/)(optional)

Using [Powershell 7](https://docs.microsoft.com/en-us/powershell/scripting/developer/module/installing-a-powershell-module?view=powershell-7) is highly recommended

Preparing to Deploy

* Unzip installation files into a local directory
* If running deployment for the first time open powershell terminal as administrator and install required modules

## Deploy Fist Instance of Lab

1. Open Powershell terminal or use previously opened terminal

2. Using powershell command navigate to the root of the directory containing source files

3. In the same terminal run Login-AzAccount and follow steps to log in to Azure

4. Run ./aclray.ps1 to deploy the lab with default settings and enter name of Resource Group, to be used for deployment, when prompted.

## Deploying secondary instances of the lab(advanced users only)

If you run into scenario multiple instances of the same lab or different versions of the lab needed, you can take advantage of the deployment customization parameters.

Detailed infomation about parameters can be found in the Appendix B.

You customize following settings in the lab:

* VM Size (default 'Standard\_B2s')
* Region (default 'eastus')
* Shutdown Time Zone – default is a current time zone of the user
* Shutdown Time (default '01:00' 24 hour time)
* Virtual Network Name (default 'ACLXRAYlabvnet')
* Container Name (default 'storageartifacts')

Example

In this example we will deploy ACLXRAY Lab into aletrnative region with aleternative Shutdown Time zone and alertnative virtual network name.

./aclxray.ps1 -RG myACLXRAYLAB -region westus -shutdownTimeZone 'Pacific Standard Time -vnetname VNET02

## Accessing Lab

Due to security concerns  VMs are no longer available via public IP addresses.  RDP access is protected by Network Security Group ACLXRAY-NSG . NSG rule will allow RDP access from your public IP address (collected at the time deployment sripts runs). If your public IP changes you will need to update NSG rule manually following instruction in the Appendix A

# Appendix

## Appendix A – Change your public IP address in the ACLXRAY-NSG

### Step 1 - Find out your current Public IP Address

You can use [What Is My IP? - Get Your Public IP address details - IPv4 - IPv6](https://www.whatismyip.com/) website or any other site you prefer.

### Step 2 – Open Network Security Group Configuration

Open Azure portal with the account you used to deploy ACLXRAY Lab.

In the resource search bar type ACLXRAY-NSG and select Network Security Group

Graphical user interface, text, application, Word

Description automatically generated

### Step 2 - Locate and “allow-rdp-in” inbound security rule

A screenshot of a computer

Description automatically generated with medium confidence

Step 4 – Update value in Source IP addresses/CIDRD ranges

Remove old value from the Source IP addresses/CIDRD ranges box and add Ip address you obtained in Step 1

Click Save at the top of the dialog. Once rule is updated, you will be able to connect to your lab servers via RDP

Graphical user interface, text, application, email

Description automatically generated

## Appendix B - ACLXRAY Lab  Deployment Script  Parameters

Documented parameters for the aclxray10.ps file

**-**vmsize

#### Description

Parameter specicifies size of each VMs in the deployment. Needs a value supported by Azure Compute configuration, to get a list of all supported size name, run followin Az powershell command:

Get-AzVMSize -Location <name of Azure Region where want to deploying this lab> | select Name

#### Properties

* Type: string
* Mandatory: YES
* Default Value: 'Standard\_B2s'

### -region

#### Description

Parameter specicifies name of the Azure region for the lab deployment. Need a value supported by Azure Resource Manager, to get list of all possible values, run following Az command:

Get-AzLocation | select Location,DisplayName

#### Properties

* Type: string
* Mandatory: YES
* Default Value: 'eastus'

### -RG

#### Description

Parameter specifies name of the resource group. Can be either existing group or name of a resource group you want to create as part of deployment.

**\*\*WARNING\*\*** If you select existing resource group, all previusly deployed ACLXRAY lab componenets will be overwritten.

#### Properties

* Type: string
* Mandatory: YES
* Default Value: NONE - value must be provided at each run

### -shutdownTimeZone

#### Description

Parameter specicifies name of the timezone for the shutdown schedule assigned to each VM. Uses standard Winodws OS Time Zone naming conventions. Complete list of all Time Zone Names can be found at Microsoft Support site https://support.microsoft.com/en-us/help/973627/microsoft-time-zone-index-values

#### Properties

* Type: string
* Mandatory: YES

### -shutDownTime

#### Description

Parameter specicifies time in 24 hour format, when shutdown schedule excutes VM shutdown

#### Properties

* Type: string
* Mandatory: YES
* Default Value: '01:00'

### -vnetname

#### Description

Parameter specifies name of the virtual network (VNET). Can be either existing VNET or name of a VNET you want to create as part of deployment.

**\*\*WARNING\*\*** If you select existing VNET name, all ACLXRAYLAB network related items will be reset to original configuration,  i.g if you converted one of the public IP addresses to static.

#### Properties

* Type: string
* Mandatory: YES
* Default Value: 'ACLXRAYlabvnet'

### -containerName

#### Description

Parameter specifies name of the storage container where DSC and custiom scripts will be uploded. Can be either existing container name or a new one.

#### Properties

* Type: string
* Mandatory: YES
* Default value: 'storageartifacts'