SELF-HOSTED

MULTI-TIER: COMMERCIAL VERSION INSTALLATION GUIDE

Version 11.0

CloudCheckr

TABLE OF CONTENTS

Introduction

This document describes how to configure a Multi-Tiered – Commercial version of CloudCheckr.

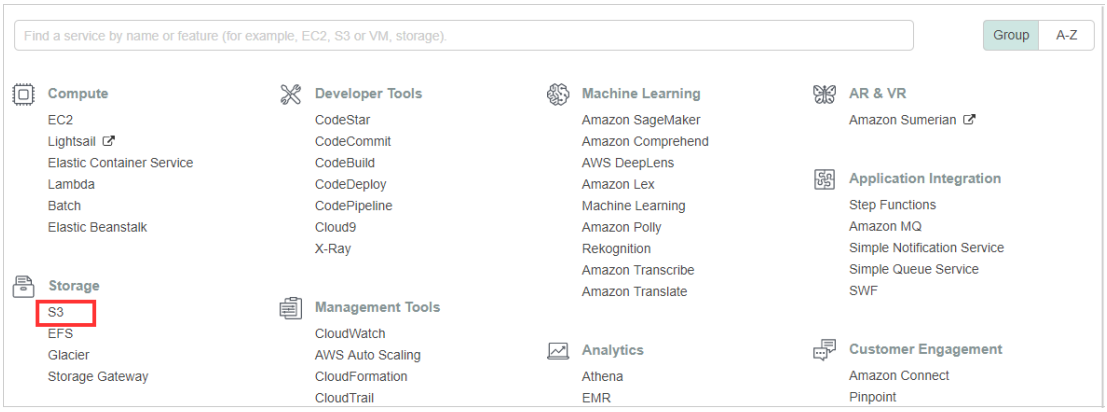
This version enables customers to use an Amazon Machine Image (AMI) to create a self-hosted version of the application within a virtual private cloud (VPC) on an Amazon Elastic Compute Cloud (Amazon EC2) instance using RDS databases.

Note: These instructions require you to record key information generated from your EC2 instances. For your convenience, use the form at the back of this document to record the data. Items you may wish to copy are highlighted in yellow.

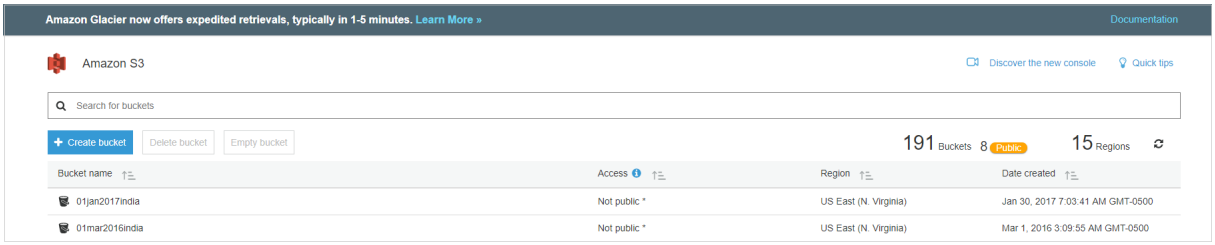
Creating Your S3 Bucket, IAM Policy, and IAM Role

Before you can purchase and configure your EC2 instances, you need to create an S3 bucket, a policy, and a role that gives access to the S3 bucket. The S3 bucket is where you will store your encryption keys and storage data.

1. Login to the AWS Management Console.
2. From the Storage section, select **S3**.



The Amazon S3 page opens.



3. Click **+ Create bucket**.

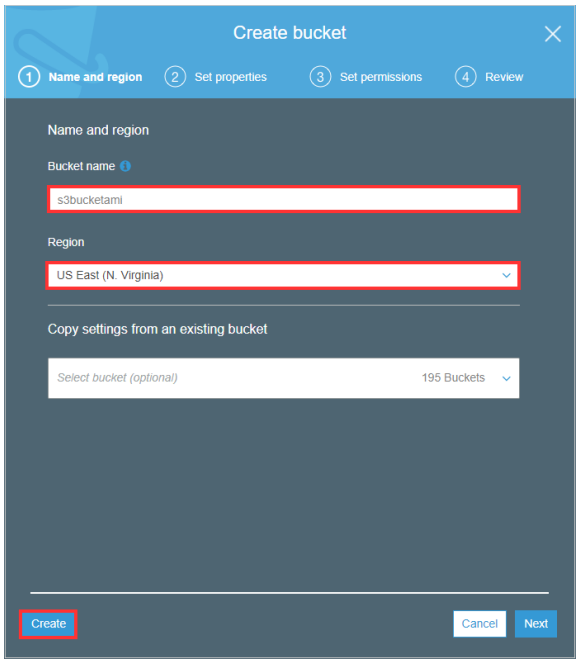
   The Create bucket configuration wizard opens.

4. Configure your S3 bucket:

   a. In the Bucket name text field, type a bucket name.

   b. From the Region drop-down menu, select a region.

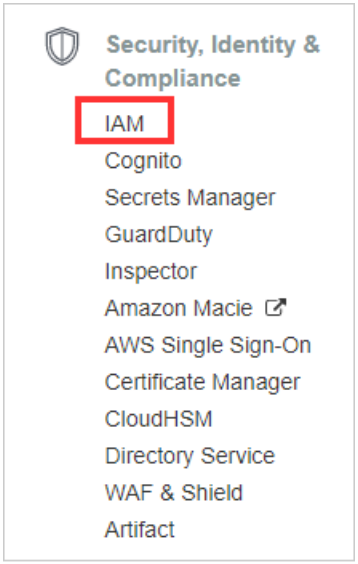
   c. Click **Create**.



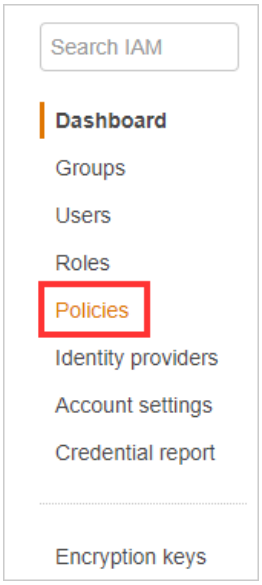
   The new S3 bucket is now displayed in the list.

5. Copy the S3 bucket name to the Required Information form.

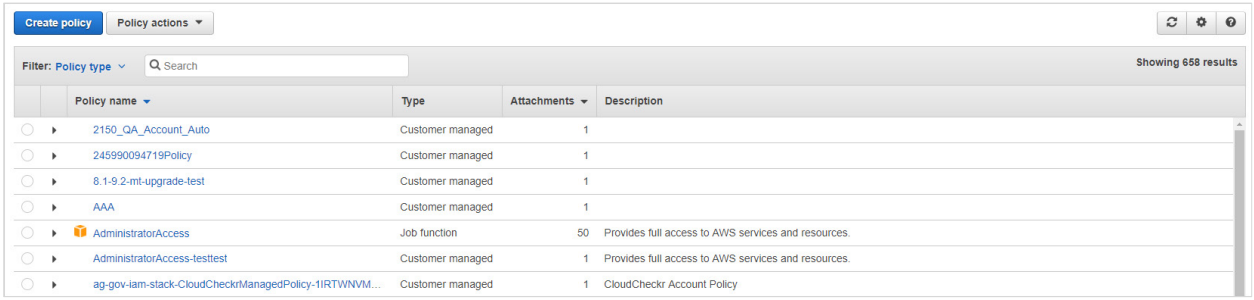
6. From the Security, Identity, & Compliance section, select **IAM**.



7. From the IAM dashboard, select **Policies**.

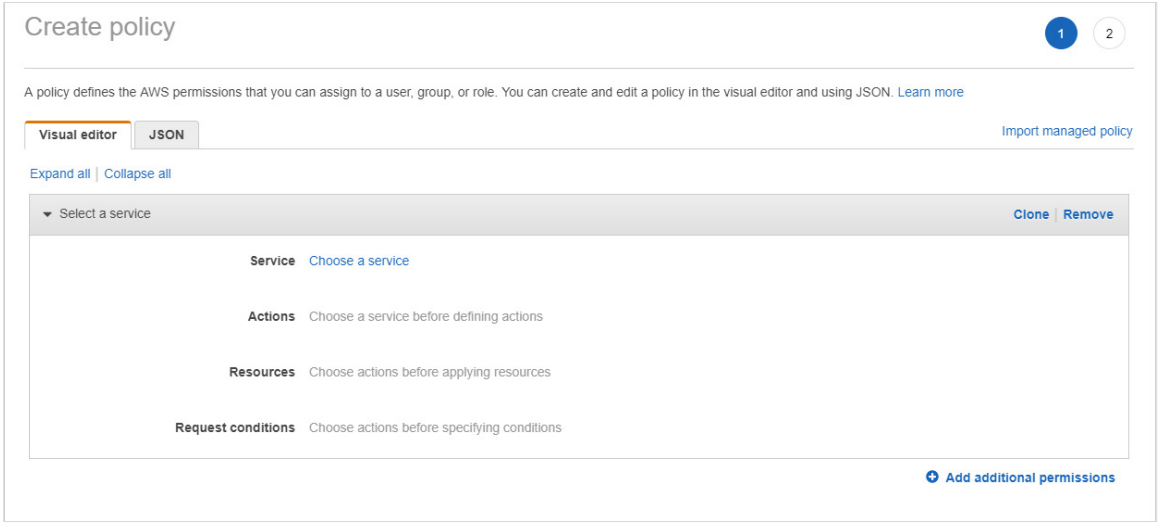


The policy page displays.



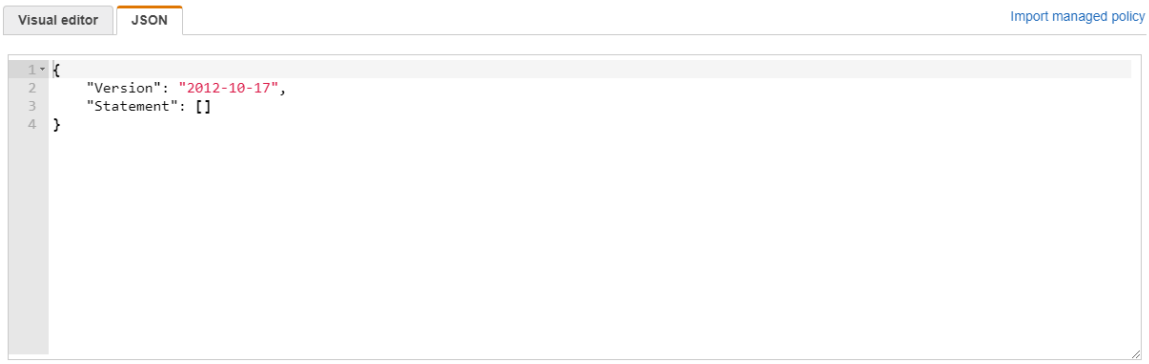
8. Click **Create policy**.

The Create policy page opens.



9. Click **JSON**.

   The JSON tab opens, allowing you to create the policy using JSON syntax.



10. Copy the full CloudCheckr IAM policy.

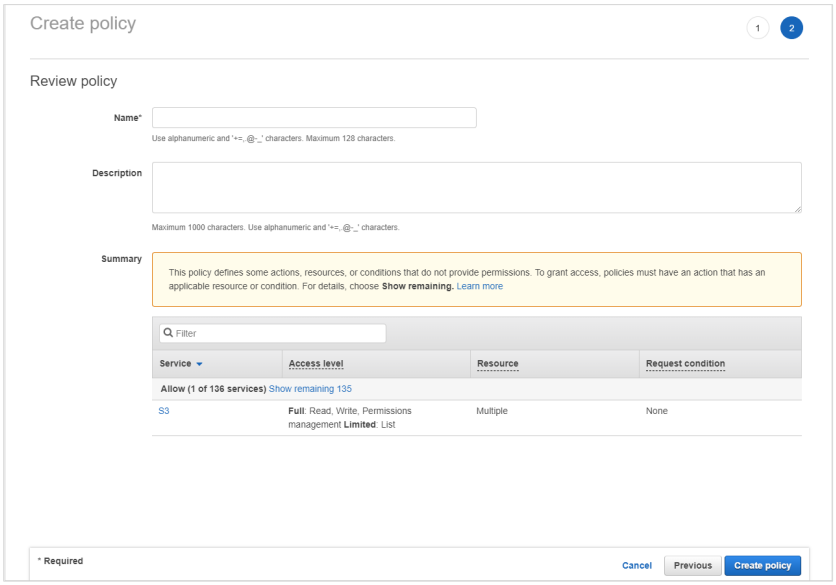
    Note: The full CloudCheckr IAM policy identified in the link is for MT – Commercial only. For Gov Cloud, use the following policy:

```
{
        "Version":"2012-10-17",
        "Statement":[
           {
              "Sid":"Stmt1489160892000",
              "Effect":"Allow",
              "Action":[
                 "s3:*"
              ],
              "Resource":[
                 "arn:aws-us-gov:s3:::bucket_name",
                 "arn:aws-us-gov:s3:::bucket_name/key_name"
              ]
           }
        ]
     }
```

    Note: The policies for the MT – Commercial only and MT – Commercial (GovCloud) use a general ARN format since ARNs may be formatted differently across regions.

11. Use the following guidelines to modify the ARNs:
    - You can use the wildcards, "*****" and "**?**" within any ARN segment.
    - An asterisk, "*****", represents a combination of zero or more characters.
    - A question mark, "**?**", represents a single character.
    - You can use multiple "*****" and "**?**" in each segment, but a wildcard cannot span segments.
12. Replace the text in the JSON tab with the policy you just copied and modified.
13. Click **Review policy**.

The Review policy page opens.



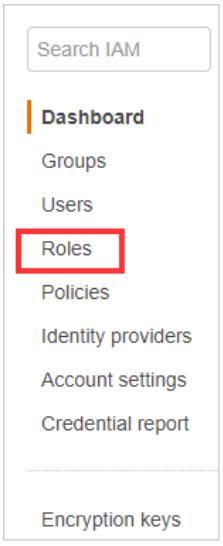
14. Type a name for the policy and click **Create policy**.

