Implementation Guide

Streamline Amazon WorkSpaces Management with Intune

Streamline Amazon WorkSpaces Management with Intune: Implementation Guide

Table of Contents

Streamline Amazon WorkSpaces Management with Intune

Publication date: **June 10, 2021** (*Document revisions*)

This guide walks you through the process of setting up Windows Intune and Amazon WorkSpaces using Hybrid Azure Active Directory Join. Specifically, you learn how to establish an Azure Active Directory environment for hybrid join and configure Microsoft Intune for Amazon WorkSpaces to allow user credential-based enrollment, extending your existing Intune Windows 10 management to Amazon WorkSpaces beyond organizational desktops and laptops.

This guide requires Bring Your Own License (BYOL) for Windows 10 Amazon WorkSpaces. License-included Amazon WorkSpaces is not supported with this implementation guide.

Overview

Amazon WorkSpaces are secure, persistent virtual desktops in the AWS Cloud. These virtual desktops are normally joined to a customer's existing domain, allowing them to work seamlessly with existing tools and corporate resources. Customers can leverage the time and effort put into the development and customization of these tools by extending them into their Amazon WorkSpaces environment. This provides flexibility for IT administrators and accelerates adoption for end-users as a customer goes through their End User Compute journey on AWS. This guide walks through the process of integrating Microsoft Autopilot with an existing BYOL Amazon WorkSpaces deployment.

Each WorkSpaces instance is assigned to a single user whose applications, documents, and settings persist throughout the lifecycle of the instance, much like existing end-user devices. Just like end-user devices, WorkSpaces instances require ongoing operating system (OS) maintenance and application updates throughout their lifecycle to stay current. Customers can use Windows Autopilot to manage existing WorkSpaces and automate the onboarding process of a WorkSpaces instance to end- users, without IT Admin involvement.

Consider the following scenario that benefits from using Windows Intune with Amazon WorkSpaces:

Streamline onboarding remote corporate users — This scenario allows users to onboard from home and access their corporate environment resources to be productive from Day 1. IT administrators create and apply configuration profiles to provisioned WorkSpaces instances, while end-users initiate the onboarding process when they log into their instance for the first time. After login, the OS and applications are fully patched, and the instance is completely compliant without IT administrator involvement. This workflow can all be accomplished without coming into an office.

Cost

The total cost for setting up Windows Autopilot with Amazon WorkSpaces varies depending on several factors, including the following:

- Amazon Elastic Compute Cloud (Amazon EC2) instance size based on number Active Directory (AD) objects already in use and in the possible future

- Less than 100,000 objects = m5.large with 100GB GP3 volume
- More than 100,000 objects = m5.2xlarge with 500GB GP3 volume + Microsoft SQL Server

This implementation uses a Microsoft trial license called Enterprise Mobility + Security E5 and an Amazon EC2 m5.large instance with 100 GB of Amazon EBS storage. It costs approximately $8.76 to complete the walkthrough if you use the default configuration recommended in this guide. This estimate assumes that the infrastructure you create during the walkthrough is running for four hours. The cost estimate is based on pricing for US East N. Virginia. A breakdown of the services used and their associated costs is provided in the following section.

Services used and costs

AWS pricing is based on your usage of each individual service. The total combined usage of each service creates your monthly bill. For this tutorial, you are charged for the use of Amazon WorkSpaces, a custom domain name, and an Amazon EC2 instance.

Amazon WorkSpaces

- **Description** — Amazon WorkSpaces is a fully managed, secure desktop computing service which runs on the AWS Cloud. Amazon WorkSpaces allows you to easily provision cloud-based virtual desktops and provide your users access to the documents, applications, and resources they need from any supported device, including Windows, Linux, and Mac computers, Chromebooks, iPads, Kindle Fire tablets, and Android tablets.
- **How pricing works** — With Amazon WorkSpaces, you pay only for the Amazon WorkSpaces you launch. There is no up-front commitment and you can delete Amazon WorkSpaces at any time.

  Amazon WorkSpaces provides the flexibility to pay monthly or hourly. With monthly billing, you pay a fixed monthly fee for unlimited usage during the month. With hourly billing you pay a

small fixed monthly fee per Amazon WorkSpace to cover infrastructure costs and storage, and a low hourly rate for each hour the Amazon WorkSpace is used during the month.

