



SELF-HOSTED

MULTI-TIER: COMMERCIAL VERSION INSTALLATION GUIDE

Version 11.0

TABLE OF CONTENTS

Introduction.....	3
Creating Your S3 Bucket, IAM Policy, and IAM Role	3
Purchasing the Multi-Tiered Commercial Version.....	14
Configuring the EC2 Instance for the Web Console, Workers, and Schedulers	19
Installing the Application	25
Connecting the EC2 Instance to the Application UI.....	29
Configuring Application Settings	34
Creating AWS Credentials	35
Creating a Trusted User	37
Updating the MT – Commercial Version.....	38
Required Information	39

Introduction

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

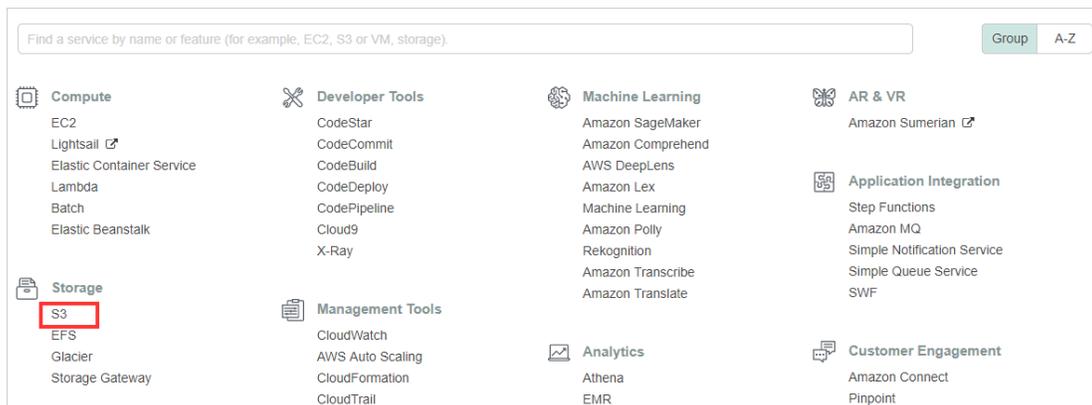
This version enables customers to use an Amazon Machine Image (AMI) to create a self-hosted version of the application within a virtual private cloud (VPC) on an Amazon Elastic Compute Cloud (Amazon EC2) instance using RDS databases.

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**.



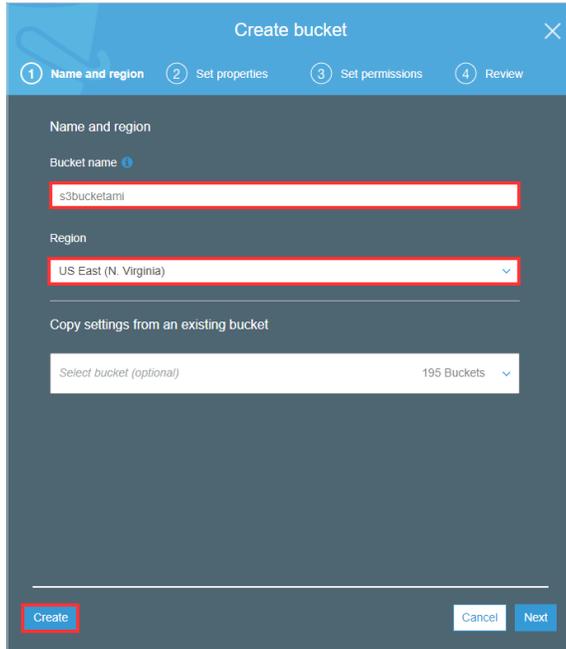
The Amazon S3 page opens.



3. Click **+ Create bucket**.

The Create bucket configuration wizard opens.

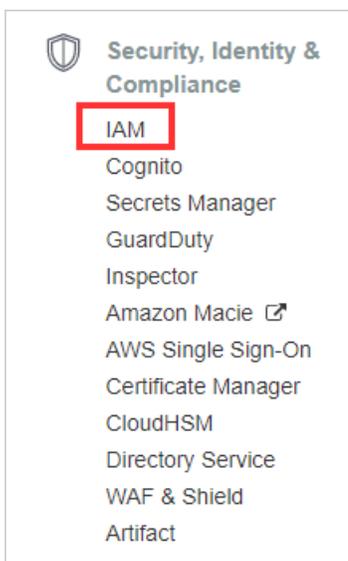
4. Configure your S3 bucket:
 - a. In the Bucket name text field, type a bucket name.
 - b. From the Region drop-down menu, select a region.
 - c. Click **Create**.



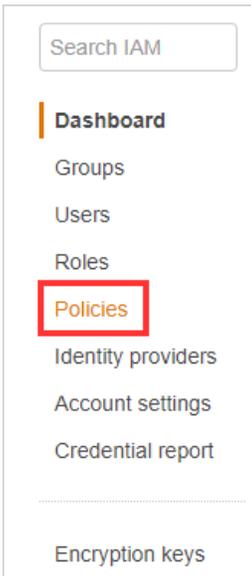
The screenshot shows the 'Create bucket' wizard in the AWS console. The title bar reads 'Create bucket' with a close button. Below the title bar are four numbered steps: 1. Name and region, 2. Set properties, 3. Set permissions, and 4. Review. The first step, 'Name and region', is currently selected. It contains three main sections: 'Bucket name' with a text input field containing 's3bucketami', 'Region' with a dropdown menu showing 'US East (N. Virginia)', and 'Copy settings from an existing bucket' with a dropdown menu showing 'Select bucket (optional)' and '195 Buckets'. At the bottom of the wizard, there are three buttons: 'Create' (highlighted with a red box), 'Cancel', and 'Next'.

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**.



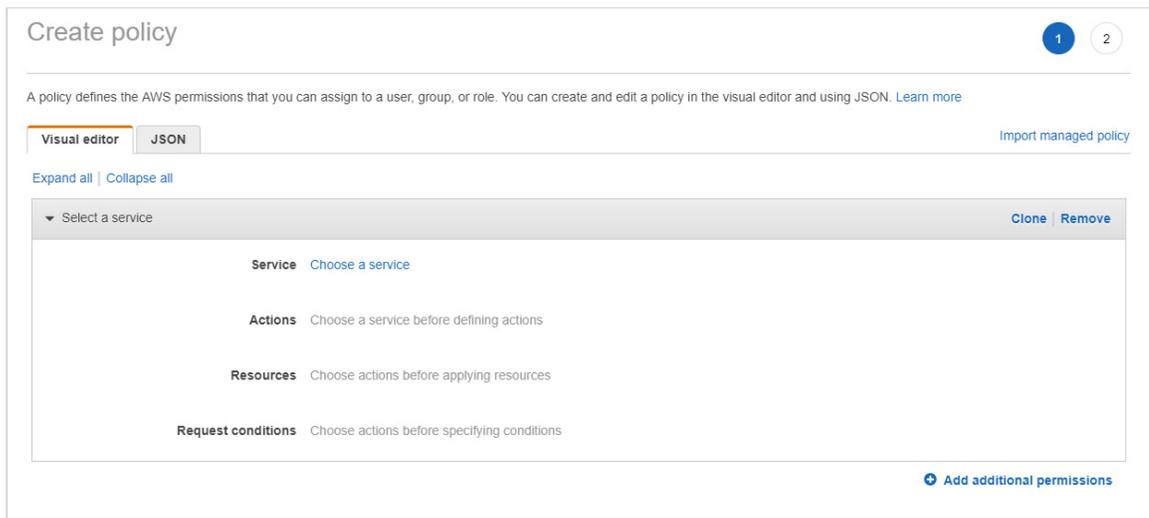
The policy page displays.

