Active Directory Domain Services on AWS

Design and planning guide

December 2018

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

The cloud is now the center of most enterprise IT strategies. Many enterprises find that a well-planned move to the cloud results in an immediate business payoff. Active Directory (AD) is a foundation of the IT infrastructure for many large enterprises. This whitepaper covers best practices for designing Active Directory Domain Services (AD DS) architecture in Amazon Web Services (AWS), including AWS Managed Microsoft AD, Active Directory on Amazon Elastic Compute Cloud (Amazon EC2) Instances, and hybrid scenarios.

Importance of Active Directory in the cloud

Microsoft Active Directory was introduced in 1999 and became standard de facto technology for centralized management of Windows computers and user authentications. Active Directory serves as a distributed hierarchical data storage for information about corporate IT infrastructure, including domain name system (DNS) zones and records, devices and users, user credentials, and access rights based on groups membership.

Currently, 95% of enterprises use Active Directory and with a variety of software products for authentication.[1] Successful adoption of cloud technology requires considering existing IT infrastructure and applications deployed on-premises. For companies running Windows workloads, reliable and secure Active Directory architecture is a critical component of every IT project.

Terminology and definitions

AWS Managed Microsoft Active Directory. AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, is Microsoft Windows Server Active Directory Domain Services (AD DS) deployed and managed by AWS for you. The service runs on actual Windows Server for the highest possible fidelity and provides the most complete implementation of AD DS functionality of cloud managed AD DS services available today.

Active Directory Connector. AD Connector is a directory gateway (proxy) with which you can redirect directory requests from AWS applications and services to your on-premises Microsoft Active Directory without caching any information in the cloud. It does not require any trusts or synchronization of user accounts.

AWS Single Sign-On. AWS Single Sign-On (SSO) is a cloud SSO service that makes it easy to centrally manage SSO access to multiple AWS accounts and business applications. With AWS SSO, you can easily manage SSO access and user permissions to all of your accounts in AWS Organizations centrally.

AWS Direct Connect. AWS Direct Connect is a cloud service solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment.

Amazon VPC. Amazon Virtual Private Cloud (VPC) lets you provision a logically isolated section of the Amazon Web Services (AWS) cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own private IP address ranges, creation of subnets, and configuration of route tables and network gateways. You can also create a hardware Virtual Private Network (VPN) connection between your corporate data center and your VPC to leverage the AWS cloud as an extension of your corporate data center.

VPC Peering. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network.

AD Sites and Services. In Active Directory, a site represents a physical or logical entity that is defined on the Domain controller. Each site is associated with an Active Directory Domain. Each site also has IP definitions of what IP addresses or ranges belong to that site. Domain controllers use site information to inform Active Directory clients about domain controllers present within the closest site to the client.

Global Catalog. A global catalog server is a domain controller that stores partial copies of all Active Directory objects in the forest. It stores a complete copy of all objects in the directory of your domain and a partial copy of all objects of all other forest domains.

Flexible Single Master Operation (FSMO) Roles. In Active Directory, some updates are performed in a single-master fashion. This means that updates are performed always on one designated DC and then replicated to all other DCs. Active Directory uses roles that are assigned to DCs for these special tasks. Because these single-master roles are not tied to one DC, they are named flexible single master operation (FSMO) roles.

Read Only Domain Controller (RODC). Read-only domain controllers (RODCs) hold a copy of the AD DS database and respond to authentication requests, but applications or other servers cannot write to them. RODCs are typically deployed in locations where physical security cannot be guaranteed.

Active Directory Trust. A trust relationship (also called a trust) is a logical relationship established between domains to allow authentication and authorization to shared resources. The authentication process verifies the identity of the user, and the

authorization process determines what the user is permitted to do on a computer system or network.

Shared responsibility model

When operating in the AWS Cloud, Security and Compliance is a shared responsibility between AWS and the customer (Figure 1). AWS is responsible for security "of" the cloud, whereas customers are responsible for security "in" the cloud.

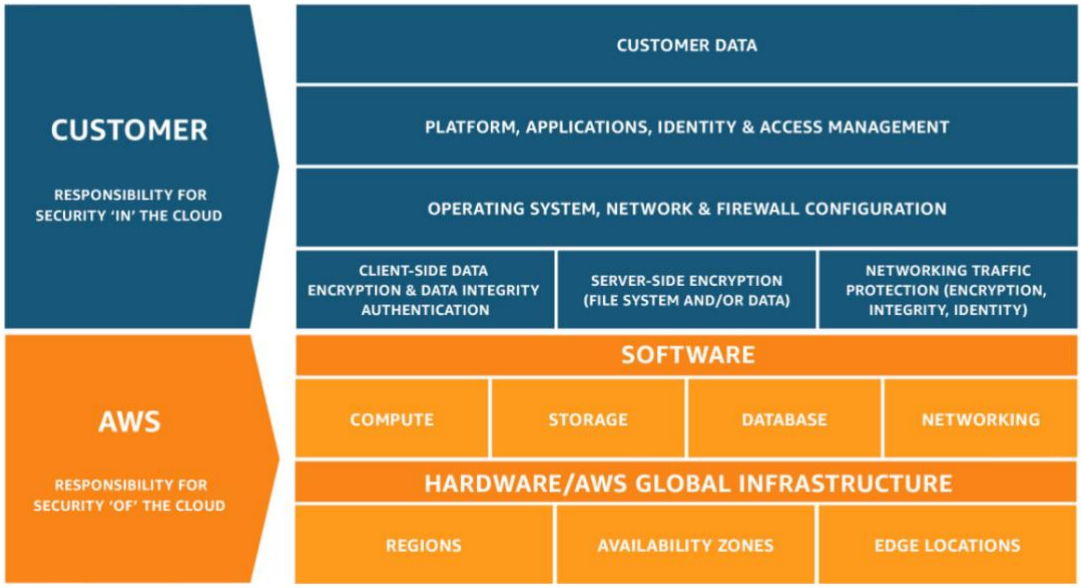

Figure 1: Shared Responsibility Model when operating in AWS Cloud

AWS is responsible for securing its software, hardware, and the facilities where AWS services are located, including securing its computing, storage, networking, and database services. In addition, AWS is responsible for the security configuration of AWS managed services, like Amazon DynamoDB, Amazon Relational Database Service (Amazon RDS), Amazon Redshift, Amazon EMR, Amazon WorkSpaces, and so on.

