Remote Desktop Gateway on the AWS Cloud

Quick Start Reference Deployment

Santiago Cardenas  
Solutions Architect, AWS Quick Start Team

April 2014  
Last update: March 2020 ([revisions](#_Document_Revisions))

This guide is also available in HTML format at [https://docs.aws.amazon.com/quickstart/latest/rd-gateway/](https://fwd.aws/5VrKP).

Contents

[About This Guide 2](#_Toc35418570)

[Quick Links 3](#_Toc35418571)

[About Quick Starts 3](#_Toc35418572)

[Overview 4](#_Toc35418573)

[Remote Desktop Gateway on AWS 4](#_Toc35418574)

[Cost and Licenses 4](#_Toc35418575)

[AWS Services 5](#_Toc35418576)

[Architecture 6](#_Toc35418577)

[Architectural Considerations 6](#_Toc35418578)

[Initial Remote Administration Architecture 6](#_Toc35418579)

[SSL Certificates 8](#_Toc35418580)

[Connection and Resource Authorization Policies 9](#_Toc35418581)

[Best Practices 9](#_Toc35418582)

[The Principle of Least Privilege 9](#_Toc35418583)

[VPC Configuration 10](#_Toc35418584)

[Network Access Control Lists 10](#_Toc35418585)

[Security Groups 11](#_Toc35418586)

[RD Gateway Architecture on AWS 13](#_Toc35418587)

[Deployment Options 15](#_Toc35418588)

[Deployment Steps 15](#_Toc35418589)

[Step 1. Prepare Your AWS Account 16](#_Toc35418590)

[Step 2. Launch the Quick Start 18](#_Toc35418591)

[Step 3. Perform Post-Deployment Tasks 24](#_Toc35418592)

[Installing the Root Certificate 25](#_Toc35418593)

[Configuring the Remote Desktop Connection Client 26](#_Toc35418594)

[Troubleshooting 28](#_Toc35418595)

[Additional Resources 29](#_Toc35418596)

[Appendix A: Setting up RD Gateway Manually on AWS 30](#_Toc35418597)

[Installing RD Gateway 30](#_Toc35418598)

[Implementing a Self-Signed Certificate 30](#_Toc35418599)

[Configuring Connection and Resource Authorization Policies 33](#_Toc35418600)

[Send Us Feedback 36](#_Toc35418601)

[Document Revisions 36](#_Toc35418602)

## About This Guide

This Quick Start deployment guide includes architectural considerations and configuration steps for deploying Remote Desktop Gateway (RD Gateway) on the Amazon Web Services (AWS) Cloud. It discusses best practices for securely accessing your Windows-based instances using the Remote Desktop Protocol (RDP) for remote administration. The Quick Start includes automated [AWS CloudFormation](https://aws.amazon.com/cloudformation/) templates that you can customize or launch directly into your AWS account.

The guide is for organizations that are running workloads in the AWS Cloud that require secure remote administrative access to Windows-based, Amazon Elastic Compute Cloud (Amazon EC2) instances over the internet. After reading this guide, IT infrastructure personnel should have a good understanding of how to design and deploy an RD Gateway infrastructure on the AWS Cloud.

## Quick Links

The links in this section are for your convenience. Before you launch the Quick Start, please review the architecture, configuration, and other considerations discussed in this guide.

* If you have an AWS account, and you’re already familiar with RD Gateway and AWS services, you can [launch the Quick Start](https://fwd.aws/66VB5) to deploy RD Gateway into a new virtual private cloud (VPC) in your AWS account. The deployment takes approximately 30 minutes. If you’re new to AWS or RD Gateway, or if you want to deploy RD Gateway into an existing VPC, please review the implementation details and follow the [step-by-step instructions](#_Deployment_Steps) provided in this guide.  [**h art**](https://console.aws.amazon.com/cloudformation/home?region=us-west-2#/stacks/new?stackName=Cloudera&templateURL=https://s3.amazonaws.com/quickstart-reference/cloudera/latest/templates/cloudera-master.template)

**[Launch   
(for new VPC)](https://fwd.aws/66VB5)**

* If you want to take a look under the covers, you can [view the AWS CloudFormation template](https://fwd.aws/87Dgp) that automates the deployment for a new VPC. You can customize the template during launch, or download and extend it for other projects.

[**View template  
(for new VPC)**](https://fwd.aws/87Dgp)

## About Quick Starts

[Quick Starts](http://aws.amazon.com/quickstart/) are automated reference deployments for key workloads on the AWS Cloud. Each Quick Start launches, configures, and runs the AWS compute, network, storage, and other services required to deploy a specific workload on AWS, using AWS best practices for security and availability.

# Overview

## Remote Desktop Gateway on AWS

AWS provides a comprehensive set of services and tools for deploying Microsoft Windows-based workloads on its highly reliable and secure cloud infrastructure. RD Gateway uses RDP over HTTPS to establish a secure, encrypted connection between remote users on the internet and Windows-based EC2 instances, without needing to configure a virtual private network (VPN) connection. This helps reduce the attack surface on your Windows-based instances while providing a remote administration solution for administrators.

This Quick Start automatically deploys and configures an RD Gateway infrastructure in the AWS Cloud from scratch, so you can securely administer your Windows-based, Amazon EC2 fleet using RDP over HTTPS. You can use the AWS CloudFormation templates included with the Quick Start to deploy a fully configured RD Gateway infrastructure in a new or existing VPC in your AWS account. You can also use the AWS CloudFormation templates as a starting point for your own implementation.

We’ve also published a set of [Quick Starts](https://aws.amazon.com/quickstart/) that provide solutions for deploying common Microsoft workloads, such as Microsoft Active Directory, Microsoft SharePoint, Microsoft Exchange, and Microsoft SQL Server, on AWS. Those Quick Starts include the RD Gateway deployment and architecture described in this guide—you can use them to deploy RD Gateway along with the additional Microsoft workload. For example, for an automated deployment that includes Active Directory Domain Services and RD gateways, see the [AWS Quick Start for Active Directory Domain Services](https://fwd.aws/N6e7B).

Implementing the RD Gateway on the AWS Cloud is an advanced topic. We recommend reviewing the Microsoft documentation for Windows Server 2016 and the AWS documentation [Connecting to Your Windows Instance](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/connecting_to_windows_instance.html).

This guide focuses on infrastructure configuration topics that require careful consideration when you are planning and deploying an RD Gateway infrastructure on the AWS Cloud. It doesn’t cover general Windows Server installation and software configuration tasks. For general software configuration guidance and best practices, consult the Microsoft product documentation.

## Cost and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using the Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

This Quick Start launches the Amazon Machine Image (AMI) for Microsoft Windows Server 2016 and includes the license for the Windows Server operating system. The AMI is updated on a regular basis with the latest service pack for the operating system, so you don’t have to install any updates. The Windows Server AMI doesn’t require Client Access Licenses (CALs) and includes two Microsoft Remote Desktop Services licenses. For details, see [Microsoft Licensing on AWS](https://aws.amazon.com/windows/resources/licensing/).

## AWS Services

The core AWS components used by this Quick Start include the following services. (If you are new to AWS, see [Getting Started with AWS](https://aws.amazon.com/getting-started/).)

* [AWS CloudFormation](http://aws.amazon.com/documentation/cloudformation/) – AWS CloudFormation gives you an easy way to create and manage a collection of related AWS resources, and provision and update them in an orderly and predictable way. You use a template to describe all the AWS resources (e.g., Amazon EC2 instances) that you want. You don't have to individually create and configure the resources or figure out dependencies—AWS CloudFormation handles all of that.
* [Amazon EC2](https://aws.amazon.com/documentation/ec2/) – The Amazon Elastic Compute Cloud (Amazon EC2) service enables you to launch virtual machine instances with a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or import your own virtual machine images.
* [Amazon VPC](https://aws.amazon.com/documentation/vpc/) – The Amazon Virtual Private Cloud (Amazon VPC) service lets you provision a private, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.
* [NAT Gateway](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html) – NAT Gateway is an AWS managed service that controls NAT gateway resources. A NAT gateway is a type of network address translation (NAT) device that enables instances in a private subnet to connect to the internet or to other AWS services, but prevents the internet from connecting to those instances.
* [IAM](http://aws.amazon.com/documentation/iam/) – AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. With IAM, you can manage users, security credentials such as access keys, and permissions that control which AWS resources users can access, from a central location.

# Architecture

## Architectural Considerations

This section describes general considerations for implementing and configuring RD Gateway in the cloud, to provide background information about the Quick Start architecture for RD Gateway.

