Active Directory Domain Services on AWS

Design and Planning Guide

November 20, 2020

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. 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

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 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 *de facto* standard technology for centralized management of Microsoft 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 for authentication. Successful adoption of cloud technology requires considering existing IT infrastructure and applications deployed on-premises. Reliable and secure Active Directory architecture is a critical IT infrastructure foundation for companies running Windows workloads.

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) that redirects directory requests from AWS applications and services to existing Microsoft Active Directory without caching any information in the cloud. It does not require any trusts or synchronization of user accounts.

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

Active Directory 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 for what IP addresses and 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.

Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically isolated section of the 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 the 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.

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.

AWS Single Sign-On (AWS 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 Transit Gateway is a service that enables customers to connect their VPCs and their on-premises networks to a single gateway.

Domain controller (DC) – an Active Directory server that responds to authentication requests and store a replica of Active Directory database.

Flexible Single Master Operation (FSMO) roles. In Active Directory, some critical updates are performed by a designated domain controller with a specific role and then replicated to all other DCs. Active Directory uses roles that are assigned to DCs for these special tasks. Refer to the Microsoft documentation web-site for more information on FSMO roles.

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.

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 provided.

VPC Peering. A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 or IPv6

addresses. Instances in either VPC can communicate with each other as if they are within the same network.

Shared responsibility model

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

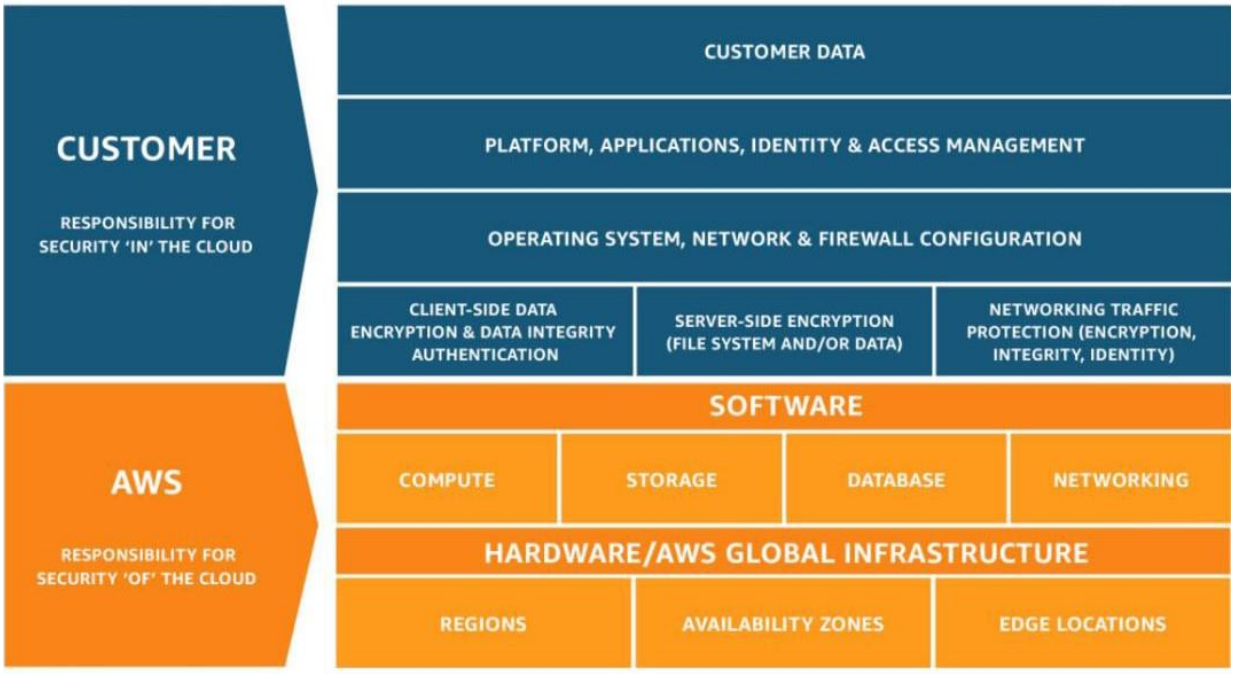

Figure 1. Shared Responsibility Model when operating in AWS Cloud

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 Active Directory environment. You can set up custom configurations and create a complex 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 instance deployment in one or multiple regions, operational management of your directory, 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 that 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 using 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 compatible with AWS Managed Microsoft AD only. Amazon FSx for Windows File Server can be deployed with AWS Managed Microsoft AD or self-managed Active Directory.

