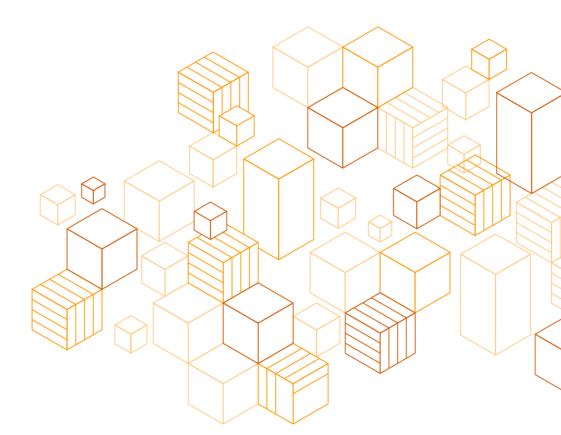
Provision Desktops in the Cloud

Learn how to provision, manage, and access Amazon Workspaces

June 2020





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.

© 2020 Amazon Web Services, Inc. or its affiliates. All rights reserved.

Contents

Step 1. Prepare an AWS Account	1
Step 2: Create the VPC and Subnets	1
Create a new VPC using the VPC wizard	2
Add a Second Private Subnet	4
Modify the Route Tables	5
Step 3: Create an Amazon WorkSpaces Directory in the Cloud	7
Step 4: Launch WorkSpaces	8
Step 5: Customize the Initial WorkSpace	12
Step 6: Create a Custom Image and Bundle	17
Step 7: Reboot, restore and rebuild	21
Reboot	21
Restore	22
Rebuild	23
Step 8: Modify Running Mode Properties	25
Step 9: Cleanup	27
Additional Resources	28

Welcome

In this project, you'll learn how to deploy virtual desktops using Amazon WorkSpaces and the AWS Directory Service. 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. The AWS Directory Service makes it easy to setup and run Microsoft Active Directory in the AWS cloud, or connect your AWS resources with an existing on-premises Microsoft Active Directory.

What you'll accomplish:

- Provision Cloud Desktops using Amazon WorkSpaces, and access them using the Amazon WorkSpaces client application, available for Windows, Linux, and Mac computers; Chromebooks; iPads, Amazon Fire tablets, and Android tablets.
- Create a new directory using Microsoft Active Directory and add users. As part
 of the project, you'll learn how to assign Amazon WorkSpaces to users in your
 Microsoft AD.
- Perform basic administrative tasks using the AWS Management Console. You'll learn how to reboot and rebuild Amazon WorkSpaces, create your own custom image which you can use for provisioning new Amazon WorkSpaces, and remove Amazon WorkSpaces.

What you'll need before starting:

- An AWS Account: You will need an AWS account to begin provisioning Amazon WorkSpaces. Sign-up for AWS.
- Skill level: A basic understanding of desktop computing and Microsoft Active Directory is helpful but not required.
- AWS Experience: No prior experience with AWS is required to complete this project.

Step 1. Prepare an AWS Account

- 1. If you don't already have one, create an AWS account.
- Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/
- 3. In the upper right corner, select a valid Region from the Region drop-down list. See the Region Table for the most up-to-date list of Regions where Amazon WorkSpaces is available.

Note: For help selecting the closest region, see the Connection Health Check page which shows Round Trip Time to all service Regions.

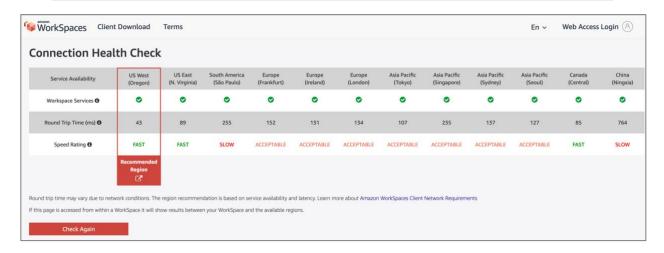


Figure 1: WorkSpaces Health Check

Step 2: Create the VPC and Subnets

For WorkSpaces to function correctly, you must have one public subnet and two private subnets. You can set this up by using the VPC Wizard. The VPC Wizard creates one public subnet, one private subnet, one NAT gateway, and an internet gateway for you. If you use the VPC Wizard, you do not need to manually create the routing tables between the subnets.

Before you create the VPC, you need to allocate an Elastic IP address.

- 1. Open the Amazon EC2 Dashboard.
- 2. In the navigation pane, under **Network & Security**, choose **Elastic IPs.**



3. Choose **Allocate Elastic IP address**, then choose **Allocate** (*Figure 2*). Take note of the resulting Elastic IP address.



