IMPLEMENTING AWS WORKSPACES

BEST PRACTICES & VENDOR SOLUTIONS

aws

PLANNING

DEPLOYMENT

OPTIMIZATION

BEST PRACTICES

SUCCESS FRAMEWORK

VENDOR SOLUTIONS

Partner Logos

Implementing AWS WorkSpaces: Executive Overview

A comprehensive guide to deploying secure, scalable Desktop-as-a-Service solutions for your organisation
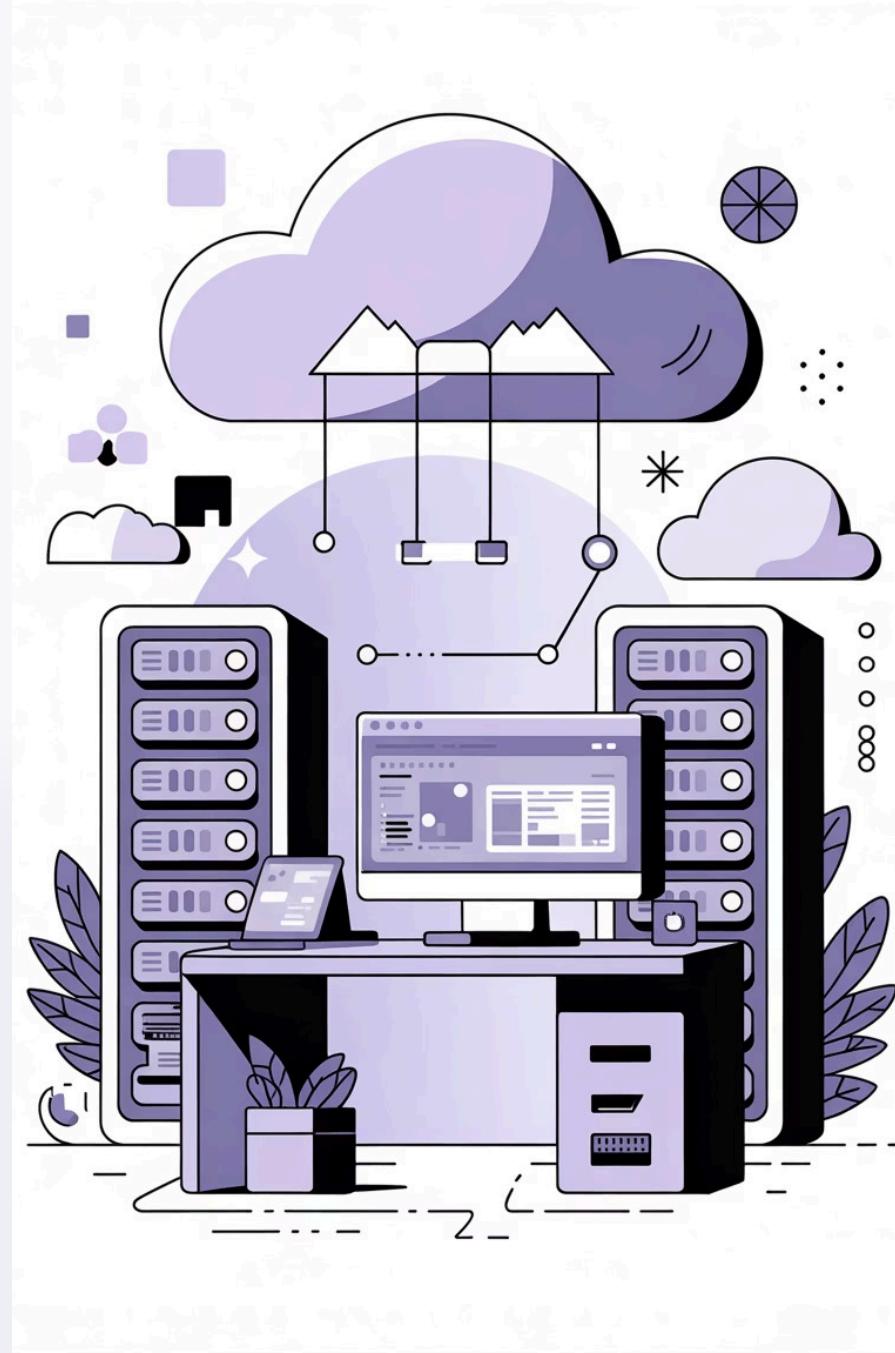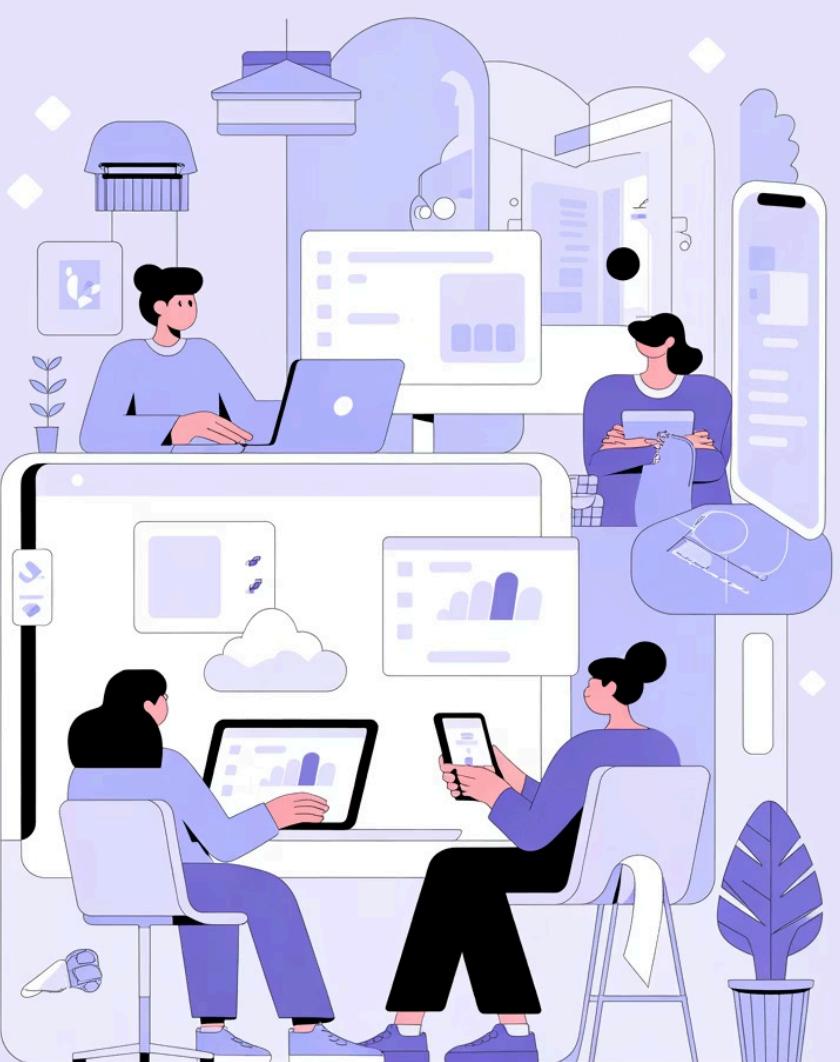
Why AWS WorkSpaces?

