



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 1.9

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	2.0.5-9
Corosync(※)	Heartbeat	3.1.0
pcs(※)	Pacemaker command	0.10.8

※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. Preparation (AWS settings)	VPC	-	-
	Subnet	-	-
	Route table	-	-
	Security Groups	-	-
	IAM	-	-
	RDS	-	-
	EFS	-	-
	Route53	-	-
	EC2	Create EC2	Create EC2
1. Install ITA	ITA1.7.2 Online install	ITA Online install	ITA Online install
		Create Apache status confirm resources	Create Apache status confirm resources
2. Apache resource setting	Apache	Stop/Deactivate Apache service	Stop/Deactivate Apache service
		-	-
3. ITA Service stop setting	-	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
6. Prepare Pacemaker for	-	Install awscil	Install awscil
		hosts settings	hosts settings
7. Pacemaker settings	Pacemaker	Cluster settings	Cluster settings
		Resource settings	Resource settings
		Pacemaker startup order setting	Pacemaker startup order setting
		Uninstall MariaDB	Uninstall MariaDB

Introduction

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.

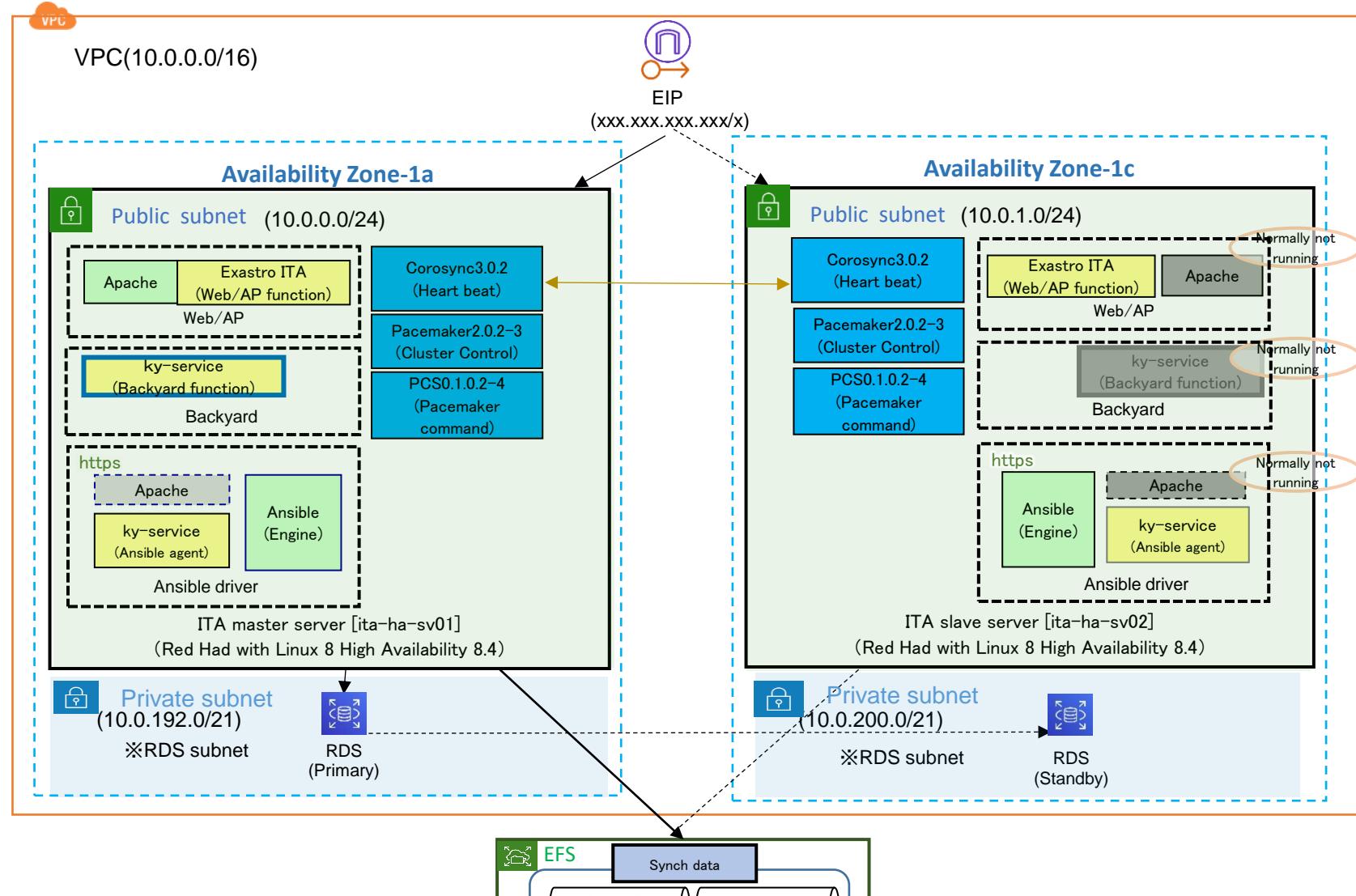
Reference URL:

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

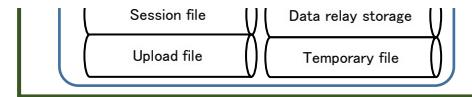
Introduction

5. System Configuration example

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



Introduction



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 | 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/tcp
Corosync	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-firewalls-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_Basic
1.1 Server requirements

https://github.com/exastro-suite/it-automation-docs/raw/master/asset/Documents/Exastro-ITA_System_Configuration_Environment_Construction_Guide_Ansible-driver
3. System requirements

