AD Lab Setup

For the Amazon Web Services (AWS) Cloud

Document Version 2.0

Document Date: 1 May, 2018

Prerequisites:

If your AWS Account is new you *may* need to do the following:

- Remove VM Instance Limit (If your account is less than 72 hours old)
- Remove Auto Scale Instance Limit
- Remove aggregated EC2 EBS Volume limit.

These tasks are done here via AWS Support: https://aws.amazon.com/contact-us/

a) Create a new EC2 Key Pair (**NOTE:** ***Make sure you download the PEM file, and store it in a safe location, as once you close the window you are unable to recover the private key)***
   a. [EC2 Service] → Network & Security → Key Pairs

b) Determine how to set up your domain for AD Lab. (ADLab requires Active Directory Services)
   a. **Domain Option 1** – Connect to an existing Active Directory Domain (**Advanced Users**) (Contact your IT Department for Information.)

   b. **Domain Option 2** – Create a new domain, using EC2 (**Advanced Users**) (Contact your IT Department for information)|

   c. **Domain Option 3** – Simple AD Services inside of AWS. (**Template Default**) (Info: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_simple_ad.html)

c) Connection Options:
   a. VPN Set Up (**Advanced Users**) (Contact your IT Department for Information)

   b. DirectConnect to your new VPCs (**Advanced Users**) (Contact your IT Department for Information)

   c. Bastion Host/Jump Box – External IP (Elastic IP) address assigned by script (**Template Default**)

Deployment:

1. Create an AWS Account
2. Subscribe to the AWS Market Place (https://aws.amazon.com/marketplace/pp/prodview-abb2lieaqfqs4)

3. Continue to configuration
    a. Fulfillment Option → AccessData Lab
    b. Version: 1.0
    c. Select Region
    (**NOTE:** AccessData Lab may not be available in all regions, check with your sales representative for information as to where the software currently is available)
    (https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.RegionsAndAvailabilityZones.html)
    d. Continue to launch
    e. Action → Launch Cloud Formation

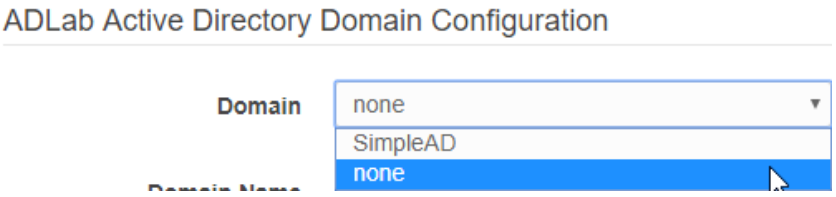
CloudFormation™ Configuration:

a. Select the Stack Name (example: adlab-mm-dd-yyyy)
b. Select Availability Zone(s)
(**Note:** If you use the default Simple AD inside of AWS you need to select two distinct Availability Zones inside the script; if you do not, the script will fail during the creation of the Active Directory)
c. Select your default IP Range (**Note:** The Script Default for the VPC is 10.0.0.0/16)
Note: Check with your IT Department for these ranges. The Default Cloud Formation Script uses a block of private IP spaces for the application.

Microsoft Active Directory Setup:

Select your preferred method of Active Directory deployment.

a. If you are joining an existing domain – select "None" in the drop down.



b. Active Directory Password: Can be any value you want. If you are joining an existing domain provide the password for the "Administrator@domain.local" user. **If your IT Department has disabled the 'Administrator' user, this will cause the script to fail as we look explicitly for that user to join the servers to the existing domain.**

ADLab EC2 Instance Configuration:

a. Key Pair: Select the EC2 Key Pair you will want to use here. You will need to have access to the corresponding PEM key here to decrypt logon passwords.
b. Instances: AccessData has tested specific instances and provide them as part of the template. If you prefer a instance type, please contact your sales representative
c. SQL Licensing Method:
    a. **BYOL:** You have a Microsoft SQL Server version **with software assurance** that allows you to use your SQL instance in a cloud environment.
    b. **AWS:** Selecting this option will spin up a server on the instance you select, **with Microsoft SQL Server installed**. This will increase the cost of your EC2 Database Instance

as there is an additional charge for Microsoft SQL Server provided by AWS. (Contact your IT Department for the best way to proceed)

ADLab AWS Storage Instance Configuration:

Note: All of these volumes are created as Elastic Block Storage Provisioned IOPS ssd with 10,000 IOPS. These are the highest performance SSD for throughput designed for latency sensitive transactional workloads. – Contact AccessData if you would like to use a different volume type.

AccessData has pre-populated the volume sizes with popular sizes for disks up to the 16 TB Volume limit for EBS Volumes. If you would like a different size, please contact your IT Department for how to attach volume(s) to your instances after the script has completed.

Incoming Network Access Information:

This can be any valid subnet in CIDR notation. The template default restricts the incoming network connections to the IP address to the host user who is launching the CloudFormation™ Template.

ADLab License Agreement:

You will be unable to proceed with the creation of the environment unless you accept the terms and conditions for the Software. (Link: https://accessdata.com/ADG_EULA)

Once the script has completed you should see the following:

- Seven (7) EC2 Virtual Servers

	Server Type	Notes
1	Bastion Host	Allows users to connect from external location(s)
2	AD Lab Client	Will need more instances or a Terminal Server
3	DPM Server	ADLab Data Processing Manager
4	Database Server	ADLab Microsoft SQL Server
5	DPE Server	AD Lab Data Processing Engine - Master Server of the AWS AutoScale Group created by the template.
6	AD Controller 1	(Not Shown as an EC2 Instance if using AWS SimpleAD)
7	AD Controller 2	(Not shown as an EC2 Instance if using AWS SimpleAD)

- 23 EBS Volumes of various sizes
    - Boot Volumes for the AD Lab Machines are all 128 GB in size.
    - Data Storage volumes are based off the variables you selected

---

To do after deployment is complete:

1. Logon to each server, and disable the Windows Firewall for the domain profile

2. Make sure you have created file shares on the 'Evidence' Volume and the 'Cases' Volume on the DPM Server.

3. Configure your local time/date settings for your locale (AWS EC2 Instances default to GMT)

4. Make sure the services on the DPM and all of your DPE Engines have been updated with the password you set in the Cloud Formation Template (SimpleAD) or with a user that your IT Department has been provided that can "Log on as a Service" on your domain.

5. Make sure your DPE(s) have the Attempt folder shared out with proper security permissions for your environment
   (Located at `C:\Ad\ADTemp` for non i3 instances. I3 Instances will have the AD Temp folder on their Z Drive after the NVME disk(s) are initialized)

6. Contact your Sales Representative for your virtual license keys for your environment (http://accessdata.com/about/contact-us)

7. Upload your Data to your environment to begin processing:
   a. Set up a VPN Connection to your VPC (**Advanced: Contact your IT Department**)
   b. Upload your evidence collection to an S3 Bucket, then download (**Slower**)
   c. Import your evidence using another service for large data transfers

Contact AccessData:

Sales:

Web: http://accessdata.com/about/contact-us

Telephone:

- **North American Customers: 1.800.574.5199**
- **International Customers: +44(0)20 7010 7800**