Customers are responsible for implementing appropriate access control policies using AWS Identity and Access Management (IAM), configuring AWS Security Groups (Firewall) to prevent unauthorized access to ports, and enabling AWS CloudTrail. Customers are also responsible for enforcing appropriate data loss prevention policies to ensure compliance with internal and external policies, as well as detecting and remediating threats arising from stolen account credentials or malicious or accidental misuse of AWS.

If you decide to run your own Active Directory on Amazon EC2 Instances, you have full administrative control of the operating system and the AD environment. You can set up custom configurations and create a complex multi-region or hybrid deployment topology. However, you must operate and support it in the same manner as you do with on-premises Active Directory.

If you use AWS Managed Microsoft AD, AWS provides operational management of your directory, including instance deployment, monitoring, backup, patching, and recovery services. You configure the service and perform administrative management of users, groups, computers, and policies.

AWS Managed Microsoft AD has been audited and approved for use in deployments that require Federal Risk and Authorization Management (FedRAMP), Payment Card Industry Data Security Standard (PCI DSS), U.S. Health Insurance Portability and Accountability Act (HIPAA), or (Service Organizational Control (SOC) compliance. When used with compliance requirements, it is your responsibility to configure the directory password policies and ensure the entire application and infrastructure deployment meets your compliance requirements. For more information, see Manage Compliance for AWS Managed Microsoft AD.

Directory services options in AWS

AWS provides a comprehensive set of services and tools for deploying Microsoft Windows workloads on its reliable and secure cloud infrastructure. AWS Active Directory Connector (AD Connector) and AWS Managed Microsoft AD are fully managed services that allow you to connect AWS applications to an existing Active Directory or host a new Active Directory in the cloud. Together, with the ability to deploy self-managed Active Directory in Amazon EC2 Instances, these services cover all cloud and hybrid scenarios for enterprise identity services.

AD Connector

AD Connector can be used in the following scenarios:

- Sign in to AWS applications, such as Amazon Chime, Amazon WorkDocs, Amazon WorkMail, or Amazon WorkSpaces using corporate credentials. (See the list of compatible applications on the AWS Documentation site.)
- Enable Access to the AWS Management Console with AD Credentials. For large enterprises, AWS recommends to use AWS Single Sign-On.

- Enable multi-factor authentication by integrating with your existing RADIUS-based MFA infrastructure.
- Join Windows EC2 instances to your on-premises Active Directory.

Note: Amazon RDS for SQL Server and Amazon FSx for Windows File Server are not compatible with AD Connector. Amazon RDS for SQL Server and Amazon FSx for Windows File Server are compatible with AWS Managed Microsoft AD only.

AWS Managed Microsoft Active Directory

By default, each AWS Managed Microsoft Active Directory has a minimum of two domain controllers, each deployed in a separate Availability Zone (AZ) for resiliency and fault tolerance. All domain controllers are exclusively yours with nothing shared with any other AWS customer. AWS provides operational management to monitor, update, backup, and recover domain controller instances. You administer users, groups, computer and group policies using standard Active Directory tools from a Windows computer joined to the AWS Managed Microsoft AD domain.

AWS Managed Microsoft AD is the only managed AD DS service today that preserves the Windows single sign-on (SSO) experience for users who access AD DS integrated applications in a hybrid IT environment. With AD DS trust support, your users can sign in once on-premises and access Windows workloads running on-premises and in the cloud. You can optionally expand the scale of the directory by adding domain controllers, thereby enabling you to distribute requests to meet your performance requirements. You can also share the directory with any account and VPC within a single AWS Region. For multi-region deployments, you can create an AWS Managed Microsoft AD in each region with a trust to a common user directory.

AWS Managed Microsoft AD enables you to forward AD security event logs to Amazon CloudWatch, giving you the ability to monitor your use of the directory and any administrative intervention performed in the course of AWS operating the service. It is also approved for applications in the AWS Cloud that are subject to compliance by the U.S. Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Federal Risk and Authorization Management (FedRAMP), or Service Organizational Control (SOC), when you enable compliance for your directory. You can also tailor security with features that enable you to manage password policies, and enable secure LDAP communications through Secure Socket

Layer (SSL)/Transport Layer Security (TLS). You can also enable multi-factor authentication (MFA) for AWS Managed Microsoft AD . This authentication provides an additional layer of security when users access AWS applications from the internet, such as Amazon WorkSpaces or Amazon QuickSight.

AWS Managed Microsoft AD is also the only managed AD DS service that enables you to extend your schema and perform LDAP write operations. These features, combined with advanced security features, such as Kerberos Constrained Delegation and Group Managed Service Account, provide the greatest degree of compatibility for Active Directory aware applications, like Microsoft SharePoint, Microsoft SQL Server Always On Availability Groups, and many .NET applications. Because Active Directory is an LDAP directory, you can also use AWS Managed Microsoft AD for Linux Secure Shell (SSH) authentication and other LDAP-enabled applications. The full list of supported AWS applications available on the AWS Documentation site.

AWS Managed Microsoft AD runs actual Window Server 2012 R2 Active Directory Domain Services and operates at the 2012 R2 functional level. AWS Managed Microsoft AD is available in two editions: Standard and Enterprise. Both editions have the same functionality but provide different storage capacity.

Edition	Storage capacity	Approximate number of objects that can be stored*	Approximate number of users in domain
Standard	1 GB	~30,000	Up to ~5,000 users
Enterprise	17 GB	~500,000	Over 5,000 users

* The number of objects varies based on type of objects, schema extensions, number of attributes, and data stored in attributes.

> **Note:** AWS Domain Administrators have full administrative access to all domains hosted on AWS. See your agreement with AWS and the AWS Data Privacy FAQ for more information about how AWS handles content that you store on AWS systems, including directory information. You do not have Domain or Enterprise Admin permissions and rely on delegated groups for administration.

AWS Managed Microsoft AD can be used for following scenarios: managing access to AWS Management Console and cloud services, joining EC2 Windows instances to Active Directory, and signing in to Amazon Chime and Amazon WorkSpaces.

For more information on this solution, see the Design consideration for AWS Managed Microsoft Active Directory in this document.

Active Directory on EC2

If you prefer to extend your Active Directory to AWS and manage it yourself for flexibility or other reasons, you have the option of running Active Directory on EC2. See the Design considerations for running Active Directory on EC2 section in this document for more information.

Comparison of Active Directory Services on AWS

The following table compares the features and functions between various Directory Services options available on AWS.