Introduction

- Installation requirements

Please refer to the all-in-one configuration isntallation 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
createparam:yes
hostgroup:yes
ansible_driver:yes
cobbler_driver:no
terraform_driver:yes
cicd_for_iac:no
```

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.

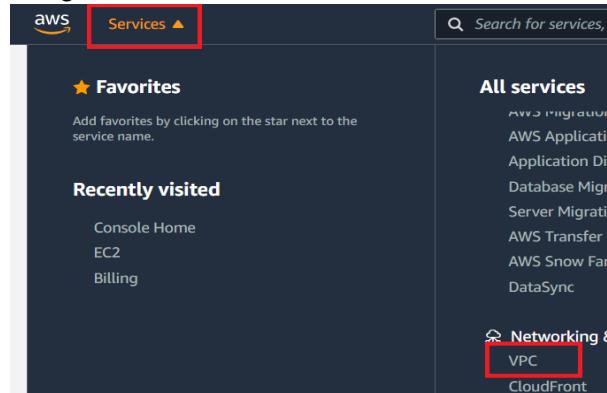
The services we will use are as following

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

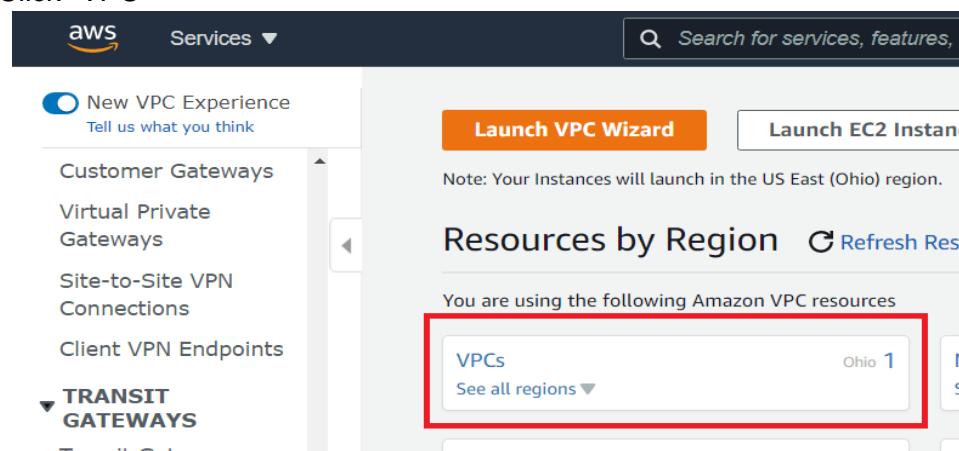
AWS Configuration manual

1.VPC

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



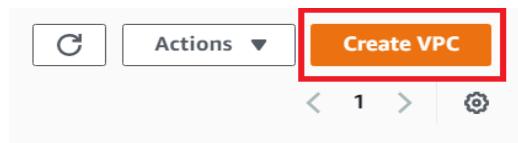
2.Click "VPC"



3.Click "Create VPC"



AWS Configuration manual



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'. Under 'IPv6 CIDR block', the radio button for 'No IPv6 CIDR block' is selected. In the 'Tenancy' section, 'Default' is chosen. The 'Tags' section shows a single tag 'Name: exastro-VPC'. At the bottom, the 'Create VPC' button is highlighted with a red box.

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 for the VPC 'vpc-0d3171fa1b8ae587e / exastro-VPC'. Key information includes: VPC ID (vpc-0d3171fa1b8ae587e), State (Available), DHCP options set (dopt-a5bb56c3), Main route table (rtb-00ad18cf6f3fb806e), IPv4 CIDR (10.0.0.0/16), and DNS resolution (Enabled). The 'Actions' dropdown menu is visible at the top right.

AWS Configuration manual



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 with a list of VPCs. A VPC named 'exastro-VPC' is selected, indicated by a red box around its checkbox. 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 screenshot shows the 'Edit DNS hostnames' dialog box. It has a section titled 'DNS hostnames' with the sub-instruction 'Indicates whether instances with public IP addresses get corresponding public DNS hostnames.' Below this, there 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. A red box highlights this checkbox. At the bottom right of the dialog is a 'Save changes' button, also highlighted with a red box.

8. Check that the DNS hostnames is activated

The screenshot shows the 'VPC Details' page for the 'exastro-VPC'. On the right side of the page, there is a summary table. In the third column, under the heading 'DNS hostnames', the status 'Enabled' is displayed. This entire row is highlighted with a red box. Other columns in the table include 'State' (Available), 'DHCP options set' (dopt-a5bb56c3), 'IPv4 CIDR' (10.0.0.0/16), 'Owner ID' (Redacted), 'Main route table' (rtb-00ad18cf6f3fb806), 'IPv6 pool' (-), 'DNS resolution' (Enabled), 'Main network ACL' (acl-0d9aeee3cb12de7f7), and 'IPv6 CIDR (Network border group)' (-).

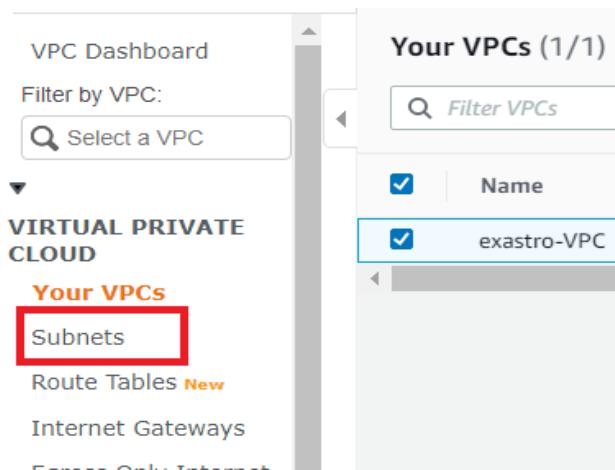
AWS Configuration manual



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 [Create subnets in this VPC](#)
vpc-0d5171fa1b8ae587e (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](#)
Q 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
Create a name for your subnet and choose the VPC and Availability Zone.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 CIDR block [Info](#)
The range of IP addresses available for your subnet.

▼ Tags - optional

Key Value - optional Remove

Add new tag
You can add 49 more tags.

Remove

Subnet 3 of 3

Subnet name
Create a name for your subnet and choose the VPC and Availability Zone.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 CIDR block [Info](#)
The range of IP addresses available for your subnet.

▼ Tags - optional

Key Value - optional Remove

Add new tag
You can add 49 more tags.

Remove

Subnet 4 of 4

Subnet name
Create a name for your subnet and choose the VPC and Availability Zone.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 CIDR block [Info](#)
The range of IP addresses available for your subnet.

▼ Tags - optional

Key Value - optional Remove

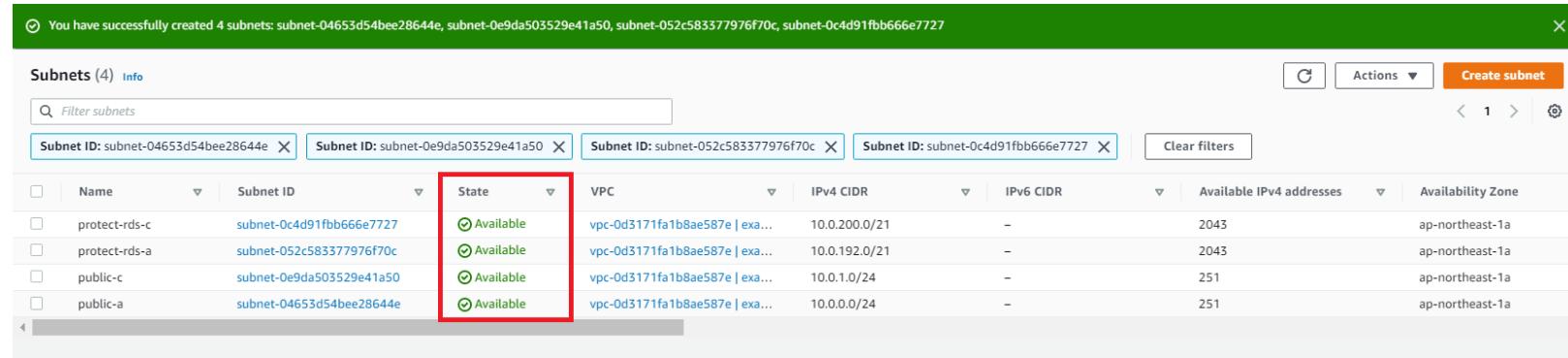
Add new tag
You can add 49 more tags.

AWS Configuration manual



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 indicates "You have successfully created 4 subnets: subnet-04653d54bee28644e, subnet-0e9da503529e41a50, subnet-052c583377976f70c, subnet-0c4d91fb666e7727". Below this, there are filter buttons for "Subnet ID: subnet-04653d54bee28644e", "Subnet ID: subnet-0e9da503529e41a50", "Subnet ID: subnet-052c583377976f70c", and "Subnet ID: subnet-0c4d91fb666e7727". The main 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

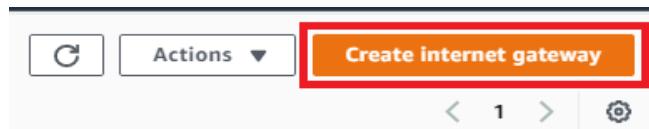
AWS Configuration manual

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.

exastro-gw

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.

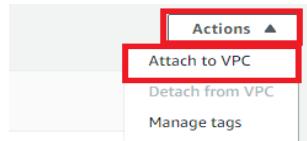
Key	Value - optional
<input type="text" value="Name"/> X	<input type="text" value="exastro-gw"/> X

[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.

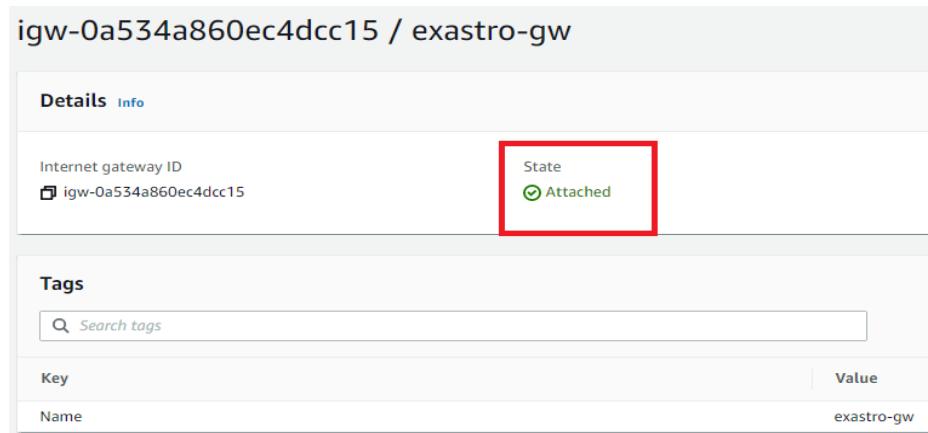


AWS Configuration manual

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



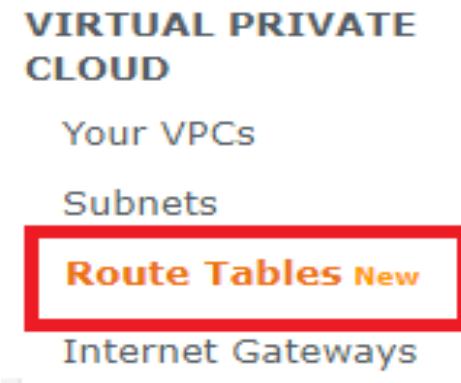
6. Check that the gateway is "Attached"



AWS Configuration manual

4.Route Tables

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



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

Route tables (1/1) Info						
<input type="text" value="Filter route tables"/> 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. At the top, there is a search bar labeled 'Filter route tables' and a filter button 'VPC: vpc-0d3171fa1b8ae587e X'. Below the search bar are two buttons: 'Clear filters' and a dropdown menu with options like 'Name', 'Route table ID', 'Explicit subnet associations', 'Edge associations', 'Main', and 'VPC'. A table lists one route table: 'rtb-00ad18cf6f3fb806e'. The table columns include 'Name', 'Route table ID', 'Explicit subnet associations', 'Edge associations', 'Main', and 'VPC'. The 'Main' column shows 'Yes' and the 'VPC' column shows 'vpc-0d3171fa1b8ae587e | exa...'. Below the table, the route table details are shown. The 'Routes' tab is highlighted with a red box. The 'Routes (1)' section shows a single route with destination '10.0.0.0/16', target 'local', and status 'Active'. There is also a 'Details' tab and tabs for 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'.