### Initial Remote Administration Architecture

In an initial RD gateway configuration, the servers in the public subnet will need an inbound security group rule permitting TCP port 3389 from the administrator’s source IP address or subnet. Windows instances sitting behind the RD Gateway in a private subnet will be in their own isolated tier. For example, a group of web server instances in a private subnet may be associated with their own web tier security group. This security group will need an inbound rule allowing connections from the RD Gateway on TCP port 3389.

Using this architecture, an administrator can use a traditional RDP connection to an RD gateway to configure the local server. The RD gateway can also be used as a jump box; that is, when an RDP connection is established to the desktop of the RD gateway, an administrator can start a new RDP client session to initiate a connection to an instance in a private subnet, as illustrated in Figure 1.

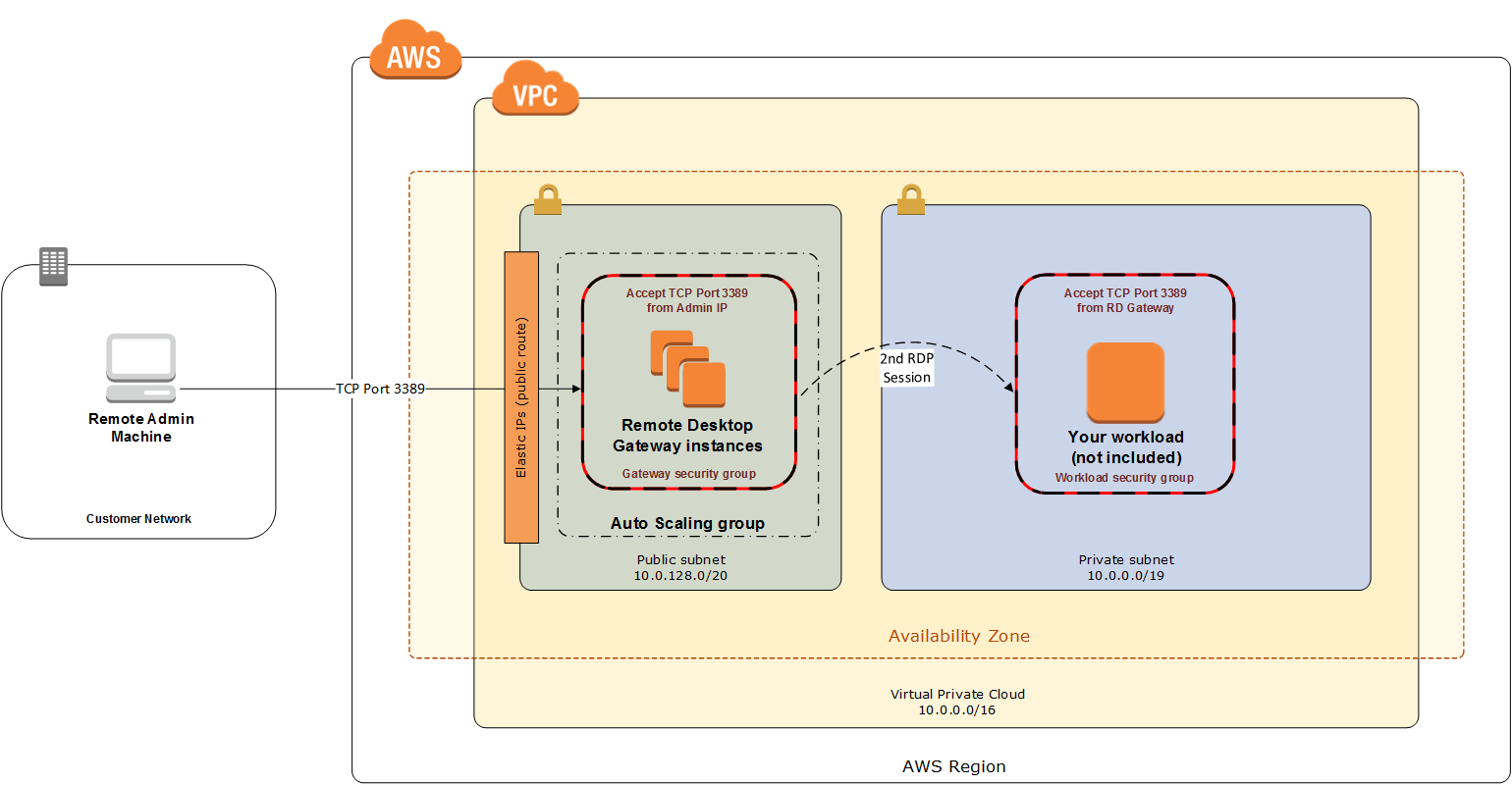


Figure 1: Initial architecture for remote administration

Although this architecture works well for initial administration, it is not recommended for the long term. To further secure connections and reduce the number of RDP sessions required to administer the servers in the private subnets, the inbound rule should be changed to permit TCP port 443, and the RD gateway service should be installed and configured with an SSL certificate, and connection and authorization policies.

The Quick Start sets up a standard TCP port 3389 connection from the administrator’s IP address. You’ll need to follow the [post-deployment steps](#_Step_3._Post-Deployment) to modify the security group for RD Gateway to use a single inbound rule permitting TCP port 443, as illustrated in Figure 2. This modification will allow a Transport Layer Security (TLS) encrypted RDP connection to be proxied through the gateway over TCP port 443 directly to one or more Windows-based instances in private subnets on TCP port 3389. This configuration increases the security of the connection and also prevents the need to initiate an RDP session to the desktop of the RD gateway.

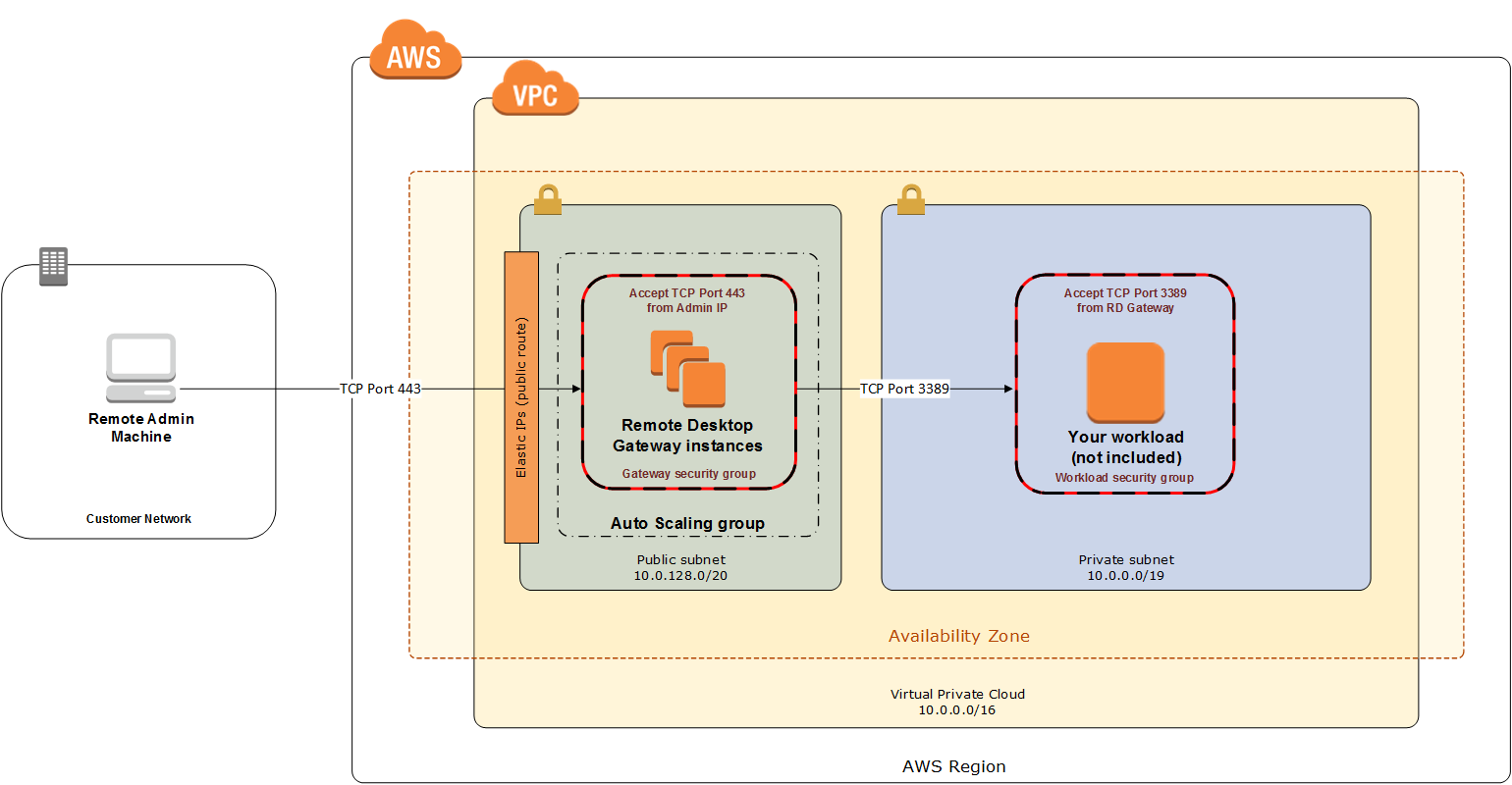


Figure 2: Architecture for RD Gateway administrative access

### SSL Certificates

The RD Gateway role uses Transport Layer Security (TLS) to encrypt communications over the internet between administrators and gateway servers. To support TLS, a valid X.509 SSL certificate must be installed on each RD gateway. Certificates can be acquired in a number of ways, including:

* Your own PKI infrastructure, such as a Microsoft Enterprise Certificate Authority (CA)
* Certificates issued by a public CA, such as Verisign or Digicert
* Self-signed certificates

For smaller test environments, implementing a self-signed certificate is a straightforward process that helps you get up and running quickly. This Quick Start automatically generates a self-signed certificate for RD Gateway. If you’re setting up RD Gateway manually, see the instructions in [Appendix A](#_Implementing_a_Self-Signed) for implementing a self-signed certificate.

However, if you have a large number of varying administrative devices that need to establish a connection to your gateways, we recommend using a public certificate.

In order for an RDP client to establish a secure connection with an RD gateway, the following certificate and DNS requirements must be met:

* The issuing CA of the certificate installed on the gateway must be trusted by the RDP client. For example, the root CA certificate must be installed in the client machine’s *Trusted Root Certification Authorities* store.
* The subject name used on the certificate installed on the gateway must match the DNS name used by the client to connect to the server; for example, rdgw1.example.com.
* The client must be able to resolve the host name (for example, rdgw1.example.com) to the Elastic IP address of the RD Gateway. This will require a Host (A) record in DNS.

There are various considerations when choosing the right CA to obtain an SSL certificate. For example, a public certificate may be ideal since the issuing CA will be widely trusted by the majority of client devices that need to connect to your gateways. On the other hand, you may choose to utilize your own PKI infrastructure to ensure that only the machines that are part of your organization will trust the issuing CA.

### Connection and Resource Authorization Policies

Users must meet specific requirements in order to connect to RD Gateway instances:

* **Connection authorization policies** – Remote Desktop connection authorization policies (RD CAPs) allow you to specify who can connect to an RD Gateway instance. For example, you can select a group of users from your domain, such as *Domain Admins*.
* **Resource authorization policies** – Remote Desktop resource authorization policies (RD RAPs) allow you to specify the internal Windows-based instances that remote users can connect to through an RD Gateway instance. For example, you can choose specific domain-joined computers, which administrators can connect to through the RD Gateway.

This Quick Start automatically sets up connection and resource authorization policies. For instructions on manually configuring these policies, see [Appendix](#_Configuring_Connection_and_1) A.

## Best Practices

### The Principle of Least Privilege

When considering remote administrative access to your environment, it is important to follow the principle of *least privilege*. This principle refers to users having the fewest possible permissions necessary to perform their job functions. This helps reduce the attack surface of your environment, making it much harder for an adversary to exploit. An attack surface can be defined as the set of exploitable vulnerabilities in your environment, including the network, software, and users who are involved in the ongoing operation of the system.

Following the principle of least privilege, we recommend reducing the attack surface of your environment by exposing the absolute minimal set of ports to the network while also restricting the source network or IP address that will have access to your EC2 instances.

In addition to the functionality that exists in the Microsoft platform, there are several AWS capabilities to help you implement the principle of least privilege, such as subnets, security groups, and trusted ingress CIDR blocks.

### VPC Configuration

Amazon VPC lets you provision a private, isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. With Amazon VPC, you can define a virtual network topology closely resembling a traditional network that you might operate on your own premises. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of route tables and network gateways.

When deploying a Windows-based architecture on the AWS Cloud, we recommend an VPC configuration that supports the following requirements:

* Critical workloads should be placed in a minimum of two Availability Zones to provide high availability.
* Instances should be placed into individual tiers. For example, in a Microsoft SharePoint deployment, you should have separate tiers for web servers, application servers, database servers, and domain controllers. Traffic between these groups can be controlled to adhere to the principle of least privilege.
* Internal application servers and other non-internet facing servers should be placed in private subnets to prevent direct access to these instances from the internet.
* RD gateways should be deployed into public subnets in each Availability Zone for remote administration. Other components, such as reverse proxy servers, can also be placed into these public subnets if needed.

This Quick Start supports these best practices, as illustrated in [Figure 5](#archdiagram). For details on the VPC design used in this Quick Start, see the [Quick Start for building a modular and scalable virtual network architecture with Amazon VPC](https://fwd.aws/9VdxN).

### Network Access Control Lists

A network access control list (ACL) is a set of permissions that can be attached to any network subnet in a VPC to provide stateless filtering of traffic. Network ACLs can be used for inbound or outbound traffic and provide an effective way to blacklist a CIDR block or individual IP addresses. These ACLs can contain ordered rules to allow or deny traffic based on IP protocol, service port, or source or destination IP address. Figure 3 shows the default ACL configuration for a VPC subnet. This configuration is used for the subnets in the Quick Start architecture.

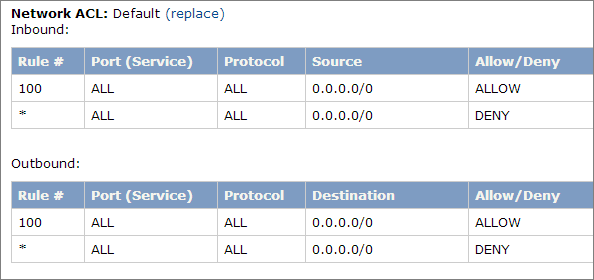


Figure 3: Default network ACL configuration for a VPC subnet

You may choose to keep the default network ACL configuration, or you may choose to lock it down with more specific rules to restrict traffic between subnets at the network level. For example, you could set a rule that would allow inbound administrative traffic on TCP port 3389 from a specific set of IP addresses. In either case, you’ll also need to implement security group rules to permit access from users connecting to RD gateways and between tiered groups of EC2 instances.

### Security Groups

All EC2 instances are required to belong to one or more security groups. Security groups allow you to set policies to control open ports and provide isolation between application tiers. In a VPC, every instance runs behind a stateful firewall with all ports closed by default. The security group contains rules responsible for opening inbound and outbound ports on that firewall. While security groups act as an instance-level firewall, they can also be associated with multiple instances, providing isolation between application tiers in your environment. For example, you can create a security group for all your web servers that will allow traffic on TCP port 3389, but only from members of the security group containing your RD Gateway servers. This is illustrated in Figure 4.

