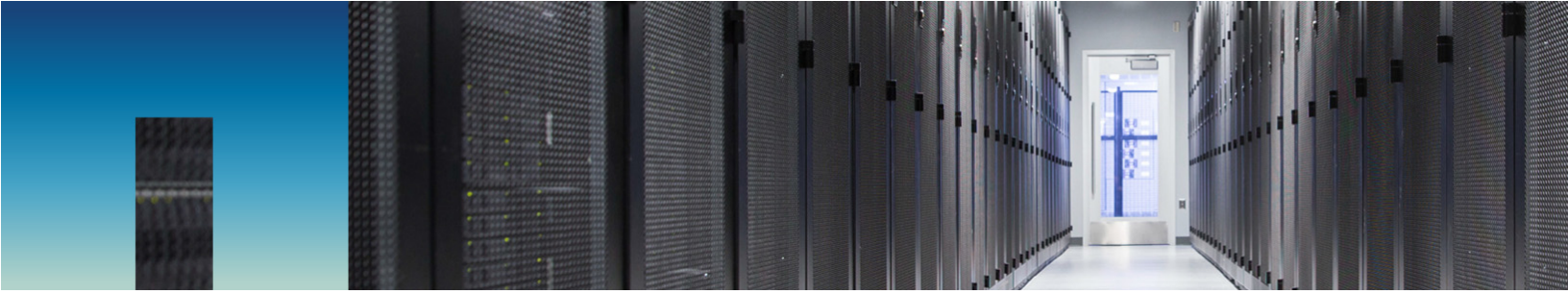


AWS Directory service setup with NetApp Cloud Volumes Service for AWS

Prabu Arjunan, NetApp
August 2019

Abstract

This document provides instructions to help users set up the AWS directory services environment for using NetApp® Cloud Volumes Service for Amazon Web Services (AWS).

NetApp®

TABLE OF CONTENTS

1 Overview

This document guides users through the required steps to integrate AWS directory services with NetApp Cloud Volumes for an AWS account.

2 Requirements

This section details the requirements to access Cloud Volumes Service for AWS.

Administrative

The following administrative tasks are required to access Cloud Volumes Service (CVS) for AWS:

- An active AWS account

  Note: The ID for the AWS account is sent to NetApp to enable access to Cloud Volumes Service for AWS in the AWS Marketplace.

- An active CVS account

Skills and Knowledge

The following skills and information are required to access Cloud Volumes Service for AWS:

- Access to and knowledge of AWS.
- Knowledge of your AWS active directory services and network settings.

  See Active Directory Design for guidelines and considerations.

Compute Resources

The following compute resources are required to access Cloud Volumes Service for AWS:

- A valid AWS account (with permissions to create AD directory services)

  Note: All AWS compute and other resources used are the sole responsibility of the user.

