



# SelectSurvey.NET AWS (Amazon Web Service) Integration

Written for V4.146.000 10/2015





## SelectSurvey.NET AWS Integration

This document is a guide to deploy SelectSurvey.NET into AWS Amazon Web Services in the Cloud.

### Contents

SelectSurvey.NET AWS (Amazon Web Service) Integration.....	1
SelectSurvey.NET AWS Integration.....	2
Setup AWS Amazon Subscription .....	3
Create an IAM User .....	3
Create a Key Pair .....	11
Create an EC2 Virtual Windows Server.....	16
Install SelectSurvey.NET on to the virtual server .....	24



## Setup AWS Amazon Subscription

A pre-requisite for deploying SelectSurvey.NET to the AWS Amazon Web Services cloud is to sign up for AWS through <http://aws.amazon.com>.

1. Signup AWS free account here: <http://aws.amazon.com/>
2. Once you complete **Contact Information**, **Payment Information**, **Identity Verification** you will need to choose **Support Plan**. Choose the one fits to your need. For this example we will choose **Basic (Free)**.



### Support Plan

All customers receive free support. Choosing a paid support plan will allow you to receive one-on-one technical assistance from experienced engineers and access many other support features. Please see below.

Please Select One

**Basic (Free)**

Contact Customer Service for account and billing questions, receive help for resources that don't pass system health checks, and access the AWS Community Forums.

**Developer (\$49/month)**

Get started on AWS - ask technical questions and get a response to your web case within 12 hours during local business hours.

**Business (Starting at \$100/month - Pricing Example) - Recommended**

24/7/365 real-time assistance by phone and chat, a 1 hour response to web cases, and help with 3rd party software. Access AWS Trusted Advisor to increase performance, fault tolerance, security, and potentially save money. ?

**Enterprise**

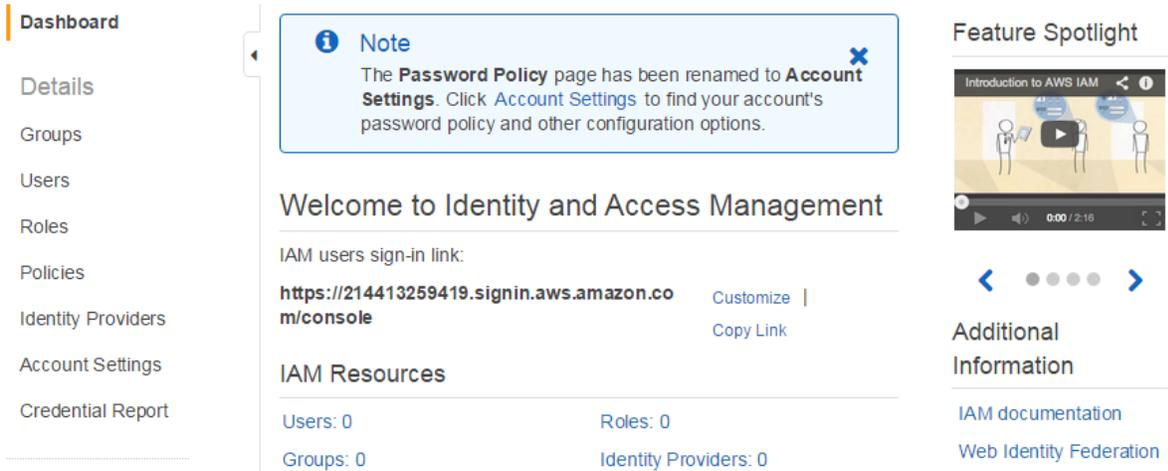
15 minute response to web cases, an assigned technical account manager (TAM) who is an expert in your use case, and white-glove case handling that notifies your TAM and the service engineering team of a critical issue.

*If you select this option, you will not be charged immediately. We will contact you to discuss your needs and finalize the signup.*

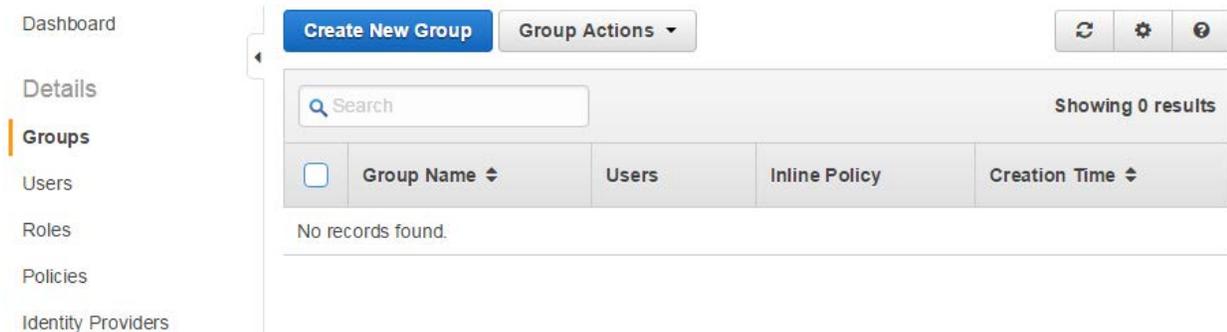
Continue

## Create an IAM User

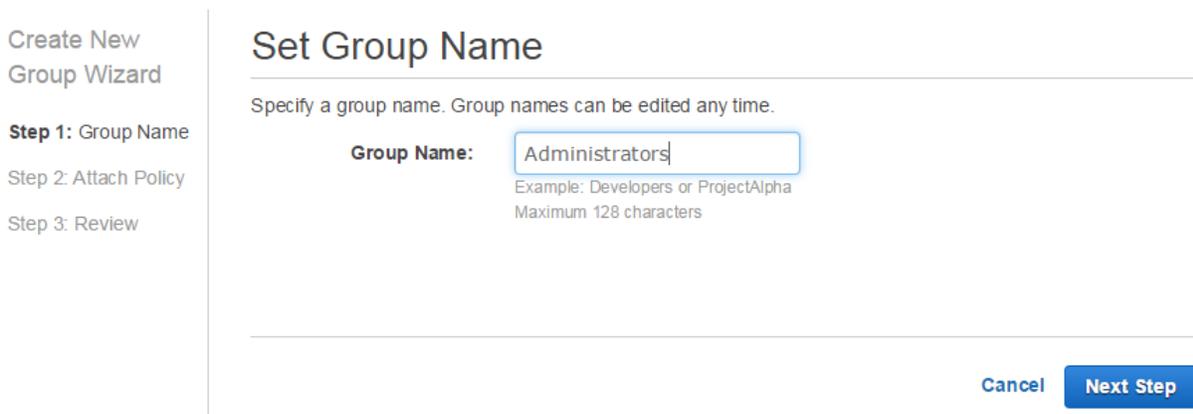
1. Go to <https://console.aws.amazon.com/iam/> and click Groups on the left pane.



