



IT Automation

All In One HA Configuration (AWS)

Install Manual

※In this Document, "Exastro IT Automation" will be written as "ITA".

Exastro IT Automation Version 1.7.2

Exastro developer

Introduction

1. About this document

- This document describes the information necessary to configure an HA cluster by combining two ITA all-in-one installed servers and OSS products. By turning the ITA into an HA Cluster, users can construct an ITA Server with more reliability and availability than what would be possible with a single Linux server.
- HA clusters configured with the use of this document will have the following functions.
 - The ITA server is always running on one of the servers and provides all the functions of the ITA Web/AP, Backyard, Ansible driver, etc.
 - If the server that is providing the service goes down, the ITA server will start on the other server in about 2–3 minutes and the service will take over. If this happens, the Database will not be lost.
- For a deploy example, please see “5. System Configuration example”
Please change values such as IP Address, Host names, Directory names and file names to fit your environment.
- This document assumes that the environment is constructed with the following.

Main software(excluding ITA)	Application	Verification ver.
Red Hat with Linux 8 High Availability	OS(EC2 image)	8.4
Pacemaker(※)	Cluster control	2.0.2–3
Corosync(※)	Heartbeat	3.0.2
pcs(※)	Pacemaker command	0.10.2–4

※These three are included in the EC2 image.

2. Scope of responsibility

- This document provides cautions and configuration examples for clustering ITA servers as reference information.

Introduction

3. Configuration procedure

- The Configuration procedure is as shown below

Item	Service	Machine no.1 (Master)	Machine no.2 (Slave)
0-1. 事前準備(AWS設定)	VPC	-	-
	Subnet	-	-
	Route table	-	-
	Security Groups	-	-
	IAM	-	-
	RDS	-	-
	EFS	-	-
	Route53	-	-
	EC2	Create EC2	Create EC2
	ElasticIP	Associating ElasticIP	-
1. Install ITA	ITA1.7.2 Online install	ITA Online install	ITA Online install
2. Apache resource settings	Apache	Create Apache status confirm resources	Create Apache status confirm resources
		Stop/Deactivate Apache service	Stop/Deactivate Apache service
3. ITA Service stop settings	-	Stop/Deactivate ITA Service	Stop/Deactivate ITA Service
4. EFS settings	EFS	Prepare EFS for usage	Prepare EFS for usage
		Common Directory settings	-
5. RDS Settings	RDS	RDS Data settings	-
		DB Connection settings	DB Connection settings
		Stop MariaDB	Stop MariaDB
		Uninstall MariaDB	Uninstall MariaDB
6. Prepare Pacemaker for us	-	Install awscil	Install awscil
		hosts settings	hosts settings
7. Pacemaker startup order	Pacemaker	Cluster settings	Cluster settings
		Resource settings	Resource settings
		Pacemaker startup order setting	Pacemaker startup order setting

Introduction

4. Linux-HA Cluster stack

- The Linux-HA cluster stack is a set of software aimed at improving server system availability and preventing data loss due to storage failure. The cluster is created of the 2 following softwares/packages.

Corosync

This software mutually monitors the server operations that makes up the HA Cluster.

Pacemaker

Pacemaker monitors the services provided by the HA Cluster and maintains the availability of the entire cluster by continuing services on other servers when the server that was providing the service goes down.

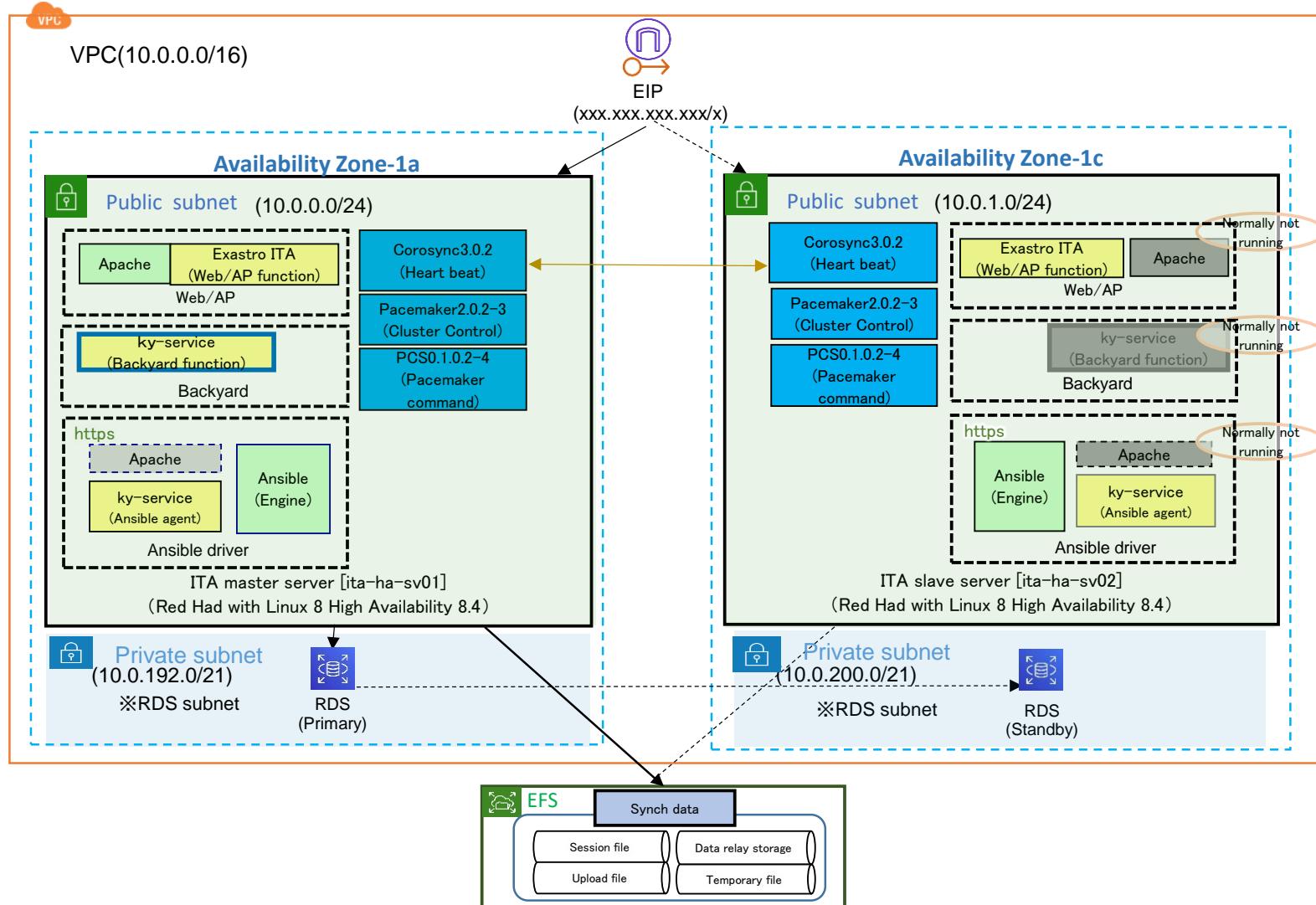
Reference URL:

<http://linux-ha.osdn.jp/wp/>

Introduction

5. System Configuration e: example

- The following figure displays the 2 ITA Cluster construction servers, the network configuration and the related programs.



Introduction

- Network conditions

- Normally, each network interface has its own IP address, but an additional IP address (ElasticIP address) is required to create the ITA server HA cluster. After being constructed, the prepared ElasticIP address will be automatically assigned to the master server side by Pacemaker.

- Network settings example

Network IF	Application	master server	slave server
ElasticIP	ITA connection	Automatically created global IP	
eth0	Local IP	10.0.0.204	10.0.1.61

※The Master server's local ip address is the local ip address configured when associating the ElasticIP Address.

- The following communication ports must be available from the client to the server.

Communication type	Port number
http	80/tcp
https	443/tcp

- Construct the cluster construction servers on the same network and make the following communication ports available.

Communication type	Port number
ssh(scp)	22/tcp
MYSQL/Aurora(RDS)	3306/tcp
NFS	2409/tcp
Pacemaker	2224,3121/tcp
Corosync	5404,5405/udp

※Pacemaker, Corosync port reference URL:

https://access.redhat.com/documentation/ja-jp/red_hat_enterprise_linux/7/html/high_availability_add-on_reference/s1火walls-haar

Introduction

6. Operation prerequisites

- The installation procedures for all software in this manual are written for online environments.
If you want to install them offline, please make sure that the software dependencies match those of the build server, and collect any libraries in advance.
- Before the construction procedure, please make sure that the following OS settings are configured.
Note that unless otherwise specified, the basic OS settings must be the same for both servers.
 - Deactivate SELinux
In order to operate an HA Cluster while SELinux is active, the user must have experience and knowledge regarding SELinux.
Since the procedure in this document has SELinux deactivated, If you want to activate SELinux, do it at your own risk.
- ITA Installation
 - For information regarding ITA Requirements, please refer to the following documents.
https://github.com/exastro-suite/it-automation-docs/raw/master/asset/Documents/Exastro-ITA_System_Configuration_Environment_Construction_Guide_Exastro-ITA_System_Configuration_Environment_Construction_Guide_Basic
1.1 Server requirements
https://github.com/exastro-suite/it-automation-docs/raw/master/asset/Documents/Exastro-ITA_System_Configuration_Environment_Construkcion_Guide_Exastro-ITA_System_Configuration_Enviroment_Construcion_Guide_Ansible-driver
3. System requirements

Introduction

- Installation requirements

Please refer to the all-in-one configuration installation manual.

You can use both the online and the offline ITA Installation manual.

<https://exastro-suite.github.io/it-automation-docs/learn.html#deploy>

This document assumes that the following standard install functions are activated.

```
ita_answers.txt function settings
ita_base:yes
material:no
createparam:yes
hostgroup:yes
ansible_driver:yes
cobbler_driver:no
terraform_driver:yes
```

This document assumes that you are installing ITA ver 1.7.x,
meaning that if you use a different version or are installing with different function setting values,
you might need to modify the contents of the target service in the following sections:

- Construction Procedure "3. ITA Service stop settings"

AWS Configuration manual

Here, we will explain the AWS Configuration process.
Please change user specific setting values, such as IP Addresses to your liking.

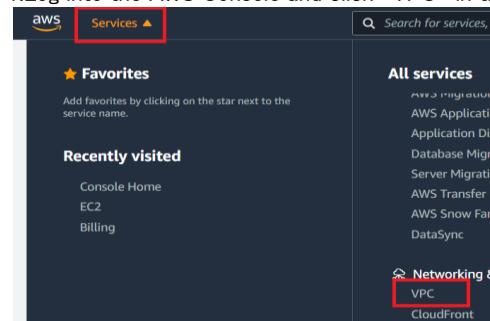
The services we will use are as following

List of services
1.VPC
2.Subnet
3.Internet Gateway
4.Route table
5.Security Group
6.IAM
7.RDS
8.EFS
9.Route53
10.EC2
11.ElasticIP

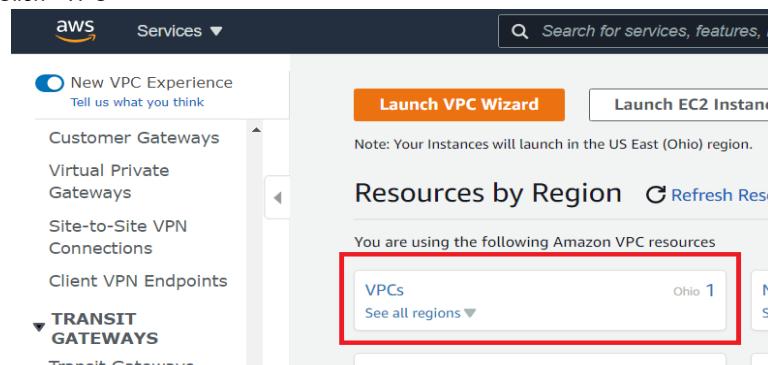
AWS Configuration manual

1.VPC

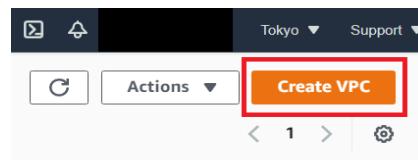
1.Log into the AWS Console and click "VPC" in the Service menu.



2.Click "VPC"



3.Click "Create VPC"



AWS Configuration manual

4.Input the necessary VPC Information

The screenshot shows the 'Create VPC' wizard. In the 'VPC settings' section, the 'Name tag - optional' field contains 'exastro-VPC' and the 'IPv4 CIDR block' field contains '10.0.0.0/16'. In the 'Tags' section, there is one tag named 'Name' with value 'exastro-VPC'. At the bottom right, the 'Create VPC' button is highlighted with a red border.