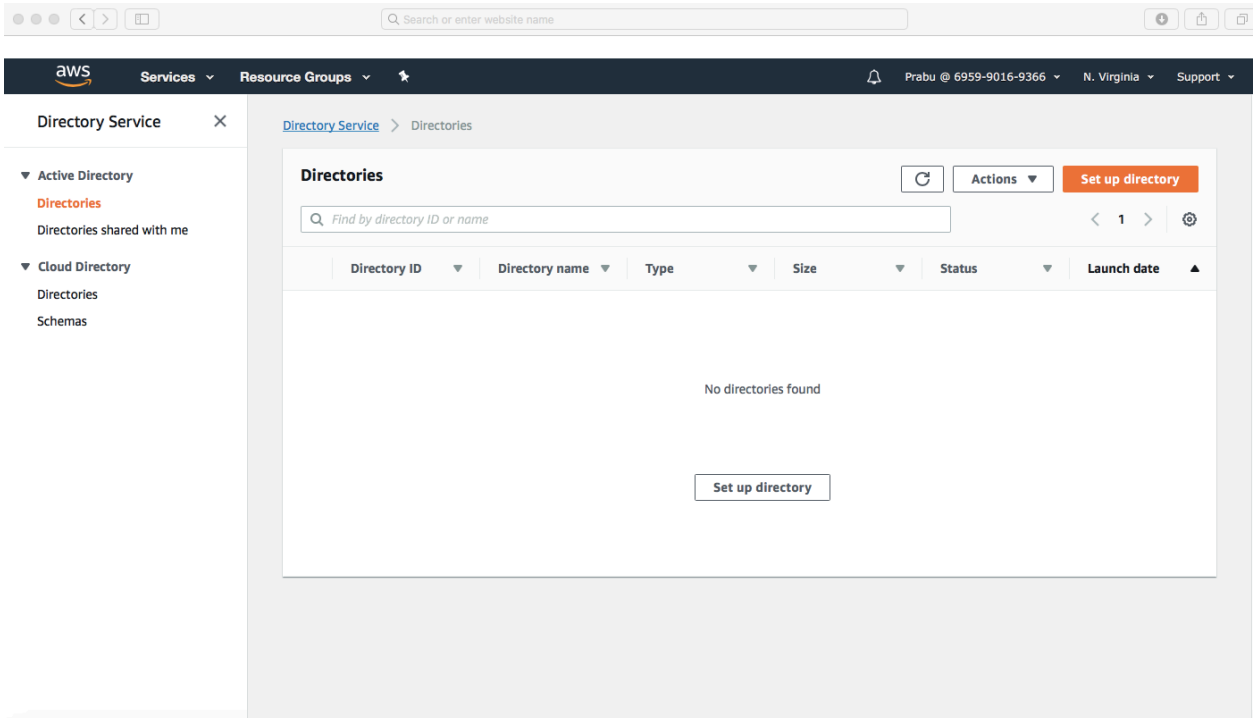
- An Internet browser

3 Creating the AWS Active Directory service

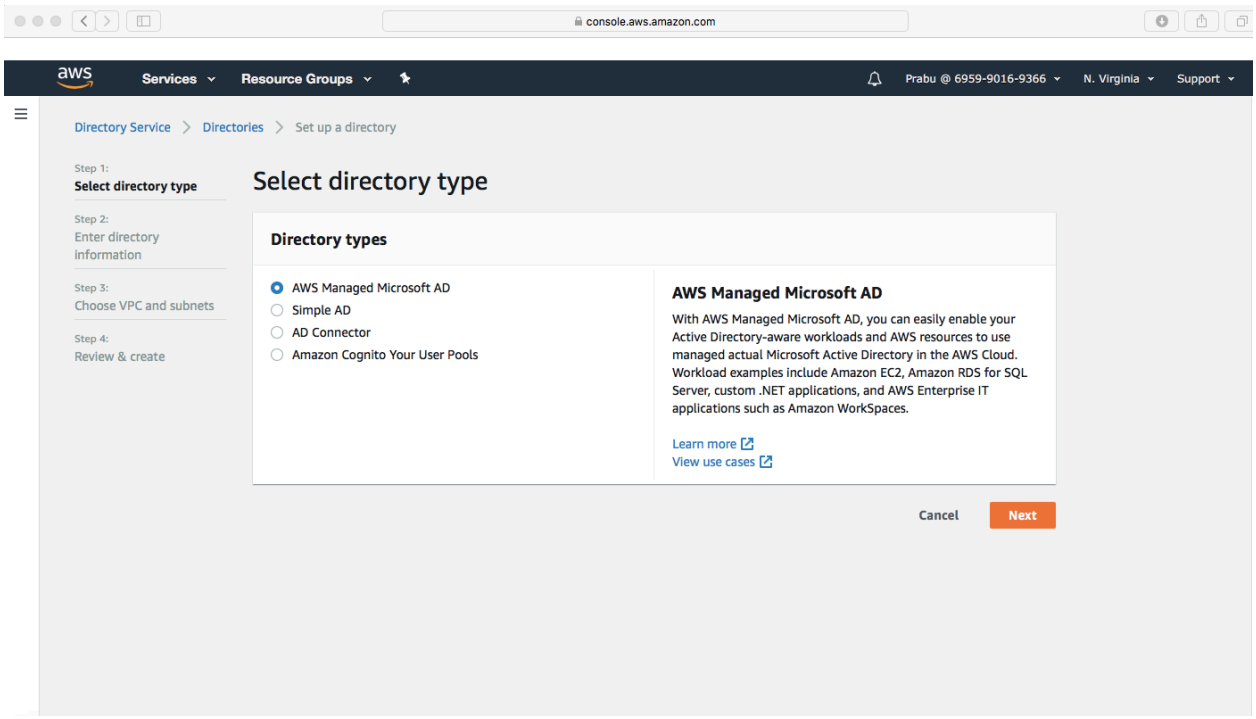
AWS Managed Microsoft AD creates a fully managed Microsoft Active Directory in the AWS Cloud. It is powered by Windows Server 2012 R2 and operates at the 2012 R2 functional level. When you create a directory with AWS Managed Microsoft AD, AWS Directory Service creates two domain controllers and adds the DNS service on your behalf. The domain controllers are created in different subnets in a VPC; this redundancy helps ensure that your directory remains accessible even if a failure occurs. If you need more domain controllers, you can add them later.

Follow the link below to get started with AWS Managed Microsoft AD
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started.html

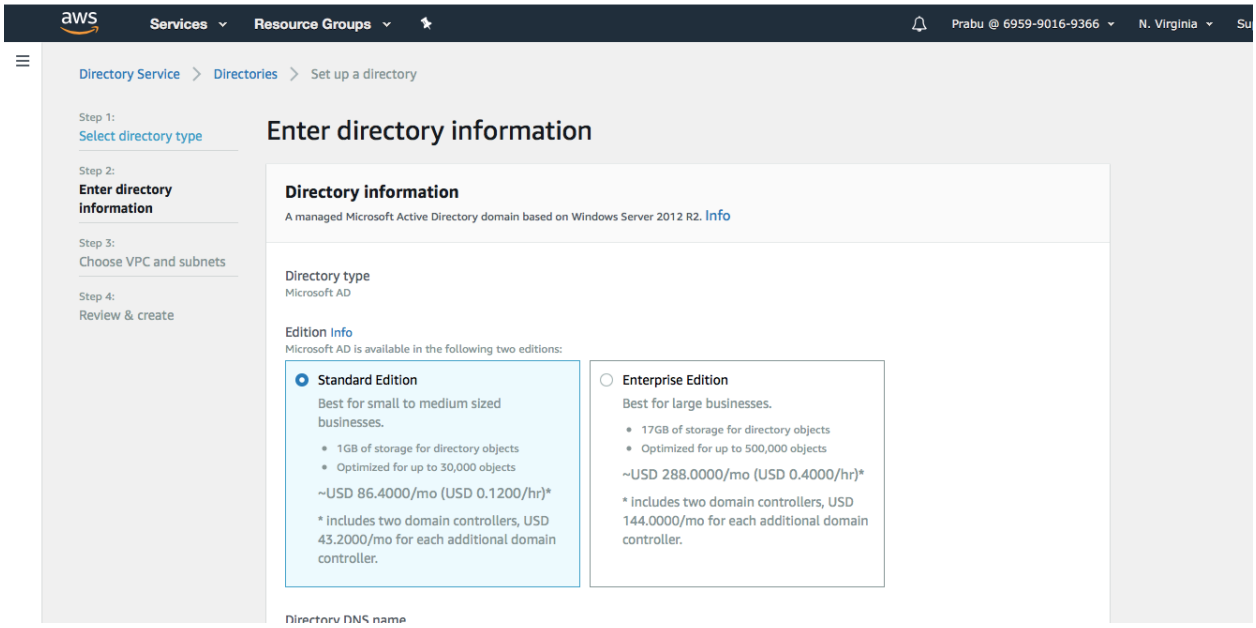
1. Log in to AWS Management console and navigate to the AWS Directory Service (DS) page.



