Amazon WorkSpaces

Administration Guide

Version 1.0

Amazon WorkSpaces: Administration Guide

Table of Contents

What is Amazon WorkSpaces?

Amazon WorkSpaces offers you an easy way to provide a cloud-based desktop experience to your users. Select from a choice of WorkSpace bundles that offer a range of different amounts of CPU, memory, storage, and a choice of applications. Then, enter user information and launch the number of WorkSpaces that you require. As soon as the WorkSpaces are ready, users can download the Amazon WorkSpaces client and connect to their WorkSpaces. Users can connect from a PC or Mac desktop computer, or an iPad, Kindle, or Android tablet.

You can create a standalone, managed directory for your users, or you can use AD Connector to connect to your on-premises directory so that your users can use their existing credentials to obtain seamless access to corporate resources. This integration works using a secure hardware VPN connection to your on-premises network using Amazon Virtual Private Cloud (Amazon VPC) or with AWS Direct Connect.

With Amazon WorkSpaces, you don't have to procure or deploy hardware or install complex software to deliver a desktop experience to your users. Amazon WorkSpaces takes care of all the heavy lifting of managing hardware and software, and tasks such as patching and maintenance, enabling you to easily deliver a high quality desktop experience to your users. When you connect Amazon WorkSpaces to your on-premises directory, you can manage your WorkSpaces with the tools you are already using for your on-premises desktops and you maintain full administrative control.

For more information, see Amazon WorkSpaces.

Amazon WorkSpaces Concepts

The terminology and concepts that are important for your understanding and use of Amazon WorkSpaces service are described below.

Contents

- Running Mode (p. 6)

Network Interfaces

Each WorkSpace has two network interfaces. One interface, known as the primary network interface, provides connectivity to the resources within your VPC as well as the Internet, and is used to join to the WorkSpaces directory.

The other interface, known as the management network interface, is connected to a secure Amazon WorkSpaces management network. The management network interface is used for interactive streaming of the WorkSpace desktop with the Amazon WorkSpaces client application, and also allows the Amazon WorkSpaces service to manage the WorkSpace. The Amazon WorkSpaces service selects the IP address for the management network interface from various address ranges, depending on the region the WorkSpaces are created in. When a directory is registered, Amazon WorkSpaces tests the VPC CIDR and the route tables in your VPC to determine if these address ranges will create a conflict. If a conflict is found in all available address ranges in the region, an error message is displayed and the directory is not registered. If you change the route tables in your VPC after the directory is registered, you may cause a conflict. It is not possible to specify manually which IP address range is used. The following table lists the IP address ranges used for each region.

Region	Management Interface IP Address Ranges
US East (N. Virginia)	172.31.0.0/16, 192.168.0.0/16, and 198.19.0.0/16
US West (Oregon)	172.31.0.0/16 and 192.168.0.0/16
EU (Ireland)	172.31.0.0/16 and 192.168.0.0/16
EU (Frankfurt)	172.31.0.0/16 and 192.168.0.0/16
Asia Pacific (Sydney)	172.31.0.0/16 and 192.168.0.0/16
Asia Pacific (Tokyo)	198.19.0.0/16
Asia Pacific (Singapore)	198.19.0.0/16

Do not modify or delete any of the network interfaces attached to a WorkSpace. Doing so may cause the WorkSpace to become unreachable.

Management Interface Ports

The following ports must be open on the management network interface of all WorkSpaces:

- Inbound TCP on port 4172. This is used for establishment of the streaming connection.
- Inbound UDP on port 4172. This is used for streaming user input.
- Inbound TCP on port 8200. This is used for management and configuration of the WorkSpace.
- Outbound UDP on port 55002. This is used for PCoIP streaming. If your firewall uses stateful filtering, the ephemeral port 55002 is automatically opened to allow return communication. If your firewall uses stateless filtering, you need to open ephemeral ports 49152 - 65535 to allow return communication.

Under normal circumstances, the Amazon WorkSpaces service properly configures these ports for your WorkSpaces. If any security or firewall software is installed on a WorkSpace that blocks any of these ports, the WorkSpace may not function correctly or may be unreachable.

Primary Interface Ports

No matter which type of directory you have, the following ports must be open on the primary network interface of all WorkSpaces:

- For Internet connectivity, the following ports must be open outbound to all destinations and inbound from the WorkSpaces VPC. You need to add these manually to the security group for your WorkSpaces if you want them to have Internet access.
  - TCP 80 (HTTP)
  - TCP 443 (HTTPS)
- To communicate with the directory controllers, the following ports must be open between your WorkSpaces VPC and your directory controllers. For a Simple AD directory, the security group created by AWS Directory Service will have these ports configured correctly. For an AD Connector directory, you may need to adjust the default security group for the VPC to open these ports.
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos authentication
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP 1024-65535 - Dynamic ports for RPC

  If any security or firewall software is installed on a WorkSpace that blocks any of these ports, the WorkSpace may not function correctly or may be unreachable.
- All WorkSpaces require that port 80 (HTTP) be open to IP address `169.254.169.254` to allow access to the EC2 metadata service. Any HTTP proxy assigned to your WorkSpaces must exclude `169.254.169.254`.

PCoIP Gateway IP Ranges

Amazon WorkSpaces uses a small range of Amazon EC2 public IP addresses for its PCoIP gateway servers. This enables customers to set more finely grained firewall policies for their devices that access Amazon WorkSpaces. The Amazon WorkSpaces service uses the PCoIP gateway to stream the desktop session to its client applications over port 4172.

Region	PCoIP Gateway Server Public IP Address Range
US East (N. Virginia)	52.23.61.0 – 52.23.62.255
US West (Oregon)	54.244.46.0 – 54.244.47.255
EU (Ireland)	52.19.124.0 – 52.19.125.255
EU (Frankfurt)	52.59.127.0 - 52.59.127.255
Asia Pacific (Singapore)	52.76.127.0 – 52.76.127.255
Asia Pacific (Sydney)	54.153.254.0 – 54.153.254.255
Asia Pacific (Tokyo)	54.250.251.0 – 54.250.251.255

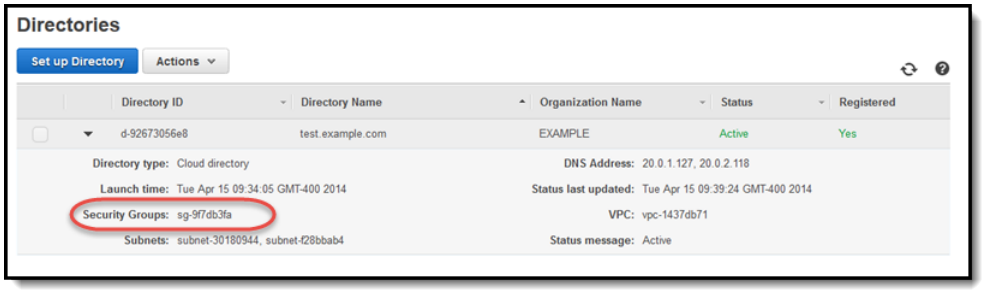
Network Health Check Servers

The Amazon WorkSpaces client application performs a network health check over port 4172. This validates whether TCP or UDP traffic streams from the client application to the Amazon WorkSpaces production servers. To do this successfully, firewall policies must take into account the following regional network health check servers.

Region	Network health check server
US East (N. Virginia)	drp-iad.amazonworkspaces.com
US West (Oregon)	drp-pdx.amazonworkspaces.com
EU (Ireland)	drp-dub.amazonworkspaces.com
EU (Frankfurt)	drp-fra.amazonworkspaces.com
Asia Pacific (Singapore)	drp-sin.amazonworkspaces.com
Asia Pacific (Sydney)	drp-syd.amazonworkspaces.com
Asia Pacific (Tokyo)	drp-nrt.amazonworkspaces.com

WorkSpaces Security Group

Amazon WorkSpaces creates a security group that is assigned to all WorkSpaces in the directory. You can find the identifier of this security group in the **Security Groups** field of the directory details, as shown in the following image.



You have the option to have an additional security group applied to your WorkSpaces when they are created or rebuilt by adding a security group. For more information, see the following topics:

Cloud Directory
Add a Security Group (p. 43)

AD Connector Directory
Add a Security Group (p. 46)

Microsoft AD Directory
Add a Security Group (p. 49)

If you need to reset the WorkSpaces security group to its original configuration, the following are the minimum port requirements for the WorkSpaces security group. Your configuration may require that additional ports be open. The directory controllers security group has a name that consists of the directory identifier followed by `_controllers`, such as `d-92673056e8_controllers`.

Outbound Rules:

- TCP 53 - directory controllers security group
- TCP 80 - 0.0.0.0/0
- TCP 88 - directory controllers security group
- TCP 135 - directory controllers security group
- TCP 389 - directory controllers security group
- TCP 443 - 0.0.0.0/0
- TCP 445 - directory controllers security group
- TCP 464 - directory controllers security group
- TCP 636 - directory controllers security group
- TCP 1024-65535 - directory controllers security group
- TCP 3268-3269 - directory controllers security group
- UDP 53 - directory controllers security group
- UDP 80 - 0.0.0.0/0
- UDP 88 - directory controllers security group
- UDP 123 - directory controllers security group
- UDP 138 - directory controllers security group
- UDP 389 - directory controllers security group
- UDP 443 - 0.0.0.0/0
- UDP 445 - directory controllers security group
- UDP 464 - directory controllers security group
- ICMP ALL - directory controllers security group

Restrictions

Amazon WorkSpaces has the following restrictions:

Topics

User Access Control

User Access Control is supported in WorkSpaces. You can set the UAC settings in your custom images or configure UAC by using group policy. Users who have administrative privileges on their WorkSpaces can also change the UAC settings through the Windows Control Panel.

Firewalls

You can install any type of security or firewall software on a WorkSpace, but Amazon WorkSpaces requires that certain inbound and outbound ports are open on the WorkSpace. If the security or firewall software you install blocks these ports, the WorkSpace may not function correctly or may be unreachable. To correct this, you must rebuild the WorkSpace. For more information about the ports that must be open to the WorkSpaces, see Management Interface Ports (p. 2) and Primary Interface Ports (p. 3).

User Accounts

Amazon WorkSpaces has the following restriction for user accounts:

- When using the Active Directory Users and Computers tool to create a new user, or reset the password for an existing user, do not set the **User must change password at next logon** setting. The user will not be able connect to their WorkSpace. Instead, assign a secure temporary password to the user and instruct them to manually change their password from within the WorkSpace the next time they log on.

Running Mode

The running mode of a WorkSpaces determines its immediate availability and how you pay for it. You can choose between the following running modes:

- **AlwaysOn** — Use when paying a fixed monthly fee for unlimited usage of your WorkSpaces. This mode is best for users who use their WorkSpace full time as their primary desktop.
- **AutoStop** — Use when paying for your WorkSpaces by the hour. With this mode, your WorkSpaces stop after a specified period of inactivity and the state of apps and data is saved. To set the automatic stop time, use **AutoStop Time (hours)**.

  When possible, the state of the desktop is saved to the root volume of the WorkSpace. The WorkSpace resumes when a user logs in; all open documents and running programs return to their saved state.

You can switch between the running modes of a WorkSpace at any time either through the console or by using the Amazon WorkSpaces API.

Setting Up Amazon WorkSpaces

Before you use Amazon WorkSpaces, complete the following tasks:

Tasks

- Create an AWS Account (p. 7)
- Creating IAM Users (p. 7)
- Controlling Access to Amazon WorkSpaces Resources (p. 9)
- Preparing Your Network (p. 12)

Create an AWS Account

Your AWS account gives you access to all services in AWS, including Amazon WorkSpaces. You are charged only for the resources that you use.

If you have an AWS account already, skip to the next task. If you don't have an AWS account, use the following procedure to create one.

To create an AWS account

1. Open https://aws.amazon.com/, and then choose **Create an AWS Account**.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Creating IAM Users

Your AWS account credentials identify you to services in AWS and grant you unlimited use of your AWS resources, such as your WorkSpaces. To allow other users to manage Amazon WorkSpaces resources without sharing your security credentials, use AWS Identity and Access Management (IAM). We recommend that everyone work as an IAM user, including the account owner. You should create an IAM user for yourself, give that IAM user administrative privileges, and use it for all your work.

Create a User with Administrator Access

If you signed up for AWS but have not created an IAM user for yourself, you can create one using the IAM console.

To create an IAM user for yourself and add the user to an Administrators group

1. Sign in to the Identity and Access Management (IAM) console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose **Users**, and then choose **Add user**.
3. For **User name**, type a user name, such as `Administrator`. The name can consist of letters, digits, and the following characters: plus (+), equal (=), comma (,), period (.), at (@), underscore (_), and hyphen (-). The name is not case sensitive and can be a maximum of 64 characters in length.
4. Select the check box next to **AWS Management Console access**, select **Custom password**, and then type the new user's password in the text box. You can optionally select **Require password reset** to force the user to select a new password the next time the user signs in.
5. Choose **Next: Permissions**.
6. On the **Set permissions for user** page, choose **Add user to group**.
7. Choose **Create group**.
8. In the **Create group** dialog box, type the name for the new group. The name can consist of letters, digits, and the following characters: plus (+), equal (=), comma (,), period (.), at (@), underscore (_), and hyphen (-). The name is not case sensitive and can be a maximum of 128 characters in length.
9. For **Filter**, choose **Job function**.
10. In the policy list, select the check box for **AdministratorAccess**. Then choose **Create group**.
11. Back in the list of groups, select the check box for your new group. Choose **Refresh** if necessary to see the group in the list.
12. Choose **Next: Review** to see the list of group memberships to be added to the new user. When you are ready to proceed, choose **Create user**.

You can use this same process to create more groups and users, and to give your users access to your AWS account resources. To learn about using policies to restrict users' permissions to specific AWS resources, go to Access Management and Example Policies for Administering AWS Resources.

Sign in Using Your IAM User Credentials

To sign in as this new IAM user, sign out of the AWS Management Console, then use the following URL, where *your_aws_account_id* is your AWS account number without the hyphens (for example, if your AWS account number is `1234-5678-9012`, your AWS account ID is `123456789012`):

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

Enter the IAM user name and password that you just created. When you're signed in, the navigation bar displays "*your_user_name @ your_aws_account_id*".

If you don't want the URL for your sign-in page to contain your AWS account ID, you can create an account alias. From the IAM dashboard, choose **Customize** and enter an alias, such as your company name. To sign in after you create an account alias, use the following URL:

```
https://your_account_alias.signin.aws.amazon.com/console/
```

To verify the sign-in link for IAM users for your account, open the IAM console and check under **AWS Account Alias** on the dashboard.

Create Additional users

You can create additional users and grant them more restricted access to AWS using IAM policies. For more information, see Controlling Access to Amazon WorkSpaces Resources (p. 9).

Controlling Access to Amazon WorkSpaces Resources

By default, IAM users don't have permissions for Amazon WorkSpaces resources and operations. To allow IAM users to manage Amazon WorkSpaces resources, you must create an IAM policy that explicitly grants them permissions, and attach the policy to the IAM users or groups that require those permissions. For more information about IAM policies, see Permissions and Policies in the *IAM User Guide* guide.

Amazon WorkSpaces also creates an IAM role to allow the Amazon WorkSpaces service access to required resources.

For more information about IAM, see Identity and Access Management (IAM) and the IAM User Guide.

Example 1: Perform all Amazon WorkSpaces tasks

The following policy statement grants an IAM user permission to perform all Amazon WorkSpaces tasks, including creating and managing directories, as well as running the quick setup procedure.

Note that although Amazon WorkSpaces fully supports the `Action` and `Resource` elements when using the API and command-line tools, you must set them both to "*" in order to use the Amazon WorkSpaces console successfully.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workspaces:*",
        "ds:*",
        "iam:PassRole",
        "iam:GetRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "kms:ListAliases",
        "kms:ListKeys",
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:CreateNetworkInterface",
        "ec2:CreateInternetGateway",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateTags",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeRouteTables",
        "ec2:DescribeVpcs",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "workdocs:RegisterDirectory",
        "workdocs:DeregisterDirectory",
        "workdocs:AddUserToGroup",
        "workdocs:RemoveUserFromGroup"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Example 2: Perform WorkSpace-specific tasks

The following policy statement grants an IAM user permission to perform only WorkSpace-specific tasks, such as launching and removing WorkSpaces. These permissions do not allow the user to manage directories or run the quick setup procedure.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workspaces:*",
        "ds:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

To also grant the user the ability to enable Amazon WorkDocs for users within Amazon WorkSpaces, add the `workdocs` operations shown here:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "workdocs:RemoveUserFromGroup"
      ],
      "Effect": "Allow",
      "Resource": "*"
```

```
    }
  ]
}
```

To also grant the user the ability to use the Launch Workspaces wizard, add the `kms` operations shown here:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "workspaces:*",
        "ds:*",
        "workdocs:AddUserToGroup",
        "workdocs:RemoveUserFromGroup",
        "kms:ListAliases",
        "kms:ListKeys"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Specifying Amazon WorkSpaces Resources in an IAM Policy

To specify an Amazon WorkSpaces resource in the `Resource` element of the policy statement, you need to use the Amazon Resource Name (ARN) of the resource. You control access to your Amazon WorkSpaces resources by either allowing or denying permissions to use the API actions specified in the `Action` element of your IAM policy statement. Amazon WorkSpaces defines ARNs for WorkSpaces and bundles.

WorkSpace ARN

A WorkSpace ARN has the following syntax:

```
arn:aws:workspaces:region:account_id:workspace/workspace_identifier
```

`region`
The region that the WorkSpace is in.

`account_id`
The AWS account ID, with no hyphens, such as `123456789012`.

`workspace_identifier`
The identifier of the WorkSpace, such as `ws-0123456789`.

The following is the format of the **Resource** element of a policy statement that identifies a specific WorkSpace:

```
"Resource":"arn:aws:workspaces:region:account_id:workspace/
workspace_identifier"
```

You can use the * wildcard to specify all WorkSpaces that belong to a specific account in a specific region.

Bundle ARN

A bundle ARN has the following syntax:

```
arn:aws:workspaces:region:account_id:workspacebundle/bundle_identifier
```

region
: The region that the WorkSpace is in.

account_id
: The AWS account ID, with no hyphens, such as `123456789012`.

bundle_identifier
: The identifier of the WorkSpace bundle, such as `wsb-0123456789`.

The following is the format of the **Resource** element of a policy statement that identifies a specific bundle:

```
"Resource":"arn:aws:workspaces:region:account_id:workspacebundle/
bundle_identifier"
```

You can use the * wildcard to specify all bundles that belong to a specific account in a specific region.

Preparing Your Network

The following topics explain how to prepare your network to use Amazon WorkSpaces.

Topics

Client Ports

To connect to your WorkSpaces, the network that your Amazon WorkSpaces clients are connected to must have certain ports open to the IP address ranges for the various AWS services (grouped in subsets). These address ranges vary by AWS region. These same ports ports must also be open on any firewall that is running on the client. For more information about the AWS IP address ranges for different regions, see AWS IP Address Ranges in the *Amazon Web Services General Reference*.

Ports for Client Applications

The Amazon WorkSpaces client application requires outbound access on the following ports:

Port 4172 (UDP and TCP)
: This port is used for streaming of the WorkSpace desktop and user input. It must be open to all IP address ranges in the `EC2` subset in the region that the WorkSpace is in.

Port 443 (TCP)
: This port is used for client application updates, registration, and authentication. The desktop client applications support the use of a proxy server for port 443 (HTTPS) traffic. For more information, see Proxy Server - Windows (p. 96) and Proxy Server - OS X (p. 99). This port must be open to the following IP address ranges:
  - The `AMAZON` subset in the `GLOBAL` region.
  - The `AMAZON` subset in the region that the WorkSpace is in.

The Amazon WorkSpaces client application performs a network health check over port 4172. This validates whether TCP or UDP traffic streams from the client application to the Amazon WorkSpaces production servers. To do this successfully, firewall policies must take into account the following regional network health check servers.

Region	Network health check server
US East (N. Virginia)	drp-iad.amazonworkspaces.com
US West (Oregon)	drp-pdx.amazonworkspaces.com
EU (Ireland)	drp-dub.amazonworkspaces.com
EU (Frankfurt)	drp-fra.amazonworkspaces.com
Asia Pacific (Singapore)	drp-sin.amazonworkspaces.com
Asia Pacific (Sydney)	drp-syd.amazonworkspaces.com
Asia Pacific (Tokyo)	drp-nrt.amazonworkspaces.com

Ports for Web Access

Amazon WorkSpaces Web Access requires inbound and outbound access for the following ports:

Port 53 (UDP)
: This port is used to access DNS servers. It must be open to your DNS server IP addresses so that the client can resolve public domain names. This port requirement is optional if you are not using DNS servers for domain name resolution.

Port 80 (UDP and TCP)
: This port is used for general HTTP traffic. It must be open to all IP address ranges in the `EC2` subset in the region that the WorkSpace is in.

Port 443 (UDP and TCP)
: This port is used for registration and authentication using HTTPS. It must be open to all IP address ranges in the `EC2` subset in the region that the WorkSpace is in.

Typically, the web browser randomly selects a source port in the high range to use for streaming traffic. Amazon WorkSpaces Web Access does not have control over the port the browser selects. You must ensure that return traffic to this port is allowed.

Amazon WorkSpaces Web Access prefers UDP over TCP for desktop streams, but falls back to TCP if UDP is not available as follows:

- Amazon WorkSpaces Web Access will work on Chrome even if all UDP ports are blocked except 53, 80, and 443, using TCP connections.
- Amazon WorkSpaces Web Access will not work on Firefox if all UDP ports are blocked except 53, 80, and 443. Additional UDP ports must be open to enable streaming.

Whitelisted Domains and Ports

For the Amazon WorkSpaces client application to be able to access the Amazon WorkSpaces service, the following domains and ports must be whitelisted on the network from which the client is trying to access the service.

Whitelisted domains and ports

Category	Whitelisted
Session Broker (PCM)	Domains: • https://skylight-cm.us-east-1.amazonaws.com • https://skylight-cm.us-west-2.amazonaws.com • https://skylight-cm.eu-west-1.amazonaws.com • https://skylight-cm.eu-central-1.amazonaws.com • https://skylight-cm.ap-southeast-1.amazonaws.com • https://skylight-cm.ap-southeast-2.amazonaws.com • https://skylight-cm.ap-northeast-1.amazonaws.com
PCoIP Session Gateway (PSG)	PCoIP Gateway IP Ranges (p. 3)
PCoIP Healthcheck (DRP)	TCP:4172 and UDP:4172 on these domains: • drp-iad.amazonworkspaces.com • drp-pdx.amazonworkspaces.com • drp-dub.amazonworkspaces.com • drp-fra.amazonworkspaces.com • drp-sin.amazonworkspaces.com • drp-syd.amazonworkspaces.com • drp-nrt.amazonworkspaces.com
Device Metrics	https://device-metrics-us-2.amazon.com/
Forrester Log Service	https://fls-na.amazon.com/
Directory Settings	Customer directory settings: • https://d21ui22avrxoh6.cloudfront.net/prod/<region>/<directory name> Login page graphics for customer directory level co-branding: • https://d1cbg795sa4g1u.cloudfront.net/prod/<region>/<directory name> CSS file to style the login pages: • https://workspaces-client-css.s3.amazonaws.com

Category	Whitelisted
Client Auto-update	https://d2td7dqidlhjx7.cloudfront.net/
Registration Dependency	https://s3.amazonaws.com
Connectivity Check	https://connectivity.amazonworkspaces.com/
User Login Pages	https://<directory id>.awsapps.com/ (where <directory id> is the customer's domain)
Web client	Outbound security group rules: • TCP:8443 • TCP:9997 • UDP:4172 • UDP:3478 Inbound security group rules: • TCP:4489
Web Access TURN Servers	Servers: • turn:*.us-east-1.rdn.amazonaws.com • turn:*.us-west-2.rdn.amazonaws.com • turn:*.eu-west-1.rdn.amazonaws.com • turn:*.eu-central-1.rdn.amazonaws.com • turn:*.ap-southeast-1.rdn.amazonaws.com • turn:*.ap-southeast-2.rdn.amazonaws.com • turn:*.ap-northeast-1.rdn.amazonaws.com

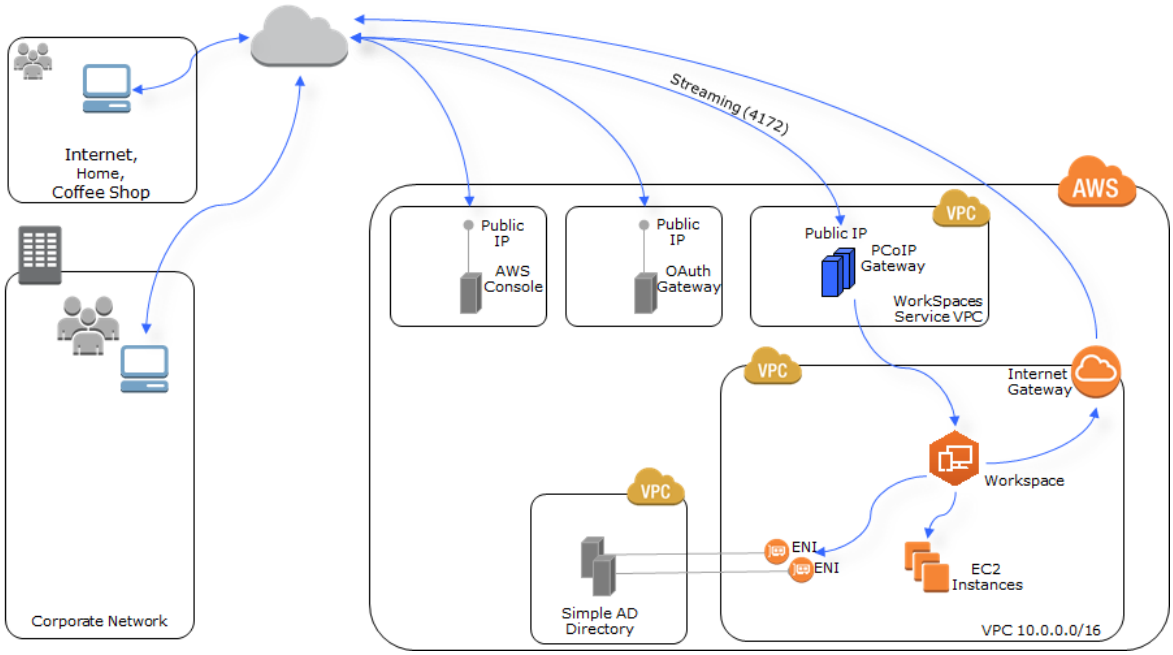
Preparing Your Network for a Simple AD Directory

Amazon WorkSpaces uses an AWS Directory Service Simple AD directory to store user and WorkSpace information in the cloud. The following topics explain how to prepare your network to set up a Simple AD directory in the cloud.

Topics

Architecture

The following diagram shows the basic architecture for Amazon WorkSpaces with a Simple AD directory.



Requirements

To create a Simple AD directory, you must meet the prerequisites identified in Prerequisites in the *AWS Directory Service Administration Guide*.

For a tutorial that explains how to set up a VPC for use with Amazon WorkSpaces, see Step 1: Create and Configure Your VPC (p. 79).

Simple AD Directory Internet Access

The WorkSpaces that you launch in a Simple AD directory cannot communicate with the Internet by default. You must use one of the following methods to provide Internet access to your WorkSpaces.

Topics

Simple AD Directory Public IP Addresses

Attach an Internet gateway to the VPC used by the directory and assign a public IP address to each WorkSpace. To assign a public IP address to your WorkSpaces, you can either manually assign an Elastic IP address to the network interface for each WorkSpace after it is created, or you can have Amazon WorkSpaces automatically assign a public IP address to each WorkSpace that is provisioned or rebuilt. For more information about automatically assigning public IP addresses in a Simple AD directory, see Internet Access (p. 43).

Topics

Internet Gateway and Routing

To setup an Internet gateway and subnet routing, perform the following steps:

1. If your VPC does not already have an Internet gateway, create an Internet gateway and attach it to the VPC used by the directory. For more information, see Adding an Internet Gateway to Your VPC in the Amazon VPC User Guide.
2. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 4).
3. Modify the route table for both WorkSpaces subnets to route all non-VPC traffic to the Internet gateway.

   WorkSpaces Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Internet gateway

Assigning an Elastic IP Address to a WorkSpace

The following procedure explains how to manually assign an Elastic IP address to the network interface of a WorkSpace.

You can have Amazon WorkSpaces automatically assign a public IP address to each WorkSpace that is provisioned or rebuilt. For more information, see Internet Access (Simple AD) (p. 43) or Internet Access (AD Connector) (p. 46).

To assign an Elastic IP address to a WorkSpace

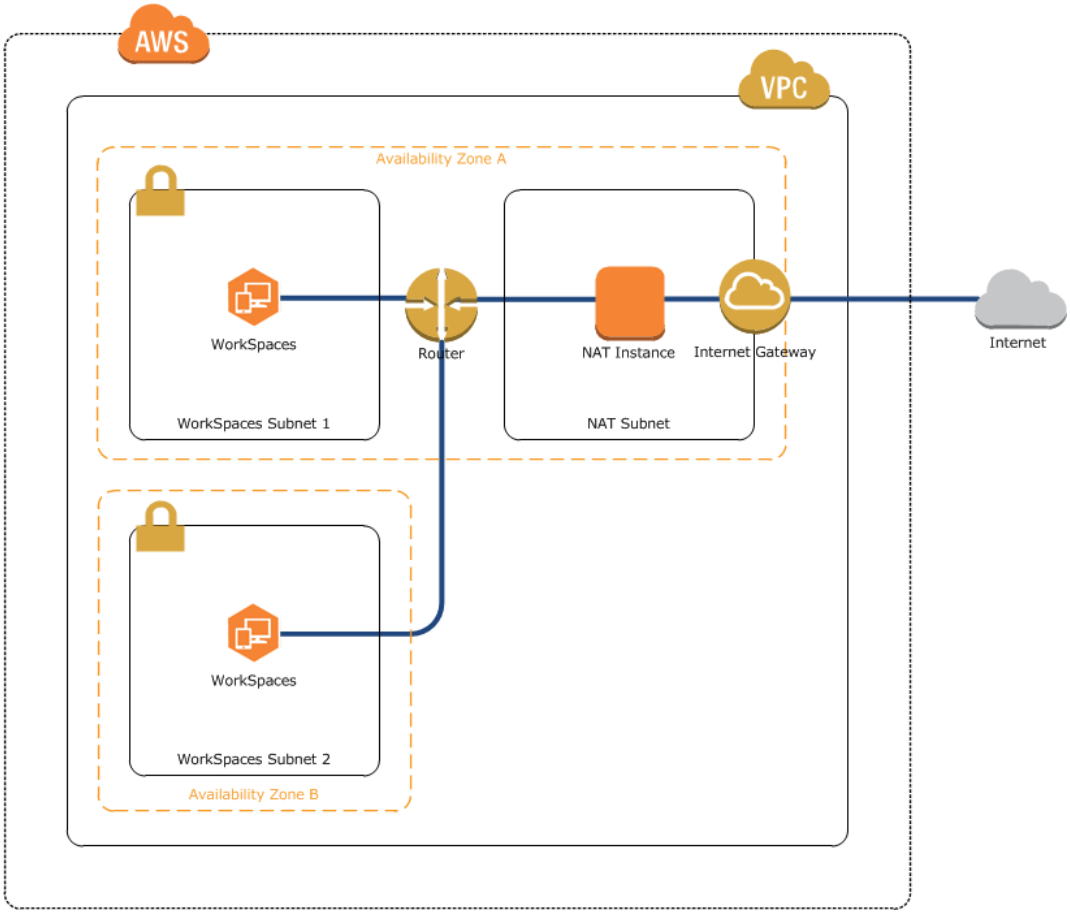
1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**, select the WorkSpace you want to apply the Elastic IP address to, and choose the right arrow button to display the details for the WorkSpace. Make a note of the **WorkSpace IP** value.
3. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
4. In the navigation pane, choose **Elastic IPs** and either select an unused VPC address or allocate a new address for VPC.
5. Select the address, choose **Associate Address**, and enter the WorkSpace IP value found in step 2 in the **Network Interface** field. The identifier of the elastic network interface (ENI) that is assigned to that IP address is displayed in the search list. This is the ENI of the WorkSpace. Select the ENI identifier. The WorkSpace IP will be displayed in the **Private IP Address** field.
6. Choose **Reassociation** so that the Elastic IP address can be reassigned later if needed, and choose **Associate**.
7. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 4).
8. The WorkSpace now has access to the Internet. Repeat this process for each existing WorkSpace.

Simple AD Directory NAT Gateway

Implement a network address translation (NAT) gateway in a public subnet (a subnet that has an Internet gateway attached to it) in the VPC used by the directory. The NAT gateway must be in a

separate subnet from your WorkSpaces. This allows all of your WorkSpaces to access the Internet. For more information about this procedure, see NAT Gateways in the *Amazon VPC User Guide*.

To set up a NAT gateway and give your WorkSpaces Internet access, perform the following steps. This example procedure assumes you have an existing VPC with two private subnets for your WorkSpaces. When completed, your VPC will look something like the following.



To set up a NAT gateway

1. Create an Internet gateway and attach it to the VPC.
2. Create a separate subnet for the NAT gateway and create the NAT gateway in this subnet. The NAT gateway must have an Elastic IP address.
3. Modify the route table that is assigned to the subnet containing the NAT gateway to route all non-VPC traffic to the Internet gateway.

   NAT Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Internet gateway

4. Create a route table that routes all non-VPC traffic to the NAT gateway and assign this route table to both WorkSpaces subnets. The route table will look like the following.

WorkSpaces Subnets Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	NAT gateway

5. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 4).
6. Your WorkSpaces now have access to the Internet. Connect to a WorkSpace and verify that you can connect to the Internet with a web browser.

   Note
   Alternatively, you can create a NAT instance in your public subnet; however, a single NAT instance creates a single point of failure. We recommend that you use a NAT gateway.

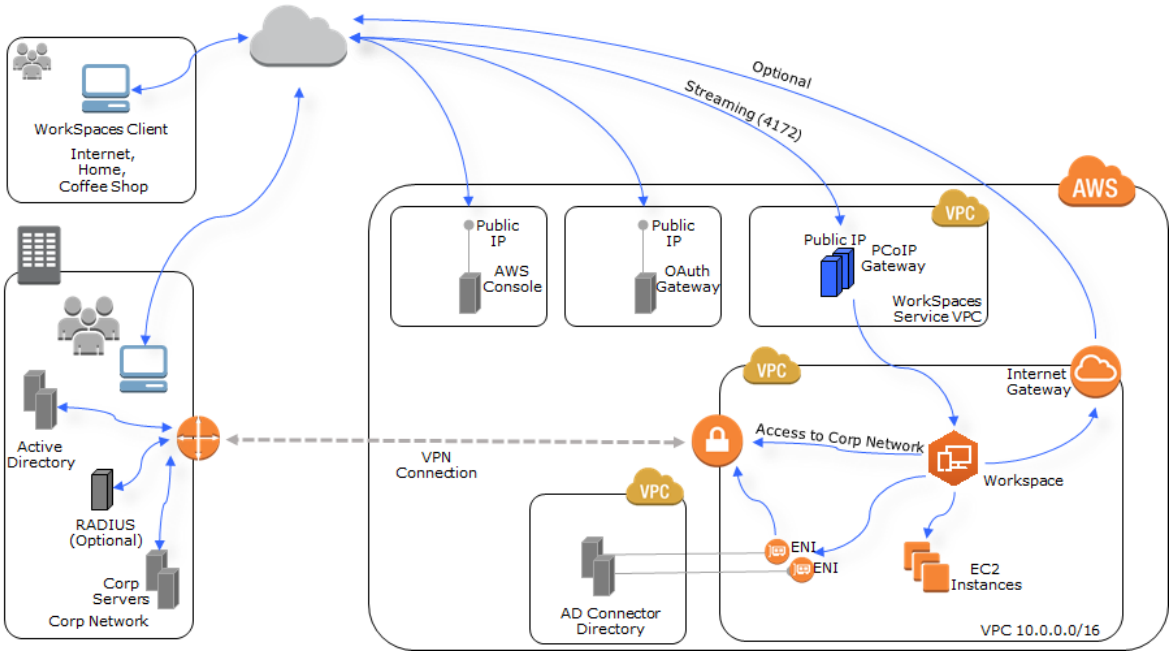
Preparing Your Network for an AD Connector Directory

Amazon WorkSpaces uses an AWS Directory Service AD Connector directory to connect to your on-premises directory. The following topics explain how to prepare to connect Amazon WorkSpaces to your on-premises directory.

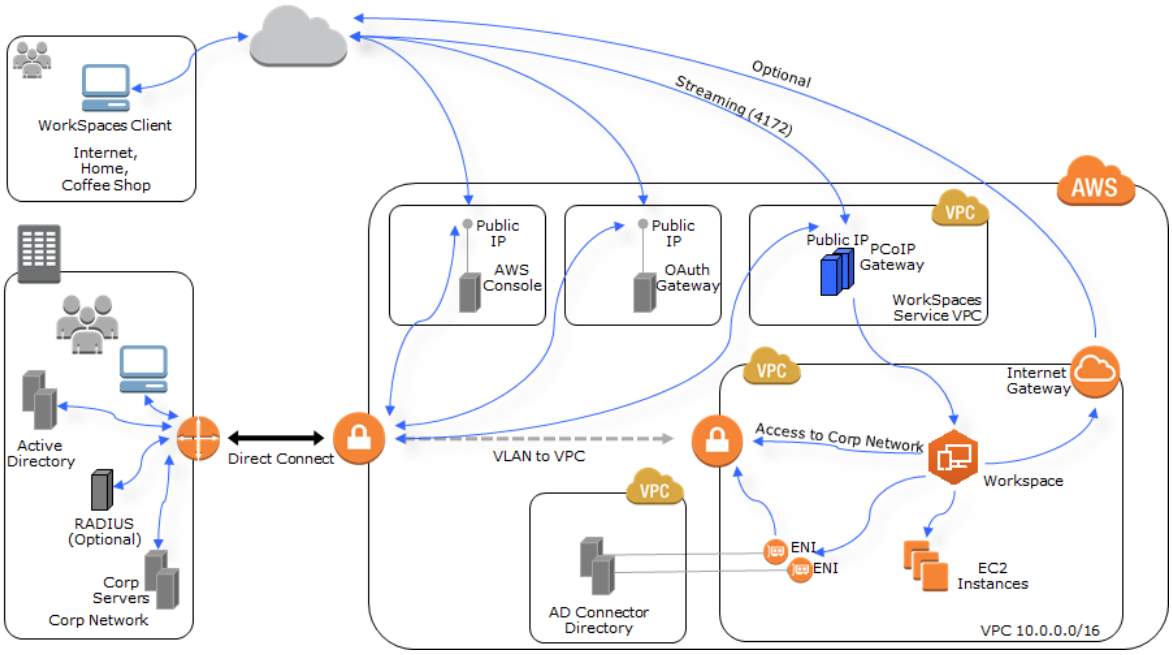
Topics

Architecture

The following is the basic system architecture of Amazon WorkSpaces when using an AD Connector directory and a VPN.



The following is the basic system architecture of Amazon WorkSpaces when using an AD Connector directory and AWS Direct Connect.



Requirements

To use AD Connector to connect to your on-premises directory, you must meet the prerequisites identified in Prerequisites in the *AWS Directory Service Administration Guide*.

In addition, you need the following:

- For Amazon WorkSpaces to communicate with your on-premises directory, the firewall for your on-premises network must have the following ports open to the CIDRs for both subnets in the VPC:
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos authentication
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP 1024-65535 - Dynamic ports for RPC

To test if these criteria are met, before connecting to your on-premises directory, see Connect Verification (p. 26).

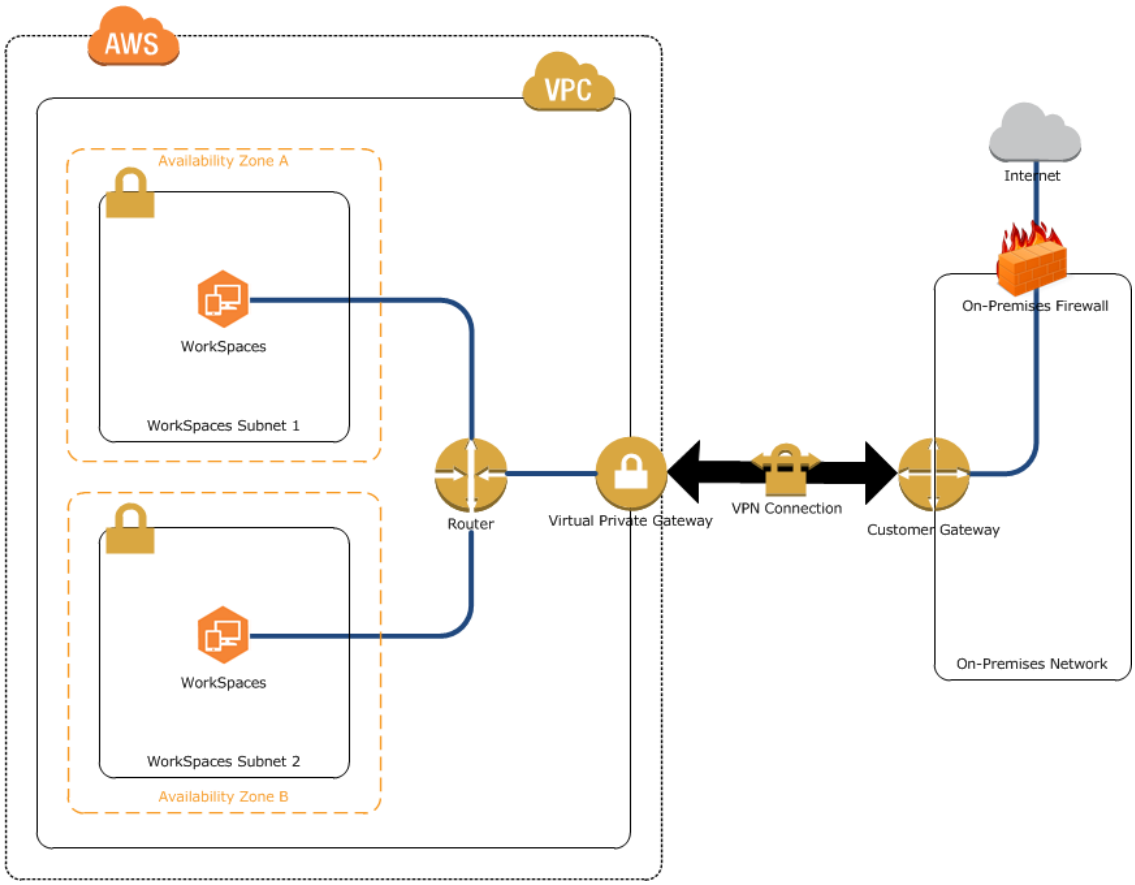
AD Connector Directory Internet Access

The WorkSpaces that you launch in an AD Connector directory cannot communicate with the Internet by default. You must use one of the following methods to provide Internet access to your WorkSpaces.

Topics

On-Premises Firewall

Give the WorkSpaces access to your on-premises network's Internet firewall. You need to adjust the route tables to give the subnets access to your firewall.



AD Connector Directory Public IP Addresses

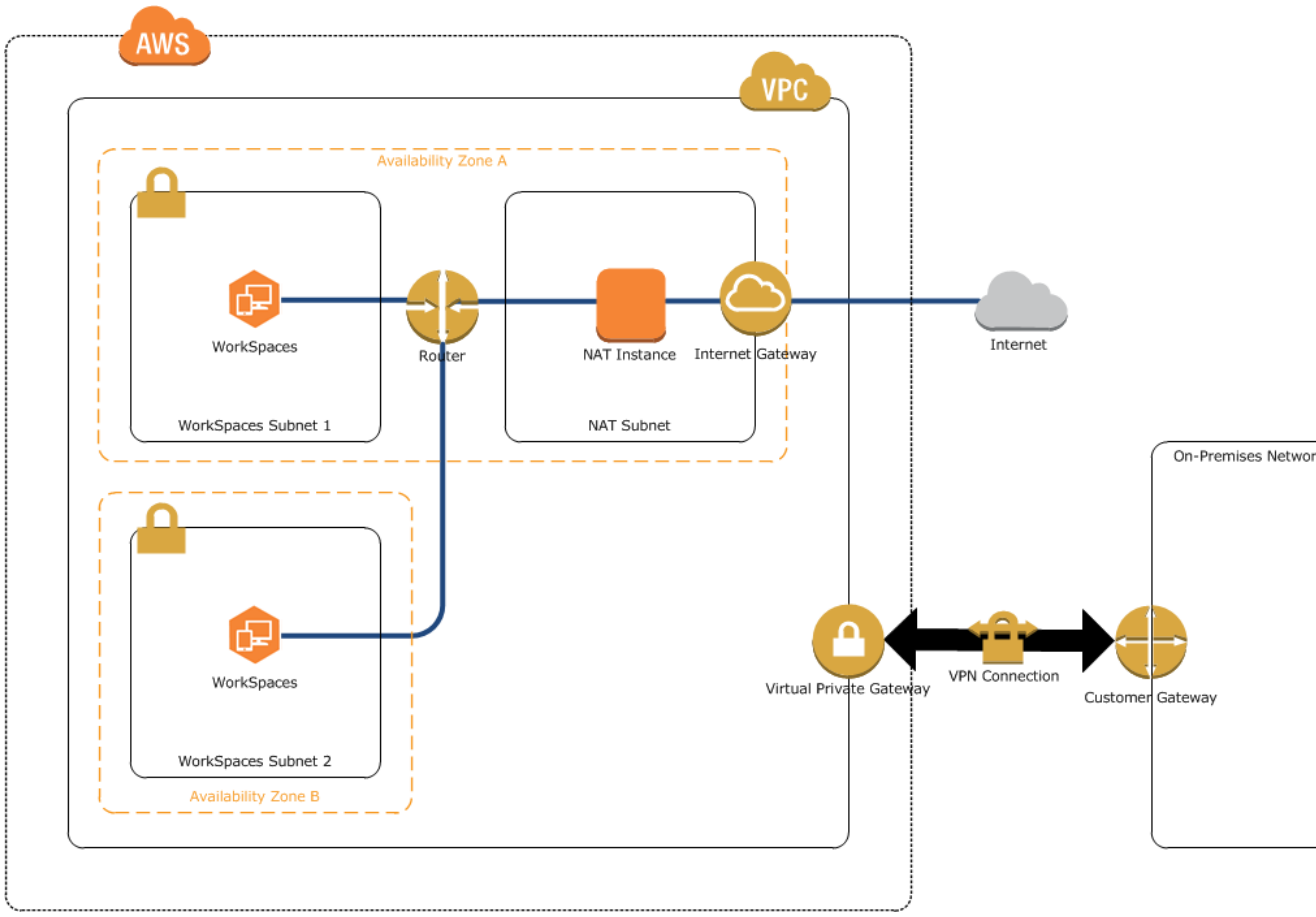
To assign a public IP address to your WorkSpaces, you can either manually assign an Elastic IP address to the network interface for each WorkSpace after it is created, or you can have Amazon WorkSpaces automatically assign a public IP address to any WorkSpaces that are provisioned or rebuilt. For more information about automatically assigning public IP addresses in an AD Connector directory, see Internet Access (p. 46).

For more information about how to set up an Internet gateway and assign Elastic IP addresses to your WorkSpaces, see Simple AD Directory Public IP Addresses (p. 16).

AD Connector Directory NAT Gateway

Implement a network address translation (NAT) gateway in a public subnet (a subnet that has an Internet gateway attached to it) in the VPC used by the directory. This allows all of your WorkSpaces access to the Internet. For more information about this procedure, see NAT Gateways in the *Amazon VPC User Guide*.

For more information about how to set up a NAT gateway to give your WorkSpaces Internet access, see Simple AD Directory NAT Gateway (p. 17). When completed, your VPC will look something like the following



To set up a NAT gateway

1. Create an Internet gateway and attach it to the VPC.
2. Create a separate subnet for the NAT gateway and create the NAT gateway in this subnet. The NAT gateway must have an Elastic IP address.
3. Modify the route table that is assigned to the subnet containing the NAT gateway to route all non-VPC traffic to the Internet gateway.

   NAT Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Internet gateway

4. Create a route table that routes all non-VPC traffic to the NAT gateway and assign this route table to both WorkSpaces subnets. The route table will look like the following.

   WorkSpaces Subnets Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	NAT gateway

5. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 4).
6. Your WorkSpaces now have access to the Internet. Connect to a WorkSpace and verify that you can connect to the Internet with a web browser.

   Note
   Alternatively, you can create a NAT instance in your public subnet; however, a single NAT instance creates a single point of failure. We recommend that you use a NAT gateway.

Multi-factor Authentication Prerequisites

To support multi-factor authentication with your AD Connector directory, you need the following:

- A Remote Authentication Dial In User Service (RADIUS) server in your on-premises network that has two client endpoints. The RADIUS client endpoints have the following requirements:
  - To create the endpoints, you need the IP addresses of the AD Connector servers. These IP addresses can be obtained from the **Directory IP Address** field of your Amazon WorkSpaces directory details.
  - Both RADIUS endpoints must use the same shared secret code.
- Your on-premises network must allow inbound traffic over the default RADIUS server port (1812) from the AD Connector servers.
- The usernames between your RADIUS server and your on-premises directory must be identical.

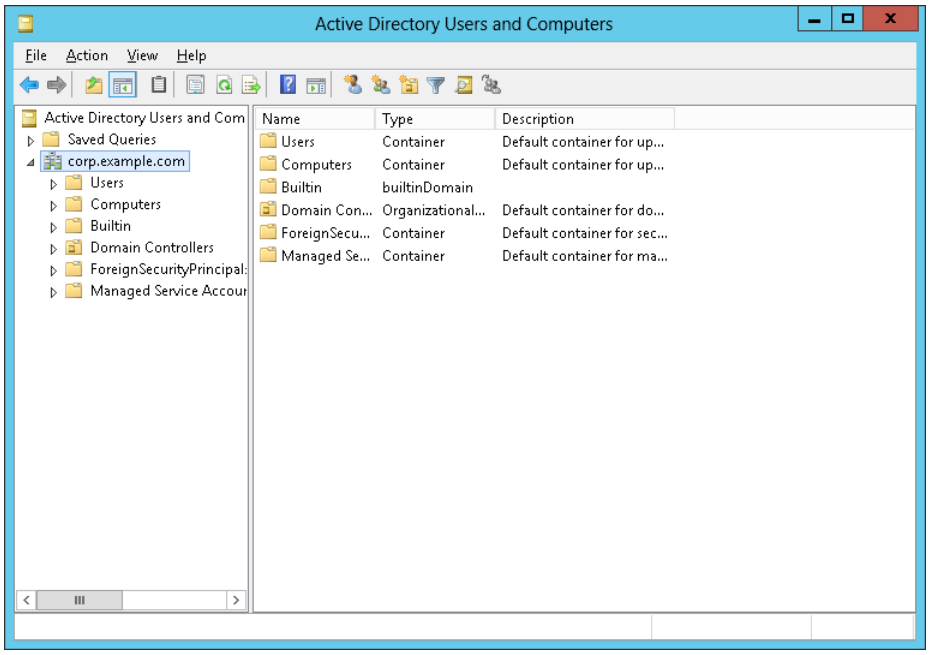
For more information about enabling multi-factor authentication with your AD Connector directory, see Multi-factor Authentication (p. 47).

Delegating Connect Privileges

For AD Connector to connect to your on-premises directory, you must have the credentials for an account in the on-premises directory that has certain privileges. While members of the **Domain Admins** group have sufficient privileges to connect to the directory, as a best practice, you should use an account that only has the minimum privileges necessary to connect to the directory. The following procedure demonstrates how to create a new group called `WorkSpaces_Connectors`, and delegate the privileges to this group that are needed to connect Amazon WorkSpaces to the directory.

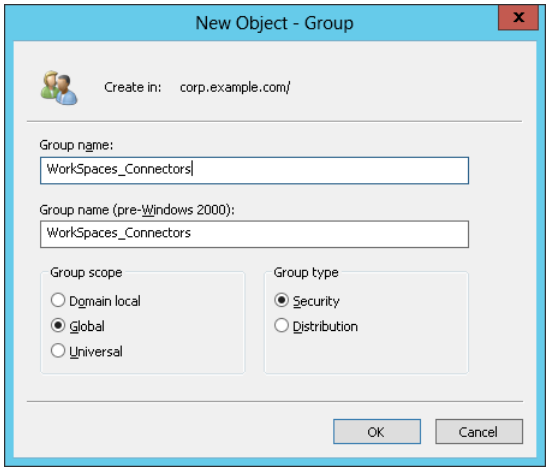
This procedure must be performed on a machine that is joined to your directory and has the **Active Directory User and Computers** MMC snap-in installed. You must also be logged in as a domain administrator.

1. Open **Active Directory User and Computers** and select your domain root in the navigation tree.

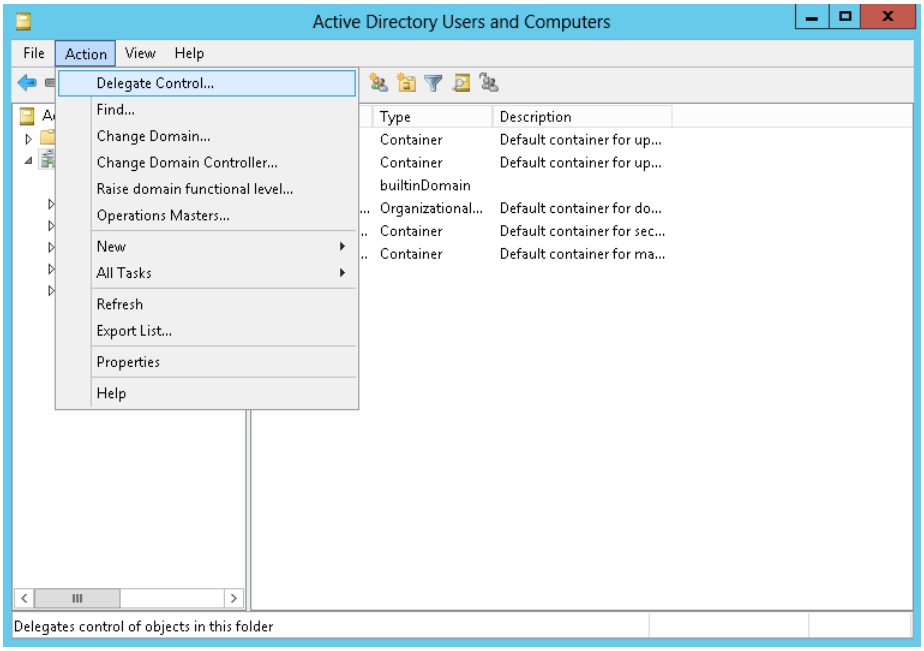


2. In the list in the left-hand pane, open the context (right-click) menu for **Users**, and choose **New**, **Group**.
3. In the **New Object - Group** dialog box, enter the following values and choose **OK**:

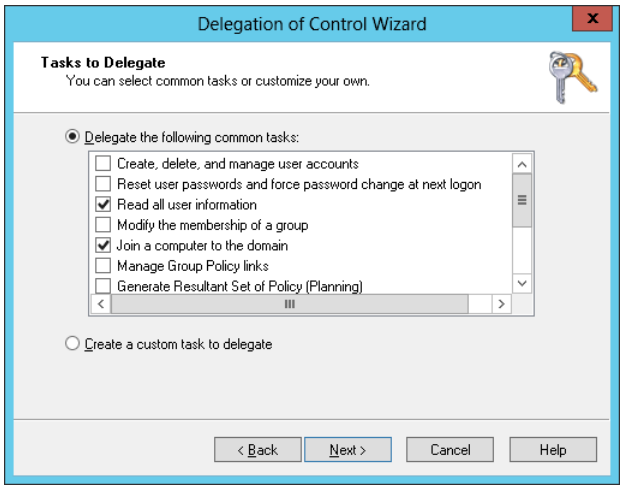
Field	Value/Selection
Group name	`WorkSpaces_Connectors`
Group scope	**Global**
Group type	**Security**



4. In the **Active Directory User and Computers** navigation tree, select your domain root. In the menu, choose **Action**, **Delegate Control**.



5. On the **Delegation of Control Wizard** page, choose **Next**, **Add**.
6. In the **Select Users, Computers, or Groups** dialog box, enter `WorkSpaces_Connectors` and choose **OK**. If more than one object is found, select the `WorkSpaces_Connectors` group created above. Choose **Next**.
7. On the **Tasks to Delegate** page, choose only **Read all user information** and **Join a computer to the domain**, then choose **Next**.



8. Verify the information on the **Completing the Delegation of Control Wizard** page, and choose **Finish**.
9. Create a user with a strong password and add that user to the `WorkSpaces_Connectors` group. The user will have sufficient privileges to connect Amazon WorkSpaces to the directory.

Connect Verification

For AD Connector to connect to your on-premises directory, the firewall for your on-premises network must have certain ports open to the CIDRs for both subnets in the VPC. To test if these conditions are

met, perform the following steps. For more information, see Connect Verification in the *AWS Directory Service Administration Guide*.

To verify the connection

1. Launch a Windows instance in the VPC and connect to it over RDP. The remaining steps are performed on the VPC instance.
2. Download and unzip the DirectoryServicePortTest test application. The source code and Visual Studio project files are included so you can modify the test application if desired.
3. From a Windows command prompt, run the **DirectoryServicePortTest** test application with the following options:

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
 "53,88,135,389,445,3268,5722,9389" -udp "53,88,123,138,389,445"
```