2. Click **Create New Group** button.



3. Give a name to your group such as *Administrators* and click **Next Step** button.



4. Type *AdministratorAccess* into search box and choose the checkbox on the left side of **AdministratorAccess** line and click **Next Step** button.

Create New  
Group Wizard

Step 1: Group Name

**Step 2: Attach Policy**

Step 3: Review

## Attach Policy

Select one or more policies to attach. Each group can have up to 10 policies attached.

Filter: Policy Type  Showing 1 results

	Policy Name	Attached Entities	Creation Time	Edited Time
<input checked="" type="checkbox"/>	AdministratorAcce...	0	2015-02-06 12:39 C...	2015-02-06 12...

Cancel Previous **Next Step**

- Review the group you created and click **Create Group** button.

Create New  
Group Wizard

Step 1: Group Name

Step 2: Attach Policy

**Step 3: Review**

## Review

Review the following information, then click **Create Group** to proceed.

<b>Group Name</b>	Administrators	<a href="#">Edit Group Name</a>
<b>Policies</b>	arn:aws:iam::aws:policy/AdministratorAccess	<a href="#">Edit Policies</a>

Cancel Previous **Create Group**

- Create IAM User: Click Users on the left pane, type the user name such as *adminUsers* and click **Create New Users** button.

- Dashboard
- Details
- Groups
- Users**
- Roles
- Policies
- Identity Providers
- Account Settings
- Credential Report

**Create New Users**
User Actions ▾

↻
⚙️
ℹ️

Showing 0 results

<input type="checkbox"/>	User Name ⇅	Groups	Password	Password Last Used ⇅	Access Keys	Creation T
No records found.						

7. Enter user names and **uncheck** **Generate an access key for each user** checkbox. Then click **Create** button.

Create User

**Enter User Names:**

1.
2.
3.
4.
5.

Maximum 64 characters each

---

**Generate an access key for each user**

Users need access keys to make secure REST or Query protocol requests to AWS service APIs.  
*For users who need access to the AWS Management Console, create a password in the Users panel after completing this wizard.*

Cancel **Create**

8. Check the users you want to add to Groups.

- Dashboard
- Details
- Groups
- Users**
- Roles
- Policies
- Identity Providers
- Account Settings
- Credential Report

---

- Encryption Keys

**Create New Users**
User Actions ▾

↻
⚙️
?

Showing 1 results

<input checked="" type="checkbox"/>	User Name ↕	Password Last Used ↕	Access Keys	Creation Time
<input checked="" type="checkbox"/>	user1		None	2015-10-10

- Add User to Groups
- Delete User
- Manage Access Keys
- Manage Password
- Manage Signing Certificates
- Manage MFA Device
- Remove User from Groups

9. Check the checkbox on the left side of the Group you wanted to add the user to and click **Add to Groups** button.

Add User to Groups

Select groups that user **user1** will be added to.

Showing 1 results

<input type="checkbox"/>	Group Name ↕	Users	Inline Policy	Creation Time ↕
<input checked="" type="checkbox"/>	Administrators	0		2015-10-10 00:23 CDT

Cancel
Add to Groups

10. As of right now we haven't set up password to our IAM and it should be empty. Click the user line to set up new password for IAM.

Dashboard

Details

Groups

**Users**

Roles

Policies

Identity Providers

Create New Users    User Actions ▾    [Refresh] [Settings] [Help]

Search     Showing 1 results

<input type="checkbox"/>	User Name ↕	Groups	Password	Password Last Used ↕	Access Keys	Creation T
<input type="checkbox"/>	user1	1		2015-10-10 01:11 CDT	None	2015-10-10

11. From the **Sign-In Credential** Section choose **Manage Password** button.

Use access keys to make secure REST or Query protocol requests to any AWS service API. For your protection, you should never share your secret keys with anyone. In addition, industry best practice recommends frequent key rotation. [Learn more about Access Keys](#)

This user does not currently have any access keys.

[Create Access Key](#)

#### Sign-In Credentials ^

**User Name** user1

[Manage Password](#)

**Password** No

**Last Used** 2015-10-10 01:11 CDT

**Multi-Factor Authentication Device** No

[Manage MFA Device](#)

**Signing Certificates** None

[Manage Signing Certificates](#)

#### SSH keys for AWS CodeCommit ^

Use SSH public keys to authenticate to AWS CodeCommit repositories. [Learn more about SSH keys](#).  
No SSH public keys are associated with this user.

[Upload SSH public key](#)

12. Choose **Assign a custom password** and click **Apply** button.

Manage Password

Users who will be using the AWS Management Console require a password. Select from the options below to manage the password for user user1.

Assign an auto-generated password  
 Assign a custom password  
 Password:   
 Confirm Password:

Require user to create a new password at next sign-in

Cancel **Apply**

13. On that Users you can see your account info. Copy and save your AWS Account ID: 123412341234.

Dashboard

Details

Groups

**Users**

Roles

Policies

Identity Providers

Account Settings

Credential Report

---

Encryption Keys

IAM > Users > user1

▼ Summary

**User ARN:** arn:aws:iam::214413259419:user/user1

**Has Password:** Yes

**Groups (for this user):** 1

**Path:** /

**Creation Time:** 2015-10-10 00:30 CDT

▼ Groups

This view shows all groups the User belongs to: **1 Group** **Add User to Groups**

Group	Actions

14. To sign in as new IAM user use this URL [https://your\\_aws\\_account\\_id.signin.aws.amazon.com/console/](https://your_aws_account_id.signin.aws.amazon.com/console/) and replace the your\_aws\_account\_id with your AWS account ID. It will ask your username and password.