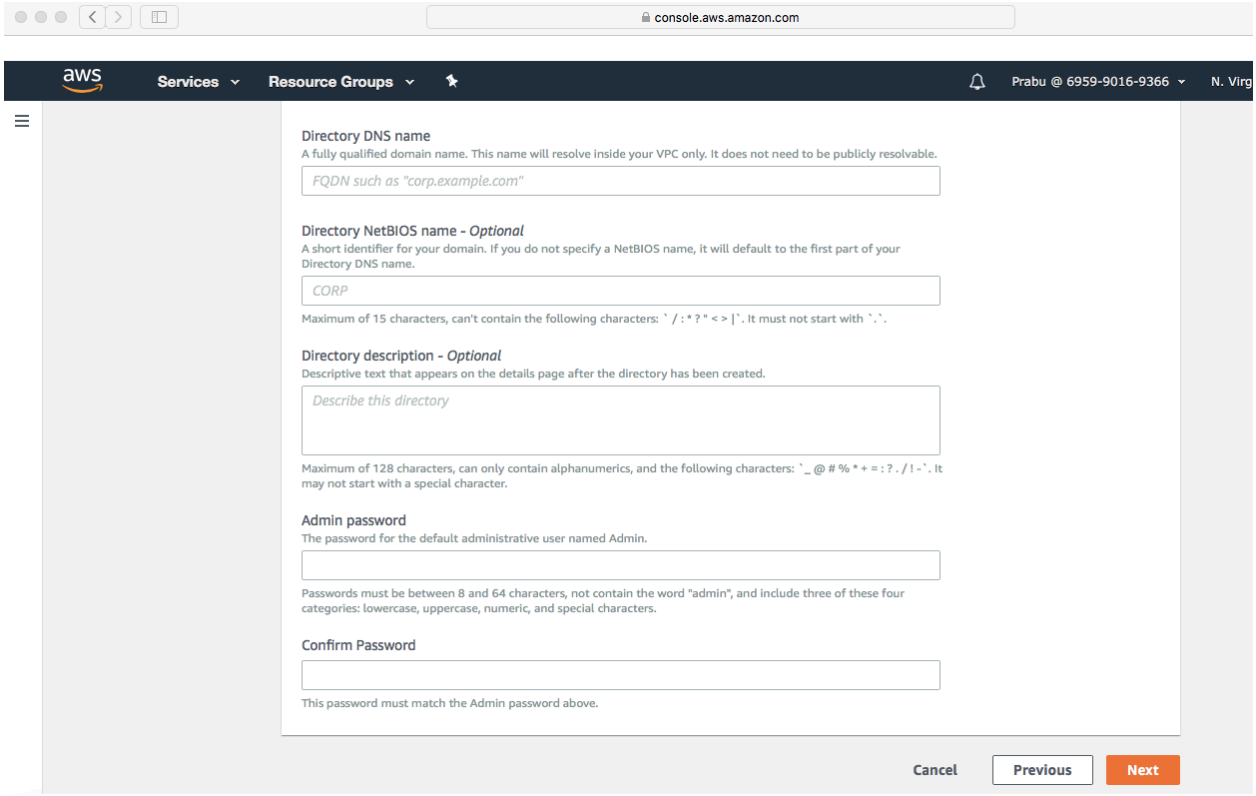
2. Click on **Set up directory**.



3. Choose **AWS Managed Microsoft AD** from the Directory types and click **Next**.



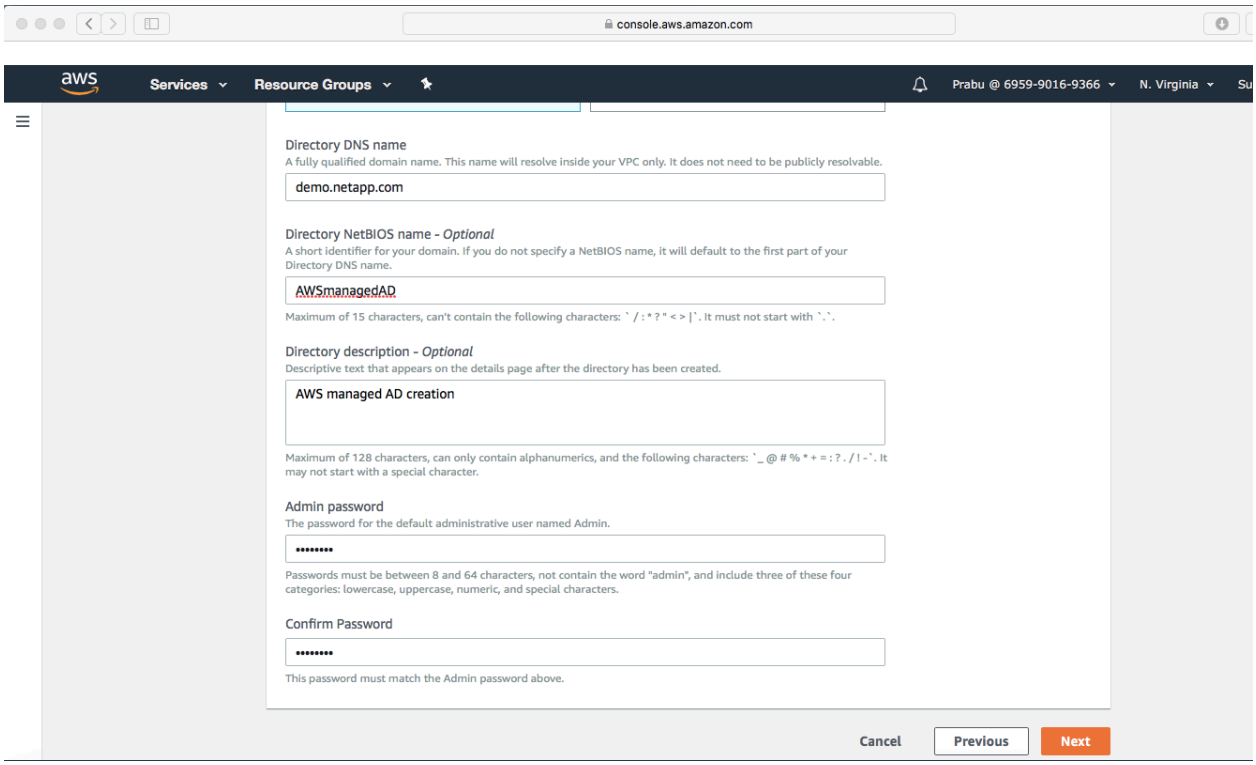
4. Choose either **Standard Edition** or **Enterprise Edition** depending on your requirements.



5. Enter the required details to create the AD directory service.

   Example inputs are shown below; enter your own values.

