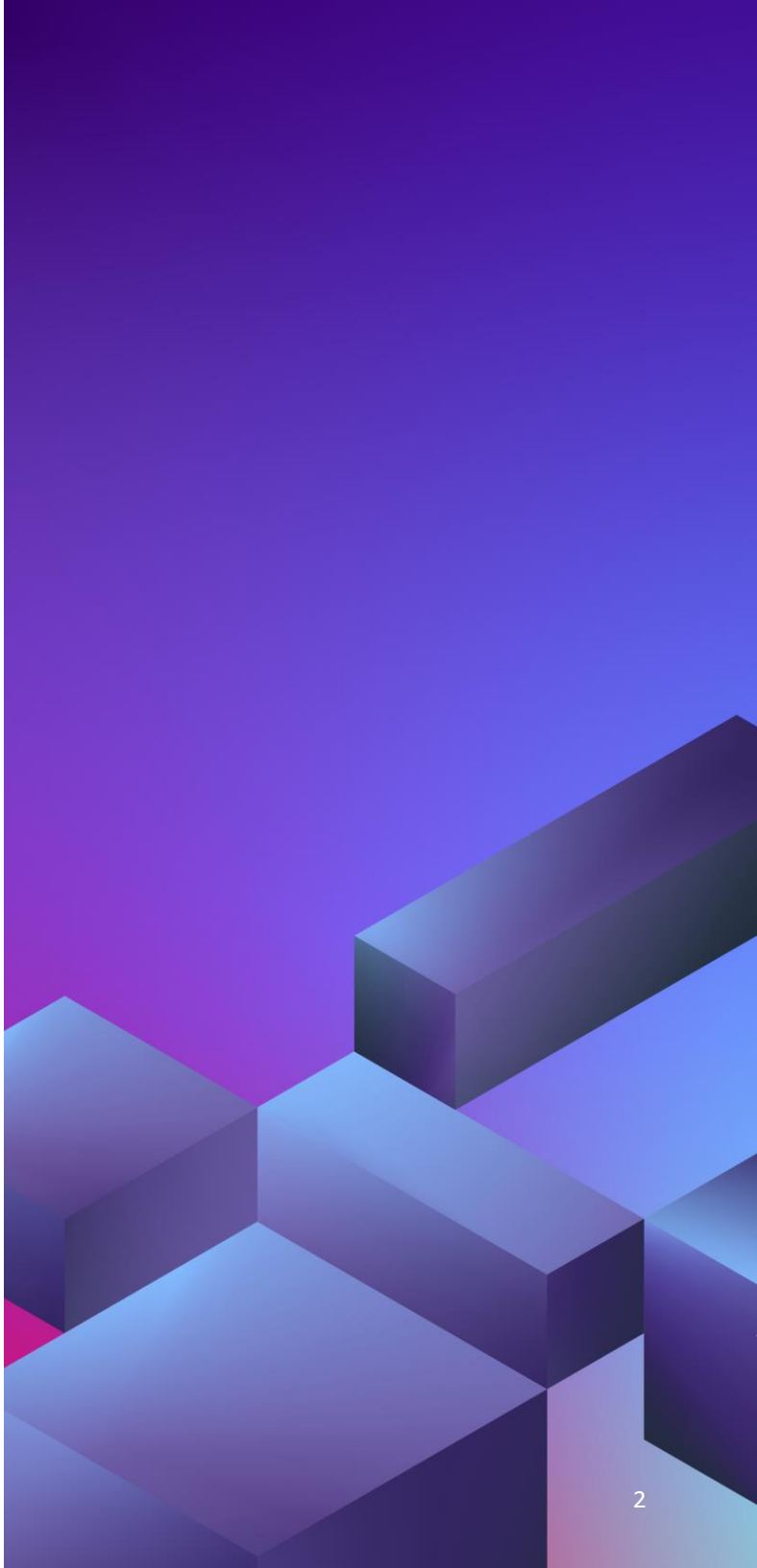
Guide to Microsoft Workloads Modernization

Introduction

For many years, companies across industries have adopted technology solutions to power the success of their business. While some had the luxury of being born in the cloud, the vast majority invested in applications designed for on-premises data centers using the prevalent technologies of the early 2000s, such as those built by Microsoft, SAP, and Oracle.

With the accelerating emergence of digitally born businesses and the increasing pressure to out-innovate competition, companies are faced with the critical task of transforming their existing technology portfolio for the digital expectations of today's customers.

AWS has helped these companies transform their existing Windows-based workloads for over 14 years. We observed the common technical choices and techniques that customers such as Expedia, Pearson, Xero, SeatGeek, and DraftKings have used to successfully modernize their Windows-based applications, data, and identity solutions. Through modernization, these customers realize benefits that include lower costs, increased scalability, faster feature delivery, and improved development and operational agility. The time is now to help your organization achieve these results and free your teams from maintaining your monolithic legacy systems. In this guide, we cover the common approaches our customers use to modernize their Windows-based applications and the tools, services, and support AWS has to help you in your modernization journey.