Account:

User Name:

Password:

I have an MFA Token ([more info](#))

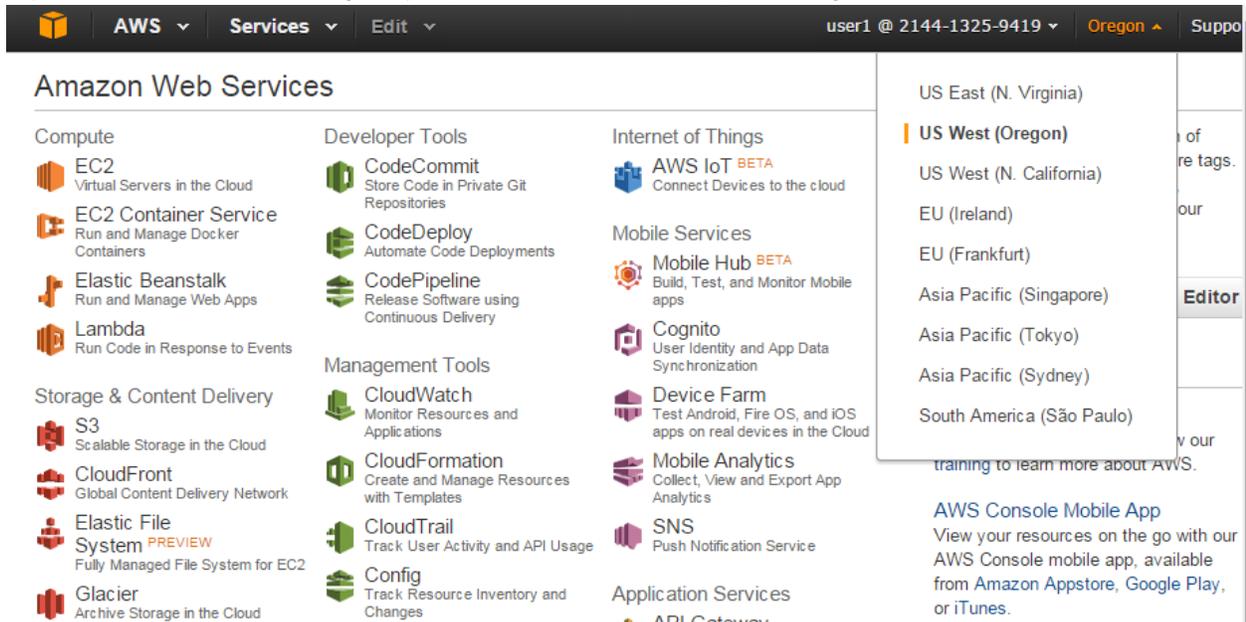
[Sign In](#)

[Sign-in using root account credentials](#)

## Create a Key Pair

### Create a Key Pair

15. If you haven't chosen a region yet please choose appropriate region and then choose EC2 from the list:



The screenshot shows the AWS Management Console interface. At the top, the navigation bar includes 'AWS', 'Services', 'Edit', and the user profile 'user1 @ 2144-1325-9419' in the 'Oregon' region. The main content area is titled 'Amazon Web Services' and displays a grid of service categories and their respective icons and descriptions. A dropdown menu is open on the right side, showing a list of regions: US East (N. Virginia), US West (Oregon) (highlighted), US West (N. California), EU (Ireland), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), and South America (São Paulo). Below the region list, there are links for 'training to learn more about AWS', 'AWS Console Mobile App', and a description of the mobile app.

16. Click the **Key Pairs** link.

- EC2 Dashboard**
- Events
- Tags
- Reports
- Limits
- INSTANCES
  - Instances
  - Spot Requests
  - Reserved Instances
- IMAGES
  - AMIs
  - Bundle Tasks
- ELASTIC BLOCK STORE
  - Volumes
  - Snapshots
- NETWORK & SECURITY
  - Security Groups

## Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region:

0 Running Instances	0 Elastic IPs
0 Volumes	0 Snapshots
0 Key Pairs	0 Load Balancers
0 Placement Groups	1 Security Groups

Easily deploy and operate applications - use Chef recipes, manage SSH users, and more. [Try OpsWorks now.](#) Hide

## Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

[Launch Instance](#)

Note: Your instances will launch in the US West (Oregon) region

## Account Attributes

[Supported Platforms](#)  
VPC

[Default VPC](#)  
vpc-b12b61d4

## Additional Information

[Getting Started Guide](#)  
[Documentation](#)

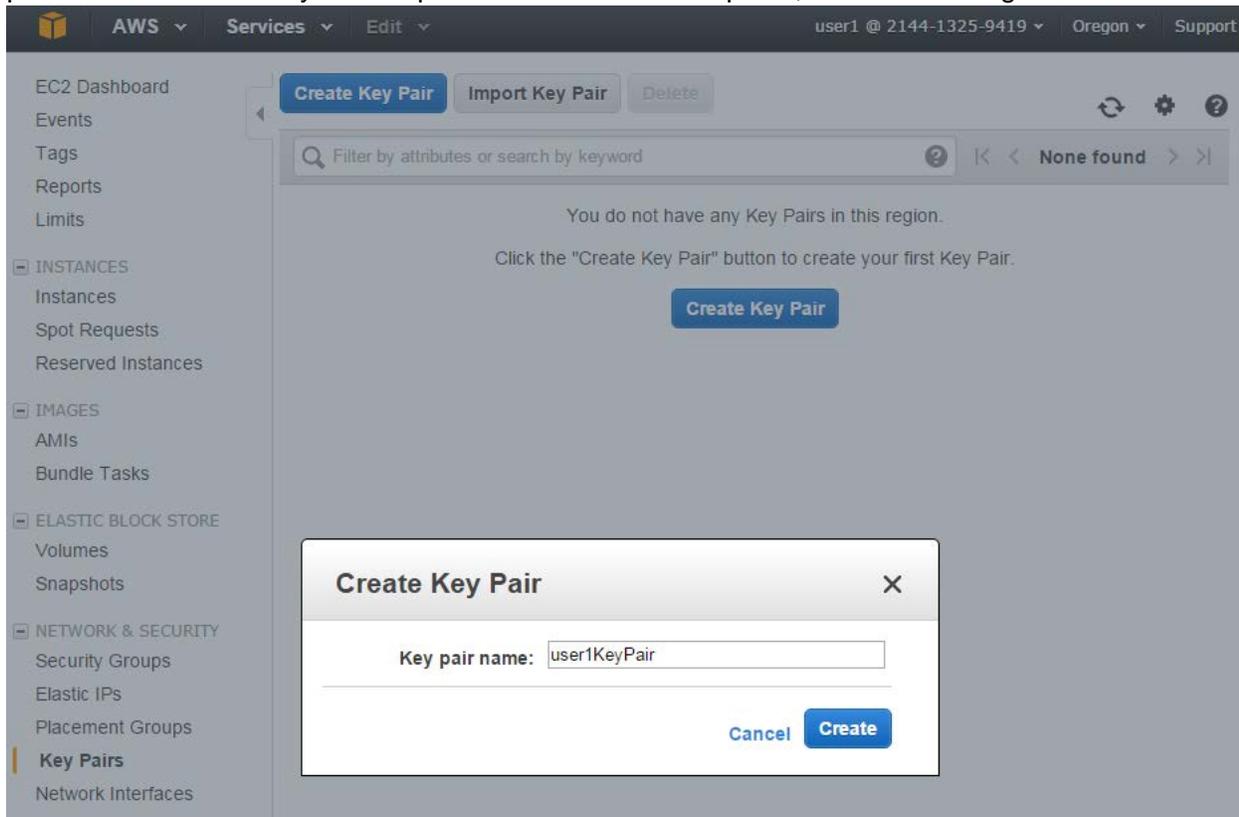
[All EC2 Resources](#)  
[Forums](#)