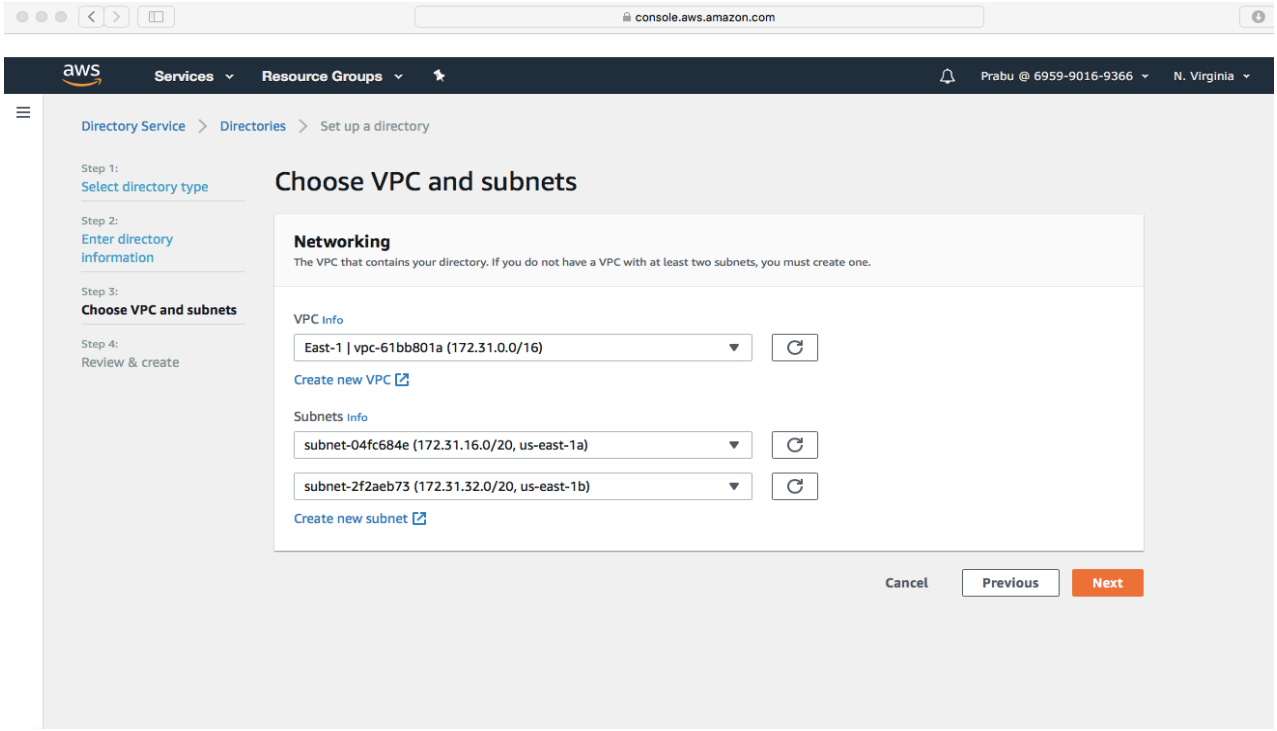
   - **Directory DNS name:** demo.netapp.com
   - **Directory NetBIOS name:** AWSmanagedAD
     If you do not specify a NetBIOS name, it will default to first part of the “Directory DNS name” you specified.
   - **Directory Description:** AWS managed AD creation
   - The default administrator user is **Admin**.
   - **Admin Password:** Netapp1!
   - **Confirm Password:** Netapp1!



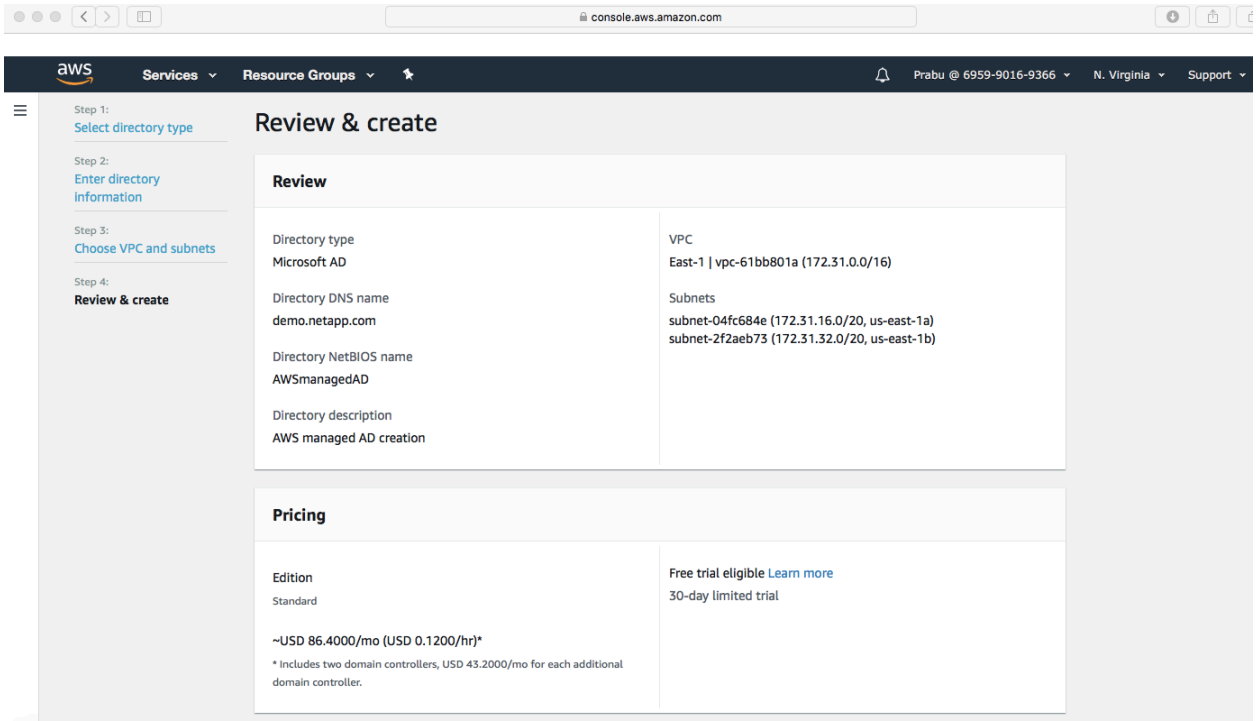
6. After entering all values, click **Next**.

7. In the “Choose VPC and subnets” page, select the VPC and subnets.

   - **VPC info:** Choose an existing VPC where the Cloud Volumes Service is already configured.
   - **Subnets:** Choose two different subnets.