<domain_name>
: The fully qualified domain name. This is used to test the forest and domain functional levels. If you exclude the domain name, the functional levels won't be tested.

<server_IP_address>
: The IP address of a domain controller in your on-premises domain. The ports will be tested against this IP address. If you exclude the IP address, the ports won't be tested.

This will determine if the necessary ports are open from the VPC to your domain. The test app also verifies the minimum forest and domain functional levels.

The output will be similar to the following:

```
Testing forest functional level.
Forest Functional Level = Windows2008R2Forest : PASSED

Testing domain functional level.
Domain Functional Level = Windows2008R2Domain : PASSED

Testing required TCP ports to <server_IP_address>:
Checking TCP port 53: PASSED
...

Testing required UDP ports to <server_IP_address>:
Checking UDP port 53: PASSED
...
```

Preparing Your Network for a Microsoft AD Directory

Amazon WorkSpaces uses a Microsoft AD directory to store user and WorkSpace information in the cloud. The following topics explain how to prepare your network to set up a Microsoft AD directory in the cloud.

Topics

Requirements

To create a Microsoft AD directory, you must meet the prerequisites identified in Prerequisites in the *AWS Directory Service Administration Guide*.

For a tutorial that explains how to set up a VPC for use with Amazon WorkSpaces, see Step 1: Create and Configure Your VPC (p. 79).

Microsoft AD Directory Internet Access

The WorkSpaces that you launch in a Microsoft AD directory cannot communicate with the Internet by default. You must use one of the following methods to provide Internet access to your WorkSpaces.

Topics

Microsoft AD Directory Public IP Addresses

Attach an Internet gateway to the VPC used by the directory and assign a public IP address to each WorkSpace. To assign a public IP address to your WorkSpaces, you can either manually assign an Elastic IP address to the network interface for each WorkSpace after it is created, or you can have Amazon WorkSpaces automatically assign a public IP address to each WorkSpace that is provisioned or rebuilt. For more information about automatically assigning public IP addresses in a Microsoft AD directory, see Internet Access (p. 43).

Topics

Internet Gateway and Routing

To set up an Internet gateway and subnet routing, perform the following steps.

To set up an Internet gateway and subnet routing

1. If your VPC does not already have an Internet gateway, create an Internet gateway and attach it to the VPC used by the directory. For more information, see Adding an Internet Gateway to Your VPC in the *Amazon VPC User Guide*.
2. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 4).
3. Modify the route table for both WorkSpaces subnets to route all non-VPC traffic to the Internet gateway.

   WorkSpaces Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Internet gateway

Assigning an Elastic IP Address to a WorkSpace

The following procedure explains how to manually assign an Elastic IP address to the network interface of a WorkSpace.

You can have Amazon WorkSpaces automatically assign a public IP address to each WorkSpace that is provisioned or rebuilt. For more information, see Internet Access (Simple AD) (p. 43) or Internet Access (AD Connector) (p. 46).

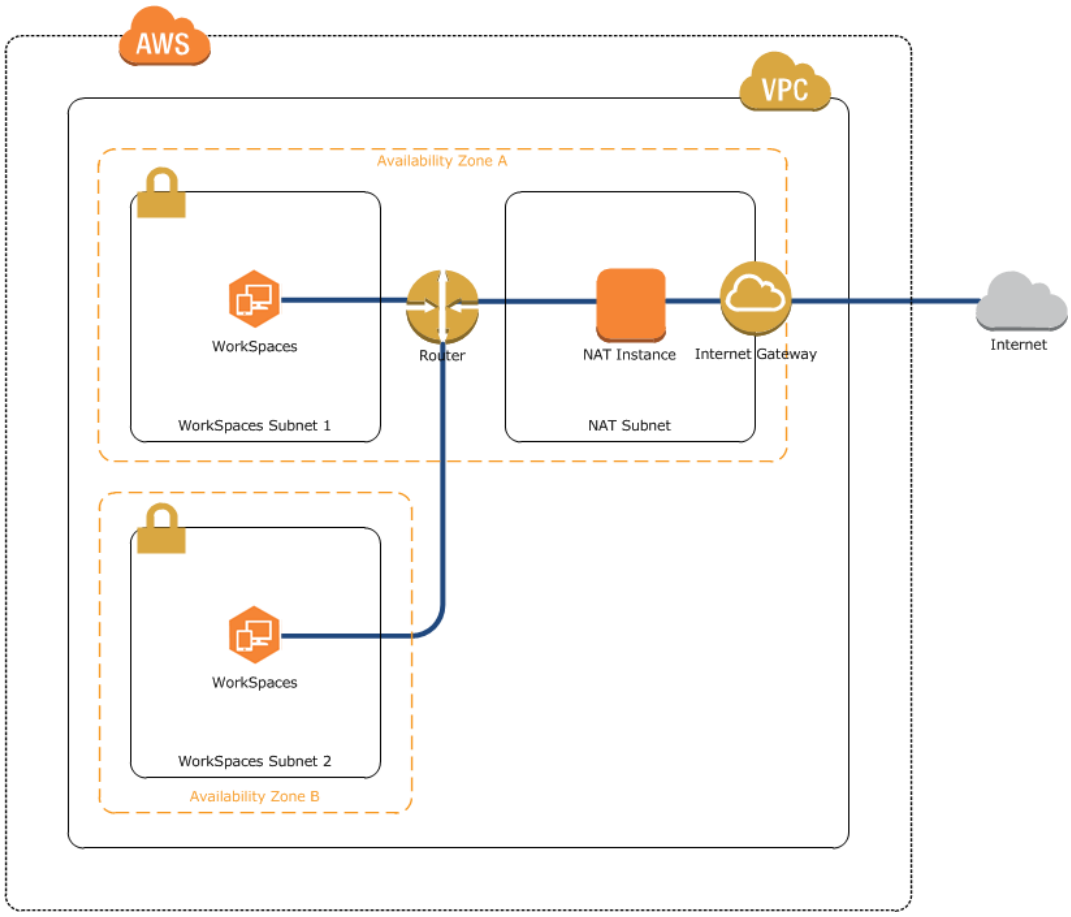
To assign an Elastic IP address to a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**, select the WorkSpace to apply the Elastic IP address to, and choose the right arrow button to display the details for the WorkSpace. Make a note of the **WorkSpace IP** value.
3. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
4. In the navigation pane, choose **Elastic IPs** and either select an unused VPC address or allocate a new address for VPC.
5. Select the address, choose **Associate Address**, and enter the WorkSpace IP value found in step 2 in the **Network Interface** field. The identifier of the elastic network interface (ENI) that is assigned to that IP address is displayed in the search list. This is the ENI of the WorkSpace. Select the ENI identifier. The WorkSpace IP is displayed in the **Private IP Address** field.
6. Choose **Reassociation** so that the Elastic IP address can be reassigned later if needed, and choose **Associate**.
7. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 4).
8. The WorkSpace now has access to the Internet. Repeat this process for each existing WorkSpace.

Microsoft AD Directory NAT Gateway

Implement a network address translation (NAT) gateway in a public subnet (a subnet that has an Internet gateway attached to it) in the VPC used by the directory. The NAT gateway must be in a separate subnet from your WorkSpaces. This allows all of your WorkSpaces to access the Internet. For more information about this procedure, see NAT Gateways in the *Amazon VPC User Guide*.

To set up a NAT gateway and give your WorkSpaces Internet access, perform the following steps. This example procedure assumes you have an existing VPC with two private subnets for your WorkSpaces. When completed, your VPC will look something like the following diagram:



To set up a NAT gateway

1. Create an Internet gateway and attach it to the VPC.
2. Create a separate subnet for the NAT gateway and launch the NAT gateway in this subnet. The NAT gateway must have an Elastic IP address.
3. Modify the route table that is assigned to the subnet containing the NAT gateway to route all non-VPC traffic to the Internet gateway.

   NAT Subnet Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	Internet gateway

4. Create a route table that routes all non-VPC traffic to the NAT gateway and assign this route table to both WorkSpaces subnets. The route table will look like the following.

   WorkSpaces Subnets Route Table

Destination	Target
VPC CIDR	local
0.0.0.0/0	NAT gateway

5. Make sure the security group for your WorkSpaces allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to all destinations (0.0.0.0/0). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 4).
6. Your WorkSpaces now have access to the Internet. Connect to a WorkSpace and verify that you can connect to the Internet with a web browser.

A single NAT instance creates a single point of failure. For high availability, you should create multiple NAT instances in different Availability Zones. For more information, see the article High Availability for Amazon VPC NAT Instances: An Example.

Note
Alternatively, you can create a NAT instance in your public subnet; however, a single NAT instance creates a single point of failure. We recommend that you use a NAT gateway.

Getting Started with Amazon WorkSpaces

Amazon WorkSpaces provides you with two ways to get started. There is a quick start procedure (p. 32) that you can use to quickly get up and running with Amazon WorkSpaces using a Simple AD directory. The quick start procedure is intended to be used for evaluation of the service. After you have completed the quick start procedure in a specific region, you cannot run it again. For more information, see Amazon WorkSpaces Quick Start (p. 32).

The second method is more advanced and provides you with more control over the creation of your directory. For more information, see Advanced Setup (p. 37).

Topics

Amazon WorkSpaces Quick Start

The quick start procedure enables you to get up and running with Amazon WorkSpaces quickly and easily.

Topics

Prerequisites

To use the Amazon WorkSpaces quick start procedure, you must meet the following prerequisites.

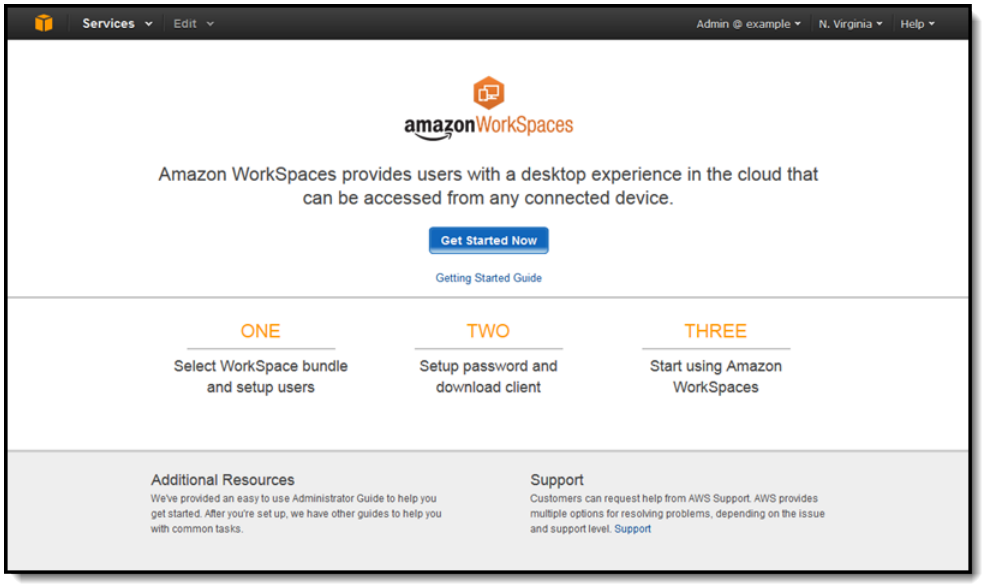
AWS Account
To use Amazon WorkSpaces, you must have an AWS account. For more information, see Create an AWS Account (p. 7).

Amazon WorkSpaces Client Prerequisites
To access your WorkSpace with one of the Amazon WorkSpaces client applications, you must meet the requirements identified in Amazon WorkSpaces Client Prerequisites (p. 94).

Get Started

Open the Amazon WorkSpaces console for your desired region, sign in with your AWS credentials, and choose **Get Started Now**.

If you're not sure which region to choose, the Connection Health Check website can recommend the best region for you. Recommendations are based on several factors, including port connectivity, connection speeds, and the ability of your device to connect to Amazon WorkSpaces services.



Choose Setup Type

Amazon WorkSpaces uses a network directory to store its user and WorkSpace information. Choose the type of Amazon WorkSpaces directory setup you want to use.

The **Quick Setup** procedure allows you to get you up and running with Amazon WorkSpaces quickly and easily. Amazon WorkSpaces creates and sets up a directory in the cloud that requires minimal management.

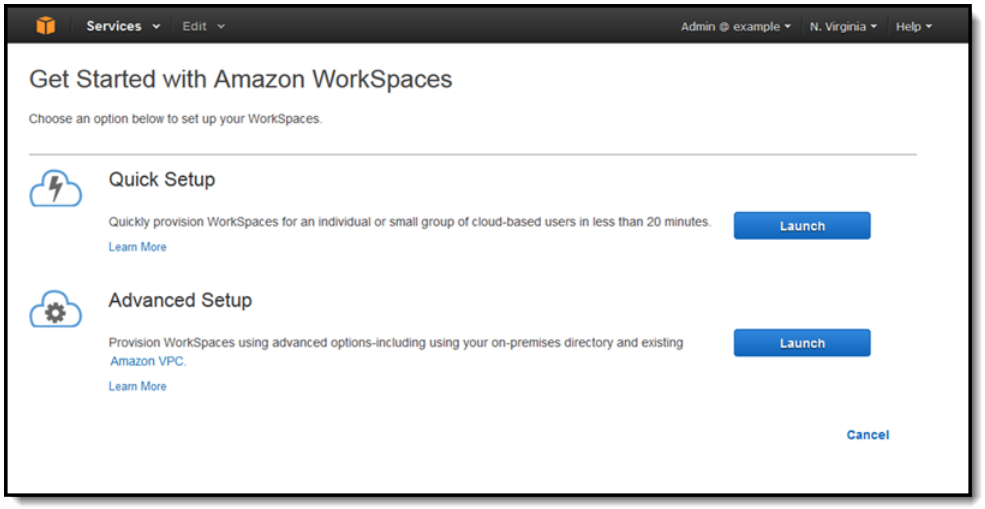
Note
Quick Setup is not supported in the EU (Frankfurt) region.

The **Advanced Setup** procedure allows you to have more control over the setup of your Amazon WorkSpaces directory. The directory can either be in the cloud, or connected to your on-premises directory.

Choose one of the following options:

- To use the quick setup, choose **Launch Quick Setup** and see Quick Setup (p. 34).

- To use advanced setup, choose **Launch Advanced Setup** and see Advanced Setup (p. 37).



Quick Setup

The Quick Setup procedure allows you to get you up and running with Amazon WorkSpaces quickly and easily. Amazon WorkSpaces creates and sets up a directory in the cloud that requires minimal management.

Note
Quick Setup is not supported in the EU (Frankfurt) region.

Quick Setup Prerequisites

This procedure creates a virtual private cloud (VPC) on your behalf. Because of this, your AWS account must have at least one VPC available to be created in the region within which you are creating WorkSpaces. Within this VPC, Amazon WorkSpaces must also create an Internet gateway, so your AWS account must have at least one Internet gateway available to be created in the region within which you are creating WorkSpaces.

For more information about VPCs, see What is Amazon VPC? in the *Amazon VPC User Guide*.

For more information about Internet gateways, see Adding an Internet Gateway to Your VPC in the *Amazon VPC User Guide*.

Select a WorkSpace Bundle and Create Users

Before you can launch a WorkSpace, you must select a WorkSpace bundle and and provide information about your users.

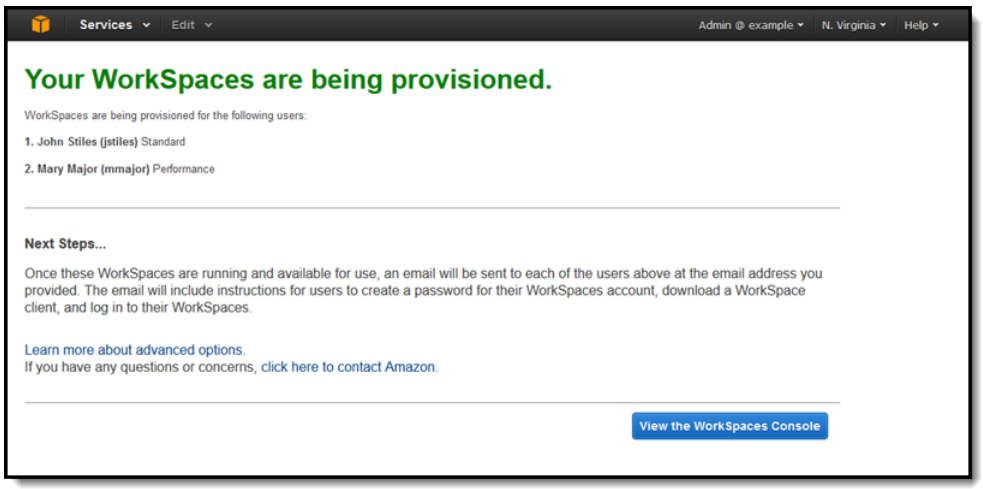
To configure a WorkSpace

1. For **Available WorkSpace Bundles**, select the desired WorkSpace bundle. If multiple operating system languages are available in your region, you can also select your desired operating system language. For more information, see Amazon WorkSpaces Bundles.
2. For **Enter User Details**, provide the requested information for each WorkSpace user. The first user entered is made the Amazon WorkSpaces administrator, and will have administrator privileges.
3. To add more users, choose **Create Additional Users**, and provide the information for the user. After you have provided the user information for all users, choose **Launch WorkSpaces**.

For more information about what Amazon WorkSpaces does during the quick start procedure, see Quick Setup Details (p. 37).

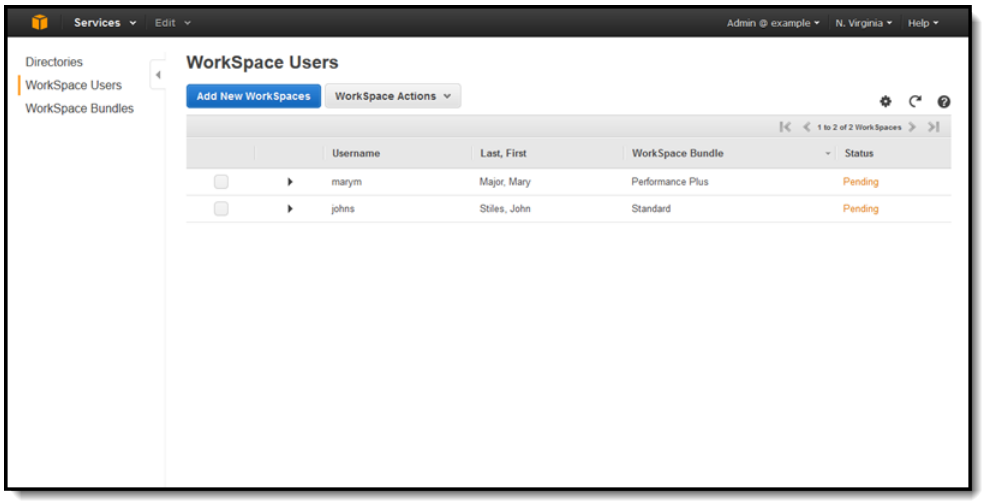
Launching WorkSpaces

It takes several minutes for the Amazon WorkSpaces infrastructure to be created and the WorkSpaces to be launched. You can monitor the status of the WorkSpaces by choosing **View the WorkSpaces Console**.



Monitor WorkSpace Status

While the WorkSpaces are being launched, you can monitor the status in the **WorkSpaces** sections of the Amazon WorkSpaces console. The WorkSpaces start in the "Pending" state and change to the "Running" state when the launch is complete.



WorkSpaces are Ready

When the WorkSpaces are ready for use, a welcome email is sent to each of the users. The welcome email contains instructions for the user to create their account, download and install a Amazon WorkSpaces client, and log in to their WorkSpace. The text of the email will be similar to the following:

```
Greetings,

A new Amazon WorkSpace has been provided for you. Follow the steps below to
 quickly get up and running with your WorkSpace:

1. Complete your user profile and download a WorkSpace client using the
 following link: link_to_registration.

2. Launch the client and enter the following registration
 code: registration_code.

3. Log in with your newly created password. Your username is username.

If you have any issues connecting to your WorkSpace, please contact your
 administrator.

You may download clients for additional devices at http://
clients.amazonworkspaces.com/

Sincerely,

Amazon WorkSpaces
```

User Registration

The user must first complete their profile by going to the registration link provided in the email. The user must complete their registration within seven days of the email being sent; otherwise, the invitation expires and you must send another invitation.

The username and email address cannot be changed, but the user can change their first name and last name. The user must also set their password for the account. The password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must also contain at least one character from three of the following categories:

- Lowercase characters (a-z)
- Uppercase characters (A-Z)
- Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Download the Client

Your users can download their client applications at any time from the Amazon WorkSpaces Client Downloads page.

Client Application Registration

The registration code included in the invitation email is used on first login only, and enables the client application to connect to the correct Amazon WorkSpaces directory. If the client application needs to be re-registered for any reason, choose **Manage Registrations** from the menu.

The client application automatically saves the last 10 valid registration codes entered. To quickly retrieve a previous registration code, choose **Saved registrations**, select the saved registration code belonging to the WorkSpace to access, and enter the login information for that WorkSpace. You can use the same code to access a WorkSpace in a different region or directory. To delete a saved

registration, choose **X** next to the registration code. To return to this page at any time, choose **Manage Registrations** from the menu of the client application.

Note
This information is saved locally, and is not persistent across devices.

Client Sign In

After the client application is registered, the user is taken to the sign in page. Here, the user enters their Amazon WorkSpaces username and the password they entered when they completed their user profile (p. 36). After the user signs in, the client application connects to their WorkSpace and displays the WorkSpace desktop.

Quick Setup Details

When you run the Amazon WorkSpaces quick setup procedure, Amazon WorkSpaces performs the following tasks on your behalf:

- Creates an IAM role to allow the Amazon WorkSpaces service to create elastic network interfaces and list your Amazon WorkSpaces directories. This role has the name `workspaces_DefaultRole`.
- Creates a virtual private cloud (VPC) under your account.

  Caution
  Unless otherwise instructed, do not modify any of the security groups, gateways, or other settings for this VPC. If you do, you run the risk of making your Amazon WorkSpaces environment inoperable.
- Sets up a Simple AD directory within the VPC that is used to store user and WorkSpace information.
- Creates a directory administrator account.
- Creates the specified user accounts and adds them to the directory.
- Creates the WorkSpace instances.
- Each WorkSpace created during quick setup receives a public IP address to provide them with Internet access. If you later create more WorkSpaces, you will need to provide them with Internet access. For more information, see Simple AD Directory Internet Access (p. 16).
- Sends invitation emails to the specified users.

