

Deploy Dual Stack Windows Server 2012 R2 in AWS

Lawrence E. Hughes
7 July 2017

This assumes that you have created a dual stack VPC, with v4 and v6 CIDR blocks, v4 and v6 subnets, etc.

Bring up AWS console.

Click the *Launch Instance* button.

In the Choose AMI page, click AWS Marketplace.

Search for *Windows Server 2012 R2*

Microsoft **Microsoft Windows Server 2012 R2** [Select](#)

★★★★★ (0) | 2017.06.14 | Sold by [Amazon Web Services](#)

Free tier eligible \$0.0082 to \$25.229/hr incl EC2 charges + other AWS usage fees

Windows, Windows Server 2012 R2 6.2.9200 | 64-bit Amazon Machine Image (AMI) | Updated: 6/14/17

Amazon EC2 running Microsoft Windows Server is a fast and dependable environment for deploying applications using the Microsoft Web Platform. Amazon EC2 enables you to run any ...

[More info](#)

Click the *Select* button.

Choose t2.micro (1 GB RAM) or t2.small (2 GB RAM)

Click *Next: Configure Instance Details* at lower right

On the *Configure Instance Details* page:

- Select your configured dual stack VPC
- Select your preferred subnet
- For *Auto-assign Public IP* choose *Use subnet setting (Enable)*
- For *Auto-assign IPv6 IP*, choose *Enable*

Network ⓘ vpc-7afc041c | VPC1 (default) [Create new VPC](#)

Subnet ⓘ subnet-c5379e9e | Default in us-west-2c
4088 IP Addresses available [Create new subnet](#)

Auto-assign Public IP ⓘ Use subnet setting (Enable)

Auto-assign IPv6 IP ⓘ Enable

Click *Next: Add Storage* button (lower right)

Volume Type <small>i</small>	Device <small>i</small>	Snapshot <small>i</small>	Size (GiB) <small>i</small>	Volume Type <small>i</small>	IOPS <small>i</small>	Throughput (MB/s) <small>i</small>	Delete on Termination <small>i</small>	Encrypted <small>i</small>
Root	/dev/sda1	snap-00276c7c1c520750e	30	General Purpose S	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

The defaults should be OK.

Click *Review and Launch* button (lower right)

On *Review Instance Launch* verify settings, then click *Launch* (lower right)

If you already have a KeyPair, select it. Otherwise create a new keypair and save it. Details for creating a new Keypair are in the Deploy FreeBSD 10.3 writeup.

Acknowledge that you have access to the private key file.

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Select a key pair

I acknowledge that I have access to the selected private key file (KP1.pem), and that without this file, I won't be able to log into my instance.

Cancel
Launch Instances

Click the *Launch Instances* button.

Within a few minutes, your instance will be launched (you can view the log):

✔ **Your instances are now launching**
The following instance launches have been initiated: [i-099c7b3437980a56e](#) [Hide launch log](#)

Creating security groups	Successful (sg-4084f3a)
Authorizing inbound rules	Successful
Initiating launches	Successful
Launch initiation complete	

Click the *View Instances* button (at lower right)

Select your new instance. You can name if you like (e.g. WS2012R2-1). View the Description:

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword 1 to 4 of 4

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (I
WS2012R2-1	i-099c7b3437980a56e	t2.micro	us-west-2c	running	2/2 checks ...	None	ec2-54-186-5-
FreeBSD-3	i-09a290415fe27fe29	t2.micro	us-west-2c	running	2/2 checks ...	None	ec2-54-190-12
	i-0a9d48af2c7e1d349	t2.micro	us-west-2c	terminated		None	
FreeBSD1	i-0cd580d7052df3343	t2.micro	us-west-2c	running	2/2 checks ...	None	ec2-34-209-2

Instance: i-099c7b3437980a56e (WS2012R2-1) Public DNS: ec2-54-186-5-103.us-west-2.compute.amazonaws.com

