Using Microsoft Active Directory Across On-Premises and AWS Cloud Windows Workloads

Justin Bradley, Specialist SA Desktop and AppStreaming
28 June 2017
What to Expect from the session

Running Windows applications and workloads in the AWS Cloud

- Why Windows workloads in AWS need Active Directory (AD)
- AD options for cloud workloads

AWS Directory Service for Microsoft Active Directory (Enterprise Edition) – “Microsoft AD”

Other AWS Directory Service solutions
Why Windows workloads in AWS need AD

Enables users to use single sign-on (SSO) on desktops and corporate applications

Provides central application/resource access management using groups

Enables central policy management of computers via group policy
AD options for cloud workloads

Domain join EC2 instances to on-premises Active Directory environment

Run/manage an Active Directory instance on EC2

AWS Directory Service

- AWS Microsoft AD, managed Active Directory service
Example: Domain join EC2 to on-premises AD

Remote Users / Admins

Domain Controllers

corporate data center

Auth/LDAP

VPN Connection

Auth/LDAP

VPC

Availability Zone

Private Subnet

WEB

APP

DB

IIS Server

App Server

SQL Server

10.0.2.0/24

Private Subnet

WEB

APP

DB

IIS Server

App Server

SQL Server

10.0.3.0/24

VPN Connection

Availability Zone

Remote

Users / Admins

Domain

Controllers

corporate data center
Example: AD on EC2 with replication or AD trust

Remote Users / Admins

Domain Controllers

corporate data center

VPC

Availability Zone

Private Subnet

Auth/ LDAP

WEB

APP

DB

DC

IIS Server

App Server

SQL Server

Domain Controller

10.0.2.0/24

VPN Connection

Trust or Replication

Remote Users / Admins

Domain Controllers

corporate data center

VPC

Availability Zone

Private Subnet

Auth/ LDAP

WEB

APP

DB

DC

IIS Server

App Server

SQL Server

Domain Controller

10.0.3.0/24
Example: AWS
Microsoft AD with AD trust to on-premises

Remote Users / Admins

Application

VPN Connection

corporate data center

Domain Controllers

AWS Managed Services

RDS SQL Server

DB

DC

Availability Zone

Private Subnet

WEB

APP

IIS Server

App Server

10.0.2.0/24

Trust

Auth/ LDAP

AWS Managed Services

RDS SQL Server

DB

DC

Availability Zone

Private Subnet

WEB

APP

IIS Server

App Server

10.0.3.0/24

Trust

Auth/ LDAP
Example: AWS Microsoft AD with everything in the cloud.
# Active Directory options for cloud workloads

<table>
<thead>
<tr>
<th>Operation Management</th>
<th>AWS Microsoft AD</th>
<th>EC2 AD Instance</th>
<th>On-Premises AD</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS managed in the cloud</td>
<td>Customer managed in the cloud</td>
<td>Customer managed own hardware</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability</th>
<th>AWS</th>
<th>EC2 AD Instance</th>
<th>On-Premises AD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Built-in redundancy and replication</td>
<td>Customer must design for high availability</td>
<td>Customer must design for high availability</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networking</th>
<th>AWS</th>
<th>EC2 AD Instance</th>
<th>On-Premises AD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust(^1) ports from cloud to on-premises (least exposed)</td>
<td>Trust(^1) or replication(^2) ports from cloud to on-premises AD</td>
<td>Ports to support cloud to on-premises AD(^3) (most exposed)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Admin Control</th>
<th>AWS</th>
<th>EC2 AD Instance</th>
<th>On-Premises AD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designated OU control; some apps unsupported</td>
<td>Full control</td>
<td>Full control</td>
<td></td>
</tr>
</tbody>
</table>

---

1. If trust to on-premises is used, open ports from DCs to on-premises DCs are needed
2. AD replication requires more open ports than forest trusts, but limited to DC to DC communications
3. Ports for domain joining, AD interactions, LDAP etc., plus other firewall decisions for cloud to on-premises access
## Selecting an Active Directory option

<table>
<thead>
<tr>
<th>AWS Microsoft AD</th>
<th>EC2 AD Instances</th>
<th>On-Premises AD</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Minimize cost, effort to run AD</td>
<td>• Require a replicated, multi-region AD solution</td>
<td>• Minimal EC2 instances require access to AD</td>
</tr>
<tr>
<td>• Amazon RDS SQL Server</td>
<td>• Need NetBIOS name resolution support</td>
<td>• Latency to AD over on-premises link is acceptable</td>
</tr>
<tr>
<td>• AWS Enterprise Applications(^1)</td>
<td>• You require permissions not yet delegated by AWS Microsoft AD</td>
<td>• Security policies allow AD ports to be exposed to internet</td>
</tr>
<tr>
<td>• Windows workloads on Amazon EC2(^2)</td>
<td>• E.g., Exchange, Sharepoint, SQL Server AlwaysOn Availability Groups</td>
<td>• Comfortable architecting highly available connectivity to on-premises AD</td>
</tr>
</tbody>
</table>

\(^1\)If users are on premises via trust, application requires update; otherwise AD Connector will be needed

\(^2\)Subject to delegation constraints
AD Connector

• AD proxy for Amazon WorkSpaces, Amazon WorkDocs, and Amazon WorkMail
  • Authentication and LDAP forwarded to on-premises AD
  • Applications can look up on-premises users and groups
  • Users authenticate using existing corporate credentials