A screenshot of the IAM Policies page. At the top, there is a 'Create policy' button and a 'Policy actions' dropdown. Below that is a filter section with 'Filter: Policy type' and a search box. The main content is a table with the following columns: Policy name, Type, Attachments, and Description. The table shows several policies, including 'AdministratorAccess' which is a Job function policy with 50 attachments.

Policy name	Type	Attachments	Description
2150_QA_Account_Auto	Customer managed	1	
245990094719Policy	Customer managed	1	
8.1-9.2-mt-upgrade-test	Customer managed	1	
AAA	Customer managed	1	
AdministratorAccess	Job function	50	Provides full access to AWS services and resources.
AdministratorAccess-testtest	Customer managed	1	Provides full access to AWS services and resources.
ag-gov-iam-stack-CloudCheckrManagedPolicy-1IRTWNVM...	Customer managed	1	CloudCheckr Account Policy

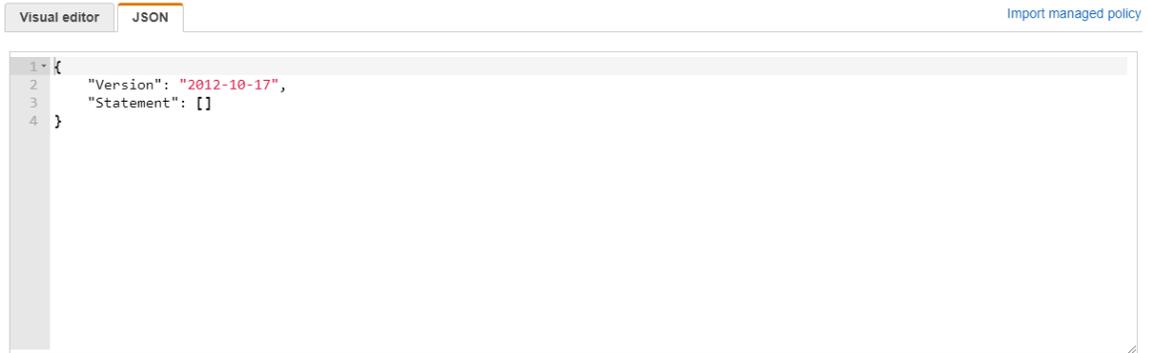
8. Click **Create policy**.

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.

Create policy

Review policy

Name:

Use alphanumeric and "+-,@_." characters. Maximum 128 characters.

Description:

Maximum 1000 characters. Use alphanumeric and "+-,@_." characters.

Summary

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose [Show remaining](#). [Learn more](#)

Filter

Service	Access level	Resource	Request condition
Allow (1 of 136 services) Show remaining 135			
S3	Full: Read, Write, Permissions management Limited: List	Multiple	None

* Required

Cancel Previous **Create policy**

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**.

Search IAM

- Dashboard
- Groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings
- Credential report
- Encryption keys

17. Click **Create role**.

The Create role page opens.

1 2 3

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web Identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	DMS	Elastic Transcoder	Machine Learning	SageMaker
Application Auto Scaling	Data Pipeline	ElasticLoadBalancing	MediaConvert	Service Catalog
Auto Scaling	DeepLens	Glue	OpsWorks	Step Functions
Batch	Directory Service	Greengrass	RDS	Storage Gateway
CloudFormation	DynamoDB	GuardDuty	Redshift	
CloudHSM	EC2	Inspector	Rekognition	
CloudWatch Events	EMR	IoT	S3	
CodeBuild	ElasticCache	Kinesis	SMS	
CodeDeploy	Elastic Beanstalk	Lambda	SNS	
Config	Elastic Container Service	Lex	SWF	

* Required

Cancel Next: Permissions

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

The Attach permissions policies page opens.

1 2 3

Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy Refresh

Filter: Policy type Search Showing 659 results

Policy name	Attachments	Description
<input type="checkbox"/> 2150_QA_Account_Auto	1	
<input type="checkbox"/> 245990094719Policy	1	
<input type="checkbox"/> 8.1-9.2-mt-upgrade-test	1	
<input type="checkbox"/> AAA	1	
<input type="checkbox"/> AdministratorAccess	50	Provides full access to AWS services and resources.
<input type="checkbox"/> AdministratorAccess-testtest	1	Provides full access to AWS services and resources.
<input type="checkbox"/> ag-gov-iam-stack-CloudCheckrManagedPolicy...	1	CloudCheckr Account Policy
<input type="checkbox"/> AG-STACK3-CCManagedPolicy-1MLMJTXU9...	1	CC Account Policy
<input type="checkbox"/> AggregateCloudTrail33	0	AggregateCloudTrail33
<input type="checkbox"/> AggregateCloudTrailMin32	1	AggregateCloudTrailMin32
<input type="checkbox"/> AggregatedEUCloudTrail	1	Aggregated EU CloudTrail Policy
<input type="checkbox"/> AISPLTest	1	AISPL Test

* Required

Cancel Previous Next: Review

19. Select the **Full CloudCheckr IAM Policy** you just created from the list.

20. Click **Next: Review**.

The Review page opens.

Create role

Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=,@_-' characters. Maximum 64 characters.

Role description

Maximum 1000 characters. Use alphanumeric and '+=,@_-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies [mnm_mtic_april](#)

* Required

[Cancel](#) [Previous](#) [Create role](#)

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.

Roles >

Summary [Delete role](#)

Role ARN arn:aws:iam::215011050627:role/

Role description Allows EC2 instances to call AWS services on your behalf. [Edit](#)

Instance Profile ARNs arn:aws:iam::215011050627:instance-profile/

Path /

Creation time 17:34 EDT

Maximum CLI/API session duration 1 hour [Edit](#)

Permissions **Trust relationships** **Access Advisor** **Revoke sessions**

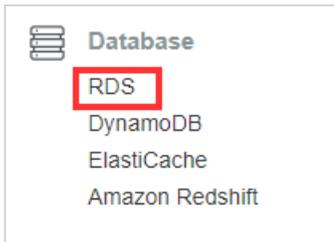
[Attach policy](#) Attached policies: 1

Policy name	Policy type
mnm_mtic_april	Managed policy

[Add inline policy](#)

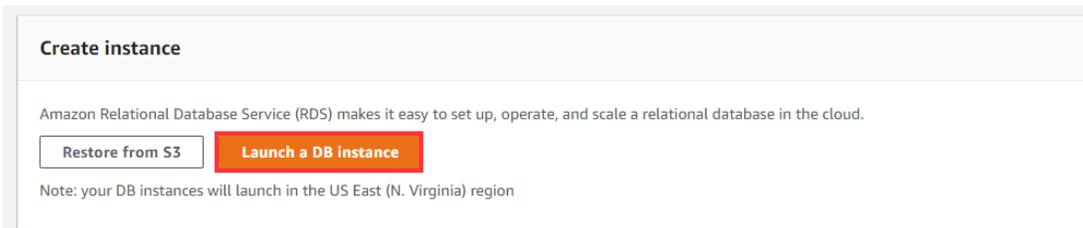
24. Return to the AWS Services page.