AWS Managed Microsoft Active Directory

AWS Directory Service lets you run Microsoft Active Directory as a managed service. By default, each AWS Managed Microsoft AD 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 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. Multi-Region replication can be used to automatically replicate your AWS Managed Microsoft AD directory data across multiple Regions so you can improve performance for users and applications in disperse geographic locations. AWS Managed Microsoft AD uses native AD replication to replicate your directory's data securely to the new Region. Multi-Region replication is only supported for the Enterprise Edition of AWS Managed Microsoft AD.

AWS Managed Microsoft AD enables you to forward all domain controller's Windows Security event log 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 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 is 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. These editions have different storage capacity; Enterprise Edition also has multi-region features.

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, deploying Amazon RDS databases with Windows authentication, using FSx for Windows File Services, and signing in to productivity tools like Amazon Chime and Amazon WorkSpaces. For more information on this solution, see 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. For more information, see Design considerations for running Active Directory on EC2 instances in this document.

Comparison of Active Directory Services on AWS

The following table compares the features and functions between various Directory Services options available on AWS. Many features are not applicable directly to AWS AD Connector, because it is actins only as a proxy to the existing Active Directory domain.

Function	AWS AD Connector	AWS Managed Microsoft AD	Active Directory on EC2
Managed service	yes	yes	no
Multi-Region deployment	n/a	yes, Enterprise	yes
Share directory with multiple accounts	no	yes	no
Supported by AWS applications (Amazon Chime, Amazon WorkSpaces, AWS Single Sign-On & etc.)	yes	yes	yes (through federation or AD Connector)

Function	AWS AD Connector	AWS Managed Microsoft AD	Active Directory on EC2
Supported by RDS (SQL Server, Oracle, MySQL, PostgreSQL, and MariaDB)	n/a	yes	no
Supported by FSx for Windows File Server	n/a	yes	yes
Creating users and groups	yes	yes	yes
Joining computers to the domain	yes	yes	yes
Create trusts with existing Active Directory domains and forests	n/a	yes	yes
Seamless domain join for Windows and Linus EC2 instances	yes	yes	yes, with AWS AD Connector
Schema extensions	n/a	yes	yes
Add domain controllers	n/a	yes	yes
Group Managed Service Accounts	n/a	yes	Depends on the Windows Server version
Kerberos constrained delegation	n/a	yes	yes
Support Microsoft Enterprise CA	n/a	yes	yes
Multi-Factor Authentication	yes, through RADIUS	yes, through RADIUS	yes, with AD Connector
Group policy	n/a	yes	yes
Active Directory Recycle bin	n/a	yes	yes
PowerShell support	n/a	yes	yes

Core infrastructure design on AWS for Windows Workloads and Directory Services

Planning AWS accounts and Organization

AWS Organizations helps you centrally manage your AWS accounts, identity services, and access policies for your workloads on AWS. Whether you are a growing startup or a large enterprise, Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts. For more information, refer to the AWS Organizations User Guide.

With AWS Organizations you can centrally define critical resources and make them available to accounts across your organization. For example, you can authenticate against your central identity store and enable applications deployed in other accounts to access it.

If your users need to manage AWS services and access AWS applications with their Active Directory credentials, we recommend integrating your identity service with the management account in AWS Organizations.

- Deploy AWS Managed AD in the management account with trust to your on-premises Active Directory to allow users from any trusted domain to access AWS Applications. Share AWS Managed AD to other accounts across your organization.
- Deploy AWS Single Sign-On in the management account to centrally manage access to multiple AWS accounts and business applications and provide users with single sign-on access to all their assigned accounts and applications from one place. AWS SSO also includes built-in integrations to many business applications, such as Salesforce, Box, and Microsoft Office 365.