[Pricing](#)  
[Contact Us](#)

## AWS Marketplace

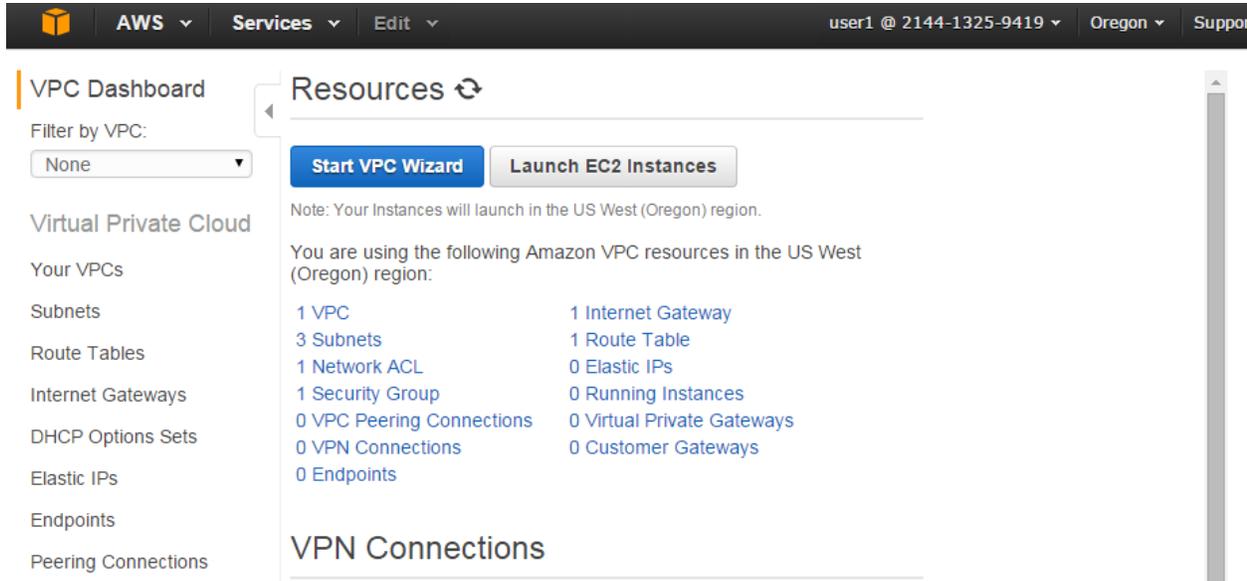
Find **free software trial** products in the AWS

- Click **Create a Key Pair** button, give a name to your key pair and click Create button. It should create key pair and downloads to your computer. Save it in secure place, we will be using it soon.



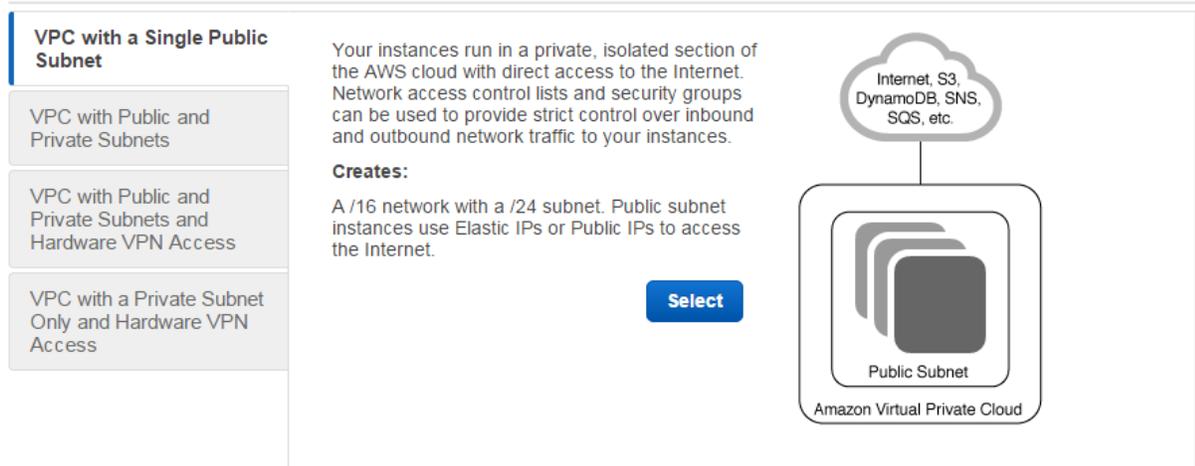
The screenshot shows the AWS Management Console interface. The left sidebar contains navigation options like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, and NETWORK & SECURITY. The main content area shows the 'Key Pairs' page with a 'Create Key Pair' button. A modal dialog box titled 'Create Key Pair' is open, with a text input field for 'Key pair name' containing 'user1KeyPair' and 'Create' and 'Cancel' buttons.

18. Open the Amazon VPC console at <https://console.aws.amazon.com/vpc/> and choose region. On the VPC dashboard, click **Start VPC Wizard** button.



