Integration guide for Veeam's Backup solution

Revision history

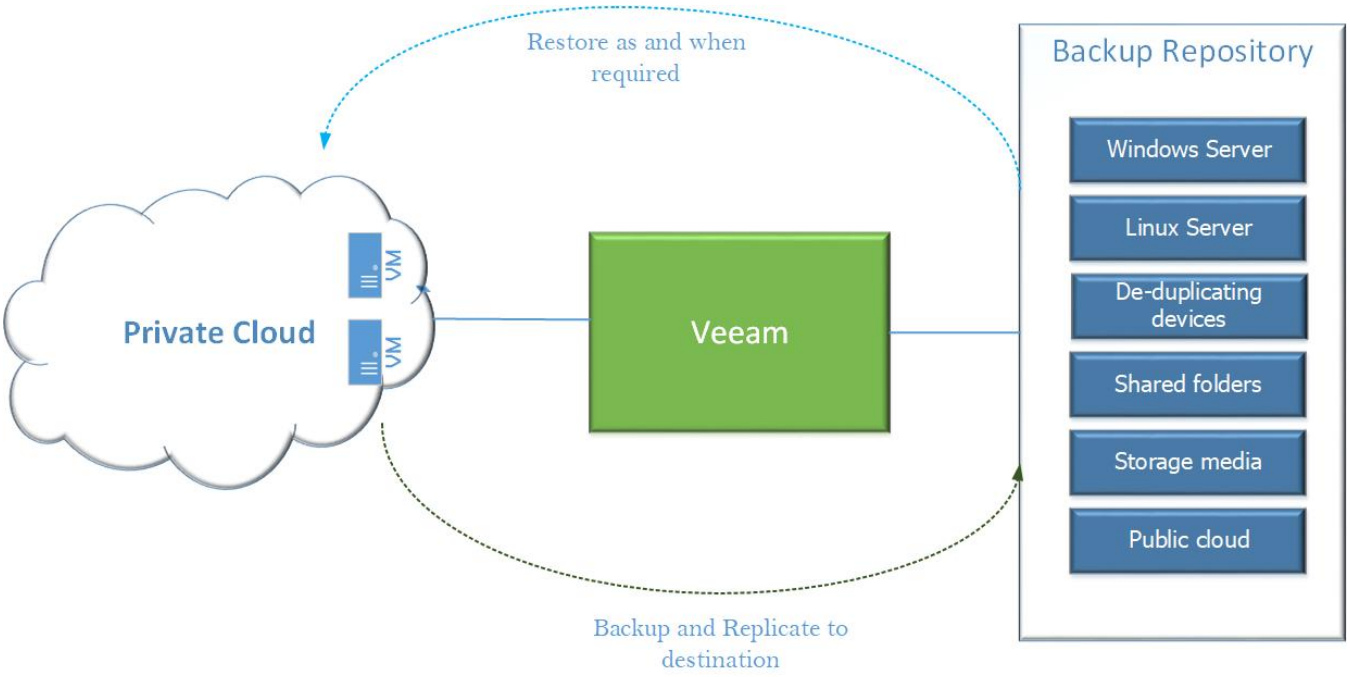
Revision	Author	Date	Description
0,85	Jyoti Ranjan	25-August-2019	Copied Agena's specific details from Investigation report on Veeam for Managed Backup of Private Cloud here
1.0	Jyoti Ranjan	27-August-2019	Re-factoring document to be more specific to Agena as asked by **AGE-275** - Getting issue details... STATUS (new story)
1.01	Jyoti Ranjan	29-August-2019	Drafted diagram to illustrate workflows instead of text for specific use cases. Also, added minute access details as asked in story **AGE-275** - Getting issue details... STATUS (new story)
1.02	Jyoti Ranjan	06-September-2019	Incorporated sections as per review comments.

Introduction

GreenLake Hybrid Cloud (GLHC) cloud platform is a flagship managed cloud offering by HPE. Gemini is one of the product line up which aims to support **VMaaS** (VM as a Service) in private cloud space with the robustness, simplicity, scalability and pay-as-you go model. In other words, the goal of the “VMaaS” offering is to reduce friction between on-prem infrastructure and customers need of public cloud like experience using on-prem hosted service. The solution will allow customers to deploy various “services” (virtual machines, networks, storage etc.) through a self-service portal. The services will run on infrastructure residing on the customer premise or in a co-location facility. In order to simplify overall user experience, HPE will manage and operate certain aspects of the solution. Customers will no longer have to deal with the complexity of managing and integrating cloud services.

As part of managing end user's virtual infrastructure, it is paramount to have a data availability strategy for cloud as things fail in production environment. Backup is of the critical aspect of data protection strategy. it is important to perform backup of user's virtual infrastructure and ability to restore it to point in time when last backup was taken. Also, it needs to be ensured that application workload gets minimal impact when backup is being carried our and restoration of failed entities (VM or virtual disk or VM files) is carried out as soon as possible. One of the way to achieve is to integrate Agena cloud with third party backup solution like Veeam, CommVault etc. In this section, we go deeper into aspects needed to integrate Veeam Backup & Replication with Agena cloud without too much focus on specific of Veeam feature. If you are looking for Veeam features in more detail, please see Veeam documentation.

The below picture depicts very simplified view of connecting Private Cloud, Veeam Backup solution and Backup devices ranging from simple Windows server to storage array to deduplication devices like HPE StoreOnce.



Approach for backup solution belong to primarily two category:

- **Manged Service.** In this case, backup solution is offered by backup service provider and backup user interface is not exposed to end user
- **Self-managed Service approach.** In this case, backup solution runs like a service where API or endpoints are exposed to end user running workloads.

GreenLake will support first approach. Our goal is to leverage customer Veeam infrastructure, the focus of section is on Managed Service mode but being managed by customer. In this case, we will not be exposing Veeam API or Veeam UI. All integration aspects, backup and restoration activities will be performed by HPE but bringing up and management of infrastructure will be done by HPE customers. HPE will use customer deployed infrastructure. It can be configured to use same infrastructure among tenants and unified jobs for backup scheduling. Or, customer can choose application category based backup infrastructure and different jobs for backup scheduling. Henceforth, customer is responsible for setting the backup policies according to the agreed service level agreement (SLA), and for performing all restore operations after receiving a request from the their end user or on failure of system. Rest of document provides more insight keeping this perspective in mind.

Assumption

Veeam integration significantly gets impacted with the size of infrastructure it has to deal for VM backup. Larger the infrastructure, the deployment architecture should have multiple instances of Veeam specific component. This document does not focus on specific sizing aspect but assumes following parameter as reference for rest of contents in document.