4.Add Route information

The screenshot shows the 'Edit routes' dialog. It has a table with columns: 'Destination', 'Target', 'Status', and 'Propagated'. There are two rows. The first row has a 'Destination' of '10.0.0.0/16', a 'Target' of 'local', a 'Status' of 'Active', and a 'Propagated' status of 'No'. The second row is being edited and has a 'Destination' of '0.0.0.0/0', a 'Target' of 'igw-0a534a860ec4dcc15', a 'Status' of 'Active', and a 'Propagated' status of 'No'. A 'Remove' button is next to the second row. At the bottom left is an 'Add route' button. At the bottom right are 'Cancel', 'Preview', and a large red-bordered 'Save changes' button.

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 includes links for VPC, Route tables, and the specific route table ID. A green banner at the top indicates that routes have been updated successfully. Below the banner, a message suggests checking network connectivity with the Reachability Analyzer. The main content area displays the route table details and its routes.

Route table ID: rtb-00ad18cf6f3fb806e

Main: Yes

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' wizard. The first step is 'Set security group details'. It includes fields for 'Security group name' (set to 'exastro'), 'Description' (optional), and 'VPC' (set to 'exastro-vpc'). Below this, the 'Inbound rules' section is highlighted with a red box, showing various predefined rules like SSH, HTTP, HTTPS, and MySQL/Aurora. At the bottom, the 'Outbound rules' section is also highlighted with a red box.

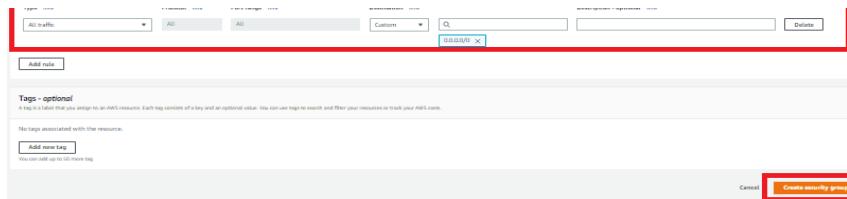
Example)

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	10.0.0.0/16 ✘
Custom UDP	UDP	5404 - 5405	10.0.0.0/16 ✘
Custom TCP	TCP	3121	10.0.0.0/16 ✘
Custom TCP	TCP	2224	10.0.0.0/16 ✘

AWS Configuration manual



※ VPC's NW address

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

Security group (sg-0cb4edaff505fe40) | exastro-sg was created successfully

Details

Security group name: exastro-sg

Security group ID: sg-0cb4edaff505fe40

Description: No description

VPC ID: vpc-0d171f1b8e507e

Owner: [REDACTED]

Inbound rules count: 9 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules | Outbound rules | Tags

You can now check network connectivity with Reachability Analyzer

Inbound rules (9)

Name	Security group rule	IP version	Type	Protocol	Port range	Source	Description
-	sg-0f12a337fd505fe40	IPv4	NFS	TCP	2049	0.0.0.0/0	-
-	sg-05f99a95940231f	IPv4	HTTP	TCP	80	165.225.97.107/32	-
-	sg-05580144defef1b	IPv4	Custom TCP	TCP	2224	0.0.0.0/0	-
-	sg-0591040a64e7e...	IPv4	Custom TCP	TCP	3121	0.0.0.0/0	-
-	sg-0e00f031a1e147e	IPv4	SSH	TCP	22	165.225.97.107/32	-
-	sg-050a015068728	IPv4	Custom UDP	UDP	5404 - 5406	0.0.0.0/0	-
-	sg-050501279fe110	IPv4	All ICMP - IPv4	ICMP	All	0.0.0.0/0	-
-	sg-0e06220f1505fe40	IPv4	HTTP	TCP	443	165.225.97.107/32	-
-	sg-0e29649320fe1505fe40	IPv4	MySQL/Aurora	TCP	3306	0.0.0.0/0	-

5. Create security group for RDS and EFS.

Create security group

Basic details

Security group name: exastro-efs

Description: For EFS

VPC: exastro-vpc

Inbound rules

Type: NFS

Protocol: TCP

Port range: 2049

Source: 10.0.0.0/16

Outbound rules

Type: All traffic

Protocol: All

Port range: All

Destination: 0.0.0.0/0

Create security group

Basic details

Security group name: exastro-rds

Description: For RDS

VPC: exastro-vpc

Inbound rules

Type: MySQL/Aurora

Protocol: TCP

Port range: 3306

Source: 10.0.0.0/16

Outbound rules

Type: All traffic

Protocol: All

Port range: All

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	10.0.0.0/16

※ VPC's NW address

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	10.0.0.0/16

※ VPC's NW address

Outbound Rule

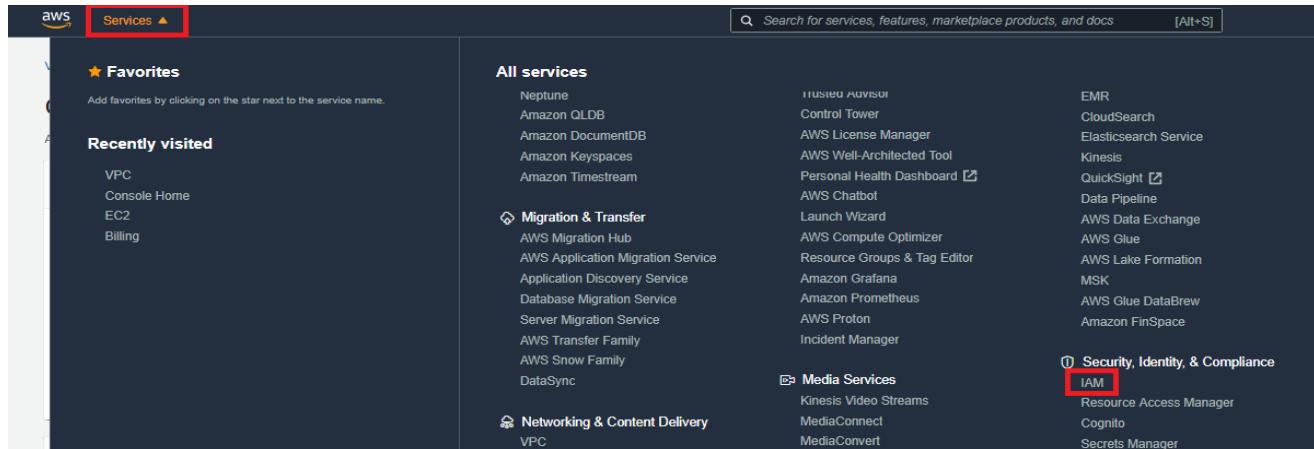
Type	Protocol	Port range	Source
All Traffic	All	All	0.0.0.0/0

AWS Configuration manual

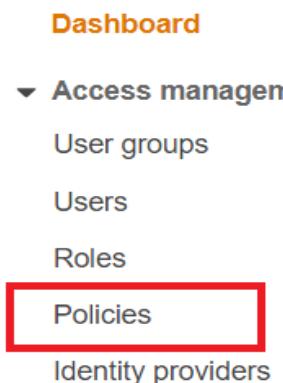
AWS Configuration manual

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



AWS Configuration manual

4. Open up the JSON tab and input the policy

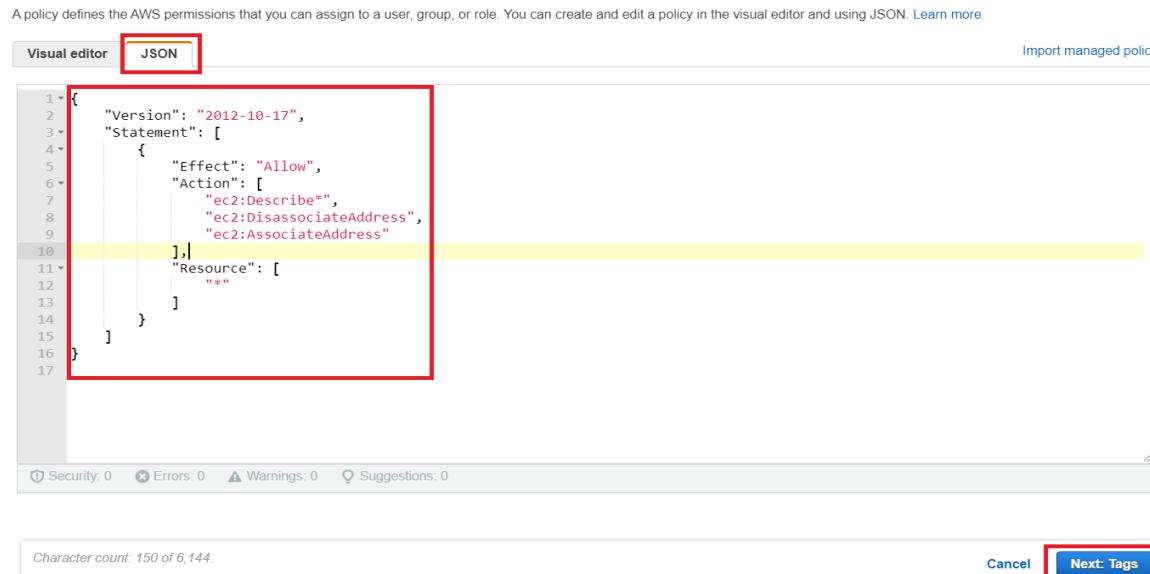
Create policy

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	<table border="1"><tr><td>Service</td><td>Access level</td><td>Resource</td><td>Request condition</td></tr><tr><td>Allow (1 of 285 services) Show remaining 284</td><td>EC2</td><td>Limited: List, Read, Write</td><td>All resources</td></tr><tr><td colspan="4">None</td></tr></table>	Service	Access level	Resource	Request condition	Allow (1 of 285 services) Show remaining 284	EC2	Limited: List, Read, Write	All resources	None			
Service	Access level	Resource	Request condition										
Allow (1 of 285 services) Show remaining 284	EC2	Limited: List, Read, Write	All resources										
None													
Tags	<table border="1"><thead><tr><th>Key</th><th>Value</th></tr></thead><tbody><tr><td colspan="2">No tags associated with the resource.</td></tr></tbody></table>	Key	Value	No tags associated with the resource.									
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.

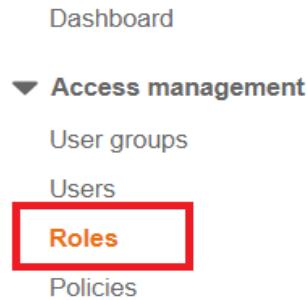
Filter policies by property or policy name and press enter

Policy Name	Type
exastro-policy	Customer managed

AWS Configuration manual

AWS Configuration manual

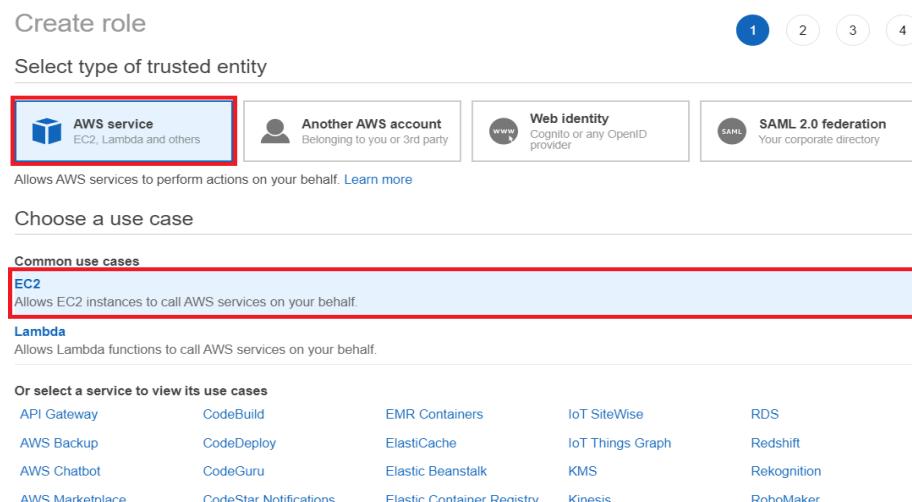
8.Go to the "Roles" menu from the list to the left



9.Click the "Create Role" button



10.Select "AWS Service" and "EC2" and click "Next: Permissions".



AWS Configuration manual

AWS Support	Comprehend	Elastic Container Service	Lake Formation	S3
Amplify	Config	Elastic Transcoder	Lambda	SMS
AppStream 2.0	Connect	Elastic Load Balancing	Lex	SNS
AppSync	DMS	EventBridge	License Manager	SWF

* Required

[Cancel](#) [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 ▾ Q exastro Showing 1 result

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

