

# 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<sup>®</sup> Cloud Volumes Service for Amazon Web Services (AWS).



#### **TABLE OF CONTENTS**

1	Overview	. 3
2	Requirements	. 3
3	Creating the AWS Active Directory service	. 4
4	Adding the Active Directory server to Cloud Volumes Service	10
5	Creating a cloud volume that uses the Active Directory server	12
Co	mmon errors messages	14
Ret	ferences	14
Vei	rsion History	14

### **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 <u>Active Directory Design</u> 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

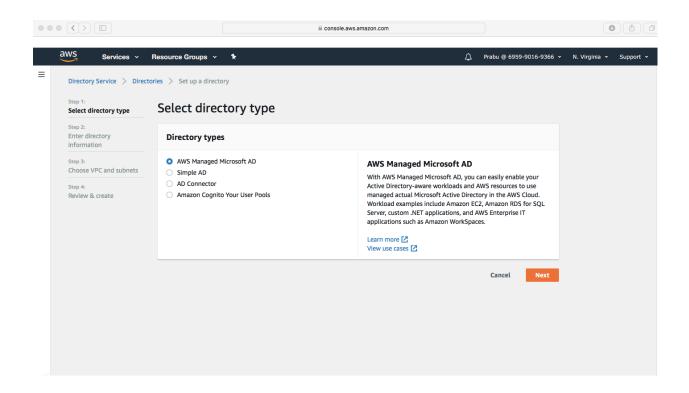
AWS Managed Microsoft AD creates a fully managed Microsoft Active Directory in the AWS Cloud. It is powered by Windows Server 2012 R2 and operates at the 2012 R2 functional level. When you create a directory with AWS Managed Microsoft AD, AWS Directory Service creates two domain controllers and adds 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 <a href="https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms">https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms</a> ad getting started.html

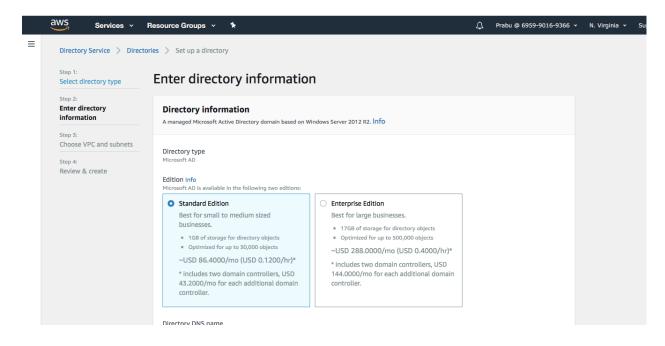
1. Log in to AWS Management console and navigate to the AWS Directory Service (DS) page.

	Q Search or enter website name		
aws Services - Res	ource Groups 👻 🎗	û Prabu @ 6959-9016-9366 ∽	N. Virginia 👻 Support 👻
Directory Service ×	Directory Service > Directories		
<ul> <li>Active Directory</li> <li>Directories</li> <li>Directories shared with me</li> </ul>	Directories           Q.         Find by directory ID or name	C Actions V	Set up directory           < 1 > ③
<ul> <li>Cloud Directory</li> <li>Directories</li> <li>Schemas</li> </ul>	Directory ID V Directory name V Type V Size	▼ Status ▼	Launch date
	No directories found		
	Set up directory		

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.

	2005					
	aws Services -	Resource Groups ~	*	$\Diamond$	Prabu @ 6959-9016-9366 •	N. Virg
Ξ	Services	Directory DNS nam A fully qualified doma FQDN such as "co Directory NetBIOS A short identifier for y Directory DNS name. CORP Maximum of 15 charae Directory descriptio Descriptive text that a Descriptive text that a Describe this direct Maximum of 128 char may not start with a sp Admin password The password for the o Passwords must be be categories: lowercase, Confirm Password	e in name. This name will resolve inside your VPC only. It does not need to be publicly resolvable. rp.example.com" name - Optional our domain. If you do not specify a NetBIOS name, it will default to the first part of your cters, can't contain the following characters: ` / :* ? * < > [`. It must not start with `.`. on - Optional ppears on the details page after the directory has been created. ttory acters, can only contain alphanumerics, and the following characters: `_@ # % * + = :?./1-`. It		H 200 (# 0555-5010-9300	
			Cano	el	Previous Next	

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!