TERMINOLOGY

Modernization approach common terms guide

Before diving deep into each modernization approach, we will define the common terms that will be used throughout this guide to establish a shared understanding. The definitions for rehost, re-platform, refactor, and rearchitect are based on Gartner's definitions of the 7 Options to Modernize Legacy Systems.

Common Terms	Definitions
Modernization	Modernization is the process of progressively transforming existing applications and infrastructure to extend into higher-value cloud-native services that unlock new business capabilities, accelerate innovation, and reduce technical debt.
Rehost	Redeploy the application component to other infrastructures (physical, virtual, or cloud) without modifying its code, features, or functions
Re-platform	Migrate to a new runtime platform, making minimal changes to the code but not the code structure, features, or functions.
Refactor	Restructure and optimize the existing code (although not its external behavior) to remove technical debt and improve nonfunctional attributes.
Rearchitect	Materially alter the code to shift it to a new application architecture and exploit new and better capabilities.
Retool	Adopt new automation and tooling to augment software delivery, build, testing, and deployment processes.

.NET APPS

.NET application modernization

Since the introduction of the cross-platform version of .NET (originally called .NET Core and now simply referred to as .NET), organizations have had new opportunities to extend their .NET applications beyond the Windows operating system.

This evolution of the .NET ecosystem has been a welcome progression by businesses and practitioners alike because it enables the removal of Windows licensing costs and brings a lightweight, modular programming ecosystem for modern applications.

AWS has developed a number of services and tools to simplify your .NET modernization journey. An ideal starting point for your .NET transformation journey is AWS Migration Hub Strategy Recommendations, which delivers prescriptive guidance on the optimal strategy and tools to help you migrate and modernize by analyzing applications, dependencies, and technical complexity. To make it easier for customers to assess the feasibility of refactoring their applications to the cross-platform version of .NET, AWS developed and open sourced the Porting Assistant for .NET tool. To simplify refactoring applications into independent services, AWS created AWS Microservice Extractor for .NET to analyze source code and runtime metrics, graph your applications, and assist in code refactoring and extraction. To simplify end-to-end refactoring of monolithic .NET Framework applications for AWS Linux, AWS released the AWS Toolkit for .NET Refactoring Visual Studio extension to incrementally update legacy .NET applications directly from the IDE. Once modernized, CloudWatch Application Insights can help you easily set up best practices health and observability and Systems Manager Fleet Manager can help you manage and troubleshoot your environments at scale.

Hundreds of customers and partners have used these tools as a starting point in their modernization assessment to identify the applications that are good candidates for refactoring to the cross-platform version of .NET with the goal of moving off of Windows to Linux. While this assessment is the common starting point for organizations with portfolios of .NET Framework–based applications, there are other approaches that are often simultaneously implemented during modernization projects. We detail each of these approaches in the sections below.

Rehost

Migrate from on-premises to Amazon Elastic Compute Cloud (Amazon EC2) Windows

During migrations from on-premises data centers to the cloud, many customers, such as Emirates, Macmillan Learning, Infor, and MyTeam11, choose to "lift and shift" their applications to the cloud without any modifications. This is a common approach because it requires minimal code changes and therefore is the fastest way to get to the cloud compared to other modernization approaches. AWS offers Windows virtual machines in Amazon Elastic Compute Cloud (Amazon EC2) and flexible licensing options for running your Windows workloads on AWS. Additionally, AWS provides AWS Optimization and Licensing Assessments to make sure your Windows workloads are rightsized when moving to the cloud and the AWS Migration Acceleration Program, which provides best practices, tools, expertise, financial incentives, and a partner ecosystem to make cloud adoption easier.

Move web-based applications to a managed service with AWS Elastic Beanstalk

For customers with web-based applications, you can lower your TCO and management overhead for these applications by moving them to a managed service. Customers typically choose this as a lower-effort approach when applications cannot be easily refactored to microservices or the cross- platform version of .NET. AWS offers AWS Elastic Beanstalk, which is an easy-to-use service that takes care of the deploying, patching, and scaling of administrative activities. To automate the process of migrating applications to AWS Elastic Beanstalk, AWS released the Windows Web Application Migration Assistant, which is an open-source, interactive Microsoft PowerShell Utility. The utility helps customers seamlessly migrate ASP.NET and ASP.NET Core web applications from IIS on Windows servers on-premises or in another cloud to AWS Elastic Beanstalk

Infor chose to go all-in on Amazon Web Services (AWS), moving its customer-facing applications to the AWS Cloud.

"Our business was growing in places like Asia and Europe, and we wanted to be able to bring up applications faster for customers in those regions," says Randy Young, director of cloud operations at Infor. "To do that, we needed more agility, and building data centers did not make sense for our customers and the business. We wanted to get away from managing our own hardware procurement and provisioning."