19. On the Set 1 **VPC with a Single Public Subnet** is selected. Just click **Select** button.

Step 1: Select a VPC Configuration



[Cancel and Exit](#)

20. On the Step 2 give a VPC name and click **Create** button.

## Step 2: VPC with a Single Public Subnet

IP CIDR block:\*  (65531 IP addresses available)

VPC name:

---

Public subnet:\*  (251 IP addresses available)

Availability Zone:\*

Subnet name:

You can add more subnets after AWS creates the VPC.

---

Add endpoints for S3 to your subnets

Subnet:

---

Enable DNS hostnames:\*  Yes  No

Hardware tenancy:\*

---

[Cancel and Exit](#) [Back](#) [Create VPC](#)

21. You should receive Success Message and click **OK** button.

VPC Dashboard

Filter by VPC:

Virtual Private Cloud

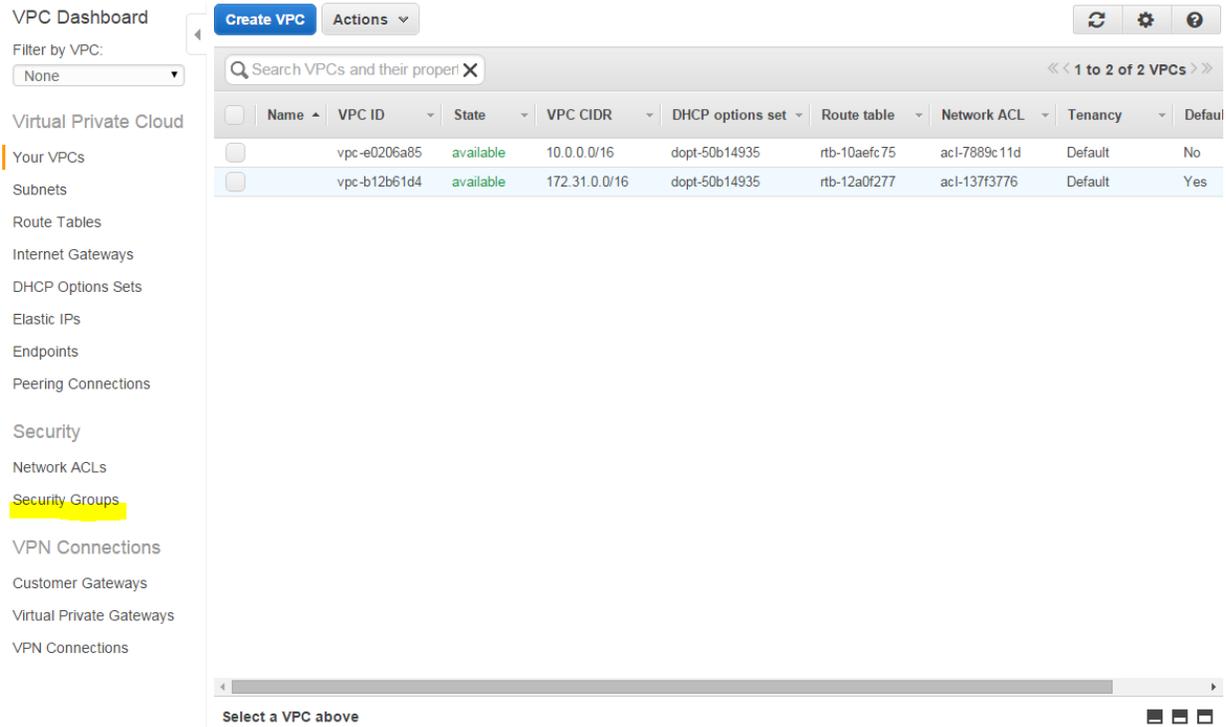
- Your VPCs
- Subnets
- Route Tables

### VPC Successfully Created

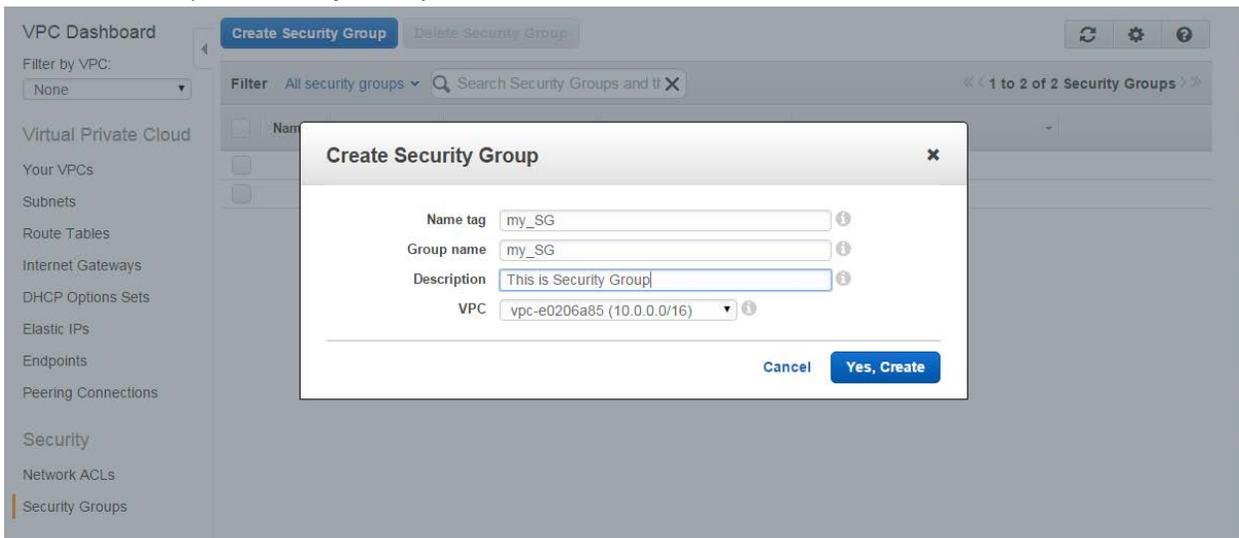
Your VPC has been successfully created.  
You can launch instances into the subnets of your VPC. For more information, see [Launching an Instance into Your Subnet](#).

[OK](#)

22. To create a security group with least privilege and click **Security Groups** on the left pane.



23. Click **Create Security Group** button. Give a name, description, VPC (make sure to choose VPC you created before) to Security Group and click **Yes, Create** button.



24. On the **Inbound** tab, create the following rules (click **Add Rule** for each new rule), and then click **Create**:

Select HTTP from the Type list, and make sure that Source is set to Anywhere (0.0.0.0/0).

