

Service Name

Amazon WorkSpaces

Service Overview

Amazon WorkSpaces is a fully managed virtual desktop infrastructure (VDI) service that enables organizations to provision virtual, cloud-based desktops for users. These desktops can run Microsoft Windows, Amazon Linux, Ubuntu Linux, Rocky Linux, or Red Hat Enterprise Linux. WorkSpaces eliminates the need to procure and deploy hardware or install complex software, allowing users to access their virtual desktops from multiple devices or web browsers. The service offers two options: WorkSpaces Personal for persistent virtual desktops tailored for users requiring highly-personalized desktop environments, and WorkSpaces Pools for non-persistent virtual desktops for users needing access to curated desktop environments on ephemeral infrastructure.

Key Use Cases

- Remote and hybrid work: Enable secure access to corporate applications and data from anywhere
- Learning environments: Provide virtual desktops for educational institutions and training programs
- Developer workstations: On-demand access to high-performance development environments
- Contact centers: Secure virtual desktops for customer service representatives
- Knowledge workers: Consistent desktop experience for office productivity applications
- Running Windows 11 on older devices: Extend hardware lifecycle by accessing modern OS through virtual desktops
- Back office and administration: Secure environments for administrative and financial operations
- Secure development workflows: Highly regulated environments meeting compliance requirements

Features

- **Multi-Platform Access:** Access WorkSpaces from Windows, Mac, Linux, Chromebooks, iPads, Android devices, and web browsers
- **Flexible Hardware Bundles:** Multiple compute types from Value to GraphicsPro.g4dn with varying vCPU, memory, and storage configurations
- **Multiple Operating Systems:** Support for Windows, Amazon Linux, Ubuntu Linux, Rocky Linux, and Red Hat Enterprise Linux

- **Custom Images and Bundles:** Create and deploy custom desktop images with pre-installed applications and configurations
- **Multi-Factor Authentication:** Integration with RADIUS servers and SAML 2.0 identity providers for enhanced security
- **Data Encryption:** Encryption at rest and in transit using AWS Key Management Service
- **Persistent Storage:** Automatic backup of user data to Amazon S3 with configurable storage sizes
- **Streaming Protocols:** Support for WorkSpaces Streaming Protocol (WSP) and PCoIP for optimized performance
- **Self-Service Management:** Users can restart, rebuild, change compute type, and manage their WorkSpaces directly
- **Multi-Region Resilience:** Cross-region redirection and standby WorkSpaces for disaster recovery

Value Proposition

Amazon WorkSpaces delivers significant advantages over traditional VDI solutions through its fully managed cloud infrastructure that eliminates hardware procurement, complex software installation, and ongoing maintenance overhead. Organizations benefit from rapid deployment capabilities, with virtual desktop deployment times reduced by up to 90% as demonstrated by companies like Ferrari:

- The service provides unmatched flexibility with support for both persistent and non-persistent desktops, multiple operating systems, and global scalability across AWS regions
- Cost optimization is built-in through flexible pricing models including AlwaysOn and AutoStop billing, integration with EC2 Reserved Instances and Savings Plans, and automated cost optimization tools
- Enhanced security features include encryption, multi-factor authentication, and Zero Trust architecture compatibility, while seamless integration with Microsoft 365 and existing enterprise systems ensures smooth adoption

Service Integration

Amazon WorkSpaces integrates extensively with core AWS services to deliver a comprehensive virtual desktop solution. Directory integration is provided through AWS Directory Service with support for Simple AD, AWS Managed Microsoft AD, and Active Directory Connector for seamless user authentication:

- Security is enhanced through AWS Key Management Service for encryption, AWS IAM for access management, and integration with RADIUS servers for multi-factor authentication

- The service leverages Amazon VPC for network isolation and security groups for access control, while Amazon CloudWatch provides comprehensive monitoring and logging capabilities
- Storage integration includes automatic backup to Amazon S3 and compatibility with Amazon FSx for Windows File Server
- For disaster recovery, WorkSpaces utilizes cross-region capabilities and integrates with AWS Backup for data protection, while AWS Systems Manager enables automated patching and configuration management

Onboarding and Offboarding

Getting started with Amazon WorkSpaces requires three essential components: a compatible client application, a directory service for user authentication, and an Amazon VPC with at least two subnets. Organizations first create a directory using Simple AD, AWS Managed Microsoft AD, or Active Directory Connector, then configure the VPC with proper security groups and DHCP options:

- WorkSpaces can be launched through the AWS Management Console by selecting bundle types, running modes, and directory settings
- Users receive invitation emails with client download instructions and connection details
- The setup process includes configuring multi-factor authentication if required, customizing bundles and images as needed, and establishing network connectivity
- Best practices recommend deploying WorkSpaces in private subnets with proper security group rules for Active Directory communications and implementing monitoring through Amazon CloudWatch for ongoing management

Getting Started Guide:

<https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html>

Data Removal

Offboarding from Amazon WorkSpaces involves terminating WorkSpaces through the AWS Management Console, CLI, or API, which permanently deletes all data stored on root and user volumes. Organizations should backup critical data before termination since the process is irreversible. Directory services and associated infrastructure components like VPCs and security groups must be separately deregistered and deleted. For compliance requirements, encryption keys used for data protection should be managed according to organizational policies, and any custom images or bundles can be deleted to remove organizational data completely.

Backup/Restore and Disaster Recovery

Amazon WorkSpaces provides comprehensive backup and disaster recovery capabilities through automatic snapshots of root and user volumes stored in Amazon S3. Multi-Region

Resilience (MRR) enables creation of standby WorkSpaces in secondary regions with cross-region redirection and DNS health check failover. Data replication can copy user data one-way from primary to secondary regions. WorkSpaces can be restored to previous snapshots when in AVAILABLE, ERROR, UNHEALTHY, or STOPPED states, though this overwrites current data with snapshot contents.

Backup Capabilities

WorkSpaces automatically creates snapshots of both root and user volumes after initial creation, during regular use, and after restoration events. These snapshots are stored in Amazon S3 for durability and can be used to restore WorkSpaces to previous states:

- The service integrates with AWS Backup for centralized backup management across AWS services
- However, WorkSpaces snapshots are service-specific and restoration requires both root and user volume snapshots to be available

Disaster Recovery

WorkSpaces supports disaster recovery through Multi-Region Resilience, enabling standby WorkSpaces in secondary AWS regions with automated failover capabilities. Cross-region redirection uses DNS health checks for automatic traffic routing during outages. While WorkSpaces doesn't directly integrate with AWS Elastic Disaster Recovery, organizations can implement comprehensive DR strategies using AWS Backup for data protection and multi-region deployment architectures for business continuity.

Recovery Objectives

Amazon WorkSpaces helps customers meet Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements through automated snapshot creation and Multi-Region Resilience features. Standby WorkSpaces can be activated within minutes during regional failures, supporting aggressive RTO targets. Data replication capabilities enable near real-time data synchronization for minimal RPO requirements. The fully managed infrastructure and automated failover mechanisms significantly reduce recovery complexity while providing predictable recovery timeframes for business continuity planning.

Service Constraints

Service Quotas:

<https://docs.aws.amazon.com/workspaces/latest/adminguide/workspaces-limits.html>

FAQ: <https://aws.amazon.com/workspaces/faqs/>

Technical Requirements

Service Documentation: <https://docs.aws.amazon.com/workspaces/latest/adminguide/>

User Guide: <https://docs.aws.amazon.com/workspaces/latest/userguide/>

API Reference: <https://docs.aws.amazon.com/workspaces/latest/api/>

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/workspaces/pricing/>

Cost Optimization

Amazon WorkSpaces offers unique cost optimization features including the Cost Optimizer solution that automatically analyzes usage patterns and converts WorkSpaces between hourly and monthly billing models to minimize costs. AutoStop mode automatically stops WorkSpaces when not in use, charging only for active hours plus a small monthly fee:

- Organizations can leverage EC2 Reserved Instances and Savings Plans for additional savings, while the ability to terminate unused WorkSpaces and optimize pool sizes reduces infrastructure costs
- Bring Your Own License (BYOL) options for Windows and Microsoft Office licenses provide significant cost savings compared to license-included bundles
- The service eliminates traditional VDI infrastructure costs including hardware procurement, maintenance, and data center operations

Savings Considerations

Primary cost savings with Amazon WorkSpaces come from eliminating upfront hardware investments and ongoing infrastructure maintenance costs associated with traditional VDI deployments. The pay-as-you-use model with AlwaysOn and AutoStop billing options ensures organizations only pay for actual usage rather than overprovisioned capacity:

- Integration with EC2 Reserved Instances and Compute Savings Plans can provide up to 72% cost savings for predictable workloads
- BYOL licensing reduces per-user costs significantly, while automated cost optimization tools prevent bill shock through intelligent workload management
- The fully managed service model eliminates IT overhead for patching, monitoring, and maintenance, allowing organizations to redirect resources to strategic initiatives while reducing total cost of ownership compared to on-premises VDI solutions