Description Status Checks Monitoring Tags

Instance ID	i-099c7b3437980a56e	Public DNS (IPv4)	ec2-54-186-5-103.us-west-2.compute.amazonaws.com
Instance state	running	IPv4 Public IP	54.186.5.103
Instance type	t2.micro	IPv6 IPs	2600:1f14:611:b600:5e95:edbb:36c9:86d8
Elastic IPs		Private DNS	ip-172-31-4-160.us-west-2.compute.internal
Availability zone	us-west-2c	Private IPs	172.31.4.160
Security groups	Microsoft Windows Server 2012 R2-2017-06-14-AutogenByAWSMP-1 view inbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-7afc041c
AMI ID	Windows_Server-2012-R2_RTM-English-64Bit-Base-2017.06.14 (ami-8d0c07f4)	Subnet ID	subnet-c5379e9e
Platform	windows	Network interfaces	eth0
IAM role	-	Source/dest. check	True
Key pair name	KP1	EBS-optimized	False
Owner	468731144912	Root device type	ebs
Launch time	July 7, 2017 at 8:42:09 AM UTC+8 (less than one hour)	Root device	/dev/sda1
Termination protection	False	Block devices	/dev/sda1
Lifecycle	normal		
Monitoring	basic		
Alarm status	None		

Now click the *Connect* button (second in top row).

Connect To Your Instance ✕

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

Download Remote Desktop File

When prompted, connect to your instance using the following details:

Public DNS ec2-54-186-5-103.us-west-2.compute.amazonaws.com

User name Administrator

Password **Get Password**

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

Close

Click the *Get Password* button.

Choose the private key file (in PEM format)

Key Pair Path **Choose File** KP1.pem

Or you can copy and paste the contents of the Key Pair below:

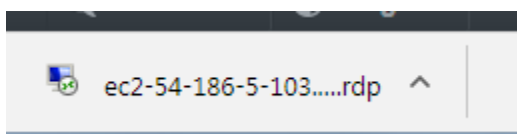
```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAIg+EGvKKvzsoOdQH0IbMG6+gjh8MFKIFjnv388XtnmrHYkMMJATOO3ZmyEt
haD3IPfWr9Kflz6aOgSDx3v/w9LS8Uj8tbYay4o1+aCM12zvWoqroArvSwUd/ZpN7PvjeUBOfm
idTw2q4wJtGdG0vPpPAjllrUc1FIVpxJEbgTdd430CMTTJfaeGrZZLHzAxCqApOwuzBN96JOnOV3
WAMKPDgdx7pOGmL406X0x4Nv83lu3XTek0pD1r+ertgVS9PI7PiRI8fF4xl0auLilqHjsOdE6I
-----
```

Decrypt Password

Click the *Decrypt Password* button:

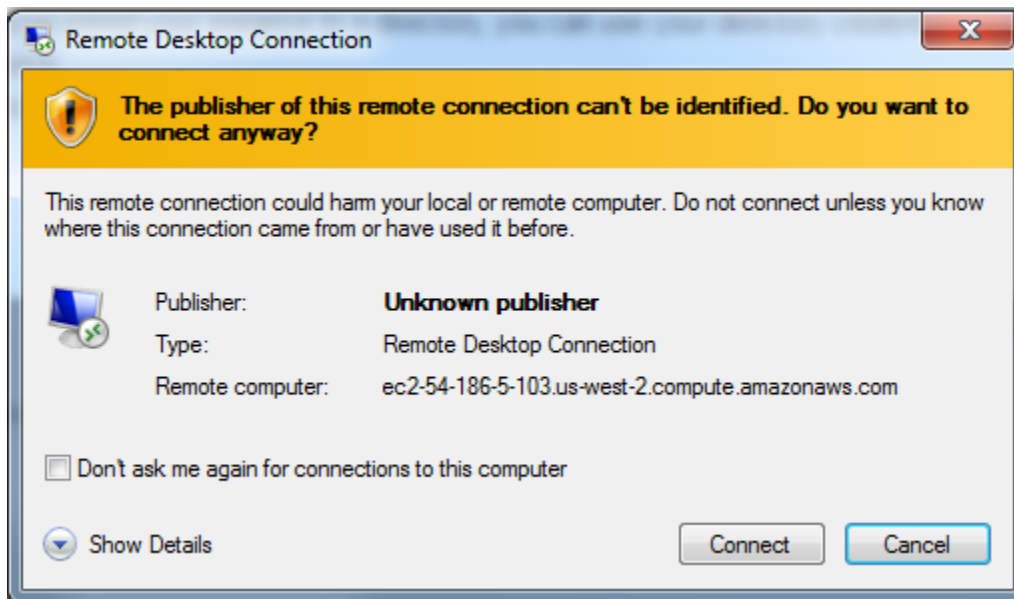
The decrypted password appears on the following screen (not shown here for security).