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

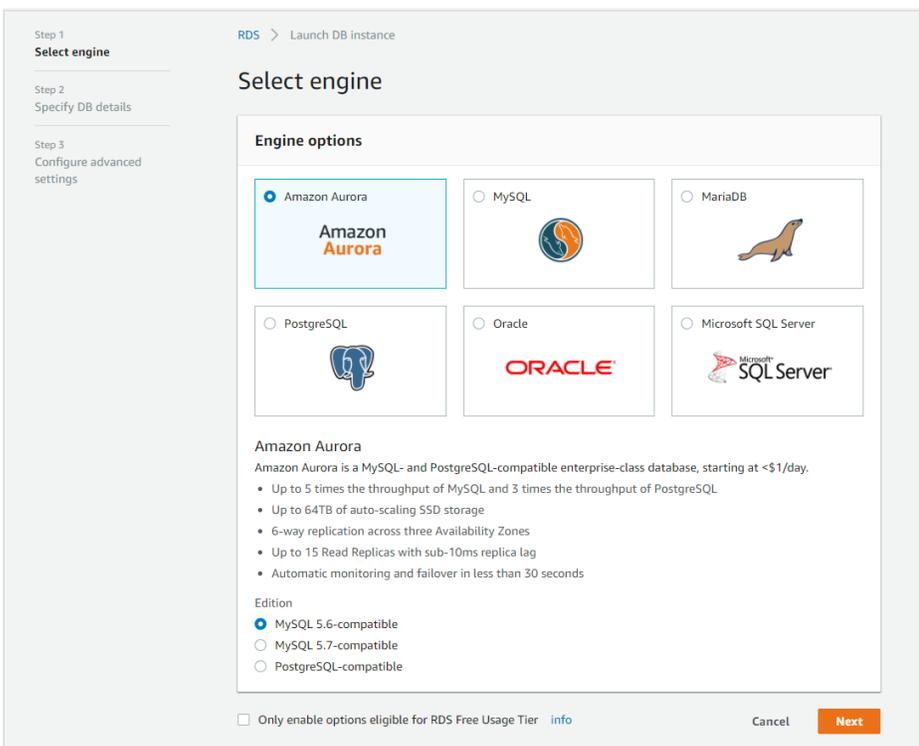


The Amazon RDS page opens.

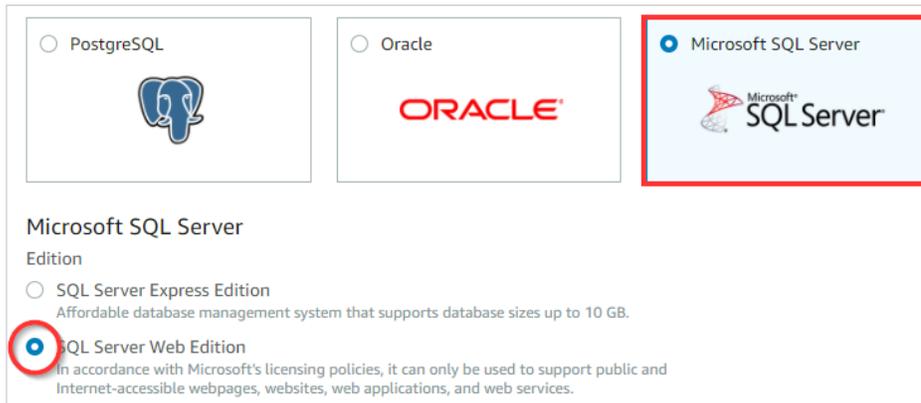
26. Navigate to the Create instance section and click **Launch a DB instance**.



27. The Select engine wizard opens.



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



PostgreSQL

Oracle

Microsoft SQL Server

Microsoft SQL Server

Edition

SQL Server Express Edition
Affordable database management system that supports database sizes up to 10 GB.

SQL Server Web Edition
In accordance with Microsoft's licensing policies, it can only be used to support public and Internet-accessible webpages, websites, web applications, and web services.

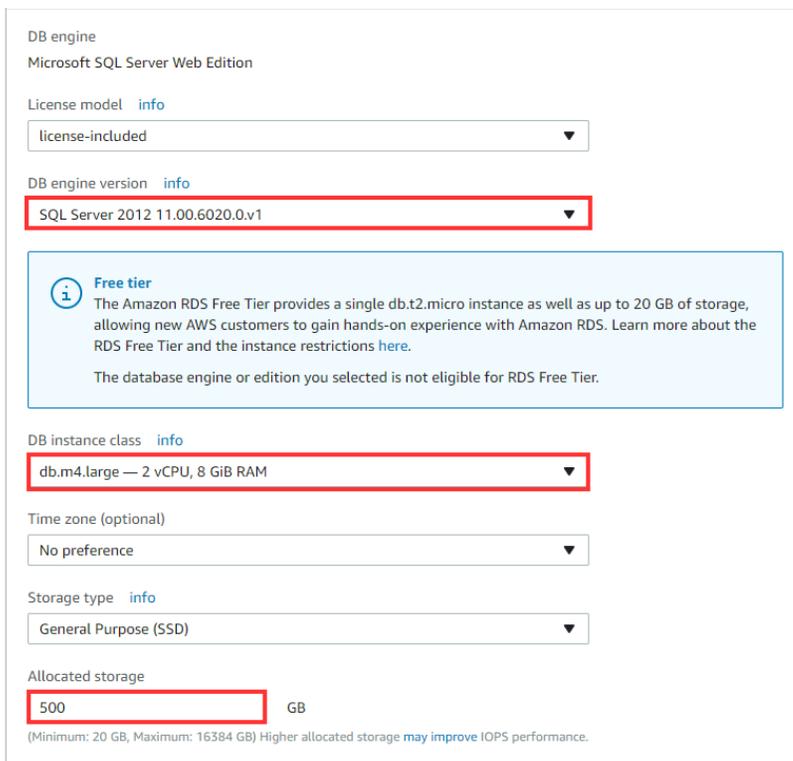
29. Click **Next**.

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.



DB engine
Microsoft SQL Server Web Edition

License model [info](#)
license-included

DB engine version [info](#)
SQL Server 2012 11.00.6020.0.v1

Free tier
The Amazon RDS Free Tier provides a single db.t2.micro instance as well as up to 20 GB of storage, allowing new AWS customers to gain hands-on experience with Amazon RDS. Learn more about the RDS Free Tier and the instance restrictions [here](#).
The database engine or edition you selected is not eligible for RDS Free Tier.

DB instance class [info](#)
db.m4.large — 2 vCPU, 8 GiB RAM

Time zone (optional)
No preference

Storage type [info](#)
General Purpose (SSD)

Allocated storage
500 GB
(Minimum: 20 GB, Maximum: 16384 GB) Higher allocated storage [may improve](#) IOPS performance.

33. Scroll down to the Settings section.

Settings

DB instance identifier [info](#)
Specify a name that is unique for all DB instances owned by your AWS account in the current region.

DB instance identifier is case insensitive, but stored as all lower-case, as in "mydbinstance".
Constraints:

- Must contain from 1 to 63 alphanumeric characters or hyphens (1 to 15 for SQL Server).
- First character must be a letter.
- Cannot end with a hyphen or contain two consecutive hyphens.

Master username [info](#)
Specify an alphanumeric string that defines the login ID for the master user.

Master Username must start with a letter. Must contain 1 to 64 alphanumeric characters.

Master password [info](#) **Confirm password** [info](#)

Master Password must be at least eight characters long, as in "mypassword". Can be any printable ASCII character except "/", "", or "@".

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.

Configure advanced settings

Network & Security

Virtual Private Cloud (VPC) [info](#)
VPC defines the virtual networking environment for this DB instance.

Only VPCs with a corresponding DB subnet group are listed.

Subnet group [info](#)
DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

Public accessibility [info](#)

Yes
EC2 instances and devices outside of the VPC hosting the DB instance will connect to the DB instances. You must also select one or more VPC security groups that specify which EC2 instances and devices can connect to the DB instance.

No
DB instance will not have a public IP address assigned. No EC2 instance or devices outside of the VPC will be able to connect.

Availability zone [info](#)

VPC security groups
Security groups have rules authorizing connections from all the EC2 instances and devices that need to access the DB instance.

Create new VPC security group

Choose existing VPC security groups

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.

CloudCheckr (2 results) showing 1 - 2



CloudCheckr Cost and Security Management

★★★★★ (0) | Version 1 | Sold by CloudCheckr

CloudCheckr Security and Cost Management provides comprehensive coverage of your AWS environment. Features include: RI purchasing recommendations, idle resource warnings,...



CloudCheckr Cost and Security Management

★★★★★ (0) | Version 7.8 | Sold by CloudCheckr Inc.