Function	AWS AD Connector	AWS Managed Microsoft AD	Active Directory on EC2
Creating users and groups	✓	✓	✓
Joining computers to the domain	✓	✓	✓
Create trusts with existing Active Directory domains and forests	-	✓	✓
Schema extensions	-	✓	✓
Add domain controllers		Yes, same region only	✓
Group Managed Service Accounts	-	✓	Depends on the Windows Server version
Kerberos constrained delegation	-	✓	✓
Support Microsoft Enterprise CA	-	✓	✓
Supported by AWS Applications	✓	✓	✓ (through federation or AD Connector)
Supported by RDS for SQL Server and FSx for Windows File Server	-	✓	-
Multi-Factor Authentication	Yes, though RADIUS	Yes, though RADIUS	Yes, with using with AD Connector

Group policy	×	✓	✓
Active Directory Recycle bin	-	✓	✓
Group Managed Service Accounts	-	✓	✓
PowerShell Support	-	✓	✓

Design consideration for AWS Managed Microsoft Active Directory

Active Directory depends on the network and accounts design. Before you select the right Active Directory topology, you must choose your network and organizational design.

Although there is no one-size-fits-all answer for how many AWS accounts a particular customer should have, most companies create more than one AWS account, as multiple accounts provide the highest level of resource and billing isolation in the following cases:

- The business requires strong fiscal and budgetary billing isolation between specific workloads, business units, or cost centers.
- The business requires administrative isolation between workloads.
- The business requires a particular workload to operate within specific AWS service limits and not impact the limits of another workload.
- The business's workloads depend on specific instance reservations to support high availability (HA) or disaster recovery (DR) capacity requirements.

Single account, AWS Region, and VPC

The simplest case is when you need to deploy a new solution in the cloud from scratch. You can deploy AWS Managed Microsoft AD in minutes and use it for most of the services and applications that require Active Directory. This solution is ideal for scenarios with no additional requirements for logical isolation between application tiers or administrative users.

Figure 2: Using AWS Managed Microsoft AD as a primary authentication service

Using multiple VPCs

Customers use multiple VPCs for various reasons. Sometimes they are used for separating applications that have different compliance requirement or applications that are run and managed by different business units. If you have multiple VPCs in the same region or account, follow these recommendations for VPC connections when designing your AWS Managed Microsoft AD architecture.

- Connect only those VPCs that really need to communicate with each other.
- Ensure that your VPC network ranges (CIDR blocks) do not overlap.
- If you have AWS Direct Connect on VPN connection with your on-premises data center, create a transit VPC to manage network routing and connectivity.
- Deploy AWS Managed Microsoft AD on the transit VPC and share it to all other VPCs.
- Create a VPC peering between a VPC with Active Directory and all other VPCs that require access to Active Directory.

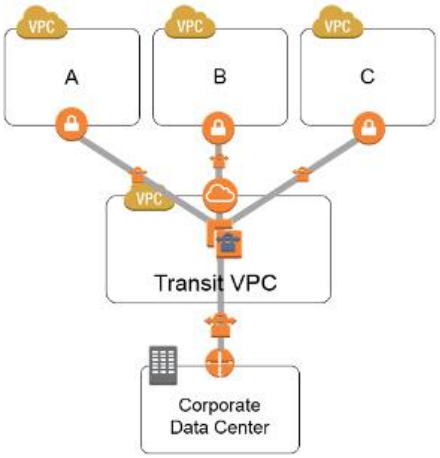

Figure 3: Using Transit VPC design

Multiple accounts and VPCs in one AWS Region

Large organizations use multiple AWS accounts for administrative delegation and billing purposes. You can share a single AWS Managed Microsoft AD with multiple AWS accounts within one AWS Region. This capability makes it easier and more cost-effective for you to manage directory-aware workloads from a single directory across accounts and VPCs. This option also allows you to use the seamless domain join feature to join your Amazon EC2 Windows instances to AWS Managed Microsoft AD.

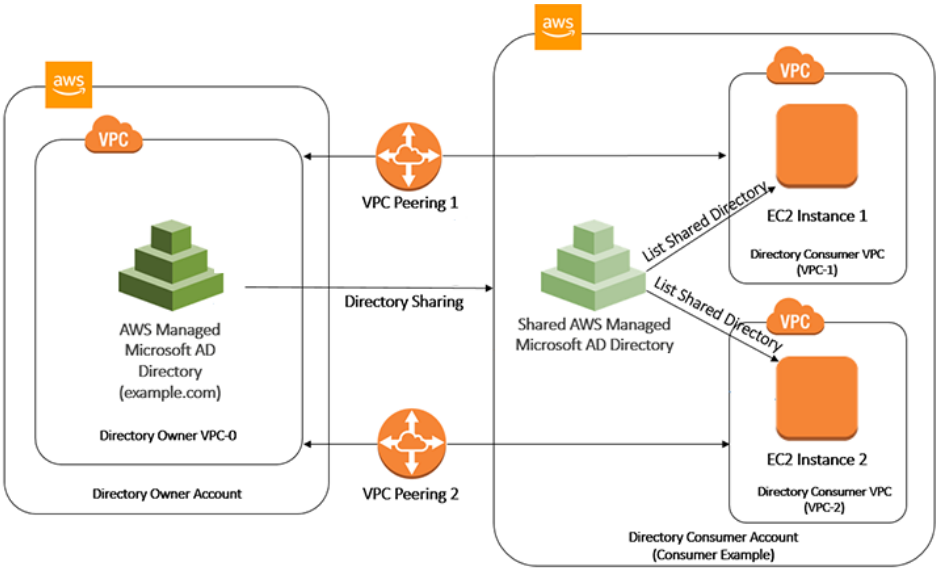

Figure 4: Sharing single AWS Managed Microsoft AD with another account

AWS recommends that you create a separate account for identity services like Active Directory and only allow a very limited group of administrators to have access to this account. Generally, you should treat Active Directory in the cloud in the same manner as on-premises AD. Just as you would limit access to a physical data center, make sure to limit administrative access to the AWS account control.

Create additional AWS accounts as necessary in your organization and share the AWS Managed Microsoft AD with them. After you have shared the service and configured routing, these users can use AD to join EC2 Windows instances, but you maintain control of all administrative tasks.