There are different bundles to choose from – Value, Standard, Performance, Power, PowerPro, Graphics and GraphicsPro. Pricing includes compute, storage, software, and bandwidth between your Amazon WorkSpace and your Amazon WorkSpaces client application. Accessing the public Internet from your Amazon WorkSpace is charged separately at current rates, published in "Data Transfer OUT". See the Amazon Workspaces Pricing page for more information.

- **Example** — In this project, you create one Amazon WorkSpace, using the Bring Your Own License (BYOL) Performance bundle, paying hourly or monthly. In the US East (N. Virginia) Region, the hourly price for the Performance bundle is $0.43 plus a $7.25 monthly fee. Assuming that your Amazon WorkSpace run for a total of 4 hours during this project, the total cost would be $8.97. Should you choose to pay monthly instead, your total cost would be $41.

> **Note**
>
> The monthly fee for Amazon WorkSpaces is prorated for the remainder of the first month of usage. The price listed is based on the Root and User Volume 80/10 option.

Amazon Route 53

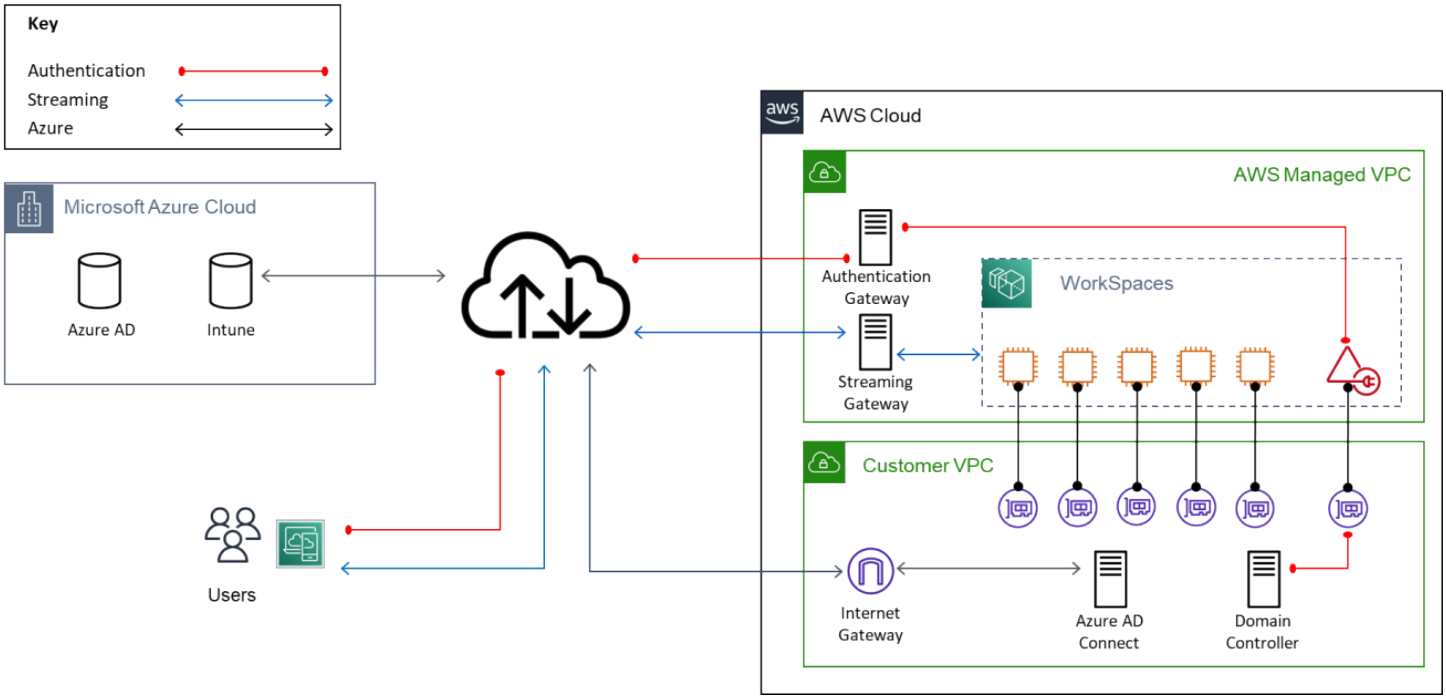
- **Description** — Amazon Route 53 is a highly available and scalable cloud Domain Name Systems (DNS) web service. It is designed to give developers and businesses an extremely reliable and cost-effective way to route end users to Internet applications by translating names such as *www.example com*. into numeric IP addresses such as 192.0.2.1, which computers use to connect to each other. Amazon Route 53 is fully compliant with IPv6 as well.
- **How pricing works** — With Amazon Route 53, you don't have to pay any upfront fees or commit to the number of queries the service answers for your domain. Like with other AWS services, you pay as you go and only for what you use:
- **Managing hosted zones** — You pay a monthly charge for each hosted zone managed with Route 53.
- **Serving DNS queries** — You incur charges for every DNS query answered by the Amazon Route 53 service, except for queries to Alias A records that are mapped to Elastic Load Balancing instances, CloudFront distributions, AWS Elastic Beanstalk environments, API Gateways, VPC endpoints, or Amazon S3 website buckets, which are provided at no additional charge.

