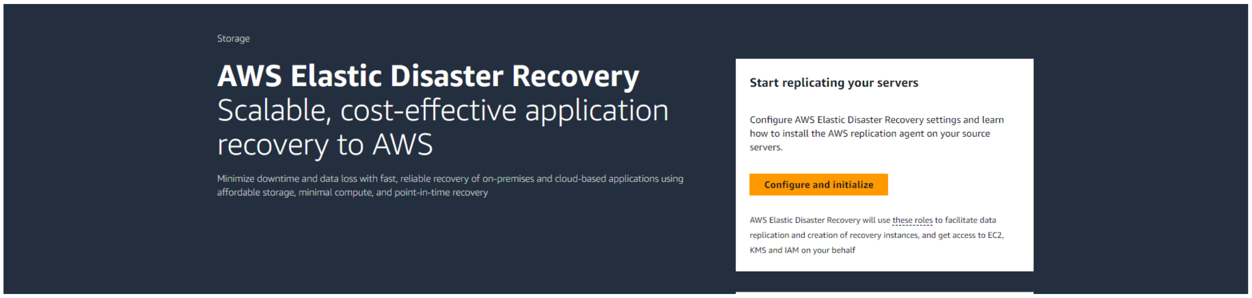
Short Description: Automation to setup AWS Elastic Disaster Recovery for all customers including new ones

Description: There are two parts in Elastic disaster recovery:

1. DRS configuration in Recovery region
2. Replication agent configuration in Instance

DRS Configuration:

1. Navigate to AWS Elastic Disaster Recovery (AWS DRS) in the AWS Management Console.



Storage

AWS Elastic Disaster Recovery
Scalable, cost-effective application recovery to AWS

Minimize downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery

Start replicating your servers

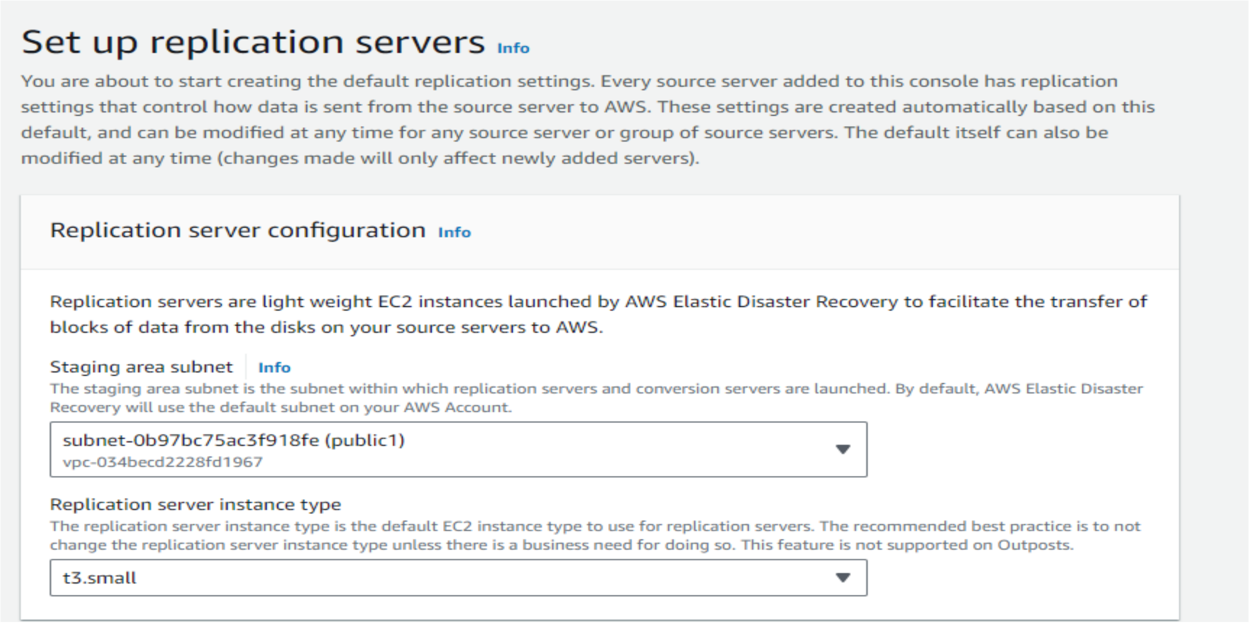
Configure AWS Elastic Disaster Recovery settings and learn how to install the AWS replication agent on your source servers.

AWS Elastic Disaster Recovery will use these roles to facilitate data replication and creation of recovery instances, and get access to EC2, KMS and IAM on your behalf

You can use the default setting, by simply choosing Next on each of the pages in this wizard or modify any of the settings to best fit your needs.

2. Specify the subnets and instance type for the replication server.

   - Staging area subnet.
   - Replication server instance type.



Set up replication servers Info

You are about to start creating the default replication settings. Every source server added to this console has replication settings that control how data is sent from the source server to AWS. These settings are created automatically based on this default, and can be modified at any time for any source server or group of source servers. The default itself can also be modified at any time (changes made will only affect newly added servers).

Replication server configuration Info

Replication servers are light weight EC2 instances launched by AWS Elastic Disaster Recovery to facilitate the transfer of blocks of data from the disks on your source servers to AWS.