Select HTTPS from the Type list, and make sure that Source is set to Anywhere (0.0.0.0/0). Select RDP from the Type list. In the Source box, ensure Custom IP is selected, and specify the public IP address of your computer or network in CIDR notation. To specify an individual IP address in CIDR notation, add the routing prefix /32. For example, if your IP address is 203.0.113.25, specify 203.0.113.25/32. If your company allocates addresses from a range, specify the entire range, such as 203.0.113.0/24.

#### Caution

For security reasons, we don't recommend that you allow RDP access from all IP addresses (0.0.0.0/0) to your instance, except for testing purposes and only for a short time.

25. Once you complete Sign In into AWS Console by using your login and password. Then click **EC2**.

## Create an EC2 Virtual Windows Server

### Amazon Web Services

#### Compute

-  **EC2**  
Virtual Servers in the Cloud
-  **EC2 Container Service**  
Run and Manage Docker Containers
-  **Elastic Beanstalk**  
Run and Manage Web Apps
-  **Lambda**  
Run Code in Response to Events

#### Developer Tools

-  **CodeCommit**  
Store Code in Private Git Repositories
-  **CodeDeploy**  
Automate Code Deployments
-  **CodePipeline**  
Release Software using Continuous Delivery

#### Internet of Things

-  **AWS IoT** BETA  
Connect Devices to the cloud

#### Mobile Services

-  **Mobile Hub** BETA  
Build, Test, and Monitor Mobile apps
-  **Cognito**  
User Identity and App Data

26. In order to choose OS for our server click Launch Instance.

- EC2 Dashboard**
- Events
- Tags
- Reports
- Limits
- INSTANCES
  - Instances
  - Spot Requests
  - Reserved Instances
- IMAGES
  - AMIs
  - Bundle Tasks
- ELASTIC BLOCK STORE
  - Volumes
  - Snapshots
- NETWORK & SECURITY

## Resources

You are using the following Amazon EC2 resources in the US West (Oregon) region:

0 Running Instances	0 Elastic IPs
0 Volumes	0 Snapshots
0 Key Pairs	0 Load Balancers
0 Placement Groups	1 Security Groups

... Easily deploy and operate applications - use Chef recipes, manage SSH users, and more. [Try OpsWorks now.](#) Hide

## Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

[Launch Instance](#)

Note: Your instances will launch in the US West (Oregon) region

## Account Attributes

Supported Platforms  
VPC

Default VPC  
vpc-b12b61d4

## Additional Information

[Getting Started Guide](#)  
[Documentation](#)  
[All EC2 Resources](#)  
[Forums](#)  
[Pricing](#)  
[Contact Us](#)

## AWS Marketplace

Find **free software trial**

27. For this example we will choose **Microsoft Windows Server 2012 R2 Base**.

### Step 1: Choose an Amazon Machine Image (AMI)

 <b>Red Hat</b>	Free tier eligible	Red Hat Enterprise Linux version 7.1 (HVM), EBS General Purpose (SSD) Volume Type	64-bit
		Root device type: ebs    Virtualization type: hvm	
 <b>SUSE Linux</b>	Free tier eligible	<b>SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7</b>	<a href="#" style="background-color: #0070c0; color: white; padding: 5px 10px; border-radius: 3px;">Select</a>
		SUSE Linux Enterprise Server 12 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.	64-bit
		Root device type: ebs    Virtualization type: hvm	
 <b>Ubuntu</b>	Free tier eligible	<b>Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-5189a661</b>	<a href="#" style="background-color: #0070c0; color: white; padding: 5px 10px; border-radius: 3px;">Select</a>
		Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical ( <a href="http://www.ubuntu.com/cloud/services">http://www.ubuntu.com/cloud/services</a> ).	64-bit
		Root device type: ebs    Virtualization type: hvm	
 <b>Windows</b>	Free tier eligible	<b>Microsoft Windows Server 2012 R2 Base - ami-dfccd1ef</b>	<a href="#" style="background-color: #0070c0; color: white; padding: 5px 10px; border-radius: 3px;">Select</a>
		Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]	64-bit
		Root device type: ebs    Virtualization type: hvm	

[Cancel and Exit](#)

28. Make sure you choose t2.micro type.

## Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation [Show/Hide Columns](#)

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Net Perform
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to

29. Click Review and Launch.

30. If this is for developing purposes you don't have to create any security group but it is not recommended. Use the Security Group you created.

## Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

**⚠ Improve your instances' security. Your security group, launch-wizard-1, is open to the world.**  
 Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.  
 You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

### AMI Details

[Edit AMI](#)

 **Microsoft Windows Server 2012 R2 Base - ami-dfccd1ef**  
 Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]  
 Free tier eligible  
 Root Device Type: ebs   Virtualization type: hvm

### Instance Type

[Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

### Security Groups

[Edit security groups](#)

31. Click **Launch** button. Then check the acknowledge checkbox and click **Launch Instances** button.

## 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](#).

Choose an existing key pair

### Select a key pair

user1KeyPair

I acknowledge that I have access to the selected private key file (user1KeyPair.pem), and that without this file, I won't be able to log into my instance.

Cancel

Launch Instances

32. Click **View Instances** button.

## Launch Status

**✓ Your instances are now launching**

The following instance launches have been initiated: [i-398d7cfd](#) [View launch log](#)

**🗨 Get notified of estimated charges**

Create [billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

### How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

- [How to connect to your Windows instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Microsoft Windows Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