Private cloud infrastructure	• Hypervisor = ESXi • Maximum number of ESXi hosts = 24 • Maximum number of VMs = 2000 • Storage media used for VM = Nimble • Maximum amount of raw storage = 100 TB • Nimble has been used as primary storage media as well primary backup. iSCSI protocol is used to connect ESXi host with primary storage media.
Backup infrastructure	• Customer is responsible for backup job configuration instead of usage of backup service by direct tenant. • Veeam services are deployed as an appliance and hence iSCSI network is used as backup network. It helps to offload the burden on management network. • Storage array (e.g. HPE 3PAR or HPE Nimble) has been used as primary backup. Usage of storage instead of tape provides foster faster restoration process and is typically used for secondary backup now a days. • Storage-level snapshots is used as VMware hypervisors are relieved of the resource usage due to long-lasting VM snapshots and their consolidation (delete) that occurs at the end of the backup operations. • Veeam Backup Proxy is configured to use 'Direct Storage Access' transport mode. • The environment is configured to use only primary backup. No secondary backup is configured.

Supported use cases

Veeam is comprehensive backup, replication and restoration solution. It supports multiple hypervisors, multiple backup media and public cloud including reasonably good DR through replication of data across multiple sites. This document focuses on backup and restoration of VM deployed in private cloud only and does not address remote site backup, disaster recovery or backup to public cloud. As of now, the following use cases are intended to support:

1. Backup of entire VM or specific virtual disks or specific files used by VM
2. Recover entire VM to the Original or Different host
3. Quickly restore to user by starting a VM directly from a backup file on regular backup storage
4. Recover individual VM files (such as VMX) and virtual disks (vhd, vhdx or vmdk)
5. Full VM recovery
6. Instant VM recovery
7. VM file and virtual disk recovery
8. Perform advanced search and restore

Deployment architecture

Veeam requires its backup infrastructure (services, network, port) to be configured so that it can connect to vCenter to perform backup of VMs over host management network and store it to destined backup repository. In context of Agena, Veeam backup infrastructure can be possibly deployed in following ways:

1. **Organic deployment.** Customer deploys Veeam on infrastructure used to user workloads or VMs.
2. **Inorganic deployment.** Customer has pre-existing deployment of Veeam and he or she wants to integrate with Agena cloud.

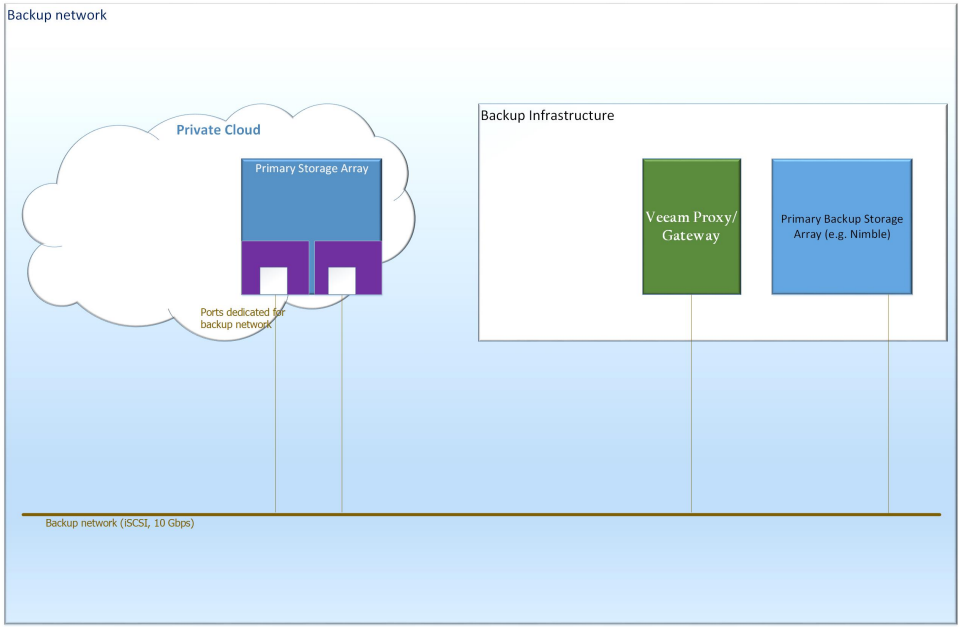
In this document, the scenario (2) is explored, where customer is responsible for hosting Veeam components.

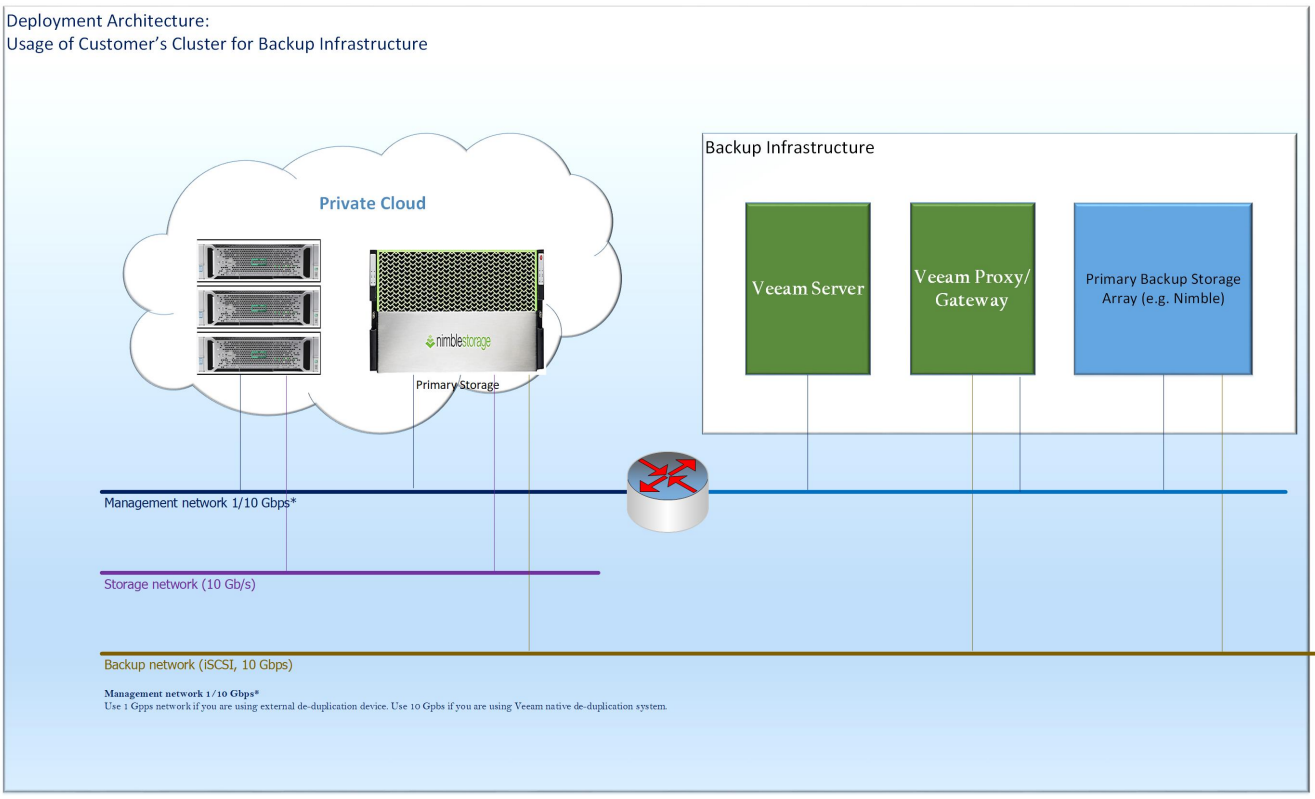
There are plenty of permutation and combination in the way Veeam and Backup devices can be integrated which can vary based on:

- Source storage media used for VMware datastore
- Destination backup media
- Organization of VMware resources like VMs, virtual disk etc
- Backup policy
- Backup restoration need and restoration mechanism applied at the time of recovery
- Data protection strategy
- etc.

It is not possible to explore and illustrate all permutation and combination in this document. This document aim to illustrate how the most common use cases can be realized by following steps detailed below. For others, refer Veeam documentation. However, it is worth to have a better understanding of networks as mentioned below.

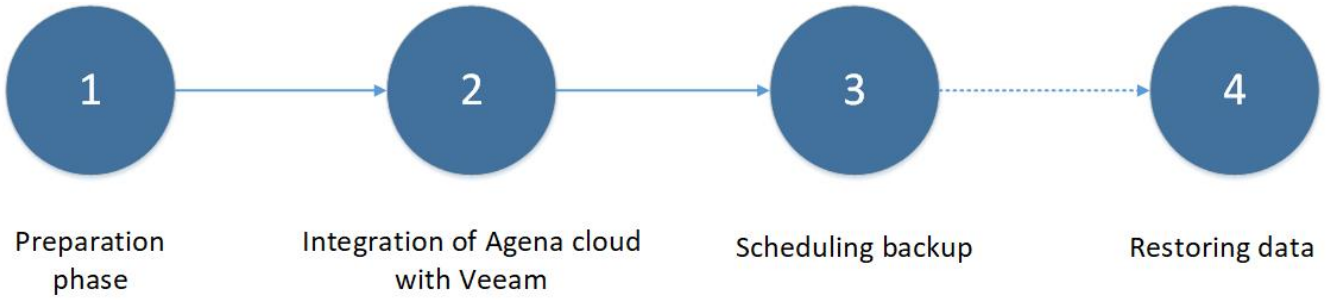
Network	Purpose	Integration specific information
Management network	It is the data center management network used to connect vCenter with ESXi hosts.	As the expectation is to use pre-deployed backup infrastructure used by customer, a routing mechanism needs to be devised w management network. It is owned by customer.Speed of network should be 1 Gbps or 10 Gbps if you are using Veeam for ded **Note:** We have not been able to find reference architecture where vCenter management network is not shared with Veeam bac two network should work fine. This piece needs to be tested in lab.
Storage network	It is used to connect ESXi host with primary storage.	It is owned by HPE. Speed of network should be 10 Gbps.

Backup network	It is used to Direct storage access during backup. It helps Proxy servers to read data directly primary storage volumes and hardware snapshots via FC or iSCSI. It greatly reduces the workload on the production hypervisor because the data path is Storage->Proxy instead of Storage->HyperVisorProxy. It is strongly recommended configuration.	Private cloud should facilitate an independent network termed as backup network) which facilitated FC or iSCSI connection am It is owned by customer. Speed of network should be 10 Gbps. To avoid undue traffic on workload or data network, it is recommended to have backup network as independent network. For th to be connected to backup network as depicted below. The requirement to have provision for iSCSI ports for backup network is 



Integration steps

The integration activity can be categorized in four groups primarily as mentioned below.



Preparation phase

In this phase, we primarily collect following sets of information which will be needed during integration phase.

<table>
<tr><td>Backup repository</td><td>Identify backup repository or backup volume in destination storage array or file store based on your backup infrastructure.</td></tr>
<tr><td>DNS information</td><td>FQDN or IP address of DNS server begin used in our vCenter environment</td></tr>
<tr><td>Source and target permission for account used to install and use Veeam

Note: This needs to be played with setup to discover more as documentation is not giving clarity.</td><td>1. Write permission on the target folder and share (applicable only if we are using filesystem as backup repository)
2. If we are using 'Direct Storage Access' mode, grant volume level access to Veeam Backup & Replication proxy server(s). The volume being referred here is storage volume used to form VMFS datastore. Also enable “Allow multiple initiator access” property in Nimble volume management UI.
3. vCenter server permission (more specific detailed below)</td></tr>
<tr><td>vCenter Server permission</td><td>1. It is preferred to have admin user with full rights unless and until there is specific reason to do that. It is so because configuring elemental operation might get interrupted because of access reason if not configured properly or changed post configuration. Considering that backup and restore is a managed service and is not exposed to end user, it is reasonably acceptable to proved admin operation.
2. Admin user name and password
a. Full rights or
b. Specific rights for activities: Backup operation, Replication, Instance VM recovery, Quick recovery, SureBackup, Entire VM recovery, Replica failover, Replica failback, File-level store and vSphere web client plug-in for Veeam backup and replication. The cumulative details for backup and replication is depicted below.
<table>
<tr><td>Cryptographic operations</td><td>• Add disk
• Direct Access
• Encrypt
• Encrypt new
• Migrate</td></tr>
<tr><td>Datastore</td><td>• Allocate space
• Browse datastore
• Low-level file operations
• Remove file</td></tr>
<tr><td>Datastore cluster</td><td>• Configure a datastore cluster</td></tr>
</table>
</td></tr>
</table>