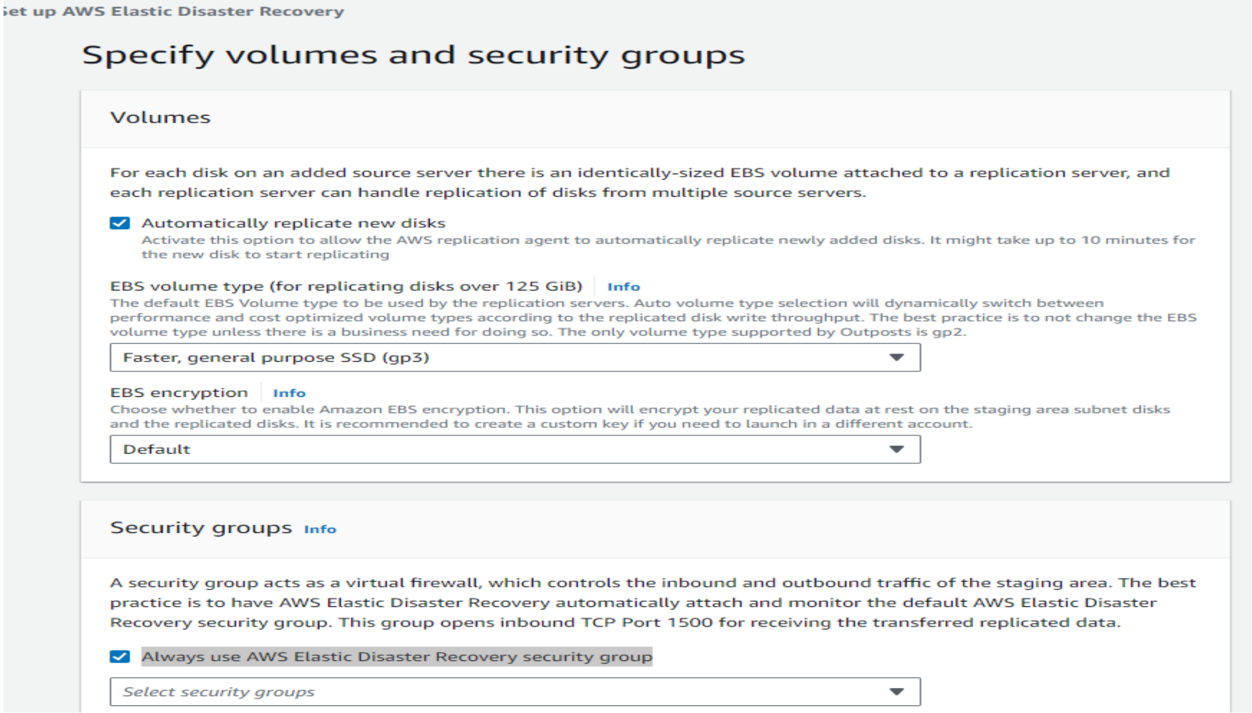
Staging area subnet Info
The staging area subnet is the subnet within which replication servers and conversion servers are launched. By default, AWS Elastic Disaster Recovery will use the default subnet on your AWS Account.

subnet-0b97bc75ac3f918fe (public1)
vpc-034becd2228fd1967

Replication server instance type
The replication server instance type is the default EC2 instance type to use for replication servers. The recommended best practice is to not change the replication server instance type unless there is a business need for doing so. This feature is not supported on Outposts.

t3.small

3. Specify volumes and security groups
    - Select Automatically replicate new disks/specific disks.
    - EBS (Elastic Block Store) Volume type Faster, general purpose SSD (gp3)
    - Encryption Default/specific encryption.
    - Security groups- Select Always use AWS Elastic Disaster Recovery security group/specific security group for disaster recovery for EDR. (Permissions: 443, TCP 1500)



;et up AWS Elastic Disaster Recovery

Specify volumes and security groups

Volumes

For each disk on an added source server there is an identically-sized EBS volume attached to a replication server, and each replication server can handle replication of disks from multiple source servers.

☑ Automatically replicate new disks
Activate this option to allow the AWS replication agent to automatically replicate newly added disks. It might take up to 10 minutes for the new disk to start replicating

EBS volume type (for replicating disks over 125 GiB) Info
The default EBS Volume type to be used by the replication servers. Auto volume type selection will dynamically switch between performance and cost optimized volume types according to the replicated disk write throughput. The best practice is to not change the EBS volume type unless there is a business need for doing so. The only volume type supported by Outposts is gp2.

Faster, general purpose SSD (gp3)

EBS encryption Info
Choose whether to enable Amazon EBS encryption. This option will encrypt your replicated data at rest on the staging area subnet disks and the replicated disks. It is recommended to create a custom key if you need to launch in a different account.