    Note: We recommend you name the policy **Full CloudCheckr IAM Policy**.

    A message at the top of the policy page indicates that your policy has been created.

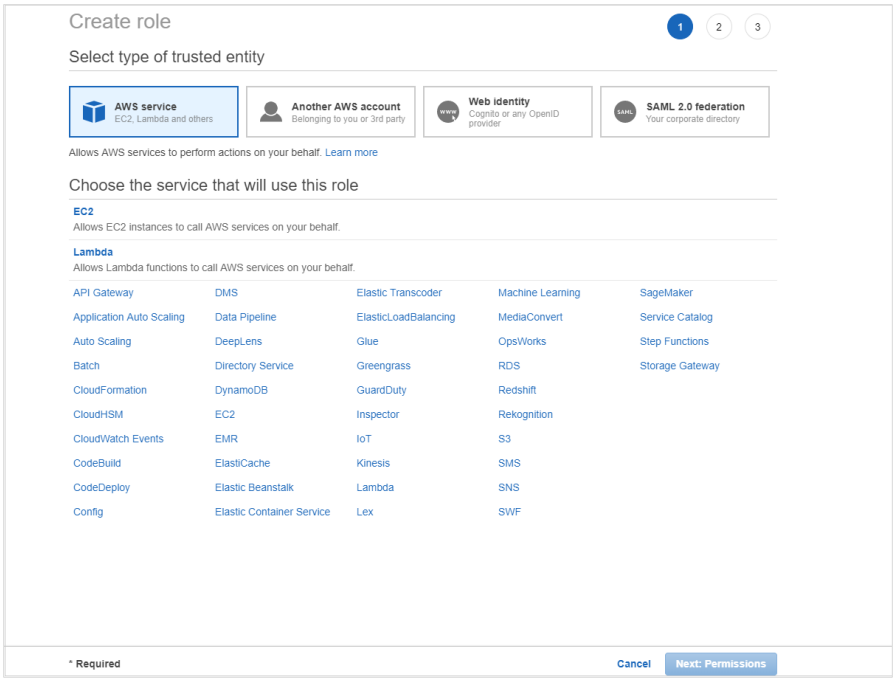
15. Copy the policy name to the Required Information form.

16. From the IAM dashboard, select **Roles**.



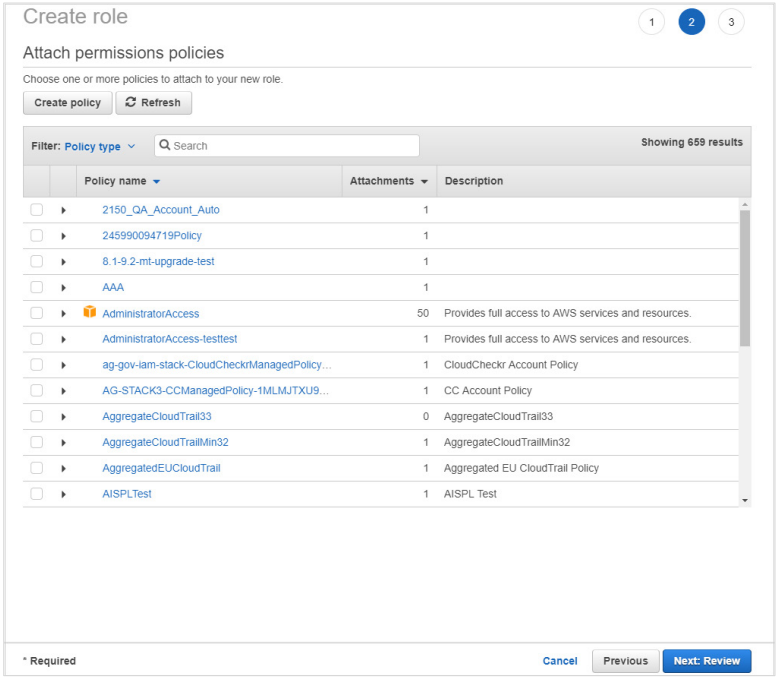
17. Click **Create role**.

The Create role page opens.



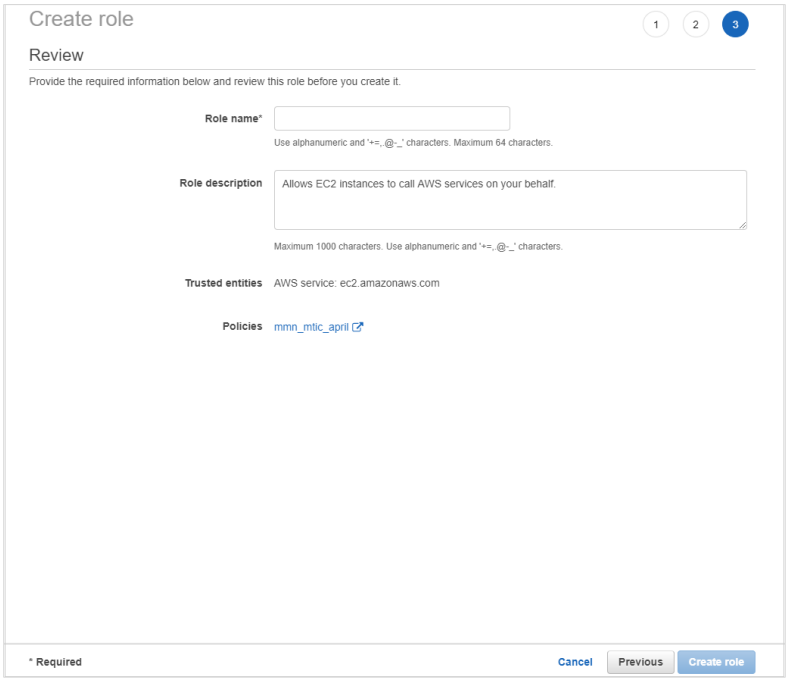
18. From the center of the page, click **EC2** and click **Next: Permissions**.

    The Attach permissions policies page opens.



19. Select the **Full CloudCheckr IAM Policy** you just created from the list.
20. Click **Next: Review**.

The Review page opens.



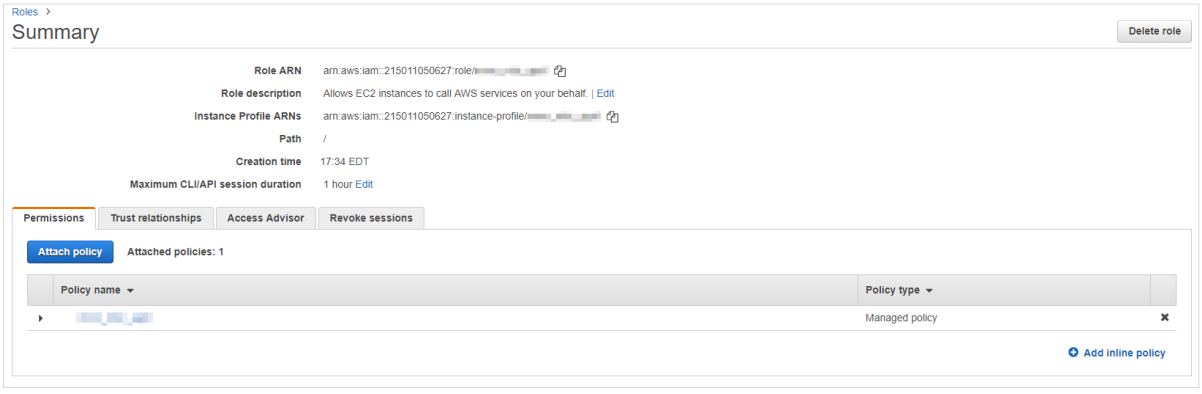
21. Type a name for the role and click **Create role**.

    The role is added to the list on the Roles page.

22. Copy the role name to the Required Information form.

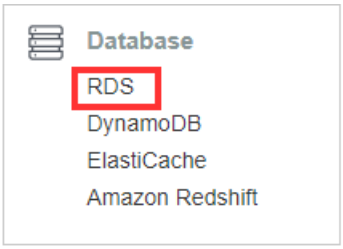
23. Locate the new role from the list and double-click the **name**.

    A summary page for the role displays and indicates that the policy is now attached.



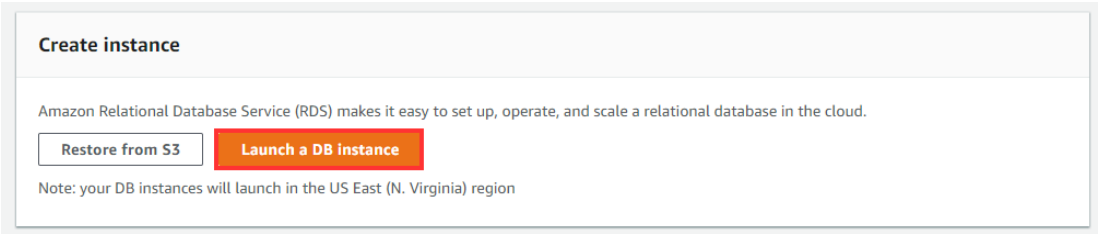
24. Return to the AWS Services page.

25. From the Database section, select **RDS**.

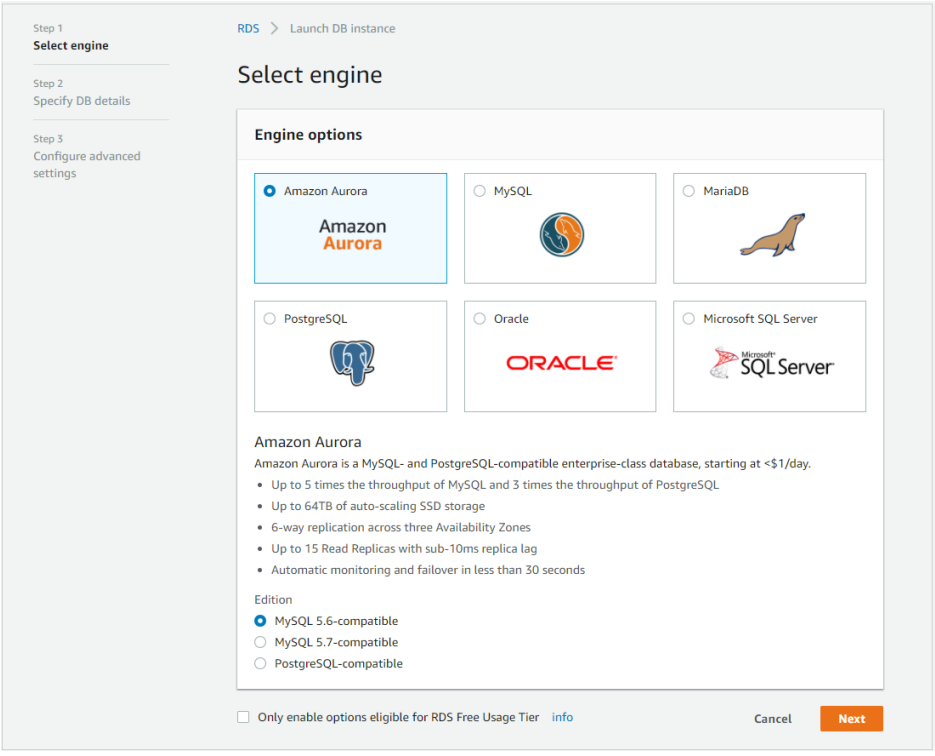


The Amazon RDS page opens.

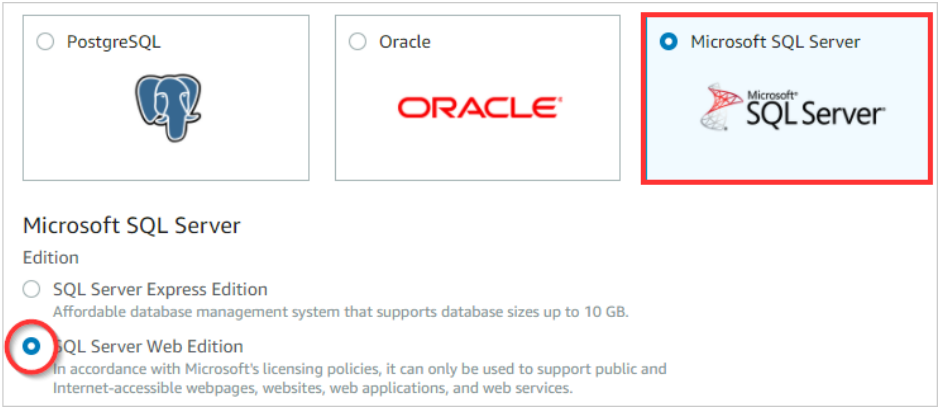
26. Navigate to the Create instance section and click **Launch a DB instance**.



27. The Select engine wizard opens.



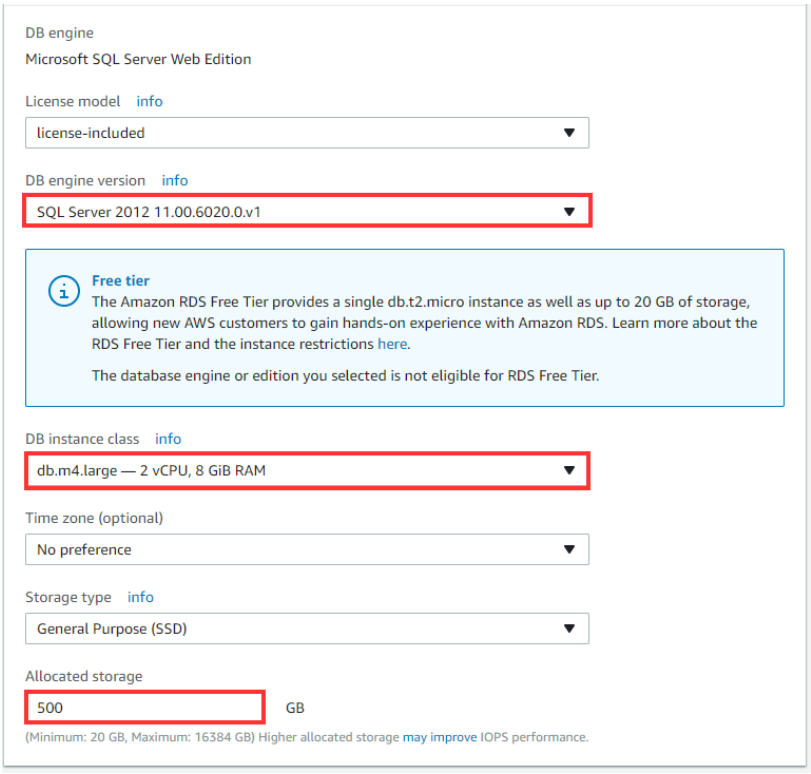
28. Select **Microsoft SQL Server and SQL Server Web Edition**.