Figure 2: Allocating an Elastic IP address

Create a new VPC using the VPC wizard

- 4. Open the Amazon VPC Dashboard.
- Choose Launch VPC Wizard.
- 6. Choose VPC with Public and Private Subnets and click Select (Figure 3)



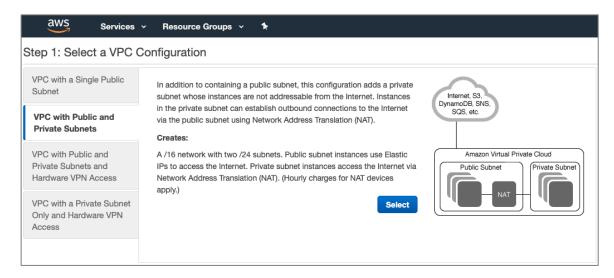


Figure 3: Creating VPCs with the VPC wizard

7. Enter the following information into the wizard:

Table 1: VPC Wizard options

Option	Value
IPv4 CIDR block	10.0.0.0/16
IPv6 CIDR block	No IPv6 CIDR Block
VPC name	WorkSpaces VPC
Public subnet's IPv4 CIDR	10.0.0.0/24
Availability Zone	No Preference
Public subnet name	WorkSpaces Public Subnet
Private subnet's IPv4 CIDR	10.0.1.0/24
Availability Zone	No Preference
Private subnet name	WorkSpaces Private Subnet 1
Elastic IP Allocation ID	Select the Elastic IP Allocation ID that corresponds with the address you created in the prior section. This is assigned to the NAT gateway
Service endpoints	Leave default
Enable DNS hostnames	Yes



Option	Value
Hardware tenancy	Default

Note: VPC and subnet names are for identification purposes only; you may use any descriptors that are meaningful to you.

8. Choose Create VPC.

It takes several minutes for the VPC to be created. After the VPC is created, proceed to the following section.

Add a Second Private Subnet

Create the second private subnet by performing the following steps:

- 1. In the **VPC Dashboard** navigation pane, choose **Subnets**.
- 2. In the list of subnets, select your private subnet (e.g., *WorkSpaces Private Subnet 1*) and view the Subnet details in the lower pane. Make a note of the **Availability Zone** of this subnet (*Figure 4*).

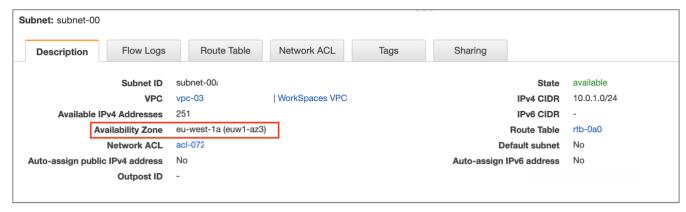


Figure 4: Identifying the Availability Zone for WorkSpaces Private Subnet 1

3. Choose **Create Subnet**, enter the following information in the **Create Subnet** dialog box:

Table 2: Subnet options

Option	Value
Name tag	WorkSpaces Private Subnet 2



Option	Value
VPC	Select your VPC. This is the VPC with the name WorkSpaces VPC
Availability Zone	Select any Availability Zone other than the one noted in step 2. The two subnets used by Amazon WorkSpaces must reside in two different Availability Zones.
IPv4 CIDR Block	10.0.2.0/24

4. Choose **Create** and then choose **Close**.

Modify the Route Tables

Modify the route tables for your subnets by performing the following steps.

- 1. In the **VPC Dashboard** navigation pane, choose **Subnets**.
- 2. In the list of subnets, select your public subnet (e.g., *WorkSpaces Public subnet*) and view the subnet details in the lower pane.
- 3. Choose the **Route Table** tab and make a note of the **Route Table** identifier for the subnet. The route table identifier is similar to *rtb-XXXXXXXX*.
- 4. In the VPC Dashboard navigation pane, choose Route Tables.
- 5. Locate the **Route Table ID** from *Step 3*, and in the **Name** column, click the edit icon to change the route table name. Change the name to **WorkSpaces Public route table**.

In the lower pane, choose the **Routes** tab and verify that the following entries are in the route table for *WorkSpaces Public route table*. Modify the route table if needed by choosing **Edit routes**.

Table 3: Public subnet route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-XXXXX

These entries route all traffic destined for the VPC locally and traffic destined to all other IP addresses to the internet gateway that was created with the VPC Wizard. (*igw-XXXXX*... identifies the internet gateway).



Note: For this example, all egress traffic is routed to the internet through the internet gateway set up on the VPC. However, if required, you can also route traffic to an IPS/IDS device that analyzes all outgoing traffic before it leaves the network.

- 6. In the **VPC Dashboard** navigation pane, choose **Subnets**.
- 7. In the list of subnets, select your private subnet (e.g., *WorkSpaces Private Subnet 1*) and view the subnet details in the lower pane.
- 8. Choose the **Route Table** tab and note the **Route Table** identifier for the subnet. The route table identifier will be similar to *rtb-XXXXXXXX*.
- 9. Select your second private subnet (e.g., *WorkSpaces Private Subnet 2*) and view the subnet details in the lower pane.
- 10. Choose the **Route Table** tab and note the **Route Table** identifier for the subnet. The route table identifier should be the same for both *WorkSpaces Private Subnet 1* and *WorkSpaces Private Subnet 2*. If the route table for *WorkSpaces Private Subnet 2* is different, edit the entry to make them the same.
- 11. In the VPC Dashboard navigation pane, choose Route Tables.
- 12. Locate the **Route Table ID** from *Step 8*, and in the **Name** column, click the edit icon to change the route table name. Change the name to *WorkSpaces Private route table*.
- 13. At the bottom of the page, choose the **Routes** tab and verify a local route for the VPC range, and a NAT route for 0.0.0.0/0.