To connect to the new instance with Remote Desktop Connection, click the *Download Remote Desktop File* button. In Chrome, this will appear at the bottom left:

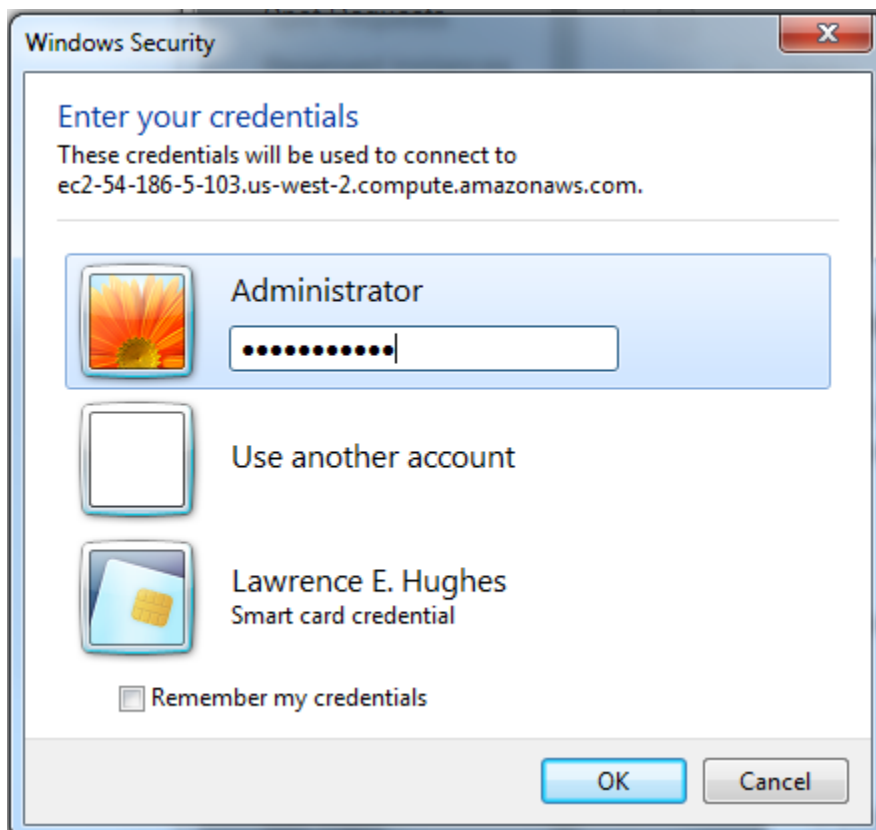


Copy the password string (highlight and Ctrl-C).

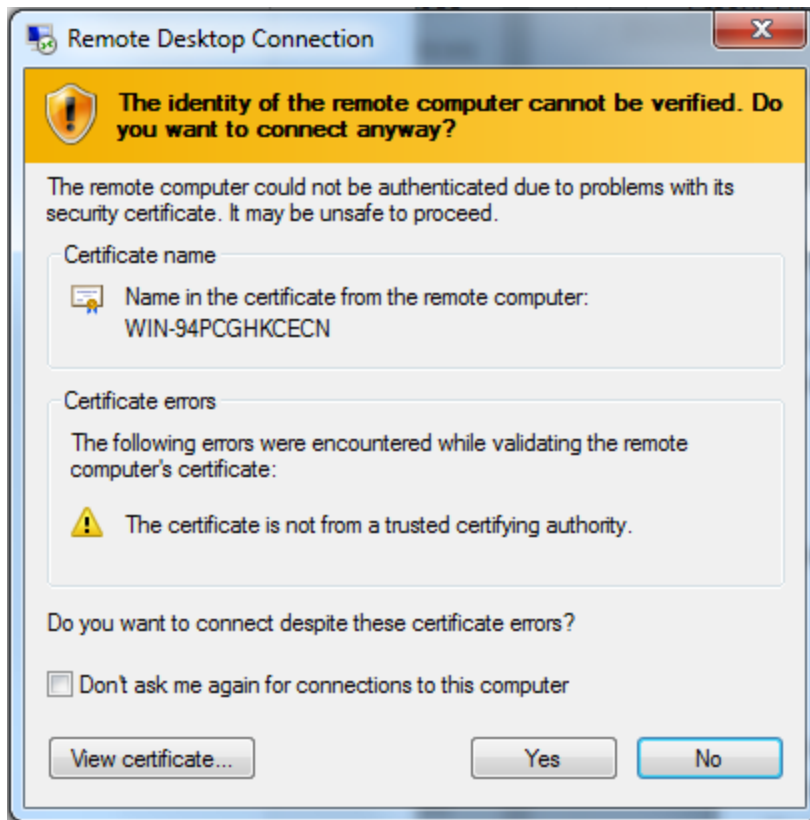
Invoke the downloaded RDP file by double clicking on it.