- **Managing domain names** — You pay an annual charge for each domain name registered via or transferred into Route 53.

  Your monthly bill from AWS will list your total usage and dollar amount for the Amazon Route 53 service separately from other AWS services.
- **Example** — In this project you will need a custom domain name that will be added to Azure Active Directory. You can use a domain name as long as it matches the fully qualified domain name of the Windows Active Directory in DNS. The cost to register a new domain name is $12 for the year and $0.50 to host it on Amazon Route 53.

Architecture overview

This deployment configures a connection between Azure AD, the Intune service from Autopilot, and an AWS managed-Virtual Private Cloud (VPC) which holds the WorkSpaces being deployed. The following diagram shows the architecture, along with a list of items/resources required to deploy Intune to an AWS managed environment/service successfully:



EC2 instances for domain resources and AD connector for WorkSpaces authentication, and internet connectivity for Microsoft Azure Cloud

Table 1 — items and resources required to deploy Intune to an AWS managed environment/service successfully

Number	Description
1	Stand-alone Windows Server OS with Azure AD Connect and Intune Connector installed extending Azure Domain-join function to Amazon WorkSpaces, Hybrid AD Join, and enabling read and writeback to Windows AD Domain. (Optional component Microsoft

Number	Description
	SQL Server can run on another host, optional configuration for OU filtering.) 1. User object that is part of Enterprise Admins AD Security Group. 2. User account with Global Admin Role in Azure AD.
2	Once Windows AD User and Security Group Objects are synchronized to Azure AD, assign Microsoft Licenses for (Intune/Office365) to Amazon WorkSpaces users Windows AD Security Group(s) (to simplify license assignment in Azure AD). MDM and MAM user scopes are enabled here.
3	Assign Microsoft MDM Group Policy to Amazon WorkSpaces Directory OUs that configures Hybrid Domain-join and prepares Amazon WorkSpace for Intune user credential-based enrollment.
4	Create the Autopilot Deployment profile for BYOL Windows 10 Amazon WorkSpaces for Hybrid joined devices that is assigned to the AD Security Group for Amazon WorkSpaces users.
5	User authenticates to Amazon WorkSpaces using Windows AD UPN that matches Azure AD UPN, initiating auto enrollment to Azure Hybrid AD join and Intune Autopilot.

Walkthrough

This section walks you through the process of setting up Windows Autopilot with Amazon WorkSpaces.

Prerequisites

You must have the following components configured to complete this walkthrough:

Azure Active Directory

- Microsoft Azure AD synchronized user objects and Windows AD user objects with matching UPNs.

> **Note**
>
> This setup requires a custom domain added to Azure Active Directory that matches the fully qualified domain name of the Windows AD in DNS. See the Azure online documentation for more information on how to add a custom domain.

- Windows AD Security Group created for Amazon WorkSpaces users and synchronized to Azure AD.
- Verify that the administrator has the necessary Azure Licensing [Azure Active Directory P1/P2] (for example, 'Enterprise Mobility + Security E5') to create Azure Active Directory user with Global Administrator assignment.