Network design considerations for AWS Managed Microsoft AD

Network design for Microsoft workloads and directory services consists of network connectivity and DNS names resolution.

To plan the network topology for your organization, refer to the whitepaper Building a Scalable and Secure Multi-VPC AWS Network Infrastructure, and consider the following recommendations:

- Plan your IP networks for Microsoft workloads without overlapping address spaces. Microsoft does not recommend using Active Directory over NAT.
- Place directory services into a centralized VPC that is reachable from any other VPC with workloads depending on Active Directory.
- By default, instances that you launch into a VPC cannot communicate with your 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 or AWS Transit Gateway.

Network port requirements and security groups

Active Directory requires certain network ports to be open to allow traffic for LDAP, AD DS replication, user authentication, Windows Time services, Distributed File System (DFS), and many more. When you deploy Active Directory on EC2 instances using the AWS Quick Start or AWS Managed Microsoft AD, it automatically creates a new security group with all required port rules. If you manually deploy your Active Directory, you need to create a security group and configure rules for all required network protocols.

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

DNS names resolution

Active Directory heavily relies on DNS services and hosts its own DNS services on domain controllers. To establish seamless name resolution in all your VPCs and your on-premises network, create a Route 53 Resolver, deploy inbound/outbound endpoints in your VPC, and configure conditional forwarders to all of your Active Directory domains (including AWS Managed AD and on-premises Active Directory) in the Route 53 Resolver.

Share centralized Route 53 Resolver endpoints across all VPC in your organization. Create conditional forwarders on your on-premises DNS servers for all Route 53 DNS

zones and DNS zones on AWS Managed AD and point them to Route 53 Resolver Endpoints.

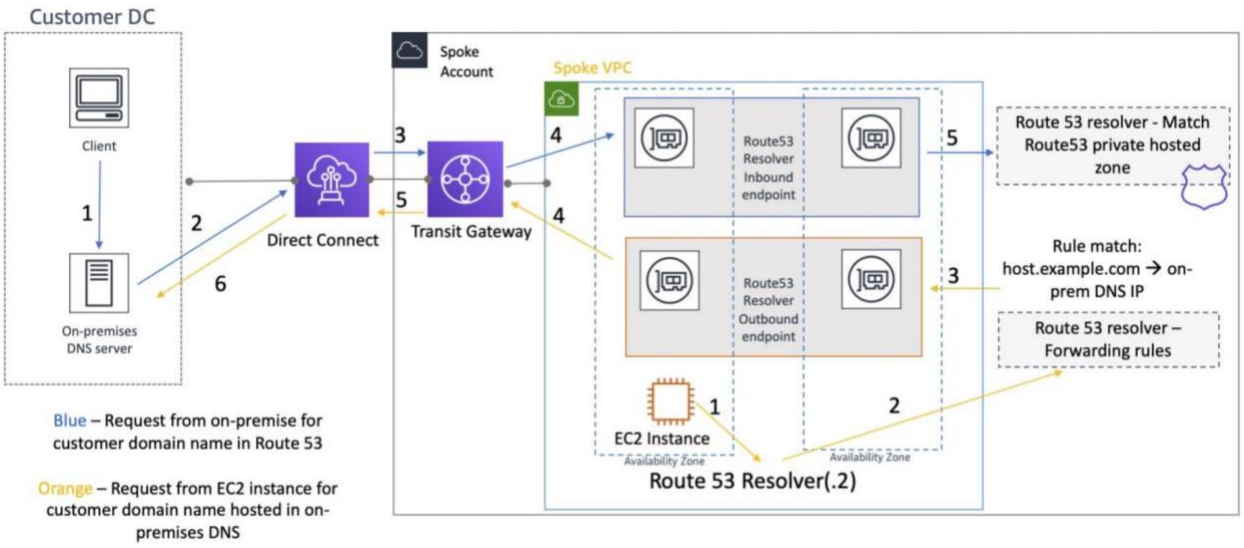

Figure 2. Route 53 Resolver configuration for hybrid network.