$\bullet \bullet \bullet \triangleleft \diamond \rangle \square$	a console.aws.amazon.com			0
aws Services - F	Resource Groups 👻 윢	۵	Prabu @ 6959-9016-9366 👻	N. Virginia 👻 Su
	Directory DNS name         A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.         demo.netapp.com         Directory NetBIOS name - Optional         A short identifier for your domain. If you do not specify a NetBIOS name, it will default to the first part of your Directory DNS name.         MXEmnanaechAD         Directory description - Optional         Descriptive text that appears on the details page after the directory has been created.         MWS managed AD creation         Maximum of 128 characters, can only contain alphanumerics, and the following characters: `_@@ # %e *+ =:?./!-`. It may not start with a special character.         Admin password         The passwords must be between 8 and 64 characters, not contain the word "admin", and include three of these four categories: lowercase, uppercase, numeric, and special characters.         Confirm Password         Image         Image         Image         Image         Image         Admin password         Image         Image         Image         Image         Image         Maximum of 128 characters, and only contain alphanumerics, and the following characters: `_@@ # %e * + =:?./!te         Image         Image         Dassoword <t< td=""><td></td><td></td><td></td></t<>			
	Cancel		Previous Next	

- 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.

		i console.aws.amazon.com		0
	aws Services ~	Resource Groups 🗸 🔭 🗘	Prabu @ 6959-9016-9366	v N. Virginia 👻
=	Directory Service > Direct	pries > Set up a directory		
	Step 1: Select directory type	Choose VPC and subnets		
	Step 2: Enter directory information	Networking The VPC that contains your directory. If you do not have a VPC with at least two subnets, you must create one.		
	Step 3: Choose VPC and subnets	VPC Info		
	Step 4: Review & create	East-1   vpc-61bb801a (172.31.0.0/16)               С		
		Subnets Info subnet-04fc684e (172.31.16.0/20, us-east-1a)		
		subnet-2f2aeb73 (172.31.32.0/20, us-east-1b)		
		Cancel	Previous Next	

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

$\bullet \bullet \bullet \checkmark \square$	<b>≙</b> con	isole.aws.amazon.com	
aws Servic	es 👻 Resource Groups 👻 🎗	Pra	ıbu @ 6959-9016-9366 × N. Virginia × Support ×
Step 1: Select directory ty	Review & create		
Step 2: Enter directory information	Review		
Step 3: Choose VPC and su	bnets Directory type Microsoft AD	VPC East-1   vpc-61bb801a (172.31.0.0/16)	
Step 4: Review & create	Directory DNS name demo.netapp.com Directory NetBIOS name AWSmanagedAD Directory description AWS managed AD creation	Subnets subnet-04fc684e (172.31.16.0/20, us-east-1a subnet-2f2aeb73 (172.31.32.0/20, us-east-1b	
	Pricing		
	Edition Standard ~USD 86.4000/mo (USD 0.1200/hr)* * Includes two domain controllers, USD 43.2000/mo for each addition domain controller.	Free trial eligible Learn more 30-day limited trial	

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.

	Q. Search or enter website name		
aws Services - Re	source Groups 👻 🔭	Д Prabu @ 6959-9016-9366	✓ N. Virginia ✓ Support <sup>×</sup>
Directory Service ×	Directory Service > Directories		
<ul> <li>Active Directory</li> <li>Directories</li> </ul>	Directories	C Actions <b>v</b>	Set up directory
Directories shared with me	Q. Find by directory ID or name		< 1 > @
Cloud Directory     Directories	Directory ID v Directory name v Type v Size	▼ Status ▼	
Schemas	O d-90671849c3 demo.netapp.com Microsoft AD Standard	⊘ Active	Mar 4, 2019

10. Click on the "Directory ID" link to display the details of the AWS DS.

aws Services - Resource	ce Groups 🗸 🔸	Ą	Prabu @ 6959-9016-9366 👻 N. Virginia 👻 Support 👻
Directory Service × D	Directory Service > Directories > d-90671849c3		
Active Directory     Directories	Directory details		Reset user password
Directories shared with me  Cloud Directory Directories Schemas Domain	Directory type Microsoft AD Edition Standard Directory ID d-90671849c3 Directory DNS name	VPC East-1   vpc-61bb801a [2] Subnets subnet-04fc684e [2] subnet-2f2aeb73 [2] Availability zones us-east-1a, us-east-1b	Status Active Last updated Monday, March 4, 2019 Launch time Monday, March 4, 2019
organizational Unit	demo.netapp.com Directory NetBIOS name AWSmanagedAD Description - Edit AWS managed AD creation	DNS address 172.31.27.8,	

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.

				Q Search or enter website name					
n NetA	pp			🚍 St	orage 🔻	🚯 us-east-1	• 0	<b>Q</b> prabu.arjunan-6	95990169366@netapp-test.co
🔒 Volume	s	<b>⊖</b> v	/olumes						
ⓒ Snapsho	ots	Acti	ons 👻	+ Create new volume				C	Search
r Active d	irectory								1–1 of 1 entries
Backups	BETA								
l Sync			Name	Export path/s	Regio		ted capacity		Actions
Support			Stage	NFS: 172.19.51.84:/loquacious-cuddly-volhard 🖓 🕐	us-ea	st-1	1 TB	2019-03-01 14:56:5	9 Available ~
	255								
API doci	umentation								