Click the *Connect* button.

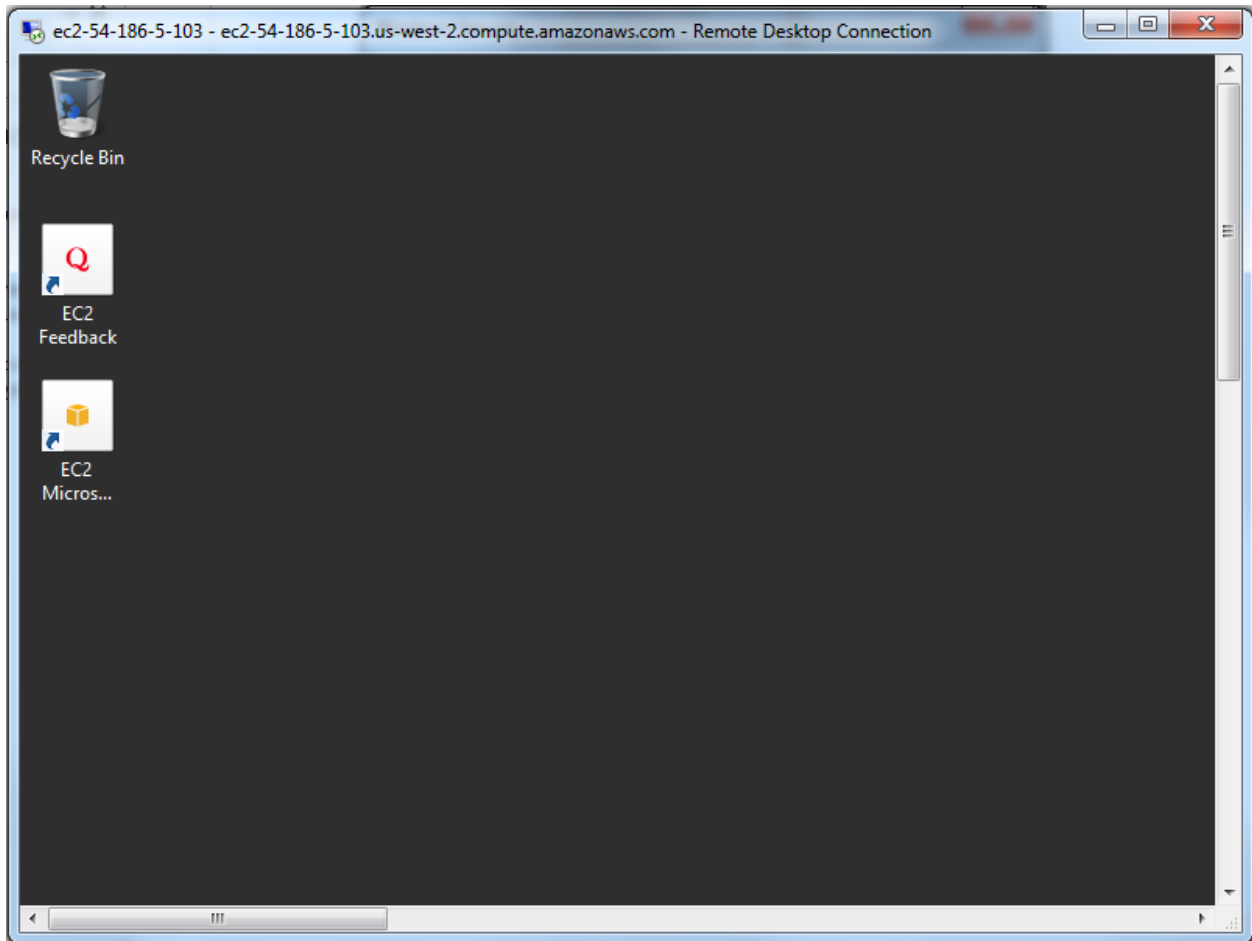


Paste the password in the password box (Ctrl-V). Click the *OK* button.