Set permissions boundary

* Required Cancel Previous **Next: Tags**

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
Add new key		

You can add 50 more tags.

AWS Configuration manual

[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.

1 2 3 4

Example)

Role Name	exastro-role
Policy	exastro-policy

* Required

Cancel

Previous

Create role

14. Check that the Role is there

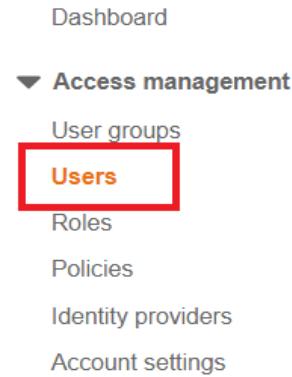
Search

Role name 

exastro-role

AWS Configuration manual

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



16.Click the "Add Users" button



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

The screenshot shows the 'Set user details' step of the 'Add user' wizard. It includes fields for 'User name' (containing 'exastro-user') and 'Access type'. The 'Programmatic access' checkbox is checked, and the 'AWS Management Console access' checkbox is unchecked. Step 1 is highlighted in blue.

Example)	
Username	exastro-user
Access type	Programmatic access

AWS Configuration manual

* Required Cancel [Next: Permissions](#)

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 'Create policy' button and a 'Filter policies' search bar containing 'exastro'. A table lists one result: 'exastro-policy' (Customer managed, Permissions policy (1)). The row for 'exastro-policy' is also highlighted with a red box.

Policy name	Type	Used as
exastro-policy	Customer managed	Permissions policy (1)

► Set permissions boundary

Cancel Previous Next: Tags

19. Press "Next step: Confirm"

The screenshot shows the 'Next step: Confirm' screen. It features three buttons: 'Cancel', 'Previous', and 'Next: Review'. The 'Next: Review' button is highlighted with a red box.

AWS Configuration manual

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>

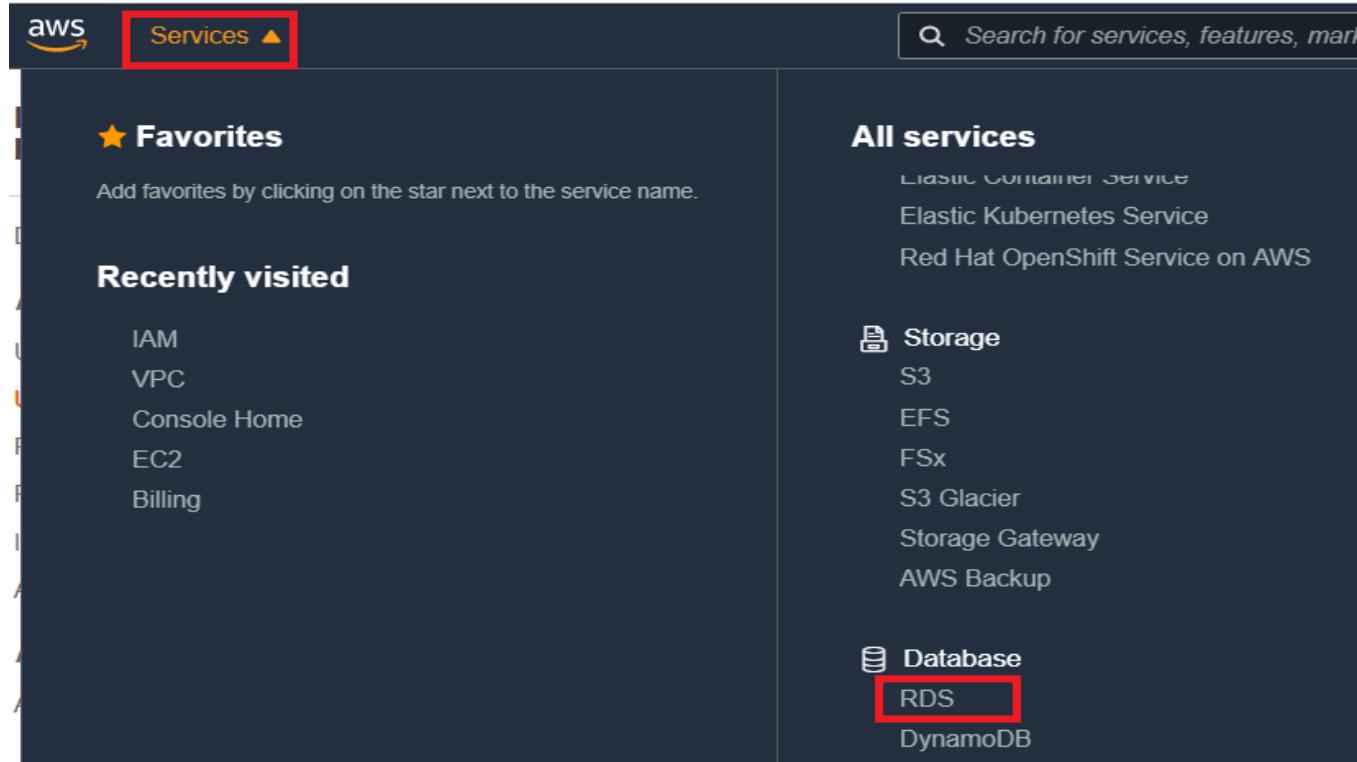
AWS Configuration manual

 Download .csv

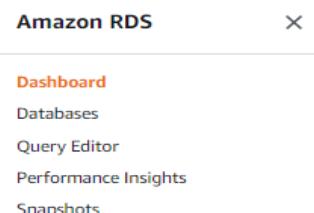
AWS Configuration manual

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

Automated backups

Reserved instances

Proxies

Subnet groups

Parameter groups

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
You won't be able to modify the name after your subnet group has been created.

Description

VPC
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.

Add subnets

Availability Zones
Choose the Availability Zones that include the subnets you want to add.

Subnets
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.

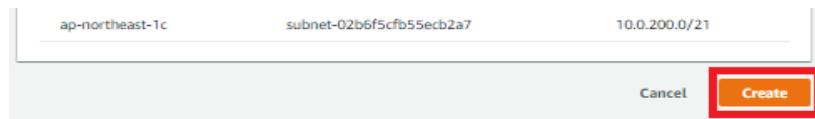
Subnets selected (2)

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

Example)

Name	exastrodb-subnet
Description	rds-subnet
VPC	exastro-VPC
Availability	ap-northeast-1a ap-northeast-1c
Subnet	subnet-097fba3cefdf69f30 (10.0.192.0/21) subnet-061dbdda51760b21d (10.0.200.0/21)

AWS Configuration manual



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

mariadb10.5

Group Name
Identifier for the DB parameter group

exastro-param

Description
Description for the DB parameter group

Test

Cancel Create

The 'Parameter group family' field, 'Group Name' field, and 'Description' field are highlighted with red boxes.

Example)

Parameter group family	mariadb10.5
Group name	exastro-param

7.Confirm that it has been created

RDS > Parameter groups	info
<p>Custom Default</p>	
Custom parameter groups (1)	
<input type="checkbox"/> Name	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 a parameter

Modify parameter group

Modifiable parameters (418)

explicit_defaults_for_timestamp

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

AWS Configuration manual

Modify parameter group

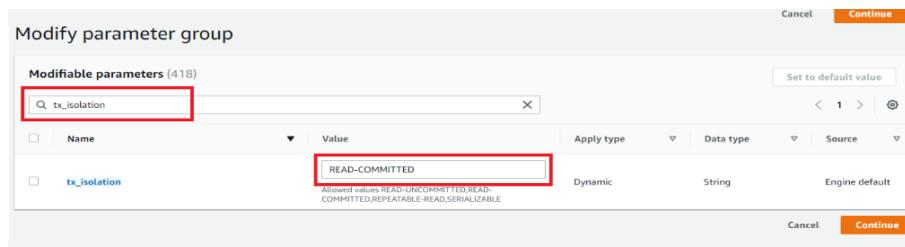
Modifiable parameters (418)

tx_isolation

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

Allowed values: READ-UNCOMMITTED, READ-COMMITTED, REPEATABLE-READ, SERIALIZABLE

Cancel Continue



AWS Configuration manual

Modify parameter group

Modifiable parameters (418)				
		Set to default value		
<input type="text" value="innodb_buffer_pool_size"/>		< 1 >		
Name	Value	Apply type	Data type	Source
<input type="checkbox"/> innodb_buffer_pool_size	<input type="text" value="536870912"/>	Dynamic	Integer	System default

Modifiable parameters (418)					
<input type="text"/> innodb_log_buffer_size		<input type="button" value="Set to default value"/>			
<input type="checkbox"/>	Name	Value	Apply type	Data type	
<input type="checkbox"/>	innodb_log_buffer_size	<input type="text" value="67108864"/>	Static	Integer	System default

Modifiable parameters (418)				
		Set to default value		
Name	Value	Apply type	Data type	Source
min_examined_row_limit	100	Dynamic	Integer	Engine default

Modifiable parameters (418)						Set to default value
<input type="checkbox"/> Name	Value	Apply type	Data type	Source		
<input checked="" type="checkbox"/> join_buffer_size	<input type="text" value="134217724"/>	Dynamic	Integer	Engine default	Cancel Save	

Modifiable parameters (418)					Set to default value
<input type="text" value="query_cache_size"/>					< 1 >
<input type="checkbox"/>	Name	Value	Apply type	Data type	Source
<input type="checkbox"/>	query_cache_size	<input type="text" value="536870912"/>	Dynamic	Integer	Engine default

Modify parameter group

Modifiable parameters (418)

Modifiable parameters (418)					Set to default value
<input type="text" value="query_cache_type"/>					< 1 >
<input type="checkbox"/>	Name	Value	Apply type	Data type	Source
<input type="checkbox"/>	query_cache_type	<input type="text" value="1"/>	Static	Integer	Engine default
Allowed values 0-2					

AWS Configuration manual

Modify parameter group

Modifiable parameters (418)

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

Allowed values 16384-1844674407370954752

Cancel Continue

AWS Configuration manual

The screenshots show the AWS RDS Modify parameter group interface. Each screen has a search bar at the top, a table of parameters, and a 'Continue' button at the bottom right.

- tmp_table_size:** The search bar contains "tmp_table_size". The table shows one row: tmp_table_size (Value: 67108864). The value field is highlighted with a red box.