Table 4: Private subnets route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	nat-XXXXX

These entries route all traffic destined for the VPC locally and traffic destined to all other IP addresses to the NAT gateway. (nat-xxxxxx... identifies the NAT gateway.)



Step 3: Create an Amazon WorkSpaces Directory in the Cloud

Amazon WorkSpaces uses a directory to store and manage WorkSpace and user information, and you can have Amazon WorkSpaces create this directory in the cloud for you using Simple AD or Microsoft Active Directory. Additionally, you can connect to an existing Active Directory using the AD Connector.

For this walkthrough, you create a Microsoft Active Directory using the Amazon Directory Service console.

- 1. Open the <u>Directory Service console</u>.
- 2. Choose **Set up directory**.
- 3. Under Directory types select AWS Managed Microsoft AD.
- 4. Choose Next.
- 5. Provide the following information:

Option	Value
Edition	Standard Edition
Directory DNS name	The fully qualified name for the directory, such as workspaces.demo.com
Directory NetBIOS name	The short name for the directory, such as workspaces
Directory description	An optional description for the directory
Admin password	The password for the directory administrator. The directory creation process creates an administrator account with the user name Admin and this password.
Confirm password	Retype the administrator password.

- 6. Choose Next.
- 7. In the Networking section, provide the following information:



Option	Value
VPC	The VPC for the directory (WorkSpaces VPC, or the VPC with IP range 10.0.0.0/16).
Subnets	Select the two private subnets, WorkSpaces Private subnet 1 and WorkSpaces Private Subnet 2 for the directory servers (IP ranges 10.0.1.0/24 and 10.0.2.0/24).

- 8. Choose Next.
- 9. Review the directory information and make any necessary changes. Then, choose **Create directory**.

Note: It takes several minutes for the directory to be created. When it has been successfully created, the **Status** value changes from **Creating** to **Active**.

Step 4: Launch WorkSpaces

Once the directory is active, you can launch WorkSpaces through the AWS Management Console.

1. Open the WorkSpaces console and choose Launch WorkSpaces (Figure 5).



Figure 5: Using the Launch WorkSpaces wizard

- 2. Select the directory you created in the previous section and choose **Next Step**. WorkSpaces registers your directory with the WorkSpaces service.
- 3. If prompted, select the private subnets you created earlier (CIDR 10.0.1.0/24 and 10.0.2.0/24, respectively) and choose **Next Step**.
 - You can now either add users to your directory or select from existing users. Since you just created this directory, you need to create at least one user.



4. Enter all of the appropriate information for the new user, and choose **Create Users**. The user account you created is automatically added to the WorkSpaces list (*Figure 6*).

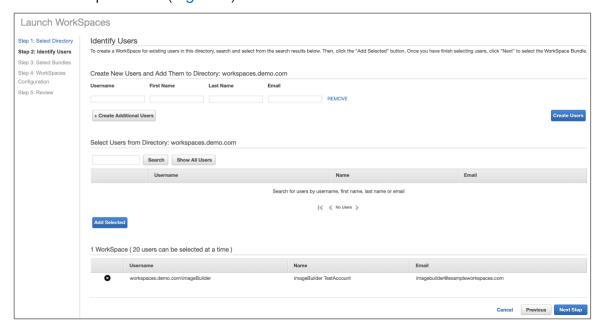


Figure 6: Creating and selecting a user

Note: The first WorkSpace you provision in this walkthrough is used to create a master image for subsequent deployments; you may want to identify this first WorkSpace by naming the first user account *ImageBuilder*.

It's important to use a valid email address where you can receive email so that you can receive the one-time activation link. For this user account to become active, you must set a password by following the instructions on the activation page. If you don't use a valid email address, you must retrieve the registration link from the console.

5. Next, you assign a WorkSpaces Bundle to the user you just created. For this walkthrough, select the **Standard with Windows 10** bundle and assign it to the user you created in the previous step. Then, choose **Next Step**.



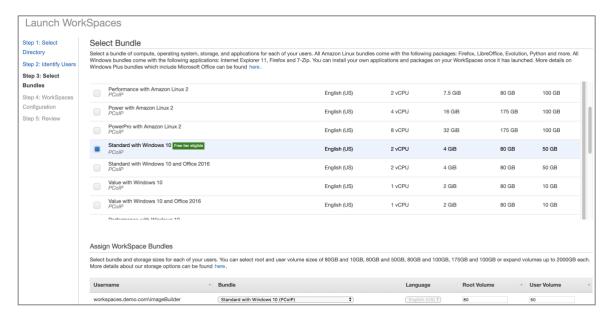


Figure 7: Selecting a WorkSpaces Bundle, and assigning it to a user

6. On the **WorkSpaces Configuration** options screen, for **Running Mode**, choose **AutoStop**. (The *AlwaysOn* running mode is used for monthly billing and *AutoStop* for hourly billing.)