Default

Security groups Info

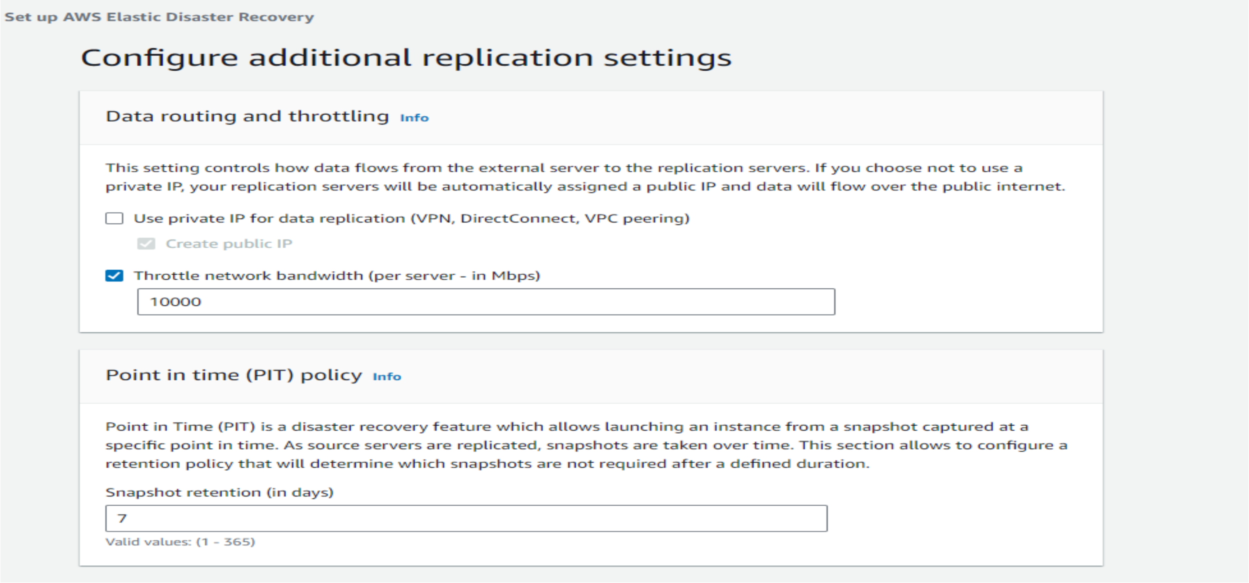
A security group acts as a virtual firewall, which controls the inbound and outbound traffic of the staging area. The best practice is to have AWS Elastic Disaster Recovery automatically attach and monitor the default AWS Elastic Disaster Recovery security group. This group opens inbound TCP Port 1500 for receiving the transferred replicated data.

☑ Always use AWS Elastic Disaster Recovery security group

Select security groups

Click Next.

4. Choose a public IP/private IP for the public replication server.
   - For Private IP, there should be a connection between replication server VPC and source server VPC.
   - Throttle network bandwidth (per server - in Mbps)- specify bandwidth
   - Point in time (PIT) policy – specify PIT in Days



Set up AWS Elastic Disaster Recovery

Configure additional replication settings

Data routing and throttling Info

This setting controls how data flows from the external server to the replication servers. If you choose not to use a private IP, your replication servers will be automatically assigned a public IP and data will flow over the public internet.

☐ Use private IP for data replication (VPN, DirectConnect, VPC peering)

☑ Create public IP

☑ Throttle network bandwidth (per server - in Mbps)

10000

Point in time (PIT) policy Info

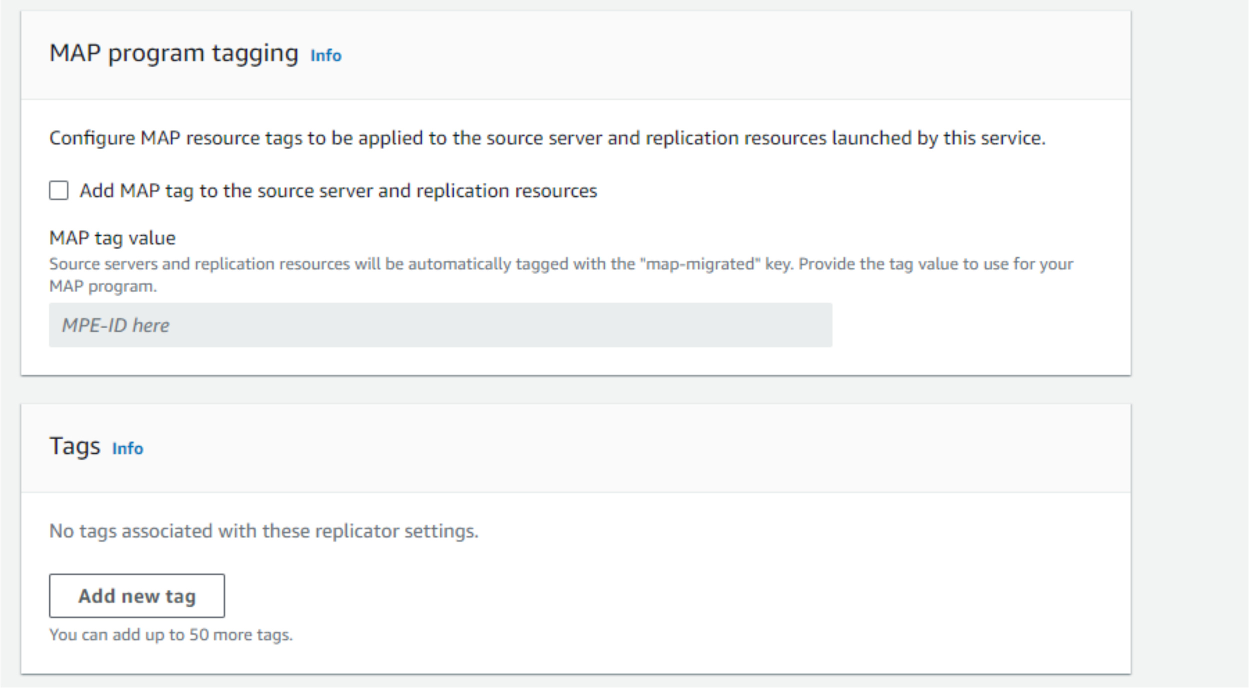
Point in Time (PIT) is a disaster recovery feature which allows launching an instance from a snapshot captured at a specific point in time. As source servers are replicated, snapshots are taken over time. This section allows to configure a retention policy that will determine which snapshots are not required after a defined duration.