Example)

Name tag	IPv4 CIDR Block
exastro-VPC	10.0.0.0/16

5.Confirm that the VPC has been created

The screenshot shows the 'Details' tab of the VPC configuration page. It displays the VPC ID (vpc-0d3171fa1b8ae587e), State (Available), and other configuration details like DHCP options set, Main route table, and DNS resolution. Below this, the 'IPv4 CIDRs' section shows the assigned CIDR block (10.0.0.0/16) with status 'Associated'. The 'Actions' dropdown menu is visible at the top right.

AWS Configuration manual

6. Return to the screen in step 2 and click the "Edit DNS hostnames" from the action pulldown menu

The screenshot shows the AWS VPC console. A VPC named 'exastro-VPC' is selected. In the 'Actions' dropdown menu, the 'Edit DNS hostnames' option is highlighted with a red box.

7. Enable DNS hostnames and press "Save Changes"

The dialog is titled 'Edit DNS hostnames'. It contains a section for 'DNS hostnames' which includes a note: 'Indicates whether instances with public IP addresses get corresponding public DNS hostnames.' Below this is a table with a single row. The first column is 'VPC ID' with value 'vpc-0d3171fa1b8ae587e'. The second column is 'DNS hostnames' with a checkbox labeled 'Enable' which is checked. At the bottom right are 'Cancel' and 'Save changes' buttons, with 'Save changes' also highlighted with a red box.

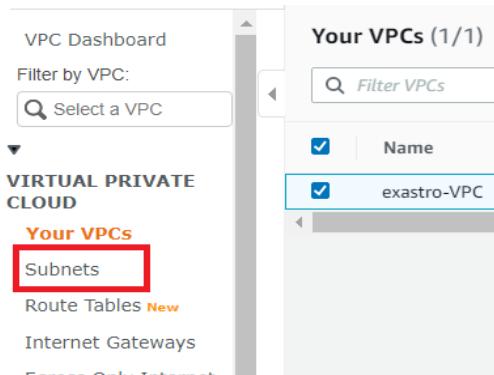
8. Check that the DNS hostnames is activated

This screenshot shows the detailed configuration of the 'exastro-VPC'. The 'DNS hostnames' section is expanded, showing it is set to 'Enabled'. Other visible settings include the VPC ID ('vpc-0d3171fa1b8ae587e'), State ('Available'), DHCP options set ('dopt-a5bb56c3'), Main route table ('rtb-00ad18cf6f3fb806e'), and Owner ID ('[REDACTED]').

AWS Configuration manual

2.Subnet

1.Go to the Subnet menu from the list on the left



2.Click the "Create Subnet" button



AWS Configuration manual

3. Select the VPC you created earlier and input subnet information

Create subnet [Info](#)

VPC

VPC ID
Contains targets in this VPC
vpc-0d3171fa1b8ae587e (exastro-VPC)

Associated VPC CIDRs
IPv4 CIDRs
10.0.0.0/16

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
public-a

Availability Zone Info
Asia Pacific (Tokyo) / ap-northeast-1a

IPv4 CIDR block Info
10.0.0.0/24

Tags - optional

Key Value - optional
Name public-a Remove
Enter key Enter value Remove
You must specify a tag key.
Add new tag
You can add 48 more tags.
Remove
Add new subnet

Cancel **Create subnet**

Example)

Subnet name	Availability zone	Ipv4 CIDR block
public-a	AsiaPacific (Tokyo)/ap-northeast-1a	10.0.0.0/24
public-c	AsiaPacific (Tokyo)/ap-northeast-1c	10.0.1.0/24
protect-rds-a	AsiaPacific (Tokyo)/ap-northeast-1a	10.0.192.0/21
protect-rds-c	AsiaPacific (Tokyo)/ap-northeast-1c	10.0.200.0/21

AWS Configuration manual

Subnet 2 of 3

Subnet name
Subnet name must be a unique name and is used to identify the subnet.

Availability Zone [Info](#)
The subnet must be located in the same Availability Zone as the VPC.

IPv4 CIDR block [Info](#)
The IPv4 CIDR block must be a valid IPv4 range and must not overlap with other subnets in the VPC.

Tags - optional

Key Value - optional

You can add 49 more tags.

Subnet 3 of 3

Subnet name
Subnet name must be a unique name and is used to identify the subnet.

Availability Zone [Info](#)
The subnet must be located in the same Availability Zone as the VPC.

IPv4 CIDR block [Info](#)
The IPv4 CIDR block must be a valid IPv4 range and must not overlap with other subnets in the VPC.

Tags - optional

Key Value - optional

You can add 49 more tags.

Subnet 4 of 4

Subnet name
Subnet name must be a unique name and is used to identify the subnet.

Availability Zone [Info](#)
The subnet must be located in the same Availability Zone as the VPC.

IPv4 CIDR block [Info](#)
The IPv4 CIDR block must be a valid IPv4 range and must not overlap with other subnets in the VPC.

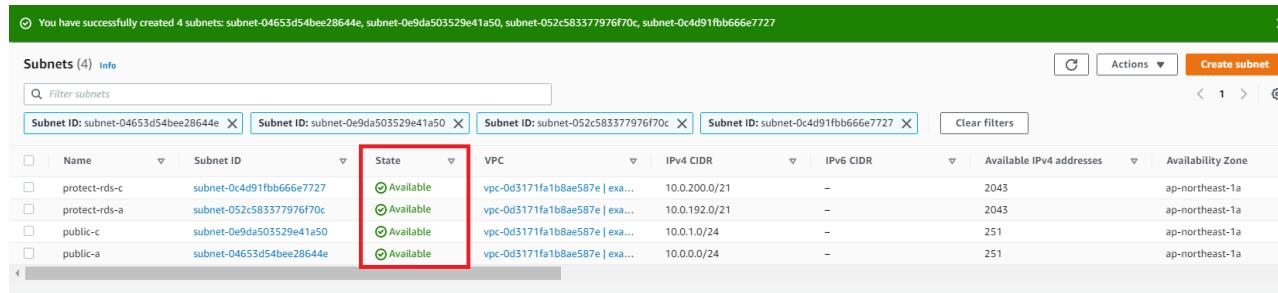
Tags - optional

Key Value - optional

You can add 49 more tags.

AWS Configuration manual

4.After creating it, check that it is available



The screenshot shows the AWS Subnets list interface. At the top, a green banner displays the message: "You have successfully created 4 subnets: subnet-04653d54bee28644e, subnet-0e9da503529e41a50, subnet-052c583377976f70c, subnet-0c4d91fb666e7727". Below this, the Subnets table lists four subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone
protect-rds-c	subnet-0c4d91fb666e7727	Available	vpc-0d3171fa1b8ae587e exa...	10.0.200.0/21	-	2043	ap-northeast-1a
protect-rds-a	subnet-052c583377976f70c	Available	vpc-0d3171fa1b8ae587e exa...	10.0.192.0/21	-	2043	ap-northeast-1a
public-c	subnet-0e9da503529e41a50	Available	vpc-0d3171fa1b8ae587e exa...	10.0.1.0/24	-	251	ap-northeast-1a
public-a	subnet-04653d54bee28644e	Available	vpc-0d3171fa1b8ae587e exa...	10.0.0.0/24	-	251	ap-northeast-1a

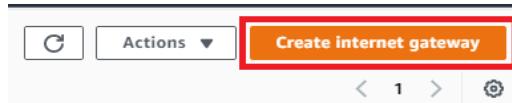
AWS Configuration manual

3. Internet Gateway

1. Go to the "Internet Gateway" menu from list on the left



2. Click the "Create Internet Gateway" button



AWS Configuration manual

3.Input the Internet Gateway information

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="exastro-gw"/> Remove

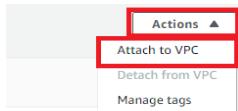
[Add new tag](#)
You can add 49 more tags.

[Cancel](#) [Create internet gateway](#)

Example)

Name tag exastro-gw

4.After creating the Internet Gateway, press the "Attach to VPC" button from the Action pulldown menu on the top right corner of the screen.

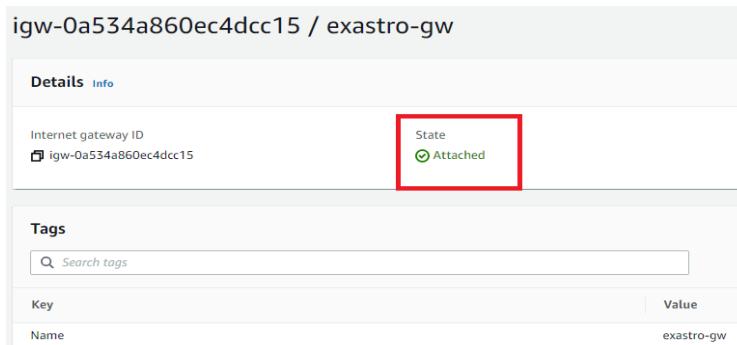


AWS Configuration manual

5. Select the VPC you created earlier and press the "Attach Internet Gateway" button



6. Check that the gateway is "Attached"



AWS Configuration manual

4.Route Tables

1. Go to the "Route Tables" menu from the list on the left

VIRTUAL PRIVATE CLOUD

Your VPCs

Subnets

Route Tables New

Internet Gateways

2. Use the search box to search with the VPC ID

Route tables (1/1) Info						
<input type="text" value="Filter route tables"/>		<input type="button" value="Clear filters"/>				
<input checked="" type="checkbox"/>	Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC
<input checked="" type="checkbox"/>	-	rtb-00ad18cf6f3fb806e	-	-	Yes	vpc-0d3171fa1b8ae587e exa...

AWS Configuration manual

3. Press the "Routes" tab under the target route table.

The screenshot shows the AWS Route Tables page with one route table listed. The 'Routes' tab is highlighted with a red box. The table details are as follows:

Name	Route table ID	Explicit subnet associat...	Main	VPC
-	rtb-00ad18cf6f5fb806e	-	-	Yes vpc-0d3171fa1b8ae587e exa...

Below the table, the 'Routes (1)' section is shown with one entry:

Destination	Target	Status
10.0.0.0/16	local	Active

4. Add Route information

The screenshot shows the 'Edit routes' dialog. A new route is being added with the following details:

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
Q 0.0.0.0/0	Q igw-0a534a860ec40cc15	-	No

The 'Add route' button is at the bottom left, and the 'Save changes' button is highlighted with a red box at the bottom right. The 'Cancel' and 'Preview' buttons are also visible.

AWS Configuration manual

5.Check that it has been added

The screenshot shows the AWS VPC Route Tables page for the route table `rtb-00ad18cf6f3fb806e`. The top navigation bar indicates that routes have been updated successfully. The main content area displays the route table details and its routes.

Route table details:

- Route table ID: `rtb-00ad18cf6f3fb806e`
- Main: Yes
- VPC: `vpc-0d3171fa1b8ae587e | exastro-VPC`
- Owner ID: [REDACTED]
- Explicit subnet associations: -

Routes (2):

Destination	Target	Status
10.0.0.0/16	local	Active
0.0.0.0/0	igw-0a534a860ec4dcc15	Active

AWS Configuration manual

5. Security Group

1. Go to the "Security Groups" menu from the list to the left



2. Click the "Create Security Group" button



3. Input the SecurityGroup Information

The screenshot shows the 'Create security group' configuration page. It includes fields for 'Group name' (exastro-sg), 'Description' (optional), and a VPC dropdown. Below these are sections for 'Inbound rules' and 'Outbound rules', both of which are highlighted with red boxes. The 'Inbound rules' section lists various port ranges and protocols, while the 'Outbound rules' section shows a single rule for 'All traffic'. At the bottom, there is a 'Create security group' button, which is highlighted with a red box.

Example)

Security group name	exastro-sg
VPC	exastro-vpc

Inbound rule

Type	Protocol	Port range	Source
SSH	TCP	22	My IP
HTTP	TCP	80	My IP
HTTPS	TCP	443	My IP
All ICMP-IPv4	IPv4	All	0.0.0.0/0
MySQL/Aurora	TCP	3306	0.0.0.0/0
NFS	TCP	2049	0.0.0.0/0
Custom UDP	UDP	5404-5405	0.0.0.0/0
Custom TCP	TCP	3121	0.0.0.0/0
CustomTCP	TCP	2224	0.0.0.0/0

Outbound rule

Type	Protocol	Port range	Source
All Traffic	All	All	0.0.0.0/0

AWS Configuration manual

4.Check that it has been created

The screenshot shows the AWS VPC Security Groups page. A success message at the top states "Security group 'sg-0cb4edaff5063fe40 - exastro-sg' was created successfully". Below this, the security group details are shown: Name is "exastro-sg", Description is "NFS share", and it is associated with the VPC "vpc-0c1317fb0dab5f7e". The Inbound rules section lists several rules, including NFS, HTTP, and MySQL. The Outbound rules section lists All traffic. At the bottom, there are tabs for "Inbound rules", "Outbound rules", and "Tags".