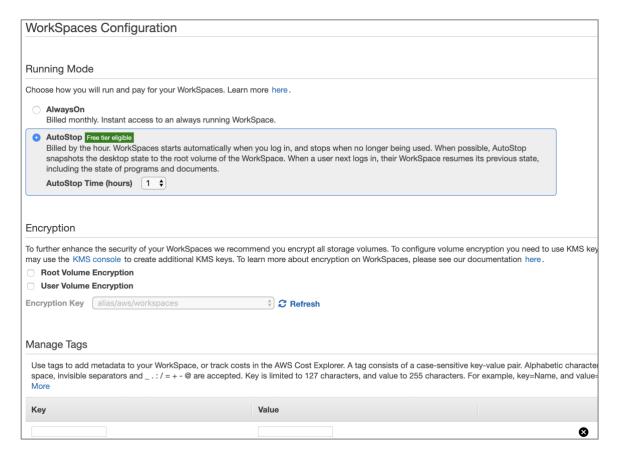


Figure 8: WorkSpaces Configuration

7. For **Encryption**, optionally select the encryption type.

Note: Selecting **Root Volume Encryption** increases the time required to provision a WorkSpace; however, there is no operational performance impact once the WorkSpace is provisioned.

- 8. For **Manage Tags**, optionally add tags.
- 9. Choose **Next Step**.
- 10. Review the WorkSpace details and then choose Launch WorkSpaces. This process takes approximately 60 minutes to complete (20 minutes if you did not select the option to encrypt the root volume). During this process, your WorkSpace shows a status of Pending. Once completed, the user account receives an email containing the registration code with instructions on downloading the client (https://clients.amazonworkspaces.com/).

If you do not receive the email, you can see the content of this message by selecting the user's WorkSpace and selecting **Actions**, **Invite User** (*Figure 9*).



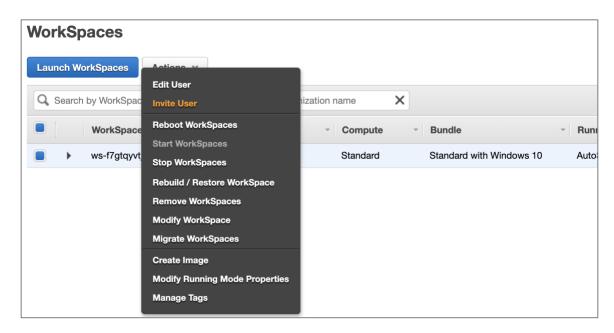


Figure 9: Retrieving the activation link for a user

11. Follow the link in the Invitation email to complete your user profile, download the WorkSpaces Client, and connect to the WorkSpace.

Step 5: Customize the Initial WorkSpace

By this point, you should be logged in to your first Amazon WorkSpace. Now, update the WorkSpace and add some applications.

Run Windows Update and apply any updates to bring your client up to date.
 Reboot when prompted.

Note: It takes around 5 minutes to reboot a WorkSpace, and note that some Windows Updates cause the restart to take longer. Once all Windows Updates have been applied, you can continue customizing this WorkSpace.

- 2. Change the Wallpaper.
- 3. Install the Chrome browser from https://www.google.com/chrome
- 4. Download and install the latest version of Notepad++ from https://notepad-plus-plus.org/download.



- Choose Start and type Server Manager (Amazon WorkSpaces Windows 10 desktop experiences is powered by Windows Server 2016) and choose Start Server Manager.
- 6. In Server Manager, choose **Manage** and then **Add Roles and Features** (*Figure 10*).

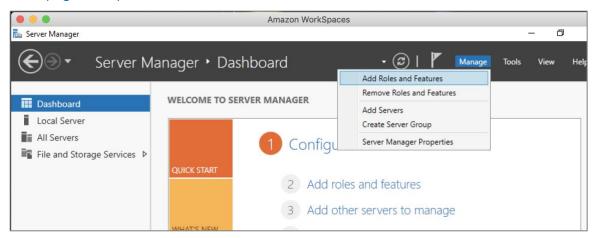


Figure 10: Adding features using Server Manager

7. Click **Next** until you see the **Features** section. Select **Remote Server Administration Tools** and then **AD DS and AD LDS Tools** (*Figure 11*).



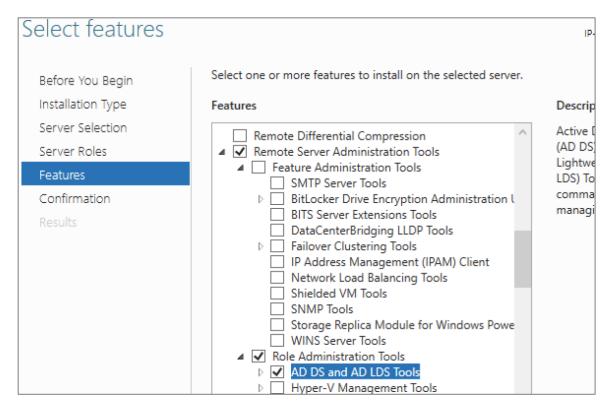


Figure 11: Adding RSAT for Active Directory administrator capabilities

- 8. Continue through the wizard until you see the **Confirmation** section and choose **Install**.
- 9. Once the wizard finishes, choose **Close**.
- 10. Back in the desktop, choose Start and type Users and Computers. You should see the Active Directory Users and Computers administrative tool. Right-click Active Directory Users and Computers, and choose Run as different user (Figure 12).