Amazon WorkSpaces

- Amazon WorkSpaces deployment is **only BYOL Windows 10 (v1809 or higher)**. This setup is required because Windows Server OS is not supported for Hybrid Azure AD Join by Microsoft.
- WorkSpaces Directory is an AD Connector for either an on-premises or Amazon EC2-based Active Directory Domain.

> **Note**
>
> This setup is required because completing the setup of hybrid Azure AD join requires an account with Enterprise Administrators AD Security Group membership.

Windows Active Directory

- Active Directory Schema must be at least version Windows Server 2012 R2 (level 69).
- Windows Server 2016 Active Directory Domain Services (AD DS) for Azure Hybrid AD Join.
- Write-able Domain Controllers must be used with Azure AD Connect instance, no redirects from Read-only Domain Controllers (RODCs) allowed.
- Full FQDN support, as NetBIOS names are not supported.
- (Large deployments - Optional) Active Directory exceeds 100,000 objects, full Microsoft SQL Server is required.

Azure AD Connect

- Create a Windows Server instance to host the following roles and meets the following minimum requirements:

- Instance must *not* be a Domain Controller
- Must not be Server Core as a full GUI is required
- Minimum of .NET Framework 4.5.1 installed for PowerShell
- Sizing of EC2 instance approximated by number of Active Directory objects
- < 100,000 - m5.large with 100 GB GP3 Volume
- > 100,000 - m5.2xlarge with 500 GB GP3 Volume + Microsoft SQL Server

- Azure AD Connect installation can be installed using the option for Express installation, however if your Active Directory exceeds 100,000 objects, the LocalDB (Microsoft SQL Server Express) created by the express installer will not work and a Custom installation must be selected.
- Ensure the following network requirements:

- TCP/UDP ports - outbound communication with Write-able Domain Controller(s)
- (If EC2) Domain Controller AWS Security Group allows standard domain controller TCP/UDP ports inbound from Azure AD Connect instance
- Allow outbound for TCP 80/443 for URLs and IP address ranges specified in Rule ID 56 of Microsoft Online network requirements.

Service accounts

- Create Accounts to Configure Azure AD Hybrid Domain Join

- Configure 'Global Administrator' Azure AD Account - required to Connect Azure AD
- Configure Windows AD Account that is an 'Enterprise Administrator' - required for service connection point (SCP)

Step 1: Establish Azure Active Directory Hybrid Environment for Amazon WorkSpaces

> **Note**
>
> Make sure you have completed an express installation for Azure AD Connect before proceeding by following the Microsoft guidelines.

The following steps help you configure Azure AD Connect after the express settings have been used for installation.

1. Connect to the Amazon EC2 instance with Azure AD Connect installed.
2. On your Amazon EC2 instance, open Azure AD Directory Connect and choose **Configure**.
3. On the **Tasks** page, choose **Configure device options**, and then choose **Next**.
4. On the **Overview** page, review the information and choose **Next**.
5. On the **Connect to Azure AD** page, enter the credentials for the Azure AD global administrator and choose **Next**.
6. On the **Device options** page, select Configure Hybrid Azure AD join and choose **Next**.

7. On the **Device systems** page, select the check box for Windows 10 or later domain-joined devices and choose **Next**.
8. On the **SCP configuration** page, select the check box for your **Forest**. Choose the **Authentication Service** drop-down list box and select **Azure Active Directory**. Choose **Add**, and then choose **Next**.
9. On the **Ready to configure** page, review the summary and choose **Configure**.
10. On the **Configuration complete** page, choose **Exit**.

Step 1a (Optional): Minimize total object synchronization

Optionally, you may want to minimize the total number of objects synchronized to Azure AD. If synchronizing all objects is acceptable, proceed to **Step 2**. Otherwise, to complete this, you must specify OU(s) for WorkSpaces users and computer objects.

1. Re-launch Azure AD Connect wizard and progressing past the welcome screen, choose **Custom synchronization options** and choose **Next**.
2. Authenticate ot Azure AD using the global administrator.
3. Leave the default setting for Active Directory and choose **Next**.
4. On the **Domain/OU Filtering** page, for **Directory**, choose your directory. Choose **Sync selected domains and OUs** and select the parent OU(s) that contain Amazon WorkSpaces users and computers. Choose **Next**.
5. On the **Optional features** page, choose **Password writeback** and keep the remaining default options. Then, choose **Next**.
6. Complete the configuration by choosing **Next** on the remainder of the Wizard settings pages.

