CLOUDBASIC

# USER DEPLOYMENT GUIDE

aws partner network

Advanced
Technology
Partner

Data & Analytics
Competency

# Introductory Material

## Introduction

CLOUDBASIC, Inc. specializes in the development of enterprise cloud technology products designed to natively integrate with the leading Cloud infrastructure providers. AWS is our preferred cloud partner and the AWS Marketplace has been our main distribution channel. Underpinning the CLOUDBASIC replication products is a MS SQL Server Enterprise (High-Availability) AlwaysOn / Mirroring compatible data replication engine. This technology combines the speed and availability of the high-end MS SQL server high-availability commercial replication capabilities with the simplicity and cost effectiveness of a new generation "virtually no administration required" tools. With CLOUDBASIC, even the most complex replication scenarios can easily be configured in minutes using a simple web-based interface.

**Use Cases**

Data replication is at the core of numerous Use Case scenarios in complex enterprise environments:

- RDS Multi-AZ and Multi-AR Disaster Recovery solutions
- Multiple Load-Balanced Read Replicas
- Database Replication – OnPrem to AWS to Amazon Redshift
- No-downtime Database migrations to AWS EC2, AWS RDS and Intercloud
- Feeding of data into S3 based Data Lakes using a number of different formats
- Intercloud fail-over solutions

Public case studies for these Use Cases along with additional deployment scenarios can be found at:

https://cloudbasic.net/case-studies/

**Overview of Typical Customer Deployment on AWS**

CLOUDBASIC for AWS is typically deployed as a preconfigured AWS Marketplace AMI in a customer controlled VPC. Security is paramount for us and our customers retain complete ownership and control of all data and AWS resources used in all deployments.

Initial setup is guided by an intuitive step-by-step wizard and usually takes about 10 minutes in the most typical deployments. CLOUDBASIC verifies access and connectivity to all involved resources and database environments before commencement of any data replication processes. Detailed instructions for configuring more complex scenarios can be found in our online documentation:

https://cloudbasic.net/documentation/configure-rds-sqlserver-alwayson/

aws partner network
Advanced Technology Partner

## Prerequisites and Requirements

A CLOUDBASIC configured AWS AMI contains all of the software and configurations required to run the service. No additional clients or downloads are needed on any of the source or destination database services. Basic knowledge of AWS is needed in order to configure the required connectivity between the CLOUDBASIC instance and the involved data repositories. For complex multi-region, multi-cloud and hybrid-cloud deployments advanced level skills will be required and consulting with the CLOUDBASIC advisors is highly recommended. To use CLOUDBASIC in the most typical scenarios, customers will need:

- An Amazon Web Services account
- A source SQL Server Database – OnPrem, EC2 hosted, RDS hosted, or from a different cloud
- A destination SQL Server – OnPrem, EC2 hosted, RDS hosted, or from a different cloud
- A VPC where the CLOUDBASIC instance will be started

Depending on your specific scenario, you may need additional resources. For more information please review the following articles in our online documentation:

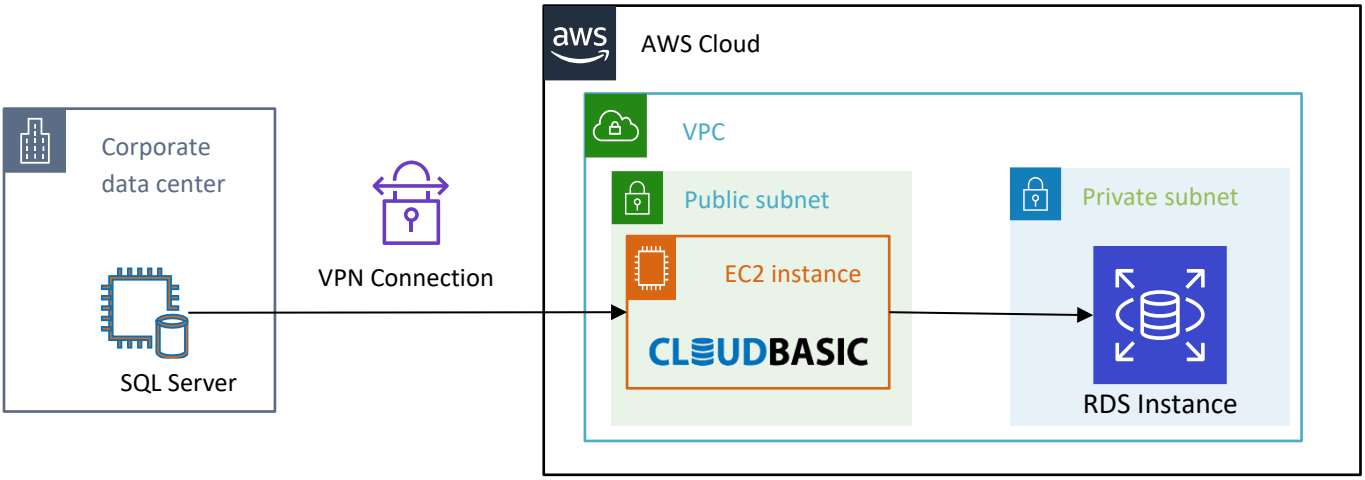
https://cloudbasic.net/documentation/configure-rds-sqlserver-alwayson/sql-server-to-redshift/

https://cloudbasic.net/documentation/configure-rds-sqlserver-alwayson/sql-server-to-s3-data-lake/

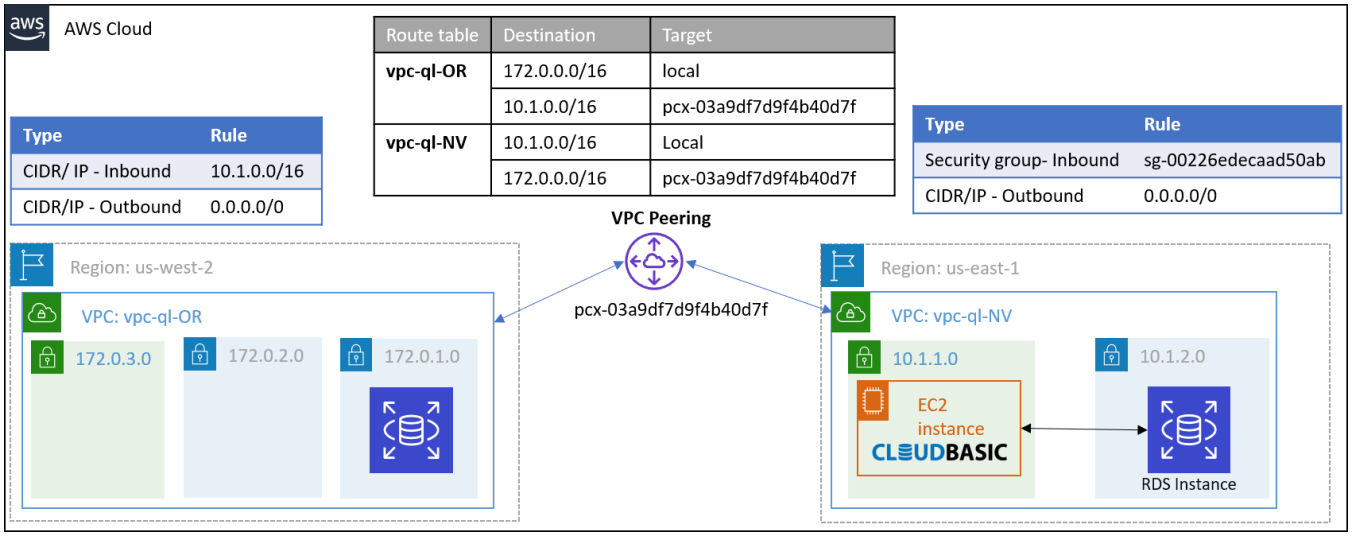
https://cloudbasic.net/documentation/configure-rds-sqlserver-alwayson/sql-server-to-redshift/

## Architecture Diagrams

CLOUDBASIC recommends that when data replication is setup, best security practices are followed and a VPN connection is used from the corporate data center to AWS. The CLOUDBASIC instance(s) is usually in the Public subnet with the Database normally in the Private subnet of a VPC.




To meet more complex Disaster Recovery or High Availability requirements CLOUDBASIC can be deployed in a cross-region architecture that utilizes VPC peering.




aws partner network
Advanced Technology Partner

# Planning Guidance

## Security

Customers retain full control and ownership of their infrastructure and are ultimately responsible for its configuration and security.

To ensure normal functioning of the CLOUDBASIC service the security group(s) assigned to the AWS instance must allow traffic on the following ports:

- TCP 1433 (or current port) when accessing MS SQL Server port
- TCP 80 (HTTP) – to access the CLOUDBASIC management console
- TCP 5439 (or current port) when accessing Amazon Redshift

In scenarios where CLOUDBASIC is configured to write to S3, access can be controlled by either providing an IAM Role or a pair of Access Key/ Secret Access Key. Please note that the recommended best security practice is to use an IAM Role.

Depending on the Replication scenario the required permissions will fall in these basic groups:

**SQL Server - to – SQL Server**

ses:SendEmail
ses:SendRawEmail

**SQL Server - to – S3 Data Lake**

ses:SendEmail
ses:SendRawEmail
s3:PutObject
s3:ListAllMyBuckets
s3:DeleteObjectVersion
s3:ListBucket
s3:DeleteObject
s3:HeadBucket

**SQL Server - to – Amazon Redshift**

ses:SendEmail
ses:SendRawEmail
s3:PutObject
s3:DeleteObjectVersion
s3:DeleteObject
s3:HeadBucket

s3:Get*
s3:List*

These default setting should be carefully reviewed before launching a CLOUDBASIC instance and can be modified using any AWS or third party provided tools.

Access to your CLOUDBASIC administrative console is through a webpage which is configured to respond on port 80 of your instance. Initially there is a single user configured with a default name of "admin" and a password of the actual EC2 Instance ID. As part of the initial login and instance verification you will be required to change this default password.

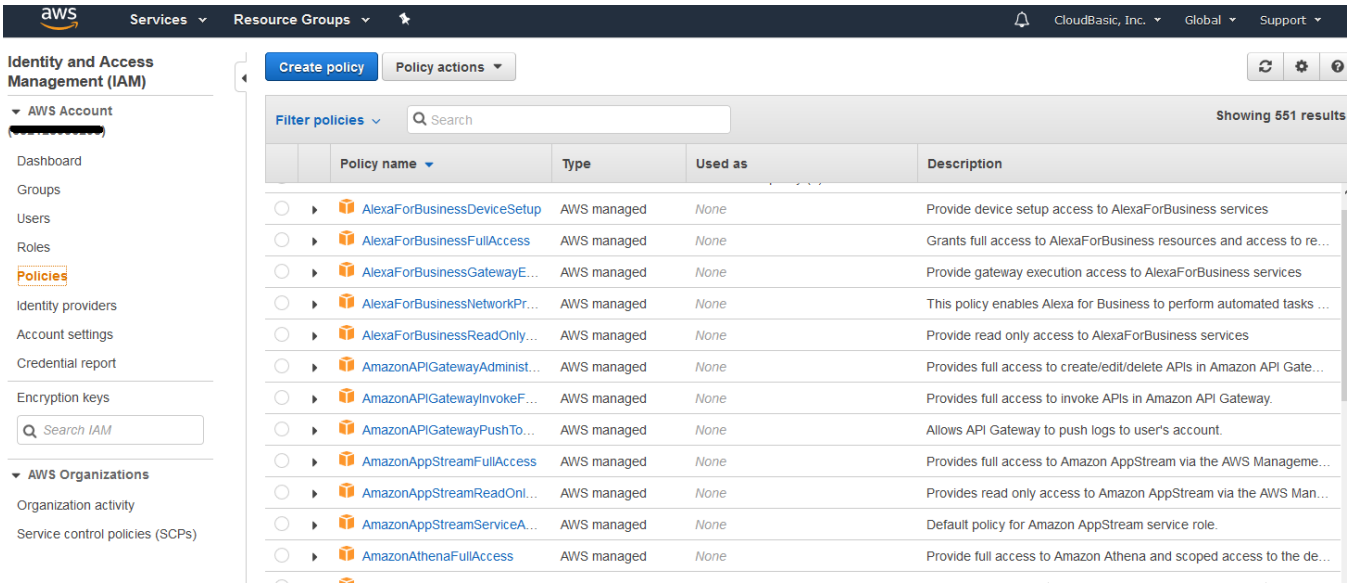
## Resource tagging

To simplify tracking of resources you can implement a tagging strategy that helps you better catalog your resources and the entities within your organization that are using them. Throughout this guide we will show several examples of resource tagging.

## Step-by-step IAM Role creation

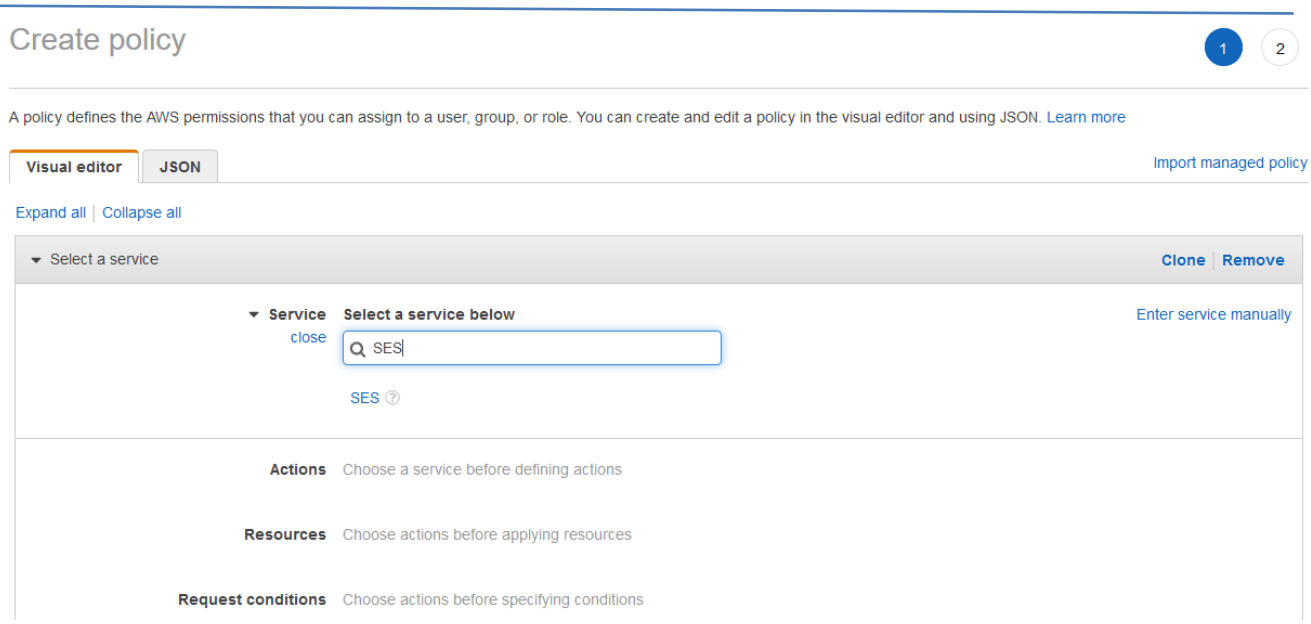
This sequence illustrates how to create and IAM Role that is needed in the SQL Server-to-Amazon Redshift scenario. We will create a custom policy to grant a very limited access to the SES service and will then create a role that will use this new policy along with the standard policy AmazonS3ReadOnlyAccess.

1. In your AWS console navigate to the IAM Service, open the Polices section in the left menu and click on the "Create policy" button

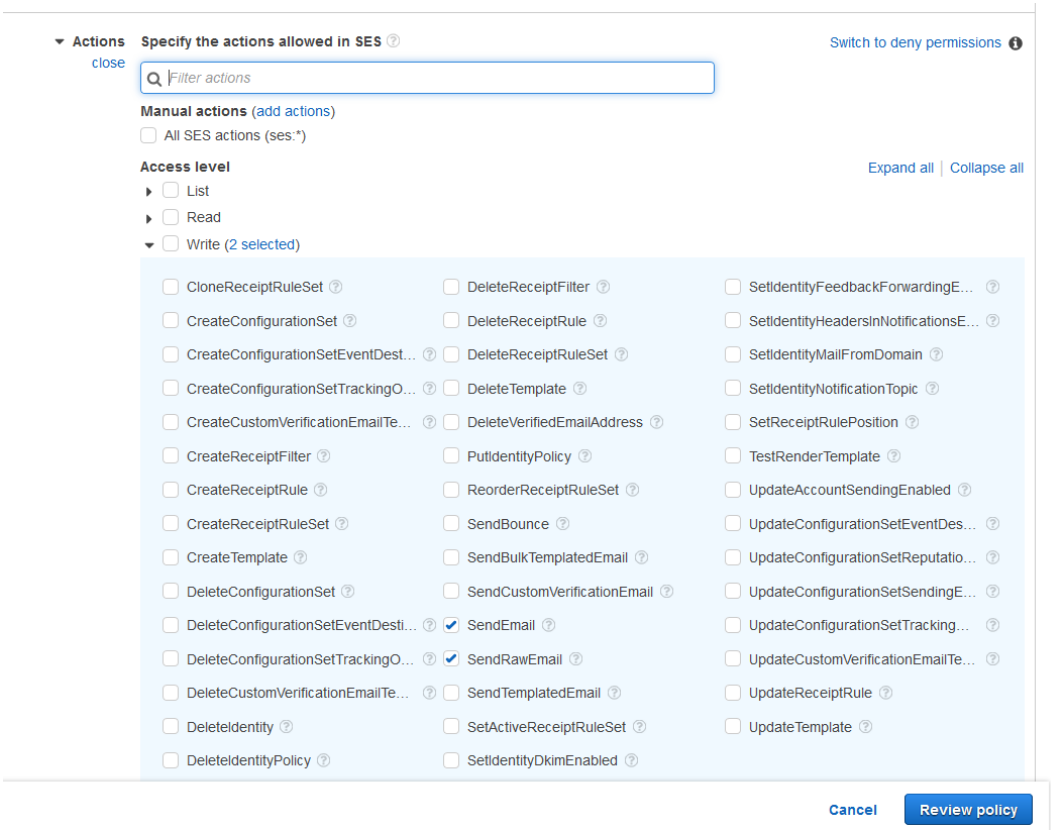



2. In the "Create Policy" dialog select the "Visual editor" tab and expand the Service dropdown. Type "SES" in the search field and select the SES Service.