Snapshot retention (in days)

7

Valid values: (1 - 365)

5. Specify tags



MAP program tagging Info

Configure MAP resource tags to be applied to the source server and replication resources launched by this service.

☐ Add MAP tag to the source server and replication resources

MAP tag value

Source servers and replication resources will be automatically tagged with the "map-migrated" key. Provide the tag value to use for your MAP program.

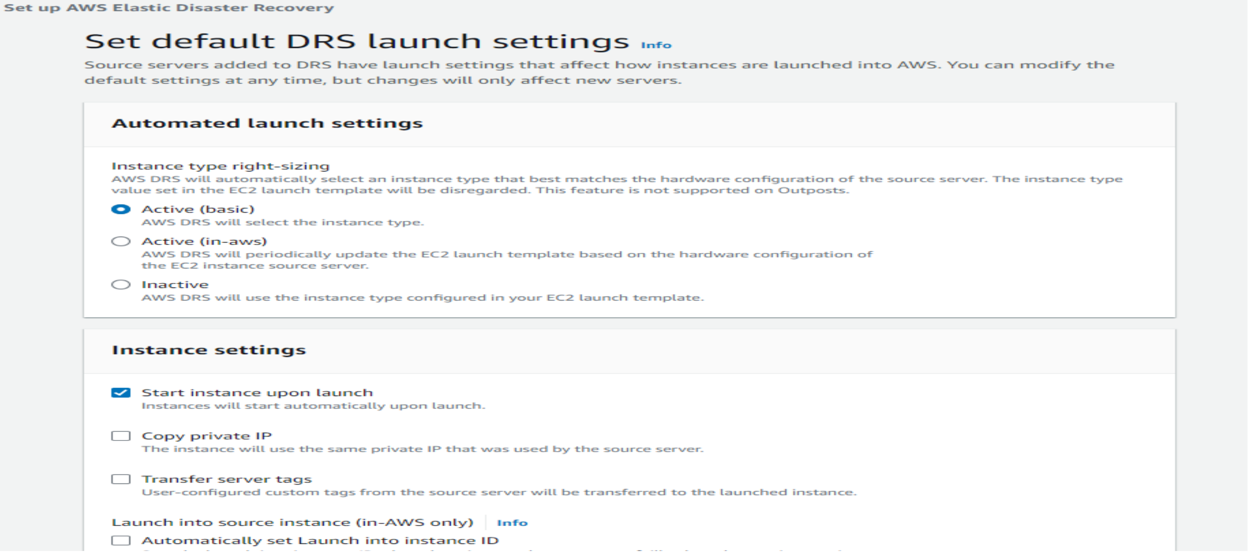
MPE-ID here

Tags Info

No tags associated with these replicator settings.

You can add up to 50 more tags.

6. Specify the launch template for the source server that will be launched in DR region.
    - Specify Automated launch settings
    - Specify Instance settings
    - Specify Licensing



Set up AWS Elastic Disaster Recovery

Set default DRS launch settings Info

Source servers added to DRS have launch settings that affect how instances are launched into AWS. You can modify the default settings at any time, but changes will only affect new servers.

Automated launch settings

Instance type right-sizing
AWS DRS will automatically select an instance type that best matches the hardware configuration of the source server. The instance type value set in the EC2 launch template will be disregarded. This feature is not supported on Outposts.

● Active (basic)
AWS DRS will select the instance type.

○ Active (in-aws)
AWS DRS will periodically update the EC2 launch template based on the hardware configuration of the EC2 instance source server.

○ Inactive
AWS DRS will use the instance type configured in your EC2 launch template.

Instance settings

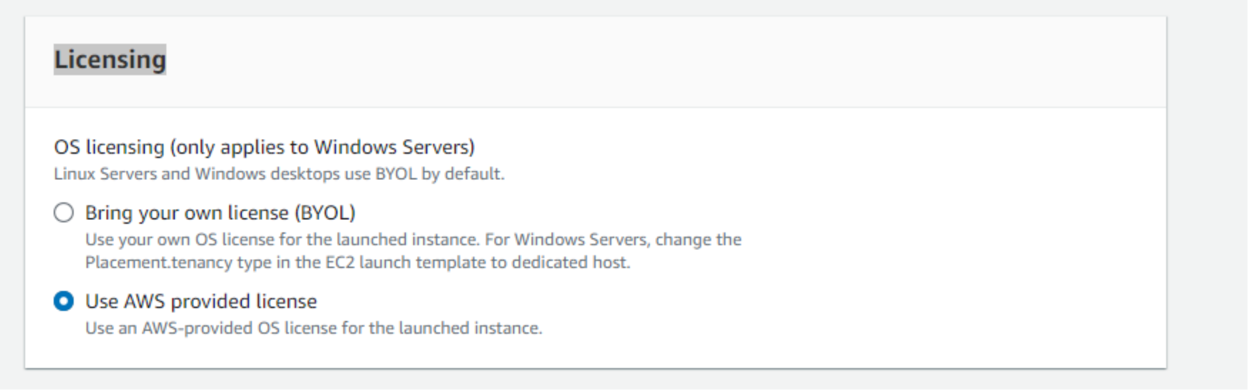
☑ Start instance upon launch
Instances will start automatically upon launch.