Re-platform

Containerize applications with Windows containers on AWS container services

Containers are quickly becoming the de facto technology for packaging applications. Since the introduction of Docker Windows Containers in 2016 and the support for Kubernetes Windows worker nodes in 2019, customers have been increasingly moving their .NET applications to Windows containers. Customers such as Autodesk and SeatGeek choose this approach to optimize resource utilization for their existing workloads, achieve consistency across environments, control the boundaries of their applications, and facilitate the adoption of DevOps practices with a common set of tooling.

This is also a common approach for commercial off-the-shelf applications, where refactoring is not an option because the source code is not available.

AWS offers support for self-managing Windows containers in Amazon EC2 and fully managed orchestration options with Amazon Elastic Container Service (Amazon ECS) and Amazon Elastic Kubernetes Service (Amazon EKS). Additionally, Windows Containers can run serverless using AWS Fargate for ECS. Finally, to accelerate the process of moving virtual machine or bare-metal- based applications to containers, AWS built AWS App2Container, which analyzes running applications and automatically generates container images with deployment templates for AWS container services Once re-platformed, you can easily add monitoring with CloudWatch Application Insights.

SeatGeek, a live-event ticketing platform, needed to make consistent, comprehensive changes across its technology stack to help clients deliver tickets for concerts, sporting events, and other live events worldwide. Overall, the team has seen a double-digit percentage cost reduction due to containerization and multi-tenancy.

“There’s a lot more leeway there: we can spin up a few additional hosts and rearrange clients wherever we need to,” says Grasso.

Refactor

As mentioned in this section's introduction, customers typically start their.NET modernization application assessments by evaluating the compatibility of their .NET Framework applications with the latest cross-platform version of .NET. Applications that have been developed in-house and contribute to business-critical functionality (revenue-generating, deliver differentiation) are frequently top candidates for refactoring. Once the set of applications has been identified, customers often combine decomposition and porting in their process of moving to the cross-platform version of .NET and Linux. This enables customers to break off pieces of monolithic applications and iteratively transition those pieces to microservices and Linux. We detail each of these concepts in the following sections.

Decompose monolithic applications to microservices

Microservices are an architectural and organizational approach to software development where software is composed of small, independent services that communicate over well-defined APIs. These services are owned by small, self-contained teams, and customers such as Gilt, Lyft, and Pearson choose this approach because it gives their teams freedom to innovate and experiment quickly, brings agility to the development and release cycle, and enables elastic scaling of individual domains.

As a leader in the educational field, Pearson provides content, assessment, and digital services to learners, educational institutions, employers, governments, and partners globally. For years, Pearson's teams managed on- premises technology, which was not scalable or efficient. A large part of Pearson's digital transformation has been its ability to reconfigure its monolithic applications into microservices. Pearson has decoupled large monolithic applications into smaller components, modernizing its processes and giving the company more flexibility in terms of functionality.

AWS offers a range of services, tools, and programs to help your teams adopt microservices-based architectures. These include AWS Migration Hub Strategy Recommendations, AWS Microservice Extractor for .NET, containers on AWS, serverless offerings on AWS, AWS Proton, networking technologies such as AWS App Mesh and Amazon API Gateway, streaming services such as Amazon Kinesis, and monitoring services with a guided solution such as CloudWatch Application Insights or for more flexibility services such as AWS CloudTrail, Amazon CloudWatch, and AWS X-Ray.

Refactor

Port applications from .NET Framework to .NET 6+ on Linux

Customers such as DraftKings, SF Match, AgriDigital, and Fileforce with .NET Framework applications often refactor to the latest cross-platform version of .NET so they can remove their Windows licensing costs and access the latest innovations from the .NET community. This approach is emphasized by Microsoft, who explained that all future enhancements will take place in this cross-platform version of .NET and that .NET Framework is now in maintenance mode.

To help enable .NET Framework to .NET Core porting, AWS now offers AWS Microservice Extractor for .NET to refactor .NET applications along with porting compatibility to modern .NET, and Porting Assistant for .NET to enable porting a .NET app to .NET 6+. AWS also contributes to open-source libraries such as CoreWCF to provide compatibility for the commonly used WCF in the latest version of .NET. Moving to the cross-platform version of .NET also brings access to the latest innovations from AWS, such as AWS Graviton2 instances that are 20 percent less expensive per hour than Intel x86 instances with up to 40 percent better performance. AWS Graviton2 helps customers running .NET realize ARM64 performance improvements with all .NET 6 Linux supported distributions (Alpine Linux, Debian, and Ubuntu). Follow the self-paced lab to get started on running .NET 6 web applications on AWS Graviton2.