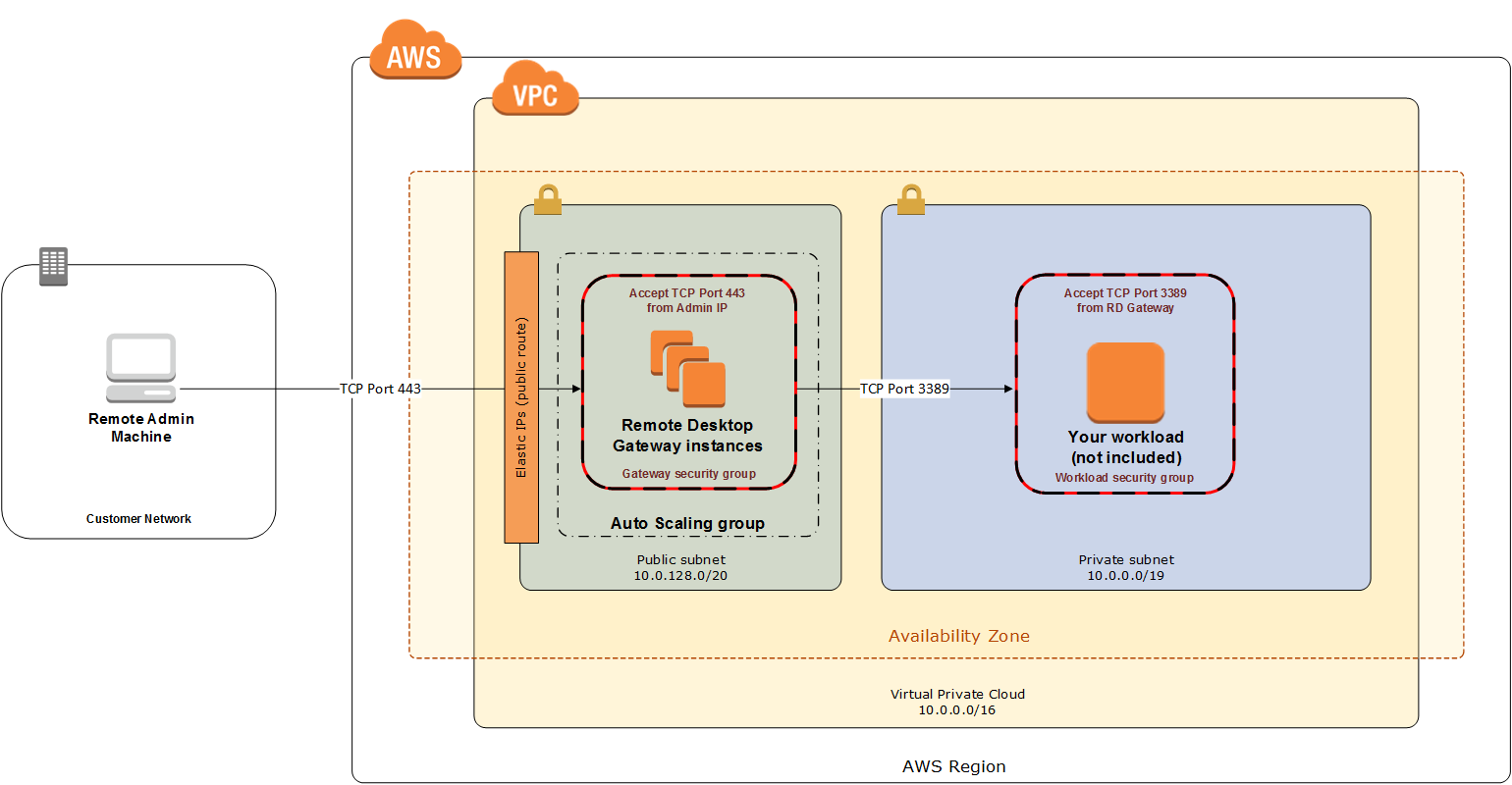


Figure 4: Security groups for RD Gateway administrative access

Notice that inbound connections from the internet are only permitted over TCP port 443 to the RD gateways. The RD gateways have an Elastic IP address assigned and have direct access to the internet. The remaining Windows instances are deployed into private subnets and are assigned private IP addresses only. Security group rules allow only the RD gateways to initiate inbound connections for remote administration to TCP port 3389 for instances in the private subnets.

In this architecture, RDP connections are established over HTTPS to the RD gateway and proxied to backend instances on the standard RDP TCP port 3389. This configuration helps you reduce the attack surface on your Windows-based instances while allowing administrators to establish connections to all your instances through a single gateway.

It’s possible to provide remote administrative access to all your Windows-based instances through one RD gateway, but we recommend placing gateways in each Availability Zone for redundancy. The Quick Start implements this best practice, as illustrated in Figure 5.

## RD Gateway Architecture on AWS

Deploying this Quick Start for a new VPC with **default parameters** builds the following RD Gateway environment in the AWS Cloud.

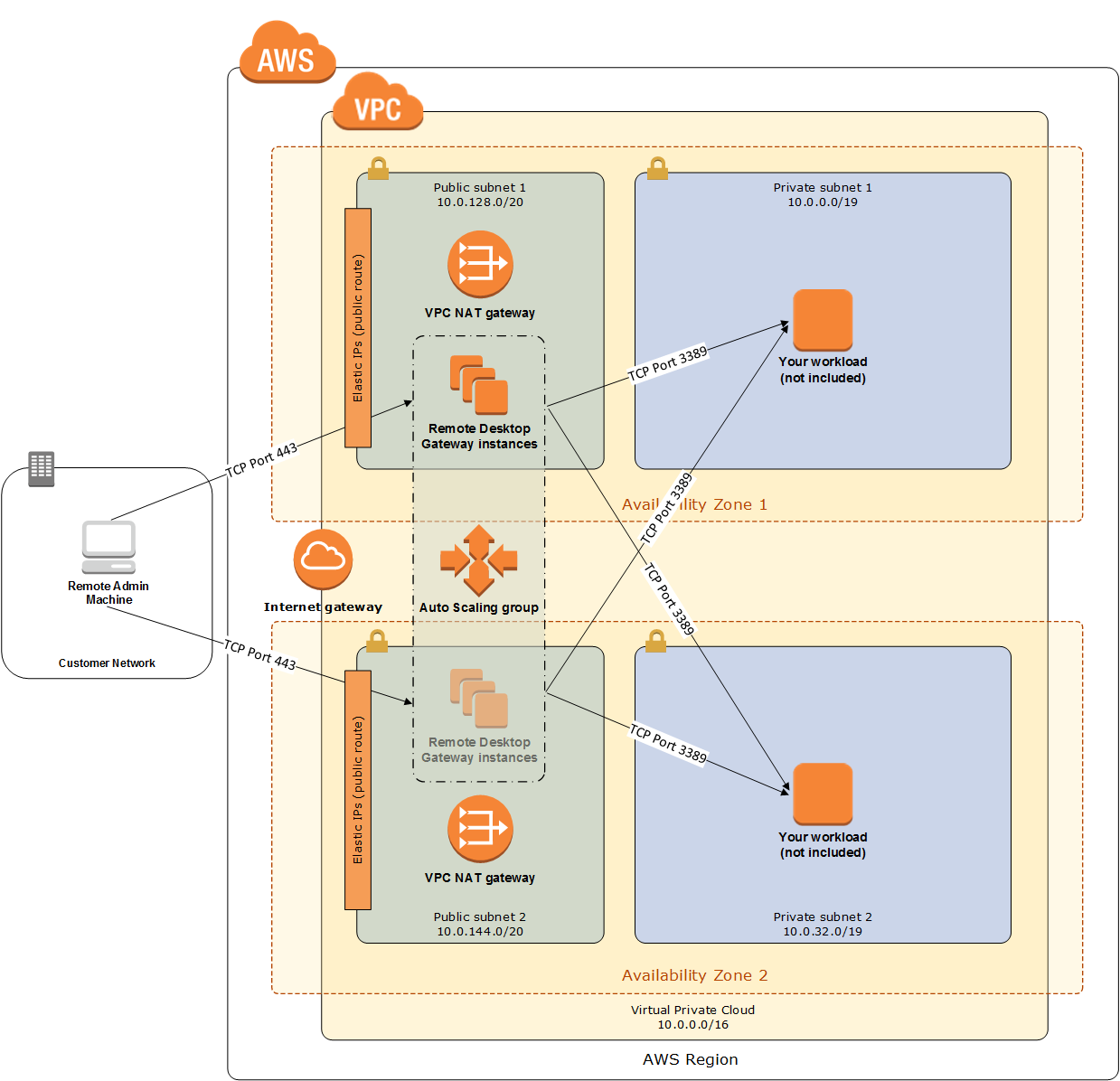


Figure 5: Quick Start architecture for RD Gateway on AWS

The Quick Start sets up the following:

* A highly available architecture that spans two Availability Zones.\*
* A VPC configured with public and private subnets according to AWS best practices, to provide you with your own virtual network on AWS.\*
* An internet gateway to allow access to the internet. This gateway is used by the RD Gateway instances to send and receive traffic.\*
* Managed network address translation (NAT) gateways to allow outbound internet access for resources in the private subnets.\*
* In each public subnet, up to four RD Gateway instances in an Auto Scaling group to provide secure remote access to instances in the private subnets. Each instance is assigned an Elastic IP address so it’s reachable directly from the internet.
* A security group for Windows-based instances that will host the RD Gateway role, with an ingress rule permitting TCP port 3389 from your administrator IP address. After deployment, you’ll modify the security group ingress rules to configure administrative access through TCP port 443 instead, as illustrated in Figure 5.
* An empty application tier for instances in private subnets. If more tiers are required, you can create additional private subnets with unique CIDR ranges.

**\*** The template that deploys the Quick Start into an existing VPC skips the tasks marked by asterisks and prompts you for your existing VPC configuration.

The Quick Start also installs a self-signed SSL certificate and configures RD CAP and RD RAP policies.

