# Title:

# How to replicate secrets in AWS Secrets Manager to multiple regions

On February xx, 2021, we launched a new feature for [AWS Secrets Manager](https://aws.amazon.com/secrets-manager/) that allows you to replicate secrets across multiple regions. P In a

[Secrets Manager](https://aws.amazon.com/secrets-manager/) enables you to store, retrieve, manage and rotate your secrets such as database credentials, API keys, and other secrets. When you create a secret using [Secrets Manager](https://aws.amazon.com/secrets-manager/), it is created and managed in an [AWS Region](https://aws.amazon.com/about-aws/global-infrastructure/) of your choosing. While scoping secrets to an [AWS Region](https://aws.amazon.com/about-aws/global-infrastructure/) is a security best practice, there are scenarios such as Disaster Recovery and cross-regional redundancy that require replication of secrets across regions. [Secrets Manager](https://aws.amazon.com/secrets-manager/) now allows you to easily replicate your secrets to one or more [AWS Regions](https://aws.amazon.com/about-aws/global-infrastructure/) to support these scenarios.

Using this feature, you can now create regional read replicas for your secrets. While creating a new secret or editing an existing secret, you can simply specify the AWS region(s) where your secrets need to be replicated. [Secrets Manager](https://aws.amazon.com/secrets-manager/) will securely create the read replica(s) of the secret and its associated metadata, eliminating the need to maintain complex solution for this functionality. Any update made to the Primary secret such as an updated secret value via automatic rotation will be automatically propagated by Secrets Manager to the Replica secrets as well, making it easy to manage the life cycle of multi-region secrets.

## Architectural overview:

Suppose that your organization has a requirement of setting up a Disaster Recovery plan.  In this example, us-east-1 is the designated primary region where you have an application running on a simple Lambda function (for this blog example I am using Python 3). You also have a [Amazon RDS](https://aws.amazon.com/rds/) – MySQL database instance running in us-east-1 and you are using [Secrets Manager](https://aws.amazon.com/secrets-manager/) to store the database credentials. Your application retrieves the secret from [Secrets Manager](https://aws.amazon.com/secrets-manager/) to access the database. As part of the disaster recovery strategy, you set up us-west-2 as the designated recovery region, where you have replicated your application, database instance and the database secret.

To elaborate, the solution architecture consists of:

* A Primary Region for creating the secret, to be us-east-1 (N. Virginia)
* A Replica Region for replicating the secret, to be us-west-2 (Oregon)
* [Amazon RDS](https://aws.amazon.com/rds/) – MySQL DB Instance in Primary and replication configured for the Replica Region. To setup Read Replica or Cross-Region Replica for [Amazon RDS](https://aws.amazon.com/rds/) see [Working with Read Replicas](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html).
* Secret created in [Secrets Manager](https://aws.amazon.com/secrets-manager/) and configured for Replication for the Replica Region.
* [AWS Lambda](https://aws.amazon.com/lambda/) functions (running on Python3) deployed in Primary and Replica Region.

This architecture is illustrated in Figure 1.

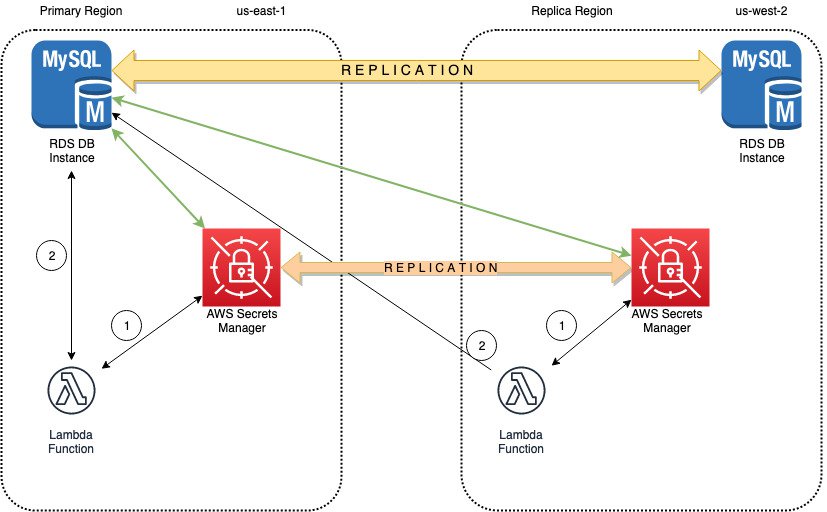


Figure 1: Architectural overview for multi-region secret replication with Primary Region active

The [Lambda](https://aws.amazon.com/lambda/) function uses the credentials stored in the secret to access the database, identified with the following steps in Figure 1:

1. [Lambda](https://aws.amazon.com/lambda/) function sends a request to [Secrets Manager](https://aws.amazon.com/secrets-manager/) to retrieve the Secret Value via the GetSecretValue API Call. Secrets Manager retrieves the Secret Value to the [Lambda](https://aws.amazon.com/lambda/) function.
2. [Lambda](https://aws.amazon.com/lambda/) function uses the Secret Value to connect to the database for retrieving the data.

As seen in the diagram above, the replicated secret in us-west-2 points to the primary database instance in us-east-1. This is because when [Secrets Manager](https://aws.amazon.com/secrets-manager/) replicates the secret, it replicates the secret value and all the associated metadata such as the database endpoint.