Here are design considerations for DNS resolution:

- Make all Active Directory DNS domains resolvable for all clients, because they are using it to locate Active Directory services and register their DNS names using dynamic updates.
- Try to keep the DNS name resolution local to the AWS Region to reduce latency.
- Use Amazon DNS Server (.2 resolver) as a forwarder for all other DNS domains that are not authoritative on your DNS Servers on Active Directory domain controllers. This setup allows your DCs to recursively resolve records in Amazon Route 53 private zone and use Route 53 Resolver conditional forwarders.
- Use Route 53 Resolver Endpoints to create DNS resolution hub and manage DNS traffic by creating conditional forwarders. For more information on designing a DNS name resolution strategy in a hybrid scenario, see the Amazon Route 53 Resolver for Hybrid Clouds blog post.

> **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.

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 administrators.

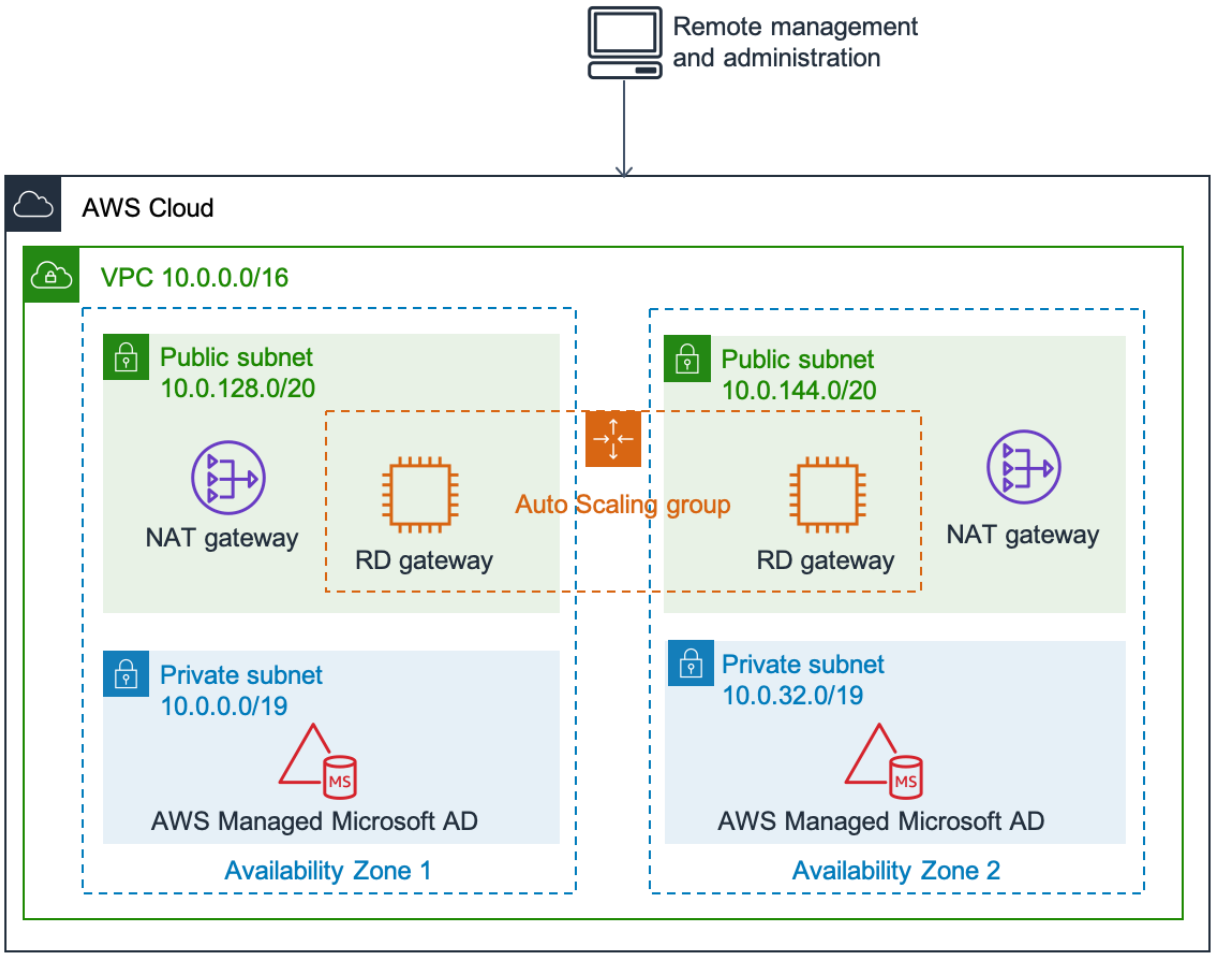

Figure 3. Managed Active Directory architecture deployed by Quick Start.

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 seamlessly join your Amazon EC2 Windows instances to AWS Managed Microsoft AD.

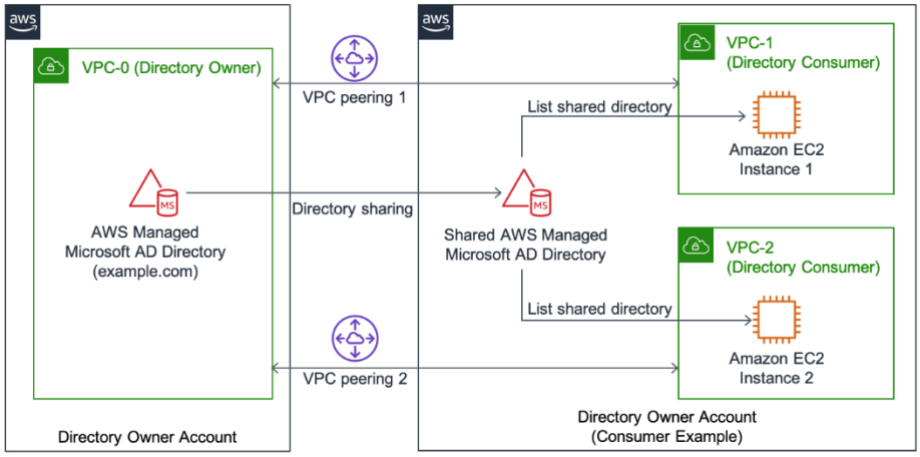

Figure 4. Sharing single AWS Managed Microsoft AD with another account.

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 Active Directory. 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 Active Directory to join EC2 Windows instances, but you maintain control of all administrative tasks.

Deploy AWS Managed AD in your management account of AWS Organizations. This allows you to use Managed AD for authentication with AWS Identity and Access Management (IAM) to access the AWS Management Console and other AWS applications using your Active Directory credentials.