- innodb_log_buffer_size:** The search bar contains "innodb_log_buffer_size". The table shows one row: innodb_log_buffer_size (Value: 67108864). The value field is highlighted with a red box.
- max_connections:** The search bar contains "max_connections". The table shows one row: max_connections (Value: 256). The value field is highlighted with a red box.
- character_set_server:** The search bar contains "character_set_server". The table shows one row: character_set_server (Value: utf8). The value field is highlighted with a red box.

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

AWS Configuration manual

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

The screenshot shows the 'Create database' configuration page. Several fields are highlighted with red boxes:

- Choose a database creation method:** 'Standard create' is selected.
- Engine options:** 'MariaDB' is selected.
- Version:** 'MariaDB 10.5.8' is selected.
- Templates:** 'Production' is selected.

※Field without examples can be left with the default value (Make sure 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



AWS Configuration manual

Region: exastro-rds
The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). 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
Type a login ID for the master user of your DB instance.
1 to 16 alphanumeric characters. First character must be a letter.

Auto generate a password
Amazon RDS can generate a password for you, or you can specify your own password.

Master password:
Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), (single quote), "(double quote) and @ (at sign).

Confirm password:

DB instance class

DB instance class: db.m6g.large
2 vCPUs 8 GiB RAM Network: 4,750 Mbps

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
Minimum: 100 GiB, Maximum: 65,536 GiB

Provisioned IOPS: 3000 IOPS
Minimum: 1,000 IOPS, Maximum: 80,000 IOPS

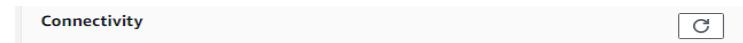
Storage autoscaling:
Provides dynamic scaling support for your database's storage based on your application's needs.

Enable storage autoscaling
Enabling this feature will allow the storage to increase once the specified threshold is exceeded.

Maximum storage threshold: 1000 GiB
Charges will apply when your database autoscales to the specified threshold
Minimum: 101 GiB, Maximum: 65,536 GiB

Availability & durability

AWS Configuration manual



AWS Configuration manual

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

exastro-VPC (vpc-09dbe5341dd5c28c0)

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.

exatrodbsubnet

Public access [Info](#)

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

No
RDS will 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 X default X

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 window for which you want automated backups of the database to be created by Amazon RDS

AWS Configuration manual

Select the period for which you want automated backups of the database to be created by Amazon KMS.

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. [Info](#)

AWS KMS Key [Info](#)
 ▾

AWS Configuration manual

Account
943001175239

KMS key ID
a73ddb74-38e3-4254-8607-d2a2bea62356

Performance Insights [Info](#)

Enable Performance Insights

Retention period [Info](#)

Default (7 days)

AWS KMS Key [Info](#)

(default) aws/rds

Account
943001175239

KMS key ID
a73ddb74-38e3-4254-8607-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

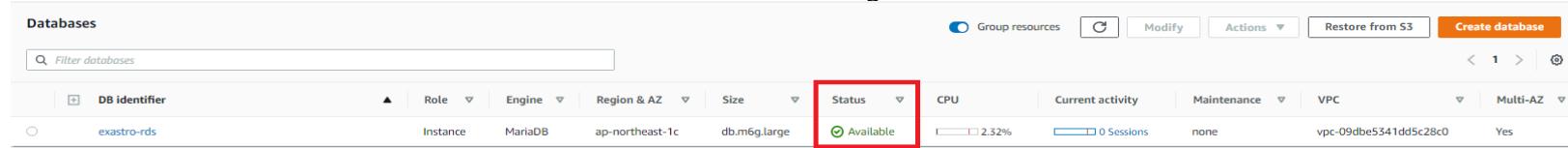
Duration
0.5 hours

Deletion protection

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

AWS Configuration manual

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

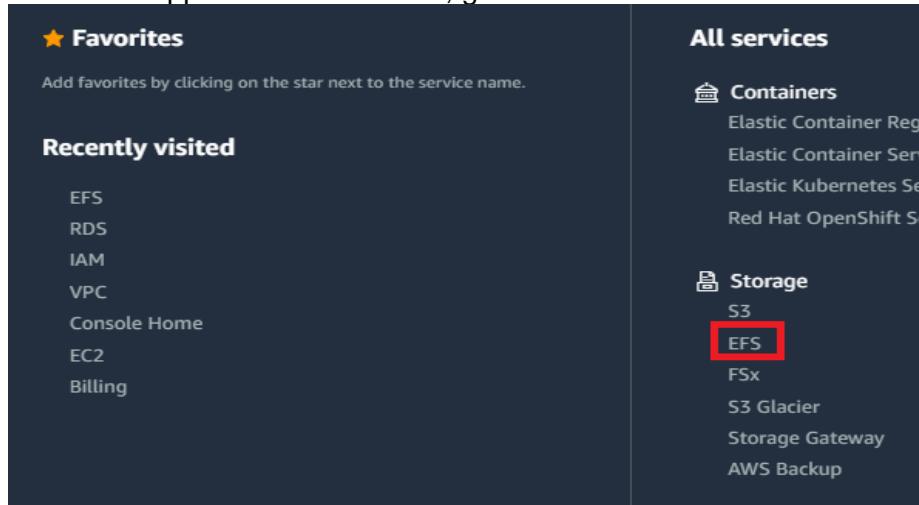


DB identifier	Role	Engine	Region & AZ	Size	Status	CPU	Current activity	Maintenance	VPC	Multi-AZ
exastro-rds	Instance	MariaDB	ap-northeast-1c	db.m6g.large	Available	<div style="width: 2.52%;">2.52%</div>	0 Sessions	none	vpc-09dbe5341dd5c28c0	Yes

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 X

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 D	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 the configuration is completed, click Next Step.

General

Name - optional
Name your file system.

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

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

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
Throughput fixed at specified amount

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

Network

Virtual Private Cloud (VPC)
Choose a VPC. Amazon EFS uses EC2 security groups to control access to your file system. [Learn more](#)

exastro-VPC

Mount targets
A mount target provides an NFSv4 endpoint at which you can mount an Amazon EFS file system. We recommend creating one mount target per Availability Zone. [Learn more](#)

Availability zone: ap-northeast-1a
Subnet ID: subnet-031fc186b7c1e20f5
IP address: Automatic

Security groups
Choose security groups
 sg-0d09125f091f12ca4 X
default
 sg-0df6f127b202f8ab8 X
exastro-efs
 Show less

Availability zone: ap-northeast-1c
Subnet ID: subnet-02cc4ae8f47e8f190
IP address: Automatic

Security groups
Choose security groups
 sg-0d09125f091f12ca4 X
default
 sg-0df6f127b202f8ab8 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 read-only access by default*
- Prevent anonymous access
- Enforce in-transit encryption for all clients

* Identity-based policies can override these default permissions.

Grant additional permissions

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-0d0c9125f091f2ca4
ap-northeast-1c	subnet-02cc4aebf47e8f190	-	sg-0df69f27b202f8abc, sg-0d0c9125f091f2ca4

Step 3: File system policy

File system policy

1

Edit

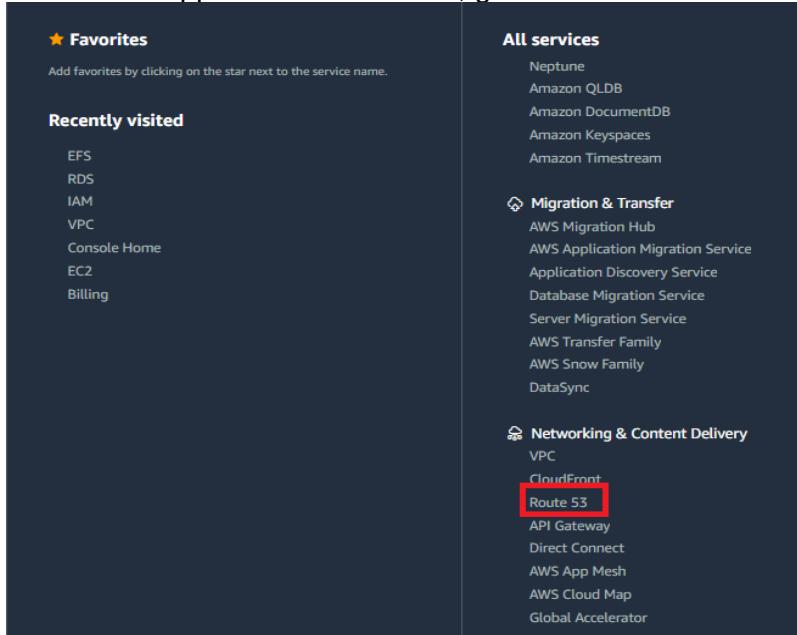
AWS Configuration manual



AWS Configuration manual

9.Route53

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



2.Press the "Create Hosted zone" button