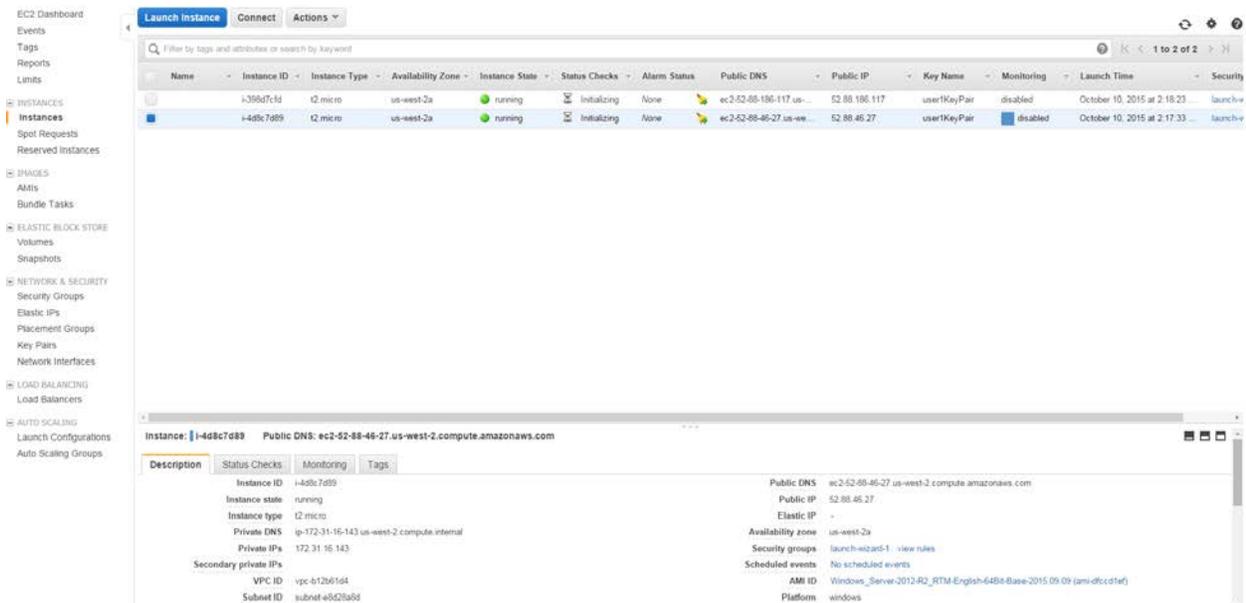
[Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)

[Create and attach additional EBS volumes](#) (Additional charges may apply)

[Manage security groups](#)

[View Instances](#)

33. You should see your instance in the list of instances.



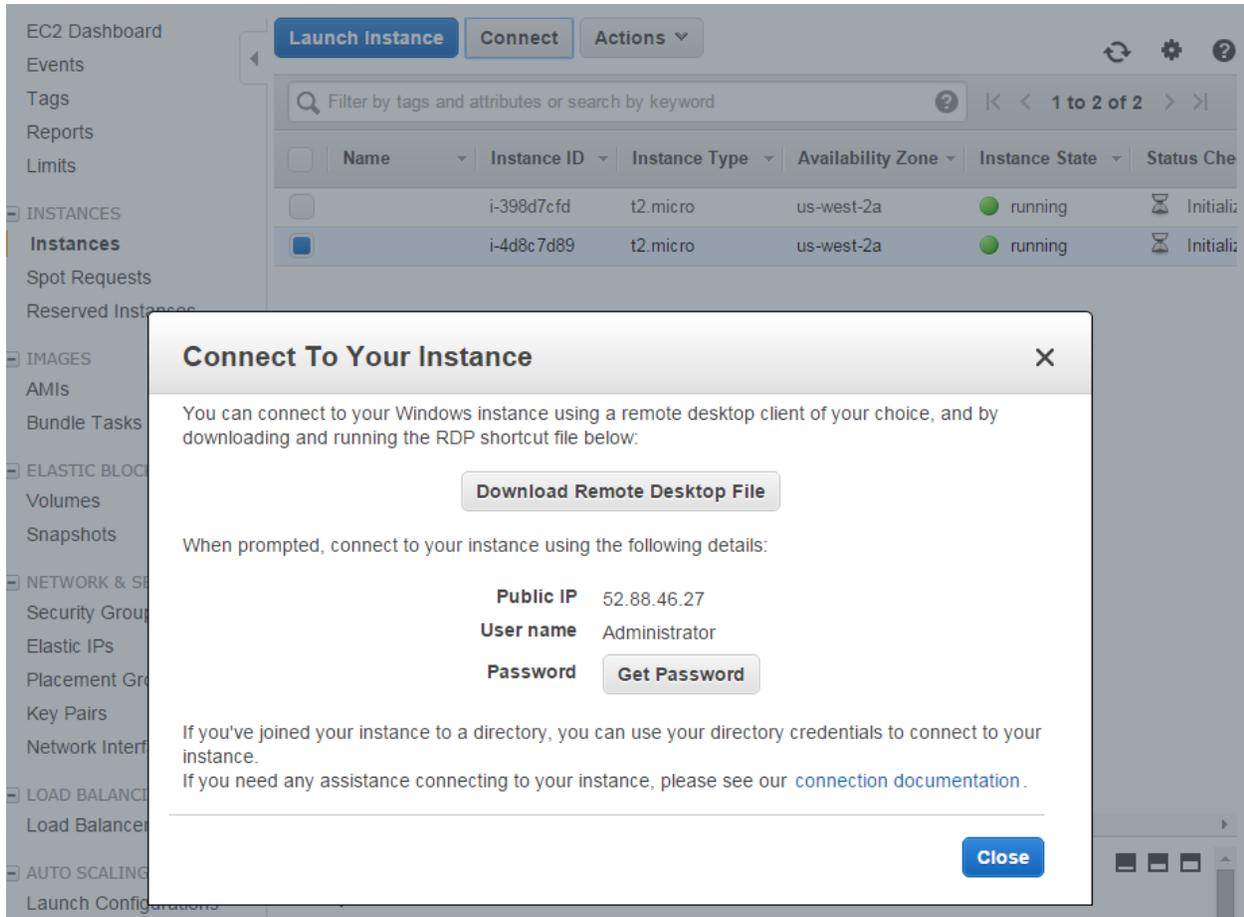
The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area displays a table of EC2 instances. Two instances are listed, both in the 'running' state. The second instance, i-4d8c7d89, is selected. Below the table, the details for this instance are shown, including its name, public DNS, public IP, instance type (t2.micro), availability zone (us-west-2a), and various configuration parameters like VPC ID and Subnet ID.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP	Key Name	Monitoring	Launch Time	Security
	i-398d7cfd	t2.micro	us-west-2a	running	Initializing	None	ec2-52-88-186-117.us-...	52.88.186.117	user1KeyPair	disabled	October 10, 2015 at 2:18:23	launch...
	i-4d8c7d89	t2.micro	us-west-2a	running	Initializing	None	ec2-52-88-46-27.us-we...	52.88.46.27	user1KeyPair	disabled	October 10, 2015 at 2:17:33	launch...