Starting from **\$3.00/hr** or from **\$12,000.00/yr** (up to 54% savings) for software + AWS usage fees

CloudCheckr Security and Cost Management provides comprehensive coverage of your AWS environment. Features include: RI purchasing recommendations, idle resource warnings,...

Windows, Windows Server 2012 R2 w/SQL Standard 2014 WIN2012R2_SQLSTD14 - 64-bit Amazon Machine Image (AMI)

showing 1 - 2

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



CloudCheckr Cost and Security Management

★★★★★ (0) | Version 7.8 | Sold by CloudCheckr Inc.

Starting from **\$3.00/hr** or from **\$12,000.00/yr** (up to 54% savings) for software + AWS usage fees

CloudCheckr Security and Cost Management provides comprehensive coverage of your AWS environment. Features include: RI purchasing recommendations, idle resource warnings,...

Windows, Windows Server 2012 R2 w/SQL Standard 2014 WIN2012R2_SQLSTD14 - 64-bit Amazon Machine Image (AMI)

The CloudCheckr Cost and Security Management page opens.



CloudCheckr Cost and Security Management

Sold by: [CloudCheckr Inc.](#)

CloudCheckr Security and Cost Management provides comprehensive coverage of your AWS environment. Features include: RI purchasing recommendations, idle resource warnings, cost [Show more](#)

Windows ☆☆☆☆☆ (0) Free Trial

Continue to Subscribe

Save to List

Typical Total Price

\$7.378/hr

Total pricing per instance for services hosted on r3.xlarge in US East (N. Virginia). [View Details](#)

Overview
Pricing
Usage
Support
Reviews

Product Overview

What's Included

Note: Always ensure your operating system is current for your needs. This product includes both of the software packages described below:



CloudCheckr Cost and Security Management

Sold by: [CloudCheckr Inc.](#)

CloudCheckr Security and Cost Management provides comprehensive coverage of your AWS environment. Features include: RI purchasing recommendations, idle resource warnings, cost tracking/allocation, CloudTrail reporting, change monitoring, security group mapping, and perimeter assessments.



Microsoft Windows Server 2012 RTM with SQL Server Standard 2014

Sold by: [Amazon Web Services](#)

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 compatible Windows-based solution on AWS' high-performance, reliable, cost-effective, cloud computing platform. Common Windows use cases include Enterprise Windows-based application hosting, website and web-service hosting, data processing, media transcoding, distributed testing, ASP.NET application hosting, and any other application requiring Windows software.

Highlights

- Hundreds of best practice checks covering security, availability, cost, and usage
- Discover and visualize what's running in AWS
- Optimize costs in AWS

4. Scroll down to the Pricing Information section.

Pricing Information

Use this tool to estimate the software and infrastructure costs based on your configuration choices. Your usage and costs might be different from this estimate. They will be reflected on your monthly AWS billing reports.

Estimating your costs

Choose your region and fulfillment option to see the pricing details. Then, modify the estimated price by choosing different instance types.

Region

US East (N. Virginia) ▼

Fulfillment Option

64-bit Amazon Machine Image (AMI) ▼

Software Pricing Details

CloudCheckr Cost and Security Management **\$6.000 /hr** >

running on r3.xlarge

Infrastructure Pricing Details

Estimated Infrastructure Cost **\$1.378 EC2/hr** >

Free Trial < Try one instance of this product for 15 days. There will be no hourly software charges for that instance, but AWS infrastructure charges still apply. Free Trials will automatically convert to a paid hourly subscription upon expiration.

The table shows current software and infrastructure pricing for services hosted in **US East (N. Virginia)**. Additional taxes or fees may apply.

CloudCheckr Cost and Security Management

Switch to annual pricing for savings up to 54%

EC2 Instance type	Hourly		Annual
	Software/hr	EC2/hr	Total/hr
<input type="radio"/> m3.large	\$3.000	\$0.704	\$3.704
<input type="radio"/> m3.xlarge	\$6.000	\$1.266	\$7.266
<input type="radio"/> m3.2xlarge	\$12.000	\$2.532	\$14.532
<input type="radio"/> m4.large	\$3.000	\$0.672	\$3.672
<input type="radio"/> m4.xlarge	\$6.000	\$0.864	\$6.864
<input type="radio"/> m4.2xlarge	\$12.000	\$1.728	\$13.728



Multi-Tier: Commercial Version Installation Guide 15

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.

Estimating your costs

Choose your region and fulfillment option to see the pricing details. Then, modify the estimated price by choosing different instance types.

Region

Fulfillment Option

Software Pricing Details

CloudCheckr Cost and Security Management **\$6.000 /hr** >
running on r3.xlarge

Infrastructure Pricing Details

Estimated Infrastructure Cost \$1.378 EC2/hr >

Free Trial Try one instance of this product for 15 days. There will be no hourly software charges for that instance, but AWS infrastructure charges still apply. Free Trials will automatically convert to a paid hourly subscription upon expiration.

The table shows current software and infrastructure pricing for services hosted in **US East (N. Virginia)**. Additional taxes or fees may apply.

CloudCheckr Cost and Security Management
 Switch to annual pricing for savings up to 54%

EC2 Instance type	Software/hr	EC2/hr	Total/hr
<input type="radio"/> m3.large	\$3.000	\$0.704	\$3.704
<input type="radio"/> m3.xlarge	\$6.000	\$1.266	\$7.266
<input type="radio"/> m3.2xlarge	\$12.000	\$2.532	\$14.532
<input type="radio"/> m4.large	\$3.000	\$0.672	\$3.672
<input type="radio"/> m4.xlarge	\$6.000	\$0.864	\$6.864
<input type="radio"/> m4.2xlarge	\$12.000	\$1.728	\$13.728

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

CloudCheckr

CloudCheckr Cost and Security Management

Continue to Subscribe

Overview
Pricing
Usage
Support
Reviews

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

Launch on EC2:

CloudCheckr Cost and Security Management on Windows Server w/SQL

1-Click Launch
Review, modify and launch

Manual Launch
With EC2 Console, API or CLI

Service Catalog
Copy to SC and Launch

Click "Accept Software Terms & Launch with 1-Click" to launch this software with the settings below

Once you accept the terms, you will have access to launch any version of this software in any supported region. For future launches, you can return to this page or launch directly from the EC2 console, APIs or CLI.

Software Pricing

Subscription Term	Applicable Instance Type
<input checked="" type="radio"/> Hourly	m3.xlarge
<input type="radio"/> Annual	m4.xlarge
	r3.2xlarge
	m4.4xlarge
	r3.4xlarge
	m4.10xlarge
	m4.2xlarge
	m4.large
	r3.xlarge
	r3.large
	m3.2xlarge

Hourly fee
\$6.00 / hour
Find instance details in EC2 instance section below.

Accept Software Terms & Launch with 1-Click

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#) and your use of AWS services is subject to the [AWS Customer Agreement](#).

Cost Estimator

\$5,312.16 / month
Additional taxes may apply.
r3.xlarge EC2 Instance usage fees
Assumes 24 hour use over 30 days

Software Charges

\$4,320.00 / month
\$4,320.00 monthly software fees for r3.xlarge

AWS Infrastructure Charges

\$992.16 / month
Cost varies for storage fees

T2, C4, C5, D2, H1, M4, M5, P2, R4, X1 and X1e instance types are only available in VPCs. To view the details for these instance types, please select a VPC.

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**.

Price for your Selections:

\$7.38 / hour
\$1.38 r3.xlarge EC2 Instance usage fees +
\$6.00 hourly software fee
Additional taxes may apply.

\$0.10 per GB-month of provisioned storage
EBS General Purpose (SSD) volumes

Accept Software Terms & Launch with 1-Click

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#) and your use of AWS services is subject to the [AWS Customer Agreement](#).

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

Thank you for subscribing to CloudCheckr Cost and Security Management

An instance of this software will be deployed on EC2 soon after your subscription completes.