aws partner network
Advanced Technology Partner

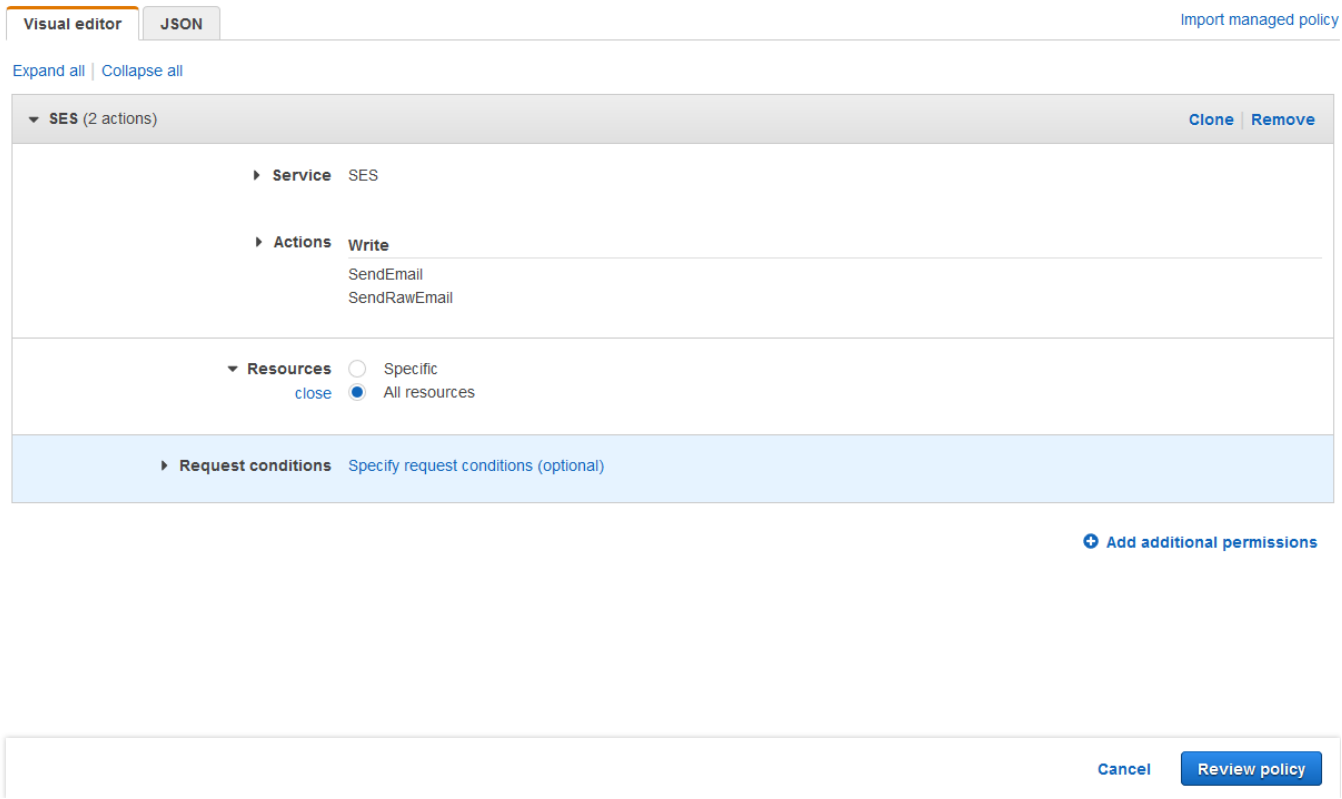



3. Under "Access level" expand the "Write" section and select the permissions
    a. "SendEmail"
    b. "SendRawEmail"

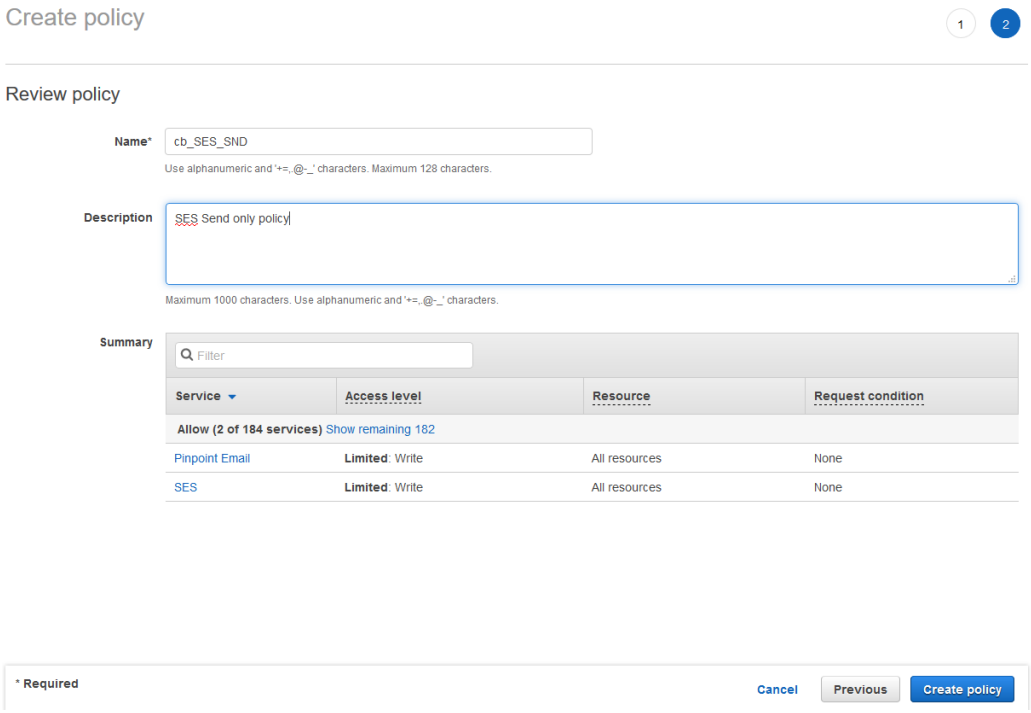



aws partner network
Advanced Technology Partner

4. Expand the "Resources" section, click on "All Resources" and then click on the "Review policy" button

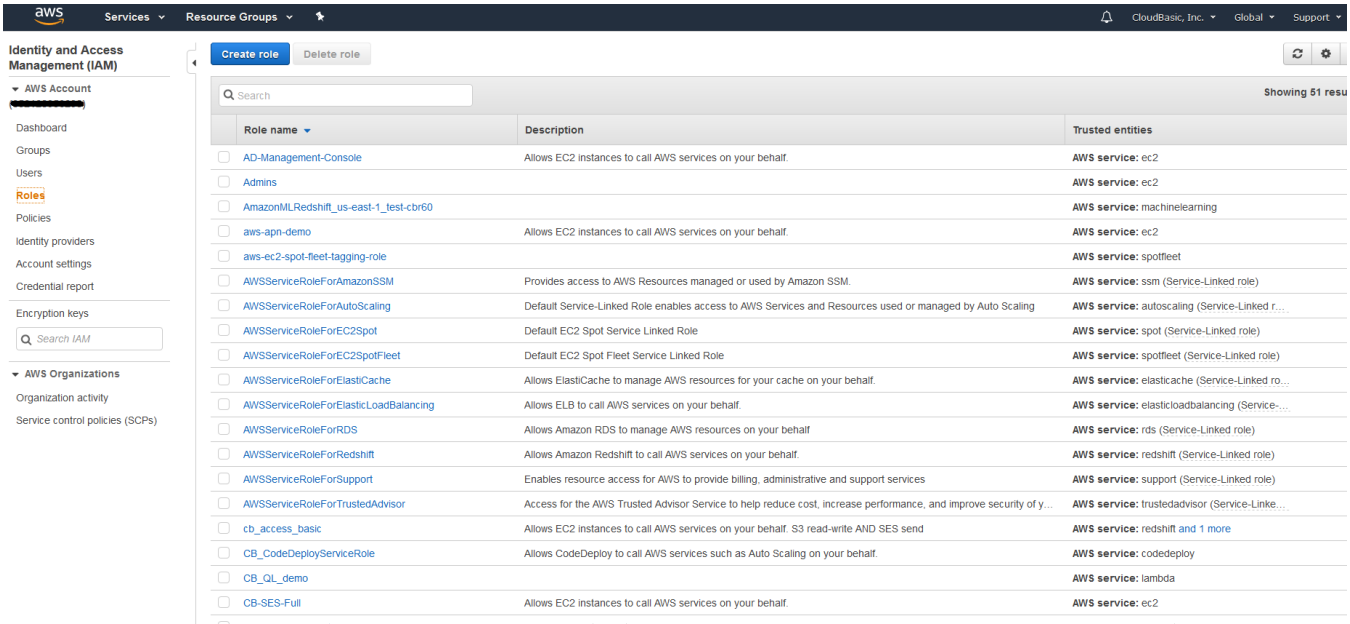



5. Enter a Name and a Description and click the "Create policy" button

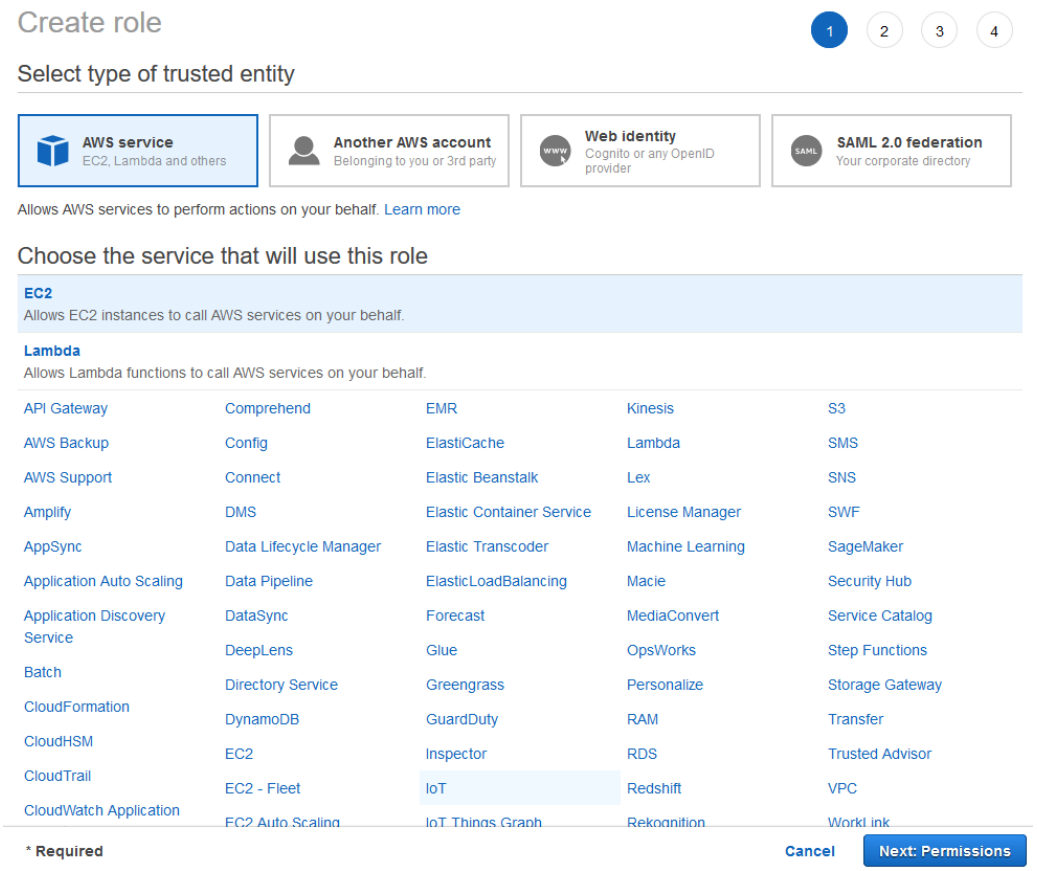



aws partner network
Advanced Technology Partner

6. Next, select the "Roles" option in the menu on the left and click on the "Create role" button.

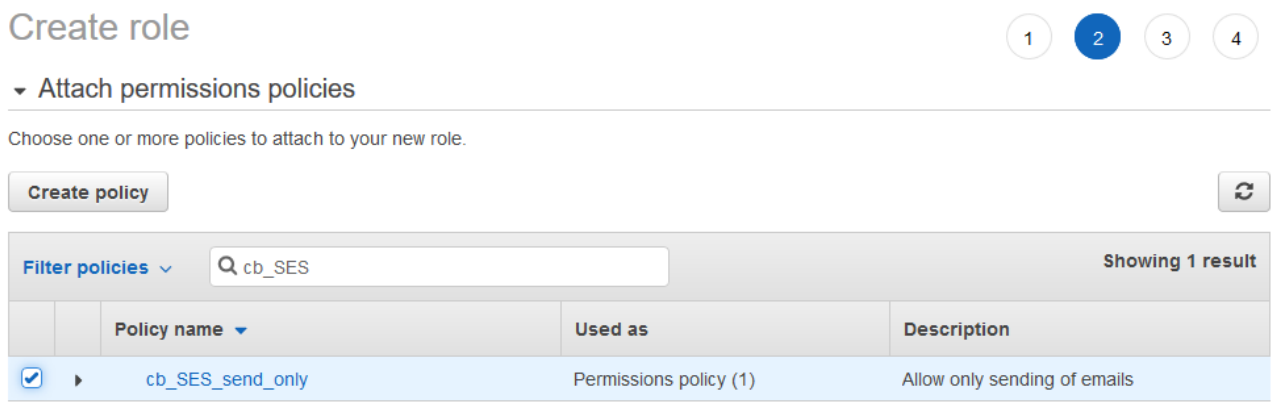



7. In the "Create role" dialog, select the "AWS service" option under "Select type of trusted entity", then select "EC2" under "Choose the service that will use this role" and click the "Next: Permissions" button.

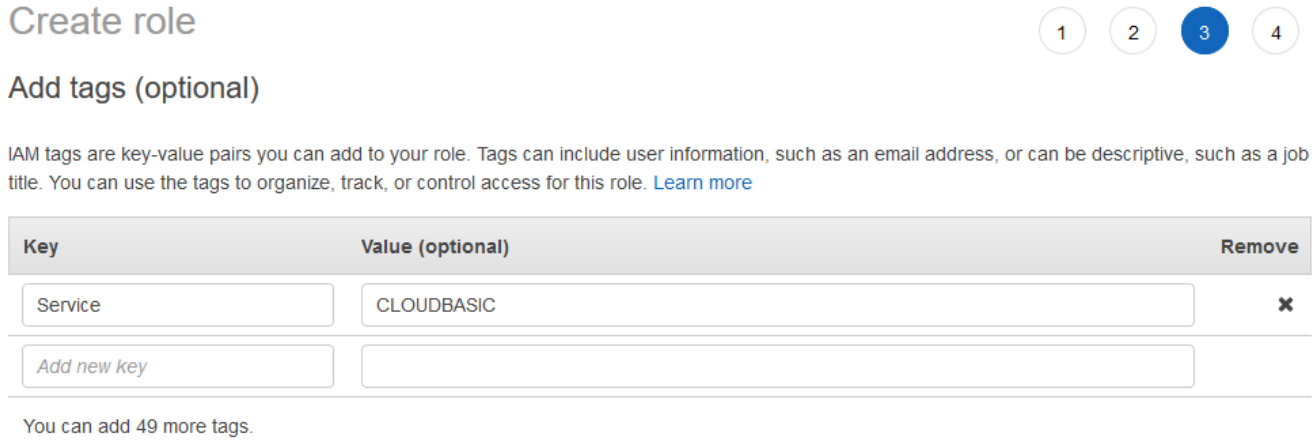



aws partner network
Advanced Technology Partner

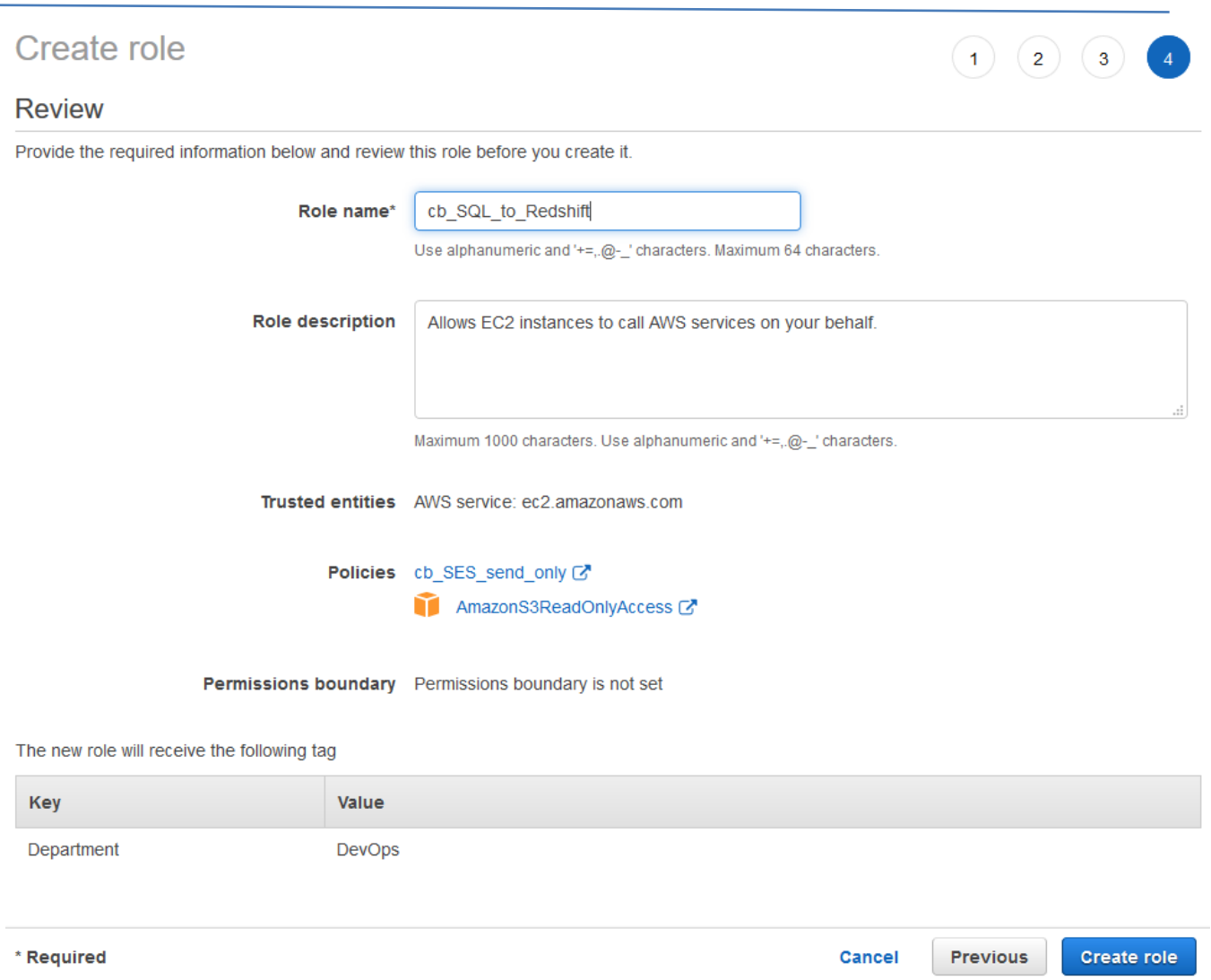
8. In the "Attach permissions policies" section find and select the policy you created




9. Repeat for the standard policy "AmazonS3ReadOnlyAccess" and click the "Next: Tags" button
10. Decide if you want to tag your new role and click the "Next: Review" button



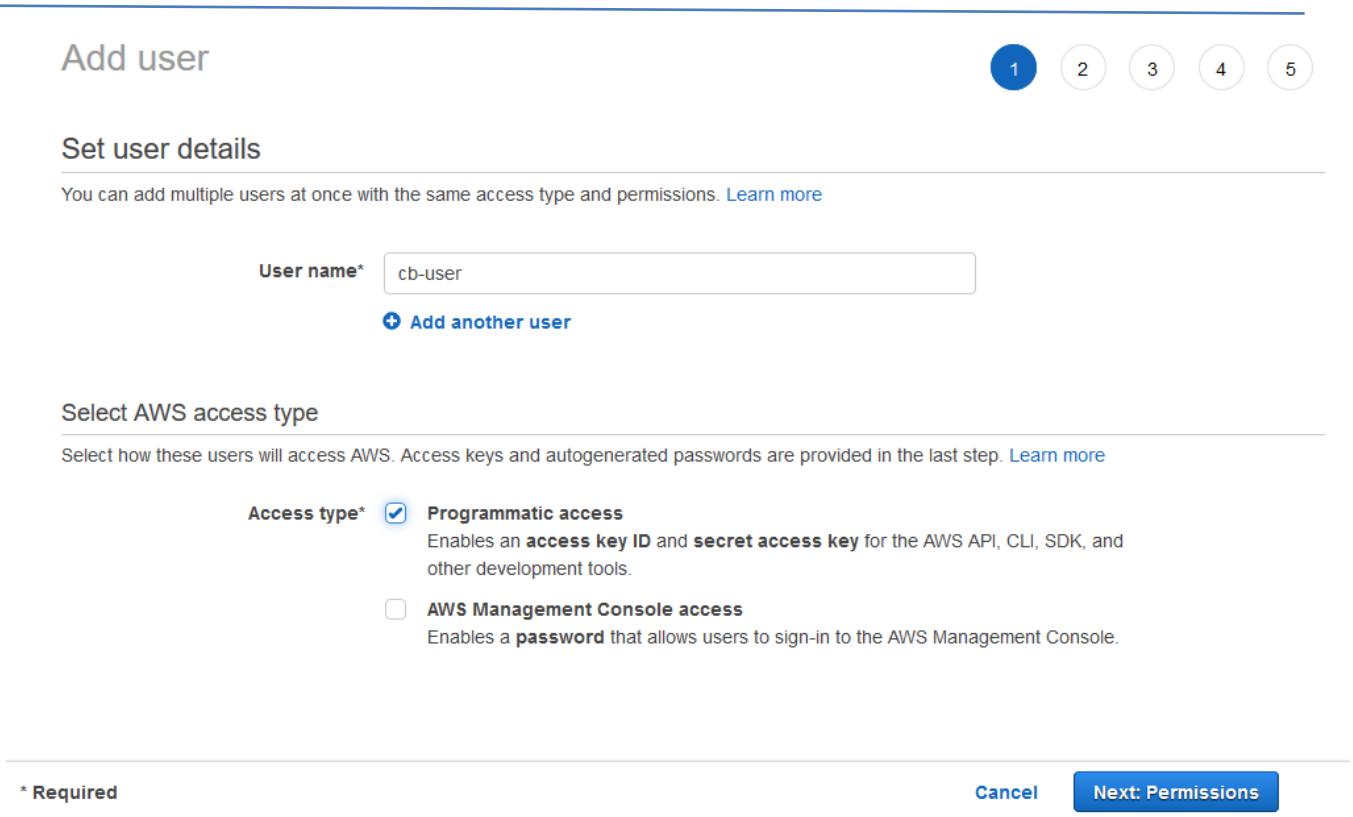

11. In the "Review" section give your Role a name and click the "Create role" button



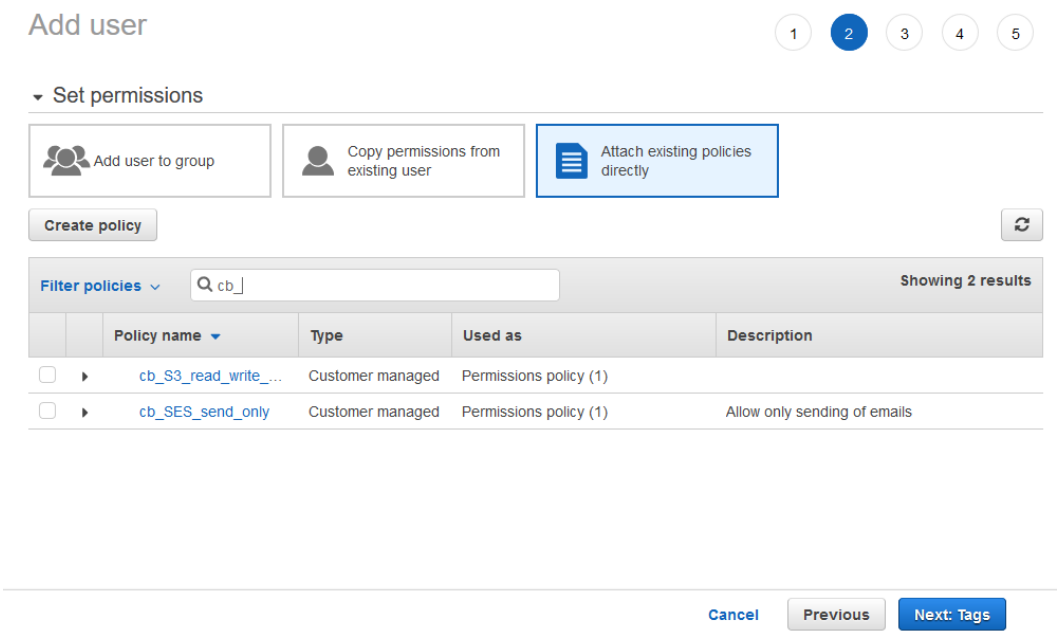

## Step-by-step access Key/ Secret creation

If your security requirements dictate that you must use an access Key/ Secret to access AWS resources the following steps will help you create and configure necessary elements.