To simplify database switchover during disaster recovery as explained later in the blog, you can configure an [Amazon Route53](https://aws.amazon.com/route53/) [CNAME Record for my database endpoint](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-rds-db.html) in the Primary Region. The database host in the secret is configured with the database CNAME Record. When the Primary Region is operating normally, the CNAME Record points to the database endpoint in the Primary Region. The requests to the database CNAME are routed to the database instance in the Primary Region as shown in the above diagram.

During disaster recovery, you can switchover to the replica region, us-west-2 to enable your application running in this region to access the [Amazon RDS](https://aws.amazon.com/rds/) Read Replica in us-west-2 using the secret stored in the same region. The database CNAME Record is also updated to point to the database endpoint in us-west-2. Since the database CNAME is used to point to the database endpoint within the secret, your application in us-west-2 can now use the replicated secret to access the database read replica in this region. Figure 2 illustrates this disaster recovery scenario.

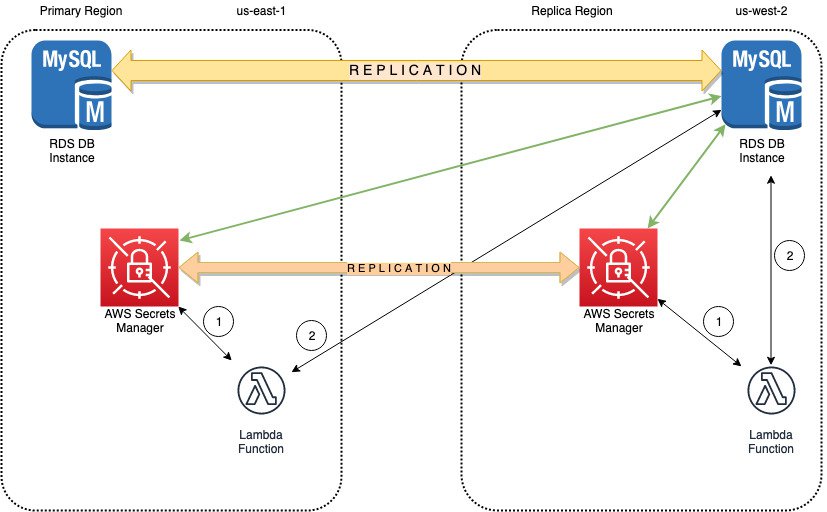


Figure 2: Architectural overview for multi-region secret replication with Replica Region active

### Prerequisites:

The procedure mentioned in this blog post assumes that the following steps have been completed prior to starting the procedure:

1. [Amazon RDS](https://aws.amazon.com/rds/) DB Instance is configured in the Primary Region with replication configured in the Replica Region.
2. [Route53](https://aws.amazon.com/route53/) [CNAME Record for database endpoint](https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-rds-db.html) configured in the Primary Region
3. The [Lambda](https://aws.amazon.com/lambda/) function is configured to connect with the [Amazon RDS](https://aws.amazon.com/rds/) database and Secrets Manager following the procedure in this [Blog Post.](https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by-using-aws-secrets-manager/)
4. Login to the [AWS Management Console](https://aws.amazon.com/console/) using a Role that has *SecretsManagerReadWrite* permissions in the Primary and Replica Region.

## Enable replication for secrets stored in AWS Secrets Manager

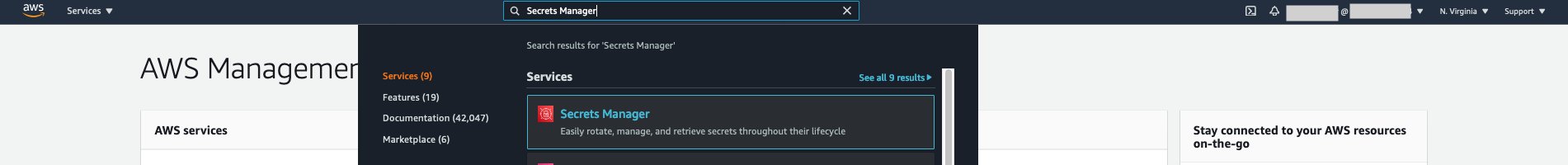
I will now walk you through the process of enabling Replication in [Secrets Manager](https://aws.amazon.com/secrets-manager/) for:

1. A new secret that is created for your [Amazon RDS](https://aws.amazon.com/rds/) database credentials.
2. An existing secret that is not configured for Replication.

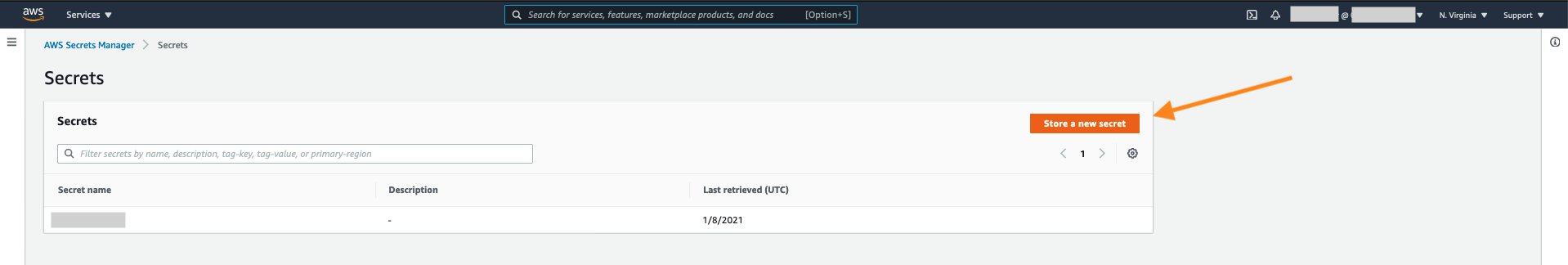
In the first scenario, I will show you the steps to create a Secret in [Secrets Manager](https://aws.amazon.com/secrets-manager/) in the Primary Region (us-east-1) and enable replication for the Replica Region (us-west-2).