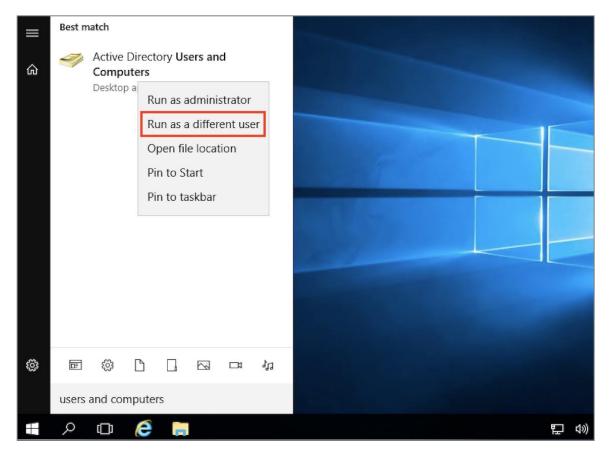


Figure 12: Run AD Users and Computers as different user

11. When prompted, enter **admin** as the username and the password you used when creating the directory in <u>Step 3: Create an Amazon WorkSpaces Directory in the Cloud</u> (*Figure 13*). This is your Microsoft AD directory.



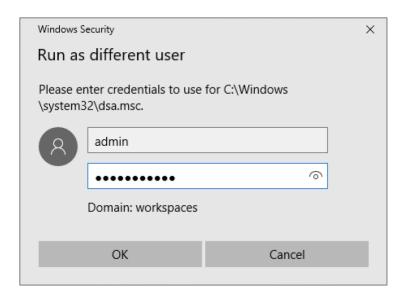


Figure 13: Run as admin

12. Go to the *workspaces.demo.com* domain, expand the **workspaces** Organization Unit (OU), and select the **Users** OU (*Figure 14*).

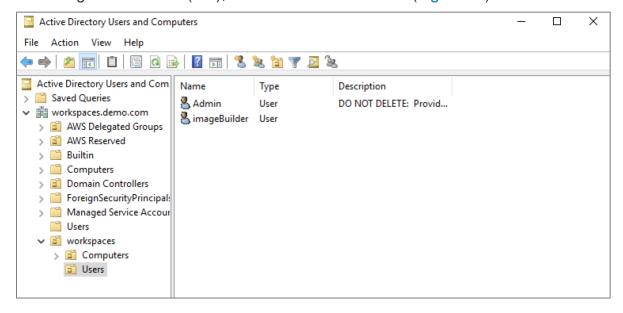


Figure 14: Active Directory view

13. On the Action menu, select New, then User, and create a new Test User in your directory (Figure 15). You use this user later when deploying an additional WorkSpace. Click Next.



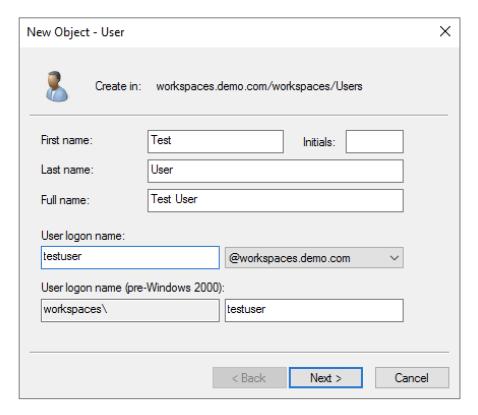


Figure 15: Adding a new user to your Active Directory

- 14. Set a password you'll remember, and clear the check box for **User must** change password at next logon.
- 15. After creating the user account, right-click **Test User**, select **Properties**, and specify an email address.

Note: Without an email address, you won't be able to provision a WorkSpace in later steps.

16. Close the **Active Directory Users and Computers** console, and restart the WorkSpace.

Step 6: Create a Custom Image and Bundle.

Now that you've customized your WorkSpace, it's time to create an image that you can use for subsequent deployments.

- 1. Open the WorkSpaces console.
- 2. Verify the status of the WorkSpace assigned to **ImageBuilder** is **AVAILABLE**.