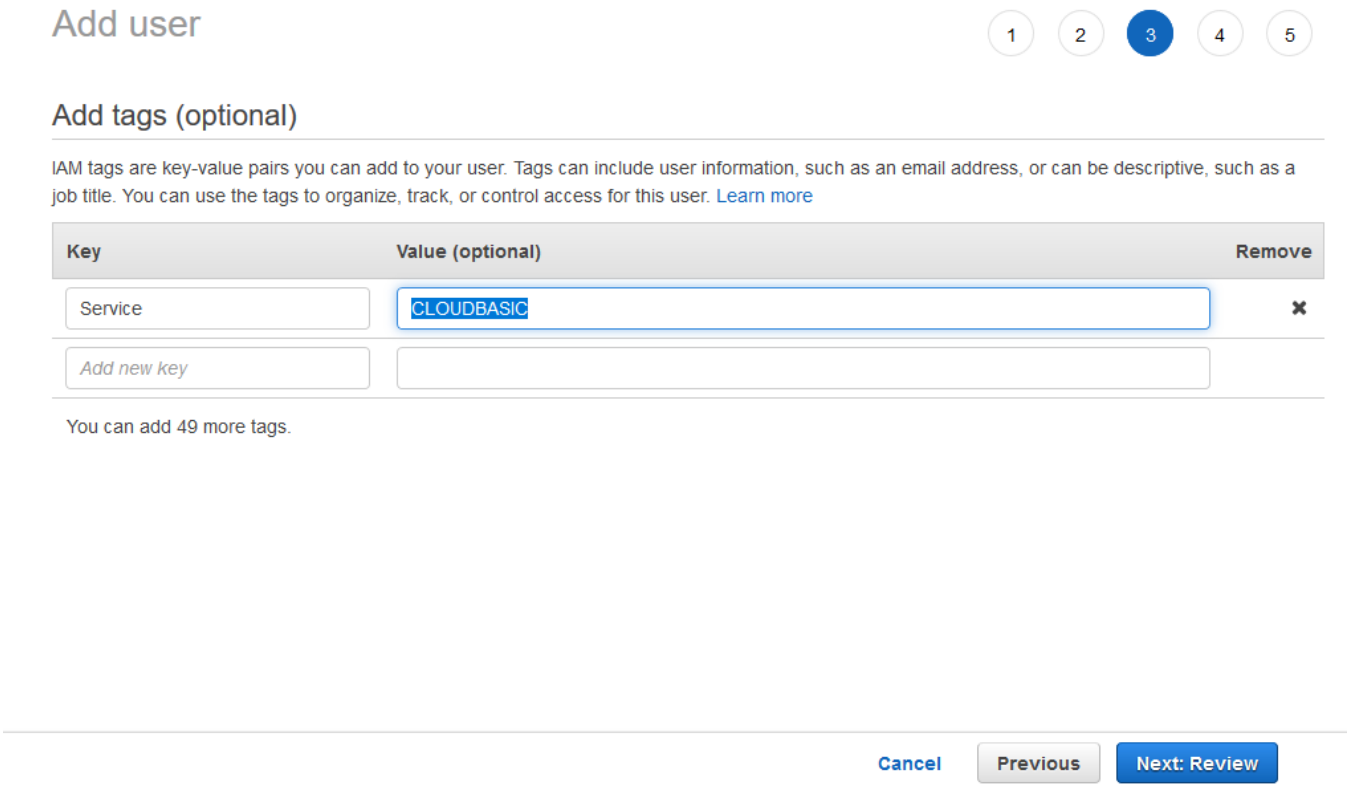
1. In your AWS console navigate to the IAM Service, open the Users section in the left menu and click on the "Create user" button. Enter the "User name", select the "Programmatic access" option and click the "Next: Permissions" button



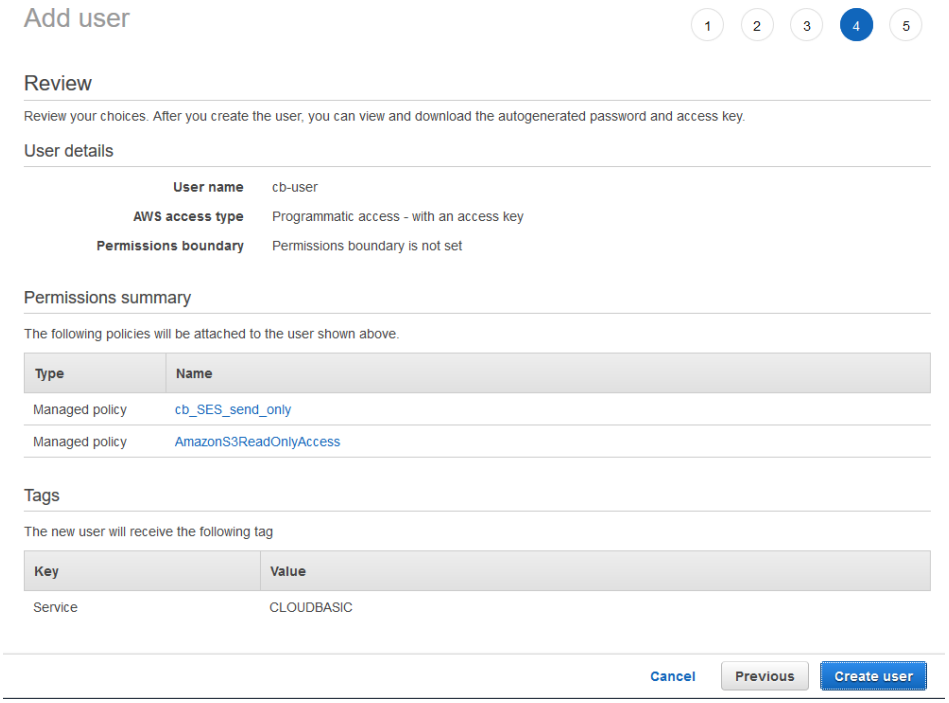

2. Click on the "Attach existing policies directly" button, select the applicable policies (for more details see the section "Step-by-step IAM Role creation") and



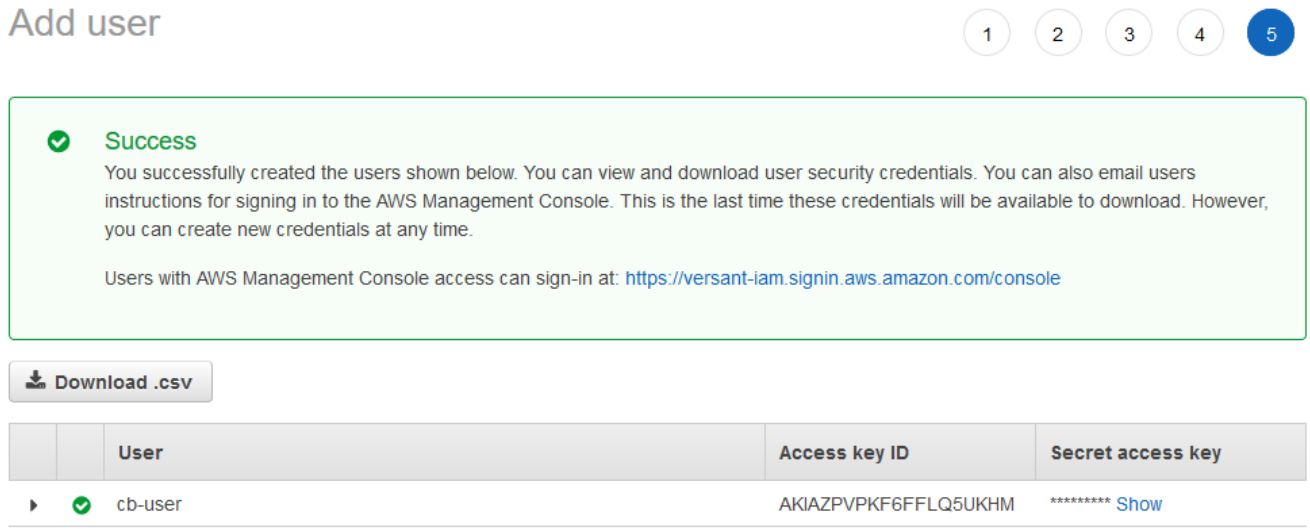
3. (Optional) Assign a tag to this user for better AWS resource tracking and click the "Next: Review" button




4. Click the "Create user" button



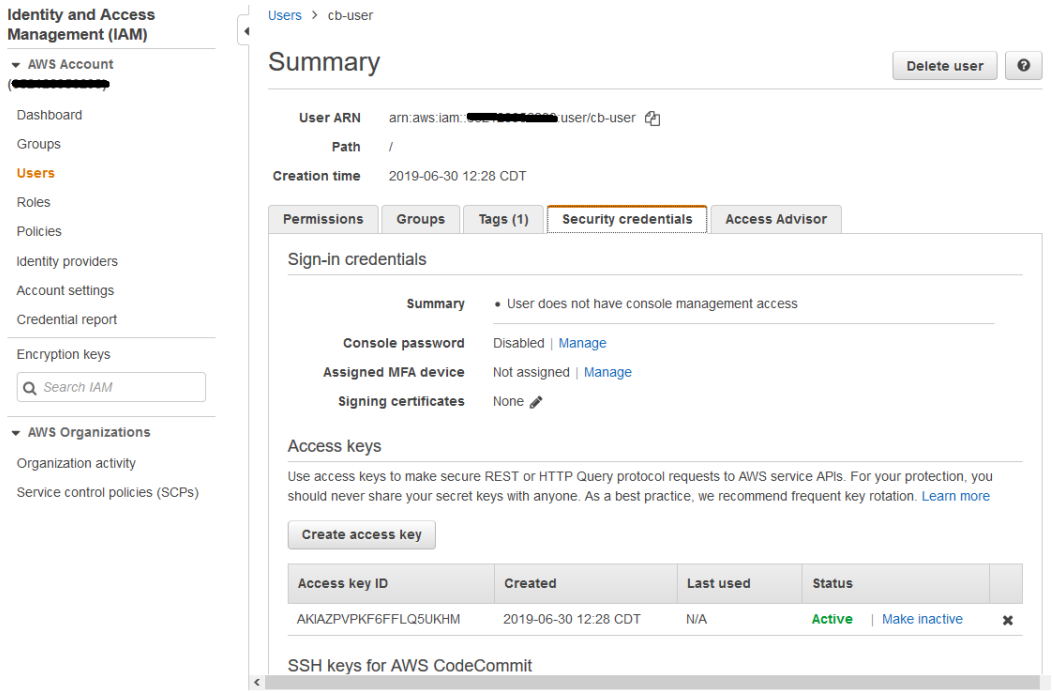
5. Click on the "Download .csv" button to download the access Key and Secret for the new user.




## Rotating access Key/ Secret

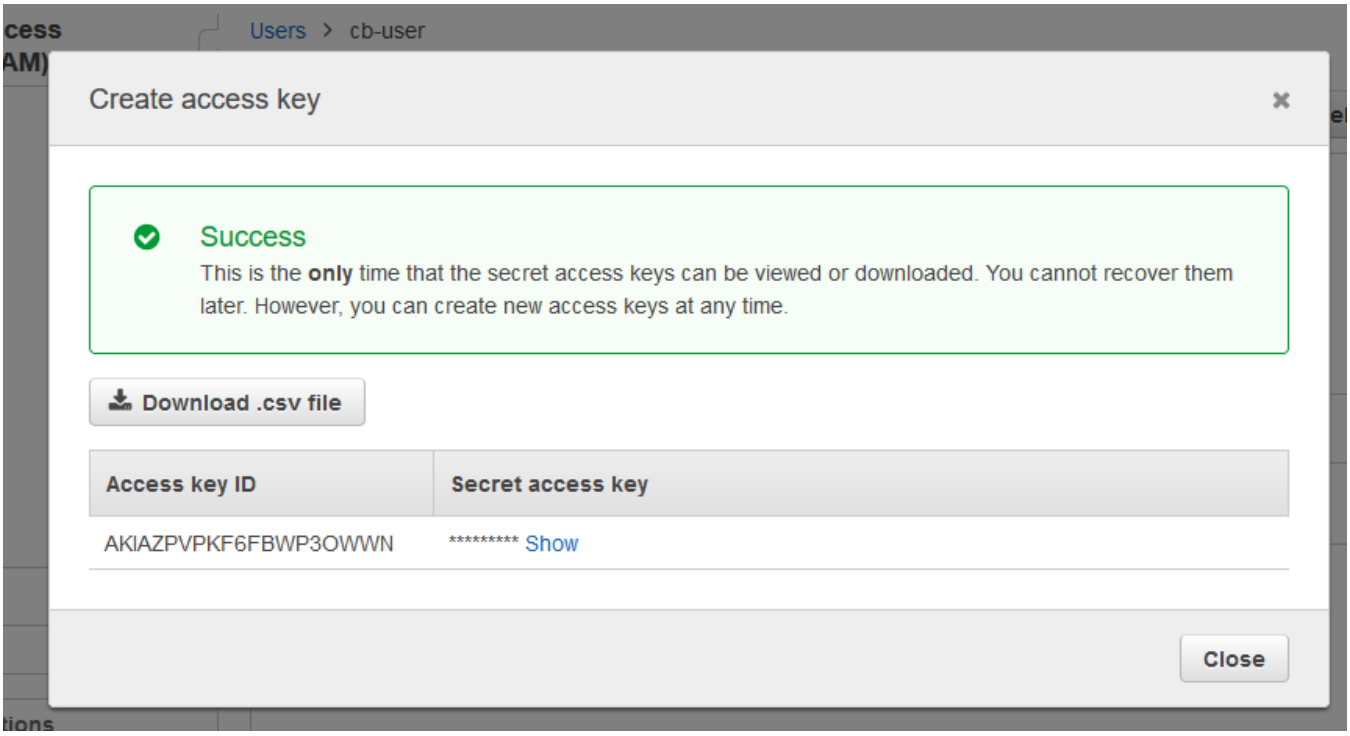
It is a best security practice to regularly change the access Key/ Secret pair if your CLOUDBASIC replications are configured to use them.

1. In your AWS console navigate to the IAM Service, open the Users section in the left menu, find and click on "User name" of the user you are using in your CLOUDBASIC installation

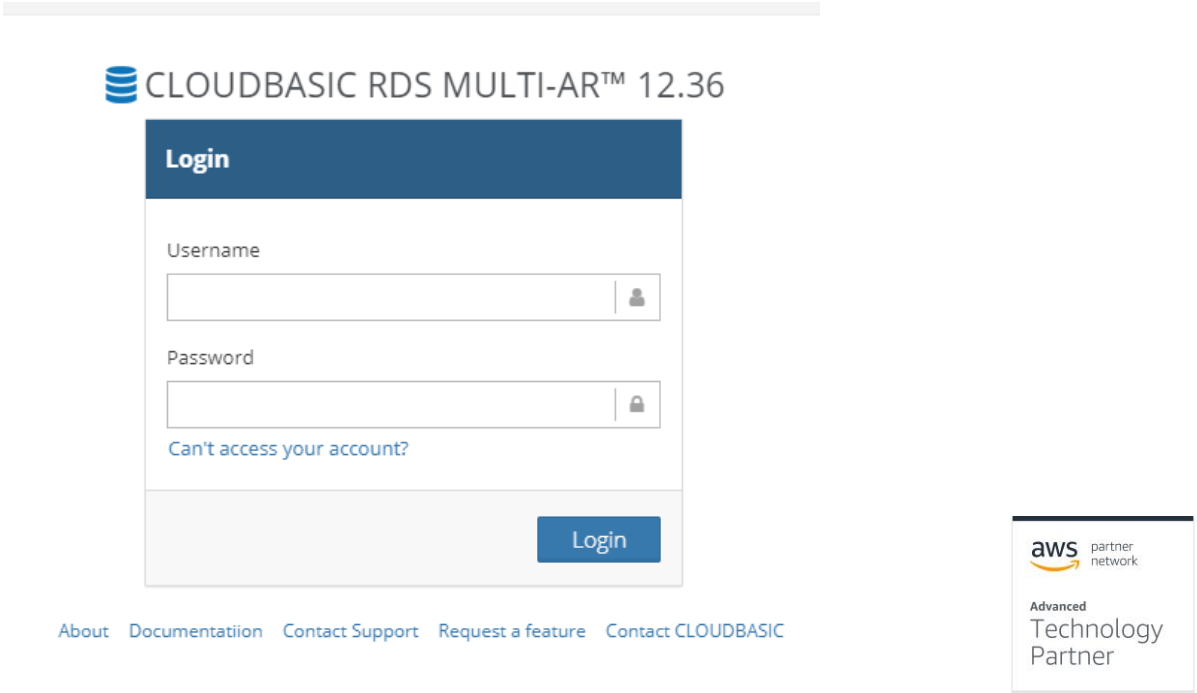



2. Open the "Security credentials" tab and click on the "Create access key" button

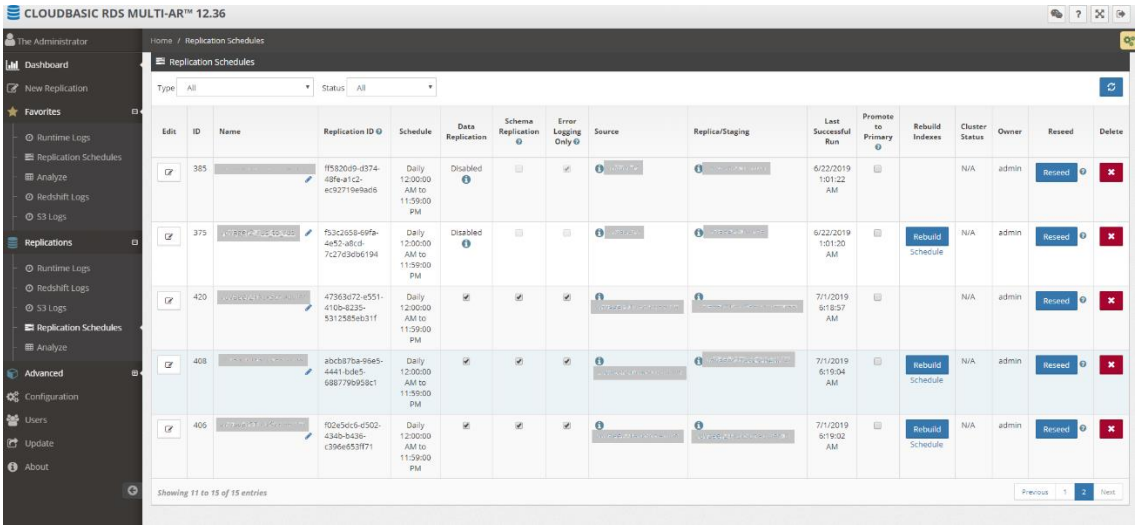
3. Click on the "Download .csv" button to save the new access Key/ Secret




4. Click on the "Make inactive" link to Inactivate the old access Key/ Secret pair. After making sure that no applications are using the old Key/ Secret pair you can delete it.
5. To rotate the access Key/ Secret in your CLOUDBASIC configuration
    a. Navigate to your CLOUDBASIC management console and log in using an administrator level credentials

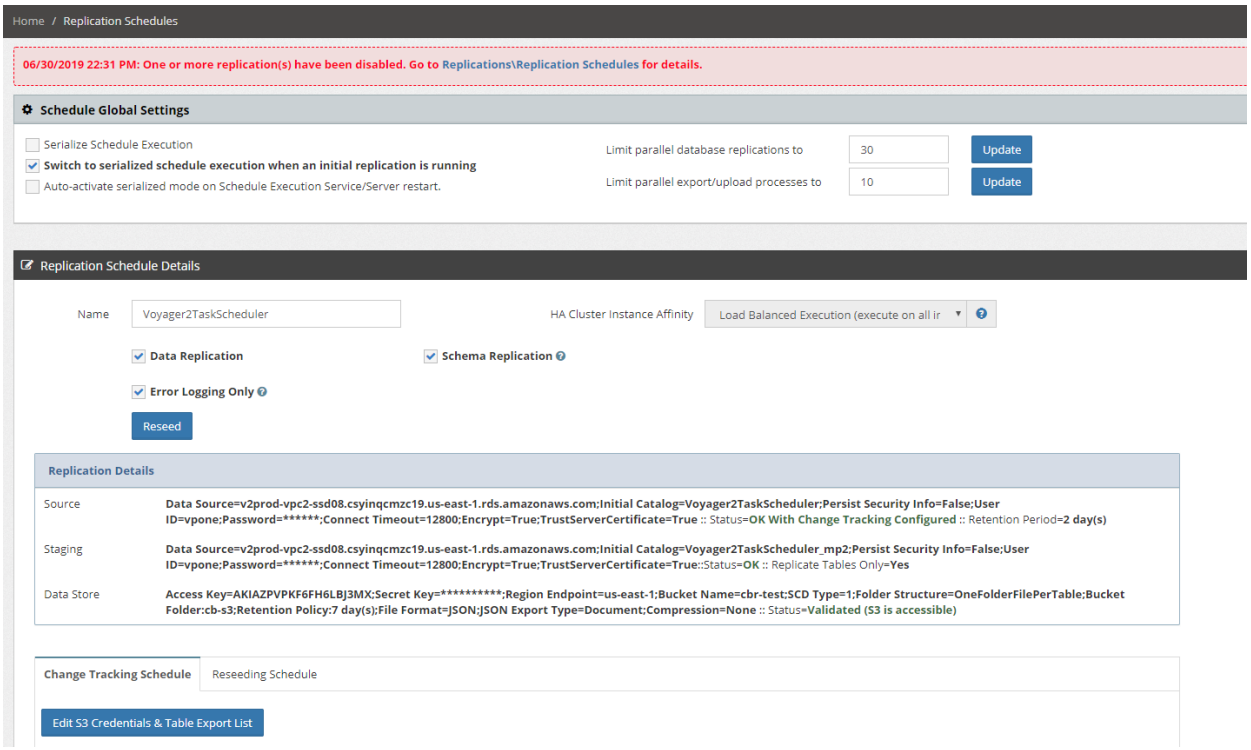


b. In the left-hand menu navigate to "Replications" and open the "Replication Schedules" menu



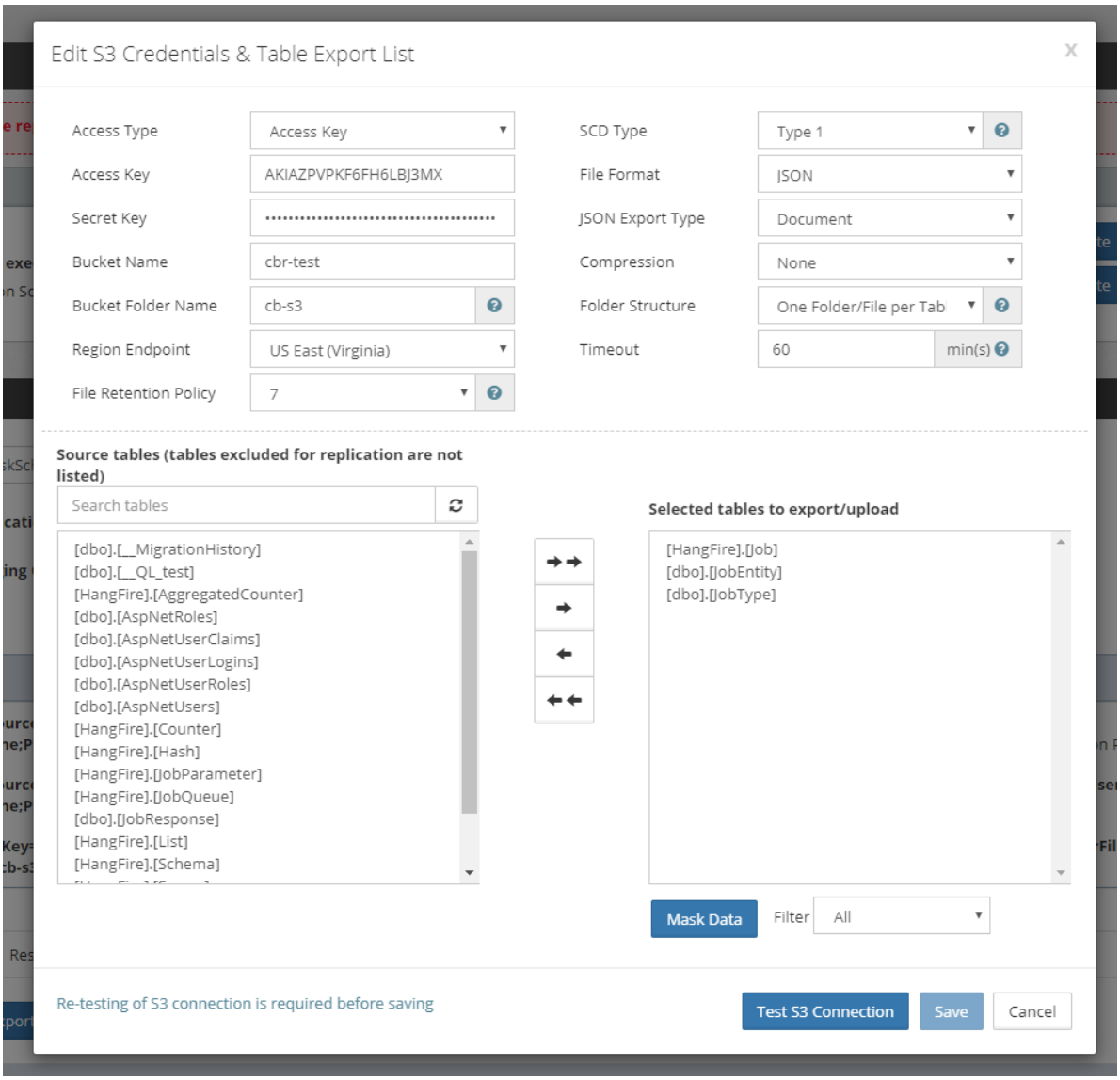

c. Find your replication in the list and click on the "Edit" button.