Multiple AWS Regions deployment

AWS Managed Microsoft AD Enterprise Edition supports Multi-Region deployment. You can use automated multi-Region replication in all Regions where AWS Managed Microsoft AD is available.

AWS services such as Amazon RDS for SQL Server and Amazon FSx connect to the local instances of the global directory. This allows your users to sign-in once to AD-aware applications running in AWS as well as AWS services like Amazon RDS for SQL Server in any AWS Region – using credentials from AWS Managed Microsoft AD or a

trusted AD domain or forest. Refer to AWS Directory Service documentation for the current list of AWS Services supporting Multi-Region replication feature.

With multi-Region replication in AWS Managed Microsoft AD, AD-aware applications such as SharePoint, SQL Server Always On, AWS services such as Amazon RDS for SQL Server, and Amazon FSx for Windows File Server, use the directory locally for high performance and are multi-Region for high resiliency. The following list comprises additional benefits of Multi-Region replication.

- It enables you to deploy a single AWS Managed Microsoft AD instance globally, quickly, and eliminates the heavy lifting of self-managing a global AD infrastructure.
- Optimal performance for workloads deployed in multiple regions.
- Multi-Region resiliency. AWS Managed Microsoft AD handles automated software updates, monitoring, recovery, and the security of the underlying AD infrastructure across all Regions.
- Disaster recovery. In the event that all domain controllers in one Region are down, AWS Managed Microsoft AD recovers the domain controllers and replicates the directory data automatically. Meanwhile domain controllers in other Regions are up and running.