### To create a secret with replication enabled

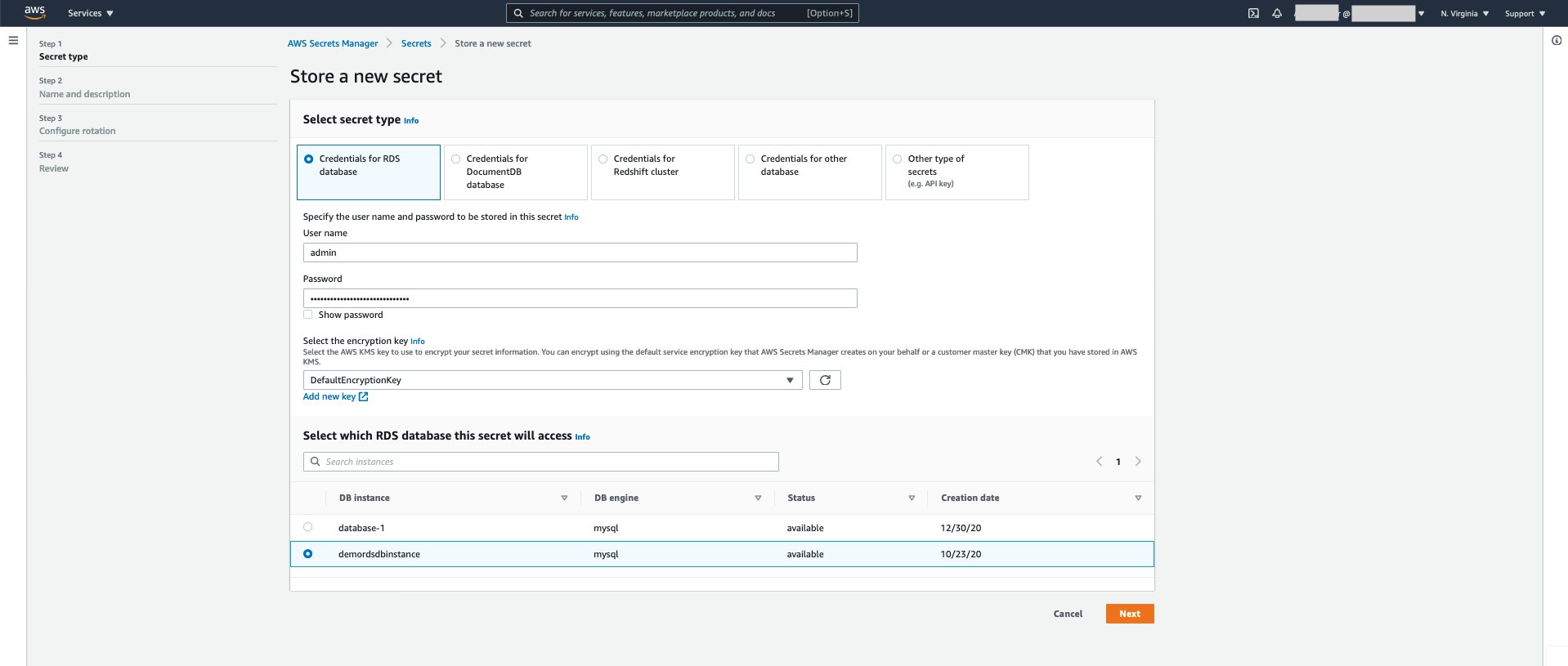
1. Navigate to the[Secrets Manager](https://aws.amazon.com/secrets-manager/)service console from [the console](https://aws.amazon.com/console/) in Primary Region (N. Virginia)



