Service Name

AWS Directory Service

Service Overview

AWS Directory Service provides multiple ways to use Microsoft Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) with other AWS services. It is a collection of directory options that store information about users, groups, and devices, enabling administrators to manage access to information and resources. The service includes three main options: AWS Managed Microsoft AD (a fully managed Microsoft Windows Server Active Directory service in the AWS Cloud), AD Connector (a proxy service for connecting existing on-premises Microsoft AD to AWS), and Simple AD (a Samba 4-based directory compatible with basic Active Directory features). The service enables migration of Active Directory-aware applications to the AWS Cloud while supporting various AWS managed applications and services.

Key Use Cases

- Enterprise directory services: Migrate Active Directory-aware applications like Microsoft SharePoint, SQL Server, and .NET applications to AWS Cloud
- Hybrid cloud integration: Extend existing on-premises Active Directory infrastructure to AWS using AD Connector or trust relationships
- Single Sign-On (SSO): Enable users to access AWS Management Console and applications using existing Active Directory credentials
- AWS service authentication: Authenticate and authorize access for AWS services like WorkSpaces, WorkDocs, RDS for SQL Server, Amazon Chime, and Amazon Connect
- Compliance workloads: Support applications subject to HIPAA and PCI DSS compliance requirements
- Multi-region deployments: Replicate directories across multiple AWS regions for global workload management

Features

- **AWS Managed Microsoft AD**: Fully managed Windows Server 2019 Active Directory with high availability, automatic patching, monitoring, and recovery across multiple Availability Zones
- **AD Connector**: Proxy service that connects AWS applications to existing on-premises Microsoft Active Directory without caching information in the cloud
- **Simple AD**: Samba 4-based directory providing basic Active Directory compatibility for low-scale, cost-effective directory needs

- **Multi-Region Replication**: Enterprise Edition feature enabling directory replication across multiple AWS regions for global workload support
- **Directory Sharing**: Share directories across multiple AWS accounts and VPCs within an organization
- **Trust Relationships**: Create trust relationships between AWS Managed Microsoft AD and existing on-premises or cloud-based Active Directory domains
- **Schema Extensions**: Extend Active Directory schema to support custom attributes and object classes
- **LDAPS Support**: Secure LDAP communications with server-side and client-side LDAPS encryption
- **Multi-Factor Authentication**: Integration with RADIUS servers for MFA support across directory types

Value Proposition

AWS Directory Service offers significant advantages over self-managed Active Directory solutions by providing a fully managed service that eliminates the operational overhead of maintaining domain controllers, patching, monitoring, and ensuring high availability. The service delivers enhanced security with built-in encryption, compliance certifications (HIPAA, PCI DSS), and AWS security best practices:

- It provides seamless integration with over 15 AWS services and applications, enabling rapid cloud adoption without requiring directory infrastructure changes
- The service offers flexible deployment options including standalone cloud directories, hybrid connectivity to on-premises infrastructure, and multi-region replication for global scalability
- Cost optimization is achieved through pay-as-you-use pricing, elimination of hardware costs, and reduced administrative overhead while maintaining enterprise-grade reliability and performance

Service Integration

AWS Directory Service integrates deeply with core AWS services including Amazon WorkSpaces for virtual desktops, Amazon WorkDocs for document collaboration, Amazon WorkMail for email services, and Amazon Chime for communications. It supports database services through Amazon RDS for SQL Server, Oracle, and PostgreSQL with Windows Authentication:

- The service enables single sign-on to the AWS Management Console through AWS IAM Identity Center integration and supports Amazon EC2 domain joining for both Windows and Linux instances
- Additional integrations include Amazon FSx for Windows File Server for shared storage, AWS Client VPN for secure remote access, Amazon Connect for contact

center solutions, AWS Transfer Family for secure file transfers, and AWS Private Certificate Authority for certificate management
- The service also works with AWS Organizations for cross-account directory sharing and AWS CloudTrail for comprehensive logging and monitoring

Onboarding and Offboarding

Customers begin by selecting the appropriate directory type based on their needs: AWS Managed Microsoft AD for full Active Directory features, AD Connector for hybrid connectivity, or Simple AD for basic requirements. The setup process requires creating an Amazon VPC with at least two subnets in different Availability Zones:

- For AWS Managed Microsoft AD, customers provide directory information including DNS name, NetBIOS name, administrator password, and VPC configuration
- The service automatically creates domain controllers and DNS services within 20-40 minutes
- Customers can then join EC2 instances to the domain, configure trust relationships with existing infrastructure, enable AWS applications, and set up user management through the AWS Management Console or Active Directory tools
- A 30-day free trial with 1,500 hours of usage is available for evaluation

Getting Started Guide: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started.html

Data Removal

When offboarding from AWS Directory Service, customers must first deauthorize all AWS applications and services connected to the directory, remove any trust relationships with external domains, and unjoin all EC2 instances from the domain. The directory deletion process permanently removes all directory data including users, groups, organizational units, and configuration settings. For AWS Managed Microsoft AD, customers should create manual snapshots before deletion for backup purposes, though snapshots have a maximum age limit of 180 days. Once a directory is deleted, all associated data is permanently removed and cannot be recovered.