"A little over a year ago, we laid out a path to lower costs, increase scalability and application flexibility, and improve developer efficiency. We identified an opportunity to get started on this path by modernizing our legacy .NET applications, with step one being a conversion to .NET Core."

The Arkansas Administrative Office of the Courts reduced their TCO by 40% with .NET modernization.

Rearchitect

Adopt event-driven and serverless architectures with AWS Lambda

With serverless computing, infrastructure management tasks like capacity provisioning and patching are handled by AWS, so you can focus on only writing code that serves your customers. Customers such as The Coca-Cola Company and Thomson Reuters choose this approach for modernizing their most business-critical applications that will be actively developed, improved, and scaled in the future. This approach typically requires more effort than each of the previously detailed modernization efforts because serverless technologies are often new to development teams and altering existing monolithic applications for serverless requires significant code and architectural changes. To operationalize serverless compute, AWS offers AWS Lambda, which is a service that lets you run code without provisioning or managing servers. With AWS Lambda, you can run code for virtually any type of application or backend service without any administration overhead. AWS also offers AWS Fargate for longer-running applications. AWS Fargate is a serverless compute engine for containers that works with both AppRunner, Amazon ECS and Amazon EKS. AWS Fargate allocates the right amount of compute, eliminating the need to choose instances and scale cluster capacity.

CoStar™

CoStar reduced compute costs by 90% through modernizing legacy .NET Applications with AWS Serverless.

"One thing that makes AWS so great is as they iterate and introduce new features like Fargate Spot and S3 Intelligent-Tiering with minimal effort we can see massive cost savings without the worry of any sunk capital costs."

– Andy Ventura, Senior Director & Chief Architect at CoStar Group

Retool

Invest in automation, DevOps, and continuous integration and continuous deployment (CI/CD)

One of the most important capabilities to develop during modernization is automation of the development and operational lifecycles. Automating the build, deployment, testing, and operational stages of your release pipeline will result in faster, higher-quality delivery of new features while freeing up your teams to focus on building new capabilities. AWS offers a comprehensive suite of services, including AWS CodePipeline to define software release workflows, AWS CodeBuild to build and test code with every new change, and AWS CodeDeploy to continuously deploy changes to target environments. These services integrate with the previously mentioned Amazon ECS, Amazon EKS, and AWS Lambda so you can automate the pipeline for your applications as you modernize. Additionally, AWS provides infrastructure-as-code tooling such as AWS CloudFormation and the AWS Cloud Development Kit (AWS CDK) for .NET so you can programmatically define and deploy the resources that support your modern applications. The combination of these capabilities enables teams to standardize on the way they deliver infrastructure and software.

Use AWS Development Tools for .NET to ease development and operations

AWS is committed to delivering a first-class experience for .NET developers, as shown by AWS's .NET 5 readiness in 2020. We understand that having proper support for .NET tools and libraries is a central component of developer productivity. AWS offers the AWS SDK for .NET for developers to natively interact with AWS services in their applications, the AWS Toolkit for Visual Studio so developers can stay in their preferred IDE when writing applications that run on AWS, and the AWS Tools for PowerShell for developers to use their familiar command-line interface (CLI). For developers who prefer Azure DevOps, AWS offers AWS Toolkit for Azure DevOps for seamless integration. To stay up to date on all things .NET on AWS, follow @dotnetonAWS on Twitter and tune into the Microsoft on AWS YouTube playlist. If you are new to .NET development on AWS, check out the Getting Started with .NET on AWS training and the .NET on AWS courses that are available on Coursera, edX, and Udemy.

WINDOWS-BASED APPS

Data modernization is a central component of customers' modernization journey for Windows- based applications. The most common database for customers with existing .NET Framework applications is SQL Server. Customers such as Expedia, ASP, and Jobvite modernize their SQL Server deployments to reduce their licensing costs, achieve the scale and performance requirements for their traffic demands, and accommodate new microservices architectures.

One of the most common approaches that customers use is to refactor their database to Amazon Aurora. While the coupling of the application to SQL Server will dictate the complexity of this action, Amazon Aurora provides MySQL and PostgreSQL compatibility with the security, availability, and reliability of commercial databases at one-tenth of the cost. AWS Migration Hub Strategy Recommendations can also assist in helping customers perform additional refactor analysis to determine the best path forward to modernize SQL Server.

If the refactoring effort is too much to take on, customers frequently choose to re-platform their self-managed SQL Server deployments to Amazon RDS for SQL Server to lower TCO through offloading the time-consuming administration tasks like hardware provisioning, database setup, patching, and backups to Amazon RDS. In addition, for customers having existing SQL Server licenses, you can choose to bring your own licenses (BYOL) to EC2. AWS Migration Hub Orchestrator can help you automate and accelerate your migrations to AWS to avoid schedule overruns.