d. In the next dialog, click the "Edit S3 Credentials & Table Export List" button




aws partner network
Advanced Technology Partner

e. Update the access Key/ Secret, click the "Test S3 connection" button and then click on "Save"




f. Repeat the same steps for any other Replication schedules that use the S3 service

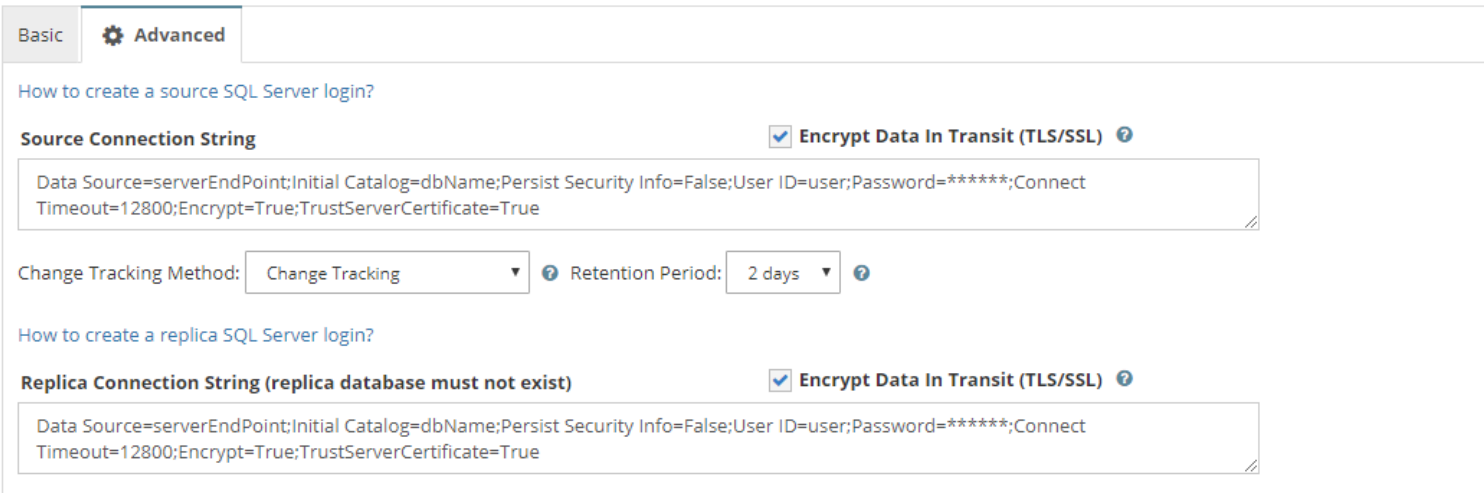
## Encryption

VPN is recommended for cross-region replications but is not mandatory. Replications can be configured with data-in-transit encryption leveraging SQL Server level TLS/SSL encryption. For connections to SQL Server 2016 and above, TLS 1.2 is activated. For connections to SQL Server 2014 and below, TLS 1.1/1.0 or SSL is activated depending on the SQL Server version and applied updates. For more information see https://support.microsoft.com/en-us/help/3135244/tls-1-2-support-for-microsoft-sql-server

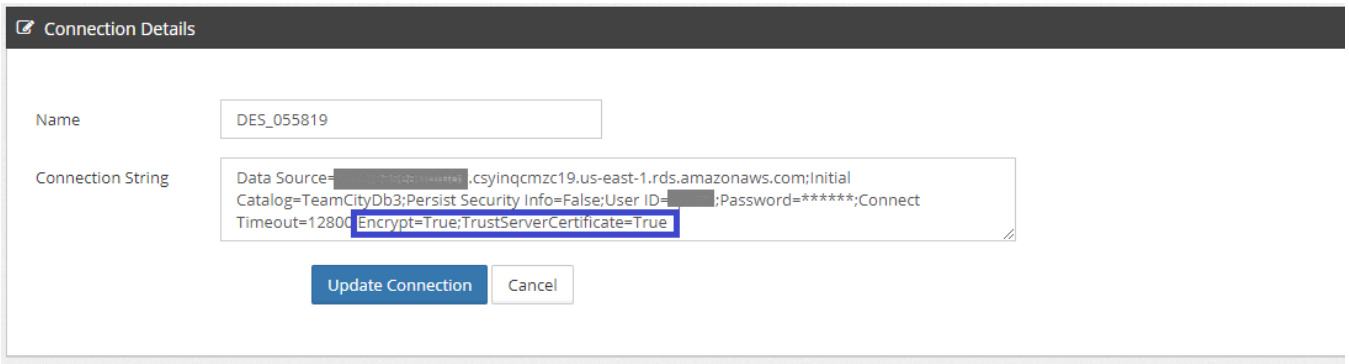
In CLOUDBASIC 10.0 and above all connections are encrypted by default. In CLOUDBASIC versions 9.11 and below, during configuration of a replication, go to

Quick Setup, in the [Advanced Tab] select "Encrypt Data In Transit" for either the source, target or both connections.

For increased security, you may select to encrypt data in transit even if the CLOUDBASIC instance, source and target SQL Servers are deployed within same VPC. Data in transit encryption introduces a negligible computational overhead.




If a replication was initially configured without activating encryption, then to activate data in transit encryption, go to Advanced/Connection Strings, locate the respective source and/or target link, add "Encrypt=True;TrustServerCertificate=True".




## Cluster communication encryption

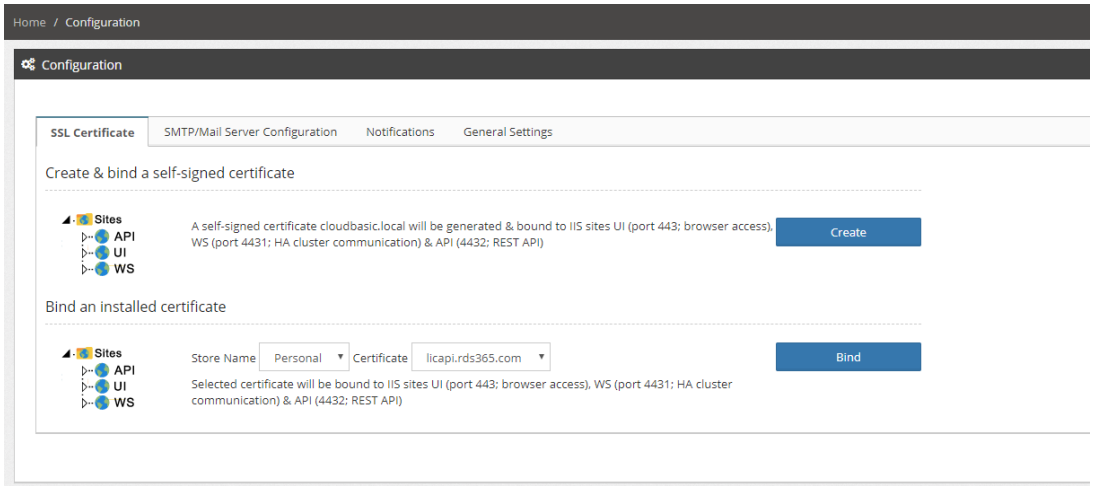
CLOUDBASIC RDS AlwaysOn/Geo-Replicate for SQL Server HA/DR version 8.0 and above features encrypted communication between Multi-AZ High-Availability Cluster instance members. HTTPS/TLS 1.2 communication is handled over port 4431 (444 in versions 8 and 9; 4431 in version 10 and above).

Product version 10.0 and above

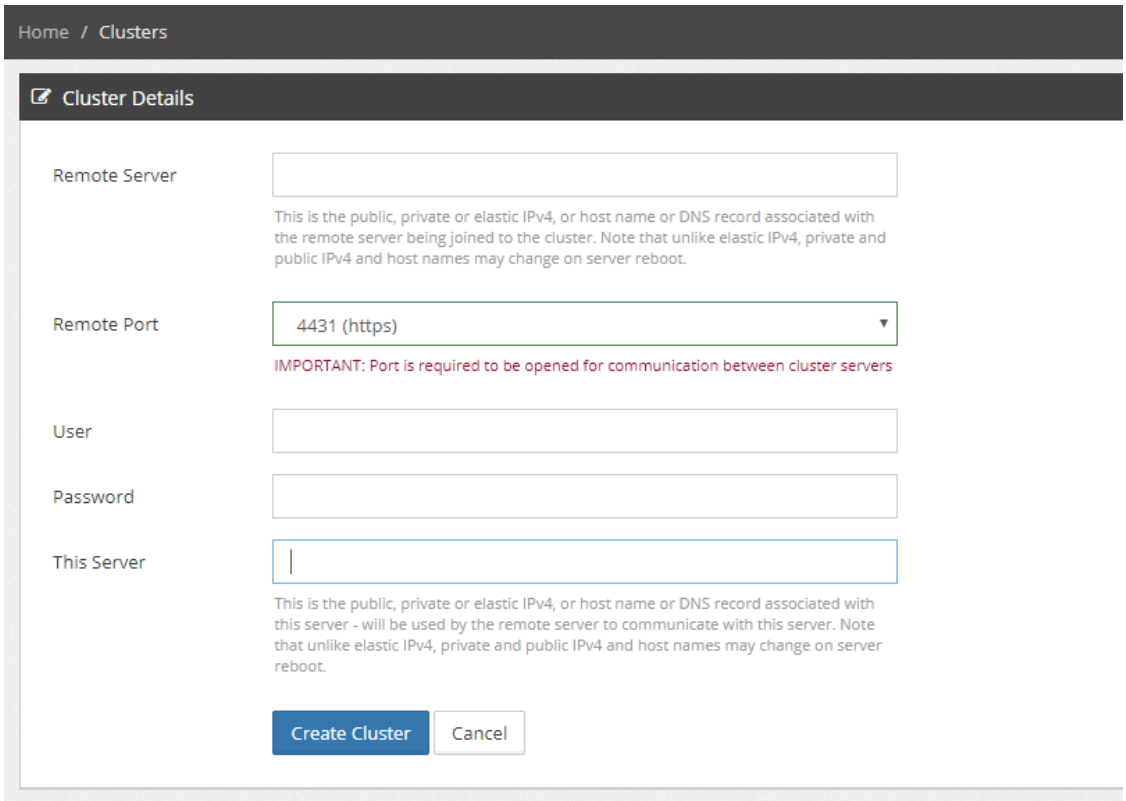
If securing Multi-AZ HA Cluster instances communication (port 4432) suffices (i.e. in test environment), a self-signed certificate can be generated and bound to the respective web server site WS (port 4431) with a click-of-a-button. Go to

/Configuration, in the top section "SSL Certificate", click [Create]. Note that the same self-signed certificate cloudbasic.local will be bound to sites UI (port 443; browser console access) and API (port 4432; REST API) as well.

To install and bind a CA issued production certificate, RDP (remote desktop) to the CLOUDBASIC Windows server, install the certificate into the Certificate Storage (default storage is [Personal]). Then go to /Configuration and click [Bind]. Note that the same certificate will be bound to sites UI (port 443; browser console access) and API (port 4432; REST API) as well.




Under /Advnaced/Multi-AZ HA Cluster, select port 4431 (https) to activate cluster instance members communication over https TLS 1.2:




For instructions on how to configure cluster communication encryption in earlier versions, please see our online documentation at [https://cloudbasic.net/documentation/encrypting-ha-cluster-communication/](https://cloudbasic.net/documentation/encrypting-ha-cluster-communication/) .

## Costs

CLOUDBASIC is available in two subscription options in the AWS Marketplace – an Annual subscription or an Hourly subscription. Prices depend on the AWS Region, the size of the selected instance and the length of the subscription. Here is an example of our current prices for the US East (N. Virginia) region:

| CLOUDBASIC Hourly Subscription Costs | | | |
|---|---|---|---|
| EC2 Instance Type | Software/ hr | EC2/ hr | Total/ hr |
| t2.medium | $1.37 | $0.064 | $1.434 |
| m4.large (*vendor recommended) | $2.74 | $0.192 | $2.932 |
| m4.xlarge | $5.48 | $0.384 | $5.864 |
| M4.2xlarge | $5.48 | $0.768 | $6.248 |

aws partner network
Advanced
Technology
Partner

| CLOUDBASIC Annual Subscription Costs | | | |
|---|---|---|---|
| EC2 Instance Type | Software/ hr | EC2/ hr | Percent Savings (%) |
| t2.medium | $9,950.00 | $0.064 | 17% |
| m4.large (*vendor recommended) | $19,950.00 | $0.192 | 17% |
| m4.xlarge | $39,950.00 | $0.384 | 17% |
| M4.2xlarge | $39,950.00 | $0.768 | 17% |

For the latest pricing and discounts, please see our AWS Marketplace listing https://aws.amazon.com/marketplace/pp/B00OU0PE5M?qid=1560792424876&sr=0-1&ref_=srh_res_product_title#pdp-pricing.

Depending on your CLOUDBASIC deployment scenario AWS costs will include:

- CLOUDBASIC fees based on selected instance type
- AWS EC2 usage charges
- EBS fees for the storage used by the CLOUDBASIC instance(s)
- S3 fees for any S3 storage used by the deployment
- Redshift usage charges when Redshift is used
- IOPS fees for any EBS or S3 storage configured with IOPS
- Data transfer fees

### Sizing

CLOUDBASIC recommends that you use at least an m4.large class instance. Please note that due to the variety of business needs, instance size is best determined during a POC when latency requirements, volume of changes, number of databases and the need for an HA cluster or a stand-alone service can be properly assessed.

## Deployment Guidance

### Deployment Assets

The CLOUDBASIC deployment is very easy and, in the most common scenario, consists of launching a single EC2 instance from the AWS Marketplace. For more complex scenarios we strongly recommend executing a joint POC, which is free to new potential customers. Please ensure that you have all Prerequisites described earlier in this guide.

1. Find the CLOUDBASIC listing in the AWS Marketplace

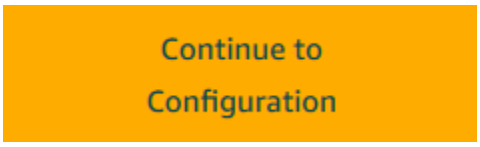
   https://aws.amazon.com/marketplace/pp/B00OU0PE5M?qid=1560819052154&sr=0-1&ref_=srh_res_product_title

2. Click on the button

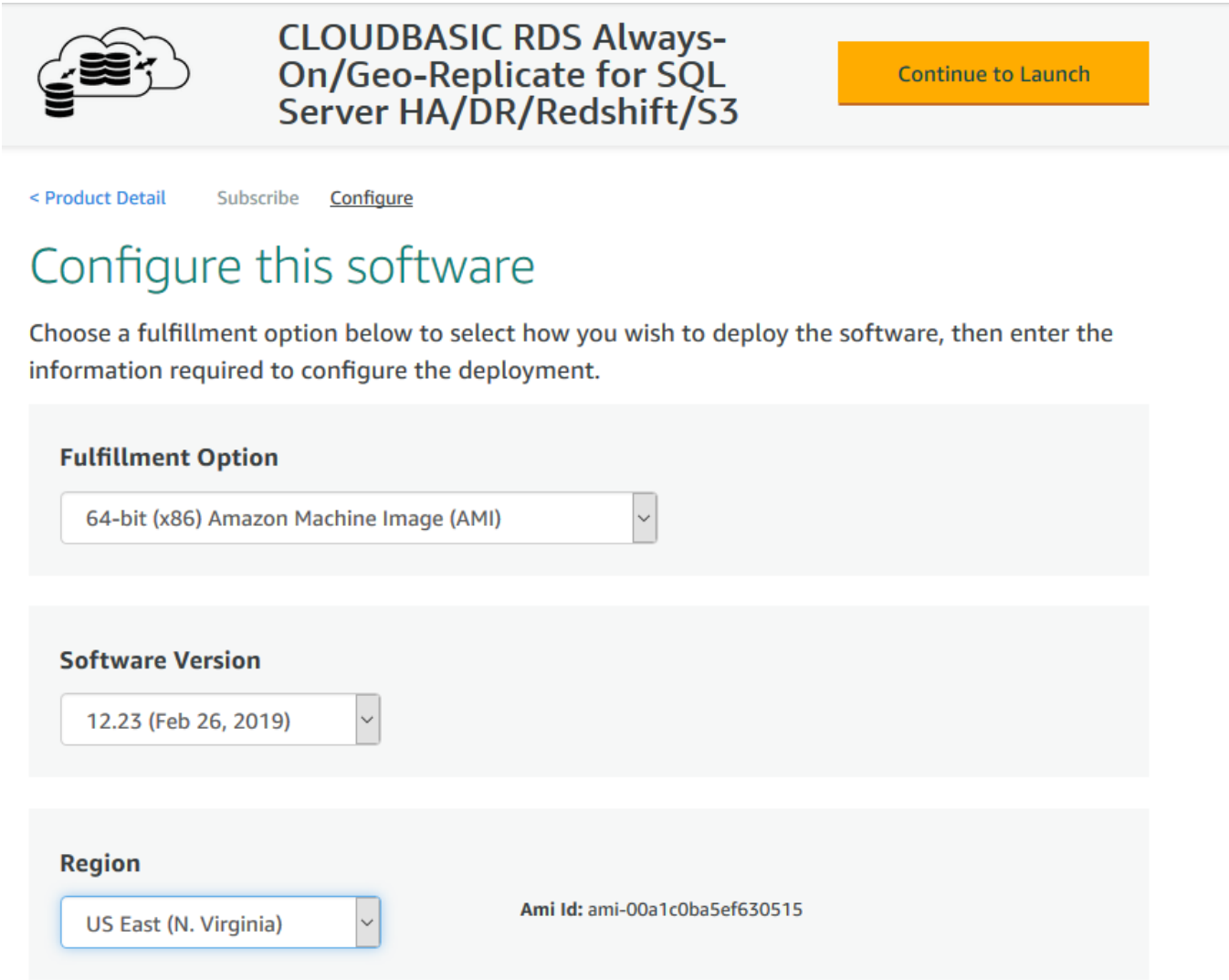
   Continue to Subscribe

aws partner network
Advanced
Technology
Partner

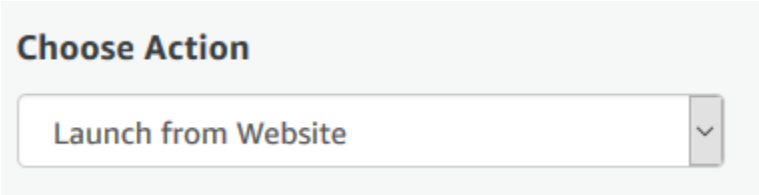
3. Decide if Annual Subscription is more appropriate for your case or you prefer the Hourly billing
4. Click on the button Continue to Configuration



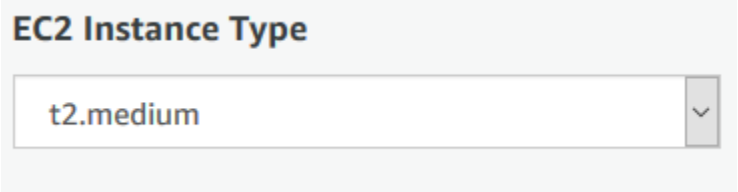

5. Verify the AWS Region where you plan to launch your CLOUDBASIC instance and click the Continue to Launch button



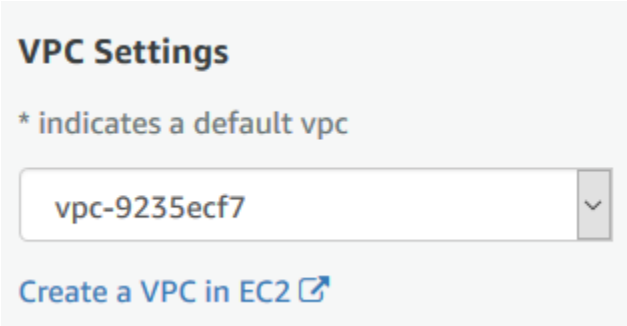

6. In the "Launch this software" section:
   a. Select the Launch from Website option

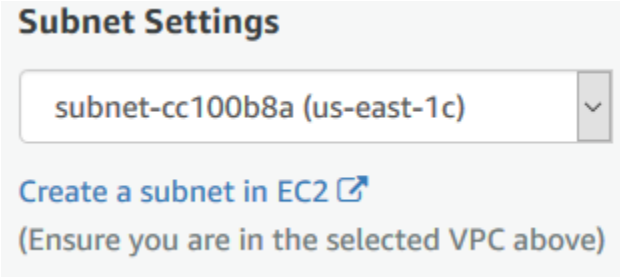



b. Select the EC2 Instance Type that best suits your needs

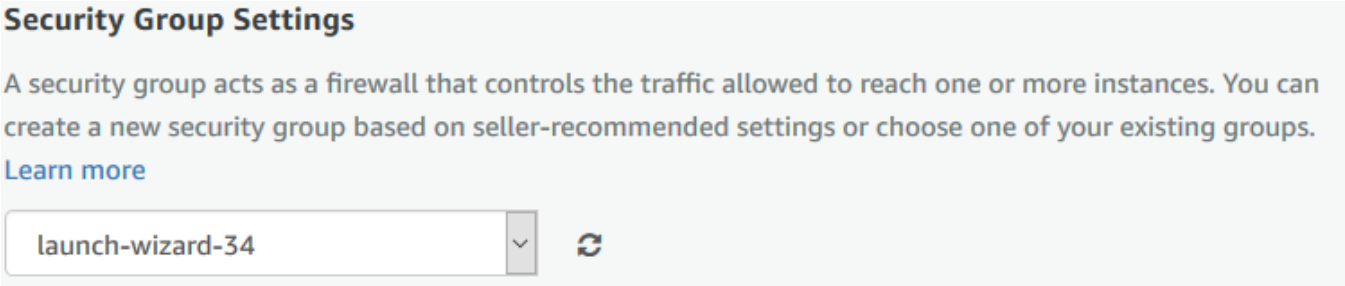



c. Select the VPC and Subnet where the CLOUDBASIC instance is to be launched.