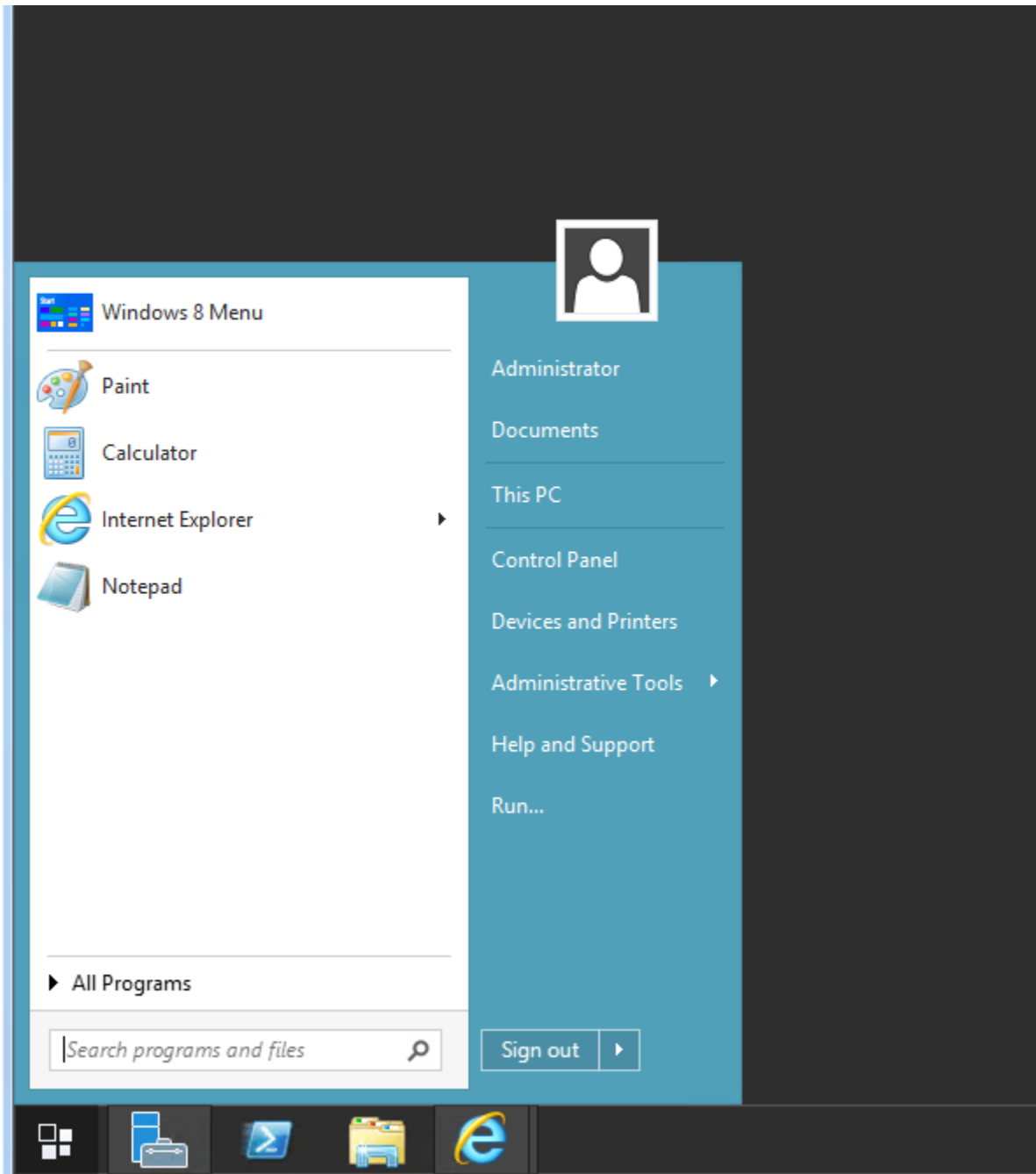


Confirm you want to connect by clicking the Yes button.

You are now connected to the new instance via RDP.



For Windows 8.x and Windows Serve 2012 R2, I like to install Start8 (from Stardock) to restore the *Start button* and *Menu*. If you are familiar with the WS2012R2 menus, feel free to use them instead.



Start Server Manager. Change the nodename and domain (e.g. to WS1.aws.sixsape.net).

Restart the server.

IP address management

By default, a random IPv6 global address has been assigned to your node. For example:

Primary private IPv4 IP	172.31.4.160
IPv4 Public IP	54.186.5.103*
IPv6 IPs	2600:1f14:611:b600:f38a:1743:e0f5:6923

The private IPv4 address is mapped to the public IPv4 address by AWS. You should not try to change it.

This is a static address (it won't change), but if you like you can change this to a manually assigned value.

To change the IPv6 address, go to *Network Interfaces* (on the EC2 dashboard), select the Windows Server 2012R2 primary network interface, then choose *Actions, Manage IP Addresses*.

Manage IP Addresses ✕

To add or edit an IPv4 public IP [Allocate an Elastic IP](#) to this instance or network interface.