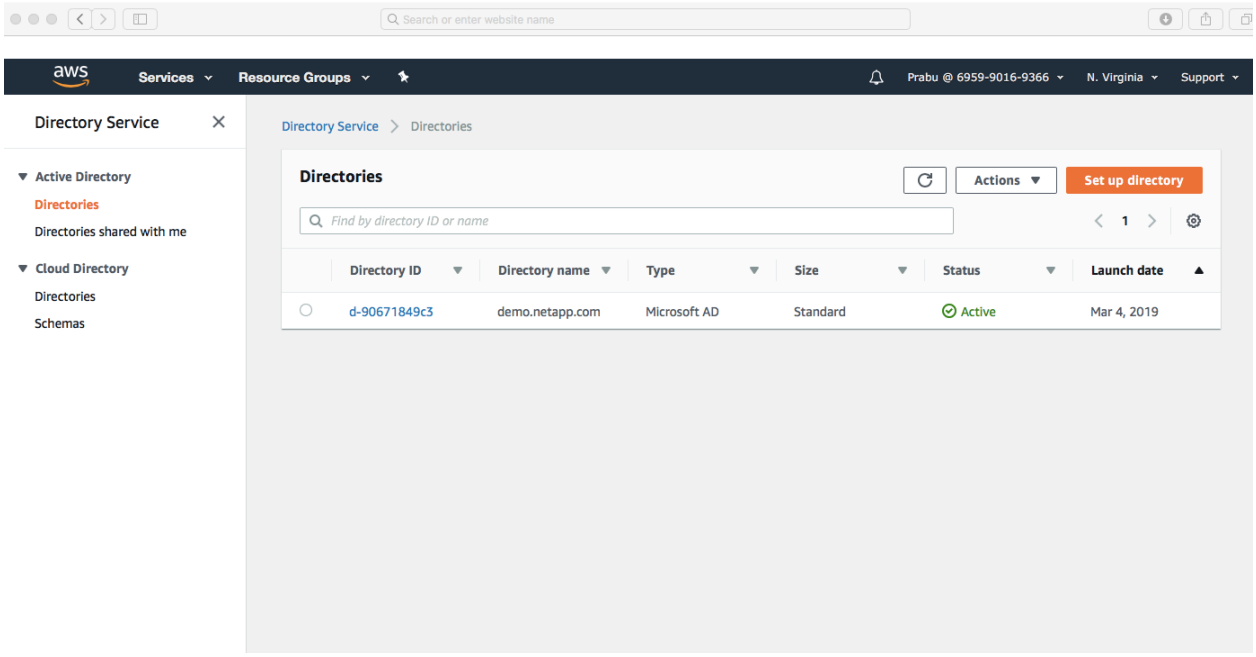
8. Click **Next** and the “Review & create” page is displayed.



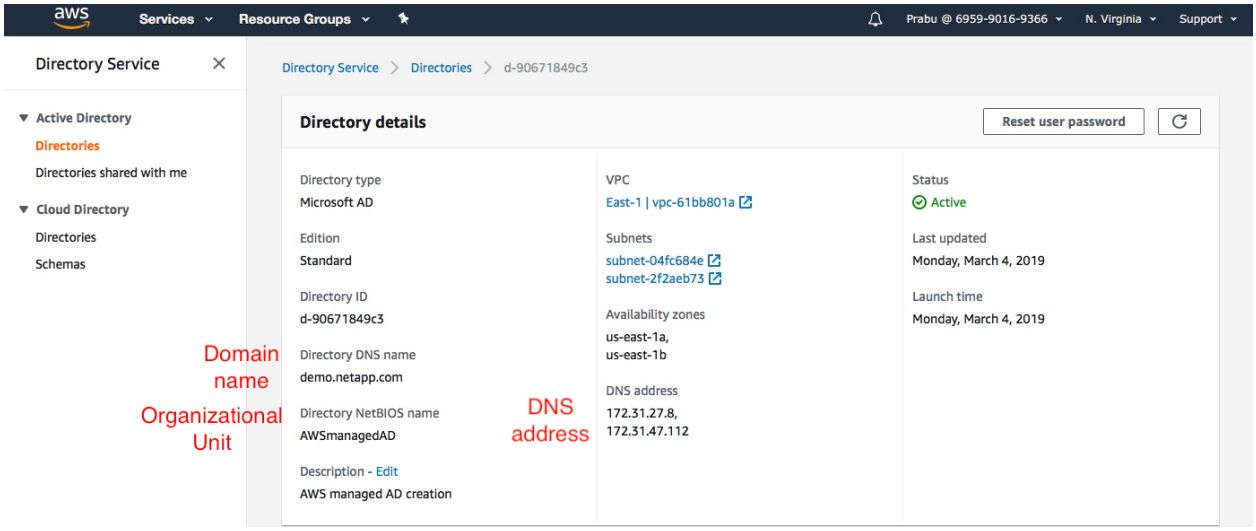
This page summarizes the information you have specified in the previous steps.

9. Review and confirm the inputs then click **Create**.

It takes approximately 45 minutes for the AWS Directory service server to be created. Once created you will able to see the directory created under Directory services.