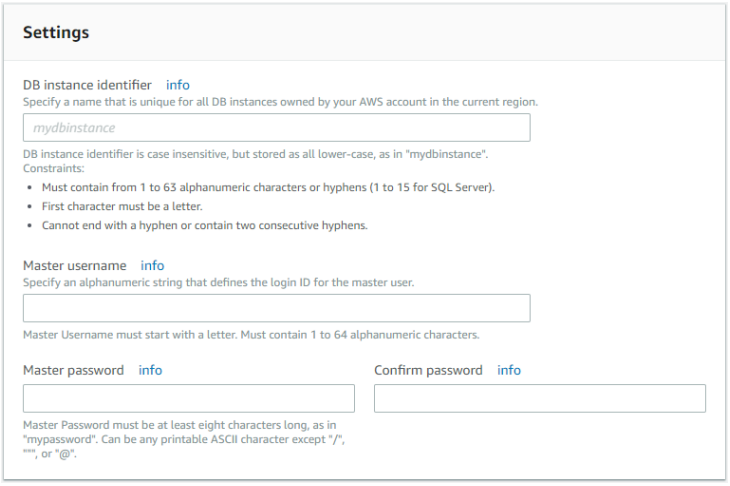
29. Click **Next**.

    The Specify DB details page opens.

30. From the DB engine version drop-down menu, select **SQL Server 11.00.6020.0.v1**.
31. From the DB instance class drop-down menu, select **db.m4.large**.
32. Type **500** for the allocated storage.

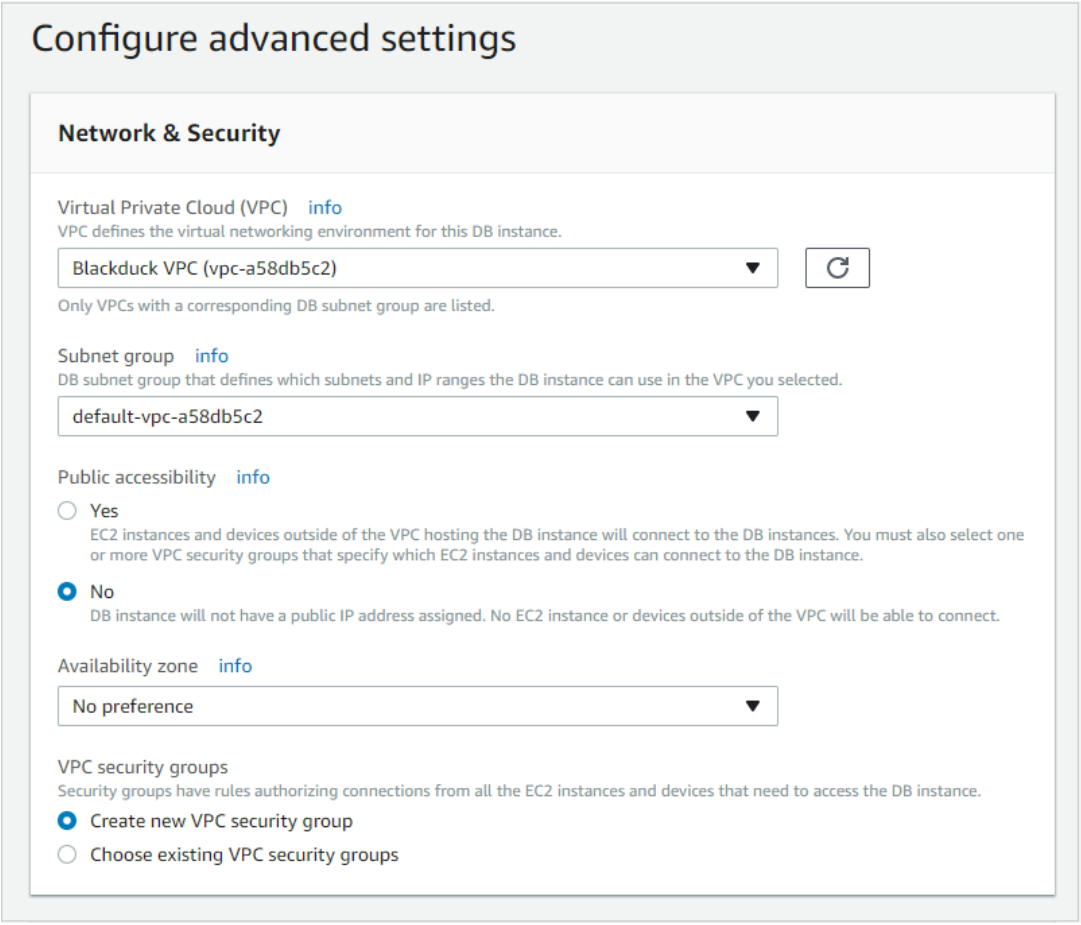


33. Scroll down to the Settings section.



34. In the DB instance identifier text field, type a name for your RDS server.
35. Create a master username and password that you will use to connect to your RDS server.
36. Copy the name, master username, and password of the RDS server to the Required Information form.
37. Click **Next**.

    The Configure advanced settings page opens.



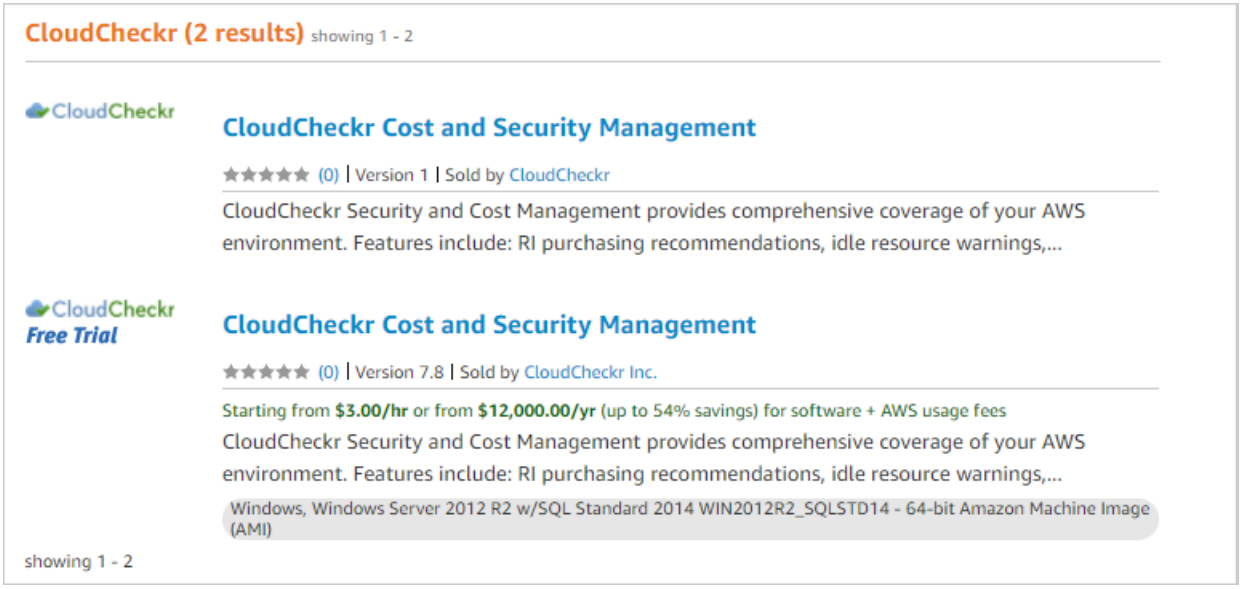
38. Configure your settings as follows:
    - VPC: appropriate VPC for your environment
    - Publicly Accessible: No
    - Availability Zone: No Preference
    - VPC Security Groups: Create a new security group. When you have your RDS and EC2 instance IP addresses, you will be able to configure rules for your security group.
    - Other settings on this screen: optional; get details from your IT department
39. Click **Launch DB instance**.

Purchasing the Multi-Tiered Commercial Version

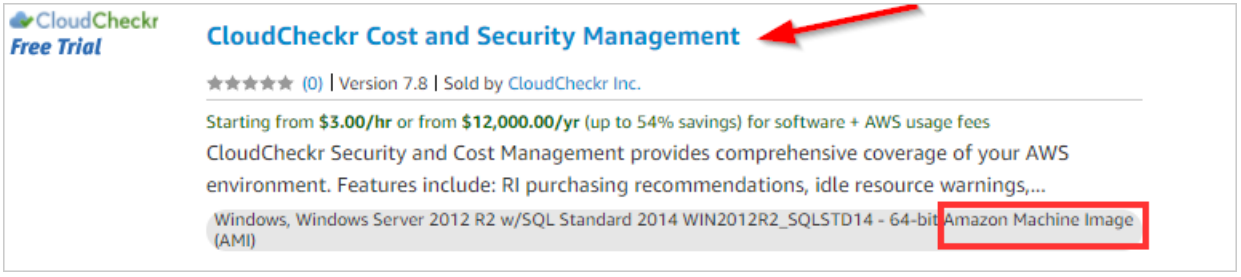
To purchase the Multi-Tiered – Commercial version of the AMI, contact a CloudCheckr account executive or purchase it from the AWS Marketplace. The preferred method of purchase is the AWS Marketplace.

1. Navigate to the AWS Marketplace.
2. In the AMI & SaaS text box, type **CloudCheckr** and press **Enter**.

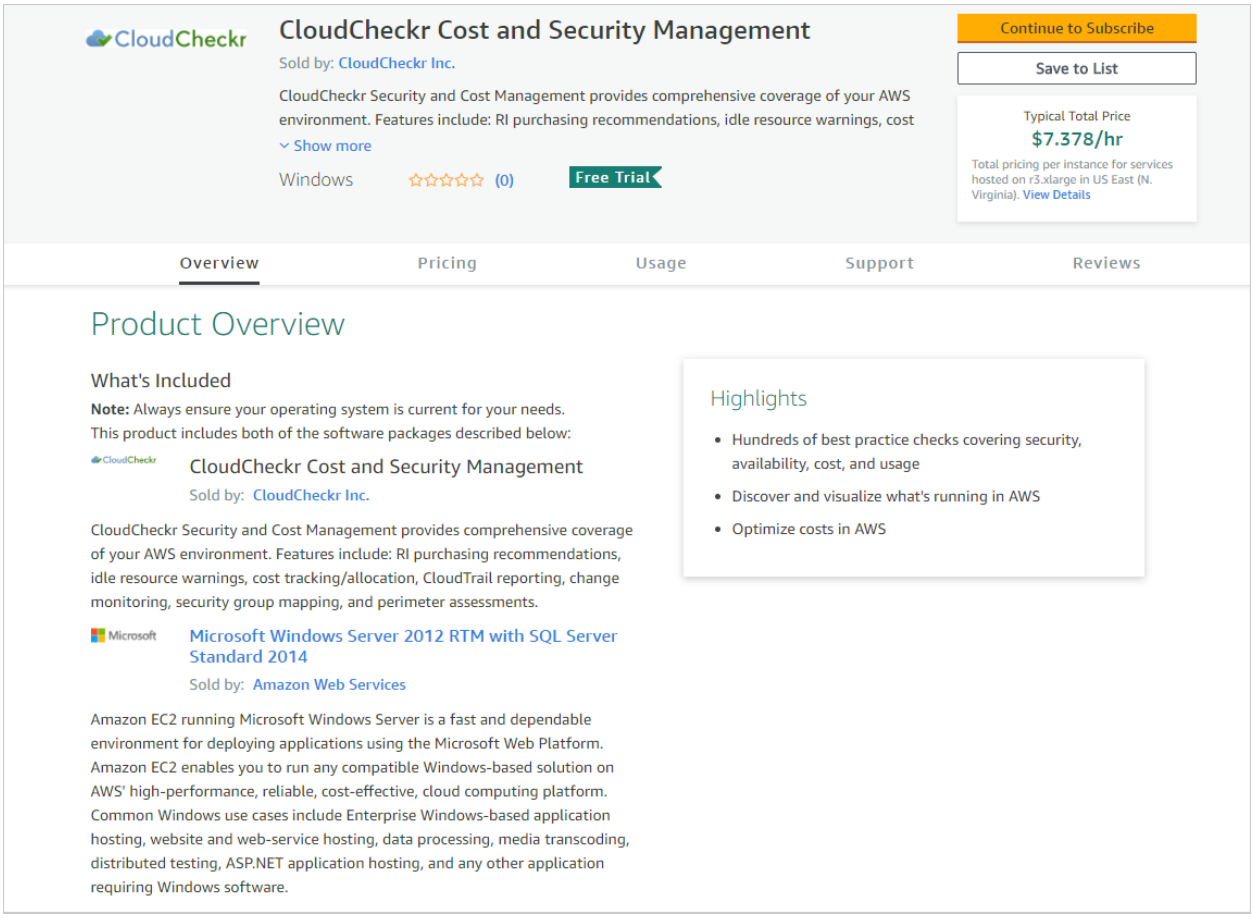
The search results display and include the SaaS and the AMI versions.