▼ **eth0: eni-70edae71 - Primary network interface - 172.31.0.0/20**

IPv4 Addresses

Private IP	Public IP
172.31.4.160	54.186.5.103

[Assign new IP](#)

IPv6 Addresses

IP Addresses	
2600:1f14:611:b600:f38a:1743:e0f5:6923	Unassign

[Assign new IP](#)

Allow reassignment ⓘ

[Cancel](#) [Yes, Update](#)

Click *Assign new IP*.

IPv6 Addresses

IP Addresses	
2600:1f14:611:b600:f38a:1743:e0f5:6923	Unassign
2600:1f14:61	Undo

[Assign new IP](#)

[Cancel](#) [Yes, Update](#)

Where it says “Auto-assign” enter the new static address. The 64 bit prefix must be the same as before. For example, 2600:1f14:611:b600::2:1. Click *Yes, Update*.

IPv6 Addresses

IP Addresses	
2600:1f14:611:b600:f38a:1743:e0f5:6923	Unassign
2600:1f14:611:b600::2:1	Unassign

[Assign new IP](#)

The new manually assigned address has been added. You can get rid of the old randomly assigned address by clicking *Unassign*, then *Yes, Update*.

IPv6 Addresses

IP Addresses	
2600:1f14:611:b600::2:1	Unassign

[Assign new IP](#)

Now, this is your official IPv6 global address:

Primary private IPv4 IP	172.31.4.160
IPv4 Public IP	54.186.5.103*
IPv6 IPs	2600:1f14:611:b600::2:1

View Network Configuration with ipconfig

```
C:\Users\Administrator>ipconfig /all
```

Windows IP Configuration

```
Host Name . . . . . : WS1
Primary Dns Suffix . . . . . : aws.sixscape.net
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : us-west-2.ec2-utilities.amazonaws.com
                                us-east-1.ec2-utilities.amazonaws.com
                                ec2-utilities.amazonaws.com
                                ec2.internal
                                compute-1.internal
                                us-west-2.compute.internal
                                aws.sixscape.net
                                sixscape.net
```

Ethernet adapter Ethernet:

```
Connection-specific DNS Suffix . : us-west-2.compute.internal
Description . . . . . : AWS PV Network Device
Physical Address. . . . . : 0A-A7-88-E8-1F-8C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2600:1f14:611:b600::2:1 (Preferred)
Lease Obtained. . . . . : Friday, July 7, 2017 1:42:06 AM
Lease Expires . . . . . : Friday, July 7, 2017 2:44:36 AM
Link-local IPv6 Address . . . . . : fe80::f8de:efbf:a3fe:4e2d%12 (Preferred)
IPv4 Address. . . . . : 172.31.4.160 (Preferred)
Subnet Mask . . . . . : 255.255.240.0
Lease Obtained. . . . . : Friday, July 7, 2017 1:15:10 AM
Lease Expires . . . . . : Friday, July 7, 2017 3:15:10 AM
Default Gateway . . . . . : fe80::8b1:a0ff:fe86:78a6%12
                                172.31.0.1
DHCP Server . . . . . : 172.31.0.1
DHCPv6 IAID . . . . . : 203554827
DHCPv6 Client DUID. . . . . : 00-01-00-01-20-F0-91-74-0A-A7-88-E8-1F-8C

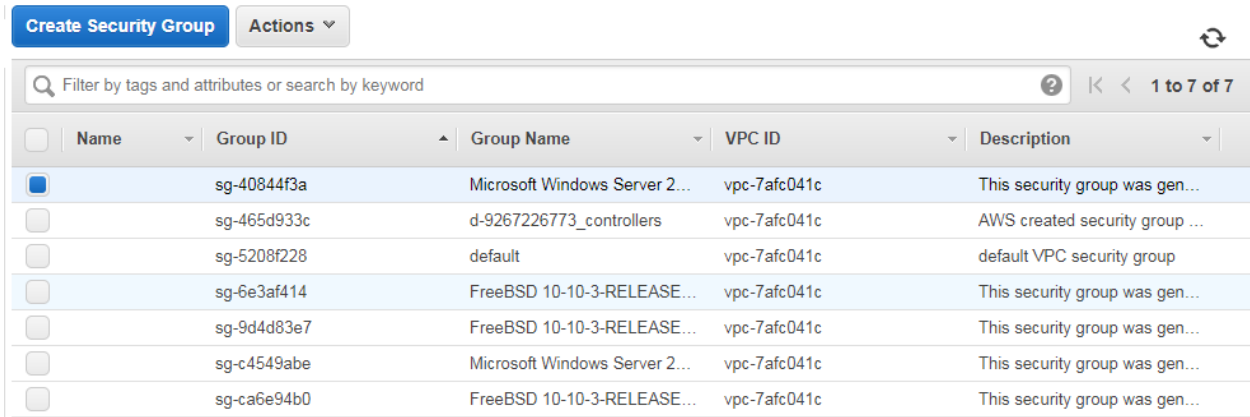
DNS Servers . . . . . : 172.31.0.2
NetBIOS over Tcpi . . . . . : EnabledNow try pinging your new node:
```

