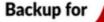


# **Prerequisites To Add AWS Account** on the BDRSuite























## Prerequisites To Add AWS Account on the BDRSuite

## Step 1: Create & Attach Policy to User

Create a new policy and attach it to a user in your AWS account using any of the following methods:

### METHOD 1 - Using JSON to create a policy

- Sign in to the AWS Management Console https://aws.amazon.com/console/
- Search for **IAM service** in the **Find Services** section and choose the service. This will redirect you to the Identity and Access Management(IAM) page.
- Choose **Policies** from the IAM Dashboard displayed on the left pane.
- Then, choose **Create policy** option and click on the **JSON** tab.
- On the JSON Editor, remove the existing text and then copy and paste the entire content from the following JSON policy document.
- Once you have entered the JSON, click on the **Review policy** button.
- On the Review policy page, provide **Name** and **Description** (optional) for the policy that you are creating and click **Create Policy**.
- Once the policy is created, you can select the user for whom the policy needs to be attached. Choose **Users** on the IAM Dashboard and select the name of the user from the list to attach the created policy.
- On the **Summary** page of the selected user, click on **Add Permissions**.
- Select Attach Existing Policies Directly option on the Grant Permission Page
- Then, select the policy created using the above JSON from the list and click **Next**: Review
- Lastly, on the Permission Summary page, click the **Add Permissions** button.

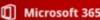




















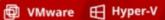


## METHOD 2 - Using Visual editor to create a policy

- Sign in to the AWS Management Console https://aws.amazon.com/console/
- Search for IAM service in the Find Services section and choose the service. This will redirect you to the Identity and Access Management(IAM) page.
- Choose **Policies** from the IAM Dashboard displayed on the left pane.
- Then, choose **Create policy** and click on the **Visual Editor** tab.
- On the Visual Editor page, click on **Choose a service**. Initially, add one of the following services (Eg: S3). Then, In the Actions section, select the Access level for the service chosen and expand each of the access levels to choose individual actions. In the Resources section, choose the 'All Resources' option. Then, click on 'Add additional **permissions**' and repeat the process to grant access to each of the services listed below.

SERVICES	ACTIONS
S3	List - ListAllMyBuckets
	Read-GetObject
	Write - CreateBucket, PutObject
STS	Read -GetCallerIdentity
SSM (System	List - ListDocuments
Manager)	Read - GetCommandInvocation
	Write - CreateDocument, SendCommand
EC2	List - DescribeAvailabilityZones, DescribeKeyPairs,
	DescribeVolumes, DescribeInstances, DescribeRegions,
	DescribeVolumeStatus, DescribeInstanceStatus,
	DescribeSnapshots, DescribeVpcs
	Tagging - CreateTags
	Write - AttachVolume, DeleteSnapshot, RegisterImage,
	CreateImage, DeleteVolume, RunInstances, CreateSnapshots,
	DeregisterImage, CreateVolume, DetachVolume























- Once you have chosen the services and actions, click on the **Review policy** button.
- On the Review policy page, provide **Name** and **Description** (optional) for the policy that you are creating and click Create Policy.
- Once the policy is created, you can select the user for whom the policy needs to be attached. Choose **Users** on the IAM Dashboard and select the name of the user from the list to attach the created policy.
- On the **Summary** page of the selected user, click on **Add Permissions**.
- Select **Attach Existing Policies Directly** option on the Grant Permission Page.
- Then, select the policy created using the above JSON from the list and click **Next**: Review
- Lastly, on the Permission Summary page, click the **Add Permissions** button.

## Step 2: Access Key ID & Secret access key

- Sign in to the AWS Management Console https://aws.amazon.com/console/
- Search for **IAM service** in the **Find Services** section and choose the service. This will redirect you to the Identity and Access Management(IAM) page.
- Choose **Users** from the IAM Dashboard displayed on the left pane.
- Select the user to whom the policy has been attached, and then choose the **Security** credentials tab.
- In the Access keys section, you can use the existing access key or create a new key:
  - If you have already generated an access key for the user, you will see the Access Keys list. The secret access key for this will be available in the .csv file which you downloaded earlier. You can use this access key details and add your AWS account on the BDR Backup Server.
  - To create a new access key, click the **Create Access Key** option. The new access 0 keys will be generated and displayed one time on the screen. Click **Download .csv** file to save the Access key ID and secret access key as a CSV file on your computer. You can use this access key details and add your AWS account on the BDR Backup Server.





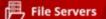


















### **USA & CANADA**

+1-512-256-8699

#### UNITED KINGDOM

+1-512-256-8699

## **Email**

vembu-sales@vembu.com vembu-support@vembu.com

www.bdrsuite.com

#### Disclaimer

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher. The information contained in this document is taken from third party sources and is for general information purposes only. The information is provided by Vembu and while we endeavour to keep the information up to date and correct, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the document or the information contained on the document for any purpose. Any reliance you place on such information is therefore strictly at your own risk.





