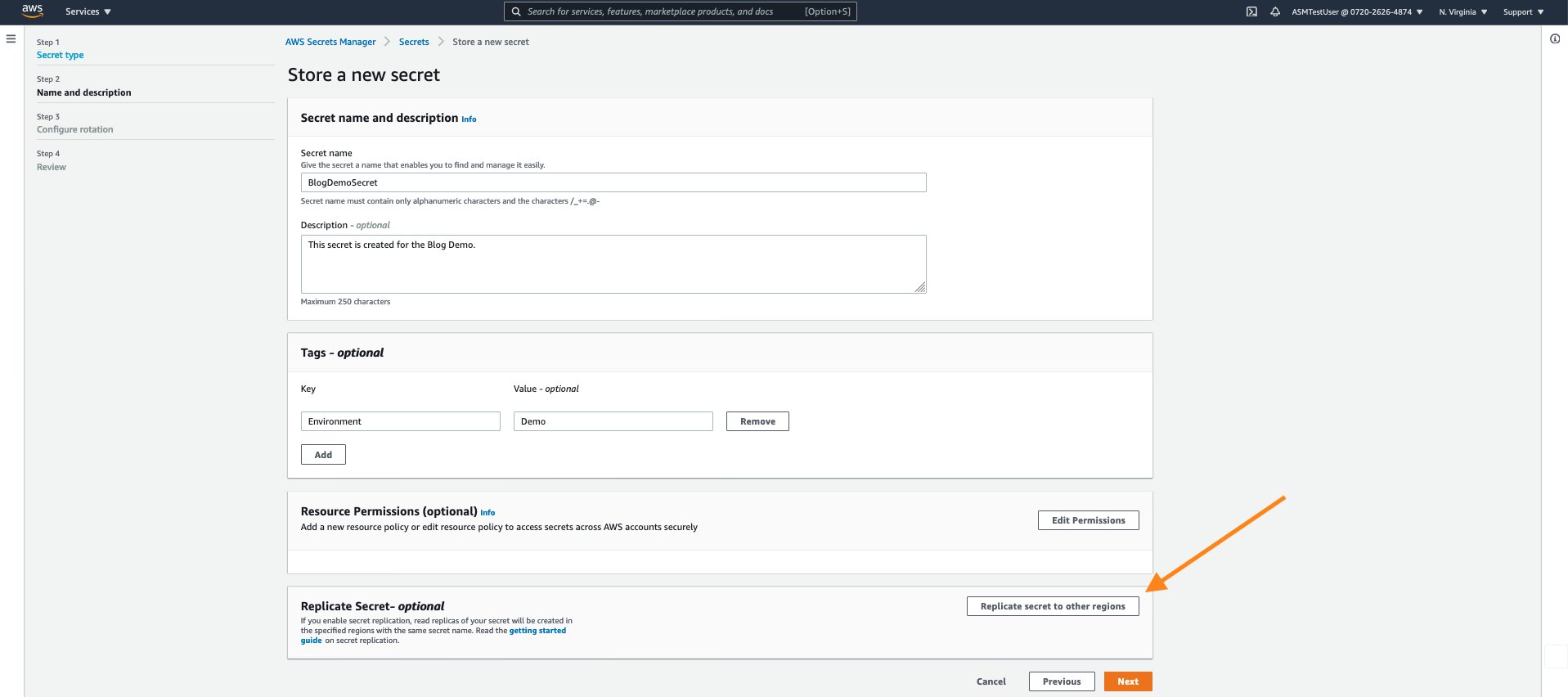
1. Next, click “Store a new secret”.



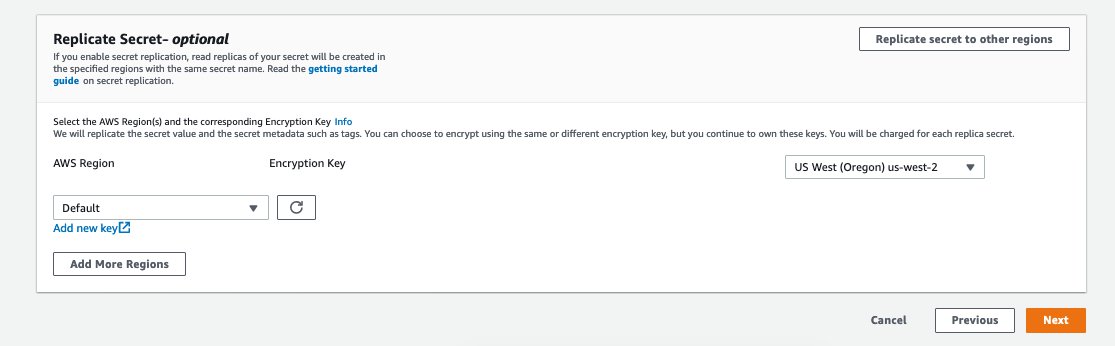
1. On the next screen, enter the [Amazon RDS](https://aws.amazon.com/rds/) database credentials that will be used to connect with the [Amazon RDS](https://aws.amazon.com/rds/) database instance. Select the Encryption Key and the [Amazon RDS](https://aws.amazon.com/rds/) DB Instance. Then click “Next” to move to the next step.



1. Next, enter the Secret Name of your choice and enter a Description. You can also add a Tag and Resource Permissions to the secret. Click on “Replicate secret to other regions” under “Replicate Secret - *optional*” section.