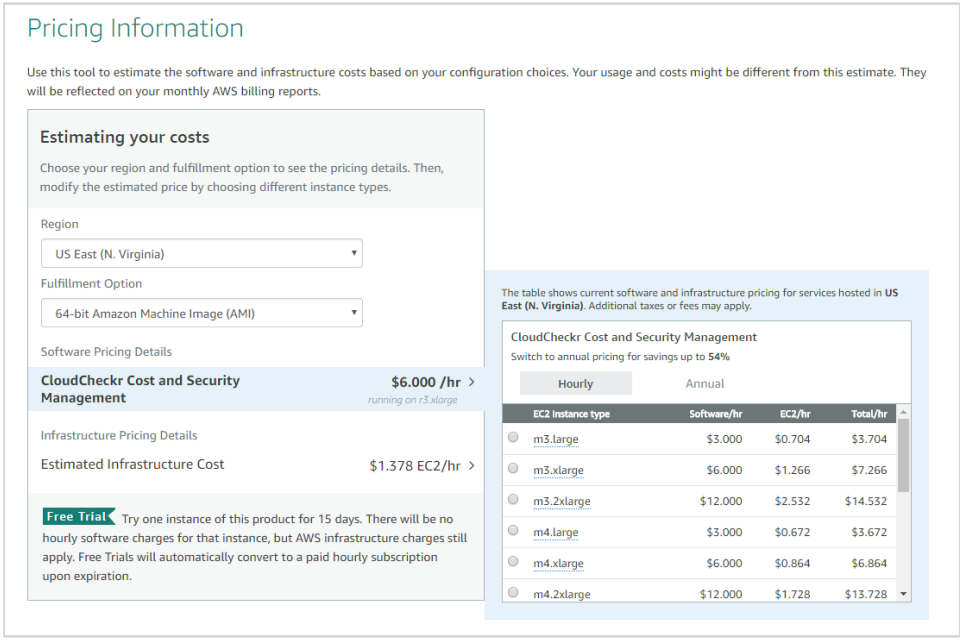
3. Click the **CloudCheckr Cost and Security Management** link for the AMI version.



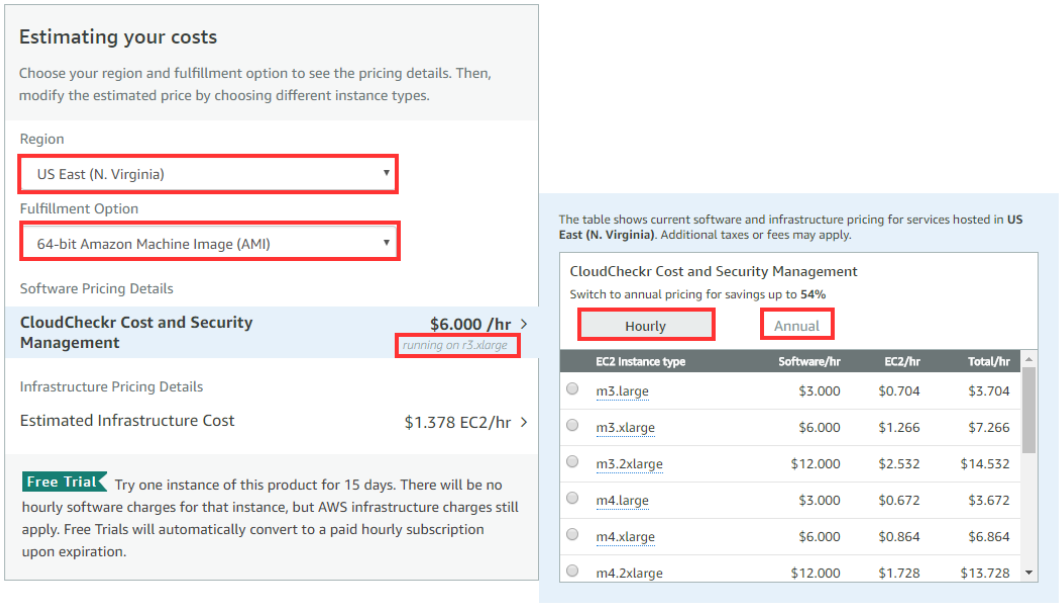
The CloudCheckr Cost and Security Management page opens.



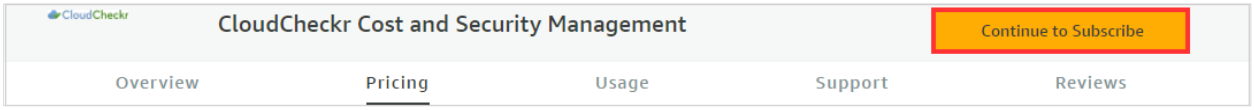
4. Scroll down to the Pricing Information section.



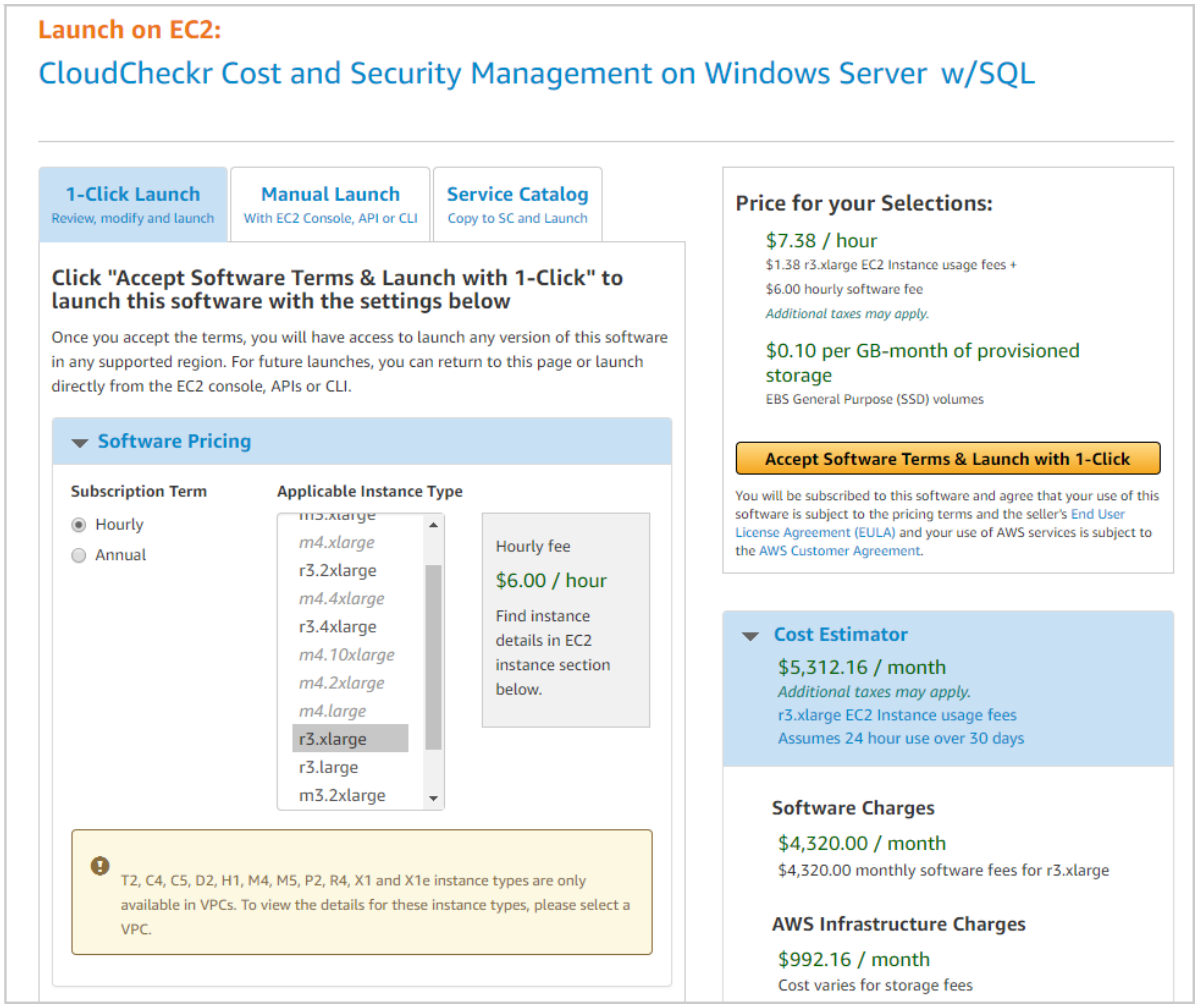
5. Configure your cost options.
   - From the Region drop-down menu, select the region where you want to deploy the AMI.
   - Leave the default fulfillment option, **64-bit Amazon Machine Image (AMI)**.
   - Click **Annual** if you wish to switch from the hourly pricing structure.
   - Leave the default EC2 instance type, **r3.xlarge**. You can choose a different type when you create the EC2 instance.



6. From the top right of the page, click **Continue to Subscribe**.

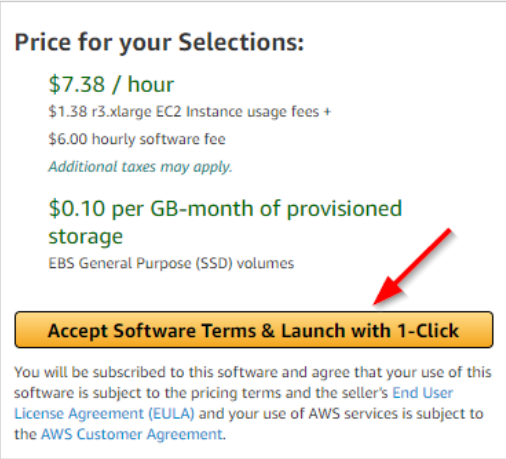


The final software terms and launch options display. 1-Click Launch is the default.

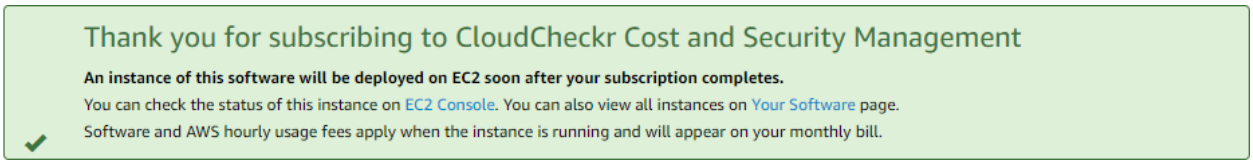


7. Select a launch option. The procedure uses 1-Click Launch.

8. Review and modify any cost settings and click **Accept Software Terms & Launch with 1-Click**.



A message indicates that the EC2 instance will launch automatically once AWS completes the subscription.



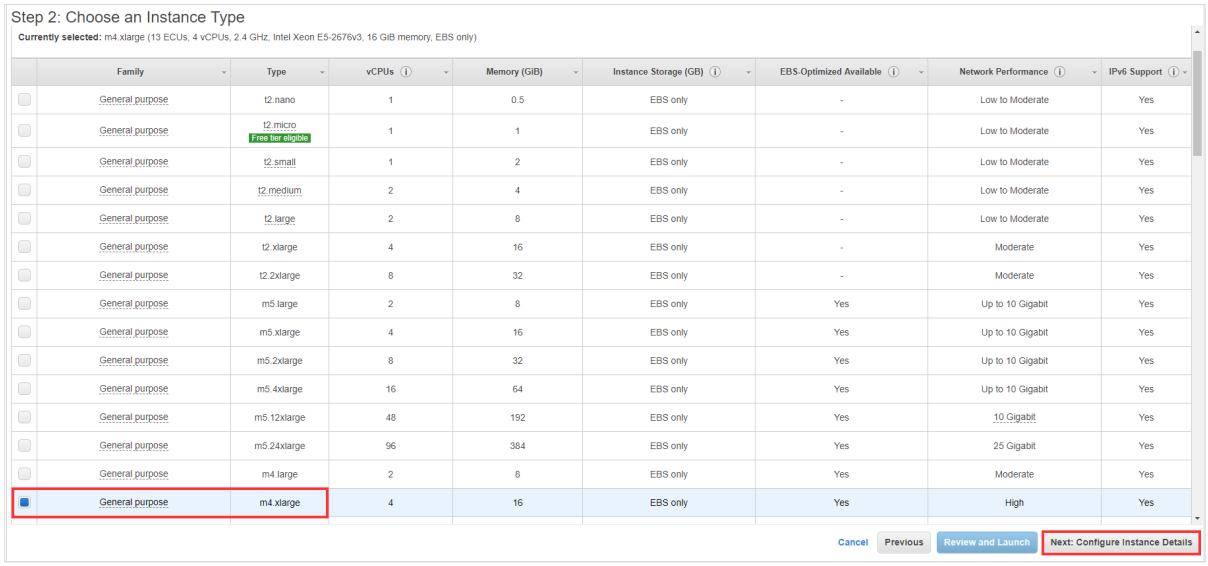
Configuring the EC2 Instance for the Web Console, Workers, and Schedulers

When your EC2 instance launches, a wizard opens automatically in the AWS Management Console.

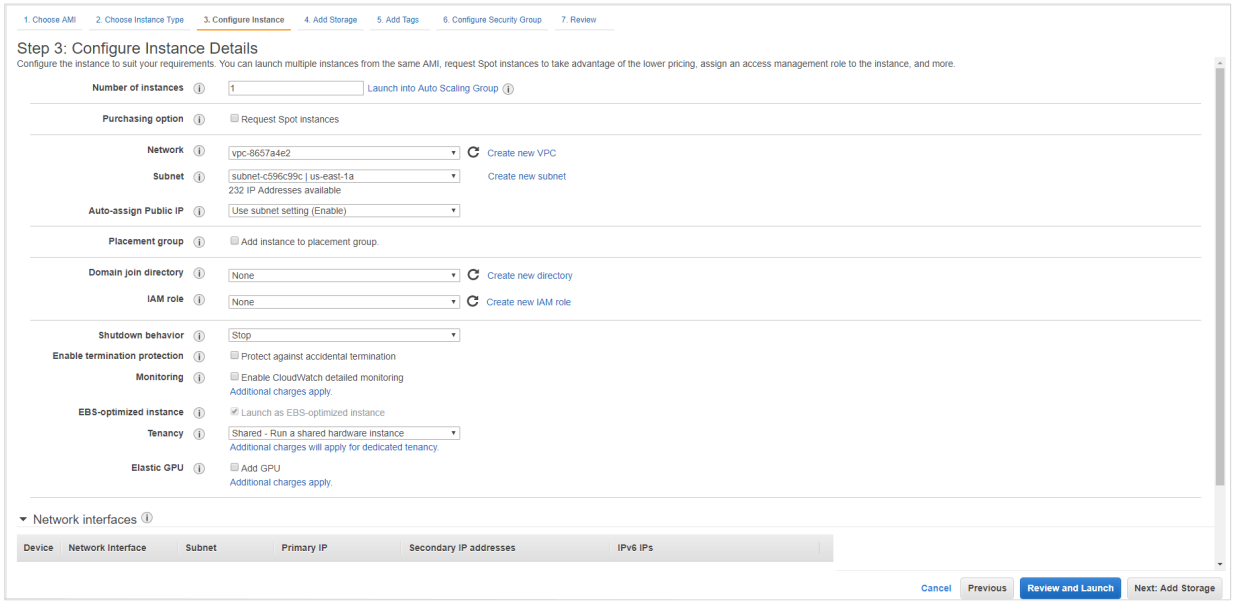
In this section, you will configure an EC2 instance for the Web Console, Workers, and Schedulers.