You can check the status of this instance on [EC2 Console](#). You can also view all instances on [Your Software](#) page.

✓ Software and AWS hourly usage fees apply when the instance is running and will appear on your monthly bill.

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 2: Choose an Instance Type

Currently selected: m4.xlarge (13 ECUs, 4 vCPUs, 2.4 GHz, Intel Xeon E5-2676v3, 16 GiB memory, EBS only)

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes
General purpose	m5.12xlarge	48	192	EBS only	Yes	10 Gigabit	Yes
General purpose	m5.24xlarge	96	384	EBS only	Yes	25 Gigabit	Yes
General purpose	m4.large	2	8	EBS only	Yes	Moderate	Yes
General purpose	m4.xlarge	4	16	EBS only	Yes	High	Yes

Cancel Previous Review and Launch **Next: Configure Instance Details**

Step 3: Configure Instance Details displays.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: Request Spot instances

Network: vpc-865744e2 Create new VPC

Subnet: subnet-c596c99c | us-east-1a Create new subnet
232 IP Addresses available

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

Placement group: Add instance to placement group

Domain join directory: None Create new directory

IAM role: None Create new IAM role

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring
Additional charges apply.

EBS-optimized instance: Launch as EBS-optimized instance

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Elastic GPU: Add GPU
Additional charges apply.

Network interfaces

Device	Network interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
--------	-------------------	--------	------------	------------------------	----------

Cancel Previous Review and Launch Next: Add Storage

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.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances [Launch into Auto Scaling Group](#)

Purchasing option Request Spot instances

Network [Create new VPC](#)

Subnet [Create new subnet](#)
46 IP Addresses available

Auto-assign Public IP

Placement group Add instance to placement group

Domain join directory [Create new directory](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Enable termination protection Protect against accidental termination

Monitoring Enable CloudWatch detailed monitoring
Additional charges apply

EBS-optimized instance Launch as EBS-optimized instance

Tenancy
Additional charges will apply for dedicated tenancy

Elastic GPU Add GPU
Additional charges apply

Network interfaces

Device	Network interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
--------	-------------------	--------	------------	------------------------	----------

Cancel Previous **Review and Launch** Next: Add Storage

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.

Step 6: Configure Security Group
 A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security group name:
 Description:

Type	Protocol	Port Range	Source	Description
Custom TCP I	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

Warning
 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

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)

Step 6: Configure Security Group
 A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security group name:
 Description:

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	Anywhere 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Anywhere 0.0.0.0/0	e.g. SSH for Admin Desktop
RDP	TCP	3389	Anywhere 0.0.0.0/0	e.g. SSH for Admin Desktop
MS SQL	TCP	1433	Anywhere 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

11. Click **Review and Launch**.

Step 7: Review Instance Launch displays.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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.

AMI Details Edit AMI

IC_MT [REDACTED]
 C2S Multi-tier Marketplace Submission (9.2)
 Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

Instance Type Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
m4.xlarge	13	4	16	EBS only	Yes	High

Security Groups Edit security groups

Security group name: mtic_april_2018
 Description: launch-wizard-78 created 2018-04-05T18:23:42.161-04:00

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
Custom TCP Rule	TCP	443	72.43.63.34/32	
Custom TCP Rule	TCP	3389	72.43.63.34/32	
Custom TCP Rule	TCP	1433	72.43.63.34/32	

Instance Details Edit instance details

Storage Edit storage

Tags Edit tags

Cancel Previous Launch

12. Click **Launch**.

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

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

▼

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

Cancel Launch Instances

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.

Launch Status

✔ Your instances are now launching
The following instance launches have been initiated: i-0e6eebb03b6174737 [View launch log](#)

ℹ 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](#)

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.

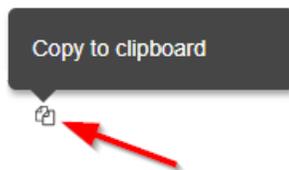
18. From the Description tab, locate the following items:

- Instance ID
- Instance Type
- Availability Zone (region code)
- Key Pair Name
- Public DNS (IPv4)
- Private DNS
- Subnet ID

The screenshot shows the AWS Management Console interface for an EC2 instance. The 'Description' tab is active, displaying various instance details. Red boxes highlight the following items:

- Instance ID: i-01662a8296af6a3f0
- Instance state: running
- Instance type: m4.xlarge
- Elastic IPs: -
- Availability zone: us-east-1a
- Security groups: [Security Group IDs]
- Scheduled events: No scheduled events
- AMI ID: [AMI ID]
- Platform: windows
- IAM role: [IAM Role]
- Key pair name: [Key Pair Name]
- ClassicLink: -
- EBS-optimized: True
- Root device type: ebs
- Root device: /dev/sda1
- Block devices: /dev/sda1, xvdf
- Elastic GPU: -
- Elastic GPU type: -
- Public DNS (IPv4): [Public DNS (IPv4)]
- IPV4 Public IP: [IPV4 Public IP]
- IPV6 IPs: -
- Private DNS: [Private DNS]
- Private IPs: 10.0.0.127
- Secondary private IPs: -
- VPC ID: vpc-87d9a3e1
- Subnet ID: subnet-a07d5afb
- Network interfaces: eth0
- Source/dest. check: True
- T2 Unlimited: -
- Owner: 215011050627
- Launch time: April 5, 2018 at 6:42:29 PM UTC-4 (13 hours)
- Termination protection: False
- Lifecycle: normal
- Monitoring: basic
- Alarm status: None
- Kernel ID: -

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

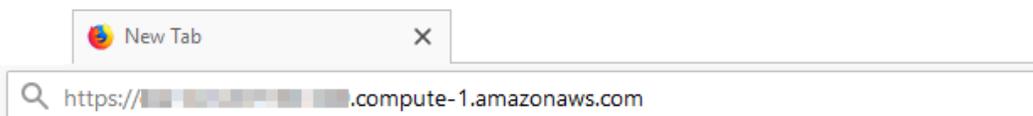


Installing the Application

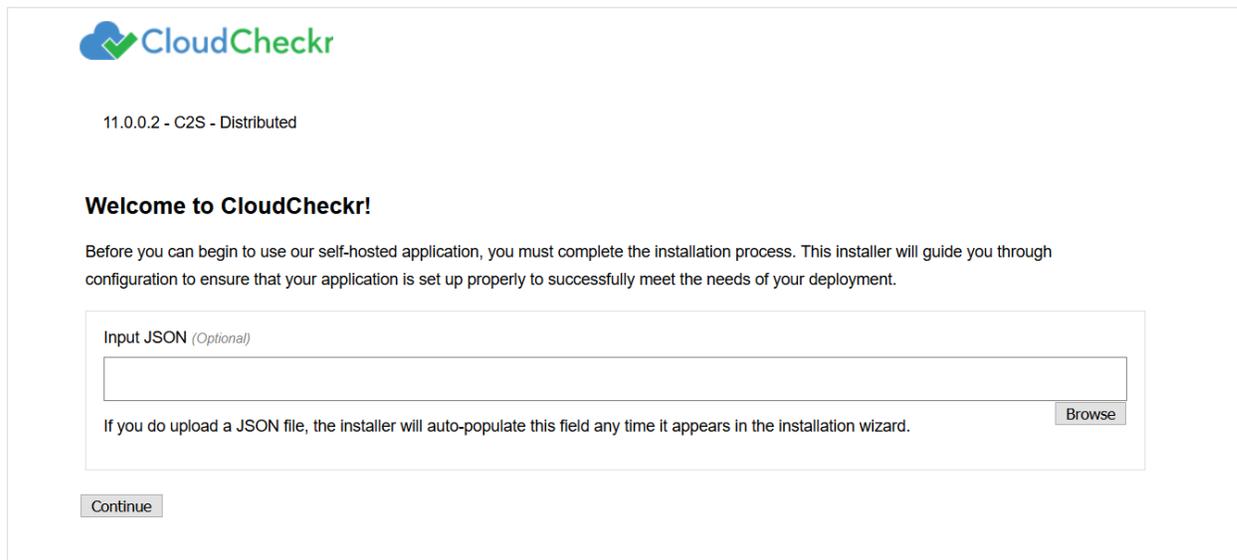
In this procedure, you will use the public IP address to connect to the EC2 instance and install the application.