5.Create security group for RDS and EFS.

The screenshot shows the "Create security group" wizard for EFS. In the "Basic details" step, the security group name is "efs" and the description is "for EFS". In the "Inbound rules" step, an NFS rule is added with TCP protocol, port range 2049, and source 0.0.0.0/0. In the "Outbound rules" step, all traffic is allowed with All protocol, All port range, and destination 0.0.0.0/0.

The screenshot shows the "Create security group" wizard for RDS. In the "Basic details" step, the security group name is "rds" and the description is "for RDS". In the "Inbound rules" step, a MySQL/Aurora rule is added with TCP protocol, port range 3306, and source 0.0.0.0/0. In the "Outbound rules" step, all traffic is allowed with All protocol, All port range, and destination 0.0.0.0/0.

Example

Security Group name	exastro-efs
VPC	exastro-vpc

Inbound Rule

Type	Protocol	Port range	Source
NFS	TCP	2049	0.0.0.0/0

Outbound rule

Type	Protocol	Port range	Source
All traffic	All	All	0.0.0.0/0

Example)

Security group name	exastro-rds
VPC	exastro-vpc

Inbound Rule

Type	Protocol	Port range	Source
MySQL/Aurora	TCP	3306	0.0.0.0/0

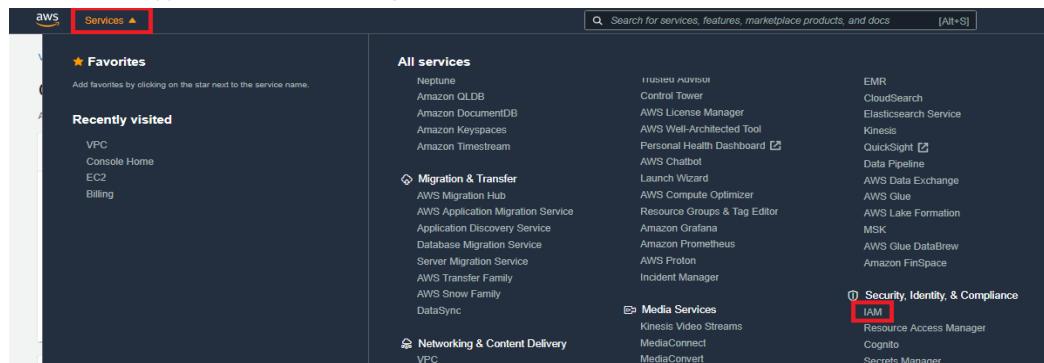
Outbound Rule

Type	Protocol	Port range	Source
All Traffic	All	All	0.0.0.0/0

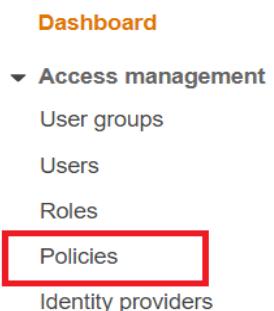
AWS Configuration manual

6.IAM

1.From the upper left "Service" list, go to "IAM"



2.Click the "Policy" button on the left



3.Click the "Create Policy" button



AWS Configuration manual

4. Open up the JSON tab and input the policy

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor **JSON** Import managed policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "ec2:Describe*",  
8         "ec2:DisassociateAddress",  
9         "ec2:AssociateAddress"  
10      ],  
11      "Resource": [  
12        "*"  
13      ]  
14    }  
15  ]  
16}  
17
```

Character count: 150 of 6,144 [Cancel](#) **Next: Tags**

Example)

Policy Contents

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "ec2:Describe*",  
        "ec2:DisassociateAddress",  
        "ec2:AssociateAddress"  
      ],  
      "Resource": [  
        "*"  
      ]  
    }  
  ]  
}
```

5. Click the “Next: Review” button



AWS Configuration manual

6.Input a Policy name and click the "Create Policy" button

Review policy

Name* exastro-policy
Use alphanumeric and '-' characters. Maximum 128 characters.

Description

Maximum 1000 characters. Use alphanumeric and '-' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 285 services) Show remaining 284	EC2	Limited: List, Read, Write	All resources
			None

Tags

Key	Value
No tags associated with the resource.	

* Required Cancel Previous Create policy

Example)

Name
exastro-policy

7.Check that it has been created

The policy exastro-policy has been created.

IAM > Policies

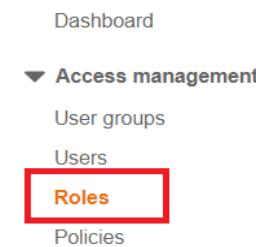
Policies (832) [Info](#)
A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter

Policy Name	Type
exastro-policy	Customer managed

AWS Configuration manual

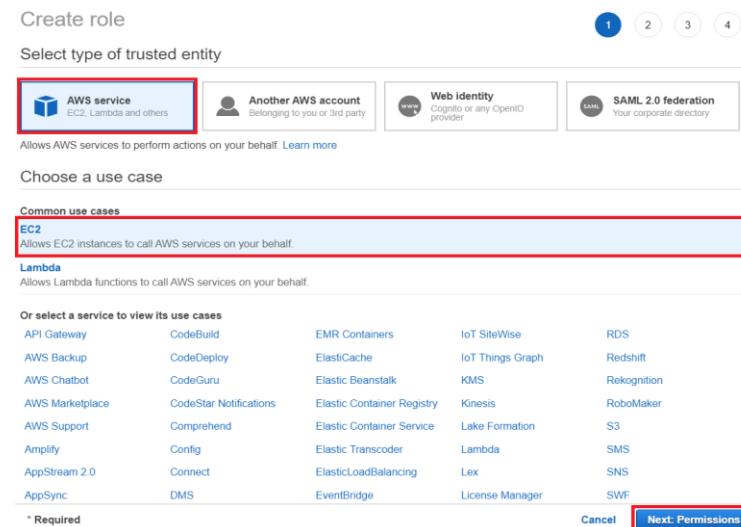
8.Go to the “Roles” menu from the list to the left



9.Click the “Create Role” button



10.Select “AWS Service” and “EC2” and click “Next: Permissions”.



AWS Configuration manual

11.Check the policy we created earlier and click "Next: tabs"

Create role

1 2 3 4

Attach permissions policies

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

Create policy

Filter policies ▾

Showing 1 result

Policy name	Used as
<input checked="" type="checkbox"/> exastro-policy	None

Set permissions boundary

12.Click the "Next: Review" button

Create role

1 2 3 4

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	<input type="button" value="Remove"/>

You can add 50 more tags.

Cancel Previous **Next: Review**

AWS Configuration manual

13 Input the role name and confirm that the selected Policy is there. If yes, Click the "Create Role" button.

Create role

Review

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

Role name* exastro-role
Use alphanumeric and '+=_,@_-' characters. Maximum 64 characters.

Role description Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and '+=_,@_-' characters.

Trusted entities AWS service: ec2.amazonaws.com

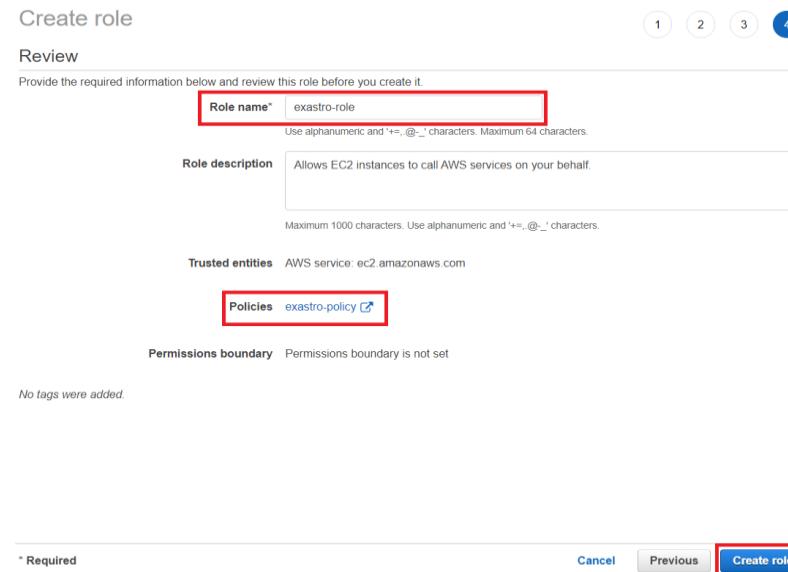
Policies exastro-policy 

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

Cancel Previous Create role



Example)

Role Name	exastro-role
Policy	exastro-policy

14.Check that the Role is there

Search

Role name

exastro-role



AWS Configuration manual

15.Go to the "User" menu from the list on the left

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

16.Click the "Add Users" button



Check the "Programmatic access" box and click "Next: Permissions"

Add user

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name* exastro-user

Add another user

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Programmatic access
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

AWS Management Console access
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

Cancel **Next: Permissions**

Example)

Username	exastro-user
Access type	Programmatic access

AWS Configuration manual

18. Select "Attach existing policies directly" and check the policy we created earlier. After that, press "Next: tags".

Add user

1 2 3 4 5

▼ Set permissions

The screenshot shows the 'Set permissions' step of the AWS IAM 'Add user' wizard. At the top, there are three options: 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly'. The third option is highlighted with a red box. Below this is a search bar with 'Filter policies' and a dropdown set to 'Showing 1 result'. A table lists a single policy: 'exastro-policy'. The table has columns for 'Policy name', 'Type', and 'Used as'. The 'Policy name' column shows 'exastro-policy' with a checked checkbox and a right-pointing arrow. The 'Type' column shows 'Customer managed'. The 'Used as' column shows 'Permissions policy (1)'. Both the policy name row and the entire table row are highlighted with a red box.

▶ Set permissions boundary

Cancel Previous Next: Tags

19. Press "Next step: Confirm"

Cancel Previous Next: Review

AWS Configuration manual

20. Confirm that the information is correct and press "Create user".

Add user

1 2 3 4 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	exastro-user
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	exastro-policy

Tags

No tags were added.

Cancel Previous Create user

21. Download the csv. ※We will use this when configuring the server



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.

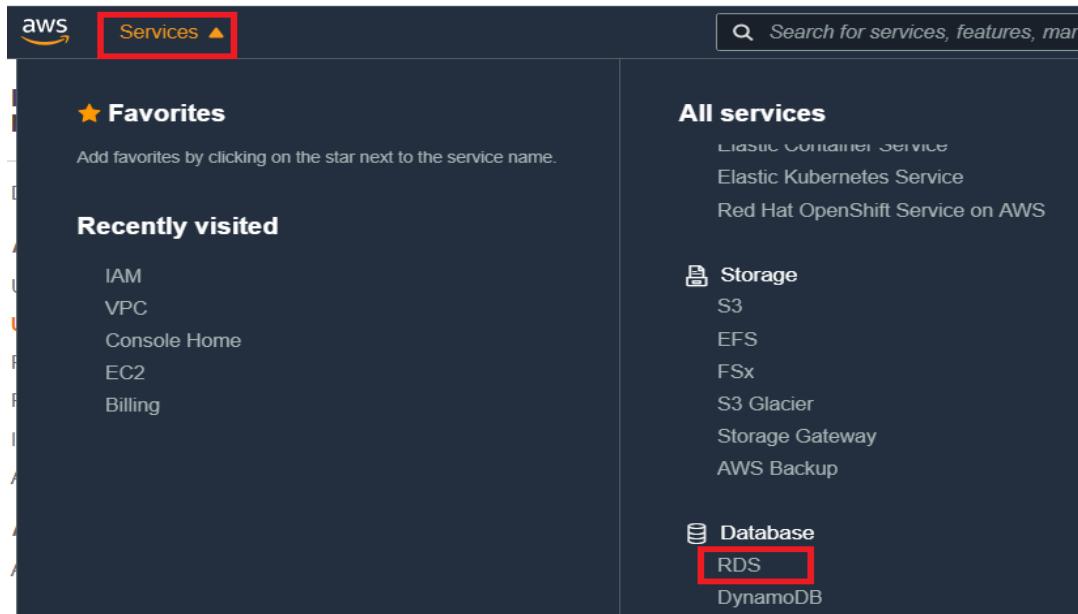
Users with AWS Management Console access can sign-in at: <https://511888867184.signin.aws.amazon.com/console>

Download .csv

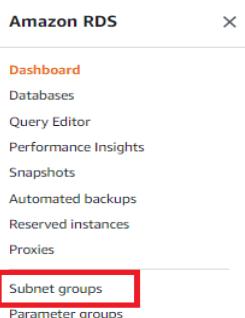
AWS Configuration manual

7.RDS

1.From the upper left "Service" list, go to "RDS"



2.Go to the "Subnet groups" menu from the list on the left



AWS Configuration manual

3.Click "Create DB Subnet group"



4.Input the DB Subnet group information and press "Create"

Create DB Subnet Group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

Subnet group details

Name	exastrodb-subnet
Description	rds-subnet
VPC	exastro-VPC (vpc-0d5171fa1b8ae587e)

Add subnets

Availability Zones	ap-northeast-1a, ap-northeast-1c
Subnets	subnet-02b6f5cfb55ecb2a7 (10.0.200.0/21), subnet-0128931eb48f85bbf (10.0.192.0/21)

Subnets selected (2)

Availability zone	Subnet ID	CIDR block
ap-northeast-1a	subnet-0128931eb48f85bbf	10.0.192.0/21
ap-northeast-1c	subnet-02b6f5cfb55ecb2a7	10.0.200.0/21

Cancel **Create**

This form is used to create a DB Subnet Group. It includes fields for Name (exastrodb-subnet), Description (rds-subnet), and VPC (exastro-VPC). The 'Add subnets' section shows selected Availability Zones (ap-northeast-1a, ap-northeast-1c) and Subnets (subnet-02b6f5cfb55ecb2a7, subnet-0128931eb48f85bbf). A summary table at the bottom lists the selected subnets by availability zone, subnet ID, and CIDR block. The 'Create' button is highlighted with a red border.