# Deployment Options

This Quick Start provides three deployment options:

* **Deploy RD Gateway into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of the VPC, subnets, NAT gateways, security groups, and other infrastructure components, and then deploys RD Gateway into this new VPC.
* **Deploy standalone RD Gateway into an existing VPC**. This option provisions standalone RD Gateway instances in your existing AWS infrastructure.
* **Deploy domain-joined RD Gateway into an existing VPC.** This is similar to the second option, except that it provides domain-joined RD Gateway instances in the existing VPC, and provides a few additional parameters for customizing this configuration.

The Quick Start provides separate templates for these three options. You can also configure CIDR blocks, instance types, and RD Gateway settings, as discussed later in the deployment steps.

# Deployment Steps

The procedure for deploying the RD Gateway architecture on AWS consists of the following steps. For detailed instructions, follow the links for each step.

[Step 1. Prepare your AWS account](#_Step_1._Prepare)

Sign up for an AWS account, choosing a region, creating a key pair, and requesting increases for account limits, if necessary.

[Step 2. Launch the Quick Start](#_Step_2._Launch)

Launch the AWS CloudFormation template into your AWS account, specify parameter values, and create the stack. The Quick Start provides separate templates for end-to-end deployment and deployment into an existing VPC.

[Step 3. Perform post-deployment tasks](#_Step_5._<Post-Configuration)

Finish configuring the AWS environment, install the root certificate, and configure the Remote Desktop Connection client.

## Step 1. Prepare Your AWS Account

1. If you don’t already have an AWS account, create one at <https://aws.amazon.com> by following the on-screen instructions. Part of the sign-up process involves receiving a phone call and entering a PIN using the phone keypad.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy RD Gateway on AWS. For more information, see [Regions and Availability Zones](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html). Regions are dispersed and located in separate geographic areas. Each Region includes at least two Availability Zones that are isolated from one another but connected through low-latency links.

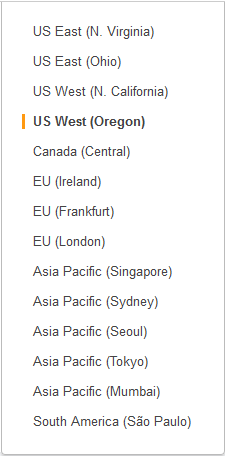


Figure 6: Choosing an AWS Region

Consider choosing a region closest to your data center or corporate network to reduce network latency between systems running on AWS and the systems and users on your corporate network.

1. Create a [key pair](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html) in your preferred region. To do this, in the navigation pane of the Amazon EC2 console, choose **Key Pairs**, **Create Key Pair**, type a name, and then choose **Create**.

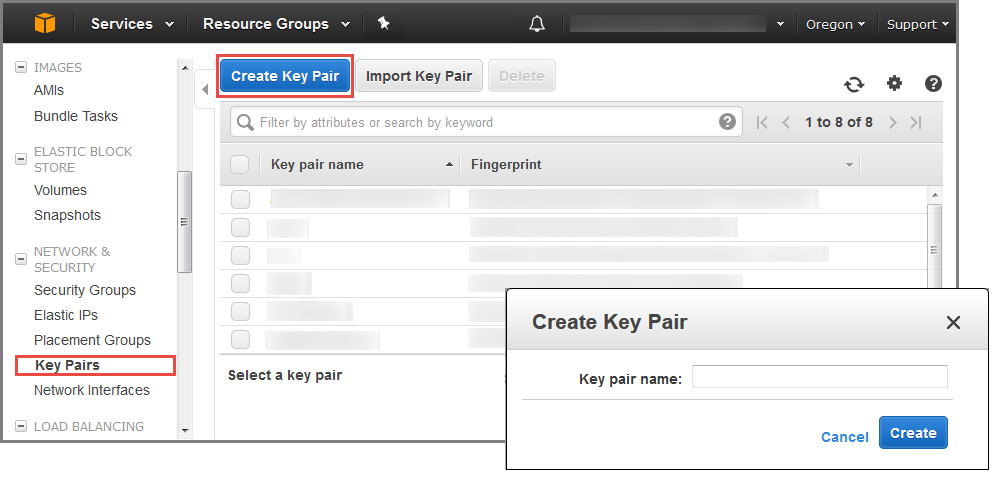


Figure 7: Creating a key pair

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. To log in to your instances, you must create a key pair. With Windows instances, the key pair is used to obtain the administrator password via the Amazon EC2 console and then log in using Remote Desktop Protocol (RDP), as explained in the [Amazon EC2 User Guide](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html#having-ec2-create-your-key-pair).

1. If necessary, [request a service limit increase](https://console.aws.amazon.com/support/home#/case/create?issueType=service-limit-increase&limitType=service-code-) for the Amazon EC2 **t2.large** instance type. To do this, in the AWS Support Center, choose **Create Case**, **Service Limit Increase**, **EC2 instances**, and then complete the fields in the limit increase form. The current default limit is 20 instances.

You might need to request an increase if you already have an existing deployment that uses this instance type, and you think you might exceed the default limit with this reference deployment. It might take a few days for the new service limit to become effective. For more information, see the [Amazon EC2 User Guide](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-resource-limits.html).

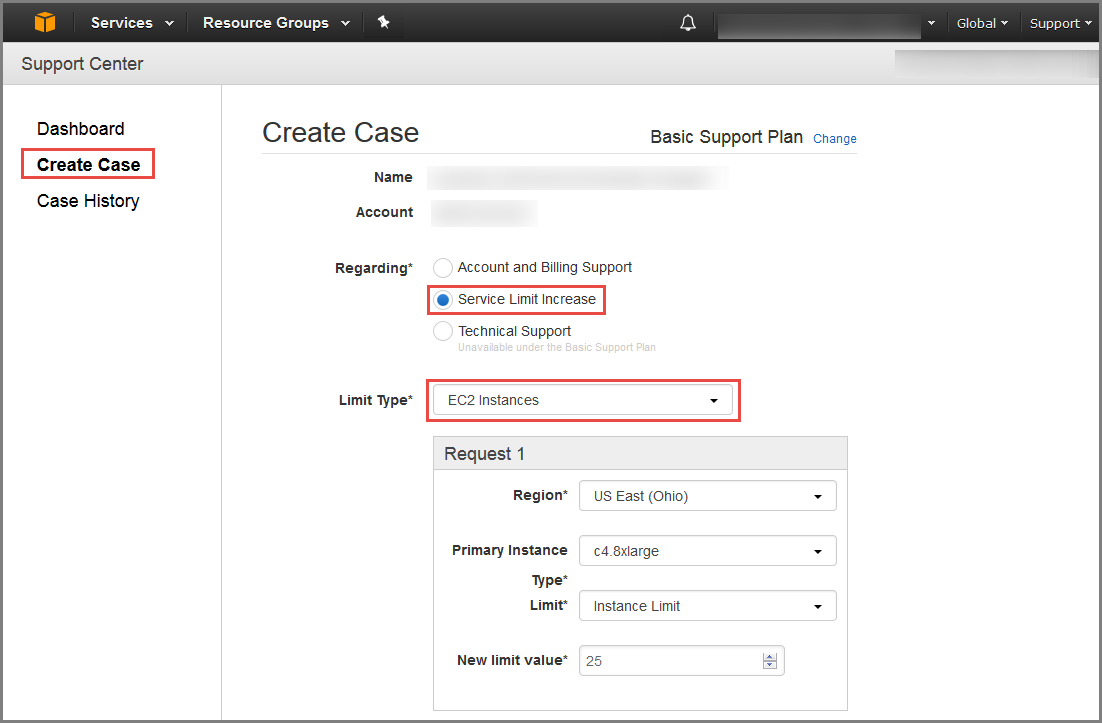


Figure 8: Requesting a service limit increase

## Step 2. Launch the Quick Start

**Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see [Deployment Options](#_Deployment_Scenarios) earlier in this guide.

|  |  |  |
| --- | --- | --- |
| [Option 1](#_Scenario_1:_Deploy_1)  [**Launch**](https://fwd.aws/66VB5)  Deploy RD Gateway into a  new VPC on AWS | [Option 2](#_Scenario_2:_Extending_1)  [**Launch**](https://fwd.aws/QmmJN)  Deploy RD Gateway into an existing VPC – standalone | Option 3  Deploy RD Gateway into an existing VPC – domain-joined  [**Launch**](https://fwd.aws/EwEqm) |

**Important** If you’re deploying RD Gateway into an existing VPC (option 2 or 3), make sure that the public subnets you choose for the RD Gateway are set to auto-assign a public IPv4 address. You’ll also need the domain name option configured in the DHCP options as explained in the [Amazon VPC documentation](http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html). You’ll be prompted for your VPC settings when you launch the Quick Start.