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.

11.0.0.2 - C2S - Distributed

Database Hostname (server name)

Database Username

Database Password

SSO URL *(Optional)*

The Single sign-on URL initiated at the identity provider service site

SSL Certificate *(Optional)*

A certificate provided by an outside service that allows network traffic to be encrypted

SSL Certificate Password File *(Optional)*

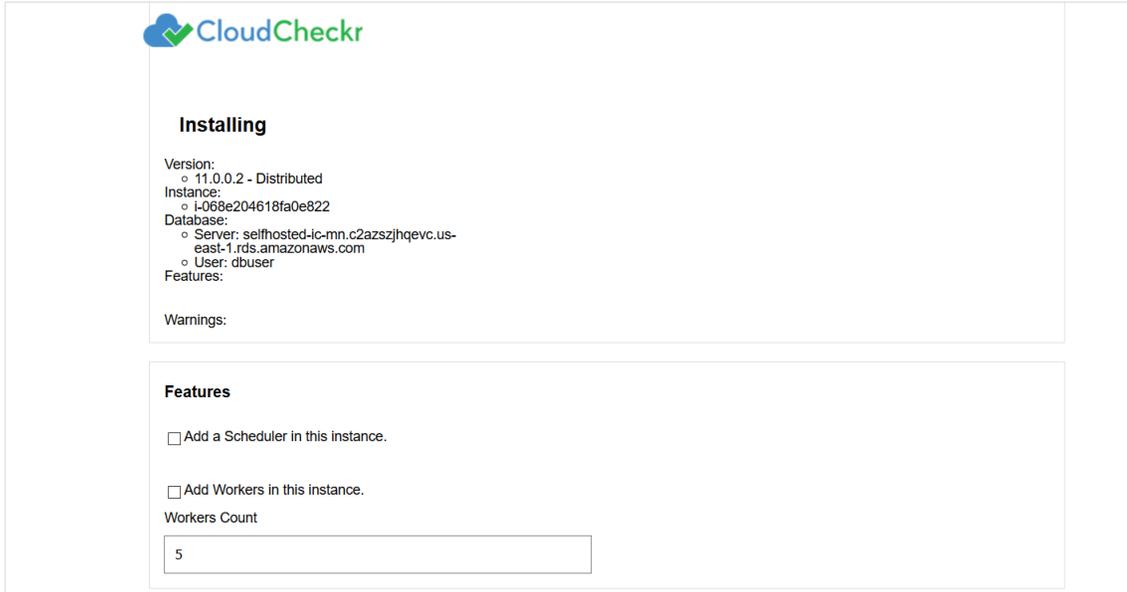
The password required for the application to use the SSL Certificate Private Key

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.



CloudCheckr

Installing

Version:
◦ 11.0.0.2 - Distributed
Instance:
◦ i-068e204618fa0e822
Database:
◦ Server: selfhosted-ic-mn.c2azszjhqevc.us-east-1.rds.amazonaws.com
◦ User: dbuser
Features:

Warnings:

Features

Add a Scheduler in this instance.

Add Workers in this instance.

Workers Count

5

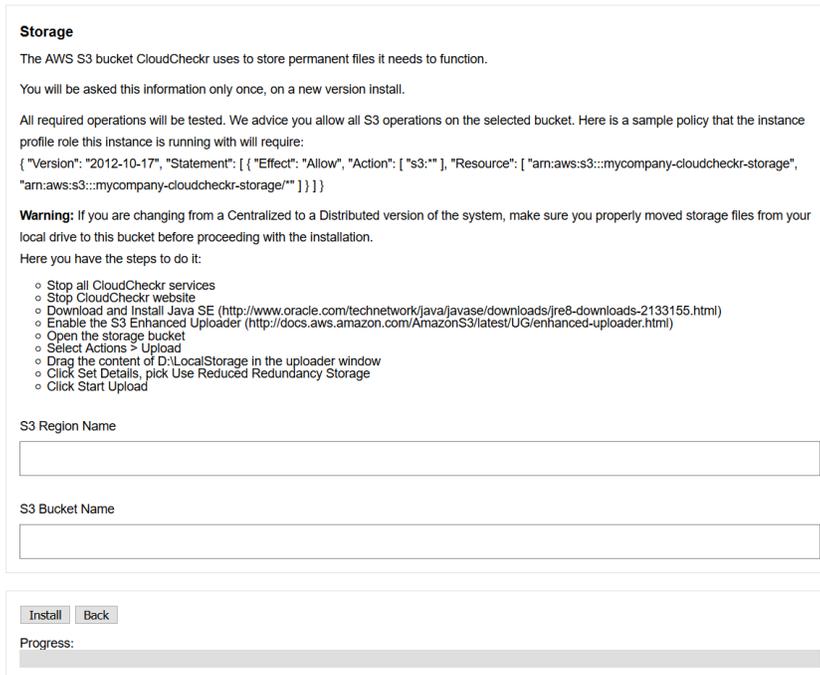
9. Select **Add a Scheduler in this instance** check box.

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.



Storage

The AWS S3 bucket CloudCheckr uses to store permanent files it needs to function.

You will be asked this information only once, on a new version install.

All required operations will be tested. We advice you allow all S3 operations on the selected bucket. Here is a sample policy that the instance profile role this instance is running with will require:

```
{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "s3:*" ], "Resource": [ "arn:aws:s3:::mycompany-cloudcheckr-storage", "arn:aws:s3:::mycompany-cloudcheckr-storage/*" ] } ] }
```

Warning: If you are changing from a Centralized to a Distributed version of the system, make sure you properly moved storage files from your local drive to this bucket before proceeding with the installation.

Here you have the steps to do it:

- Stop all CloudCheckr services
- Stop CloudCheckr website
- Download and Install Java SE (<http://www.oracle.com/technetwork/java/javase/downloads/jre8-downloads-2133155.html>)
- Enable the S3 Enhanced Uploader (<http://docs.aws.amazon.com/AmazonS3/latest/UG/enhanced-uploader.html>)
- Open the storage bucket
- Select Actions > Upload
- Drag the content of D:\LocalStorage in the uploader window
- Click Set Details, pick Use Reduced Redundancy Storage
- Click Start Upload

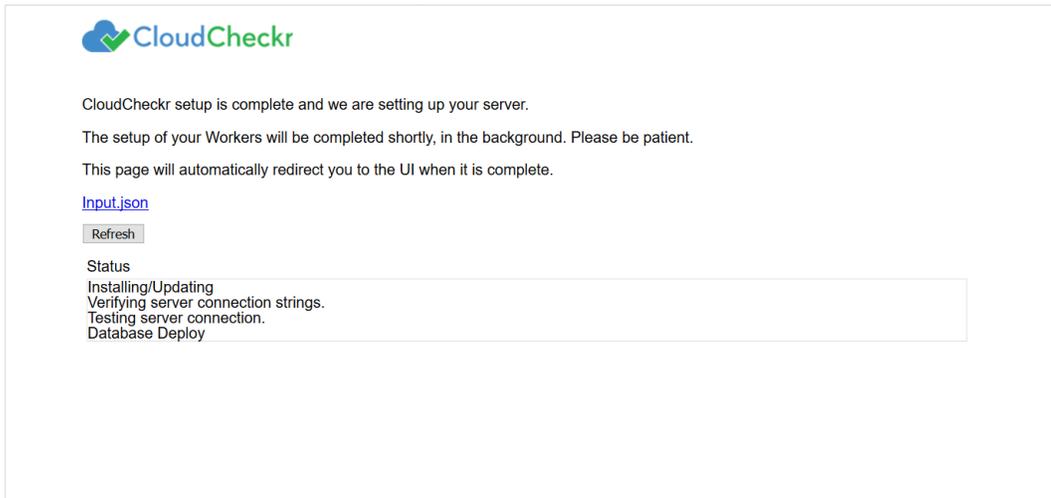
S3 Region Name

S3 Bucket Name

Progress:

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.