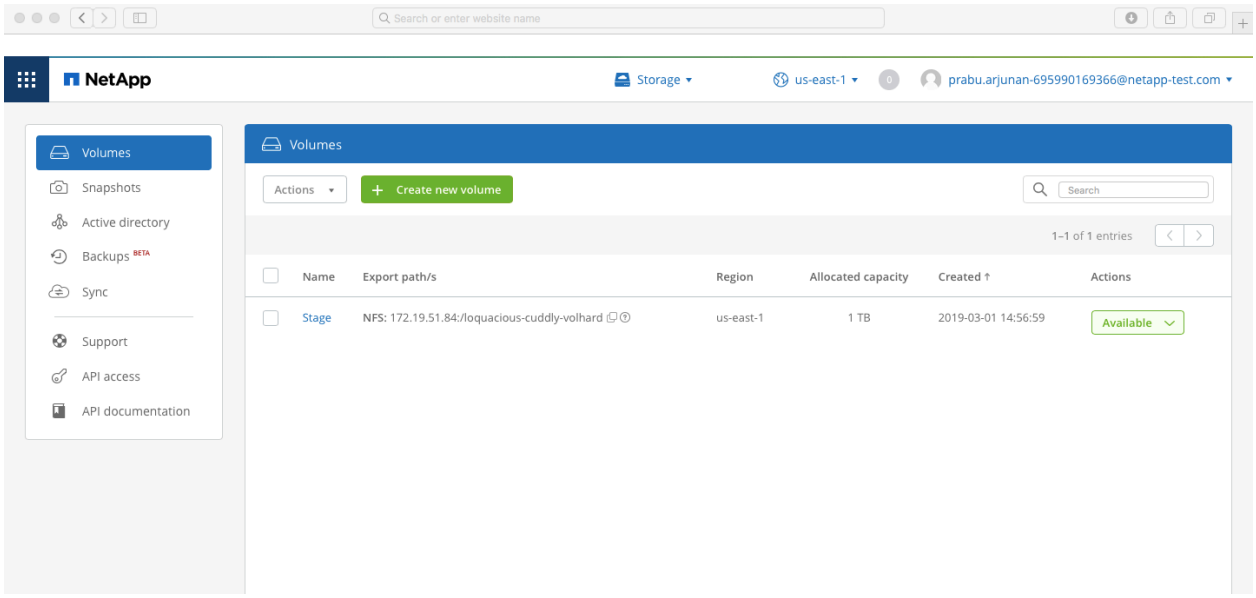
10. Click on the “Directory ID” **link** to display the details of the AWS DS.



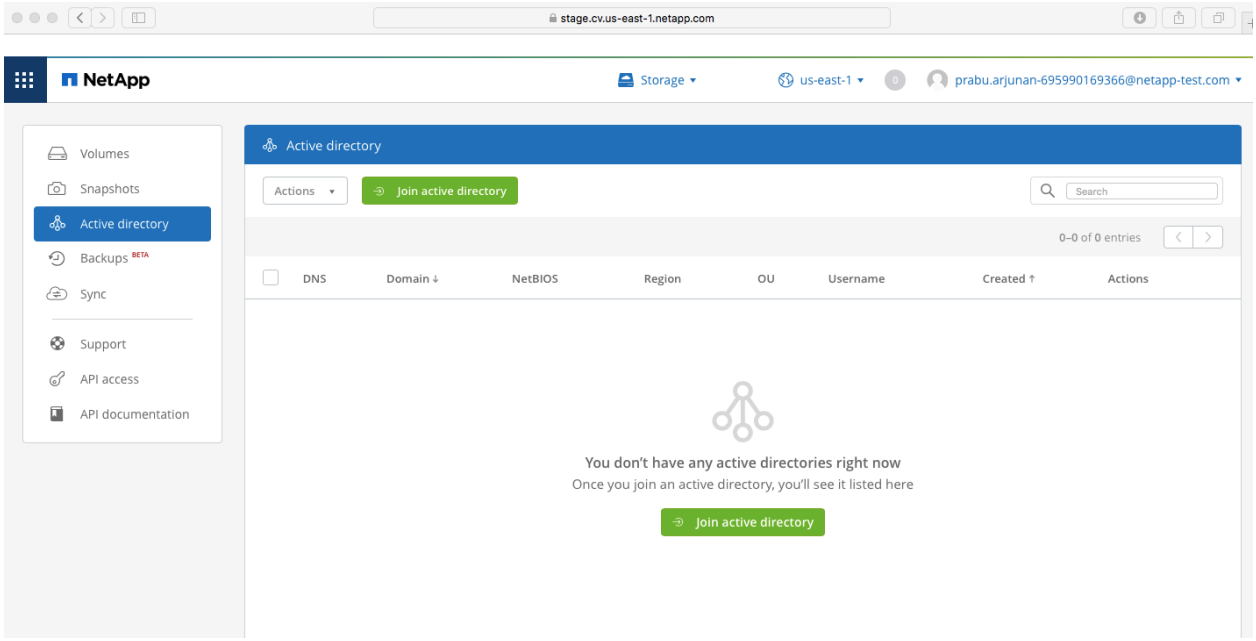
Make note of the items highlighted in red above as you will need to enter these values when applying the directory service to your cloud volume.

4 Adding the Active Directory server to Cloud Volumes Service

1. Navigate to NetApp cloud central so you can join the AWS Managed Microsoft AD to your cloud volumes.

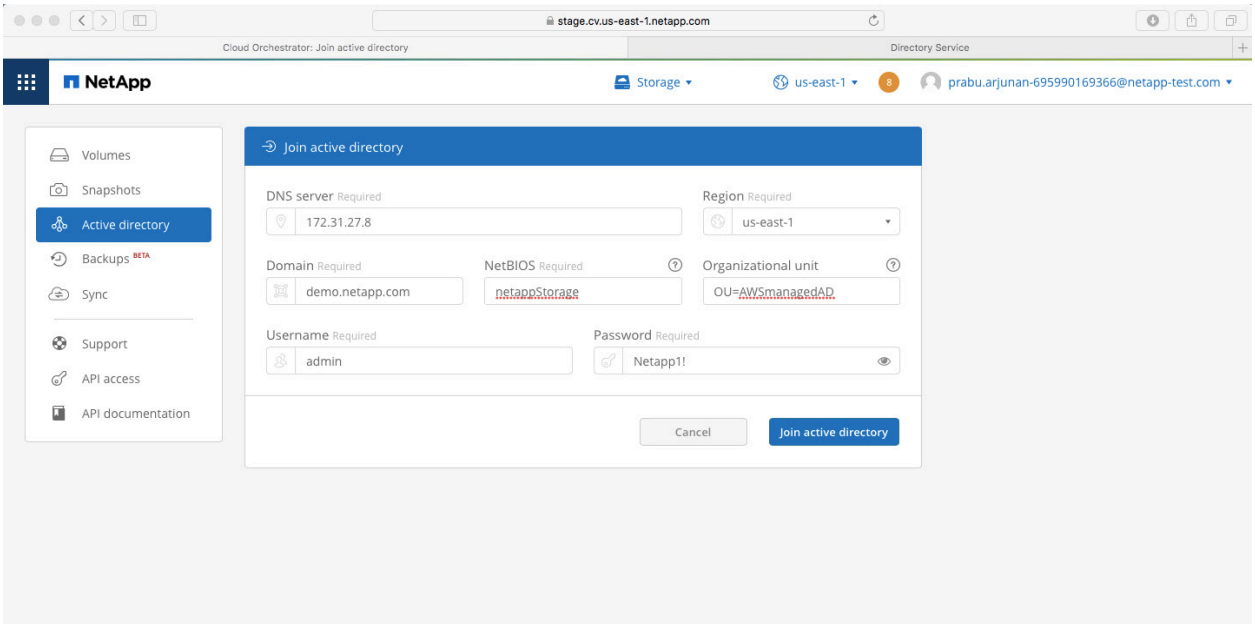


2. Click on **Active directory** on the left navigation pane.



3. Click **Join active directory**.

4. Enter the specific details about the “Directory” you created in the “AWS directory services”:



a. In the DNS server field, enter the IP address of the AWS DNS server.
(Go to AWS DS and find the IP address mentioned under **“DNS address”**).

