ACLXRAY Labdeploy instructions

In this repository you will find files nesssary for deploying ACLXray Lab.

# 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 to save costs

\* Azure Loadblancer with NAT tranlation for RDP

\* Public IP addresses for Load Balancer

\* Two forests

\* File server attached to each forest

\* Users in each forest

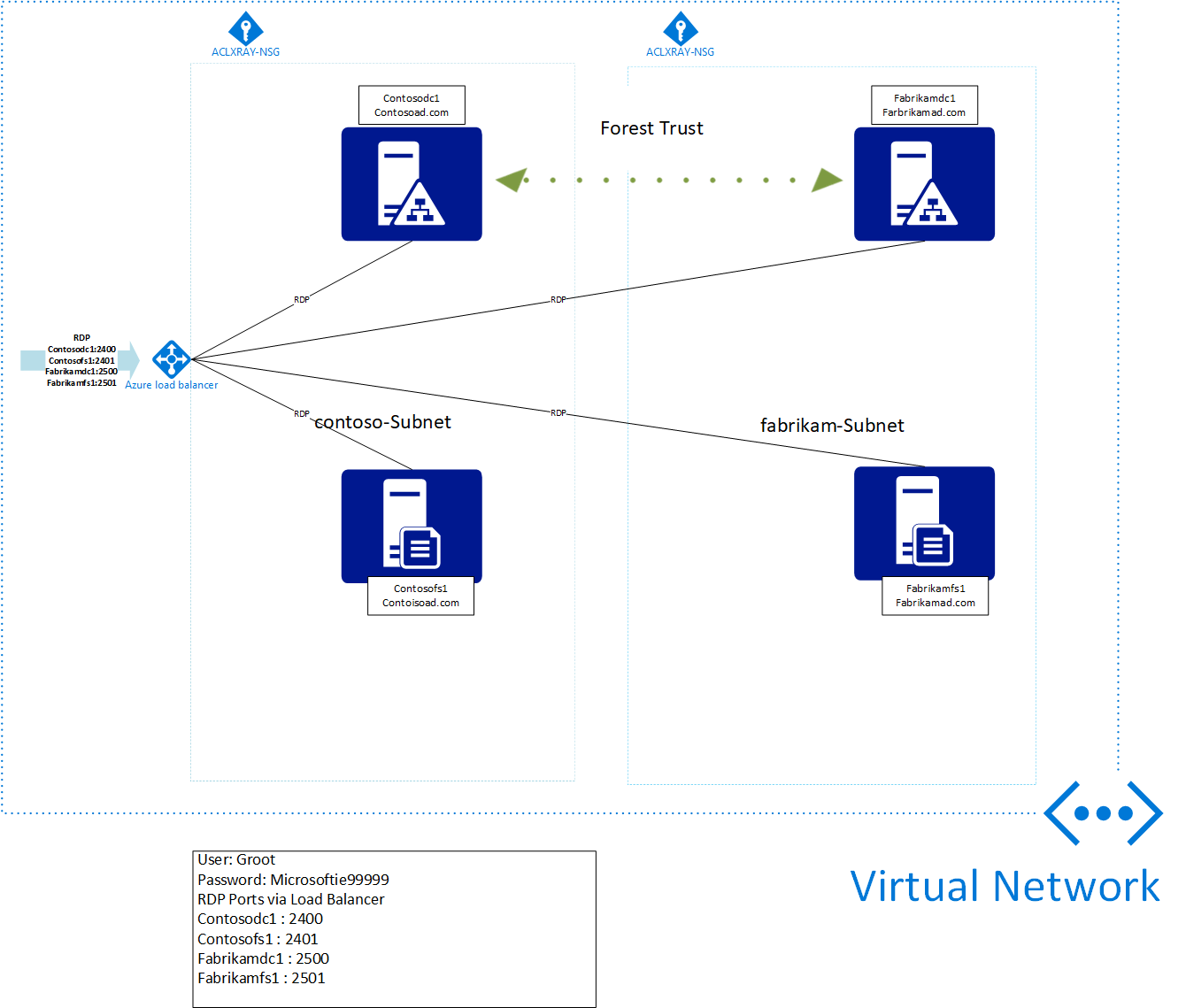
\* Randomly generated groups with random memberships

\* Random ACLs on OUs and files

\* Four accounts with SIM history entries

**\*\*WARNING\*\***: Because all groups and ACLs are created randomly, if you delete and re-deploy lab you will have diffirent settings. SupportFiles folder has two scripts that can help with creating disk snapshots of each VM and then creating a new lab VMs from snapshot if you want to roll back changes. Scripts are provided as is.

# 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 [installed](https://docs.microsoft.com/en-us/powershell/scripting/developer/module/installing-a-powershell-module?view=powershell-7) on your source system.

  \* Az

  \* PSDscResources

  \* ActiveDirectoryDsc

\* [VSCode editor](https://code.visualstudio.com/)(optional)

Prepare 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 Lab with default settings

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 ./aclray10.ps1 to deploy the lab with default settings and enter name of Resource Group, to be used for deployment, when prompted.

**### Deploy with custom settings**

Detailed ifomation about parameters can be  found in the section below

You customize following settings in the lab:

\* VM Size (default 'Standard\_B2s')

\* Region  (default 'eastus')

\* Shutdown Time Zone (default 'Eastern Standard Time')

\* 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.

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

## Accessing Lab

Due to security concerns and to save costs VMs are no longer assigned public IP addresss. Instead a public Loadblancer with NAT translation is created and each vm can be reached with RDP client using designated ports. Public Ip of the loadblancer will have randomly assigned DNS name which can be used to access VMs via RDP. There are two main ways to access servers via RDP

### Using aclxray script output

After script is finished running FQDN and ports for each VM will be printed in the terminal window. Copy and save these entries and use them with RDP client

### Using RDP connection script

In the terminal window, login to Azure and select subscription where your lab is running, navigate to SupportFile folder and execute "connect-aclxraylabServers.ps1" script. Script will guide you through the necessary steps and will open RDP window for you.

# Labdeploy Deployment 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

\* Default Value: 'Eastern Standard Time'

### -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'