Multiple AWS Regions deployment

AWS Managed Microsoft AD can be only deployed in one region. Therefore, in a case of multiple region infrastructure, there are two options:

- Deploy AWS Managed Microsoft AD in each AWS Region and establish trust relationships between them.
- Deploy Active Directory with domain controllers on EC2 Instances. Treat each AWS Region as an AD site and deploy Domain controllers in at least two Availability Zones per AWS Region.

Both options provide a technically working solution. AWS Managed Microsoft AD is preferable because of lower management overhead, and it also provides compatibility with Amazon RDS for SQL Server.

AWS Managed Microsoft AD supports all three trust relationship directions to other AD forests and domains: incoming, outgoing, and two-way. AD forest trusts can be created between two forests only and cannot be extended to a third forest. This means that if you have more than two forests, you must create a trust between each pair of forests to enable authentication, as shown in Figure 5.

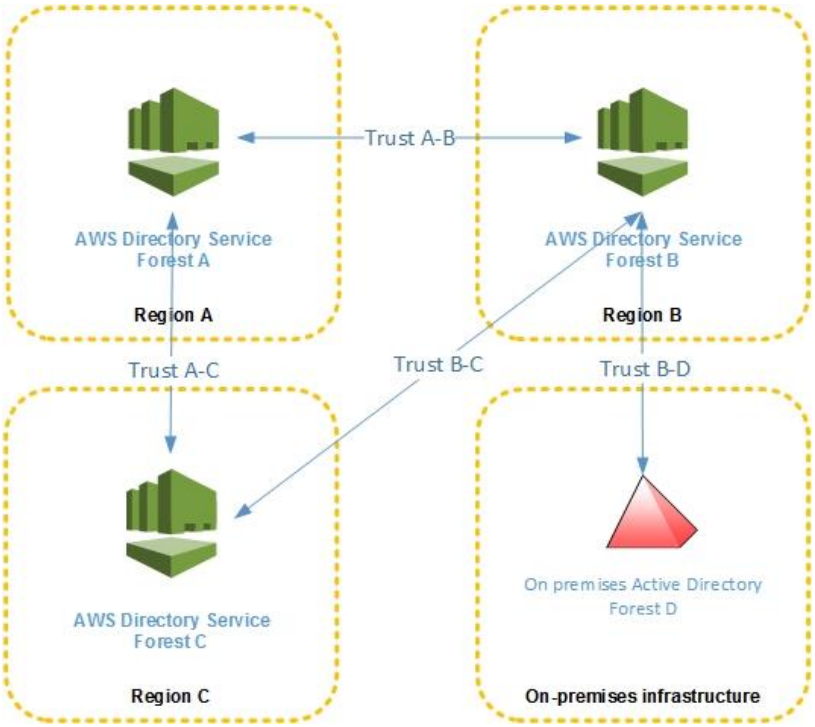

Figure 5: Active Directory forest trusts between AWS Managed Microsoft AD forests in three regions

In this example, users in on-premises Active Directory forest D can only access services in the forest B, but not in A or C. To enable access to forests A and C, you must create additional trust relationships. If you use a large number of AWS Regions, Active Directory on EC2 instances may have a simpler design with only one forest.

Enable Multi-Factor Authentication for AWS Managed Microsoft AD

You can enable multi-factor authentication (MFA) for your AWS Managed Microsoft AD to increase security when your users specify their AD credentials to access supported Amazon enterprise applications. When you enable MFA, your users enter their username and password (first factor), and then enter an authentication code (second factor) they obtain from your virtual or hardware MFA solution. These factors together provide additional security by preventing access to your Amazon enterprise applications, unless users supply valid user credentials and a valid MFA code.

To enable MFA, you must have an MFA solution that is a remote authentication dial-in user service (RADIUS) server, or you must have an MFA plugin to a RADIUS server already implemented in your on-premises infrastructure. Your MFA solution should

implement one time passcodes (OTP) that users obtain from a hardware device or from software running on a device (such as a cell phone).

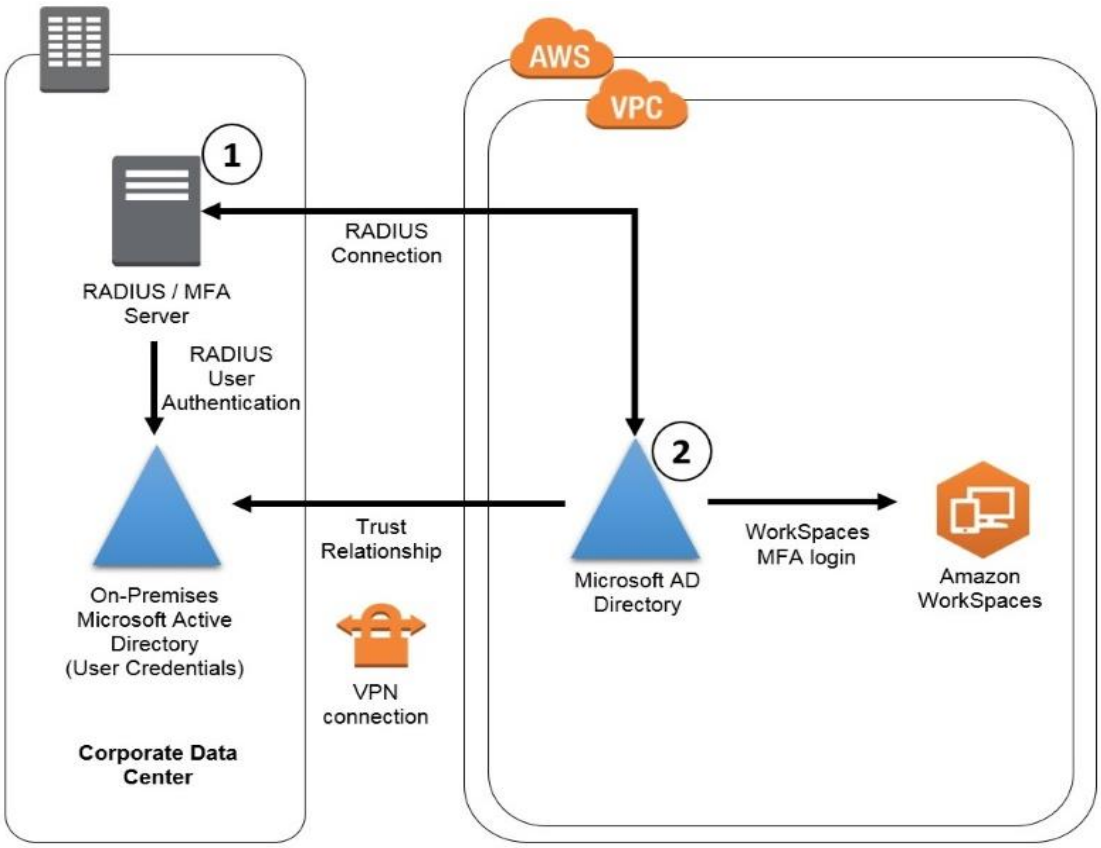

Figure 6: Using AWS Managed Microsoft Active Directory with MFA for access to Amazon Workspaces

A detailed description of this solution is available on the AWS Security Blog.