b. In the Domain field, enter the domain for the SMB share.
(Go to AWS DS and find the name mentioned under **“Directory DNS name”**).

c. In the NetBIOS field, enter a NetBIOS name for the SMB server that will be created. (NetBIOS will create a new active directory machine account with the specified name for the SMB server. This must be a unique name in the Active directory).
In this example the NetBIOS name is **“netappStorage**”.

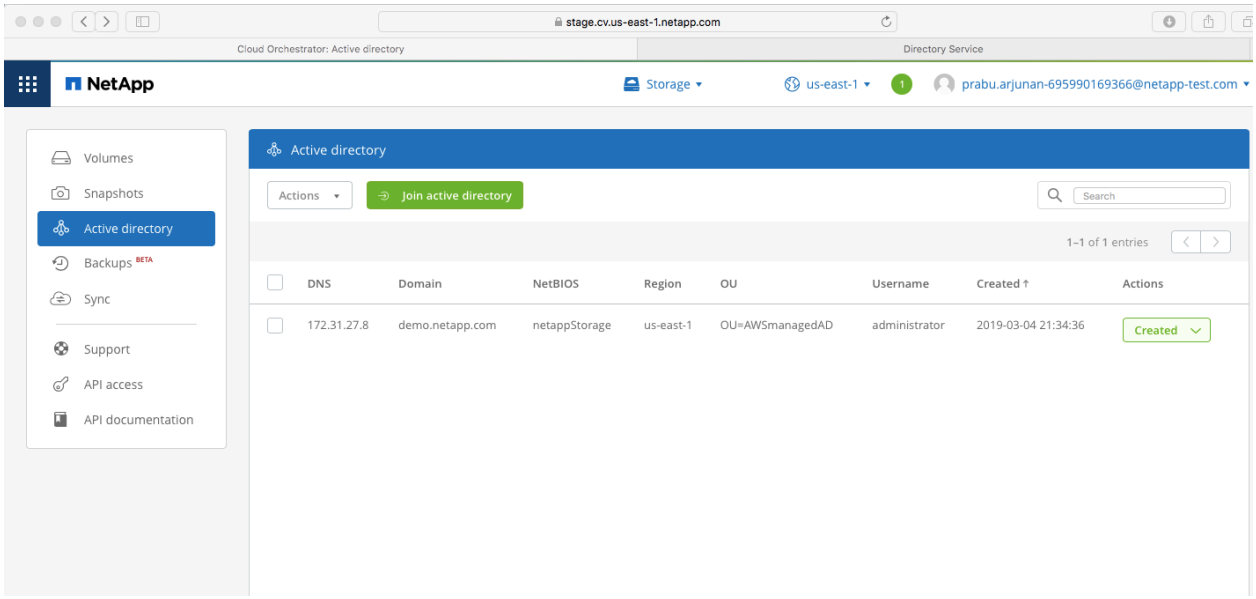
d. In the Organizational unit field, enter the “Directory NetBIOS name” of the Directory server
*(*Go to AWS DS and find the name mentioned under ***“Directory NetBIOS name”)*.
Note: The Organizational unit must be entered in the following format, OU=<*NetBIOS_name*>.
In this example the organizational unit name is **“OU=AWSmanagedAD”**

To use a nested OU you must call out the lowest level OU first up to the highest level OU. For example: “OU=NestedOU,OU=RootOU” or “OU=THIRDLEVEL,OU=SECONDLEVEL,OU=FIRSTLEVEL”.

e. In the Username field, enter the username for your Active Directory server administrator.
In this example we used “Admin”.

f. In the Password field, enter the password of the AD administrator that you specified in Username.
In this example we used “Netapp1!” as password while creating the directory.

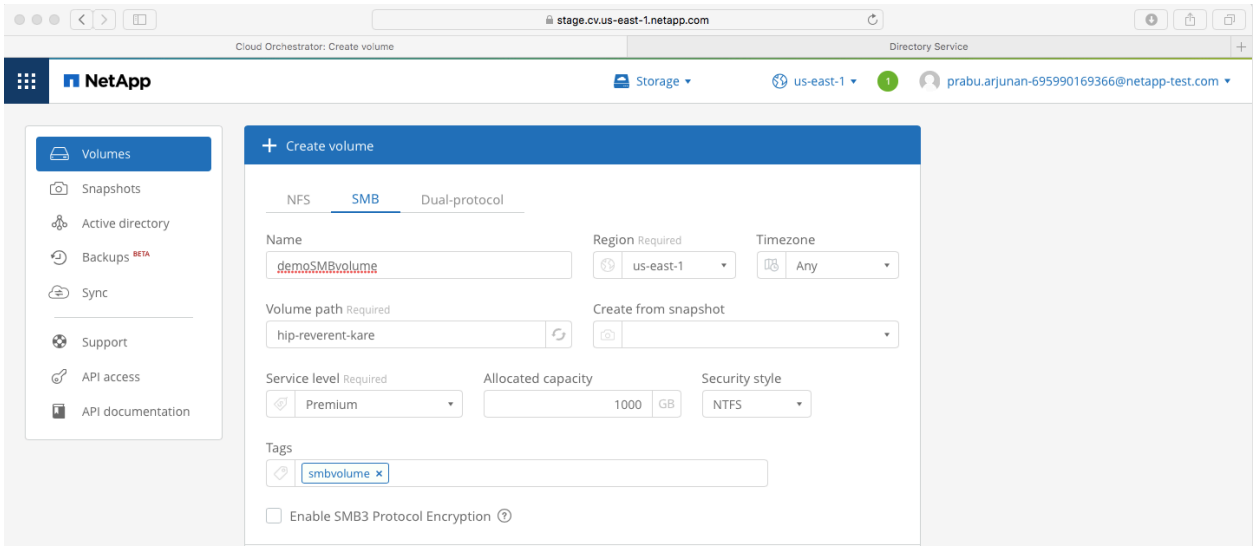
5. Click **Join active directory** to create the relationship.