Instance: **i-4d8c7d89** Public DNS: **ec2-52-88-46-27.us-west-2.compute.amazonaws.com**

Description	Status Checks	Monitoring	Tags
Instance ID	i-4d8c7d89		
Instance state	running		
Instance type	t2.micro		
Private DNS	ip-172-31-16-143.us-west-2.compute.internal		
Private IP	172.31.16.143		
Secondary private IPs			
VPC ID	vpc-61266164		
Subnet ID	subnet-4820a8d4		
Public DNS	ec2-52-88-46-27.us-west-2.compute.amazonaws.com		
Public IP	52.88.46.27		
Elastic IP	-		
Availability zone	us-west-2a		
Security groups	launch-wizard-1 - view rules		
Scheduled events	No scheduled events		
AMI ID	Windows_Server-2012-R2_RTM-English-64Bit-Base-2015.09.09 (ami-dfccc1ef)		
Platform	windows		

34. In order to connect to your server via RDP, choose your instance and click **Connect** button. The “Connect to Your Instance” window should pop up. You can download Remote Desktop file for connection or you can use Public IP and Username. To get the password click **Get Password** button.



35. Choose the Key Pair file you downloaded earlier. To Decrypt the password click **Decrypt Password** button.

## Connect To Your Instance > Get Password



The following Key Pair was associated with this instance when it was created.

**Key Name** user1KeyPair.pem

In order to retrieve your password you will need to specify the path of this Key Pair on your local machine:

**Key Pair Path**  user1KeyPair.pem

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

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAgEHLwnIldHfF/QXDnp9QVvoI9aOARDCChd8DrImaLhjoUndC0y2oOA1NVTk
NS2YkFHevh01MOTT6MwTtdFdFnloF+nvkB2wI1kLNofNj+IcIV2a+2RUW//tsJpwP8rHtiHhzcft
Lba+z1iJSLeDUzHcaT9/IY+wuN55d12HFViNKcnQfpgUGIV0Poe+h9g4Hy8M888jG1kF731RChnq
Da2MM3a0ltczQE3pUUAHB0DNqJcYcU07CU+5f756qpVMZrxX4pa1Ka8Lm3n0MMS5xBCTYmbIQIAu
```

36. Now you should see all the information you need to connect to your.

### 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:

<b>Public IP</b>	52.88.46.27
<b>User name</b>	Administrator
<b>Password</b>	EK3j7@;Eeo

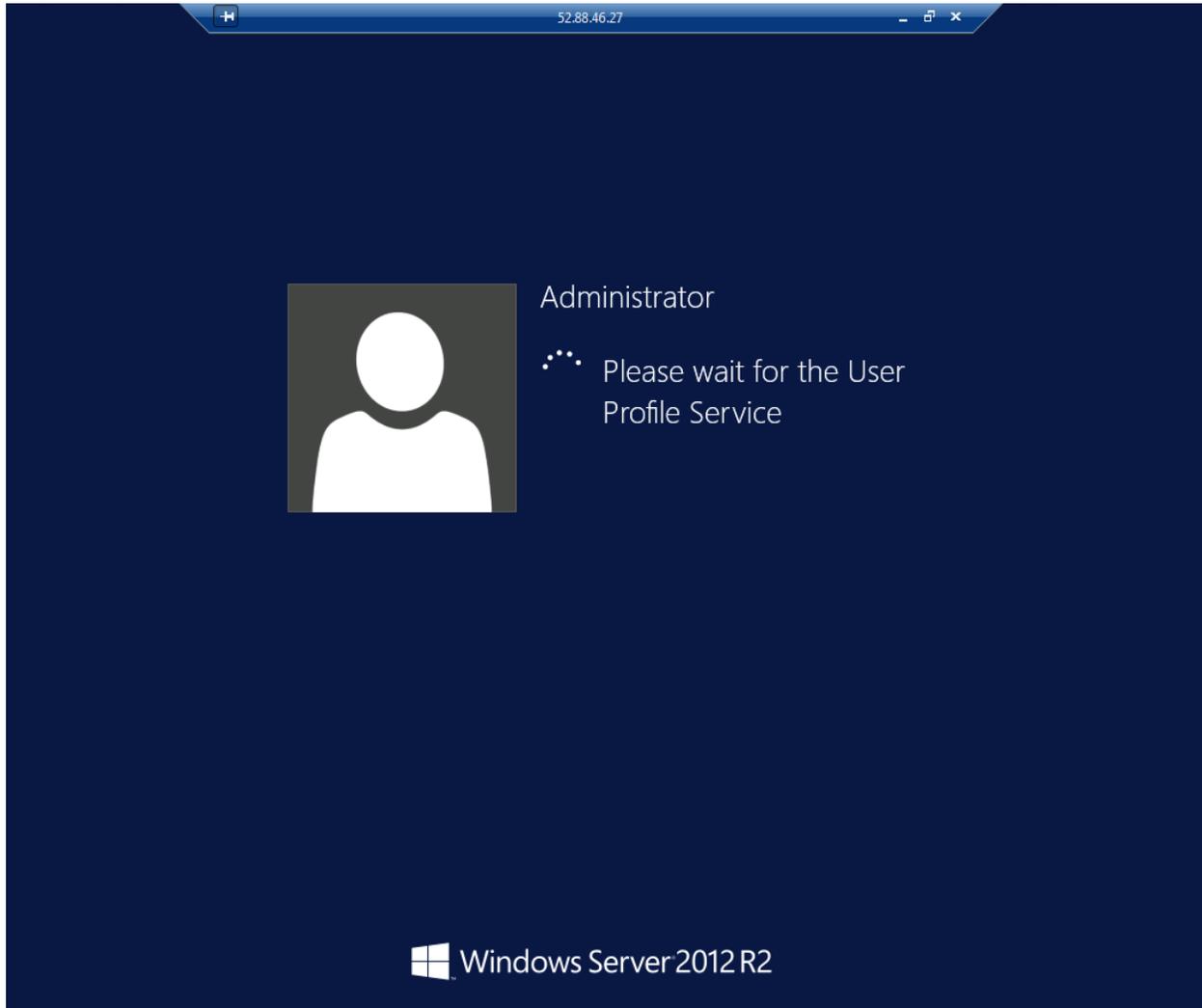
If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.  
If you need any assistance connecting to your instance, please see our [connection documentation](#).

---

[Close](#)

server.39.

37. Login to you server with the information. First time it takes several minutes to setup your server.



Finally you should see your server is ready for the installation of SelectSurvey.NET.

### *Install SelectSurvey.NET on to the virtual server*

Now follow the SelectSurvey.NET Installation guide for a normal server software install.