Example)

Name	exastrodb-subnet
Description	rds-subnet
VPC	exastro-VPC
Availability	ap-northeast-1a ap-northeast-1c
Subnet	subnet-097fba3cefd69f30 (10.0.192.0/21) subnet-061dbddaa51760b21d (10.0.200.0/21)

AWS Configuration manual

5.Click the Parameter group on the right and press "Create Parameter Group"



6.Select the Parameter Group family, input the Group name and press the "Create" button ※Description is optional

Create parameter group

Parameter group details

Parameter group family
DB family that this DB parameter group will apply to

Group Name
Identifier for the DB parameter group

Description
Description for the DB parameter group

Example)

Parameter group family	mariadb10.5
Group name	exastro-param

7.Confirm that it has been created

RDS > Parameter groups	
Parameter groups	
	Info
<input type="radio"/> Custom	<input type="radio"/> Default
Custom parameter groups (1)	
<input type="button" value="Filter custom parameter groups"/>	
<input type="checkbox"/> Name	<input type="text" value="Family"/>
<input type="checkbox"/> exastro-param	mariadb10.5

8.Click the Parameter group you created and start configure the Parameter settings ※Make sure that you click "Save changes" everytime you change something

Modify parameter group

Modifiable parameters (418)

Name	Value	Apply type	Data type	Source
explicit_defaults_for_timestamp	1	Static	Boolean	Modified

Modify parameter group

Modifiable parameters (418)

Name	Value	Apply type	Data type	Source
tx_isolation	READ-COMMITTED	Dynamic	String	Engine default

AWS Configuration manual

Modify parameter group

Modifiable parameters (418)

Q innodb_buffer_pool_size

Name	Value	Apply type	Data type	Source
innodb_buffer_pool_size	536870912	Dynamic	Integer	System default

Cancel Continue

Modify parameter group

Modifiable parameters (418)

Q innodb_log_buffer_size

Name	Value	Apply type	Data type	Source
innodb_log_buffer_size	67108864	Static	Integer	System default

Allowed values 261144-423967295

Cancel Continue

Modify parameter group

Modifiable parameters (418)

Q min_examined_row_limit

Name	Value	Apply type	Data type	Source
min_examined_row_limit	100	Dynamic	Integer	Engine default

Allowed values 0-18446744073709551615

Cancel Continue

Modify parameter group

Modifiable parameters (418)

Q join_buffer_size

Name	Value	Apply type	Data type	Source
join_buffer_size	134217728	Dynamic	Integer	Engine default

Allowed values 16384-18446744073709551615

Cancel Continue

Modify parameter group

Modifiable parameters (418)

Q query_cache_size

Name	Value	Apply type	Data type	Source
query_cache_size	536870912	Dynamic	Integer	Engine default

Allowed values 192-5242880-18446744073709551615

Cancel Continue

Modify parameter group

Modifiable parameters (418)

Q query_cache_type

Name	Value	Apply type	Data type	Source
query_cache_type	1	Static	Integer	Engine default

Allowed values 0-2

Cancel Continue

Modify parameter group

Modifiable parameters (418)

Q max_heap_table_size

Name	Value	Apply type	Data type	Source
max_heap_table_size	67108864	Dynamic	Integer	Engine default

Allowed values 16384-18446744073709551615

Cancel Continue

Modify parameter group

AWS Configuration manual

The screenshot shows the AWS RDS Modify Parameter Group interface. It consists of four stacked configuration steps:

- Step 1: tmp_table_size**
Parameter: tmp_table_size
Value: 67108864
- Step 2: mrr_buffer_size**
Parameter: mrr_buffer_size
Value: 67108864
- Step 3: max_connections**
Parameter: max_connections
Value: 256
- Step 4: character_set_server**
Parameter: character_set_server
Value: utf8

Each step has a "Continue" button at the bottom right.

Parameter	Value
explicit_defaults_for_timestamp	1
tx_isolation	READ-COMMITTED
innodb_buffer_pool_size	536870912
innodb_log_buffer_size	67108864
min_examined_row_limit	100
join_buffer_size	134217728
query_cache_size	536870912
query_cache_type	1
max_heap_table_size	67108864
tmp_table_size	67108864
mrr_buffer_size	67108864
max_connections	256
character_set_server	utf8

AWS Configuration manual

9.After you've saved, click the "Create Database" from the Dashboard in the menu on the left.



10.Create RDS

Create database

The configuration page includes sections for 'Choose a database creation method', 'Engine options' (with MariaDB selected), 'Version' (set to MariaDB 10.5.8), and 'Templates' (Production selected).

※Field without examples can be left with the default value (Make sure to check Example)

Creation method	Standard create
Engine option	MariaDB
Version	MariaDB 10.5.8
Template	Production
DB Instance identifier	exastro-rds
Master user name	admin
Availability and Durability	Create a standby instance
VPC	exastro-VPC
Subnet Group	exastrodb-subnet
Public access	No
VPC Security group	Choose existing exastro-rds
Database port	3306
DB Parameter group	exastro-param
Option group	defaultmariadb-10.5
Backup	Enable automated backups
Monitoring	Enable Enhanced monitoring
Log exports	Audit log Error log General log Slow query log
Select window	Saturday 03:00 0.5 hours

AWS Configuration manual

Region: exastro-rds

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "HyphenBalance"). Constraints: 1 to 60 alphanumeric characters or hyphens. First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

Credentials Settings

Master username: admin

Master password: *********

Confirm password: *********

DB instance class

DB instance class: db.m6g.large

Standard classes (includes m classes)

Memory optimized classes (includes r and x classes)

Burstable classes (includes t classes)

Include previous generation classes

Storage

Storage type: Provisioned IOPS (SSD)

Allocated storage: 100 GiB

Provisioned IOPS: 3000 IOPS

Storage autoscaling

Enable storage autoscaling

Maximum storage threshold: 1000 GiB

Availability & durability

Multi-AZ deployment:

- Create a standby instance (recommended for production usage)
Creates a standby in a different Availability Zone (AZ) to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups.
- Do not create a standby instance

Connectivity

AWS Configuration manual

Virtual private cloud (VPC) [Info](#)
VPC that defines the virtual networking environment for this DB instance.

exastro-VPC (vpc-09dbe5341dd5c2c0)

Only VPCs with a corresponding DB subnet group are listed.

ⓘ After a database is created, you can't change the VPC selection.

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

exastrodb-subnet

Public access [Info](#)
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that Amazon EC2 instances and devices inside the VPC can connect to the database.

Yes
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that Amazon EC2 instances and devices inside the VPC can connect to the database.

No
No IP with not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group
Choose a VPC security group to allow access to your database. Ensure that the security group rules allow the appropriate incoming traffic.

Choose existing
Choose existing VPC security groups

Create new
Create new VPC security group

Existing VPC security groups
Choose VPC security groups

exastro-rds default

▼ Additional configuration

Database port [Info](#)
TCP/IP port that the database will use for application connections.

3306

▼ Additional configuration

Database options

Initial database name [Info](#)

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)
exastro-param

Option group [Info](#)
default:mariadb-10-5

Backup

Enable automated backups
Creates a point-in-time snapshot of your database

Backup retention period [Info](#)
Choose the number of days that RDS should retain automatic backups for this instance.

7 days

Backup window [Info](#)
Select the period for which you want automated backups of the database to be created by Amazon RDS.

Select window

No preference

Copy tags to snapshots

Encryption

Enable encryption
Choose to encrypt the given instance. Master key IDs and aliases appear in the list after they have been created using the AWS Key Management Service console.

AWS KMS Key [Info](#)
(default) aws/rds

AWS Configuration manual

Account
943001175239

KMS key ID
a75ddb74-38e3-4254-8607-d2a2bea62356

Performance Insights [Info](#)
 Enable Performance Insights
Retention period [Info](#)

AWS KMS Key [Info](#)

Account
943001175239

KMS key ID
a75ddb74-38e3-4254-8607-d2a2bea62356

⚠ You can't change the KMS key after enabling Performance Insights.

Monitoring
 Enable Enhanced monitoring
Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU

Granularity
60 seconds

Monitoring Role
default

Clicking "Create database" will authorize RDS to create the IAM role rds-monitoring-role

Log exports
Select the log types to publish to Amazon CloudWatch Logs
 Audit log
 Error log
 General log
 Slow query log

IAM role
The following service-linked role is used for publishing logs to CloudWatch Logs.
RDS service-linked role

ⓘ Ensure that general, slow query, and audit logs are turned on. Error logs are enabled by default. [Learn more](#)

Maintenance
Auto minor version upgrade [Info](#)
 Enable auto minor version upgrade
Enabling auto minor version upgrade will automatically upgrade to new minor versions as they are released. The automatic upgrades occur during the maintenance window for the database.

Maintenance window [Info](#)
Select the period you want pending modifications or maintenance applied to the database by Amazon RDS.
 Select window
 No preference

Start day Saturday
Start time 03 : 00 UTC
Duration 0.5 hours

Deletion protection
 Enable deletion protection
Protects the database from being deleted accidentally. While this option is enabled, you can't delete the database.

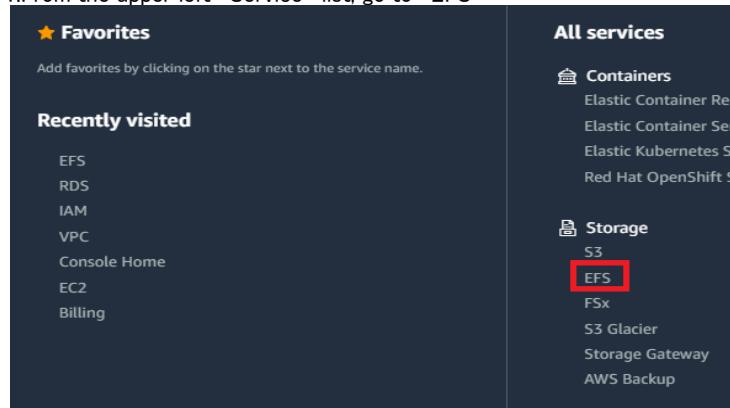
Check that the RDS has been created and it can be used ※This might take some time

Databases											<input type="checkbox"/> Group resources	<input type="button" value=""/>	<input type="button" value="Modify"/>	<input type="button" value="Actions"/>	<input type="button" value="Restore from S3"/>	<input type="button" value="Create database"/>					
<input type="button" value="Filter databases"/>																					
	<input type="checkbox"/>	DB identifier	▲	Role	▼	Engine	▼	Region & AZ	▼	Size	▼	Status	▼	CPU	Current activity	Maintenance	▼	VPC	▼	Multi-AZ	▼
	<input type="radio"/>	exastro-rds		Instance		MariaDB		ap-northeast-1c		db.m6g.large		Available		<div style="width: 2.52%; background-color: #0070C0;"></div> 2.52%	<div style="width: 0%; background-color: #00A0A0;"></div> 0 Sessions	none		vpc-09dbe5341dd5c28c0	Yes		

AWS Configuration manual

8.EFS

1.From the upper left "Service" list, go to "EFS"



2.Click the "Create File system" button

Create file system

Create an EFS file system with service recommended settings.

Create file system

AWS Configuration manual

3. Input name, select the VPC you created and the Region. After that, click the "Customize" button.

Create file system

Create an EFS file system with service recommended settings. [Learn more](#)

Name - optional
Name your file system.