Expedia®

aws

As Expedia Group (Expedia) continues to grow as a leading online travel platform, so does its innovation in global payments. Part of its legacy system migrated to Amazon Aurora, a MySQL- and PostgreSQL-compatible relational database built for the cloud, which has the simplicity and cost-effectiveness of open-source databases and the performance of a commercial database. Using Amazon Aurora and more than 20 other services from AWS, Expedia cut costs and enabled staff to focus on core business by automating manual processes. Expedia also now delivers near-real-time data to its users and internal teams, resulting in a streamlined payment process and improved visibility and insights for its supply partners.

11

Rehost

Migrate from on-premises to SQL Server on Amazon EC2 Windows

Similar to .NET applications, customers choose to “lift and shift” their SQL databases to the cloud to minimize changes and quickly move to the cloud. Migration Hub Orchestrator provides two predefined workflow templates to automate manual tasks to save time and streamline your migrations to Amazon EC2. One is rehosting applications to EC2 using AWS Application Migration Service (AWS MGN). The other is rehosting SQL Server Databases on EC2 using native backup and restore.

By moving your SQL Server workloads to AWS, customers can realize significant benefits according to IDC and Principled Technologies.

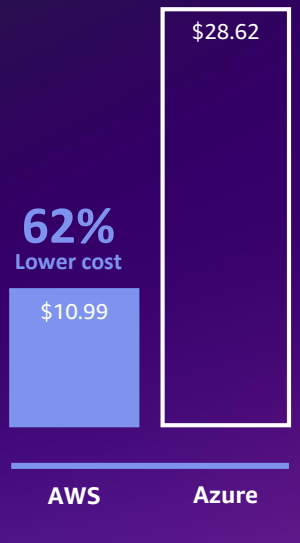
96%
reduction in unplanned downtime

71%
faster deployment

26%
higher developer productivity

Additionally, customers can use AWS Optimization and Licensing Assessments, AWS Migration Acceleration Program, and AWS Database Migration Service to efficiently migrate SQL Server workloads to AWS.

AWS is 62% cheaper than Azure per price/ performance
(Price from 1,000 NOPM)



Source: Benchmarking report from Principled Technologies

AWS saves 36% in cost compared to on-premises
(Average CPU cores per customer)

Source: Migration evaluation blog

Re-platform

Move SQL Server from Amazon EC2 Windows to Amazon EC2 Linux

Re-platforming SQL Server on Amazon EC2 Linux is a good option for customers with in-house Linux administration resources. SQL Server on Amazon EC2 Linux provides a familiar experience to Windows administrators and brings cost savings due to the removal of Windows licensing costs. The majority of the tools that developers and DBAs use to work with SQL Server on Windows platform work as-is with Linux. With this approach, customers have the flexibility to choose from Linux distributions, including Red Hat Enterprise Linux, Ubuntu, SUSE Linux Enterprise Server, and Amazon Linux 2. Additionally, customers can use the AWS Windows to Linux re-platforming assistant for Microsoft SQL Server Databases, which is a PowerShell scripting utility that checks for common SQL Server 2017 Linux incompatibilities and initiates the backup and restore of databases from your source Windows Server machine to a target Amazon EC2 Linux instance. If you consider this approach for your SQL Server deployments, review the list of unsupported features for the SQL Server Linux distribution.

Move to managed with Amazon RDS SQL Server

Customers such as Hearst Corporation, OutSystems, and Unilever frequently choose to re-platform their self-managed SQL Server deployments to fully managed Amazon RDS for SQL Server to offload operational tasks such as provisioning, configuration, patching, backups, and high-availability deployment. Migration Hub Orchestrator provides a predefined workflow template to automate your replatforming SQL Server databases to Amazon RDS using native backup and restore.

outsystems

OutSystems is a diversified software company that provides a platform to enable customers to build, integrate, deploy, and manage applications. Using Amazon RDS for SQL Server and other AWS services, OutSystems was able to double the cloud-based segment of its business in six months while serving customers in 25 countries. Jerry Zeephat, head of global product marketing at OutSystems, says, “We are very big users of Amazon RDS. It’s really important for what we do and what our customers do. It’s high security, it’s high availability and it’s very fast to deploy. Our customers can carve out what they need so you don’t have to worry about maintenance of a database. It’s just a service we provide.”

This approach is a lower-effort option compared to refactoring because it requires minimal code changes to implement. Amazon RDS SQL Server also supports the “License Included” licensing model to remove the need to purchase separate Microsoft SQL Server licenses. Additionally, you can take advantage of hourly pricing with no upfront fees or long-term commitments. You also have the option to purchase reserved DB instances under one- or three-year reservation terms, which can achieve up to 65 percent net cost savings.