To deploy AWS Managed Microsoft AD across multiple Regions, you must create it in Primary region and after that add one or more Replicated regions. Consider following factors for your Active Directory design:

- When you deploy a new Region, AWS Managed Microsoft AD creates two domain controllers in the selected VPC in the new Region. You can add more domains controllers later for scalability.
- AWS Managed Microsoft AD uses a backend network for replication and communications between domain controllers.
- AWS Managed Microsoft AD creates a new Active Directory Site and names it the same name of the Region. For example, us-east-1. You can also rename this later using the Active Directory Sites & Services tool
- AWS Managed AD is configured to use change notifications for inter-site replications to eliminate replication delays.

After you add your new Region, you can do any of the following tasks:

- Add more domain controllers to the new Region for horizontal scalability.
- Share your directory with more AWS accounts per Region. Directory sharing configurations are not replicated from the primary Region and you may have different sharing configuration in different region based on your security requirements.
- Enable log forwarding to retrieve your directory's security logs using Amazon CloudWatch Logs from the new Region. When you enable log forwarding, you must provide a log group name in each Region where you replicated your directory.
- Enable Amazon Simple Notification Service (Amazon SNS) monitoring for the new Region to track your directory health status per Region.

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 Active Directory credentials to access supported Amazon enterprise applications. When you enable MFA, your users enter their user name and password (first factor), and then enter an authentication code (second factor) that 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 mobile phone).

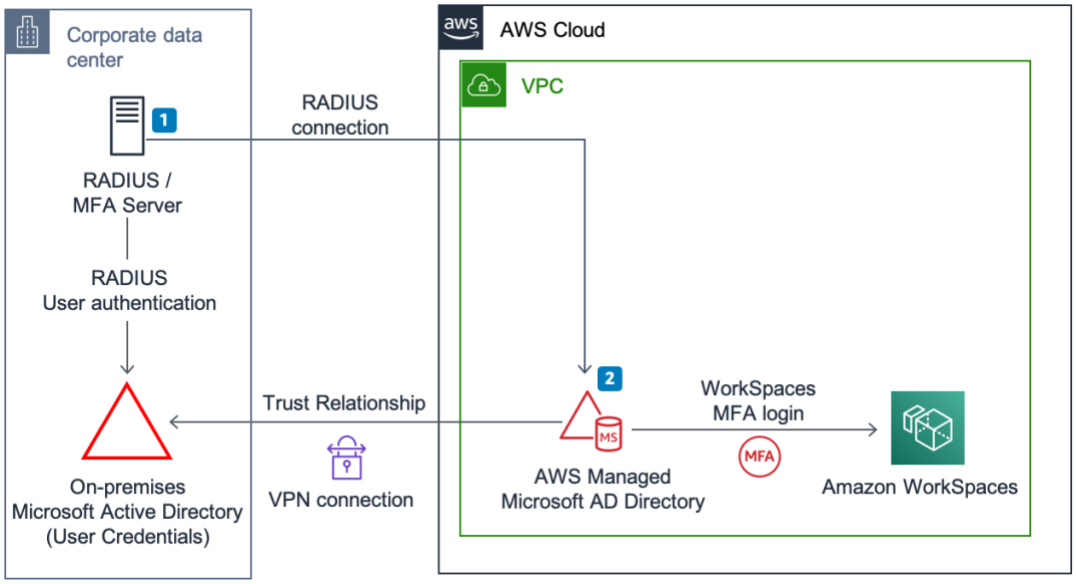

Figure 6. Using AWS Managed Microsoft Active Directory with MFA for access to Amazon WorkSpaces

A more 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 level 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. Depending on the number of Regions where you are deploying your solution, your Active Directory design may slightly differ. 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 need 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 AWS Transit Gateway.