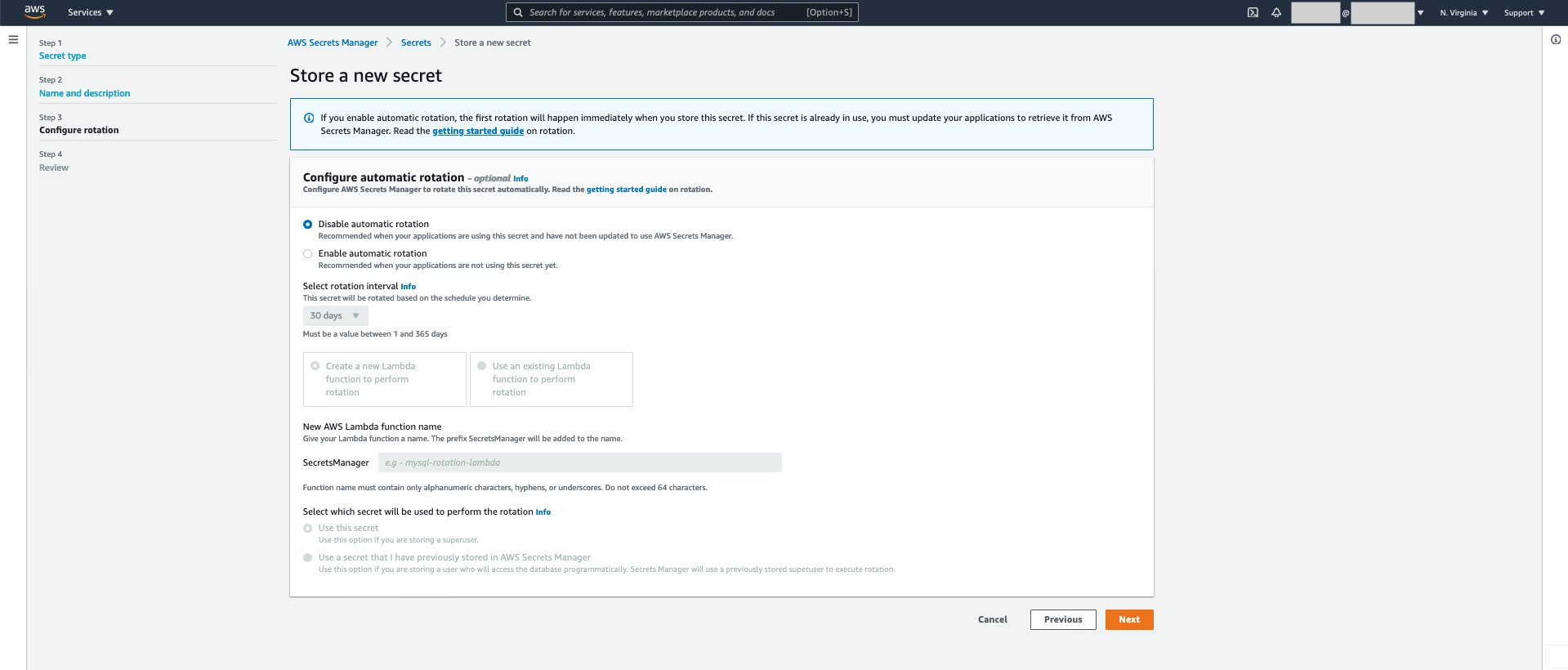


1. Select the Replica Region - “US West (Oregon) us-west-2” from the AWS Region drop down list and select the “Default” Encryption Key for storing your secret in the Replica Region.

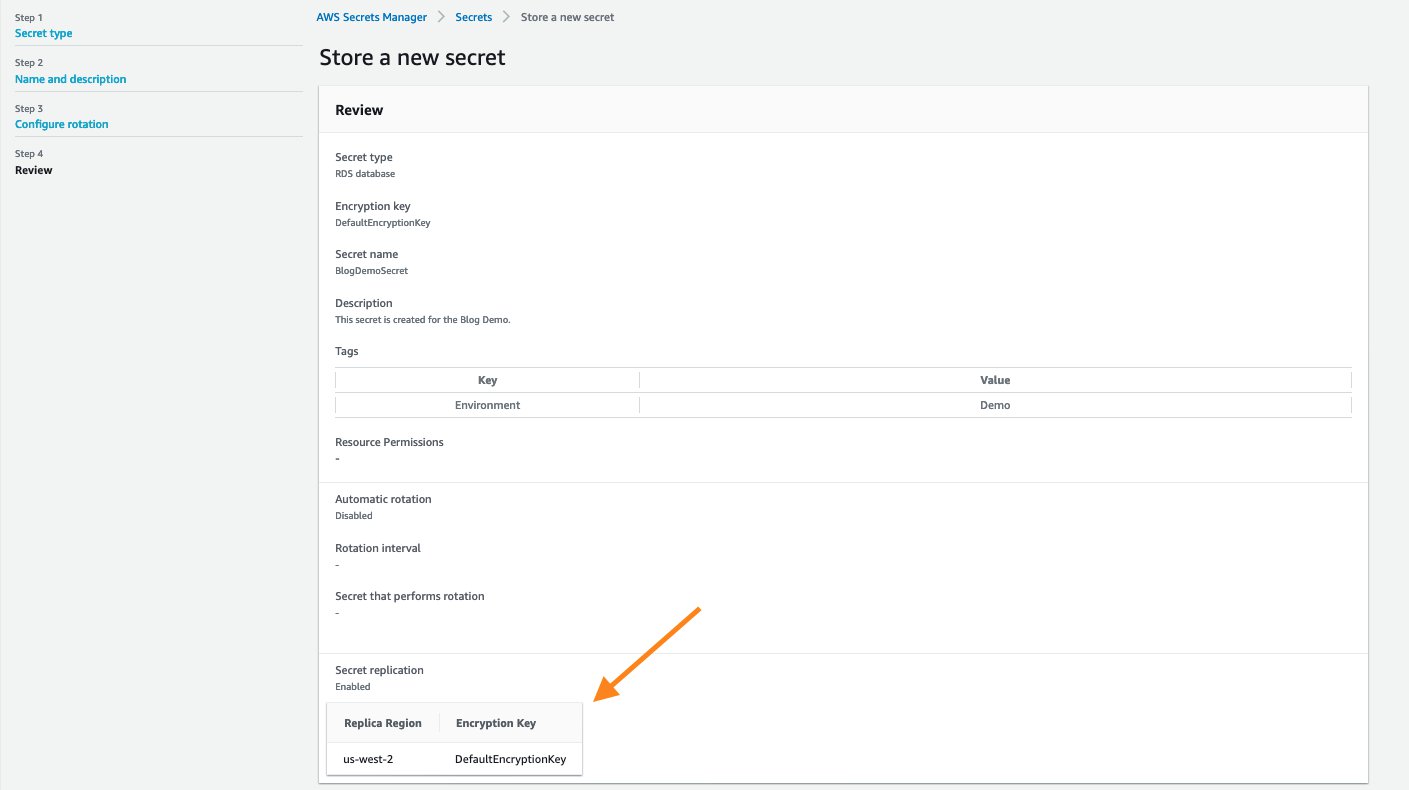


Click “Next” to move to the next steps.