Since you selected the AMI from the AWS Marketplace, Step 1 is complete. The first step you will see is Step 2: Choose an Instance Type.

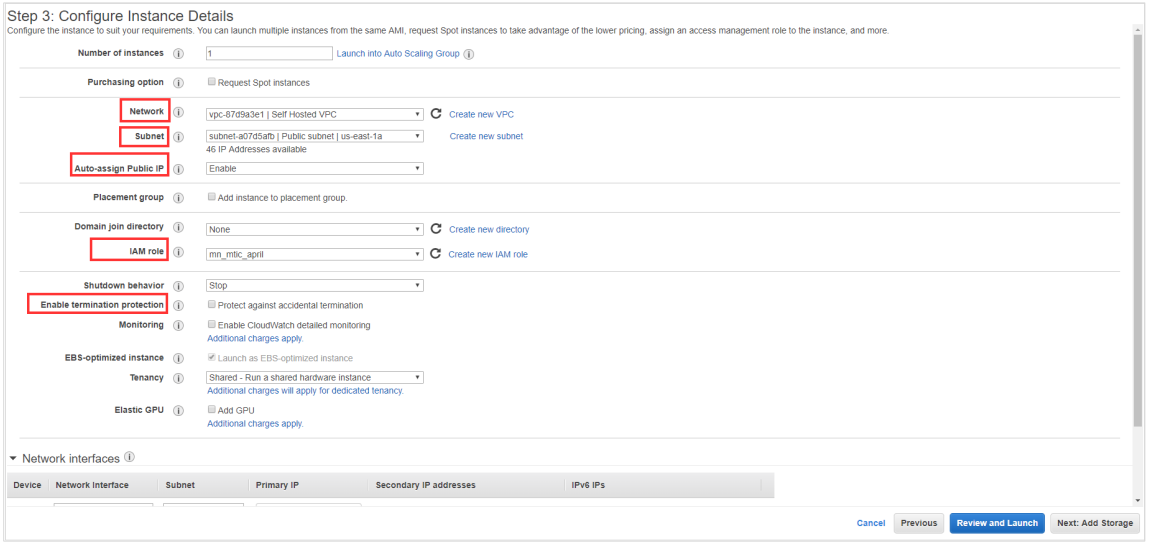
1. Select the box next to your preferred instant type. In this procedure, we chose **m4.xlarge**.
2. Click **Next: Configure Instance Details**.



Step 3: Configure Instance Details displays.



3. Configure the following details to ensure you have the correct access to the EC2 instance:
    - From the Network drop-down menu, select a **network** with a VPC.
    - In the Subnet drop-down menu, select a **public** or **private subnet**: Public subnet is recommended if you want to access your EC2 instance from the internet.
    - From the Auto-assign Public IP drop-down menu, select **Enable**.
    - From the IAM role drop-down menu, select the IAM role you just created.
    - From the Enable termination protection option, select the **Protect against accidental termination** check box.
    - Leave the remaining options in their default state.

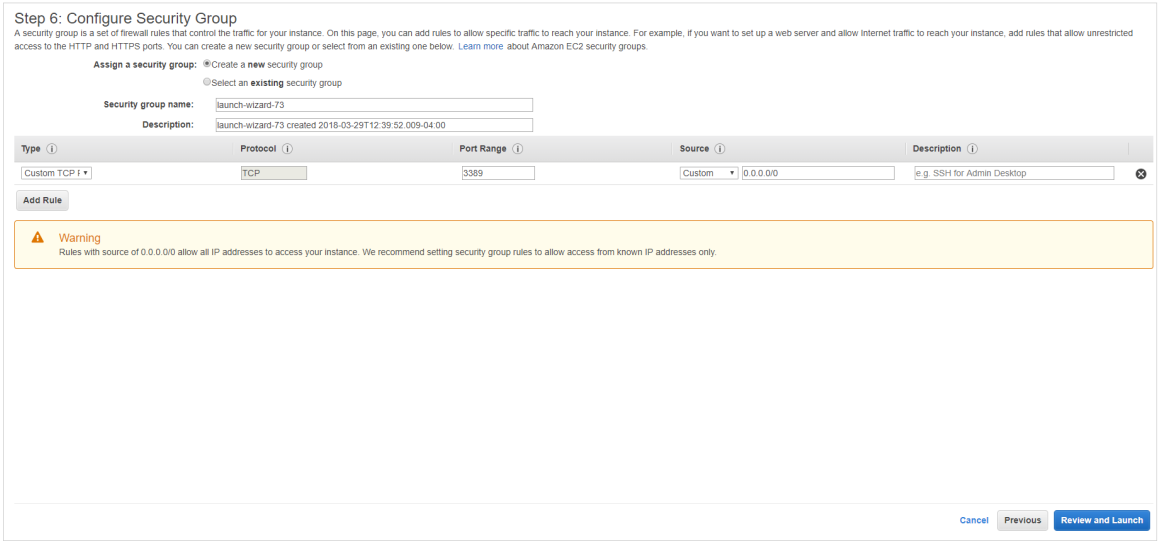


4. Click **Next: Add Storage**.

    Step 4: Add Storage screen displays.
5. Leave the default settings on this screen.
6. Click **Next: Add Tags**.

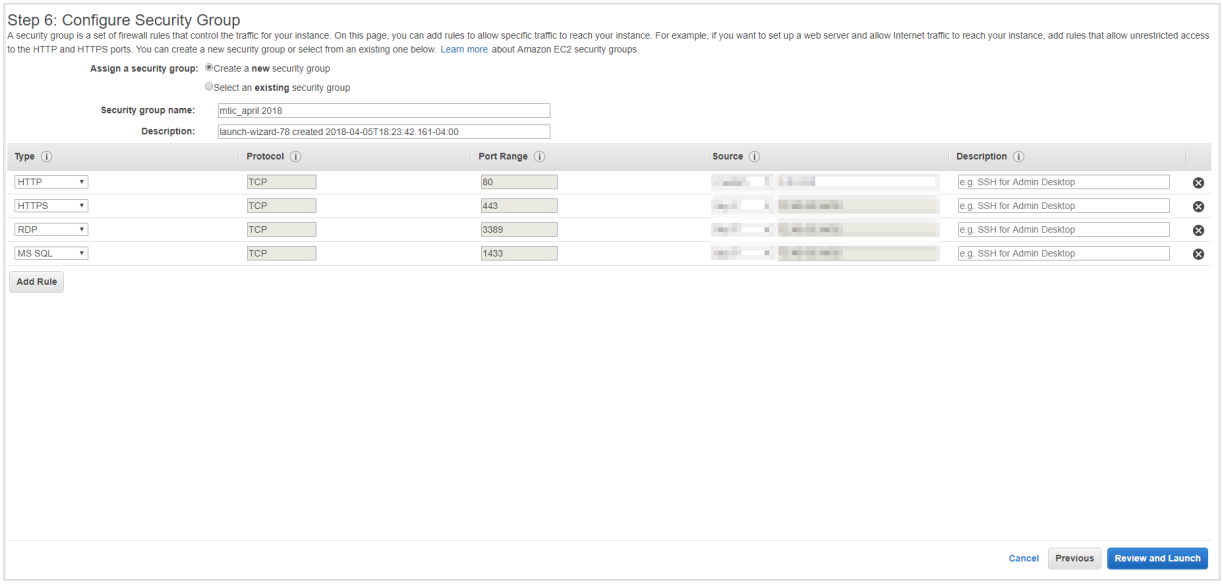
    Step 5: Add Tags displays.
7. Add tags if needed and click **Next: Configure Security Group**.

Step 6: Configure Security Group displays.



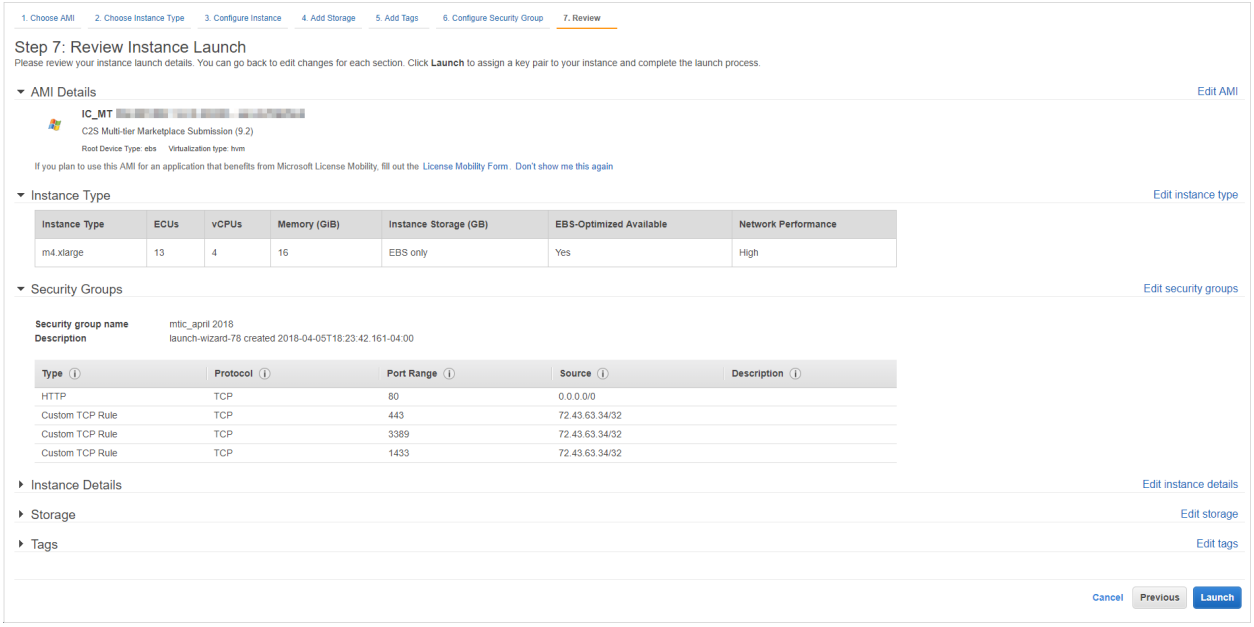
Since the EC2 instance is on the internet, you must designate a security group to manage access.

8. From the Assign a security group option, select **Create a new security group**.
9. In the Security group name, type a **name**
10. Add the following rules:
    - HTTP | TCP | Port 80 | 0.0.0.0/0 (provides access from a Web browser)
    - HTTPS | TCP | Port 443 | 0.0.0.0/0 (provides access from a Web browser)
    - RDP | TCP | Port 3389 | *Your IP address* (provides access from remote desktop)
    - MS SQL | TCP | Port 1433 | *Your Security Group* (provides access to Microsoft SQL server)



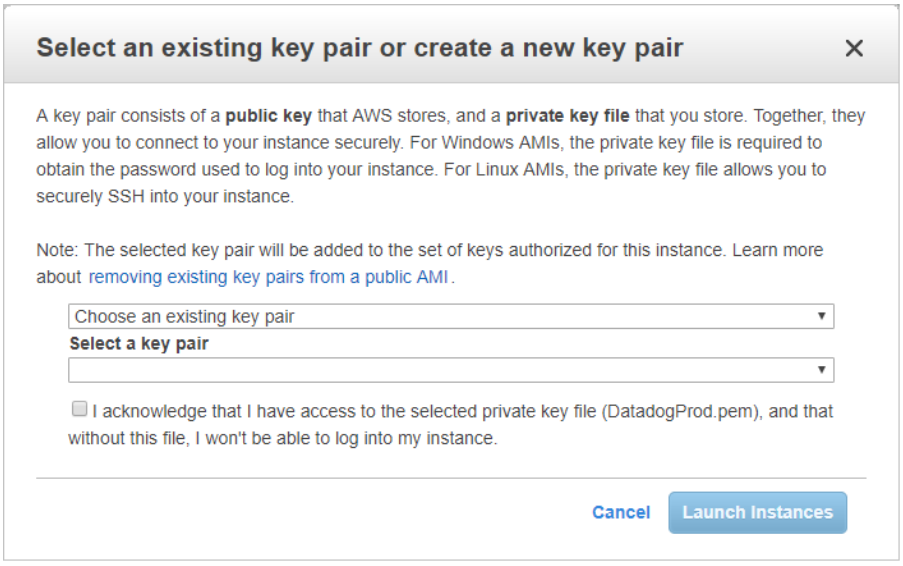
11. Click **Review and Launch**.

Step 7: Review Instance Launch displays.



12. Click **Launch**.

    The Select an existing key pair or create a new key pair dialog box opens.



13. From the first drop-down menu, select Choose an existing key pair or create a new key pair.

    To choose an existing key pair:

    a. Verify that **Choose an existing key pair** is selected in the top drop-down menu.

    b. In the Select a key pair drop-down menu, select an existing key pair.

    c. Select the **I acknowledge…** checkbox.

To create a new key pair:

a. In the top drop-down menu, select **Create a new key pair**. The Key pair name text box displays.