☐ Copy private IP
The instance will use the same private IP that was used by the source server.

☐ Transfer server tags
User-configured custom tags from the source server will be transferred to the launched instance.

Launch into source instance (in-AWS only) | Info

☐ Automatically set Launch into instance ID



Licensing

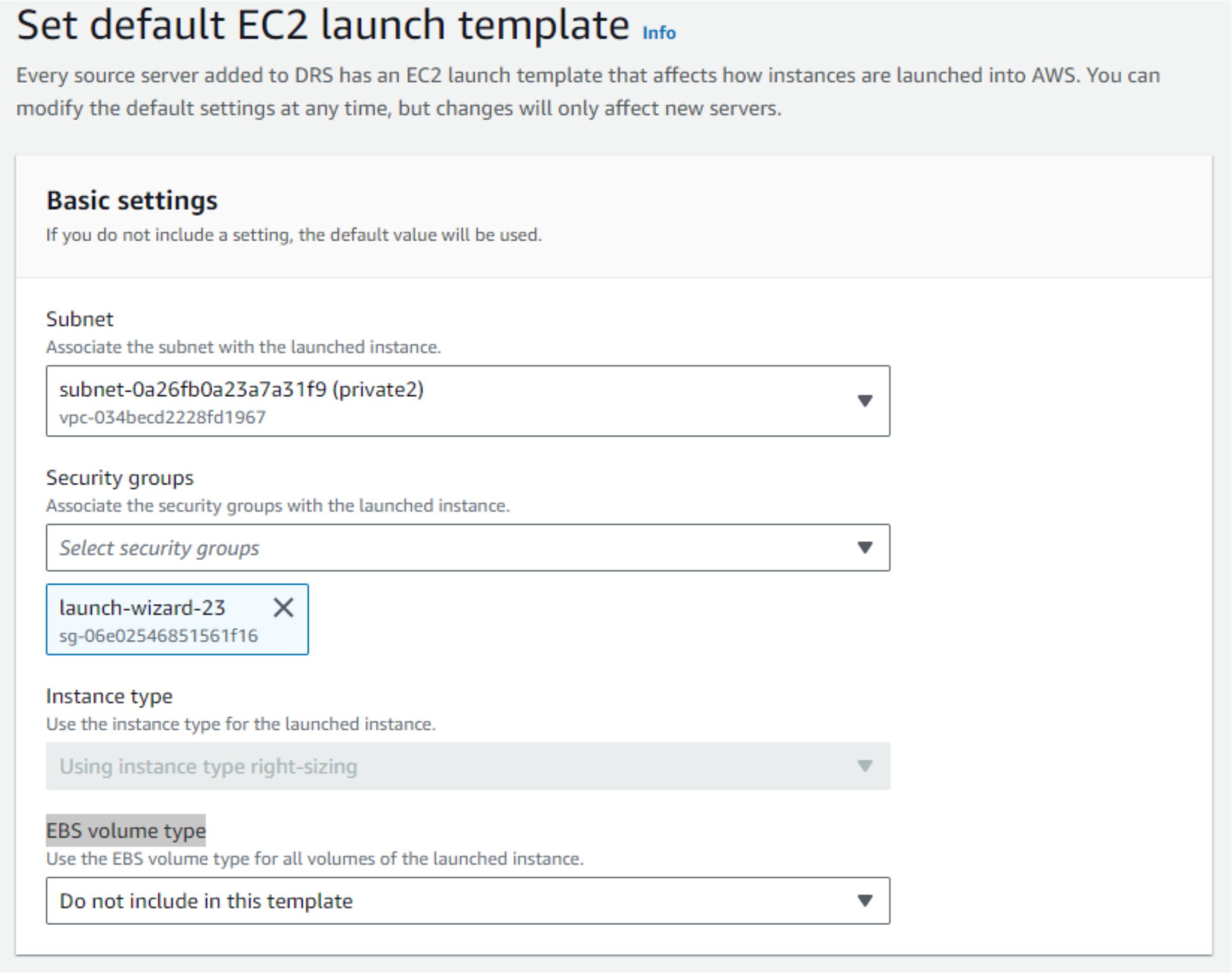
OS licensing (only applies to Windows Servers)
Linux Servers and Windows desktops use BYOL by default.

○ Bring your own license (BYOL)
Use your own OS license for the launched instance. For Windows Servers, change the Placement.tenancy type in the EC2 launch template to dedicated host.

● Use AWS provided license
Use an AWS-provided OS license for the launched instance.

Click Next.

7. Set default EC2 launch template for DR region:
    - Subnet- Free text
    - Security groups
    - Instance type
    - EBS volume type



Set default EC2 launch template

Every source server added to DRS has an EC2 launch template that affects how instances are launched into AWS. You can modify the default settings at any time, but changes will only affect new servers.

Basic settings

If you do not include a setting, the default value will be used.

Subnet

Associate the subnet with the launched instance.

subnet-0a26fb0a23a7a31f9 (private2)
vpc-034becd2228fd1967

Security groups

Associate the security groups with the launched instance.

Select security groups

launch-wizard-23
sg-06e02546851561f16

Instance type

Use the instance type for the launched instance.