Enterprise-Grade Virtual Desktops

AWS WorkSpaces delivers fully managed Desktop-as-a-Service (DaaS), enabling rapid deployment of Windows or Linux desktops without the complexity of traditional infrastructure.

This powerful solution removes hardware procurement burdens and complex software installation processes, allowing IT teams to focus on strategic initiatives rather than maintenance.

Built for Modern Work

Supporting secure remote access for hybrid and remote workforces, WorkSpaces provides consistent desktop experiences across devices whilst maintaining enterprise security standards.

Scale seamlessly from tens to thousands of users, with flexible pricing models that adapt to your organisation's needs and usage patterns.

DigitalWorkplace.pro
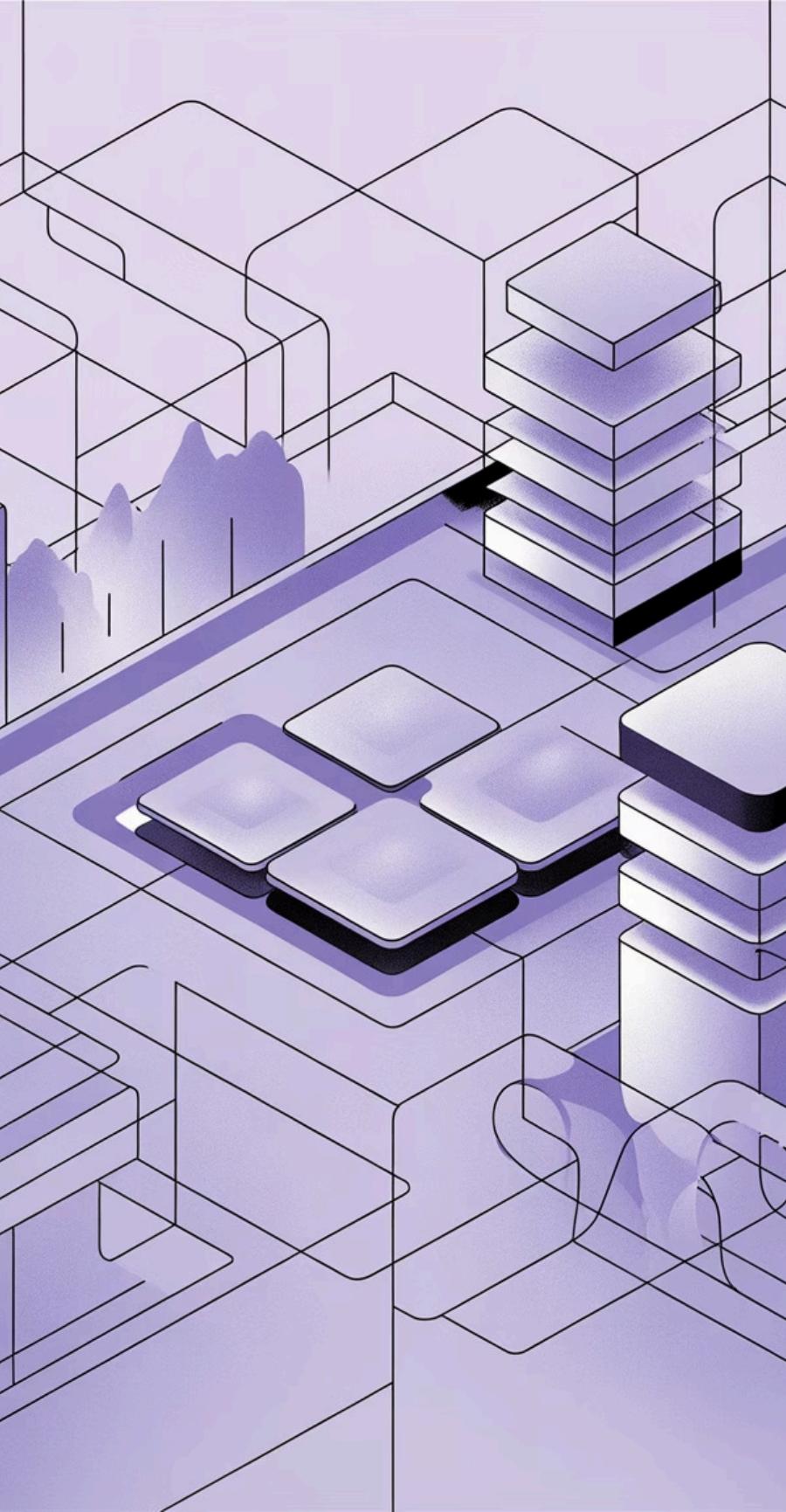
Designing Your Network for WorkSpaces Success

High Availability Foundation

Deploy Active Directory Domain Services (AD DS) in dedicated private subnets across two Availability Zones to ensure continuous operation and disaster recovery capabilities.

Security Segmentation

Separate AD DS, AD Connector, and WorkSpaces subnets within your Amazon VPC to maintain robust security boundaries whilst optimising performance and management.

Seamless Integration

Use VPC peering to connect your WorkSpaces VPC with existing AD DS deployments, enabling seamless integration with current infrastructure without compromising isolation.

Securing Your WorkSpaces Environment

1

Data in Transit Protection

Encrypt all data transmissions using HTTPS and PCoIP protocols with AES-128/256 encryption, ensuring secure communication between endpoints and cloud infrastructure.

2

Data at Rest Encryption

Enable comprehensive encryption at rest leveraging AWS Key Management Service (KMS) with customer master keys (CMKs) for complete control over your encryption keys and data security.