• Supports EC2 seamless domain join
  • EC2 discovers domain name from AD Connector
  • EC2 by-passes AD Connector for everything else

• Customers who intend to run Windows applications and workloads in AWS should use Microsoft AD
AWS Directory Service: Microsoft AD

  - Multiple Availability Zone deployment – Highly available directory
  - AWS monitoring, software updates, and daily snapshots – Eliminates operational overhead
- Customer-administered users/groups/computers and policy control
  - Create users, groups, and policies with Windows native AD tools – Familiar tools for administration
  - Kerberos-based single sign-on – Same end-user experience as on-premises
  - EC2 seamless domain-join – Policy managed EC2 instances
- Enables use of AWS applications and services
  - RDS SQL Server, WorkSpaces, WorkDocs, WorkMail – More ways to benefit from AWS services
- Easy to set up trust relationships
  - SSO with on-premises user accounts – End users can keep current identities
  - Share on-premises resources with EC2 – Keep existing group policy infrastructure
Microsoft AD resource domain via trusts

Establish one-way trust from AWS Microsoft AD to existing corporate domain
Domain users access resource domain in AWS without having to re-authenticate
If EC2 instances require access to on-premises devices (e.g., printers), a two-way trust is required.
Resource Forest – One-way transitive trust

1 If using Amazon WorkSpaces, the Trust must be a two-way transitive trust
Setting up AWS Directory Service

1) Select **Directory Service** in the AWS Console

2) Select **Set up directory** from the menu

3) Select **Create Microsoft AD** for the directory type

4) Configure the **Directory** and **VPC** details

User, group, policy management via Microsoft tools on domain-joined computers
AWS Microsoft AD known limitations

Roadmap items
- LDAPS
- Application enablement
- Support for more than 50,000 users

Applications not yet supported
- Those requiring
  - Elevated permissions to install or run
  - Container access
  - Managed service account creation
  - Running code on the domain controller, or registry changes
- Examples: Microsoft Exchange, SharePoint, AD Federation Services
AWS Microsoft AD - Summary

AWS managed domain controllers in different Availability Zones
Automatic patching, replication, and daily snapshots
Easy setup and administration via the AWS console and existing tools
Delegated administrative rights to dedicated OU
  • Create, read, update, and delete users and groups
  • Domain-joined machines added to DNS, assigned static IP addresses within VPC
  • Apply group policies

750 hour free trial for new AWS Directory Service customers
AD On EC2 Windows
Active Directory architecture

Managing your own Active Directory

IP addressing and DNS

Availability strategy

Global catalog servers

Sites & services

Domain-joining instances

Supporting AWS enterprise apps
Active Directory instance on EC2

Customer-managed Active Directory server running on EC2

- Customer responsible for patching, monitoring, snapshots, and high availability
- Connectivity via VPN or AWS Direct Connect
- Security groups must allow traffic to and from on-premises data center
- AD sites and subnets must be properly defined
- Site-link costs must be configured
- Enable domain members for "Try Next Closest Site" group policy setting

Supports use cases and applications that require schema extension

- Microsoft SQL Server
- Microsoft SharePoint
- Microsoft Exchange
- Microsoft Lync/Skype for Business
Microsoft workloads in Amazon VPC

Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP/IP network. The options field of a DHCP message contains configuration parameters.

Name tag: awslabs

Specify at least one of the following configuration parameters:

- Domain name: awslabs.net
- Domain name servers: 10.0.2.10, 10.0.3.10
- NTP servers: 10.0.2.10, 10.0.3.10
- NetBIOS name servers: 10.0.2.10, 10.0.3.10
- NetBIOS node type: 2

Cancel  Yes, Create
AD forest spanning AWS and corporate data center
AD forest spanning AWS and corporate data center

DC1 goes down, where do clients in London go for Directory Services?
AD forest spanning AWS and corporate data center

Properly implemented site topology and "Try Next Closest Site" policy enabled. Clients use least cost path to DC.
Adding Microsoft AD for AWS apps and services

VPC

Availability Zone

Private Subnet

10.0.2.0/24

APP

WEB

IIS Server

App Server

Domain Controller

Trust or Replication

VPN Connection

Remote Users / Admins

Domain Controllers

corporate data center

Auth/ LDAP

Auth/ LDAP

Auth/ LDAP

Trust

AWS Managed Services

Microsoft AD DC

DB

VDI

WorkSpaces

DC

RDS SQL Server

Trust

AWS Managed Services

Microsoft AD DC

DB

VDI

WorkSpaces

DC

RDS SQL Server

Microsoft AD DC
References

Documentation

• AWS Directory Service – aws.amazon.com/directoryservice
• Microsoft AD - aws.amazon.com/documentation/directory-service/
• Amazon RDS SQL Server - aws.amazon.com/documentation/rds/

Quick Starts - aws.amazon.com/quickstart/

• Active Directory DS (Microsoft AD)
• Exchange Server 2013
• SharePoint 2016 Enterprise
• Lync Server 2013
• SQL Server 2014 AlwaysOn
• PowerShell DSC
WIN201 - Simplifying Microsoft Architectures with AWS services (WIN201)
WIN301 - Bring Microsoft Applications to AWS to Stay License Compliant
WIN403 – Migrate Applications to AWS Quickly, Multisite Replication and SQL HA
ARC409 – Deploying Your First 100K Windows Users
DEV303 - Deploying and Managing .NET Pipelines and Microsoft Workloads
Justin Bradley, Specialist SA Desktop and AppStreaming