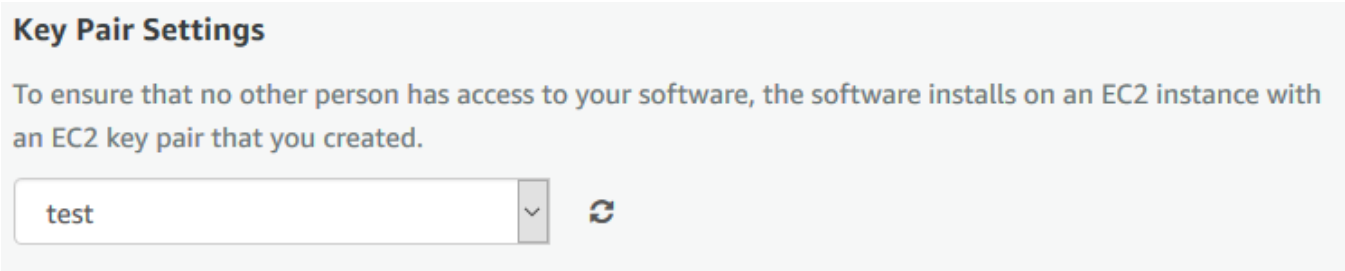



d. Choose the Security Group to be used

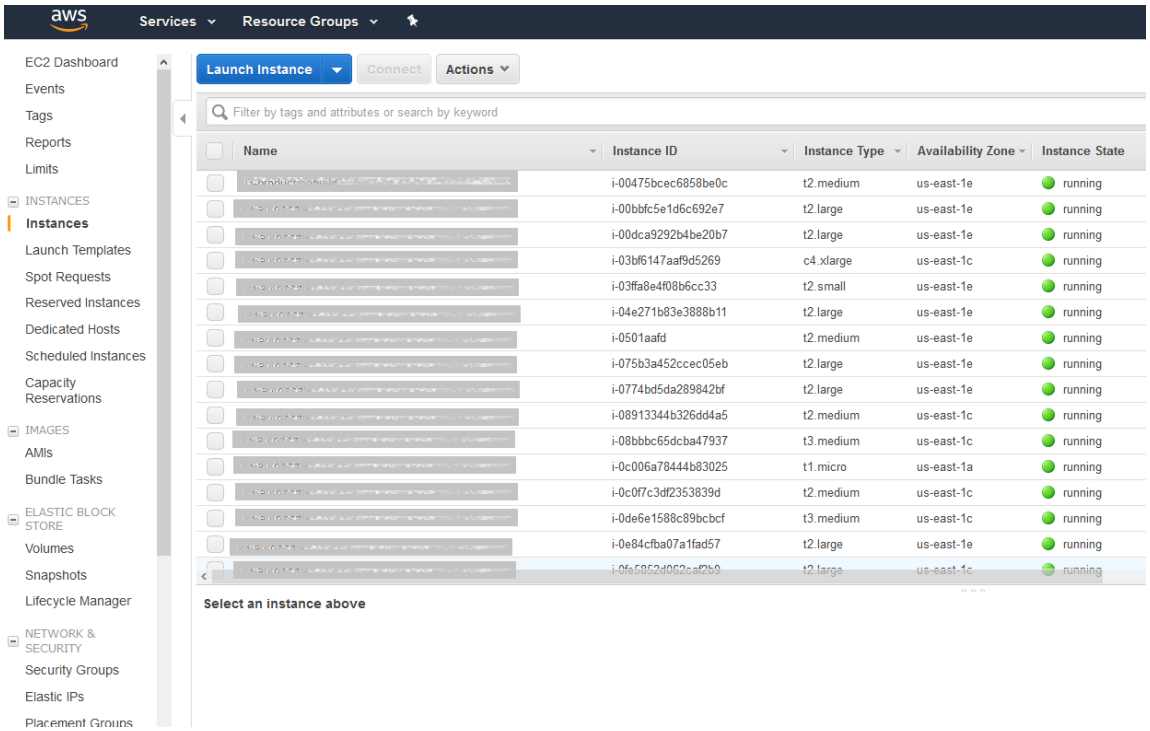



e. Select a Key Pair to launch the instance with

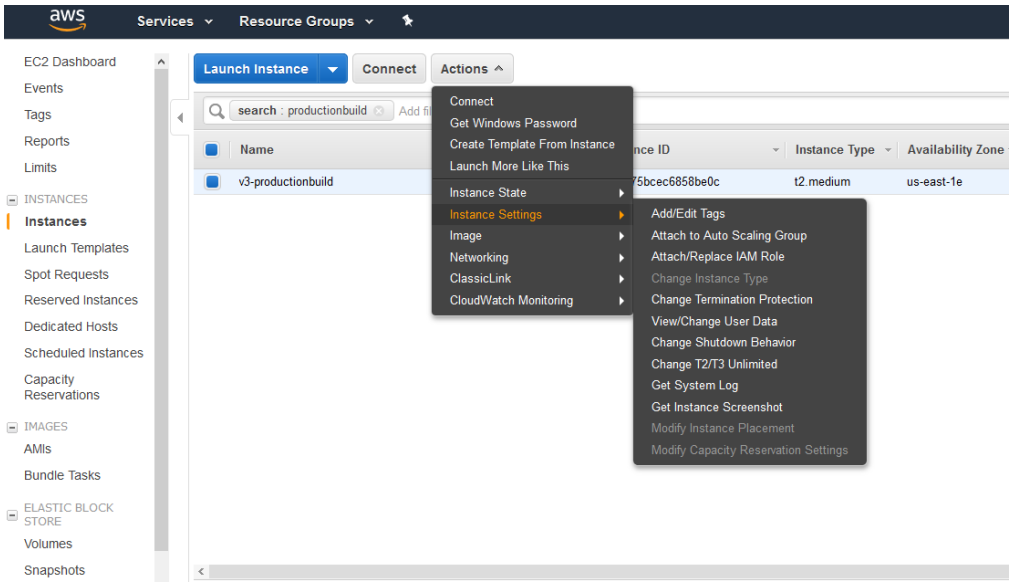



f. Click the Launch button


7. (Optional) To assign an IAM Role to your newly launched instance
   a. navigate to the AWS EC2 service, expand the Instances section in the left menu and select the Instances option

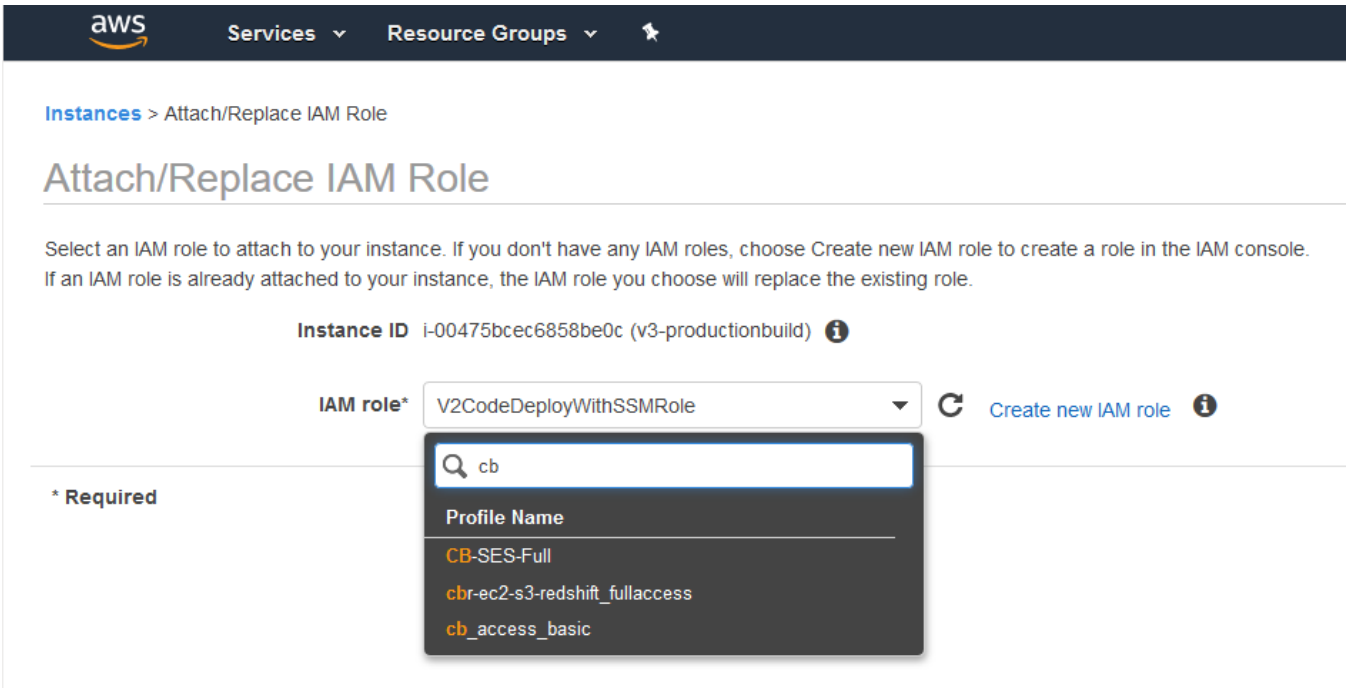



b. Find and select your new CLOUDBASIC instance
c. In the "Actions" menu expand the "Instance Settings" section and select the "Attach/ Replace IAM Role"

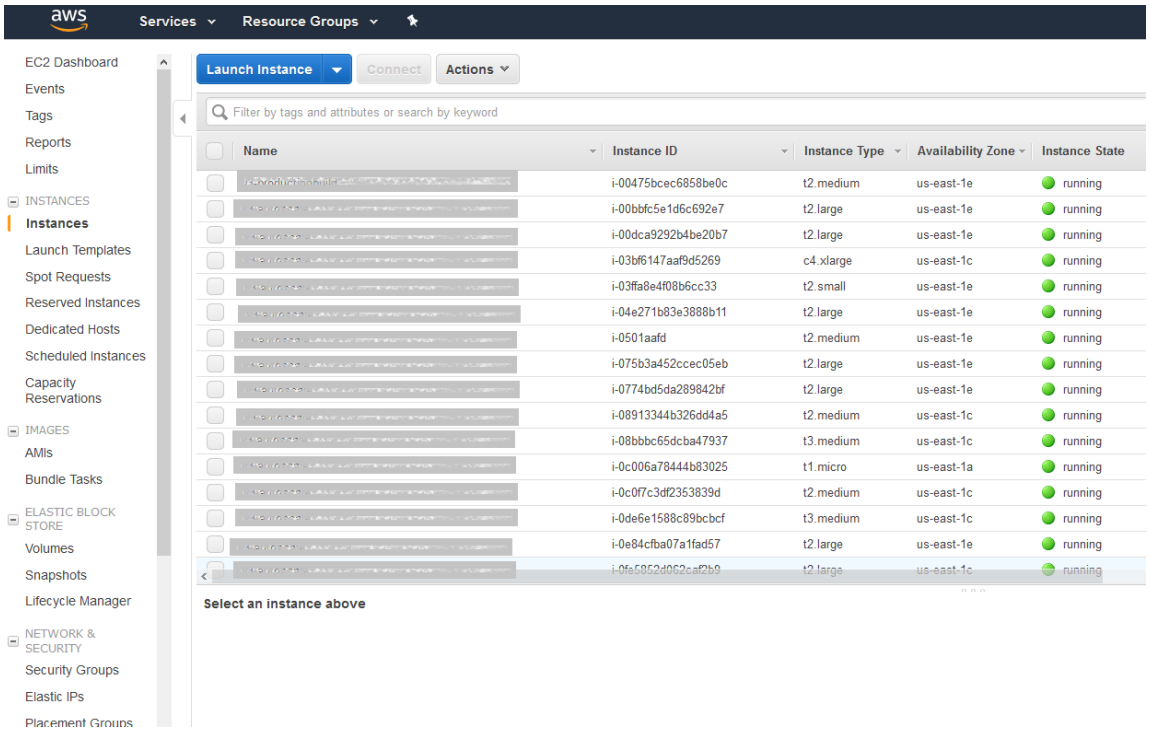



d. Select the IAM role that you want to assign (for instruction on how to create one, see the section Security in this guide) and click the "Apply" button

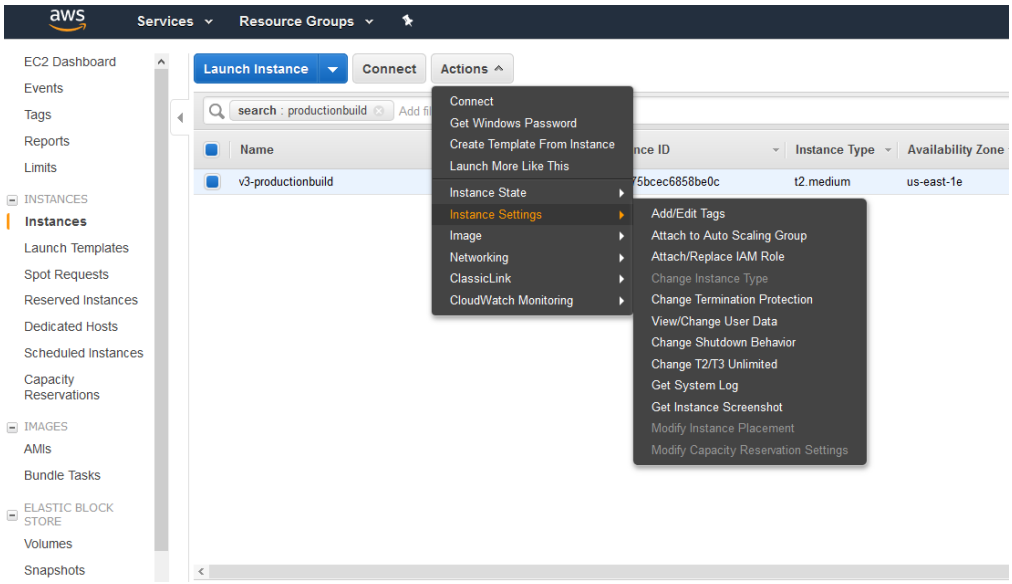
aws partner network
Advanced Technology Partner




8. (Optional) To tag your instance
    a. navigate to the AWS EC2 service, expand the Instances section in the left menu and select the Instances option

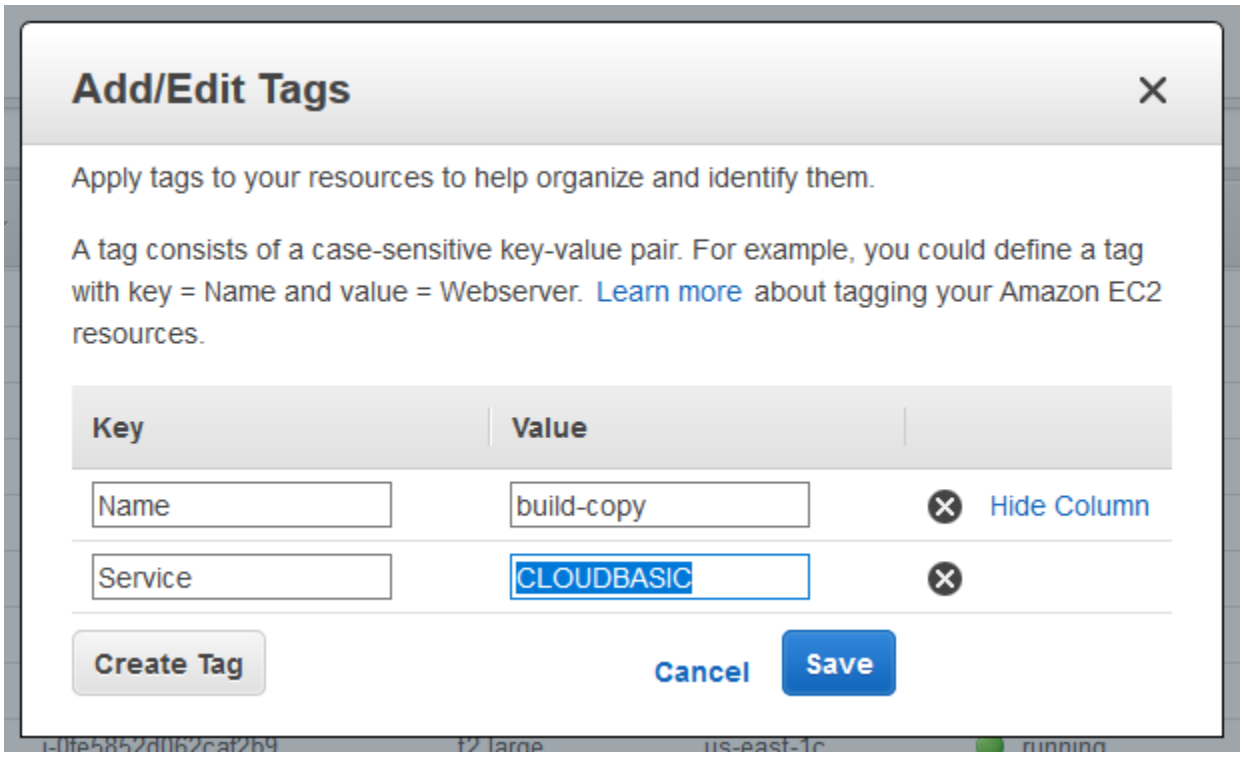



b. Find and select your new CLOUDBASIC instance
c. In the "Actions" menu expand the "Instance Settings" section and select the "Add/Edit Tags"

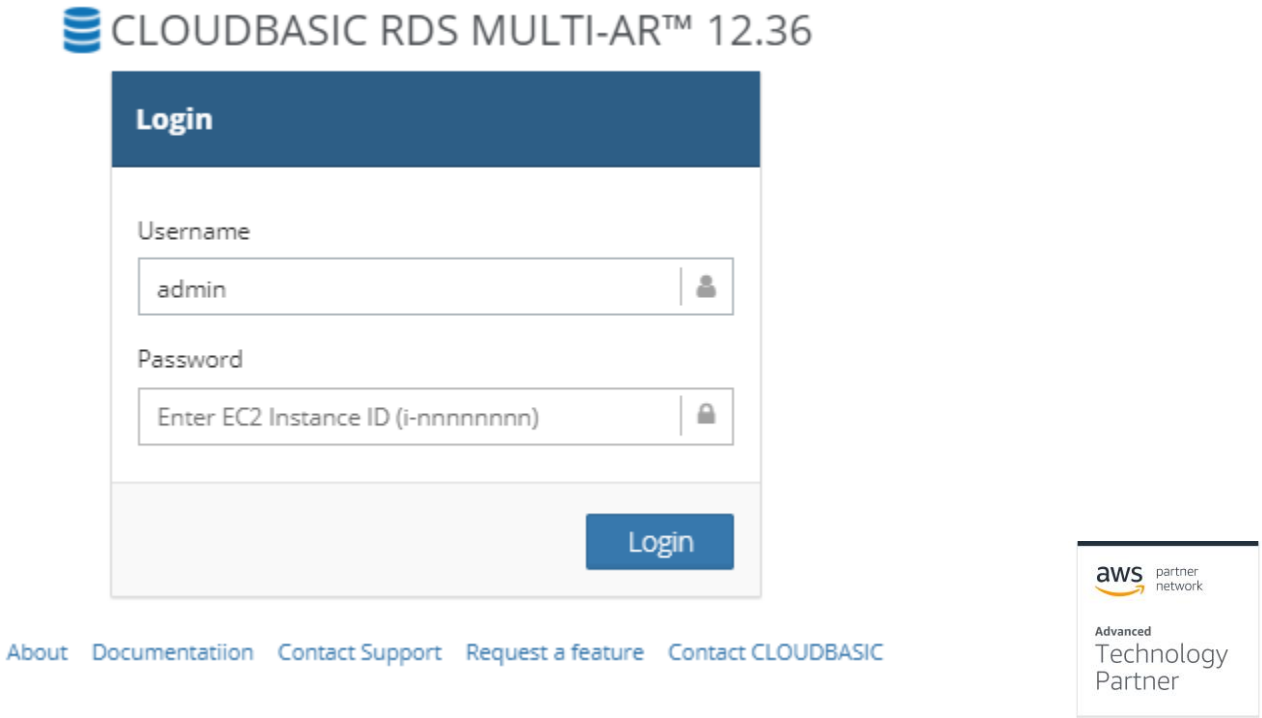



d. In the "Add/Edit Tags" dialog enter the tag keys and values and click the "Save" button

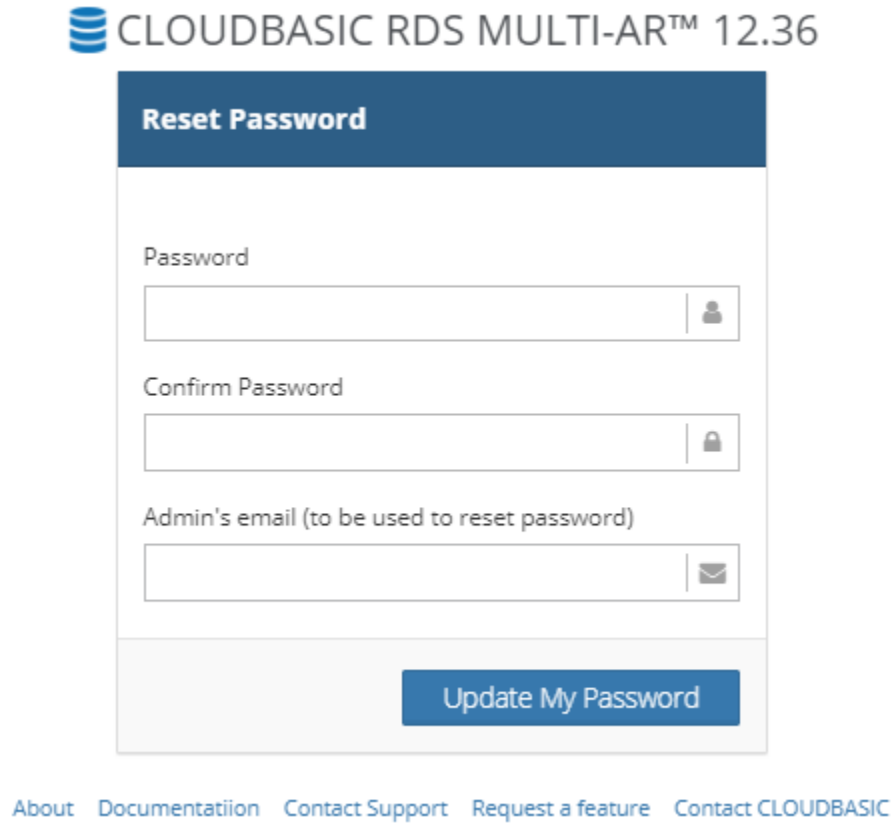
aws partner network
Advanced Technology Partner



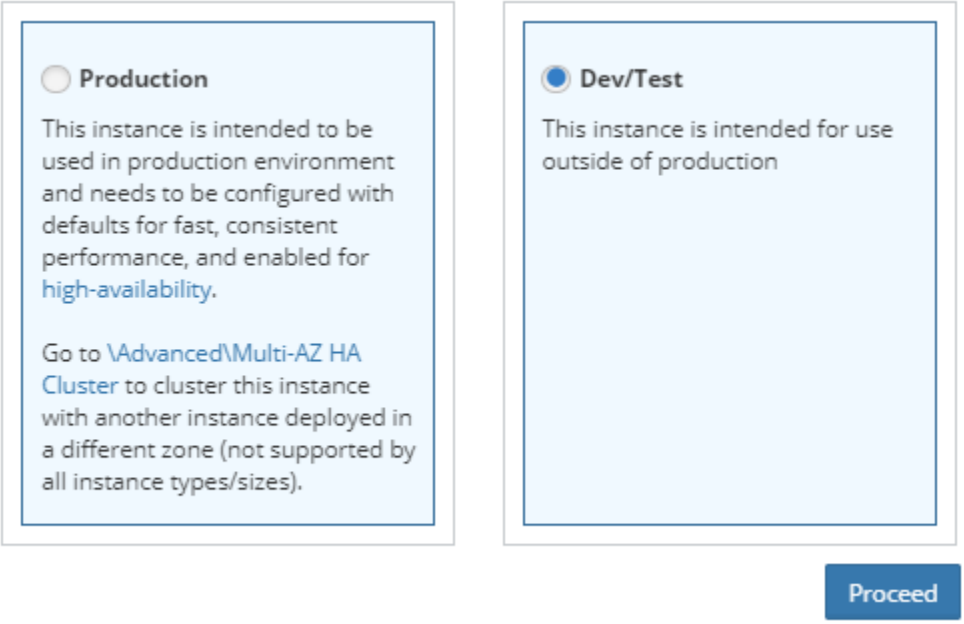

9. Once your instance is up and running, you can access the CLOUDBASIC management console on port 80 using the IP assigned to the instance. You will be prompted with the Activate Instance dialog.



