BDRSuite
Backup & Disaster Recovery

Prerequisites to Add Azure Account for Azure VM Backup & Recovery using BDRSuite

Prerequisites to Add Azure Account for Azure VM Backup & Recovery using BDRSuite

Step 1 : Generate Application ID

- Sign in to your **Azure Account** through the [Azure Portal.]

Note: Make sure the user account you use has sufficient permission to register an application and assign a role to it.

- Search and locate the **Microsoft Entra ID (formerly Azure Active Directory).** On the Microsoft Entra ID (formerly Azure Active Directory) page, select App registrations under Manage on the left pane and click on New registration.

- Then **'Register an application**' page will appear and enter the following details to register your application.
    - **Name** - Enter a display name for the application.
    - **Supported account types** - Choose the option **"Accounts in this organizational directory only"**

- Finally, click on the **Register** button. The Azure Microsoft Entra ID (formerly Azure Active Directory) assigns a unique **Application (client) ID,** which appears on the page to which you are redirected.

Step 2: Generate Application Password

- Select **Certificates & secrets** under **Manage** on the left pane.

- Click on **New client secret** which opens a separate section: **Add a client secret.** On this page, choose **24 months** from the Expires option and click **Add.** This will generate and display the application password (under the 'Value' column).

  Note:

    - Make sure you copy the application password (Value) as the portal will display it only once. (You can use the copy to clipboard icon to copy the password).

    - Once the generated application password has expired, create a new client secret and update it on the BDRSuite. If the expired password is not updated, backups will fail.

Step 3: Create Role

- On the **Home page,** under the **Azure Services section,** select **'Subscriptions'** (or) search for and select **'Subscriptions'** from the Search box at the top.

- From the list of **Subscriptions**, click on the subscription that you plan to use in **BDRSuite** to configure backup from.

- On the left pane of the selected Subscription page, click **Access control (IAM)** and then click **Add -> Add custom role**

- On the **Add custom role page** add the following roles:

    - On the **Basics Tab,** Enter a Custom **Role name** (bdrsuite-azure-backup-restore-role) and for **Baseline Permissions,** select the option: **start from scratch.** Click Next.

    - 'Permissons' Tab - Click next and move to Assignable Scopes tab.

    - On the **Assignable Scopes Tab:** Click on "+Add Assignable Scopes" option to add any other subscriptions you have access to. On the Add assignable scopes dialog, select a subscription to add as an assignable scope.

        Note: Please make sure to select any other subscriptions associated with this account if you intend to use them for backup and recovery. Otherwise, you will need to perform the steps separately for each subscription later.

    - On the **JSON Tab,** click "Edit", Under "permissions", copy and paste the entire content from the following JSON policy document and finally **"Save"** it.

    - On the **Review + Create** tab, review the role assignment settings and click **the Review + Create button.**

Step 4: Add Role Assignment

- On the Home page, under the **Azure Services section,** select **'Subscriptions'** (or) search for and select **'Subscriptions'** from the Search box at the top.
- From the list of subscriptions, click on the subscription that you plan to use in **BDRSuite.**
- On the left pane of the selected subscription page, click **Access control (IAM)** and then click **Add -> Add role assignment**
- On the Add the role assignment page add the following roles:
  - Under **Role** tab, select the role created above (bdrsuite-azure-backup-restore-role) and click next
  - On the **Members Tab:**
    - For the field: **'Assign access to',** select the option: **User, group, or service principal.**
    - For the field: **Members,** click **'Select Members'** which opens a dialog box. Search and select the application that you have created (in step 1) and click the **'Select'** button. Then, click the **Next button.**
    - On the **Review + assign** tab, review the role assignment settings and click the Review + assign button.

Step 5: Add Azure Account on the BDRSuite

- On the BDRSuite, navigate to the **Cloud Workloads ->Data Source-> Azure Backup -> Azure Accounts page**

- Click on the **'Add Azure Account'** button which opens a dialog box. Then, enter the following details and click 'Save'.

    - **Tenant ID -** On the Azure Portal, navigate to the Microsoft Entra ID (formerly Azure Active Directory) page where you can find the 'Tenant ID' under the Basic information section.

    - **Application ID -** On the Azure Portal, navigate to the Microsoft Entra ID (formerly Azure Active Directory) page and select 'App registrations' from the left pane. Click on the application that you have created (in step 1) and you can find the 'Application (client) ID' under Essentials section.

    - **Application Password -** Provide the Application Password (Value) that you copied after creating the client secret.

BDRSuite
Backup & Disaster Recovery

USA & CANADA

+1-512-960-1319

UNITED KINGDOM

+44-190-051-2324

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.