3

Multi-Factor Authentication

Implement robust Multi-Factor Authentication (MFA) via AWS Directory Service, integrating with RADIUS servers to provide enhanced identity protection and prevent unauthorised access.

Network Security Controls and Access Management
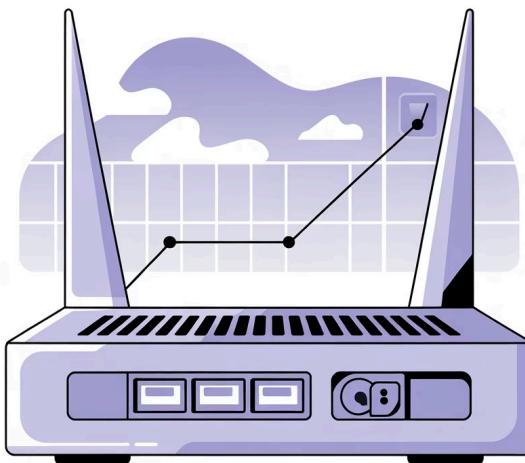
Granular Traffic Control

Use Security Groups to restrict WorkSpaces network traffic with precision. Allow only necessary ports for AD DS replication, authentication, and management functions whilst blocking all other traffic by default.

User Access Policies

Control user access through IP Access Control Groups and Trusted Devices policies, ensuring only authorised devices from approved locations can connect to your WorkSpaces environment.

Outbound Internet Management

Restrict outbound internet access with firewall implicit deny rules. Maintain allowlists specifically for patch management and essential administrative tasks to minimise attack surface.

Directory Service Integration Options

AD Connector

Proxy authentication to on-premises Active Directory without syncing passwords to the cloud. Ideal for organisations maintaining existing AD infrastructure whilst leveraging cloud resources.

AWS Managed Microsoft AD

Fully managed, scalable directory service with native support for trusts and hybrid deployments. Perfect for complex environments requiring full AD functionality in the cloud.

Simple AD

Lightweight directory solution for smaller deployments or isolated environments. Cost-effective option for organisations with basic directory requirements and limited user counts.

Vendor Solutions & Real-World Use Case

PwC Secure Environment Implementation

01

Secure Foundation

PwC designed a WorkSpaces environment for regulated workloads with strict network boundaries and comprehensive outbound restrictions to meet compliance requirements.

02

Hybrid Connectivity

Leveraged AWS Transit Gateway and Direct Connect for robust hybrid connectivity with on-premises data centres, ensuring low-latency access to critical systems.

03

Compliance & Control

Enabled regulatory compliance through advanced identity management, end-to-end encryption, continuous monitoring, and controlled software package deployment processes.

Choosing the Right WorkSpaces Bundle & Endpoints

Bundle Selection

Select bundles based on user workload requirements:

- 2GB RAM for light users (email, web browsing)
- 4-8GB RAM for standard productivity
- 16GB RAM for power users and development

Billing Optimisation

Consider billing options strategically:

- Monthly billing for full-time users
- Hourly billing for intermittent use
- AutoStop for cost control

Endpoint Devices

Evaluate endpoint options:

- Traditional desktops with WorkSpaces client
- PCoIP Zero Clients for lower power consumption
- Simplified management and enhanced security

Monitoring, Logging, and Ongoing Management

Comprehensive Monitoring

Use AWS CloudWatch and CloudTrail to monitor WorkSpaces usage, performance metrics, and security events in real-time. Set up automated alerts for anomalous behaviour and capacity thresholds.

Automated Management

Automate patch management and software deployment using existing enterprise tools like Microsoft SCCM or Ansible. Maintain consistency across your WorkSpaces fleet whilst reducing manual intervention.

Continuous Optimisation

Regularly review security group rules and directory service health for compliance adherence and optimisation opportunities. Conduct quarterly audits of access patterns and resource utilisation.

Summary & Next Steps

Scalable Foundation

AWS WorkSpaces offers scalable, secure virtual desktops with flexible deployment options that grow with your organisation's needs.

Best Practices

Follow proven best practices in network design, security, directory integration, and endpoint management for deployment success.

Expert Partnership

Partner with AWS vendors and consult experts like PwC for tailored, compliant solutions that meet your specific requirements.

Begin Your Journey

Start your WorkSpaces journey today to empower your remote workforce securely and efficiently, transforming how your organisation works.