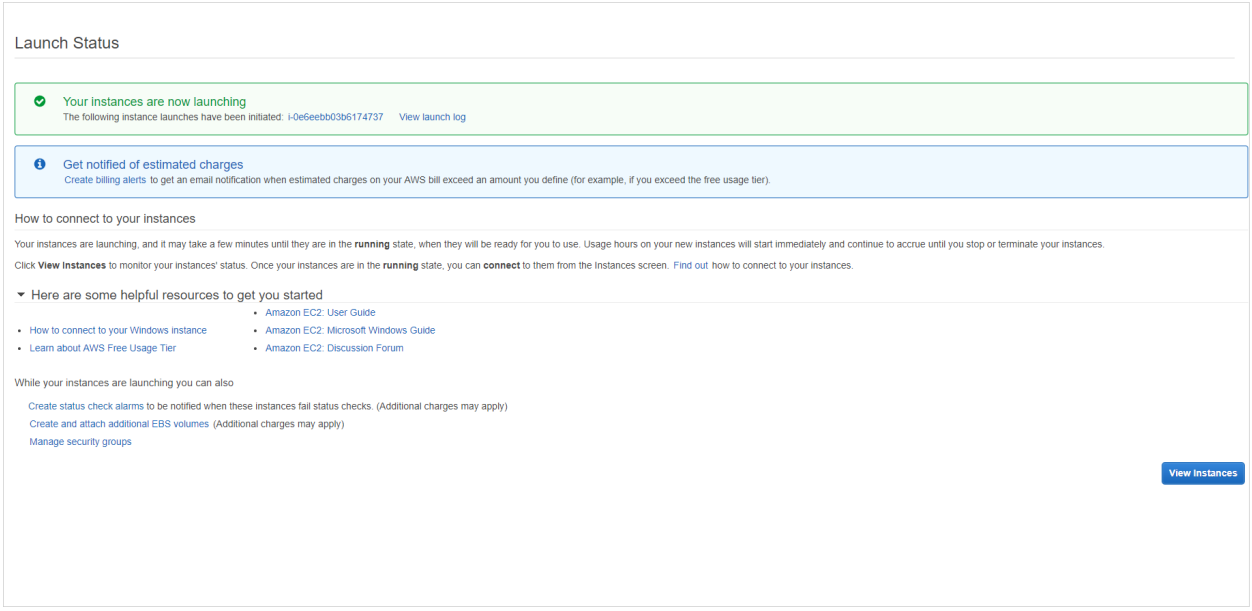
b. In the Key pair name text box, type the name of the key pair.

c. Click **Download Key Pair**. A .PEM file will download to your desktop.

d. Save the .PEM file because you will not be able to generate it again.

14. Click **Launch Instances**.

    The Launch Status screen displays.



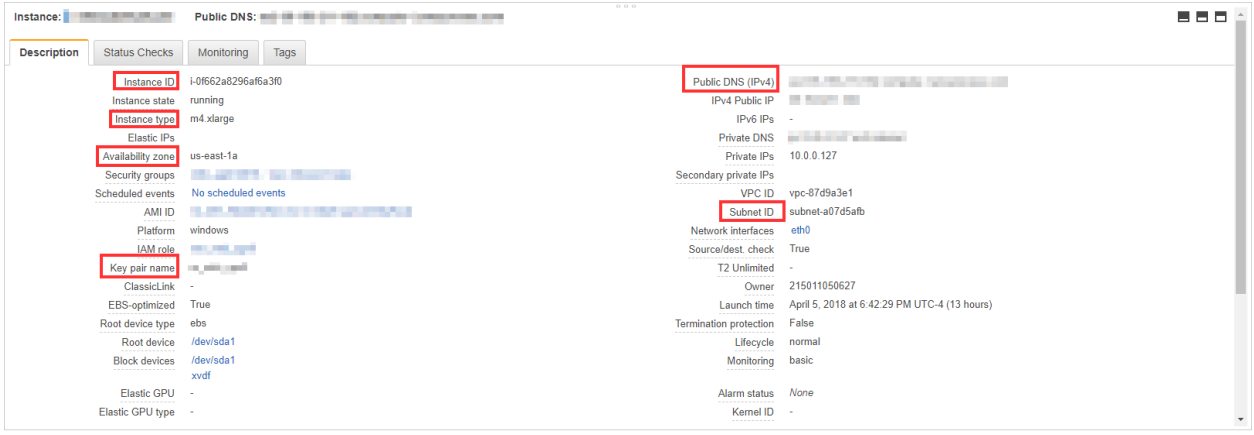
    Your EC2 instance will be available from the EC2 list in 5 to 10 minutes.

15. Once the new E2 instance is generated, go back to the EC2 dashboard.

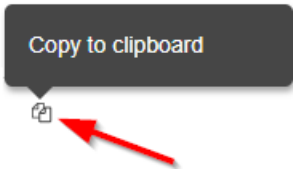
16. Select **Instances > Instances**.

17. Select the box next to your new EC2 instance.

18. From the Description tab, locate the following items:
    - Instance ID
    - Instance Type
    - Availability Zone (region code)
    - Key Pair Name
    - Public DNS (IPv4)
    - Private DNS
    - Subnet ID



19. Click the **Copy** icon next each of those items and paste the values into the Required Information form.

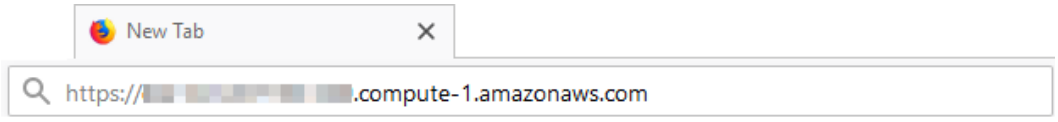


Installing the Application

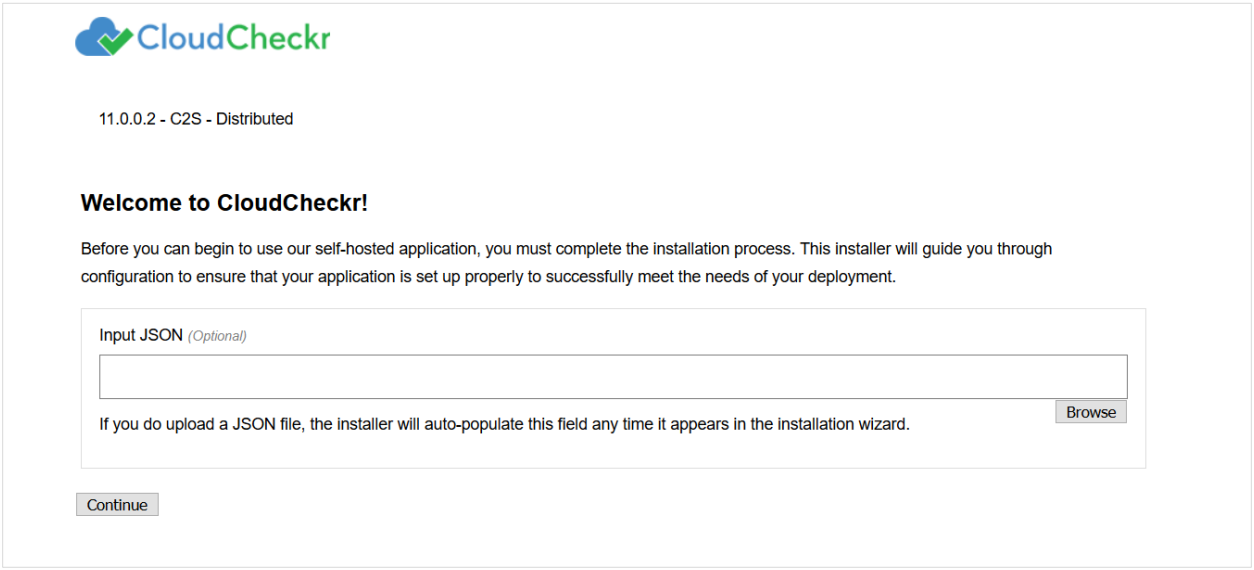
In this procedure, you will use the public IP address to connect to the EC2 instance and install the application.

Note: During the Web Console configuration, there is reference to the EC2 instance's Public DNS. This is **not** a publicly accessible resource, but the reference to it as **public** only correlates to the AWS configuration screen. Your EC2 instances are completely isolated from the internet.

1. Open your Web browser. This procedure shows Mozilla Firefox as an example.
2. Click + to open a new tab.
3. In the address bar, type **https://**
4. Paste the public DNS URL into the address bar.



The initial application screen, associated with the new EC2 instance, opens.

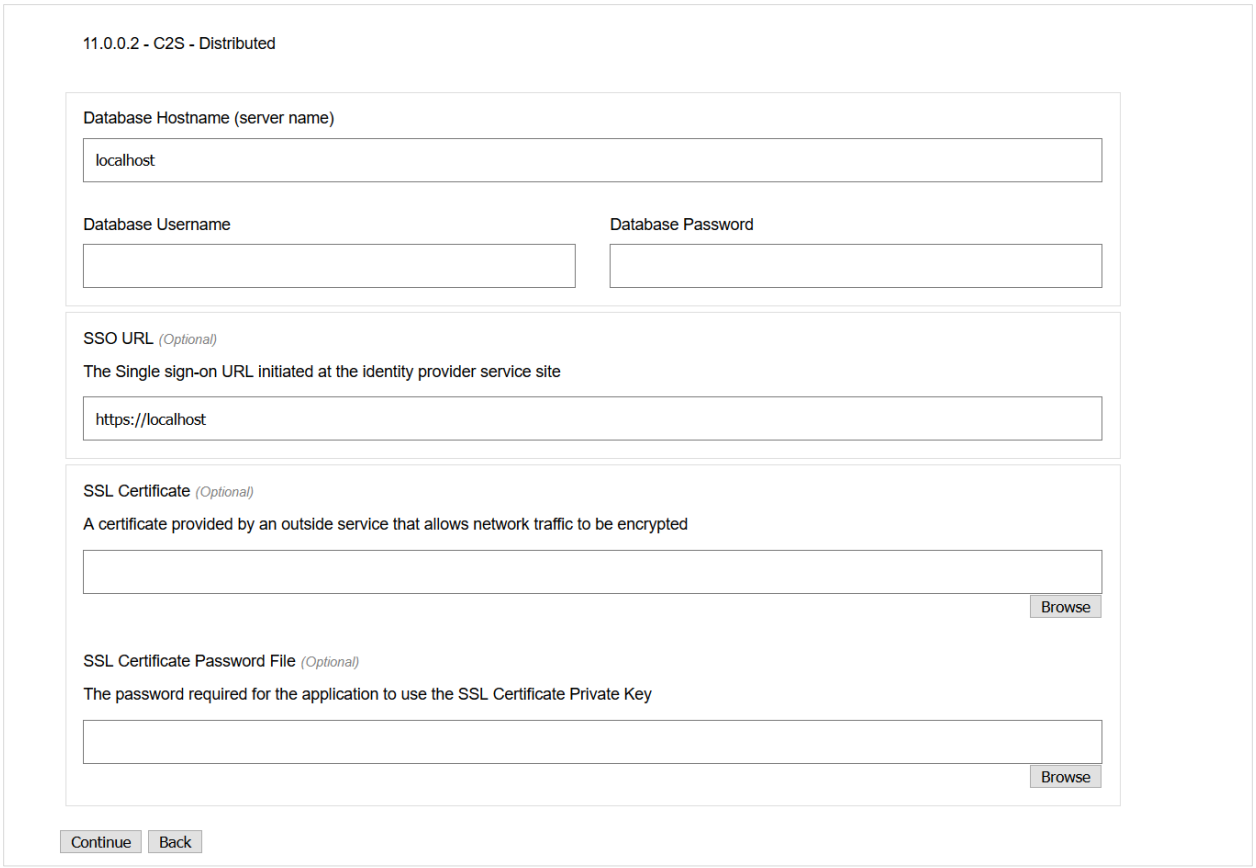


Note: The Input JSON text field is an optional feature that allows the installer to auto-populate your configuration information any time it is required in the installation wizard. If you do not want to use the website to configure CloudCheckr, you can load the file using the command line:

"C:\CloudCheckr\Package\Installer\CC.AmazonInstaller.exe -inputFile (path-to-input-file)"

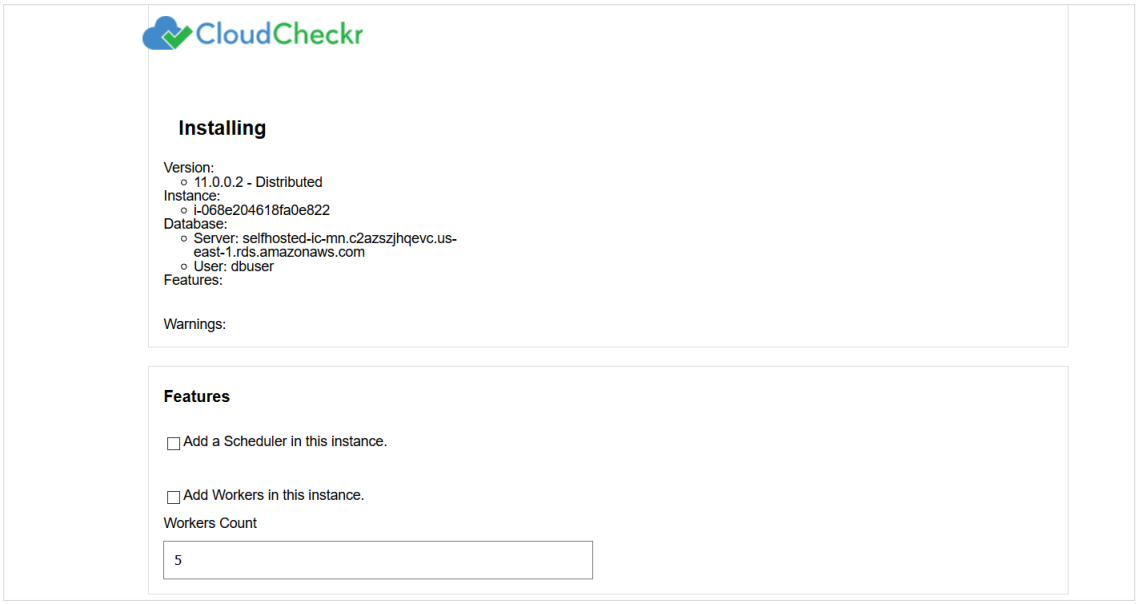
5. If applicable, upload a JSON file by clicking **Browse** to navigate to the file location.
   - See The input JSON file section for more details.
6. Click **Continue**.