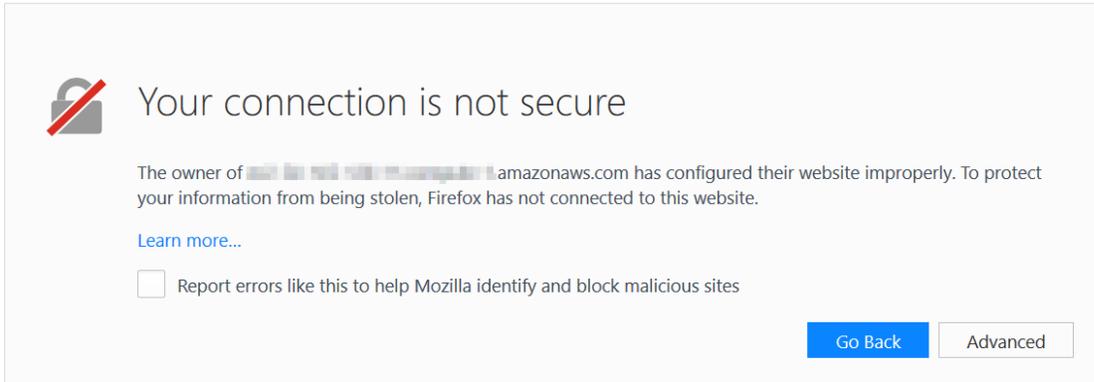
At this point, you can download the Input JSON file for later use. The file contains the exact configuration that you set up earlier in the installation process. Since the filename is not important as part of ingestion, feel free to rename the file. If you forget to click the **Input.json** link, and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

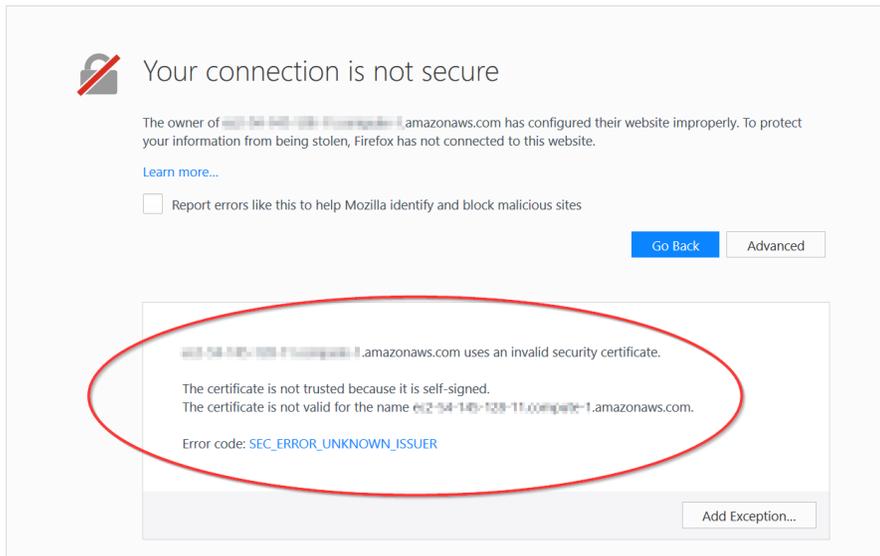


Note: The content and look-and-feel of the warning message depends on the browser in use.

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.

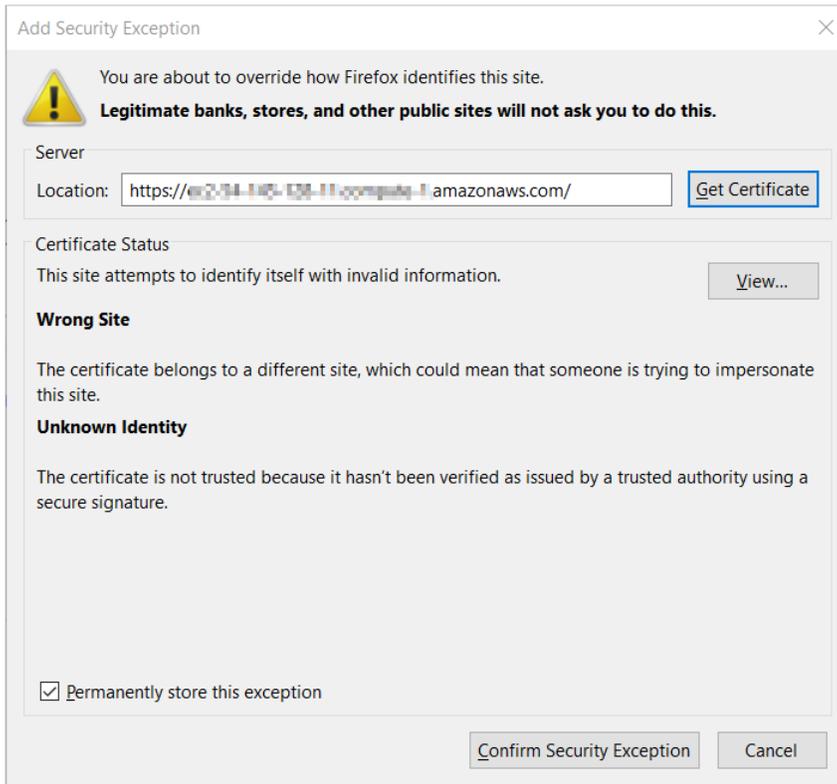
1. Click **Advanced** to get more information about the warning.

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



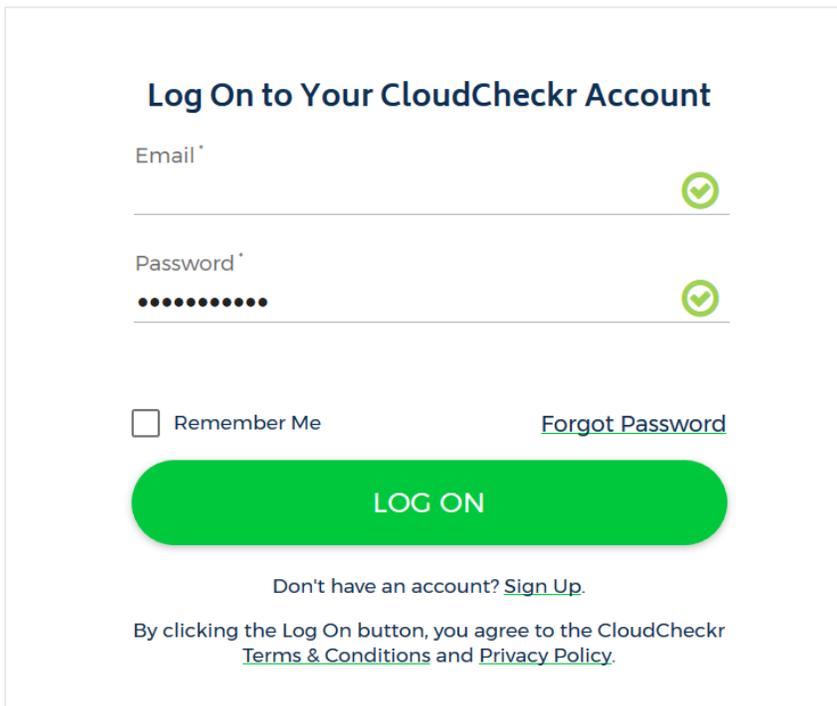
2. Click **Add Exception...** to add the EC2 instance as a security exception.