Name must not be longer than 256 characters, and must only contain letters, numbers, and these characters: + - = . _ : /

Virtual Private Cloud (VPC)
Choose the VPC where you want EC2 instances to connect to your file system. [Learn more](#)

exastro-VPC

Availability and Durability
Choose Regional (recommended) to create a file system using regional storage classes. Choose One Zone to create a file system using One Zone storage classes. [Learn more](#)

Regional
Stores data redundantly across multiple AZs

One Zone
Stores data redundantly within a single AZ

[Cancel](#) [Customize](#) [Create](#)

Example)

Name - Option	exastro-efs
VPC	exastro-VPC
Availability and Durability	Regional

AWS Configuration manual

4. Make sure that Automatic backups is enabled. select the VPC you created earlier and add the Security group for EFS you created earlier. After that, press General

Name - optional
Name your file system:
exastro-efs

Availability and Durability
Choose Regional (recommended) to create a file system using regional storage classes. Choose One Zone to create a file system using One Zone storage classes. Learn more [\[?\]](#)

Regional
Stores data redundancy across multiple AZs

One Zone
Stores data redundancy within a single AZ

Automatic backups
Automatically backup your file system data with AWS Backup using recommended settings. Additional pricing applies. Learn more [\[?\]](#)

Enable automatic backups

Lifecycle management
Automatically save money as access patterns change by moving files into the Standard - Infrequent Access storage class. Learn more [\[?\]](#)

30 days since last access

Performance mode
Set your file system's performance mode based on IOPS required. Learn more [\[?\]](#)

General Purpose
Ideal for latency-sensitive use cases, like web serving environments and content management systems

Max I/O
Scale to higher levels of aggregate throughput and operations per second

Throughput mode
Set how your file system's throughput limits are determined. Learn more [\[?\]](#)

Bursting
Throughput scales with file system size

Provisioned

Encryption
Choose to enable encryption of your file system's data at rest. Uses the AWS KMS service key (aws/elasticfilesystem) by default. Learn more [\[?\]](#)

Enable encryption of data at rest

Customize encryption settings

Network access

Virtual Private Cloud (VPC)
Select the VPC that contains your file system. Learn more [\[?\]](#)

vpc-0960be5541d65c28e0
selected

Mount targets
A mount target provides an IP endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. Learn more [\[?\]](#)

Availability zone	Subnet ID	IP address
ap-northeast-1a	subnet-031f188a7c2e205	Automatic
ap-northeast-1c	subnet-02cc4eaef47abf190	Automatic

Security groups
Choose security groups

sg-00d09125509112ca4 X
default

sg-0ff9f27202fbabc X
exastro-efs

Show less

sg-00d09125509112ca4 X
default

sg-0ff9f27202fbabc X
exastro-efs

Show less

Add mount target

Cancel Previous Next

Example)

Network	exastro-VPC
Security Group	exastro-efs

AWS Configuration manual

5.Press "Next"

File system policy - optional

Policy options

Select one or more of these common policy options, or create a custom policy using the editor.

Learn more [\[?\]](#)

- Prevent root access by default*
- Enforce logging activity by default*
- Prevent anonymous access
- Enforce in-transit encryption for all clients

* Identity-based policies can override these default permissions.

Grant additional permissions

Policy editor (JSON)

```
1
```

Manual changes will prevent the use of the policy options on the left until the editor is cleared.

Cancel Previous Next

6.Confirm the contents and press the "Next" button

Review and create

Step 1: File system settings

File system

Field	Value	Is editable?
Name	exastro-efs	Yes
Performance mode	General Purpose	No
Throughput mode	Bursting	Yes
Encrypted	Yes	No
KMS Key ID	-	No
Lifecycle policy	30 days since last access	Yes
Automatic backups	Yes	Yes
VPC ID	vpc-09dbe5341dd5c28c0 (exastro-VPC)	Yes
Availability Zone	Regional	No

Tags

Tag key Tag value

No tags associated with this resource

Manage tags

Step 2: Network access

Mount targets

Availability zone	Subnet	IP address	Security groups
ap-northeast-1a	subnet-031fc186b7c1e20f5	-	sg-0df69f27b202f8abc, sg-0x0c9125f091f2ca4
ap-northeast-1c	subnet-02cc4ae6f47c8f190	-	sg-0df69f27b202f8abc, sg-0x0c9125f091f2ca4

Step 3: File system policy

File system policy

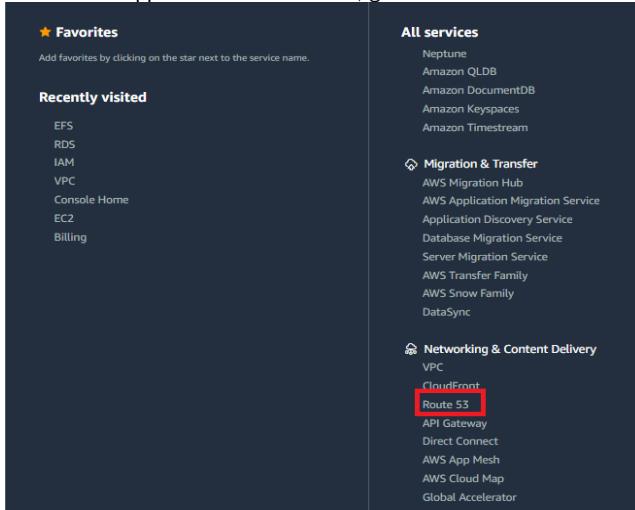
```
1
```

Cancel Previous Create

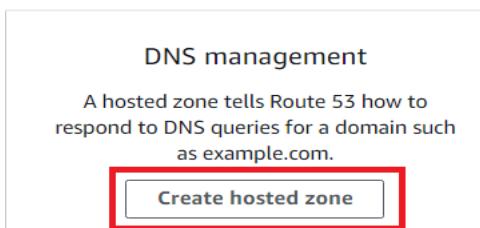
AWS Configuration manual

9.Route53

1.From the upper left "Service" list, go to "Route54"



2.Press the "Create Hosted zone" button



AWS Configuration manual

3. Input the Domain name, check the Private Host Zone, Select the Tokyo relation and VPC and then press "Create Host Zone".

Create hosted zone [Info](#)

Hosted zone configuration
A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name [Info](#)
This is the name of the domain that you want to route traffic for.
 exastro-aws.local
Valid characters: a-z, 0-9, ! * # \$ % & ^ () * + , - / ; < = > ? @ [\] ^ _ ` { } , ~

Description - optional [Info](#)
This value lets you distinguish hosted zones that have the same name.

The description can have up to 256 characters. 4/256

Type [Info](#)
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.
 Public hosted zone
A public hosted zone determines how traffic is routed on the internet.
 Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC. Private hosted zone

VPCs to associate with the hosted zone [Info](#)
To use this hosted zone to resolve DNS queries for one or more VPCs, choose the VPCs. To associate a VPC with a hosted zone when the VPC was created using a different AWS account, you must use a programmatic method, such as the AWS CLI.

For each VPC that you associate with a private hosted zone, you must set the Amazon VPC settings enableDnsHostnames and enableDnsSupport to true.

Region [Info](#) VPC ID [Info](#)
 Asia Pacific (Tokyo) [ap-northeast-1] vpc-09dbe5341dd5c28c0 X Remove VPC

Add VPC

Tags [Info](#)
Apply tags to hosted zones to help organize and identify them.

No tags associated with the resource.

Add tag

You can add up to 50 more tags.

Cancel Create hosted zone

Example)

Domain name	exastro-aws.local
Type	Private hosted zone
Relation	Asia Pacific (Tokyo) [ap-northeast-1]
VPC ID	vpc-09dbe5341dd5c28c0

4. Press the "Create Record" button

Records (2) Hosted zone tags (0)

Records (2) [Info](#)
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

Create record

Record name	Type	Routin...	Differ...	Value/Route traffic to
exastro-aws.local	NS	Simple	-	ns-1516.awdns-00.co.uk. ns-0.awdns-00.com. ns-1024.awdns-00.org. ns-512.awdns-00.net.
exastro-aws.local	SOA	Simple	-	ns-1516.awdns-00.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

AWS Configuration manual

5.Select Record name and CNAME and then input the RDS Endpoint value.

Route 53 > Hosted zones > exastro-aws.local > Create record

Quick create record [Info](#) [Switch to wizard](#) [Add another record](#)

Record name [Info](#) rds.exastro-aws.local [Delete](#)

Record type [Info](#) CNAME – Routes traffic to another domain n... [Value](#) [Info](#) Alias exastro-rds.chatwnliry.ap-northeast-1.rds.amazonaws.com
Valid characters: a-z, 0-9, ! # \$ % & ') * + , - / ; < = > ? @ [\] ^ _ { } . ~ Enter multiple values on separate lines.

TTL (seconds) [Info](#) 300 [Delete](#)

Routing policy [Info](#) Simple routing [Delete](#)

1m 1h 1d [Delete](#)

Recommended values: 60 to 172800 (two days)

[Cancel](#) [Create records](#)

Example)

Record name	rds
Record type	CNAME
Value	RDS End point

6.Select Record name and CNAME and then input the EFS Endpoint value.

Quick create record [Info](#) [Switch to wizard](#) [Add another record](#)

Record name [Info](#) efs.exastro-aws.local [Delete](#)

Record type [Info](#) CNAME – Routes traffic to another domain n... [Value](#) [Info](#) Alias fs-9d4dc2bd.efs.ap-northeast-1.amazonaws.com
Valid characters: a-z, 0-9, ! # \$ % & ') * + , - / ; < = > ? @ [\] ^ _ { } . ~ Enter multiple values on separate lines.

TTL (seconds) [Info](#) 300 [Delete](#)

Routing policy [Info](#) Simple routing [Delete](#)

1m 1h 1d [Delete](#)

Recommended values: 60 to 172800 (two days)

[Cancel](#) [Create records](#)

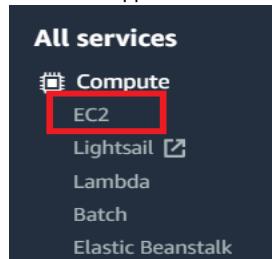
Example)

Record name	efs
Record type	CNAME
Value	EFS End point

AWS Configuration manual

10.EC2

1.From the upper left "Service" list, go to "EC2"



2.Click "Launch Instance"

A screenshot of the AWS EC2 'Launch instance' page. The 'Launch instance' button is highlighted with a red box. The page shows resource statistics and various configuration options for launching an instance.

3.Input "Red Hat Enterprise Linux 8.4 with High Availability" in the search box and select it. ※Select the image with Pacemaker, Corosync and pcs already

A screenshot of the AWS Marketplace search results. A specific item, 'Red Hat Enterprise Linux 8.4 with High Availability', is highlighted with a red box. The search bar at the top also contains the search term.

AWS Configuration manual

4. Select Size ※Make sure that it meets the Exastro Minimum specs

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized for different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they're used for running workloads.

Filter by: All instance families • Current generation • Show Hide Columns

Currently selected: t3.small | 1 vCPU, 2.0 GiB, ~2.0 memory, EBS only

Note: The vendor recommends using a large instance or larger for the best experience with this product.

Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS Optimized Available	Network Performance	IPv4 Support
t3	t3.nano	1	0.5	EBS only	-	Low to Moderate	Yes
t3	t3.small	1	1	EBS only	-	Low to Moderate	Yes
t3	t3.medium	2	2	EBS only	-	Low to Moderate	Yes
t3	t3.large	4	8	EBS only	-	Low to Moderate	Yes
t3	t3.xlarge	8	16	EBS only	-	Moderate	Yes
t3	t3.2xlarge	2	32	EBS only	-	Moderate	Yes
t3	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.small	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.medium	2	2	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.large	4	4	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.xlarge	8	8	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3.2xlarge	16	16	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3a.small	2	1	EBS only	Yes	Up to 5 Gigabit	Yes
t3	t3a.medium	2	2	EBS only	Yes	Up to 5 Gigabit	Yes

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

5. Select the created VPC, Public Subnet, Automatically assigned Public IP, created IAM Role and press the "Next: Add storage".