The screenshot shows the 'DNS management' page. It includes a descriptive text about hosted zones and a large 'Create hosted zone' button, which is highlighted with a red box.

DNS management

A hosted zone tells Route 53 how to respond to DNS queries for a domain such as example.com.

Create hosted zone

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.

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](#)
 ▼ X

Tags [Info](#)
Apply tags to hosted zones to help organize and identify them.
No tags associated with the resource.

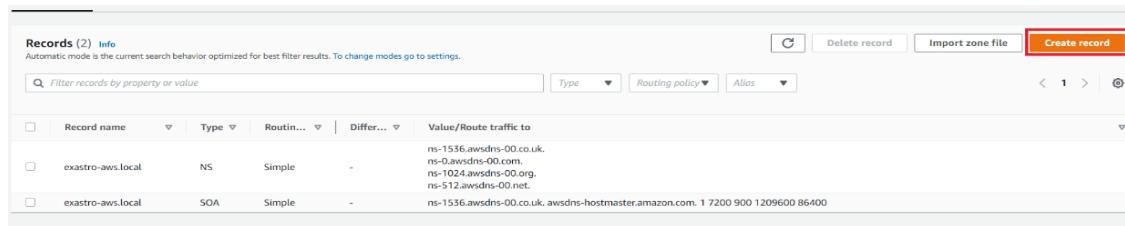
You can add up to 50 more tags.

4. Press the "Create Record" button

Example)

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

AWS Configuration manual



The screenshot shows the AWS Route 53 'Records' page. At the top, there are buttons for 'Info', 'Delete record', 'Import zone file', and a prominent 'Create record' button, which is highlighted with a red box. Below these are search and filter options: 'Filter records by property or value', dropdown menus for 'Type' (set to 'Routing policy'), 'Alias' (set to 'No'), and a page number indicator '1'. The main table lists two records:

Record name	Type	Routing policy	Differences	Value/Route traffic to
exastro-aws.local	NS	Simple	-	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
exastro-aws.local	SOA	Simple	-	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

AWS Configuration manual

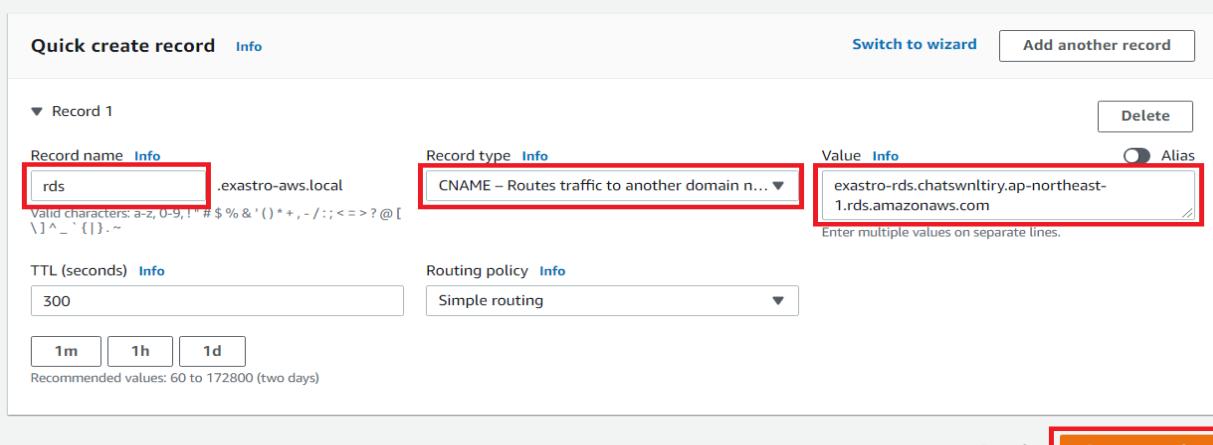
5. Select Record name and CNAME and then input the RDS Endpoint value.

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

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

Record name [Info](#) rds [Delete](#) Alias
Record type [Info](#) CNAME – Routes traffic to another domain n...
Value [Info](#) exastro-rds.chatswnliriy.ap-northeast-1.rds.amazonaws.com
Valid characters: a-z, 0-9, ! # \$ % & ' () * + , - / ; < = > ? @ [\] ^ _ { } . ~
TTL (seconds) [Info](#) 300 Routing policy [Info](#) Simple routing
1m 1h 1d Recommended values: 60 to 172800 (two days)

Cancel [Create records](#)



Example)

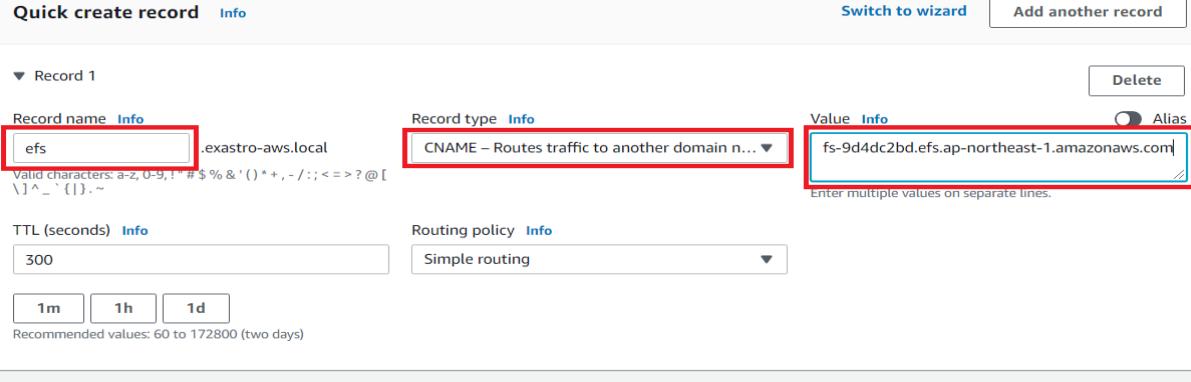
Record name	rds
Record type	CNAME
Value	RDS End point

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 [Delete](#) Alias
Record type [Info](#) CNAME – Routes traffic to another domain n...
Value [Info](#) fs-9d4dc2bd.efs.ap-northeast-1.amazonaws.com
Valid characters: a-z, 0-9, ! # \$ % & ' () * + , - / ; < = > ? @ [\] ^ _ { } . ~
TTL (seconds) [Info](#) 300 Routing policy [Info](#) Simple routing
1m 1h 1d Recommended values: 60 to 172800 (two days)

Cancel [Create records](#)



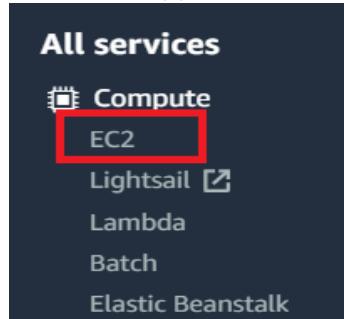
Example)

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"



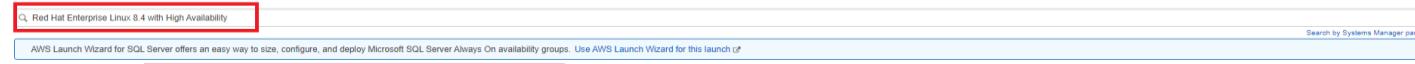
2.Click "Launch Instance"

The screenshot shows the 'Launch instance' step of the AWS Launch Wizard. A red box highlights the 'Launch instance' button. The 'Account attributes' and 'Explore AWS' sections are also visible on the right side of the screen.

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 insta

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.



AWS Configuration manual

The screenshot shows the AWS Marketplace interface. On the left, a sidebar lists navigation options: Quick Start (0), My AMIs (0), AWS Marketplace (1) (which is selected and highlighted in orange), and Community AMIs (0). Below these are Categories and All Categories. A red box highlights the AWS Marketplace section. In the main content area, a product card for "Red Hat Enterprise Linux 8.4 with High Availability" is displayed. The card includes a small icon of a red hat, the product name, a rating of 4 stars, and the developer "Amazon Web Services". It also shows "Linux/Unix, Red Hat Enterprise Linux 8 | 64-bit (x86) Amazon Machine Image (AMI)" and the update date "Updated: 6/29/21". A "Select" button is located at the bottom right of the card.

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 to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

The screenshot shows the AWS Step 2: Choose an Instance Type page. The search bar at the top contains 'exastro'. A note below says 'Note: The vendor recommends using a m4.large instance (or larger) for the best experience with this product.' The table lists various instance types across families (t2, m3, etc.) with columns for Family, Type, vCPUs, Memory (GB), Instance Storage (GB), EBS-Optimized Available, Network Performance, and IPv4 Support. The 'm3.micro' row is highlighted with a red border. At the bottom, there are buttons for 'Cancel', 'Previous', 'Review and Launch', and 'Next: Configure Instance Details'.

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

The screenshot shows the AWS Step 3: Configure Instance Details page. It includes fields for Number of instances (1), Purchasing option (Request Spot instances), Network (exastro-VPC), Subnet (public-a), Auto-assign Public IP (Enable), IAM role (exastro-role), CPU options, Shutdown behavior (Stop), EBS-optimized instance (Shared - Run a shared hardware instance), Credit specification (Unlimited), and File systems. The 'Network' and 'Subnet' fields are highlighted with red borders. The 'Auto-assign Public IP' and 'IAM role' fields are also highlighted with red borders. At the bottom, there is a 'Network interfaces' section with a table showing Device (eth0), Network Interface (Auto-assign), Subnet (public-a), Primary IP (None), Secondary (None), IPv6 IPs (None), IPv4 Prefixes (None), and IPv6 Prefixes (None). A note states 'The selected subnet does not support IPv6 because it does not have an IPv6 CIDR.'

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

AWS Configuration manual

Add Device

Advanced Details

Enclave Enabled Enabled V1 and V2 (token optional)

Metadata accessible Metadata version Metadata token response hop limit

Metadata token response hop limit User data As text As file Input It already base64 encoded
(Optional)

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