Step 2: Configure Group Policy to Hybrid-join Azure Active Directory

If the Group Policy Management console has not already been installed on your management device, visit the Microsoft documentation for download and instructions.

1. From a Windows domain-joined resource with server administration tools installed, launch the Group Policy Management console from Windows Administrative Tools.
2. In the navigation pane, navigate to **Forest > Domains > Domain Name > WorkSpaces OU.**

3. Right-click the WorkSpaces OU and choose **Create and Link New GPO**.
4. In the **New GPO** window, type *Hybrid Azure AD Join* and choose **OK**.
5. Right-click the new GPO and choose **Edit.**
6. Navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components/MDM**.
7. Double-click **Enable MDM automatic enrollment using default Azure AD Credentials**.
8. Select **Enabled** and choose the **Select Credential Type to Use** drop-down list. Choose **User Credential**.
9. Close the **Group Policy Management** console.

Step 3: Assign Azure Intune Licensing to Amazon WorkSpaces User Group

> **Note**
>
> All synchronized Windows AD users must have a *Usage location* defined in the Settings section of user profiles. If this setting is missing, Azure licensing will not be saved correctly as not all licensed features are available in all countries. If not previously completed, enable group-based licensing.

1. Go to https://portal.azure.com and authenticate with the Azure AD global administrator credentials.
2. Choose **Azure Active Directory**.
3. In the **Manage** section, choose **Licenses**.
4. In the **Manage** section, choose **All products**.
5. Choose the licensed feature (**Enterprise Mobility + Security E5**).
6. In the **General** section, choose **Licensed groups** and then choose **+ Assign**.
7. Choose **Add users and groups**.
8. In the right pane of **Add users and groups**, scroll through the list or search for the AD Security Group for WorkSpaces users, and choose **Select**.
9. Choose **Review + assign**.

10. Choose **Assign**.

Step 4: Configure Intune Windows Enrollment for Amazon WorkSpaces

1. Go to https://endpoint.microsoft.com and authenticate using the Azure AD global administrator credentials.
2. Navigate to **Devices > Device enrollment - Enroll devices**.
3. In Windows Autopilot Deployment Program, choose **Intune Connector for Active Directory**.
4. Do one of the following:
   - If there is no Connector in the list, choose **+ Add** to open the details pane.
   - If there is an Intune Connector deployed already, skip to Step 12 in this section.
5. Choose **Download the on-premises Intune Connector for Active Directory** to download and install on the Azure AD Connect instance specified in Step 1.
6. Using the controls in your web browser, save the file ODJConnectorBootstrapper.exe to your Downloads folder and open the file to begin the installation.
7. On the **Intune Connector for Active Directory** setup wizard, select the check box to agree to the licensing terms and conditions and then choose **Install**.
8. If a User Account Control (UAC) dialog box appears, choose **Yes** to continue.
9. On the **Installation completed** screen, choose **Configure Now**.
10. If a User Account Control (UAC) dialog box appears, choose **Yes** to continue.
11. On the **Enrollment** page, choose **Sign-in** to log in with the same Azure account (Global admin role assigned) you used previously in Step 1. Choose **Yes** to remain signed in.

    Once completed, a message appears confirming Intune connector is enrolled for Active Directory.
12. Return to https://endpoint.microsoft.com to verify the connector status displays as **Active**.
13. Navigate to **Devices > Device enrollment - Enroll devices** and in the **General** section, choose **Automatic enrollment**.
14. On the **Configure** page, for MDM user scope, choose **All** and choose **Save**.

Step 5: Authenticate to Amazon WorkSpaces Client using Windows AD UPN

1. On a connected device, launch the Amazon WorkSpaces Client.
2. In the **username** field, enter the username in the Windows AD UPN format (for example, username@subdomain.example.com)
3. Once logged in, wait approximately five minutes, then launch a command prompt (cmd.exe).

   Verify Hybrid AD Join configuration using the following command: `dsregcmd`

   `/status`

If Hybrid AD Join configuration is unsuccessful, visit the Microsoft documentation for troubleshooting Azure Active Directory devices.