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 Fixed instances

Network: exastro-VPC Create new VPC
Subnet: public-a Create new subnet

Auto-assign Public IP: Enabled

Placement group: Add instance to placement group
Capacity Reservation: Open

Domain join directory: /etc/hostname Create new directory
IAM role: exastro-role Create new IAM role

CPU options: Specify CPU options

Shutdown behavior: Stop Terminate
Stop/terminate behavior: Stop Terminate
Enable termination protection: Protect against accidental termination
Monitoring: Enable CloudWatch detailed monitoring
Additional charges apply

EBS-optimized instance: Dedicated Shared For a shared-baseline instance
Tenancy: Shared Additional charges will apply for dedicated tenancy
Elastic Inference: Add an Elastic Inference accelerator
Additional charges apply

Credit specification: Unlimited
Additional charges may apply

File systems: Add file system Create new file system

Network interfaces: Device: Network interface: Subnet: Primary IP: Secondary IP: IPv4 Prefixes: IPv6 Prefixes:

Add Device: Network interface: Subnet: Primary IP: Secondary IP: IPv4 Prefixes: IPv6 Prefixes:

Advanced Details: Enclose: Enable
Metadata accessibility: Enabled
Metadata version: V1 and V2 (both optional)
Metadata token response timeout: 10s
User data: As text As URL Input is already base64 encoded

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

Example)

Ita-ha-sv01	Network	exastro-VPC
	Subnet	public-a
	Auto-assign public IP	Activate
	IAM Role	exastro-role
	Security Group	exastro-sg

Example)

Ita-ha-sv02	Network	exastro-VPC
	Subnet	public-c
	Auto-assign public IP	Activate
	IAM Role	exastro-role
	Security Group	exastro-sg

AWS Configuration manual

6. Click "Next: Add Tags"

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more about storage options in Amazon EC2](#)

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (Mbps)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0c2aa1e396810460	10	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about the usage tier eligibility and usage restrictions.

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

7.Click "Next: Configure Security Group"

Step 5: Add Tags

A tag consists of a key and a descriptive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more about tagging your Amazon EC2 resources](#).

Key	(256 characters maximum)	Value	(256 characters maximum)	Instances	Volumes	Network Interfaces
This resource currently has no tags.						

Choose the Add tag button or click to add a Name tag.
Make sure your IAM policy includes permissions to create tags.

[Add Tag](#) (Up to 50 tags maximum)

Cancel Previous Review and Launch **Next: Configure Security Group**

AWS Configuration manual

8.Select the security group you created and click the "Review and launch" button

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 ID	Name	Description	Actions
sg-0d0c91250912ca4	default	default VPC security group	Copy to new Copy to new Copy to new
sg-0df9f92fb2028abc	exastro-efs	exastro-vpc	Copy to new Copy to new Copy to new
sg-04e516265564a97e	exastro-rds	test	Copy to new Copy to new Copy to new
sg-0c4e830313c3e3dc1	exastro-sg	test	Copy to new Copy to new Copy to new

Inbound rules for sg-0c4e830313c3e3dc1 (Selected security groups: sg-0c4e830313c3e3dc1)					
Type	Protocol	Port Range	Source	Description	
HTTP	TCP	80	0.0.0.0/0		
Custom TCP Rule	TCP	2224	0.0.0.0/0		
SSH	TCP	22	0.0.0.0/0		
Custom UDP Rule	UDP	5404 - 5405	0.0.0.0/0		
Custom TCP Rule	TCP	3121	0.0.0.0/0		
MySQL/Aurora	TCP	3306	0.0.0.0/0		
HTTPS	TCP	443	0.0.0.0/0		
All ICMP - IPv4	All	N/A	0.0.0.0/0		

[Cancel](#) [Previous](#) **[Review and Launch](#)**

9.Confirm the contents. If there are no problems, click the "Launch" button.※This creates 1 public-a and 1 public-c

* AMI Details

Red Hat Enterprise Linux 8.4 with High Availability
Provided by Red Hat, Inc.
AMI Type: aia
Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on 12 month instance. Additional fees or fees may apply.
Software charges will begin once you launch this AMI and continue until you terminate the instance.

If you have an existing license entitlement to use this software, then you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, 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.

* Instance Type

Instance Type	EC2n	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance
D.8xlarge	-	2	2	EBS only	Yes	Up to 8 Gigabit

[Edit Instance type](#)

* Security Groups

Security Group ID	Name	Description
sg-0c4e830313c3e3dc1	exastro-sg	test

[Edit security groups](#)

All selected security groups inbound rules

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
Custom TCP Rule	TCP	2224	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
Custom UDP Rule	UDP	5404 - 5405	0.0.0.0/0	
Custom TCP Rule	TCP	3121	0.0.0.0/0	
MySQL/Aurora	TCP	3306	0.0.0.0/0	
HTTPS	TCP	443	0.0.0.0/0	
All ICMP - IPv4	All	N/A	0.0.0.0/0	
NFS	TCP	2049	0.0.0.0/0	

[Cancel](#) [Previous](#) **[Launch](#)**

AWS Configuration manual

10.If you need a key for SSH, create it here

Select an existing key pair or create a new key pair

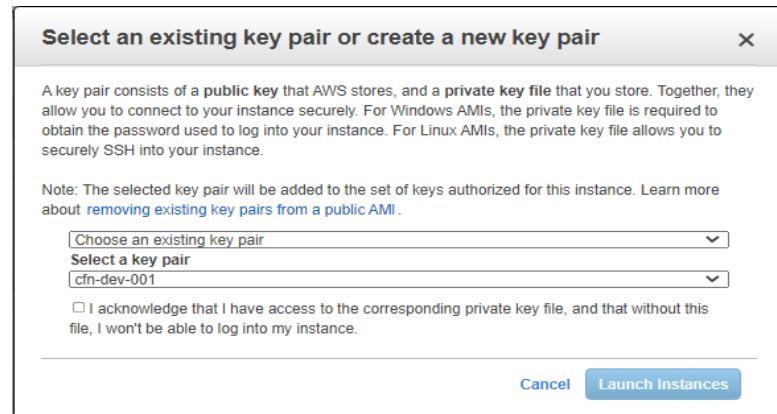
A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows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

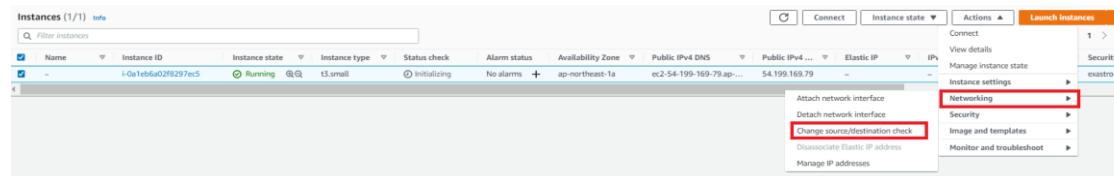
Choose an existing key pair
Select a key pair
cfn-dev-001

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

Cancel Launch Instances



11.After creating it, go to Action ->Networking->Change source/destination deck



Instances (1/1) **Info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPs
i-0a1eb6a02f8297ec5	i-0a1eb6a02f8297ec5	Running	t3.small	Initializing	No alarms	ap-northeast-1a	ec2-54-199-169-79.ap...	54.199.169.79	-	-

Actions ▾

Connect View details Manage instance state Instance settings **Networking** Attach network interface Detach network interface Change source/destination check Dissociate Elastic IP address Manage IP addresses

Security Security Image and templates Monitor and troubleshoot

12.Put a check in the "stop" box and press "save" ✎Runs for 2 machines

Source / destination check **Info**

Each EC2 instance performs source and destination checks by default. The instance must be the source or destination of all the traffic it sends and receives.

Instance ID i-0a1eb6a02f8297ec5

Network interface **Info**
en-0010742d1a5a52116

Source / destination checking **Info**
 Stop

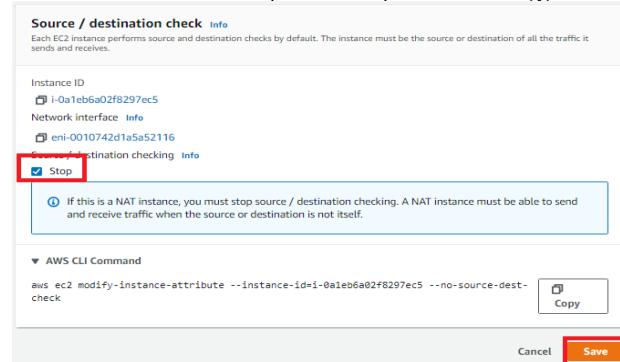
If this is a NAT instance, you must stop source / destination checking. A NAT instance must be able to send and receive traffic when the source or destination is not itself.

AWS CLI Command

```
aws ec2 modify-instance-attribute --instance-id=i-0a1eb6a02f8297ec5 --no-source-dest-check
```

Copy

Cancel Save



AWS Configuration manual

11.Elastic IP

1.Go to the "Elastic IP" menu from the list on the left

▼ Elastic Block Store

Volumes

Snapshots

Lifecycle Manager New

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

2.Click "Allocate Elastic IP Address".



AWS Configuration manual

3.Check that the Network border group is set to "Tokyo region" and click the "Allocate" button.

Allocate Elastic IP address [Info](#)

Elastic IP address settings [Info](#)

Network Border Group [Info](#)
ap-northeast-1

Public IPv4 address pool

Amazon's pool of IPv4 addresses

Public IPv4 address that you bring to your AWS account (option disabled because no pools found) [Learn more](#)

Customer owned pool of IPv4 addresses (option disabled because no customer owned pools found) [Learn more](#)

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. [Learn more](#)

[Create accelerator](#)

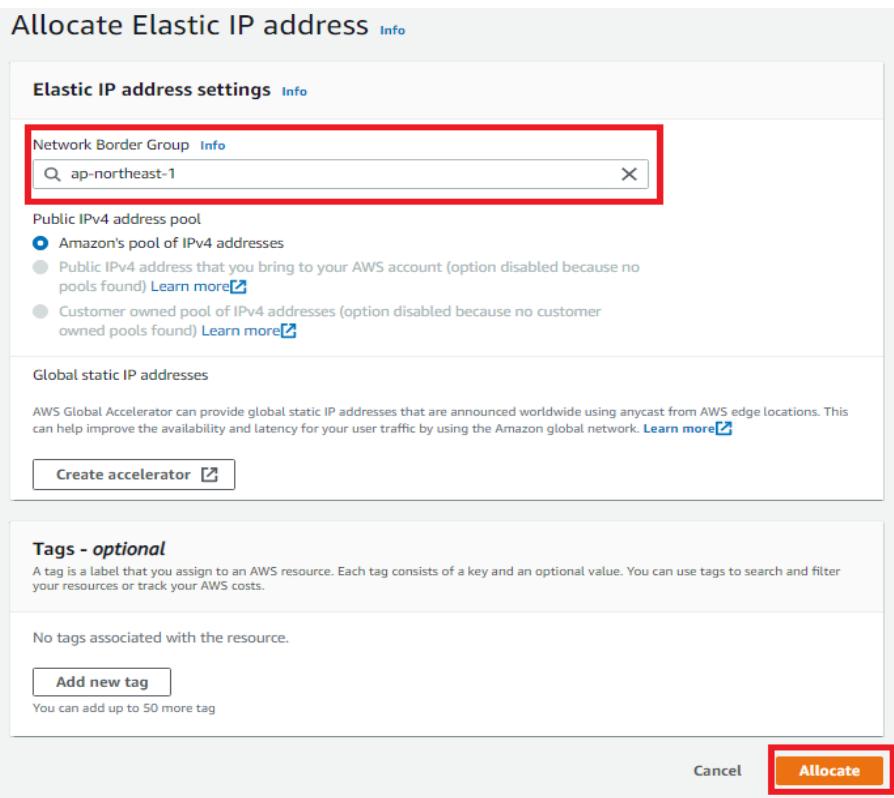
Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

[Add new tag](#)
You can add up to 50 more tag

[Cancel](#) **Allocate**

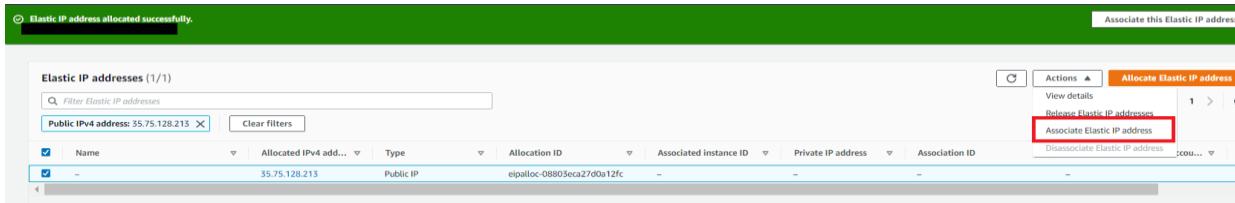


4.After the IP Address has been generated, go to Action-> Associate Elastic IP address

Elastic IP address allocated successfully. [Associate this Elastic IP address](#)

Elastic IP addresses (1/1)							
Filter Elastic IP addresses							
Actions Allocate Elastic IP address							
View details							
<input checked="" type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	Associated instance ID	Private IP address	Association ID
<input checked="" type="checkbox"/>	-	35.75.128.213	Public IP	eipalloc-08803eca27d0a12fc	-	-	-

[Release Elastic IP address](#) **Associate Elastic IP address** [Dissociate Elastic IP address](#)



AWS Configuration manual

5. Select Instance (The instance that is running in public-a), input the Private IP Address (A list will pop up, so select from there) and click the "Associate" | Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (35.75.128.213)

Elastic IP address: 35.75.128.213

Resource type
Choose the type of resource with which to associate the Elastic IP address.