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 (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-0c2aa1e8396810460	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 free 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 case-sensitive 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	(128 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-0d0c9125f091f2ca4	default	default VPC security group	Copy to new
sg-0df69f27b2028abc	exastro-efs	exastro-vpc	Copy to new
sg-04e516265564a9f7e	exastro-rds	test	Copy to new
sg-0c4e830313c3e3dc1	exastro-sg	test	Copy to new

Inbound rules for sg-0c4e830313c3e3dc1 (Selected security groups: sg-0c4e830313c3e3dc1)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	[REDACTED]	
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	[REDACTED]	
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.
Root Device Type: ebs Virtualization type: hvm

Hourly Software Fees: \$0.00 per hour on t3 small instance. Additional taxes 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	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t3.small	-	2	2	EBS only	Yes	Up to 5 Gigabit

Security Groups

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

All selected security groups inbound rules

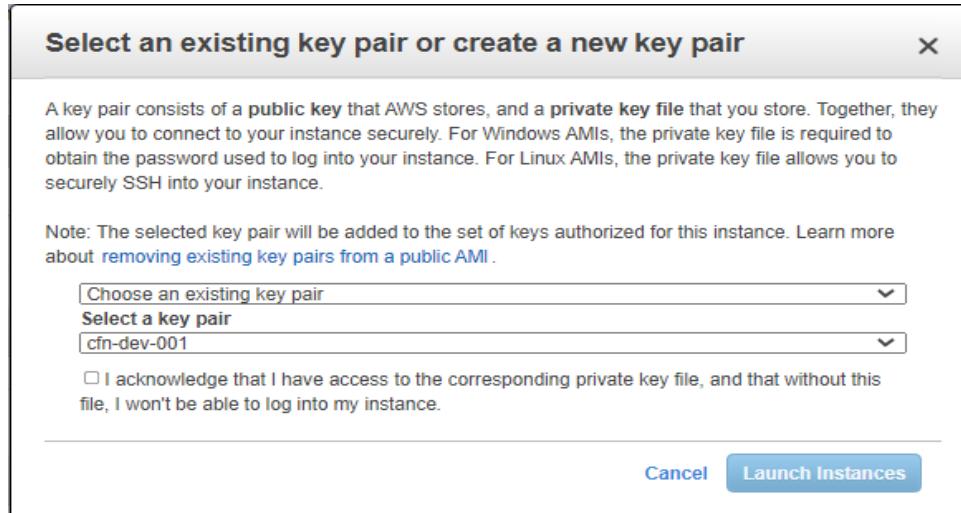
Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	[REDACTED]	
Custom TCP Rule	TCP	2224	0.0.0.0/0	
SSH	TCP	22	0.0.0.0/0	
Custom UDP Rule	UDP	5404 - 5405	0.0.0.0/0	
Custom TCP Rule	TCP	3121	0.0.0.0/0	
MySQL/Aurora	TCP	3306	0.0.0.0/0	
HTTPS	TCP	443	[REDACTED]	

AWS Configuration manual

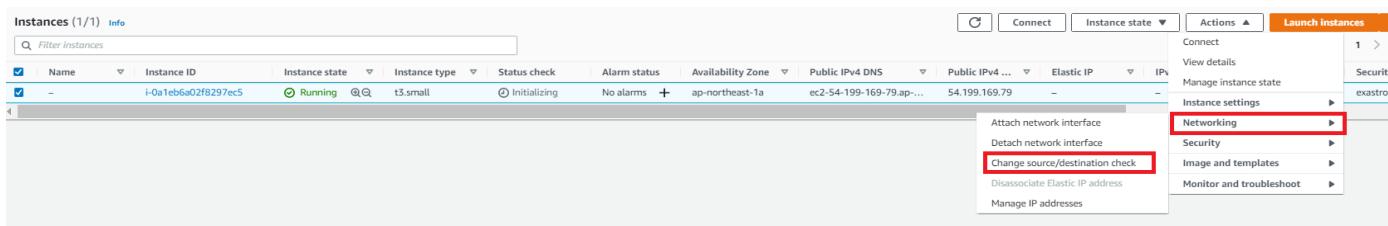


AWS Configuration manual

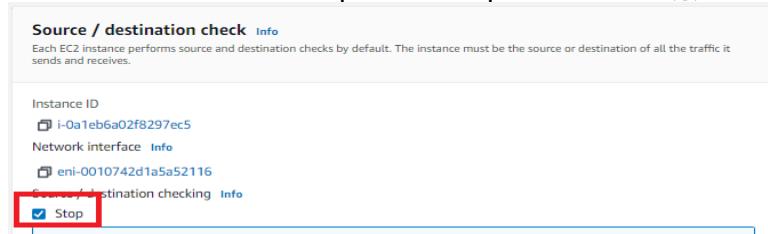
10.If you need a key for SSH, create it here



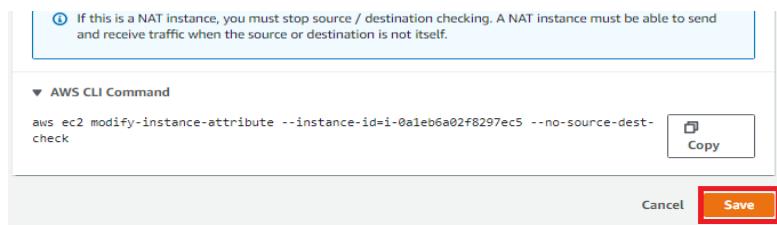
11.After creating it, go to Action ->Networking->Change source/destination deck



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



AWS Configuration manual



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](#)
 [X](#)

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](#)

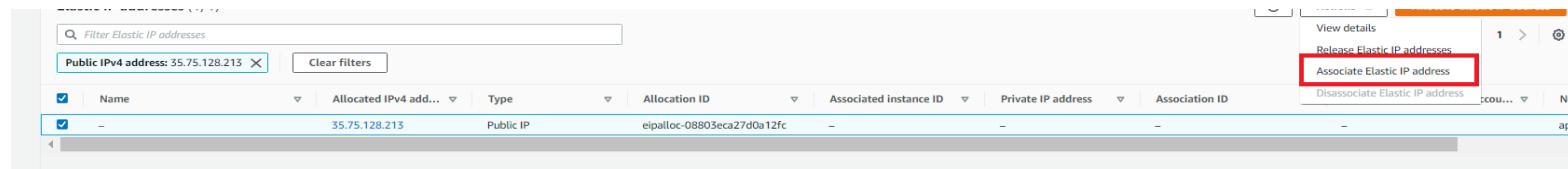
You can add up to 50 more tag

[Cancel](#) [Allocate](#)

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



AWS Configuration manual



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 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

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

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

This concludes the AWS settings.

The next slides will be a step to 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	Remarks
			(※When "Master" and "Slave" server configuration is required, please configure them in parallel)	
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-1.8.0 -type f xargs -l{} 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
3-1	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_bulk_excel-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 ● systemctl stop ky_terraform_execute-workflow.service ● systemctl stop ky_terraform_checkcondition-workflow.service ● systemctl stop ky_terraform_varsautolistup-workflow.service ● systemctl stop ky_terraform_valautosetup-workflow.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_bulk_excel-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
			<code>systemctl disable ky_terraform_execute-workflow.service systemctl disable ky_terraform_checkcondition-workflow.service systemctl disable ky_terraform_varsautolistup-workflow.service systemctl disable ky_terraform_valautosetup-workflow.service</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
4.EFS Settings				
4-1	Configure the timezone to Asia/Tokyo	●	timedatectl set-timezone Asia/Tokyo	
4-2	Prepare EFS for usage	●	<pre>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</pre>	
4-3	Configure EFS Common files	●	<pre>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</pre>	Change the red text to fit your environment Perform this step after you have created EFS from the AWS Console

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.	●	<pre>vi /etc/systemd/system/mount-nfs-sequentially.service</pre> <p>[Unit] Description=Workaround for mounting NFS file systems sequentially at boot time After=remote-fs.target</p> <p>[Service] Type=oneshot ExecStart=/bin/mount -avt nfs4 RemainAfterExit=yes</p> <p>[Install] WantedBy=multi-user.target</p>	
		●	<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				
requis	•RDS is created •ITA is installed			
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>'@'%' 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 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] 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	● ●	<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.loc", the following command can be used to get a string with base64 and rot13.</p> <p><code>echo -ne "mysql:dbname=ITA_DB;host=rds.exastro-aws.loc" 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>	
	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>	
5-5	Stop MariaDB	● ●	<code>systemctl disable mariadb</code> <code>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 mariadberrmsg.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	Remarks
			(※When "Master" and "Slave" server configuration is required, please configure them in parallel)	
6.Pacemaker preparation				
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 w
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
7.Pacemaker settings				
7-1	Configure password for the "hacluster" user ID (pcs admin account).	● ●	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
7-2	Start pcasd service and configure pcasd so it is active when the system starts.	● ●	systemctl enable pcasd systemctl start pcasd systemctl status pcasd	
7-3	Authenticate cluster	●	pcs host auth \${ha1_name} \${ha2_name} Username: hacluster Password:(Password set with "passwd hacluster")	Change the red text to fit your environment