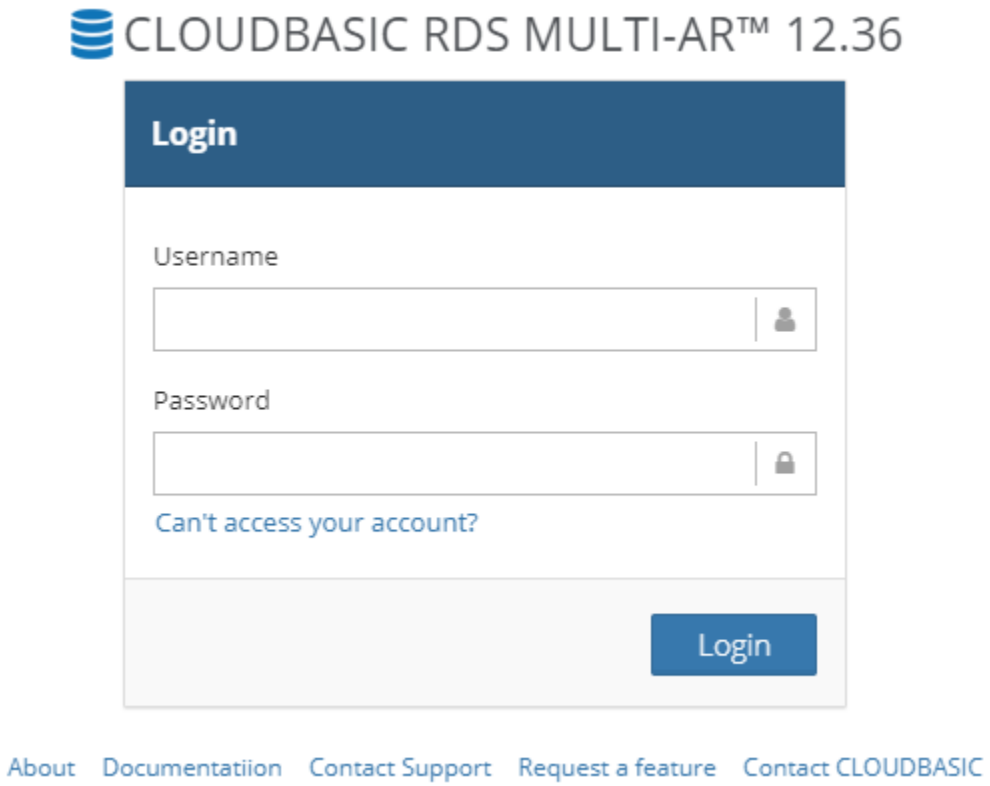
10. Select your new password and provide the email address to be used for administrative purposes




11. For evaluation or testing purposes select the "Dev/ Test". For production environments that need High Availability we recommend a cluster deployment.




12. After you have activated your instance, login to the admin console using the default user "admin" and the password you created during activation




13. For additional instructions on how to setup CLOUDBASIC replications for various use cases, please referrer to the following article in our documentation:

https://cloudbasic.net/documentation/configure-rds-sqlserver-alwayson/

## Deploying with AWS Active Directory Service

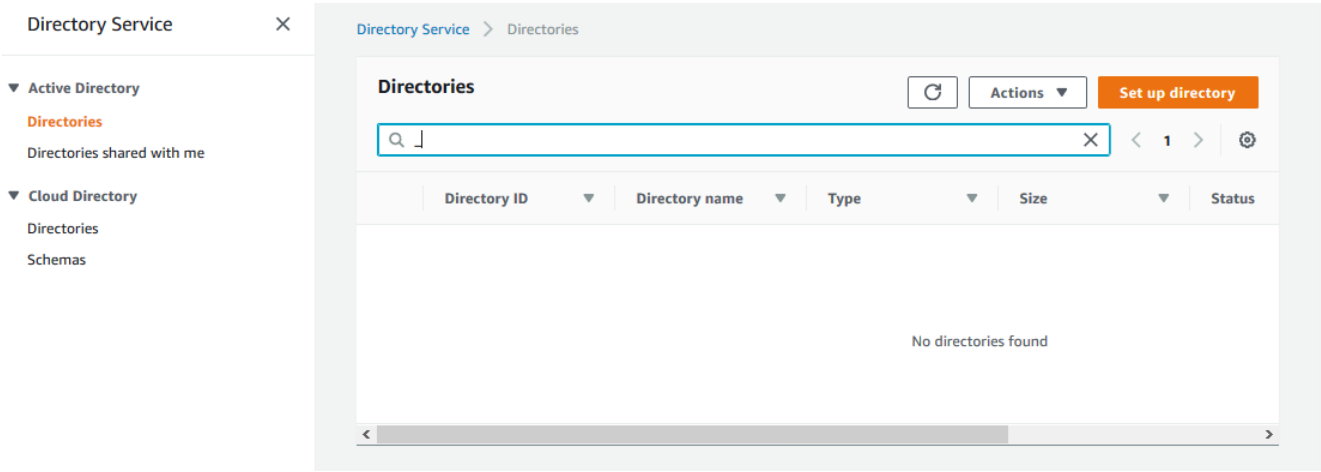
Many CLOUDBASIC customers operate in enterprise environments and utilize Active Directory to manage security and resources. The following steps describe how to setup CLOUDBASIC to work with the AWS Active Directory Service.

**Setting up AWS Active Directory Service**

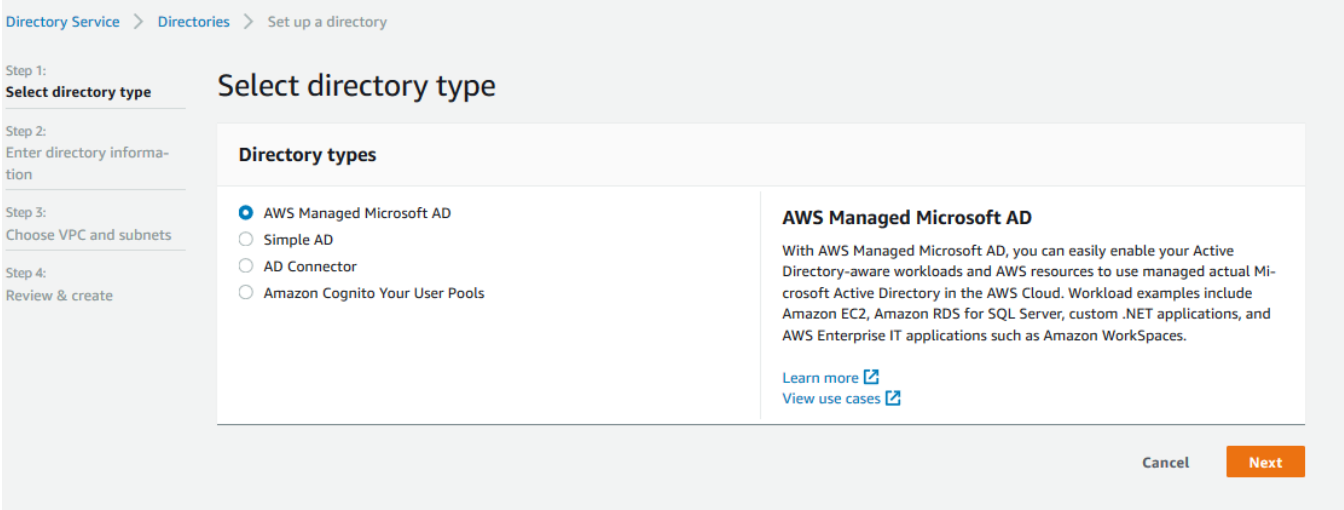
1. Review the AWS Active Directory Service prerequisites

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started_prereqs.html

2. In the Directory Service management console expand the Active Directory section and select the Directories option. In the upper right corner, click the "Set up Directory" button




3. In the "Select directory type" dialog, choose the "AWS Managed Microsoft AD" option




4. Choose between Standard and Enterprise edition, fill out the rest of the form and click "Next"

Directory Service > Directories > Set up a directory

Step 1:
Select directory type

Step 2:
**Enter directory information**

Step 3:
Choose VPC and subnets

Step 4:
Review & create

# Enter directory information

## Directory information

A managed Microsoft Active Directory domain based on Windows Server 2012 R2. Info

Directory type
Microsoft AD

Edition Info
Microsoft AD is available in the following two editions:

**Standard Edition**
Best for small to medium sized businesses.
- 1GB of storage for directory objects
- Optimized for up to 30,000 objects

~USD 86.4000/mo (USD 0.1200/hr)*

* includes two domain controllers, USD 43.2000/mo for each additional domain controller.

**Enterprise Edition**
Best for large businesses.
- 17GB of storage for directory objects
- Optimized for up to 500,000 objects

~USD 288.0000/mo (USD 0.4000/hr)*

* includes two domain controllers, USD 144.0000/mo for each additional domain controller.

Directory DNS name
A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.

ad.cloudbasic.net

Directory NetBIOS name - *Optional*
A short identifier for your domain. If you do not specify a NetBIOS name, it will default to the first part of your Directory DNS name.

cbr

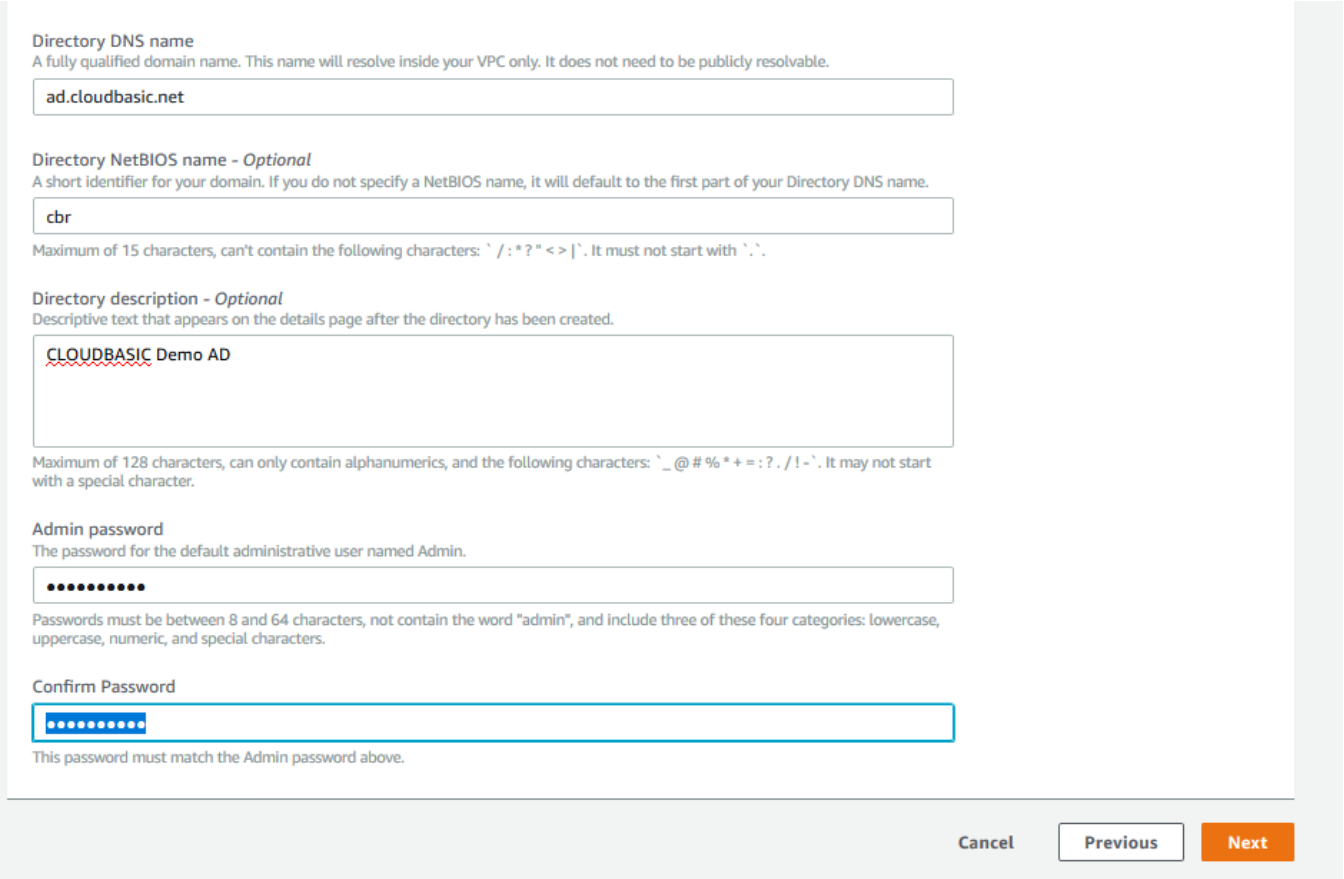
Maximum of 15 characters, can't contain the following characters: ` / : * ? " < > | `. It must not start with `.`.

Directory description - *Optional*
Descriptive text that appears on the details page after the directory has been created.

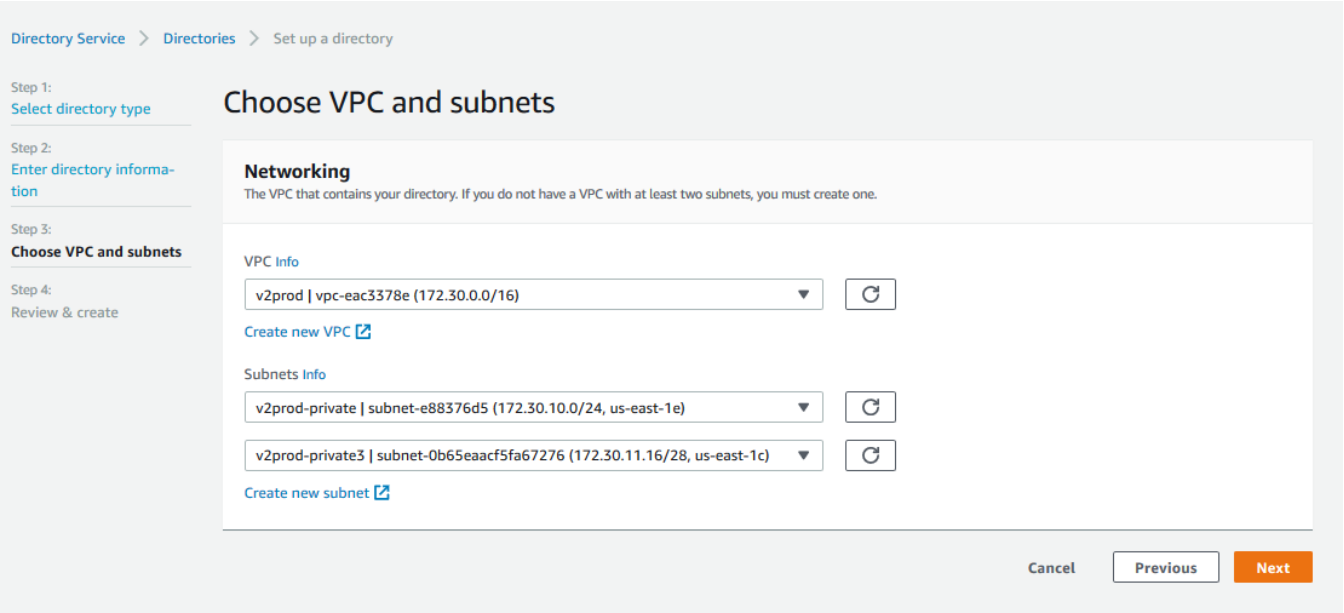
CLOUDBASIC Demo AD

Maximum of 128 characters, can only contain alphanumerics, and the following characters: `_ @ # % * + = : ? . / ! - `. It may not start with a special character.

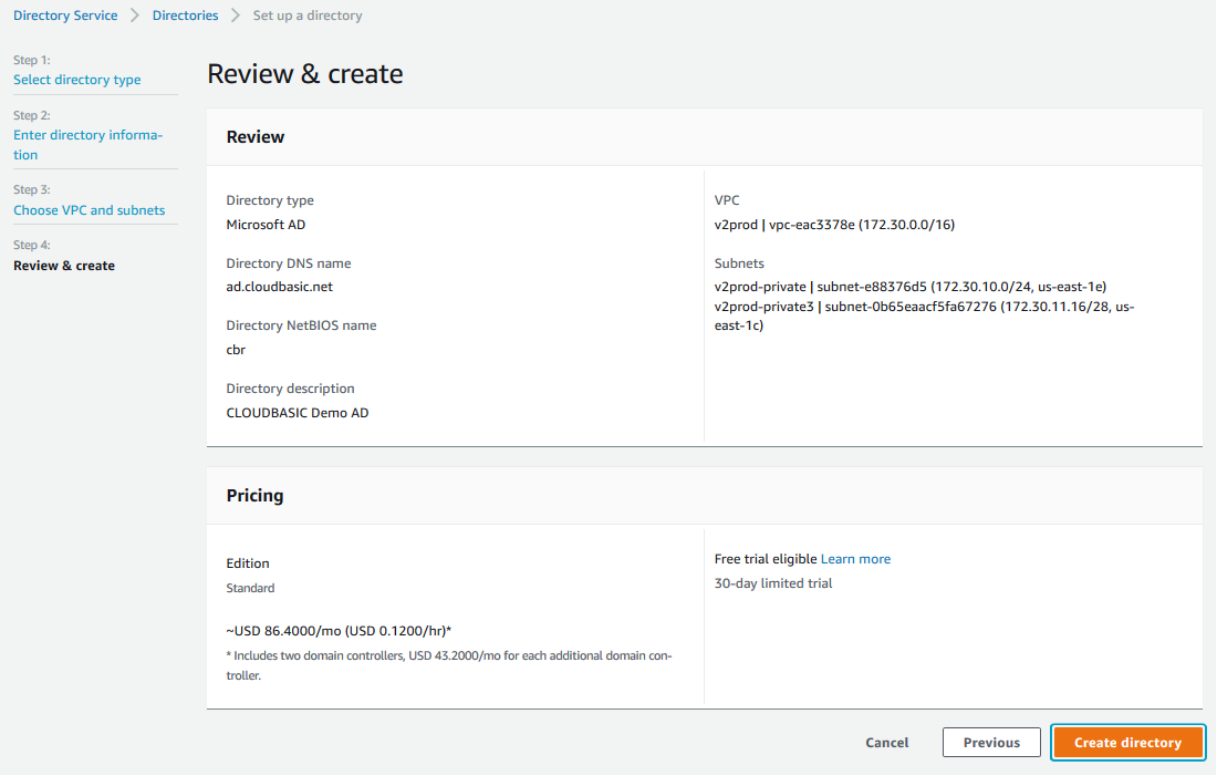
aws partner network
Advanced
Technology
Partner




5. Select the VPC and subnets where your AD Service will be installed

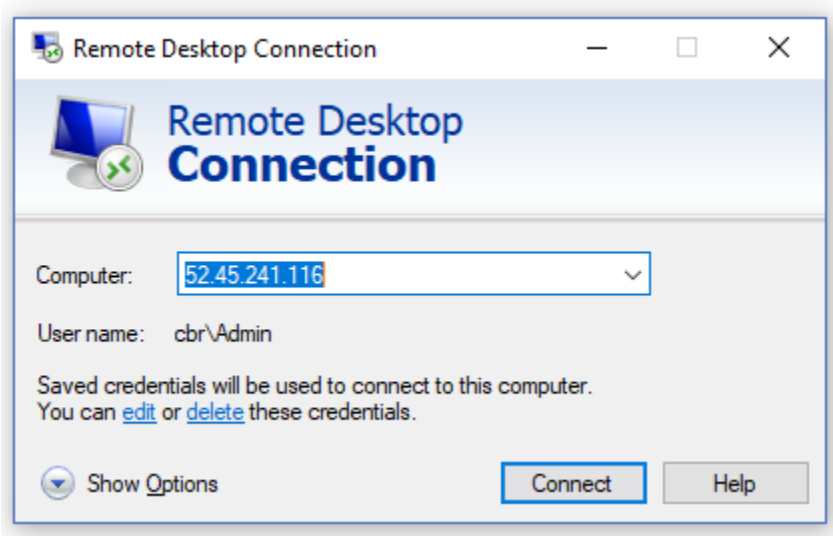



6. Finally, review the parameters of your new directory and click "Create Directory"

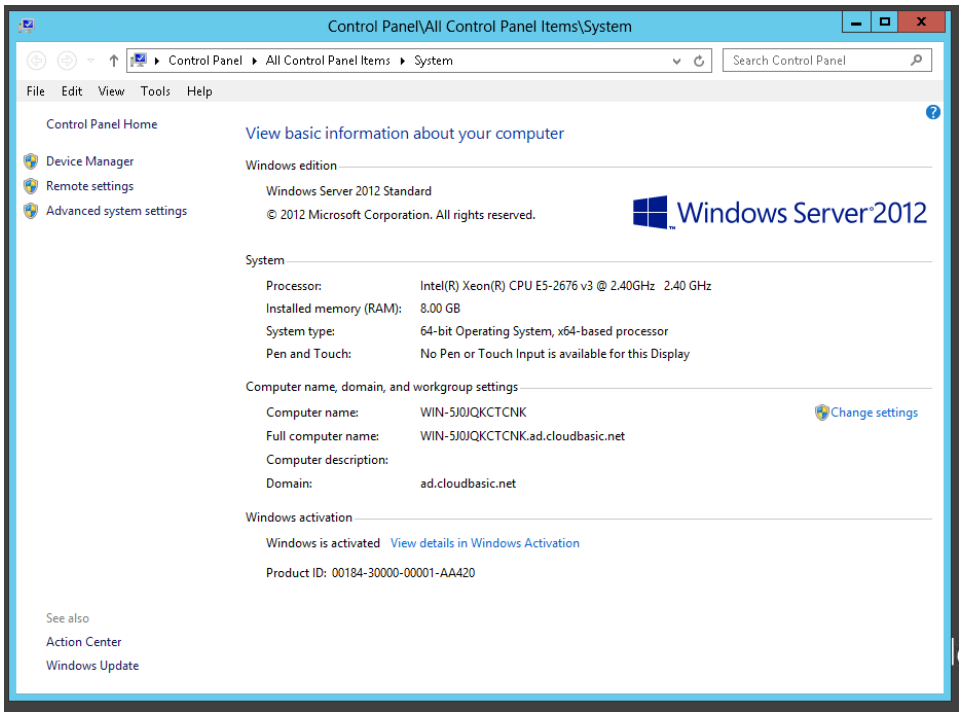



7. Please note that the AWS AD Service does not include tools for AD configuration and you will need to do that on your own using and instance from the EC2 service. The details of AD administration are beyond the scope of this guide and will not be covered here.