Refactor

Refactor SQL Server to Amazon Aurora

One of the most common approaches for modernizing SQL Server is to refactor the data access code and usage to Amazon Aurora MySQL or PostgreSQL. Customers choose this approach to remove their SQL Server licensing costs and to take advantage of the scale, performance, and simplicity of Amazon Aurora. During AWS re:Invent 2021, AWS announced the GA of Babelfish for Amazon Aurora PostgreSQL, which is a migration accelerator that enables Amazon Aurora to understand commands from applications written for SQL Server. With Babelfish, customer apps that were originally written for SQL Server can now work with Aurora with fewer code changes. Additionally, AWS offers the AWS Schema Conversion Tool, which automatically converts SQL Server schema, functions, and statements to Amazon Aurora equivalents to accelerate the refactoring effort.

DOW JONES

Dow Jones migrated their Market Data system from SQL Server to Aurora MySQL and reduced their processing times from 8 hours to 3 hours.

ASP reduced costs by 65% on SQL Server licensing and simplified their operations by modernizing from Amazon RDS for SQL Server to Amazon Aurora.

Rearchitect

Rearchitect SQL Server to purpose-built, open-source, and NoSQL databases

The trend toward microservices architectures has led to the use of separate databases that are best suited for the use case of the individual services. Customers choose this approach when they are breaking down their monolithic architectures to microservices and have query pattern, scale, or performance requirements that traditional relational databases do not provide. AWS offers the broadest set of fully managed, purpose-built databases for your application needs that include Amazon DynamoDB for high-traffic key-value workloads, Amazon DocumentDB (with MongoDB compatibility) for catalog, user profile, and content management workloads, Amazon Timestream for time-series workloads, and Amazon Neptune for relationship-driven graph workloads.

Active Directory identity modernization

Active Directory (AD) has been the primary identity solution for customers with Windows-based workloads since it was introduced in 1999. Many customers have spent considerable time and resources building and tuning their on-premises AD deployments to fit their organization's identity and access control needs.

AD is a complex set of services that covers multiple use cases, including serving as a central directory, authentication for users and computers, access management to infrastructure resources and applications, and configuration management for servers and workstations. However, as customers migrate their workloads to the cloud and increasingly adopt remote working styles, their on-premises AD deployments that rely on older protocols and network concepts create problems for federating access across their on-premises and cloud environments. Because of this, customers need new identity solutions that integrate with their existing AD deployments while providing a single- sign-on (SSO) interface for them to connect their services and resources no matter where they are deployed. In the following sections, we cover the common approaches that customers use to modernize their AD deployments as their business moves to the cloud and the workforce adapts to new styles of working from anywhere.

AWS identity services

AWS has the following set of identity services for customers migrating and modernizing their Windows-based workloads.

Services	Description
AWS Directory Service	Managed Microsoft Active Directory service and Active Directory Connector to integrate existing AD or deploy a managed AD in the cloud.
AWS Identity Center	Cloud-based single-sign-on service and seamless access to AWS accounts and services.
AWS Identity and Access Management (IAM)	Securely manage access to AWS services and resources.
AWS Resource Access Manager	Helps to securely share your resources across AWS accounts.
AWS Organizations	Centralize governance and management across AWS accounts.
Amazon Cognito	Cloud-native identity provider service for web and mobile applications.

Extend

Connect existing on-premises AD to AWS resources

Many customers have existing on-premises AD deployments they need to use for the resources they deploy in AWS. For these customers that want to continue using their on-premises AD deployments, AWS offers the AWS Active Directory Connector (AD Connector), AWS Managed Microsoft AD, and the ability to self-manage AD in the cloud on Amazon EC2 Windows. AD Connector enables customers to use their existing self-managed AD domain and existing credentials to log on to AWS applications such as Amazon WorkSpaces and Amazon WorkDocs, manage AWS resources in the AWS Management Console, or join Amazon EC2 instances to the domain. However, for customers that have more complex topologies that span multiple regions and accounts, it's often easier to use AWS Managed Microsoft AD. Customers deploy AWS Managed Microsoft AD as a resource forest in the cloud to run their workloads while simultaneously using their existing on-premises AD deployment for users and workstation management to avoid complex migrations. One- and two-way (incoming, outgoing, and bidirectional) external and forest trusts can be used to establish connectivity for on-premises users to access the AWS Management Console or AWS Managed Services such as Amazon Relational Database Service for SQL Server, Oracle, PostgreSQL, MySQL, and Amazon FSx.

Rehost

Migrate existing AD to Amazon EC2

For customers that have requirements for higher availability of their AD resources, a typical pattern is to deploy additional domain controllers in the cloud, treating the new Amazon Virtual Private Cloud (VPC) as one or more data centers in their infrastructure.