Advanced Setup

Amazon WorkSpaces uses an AWS Directory Service directory to store its user and WorkSpace account information. This can be a Microsoft AD directory, Simple AD directory, or AD Connector directory. You can enable Amazon WorkSpaces to work with an existing directory, or you can have Amazon WorkSpaces create a directory for you.

Choose one of the following options:

- To enable Amazon WorkSpaces to work with an existing AWS Directory Service directory, see Registering With a Directory (p. 41).
- To enable Amazon WorkSpaces to work with an AWS Directory Service for Microsoft AD, see Preparing Your Network for a Microsoft AD Directory (p. 27).
- To create a directory in the cloud, see Create an Amazon WorkSpaces Directory in the Cloud (p. 38) to learn how to create a Simple AD directory in the cloud.
- To connect to your on-premises directory, see Connect Amazon WorkSpaces to Your Directory (p. 39) to learn how to use AD Connector to connect to your directory.
- For a step-by-step tutorial that describes all of the steps necessary to manually create and configure a new VPC, Simple AD directory, and a WorkSpace, see Tutorial: Creating a Simple AD Directory (p. 78).

Topics

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 AD.

Creating a Simple AD or Microsoft AD Directory

You can create a Simple AD directory or Microsoft AD directory by using two different service consoles:

- AWS Directory Service
- Amazon WorkSpaces

Topics

Create the Directory with the AWS Directory Service Console

To create a Simple AD directory or Microsoft AD directory by using the AWS Directory Service console, perform the following steps.

To create a Simple AD directory or Microsoft AD directory

1. Open the AWS Directory Service console.
2. Follow the steps in Create Your Directory in the *AWS Directory Service Administration Guide*.

Create the Directory with the Amazon WorkSpaces Console

To create a Simple AD directory or Microsoft AD directory using the Amazon WorkSpaces console, perform the following steps.

To create a Simple AD directory or Microsoft AD directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**, **Set up Directory**.
3. Follow the steps in Create Your Directory in the *AWS Directory Service Administration Guide*.

Simple AD and Microsoft AD Directory Setup Details

When you create a Simple AD or Microsoft AD directory, Amazon WorkSpaces performs the following tasks on your behalf:

- Creates an IAM role to allow the Amazon WorkSpaces service to create elastic network interfaces and list your Amazon WorkSpaces directories. This role has the name `workspaces_DefaultRole`.

- Sets up a directory within the VPC that is used to store user and WorkSpace information.
- Creates a directory administrator account with the user name `Administrator` (Simple AD) or `Admin` (Microsoft AD) and the specified password. You use this account to manage your directory.
- Creates two security groups, one for the directory controllers and another for the WorkSpaces in the directory.

Connect Amazon WorkSpaces to Your Directory

Amazon WorkSpaces uses a network directory to store and manage WorkSpace and user information. You can use AD Connector to connect Amazon WorkSpaces to your on-premises directory, which allows your users to sign into their WorkSpace using their on-premises credentials. It also gives them access, from their WorkSpace, to the same on-premises resources that they have access to locally.

You can connect to your directory by using two different service consoles:

- AWS Directory Service
- Amazon WorkSpaces

Connecting to Your Directory Using the AWS Directory Service Console

To use AD Connector to connect to your on-premises directory in the AWS Directory Service console, perform the following steps.

To connect to a directory

1. Open the AWS Directory Service console.
2. Follow the steps in Create Your Directory in the *AWS Directory Service Administration Guide*.

Connecting to Your Directory Using the Amazon WorkSpaces Console

To use AD Connector to connect to your on-premises directory in the Amazon WorkSpaces console, perform the following steps.

To connect to a directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**, **Set up Directory**
3. Follow the steps in Create Your Directory in the *AWS Directory Service Administration Guide*.

Amazon WorkSpaces Management

Amazon WorkSpaces is a fully-managed desktop computing service in the cloud. Amazon WorkSpaces allows customers to launch cloud-based desktops that allow end-users to access the documents, applications, and resources they need with the device of their choice, including laptops, iPads, Kindle Fire, or Android tablets. For more information, see Amazon WorkSpaces.

Amazon WorkSpaces uses a network directory to store its user and WorkSpace information. This directory can either be a directory in the cloud, or connected to your on-premises directory.

In a cloud directory, the user and WorkSpace information is stored in a standalone directory that resides in one of your VPCs. WorkSpace users exist solely within this directory and are not linked to any external entities. Amazon WorkSpaces sets up this directory for you when you create a cloud directory. You should use a cloud directory if you do not already have an on-premises directory, or if your users do not need access to any on-premises resources. For more information, see Create an Amazon WorkSpaces Directory in the Cloud (p. 38).

In a connected directory, user and WorkSpace information is stored in your on-premises directory. WorkSpace users are selected from the users that already exist within your on-premises directory. The WorkSpaces that you create are represented as machine accounts within your directory. You should use a connected directory if your users need access to any on-premises resources. For more information, see Connect Amazon WorkSpaces to Your Directory (p. 39).

No matter which type of directory you use, you are responsible for providing Internet access to the WorkSpaces. More detailed information about how to provide this is given in specific topics.

Because Amazon WorkSpaces uses a directory that is compatible with Active Directory to store its user and WorkSpace information, you can use whichever Active Directory tools you are familiar with to administrate these objects. You can easily set up a directory management WorkSpace within Amazon WorkSpaces to perform these operations from. For more information, see Set Up a Directory Administration WorkSpace (p. 65). As an alternative, you can join a Windows EC2 instance to this directory and install the Active Directory Administration Tools on the instance. For more information about joining a Windows instance to a directory, see Joining an Amazon EC2 Instance to a Directory (p. 66). For more information about installing the Active Directory Administration Tools on either a WorkSpace or instance, see Installing the Active Directory Administration Tools (p. 66).

Topics

Amazon WorkSpaces Console

After your directory is created, you use the Amazon WorkSpaces console to perform certain functions, such as launching WorkSpaces or deleting your directory.

Topics

Directory Management

You use the Amazon WorkSpaces management console to perform certain directory-related actions, such as creating a new directory or deleting an existing directory. After a directory is created, most administrative functions are performed with directory management tools, such as the Active Directory Administration Tools. For more information, see Amazon WorkSpaces Directory Administration (p. 65).

Topics

Registration

Amazon WorkSpaces allows you to use an existing AWS Directory Service directory to store your Amazon WorkSpaces users and resources. The **Directories** list displays all of your AWS Directory Service directories in the current region, and indicates if Amazon WorkSpaces is registered with each directory.

Topics

Registering With a Directory

To allow Amazon WorkSpaces to use an existing AWS Directory Service directory, you must register Amazon WorkSpaces with the directory.

To register with a directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.

2. In the navigation pane, choose **Getting Started**, **Advanced Setup**, **Create Simple AD**, and **Directories**.
3. Select the directory to register with and choose **Actions**, **Register**.
4. In the **Register directory** dialog box, select whether you want Amazon WorkDocs to be registered with the directory, and choose **Register**.

   Note
   This option is only presented if Amazon WorkDocs is available in the selected region.

   After the service is registered with the directory, you can launch WorkSpaces for the users in the directory.

Deregistering From a Directory

You can also deregister Amazon WorkSpaces from a directory so that it can no longer be used with the service. You must deregister the service from a directory before you can delete the directory. If you have any Amazon WAM applications assigned to your users, you must also remove all of those assignments before you can delete a directory. For more information, see Removing All Application Assignments in the *Amazon WAM Administration Guide*.

To deregister Amazon WorkSpaces from a directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select a directory and choose **Actions**, **Deregister**.
4. In the **Deregister directory** dialog box, verify that you want to deregister the service from the directory, and choose **Deregister**.

Managing A Simple AD Directory

The following topics explain the different management actions you can perform on a Simple AD directory.

Topics

Update Simple AD Directory Information

You can use the Amazon WorkSpaces console to change the following settings for a Simple AD directory:

Contents

Default Organizational Unit

The default organizational unit is the organizational unit that the WorkSpace machine accounts are placed in. If this is not set, the WorkSpaces machine accounts are placed in the Computers

organizational unit. You can either select an organizational unit from the current WorkSpaces directory, or specify an organizational unit in a separate target domain.

To select an organizational unit

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Target Domain and Organizational Unit** section.
5. Enter all or part of the desired organizational unit name and choose **Search OU**. Alternatively, you can search for all organizational units by choosing **List all OU**.
6. Select the desired organizational unit and choose **Update**. The machine accounts for all WorkSpaces that are created or rebuilt after this setting is changed are placed in the selected organizational unit.

Add a Security Group

Amazon WorkSpaces creates a security group that is assigned to all WorkSpaces in the directory. You have the option to have an additional security group applied to your WorkSpaces when they are created or rebuilt by performing the following steps.

To add a security group

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Security Group** section.
5. To create a new security group, choose **Create New**.
6. Select the desired security group and choose **Update**. All WorkSpaces that are created or rebuilt after this setting is changed include the specified security group.

Internet Access

You can have Amazon WorkSpaces assign a public IP address to all WorkSpaces that are provisioned or rebuilt.

To enable public IP addresses

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, then choose **Actions**, **Update Details**.
4. Expand **Internet Access**.
5. To have Amazon WorkSpaces assign a public IP address to every WorkSpace that is created or rebuilt, choose **Enable**. Otherwise, choose **Disable**. When you have completed your selection, choose **Update**.

This setting only applies to WorkSpaces that are provisioned or rebuilt after the setting is enabled. If you need to have a public IP address applied to an existing WorkSpace, you must either rebuild the WorkSpace, or manually assign an Elastic IP address to the WorkSpace. For more information about rebuilding a WorkSpace, see Rebuild a WorkSpace (p. 58). For more information about assigning an Elastic IP address to an existing WorkSpace, see Assigning an Elastic IP Address to a WorkSpace (p. 17).

Local Administrator Setting

You can choose whether your users are local administrators on their WorkSpaces. Users are local administrators by default, which enables them to install applications and modify settings on their WorkSpaces.

To set local administrator permissions

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand the **Local Administrator Setting** section.
5. To set users as local administrators, choose **Enable**. Otherwise, choose **Disable**.
6. Choose **Update**. This setting applies to all WorkSpaces that are created or rebuilt after this setting is changed.

Maintenance Mode

Enable maintenance mode to ensure that WorkSpaces configured as AutoStop are updated automatically. These WorkSpaces will be started once every month to download and install important service, security, and Windows updates. If you manage updates to your WorkSpaces on a regular basis, you can disable maintenance mode.

To set maintenance mode

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand the **Maintenance Mode** section.
5. To enable maintenance on your AutoStop WorkSpaces, choose **Enabled**. Otherwise, choose **Disabled**.
6. Choose **Update**.

Deleting a Simple AD Directory

Before you can delete a Simple AD directory, you must first remove all WorkSpaces from the directory. For more information about removing WorkSpaces, see Remove a WorkSpace (p. 58). To delete a cloud directory, perform the following steps.

To delete a directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory to delete and choose **Actions**, **Deregister**.
4. Verify the information in the **Deregister Directory** dialog box, and choose **Deregister**.
5. Select the directory to delete and choose **Actions**, **Delete**.
6. Verify the information in the **Delete Directory** dialog box, and choose **Delete**.

Managing an AD Connector Directory

When connecting Amazon WorkSpaces to your on-premises directory, you direct Amazon WorkSpaces to use your on-premises directory as a source of identities for users who will be using the WorkSpaces.

Topics

Update the Connected Directory Information

You can use the Amazon WorkSpaces console to change the following settings for a connected directory:

Topics

Target Domain and Default Organizational Unit

The default organizational unit is the organizational unit that your WorkSpace machine accounts are placed in. If this is not set, your WorkSpaces machine accounts are placed in the Computers organizational unit of the directory that your AD Connector directory is connected to. You can either select an organizational unit from the connected directory, or specify an organizational unit in a separate target domain. If you require more than one organizational unit for your WorkSpaces machine accounts, you have to create a separate AD Connector directory for each organizational unit.

The target domain is the directory that your WorkSpace machine accounts are created in. This allows you to use separate user and resource directories for your WorkSpaces. If a target domain is not specified, your WorkSpace machine accounts are created in the directory that your AD Connector directory is connected to. The following are the requirements for the target domain:

- The target domain must either be a child of the directory that your AD Connector directory is connected to, or, at a minimum, have a one-way trust with this directory.
- The DNS servers for your AD Connector directory must be able to resolve the fully-qualified distinguished name of the target domain.
- The same connectivity and firewall requirements that exist between your VPC and your on-premises directory must also exist between your VPC and the target domain. For more information, see Requirements (p. 20).
- The service account for your AD Connector directory must have the following privileges in the target domain:
  - Create computer objects
  - Join computers to the domain

To select an organizational unit

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Target Domain and Organizational Unit** section.
5. Enter all or part of the desired organizational unit name and choose **Search OU**. Alternatively, you can search for all organizational units by choosing **List all OU**.

6. Select the desired organizational unit and choose **Update**. The machine accounts for all WorkSpaces that are created or rebuilt after this setting is changed are placed in the selected organizational unit.

To specify a target domain and organizational unit

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Target Domain and Organizational Unit** section.
5. Enter the full LDAP distinguished name for the target domain and organizational unit in the **Selected OU** field, for example `OU=WorkSpaces_machines,DC=machines,DC=example,DC=com`, and choose **Update**. The machine accounts for all WorkSpaces that are created or rebuilt after this setting is changed are created in the specified domain and organizational unit.

Add a Security Group

Amazon WorkSpaces creates a security group that is assigned to all WorkSpaces in the directory. You have the option to have an additional security group applied to your WorkSpaces when they are created or rebuilt by performing the following steps.

To add a security group

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Security Group** section.
5. To create a new security group, choose **Create New**.
6. Select the desired security group and choose **Update**. All WorkSpaces that are created or rebuilt after this setting is changed include the specified security group.

Internet Access

You can have Amazon WorkSpaces assign a public IP address to all WorkSpaces that are provisioned or rebuilt.

To enable public IP addresses

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, then choose **Actions**, **Update Details**.
4. Expand **Internet Access**.
5. To have Amazon WorkSpaces assign a public IP address to every WorkSpace that is created or rebuilt, choose **Enable**. Otherwise, choose **Disable**. When you have completed your selection, choose **Update**.

This setting only applies to WorkSpaces that are provisioned or rebuilt after the setting is enabled. If you need to have a public IP address applied to an existing WorkSpace, you must either rebuild the WorkSpace, or manually assign an Elastic IP address to the WorkSpace. For more information about rebuilding a WorkSpace, see Rebuild a WorkSpace (p. 58). For more information about

assigning an Elastic IP address to an existing WorkSpace, see Assigning an Elastic IP Address to a WorkSpace (p. 17).

Maintenance Mode

Enable maintenance mode to ensure that WorkSpaces configured as AutoStop are updated automatically. These WorkSpaces will be started once every month to download and install important service, security, and Windows updates. If you manage updates to your WorkSpaces on a regular basis, you can disable maintenance mode.

To set maintenance mode

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand the **Maintenance Mode** section.
5. To enable maintenance on your AutoStop WorkSpaces, choose **Enabled**. Otherwise, choose **Disabled**.
6. Choose **Update**.

Update the WorkSpaces Connect Account

The WorkSpaces Connect account is the account that is used to read users and groups, and create Amazon WorkSpaces machine accounts in your directory. For more information about this account, see the Requirements (p. 20) section.

To update the WorkSpaces Connect account

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Update WorkSpaces Connect Account** section.
5. Enter the new service account username and password and choose **Update**. The new account is used to access your on-premises directory.

Multi-factor Authentication

You can enable multi-factor authentication for your AD Connector directory by performing the following procedure. For more information about using multi-factor authentication with Amazon WorkSpaces, see Multi-factor Authentication Prerequisites (p. 24).

To enable multi-factor authentication

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Multi-Factor Authentication** section.
5. Enter the following values and choose **Update** or **Update and Exit**.

   Enable Multi-Factor Authentication
   Check to enable multi-factor authentication.

   RADIUS server IP address(es)
   The IP addresses of your RADIUS server endpoints, or the IP address of your RADIUS server load balancer. You can enter multiple IP addresses by separating them with a comma (e.g., `192.0.0.0,192.0.0.12`).

Port
The port that your RADIUS server is using for communications. Your on-premises network must allow inbound traffic over the default RADIUS server port (1812) from the AD Connector servers.

Shared secret code
The shared secret code that was specified when your RADIUS endpoints were created.

Confirm shared secret code
Confirm the shared secret code for your RADIUS endpoints.

Protocol
Select the protocol that was specified when your RADIUS endpoints were created.

Server timeout
The amount of time, in seconds, to wait for the RADIUS server to respond. This must be a value between 1 and 20.

Max retries
The number of times that communication with the RADIUS server is attempted. This must be a value between 0 and 10.

Multi-factor authentication is available when the **RADIUS Status** changes to **Enabled**. During the time that the multi-factor authentication is being set up, your users will not be able to log in to their WorkSpaces.

Disconnecting a Directory

Before you can disconnect from your directory, you must first remove all WorkSpaces from the directory. For more information about removing WorkSpaces, see Remove a WorkSpace (p. 58).

To disconnect from your directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory to disconnect and choose **Directory Actions**, **Deregister**.
4. Verify the information in the **Deregister Directory** dialog box, and choose **Deregister**.
5. Select the directory to disconnect and choose **Actions**, **Delete**.
6. Verify the information in the **Delete Directory** dialog box, and choose **Delete**.

Managing a Microsoft AD Directory

The following topics explain the different management actions you can perform on a Microsoft AD directory.

Topics

Update Microsoft AD Directory Information

You can use the Amazon WorkSpaces console to change the following settings for a Microsoft AD directory:

Contents

Default Organizational Unit

The default organizational unit is the organizational unit that the WorkSpace machine accounts are placed in. If this is not set, the WorkSpaces machine accounts are placed in the Computers organizational unit. You can either select an organizational unit from the current WorkSpaces directory, or specify an organizational unit in a separate target domain.

To select an organizational unit

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Target Domain and Organizational Unit** section.
5. Enter all or part of the desired organizational unit name and choose **Search OU**. Alternatively, you can search for all organizational units by choosing **List all OU**.
6. Select the desired organizational unit and choose **Update**. The machine accounts for all WorkSpaces that are created or rebuilt after this setting is changed are placed in the selected organizational unit.

Add a Security Group

Amazon WorkSpaces creates a security group that is assigned to all WorkSpaces in the directory. You have the option to have an additional security group applied to your WorkSpaces when they are created or rebuilt, by performing the following steps.

To add a security group

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose**Directories**.
3. Select your directory and choose **Actions**, **Update Details**.
4. Expand the **Security Group** section.
5. To create a new security group, choose **Create New**.
6. Select the desired security group and choose **Update**. All WorkSpaces that are created or rebuilt after this setting is changed include the specified security group.

Internet Access

You can have Amazon WorkSpaces assign a public IP address to all WorkSpaces that are provisioned or rebuilt.

To enable public IP addresses

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, then choose **Actions**, **Update Details**.
4. Expand **Internet Access**.
5. To have Amazon WorkSpaces assign a public IP address to every WorkSpace that is created or rebuilt, choose **Enable**. Otherwise, choose **Disable**. When you have completed your selection, choose **Update**.

This setting only applies to WorkSpaces that are provisioned or rebuilt after the setting is enabled. If you need to have a public IP address applied to an existing WorkSpace, you must either rebuild the WorkSpace, or manually assign an Elastic IP address to the WorkSpace. For more information about rebuilding a WorkSpace, see Rebuild a WorkSpace (p. 58). For more information about assigning an Elastic IP address to an existing WorkSpace, see Assigning an Elastic IP Address to a WorkSpace (p. 17).

Local Administrator Setting

You can choose whether your users are local administrators on their WorkSpaces. Users are local administrators by default, which enables them to install applications and modify settings on their WorkSpaces.

To set local administrator permissions

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand the **Local Administrator Setting** section.
5. To set users as local administrators, choose **Enable**. Otherwise, choose **Disable**.
6. Choose **Update**. This setting applies to all WorkSpaces that are created or rebuilt after this setting is changed.

Maintenance Mode

Enable maintenance mode to ensure that WorkSpaces configured as AutoStop are updated automatically. These WorkSpaces will be started once every month to download and install important service, security, and Windows updates. If you manage updates to your WorkSpaces on a regular basis, you can disable maintenance mode.

To set maintenance mode

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select your directory, and choose **Actions**, **Update Details**.
4. Expand the **Maintenance Mode** section.
5. To enable maintenance on your AutoStop WorkSpaces, choose **Enabled**. Otherwise, choose **Disabled**.
6. Choose **Update**.

Deleting a Microsoft AD Directory

Before you can delete a Microsoft AD directory, you must first remove all WorkSpaces from the directory. For more information about removing WorkSpaces, see Remove a WorkSpace (p. 58). To delete a cloud directory, perform the following steps.

To delete a directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories**.
3. Select the directory to delete and choose **Actions**, **Deregister**.
4. Verify the information in the **Deregister Directory** dialog box, and choose **Deregister**.

5. Select the directory to delete and choose **Actions**, **Delete**.
6. Verify the information in the **Delete Directory** dialog box and choose **Delete**.

WorkSpace Management

In Amazon WorkSpaces, each WorkSpace is assigned to a single user. Therefore, whenever you launch a new WorkSpace, you must assign that WorkSpace to a user that does not already have a WorkSpace. WorkSpaces are only available to a single user and cannot be shared between separate users.

As an Amazon WorkSpaces administrator, you use the Amazon WorkSpaces console to perform the following tasks to manage users and WorkSpaces.

Topics

Launching a WorkSpace

How you launch a WorkSpace varies depending on the type of directory you have:

- To launch a WorkSpace in a cloud directory, see Launching WorkSpaces in a Cloud Directory (p. 51).
- To launch a WorkSpace in a connected directory, see Launching WorkSpaces in a Connected Directory (p. 52).

Launching WorkSpaces in a Cloud Directory

With an Amazon WorkSpaces cloud directory, you use Amazon WorkSpaces to create users that can access your WorkSpaces.

To launch a WorkSpace for a user

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**, **Launch WorkSpaces**.
3. For **Select a Directory**, select your cloud directory. This is the directory from which users are selected.

   If this is the first time you have launched a WorkSpace in this directory, you can enable or disable the Amazon WorkDocs service for all users in the directory. For more information about Amazon

WorkDocs, see Amazon WorkDocs Sync Client Help in the *Amazon WorkDocs Administration Guide*. Make your choice and choose **Next**.

Note
This option is only presented if Amazon WorkDocs is available in the selected region.

4. Select the users for which to launch a WorkSpace. You can search for all or part of the user's name, or use the wildcard character (*) to extend the search. You can also choose **Show All Users**. If a user does not have an email address, you will not be able to launch a WorkSpace for that user.

   When you have selected the desired users, choose **Add Selected**. The selected users are added to the **WorkSpaces** list.

   If you want to create a new user, enter the information for the new user. If you want to create another user, choose **Create Additional Users** and enter the information for the additional user. Repeat this process for all new users and choose **Create Users**. The new users are added to the **WorkSpaces** list.

   Repeat this step until you have selected or created all of the desired users, then choose **Next**.
5. Select the default WorkSpace bundle to be used for the WorkSpaces. If multiple operating system languages are available in your region, you can also select your desired operating system language. You can customize these settings for individual WorkSpaces in the **Assign WorkSpace Bundles** list, if desired. For more information about the different bundles that are available, see Amazon WorkSpaces Product Details. When you have completed your selections, choose **Next**.
6. Choose the running mode of your WorkSpace as follows:

   - **AlwaysOn** — Use when paying a fixed monthly fee for unlimited usage of your WorkSpaces. This mode is best for users who use their WorkSpace full time as their primary desktop.
   - **AutoStop** — Use when paying for your WorkSpaces by the hour. With this mode, your WorkSpaces stop after a specified period of inactivity and the state of apps and data is saved. To set the automatic stop time, use **AutoStop Time (hours)**.

     When possible, the state of the desktop is saved to the root volume of the WorkSpace. The WorkSpace resumes when a user logs in; all open documents and running programs return to their saved state.
7. Make any changes needed to the list of users or the bundle to use for the WorkSpaces, then choose **Launch WorkSpaces**.

When launching WorkSpaces in a cloud directory, Amazon WorkSpaces assigns the security group it created for directory members to the WorkSpace. For more information about the security group, see WorkSpaces Security Group (p. 4).

It takes several minutes for the WorkSpaces to be launched. When the WorkSpaces are ready for use, an invitation email is sent to unregistered users with registration instructions. If a user has already registered, you must send a welcome email instead. The welcome email contains instructions to download and install a Amazon WorkSpaces client and log in to their WorkSpace. For more information, see Resend an Invitation (p. 53).

Launching WorkSpaces in a Connected Directory

When Amazon WorkSpaces is connected to your on-premises directory, you do not add or remove users with the Amazon WorkSpaces console. Instead, you select existing users in your directory when you are launching WorkSpaces.

To launch a WorkSpace for an existing user

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.

2. In the navigation pane, choose **WorkSpaces**, **Launch WorkSpaces**.
3. For **Select a Directory**, select your connected directory. This is the directory from which users are selected.

   If this is the first time you have launched a WorkSpace in this directory, you can enable or disable the Amazon WorkDocs service for all users in the directory. For more information about Amazon WorkDocs, see Amazon WorkDocs Sync Client Help in the *Amazon WorkDocs Administration Guide*. Make your choice and choose **Next**.

   Note
   This option is only presented if Amazon WorkDocs is available in the selected region.
4. Select the users for which to launch a WorkSpace. You can search for all or part of the user's name, or use the wildcard character (*) to extend the search. You can also choose **Show All Users** . If a user does not have an email address, you will not be able to launch a WorkSpace for that user.

   When you have selected the desired users, choose **Add Selected**. The selected users are moved to the **WorkSpaces** list.

   Repeat this step until you have selected all of the desired users, then choose **Next**.
5. Select the default WorkSpace bundle to be used for the WorkSpaces. If multiple operating system languages are available in your region, you can also select your desired operating system language. You can customize these settings for individual WorkSpaces in the **Assign WorkSpace Bundles** list, if desired. For more information about the different bundles that are available, see Amazon WorkSpaces Product Details. When you have completed your selections, choose **Next**.
6. Choose the running mode of your WorkSpace as follows:

   - **AlwaysOn** — Use when paying a fixed monthly fee for unlimited usage of your WorkSpaces. This mode is best for users who use their WorkSpace full time as their primary desktop.
   - **AutoStop** — Use when paying for your WorkSpaces by the hour. With this mode, your WorkSpaces stop after a specified period of inactivity and the state of apps and data is saved. To set the automatic stop time, use **AutoStop Time (hours)**.