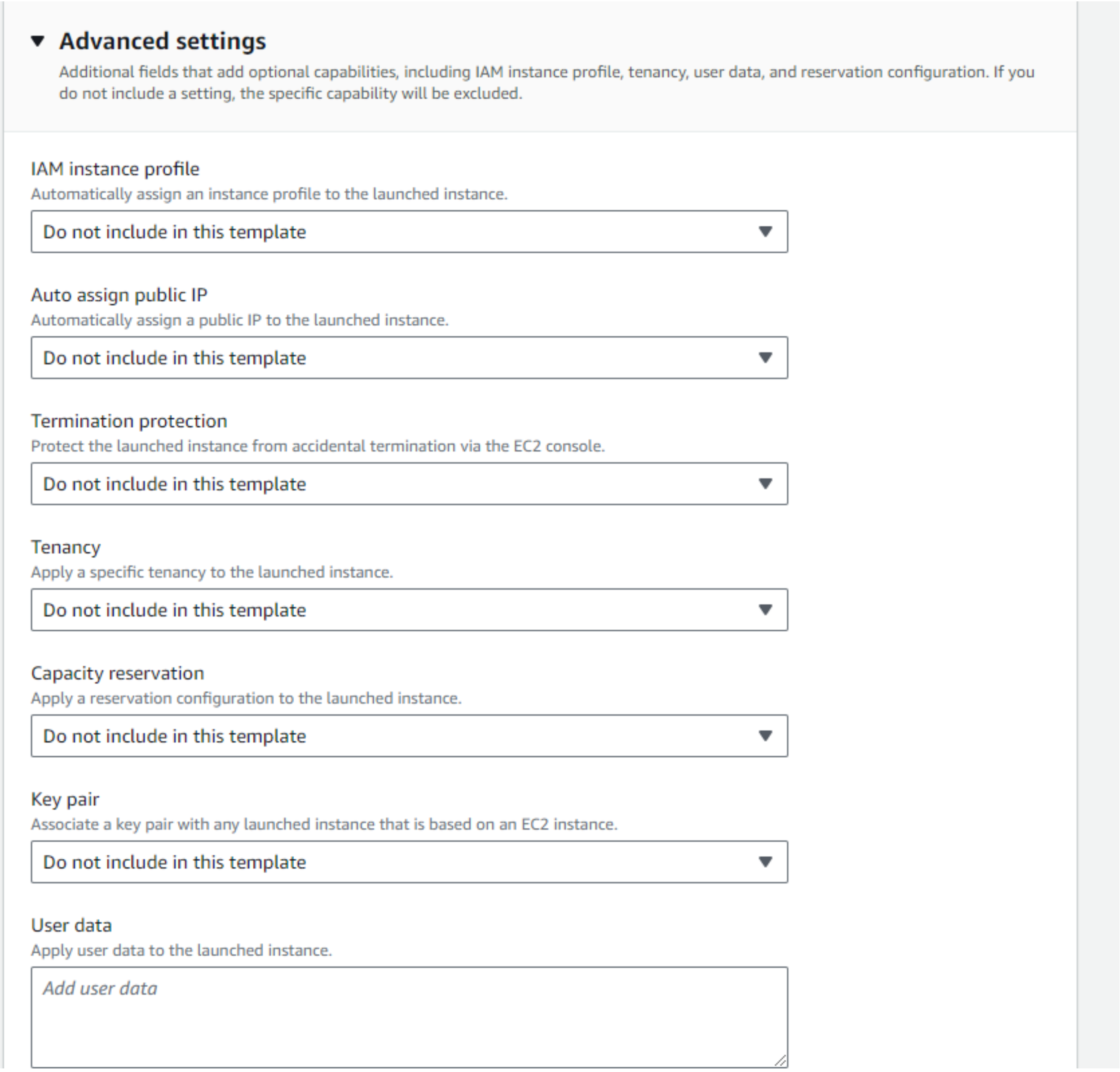
Using instance type right-sizing

EBS volume type

Use the EBS volume type for all volumes of the launched instance.

Do not include in this template

8. Advanced settings
    - IAM Instance profile
    - Tenancy
    - Key Pair
    - Other option: Default/specific for DR Instance



▼ **Advanced settings**

Additional fields that add optional capabilities, including IAM instance profile, tenancy, user data, and reservation configuration. If you do not include a setting, the specific capability will be excluded.

IAM instance profile
Automatically assign an instance profile to the launched instance.
Do not include in this template ▼

Auto assign public IP
Automatically assign a public IP to the launched instance.
Do not include in this template ▼

Termination protection
Protect the launched instance from accidental termination via the EC2 console.
Do not include in this template ▼

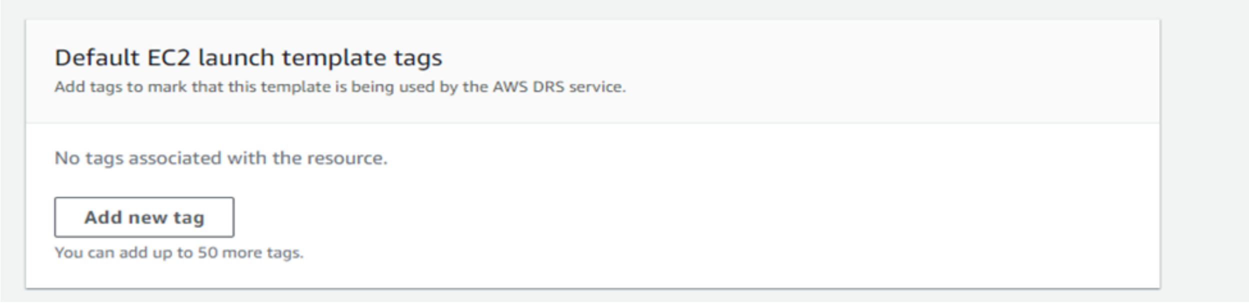
Tenancy
Apply a specific tenancy to the launched instance.
Do not include in this template ▼