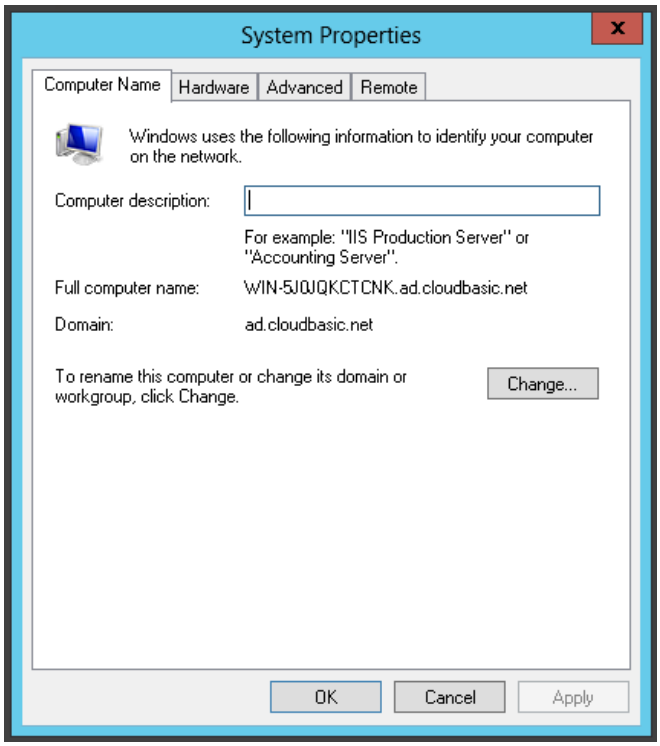
8. Joining your CLOUDBASIC instance to the AD Service
    a. RDP into your CLOUDBASIC instance using an AD user with enough privileges to modify the machine.



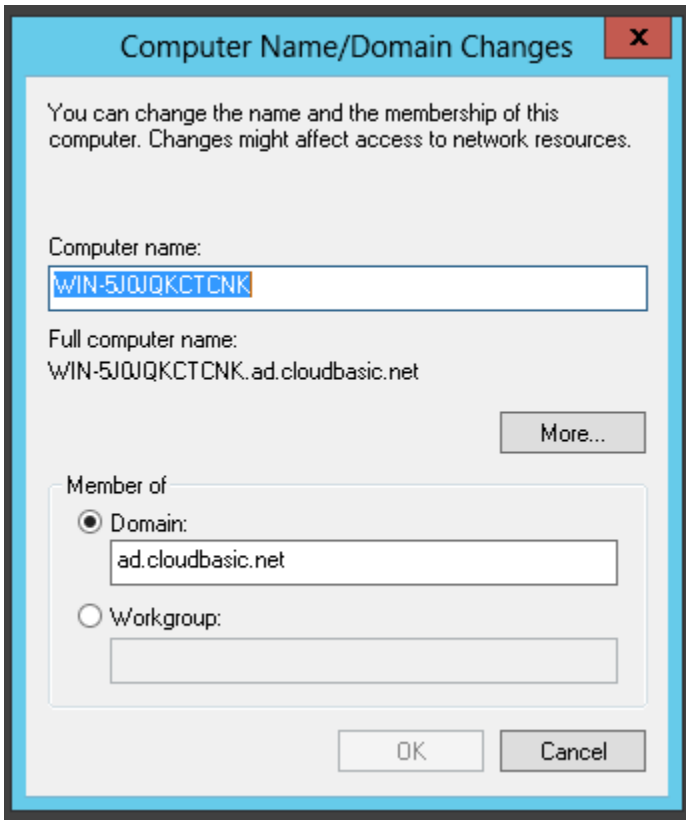

    b. Open a Windows Explorer window and navigate to "Control Panel\All Control Panel Items\System". Click on "Change Settings"



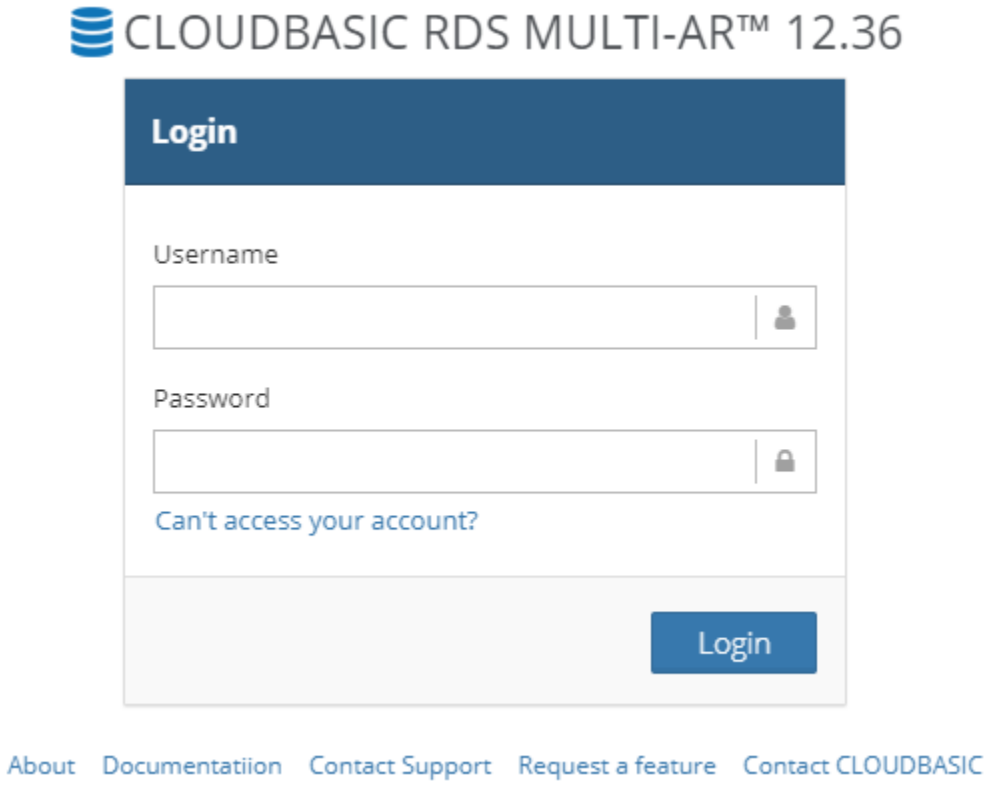

    c. In the "System Properties" window select the "Computer Name" tab and click on the "Change" button



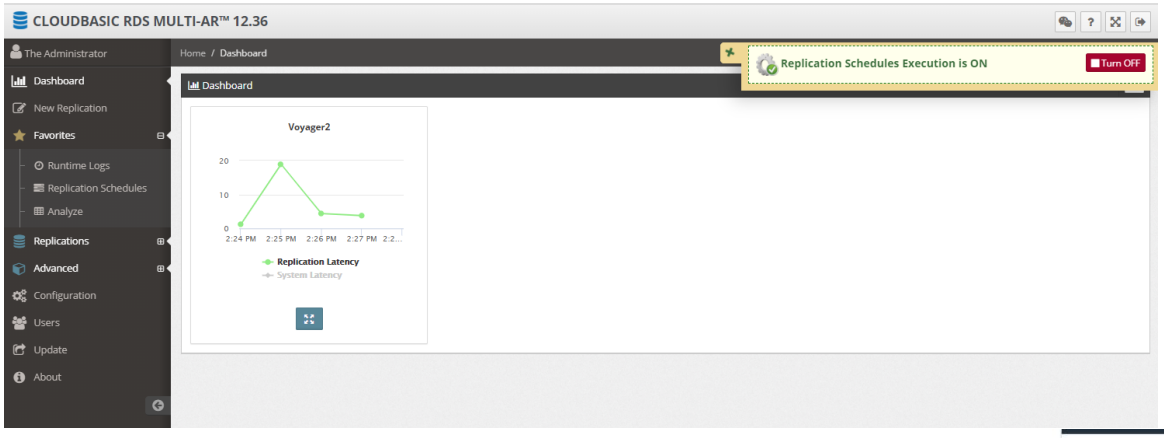

d. In the "Computer Name/ Domain Changes" select the "Domain" option in the "Member of" section and enter the name of your AD domain. Click OK and then provide an AD administrator account to complete the change.



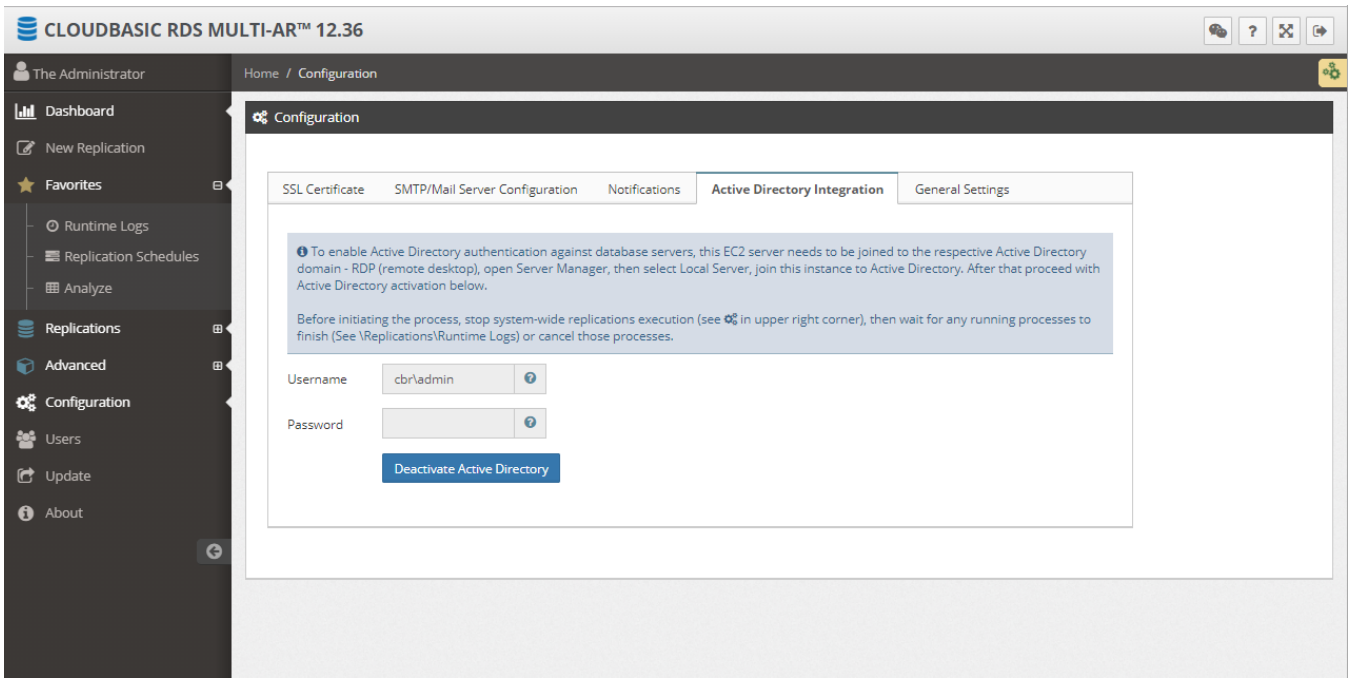
e. Reboot your CLOUDBASIC instance in order to complete the setup
f. Next, to configure your CLOUDBASIC instance to use Active Directory:
   i. Login to your CLOUDBASIC console




   ii. Stop the system-wide replication execution by pressing the gear button in the upper right corner and then clicking the "Turn OFF" red button

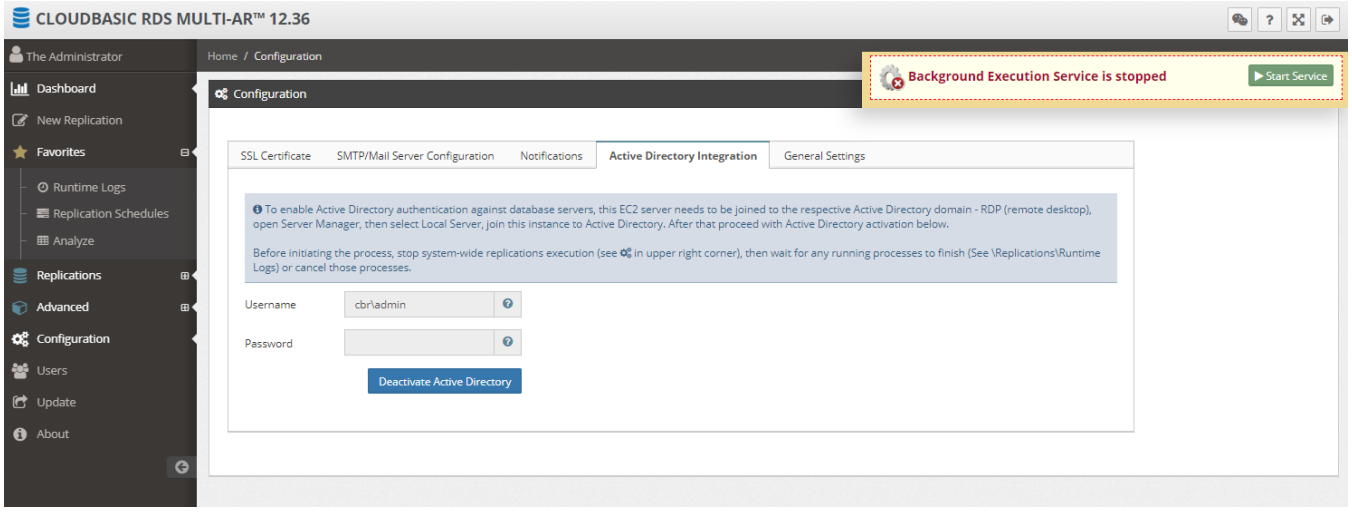


iii. Select the "Configuration" option in the left-hand menu and navigate to the "Active Directory Integration" tab




iv. Enter the AD user name and password that the CLOUDBASIC Replication services should run under and click the "Activate Active Directory" button.

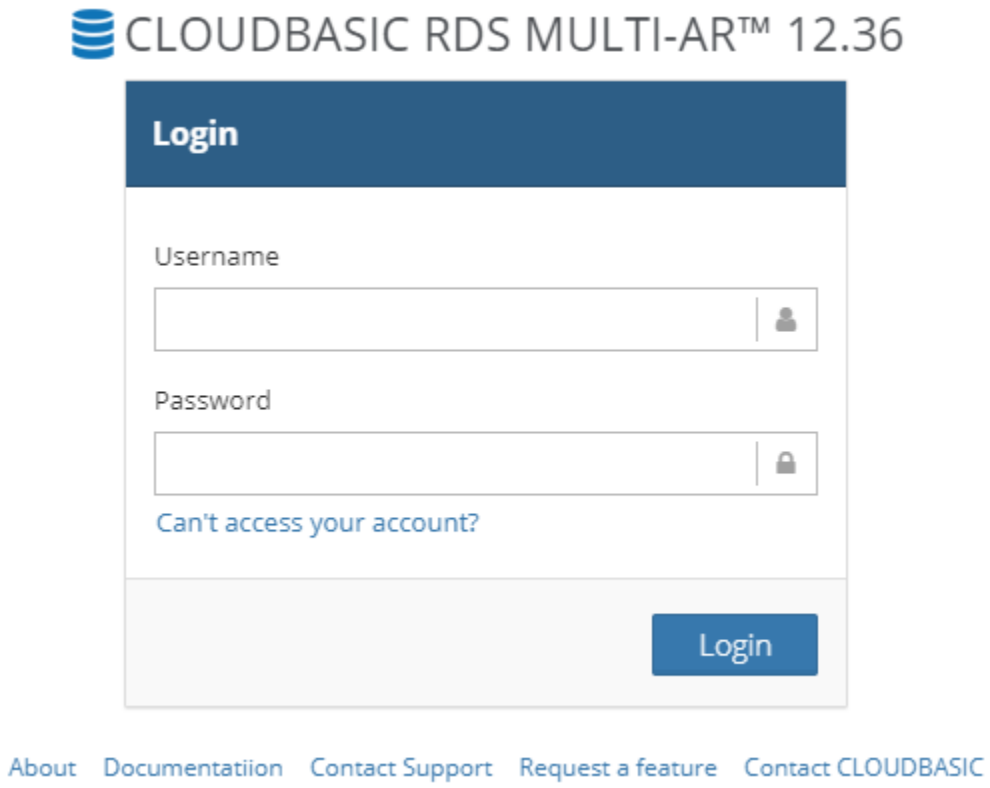
v. Restart the system-wide replication execution by pressing the green "Start Service" button in the upper right corner




## Testing your instance

Your CLOUDBASIC instance is preconfigured to respond to HTTP requests on port

80 with the login screen of the management console.



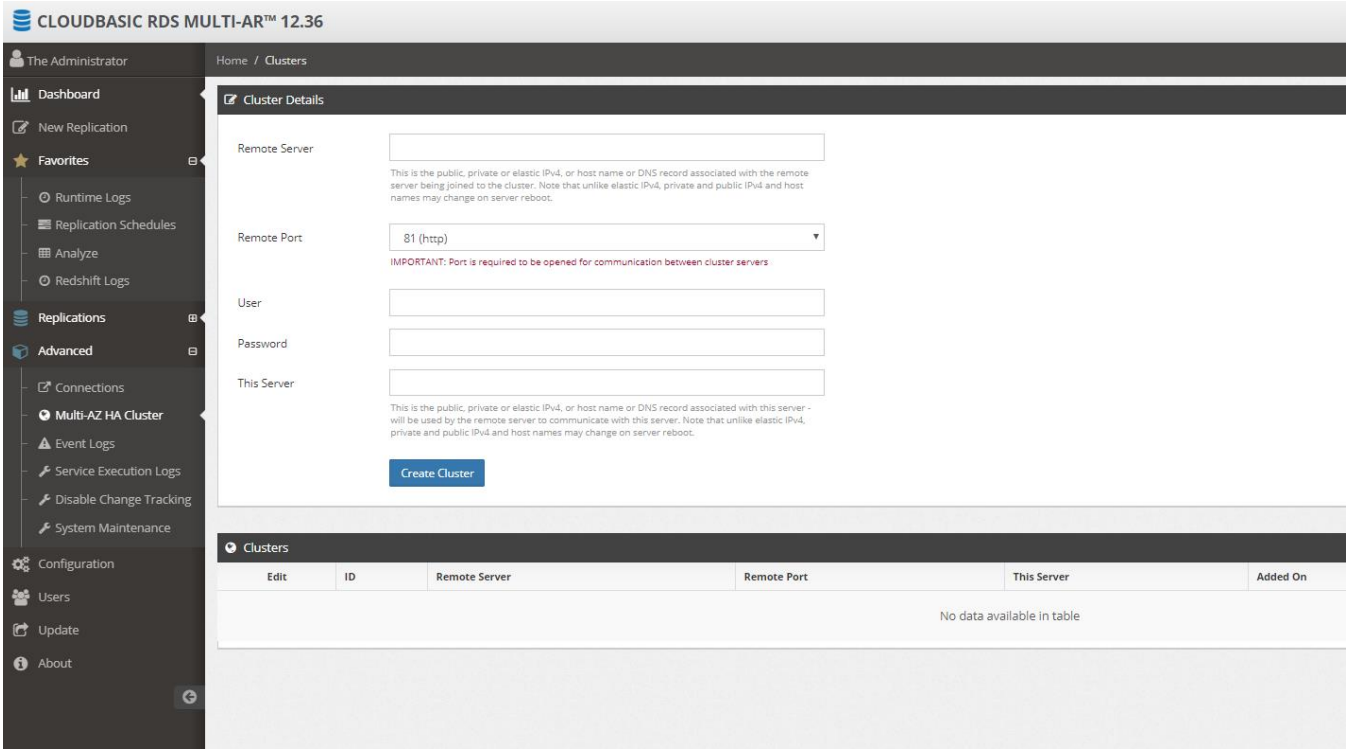

If this is not the behavior that you are observing, verify that the instance is running and the assigned security group allows to communicate with the instance on port 80.