Active Directory permissions delegation

When you use AWS Managed Microsoft AD, AWS assumes responsibility for some of the Service Owners tasks so that you may focus on other business critical tasks.

The following service-level tasks are automatically performed by AWS

- Taking snapshots of the Directory Service and providing the ability to recover data.
- Creating trusts by administrator request.
- Extending Active Directory schema by administrator request.

- Managing Active Directory forest configuration.
- Managing, monitoring, and updating domain controllers.
- Managing and monitoring DNS service for Active Directory.
- Managing and monitoring Active Directory replication.
- Managing Active Directory sites and networks configuration.

With AWS Managed Microsoft AD, you also may delegate administrative permissions to some groups in your organization. These permissions include managing user accounts, joining computers to the domain, managing Group Policies and password policies, managing DNS, DHCP DFS, RAS, CA and other services. The full list of permissions that can be delegated is described in the AWS Directory Service Administration Guide.

Work with all teams that are using Active Directory services in your organization and create a list with all of the permissions that must be delegated. Plan security groups for different administrative roles and use AWS Managed Microsoft AD Delegated Groups to assign permissions. Check the AWS Directory Service Administration Guide to make sure that it is possible to delegate all of the required permissions.

Design considerations for running Active Directory on EC2 instances

If you cannot use AWS Managed Microsoft AD and you have Windows workloads you want to deploy on AWS, you can still run Active Directory on EC2 instances in AWS and support any Microsoft workload you need to run. Depending on whether you have Windows workloads in a single region or multiple regions, your Active Directory deployment may differ slightly. The following section provides a deployment guide and recommendation on how you can deploy Active Directory on EC2 instances in AWS.

Single region deployment

This deployment scenario is applicable if you are operating in a single region or you do not require Active Directory to be in more than a single region. The deployment options or architecture patterns are not significantly different whether you are operating in a single VPC or multiple VPCs. If you are using multiple VPCs, you must ensure that network connectivity between the VPCs is available through VPC peering, VPN, or other mechanisms.

The following diagrams depict how Active Directory can be deployed in a single region in a single VPC or multiple VPCs.

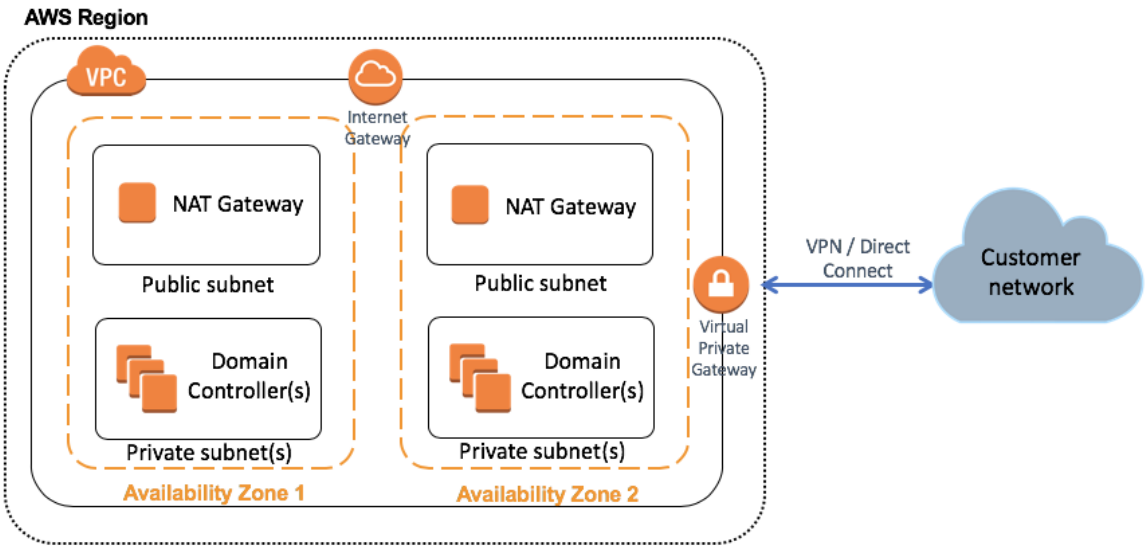

Figure 7: Deploying Active Directory on EC2 instances in a single region for single VPC

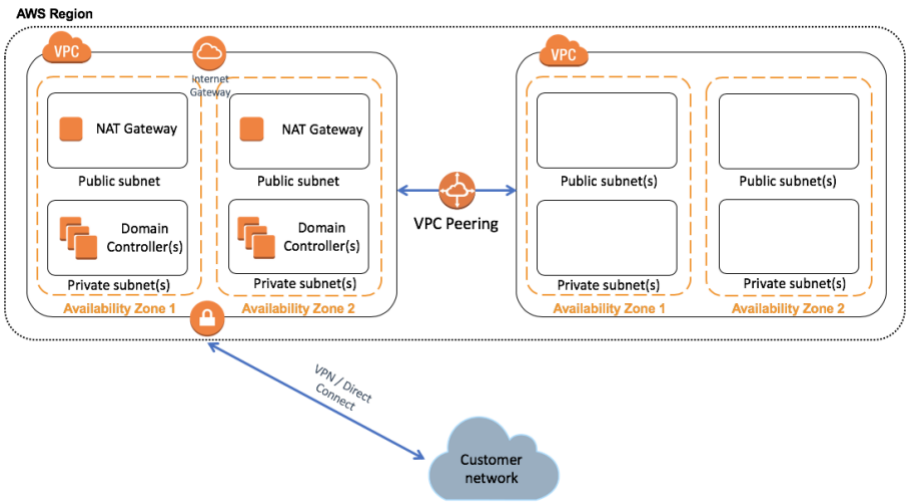

Figure 8: Deploying Active Directory on EC2 instances in a single region for multiple VPC's

Consider the following points when deploying Active Directory in this architecture:

- We recommend deploying at least two domain controllers in a region using the N+1 configuration. These domain controllers should be placed in different AZs for availability reasons.
- DCs and other non-internet facing servers should be placed in private subnets.
- If you require additional DCs due to performance, you can add more DCs to existing AZs or deploy to another available AZ.
- For AD Sites and Services, configure the entire VPC or VPCs in that region as a single site and define them accordingly. This setup ensures your member servers can reach all of the DCs in the region as first priority.
- If you have multiple VPCs, you can centralize the Active Directory services in one of the existing VPCs or create a shared services VPC to centralize the domain controllers.
- You must ensure you have highly available network connectivity between VPCs, such as VPC peering. If you are connecting the VPCs using VPNs or other methods, ensure connectivity is highly available.