Backup/Restore and Disaster Recovery

AWS Directory Service provides automated daily snapshots for AWS Managed Microsoft AD directories with a retention period determined by AWS. Customers can create up to 5 manual snapshots per directory for point-in-time recovery, with snapshots having a maximum supported age of 180 days. Directory restoration from snapshots moves the directory back in time and may result in data loss for changes made after the snapshot date. The service includes built-in high availability across multiple Availability Zones and automatic recovery capabilities. However, snapshots cannot be created for AD Connector directories since they only proxy requests to existing infrastructure.

Backup Capabilities

AWS Directory Service supports manual snapshot creation for AWS Managed Microsoft AD directories, allowing up to 5 snapshots per directory with 180-day maximum age. The service includes automated daily snapshots managed by AWS:

- While AWS Directory Service does not directly integrate with AWS Backup service, customers can implement backup strategies for connected resources and applications
- AD Connector and Simple AD have limited backup capabilities since AD Connector proxies to existing infrastructure and Simple AD data recovery relies on directory recreation

Disaster Recovery

AWS Directory Service provides built-in disaster recovery through multi-Availability Zone deployment of domain controllers, ensuring service continuity if one zone fails. Enterprise Edition supports multi-region replication for geographic disaster recovery:

- The service does not directly integrate with AWS Elastic Disaster Recovery, but supports disaster recovery strategies through snapshot restoration, cross-region replication, and integration with other AWS disaster recovery services
- Trust relationships and hybrid connectivity options provide additional resilience by maintaining connections to on-premises infrastructure as backup authentication sources

Recovery Objectives

AWS Directory Service helps customers achieve Recovery Point Objectives (RPO) through manual snapshots that can be created as frequently as needed within the 5-snapshot limit, providing point-in-time recovery capabilities. Recovery Time Objectives (RTO) are supported through built-in high availability across multiple Availability Zones for automatic failover, and multi-region replication in Enterprise Edition for faster geographic recovery. The service’s automated recovery mechanisms and managed infrastructure reduce RTO compared to self-managed solutions, while snapshot restoration capabilities enable RPO management based on backup frequency requirements.

Service Constraints

Service Quotas: https://docs.aws.amazon.com/general/latest/gr/ds_region.html

FAQ: https://aws.amazon.com/directoryservice/faqs/

Technical Requirements

Service Documentation: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

User Guide: https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

API Reference: https://docs.aws.amazon.com/directoryservice/latest/devguide/welcome.html

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: https://aws.amazon.com/directoryservice/pricing/

Cost Optimization

AWS Directory Service offers several unique cost optimization opportunities including right-sizing directory editions based on object count and feature requirements (Standard vs Enterprise vs Hybrid), optimizing domain controller count by monitoring CloudWatch performance metrics, and leveraging directory sharing to reduce costs across multiple AWS accounts rather than creating separate directories. The 30-day free trial provides 1,500 hours for evaluation without upfront costs:

- Customers can reduce data transfer costs by avoiding NETLOGON and SYSVOL shares for file storage in multi-region deployments
- Simple AD and AD Connector offer no-cost options when used with WorkSpaces, WorkDocs, or WorkMail with minimum user requirements, providing significant savings for basic directory needs

Savings Considerations

Primary cost savings include eliminating on-premises directory infrastructure costs (hardware, software licenses, maintenance), reducing administrative overhead through fully managed services, and paying only for actual usage without upfront commitments. The service eliminates Windows Server licensing costs for domain controllers and reduces operational expenses through automated patching, monitoring, and high availability management:

- Multi-account directory sharing prevents duplicate directory costs across organizations
- Customers can achieve additional savings by choosing appropriate directory types (Simple AD for basic needs, AD Connector for hybrid scenarios), optimizing domain controller counts based on actual performance requirements, and leveraging the free tier benefits when using directories with qualifying AWS applications like WorkSpaces with minimum user thresholds