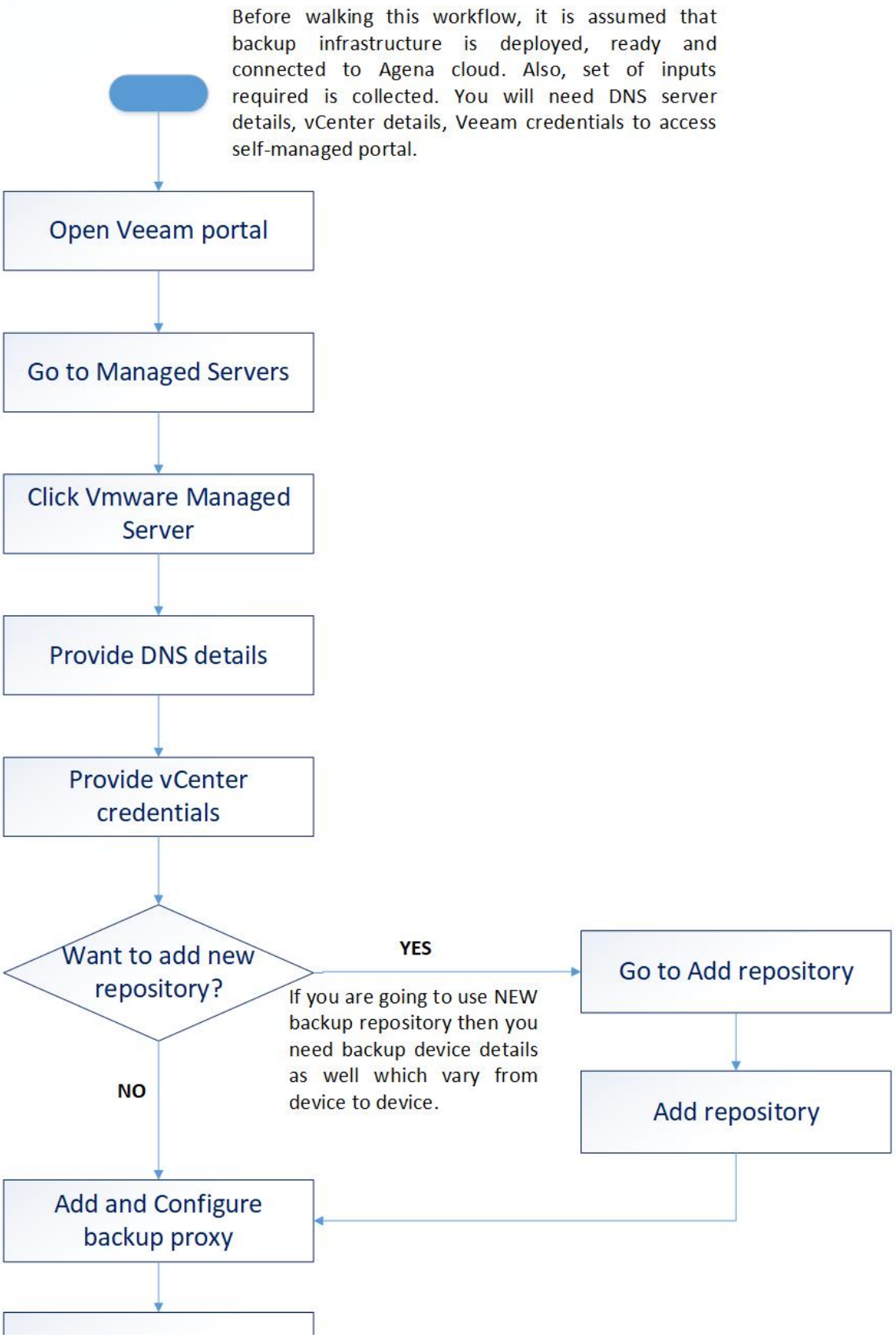
Extension	• Register extension • Unregister extension
Folder	• Create folder Delete folder
Global	• Disable methods • Enable methods • Licenses • Log event • Manage custom attributes • Set custom attribute • Settings
Host	• Network configuration • Storage partition configuration
Network	• Assign network • Configure
Resource	• Assign virtual machine to resource pool • Create resource pool • Migrate powered off virtual machine • Migrate powered on virtual machine • Remove resource pool
Storage Profiles	• Profile-driven storage update • Profile-driven storage view

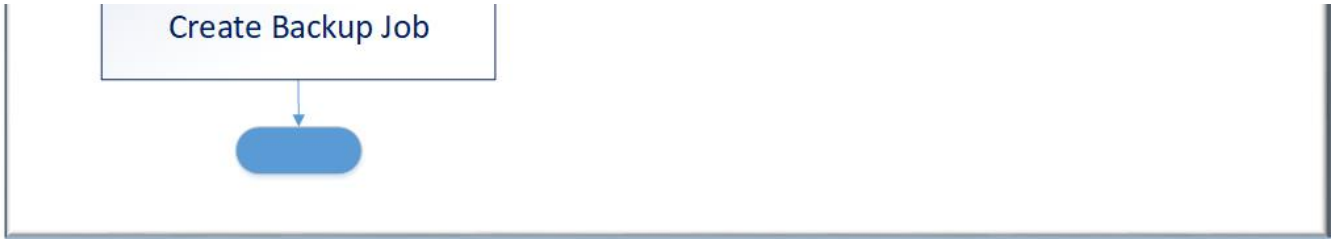
<table>
<tr><td></td><td>
<table>
<tr><td>Virtual Machine</td><td>
<table>
<tr><td>Change Configuration</td><td>• Acquire disk lease
• Add existing disk
• Add new disk
• Add or remove device
• Advanced configuration
• Change Settings
• Change resource
• Extend virtual disk
• Modify device settings
• Remove disk
• Rename
• Set annotation
• Toggle disk change tracking</td></tr>
<tr><td>Guest operations</td><td>• Guest operation modifications
• Guest operation program execution
• Guest operation queries</td></tr>
<tr><td>Interaction</td><td>• Console interaction
• Connect devices
• Guest operating system management by VIX API
• Power Off
• Power On
• Suspend</td></tr>
<tr><td>Edit Inventory</td><td>• Register
• Remove
• Unregister</td></tr>
<tr><td>Provisioning</td><td>• Allow disk access
• Allow read-only disk access
• Allow virtual machine download
• Allow virtual machine files upload</td></tr>
<tr><td>Snapshot Management</td><td>• Create snapshot
• Remove snapshot
• Revert to snapshot</td></tr>
</table>
</td></tr>
<tr><td>vSphere Tagging</td><td>• Assign or Unassign vSphere Tag</td></tr>
<tr><td>dvPort Group</td><td>• Create
• Delete</td></tr>
<tr><td>vApp</td><td>• Add virtual machine
• Assign resource pool
• Unregister</td></tr>
</table>
</td></tr>
<tr><td>Credential for Veeam services</td><td>1. Host name or the IP address of the Veeam Backup Enterprise Manager.
2. HTTP(S) port of the Veeam Backup Enterprise Manager API
3. Username and password to authenticate with the Veeam Backup Enterprise Manager.</td></tr>
</table>

Integration of Agena cloud with Veeam

The below workflow how one can integrate Veeam with private cloud for backup and restoration activity of VM, virtual disks and VM files.