If you’re domain-joining the RD Gateway instances (option 3), make sure that the DHCP options set for the VPC specifies the Active Directory domain as the domain name, and the Active Directory domain controllers as the domain name servers for the VPC. This enables the RD Gateway instance to find the domain to join via DNS.

Each deployment takes about 30 minutes to complete.

1. Check the region that’s displayed in the upper-right corner of the navigation bar, and change it if necessary. This is where the network infrastructure for RD Gateway will be built. The template is launched in the US East (Ohio) Region by default.
2. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
3. On the **Specify Details** page, change the stack name if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.

In the following tables, parameters are listed by category and described separately for the three deployment options:

* [Parameters for deploying RD Gateway into a new VPC](#sc1)
* [Parameters for deploying RD Gateway into an existing VPC](#sc2) (standalone)
* [Parameters for deploying RD Gateway into an existing VPC (domain-joined)](#sc3)
* **Option 1: Parameters for deploying RD Gateway into a new VPC**

[View template](https://fwd.aws/87Dgp)

*VPC Network Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Availability Zones (AvailabilityZones) | *Requires input* | The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify. |
| VPC CIDR (VPCCIDR) | 10.0.0.0/16 | CIDR block for the VPC to create. |
| Private Subnet 1 CIDR (PrivateSubnet1CIDR) | 10.0.0.0/19 | CIDR block for the private subnet located in Availability Zone 1. |
| Private Subnet 2 CIDR (PrivateSubnet2CIDR) | 10.0.32.0/19 | CIDR block for the private subnet located in Availability Zone 2. |
| Public Subnet 1 CIDR (PublicSubnet1CIDR) | 10.0.128.0/20 | CIDR block for the public (DMZ) subnet located in Availability Zone 1. |
| Public Subnet 2 CIDR (PublicSubnet2CIDR) | 10.0.144.0/20 | CIDR block for the public (DMZ) subnet located in Availability Zone 2. |
| Allowed Remote Desktop Gateway External Access CIDR (RDGWCIDR) | *Requires input* | The CIDR IP range that is permitted to access the RD Gateway instances. We recommend that you set this value to a trusted IP range. For example, you might want to grant only your corporate network access to the software. |

*Amazon EC2 Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Key Pair Name (KeyPairName) | *Requires input* | Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region. |
| Remote Desktop Gateway Instance Type (RDGWInstanceType) | t2.large | EC2 instance type for RD Gateway instances. |

*Microsoft Remote Desktop Gateway Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Number of RDGW Hosts (NumberOfRDGWHosts) | 1 | The number of RD Gateway instances to create. You can choose 1-4 instances. |
| Admin User Name (AdminUser) | StackAdmin | User name for the new local administrator account. |
| Admin Password (AdminPassword) | *Requires input* | Password for the new administrator account. This must be a [complex password](https://technet.microsoft.com/en-us/library/hh994562.aspx) that’s at least 8 characters long. |
| Domain DNS Name (DomainDNSName) | example.com | Fully qualified domain name (FQDN) of the forest root domain. |

*AWS Quick Start Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Quick Start S3 Bucket Name (QSS3BucketName) | aws-quickstart | S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you’ve created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen. |
| Quick Start S3 Key Prefix (QSS3KeyPrefix) | quickstart-microsoft-rdgateway/ | The [S3 key name prefix](https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html) used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes. |

* **Option 2: Parameters for deploying RD Gateway into an existing VPC (standalone)**

[View template](https://fwd.aws/REkAP)

*Network Configuration:*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Parameter label (name) | Default | | Description | |
| VPC ID (VPCID) | *Requires input* | | ID of the existing VPC where you want to deploy RD Gateway (e.g., vpc-0343606e). | |
| Public Subnet 1 ID (PublicSubnet1ID) | *Requires input* | | ID of the public subnet in Availability Zone 1 in your existing VPC (e.g., subnet-a0246dcd). | |
| Public Subnet 2 ID (PublicSubnet2ID) | *Requires input* | | ID of the public subnet in Availability Zone 2 in your existing VPC (e.g., subnet-e3246d8e). | |
| Allowed Remote Desktop Gateway External Access CIDR (RDGWCIDR) | | *Requires input* | | The CIDR IP range that is permitted to access the RD Gateway instances. We recommend that you set this value to a trusted IP range. For example, you might want to grant only your corporate network access to the software. | |

*Amazon EC2 Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Key Pair Name (KeyPairName) | *Requires input* | Public/private key pair, which allows you to connect securely to your instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region. |
| Remote Desktop Gateway Instance Type (RDGWInstanceType) | t2.large | EC2 instance type for RD Gateway instances. |

*Microsoft Remote Desktop Gateway Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Number of RDGW Hosts (NumberOfRDGWHosts) | 1 | The number of RD Gateway instances to create. You can choose 1-4 instances. |
| Admin User Name (AdminUser) | StackAdmin | User name for the new local administrator account. |
| Admin Password (AdminPassword) | *Requires input* | Password for the new administrator account. This must be a [complex password](https://technet.microsoft.com/en-us/library/hh994562.aspx) that’s at least 8 characters long. |
| Domain DNS Name (DomainDNSName) | example.com | Fully qualified domain name (FQDN) of the forest root domain. |

*AWS Quick Start Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Quick Start S3 Bucket Name (QSS3BucketName) | aws-quickstart | S3 bucket where the Quick Start templates and scripts are installed. Use this parameter to specify the S3 bucket name you’ve created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen. |
| Quick Start S3 Key Prefix (QSS3KeyPrefix) | quickstart-microsoft-rdgateway/ | The [S3 key name prefix](https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingMetadata.html) used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes. |

* **Option 3: Parameters for deploying RD Gateway into an existing VPC (domain-joined)**

[View template](https://fwd.aws/YxRD7)

The template for the domain-joined RD Gateway deployment provides the same parameters as the template for the standalone deployment, except for the following RD Gateway and Active Directory settings.

*Microsoft Active Directory Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Domain DNS Name (DomainDNSName) | example.com | Fully qualified domain name (FQDN) of the forest root domain. |
| Domain NetBIOS Name (DomainNetBIOSName) | example | NetBIOS name of the domain (up to 15 characters) for users of earlier versions of Windows. |
| Domain Member Security Group ID (DomainMemberSGID) | *Requires input* | ID of the domain member security group (e.g., sg-7f16e910). |
| Domain Admin User Name (DomainAdminUser) | StackAdmin | User name for the domain administrator. This is separate from the default administrator account. |
| Domain Admin Password (DomainAdminPassword) | *Requires input* | Password for the domain administrator user. This must be a [complex password](https://technet.microsoft.com/en-us/library/hh994562.aspx) that’s at least 8 characters long. |

*Microsoft Remote Desktop Gateway Configuration:*

|  |  |  |
| --- | --- | --- |
| Parameter label (name) | Default | Description |
| Number of RDGW Hosts (NumberOfRDGWHosts) | 1 | The number of RD Gateway instances to create. You can choose 1-4 instances. |

1. On the **Options** page, you can [specify tags](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-resource-tags.html) (key-value pairs) for resources in your stack and [set advanced options](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cfn-console-add-tags.html). When you’re done, choose **Next**.
2. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.
3. Choose **Create** to deploy the stack.
4. Monitor the status of the stack. When the status is **CREATE\_COMPLETE**, the deployment is ready.
5. Use the URLs displayed in the **Outputs** tab for the stack to view the resources that were created.

## Step 3. Perform Post-Deployment Tasks

After you launch the AWS CloudFormation template for one of the three scenarios in the previous sections and build the stack, follow these steps to complete the configuration of your AWS environment:

1. Create security groups for your Windows-based instances that will be located in private VPC subnets. Create an ingress rule permitting TCP port 3389 from the RD Gateway security group, CIDR range, or IP address. Associate these groups with instances as they are launched into the private subnets.
2. Make sure that your administrative clients can resolve the name for the RD Gateway endpoint (e.g., win-1a2b3c4d5e6.example.com). You can create an A (Host) record in DNS that maps the FQDN to the RD gateway’s Elastic IP or public IP address. For testing purposes, you can configure this mapping in the local host’s file on the machine.
3. Configure administrative clients with the proper configuration settings. This includes installing the root certificate from each RD Gateway server on the client machines (see the next section for instructions). When you use the AWS CloudFormation templates, the default location for the root certificate will be *c:\<servername>.cer* on each RD Gateway server.
4. Modify the RD Gateway security group. Remove the ingress rule permitting TCP port 3389. Create a new ingress rule permitting TCP port 443 from your administrator’s IP address.
5. Make sure that instances in private subnets are associated with a security group containing ingress rules permitting the RD Gateway server IP address to connect via TCP port 3389.
6. Configure the Remote Desktop connection for administrative clients, as described [later in this section](#_Configuring_the_Remote).