Capacity reservation
Apply a reservation configuration to the launched instance.
Do not include in this template ▼

Key pair
Associate a key pair with any launched instance that is based on an EC2 instance.
Do not include in this template ▼

User data
Apply user data to the launched instance.
Add user data

9. Default EC2 launch template tags:



Default EC2 launch template tags

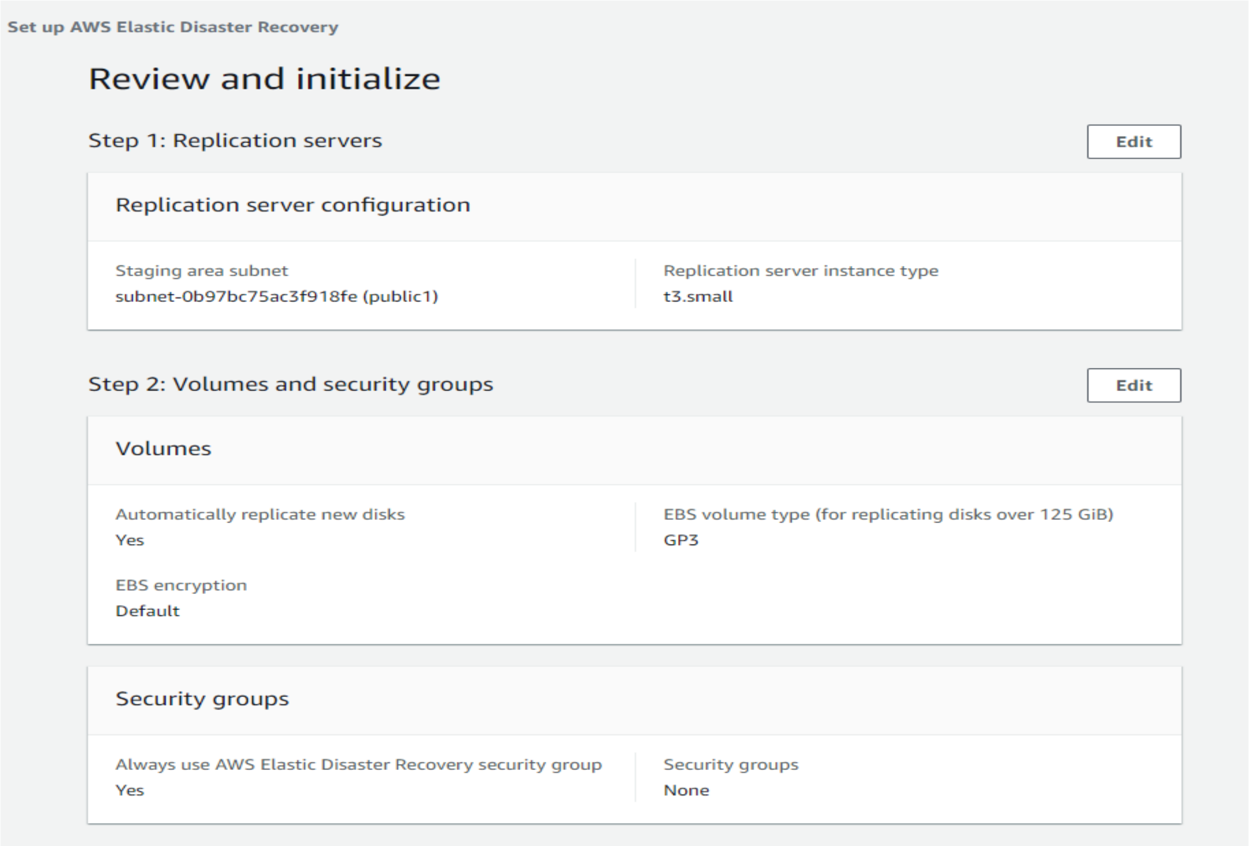
Add tags to mark that this template is being used by the AWS DRS service.

No tags associated with the resource.

You can add up to 50 more tags.

Click Next.

10. Review and initialize - Configure and initialize



Set up AWS Elastic Disaster Recovery

Review and initialize

Step 1: Replication servers

Replication server configuration

Staging area subnet
subnet-0b97bc75ac3f918fe (public1)