Multi-region/global deployment

If you are operating in more than one region and require Active Directory to be available in these regions, use the multi-region/global deployment scenario. Within each of the regions, use the guidelines for single region deployment as all of the single region best practices still apply.

The following diagrams depicts how Active Directory can be deployed in multiple regions. In this example, we are showing Active Directory deployed in three regions that are interconnected to each other using cross-region VPC peering. In addition, these regions are also connected to the corporate network using AWS Direct Connect and VPN.

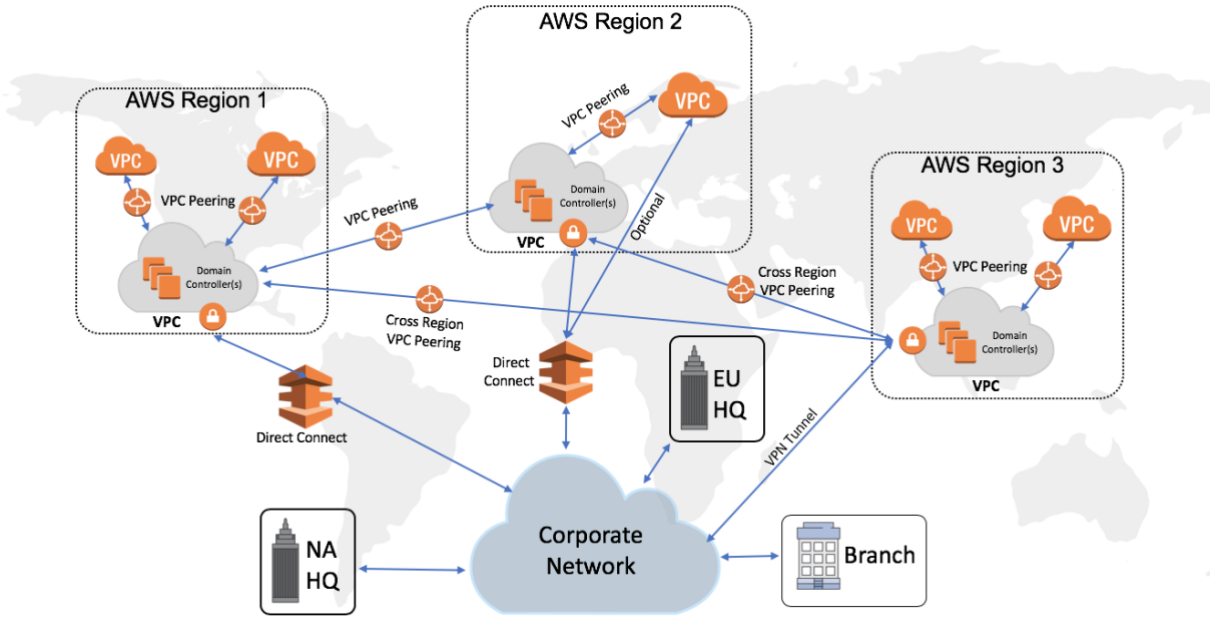

Figure 9: Deploying Active Directory on EC2 instances in multiple regions with multiple VPC's

Consider the following recommendations when deploying Active Directory in this architecture:

- Deploy at least two domain controllers in each region in the N+1 configuration. These domain controllers should be placed in different AZs for availability reasons.
- AD Sites and Services, configure VPCs in a region as a single site and define them accordingly. This configuration ensures all of your member servers can reach all of the DCs in the region as first priority.
- Ensure robust inter-region connectivity exists between all of the regions. Within AWS, you can leverage cross-region VPC peering to achieve highly available private connectivity between the regions. You can also leverage the Transit VPC solution to interconnect multiple regions.

Network connectivity

By default, instances that you launch into a VPC cannot communicate with on-premises network. To extend your existing AD DS into the AWS Cloud, you must connect your on-premises network to the VPC in one of two ways: by using Virtual

Private Network (VPN) tunnels or by using AWS Direct Connect. To connect multiple VPCs in AWS, you can use VPC peering.

IPsec VPN tunnel

The easiest way for extending your on-premises network to your VPC is through IPsec VPN tunnels. Within the VPC, you can create a virtual private gateway that acts as a VPN concentrator on the AWS side of the VPN tunnel. A customer gateway is the anchor on your side of that connection. The customer side gateway can be a physical device or a software appliance. Multiple VPN configuration options are available, including the ability to use multiple on-premises customer gateways and configuring redundant VPN connections to provide failover. For details, see VPN Configuration Examples in the Amazon Virtual Private Cloud User Guide.

Direct Connect

With Direct Connect, you can create virtual interfaces directly to the AWS, bypassing Internet service providers in your network path. There are different configuration choices available when you provision two dedicated connections, including active/active (BGP multipath), and active/passive (failover). For implementation details, see Getting Started in the AWS Direct Connect User Guide.

VPC peering

You can use VPC peering to connect multiple VPCs in the same region or another and within a same account or between different accounts; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck. You can use VPC peering connections to reliably connect multiple VPCs so your Active Directory can be centralized and still be utilized by all of the Microsoft workloads in various VPCs.

Designing AD sites and services topology

It's important to define the AD site correctly along with proper subnet definitions to avoid clients from using domain controllers that are located far away as this would cause increased latency.

Follow these best practices for configuring sites and services:

- Configure one AD site per AWS Region. If you are operating in multiple AWS Regions, we recommend configuring one AD site for each of these regions.