The next screen in the wizard opens.



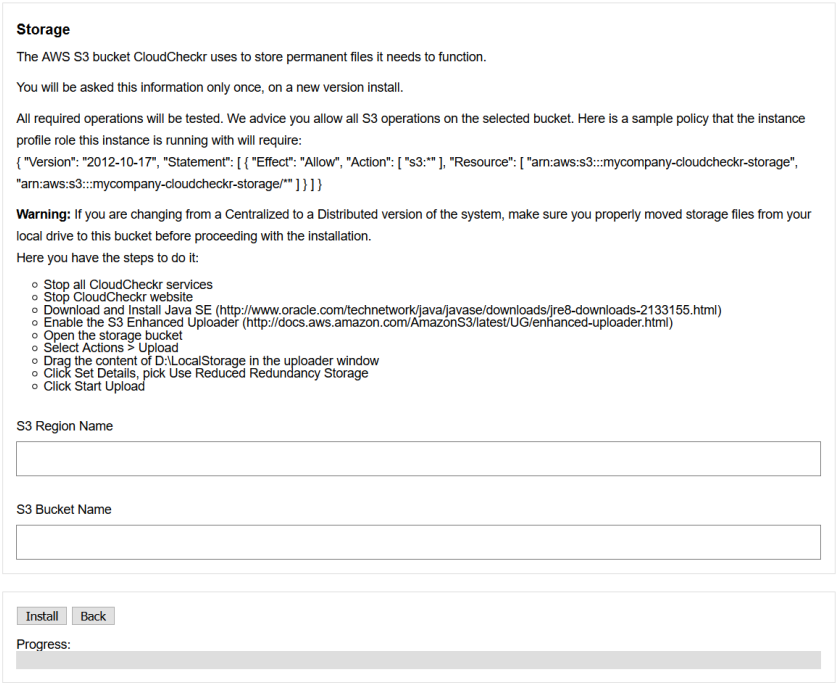
7. Provide the following information:
   - Database Hostname (server name): the private IP address the Microsoft SQL server
   - Database Username: user name of Microsoft SQL server
   - Database Password: password for the Microsoft SQL server
   - SSO URL: Single Sign-On URL
   - SSL Certificate: allows network traffic to be encrypted
   - SSL Certificate Password File: password required for the application to use the SSL certificate private key
8. Click **Continue**.

The next screen indicates that the application will install the latest version of the software on the EC2 instance.



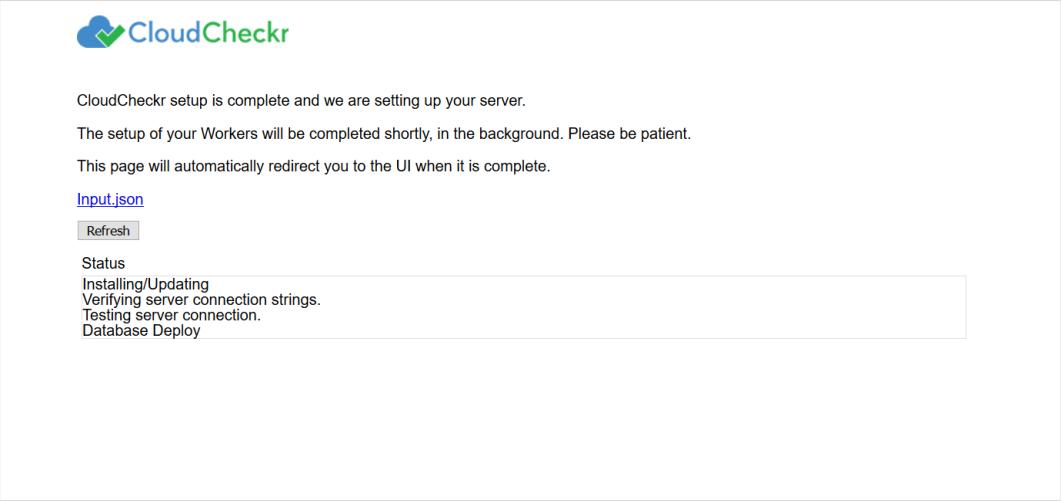
9. Select **Add a Scheduler in this instance** check box.
10. Select **Add Workers in this instance** check box.

    Note: The default number for the worker count is 5. If you plan on having more than 10 AWS accounts, increase the number to 25.
11. Scroll down to the Storage section.
12. Type the S3 region code and S3 bucket name.



13. Click **Install**.

When that page is done loading, another Status page displays.



While CloudCheckr installs, a status page updates automatically as the following tasks are completed:

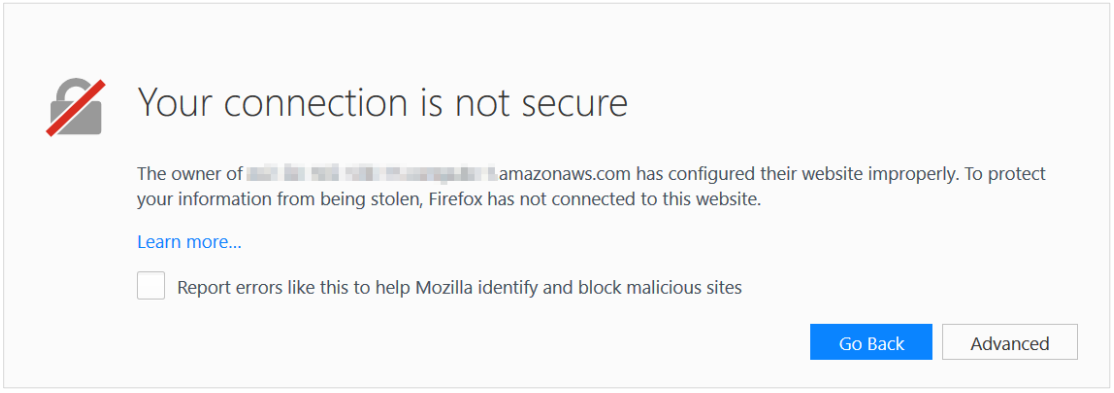
- Setup and testing of server settings
- Setup of database where user accounts and data get stored
- Installation of the console (Web and application UI)
- Configuration of the workers:
    - Workers are Microsoft Windows® services that pick up a job and go to Amazon to collect your data, via the AWS API, and store it in the database that will be exposed to the UI.

At this point, you can download the Input JSON file for later use. The file contains the exact configuration that you set up earlier in the installation process. Since the filename is not important as part of ingestion, feel free to rename the file. If you forget to click the **Input.json** link, and you want to use the file later, you can find it on the machine at: C:\CloudCheckr\Input.JSON

Note: The installation process may take a few minutes because the application must install the Microsoft Windows® services, deploy, and populate the correct databases.

Connecting the EC2 Instance to the Application UI

When the configuration is complete, a warning message indicates that your connection is not secure.

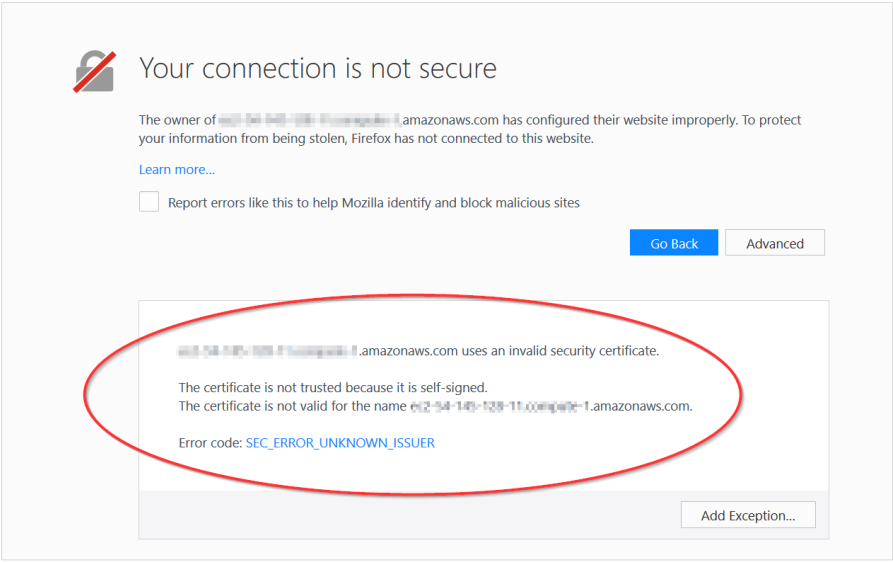


Note: The content and look-and-feel of the warning message depends on the browser in use.

The application requires a secure connection with a certificate owned by the domain. Since you are launching the application in a self-hosted environment, it cannot automatically create a certificate.

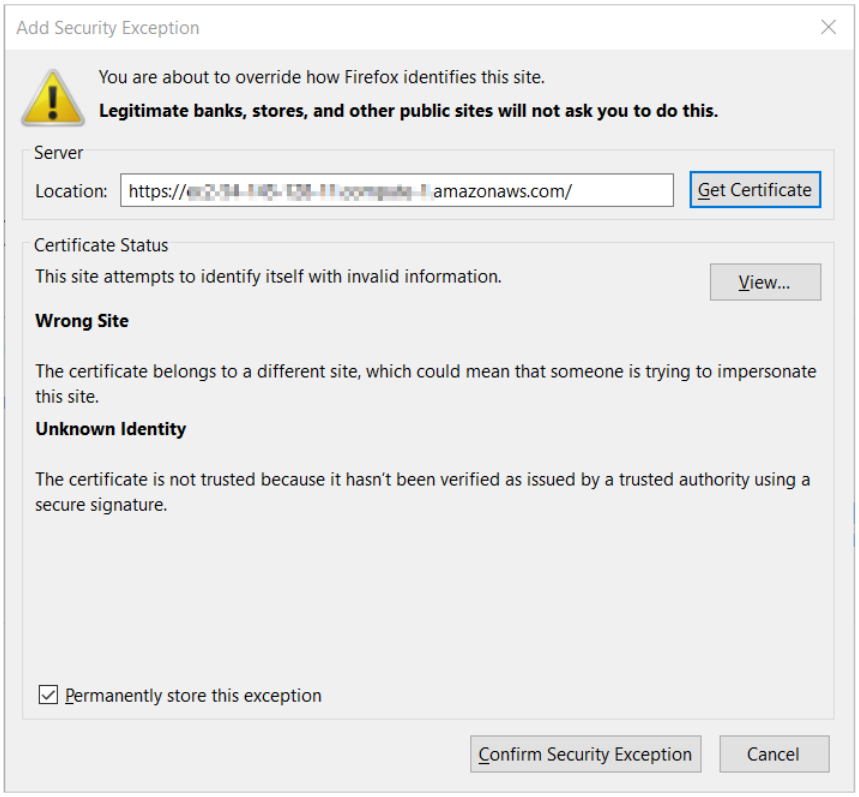
1. Click **Advanced** to get more information about the warning.

   A message indicates that the certificate is not trusted or valid.



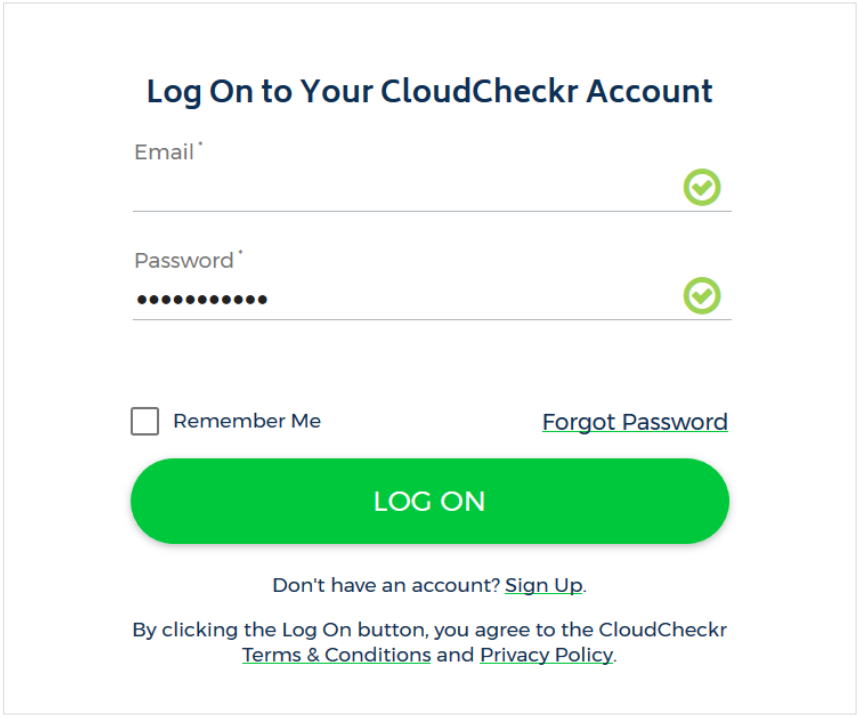
2. Click **Add Exception...** to add the EC2 instance as a security exception.

The Add Security Exception dialog box opens.



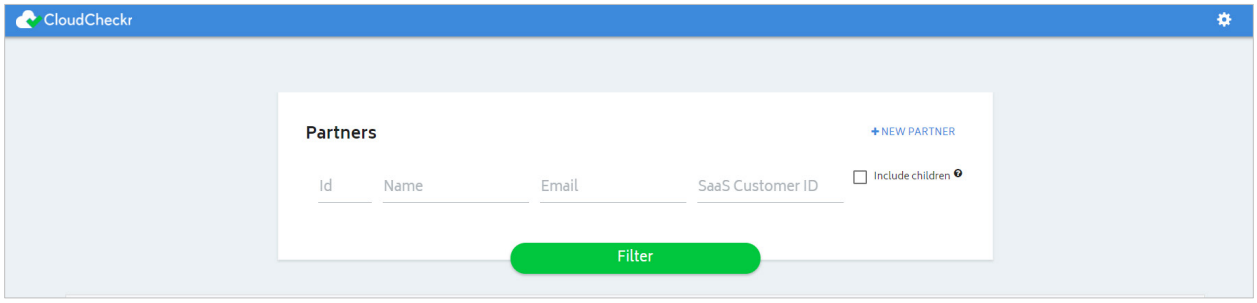
3. Verify that **Permanently store this exception** is selected and click **Confirm Security Exception**.