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

•				🗎 stage	cv.us-east-1.netapp.com				0 1
•	NetApp				Storage 🔹	🕥 us-	east-1 🔻 💿	<b>Prabu.arjunan-69</b>	5990169366@netapp-test.com
	Volumes	ం Active direct	ory						
Ó	Snapshots	Actions 🔻	∋ Join active dire	ctory				Q	Search
ሔ	Active directory								0-0 of 0 entries
9	Backups BETA	DNS	Domain ↓	NetBIOS	Region	OU	Username	Created ↑	Actions
٢	Sync	DNS	Domain +	Netbios	Region	00	Username	Created +	Actions
Ø	Support								
Ì	API access					0			
Ā	API documentation				d	To			
				,	ou don't have any ac		os right now		
					ce you join an active dir			2	
					Join ao	ctive directory			

- 3. Click Join active directory.
- 4. Enter the specific details about the "Directory" you created in the "AWS directory services":

		a stage.cv.us-ease	st-1.netapp.com		Ċ	
	Cloud Orchestrator: Join active directory				Dire	ctory Service +
III NetApp		<b>a</b>	Storage •	🔇 us-east-1 ▼	8	🔘 prabu.arjunan-695990169366@netapp-test.com 🔻
🖨 Volumes	⊕ Join active directory					
Snapshots	DNS server Required		Reg	ion Required		
ും Active directory	0 172.31.27.8			us-east-1	•	
Backups BETA	Domain Required	NetBIOS Required	⑦ Org	anizational unit	(?)	
la Sync	demo.netapp.com	netappStorage	0	U=AWSmanagedAD		
Support	Username Required	Passw	ord Required			
API access	admin		Netapp1!		۲	
API documentatio	n					
			Cancel	Join active dire	tory	

- 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.

- ••• <> Ċ 0 1 6 a stage.cv.us-east-1.netapp.com Cloud Orche rator: Active d Di ory Service .... 🗖 NetApp 🖴 Storage 🔹 🚯 us-east-1 🔹 👔 🔘 prabu.arjunan-695990169366@netapp-test.com 🔹 🖂 Volumes Snapshots Actions 🔻 Q Search 1–1 of 1 entries Backups BETA DNS Domain NetBIOS Region OU Username Created ↑ Actions 🚖 Sync 2019-03-04 21:34:36 172.31.27.8 demo.netapp.com netappStorage us-east-1 OU=AWSmanagedAD administrator Created 🗸 Support API access API documentation
- 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.

	l stag	ge.cv.us-east-1.netapp.com	Ċ	
Cloud	d Orchestrator: Create volume		C	birectory Service +
III NetApp		Storage 🔻	🚯 us-east-1 ▾ 🚺	
🖨 Volumes	+ Create volume			
Snapshots	NFS SMB Dual-protocol			
Active directory			_	
Backups BETA	Name demoSMBvolume	Region Required	Timezone	
Ĝ Sync	Volume path Required	Create from snapshot		
Support	hip-reverent-kare		v	
API access	Service level Required Allocated capac	ity Securit	ty style	
API documentation	Image: Premium         •	1000 GB NTFS	5 · ·	
	Tags       Image: Smbvolume ×       Enable SMB3 Protocol Encryption ⑦			

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.

Active directory		~
Available settings	<>	
DNS server       Image: DNS server	Domain       Image: Display the second s	
Username	Password	
Snapshot policy		^
	Cancel	Create volume

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

		Cloud On	chestrator: Volume:	3		Directory Service		
	NetApp			Storage 👻	🚯 us-east-1 י	n 🕕 🕥 pra	bu.arjunan-695990169	366@netapp-test.cor
			Volumes					
<u> </u>	Volumes		volumes					
$\bigcirc$	Snapshots	Act	tions 🔹 📕	- Create new volume			Q Search	1
₰₺	Active directory						1–3 of 3	entries < >
*)	Backups BETA							
Ð	Sync		Name	Export path/s	Region	Allocated capacity	Created ↑	Actions
			demo	SMB: \\netappStorage.demo.netapp.com\sleepy-happy-bartik 🖓	I us-east-1	1 TB	2019-03-04 22:11:26	Available 🗸
Ø	Support		smbVolume					
ð	API access		SMB: \\netappStorage.demo.netapp.com\fastidious-jovial-knuth	🖓 us-east-1	1 TB	2019-03-04 21:50:33	Available 🗸	
-			smbVolume					
R	API documentation		Stage	NFS: 172.19.51.84:/loquacious-cuddly-volhard 🖵 💿	us-east-1	1 TB	2019-03-01 14:56:59	Available 🗸
								Available V

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 <u>https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms\_ad\_getting\_started.html</u>
- Setup the pre-requisites required for AWS Managed Microsoft AD Prerequisites
- Instructions to complete the AWS DS setup. <u>https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms ad getting started create directory.html</u>
- For more information, see <u>Deploy Additional Domain Controllers.</u>

### **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		

#### **Copyright Information**

Copyright © 2019 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

#### Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <u>http://www.netapp.com/TM</u> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