## Setting up a Highly Available CLOUDBASIC deployment

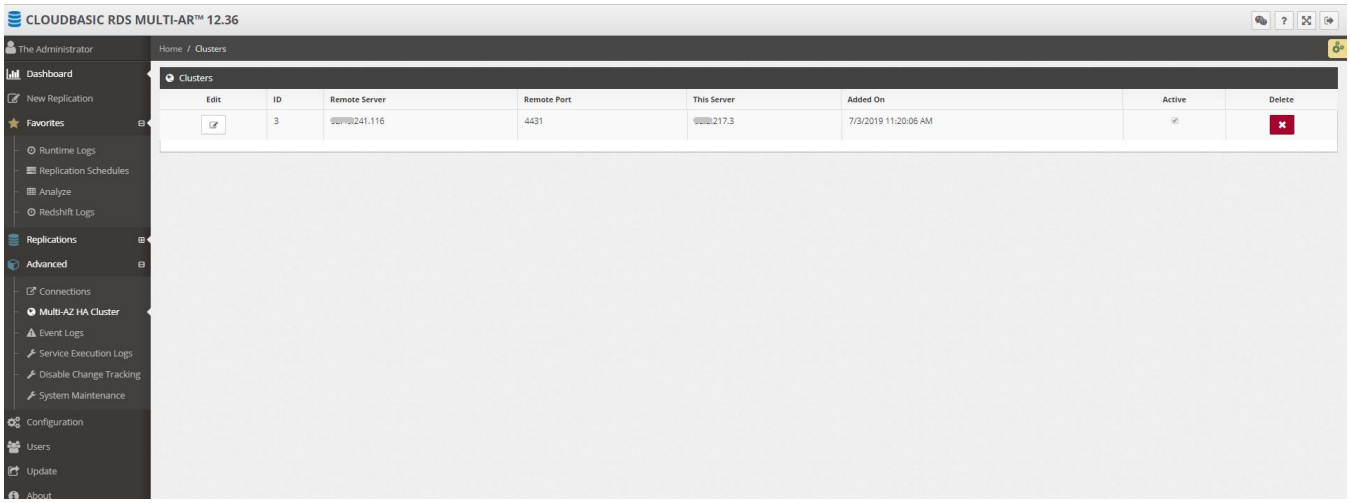
For production deployment scenarios that demand highly available architectures, CLOUDBASIC can be deployed in a Multi-AZ or Multi-Region configuration. This type of deployments require two instances in separate AZs or Regions that are setup to compete with each other for replication tasks and are fully capable of handling the complete workload in cases when there is a failure of any severity – a VM, an AZ or a whole Region.

1. For Multi-AR, setup your VPCs and VPC-peering as demonstrated in the section "Architecture Diagrams" of this guide
2. Create a CLOUDBASIC instance in each VPC by following the direction in the section "Deployment Assets"
3. Ensure that the Security Groups assigned to each instance allow communication between the two on port 81 for unencrypted traffic or port 4431 if traffic is to be encrypted.

4. If you need traffic to be encrypted between the two instances, follow the steps in the "Cluster communication encryption" section
5. To initialize your CLOUDBASIC High Availability cluster, login to one of the instances, expand the section "Advanced" in the left-hand menu, and select the "Multi-AZ HA Cluster"




6. Fill out the "Cluster Details" form
    a. In the field "Remote Server" enter the IP address of the second (remote) CLOUDBASIC instance you created in Step 2.
    b. In the field "Remote Port" select how the instances will communicate with each other
    c. In the field "User" enter the username that this instance will use to authenticate itself with when communication with the remote instance
    d. In the field "Password" enter the password of the remote user
    e. In the field "This Server" enter the IP address of the instance you are working with
7. Click "Create Cluster"
8. You now have a Highly Available CLOUDBASIC cluster




## Setting up an automated RDS SQL Server cross-region failover

Scenarios where high assurance of uninterrupted RDS SQL Server operation is critically important require close orchestration between AWS services and a Multi-AR CLOUDBASIC deployment. The following guide demonstrates how to leverage CloudWatch, Route 53 HealthCheck, Lambda and CLOUDBASIC API to achieve automated cross-region RDS SQL Server failover.

The overall strategy is based on the following high-level workflow:

"**An RDS CloudWatch alarm goes into INSSUFICIENT DATA state**" because the monitored RDS instance goes down

-> This condition triggers a "**Route53 Health Check to FAIL**"

-> Which then triggers "**A ROUTE 53 Health Check alarm to go into ALARM state**"

-> Which causes a notification to be send to an SNS topic

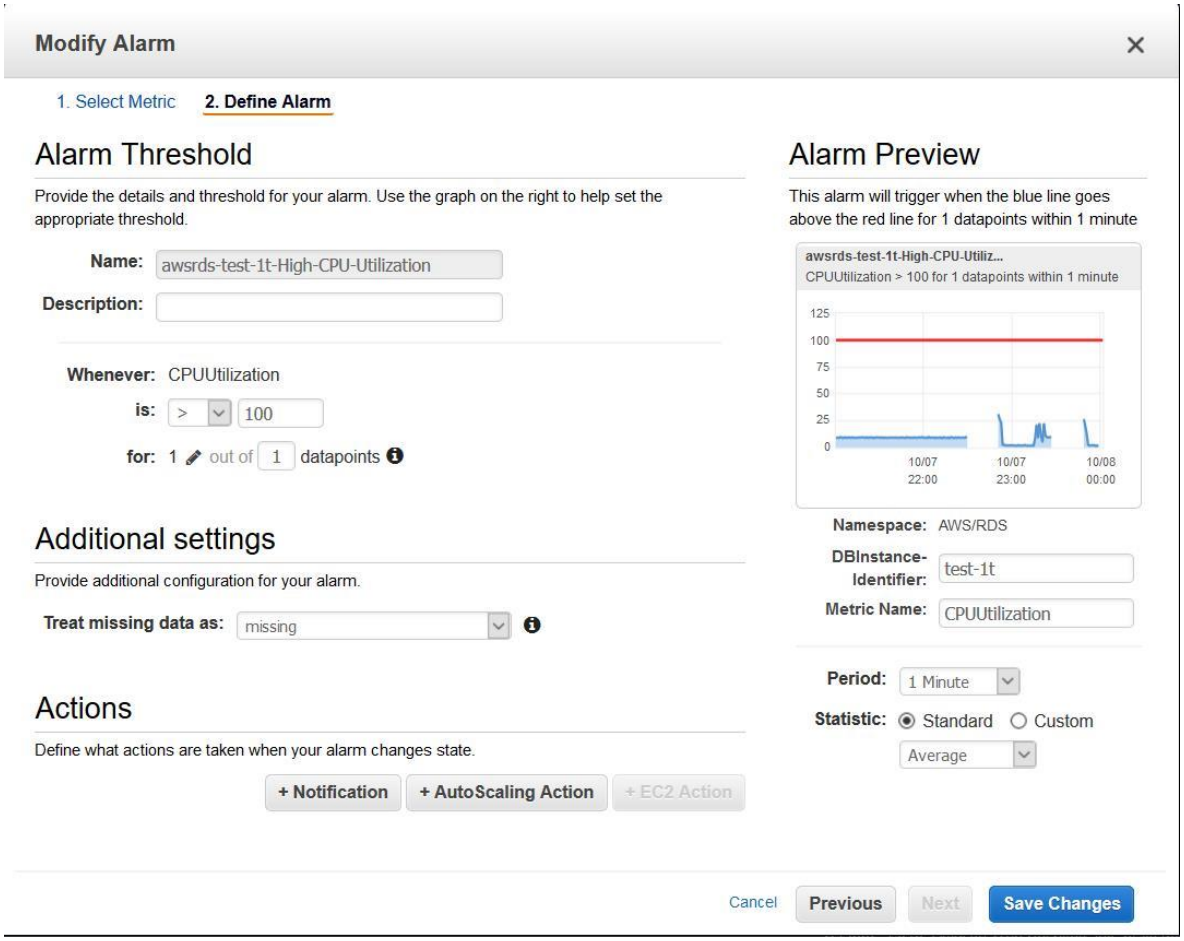
-> Which triggers LAMBDA functions that are subscribers to the SNS topic to execute

-> The LAMBDA functions call CloudBasic API methods to configure the secondary RDS for Primary duties (activation of constraints, triggers, etc,) and to switch the Route53 record to point to the new Primary RDS instance

aws partner network
Advanced
Technology
Partner

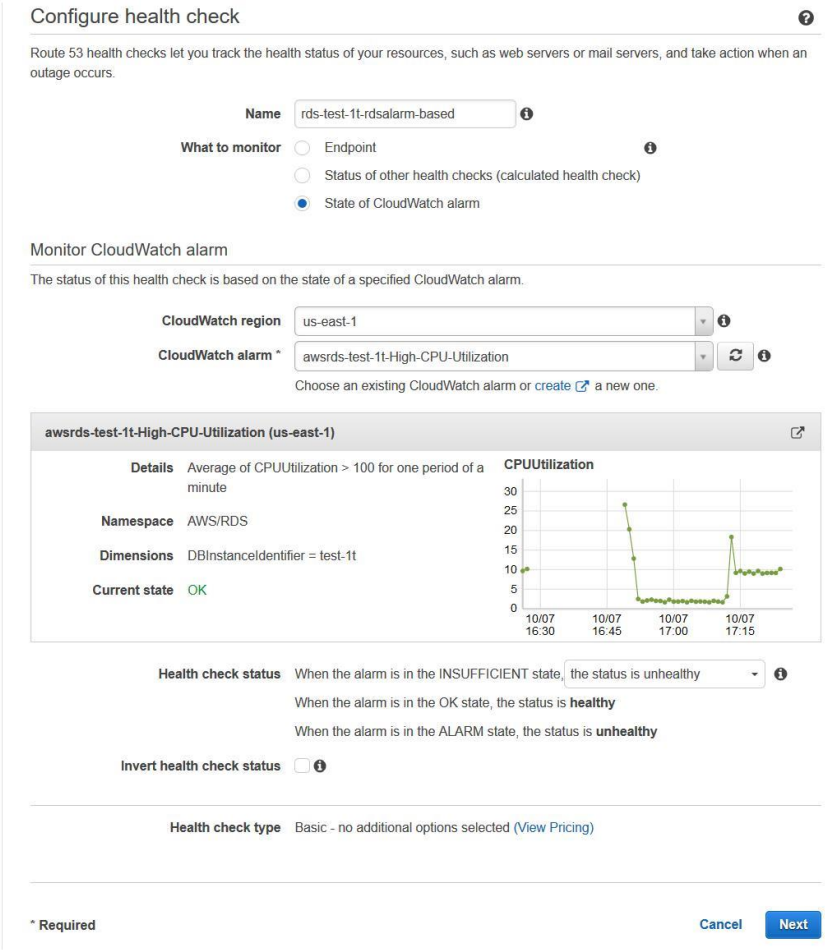
Here is how to setup the individual components of this workflow:

1. Setup a CloudWatch alarm for your RDS instance
    a. Select the CPUUtilization metric and configure to look for condition of CPUUtilization > 100 %
    b. Configure to look for "1 out of 1 datapoints"
    c. Period to be "1 minute"
    d. Configure Statistic to be "Standard" and select "Average"

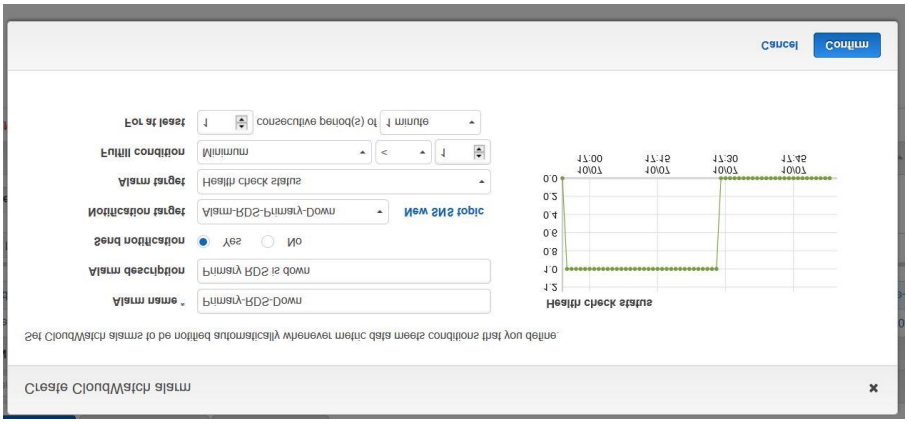



*<u>Note</u>: The goal is to configure a CloudWatch alarm that will never be triggered based on the triggering condition.*

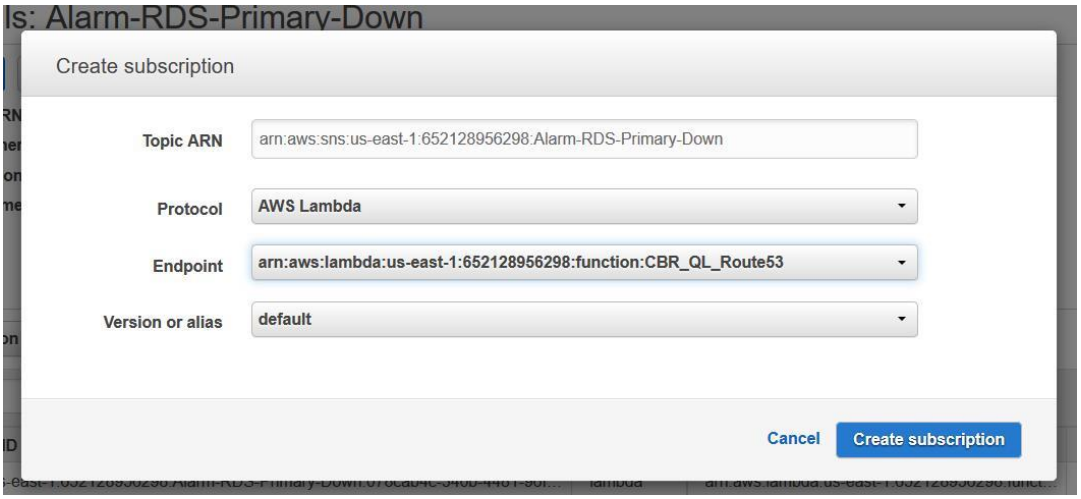
2. Setup a Route53 Health check to monitor the RDS CloudWatch alarm
    a. In the "What to monitor" select "State of CloudWatch" alarm
    b. Under the "Monitor CloudWatch alarm" section select the AWS Region and the name of your RDS CloudWatch alarm
    c. **VERY IMPORTANT** in the "Health check status" section, for the "When the alarm is in the INSUFFICIENT state" select the "the status is unhealthy" option




3. Set up a Route53 Health check alarm
    a. Select the Route53 Health check you created in the last step
    b. In the Alarms tab click on "Create alarm"
    c. Under "Send notification" select "Yes"
    d. Create a new SNS topic
    e. Click on "Confirm"



4. Setup your Lambda functions as subscribers to the SNS topic
    a. In the SNS service select the SNS topic you created in the previous step
    b. In the "Subscriptions" section click the "Create subscription" button
        i. Under "Protocol" select "AWS Lambda"
        ii. Under "End point" select the Lambda function you would like to call




5. When setting up your Lambda functions refer to our GitHub library

https://github.com/cloudbasic

    a. Promoting an RDS replica to primary status

    https://github.com/cloudbasic/Lambda-Promote-to-Primary

    b. Switching a Route 53 record

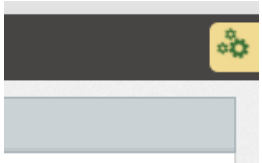
    https://github.com/cloudbasic/Lambda-Update-Route53

# Operational Guidance

## Health Check

When CLOUDBASIC is operating normally it will respond on port 80 of your instance. Use the AWS EC2 console to monitor the basic performance metrics of your instance and to verify that it is not being overloaded.

The health of the replication service and the status of individual replication schedules can be verified in the CLOUDBASIC management console. When the service is operating normally you will see a spinning set of gears in the upper right corner.



For more details on how to monitor the progress of individual replication schedules please see our online documentation

https://cloudbasic.net/documentation/monitor-continuous-copy-relationship/

## Backup and Recovery

CLOUDBASIC RDS AlwaysOn/Geo-Replicate allows replication servers deployed in different availability zones (Multi-AZ) or multi-availability-regions (Multi-AR) to be clustered achieving High-Availability replication processing. The replication workload is load balanced by default. If one server goes down the other one picks up the replication workload. Lower latency can be achieved (version 10.12 and above only) by assigning affinity to the server replicating with lower lag.

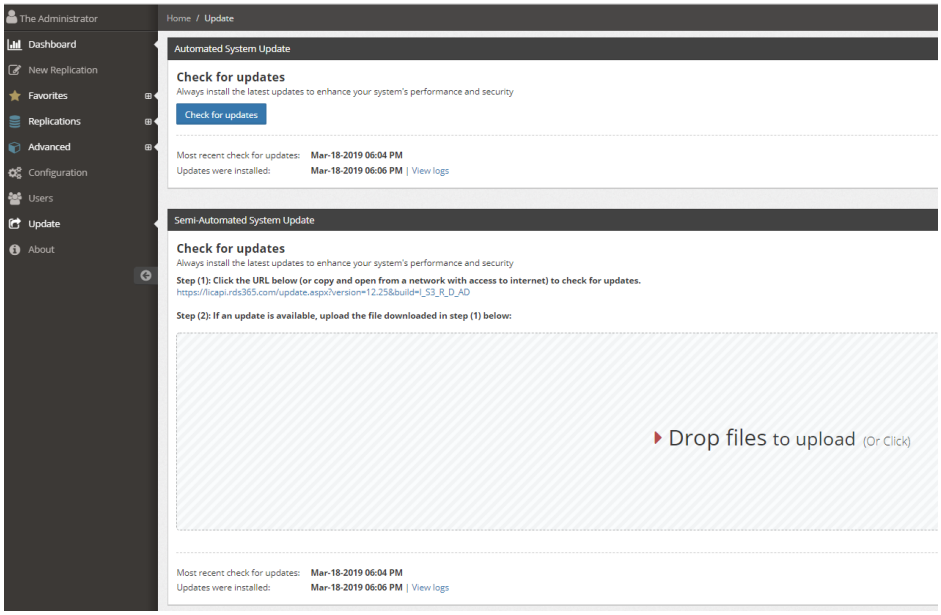
For more detailed information, please see our online documentation

https://cloudbasic.net/documentation/multiaz-high-availability-cluster/

In deployment scenarios where a CLOUDBASIC cluster is not justified, the recovery of a failed instance will require the complete rebuild of the instance along with the replication schedules. Please note that this process will result in reseeding of all replicated databases and can take a very long time depending on the amount of data, the size of your CLOUDBASIC instance and the speed of all involved network connections.

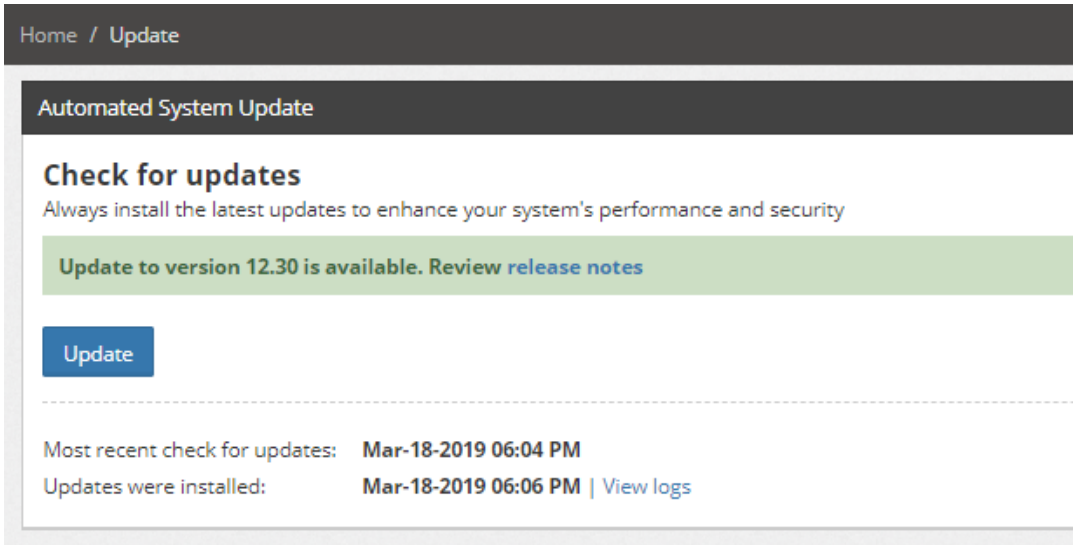
## Routine Maintenance

Your CLOUDBASIC instance comes with the ability to check for newer releases. To update your CLOUDBASIC instance to the latest version of the software supported in your use case, select "Update" from the menu on the left. CLOUDBASIC supports two ways to update the version of the software you are using



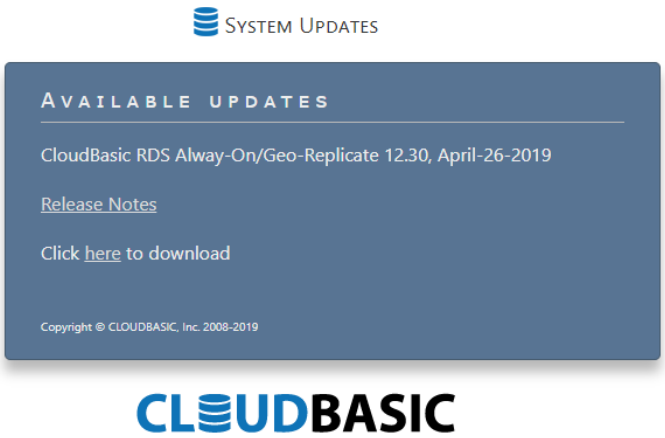

## Fully automated updates

When your CLOUDBASIC instance is configured to have access to the Internet, clicking the "Check for updates" button causes the instance to check with the CLOUDBASIC servers whether a newer version is available. If a new version is available, you will see the "Update" button along with a link to the "Release notes".




## Manual updates

When your CLOUDBASIC instance cannot access the Internet, you will need to obtain and upload the update package manually. Just follow the steps in the section "Semi-automated System Update". You will be taken to a page that looks like this and will be able to download the appropriate version.




### Emergency Maintenance

As described in the section "Backup and Recovery", the best practice to address emergency situations is to deploy CLOUDBASIC in a High Availability configuration with nodes in multiple Availability Zones or AWS Regions.

### Support

All CLOUDBASIC customers receive the Basic Support, which comes included with all service subscription plans. In addition, 24x7 access is provided to online documentation, white papers, and case studies. Priority over the phone Technical Support and Advisory Services are available to higher service tiers and Premium Support subscribers. Please refer to our online documentation for additional details

https://cloudbasic.net/supportplans/

### Support Costs

Support is included with a CLOUDBASIC AWS Marketplace subscription.

## Accessibility

### Reference Materials

Additional consideration along with more detailed discussions of CLOUDBASIC deployment scenarios are available at:

https://cloudbasic.net/documentation/

## Localization

This user guide is available in English.