- Define the entire VPC as a subnet and assign it to the AD site defined for this region.
- If you have multiple VPCs in the same region, define each of these VPCs as separate subnets and assign it to the single AD site set up for this region. This setup allows you to use domain controllers in that region to service all clients in that region.
- If you have turned on IPv6 in your Amazon VPC, create the necessary IPv6 subnet definition and assign it to this AD site.
- Define all IP ranges. If clients exist in undefined IP ranges, the clients might not be associated with the correct AD site.
- If you have reliable high-speed connectivity between all of the sites, you can use a single site link for all of your AD sites and maintain a single replication configuration.

Designing DNS resolution

Active Directory Domain Services (AD DS) uses DNS name resolution services to make it possible for clients to locate domain controllers and for the domain controllers that host the directory service to communicate with each other.[2]

Here are some design considerations for DNS resolution:

- Use DNS best practices, like Active Directory integrated zones as well as secure dynamic updates.
- Use domain controllers as DNS servers since domain controllers support features like dynamic updates from Windows DNS clients. Other DNS server types, such as unbound, may not support these features.
- To use DCs as DNS servers, set up DHCP options sets on all of the required VPCs. If you have VPCs that do not have any DCs, you can still set the DHCP scope options since VPC peering (or other network connectivity) make these DNS servers reachable. See DHCP Options Sets in the Amazon Virtual Private Cloud User Guide for more information.
- If you cannot set the DHCP options sets in all the VPCs, then use configuration management tools to selectively set DNS for Windows Servers to point to the domain controllers for DNS.

- Keep the DNS name resolution local to the region and do not cross the region boundary. Therefore, all of the Windows servers in a given region should always use DCs in the same region for DNS.
- If you also have Amazon Route 53 private zones that must be resolved, you can set up your DCs to use Amazon DNS Server (.2 resolver) for all other DNS domains that are not authoritative in AD DNS. This setup allows your DCs to recursively resolve records in Amazon Route 53 private zone.

> **Note:** The Amazon EC2 instance limits the number of packets that can be sent to the Amazon provided DNS server to a maximum of 1024 packets per second per network interface. This limit cannot be increased. If you run into this performance limit, you must set up conditional forwarding for Amazon Route 53 private zones to use the Amazon DNS Server (.2 resolver) and use root hints for Internet name resolution. This setup reduces the chances of you exceeding the 1024 packet limit on AWS DNS resolver.

- If you want to set up hybrid DNS resolution between your data center and AWS, you must set up conditional forwarding on both DNS servers (AWS and on-premises). You must also make sure network path and connectivity (TCP 53 and UDP 53) exist between these DNS servers. You can use VPN or AWS Direct Connect to set up connection between AWS and on-premises DNS servers.

The following figure is an example of DNS resolution design within a single AWS Region. If you have a multi-region deployment, you should deploy similar architecture in each of the regions so that the DNS resolution is highly available and does not depend on any one region.

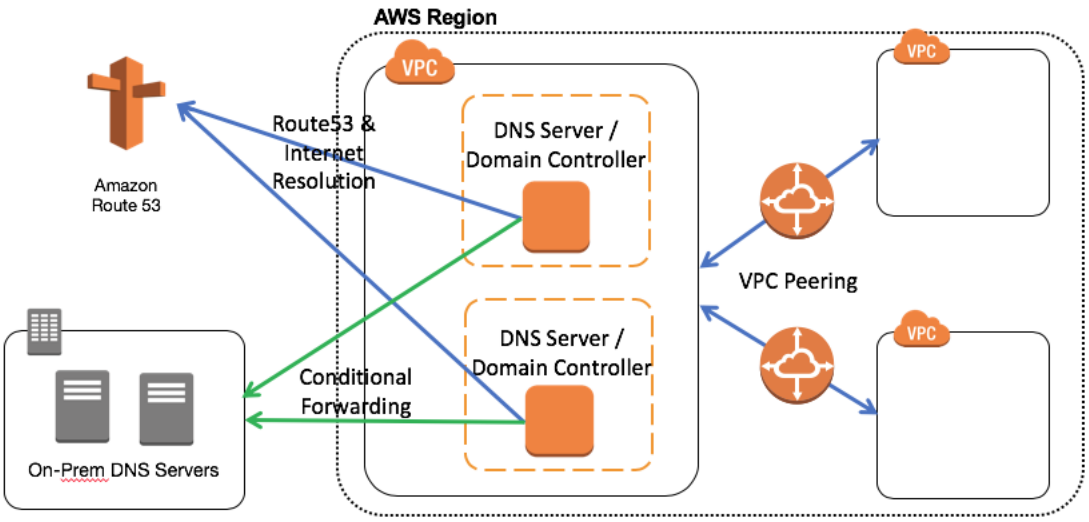

Figure 10: Example of Single Region DNS Setup

For more information on designing a DNS name resolution strategy in a hybrid scenario, see the Hybrid Cloud DNS Solutions Options for Amazon VPC whitepaper.

Trust relationships with on-premises AD

Whether you are deploying Active Directory on EC2 instances or using AWS Managed Microsoft AD, these are the three common deployment patterns seen on AWS.

1. **Deploy a standalone forest/domain on AWS with no trust.** In this model, you set up a new forest and domain on AWS which is different and separate from the current Active Directory that is running on-premises. The main reason for this deployment is keeping the data (accounts/resources) separate between the two domains.

   In this deployment, both accounts (user credentials, service accounts) and resources (computer objects) reside in Active Directory running on AWS and most or all of the member servers run on AWS in single or multiple regions. For this deployment, there is no network connectivity requirement between on-premises and AWS for the purposes of Active Directory as nothing is shared between the two AD forests.

2. **Deploy a new forest/domain on AWS with one-way trust**. If you are planning on leveraging credentials from an on-premises AD on AWS member servers,

you must establish at least a one-way trust to the Active Directory running on AWS. In this model, the AWS domain becomes the resource domain where computer objects are located and on-premises domain becomes the account domain (see diagram below).

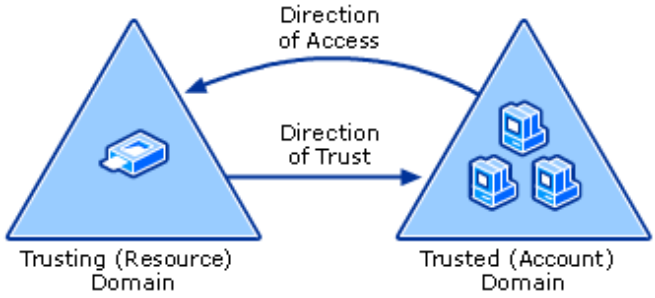

Figure 11: One-way trust relationship

Note that you must have robust connectivity between your data center and AWS without which authentications could fail. Generally, a two-way trust is not commonly deployed because customers choose to extend their Active Directory domain to AWS if they have such a requirement.