3. Select the ImageBuilder WorkSpace, choose **Actions**, **Create Image** (*Figure* 16).

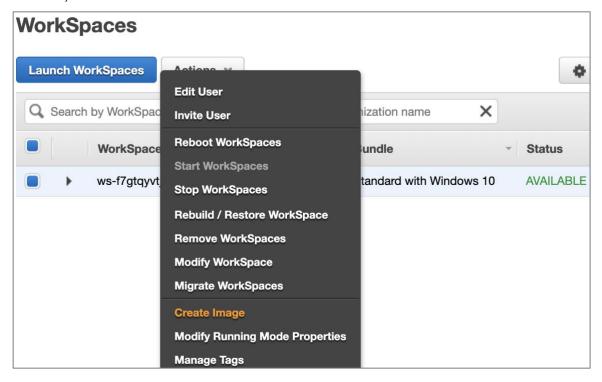


Figure 16: Creating a new image for future WorkSpaces

4. Give the image a name and a description, then choose **Create Image** (*Figure* 17).

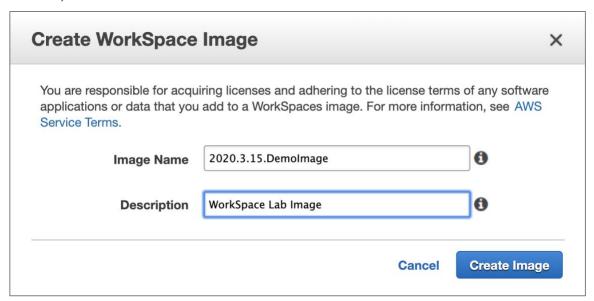


Figure 17: Naming your new image



Note: This process takes approximately 45 minutes to complete. The ImageBuilder WorkSpace is unavailable during this time. You can monitor the progress from the **Images** section of the WorkSpaces console. Once the Image status changes to **AVAILABLE**, your ImageBuilder WorkSpace restarts and is available for use again.

Once the image is complete, you need to create a bundle based on this Image.

5. On the **Images** page, select the new image, choose **Actions**, and **Create Bundle** (*Figure 18*).



Figure 18: Creating a bundle with your new image

6. Give the bundle a name, description, select its type and set a size for the User Volume, then choose **Create Bundle** (*Figure 19*).

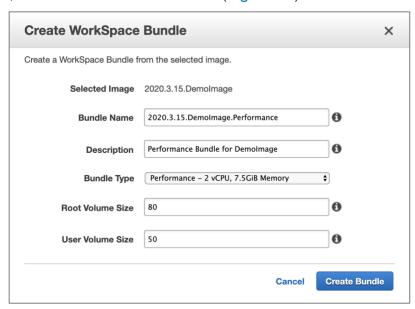


Figure 19: Creating your new bundle



Note: As you can see, the Bundle Type does not have to match the type you used when creating the initial WorkSpace.

- 7. Back on the main WorkSpaces console, choose Launch WorkSpace.
- 8. Select the *workspaces.demo.com* directory and choose **Next Step**.
- Choose Show All Users and select the Test User account you created previously. Then, choose Add Selected, and Next Step.
- 10. Select the bundle you created in the previous and choose **Next Step** (*Figure 20*).

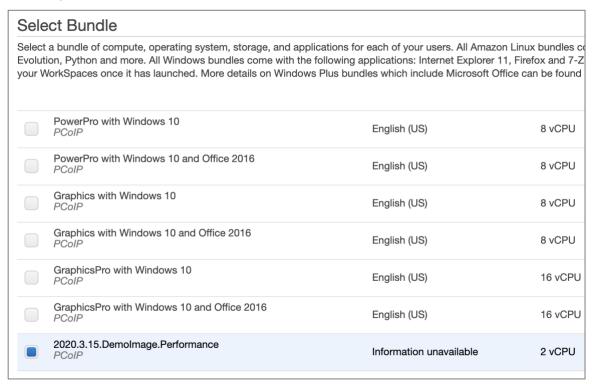


Figure 20: Using your new bundle to create a new WorkSpace

- 11. On the WorkSpaces Configuration screen, for running mode, choose **AutoStop**. Then, choose **Next Step**.
- 12. On the **Review & Launch** screen, choose **Launch WorkSpaces**.

Note: WorkSpaces may take up to 20 minutes to become available. If you selected the option to encrypt the root volume, the provisioning might take up to 60 minutes.



13. Once the WorkSpace for Test User is complete, connect to the WorkSpace using the WorkSpaces client.

Note: Registration codes are unique per directory, so the registration code will be the same as it was for your initial WorkSpace.

Once you're at the desktop for the Test User WorkSpace, you should see:

- The Wallpaper is the same as for your ImageBuilder WorkSpace.
- Chrome and Notepad++ are installed.
- The Active Directory Remote Server Administration Tools are already available.
- The WorkSpace has all Windows Updates available up to the point where you created the Image.

Step 7: Reboot, restore and rebuild

The three primary actions you'll use when troubleshooting a WorkSpace are reboot, restore, and rebuild. If you're connected to the WorkSpace, you can always restart the WorkSpace as with any other Windows client, from the Start menu. For this example, we're going to connect to the WorkSpace, then force an administrative reboot from the WorkSpaces console.

Reboot

 After confirming the state of the Test User WorkSpace, connect to the WorkSpace, then go back to the main screen of the WorkSpaces console. While still logged in and connected to the Test User WorkSpace, select the Test User WorkSpace in the console, choose **Actions**, and then **Reboot Workspaces** (*Figure 21*).

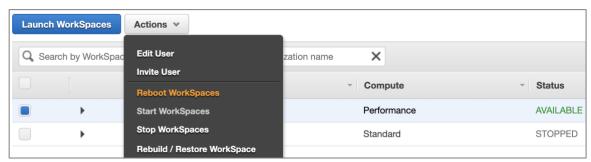


Figure 21: Rebooting your WorkSpace



You are disconnected from the WorkSpace while it reboots.