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

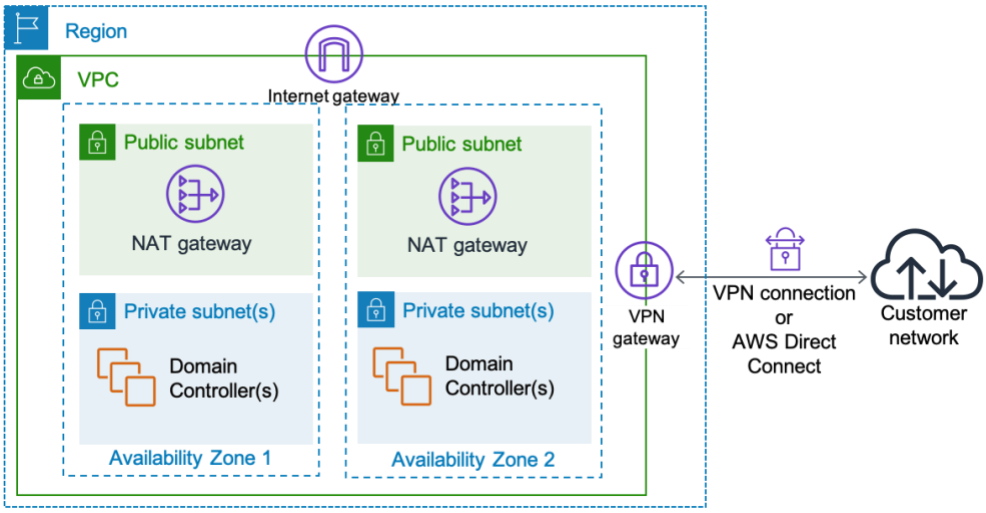

Figure 7. Deploying Active Directory on EC2 instances in a single Region for single VPC.

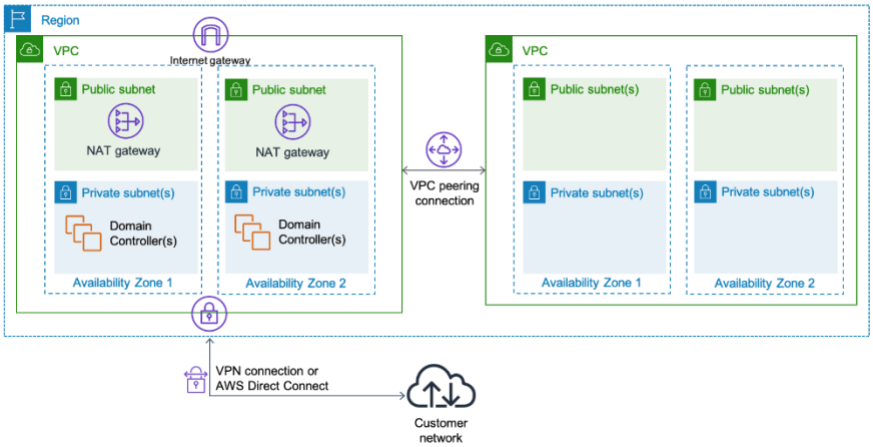

Figure 8. Deploying Active Directory on EC2 instances in a single Region for multiple VPCs.

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

- We recommend deploying at least two domain controllers (DCs) in a Region. 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.

- Configure VPCs in a Region as a single Active Directory site and define Active Directory subnets accordingly. This configuration ensures that all of your clients correctly select the closest available DC.
- 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.
- If you want to use your self-managed Active Directory credentials to access AWS Services or third-party services, you can integrate your self-managed AD with AWS IAM and AWS Single Sign-On using AWS AD Connector or AWS Managed AD through a trust relationship. In these cases, AD Connector or AWS Managed AD must be deployed in the management account of your organization.

Multi-region/global deployment of self-managed AD

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 depict 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.