Instance
 Network interface

⚠ If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. Learn more

Instance
i-0a1eb6a02f8297ec5

Private IP address
The private IP address with which to associate the Elastic IP address.

10.0.0.88

Reassociation
Specify whether the Elastic IP address can be reassigned with a different resource if it already associated with a resource.

Allow this Elastic IP address to be reassigned

Cancel Associate

This concludes the AWS settings.

The next slides will be a step by step guide on how to construct.

Construction procedure

Execution user/Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
1. Install ITA				
1-1	Install ITA	●	Please see the All in one installation manual below https://exastro-suite.github.io/it-automation-docs/learn_ia.html#deploy	
1-2	Configure	●	find / (Install file directory) /it-automation-1.7.2 -type f xargs -I{} sed -i -e "s:%%%%%ITA_DIRECTORY%%%%%:/ (ITA Installation directory) :g" {}	Change the red text to fit your environment
2. Configure Apache Resources				
2-1	Create the Apache Server status	●	cat > /etc/httpd/conf.d/server_status.conf << STAT ExtendedStatus On <Location /server-status> SetHandler server-status Order deny,allow Deny from all Allow from localhost </Location> STAT	Install the commands together
2-2	Stop/Deactivate Apache service	●	systemctl disable httpd systemctl stop httpd	
2-3	Copy https server certification/hidden key from master to slave.	●	scp -r -i [key].pem /etc/pki/tls/certs/ (https server certificate name) .crt <slave server local ip address>/etc/pki/tls/certs/ scp -r -i [key].pem /etc/pki/tls/certs/ (https server secret key name) .key <slaveserver local ip address>/etc/pki/tls/certs/	Change the red text to fit your environment (Change the https server certificate/secret key to the name of the files that was created when the ITA Server was installed)

Construction procedure

Execution user／Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
3.ITA Stop settings				
3-1	Deactivate ky-service	●	<pre>systemctl stop ky_activedirectory_roleuser_replication-workflow.service systemctl stop ky_ansible_execute-workflow.service systemctl stop ky_ansible_towermasterSync-workflow.service systemctl stop ky_change_col_to_row.service systemctl stop ky_cmdbmenuanalysis-workflow.service systemctl stop ky_create_er-workflow.service systemctl stop ky_create_param_menu_execute.service systemctl stop ky_data_portability_execute-workflow.service systemctl stop ky_hostgroup_check_loop.service systemctl stop ky_hostgroup_split.service systemctl stop ky_legacy_role_valautostup-workflow.service systemctl stop ky_legacy_role_varsautolistup-workflow.service systemctl stop ky_legacy_valautostup-workflow.service systemctl stop ky_legacy_varsautolistup-workflow.service systemctl stop ky_mail.service systemctl stop ky_pioneer_valautostup-workflow.service systemctl stop ky_pioneer_varsautolistup-workflow.service systemctl stop ky_std_checkcondition_linklist.service systemctl stop ky_std_synchronize_Collector.service systemctl stop ky_std_synchronize_Conductor.service systemctl stop ky_std_synchronize_regularly2.service systemctl stop ky_std_synchronize_regularly.service systemctl stop ky_std_synchronize_symphony.service</pre>	Some services might not exist depending on the ITA Version. In that case, there will be no need to stop said service.
3-2	Deactivate the ky-service automatic run settings	●	<pre>systemctl disable ky_activedirectory_roleuser_replication-workflow.service systemctl disable ky_ansible_execute-workflow.service systemctl disable ky_ansible_towermasterSync-workflow.service systemctl disable ky_change_col_to_row.service systemctl disable ky_cmdbmenuanalysis-workflow.service systemctl disable ky_create_er-workflow.service systemctl disable ky_create_param_menu_execute.service systemctl disable ky_data_portability_execute-workflow.service systemctl disable ky_hostgroup_check_loop.service systemctl disable ky_hostgroup_split.service systemctl disable ky_legacy_role_valautostup-workflow.service systemctl disable ky_legacy_role_varsautolistup-workflow.service systemctl disable ky_legacy_valautostup-workflow.service systemctl disable ky_legacy_varsautolistup-workflow.service systemctl disable ky_mail.service systemctl disable ky_pioneer_valautostup-workflow.service systemctl disable ky_pioneer_varsautolistup-workflow.service systemctl disable ky_std_checkcondition_linklist.service systemctl disable ky_std_synchronize_Collector.service systemctl disable ky_std_synchronize_Conductor.service systemctl disable ky_std_synchronize_regularly2.service systemctl disable ky_std_synchronize_regularly.service systemctl disable ky_std_synchronize_symphony.service</pre>	Some services might not exist depending on the ITA Version. In that case, there will be no need to deactivate said service.

Construction procedure

Execution user／Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
4.EFS Settings				
4-1	Configure the timezone to Asia/Tokyo	●	timedatectl set-timezone Asia/Tokyo	
4-2	Prepare EFS for usage	●	cd /tmp yum -y install git git clone https://github.com/aws/efs-utils yum -y install make rpm-build cd efs-utils make rpm yum -y install ./build/amazon-efs-utils*rpm	
4-3	Configure EFS Common files	●	mount -t efs -o tls [name resolution settings information of the EFS registered to Route53]:/ /mnt cd /mnt mkdir -p ./ (ITA Installation directory) /data relay storage/symphony mkdir -p ./ (ITA Installation directory) /data_relay_storage/conductor mkdir -p ./ (ITA Installation directory) /data_relay_storage/ansible_driver mkdir -p ./ (ITA Installation directory) /ita sessions mkdir -p ./ (ITA Installation directory) /ita-root/webconfs/sheets mkdir -p ./ (ITA Installation directory) /ita-root/webconfs/users mkdir -p ./ (ITA Installation directory) /ita-root/temp mkdir -p ./ (ITA Installation directory) /ita-root/uploadfiles mkdir -p ./ (ITA Installation directory) /ita-root/webroot/uploadfiles mkdir -p ./ (ITA Installation directory) /ita-root/webroot/menus/sheets mkdir -p ./ (ITA Installation directory) /ita-root/webroot/menus/users chmod 777 ./ (ITA Installation directory) /data_relay_storage/symphony chmod 777 ./ (ITA Installation directory) /data_relay_storage/conductor chmod 777 ./ (ITA Installation directory) /data_relay_storage/ansible_driver chmod 777 ./ (ITA Installation directory) /ita sessions chmod 755 ./ (ITA Installation directory) /ita-root/webconfs/sheets chmod 755 ./ (ITA Installation directory) /ita-root/webconfs/users chmod 777 ./ (ITA Installation directory) /ita-root/temp chmod 777 ./ (ITA Installation directory) /ita-root/uploadfiles chmod 777 ./ (ITA Installation directory) /ita-root/webroot/uploadfiles chmod 755 ./ (ITA Installation directory) /ita-root/webroot/menus/sheets chmod 755 ./ (ITA Installation directory) /ita-root/webroot/menus/users	Change the red text to fit your environment. Perform this step after you have created EFS from the AWS CloudFormation stack.

Construction procedure

Execution user／Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
4-4	Copy common files	●	<pre>cp -rp /{ITA Installation directory}/data_relay_storage/symphony /mnt/{ITA Installation directory}/data_relay_storage/ cp -rp /{ITA Installation directory}/data_relay_storage/conductor /mnt/{ITA Installation directory}/data_relay_storage/ cp -rp /{ITA Installation directory}/data_relay_storage/ansible_driver /mnt/{ITA Installation directory}/data_relay_storage/ cp -rp /{ITA Installation directory}/ita_sessions /mnt/{ITA Installation directory}/ cp -rp /{ITA Installation directory}/ita-root/webconfs/sheets /mnt/{ITA Installation directory}/ita-root/webconfs/ cp -rp /{ITA Installation directory}/ita-root/webconfs/users /mnt/{ITA Installation directory}/ita-root/webconfs/ cp -rp /{ITA Installation directory}/ita-root/temp /mnt/{ITA Installation directory}/ita-root/ cp -rp /{ITA Installation directory}/ita-root/uploadfiles /mnt/{ITA Installation directory}/ita-root/ cp -rp /{ITA Installation directory}/ita-root/webroot/uploadfiles /mnt/{ITA Installation directory}/ita- root/webroot/ cp -rp /{ITA Installation directory}/ita-root/webroot/menus/sheets /mnt/{ITA Installation directory}/ita- root/webroot/menus/ cp -rp /{ITA Installation directory}/ita-root/webroot/menus/users /mnt/{ITA Installation directory}/ita- root/webroot/menus/ cd /tmp umount /mnt</pre>	
4-5	Configure the settings that mounts multiple directories. Create Settings file	●	<pre>vi /etc/systemd/system/mount-nfs-sequentially.service [Unit] Description=Workaround for mounting NFS file systems sequentially at boot time After=remote-fs.target [Service] Type=oneshot ExecStart=/bin/mount -avt nfs4 RemainAfterExit=yes [Install] WantedBy=multi-user.target</pre>	
	Reflect the settings above	●	<pre>systemctl daemon-reload systemctl enable mount-nfs-sequentially.service</pre>	

Construction procedure

Execution user／Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
5.RDS Settings				
5-1	Connect to RDS	●	<pre>mysql -h [DB Host name(name resolution settings information of the EFS registered to Route53)] -P 3306 -u admin -p<admin password> 例)mysql -h rds.exastro-aws.local -P 3306 -u admin -p*****</pre>	Change the red text to fit your environment
5-2	Create User and DB	●	<pre>CREATE USER '<username>' IDENTIFIED BY '<password>'; CREATE USER '<username>'@'localhost' IDENTIFIED BY '<password>'; CREATE DATABASE [DB name] CHARACTER SET utf8; GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, INDEX, ALTER, CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EVENT, TRIGGER ON [DB name].* TO '<username>%'@'%' WITH GRANT OPTION; GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, REFERENCES, INDEX, ALTER, CREATE TEMPORARY TABLES, LOCK TABLES, EXECUTE, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EVENT, TRIGGER ON [DB name].* TO '<username>'@'localhost' WITH GRANT OPTION; exit</pre>	Change the red text to fit your environment
5-3	Flow data to DB	●	<pre>mysqldump --default-character-set=utf8 -u <DB username configured in ita_answer.txt> -p<DB password configured in ita_answer.txt> [DB name configured in ita_answer.txt] > ITA_DB.sql sed -i 's/DEFINER=[*]@*/`/g' ITA_DB.sql mysql --default-character-set=utf8 -h [DB Host name(name resolution settings information of the EFS registered to Route53.)] -P 3306 -u <RDS master username> -p<RDS Master password> [DB name] < ITA_DB.sql Example) mysql --default-character-set=utf8 -h rds.exastro-aws.local -P 3306 -u admin -p***** ITA_DB < ITA_DB.sql</pre>	Change the red text to fit your environment

Construction procedure

Execution user/Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
5-4	Configure DB Connection			
	Configure MariaDB Connection information	● ●	<p>①Create a base64-encoded, rot13-encrypted string of the following characters. <code>echo -ne "mysql:dbname=[DB name];host=[DB host name (name resolution settings information of the EFS registered to Route53)]" base64 tr '[A-Za-z]' '[N-ZA-Mn-za-m]'</code></p> <p>②Write the created character string into the following file ※Delete the value already there. <code>vi /[ITA Installation directory]/ita-root/confs/commonconfs/db connection string.txt</code></p>	<p>Example: If the ITA DB name is "ITA_DB" and the DNS name registered to Route53 is "rds.exastro-aws.local", the following command can be used to get a string with base64 <code>echo -ne "mysql:dbname=ITA_DB;host=rds.exastro-aws.local" base64 tr '[A-Za-z]' '[N-ZA-Mn-za-m]'</code></p> <p>Change the red text to fit your environment</p>
	Configure MariaDB User information	● ●	<p>①Create a base64-encoded, rot13-encrypted Maria DB username. <code>echo -ne "<Username>" base64 tr '[A-Za-z]' '[N-ZA-Mn-za-m]'</code></p> <p>②Write the created character string into the following file ※Delete the value already there. <code>vi /[ITA Installation directory]/ita-root/confs/commonconfs/db username.txt</code></p>	<p>Example: If the MariaDB user name is "ITA_USER", the following command can be used to get a string with base64 <code>echo -ne "ITA_USER" base64 tr '[A-Za-z]' '[N-ZA-Mn-za-m]'</code></p> <p>Change the red text to fit your environment</p>
	Configure mariaDB Password information	● ●	<p>①Create a base64-encoded, rot13-encrypted Maria DB password. <code>echo -ne "<password>" base64 tr '[A-Za-z]' '[N-ZA-Mn-za-m]'</code></p> <p>②Write the created character string into the following file ※Delete the value already there. <code>vi /[ITA Installation directory]/ita-root/confs/commonconfs/db password.txt</code></p>	<p>Example: If the MariaDB Password is "ITA_PASSWORD", the following command can be used to get a string with base64 <code>echo -ne "ITA_PASSWORD" base64 tr '[A-Za-z]' '[N-ZA-Mn-za-m]'</code></p> <p>Change the red text to fit your environment</p>
5-7	Stop MariaDB	● ●	<code>systemctl disable mariadb systemctl stop mariadb</code>	
5-8	Delete MariaDB	● ●	<code>yum list installed grep -i mariadb</code> <code>yum remove mariadb.x86_64 mariadb-backup.x86_64 mariadb-common.x86_64 mariadb-connector-c.x86_64 mariadb-connector-c-config.noarch mariadb-errmsg.x86_64 mariadb-gssapi-server.x86_64 mariadb- server.x86_64 mariadb-server-utils.x86_64</code>	