This technique is used to keep AD resources available even in a case of connectivity issues between your on-premises and cloud networks. For high availability, it's recommended to deploy at least two domain controllers in each region and place them in different Availability Zones. The best- practice configuration is to have VPCs in a region as a single AD site and define subnets accordingly to ensure that clients select the closest available domain controller. AWS offers VPC peering to achieve highly available private connectivity between regions and AWS Transit Gateway to interconnect multiple VPCs and on-premises networks through a central hub. For a fast onboarding experience, AWS provides the Quick Start for Active Directory to help customers deploy new self-managed AD in the cloud, extend existing on-premises domains to AWS, or deploy AWS Managed Microsoft AD. For each scenario, you have the option to use a new or existing VPC and the option of deploying a one or two-tier Microsoft Public Key Infrastructure.

The International Air Transport Association (IATA) is the trade association for the world's airlines, representing 250 airlines which account for 84 percent of the world's air traffic. "We needed the best in breed in terms of cloud platform, so we chose AWS," Buchner says. "Moving to AWS was our only option if we wanted to survive in a world that's going faster and faster." IATA solutions on AWS run in Amazon Virtual Private Cloud (Amazon VPC) and are fully integrated with IATA's existing Active Directory service. AWS is currently ISO 27001–certified, which was a requirement for IATA since the BI platform manages highly confidential information.

Re-platform

Move to managed with AWS Managed Microsoft AD

Customers often re-platform their existing AD infrastructure using AWS Managed Microsoft AD to remove the operational overhead of operating their AD deployments while limiting the number of required code changes.

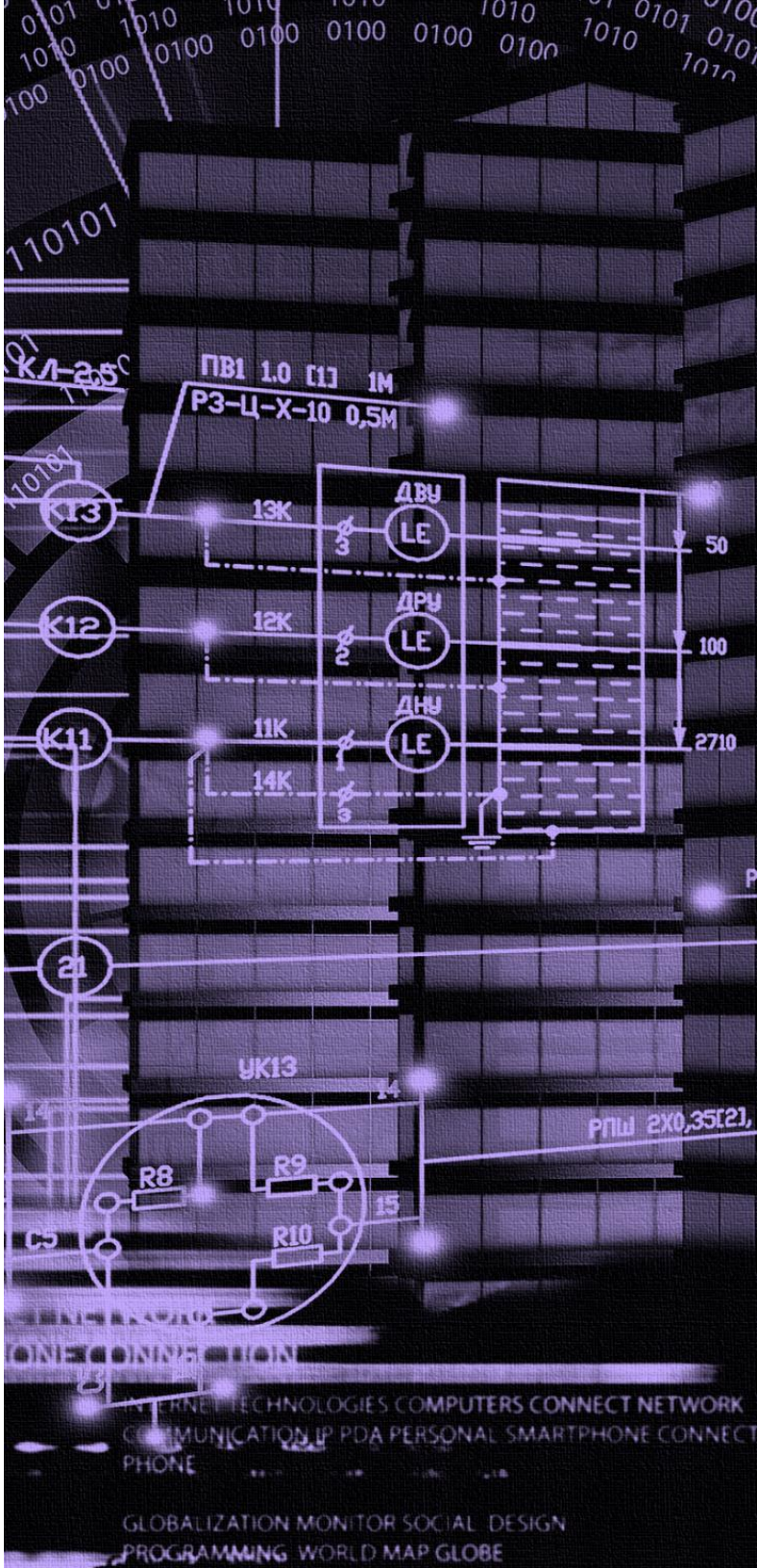
AWS Managed AD is a full deployment of Microsoft AD in one or many regions that automatically takes care of common tasks such as monitoring, backup, patching, and recovery services. With AWS Managed AD, each directory is deployed across multiple Availability Zones, and monitoring automatically detects and replaces domain controllers that fail. Data replication and automated daily snapshots are configured for you. You do not have to install software, and AWS handles all patching and software updates. Through integration with AWS Single Sign-On, AWS Managed AD can be used to federate the access to common business applications, including Salesforce, Box, and Office 365. Additionally, AWS Managed 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), US Health Insurance Portability and Accountability Act (HIPAA), or Service Organization Control (SOC) compliance.