7-4	Specify cluster and start	●	pcs cluster setup aws-cluster --start <ita-ha-sv01 host name> <ita-ha-sv02 host name> --force	
7-5	Configure the clusters so they run automatically	●	pcs cluster enable --all	
7-6	STONITH (Shoot The Other Node In The Head) オプションを無効にする	●	pcs property set stonith-enabled=false	
7-7	Deactivate STONITH (Shoot The Other Node In The Head) option	●	pcs property set no-quorum-policy=ignore	
7-8	Configure attribute wait time.	●	pcs property set transition-delay="0s"	
7-9	Deactivate automatic failback.	●	pcs resource defaults resource-stickiness="INFINITY" migration-threshold="1"	
7-10	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
7-11	Treat the Pacemaker internal process like a Node failure if something happens to it	● ●	sed -i 's/^\! PCMK_\fail_\fast.*\$/PCMK_fail_fast=yes/' /etc/sysconfig/pacemaker	
7-12	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	
7-13	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- pcmk.suppressions --gen-suppressions=all" AWS_DEFAULT_REGION=ap-northeast-1 ←Described 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)

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
7-14	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	
7-15	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="120s" interval="0s" on-fail="restart" \ op monitor timeout="20s" interval="30s" on-fail="restart" \ op stop timeout="120s" interval="0s" on-fail="block"	Change the red text to fit your environment
7-16	Configure httpd and eip resource group	●	pcs resource group add exastro httpd eip	
7-17	Configure EFS Resources	●	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' fstype='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' fstype='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' fstype='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' fstype='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' fstype='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' fstype='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' fstype='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' fstype='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' fstype='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' fstype='nfs' pcs resource create menus_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' fstype='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
7-18	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>	
7-19	Configure ky file resources	●	<pre>pcs resource create ky_activedirectory_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_bulk_excel-workflow systemd:ky_bulk_excel-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 \ </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	Remarks
			(※When "Master" and "Slave" server configuration is required, please configure them in parallel)	
			op start interval=0s timeout=60 \ op stop interval=0s timeout=60	

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
7-19	Configure ky file resources (Continued from last page)		<pre>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 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
			pcs resource create ky_terraform_execute-workflow systemd:ky_terraform_execute-workflow \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60	

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
7-19	Configure ky file resources (Continued from last page)		<pre>pcs resource create ky_terraform_checkcondition-workflow systemd:ky_terraform_checkcondition-workflow \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_terraform_varsautolistup-workflow systemd:ky_terraform_varsautolistup-workflow \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60 pcs resource create ky_terraform_valautosetup-workflow systemd:ky_terraform_valautosetup-workflow \ op monitor interval=30 timeout=60 \ op start interval=0s timeout=60 \ op stop interval=0s timeout=60</pre>	
7-20	Group ky resources	●	<pre>pcs resource group add ky_services ky_activedirectory_roleuser_replication-workflow ky_ansible_execute-workflow ky_ansible_towermasterSync-workflow ky_bulk_excel-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 ky_terraform_execute-workflow ky_terraform_checkcondition-workflow ky_terraform_varsautolistup-</pre>	
7-21	Specify the resources created up until this point and specify the recourse group start/stop s	●	<pre>pcs constraint order set efsmount ky_services exastro</pre>	
7-22	Specify the constraint where all the resources created up until this point will start in the sam	●	<pre>pcs constraint colocation set efsmount ky_services exastro</pre>	
7-23	Start the HA Software services	● ●	<pre>systemctl enable corosync systemctl enable pacemaker systemctl start corosync systemctl start pacemaker</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
7-24	Confirm the Cluster status	● ●	<p>pcs status</p> <p>(Display example)</p> <p>Cluster Summary:</p> <ul style="list-style-type: none"> * 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 <p>Node List:</p> <ul style="list-style-type: none"> * Online: [<ita-ha-sv01's host name> <ita-ha-sv02's host name> —Both master and slave are online <p>Full List of Resources:</p> <ul style="list-style-type: none"> * Resource Group: exastro: <ul style="list-style-type: none"> * 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: <ul style="list-style-type: none"> * 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> * temp (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: <ul style="list-style-type: none"> ~~~~~ Abbr ~~~~~ <p>Daemon Status:</p> <ul style="list-style-type: none"> corosync: active/enabled pacemaker: active/enabled pcsd: active/enabled 	Change the red text to fit your environment
7-25	Check ITA Connection	●	Use the URL below to access the Login screen http(s)://(ElasticIP)	Change the red text to fit your environment
7-26	Delete MariaDB	● ●	yum list installed grep -i mariadb 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	Delete MariaDB only after you have checked that ITA can be accessed successfully.

End of Procedure