### Installing the Root Certificate

The Quick Start implements a self-signed certificate on the RD gateway intances. After deployment, you must install the root certificate on your administrative clients before you configure the RDP client to connect to your RD gateway instances. The root certificate will automatically be stored as *c:\<servername>.cer.*

To distribute this file to administrator workstations and install it, follow these steps:

1. Open a Command Prompt window using administrative credentials.
2. Type **mmc** and press **Enter**.
3. In the Console Root window, on the **File** menu, choose **Add/Remove Snap In**.
4. In the **Add Standalone Snap-in** dialog box, choose **Certificates**, and then choose **Add**.
5. In the **Certificates snap-in** dialog box, choose **Computer account**, and then choose **Next**.
6. In the **Select Computer** dialog box, choose **Finish**.
7. In the **Add Standalone Snap-in** dialog box, choose **Close**.
8. On the **Add/Remove Snap-in** dialog box, choose **OK**.
9. In the Console Root window, expand **Certificates (Local Computer)**.
10. Under **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**.
11. Open the context (right-click) window for **Certificates**, and choose **All Tasks** > **Import**.
12. Navigate to the root certificate (e.g., RDGW1.cer) to complete the installation.

**Note** The root certificate will be stored as *c:\<servername>.cer* on each RD gateway when deploying servers using the CloudFormation templates.

### Configuring the Remote Desktop Connection Client

Use these steps to configure the Remote Desktop connection on administrative clients:

1. Start the Remote Desktop Connection client.
2. In the computer name field, type the name or IP address of the Windows instance you want to connect to. Keep in mind that this instance needs to be reachable only from the RD gateway, not from the client machine.

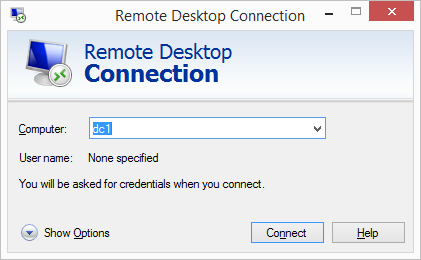


Figure 9: The Remote Desktop Connection client

1. Choose **Show Options**. On the **Advanced** tab, choose **Settings**.
2. Choose **Use these RD Gateway server settings**. For server name, specify the FQDN of the RD gateway. If the RD gateway and the server you want to connect to are in the same domain, choose **Use my RD Gateway credentials for the remote computer**,and then choose **OK**.

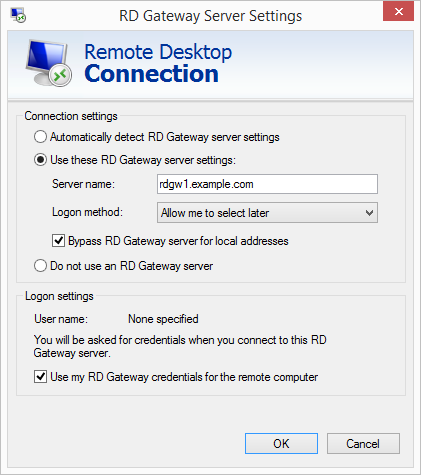


Figure 10: Advanced properties for the Remote Desktop Connection client

**Important** The FQDN server name of the RD Gateway host **must** match the certificate and the DNS record (or local HOSTS file entry). Otherwise, the secure connection will generate warnings and might fail.

1. Enter your credentials, and then choose **OK** to connect to the server. You can supply the same set of credentials for the RD gateway and the destination server, as shown in Figure 11. If your servers are not domain-joined, you will need to authenticate twice: once for the RD gateway and once for the destination server.

If your servers aren’t domain-joined, when prompted for the RD Gateway server credentials, provide the **Admin User Name** and **Admin Password** credentials you set in [step 2](#_Step_3._<Pre-Launch), when you launched the Quick Start. Check the **Remember my credentials** box. (Otherwise, if you’re connecting from a Windows computer, you’ll get prompted for your credentials repeatedly, and will be blocked from entering your remote computer credentials.)

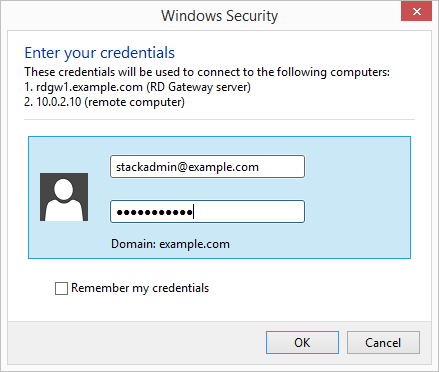


Figure 11: Providing credentials for the RD gateway and destination server

# Troubleshooting

**Q.** I encountered a CREATE\_FAILED error when I launched the Quick Start.

**A.** If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack’s state will be retained and the instance will be left running, so you can troubleshoot the issue. (You'll want to look at the log files in %ProgramFiles%\Amazon\EC2ConfigService and C:\cfn\log.)

**Important** When you set **Rollback on failure** to **No**, you’ll continue to incur AWS charges for this stack. Please make sure to delete the stack when you’ve finished troubleshooting.

For additional information, see [Troubleshooting AWS CloudFormation](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/troubleshooting.html) on the AWS website.

**Q.** I encountered a size limitation error when I deployed the AWS Cloudformation templates.

**A.** We recommend that you launch the Quick Start templates from the location we’ve provided or from another S3 bucket. If you deploy the templates from a local copy on your computer or from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the [AWS documentation](http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cloudformation-limits.html).

# Additional Resources

**AWS services**

* Amazon EC2 user guide for Windows  
  <https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/>
* AWS CloudFormation  
  <https://aws.amazon.com/documentation/cloudformation/>
* Amazon VPC  
  <https://aws.amazon.com/documentation/vpc/>

**Deploying Microsoft software on AWS**

* Securing the Microsoft platform on AWS  
  <https://d1.awsstatic.com/whitepapers/aws-microsoft-platform-security.pdf>
* Microsoft Licensing Mobility   
  <https://aws.amazon.com/windows/resources/licensemobility/>
* Windows Server on AWS  
  <https://aws.amazon.com/windows/>

**AWS Quick Starts**

* AWS Quick Start home page  
  <https://aws.amazon.com/quickstart/>
* Active Directory Domain Services on AWS  
  [https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/](https://fwd.aws/N6e7B)
* Building a Modular and Scalable Virtual Network Architecture with Amazon VPC  
  [https://docs.aws.amazon.com/quickstart/latest/vpc/](https://fwd.aws/9VdxN)

# Appendix A: Setting up RD Gateway Manually on AWS

In the following sections, we’ve provided information on the manual setup and configuration tasks for RD Gateway. These tasks are automated by the Quick Start templates. If you decide to perform them manually, you’ll need to set up the VPC architecture described in the [Best Practices](#_Considerations_When_Deploying) section and illustrated in [Figure 3](#archdiagram). For details on the recommended VPC design, see the [Quick Start for building a modular and scalable virtual network architecture with Amazon VPC](https://fwd.aws/9VdxN).

## Installing RD Gateway

The installation of the RD Gateway role is straightforward. Use the following command from a PowerShell instance started with administrative privileges:

Install-WindowsFeature RDS-Gateway –IncludeManagementTools

Once complete, the RD Gateway role, along with all prerequisite software and administration tools, will be installed on your EC2 instance running Windows Server 2016.

## Implementing a Self-Signed Certificate

[If you decide to use a self-signed certificate](#_SSL_Certificates), you will need to install the root CA certificate on every client device. As an automated solution, the AWS CloudFormation templates provided in this guide use a self-signed certificate for the RD Gateway service. If you aren’t using the automated deployment, you can use RD Gateway management tools, which provide a mechanism for generating a self-signed certificate.

1. Launch the **RD Gateway Manager**.
2. Open the context (right-click) menu for the local server name, and then choose **Properties**.

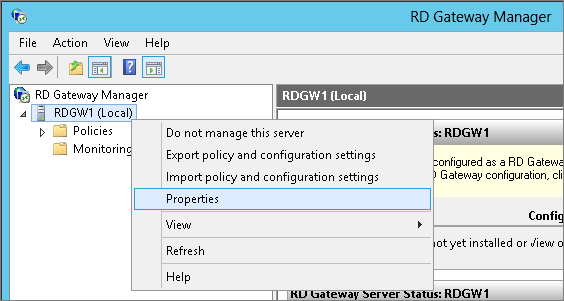


Figure 13: Navigating the RD Gateway Manager

1. On the **SSL Certificate** tab, make sure that **Create a self-signed certificate** is selected, and then choose **Create and Import a Certificate**.