   The log in screen of the application opens.



4. In the Email text field, type **sysuser**
5. In the Password text field, paste the **EC2 instance ID**.
6. Click **LOG ON**.

   The Partners landing page opens.

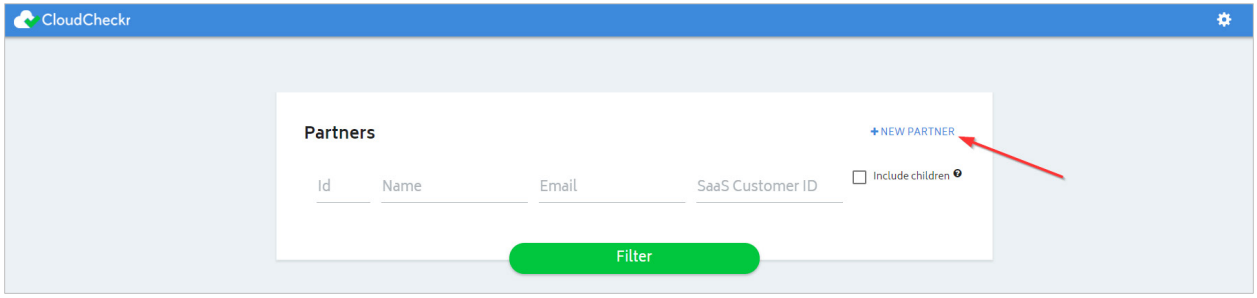


Partners are the top-level container within the application where you can generate and store multiple AWS accounts.

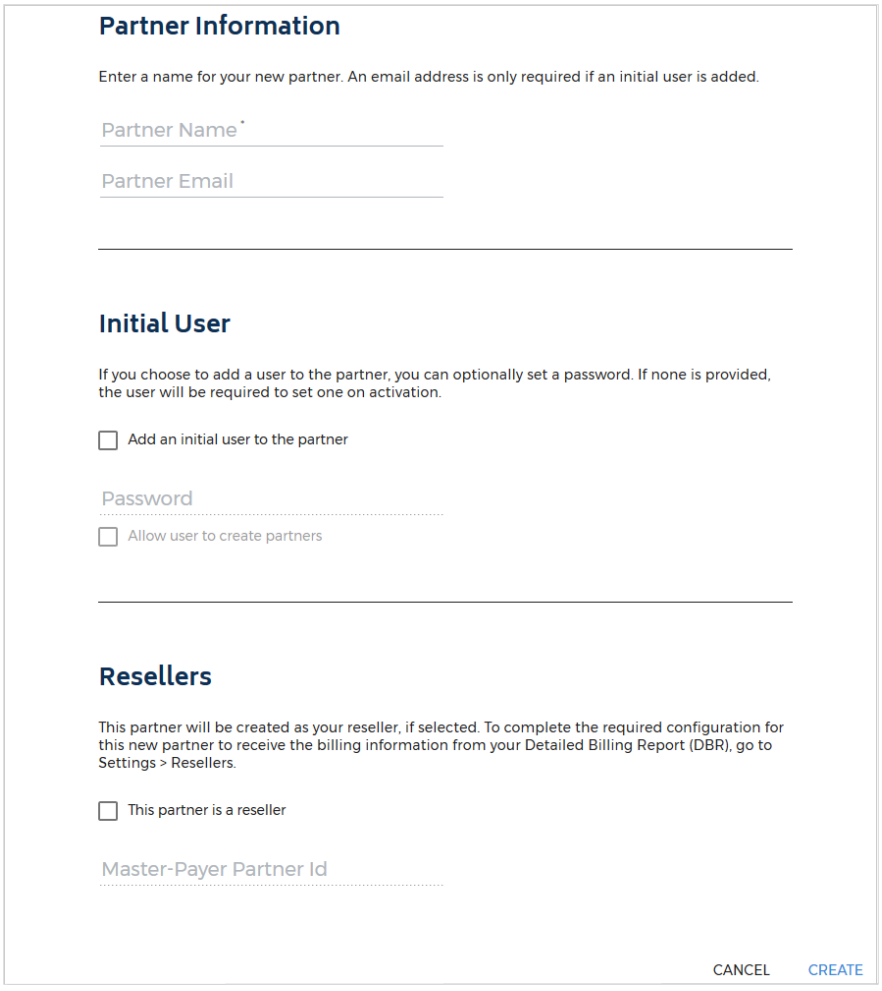
In most cases, you only need to create one partner.

Note: Once you have logged in, change the password immediately.

7. Click **+ NEW PARTNER**.

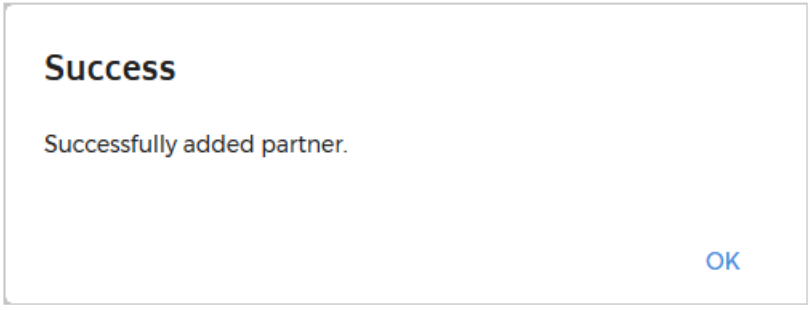


A dialog box opens.



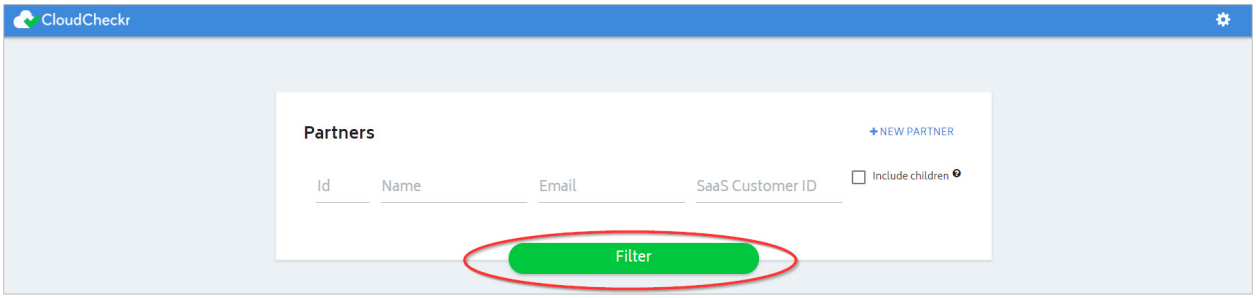
8. In the Partner Name text field, type a **partner name**.
9. In the Partner Email text field, type an **email address**.
10. Click **CREATE**.

    A message indicates that the partner was successfully added.



11. Click **OK**.

12. Click **Filter**.



The new partner is now displayed in the partners list.

Configuring Application Settings

Before you can use the self-hosted version, you must configure the application settings to ensure it has the same functionality as the SaaS version.

You will complete these actions on the Configuration page in the MT version.

1. From the menu bar, select **Settings > System > Configuration**.

   The Application-wide Configuration page opens.
2. Configure the SMTP settings to enable the application to send emails to users. Emails may include activation emails for new users, alerts, and report data.
3. In the URL for CloudCheckr section:
   a. Type the URL that will be shown on any application-generated emails.

      Note: The default **localhost** designation displays the DNS for the EC2 instance that is hosting your version of the application. This URL is external-facing.
   b. In the Workers Count text field, type the number of workers.
4. In the Proxy section, type the proxy details.

Creating AWS Credentials

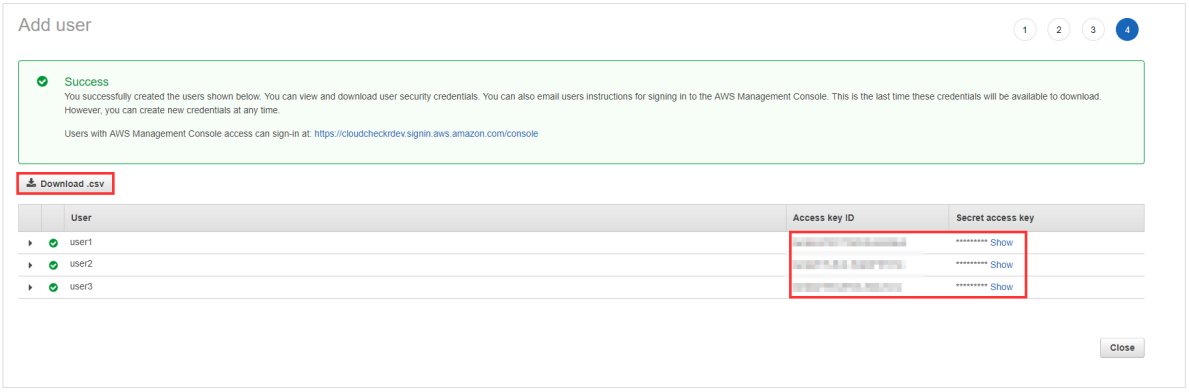
To allow the application to analyze data from AWS, you need to create AWS credentials, so the application can access your AWS account(s).

Although the preferred method for creating credentials is to create a cross-account access role, our application currently requires an access key and secret key for each account.

We recommend that you create three IAM users with access keys and secret keys.

1. Return to the AWS Management Console.
2. Review the topic in the Support Knowledgebase, Creating AWS Credentials Using IAM Access Keys and perform the steps in the prescribed order:
   a. Create an IAM user group.
   b. Attach the AWS Read-Only Access policy to the IAM user group.
   c. Create three IAM users and add them to the IAM user group.

      Note: After you create the users, download the .CSV file or copy the access and secret access keys to your PC.



   d. Add a secondary policy.

      Note: Make sure it contains the following permissions:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1470231538000",
         "Effect":"Allow",
         "Action":[
            "ec2:DescribeReservedInstancesOfferings",
            "ec2:DescribeSpotPriceHistory",
            "ec2:DescribeAvailabilityZones"
         ],
         "Resource":[
            " arn:aws:ec2:*:AWS-ACCOUNT-ID:instance/*"
         ]
      }
   ]
}
```

e. Attach the secondary policy to the IAM user group.

3. Return to the application.
4. Copy the access and secret access keys for the three IAM users into the appropriate credential sections.

   The Pricing Job collects on-demand pricing in AWS, saves it to a database, and ensures the data is updated regularly. The access and secret access keys for each IAM user allows the application to access the AWS API to retrieve data regularly.

Creating a Trusted User

You must create a trusted user in AWS if you want to use cross-account roles to control access to your AWS accounts. Name the user appropriately for easy identification (EX: **CloudCheckrTrustedUser**).

1. Return to the AWS Management Console.
2. Follow the steps in Creating AWS Credentials Using IAM Access Keys.
   a. When creating the new secondary policy for the trusted user, ensure it allows `sts:AssumeRole` to all resources as indicated in this example:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"Stmt1474398174000",
         "Effect":"Allow",
         "Action":[
            "sts:AssumeRole"
         ],
         "Resource":[
            "arn:aws:iam::AWS-ACCOUNT-ID"
         ]
      }
   ]
}
```

3. Return to the self-hosted application.
4. Copy the access key and secret access key of the trusted user to support cross-account roles.
5. At the bottom of the page, click **Save Settings**.

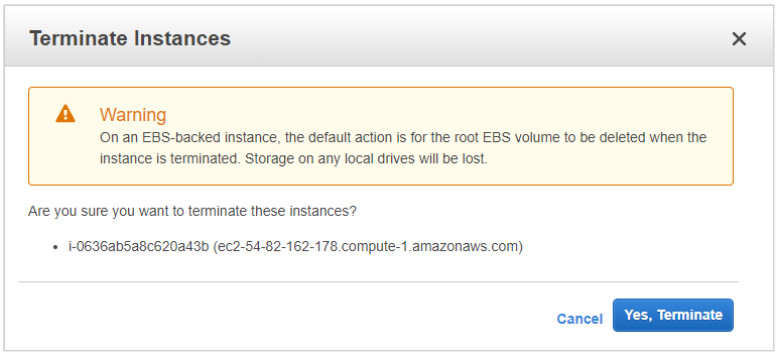
Updating the MT – Commercial Version

CloudCheckr updates the SaaS version of the application regularly. However, CloudCheckr keeps the MT – Commercial version a few revisions behind to maximize stability.

Note: If you acquired the self-hosted version from the AWS Marketplace, AWS will email you when a new version is available.

1. Return to the AWS Management Console.
2. From the Compute section, select **EC2**.
3. Select **Instances > Instances**.
4. Select the box next to the EC2 instance that contains the Web Console, Workers, and Scheduler.
5. From the Actions menu, select **Instant State > Terminate**.

   A message displays and prompts you to confirm your selection.



6. Click **Yes, Terminate**.
7. Select the **new EC2 instance** from the list, copy its Public DNS, and paste it into a new browser window.

   The first installation screen, associated with the new EC2 instance, opens.
8. Click **Verify Installation**.

   The next screen indicates that CloudCheckr will install the latest version of the software.
9. Click **Install**.

Required Information

Attribute	Value
S3 Bucket Name	
Policy Name	
Role Name	
Name of RDS Server	
Master Username and Password of RDS Server	
EC2 Instance ID	
EC Instance Type	
Availability Zone (region code)	
Private Key (.PEM) File Location and Name	
Public DNS Name (IPv4)	
Private DNS	
Subnet ID	

Learn more about the CloudCheckr Cloud Management Platform at www.cloudcheckr.com.