Steps to add Veeam for Private cloud's backup





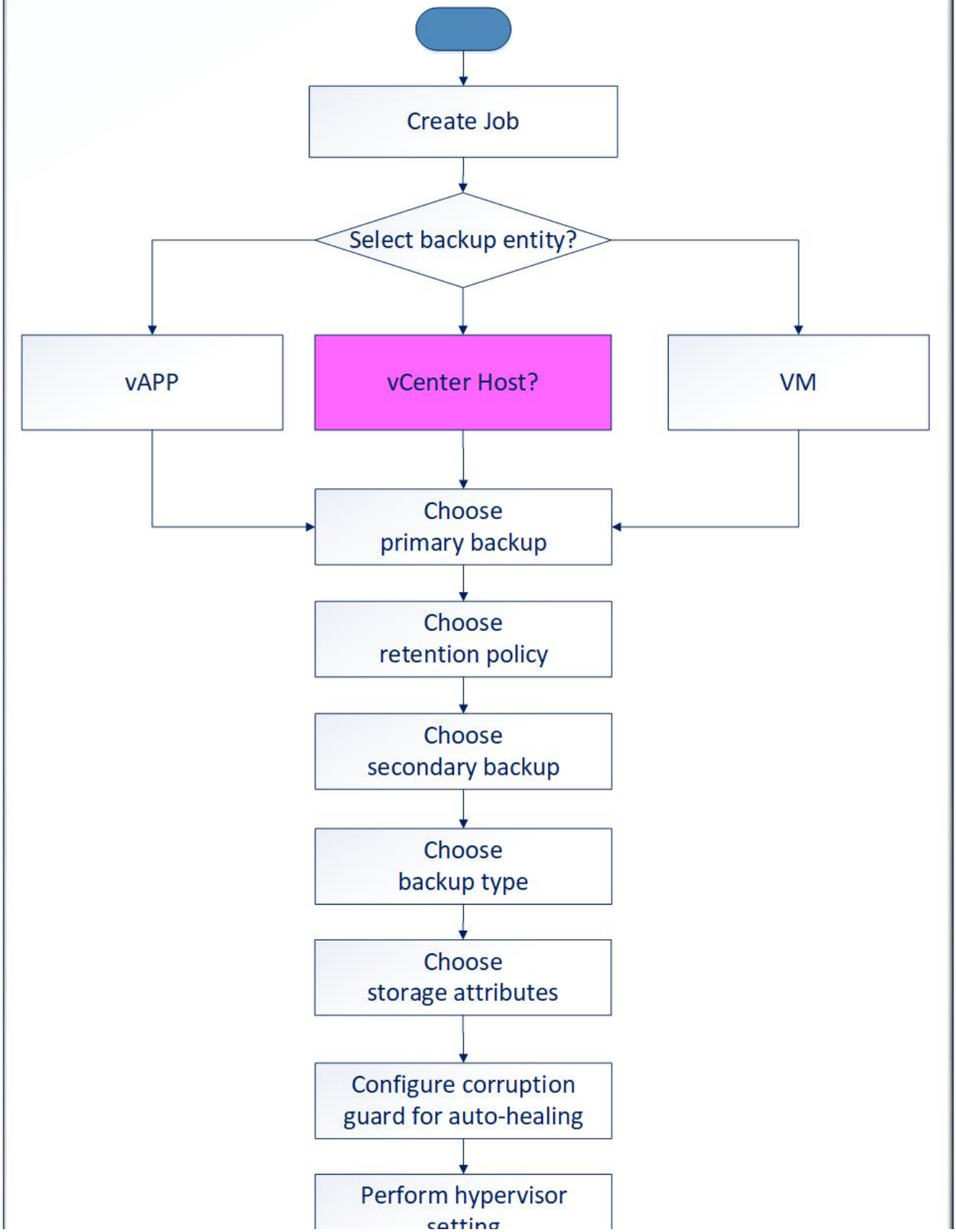
Scheduling backup

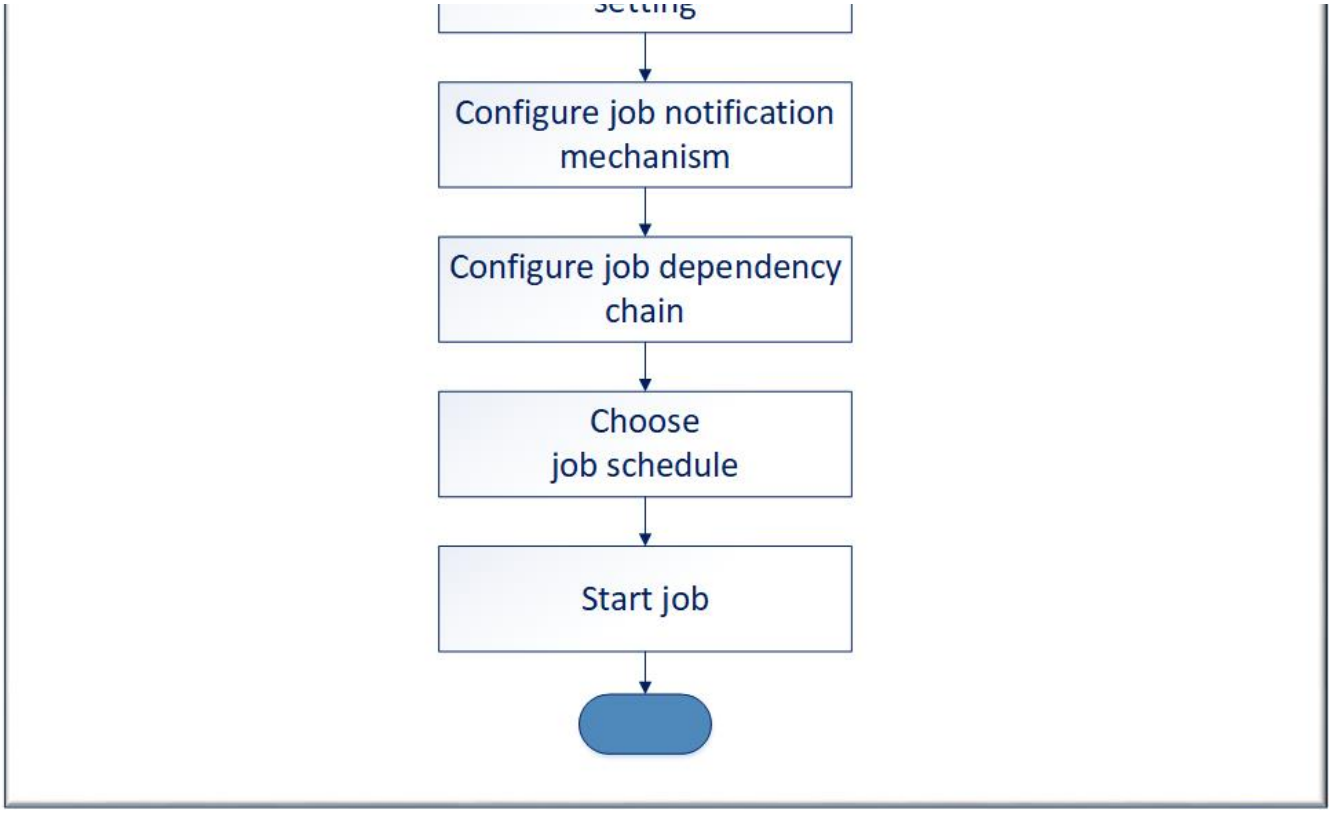
As mentioned above, job is the one which provides scheduling of backup. Configuration of job is very much tied to customer requirement and workload characteristics. We do recommend following standard values, if there is no specific requirement.