     When possible, the state of the desktop is saved to the root volume of the WorkSpace. The WorkSpace resumes when a user logs in; all open documents and running programs return to their saved state.
7. Make any changes needed to the list of users or the bundle to use for the WorkSpaces, then choose **Launch WorkSpaces**.

When launching WorkSpaces in a connected directory, Amazon WorkSpaces assigns the default VPC security group to the WorkSpace.

It takes several minutes for the WorkSpaces to be launched. When the WorkSpaces are ready for use, you must send a welcome email to each of the users. The welcome email contains instructions for the users to download and install a Amazon WorkSpaces client and log in to their WorkSpace. For more information, see Resend an Invitation (p. 53).

Resend an Invitation

On some occasions, you may need to send an invitation email to a user manually.

To resend an invitation email

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the user to send the invitation to and choose **Actions**, **Invite User**.

4. Copy the email body text and paste it into an email to the user using your own email application. You can modify the body text if desired. When the invitation email is ready, send it to the user.

Encrypt a WorkSpace

Amazon WorkSpaces is integrated with the AWS Key Management Service (AWS KMS). This enables you to encrypt storage volumes of WorkSpaces using customer master keys (CMK). When you launch a new WorkSpace, you have the option to encrypt the root volume (C: drive) and the user volume (D: drive). This ensures that the data stored at rest, disk I/O to the volume, and snapshots created from the volumes are all encrypted.

Prerequisites

You need a AWS KMS CMK before you can begin the encryption process.

The first time you launch a WorkSpace from the Amazon WorkSpaces console in a region, a default CMK is created for you automatically. You can select this key to encrypt the user and root volumes of your WorkSpace.

Alternately, you can select a CMK that you created using AWS KMS. For more information about creating keys, see Creating Keys in the *AWS Key Management Service Developer Guide*. For more information about creating keys using the AWS KMS API, see Working With Keys in the *AWS Key Management Service Developer Guide*.

You must meet the following requirements to use a AWS KMS CMK to encrypt your WorkSpaces:

- The key must be enabled.
- You must have the correct permissions and policies associated with the key. For more information, see IAM Permissions and Roles for Encryption (p. 55).
- One AWS KMS CMK can be used to encrypt up to 30 WorkSpaces in a region.

Limits

- Creating a custom image from an encrypted WorkSpace is not supported.
- Disabling encryption for an encrypted WorkSpace is not currently supported.
- WorkSpaces launched with root volume encryption enabled might take up to an hour to provision.

Encrypting WorkSpaces

To encrypt a WorkSpace using the console

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Launch a new WorkSpace. For more information, see Launching a WorkSpace (p. 51).
3. When prompted to do so, choose the volumes to encrypt. Values can be **Root Volume**, **User Volume**, or both volumes.
4. Choose your AWS KMS CMK from the **Encryption Key** menu.
5. Choose **Next Step** to review the encryption information that you specified.
6. Choose **Launch WorkSpaces** to complete the process.

To encrypt a WorkSpace using the API

- Use the CreateWorkSpaces action and set the following fields:
  - RootVolumeEncryptionEnabled

- UserVolumeEncryptionEnabled
- VolumeEncyptionKey

Maintaining Encrypted WorkSpaces

To see which WorkSpaces and volumes have been encrypted from the Amazon WorkSpaces console, choose **WorkSpaces** from the navigation bar on the left. The **Volume Encryption** column shows whether each WorkSpace has encryption enabled or disabled. To see which specific volumes have been encrypted, expand the WorkSpace entry to see the **Encrypted Volumes** field.

Alternately, you can check the same encryption information with the DescribeWorkSpaces action.

To reboot or rebuild an encrypted WorkSpace, first make sure that the AWS KMS CMK is enabled; otherwise, the WorkSpace becomes unusable.

IAM Permissions and Roles for Encryption

Amazon WorkSpaces encryption privileges require limited AWS KMS access on a given key for the IAM user who launches encrypted WorkSpaces. The following is a sample key policy that can be used. This policy enables you to separate the principals that can manage the AWS KMS CMK from those that can use it. The account ID and IAM user name must be modified to match your account.

The first statement matches the default AWS KMS key policy. The second and third statements define which AWS principals can manage and use the key, respectively. The fourth statement enables AWS services that are integrated with AWS KMS to use the key on behalf of the specified principal. This statement enables AWS services to create and manage grants. The condition uses a context key that is set only for AWS KMS calls made by AWS services on behalf of the customers.

> **Note**
> If you're using the default AWS KMS CMK that Amazon WorkSpaces created for you, skip the following AWS KMS key policy and proceed to the second and third IAM user-based policies below.

```
{
  "Id": "key-consolepolicy-1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::012345678901:root"},
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::012345678901:user/Alice"},
      "Action": [
        "kms:Create*",
        "kms:Describe*",
        "kms:Enable*",
        "kms:List*",
        "kms:Put*",
        "kms:Update*",
        "kms:Revoke*",
        "kms:Disable*",
```

```
        "kms:Get*",
        "kms:Delete*"
       ],
      "Resource": "*"
    },
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::012345678901:user/Alice"},
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    },
    {
      "Sid": "Allow attachment of persistent resources",
      "Effect": "Allow",
      "Principal": {"AWS": "arn:aws:iam::012345678901:user/Alice"},
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {"Bool": {"kms:GrantIsForAWSResource": "true"}}
    }
  ]
}
```

The IAM policy for a user or role that is encrypting a WorkSpace should include usage permissions on the CMK, as well as access to WorkSpaces. The following is a sample policy that can be attached to an IAM user to grant them WorkSpaces privileges.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:*",
                "ds:DescribeDirectories",
                "workspaces:*",
                "workspaces:DescribeWorkspaceBundles",
                "wam:CreateWorkspaces",
                "wam:DescribeWorkspaceBundles",
                "wam:DescribeWorkspaceDirectories",
                "wam:DescribeWorkspaces",
                "wam:RebootWorkspaces",
                "wam:RebuildWorkspaces"
            ],
            "Resource": "*"
        }
    ]
}
```

The following is the IAM policy required by the user for using AWS KMS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow IAM user to select and use KMS keys in WorkSpaces",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:Describe*",
                "kms:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Tag a WorkSpace

You can add and remove tags on WorkSpaces by using the Amazon WorkSpaces console, CLI, or API. You can use tags to categorize your WorkSpaces in different ways, such as by purpose, owner, or department. Each tag consists of a key and optional value that you define. Each tag automatically applies to all WAM applications and WAM related service charges associated with the WorkSpace.

You can also use tags to organize your AWS account bill to reflect your own cost structure. To do this, sign up to get your AWS account bill with tag key values included. For more information about how to do this, see Setting Up Your Monthly Cost Allocation Report.

Tagging WorkSpaces

You can either apply tags to existing WorkSpaces or during the launch of new WorkSpaces. Note that tags added to existing WorkSpaces appear in your cost allocation report on the first of the following month for WorkSpaces renewed in that month.

Restrictions

- The maximum number of tags per WorkSpace is 50.
- The maximum key length is 127 characters.
- The maximum value length is 255 characters.
- Tag keys and values are both case-sensitive.
- Tags with a prefix of "aws:" or "aws:workspaces:" cannot be used. These prefixes are reserved for AWS and WorkSpaces, respectively. Tags with these prefixes cannot be edited or deleted.

To apply tags to new WorkSpaces from the console during launch

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. Choose **Launch WorkSpaces** and assign WorkSpaces bundles to your users.
3. In **Step 4: WorkSpaces Configuration**, enter a key and value pair to create a new tag for the set of WorkSpaces.

To apply tags to existing WorkSpaces using the console

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.

2. Choose **WorkSpaces**, **Actions**, and **Manage Tags**.
3. Enter a key and value pair to create a new tag for the set of WorkSpaces.

To apply tags to WorkSpaces with the API or CLI

Use the CreateWorkspaces, CreateTags, DescribeTags, and DeleteTags actions.

Reboot a WorkSpace

Occasionally, you may find it necessary to reboot a WorkSpace manually. Rebooting a WorkSpace performs a shutdown and restart of the WorkSpace. The user data, operating system, and system settings are not affected.

To reboot a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpaces to be rebooted and choose **Actions**, **Reboot WorkSpaces**.
4. Verify the information in the **Reboot WorkSpaces** dialog box, enter `REBOOT` in the verification field, and choose **Reboot WorkSpaces**.

Rebuild a WorkSpace

If needed, you can rebuild the operating system of a WorkSpace to its original state. Rebuilding a WorkSpace causes the following to occur:

- The system is restored to the most recent image of the bundle that the WorkSpace is created from. Any applications that have been installed, or system settings that have been made after the WorkSpace was created are lost.
- The data drive (D drive) is recreated from the last automatic snapshot taken of the data drive. The current contents of the data drive is overwritten. Automatic snapshots of the data drive are taken every 12 hours, so the snapshot can be as much as 12 hours old.

To rebuild a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the user assigned to the WorkSpace to be rebuilt and choose **Actions**, **Rebuild WorkSpace**.
4. Verify the information in the **Rebuild WorkSpace** dialog box and choose **Rebuild WorkSpace**.

The WorkSpace is rebuilt and ready for use after the **Status** value changes to **Running**.

Remove a WorkSpace

When you remove a WorkSpace, the user is no longer able to access the WorkSpace.

> **Important**
> This is a permanent action and cannot be undone. The user's data is not maintained and will be destroyed. If you need guidance on backing up a WorkSpace user's data, contact AWS Support.

To remove a WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpaces to be removed and choose **Actions**, **Remove WorkSpaces**.
4. Verify the information in the **Remove WorkSpaces** dialog box, enter `REMOVE` in the verification field, and choose **Remove WorkSpaces**.

Edit User Information

You can use the Amazon WorkSpaces console to edit the following information for a user:

- First name
- Last name
- Email address

To edit user information

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select a user and choose **Actions**, **Edit User**.
4. Modify the user information in the **Edit User** dialog box and choose **Update**.

Stop an AutoStop WorkSpace

When your AutoStop WorkSpaces are not in use, they are automatically stopped after a specified period of inactivity, and hourly metering is suspended. To further optimize costs, you can suspend the hourly charges associated with AutoStop WorkSpaces. The WorkSpace will be stopped and all apps and data saved for the next time a user logs in to the WorkSpace.

To stop an AutoStop WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpaces to be stopped and choose **Actions**, **Stop WorkSpaces**.
4. Verify the information in the **Stop WorkSpaces** dialog box, type `STOP` in the verification field, and choose **Stop WorkSpaces**.

To remove the fixed infrastructure costs associated with AutoStop WorkSpaces, remove the WorkSpace from your account. For more information, see Remove a WorkSpace (p. 58).

Start an AutoStop WorkSpace

When a user reconnects to a stopped WorkSpace, it resumes from where it left off, typically in under 90 seconds.

To start an AutoStop WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpaces to be started and choose **Actions**, **Start WorkSpaces**.

4. Verify the information in the **Start WorkSpaces** dialog box, enter `START` in the verification field, and choose **Start WorkSpaces**.

Restart an AutoStop WorkSpace

You can restart AutoStop WorkSpaces that are available or in an error state.

To restart an AutoStop WorkSpace

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpaces to be restarted and choose **Actions**, **Reboot WorkSpaces**.
4. Verify the information in the **Reboot WorkSpaces** dialog box, enter `REBOOT` in the verification field, and choose **Reboot WorkSpaces**.

Modify Running Mode Properties

You can change the running mode properties of your WorkSpaces between AlwaysOn (billed monthly) and AutoStop (billed by the hour).

> **Note**
> If you are changing an existing WorkSpace from AlwaysOn to AutoStop, first reboot the WorkSpace to apply the required updates.

To modify Running Mode properties

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**.
3. Select the WorkSpaces to modify and choose **Actions**, **Modify Running Mode Properties**.
4. Enter the required information in the **Modify Running Mode Properties** dialog box, and choose **Modify**.

WorkSpace Bundle Management

Amazon WorkSpaces allows you to create and save custom WorkSpace bundles. You can then launch WorkSpaces from your own bundles that are pre-configured and have whatever software you need already installed.

Topics

Create a Bundle

To create a bundle, perform the following steps.

To create a new bundle

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpace Images**.

3. Select the image from which to create the bundle and choose **Actions**, **Create Bundle**.
4. In the **Create WorkSpace Bundle** dialog box, enter a name and description for the bundle, select the desired hardware, and choose **Create Bundle**. The bundle is immediately available. You can launch a WorkSpace from the bundle by selecting the bundle in the **WorkSpace Bundles** list and choosing **Launch WorkSpaces**.

Update a Bundle

You can update a bundle after it has been created. For example, you may want the latest operating system and application patches to be available on your WorkSpaces launched from the bundle. You may also want to add more applications to your bundle so that they are available on new WorkSpaces.

Notes

- The new image must have the same base software package (Plus or Standard) as the original image.
- Existing WorkSpaces that are based on the bundle being updated are not affected. To update a running WorkSpace with the latest bundle, you need to rebuild the WorkSpace.

To update a bundle, performing the following steps.

To update a bundle

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpace Bundles**.
3. Select the bundle to update and choose **Actions**, **Update Bundle**.
4. In the **Update WorkSpace Bundle** dialog box, select the new or updated image and choose **Update Bundle**.

Delete a Bundle

You can delete unused bundles if needed. If you delete a bundle that is being used, the bundle is placed in a delete queue and is deleted after all of the WorkSpaces that are created from the bundle have been deleted.

To delete a bundle, perform the following steps.

To delete a bundle

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpace Bundles**.
3. Select the bundle to delete and choose **Actions**, **Delete Bundle**.
4. In the **Delete WorkSpace Bundle** dialog box, verify that you want to delete the bundle and choose **Delete Bundle**.

WorkSpace Image Management

Amazon WorkSpaces allows you to create custom images from running WorkSpaces, and create custom bundles from those images. You can then launch WorkSpaces from your own bundles that are pre-configured and have whatever software you need already installed. For more information about custom bundles, see WorkSpace Bundle Management (p. 60).

When you create an image, the following items are captured from the WorkSpace:

- The entire contents of the `C:\` drive.
- The entire contents of the user profile in `D:\Users\<username>`, except for the following items:
  - contacts
  - downloads
  - music
  - pictures
  - saved games
  - videos
  - .virtualbox
  - tracing
  - podcasts
  - virtual machines
  - appdata\local\temp
  - appdata\roaming\apple computer\mobilesync\
  - appdata\roaming\apple computer\logs\
  - appdata\roaming\apple computer\itunes\iphone software updates\
  - appdata\roaming\macromedia\flash player\macromedia.com\support\flashplayer\sys\
  - appdata\roaming\macromedia\flash player\#sharedobjects\
  - appdata\roaming\adobe\flash player\assetcache\
  - appdata\roaming\microsoft\windows\recent\
  - appdata\roaming\microsoft\office\recent\
  - appdata\roaming\microsoft office\live meeting
  - appdata\roaming\microsoft shared\livemeeting shared\
  - appdata\roaming\mozilla\firefox\crash reports\
  - appdata\roaming\mcafee\common framework\
  - appdata\local\microsoft\feeds cache
  - appdata\local\microsoft\windows\temporary internet files\
  - appdata\local\microsoft\windows\history\
  - appdata\local\microsoft\internet explorer\domstore\
  - appdata\local\microsoft\internet explorer\imagestore\
  - appdata\locallow\microsoft\internet explorer\iconcache\
  - appdata\locallow\microsoft\internet explorer\domstore\
  - appdata\locallow\microsoft\internet explorer\imagestore\
  - appdata\local\microsoft\internet explorer\recovery\
  - appdata\local\mozilla\firefox\profiles\

Topics

Requirements

The following are the requirements for creating images:

- All applications must be installed on the `C:\` drive, or in the user profile under `D:\Users\<username>`. Applications that are installed anywhere else will not be captured.
- All installed applications must be compatible with Microsoft Sysprep.
- Do not delete the user profile on the WorkSpace. The user profile is needed to create the image.
- The total size of the user profile (files and data) must be less than 10 GB.
- The `C:\` drive must have enough available space for the contents of the user profile, plus an additional 2 GB.
- No application services that use domain user credentials can be running on the WorkSpace when the image is created. For example, you cannot have a Microsoft SQL Server Express installation running with a domain user's credentials when you create the image. You must use a local system account instead.

Best Practices for Image Creation

When creating WorkSpace images, we recommend that you follow these best practices:

- Make sure you have enough space on the `C:\` drive of the WorkSpace for the applications that you plan to install.
- Before creating an image, make sure that you install all operating system and application updates and patches.
- Delete any cached data from the WorkSpace that you do not want to preserve. This includes browser history, any cached data or files, and browser cookies.
- All application configuration settings, such as email profiles, are captured in the image. You should delete any of these that you do not want to be copied to the WorkSpaces created from this image.
- When you select an image name, use a name that includes a short name and a version or date, to help identify the image.
- If you want to use Amazon WAM with Amazon WorkSpaces created from custom images, don't launch the Amazon WAM client in the WorkSpace that is used to create the custom image. This ensures that the WorkSpaces you launch from the custom image you create won't have any Amazon WAM configuration tied to the WorkSpace where you originally created the image.

Create an Image

To create an image from a running WorkSpace, perform the following steps.

To create an image

1. Make sure that the user is logged out of, or disconnected from, the WorkSpace from which you are creating the image.
2. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
3. In the navigation pane, choose **WorkSpaces** and select the WorkSpace to create the image from.
4. Choose **Actions**, **Create Image**.
5. In the **Create WorkSpace Image** dialog box, enter a name and a description for the image. You cannot overwrite an existing image, so you must choose a unique name. When complete, choose **Create Image**.

   It can take up to an hour for the image to be created. During this time, the WorkSpace that the image is created from will be unavailable. You can monitor the status of the image by choosing **WorkSpace Images** in the navigation pane. The image is complete when the status changes to **Available**.

Delete an Image

You can delete any of your images. Any existing WorkSpaces that are based on bundles that use the image are not affected, but you won't be able to rebuild or launch any WorkSpaces that use those bundles. As a best practice, do not delete an image that is being used by a custom bundle.

To delete a WorkSpace image, perform the following steps.

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpace Images**.
3. Select the image to delete and choose **Actions**, **Delete Image**.
4. In the **Delete WorkSpace Image** dialog box, verify that you want to delete the image and choose **Delete Image**.

Use Your Windows Desktop Images

If your licensing agreement with Microsoft allows for it, you can use your Windows 7 or Windows 10 Enterprise or Professional desktop images for your Amazon WorkSpaces. To do this, you need to bring your own Microsoft Windows License (BYOL) and provide a Windows 7 or Windows 10 image that meets the requirements listed below. To stay compliant with Microsoft licensing terms, BYOL also requires that you run your Amazon WorkSpaces on hardware that is dedicated to you on the AWS cloud. By bringing your own license, you can save money and provide a consistent experience for all your users. For more information, see Amazon WorkSpaces Pricing.

> **Note**
> Amazon WorkSpaces running Windows 7 or Windows 10 Professional can only be streamed to a single monitor. This is due to limitations of the operating system running in virtual environments.

Prerequisites

Before you begin, make sure that you meet the following requirements:

- You have reviewed the Requirements and Limitations for importing Windows operating systems.
- Your Microsoft licensing agreement allows for Windows 7 or Windows 10 Enterprise or Professional to be run in a virtual hosted environment.
- Your Windows 7 or Windows 10 OS is 64-bit and activated against your key management servers.
- Your Windows 7 or Windows 10 OS has "English (United States)" set as the primary language.
- Your base image contains no additional software beyond what comes with Windows 7 or Windows 10. You can add additional software, like an anti-virus solution, and create a custom image at a later time. For more information, see WorkSpace Image Management (p. 61)
- You have created the following account with local administrator access before you share the image: WorkSpaces_BYOL. The password for this account will be requested at a later time.
- The image that you are importing is on a single volume that is smaller than 80 GB, and the format of the image is OVA.
- Amazon WorkSpaces uses a management interface. It's connected to a secure Amazon WorkSpaces management network used for interactive streaming. It allows for the service to manage your WorkSpaces. Confirm that Amazon WorkSpaces can use one of the following sets of IP ranges for the management interface:
  - 198.18.0.0/15
  - 100.64.0.0/10
  - 10.0.0.0/8

  - 172.16.0.0/12
  - 192.168.0.0/16
- You must use a minimum of 200 Amazon WorkSpaces in order to run your Amazon WorkSpaces on dedicated hardware. Running your Amazon WorkSpaces on dedicated hardware is necessary to comply with Microsoft licensing requirements.

Getting Started

To get started, contact your AWS account manager or Sales representative, or create a Technical Support case for Amazon WorkSpaces. Your contact will verify whether you have enough dedicated capacity allocated to your account and guide you through BYOL setup.

Amazon WorkSpaces Directory Administration

After a directory is created, most administrative functions are performed with directory management tools, such as the Active Directory Administration Tools. You use the Amazon WorkSpaces management console to perform certain directory-related actions, such as creating a new directory or deleting an existing directory. For more information, see Directory Management (p. 41).

Topics

Set Up a Directory Administration WorkSpace

To set up an administration WorkSpace

1. Create a WorkSpace for you or another directory administrator.
2. After the WorkSpace is set up and running, connect to the WorkSpace with one of the Amazon WorkSpaces client applications.
3. Install the Active Directory Administration Tools on the instance as explained in Installing the Active Directory Administration Tools (p. 66).

The following are just some of the administration tools that you can use from this WorkSpace.

Tool	Description
redircmp.exe	Changes the default container that new WorkSpaces are created in to the specified organizational unit (OU).
Event Viewer	Allows you to view the event logs of a WorkSpace. Connect the Event Viewer to the IP address of the WorkSpace, which is available from the WorkSpace details page.

Tool	Description
Active Directory Users and Computers	Used to administer and publish information in the directory, such as users, groups, and organizational units.

Joining an Amazon EC2 Instance to a Directory

You can seamlessly join an EC2 instance to your directory domain when the instance is launched using the Amazon EC2 Simple Systems Manager. For more information, see Seamlessly Joining a Windows Instance to an AWS Directory Service Domain in the *Amazon EC2 User Guide for Windows Instances*.

For more information about manually launching and joining an instance to your directory, see Joining an Instance to an AWS Directory Service Directory in the *AWS Directory Service Administration Guide*.

Installing the Active Directory Administration Tools

To manage your directory from a WorkSpace or an Amazon EC2 Windows instance, you need to install the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools on the WorkSpace or instance. For more information, see Installing the Active Directory Administration Tools in the *AWS Directory Service Administration Guide*.

Topics

Simple AD Directory Administration

When you create a Simple AD directory, a directory administrator account is created for you. The username is `Administrator` and the password is the password you specified when you created the directory. You use this account to administrate your Simple AD directory. When you run any of the Active Directory Administration Tools, you must run them as the directory administrator by following these steps:

1. Open the **Administrative Tools**.
2. Hold down the shift key, right-click on the tool shortcut, and choose **Run as different user**.
3. Enter `Administrator` for the user name and the administrator password.

You can now perform any directory administration tasks that are needed. You can also promote any of your Amazon WorkSpaces user accounts to a directory administrator. To do this, perform the following steps:

Promote a user to a directory administrator

1. Run the Active Directory Users and Computers tool as the directory administrator.
2. Navigate to the **Users** folder under your domain and select the user to promote.
3. In the menu, choose **Action**, **Properties**.
4. In the user properties dialog box, choose **Member of**.
5. Add the user to the following groups and choose **OK**.
   - Administrators
   - Domain Admins

- Enterprise Admins
- Group Policy Creator Owners
- Schema Admins

The user is now a directory administrator.

Creating Users and Groups

You can create users and groups with the Active Directory Users and Computers tool, which is part of the Active Directory Domain Services and Active Directory Lightweight Directory Services Tools. Users represent individual people or entities that have access to your directory. Groups are very useful for giving or denying privileges to groups of users, rather than having to apply those privileges to each individual user. If a user moves to a different organization, you move that user to a different group and they automatically receive the privileges needed for the new organization.

The following examples demonstrate how to create a user, create a group, and add the user to the group. To create users and groups in a directory, you must be connected to a Windows instance that is a member of the directory, and be logged in as a user that has privileges to create users and groups.

To create a user

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. In the directory tree, open your directory and choose the **Users** folder.
3. Choose **Action**, **New**, and **User** to open the new user wizard.
4. In the first page of the new user wizard, enter `Mary` for **First name**, `Major` for **Last name**, and `marym` for **User logon name**. Choose **Next**.
5. In the second page of the new user wizard, enter a secure password for **Password** and **Confirm Password**. Make sure that the **User must change password at next logon** option is not selected. Set the other options as needed for your directory, and choose **Next**.
6. In the third page of the new user wizard, verify the new user information is correct and choose **Finish**. The new user, **Mary Major**, appears in the **Users** folder.

To create a group

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. In the directory tree, open your directory and choose the **Users** folder.
3. Choose **Action**, **New**, and **Group** to open the new group wizard.

4. For **Group name**, enter `Division Managers` , choose **Global** for the **Group scope**, and **Security** for the **Group type**. Choose **OK**. The new group, **Division Managers**, appears in the **Users** folder.

To add a user to a group

1. Open the Active Directory Users and Computers tool. There is a shortcut to this tool in the **Administrative Tools** folder.

   Tip
   You can run the following from a command prompt on the instance to open the Active Directory Users and Computers tool box directly.

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. In the directory tree, open your directory and choose **Users**, **Division Managers**.
3. Choose **Action**, **Properties** to open the properties dialog box for the **Division Managers** group.
4. Choose **Members**, **Add...**.
5. For **Enter the object names to select**, enter `marym` and choose **OK**. **Mary Major** is displayed in the **Members** list. Choose **OK** again to update the group membership.
6. Verify that Mary Major is now a member of the **Division Managers** group by choosing **Mary Major** in the **Users** folder, **Action**, **Properties**, and **Member Of**. **Division Managers** should be in the list of groups to which Mary Major belongs.

User Passwords

Users can change their password from within their WorkSpace by following the instructions at Change your Windows password.

As the directory administrator, you can use the Active Directory Users and Computers tool to reset the password for an existing user. When you do this, do not set the **User must change password at next logon** setting. The user will not be able connect to their WorkSpace. Instead, assign a secure temporary password to the user and instruct them to manually change their password from within the WorkSpace the next time they log on.

Remove a User

Because Amazon WorkSpaces uses Active Directory to store its user information, you can use whichever Active Directory tools you are familiar with to delete a user object. For more information about accessing these objects, see Directory Management (p. 41).

Note
Before you can remove a user, you must remove the WorkSpace assigned to that user. For more information about removing WorkSpaces, see Remove a WorkSpace (p. 58).

Using Group Policy to Manage WorkSpaces and Users

Because Amazon WorkSpaces uses an Active Directory-compatible directory, you can apply Group Policy settings to the WorkSpaces and users that are part of your directory. We recommend that you create and manage an organizational unit for your Amazon WorkSpaces machine accounts, and another organizational unit for your Amazon WorkSpaces user accounts. You can then apply Group

Policy settings that are specific to your WorkSpaces to these organizational units, and those settings are applied to all of your WorkSpaces or Amazon WorkSpaces users.

Group Policy settings can affect your WorkSpace users' experience in several ways:

- Depending on the number of custom Group Policy settings applied to a WorkSpace, a user's first login to their WorkSpace after it is launched or rebooted may take several minutes.
- Changes to Group Policy settings may cause an active session to be closed when a user is not connected to the WorkSpace.
- Some Group Policy settings force a user to log off when they are disconnected from a session. Any applications that a user has open on the WorkSpace are closed.
- Implementing an interactive logon message to display a logon banner prevents users from being able to access their WorkSpace. The interactive logon message Group Policy setting is not currently supported by Amazon WorkSpaces.

For more information about how to distribute an application to your WorkSpaces using Group Policy, see Tutorial: Distributing an Application Using Group Policy (p. 84).

Topics

Installing the Group Policy Administrative Template

To use the Group Policy settings that are specific to Amazon WorkSpaces, you need to install the Group Policy administrative template. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your directory.

To install the Group Policy administrative template

1. From a running WorkSpace, make a copy of the `pcoip.adm` file in the `C:\Program Files (x86)\Teradici\PCoIP Agent\configuration` directory.
2. Open the Group Policy Management tool and navigate to the organizational unit in your domain that contains your WorkSpaces machine accounts.
3. Open the context (right-click) menu for the machine account organizational unit and choose **Create a GPO in this domain, and link it here**.
4. In the **New GPO** dialog box, enter a descriptive name for the Group Policy object, such as **WorkSpaces Machine Policies**, and leave **Source Starter GPO** set to **(none)**. Choose **OK**.
5. Open the context (right-click) menu for the new Group Policy object and choose **Edit**.
6. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, and **Administrative Templates**. Choose **Action**, **Add/Remove Templates** from the main menu.
7. In the **Add/Remove Templates** dialog box, choose **Add**, select the `pcoip.adm` file copied previously, and then choose **Open**, **Close**.
8. Close the Group Policy Management Editor. You can now use this Group Policy object to modify the Group Policy settings that are specific to Amazon WorkSpaces.

Local Printer Support

By default, Amazon WorkSpaces supports local printer redirection. You can use Group Policy settings to disable this feature if needed.

To enable or disable local printer support

1. Make sure that the most recent Amazon WorkSpaces Group Policy administrative template (p. 69) is installed in your domain.
2. Open the Group Policy Management tool and navigate to and select the WorkSpaces Group Policy object for your WorkSpaces machine accounts. Choose **Action**, **Edit** in the main menu.
3. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Classic Administrative Templates**,**PCoIP Session Variables**, and **Overridable Administration Defaults**.
4. Open the **Configure remote printing** setting.
5. In the **Configure remote printing** dialog box, choose **Enabled** and set the **Configure remote printing** option to the desired setting, enabled or disabled, and choose **OK**.

The Group Policy setting change takes effect after the WorkSpace's next Group Policy settings update and the session is restarted.

Clipboard Redirection

By default, Amazon WorkSpaces supports clipboard redirection. You can use Group Policy settings to disable this feature if needed.

To enable or disable clipboard redirection

1. Make sure that the most recent Amazon WorkSpaces Group Policy administrative template (p. 69) is installed in your domain.
2. Open the Group Policy Management tool and navigate to and select the WorkSpaces Group Policy object for your WorkSpaces machine accounts. Choose **Action**, **Edit** in the main menu.
3. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**,**Classic Administrative Templates**, **PCoIP Session Variables**, and **Overridable Administration Defaults**.
4. Open the **Configure clipboard redirection** setting.
5. In the **Configure clipboard redirection** dialog box, choose **Enabled** and set the **Configure clipboard redirection** option to the desired setting, enabled or disabled, and choose **OK**.

The Group Policy setting change takes effect after the WorkSpace's next Group Policy settings update and the session is restarted.

Setting the Session Resume Timeout

When using the Amazon WorkSpaces client applications, an interruption of network connectivity causes an active session to be disconnected. This can be caused by events such as closing the laptop lid, or the loss of your wireless network connection. The Amazon WorkSpaces client applications for Windows and OS X attempt to reconnect the session automatically if network connectivity is regained within a certain amount of time. The default session resume timeout is 20 minutes, but you can modify that value for WorkSpaces that are controlled by your domain's Group Policy settings.

To set the automatic session resume timeout value

1. Make sure that the most recent Amazon WorkSpaces Group Policy administrative template (p. 69) is installed in your domain.
2. Open the Group Policy Management tool and navigate to and select the WorkSpaces Group Policy object for your WorkSpaces machine accounts. Choose **Action**, **Edit** in the main menu.
3. In the Group Policy Management Editor, choose **Computer Configuration**, **Policies**, **Administrative Templates**, **Classic Administrative Templates**, and **PCoIP Session Variables**.

To allow the user to override your setting, choose **Overridable Administration Defaults**; otherwise, choose **Not Overridable Administration Defaults**.

4. Open the **Configure Session Automatic Reconnection Policy** setting.
5. In the **Configure Session Automatic Reconnection Policy** dialog box, choose **Enabled**, set the **Configure Session Automatic Reconnection Policy** option to the desired timeout, in minutes, and choose **OK**.

The Group Policy setting change takes effect after the WorkSpace's next Group Policy settings update and the session is restarted.

File Sharing

You can allow file sharing between your WorkSpaces, as well as Amazon EC2 instances that are joined to your directory, by allowing inbound and outbound TCP traffic on port 445 from the VPC that the WorkSpaces/instances are running in, such as `10.0.0.0/16`. You can either modify the existing security group, or create a new security group and add it to the WorkSpaces/instances. You can find both the security group and VPC identifiers for your WorkSpaces in the directory details in the Amazon WorkSpaces console. For more information about adding a security group to WorkSpaces in a cloud directory, see Add a Security Group (p. 43). For more information about adding a security group to WorkSpaces in a connected directory, see Add a Security Group (p. 46). For information about how to find the WorkSpaces security group, see WorkSpaces Security Group (p. 4).

When you share a folder, you should, at a minimum, only share the folder with authenticated users from the directory that the WorkSpace or instance belongs to. To do this, select the `Authenticated Users` group when selecting the users to share the folder with. You can select individual users or groups if you want to restrict access to the share even further.

After you share a folder, the shared folder can be accessed from another WorkSpace or instance using the machine IP address and path of the folder, such as `\\<machine_IP_address>\<share_name>`. If the DNS name of the machine that is sharing files can be resolved, you can use the UNC path such as `\\<machine_name>\<share_name>`.

Enabling PCoIP Zero Client

To allow access to your WorkSpaces from PCoIP zero client devices, you need to launch and configure an EC2 instance with PCoIP Connection Manager for Amazon WorkSpaces. Go to the AWS Marketplace to find an Amazon Machine Image (AMI) that you can use to launch an instance with PCoIP Connection Manager for Amazon WorkSpaces. For more information about how to launch the AMI and configure the connection manager, see *Deploying the PCoIP Connection Manager for Amazon WorkSpaces* in the PCoIP Connection Manager User Guide.

For information about setting up and connecting with a PCoIP zero client device, see PCoIP Zero Client Help (p. 110).

Monitoring Amazon WorkSpaces Metrics

Amazon WorkSpaces and Amazon CloudWatch are integrated, so you can gather and analyze performance metrics. You can monitor these metrics using the CloudWatch console, the CloudWatch command-line interface, or programmatically using the CloudWatch API. CloudWatch also allows you to set alarms when you reach a specified threshold for a metric.

For more information about using CloudWatch and alarms, see the Amazon CloudWatch User Guide.

Topics

Amazon WorkSpaces Metrics

The `AWS/WorkSpaces` namespace includes the following metrics.

Metric	Description	Dimensions	Statistics Available	Units
`Available`[1]	The number of WorkSpaces that returned a healthy status.	`DirectoryId` `WorkspaceId`	Average, Sum, Maximum, Minimum, Data Samples	Count
`Unhealthy`[1]	The number of WorkSpaces that returned an unhealthy status.	`DirectoryId` `WorkspaceId`	Average, Sum, Maximum, Minimum, Data Samples	Count
`ConnectionAttempt`[2]	The number of connection attempts.	`DirectoryId` `WorkspaceId`	Average, Sum, Maximum, Minimum, Data Samples	Count
`ConnectionSuccess`[2]	The number of successful connections.	`DirectoryId` `WorkspaceId`	Average, Sum, Maximum, Minimum, Data Samples	Count
`ConnectionFailure`[2]	The number of failed connections.	`DirectoryId` `WorkspaceId`	Average, Sum, Maximum, Minimum, Data Samples	Count
`SessionLaunchTime`[2]	The amount of time it takes to initiate a WorkSpaces session.	`DirectoryID` `WorkspaceID`	Average, Sum, Maximum, Minimum, Data Samples	Second (time)
`InSessionLatency`[2]	The round trip time between the WorkSpaces client and the WorkSpace.	`DirectoryID` `WorkspaceID`	Average, Sum, Maximum, Minimum, Data Samples	Millisecond (time)
`SessionDisconnect`[2]	The number of connections that were closed, including user-initiated and failed connections.	`DirectoryID` `WorkspaceID`	Average, Sum, Maximum, Minimum, Data Samples	Count

Metric	Description	Dimensions	Statistics Available	Units
`UserConnected`[3]	The number of WorkSpaces that have a user connected.	`DirectoryID` `WorkspaceID`	Average, Sum, Maximum, Minimum, Data Samples	Count
`Stopped`	The number of WorkSpaces that are stopped.	`DirectoryID` `WorkspaceID`	Average, Sum, Maximum, Minimum, Data Samples	Count
`Maintenance`[4]	The number of WorkSpaces that are under maintenance.	`DirectoryID` `WorkspaceID`	Average, Sum, Maximum, Minimum, Data Samples	Count

[1] Amazon WorkSpaces periodically sends status requests to a WorkSpace. A WorkSpace is marked `Available` when it responds to these requests, and `Unhealthy` when it fails to respond to these requests. These metrics are available at a per-WorkSpace granularity, and also aggregated for all WorkSpaces in an organization.

[2] Amazon WorkSpaces records metrics on connections made to each WorkSpace. These metrics are emitted after a user has successfully authenticated via the WorkSpaces client and the client then initiates a session. The metrics are available at a per-WorkSpace granularity, and also aggregated for all WorkSpaces in a directory.

[3] Amazon WorkSpaces periodically sends connection status requests to a WorkSpace. Users are reported as connected when they are actively using their sessions. This metric is available at a per-WorkSpace granularity, and is also aggregated for all WorkSpaces in an organization.

[4] This metric applies to WorkSpaces that are configured with an AutoStop running mode. If you have maintenance enabled for your WorkSpaces, this metric captures the number of WorkSpaces that are currently under maintenance. This metric is available at a per-WorkSpace granularity, which describes when a WorkSpace went into maintenance and when it was removed.

Dimensions for Amazon WorkSpaces Metrics

Amazon WorkSpaces metrics are available for the following dimensions.

Dimension	Description
`DirectoryId`	Limits the data you receive to the WorkSpaces in the specified directory. The `DirectoryId` value is in the form of `d-XXXXXXXXXX`.
`WorkspaceId`	Limits the data you receive to the specified WorkSpace. The `WorkspaceId` value is in the form`ws-XXXXXXXXXX`.

Monitoring Example

The following example demonstrates how you can use the Amazon WorkSpaces CLI and CloudWatch CLI to respond to a CloudWatch alarm and determine which WorkSpaces in a directory have experienced connection failures.

1. Determine which directory the alarm applies to.