Wait around five minutes for the workspace to transition states from AVAILABLE to REBOOTING, and back to AVAILABLE, then reconnect.

Restore

Automatic snapshots for use when restoring a WorkSpaces are scheduled every 12 hours. If the WorkSpace is healthy, snapshots of both the System volume and the User Data volume are created around the same time. Restoring a WorkSpace recreates both the root volume and user volume based on the most recent snapshots, meaning that the System volume (drive C:\) is restored to the most recent snapshot, so any application or system settings that took place after the snapshot timestamp are lost. The User Data volume (drive D:\) is recreated and its content overwritten.

You can restore a WorkSpace as follows:

- Log back in to the WorkSpaces console.
- Select the Test User WorkSpace.
- 3. Choose Actions, then Rebuild / Restore WorkSpace (Figure 22).

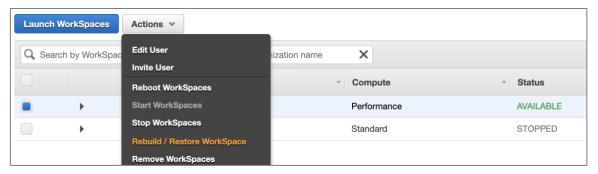


Figure 22: Rebuild/Restore a WorkSpace

 On the pop up window, select Restore WorkSpace and choose Rebuild / Restore WorkSpace (Figure 23).



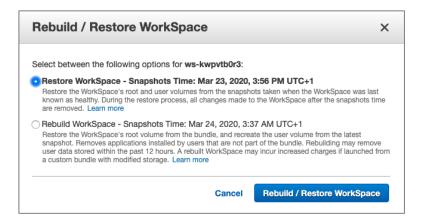


Figure 23: Restoring a WorkSpace

Rebuild

Rebuilding a WorkSpace is a more destructive action. Unlike the restore option, the System volume (drive C:\) is rebuilt from the bundle used to provision the WorkSpace, and the User Data volume (drive D:\) is restored to the last snapshot. Any new applications installed to the System volume are not restored. For this lab, if you want to see the snapshot recovery in action, you may want to write some data files to the D:\ drive, then come back 12 hours later to try the rebuild operation.

Now, see how a rebuild works with an example:

- 1. Connect to the Test User WorkSpace.
- 2. Go to **Add or Remove Programs**.
- 3. Uninstall Notepad++
- 4. Go to https://sublimetext.com/3 and download the installer for Windows 64 bit. Save the downloaded file to the D:\ drive.
- 5. Run the install with the default install directory of C:\Program Files\Sublime Text 3.

Now, your Test User WorkSpace has Sublime Text 3 installed, but you've removed Notepad++.



Note: If you rebuild right now, you'll revert to the prior state, but since this WorkSpace is less than 12 hours old, you will not get an updated snapshot of the D:\ volume. To see the data volume snapshot restore at work, you'll have to pause the lab and come back tomorrow. If you want, go ahead and copy some additional files to the D:\ volume.

...12 hours later...

Welcome back! Let's continue with the rebuild operation:

- 1. Log back in to the WorkSpaces console.
- 2. Select the Test User WorkSpace.
- 3. Choose **Actions** and then **Rebuild / Restore WorkSpace** (*Figure 24*).

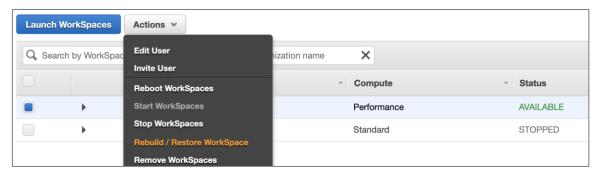


Figure 24: Rebuilding a WorkSpace

 On the pop up window, select Rebuild WorkSpace and choose Rebuild / Restore WorkSpace (Figure 25).

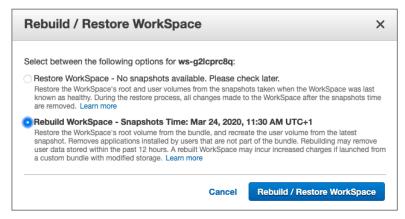


Figure 25: Rebuilding a WorkSpace dialog box



The rebuild operation takes about half an hour to complete. Once the process is complete, reconnect to the Test User WorkSpace. You should notice the following:

- SublimeText is gone.
- Notepad++ is back
- Assuming you waited at least 12 hours, any files you created on the D:\ drive
 are still present. This would include the SublimeText installer your previously
 download and saved to the D:\ volume.

Step 8: Modify Running Mode Properties

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 WorkSpace to cover infrastructure costs and storage, and a low hourly rate for each hour the WorkSpace is used during the month. To pay monthly, your Amazon WorkSpaces needs to be configured to run in the AlwaysOn running mode. To pay hourly, your Amazon WorkSpace needs to be configured to run in the AutoStop running mode. You can mix monthly and hourly billing within your AWS account, and you can also switch between billing options at any time during a billing period to optimize your AWS bill. To learn more about billing options and pricing, see Amazon WorkSpaces Pricing.