Retention period	7 days
Number of simultaneous backup	10
Number of job / VMs	30
Backup type	'Forever Forward Incremental Backup'

The steps to create backup job is depicted below.

Steps to create and schedule backup job





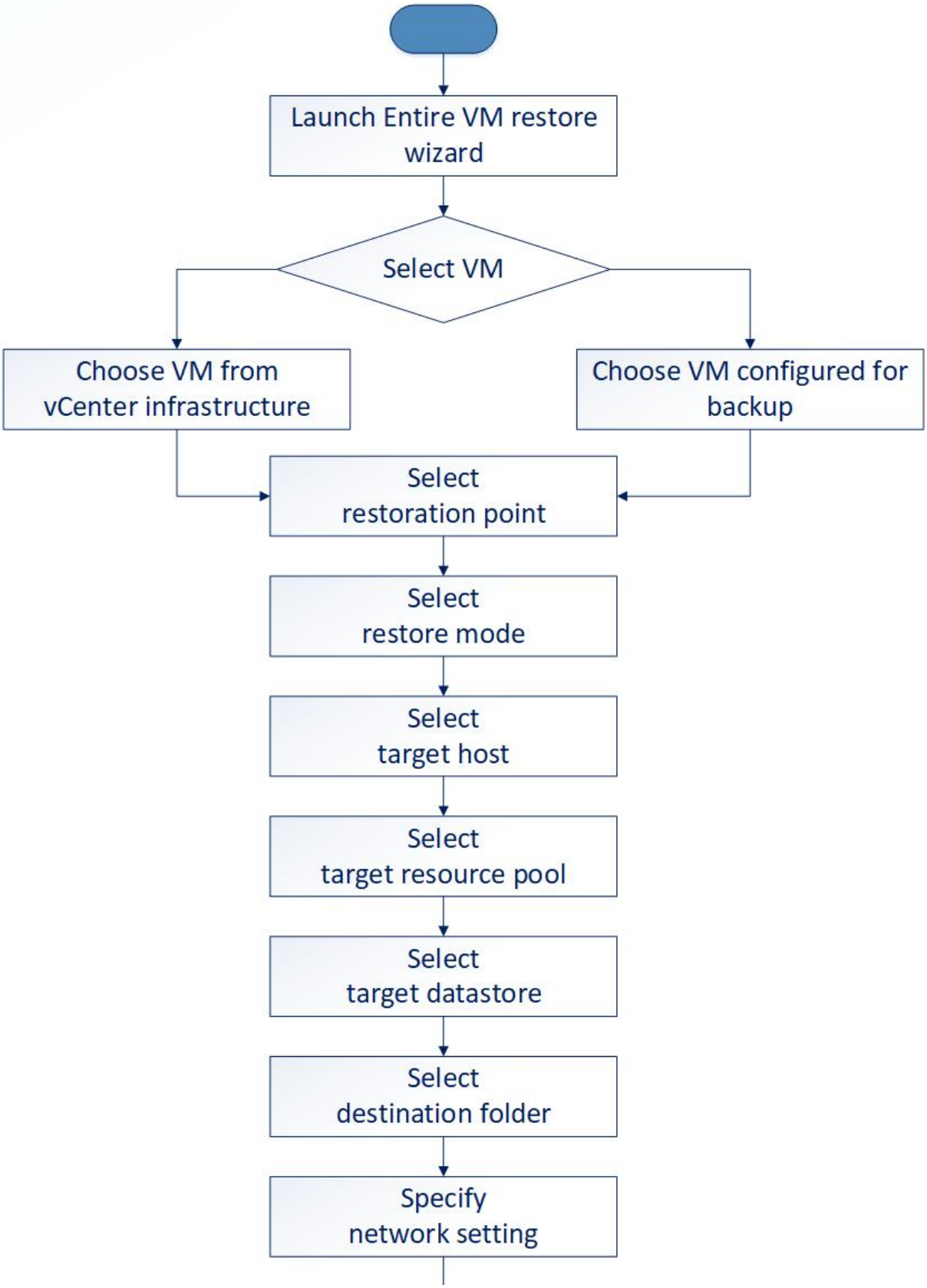
Restoring data

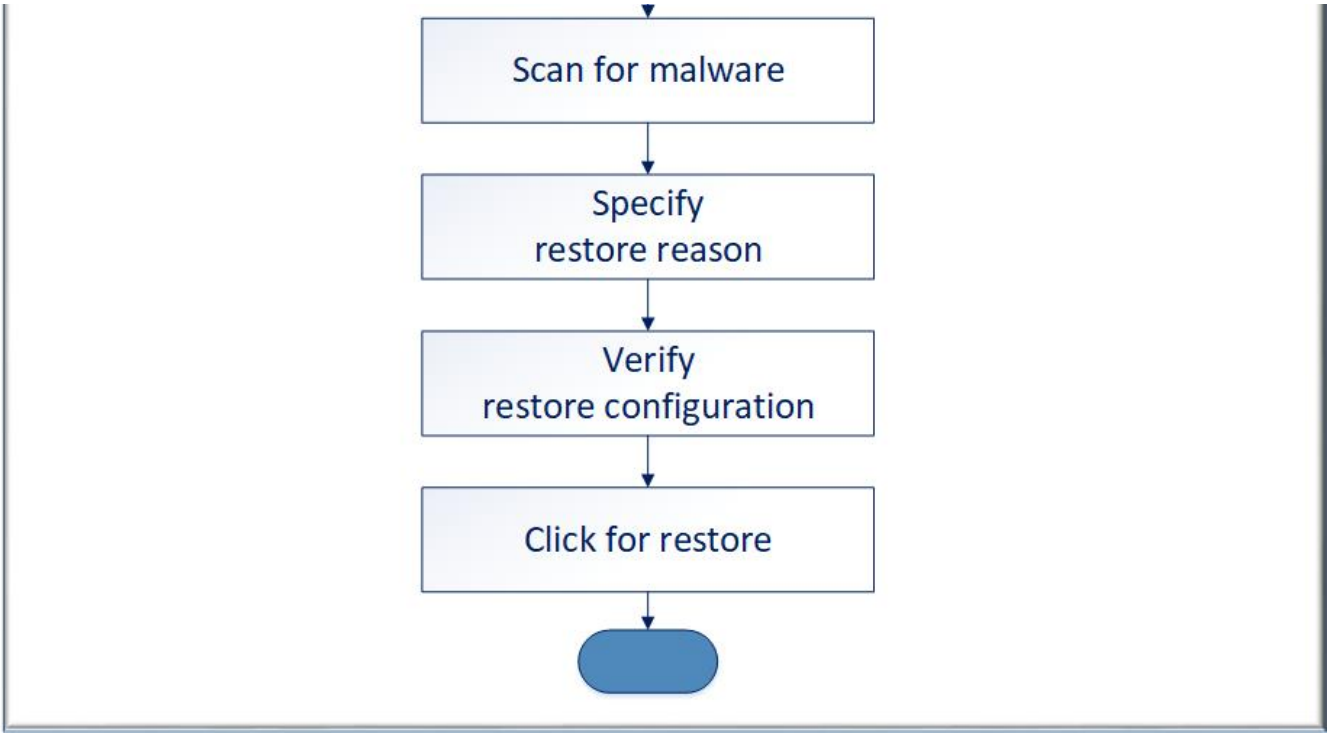
The restoration process depends upon what entities are backed up and which one you want to restore at given point of time. Veeam provides many eco-system. In the context of Agena, our focus will be primarily on restoring following entities:

- Restore VM using instant recovery - should be used only for ultra production restoration need
- Restore entire VM
- Restore virtual disk
- Restore VM files

The 'Restore entire VM' use case is commonly used. The workflow for same is depicted below. For other use case please refer Veeam documentation.

Steps to restore entire VM





Best practices (general recommendation)

Backup strategy	• Define your data protection strategy • Category workloads in the terms of medium, high and critical workload • Adhere to 3-2-1 rule

Backup infrastructure	• Use 10 Gbps if you are relying on Veeam Backup Proxy for de-duplication.
	• Do not deploy backup infrastructure in source cloud infrastructure being backed up. Keep source and backup destination different.
	• Veeam deployment
	  • Deploy multiple Backup and Replication server if numbers of VMs are greater than 500.
	  • Use independent instance of Microsoft SQL Server
	• Backup repository
	  • Use Nimble as primary backup storage to meet better RTO instead of tape.
	  • Use secondary backup at remote site

Job configuration	• Number of backups = 10 • Retention period = 7 days • Use 'Forever Forward Incremental Backup' as backup algorithm • Number of VMs per backup job = 30 • [Optional] For backup of secondary backup, use backup copy job in the chain of backup operation.

Integration with Morpheus

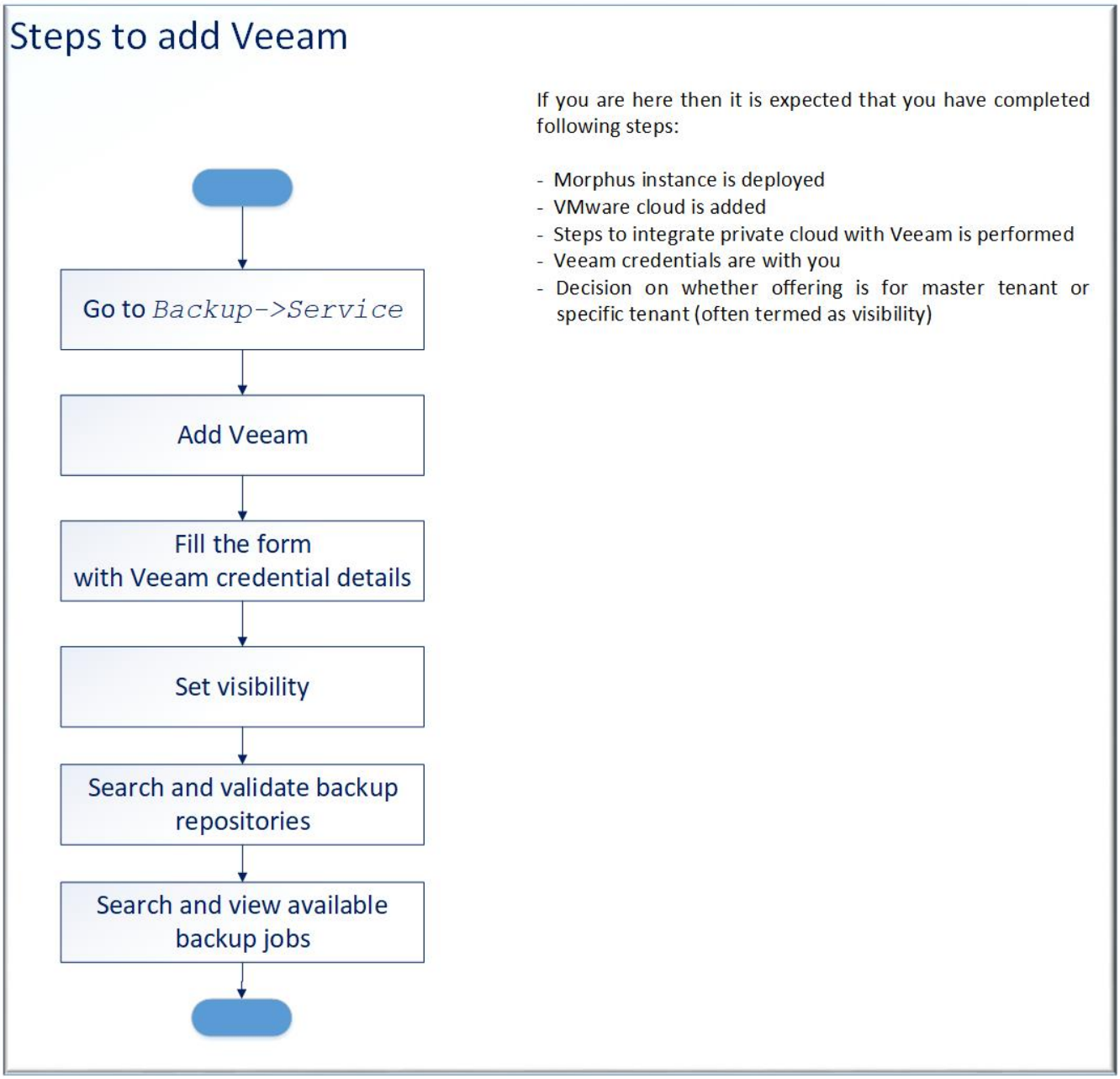
Morpheus provides ability to add Veeam as backup provider along with supporting its own internal backup mechanism. The supported operations related to backup are:

1. Scheduled automatic Backups
2. Create Backups on demand
3. .Copy Snapshots to backup repository (if added)
4. Choose default backup provider

This section talks about how we can use Morpheus in conjunction with Veeam. The following aspects have been covered.

