FirstNet Veeam Backup for Office 365

Enablement of Veeam Backup for Office 365 backups requires the correct permissions and roles be configured within the customers Microsoft Office 365 tenant. Such tasks will need to be performed by the customer or customers support team who have the correct privileged access within the Microsoft Office 365 tenant and Azure Active Directory. FirstNet will provide customer with the requirements.

A user account with the Global administrator role assigned using basic authentication is the quickest and easiest credential method to configure. Additional authentication mechanisms like modern authentication and modern authentication with legacy protocols allowed can also be configured if required.

If the customer has access to their own Veeam Backup & Replication server then self-service restores can be performed at any time using the supplied Veeam Cloud Connect credentials and the Veeam Explorers. Additional restoration of data into the customers Microsoft Office 365 tenant can be performed by FirstNet at the customer's request.

1. Customer responsibilities
   - 1.1 Provide FirstNet with the required storage requirement.
   - 1.2 Provide FirstNet with the retention period required for backed up items.
     - 1.2.1 Retention period is measured in years.
     - 1.2.2 Default period is 3 years.
     - 1.2.3 Individual items will be deleted from the backup repository once their creation or last modification date exceeds the retention period.
     - 1.2.4 Retention policy is applied daily.
   - 1.3 Provide FirstNet with a list of the Microsoft Office 365 services requiring backup. Available services include the following.
     - 1.3.1 Exchange Online
     - 1.3.2 SharePoint Online and OneDrive for Business
     - 1.3.3 Microsoft Teams
   - 1.4 Provide FirstNet with credentials and an authentication mechanism, either modern authentication, modern authentication with legacy protocols allowed or basic authentication.
     - 1.4.1 Modern authentication will configure an Azure AD App registration using certificate-based authentication. A user with the Global administrator role in the customers tenant will need to approve this registration at the time of backup configuration.
     - 1.4.2 Modern authentication with legacy protocols allowed will require an Azure AD App registration using certificate-based authentication be created in the customer tenant Azure AD before configuration of the backup commences.
       The certificate will be supplied by FirstNet.
       A user account in the customer tenant will be required and must be a member of the Organization Management group and have the Role Management and Site Collection Administrator role assigned.
       If the customer is using ADFS then MFA must be disabled for this user account.
       Password expiration must be disabled for this user account.
     - 1.4.3 Basic authentication requires a user account in the customer tenant that is a member of the Organization Management group and has the Role Management, ApplicationImpersonation and Site Collection Administrator role assigned.
       If the customer is using ADFS then MFA must be disabled for this user account.
       Password expiration must be disabled for this user account.

1.5 Provide FirstNet with a list of Users, Groups, Sites, Teams or Organizations to be backed up.
The User list needs to include the user account name and service to be backed up.
The Group list needs to include the group name and service to be backed up.
The Site list needs to include the SharePoint sites to be backed up.
The Team list needs to include the Teams to be backup up.
The Organization list needs to include the tenant organization name to be backed up.
Services available to be backed up include Mail, Archive, OneDrive and Site.

1.6 Notify FirstNet of any changes to the retention policy and Microsoft Office 365 service requirement indicated in sections 1.2 and 1.3.

1.7 Notify FirstNet of any changes to the authentication mechanism or credentials configured in the backup as indicated in section 1.4.

1.8 Notify FirstNet of any additions, changes or deletions to the items indicated in section1.5.

1.9 Notify FirstNet via the FirstNet ticketing system of any data restoration required.

2. FirstNet responsibilities

2.1 FirstNet will ensure the backup runs as per the configured schedule. The default backup schedule is to run the backup job daily.

2.2 FirstNet will notify the customer of any backup failures. By default, backup jobs will be retried 3 times. After the third failure FirstNet will notify the customer technical contact of the backup job failure.

2.3 FirstNet will provide the customer Veeam Cloud Connect credentials for use with their Veeam Backup & Replication server to facilitate self-service restores of data using the Veeam Explorers.

2.4 FirstNet will restore any data required into the customers Microsoft Office 365 tenant or to a location of the customers choosing once a support request has been logged by the customer or the customers support team on the FirstNet ticketing system.