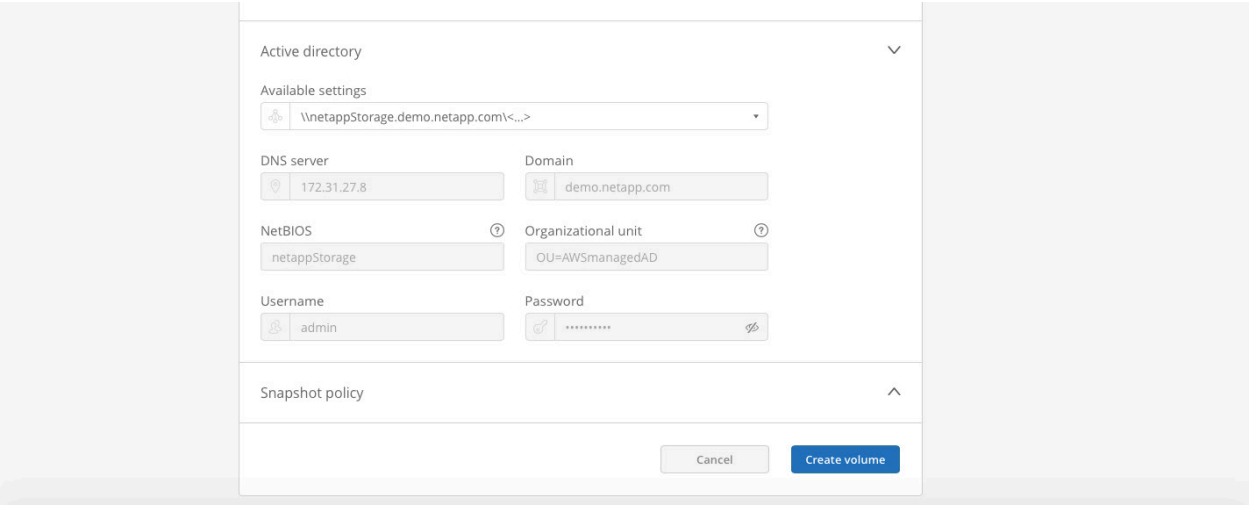
5 Creating a cloud volume that uses the Active Directory server

1. Navigate to “Volumes”, click on **Create new volume**, and choose **SMB**.

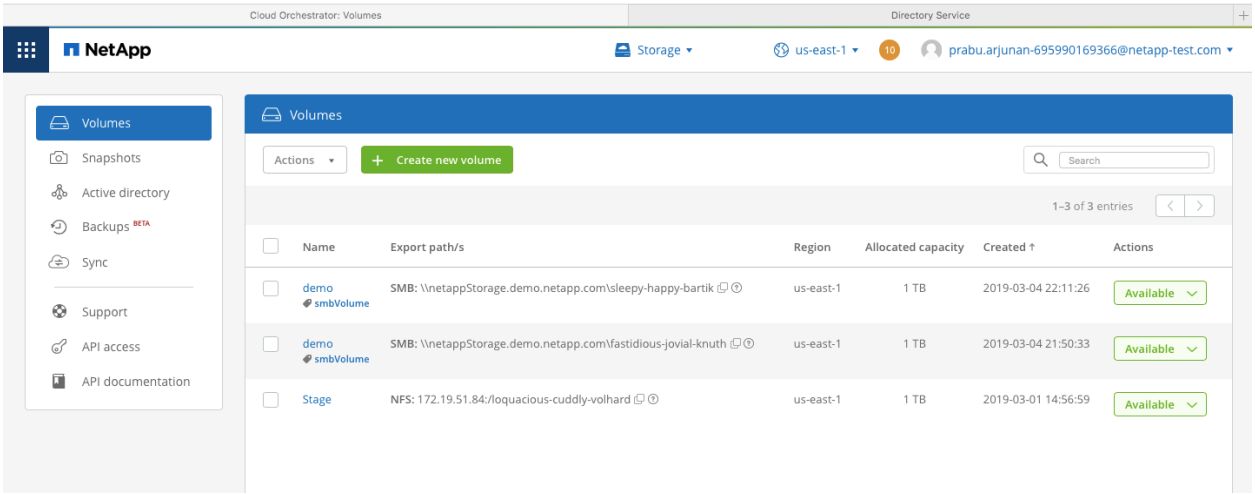
2. Enter the required information to create the volume.



3. In the Active directory section click on the “drop down list” of available settings and select the Microsoft Active Directory you created in the AWS Cloud.



4. Click **Create volume** to create the SMB volume.



Once the volume is created, it will be listed as *Available* and the export path will be listed.

Common errors messages

The following are the common error messages:

- Error

There was a problem creating volume: Error when creating - Failed to create the Active Directory machine account "NETAPPSTORAGE". Reason: Kerberos Error: Pre-authentication information was invalid Details: Error: Machine account creation procedure failed [894] Loaded the preliminary configuration. [1011] Successfully connected to ip 172.31.27.8, port 88 using TCP **[1443] FAILURE: Could not authenticate as ** 'administrator@DEMO.NETAPP.COM': CIFS server account ** password does not match password stored in Active ** Directory (KRB5KDC_ERR_PREAUTH_FAILED) .

- Fix

As per the initial AD directory settings, the correct username and password have to be specified.

References

The following references were used in this document:

- Getting started with AWS Managed Microsoft AD
  https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started.html
- Setup the pre-requisites required for
  AWS Managed Microsoft AD Prerequisites
- Instructions to complete the AWS DS setup.
  https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started_create_directory.html
- For more information, see
  Deploy Additional Domain Controllers.

Version History

Version	Date	Document Version History
Version 1.0	March 6 2019	Initial release.
1.0.1	August 1	Added link to AWS AD design considerations

NetApp