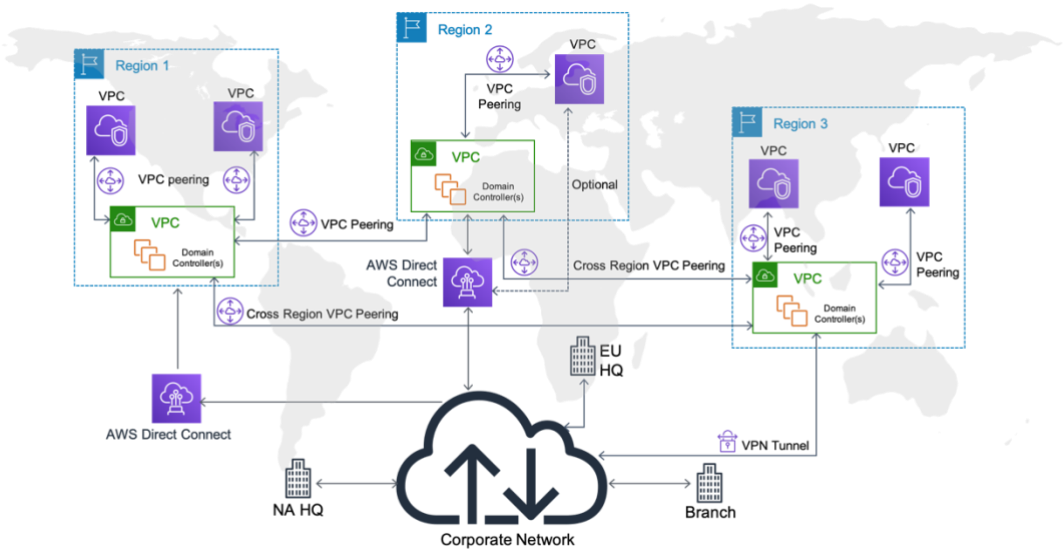

Figure 9. Deploying Active Directory on EC2 instances in multiple Regions with multiple VPCs.

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

- Deploy at least two domain controllers in each Region. These domain controllers should be placed in different AZs for availability reasons.
- Configure VPCs in a region as a single Active Directory site and define Active Directory subnets accordingly. This configuration ensures all of your clients will correctly select the closest available domain controller.
- 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.

Designing Active Directory sites and services topology

It's important to define Active Directory sites and subnets correctly to avoid clients from using domain controllers that are located far away as this would cause increased latency. See [How Domain Controllers are Located in Windows.]

Follow these best practices for configuring sites and services:

- Configure one Active Directory site per AWS Region. If you are operating in multiple AWS Regions, we recommend configuring one Active Directory site for each of these Regions.
- Define the entire VPC as a subnet and assign it to the Active Directory 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 Active Directory 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 enabled IPv6 in your Amazon VPC, create the necessary IPv6 subnet definition and assign it to this Active Directory site.
- Define all IP address ranges. If clients exist in undefined IP address ranges, the clients might not be associated with the correct Active Directory 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.
- Use consistent sites names in all AD forests connected by trusts.

Security considerations

Trust relationships with on-premises Active Directory

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. 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 Active Directory forests.

2. Deploy a new forest/domain on AWS with one-way trust. If you are planning on leveraging credentials from an on-premises Active Directory 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.

> **Note:** You must have robust connectivity between your data center and AWS. A connectivity issue can break the authentication and make the whole solution not accessible for users. Consider to extend your Active Directory domains to AWS to eliminate dependency on connectivity with on-premises infrastructure or deploy a multi-path AWS Direct Connect or VPN connection.

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.)

When you use cross-forest trust relationships in Active Directory, you need to use consistent Active Directory site names in both forests to have optimal performance. Refer to the article Domain Locator Across a Forest Trust for more information.

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

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 the AWS Management Console, they are prompted for their user name 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 Amazon 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.
- Follow Microsoft-recommended security configuration baselines and Best Practices for Securing Active Directory.

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 Active Directory database, we recommend adding global catalog role to all of your domain

controllers in multi-domain forests (except the domain controller with the Infrastructure Master role).

If you are hosting Microsoft Exchange in AWS Cloud, at least one global catalog server is required in a 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 Active Directory 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 need to have full administrative control on your Active directory. 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

Contributors to this document include:

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

Further Reading

For additional information, see:

- 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
November 2020	AWS Managed Microsoft AD multi-region feature update
August 2020	Numerous updates throughout
December 2018	First publication