1. Next is the “Configure Rotation” section. For this Demo I choose not to enable rotation so I select “Disable automatic rotation” radio button. However, if you want to enable Rotation you can choose to Enable automatic rotation by following the guidance mentioned in the [User Guide](https://docs.aws.amazon.com/secretsmanager/latest/userguide/enable-rotation-rds.html). When you enable rotation in the Primary Region, any changes to the secret from the rotation process are also replicated to the Replica Region.



Click “Next” and move to the Review screen. Here you can see the summary of the secret configuration including the Secret Replication configuration.

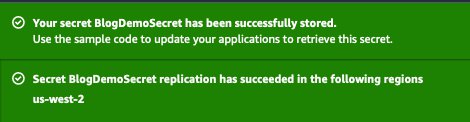


1. Scroll down the screen and click “Store”.

On top of the screen, you will see two banners providing status on:

1. Creation of the secret in the Primary Region
2. Replication of the secret in the Secondary Region

Once the creation and replication is successful, the following messages will appear on the top of the screen:

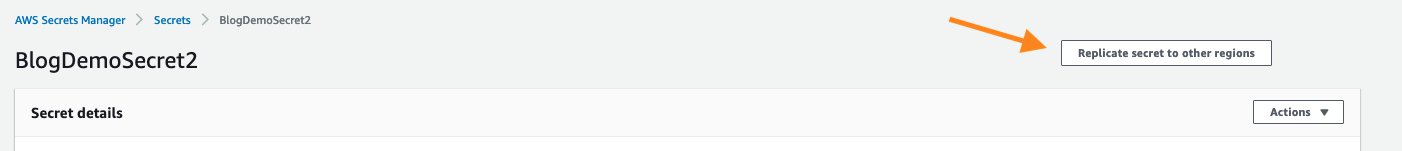


At this point, you have created a secret in the Primary Region (us-east-1) and enabled the replication in a Replica Region (us-west-2). You can now use this secret in the Replica Region as well.

Now syouthe You can also configure replication for existing secrets.

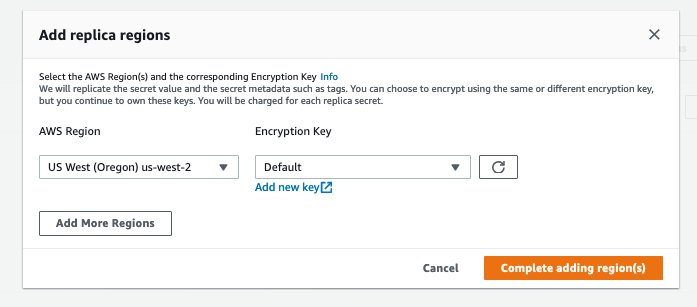
### To enable multi-region replication for existing secrets

1. Click on the secret name from the [Secrets Manager](https://aws.amazon.com/secrets-manager/) service console and clicking “Replicate secret to other regions” on the top of the screen.



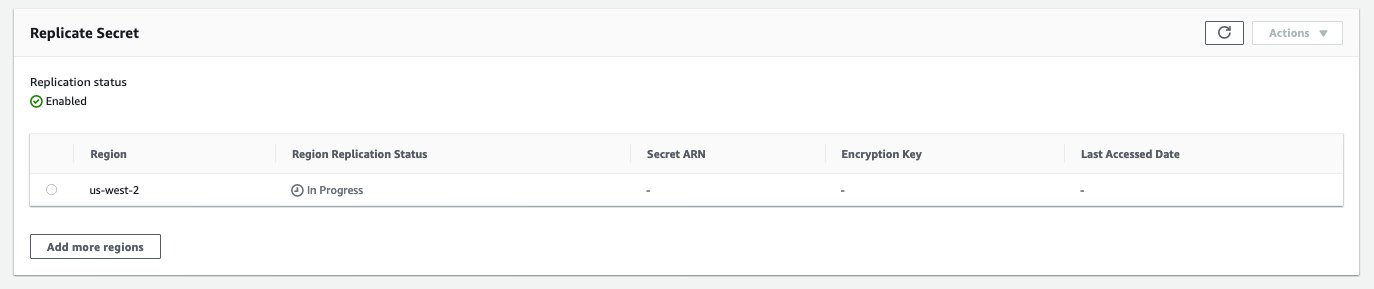
This will open a pop-up to configure the Replica Region and the KMS key for encrypting the secret in the Replica Region.

2. You can c for the Replica region

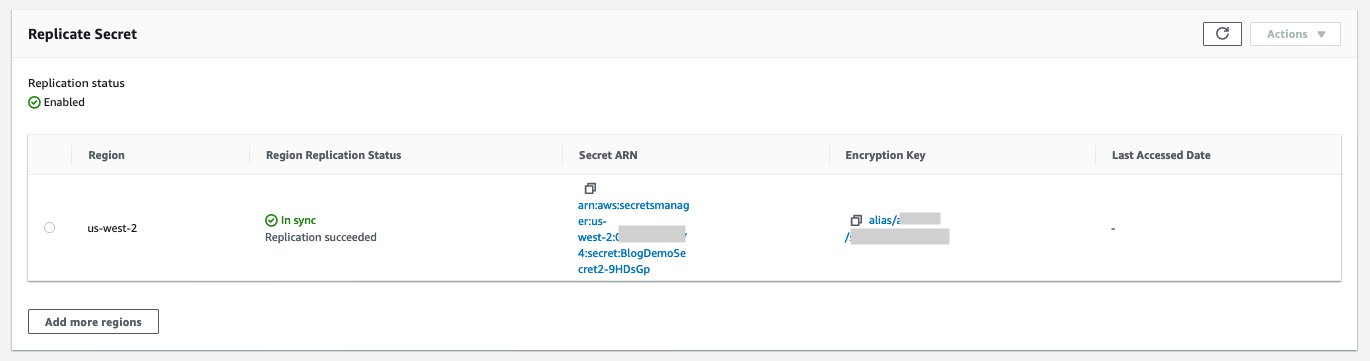


This will start the Replication process of the secret from the Primary Region to the Replica Region.