Notes:

- MAC address is 0a-a7-88-E8-1F-8C
- IPv4 private address is 172.31.4.160 (assigned by AWS via DHCPv4, it will be static)
- IPv4 netmask is 255.255.240.0 (/20)
- IPv4 default gateway is 172.31.0.1 (also address of DHCPv4 server)
- IPv4 address of DNS is 172.31.0.2
- IPv6 address is 2600:1f14:611:b600::2:1 (manually configured, but obtained via DHCPv6)
- IPv6 default gateway is fe80::8b1:a0ff:fe86:78a6 (discovered via ND)
- There are currently no IPv6 addresses for DNS (to be fixed)

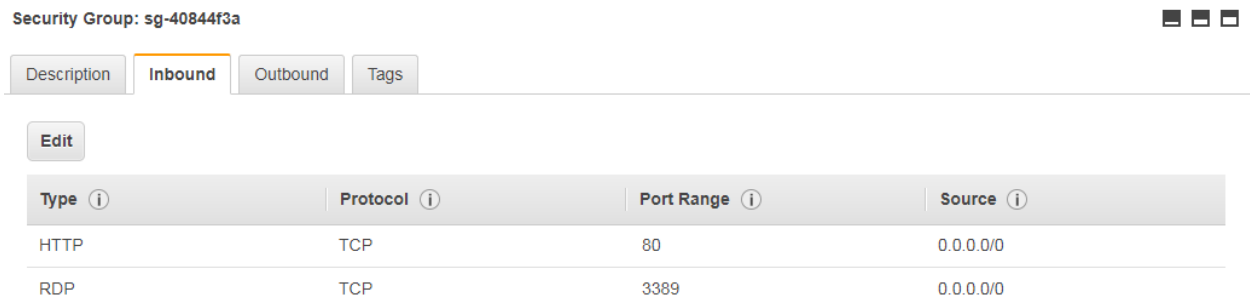
Firewall Rules

By default, a new security group (set of network access rules) has been created for you. You can think of this as a host-based firewall. Be aware that there is also a network level set of firewall rules that may also be affecting traffic to you. To view and change it, select *Security Groups*, then select only the one for the new Windows Server instance:



<input type="checkbox"/>	Name	Group ID	Group Name	VPC ID	Description
<input checked="" type="checkbox"/>		sg-40844f3a	Microsoft Windows Server 2...	vpc-7afc041c	This security group was gen...
<input type="checkbox"/>		sg-465d933c	d-9267226773_controllers	vpc-7afc041c	AWS created security group ...
<input type="checkbox"/>		sg-5208f228	default	vpc-7afc041c	default VPC security group
<input type="checkbox"/>		sg-6e3af414	FreeBSD 10-10-3-RELEASE...	vpc-7afc041c	This security group was gen...
<input type="checkbox"/>		sg-9d4d83e7	FreeBSD 10-10-3-RELEASE...	vpc-7afc041c	This security group was gen...
<input type="checkbox"/>		sg-c4549abe	Microsoft Windows Server 2...	vpc-7afc041c	This security group was gen...
<input type="checkbox"/>		sg-ca6e94b0	FreeBSD 10-10-3-RELEASE...	vpc-7afc041c	This security group was gen...

At the bottom, select *Inbound* to view the current rules:



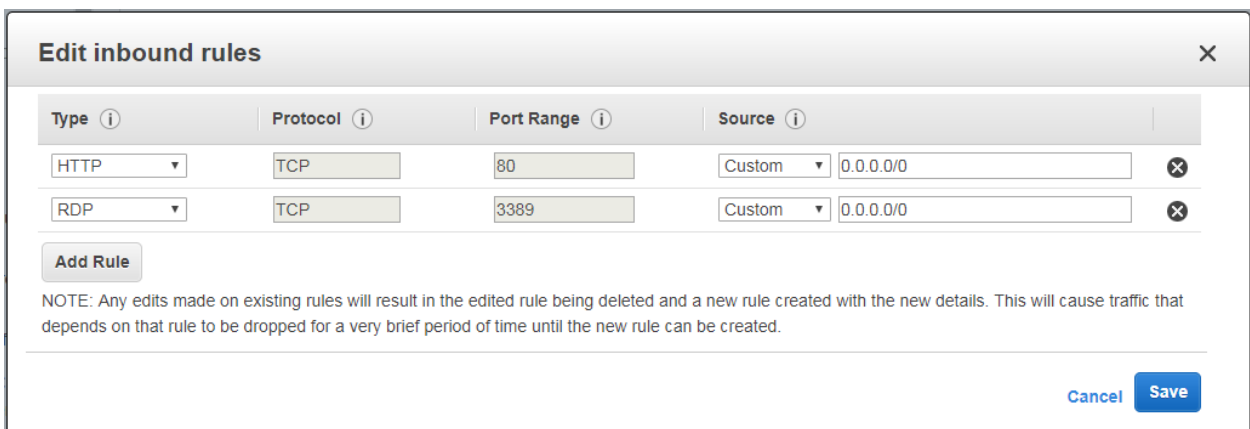
Security Group: sg-40844f3a

Description **Inbound** Outbound Tags

Edit

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
RDP	TCP	3389	0.0.0.0/0

Currently it will accept HTTP on port 80 and RDP on port 3389, over IPv4. All other incoming traffic is blocked. Click *Edit*:



Edit inbound rules

Type	Protocol	Port Range	Source
HTTP	TCP	80	Custom 0.0.0.0/0
RDP	TCP	3389	Custom 0.0.0.0/0

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Save

Allow HTTP and RDP on both IPv4 and IPv6. Click the box with 0.0.0.0/0 and add ", ::/0".. Do the same for RDP:

Edit inbound rules

Type	Protocol	Port Range	Source
HTTP	TCP	80	Custom 0.0.0.0/0, ::/0
RDP	TCP	3389	Custom 0.0.0.0/0, ::/0

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Save

Click **Save**. The new rules appear:

Security Group: sg-40844f3a

Description **Inbound** Outbound Tags

Edit

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0
HTTP	TCP	80	::/0
RDP	TCP	3389	0.0.0.0/0
RDP	TCP	3389	::/0

Allow ICMPv4 and ICMPv6 from anywhere (this will allow your new instance to receive pings). Click **Edit**. Click **Add Rule**.

Edit inbound rules

Type	Protocol	Port Range	Source
HTTP	TCP	80	Custom 0.0.0.0/0
HTTP	TCP	80	Custom ::/0
RDP	TCP	3389	Custom 0.0.0.0/0
RDP	TCP	3389	Custom ::/0
All ICMP - IPv4	ICMP	0 - 65535	Custom 0.0.0.0/0
All ICMP - IPv6	IPV6 ICMP	All	Custom ::/0

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Save

Add All ICMP-IPv4 to 0.0.0.0/0 and all ICMP-IPv6 to ::/0. Click **Save**.

Description Inbound Outbound Tags

Edit

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTP	TCP	80	0.0.0.0/0
HTTP	TCP	80	::/0
Custom ICMP Rule - IPv6	All	N/A	::/0
RDP	TCP	3389	0.0.0.0/0
RDP	TCP	3389	::/0
All ICMP - IPv4	All	N/A	0.0.0.0/0

Now, trying pinging the IPv4 and IPv6 global addresses from any outside node:

```
C:\Windows\system32>ping 54.186.5.103
```

```
Pinging 54.186.5.103 with 32 bytes of data:  
Reply from 54.186.5.103: bytes=32 time=195ms TTL=112  
Reply from 54.186.5.103: bytes=32 time=194ms TTL=112  
Reply from 54.186.5.103: bytes=32 time=194ms TTL=112  
Reply from 54.186.5.103: bytes=32 time=195ms TTL=112
```

```
Ping statistics for 54.186.5.103:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 194ms, Maximum = 195ms, Average = 194ms
```

```
C:\Windows\system32>ping 2600:1f14:611:b600::2:1
```

```
Pinging 2600:1f14:611:b600::2:1 with 32 bytes of data:  
Reply from 2600:1f14:611:b600::2:1: time=226ms  
Reply from 2600:1f14:611:b600::2:1: time=226ms  
Reply from 2600:1f14:611:b600::2:1: time=226ms  
Reply from 2600:1f14:611:b600::2:1: time=226ms
```

```
Ping statistics for 2600:1f14:611:b600::2:1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 226ms, Maximum = 226ms, Average = 226ms
```