The Add Security Exception dialog box opens.



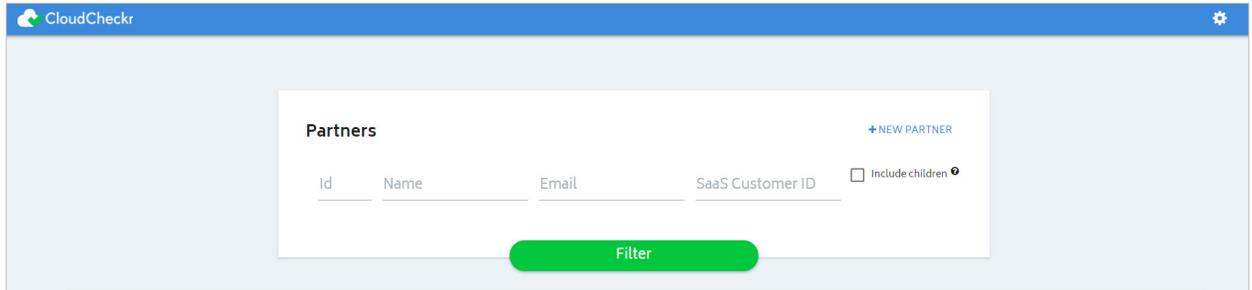
3. Verify that **Permanently store this exception** is selected and click **Confirm Security Exception**.

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.

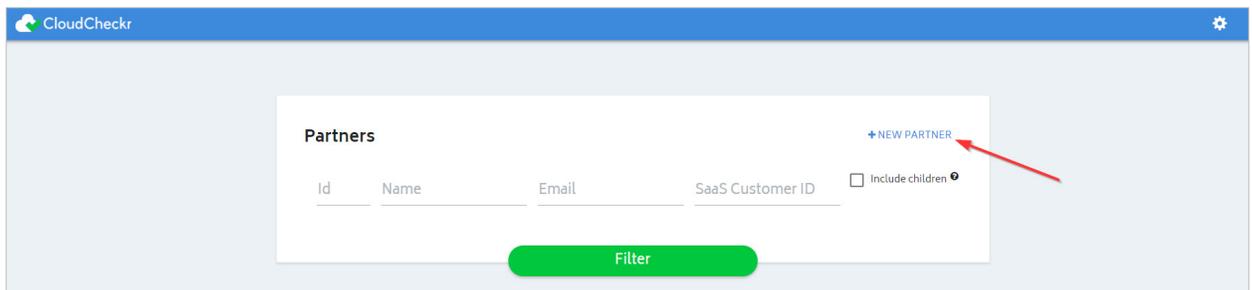


Partners are the top-level container within the application where you can generate and store multiple AWS accounts.

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.

Partner Information

Enter a name for your new partner. An email address is only required if an initial user is added.

Partner Name

Partner Email

Initial User

If you choose to add a user to the partner, you can optionally set a password. If none is provided, the user will be required to set one on activation.

Add an initial user to the partner

Password

Allow user to create partners

Resellers

This partner will be created as your reseller, if selected. To complete the required configuration for this new partner to receive the billing information from your Detailed Billing Report (DBR), go to Settings > Resellers.

This partner is a reseller

Master-Payer Partner Id

CANCEL CREATE

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.

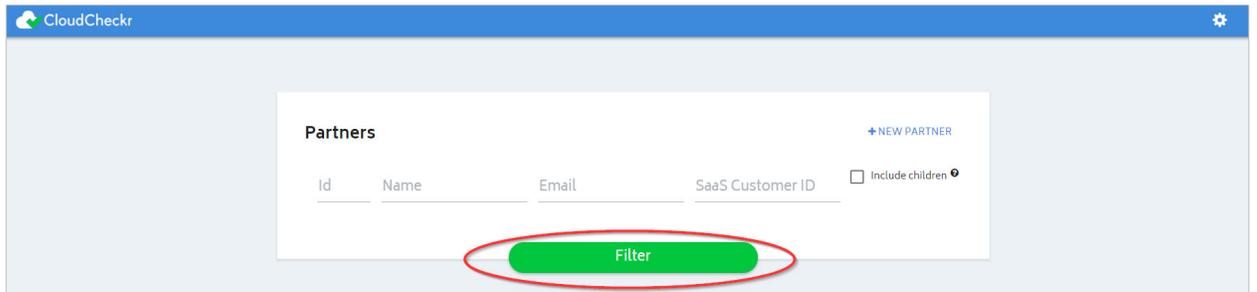
Success

Successfully added partner.

OK

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

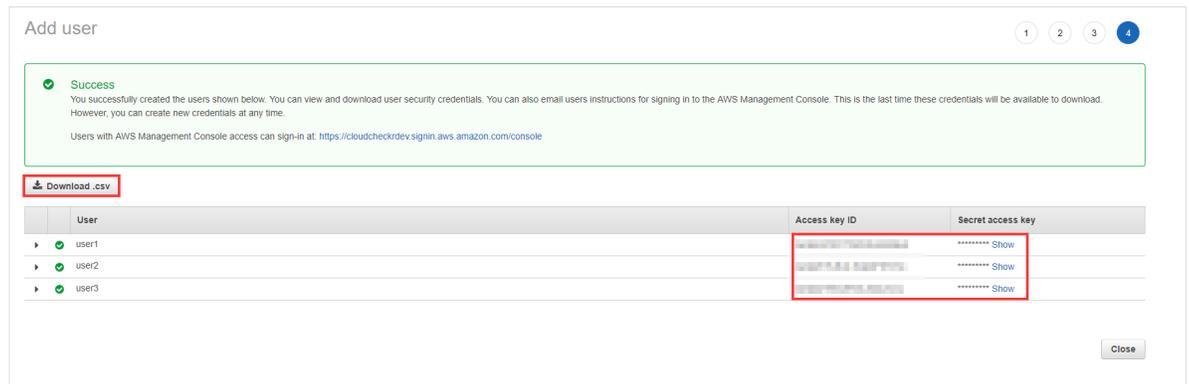
To allow the application to analyze data from AWS, you need to create AWS credentials, so the application can access your AWS account(s).

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.



The screenshot shows the 'Add user' dialog in the AWS Management Console. At the top, there are four numbered steps, with step 4 being the current one. A green success message states: 'Success. You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time. Users with AWS Management Console access can sign-in at: https://cloudcheckrdev.signin.aws.amazon.com/console'. Below the message is a 'Download .csv' button. A table lists three users: user1, user2, and user3. Each user has an 'Access key ID' and a 'Secret access key' column. The secret access keys are masked with asterisks and have a 'Show' link next to them. A 'Close' button is located at the bottom right of the dialog.

User	Access key ID	Secret access key
user1	AKIAI44QH8D8DFK1H5G5	***** Show
user2	AKIAI44QH8D8DFK1H5G5	***** Show
user3	AKIAI44QH8D8DFK1H5G5	***** Show

- 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**.

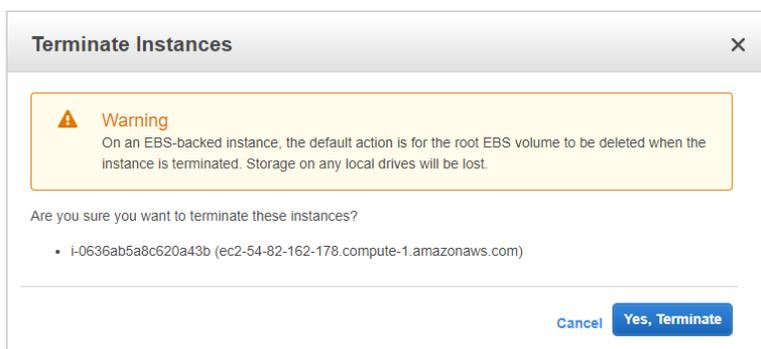
Updating the MT – Commercial Version

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.