3. **Extend your existing domain to AWS**. In this model, you extend your existing Active Directory deployment from on-premises to AWS which means adding additional domain controllers (running on Amazon EC2) to your existing domain and placing them in multiple AZs within your Amazon VPC. If you are operating in multiple regions, add domain controllers in each of these regions. This deployment is easy, flexible, and provides the following advantages:
    - You are not required to set up additional trusts.
    - DCs in AWS are handling both accounts and resources.
    - More resilient to network connectivity issues.
    - You can seamlessly set up and use AWS Cloud in a hybrid scenario with least impact to the applications. (Note that network connectivity is required between your data center and AWS for initial and on-going replication of data between the domain controllers.)

See How Domain and Forest Trusts Work on the Microsoft Docs website for more information.

Security considerations

Multi factor authentication

Multi-factor authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when users sign in to an AWS console, they are prompted for their username and password (the first factor—what they know), then prompted for an authentication response from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources. We recommend enabling MFA on all of your privileged accounts regardless of whether you are using IAM or federating through SSO.

AWS account security

Since you are running your domain controllers on EC2, securing your AWS account is an important process in securing your Active Directory domain. Follow these recommendations to make sure your AWS account is secure.

- Enable MFA and then lock away your AWS root user credential
- Use IAM Groups to manage permission if you are using IAM users
- Grant least privilege to all your users within AWS
- Enable MFA for all privileged users
- Use EC2 Roles for applications that run on EC2 instances
- Do not share access keys
- Rotate credentials regularly
- Turn on and analyze log files in AWS CloudTrail, VPC Flow logs and Amazon S3 bucket logs
- Turn on encryption for data at rest and in transit where necessary

Domain controller security

Domain controllers provide the physical storage for the AD DS database, in addition to providing the services and data that allow enterprises to effectively manage their servers, workstations, users, and applications. If privileged access to a domain controller is obtained by a malicious user, that user can modify, corrupt, or destroy the AD DS database and, by extension, all of the systems and accounts that are managed

by Active Directory. Make sure your domain controller is secure to avoid compromising your Active Directory data.

The following points are some of the best practices to secure domain controllers running on AWS:

- Secure the AWS account where the domain controllers are running by following least privilege and role-based access control.
- Ensure unauthorized users don't have access in your AWS account to create/access Amazon Elastic Block Store (Amazon EBS) snapshots, launch or terminate EC2 Instances, or create/copy EBS volumes.
- Ensure you are deploying your domain controllers in a private subnet without Internet access. Ensure that subnets where domain controllers are running don't have a route to a NAT gateway or other device that would provide outbound Internet access.
- Keep your security patches up-to-date on your domain controllers. We recommend you first test the security patches in a non-production environment.
- Restrict ports and protocols that are allowed into the domain controllers by using security groups. Allow remote management like remote desktop protocol (RDP) only from trusted networks.
- Leverage the Amazon EBS encryption feature to encrypt the root and additional volumes of your domain controllers and use AWS Key Management Service (AWS KMS) for key management.

Security group configuration

When launched, Amazon EC2 Instances must be associated with a security group, which acts as a stateful firewall with rules scoped by protocol, port number, source and destination IP address, and other security groups.

We recommend configuring AWS Security Groups to control access to the domain controllers so that only the required Active Directory ports are allowed into the DCs and from selective origin networks where clients or other domain controllers reside.

For step-by-step guidance for implementing rules, see Adding Rules to a Security Group in the Amazon EC2 User Guide.

Network port configuration

Active Directory requires certain network ports open to allow traffic for LDAP, AD DS replication, user authentication, Windows Time services, Distributed File System (DFS), and many more.

For a complete list of ports, see Active Directory and Active Directory Domain Services Port Requirements in the Microsoft TechNet Library.

Other considerations

FSMO Roles. You can follow the same recommendation you would follow for your on-premises deployment to determine FSMO roles on DCs. See also best practices from Microsoft. In the case of AWS Managed Microsoft AD, all domain controllers and FSMO roles assignments are managed by AWS and do not require you to manage or change them.

Global Catalog. Unless you have slow connections or an extremely large AD database, we recommend making all of your domain controllers (except the DC with the infrastructure master role) also global catalog servers so that clients have no problems reaching a global catalog when needed.

If you are hosting Microsoft Exchange in AWS cloud, at least one global catalog server is required on the site with Exchange servers. For more information about global catalog, see Microsoft documentation. Since there is only one domain in the forest for AWS Managed Microsoft AD, all domain controllers are configured as global catalog and will have full information about all objects.

Read Only Domain Controllers (RODC). It's possible to deploy RODC on AWS if you are running AD on EC2 Instances and require it, and there are no special considerations for doing so. AWS Managed Microsoft AD does not support RODCs. All of the domain controllers that are deployed as a part of AWS Managed Microsoft AD are writable domain controllers.

Conclusion

AWS provides several options for deploying and managing Active Directory Domain Services in the cloud and hybrid environments. You can leverage AWS Managed Microsoft AD if you no longer want to focus on heavy lifting like managing the

availability of the domain controllers, patching, backups, and so on. Or, you can run Active Directory on EC2 Instances if you want more flexibility in your deployment configuration. In this whitepaper we have discussed these two main approaches of deploying Active Directory on AWS and have provided you with guidance and consideration for each of the design. Depending on our deployment pattern, scale, requirements and SLA, you may select one of these options to support your Windows workloads on AWS.

Contributors

The following individuals and organizations contributed to this document:

- Vinod Madabushi, Enterprise Solutions Architect, Amazon Web Services
- Vladimir Provorov, Senior Solutions Architect, Amazon Web Services

Further Reading

For additional information, see the following:

- AWS Whitepapers
- AWS Directory Service
- Microsoft Workloads on AWS
- Active Directory Domain Services on the AWS Cloud: Quick Start Reference Deployment
- AWS Documentation

Document Revisions

Date	Description
December 2018	First publication

Notes

[1] http://download.microsoft.com/download/f/c/a/fca7c6e3-7153-4fb1-9825-0b1bb26f14e0/an-overview-of-aad.docx

[2] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/dns-and-ad-ds