Construction procedure

Execution user/Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
6.Pacemaker settings				
6-1	Install awscli	●	yum -y install awscli	
6-2	Check the credentials.csv created in the User creation	●	aws configure AWS Access Key ID [None]: ***** AWS Secret Access Key [None]: ***** Default region name [None]: ap-northeast-1 Default output format [None]: json	Change the red text to fit your environment Make sure that you are referring the csv you downloaded when creating a user.
6-3	Register host name and IP Address to hosts	●	uname -n vi /etc/hosts Local IP Host name Local IP Host name Example) 10.0.0.204 <ita-ha-sv01's host name> 10.0.1.61 <ita-ha-sv02's host name>	Change the red text to fit your environment
6-4	Configure the password of the user that will be the admin account for pcscd, "hacluster".	●	passwd hacluster New Password:xxxxxx Please input the new password again.:xxxxxx passwd: All authentication tokens have been updated correctly.	Change the red text to fit your environment
6-5	Start the pcscd service and configure the pcscd so that it is active when the system starts.	●	systemctl enable pcscd systemctl start pcscd systemctl status pcscd	
6-6	Authenticate cluster	●	pcs host auth <ita-ha-sv01's host name> <ita-ha-sv02's host name> Username: hacluster Password:Password set in passwd hacluster	Change the red text to fit your environment
6-7	Specify cluster and start	●	pcs cluster setup aws-cluster --start <ita-ha-sv01's host name> <ita-ha-sv02's host name> --force	Change the red text to fit your environment
6-8	Configure the cluster so it starts automatically	●	pcs cluster enable --all	
6-9	Deactivate the STONITH (Shoot The Other Node In The Head) option	●	pcs property set stonith-enabled=false	
6-10	Make sure that the system keeps managing all the nodes and does not perform any special act	●	pcs property set no-quorum-policy=ignore	
6-11	Configure property delay time	●	pcs property set transition-delay="0s"	
6-12	Deactivate Automatic failback	●	pcs resource defaults resource-stickiness="INFINITY" migration-threshold="1"	
6-13	Configure corosync	●	cp -p /usr/lib/systemd/system/corosync.service /etc/systemd/system/ sed -i 's/^#Restart=on-*\$/Restart=on-failure/' /etc/systemd/system/corosync.service sed -i 's/^#RestartSec=.*\$/RestartSec=70/' /etc/systemd/system/corosync.service	

Construction procedure

Execution user/Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
6-14	Treat the Pacemaker internal process like a Node failure if something happens to it	●	sed -i 's/^# PCMK_failfast.*\$/PCMK_failfast=yes/' /etc/sysconfig/pacemaker	
6-15	Configure corosync	●	cp -p /usr/lib/systemd/system/pacemaker.service /etc/systemd/system sed -i 's/# ExecStopPost=\/bin\/sh\/*ExecStopPost=\/bin\/sh -c pidof crmd \ \ killall -TERM corosync\/*' /etc/systemd/system/pacemaker.service	
6-16	Configure IP Replacement	●	vi /etc/sysconfig/pacemaker /etc/sysconfig/pacemaker contents # Set the options to pass to valgrind, when valgrind is enabled. See # valgrind(1) man page for details. “--vgdb=no” is specified because # pacemaker-execd can lower privileges when executing commands, which would # otherwise leave a bunch of unremovable files in /tmp. VALGRIND_OPTS="--leak-check=full --trace-children=no --vgdb=no --num-callers=25 --log- file=/var/lib/pacemaker/valgrind-%p --suppressions=/usr/share/pacemaker/tests/valgrind- pacmk.suppressions --gen-suppressions=all" AWS_DEFAULT_REGION=ap-northeast-1 ←written section	Change the red text to fit your environment (If the Region is set to Tokyo, add “AWS_DEFAULT_REGION=ap-northeast-1” to the end)
6-17	Configure httpd	●	pcs resource create httpd systemd:httpd ¶ op monitor interval=60 timeout=100 ¶ op start interval=0s timeout=100 ¶ op stop interval=0s timeout=100	
6-18	Configure eip	●	pcs resource create eip ocf:heartbeat:awseip ¶ elastic_ip="ElasticIP's IP Address" awscli="\$(which aws)" ¶ allocation_id=ElasticIP assigned ID ¶ op start timeout="60s" interval="0s" on-fail="stop" ¶ op monitor timeout="60s" interval="10s" on-fail="restart" ¶ op stop timeout="60s" interval="0s" on-fail="block"	Change the red text to fit your environment
6-19	Configure httpd, eip resource group	●	pcs resource group add exastro httpd eip	
6-20	Configure EFS Resource	●	pcs resource create symphony Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/data_relay/storage/symphony' directory='/(ITA Installation directory)/data_relay/storage/symphony' ftype=nfs' pcs resource create conductor Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/data_relay/storage/conductor' directory='/(ITA Installation directory)/data_relay/storage/conductor' ftype=nfs' pcs resource create ansible_driver Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/data_relay/storage/ansible_driver' directory='/(ITA Installation directory)/data_relay/storage/ansible_driver' ftype=nfs' pcs resource create ita_sessions Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/ita_sessions' directory='/(ITA Installation directory)/ita_sessions' ftype=nfs' pcs resource create webconfs sheets Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/ita-root/webconfs/sheets' directory='/(ITA Installation directory)/ita-root/webconfs/sheets' ftype=nfs' pcs resource create webconfs users Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/ita-root/webconfs/users' directory='/(ITA Installation directory)/ita-root/webconfs/users' ftype=nfs' pcs resource create temp Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/ita-root/temp' directory='/(ITA Installation directory)/ita- root/temp' ftype=nfs' pcs resource create uploadfiles Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/ita-root/uploadfiles' directory='/(ITA Installation directory)/ita-root/uploadfiles' ftype=nfs' pcs resource create webroot_uploadfiles Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/ita-root/webroot/uploadfiles' directory='/(ITA Installation directory)/ita-root/webroot/uploadfiles' ftype=nfs' pcs resource create menus_sheets Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/ita-root/webroot/menus/sheets' directory='/(ITA Installation directory)/ita-root/webroot/menus/sheets' ftype=nfs' pcs resource create menu_users Filesystem device=[name resolution settings information of the EFS registered to Route53]:/(ITA Installation directory)/ita-root/webroot/menus/users' directory='/(ITA Installation directory)/ita-root/webroot/menus/users' ftype=nfs'	Change the red text to fit your environment

Construction procedure

Execution user/Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
6-21	Configure EFS resource group	●	<pre>pcs resource group add efsmount symphony conductor ansible_driver ita_sessions webconfs_sheets webconfs_users temp uploadfiles webroot_uploadfiles menus_sheets menus_users</pre>	
6-22	Configure each ky file resource	●	<pre>pcs resource create ky_activatedirectory_roleuser_replication--workflow systemd:ky_ansible_execute--workflow op monitor interval=60 timeout=100 op start interval=0s timeout=100 op stop interval=0s timeout=100 pcs resource create ky_ansible_execute--workflow systemd:ky_ansible_execute--workflow op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_ansible_towermasterSync--workflow systemd:ky_ansible_towermasterSync--workflow op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_change_col_to_row systemd:ky_change_col_to_row op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_cmdbmenuanalysis--workflow systemd:ky_cmdbmenuanalysis--workflow op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_create_er--workflow systemd:ky_create_er--workflow op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_create_param_menu_execute systemd:ky_create_param_menu_execute op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_data_portability_execute--workflow systemd:ky_data_portability_execute--workflow op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_hostgroup_check_loop systemd:ky_hostgroup_check_loop op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_hostgroup_split systemd:ky_hostgroup_split op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_legacy_role_valautostup--workflow systemd:ky_legacy_role_valautostup--workflow op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_legacy_role_varsautolistup--workflow systemd:ky_legacy_role_varsautolistup--workflow op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60 pcs resource create ky_legacy_valautostup--workflow systemd:ky_legacy_valautostup--workflow op monitor interval=30 timeout=60 op start interval=0s timeout=60 op stop interval=0s timeout=60</pre>	

Construction procedure

Execution user／Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
			<pre>pcs resource create ky_legacy_varsautolistup-workflow systemd:ky_legacy_varsautolistup-workflow \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_pioneer_valautostup-workflow systemd:ky_pioneer_valautostup-workflow \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_pioneer_varsautolistup-workflow systemd:ky_pioneer_varsautolistup-workflow \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_std_checkcondition-linklist systemd:ky_std_checkcondition-linklist \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_std_synchronize-Conductor systemd:ky_std_synchronize-Conductor \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_std_synchronize-regularly systemd:ky_std_synchronize-regularly \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_std_synchronize-regularly2 systemd:ky_std_synchronize-regularly2 \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_std_synchronize-symphony systemd:ky_std_synchronize-symphony \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60</pre>	

Construction procedure

Execution user/Connection conditions
Run everything as root user
Make sure that the root user can log in through ssh

No.	Operation	Server master slave	Contents (※When "Master" and "Slave" server configuration is required, please configure them in parallel)	Remarks
6-23	Group ky resources	●	pcs resource group add ky_services ky_activedirectory_roleuser_replication=workflow ky_ansible_execute=workflow ky_ansible_towermasterSync=workflow ky_change_col_to_row_ky_cmdbmenuanalysis=workflow ky_create_er=workflow ky_create_param_menu_execute_ky_data_portability_execute=workflow ky_hostgroup_check_loop_ky_hostgroup_split_ky_legacy_role_valautostup=workflow ky_legacy_role_varsautolistup=workflow ky_legacy_valautostup=workflow ky_legacy_varsautolistup=workflow ky_pioneer_valautostup=workflow ky_pioneer_varsautolistup=workflow ky_std_checkcondition_linklist ky_std_synchronize_Conductor ky_std_synchronize_regularly ky_std_synchronize_regularly2 ky_std_synchronize_symphony	
6-24	specify the resources created up until this point and specify the resource group start/stop set	●	pcs constraint order set efsmount ky_services exastro	
6-25	Specify the constraint where all the resources created up until this point will start in the same	●	pcs constraint colocation set efsmount ky_services exastro	
6-26	Start the HA Software services	●	● systemctl enable corosync systemctl enable pacemaker systemctl start corosync systemctl start pacemaker	
6-27	Confirm the Cluster status	●	● pcs status (表示例) Cluster name: aws-cluster Cluster Summary: * Stack: corosync * Current DC: <ita-ha-sv01's host name> (version 2.0.5-9.el8_4.1-ba59be7122) – partition with quorum * Last updated: Thu Jun 10 06:46:16 2021 * Last change: Wed Jun 9 18:39:29 2021 by root via cibadmin on <ita-ha-sv01's host name> * 2 nodes configured —Make sure that this is displayed * 34 resource instances configured Node List: * Online: [<ita-ha-sv01's host name> <ita-ha-sv02's host name> —Both master and slave are online Full List of Resources: * Resource Group: exastro: * eip (ocf:heartbeat:awseip): Started <ita-ha-sv01's host name> —Master has "Started" * httpd (systemd:httpd): Started <ita-ha-sv01's host name> * Resource Group: efsmount: * symphony (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * conductor (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * ansible driver (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * ita_sessions (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * webconfs_sheets (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * webconfs_users (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * tempo (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * uploadfiles (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * webroot_uploadfiles (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * menus_sheets (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * menus_users (ocf:heartbeat:Filesystem): Started <ita-ha-sv01's host name> * Resource Group: ky.services: ~~~~~Abbr~~~~~ Daemon Status: corosync: active/enabled pacemaker: active/enabled pcsd: active/enabled	Change the red text to fit your environment
6-28	Confirm ITA Connection	●	Use the URL below to access the Login screen http://(ElasticIP)	Change the red text to fit your environment

Operation Complete