Scrolling down to the “Replicate Secret” section, I see that the replication to us-west-2 region is in progress:



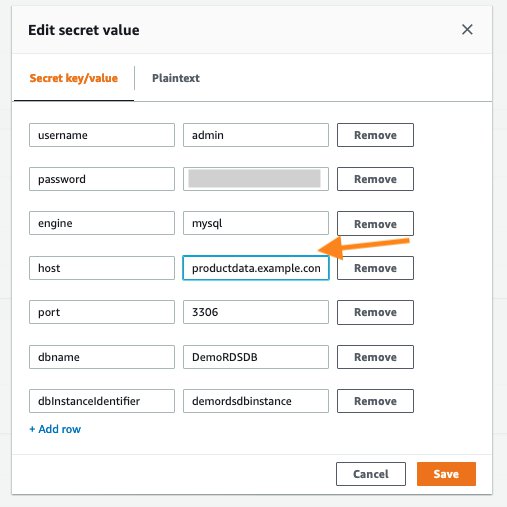
Once the Replication is succeeded, I can review the replication details that I have configured for my secret. I can also choose to add more Regions for replicating my secret by clicking on “Add more regions”.



Now you can also update the *host* in your secret to the CNAME Record of the Database endpoint.

## To update secret with CNAME Record

1. Follow the process mentioned [here](https://docs.aws.amazon.com/secretsmanager/latest/userguide/manage_update-secret.html) to update the secret value for *host* with the CNAME Record.

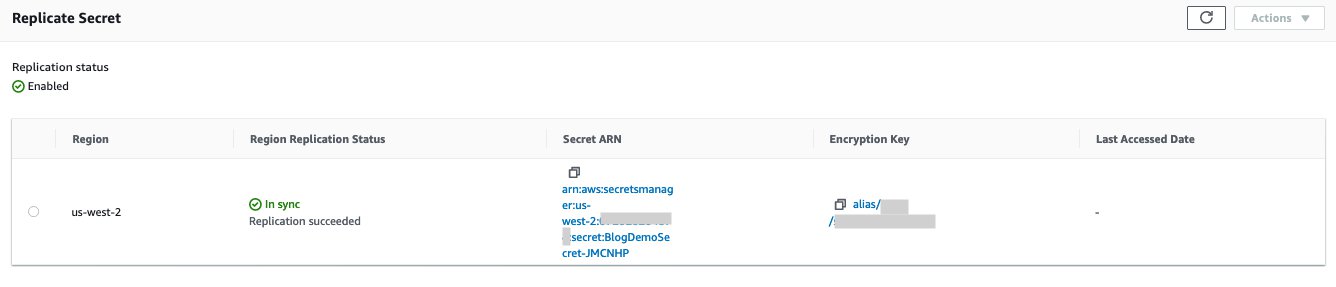


2. After you click “Save”, you will see a banner on top of the screen with the following message that indicates that the secret was successfully edited:



Since the secret is setup for Replication, you can also review the sync status of your secret to the Replica Region after the update was made to the secret.

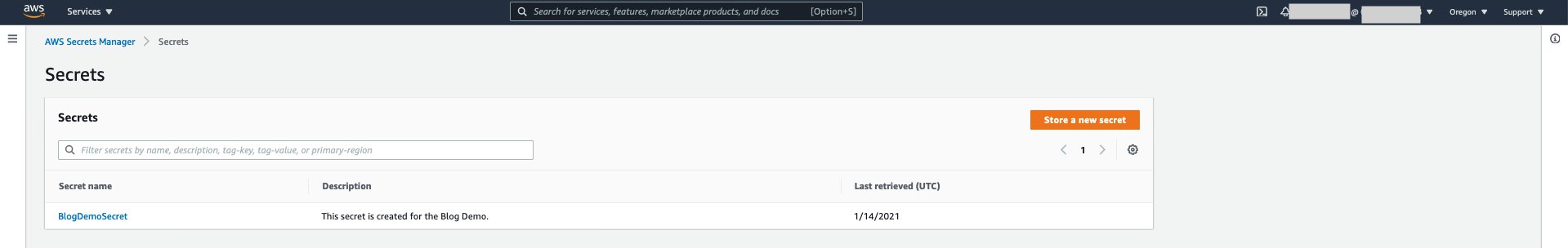
1. You can scroll down to the “Replicate Secret” section and review the “Region Replication Status”.