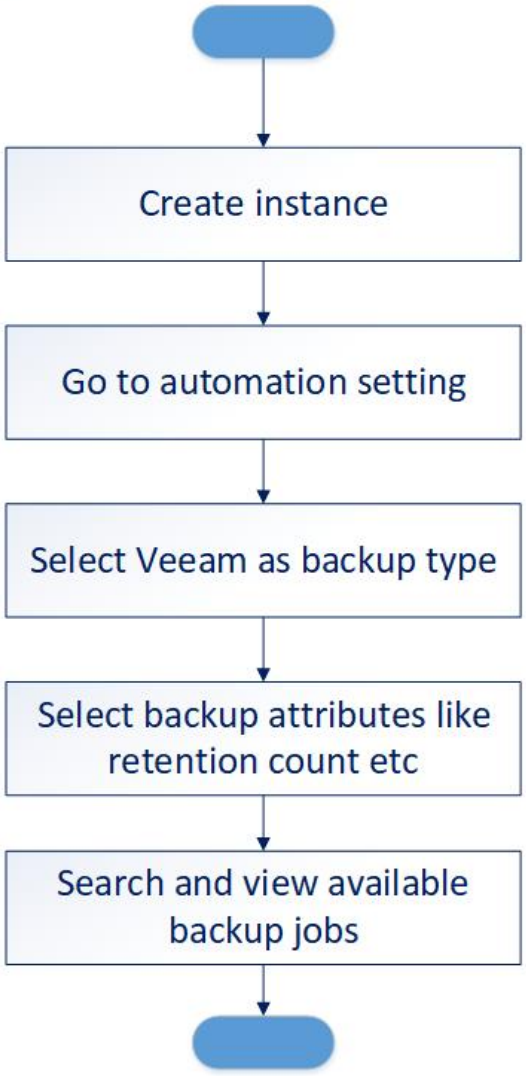
1. Adding Veeam as backup provider
2. Creating Backup
3. Restoring VM from backup

Adding Veeam as backup provider



Creating backup

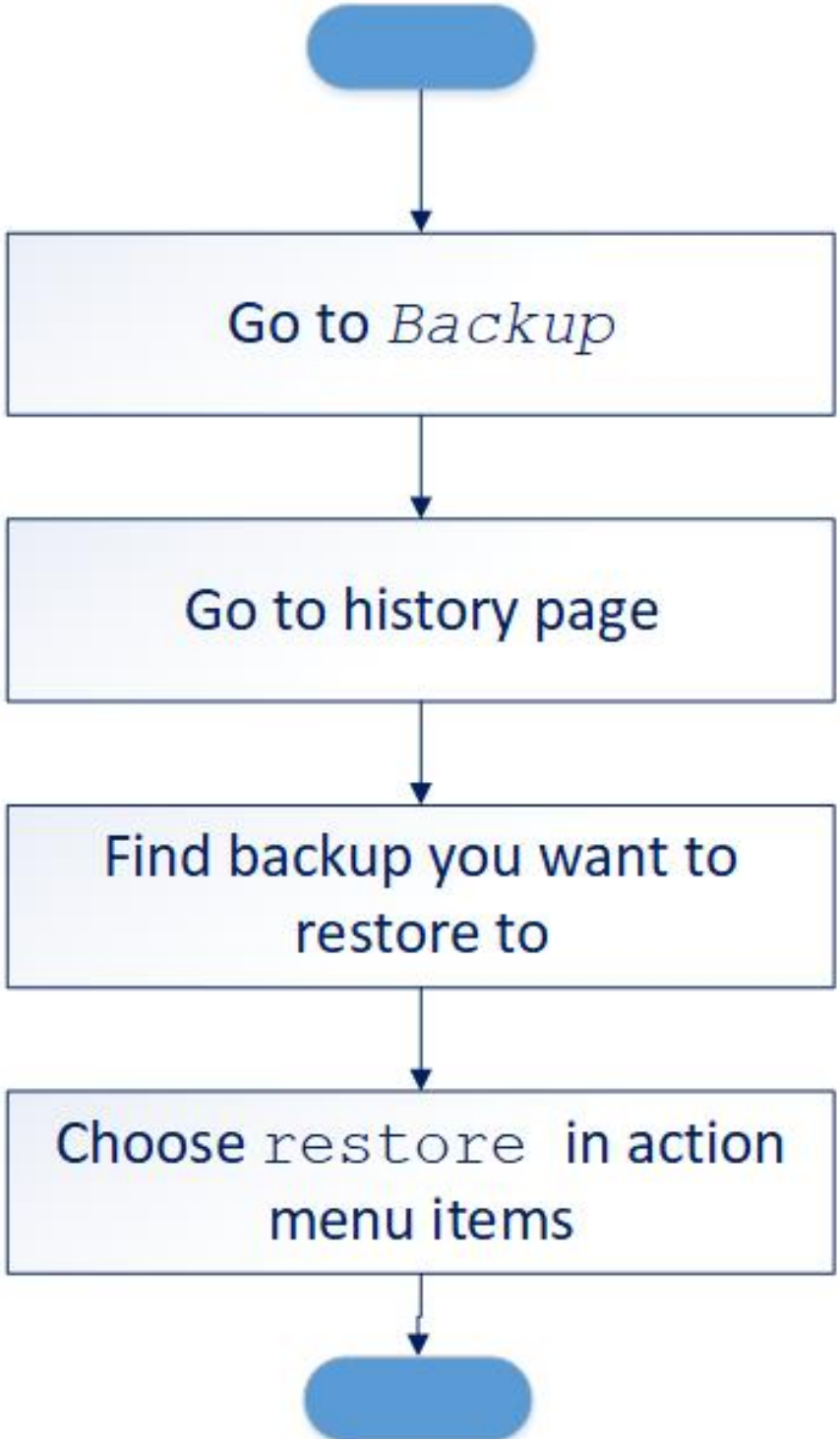
Configuring backup of instances



This illustrates how we can configure backup of virtual instances at the time of provisioning. The workflow assumes that global settings has enabled backup. If not please go to `Administration -> Backups` and enable Create backups.

Restoring instance

Steps to restore VM instances



Summary

Veeam Backup, Replication and Restoration provides a rich feature set to solve data availability and protection strategy for Private cloud of varying size. Based on size of private cloud, backup infrastructure for Veeam should be scaled for specific component to avoid sluggish performance. Integration of Veeam involves primarily following steps:

- Collect datasets needed to add and configure Veeam
- Adding Veeam
- Configuring backup job
- On demand, restoring data from backup repository

It is strongly recommended to use storage array as primary backup device and configure Veeam backup proxy in 'Direct Storage Access' mode to avoid data traffic with ESXi host at the time of backup and restoration.