To change the running mode for one of your WorkSpaces:

- 1. Log back in to the WorkSpaces console.
- 2. Select the Test User WorkSpace (previously configured to run in the AutoStop running mode).
- 3. Click Actions, and select Modify Running Mode Properties (Figure 26).



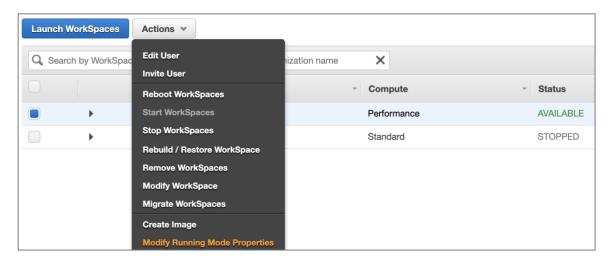


Figure 26: Changing the Running Mode Properties

4. Select the new running mode for your WorkSpace (*Figure 27*).

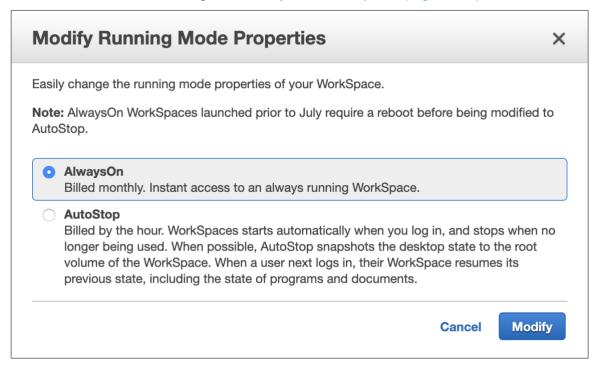


Figure 27: Changing the Running Mode Properties dialog box

5. You'll see the Running Mode reflected in the console.

To help customers monitor their WorkSpace usage and optimize costs, AWS also offers the Amazon WorkSpaces Cost Optimizer, an AWS Solution Implementation that analyzes all of your Amazon WorkSpaces usage data and automatically converts the



WorkSpace to the most cost-effective billing option (hourly or monthly) depending on user's individual usage.

Step 9: Cleanup

Congratulations! You've successfully provisioned a WorkSpace, created an Image of the initial WorkSpace, created a Bundle from the Image, deployed a new WorkSpace from a custom Bundle, rebooted, restored, rebuilt a WorkSpace and switched Running Modes.

If you're ready to clean up the environment, you need to delete components in the right order.

Go to the WorkSpaces console. Under **Bundles**, select your custom bundle, choose **Actions**, and **Delete Bundle**. The action does not succeed, because all WorkSpaces built from that bundle must be deleted first. The same is true if you attempt to delete the Image while a Bundle is still attached to the Image.

To clean up:

- Go to the WorkSpace page, select both the Test User and ImageBuilder WorkSpaces. Choose Actions, Remove WorkSpaces, and confirm by typing REMOVE and choosing Remove WorkSpaces.
- 2. After the WorkSpaces terminate, go to **Bundles**, select the custom bundle, choose **Actions**, **Delete Bundle**.
- 3. Go to Images. Select the custom image, Actions, Delete Image.
- 4. If you want to delete the directory, you'll need to de-register it from the WorkSpace service. Go to the **Directories** tab of the WorkSpaces console. Select the directory, choose **Actions**, **Deregister** (*Figure 28*).

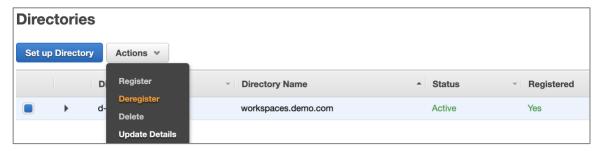


Figure 28: Deregistering Amazon WorkSpaces from your Microsoft AD service



5. Select the Directory again, but this time, choose **Actions**, then **Delete** and confirm (*Figure 29*).



Figure 29: Deleting your Microsoft AD

It will take a few minutes for the directory to delete. Wait for the process to complete.

- 6. In the VPC console, delete the NAT Gateway associated with the WorkSpaces VPC.
- 7. In the VPC console, and delete the WorkSpaces VPC (Figure 30).

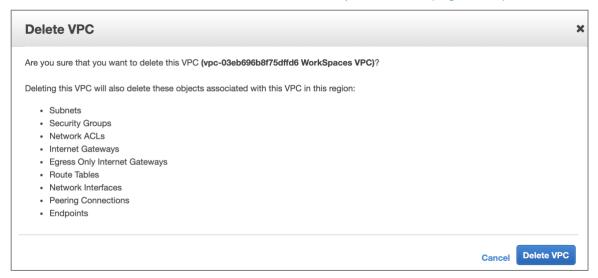


Figure 30: Deleting your WorkSpaces VPC

8. In the EC2 console, release the Elastic IP address that was previously associated to the NAT Gateway.

Additional Resources

For additional information, see:



- Amazon WorkSpaces Downloadable Clients
- Amazon WorkSpaces Connection Health Check
- Amazon WorkSpaces FAQs
- Amazon WorkSpaces Administration Guide

