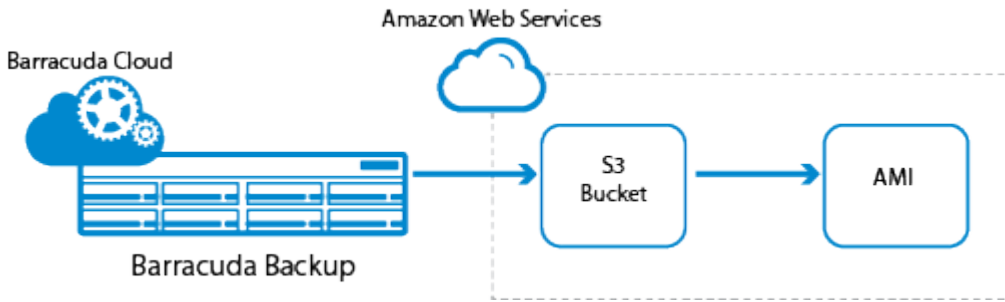




# Amazon Web Services Recovery

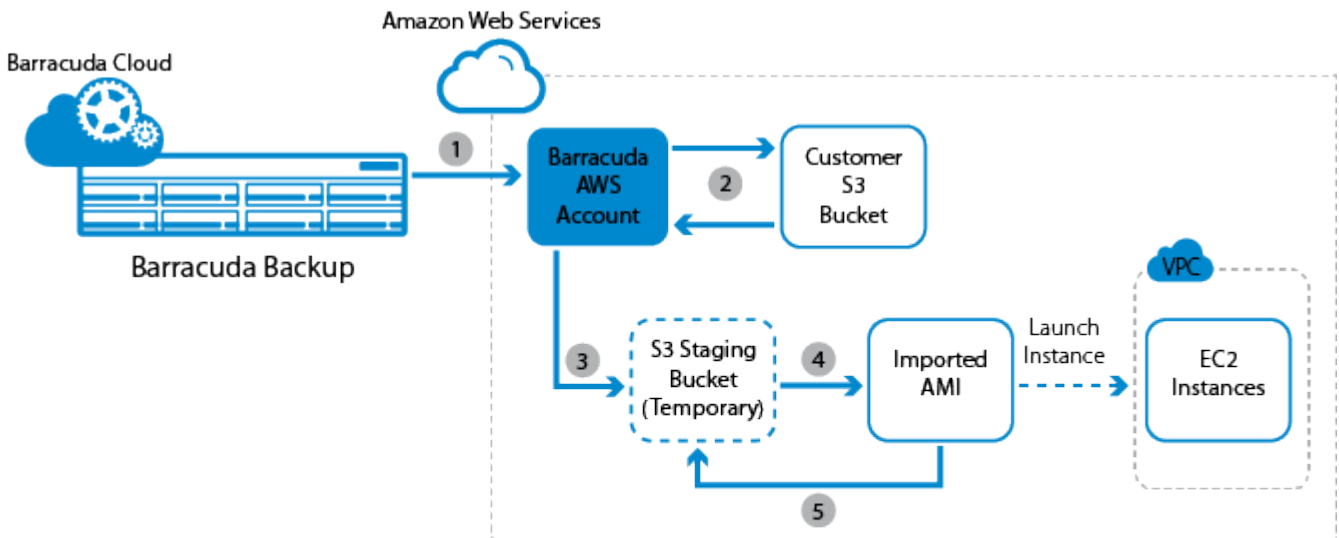
Restore Barracuda Backup virtual image backups to an Amazon Web Services (AWS) instance.

Once the Barracuda Backup appliance is installed on-premises and managed from Barracuda Cloud, binary data is stored in the customer's AWS S3 bucket, and metadata is stored in Barracuda's account and infrastructure within AWS. Data can be recovered back to the Barracuda Backup or to AWS AMI.



An Amazon Machine Image (AMI) provides the information required to launch an instance; a virtual server in the cloud. Specify an AMI when you launch an instance, and launch as many instances from an AMI as needed; you can launch instances from as many different AMIs as necessary. An AMI includes:

- A root volume template for the instance (for example, an operating system, an application server, and applications)
- Launch permissions that control which Amazon Web Services (AWS) accounts can use the AMI to launch instances
- A block device mapping that specifies the volumes to attach to the instance when launched



- 1 Restore to AMI is initiated from Barracuda Backup.
- 2 Data is copied from customer S3 bucket, passes through Barracuda's AWS account, and is decompressed and decrypted.
- 3 The VM Image is assembled in a temporary (staging) S3 bucket in the customer account.
- 4 AWS VM Import is called, which creates the AMI.
- 5 Upon successful AMI creation or failure, the temporary (staging) S3 bucket is deleted.

## In this Section

- [How to Restore VMware and Hyper-V Backups to Amazon Web Services](#)
- [How to Configure the Amazon Web Services Import Service Role](#)