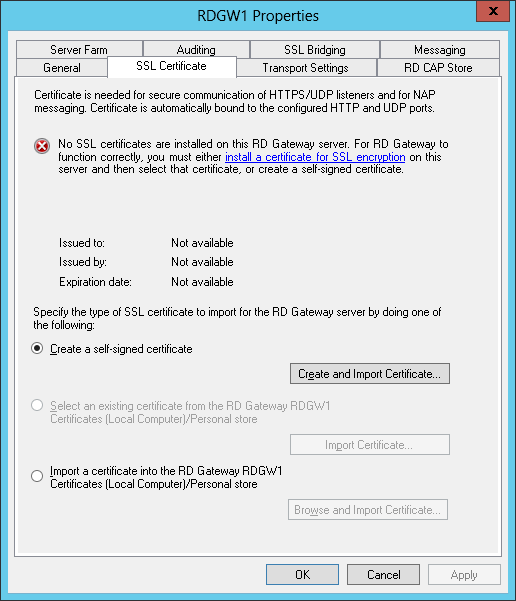


Figure 14: SSL certificate settings on the RD gateway

1. Make sure that the correct fully-qualified domain name (FQDN) is listed for the **Certificate name**. Make note of the root certificate location, and then choose **OK**.



Figure 15: Creating a self-signed certificate

1. After you install the certificate, close and reopen the server’s **Properties** dialog box to verify that the new self-signed certificate was successfully installed.

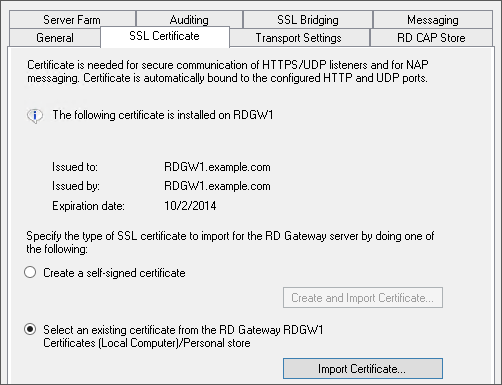


Figure 16: Viewing the SSL certificate settings after creating a new certificate

## Configuring Connection and Resource Authorization Policies

During manual deployment, once you’ve installed the RD Gateway role and an SSL certificate, you’ll be ready to configure connection and resource authorization policies. (Note that the Quick Start templates automatically configure these for you.)

To configure the policies:

1. Launch the RD Gateway Manager.
2. Open the context (right-click) menu for the **Policies** branch, and choose **Create New Authorization Policies**.

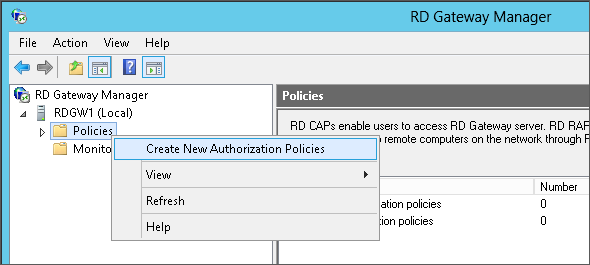


Figure 17: Navigating the RD Gateway Manager

1. In the **Create New Authorization Policies** wizard, choose **Create a RD CAP and a RD RAP (recommended)**, and then choose **Next**.

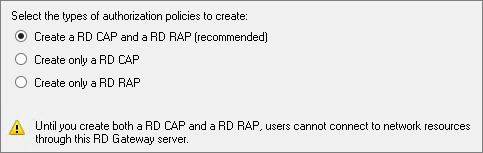


Figure 18: Selecting authorization policies

1. Enter a friendly name for your RD CAP, and then choose **Next**.
2. On the **Select Requirements** screen, define the authentication method and groups that should be permitted to connect to the RD gateway, and then choose **Next**.

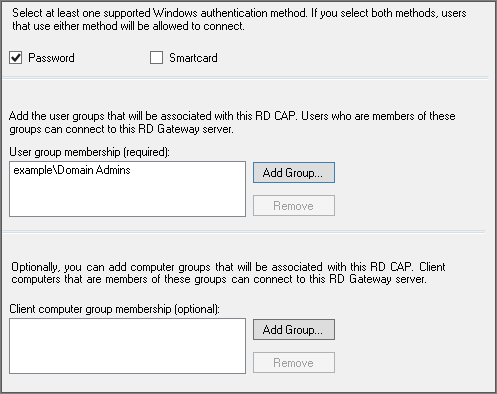


Figure 19: Configuring authentication method and groups for RD CAP

1. Choose whether to enable or disable device redirection, and then choose **Next**.
2. Specify your timeout and reconnection settings, and then choose **Next**.
3. On the **RD CAP Settings Summary** screen, choose **Next**.
4. Enter a friendly name for your RD RAP, and then choose **Next**.
5. Select the user groups that will be associated with the RAP, and then choose **Next**.

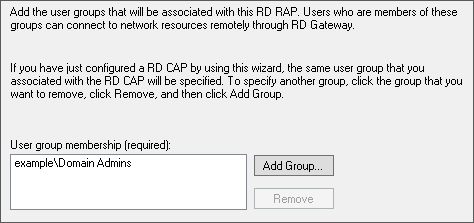


Figure 20: Selecting group memberships for RD RAP

1. Select the Windows-based instances (network resources) that administrators should be able to connect to through the RD gateway. This can be a security group in Active Directory that contains specific computers. The following example allows administrators to connect to any computer. Choose **Next**.

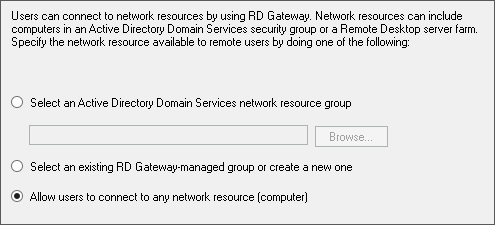


Figure 21: Selecting network resources

1. Allow connections to TCP port 3389, and then choose **Next**.

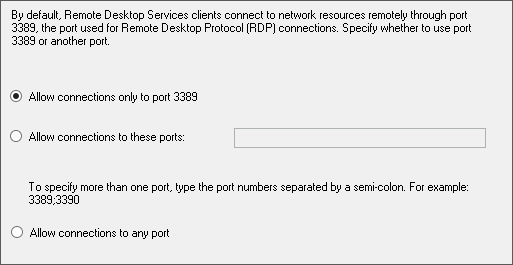


Figure 22: Selecting the RDP port

1. Choose **Finish**,and then **Close.**

# Send Us Feedback

You can visit our [GitHub repository](https://fwd.aws/wqNzk) to download the templates and scripts for this Quick Start, to post your feedback, and to share your customizations with others.

# Document Revisions

|  |  |  |
| --- | --- | --- |
| Date | Change | In sections |
| March 2020 | Removed Appendix A; renamed Appendix B to Appendix A. | Appendix A, Appendix B |
| October 2019 | Modified the note for existing VPC deployment scenario. | [Step 2. Launch the Quick Start](#_Step_3._<Pre-Launch) |
| June 2017 | Added Auto Scaling group for RD Gateway instances, Elastic IP address assignments, and S3 portability enhancements. Removed Active Directory server IP dependency. Reorganized and revised guide to focus on automated deployments. | Changes throughout guide |
| September 2016 | Added parameters for configuring the location of Quick Start assets; clarified post-deployment steps. | [Deployment Steps](#_Automated_Deployment) |
| July 2016 | Updated the templates to use NAT gateways and an updated VPC configuration; added template for domain-joined RD Gateway instances. | [Deployment Steps](#_Automated_Deployment) |
| September 2015 | Changed the default type for RD Gateway instances from m3.xlarge to m4.xlarge for better performance and price. | [Deployment Steps](#_Automated_Deployment) |
| March 2015 | Optimized the underlying VPC design to support expansion and to reduce complexity. | [Architecture diagram](#archdiagram) |
| November 2014 | Changed the default type for NATInstanceType to t2.small to support the EU (Frankfurt) region. | [Deployment Steps](#_Automated_Deployment) |
| April 2014 | Initial publication | — |

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

**Notices**

This document is provided for informational purposes only. It represents AWS’s current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS’s products or services, each of which is provided “as is” without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at <http://aws.amazon.com/apache2.0/> or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.