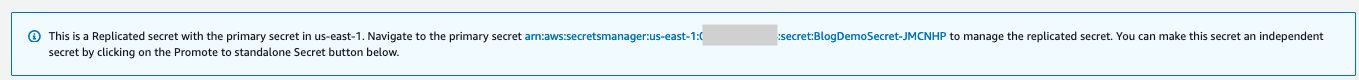
Now that you have configured the secret for Replication in the Primary Region, you can access the secret from the Replica Region.a simple Lambda function deployed in

## To access the secret from the Replica Region

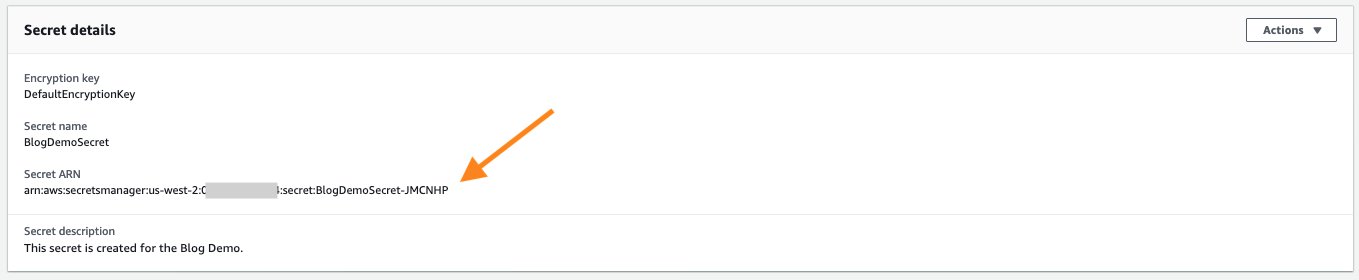
1. Navigate to the[Secrets Manager](https://aws.amazon.com/secrets-manager/)service console from [the console](https://aws.amazon.com/console/) in the Replica Region (Oregon) and view the secret that you created in the Primary Region (N. Virginia).



1. You can click on the Secret name and review the details replicated from the Primary Region. A secret that is configured for Replication will display a banner on the top stating the replication details.



You can simply use the Secret ARN to retrieve the secret value from the Lambda function or application deployed in your Replica Region (Oregon).



During a Disaster Recovery scenario when the Primary Region is not available, you can update the CNAME Record to point to the database instance endpoint in us-west-2.

For this demo, my application deployed in the Replica Region is configured to use the replicated secret ARN.

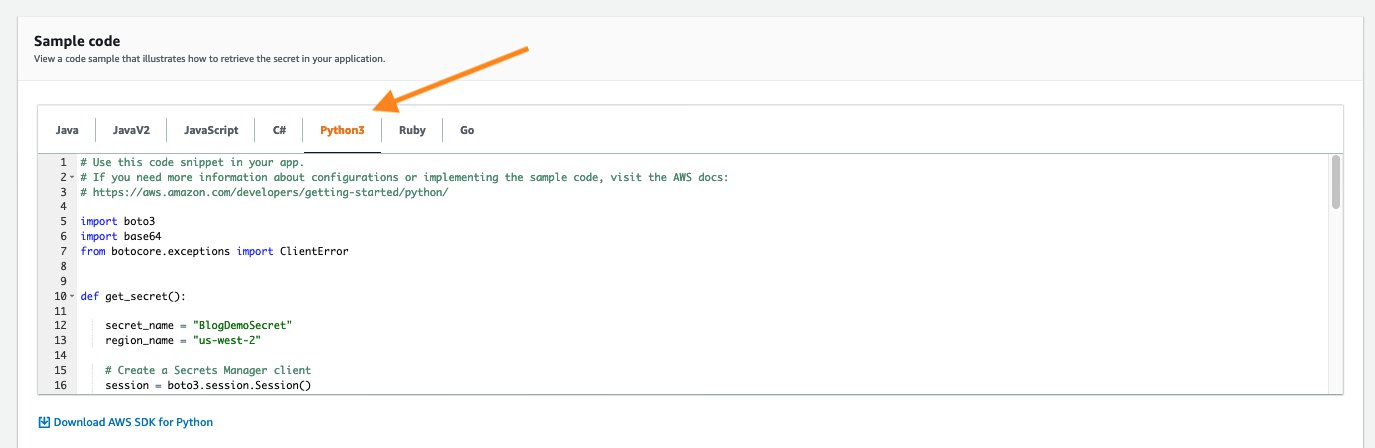
Let’s suppose your sample Lambda function defines the Secret Name and the Region in the environment variables. The SECRET\_NAME Environment Variable is the ARN of your replicated secret in the Replica Region.



In the Replica Region, you can now refer to the Secret ARN in my [Lambda](https://aws.amazon.com/lambda/) function code to retrieve the Secret Value for connecting to the database:



Alternately, you can simply use the Sample code for Python3 of the Replicated secret to retrieve the Secret Value from the [Lambda](https://aws.amazon.com/lambda/) function in the Replica Region.



## Summary:

When planning for Disaster Recovery, you can configure replication of your secrets in [Secrets Manager](https://aws.amazon.com/secrets-manager/) to enable redundancy of your secrets. This feature reduces the overhead of deploying and maintaining additional configuration for secret replication and retrieval across [AWS Regions](https://aws.amazon.com/about-aws/global-infrastructure/). In this blog, I showed you how to create a Secret and configure it for multi-region replication. I also demonstrated how you can configure replication for existing secrets across multiple regions.

I showed you how to use secrets from the Replica Region and configure a sample [Lambda](https://aws.amazon.com/lambda/) function to retrieve secret value. When Replication is configured for secrets, you can simply retrieve the secrets in the Replica Region in a similar way as you would in the Primary Region.

If you have feedback about this blog post, submit comments in the Comments section below. If you have questions about this blog post, start a new thread on the [AWS Secrets Manager forum](https://forums.aws.amazon.com/forum.jspa?forumID=296).