```
aws cloudwatch describe-alarms --state-value "ALARM"

{
  "MetricAlarms" : [
    {
      ...
      "Dimensions" : [
        {
          "Name" : "DirectoryId",
          "Value" : "<directory_id>"
        }
      ],
      ...
    }
  ]
}
```

2. Get the list of WorkSpaces in the specified directory.

```
aws workspaces describe-workspaces --directory-id <directory_id>

{
  "Workspaces" : [
    {
      ...
      "WorkspaceId" : "<workspace1_id>",
      ...
    },
    {
      ...
      "WorkspaceId" : "<workspace2_id>",
      ...
    },
    {
      ...
      "WorkspaceId" : "<workspace3_id>",
      ...
    }
  ]
}
```

3. Get the CloudWatch metrics for each WorkSpace in the directory.

```
aws cloudwatch get-metric-statistics \
--namespace AWS/WorkSpaces \
--metric-name ConnectionFailure \
--start-time 2015-04-27T00:00:00Z \
--end-time 2015-04-28T00:00:00Z \
--period 3600 \
--statistics Sum \
--dimensions "Name=WorkspaceId,Value=<workspace_id>"

{
  "Datapoints" : [
    {
      "Timestamp" : "2015-04-27T00:18:00Z",
```

```
      "Sum" : 1.0,
      "Unit" : "Count"
    },
    {
      "Timestamp" : "2014-04-27T01:18:00Z",
      "Sum" : 0.0,
      "Unit" : "Count"
    }
  ],
  "Label" : "ConnectionFailure"
}
```

Troubleshooting Amazon WorkSpaces Administration Issues

Topics

Launching WorkSpaces in my connected directory often fails

Verify that the two DNS servers or domain controllers in your on-premises directory are accessible from each of the subnets that you specified when you connected to your directory. You can verify this connectivity by launching an EC2 instance in each subnet and joining the instance to your directory, using the IP addresses of the two DNS servers. For more information about joining an instance to your directory, see Joining an Amazon EC2 Instance to a Directory (p. 66).

Can't connect to a WorkSpace with an interactive logon banner

Implementing an interactive logon message to display a logon banner will prevent users from being able to access their WorkSpace. The interactive logon message Group Policy setting is not currently supported by Amazon WorkSpaces.

None of the WorkSpaces in my directory can connect to the Internet

WorkSpaces cannot communicate with the Internet by default. You must explicitly provide Internet access. For a cloud directory, see Simple AD Directory Internet Access (p. 16). For a connected directory, see AD Connector Directory Internet Access (p. 21).

I receive a "DNS unavailable" error when I try to connect to my on-premises directory

You receive an error message similar to the following when connecting to your on-premises directory:

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector must be able to communicate with your on-premises DNS servers via TCP and UDP over port 53. Verify that your security groups and on-premises firewalls allow TCP and UDP communication over this port. For more information, see Preparing Your Network for an AD Connector Directory (p. 19).

I receive a "Connectivity issues detected" error when I try to connect to my on-premises directory

You receive an error message similar to the following when connecting to your on-premises directory:

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP
 address>
Kerberos/authentication unavailable (TCP port 88) for IP: <IP address>
Please ensure that the listed ports are available and retry the operation.
```

AD Connector must be able to communicate with your on-premises domain controllers via TCP and UDP over the following ports. Verify that your security groups and on-premises firewalls allow TCP and UDP communication over these ports. For more information, see Preparing Your Network for an AD Connector Directory (p. 19).

- 88 (Kerberos)
- 389 (LDAP)

I receive an "SRV record" error when I try to connect to my on-premises directory

You receive an error message similar to one or more of the following when connecting to your on-premises directory:

```
SRV record for LDAP does not exist for IP: <DNS IP address>

SRV record for Kerberos does not exist for IP: <DNS IP address>
```

AD Connector needs to obtain the `_ldap._tcp.<DnsDomainName>` and `_kerberos._tcp.<DnsDomainName>` SRV records when connecting to your directory. You will get this error if the service cannot obtain these records from the DNS servers that you specified when connecting to your directory. Make sure that your DNS servers contains these SRV records. For more information about SRV records, see SRV Resource Records on Microsoft TechNet.

One of my WorkSpaces has a state of "Unhealthy"

The Amazon WorkSpaces service periodically sends status requests to a WorkSpace. A WorkSpace is marked `Unhealthy` when it fails to respond to these requests. Common causes for this problem are:

- An application on the WorkSpace is blocking network ports which prevents the WorkSpace from responding to the status request.
- High CPU utilization is preventing the WorkSpace from responding to the status request in a timely manner.
- The computer name of the WorkSpace has been changed. This prevents a secure channel from being established between Amazon WorkSpaces and the WorkSpace.

You can attempt to correct the situation using the following methods:

- Reboot the WorkSpace from the Amazon WorkSpaces console. For more information, see Reboot a WorkSpace (p. 58).
- Connect to the unhealthy WorkSpace using the following procedure:

  Note
  This procedure should only be used for troubleshooting purposes.

  1. Using a WorkSpaces client, connect to an operational WorkSpace in the same directory as the unhealthy WorkSpace.
  2. From the operational WorkSpace, use Remote Desktop Protocol (RDP) to connect to the unhealthy WorkSpace using the IP address of the unhealthy WorkSpace. The IP address of the WorkSpace is provided in the WorkSpace information in the Amazon WorkSpaces console. Depending on the extent of the problems on the WorkSpace, you may not be able to connect to the unhealthy WorkSpace.
  3. On the unhealthy WorkSpace, confirm that the minimum port requirements are met. For more information about the minimum port requirements for WorkSpaces, see Amazon WorkSpaces Concepts (p. 1).
- Rebuild the WorkSpace from the Amazon WorkSpaces console. For more information, see Rebuild a WorkSpace (p. 58). Because rebuilding a WorkSpace can potentially cause a loss of data, this option should only be used if all other attempts to correct the problem have been unsuccessful.

The state of my apps was not saved when my WorkSpace was stopped

To save the state of your apps, you must have enough free space on the root volume of your WorkSpace to store the total memory offered on the WorkSpace bundle. For example, a Standard Workspace has 4 GB of memory, so you must have 4 GB of free space on the root volume of the WorkSpace.

Also, if the Amazon WorkSpaces service could not communicate with the WorkSpace when a stop request is issued, it will force shut down the operating system and the state of the apps will not be saved.

Tutorials

The following tutorials will help you perform detailed tasks using Amazon WorkSpaces.

Topics

Tutorial: Creating a Simple AD Directory

The following tutorial walks you through all of the steps necessary to set up a Simple AD directory for use with Amazon WorkSpaces. This tutorial explains how to complete the following tasks:

- Create a VPC for use with the Simple AD directory. This VPC will contain the following:
  - One public subnet and two private subnets.
  - An Internet gateway to use with the public subnet. The two private subnets are used for your WorkSpaces.
  - An Amazon EC2 instance to perform network address translation (NAT), or a NAT gateway. The NAT device is required to provide Internet access to your WorkSpaces.
- Create a Simple AD directory in your VPC.
- Create a user in your directory, launch a WorkSpace for that user, and test the WorkSpace.

Prerequisites

This tutorial assumes the following:

- You have an active AWS account.
- Your account has not reached its limit of VPCs in the region you want to use Amazon WorkSpaces in.
- You do not have an existing VPC in the region with a CIDR of 10.0.0.0/16.
- You have an available Elastic IP address for a VPC in your account for the NAT gateway.

Notes

This tutorial is intended to get you started with Amazon WorkSpaces quickly and easily, but is not intended to be used in a large scale production environment. The following notes provide additional information.

- For more information about Amazon VPC, see the following topics in the *Amazon VPC User Guide*:
  - What is Amazon VPC?
  - Subnets in Your VPC
- For more information about managing your directory, see Simple AD Directory Administration (p. 66).
- A single NAT instance creates a single point of failure. We recommend that you create a NAT gateway instead. If you want to use a NAT instance, you should create multiple NAT instances in different Availability Zones for high availability. For more information, see the article High Availability for Amazon VPC NAT Instances: An Example.

Step 1: Create and Configure Your VPC

The following sections demonstrate how to create and configure a VPC for use with a Simple AD directory.

Topics

Create a VPC

This tutorial uses one of the VPC creation wizards to create the following:

- The VPC
- The public subnet
- One of the private subnets
- The Internet gateway
- The NAT gateway

To create your VPC using the VPC wizard

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **VPC Dashboard**, **Start VPC Wizard**. If you do not already have any VPC resources, locate the **Your Virtual Private Cloud** area of the dashboard and choose **Get started creating a VPC**.
3. Choose **VPC with Public and Private Subnets**, **Select**.
4. Enter the following information into the wizard and choose **Create VPC**.

   #### VPC wizard fields

   IP CIDR block
   `10.0.0.0/16`

   VPC name
   `WorkSpaces VPC`

Public subnet
`10.0.0.0/24`

Availability Zone
No Preference

Public subnet name
`NAT subnet`

Private subnet
`10.0.1.0/24`

Availability Zone
No Preference

Private subnet name
`WorkSpaces subnet 1`

Elastic IP Allocation ID
Select an available Elastic IP address to assign to the NAT gateway

Enable DNS hostnames
Leave default selection

Hardware tenancy
Default

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

   Note
   If you prefer to launch a NAT instance instead, choose **Use a NAT instance instead** in the wizard, and select an instance type and key pair.

Add a Second Private Subnet

Create the second private subnet by perform the following steps:

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose **Subnets**, select the subnet with the name `WorkSpaces subnet 1`, and choose the **Summary** tab at the bottom of the page. Make a note of the Availability Zone of this subnet.
3. Choose **Create Subnet**, enter the following information in the **Create Subnet** dialog box, and choose **Yes, Create**.

   Subnet 2 Settings

   Name tag
   `WorkSpaces subnet 2`

   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 different Availability Zones.

   CIDR Block
   `10.0.2.0/24`

Modify the Route Tables

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

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.

2. In the navigation pane, choose **Subnets** and select the subnet with the name `NAT subnet`. At the bottom of the page, choose the **Route Table** tab and make a note of the **Route Table** identifier for the subnet. The route table identifier will be similar to `rtb-xxxxxxxx`.
3. In the navigation pane, choose **Route Tables**, select the route table identified in the previous step, and change the name to `NAT route table`.
4. At the bottom of the page, choose the **Routes** tab and verify that the following entries are in the route table for `NAT route table`. Modify the route table if needed by choosing **Edit**.

   NAT Subnet Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-xxxxxxxx*

   This routes all traffic destined for the VPC locally, and traffic destined to all other IP addresses to the Internet gateway that was created with the Amazon VPC wizard. *igw-xxxxxxxx* identifies the Internet
5. In the navigation pane, choose **Subnets** and select the subnet with the name `WorkSpaces subnet 1`. At the bottom of the page, choose the **Route Table** tab and make a note of the **Route Table** identifier for the subnet. The route table identifier will be similar to `rtb-xxxxxxxx`.
6. Select the subnet with the name `WorkSpaces subnet 2` and choose the **Route Table** tab at the bottom of the page. The route table identifier should be the same for `WorkSpaces subnet 1` and `WorkSpaces subnet 2`. If the route table for `WorkSpaces subnet 2` is different, change the route table for `WorkSpaces subnet 2` to the same as that for `WorkSpaces subnet 1`.
7. In the navigation pane, choose **Route Tables**, select the WorkSpaces route table identified previously, and change the name to `WorkSpaces route table`.
8. At the bottom of the page, choose the **Routes** tab and verify that the following entries are in the route table for `WorkSpaces route table`. Modify the route table if needed by choosing **Edit**.

   WorkSpaces Subnets Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*nat-xxxxxxxx*

   This routes all traffic destined for the VPC locally, and traffic destined to all other IP addresses to the NAT gateway *nat-xxxxxxxx*.

   Note
   If you launched a NAT instance instead, the route points to *eni-xxxxxxxx/i-xxxxxxxx* for the NAT instance.

(Optional) Configure NAT Instance Options

If you launched a NAT instance instead of a NAT gateway, modify the security group associated with the NAT instance to contain the following inbound rules:

NAT Security Group Inbound Rules

Type	Protocol	Port Range	Source
HTTP	TCP	80	10.0.1.0/24
HTTP	TCP	80	10.0.2.0/24
HTTPS	TCP	443	10.0.1.0/24
HTTPS	TCP	443	10.0.2.0/24

This allows inbound traffic on ports 80 (HTTP) and 443 (HTTPS) to the NAT from the two private subnets.

Modify the security group associated with the NAT instance to contain the following outbound rules:

NAT Security Group Outbound Rules

Type	Protocol	Port Range	Destination
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

This allows outbound traffic on ports 80 (HTTP) and 443 (HTTPS) to any destination.

For the NAT instance to operate correctly, the *`Source/Destination Check`* attribute must be disabled. Although the Amazon VPC wizard does this for you, these instructions are included so you can do this yourself if needed. You can also use this procedure to verify that the *`Source/Destination Check`* attribute has been disabled.

To verify that the source/destination check attribute is disabled

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose **Instances** and find the NAT instance that is in your VPC. The NAT instance will have a private IP address in the address range 10.0.0.0/24. Change the name of the NAT instance to `WorkSpaces NAT instance`.
3. With the NAT instance selected, choose **Actions**, **Change Source/Dest. Check**. If **Status** is **Disabled**, the attribute is already disabled. If **Status** is **Enabled**, choose **Yes, Disable**.

Step 2: Create the Simple AD Directory

To create your Simple AD directory, perform the following steps. For more information about this process, see Create the Directory with the Amazon WorkSpaces Console (p. 38).

To create a cloud directory

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **Directories** and **Set up Directory**
3. In the **Simple AD** area, choose **Create Simple AD**.
4. Enter values in the following fields:

   Organization Name
   Enter a globally unique name for your organization, such as *`yourname`*`-example-dir`. This must be at least four characters in length and can contain only alphanumeric characters and

hyphens. The name cannot begin or end with a hyphen. An error is returned when you choose **Continue** if the organization name has already been used.

Directory DNS
`example.com`

NetBIOS name
`EXAMPLE`

Administrator password
The password for the directory administrator. The directory creation process creates an administrator account with the username `Administrator` and this password. For password requirements, see the note following the table.

The directory administrator password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must also contain at least one character from three of the following four categories:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password
Re-enter the administrator password.

5. Enter values in the following fields in the **VPC Details** section and choose **Continue**.

   VPC
   The VPC for the directory.

   Subnets
   Select the subnets for the directory servers. The two subnets must be in different Availability Zones.

6. Review the directory information and make any necessary changes. When the information is correct, choose **Create Simple AD**.

Step 3: Create a WorkSpace

The following procedure creates a new user in your Simple AD directory and launches a WorkSpace for that user. For more information about this procedure, see Launching WorkSpaces in a Cloud Directory (p. 51).