Replication server instance type
t3.small

Step 2: Volumes and security groups

Volumes

Automatically replicate new disks
Yes

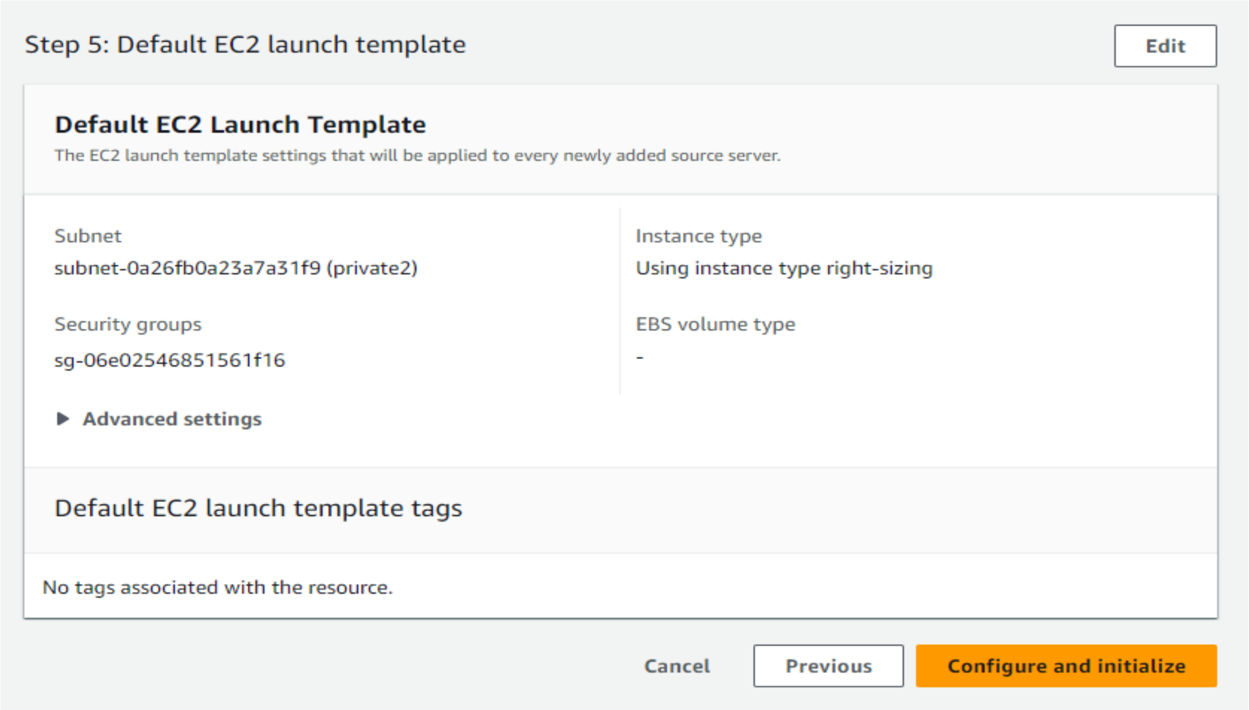
EBS volume type (for replicating disks over 125 GiB)
GP3

EBS encryption
Default

Security groups

Always use AWS Elastic Disaster Recovery security group
Yes

Security groups
None



Step 5: Default EC2 launch template

Default EC2 Launch Template

The EC2 launch template settings that will be applied to every newly added source server.

Subnet
subnet-0a26fb0a23a7a31f9 (private2)

Instance type
Using instance type right-sizing

Security groups
sg-06e02546851561f16

EBS volume type
-

Default EC2 launch template tags

No tags associated with the resource.

Replication agent installation and configuration in DC instances:

1. Access the EC2 console and select the EC2 instance.
2. From the top right-hand menu, select Actions > Security > Modify IAM role.

   Or Need AWS Access Key ID and the AWS Secret Access Key to install replication agent.

3. Use a role that contains the AWSElasticDisasterRecoveryEc2InstancePolicy policy.

4. RDP into instance and install using URL for windows.

   Or SSH into instance and install using URL for Linux.

5. For Linux:

   Download agent from:

   - wget -O ./aws-replication-installer-init https://aws-elastic-disaster-recovery-<REGION>.s3.<REGION>.amazonaws.com/latest/linux/aws-replication-installer-init

   Note: Replace <REGION> with the AWS Region into which you are replicating.

Installation:

- Execution permission:chmod +x aws-replication-installer-init;
- run pyrhon script: sudo ./aws-replication-installer-init
- The installer will prompt you to enter your AWS Region Name, the AWS Access Key ID and AWS Secret Access Key (if role was not attached) that you previously generated. Enter the complete AWS Region name (for example, eu-central-1), the full AWS Access Key ID and the full AWS Secret Access Key.
- Once you have entered your credentials, the installer will identify volumes for replication. The installer will display the identified disks and prompt you to choose the disks you want to replicate.
- After all the disks that will be replicated have been successfully identified, the installer will download and install the AWS Replication Agent on the source server.
- Once the AWS Replication Agent is installed, the server will be added to the AWS Elastic Disaster Recovery console and will undergo the initial sync process. The installer will provide you with the source server's ID.

6. For Windows:

Download agent:

- The agent installer follows the following format: https://aws-elastic-disaster-recovery-<REGION>.s3.<REGION>.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Note: Replace <REGION> with the AWS Region into which you are replicating.

- Run the agent installer file AWSReplicationWindowsInstaller.exe as an Administrator.
- The installer will prompt you to enter your AWS Region Name, the AWS Access Key ID and the AWS Secret Access Key that you previously generated.
- Once you have entered your credentials, the installer will verify that the source server has enough free disk space for Agent installation and identify volumes for replication. The installer will display the identified disks and prompt you to choose the disks you want to replicate.
- After all the disks that will be replicated have been successfully identified, the installer will download and install the AWS Replication Agent on the source server.
- Once the AWS Replication Agent is installed, the server will be added to the Elastic Disaster Recovery Console and will undergo the initial sync process. The installer will provide you with the source server's ID.

Reference:

1. AWS Elastic Disaster Recovery