2.5 FirstNet will ensure sufficient backup storage capacity is available to facilitate the backup of the customer data.

3. Considerations and Limitations

3.1 When using modern authentication, the following must be noted.

3.1.1 Backup

3.1.1.1 Discovery Search and Public Folder mailboxes are not supported.

3.1.1.2 Dynamic Distribution groups are not supported.

3.1.1.3 The ‘type’ property for shared and resource/equipment mailboxes cannot be resolved. Such mailboxes will be available for backup with a general ‘User’ type.

3.1.1.4 SharePoint Web Parts can only be backed up if their ‘exportmode’ property is enabled. Non exportable Web Parts are not supported.

3.1.2 Restore

3.1.2.1 OneNote restore is not supported.

3.1.2.2 SharePoint Web Part customized template cannot be preserved upon a restore. All Web Parts will be restored with the default template.

3.1.2.3 The ‘Allow multiple responses’ setting in survey lists within team modern sites is not preserved upon a restore.

3.2 To backup user mailboxes, make sure that a mailbox has a valid Microsoft Office 365 license.

3.3 To backup up public folder mailboxes, the Veeam Backup account must have a valid Exchange Online license and an active mailbox within the Microsoft Office 365 organization.

3.4 Veeam Backup for Microsoft Office 365 backs up public folders that are located under the IPM_SUBTREE folder only.

3.5 Project Web Apps are not supported for backup.
3.6 On-premises service accounts cannot be used for multi-factor authentication.
3.7 You can select only the root public mailbox when backing up public mailboxes. The child folders of the selected public mailbox will be backed up as well.
3.8 If you modify a retention policy tag for a folder, Veeam Backup for Microsoft Office 365 will perform full synchronization of that folder during the subsequent backup job session.
3.9 A SharePoint Site Collection hierarchy is not supported if the root site was not configured. Make sure to configure the root site in advance using a SharePoint site template of your choice. Otherwise, the following error occurs: Error: Failed to find web template ID for: STS#-1. This organization account might be missing a valid SharePoint license. Web configuration is not complete.
3.10 When backing up Microsoft Exchange mailboxes, Veeam Backup for Microsoft Office 365 does not create a new version of an item of which the Read/Unread property was changed. That said, the Read/Unread property of each of the backed-up items always remains the same as it was during the initial backup.
3.11 Veeam Backup for Microsoft Office 365 does not back up the following Microsoft Teams objects.
  3.11.1 Private channels.
  3.11.2 One-on-one and group chats.
  3.11.3 Audio and video calls.
  3.11.4 Video recordings.
  3.11.5 Contacts.
  3.11.6 Calendar: information about meetings and meeting chats.
  3.11.7 Code snippets in posts.
  3.11.8 Banner notifications in posts.
  3.11.9 Data of applications added as channel tabs that does not reside in the SharePoint document library of the channel.
3.12 As part of Microsoft Teams data backup, Veeam Backup for Microsoft Office 365 backs up only the following types of channel tabs: Website, Planner, Word, Excel, PowerPoint, Visio, PDF, Document Library, OneNote, SharePoint, Stream, Forms, Power BI, Flow and Azure DevOps
3.13 Veeam Backup for Microsoft Office 365 cannot backup SharePoint Online sites if their domain names were changed.
3.14 SharePoint sites with a red X over the symbol mean that there is an empty sector of the template and supported content is available in the subsites.
3.15 Microsoft Teams messages cannot be restored directly back to Teams.
3.16 Veeam Backup for Microsoft Office 365 restores public folders that are located under the IPM_SUBTREE folder only.
3.17 Bulk restore (restore of multiple objects) is not supported for public folder mailboxes. Use the regular per-object restore instead.
3.18 Cross-tenant restore to Microsoft Office 365 is only possible for Exchange Online objects, not for SharePoint sites.
3.19 Restore of OneNote notebooks from backups of Microsoft SharePoint and Microsoft Teams data for organizations with modern app-only authentication is not supported.
3.20 Restore of OneNote tabs from backups of Microsoft Teams data may fail with the "Configuration size exceeded. Provided: '4117' bytes MaxAllowed: '4096' bytes" error if the OneNote tab name includes non-Latin or special characters.

More information regarding specific permission requirements and information on the use of the Veeam Explorer can be found at the link below.

Veeam Backup for Microsoft Office 365 Guide

E&OE
18 March 2021