To launch a WorkSpace for a user

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpaces**, **Launch WorkSpaces**.
3. For **Select Directory**, select your cloud directory, `example.com`. For **Enable WorkDocs for all users in this Directory**, choose **Yes**, **Next**

   For more information about Amazon WorkDocs, see Amazon WorkDocs Sync Client Help in the *Amazon WorkDocs Administration Guide*.

   Note
   This option is only presented if Amazon WorkDocs is available in the selected region.

4. Enter the following information for the new user and choose **Create Users**, which adds the new user to the **WorkSpaces** list. Choose **Next**.

Test User Information

Username
`johndoe`

First Name
`John`

Last Name
`Doe`

Email
Enter a valid email address you have access to. The registration and invitation email is sent to this address.

5. In **WorkSpace Bundles**, select the **Value** bundle, then choose **Next**.
6. Verify the user and bundle to use for the WorkSpaces, then choose **Launch WorkSpaces**.

   It takes several minutes for the WorkSpace to be launched. When the WorkSpace is ready for use, an invitation email is sent to the email address specified for the new user that contains instructions for completing their user profile, how to download and install an Amazon WorkSpaces client, and log in to their WorkSpace.
7. When you receive the invitation email, open the link in the email to complete your user profile. Enter a password for the new user, verify the new password, and choose **Update User** to complete your user profile. Do not forget this password. It is used to connect to your workspace.

Step 4: Test the WorkSpace

To test the WorkSpace and verify that it has Internet connectivity, perform the following steps:

1. Download and install the desired Amazon WorkSpaces client application from http://clients.amazonworkspaces.com/.
2. Launch the client application. If this is the first time you have run the application on this client, enter the registration code provided in the invitation email and choose **Register**. If the client application has already been registered on this client, choose the gear icon at the top of the login page and **Register**. Enter the registration code provided in the invitation email and choose **Register**.
3. Connect to the WorkSpace by entering the username (`johndoe`) and password for the user, and choose **Sign In**.
4. After your WorkSpace desktop is displayed, open the web browser, navigate to `http://aws.amazon.com/workspaces/`, and verify that you can view the page.

Congratulations! Your Amazon WorkSpaces cloud directory has been created, and your first WorkSpace is working correctly and has Internet access.

Tutorial: Distributing an Application Using Group Policy

A common use of Group Policy settings is to install a particular application on the WorkSpaces of particular users. The following example walks you through all of the steps necessary to install the AWS CLI on the WorkSpaces of all users that belong to a specific Active Directory organizational unit (OU). To complete this scenario, you need the following:

- An Amazon WorkSpaces cloud directory.

- One of the following:
  - An administration WorkSpace that has the Active Directory Administration Tools and Group Policy Management tools installed. For more information, see Set Up a Directory Administration WorkSpace (p. 65) and Installing the Active Directory Administration Tools (p. 66).
  - An EC2 instance joined to the directory that has the Active Directory Administration Tools and Group Policy Management tools installed. For more information, see Joining an Amazon EC2 Instance to a Directory (p. 66) and Installing the Active Directory Administration Tools (p. 66).
- One or more WorkSpaces to install the application on.

Note
With Group Policy, you can only install `.msi` and `.zap` files. You cannot install `.exe` files.

Topics

Launch a File Server

Launch an EC2 instance in your VPC to serve as a file server. The file server will be the source of the application installation package.

To launch a file server

1. From within the instance, change the name of the instance to something meaningful, such as `FS1`. It is much easier to change the machine name before it is joined to the Amazon WorkSpaces directory.
2. Join this instance to your directory, as explained in Joining an Amazon EC2 Instance to a Directory (p. 66).
3. Modify the security group for the file server and directory members to allow inbound and outbound TCP traffic on port 445 from all addresses within the VPC. Depending on your implementation, these may or may not be the same security group. For more information, see File Sharing (p. 71).
4. Create a directory on the file server and give the directory a meaningful name, such as `Installers`.
5. Share the directory with the **Authenticated Users** group from the directory, giving them read-only access to the share. This share can be accessed using a UNC path such as `\\FS1\Installers`.
6. Download the 64-bit AWS CLI installer from https://s3.amazonaws.com/aws-cli/AWSCLI64.msi and copy it to the `\\FS1\Installers` share.

Create an Organizational Unit

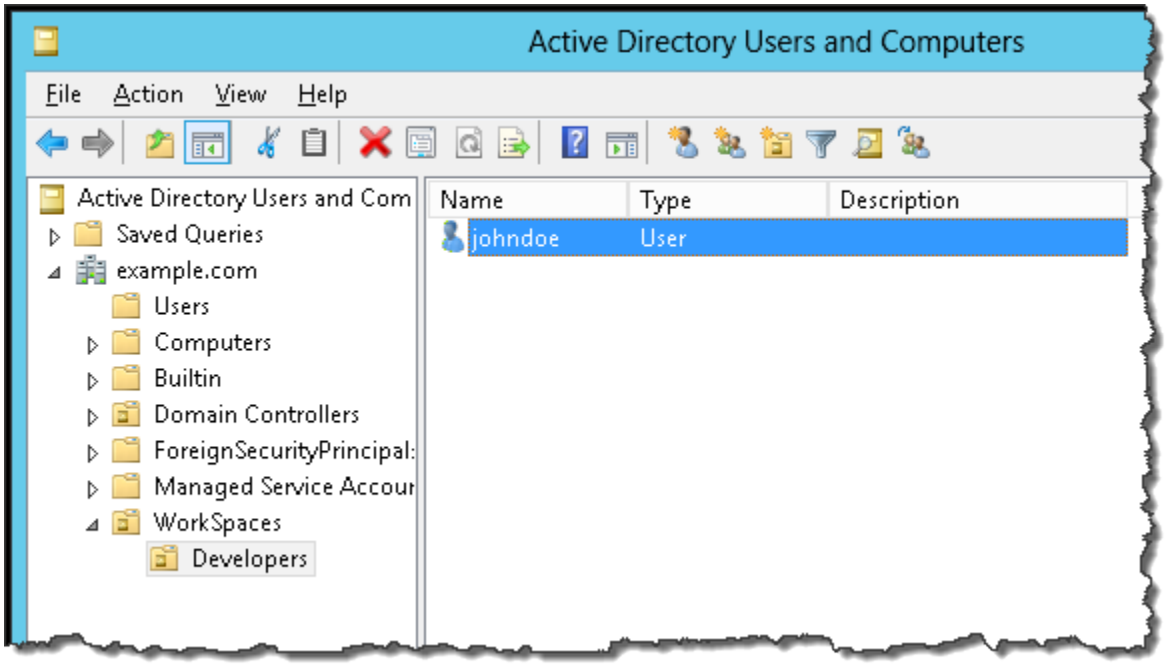
Create an Active Directory organizational unit to assign the group policy to. All users that are members of this OU will have the Group Policy applied.

In **Active Directory Users and Computers**, perform the following steps.

To create an organizational unit

1. Create a **WorkSpaces** organizational unit (OU). Under the **WorkSpaces** OU, create a **Developers** OU.

2. Move the Amazon WorkSpaces user that the application should be installed for to the **Developers** OU. By default, Amazon WorkSpaces creates its users in the **Users** folder under the domain.

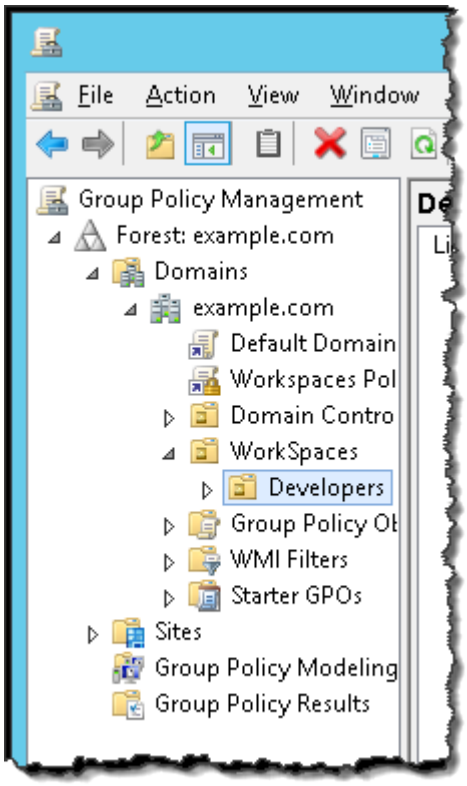


Create a Group Policy to Install the Application

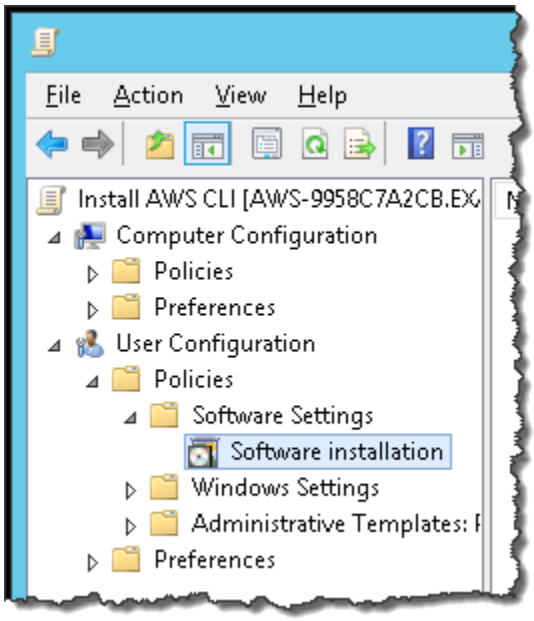
Add a Group Policy setting to the OU that installs the AWS CLI.

To install an application using Group Policy

1. Open the Group Policy Management tool and navigate to the **Developers** OU in your domain. This is the OU you created in Create an Organizational Unit (p. 85).



2. Open the context (right-click) menu for the **Developers** OU and choose **Create a GPO in this domain, and link it here**.
3. In the **New GPO** dialog box, enter **Install AWS CLI** for the **Name** and leave **Source Starter GPO** set to **(none)**. Choose **OK**.
4. Open the context (right-click) menu for the **Install AWS CLI** GPO and choose **Edit**.
5. In the **Group Policy Management Editor** dialog box, choose **User Configuration**, **Policies**, **Software Settings**, **Software installation**.
6. Open the context (right-click) menu for **Software installation** and choose **New**, **Package**. In the **Open** dialog box, enter the UNC path of the shared folder that contains the AWS CLI installer (e.g. `\\FS1\Installers`) and select the AWS CLI installer. In the **Deploy Software** dialog box, choose **Assigned**, **OK**.



7. Open the context (right-click) menu for the AWS CLI package just created and choose **Properties**. In the properties dialog box, choose the **Deployment** tab. For **Deployment options**, choose **Install this application at logon**. For **Installation user interface options**, choose **Basic**. Choose **OK**.
8. Close the **Group Policy Management Editor** dialog box.

Results

The next time the user that belongs to the **Developers** OU logs in to their WorkSpace, the AWS CLI is installed. You can verify the installation by opening a command prompt on the WorkSpace and running the following command:

```
D:\Users\johndoe>aws --version
```

If the AWS CLI is not installed, an error is returned. Otherwise, the version information is displayed.

Tutorial: Create a Custom Bundle

The following procedure takes you through all of the steps needed to create a custom bundle, update that bundle, and update a WorkSpace that was created from the bundle.

Topics

Prerequisites

This tutorial assumes the following:

- You have an active AWS account.
- You have an existing Simple AD or AD Connector directory.
- Your AWS account has the capacity to create two WorkSpaces. You can request an increase in this limit by using the Amazon WorkSpaces Limits form.
- Your AWS account has the capacity to create two WorkSpace images in your directory.
- The WorkSpaces in your directory have access to the Internet. For more information, see Simple AD Directory Internet Access (p. 16) or AD Connector Directory Internet Access (p. 21).

Step 1: Create the Image

Launch a WorkSpace, customize the WorkSpace, and create an image of the WorkSpace.

Note
When you create an image, the following items are captured from the WorkSpace:

- All items in the C:\ drive
- All items in D:\Users\<*user_name*>, except for the following folders, which are copied to C:\Users\Default:
  - Contacts
  - Downloads
  - Favorites
  - Music
  - Pictures
  - Saved games
  - Videos
  - Podcasts
  - Virtual machines
  - Temporary folders
  - Cache folders
- All registry entries from the HKey current user (HKCU), which are also copied to the default user

To create the image

1. Create two WorkSpaces users in your directory, one with the username `image_gen`, and another with the username `bundle_user`.
2. Following the procedure in Launching a WorkSpace (p. 51), launch a WorkSpace that is assigned to `image_gen`. The WorkSpace infrastructure type is not important because the infrastructure type of the bundle is set when the bundle is created. To reduce the cost of this WorkSpace, you should select the most inexpensive infrastructure type. If you need the Plus package in the bundle, select that as well.
3. When the `image_gen` WorkSpace is available, connect to it.
4. On the `image_gen` WorkSpace, perform the following:
   - Install Notepad++ from http://notepad-plus-plus.org/.
   - Add a bookmark to `http://aws.amazon.com/documentation/` to Mozilla Firefox.

- Download and install all operating system and application updates and patches.
- Delete all browser history, cached content, and cookies.

5. Log off of the `image_gen` WorkSpace.
6. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
7. In the navigation pane, choose **WorkSpaces** and choose the `image_gen` WorkSpace.
8. Choose **Actions**, **Create Image**.
9. In the **Create WorkSpace Image** dialog box, enter the following information and choose **Create Image**.

   Image Name
   `Image 1`

   Description
   `My first image`

   It can take up to an hour for the image to be created. After the image is created, proceed to Step 2: Create the Bundle (p. 90).

Step 2: Create the Bundle

Create a custom bundle from the WorkSpace image.

To create the bundle

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpace Images**.
3. Choose the **Image 1** image, **Actions**, **Create Bundle**.
4. In the **Create WorkSpace Bundle** dialog box, enter the following information and choose **Create Bundle**.

   Bundle Name
   `Bundle 1`

   Description
   `My first bundle`

   Hardware Type
   Value

After the bundle is created, proceed to Step 3: Launch a WorkSpace from the Bundle (p. 90).

Step 3: Launch a WorkSpace from the Bundle

Launch a WorkSpace from the custom bundle and verify that the WorkSpace contains the changes made to the image.

To launch a WorkSpace from a custom bundle and verify the image

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpace Bundles**.
3. Select the bundle from which to create the WorkSpace and choose **Launch WorkSpace**.
4. Proceed with the steps to launch the WorkSpace. When selecting the user for which to launch the WorkSpace, choose `bundle_user`.

5. When the `bundle_user` WorkSpace is available, connect to it using any of the WorkSpaces client applications.
6. On the `bundle_user` WorkSpace, verify the following:

   - Notepad++ is installed and operational.
   - Mozilla Firefox contains a bookmark to `http://aws.amazon.com/documentation/`.

Step 4: Modify the Image

Modify the image.

1. Connect to the `image_gen` WorkSpace.
2. On the `image_gen` WorkSpace, make the following changes:

   - Install the Google Chrome browser from http://www.google.com/chrome/browser/.
   - Add a file to the My Documents folder called `Text Document.txt`. Open `Text Document.txt` in a text editor, add the following text to the file, and save the file.

     ```
     The quick brown fox jumps over the lazy dog.
     ```
3. Log off from the `image_gen` WorkSpace. Do not shut down the WorkSpace.
4. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
5. In the navigation pane, choose **WorkSpaces** and choose the `image_gen` WorkSpace.
6. Choose **Actions**, **Create Image**.
7. In the **Create WorkSpace Image** dialog box, enter the following information and choose **Create Image**.

   Image Name
   `Image 2`
   Description
   `My second image`

   It can take up to an hour for the image to be created. After the image is created, proceed to Step 5: Update the Bundle (p. 91).

Step 5: Update the Bundle

Update the custom bundle to use the updated image.

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.
2. In the navigation pane, choose **WorkSpace Bundles**.
3. On the **WorkSpace Bundles** page, choose `Bundle 1`, **Actions**, **Update Bundle**.
4. In the **Update WorkSpace Bundle** dialog box, choose **Image 2**, **Update Bundle**.

   The **Image Name** for `Bundle 1` is updated to **Image 2**. Proceed to Step 6: Rebuild the Custom Bundle WorkSpace (p. 91).

Step 6: Rebuild the Custom Bundle WorkSpace

Rebuild an existing WorkSpace to update it to the new image.

1. Open the Amazon WorkSpaces console at https://console.aws.amazon.com/workspaces/.

2. In the navigation pane, choose **WorkSpaces**.
3. Select the `bundle_user` WorkSpace, choose **Actions**, **Rebuild WorkSpace**.

   When the `bundle_user` WorkSpace is running again, proceed to the next step.
4. When the rebuilt `bundle_user` WorkSpace is available, connect to it using any of the WorkSpaces client applications.
5. On the `bundle_user` WorkSpace, verify the following:

   - Notepad++ is installed and operational.
   - Mozilla Firefox contains a bookmark to `http://aws.amazon.com/documentation/`.
   - The Google Chrome browser is installed and operational.
   - The file `Text Document.txt` exists in your My Documents folder, and contains the following text:

     ```
     The quick brown fox jumps over the lazy dog.
     ```
6. Congratulations! You have successfully completed this tutorial. You can safely delete the following objects if you no longer need them.

   - The `bundle_user` WorkSpace.
   - The `image_gen` WorkSpace.
   - The `Bundle 1` bundle.
   - The `Image 1` image.
   - The `Image 2` image.
   - The `image_gen` and `bundle_user` users. These users need to be deleted using your preferred Active Directory management tools.

Amazon WorkSpaces Client Help

Client applications are available for the following platforms and devices:

- Microsoft Windows 7, Windows 8, and Windows 10
- Apple Mac OS X 10.8.1 and later
- Apple iPad 2, 3, and 4 with iOS 7.0 and later
- Apple iPad Retina with iOS 7.0 and later
- Apple iPad Mini with iOS 7.0 and later
- Apple iPad Pro with iOS 9.0 and later
- Amazon Fire tablets released after 2012 with Fire OS 4.0 and later
- Samsung and Nexus tablets with Android OS 4.2 and later
- Chromebook with Chrome OS version 45 and later

Most keyboards and pointing devices are supported by the Amazon WorkSpaces client applications. This includes many different types of USB and Bluetooth input devices. If you encounter an issue with a particular device, report the problem at https://console.aws.amazon.com/support/home#/. Other locally attached peripherals, such as storage devices, are not supported.

Completing Your User Profile

When your user account is first created, you need to use the registration link specified in the welcome email to complete your user profile. You must complete your registration within seven days of the email being sent; otherwise, the invitation expires and your administrator will have to send another invitation. Your username and email address cannot be changed, but you can change your first name and last name. You must also set your password for the account. The password is case-sensitive and must be between 8 and 64 characters in length, inclusive. It must also contain at least one character from three of the following categories:

- Lowercase characters (a-z)
- Uppercase characters (A-Z)

- Numbers (0-9)
- Non-alphanumeric characters (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Enter your information in the page and choose **Update User**.

After you have completed your user registration, you can download the Amazon WorkSpaces client applications from Amazon WorkSpaces Client Downloads.

Amazon WorkSpaces Client Prerequisites

Your Amazon WorkSpaces users access their workspaces using a client device. To provide your users with a good experience using Amazon WorkSpaces, they must meet the following minimum system requirements.

- To run the Amazon WorkSpaces client application, users must have a PC, Mac, iPad, Kindle, Android tablet, or Chromebook. To run Amazon WorkSpaces Web Access, they must have a PC or Mac running a Chrome or Firefox web browser.
- The client device must have a broadband Internet connection.
- The network that the client is connected to, and any firewall on the client itself, must have certain ports open to the IP address ranges for various AWS services. These same ports must also be open on any firewall that is running on the client as well. Some networks may have some or all of these ports closed. In this case, you will need to work with your network administrators to have these ports enabled. For more information, see Client Ports (p. 12).
- A round trip time (RTT) to the region that your WorkSpaces are in of less than 100ms is suggested. For more information, and to test the network latency, see Latency Threshold (p. 94).
- If your users are accessing a WorkSpace through a virtual private network (VPN), the connection must support a maximum transmission unit (MTU) of at least 1200 bytes. For more information, see MTU Threshold (p. 95).
- The Amazon WorkSpaces client applications require HTTPS access to Amazon WorkSpaces resources hosted by the service and Amazon Simple Storage Service (Amazon S3). The Amazon WorkSpaces client applications do not support proxy redirection at the application level. This is required to successfully register and use the Amazon WorkSpaces client application. For more information, see HTTPS Access (p. 95).

You can verify that all of these requirements are met by performing the following steps:

To test client network access

1. Open a Amazon WorkSpaces client and type your registration code.
2. Choose **Network** in the lower right corner of the client application. The client application tests the network connection, ports, and round trip time and reports the results of these tests.
3. Choose **Dismiss** to return to the login page.

Latency Threshold

As with any networking service, network latency has an effect on the performance of the Amazon WorkSpaces client applications. For optimal performance, the round trip time (RTT) from the client's network to the region that your WorkSpaces are in should be less than 100ms. The Amazon WorkSpaces client applications remains functional with an RTT between 100ms and 250ms, although performance is degraded.

MTU Threshold

If you are accessing a WorkSpace through a virtual private network (VPN), your connection must support a maximum transmission unit (MTU) of at least 1200 bytes.

HTTPS Access

The Amazon WorkSpaces client applications require HTTPS access to Amazon WorkSpaces resources hosted by the service and Amazon S3. This is required to successfully register and use the Amazon WorkSpaces client application.

Amazon WorkSpaces Windows Client Help

The following information will help you get started with the Amazon WorkSpaces Windows client application.

Contents

Setup and Installation

Download and install the Windows client application from Amazon WorkSpaces Client Downloads.

Connecting to Your WorkSpace

To connect to your WorkSpace, complete the following procedure.

To connect to your WorkSpace

1. The first time that you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and choosing **Options**, **Register** on the login screen menu.
2. Enter your username and password in the login screen and choose **Sign In**. If your Amazon WorkSpaces administrator has enabled multi-factor authentication for your organization's WorkSpaces, you are prompted for a passcode to complete your login. Your Amazon WorkSpaces administrator will provide more information about how to obtain your passcode.
3. If your Amazon WorkSpaces administrator has not disabled the "Remember Me" feature, you are prompted to save your credentials securely so that you can connect to your WorkSpace easily while the client application remains running. Your credentials are securely cached up to the maximum lifetime of your Kerberos ticket.

After the client application connects to your WorkSpace, your WorkSpace desktop is displayed.

4. (Optional) If your WorkSpace uses an AD Connector directory, you can update the maximum lifetime of the Kerberos ticket by following the steps in Configuring Kerberos Policies in the Microsoft TechNet Library. If you need to disable the "Remember Me" feature, search for help in the Amazon WorkSpaces forum.

An interruption of network connectivity causes an active session to be disconnected. This can be caused by events such as closing the laptop lid, or the loss of your wireless network connection. The Amazon WorkSpaces client application for Windows attempts to reconnect the session automatically if network connectivity is regained within a certain amount of time. The default session resume timeout is 20 minutes, but this timeout may be modified by your network administrator through your domain's Group Policy settings. For more information, see Setting the Session Resume Timeout (p. 70).

Client Views

You can switch to full screen mode by choosing **View**, **Show Fullscreen** in the client application menu.

While in full screen mode, you can switch back to window mode by moving the mouse cursor to the top of the screen. The client application menu is displayed, and you can choose **View**, **Exit Fullscreen** in the client application menu.

The Amazon WorkSpaces Windows client application supports no more than two monitors. The client application automatically uses both monitors when it goes into full-screen mode. The maximum supported resolution of each monitor is 2560x1600 pixels.

Client Language

You can select the language displayed by the client by performing the following steps.

> **Note**
> In the client, Japanese is available in all regions. However, Japanese is only available in Tokyo for individual WorkSpaces.

To select the client language

1. In the Amazon WorkSpaces client application, open the **Advanced Settings** dialog box.
2. Enter your desired language in the **Select a language** list and choose **Save**.
3. Restart the client.

Proxy Server

If your network requires you to use a proxy server to access the Internet, you can enable the Amazon WorkSpaces client application to use a proxy for HTTPS (port 443) traffic. Proxy with authentication is not currently supported.

> **Note**
> The Amazon WorkSpaces client applications use the HTTPS port for updates, registration, and authentication. The desktop streaming connections to the WorkSpace require port 4172 to be enabled, and do not go through the proxy server.

To use a proxy server

1. In the Amazon WorkSpaces client application, open the **Advanced Settings** dialog box.
2. In the **Proxy Server Setting** area, check **Use Proxy Server**, enter the proxy server address and port, and choose **Save**.

Command Shortcuts

The Amazon WorkSpaces Windows client supports the following command shortcuts:

- Ctrl+Alt+Enter - Toggle fullscreen display
- Ctrl+Alt+F12 - Disconnect session

Troubleshooting

After logging in, the client application only displays a white page and I cannot connect to my WorkSpace.

This problem can be caused by expired VeriSign/Symantec certificates on your client computer (not your WorkSpace). Remove the expired certificate and launch the client application again.

To find and remove expired VeriSign/Symantec certificates

1. In the Windows **Control Panel**, choose **Internet Options**.
2. In the **Internet Properties** dialog box, choose **Content**, **Certificates**.
3. In the **Certificates** dialog box, choose the **Intermediate Certificate Authorities** tab. In the list of certificates, select all certificates that were issued by VeriSign or Symantec that are also expired, and choose **Remove**. Do not remove any certificates that are not expired.
4. On the **Trusted Root Certificate Authorities** tab, select all certificates that were issued by VeriSign or Symantec that are also expired, and choose **Remove**. Do not remove any certificates that are not expired.
5. Close the **Certificates** dialog box as well as the **Internet Properties** dialog box.

Amazon WorkSpaces OS X Client Help

The following information will help you get started with the Amazon WorkSpaces OS X client application.

Contents

Setup and Installation

The Amazon WorkSpaces OS X client application requires the following:

- Mac OS X 10.8.1 or later

Download and install the Amazon WorkSpaces OS X client from Amazon WorkSpaces Client Downloads.

Connecting to Your WorkSpace

To connect to your WorkSpace, complete the following procedure.

To connect to your WorkSpace

1. The first time that you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and choosing **Options**, **Register** in the upper-left corner on the login screen menu.
2. Enter your username and password in the login screen and choose **Sign In**. If your Amazon WorkSpaces administrator has enabled multi-factor authentication for your organization's WorkSpaces, you are prompted for a passcode to complete your login. Your Amazon WorkSpaces administrator will provide more information about how to obtain your passcode.
3. If your Amazon WorkSpaces administrator has not disabled the "Remember Me" feature, you are prompted to save your credentials securely so that you can connect to your WorkSpace easily while the client application remains running. Your credentials are securely cached up to the maximum lifetime of your Kerberos ticket.