Capital One is a major American bank and credit card issuer with over $28 billion in revenue. Capital One is using AWS Managed AD across many regions and applications, integrating with managed services like Amazon RDS. Capital One started by migrating Microsoft workloads, including Windows to Amazon EC2, reducing their data center footprint drastically while increasing their agility and flexibility. As a sophisticated AWS customer looking to run new workloads in the cloud, Capital One was able to address security and compliance concerns by running Managed AD instances in multiple regions. Better yet, adopting AWS Managed AD opened the door for Capital One to adopt Amazon RDS for SQL Server, moving away from managing their own SQL Server workloads on Amazon EC2 toward a lower-overhead solution designed for the cloud.

Rearchitect

Move workloads to use modern identity services with Amazon Cognito

A higher-effort approach to AD modernization is to rearchitect applications with modern identity services and protocols. For many customers, AD does not meet the scale, performance, and availability requirements of their modern web and mobile applications. These use cases have new standards that customers expect, such as the ability to access the application anywhere at any time on any device, seamless integration with popular identity providers, and the ability to log in both online and offline. To help customers solve for these modern demands, AWS offers AWS Cognito, which is a cloud- native identity service for user sign-up, sign-in, and access control to web and mobile apps. Amazon Cognito scales to millions of users and supports sign-in with social identity providers, such as Apple, Facebook, Google, and Amazon and enterprise identity providers via SAML 2.0 and OpenID Connect. Customers that need to provide access to AWS Cognito-based applications while retaining existing AD functionality for user authentication can use Active Directory Federation Services (AD FS) and integrate with Amazon Cognito as a SAML 2.0 identity source.



Retool

Adopt new cloud-based tools to simplify identity management

As customers migrate workloads from on-premises to the cloud, one of the primary challenges is handling the resource and infrastructure sprawl while enforcing security and compliance best practices. AWS offers many tools such as AWS Systems Manager Fleet Manager (GUI at scale management), AWS Systems Manager, Amazon CloudWatch Application Insights (guided), Amazon CloudWatch (self-service), and Amazon Kinesis that can be used to define, monitor, analyze, and maintain the organization's security posture in the cloud.

For example, customers use Fleet Manager to 1-click RDP via a web browser into their Amazon EC2 Windows instances, manage configuration baselines, maintain security and compliance, and connect with IT service management systems. For quickly and easily setting up monitoring for your workloads and containers, CloudWatch Application Insights can discover your resources and set up best practice metrics, alarms and logs to ensure your modernized environment is healthy. Customers such as Autodesk have gone further with AWS Systems Manager and custom CloudWatch metrics along with the Amazon Kinesis Agent for Microsoft to collect, parse, transform, and stream Windows events, logs, and metrics at scale. Retooling your management and monitoring arsenal with native AWS services is a common approach to satisfy the requirements of your modern applications while removing the need to purchase or develop tooling for these administrative tasks.

AUTODESK

"Autodesk builds software tools and services that help our customers design and make anything. These tools and services must be reliable so they can get their job done. A fundamental part of any trusted cloud connected software is observability and this starts with collecting log data. The new Amazon Kinesis Agent for Microsoft Windows simplifies workflows for streaming logs by eliminating the need for complicated interconnected systems and tools. The agent is easy to set up, configure, and update. The Amazon Kinesis Agent for Microsoft Windows significantly reduces the complexity of log collection and management."

– Ben Cochran, Senior Director, Cloud Engineering, Autodesk

CONCLUSION

There are many options that customers use to transform their Windows workloads to take advantage of modern development and operational practices. No matter where you are in your cloud journey, AWS is here to help with proven services, support, and partners to power the evolution of your applications. We'd love to talk to you about your modernization approach, and we invite you to email microsoft-modernization-interest@amazon.com to get in touch with AWS experts.

Learn more about modernization applications on AWS ›

Connect with an expert to accelerate your Windows modernization ›