Step 6: Confirm Amazon WorkSpaces Intune Enrollment

1. Return to https://endpoint.microsoft.com and refresh the page.
2. Navigate to **Devices > Windows devices**.
3. Confirm the Amazon WorkSpaces instance has been added to the group by comparing the machine names to the device names in the list.

General Intune considerations

If this is your first time using Amazon WorkSpaces to manage Windows 10 through Intune, here are some general pointers to get you started on the right path.

- Although Microsoft Azure licensing and assignments must be made to user security groups, almost all Intune assignments must be made to device security groups. That means for every user you add to a security group, you must also add a WorkSpaces Computer Object to a device security group.
- Intune configurations and policies that conflict with existing GPOs will break Windows updates. This means any SCCM, WSUS, and/or GPOs for Windows Update must be removed for Intune Windows Update Rings to function successfully in your hybrid environment.

- Windows 10 Device Restrictions must be enabled in your Intune device configuration profile to share reporting and telemetry with Intune. Without this, Windows updates, and feature updates especially, will not successfully complete.
- It is recommended that you create an additional Configuration profile for Delivery Optimization. Enabling the setting HTTP blended with peering behind the same NAT (restricted to the same Subnet mask) will set all WorkSpaces within an Availability Zone to optimize internet downloads and share Windows updates amongst each other. Additionally, to optimize system volumes, set the cache drive to D: and Minimum disk size required for peer caching that does not exceed the total user volume size in GB.
- Feature Update profiles do not deploy feature updates; they are for monitoring the feature update deployment. If your Feature Update profile is properly assigned to the device security group that has your WorkSpace hostname and telemetry enabled, monitoring provides the status of Amazon WorkSpaces Feature updates (such as Pending updates, Up to date, or Failed).
- Features Updates are deployed from your Update Rings profile and must include a deferral period, device security group that matches your Feature Update policy, and (as stated previously) no conflicting SCCM, WSUS, and/or GPOs for Windows update. Feature updates are deployed automatically to not exceed the version assigned in your Feature Update profile.
- Feature updates can be paused individually from your running Update Rings profile to give the administrator time to set the proper WorkSpaces Registry settings for feature update in-place upgrades. Selecting Pause prevents your Amazon Workspaces from receiving feature updates for up to 35 days. Pausing updates can optionally be extended as required.

Step 7: Clean Up

After setting up this implementation, you can keep your configuration running or clean up all resources. For pricing details on this configuration, see the *Cost* section of this document. To delete the AWS resources that you created for this walkthrough, so that you no longer accrue charges, complete the following steps:

1. Shut down and end any launched Amazon WorkSpaces.
2. Shut down and deregister any launched directories.
3. Delete the Amazon EC2 instance.
4. Remove your custom domain name from Amazon Route 53.
5. Revoke any assigned licenses used for Azure AD and Intune.

Conclusion

In this guide, you established and configured Azure AD Hybrid Join and the respective Group Policy settings. You configured Microsoft Intune for Amazon WorkSpaces Windows enrollment using setup user credential-based initialization. Finally, you confirmed and validated your setup and began managing your WorkSpaces deployment from Intune.

Contributors

Contributors to this document include:

- Asriel Agronin, Sr. EUC Solutions Architect, Amazon Web Services
- Naviero Magee, Principal EUC Solutions Architect, Amazon Web Services
- Andrew Morgan, EUC Solutions Architect, Amazon Web Services
- Dustin Shelton, Sr. EUC Solutions Architect, Amazon Web Services
- Andy Soderberg-Rivkin, EUC Solutions Architect, Amazon Web Services
- Stephen K. Stetler, Sr. EUC Solutions Architect, Amazon Web Services
- Justin Stokes, Sr. Solutions Architect Manager, Amazon Web Services

Additional resources

For additional information, see:

- *Best Practices for Deploying Amazon WorkSpaces* (AWS whitepaper)
- Amazon WorkSpaces Documentation

Document revisions

To be notified about updates to this whitepaper, subscribe to the RSS feed.

Change	Description	Date
Initial publication	Whitepaper published.	June 10, 2021

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.

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the *AWS Glossary Reference*.