   After the client application connects to your WorkSpace, your WorkSpace desktop is displayed.
4. (Optional) If your WorkSpace uses an AD Connector directory, you can update the maximum lifetime of the Kerberos ticket by following the steps in Configuring Kerberos Policies in the Microsoft TechNet Library. If you need to disable the "Remember Me" feature, search for help in the Amazon WorkSpaces forum.

An interruption of network connectivity causes an active session to be disconnected. This can be caused by events such as closing the laptop lid, or the loss of your wireless network connection. The Amazon WorkSpaces client application for OS X attempts to reconnect the session automatically if network connectivity is regained within a certain amount of time. The default session resume timeout is 20 minutes, but this timeout may be modified by your network administrator through your domain's Group Policy settings. For more information, see Setting the Session Resume Timeout (p. 70).

Client Views

You can switch to full screen mode by choosing **View**, **Show Fullscreen** in the client application menu.

While in full screen mode, you can switch back to window mode by moving the mouse cursor to the top of the screen. The client application menu is displayed, and you can choose **View**, **Exit Fullscreen** in the client application menu.

The Amazon WorkSpaces OS X client application supports up to two monitors. The client application automatically uses the first two monitors when it goes into full-screen mode. The maximum supported resolution of each monitor is 2560x1600 pixels.

Client Language

You can select the language displayed by the client by performing the following steps.

> **Note**
> In the client, Japanese is available in all regions. However, Japanese is only available in Tokyo for individual WorkSpaces.

To select the client language

1. In the Amazon WorkSpaces client application, open the **Advanced Settings** dialog box.

2. Enter your desired language in the **Select a language** list and choose **Save**.
3. Restart the client.

Proxy Server

If your network requires you to use a proxy server to access the Internet, you can enable the Amazon WorkSpaces client application to use a proxy for HTTPS (port 443) traffic. Proxy with authentication is not currently supported.

> **Note**
> The Amazon WorkSpaces client applications use the HTTPS port for updates, registration, and authentication. The desktop streaming connections to the WorkSpace require port 4172 to be enabled, and do not go through the proxy server.

To use a proxy server

1. In the Amazon WorkSpaces client application, open the **Advanced Settings** dialog box.
2. In the **Proxy Server Setting** area, check **Use Proxy Server**, enter the proxy server address and port, and choose **Save**.

Command Shortcuts

The Amazon WorkSpaces OS X client supports the following command shortcuts:

- Control+Option+Return—Toggle fullscreen display
- Control+Option+F12—Disconnect session

Amazon WorkSpaces iPad Client Help

The following information will help you get started with the Amazon WorkSpaces iPad client application.

Contents

Setup and Installation

The Amazon WorkSpaces iPad client application requires the following:

- An iPad 2 or iPad Retina with iOS 7.0 or later.

To download and install the client application, complete the following procedure.

To download and install the client application

1. On your iPad, search the App Store for the Amazon WorkSpaces client application.
2. Download and install the application.
3. Verify that the Amazon WorkSpaces client application icon appears on one of the iPad desktops.

Connecting to Your WorkSpace

To connect to your WorkSpace, complete the following procedure.

To connect to your WorkSpace

1. On your iPad, open the Amazon WorkSpaces client application.
2. The first time that you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and choosing **Enter new registration code** on the login screen.
3. Enter your username and password and choose **Sign In**. If your Amazon WorkSpaces administrator has enabled multi-factor authentication for your organization's WorkSpaces, you are prompted for a passcode to complete your login. Your Amazon WorkSpaces administrator will provide more information about how to obtain your passcode.
4. If your Amazon WorkSpaces administrator has not disabled the "Remember Me" feature, you are prompted to save your credentials securely so that you can connect to your WorkSpace easily in the future. Your credentials will be securely cached up to the maximum lifetime of your Kerberos ticket.

   After the client application connects to your WorkSpace, your WorkSpace desktop is displayed.

   (Optional) If your WorkSpace uses an AD Connector directory, you can update the maximum lifetime of the Kerberos ticket by following the steps in Configuring Kerberos Policies in the Microsoft TechNet Library. If you need to disable the "Remember Me" feature, search for help in the Amazon WorkSpaces forum.

Gestures

The following are the gestures that are supported for the Amazon WorkSpaces iPad client application.

Single tap

Equivalent to a single click in Windows.

Double tap

Equivalent to a double click in Windows.

Two finger single tap

Equivalent to a right-click in Windows.

Two finger double tap

Toggles the on-screen keyboard display.

Swipe from left

Displays the radial menu. For more information, see Radial Menu (p. 101)

Two finger scroll

Scrolls vertically.

Two finger pinch

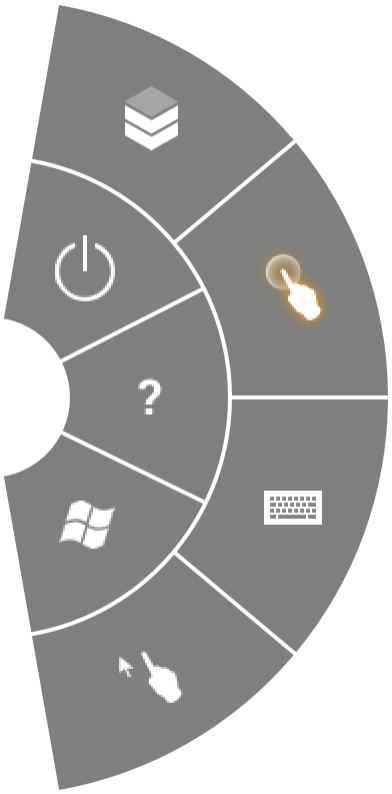
Zooms display in or out.

Two finger pan

Pans the desktop when zoomed in.

Radial Menu

The radial menu is displayed by swiping from the left side of the screen.



The radial menu provides quick access to the following features:

Connection Status

Displays the connection status.

Disconnect

Allows you to disconnect the client application without logging off.

Direct Mouse Mode

Sets the input to direct mouse mode. For more information, see Mouse Modes (p. 103).

Help

Displays the command and gesture tutorial.

Keyboard

Toggles the display of the on-screen keyboard.

Windows Start Menu

Displays the Windows Start Menu.

Offset Mouse Mode

Sets the input to offset mouse mode. For more information, see Mouse Modes (p. 103).

Keyboard

To toggle the display of the on-screen keyboard, double-tap with two fingers anywhere on the screen. Special key combinations are displayed in the top row of the keyboard.

Mouse Modes

The mouse mode is set using the radial menu (p. 101).

Direct Mode

In direct mouse mode, the mouse cursor is placed wherever you tap your finger. In this mode, a single tap is equivalent to a left mouse button click and a two finger single tap is equivalent to a right mouse button click.

Offset Mode

In offset mouse mode, the mouse cursor tracks the movement of your finger on the screen. In this mode, simulate a left mouse button click by tapping the left mouse button icon.

Simulate a right mouse button click by tapping the right mouse button icon.

Disconnect

To disconnect the iPad client, display the radial menu, tap the disconnect icon, and tap **Disconnect**. You can also log off the WorkSpace, which disconnects the client.

Amazon WorkSpaces Android Client Help

The following information will help you get started with the Amazon WorkSpaces Android client application.

Contents

Requirements

The Amazon WorkSpaces Android client application requires the following:

- Amazon Kindle Fire HDX or Kindle HD 7
- A Samsung or Nexus tablet with Android OS 4.2 and later. The Amazon WorkSpaces Android client application works on most Android tablets with Android version 4.2 or later, but there may be some devices that are not compatible. If you encounter any problems with your particular device, please report the problem in the Amazon WorkSpaces forum.

Setup and Installation

To download and install the client application, complete the following procedure.

To download and install the client application

1. On your tablet, go to http://clients.amazonworkspaces.com/ and choose the link for your tablet.
2. Download and install the application.
3. Verify that the Amazon WorkSpaces client application icon appears on one of the tablet desktops.

Connecting to Your WorkSpace

To connect to your WorkSpace, complete the following procedure.

To connect to your WorkSpace

1. On your tablet, open the Amazon WorkSpaces client application.
2. The first time that you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and username to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and tapping **Enter new registration code** on the login screen.
3. Enter your username and password and tap **Sign In**. If your Amazon WorkSpaces administrator has enabled multi-factor authentication for your organization's WorkSpaces, you are prompted for a passcode to complete your login. Your Amazon WorkSpaces administrator will provide more information about how to obtain your passcode.
4. If your Amazon WorkSpaces administrator has not disabled the "Remember Me" feature, you are prompted to save your credentials securely so that you can connect to your WorkSpace easily in the future. Your credentials will be securely cached up to the maximum lifetime of your Kerberos ticket.

   After the client application connects to your WorkSpace, your WorkSpace desktop is displayed.

   (Optional) If your WorkSpace uses an AD Connector directory, you can update the maximum lifetime of the Kerberos ticket by following the steps in Configuring Kerberos Policies in the Microsoft TechNet Library. If you need to disable the "Remember Me" feature, search for help in the Amazon WorkSpaces forum.

Gestures

The following are the gestures that are supported for the Amazon WorkSpaces Android client application.

Single tap

Equivalent to a single click in Windows.

Double tap

Equivalent to a double click in Windows.

Two finger single tap

Equivalent to a right-click in Windows.

Two finger double tap

Toggles the on-screen keyboard display.

Swipe from left

Displays the radial menu. For more information, see Radial Menu (p. 105)

Two finger scroll

Scrolls vertically.

Two finger pinch

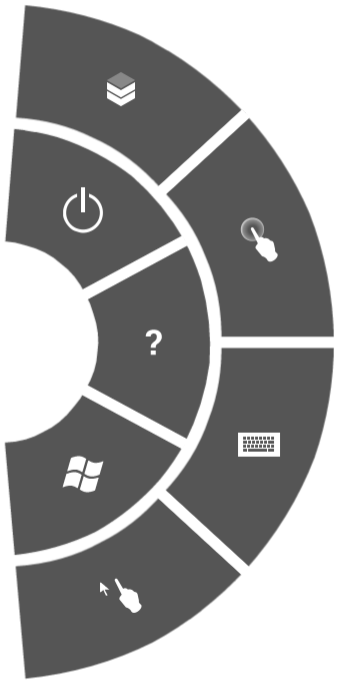
Zooms display in or out.

Two finger pan

Pans the desktop when zoomed in.

Radial Menu

The radial menu is displayed by swiping from the left side of the screen.



The radial menu provides quick access to the following features:

Connection Status

Displays the connection status.

Disconnect

Allows you to disconnect the client application without logging off.

Direct Mouse Mode

Sets the input to direct mouse mode. For more information, see Mouse Modes (p. 107).

Help

Displays the command and gesture tutorial.

Keyboard

Toggles the display of the on-screen keyboard.

Windows Start Menu

Displays the Windows Start Menu.

Offset Mouse Mode

Sets the input to offset mouse mode. For more information, see Mouse Modes (p. 107).

Keyboard

To toggle the display of the on-screen keyboard, double-tap with two fingers anywhere on the screen. Special key combinations are displayed in the top row of the keyboard.

Mouse Modes

The mouse mode is set using the radial menu (p. 105).

Direct Mode

In direct mouse mode, the mouse cursor is placed wherever you tap your finger. In this mode, a single tap is equivalent to a left mouse button click and a two finger single tap is equivalent to a right mouse button click.

Offset Mode

In offset mouse mode, the mouse cursor tracks the movement of your finger on the screen. In this mode, simulate a left mouse button click by tapping the left mouse button icon.

Simulate a right mouse button click by tapping the right mouse button icon.

Disconnect

To disconnect the Android client, display the radial menu, tap the disconnect icon, and tap **Disconnect**. You can also log off the WorkSpace, which disconnects the client.

Amazon WorkSpaces Chromebook Client Help

The following information will help you get started with the Amazon WorkSpaces Chromebook client application.

Contents

Setup and Installation

The Amazon WorkSpaces Chromebook client application requires the following:

- A Chromebook with Chrome OS version 45 or later. The Amazon WorkSpaces Chromebook client application works on most Chromebooks with version 45 or later, but there may be some devices

that are not compatible. If you encounter any problems with your particular device, report the problem in the Amazon WorkSpaces forum.

To download and install the client application, complete the following procedure.

To download and install the client application

1. On your Chromebook, go to http://clients.amazonworkspaces.com/ and choose the link for your Chromebook.
2. Download and install the application.
3. Verify that the Amazon WorkSpaces client application icon appears in your Chromebook search.

Connecting to Your WorkSpace

To connect to your WorkSpace, complete the following procedure.

To connect to your WorkSpace

1. On your Chromebook, open the Amazon WorkSpaces client application.
2. The first time that you run the client application, you are prompted for your registration code, which is contained in your welcome email. The Amazon WorkSpaces client application uses the registration code and user name to identify which WorkSpace to connect to. When you launch the client application later, the same registration code is used. You can enter a different registration code by launching the client application and choosing **Enter new registration code** on the login screen.
3. Enter your user name and password and choose **Sign In**. If your Amazon WorkSpaces administrator has enabled multi-factor authentication for your organization's WorkSpaces, you are prompted for a passcode to complete your login. Your Amazon WorkSpaces administrator will provide more information about how to obtain your passcode.
4. If your Amazon WorkSpaces administrator has not disabled the "Remember Me" feature, you are prompted to save your credentials securely so that you can connect to your WorkSpace easily in the future. Your credentials are securely cached while the application is running.

   After the client application connects to your WorkSpace, your WorkSpace desktop is displayed.

   (Optional) If your WorkSpace uses an AD Connector directory, you can update the maximum lifetime of the Kerberos ticket by following the steps in Configuring Kerberos Policies in the Microsoft TechNet Library. If you need to disable the "Remember Me" feature, search for help in the Amazon WorkSpaces forum.

Gestures

The following are the gestures that are supported for the Amazon WorkSpaces Chromebook client application.

Single tap

Equivalent to a single click in Windows.

Double tap

Equivalent to a double click in Windows.

Two finger single tap

Equivalent to a right-click in Windows.

Two finger scroll

Scrolls vertically.

Amazon WorkSpaces Web Access

Users can access their WorkSpaces from any location using a web browser. This is ideal for users who must use a locked-down device or restrictive network. Instead of using a traditional remote access solution and installing the appropriate client application, users can visit the website to access their work resources.

Website

If you have Amazon WorkSpaces Web Access enabled, open Amazon WorkSpaces Web Access to log on to your WorkSpace through your web browser.

Requirements

The following operating systems are supported:

- Windows
- Mac
- Linux

The following web browsers are supported:

- Chrome 53 and later
- Firefox 49 and later

You must have web connectivity.

Client Views

Amazon WorkSpaces Web Access supports multiple screen resolutions. The minimum supported resolution is 960x720 pixels, and the maximum supported resolution is 2560x1600 pixels.

Proxy Servers

If you are required to use a proxy server to access the Internet, you can configure your browser to use the proxy server. Amazon WorkSpaces Web Access respects the settings for all related traffic.

Limits

- Proxy with authentication is not currently supported.
- Proxy server support for Web Access can vary by browser. Chrome (versions 55 and later) supports Web Access traffic routed through a web proxy, while the current Firefox does not.

PCoIP Zero Client Help

You can set up and use a PCoIP zero client device with Amazon WorkSpaces. For more information, see *Connecting to Amazon WorkSpaces Desktops* in the PCoIP Connection Manager User Guide.

Requirements

To use a PCoIP zero client with Amazon WorkSpaces, you need the following:

- An EC2 instance with Teradici PCoIP Connection Manager for Amazon WorkSpaces. This is set up by your Amazon WorkSpaces administrator. Your administrator provides you with the server URI you need to connect to your WorkSpace. For more information, see Enabling PCoIP Zero Client (p. 71).
- A Tera2 zero client device that has firmware version 4.6.0 or later.

Set Up the Zero Client Connection

Before you connect your zero client device to your WorkSpace for the first time, you might need to change some settings. Your Amazon WorkSpaces administrator can provide you with additional setup instructions that are needed for your particular environment.

Session Connection

To set the session connection

1. From the PCoIP zero client device, choose **Options**, **Configuration**, and **Session**.
2. If the page is locked, choose **Unlock** and enter your zero client password (if required).
3. For **Connection Type**, choose **PCoIP Connection Manager**.
4. For **Server URI**, copy the server URI provided by your administrator, and then choose **OK**.

Connect to Your WorkSpace

To connect to your WorkSpace

1. From the PCoIP zero client device, choose **PCoIP Connection Manager for Amazon WorkSpaces** for **Server**, and then choose **Connect**.
2. On the login page, type your Amazon WorkSpaces user name and password, and choose **Login**.

Disconnect from the Zero Client

To disconnect the zero client from your WorkSpace, you can press Ctrl+Alt+F12. Alternatively, you can log off the WorkSpace, which disconnects the client.

Printing From a WorkSpace

The following printing methods are supported by Amazon WorkSpaces.

Printing Methods

- Local Printers (p. 111)

- Other Printing Methods (p. 111)

Local Printers

Amazon WorkSpaces supports local printer redirection. When you print from an application in your WorkSpace, the local printers are contained in your list of available printers. The local printers have "(Local – *<workspace username>*.*<directory name>*.*<client computer name>*)" appended to the printer's display name. Select one of the local printers and your documents are printed on that printer.

In some cases, you need to download and install the driver for your local printer manually on the WorkSpace. When you install a printer driver on your WorkSpace, there are different types of drivers that you may encounter:

- Add Printer wizard driver. This driver includes only the printer drivers, and are for users who are familiar with installation using the Add Printer wizard in Windows.
- Printer model-specific drivers which do not require communication with the printer. In these cases, you can install the printer driver directly.
- Printer model-specific drivers which require communication with the printer. In these cases, you can use the printer driver files to add a local printer using an existing port (LPT1:). After selecting the port, you can choose **Have Disk** and select the `.INF` file for the printer driver.

After installing the printer driver, you must restart the WorkSpace for the new printer to be recognized.

If you cannot print to your local printer from your WorkSpace, make sure you can print to your local printer from your client computer. If you cannot print from your client computer, refer to the printer documentation and support to resolve the issue. If you can print from your client computer, contact AWS Support for further assistance.

Other Printing Methods

You can also use one of the following methods to print from a WorkSpace:

- In a connected directory, you can attach your WorkSpace to network printers that are exposed through Active Directory.
- Use a cloud printing service, such as Google Cloud Print or HP Mobile Printing.
- Print to a file, transfer the file to your local desktop, and print the file locally to an attached printer.

Amazon WorkDocs Sync Client Help

Amazon WorkDocs provides a client synchronization application that allows you to continuously, automatically, and securely back up documents from your WorkSpaces to the Amazon WorkDocs service. For more information about Amazon WorkDocs, see Amazon WorkDocs Sync Client Help in the *Amazon WorkDocs Administration Guide*.

Troubleshooting Amazon WorkSpaces Client Issues

The following are common issues that you might have with your WorkSpaces client.

Issues

My WorkSpaces client gives me a network error, but I am able to use other network enabled apps on my device

The WorkSpaces client applications rely on access to resources in the AWS cloud and require a connection that provides at least 1 Mbps download bandwidth. If your device has an intermittent connection to the network, the WorkSpaces client application may report an issue with the network.

It sometimes takes several minutes to log in to my WorkSpace

Group Policy settings set by your system administrator can cause a delay on login after your WorkSpace has been launched or rebooted. This delay occurs while the Group Policy settings are being applied to the WorkSpace and is normal.

Sometimes I am logged off of my WorkSpace, even though I closed the session, but did not log off

Your system administrator applied a new or updated Group Policy setting to your WorkSpace that requires a logoff of a disconnected session.

I can't connect to the Internet from my WorkSpace

WorkSpaces cannot communicate with the Internet by default. Your administrator must explicitly provide Internet access. For more information about providing Internet access to your WorkSpace, see Simple AD Directory Internet Access (p. 16) or AD Connector Directory Internet Access (p. 21).

I installed a third-party security software package and now I can't connect to my WorkSpace

You can install any type of security or firewall software on your WorkSpace, but Amazon WorkSpaces requires that certain inbound and outbound ports are open on the WorkSpace. If the security or firewall software that you install blocks these ports, the WorkSpace might not function correctly or might

become unreachable. For more information about the ports that must be open to your WorkSpace, see Management Interface Ports (p. 2) and Primary Interface Ports (p. 3).

To restore your WorkSpace, ask your administrator to rebuild your WorkSpace. You will have to re-install the software and properly configure port access for your WorkSpace.

I am getting a 'network connection is slow' warning when connected to my WorkSpace

If the roundtrip time from your client to your WorkSpace is longer than 100ms, you can still use your WorkSpace, but this may result in a poor experience. A slow roundtrip time can be caused by many factors, but the following are the most common:

- You are too far from the AWS region that your WorkSpace resides in. For the best WorkSpace experience, you should be within 2000 miles of the AWS region that your WorkSpace is in.
- Your network connection is inconsistent or slow. For the best experience, your network connection should provide at least 300 kbps, with capability to provide over 1 Mbps when viewing video or using graphics intensive applications on your WorkSpace.

I got an invalid certificate error on the client application. What does that mean?

The WorkSpaces client application validates the identity of the WorkSpaces service through an SSL certificate. If the root certificate authority of the Amazon WorkSpaces service cannot be verified, the client application displays an error and prevents any connection to the service. The most common cause is a proxy server that is removing the root certificate authority and returning an incomplete certificate to the client application. Contact your network administrator for additional help.

I see the following error message: "Your device is not able to connect to the WorkSpaces Registration service."

When registration service failure occurs, you might see the following error message on the **Connection Health Check** page: "Your device is not able to connect to the WorkSpaces Registration service. You will not be able to register your device with WorkSpaces. Please check your network settings."

This error occurs when the WorkSpaces client application can’t reach the registration service. Typically, this happens when the WorkSpaces directory has been deleted. To resolve this error, make sure that the registration code is valid and corresponds to a running directory in the AWS cloud. For more information, see Advanced Setup (p. 37).

Amazon WorkSpaces Limits

The following are the limits for Amazon WorkSpaces, per region. To request a limit increase, use the Amazon WorkSpaces Limits form.

Resource	Limit
WorkSpaces	1
Images	5

Document History

The following table describes important additions to the Amazon WorkSpaces service and its documentation set. We also update the documentation frequently to address the feedback that you send us.

Change	Description	Date Changed
Windows Server 2016 bundles	Amazon WorkSpaces now offers bundles that come with a Windows 10 desktop experience, powered by Windows Server 2016.	November 29, 2016
Web access	Access your WorkSpaces from a web browser. For more information, see Amazon WorkSpaces Web Access (p. 109).	November 18, 2016
Hourly WorkSpaces	You can configure your WorkSpaces so that users are billed by the hour.	August 18, 2016
Windows 10 BYOL	Bring your Windows 10 Desktop License to Amazon WorkSpaces (BYOL). For more information, see Use Your Windows Desktop Images (p. 64).	July 21, 2016
Tagging support	You can now use tags to manage and track your WorkSpaces. For more information, see Tag a WorkSpace (p. 57).	May 17, 2016
Saved registrations	Every time you enter a new registration code, the WorkSpaces client stores it. This makes it easier to switch between WorkSpaces in different directories or regions. For more information, see Client Application Registration (p. 36).	January 28, 2016
Microsoft AD support	Multiple additions for Microsoft AD support.	December 3, 2015
Windows 7 BYOL Chromebook client WorkSpace encryption	Bring your Windows 7 Desktop License to Amazon WorkSpaces (BYOL). For more information, see Use Your Windows Desktop Images (p. 64). Chromebook client added. For more information, see Amazon WorkSpaces Chromebook Client Help (p. 107).	October 1, 2015

Change	Description	Date Changed
	WorkSpace encryption. For more information, see Encrypt a WorkSpace (p. 54).	
Add CloudWatch monitoring	Added information about CloudWatch monitoring. For more information, see Monitoring Amazon WorkSpaces Metrics (p. 71).	April 28th, 2015
Automatic session reconnect	Added information about the auto session reconnect feature in the WorkSpaces desktop client applications. For more information, see the following topics: • Connecting to Your WorkSpace (p. 95) • Connecting to Your WorkSpace (p. 98) • Setting the Session Resume Timeout (p. 70)	March 31st, 2015
Public IP addresses	Added support for automatically assigning a public IP address to your WorkSpaces. For more information, see the following documentation: • Simple AD Internet Access (p. 43) • AD Connector Internet Access (p. 46)	January 23rd, 2015
Amazon WorkSpaces launched in Asia Pacific (Singapore)	Amazon WorkSpaces is now available in the Asia Pacific (Singapore) region.	January 15th, 2015
Value bundle added Standard bundle updates Office 2013 added	The Value bundle is now available. The Standard bundle hardware has been upgraded. Microsoft Office 2013 is now available in Plus packages.	November 6th, 2014
Image and bundle support	Added support for images and custom bundles. For more information, see the following documentation: • WorkSpace Image Management (p. 61) • WorkSpace Bundle Management (p. 60)	October 28th, 2014
PCoIP zero client support	You can now access Amazon WorkSpaces PCoIP zero client devices. For more information, see the following documentation: • Enabling PCoIP Zero Client (p. 71) • PCoIP Zero Client Help (p. 110)	October 15th, 2014
Amazon WorkSpaces launched in Asia Pacific (Tokyo)	Amazon WorkSpaces is now available in the Asia Pacific (Tokyo) region.	August 26th, 2014
Local printer support	Added support for local printers. For more information, see Printing From a WorkSpace (p. 110).	August 26th, 2014
Multi-factor authentication	Added support for multi-factor authentication in connected directories. For more information, see the following topics: • Multi-factor Authentication Prerequisites (p. 24) • Multi-factor Authentication (p. 47)	August 11th, 2014

Change	Description	Date Changed
Default OU support	You can now select a default Organizational Unit (OU) where your WorkSpace machine accounts are placed. For more information, see the following documenation: **Simple AD Directory** Default Organizational Unit (p. 42) **AD Connector Directory** Target Domain and Default Organizational Unit (p. 45)	July 7th, 2014
Target domain support	You can now select a separate domain where your WorkSpace machine accounts are created. For more information, see Target Domain and Default Organizational Unit (p. 45).	July 7th, 2014
Add security group	The ability to add a security group to your WorkSpaces. For more information, see the following topics: **Simple AD Directory** Add a Security Group (p. 43) **AD Connector Directory** Add a Security Group (p. 46)	July 7th, 2014
Amazon WorkSpaces launched in Asia Pacific (Sydney)	Amazon WorkSpaces is now available in the Asia Pacific (Sydney) region.	May 15th, 2014
Amazon WorkSpaces launched in EU (Ireland)	Amazon WorkSpaces is now available in the EU (Ireland) region.	May 5th, 2014
Public beta	Amazon WorkSpaces is now available as a public beta.	March 25th, 2014