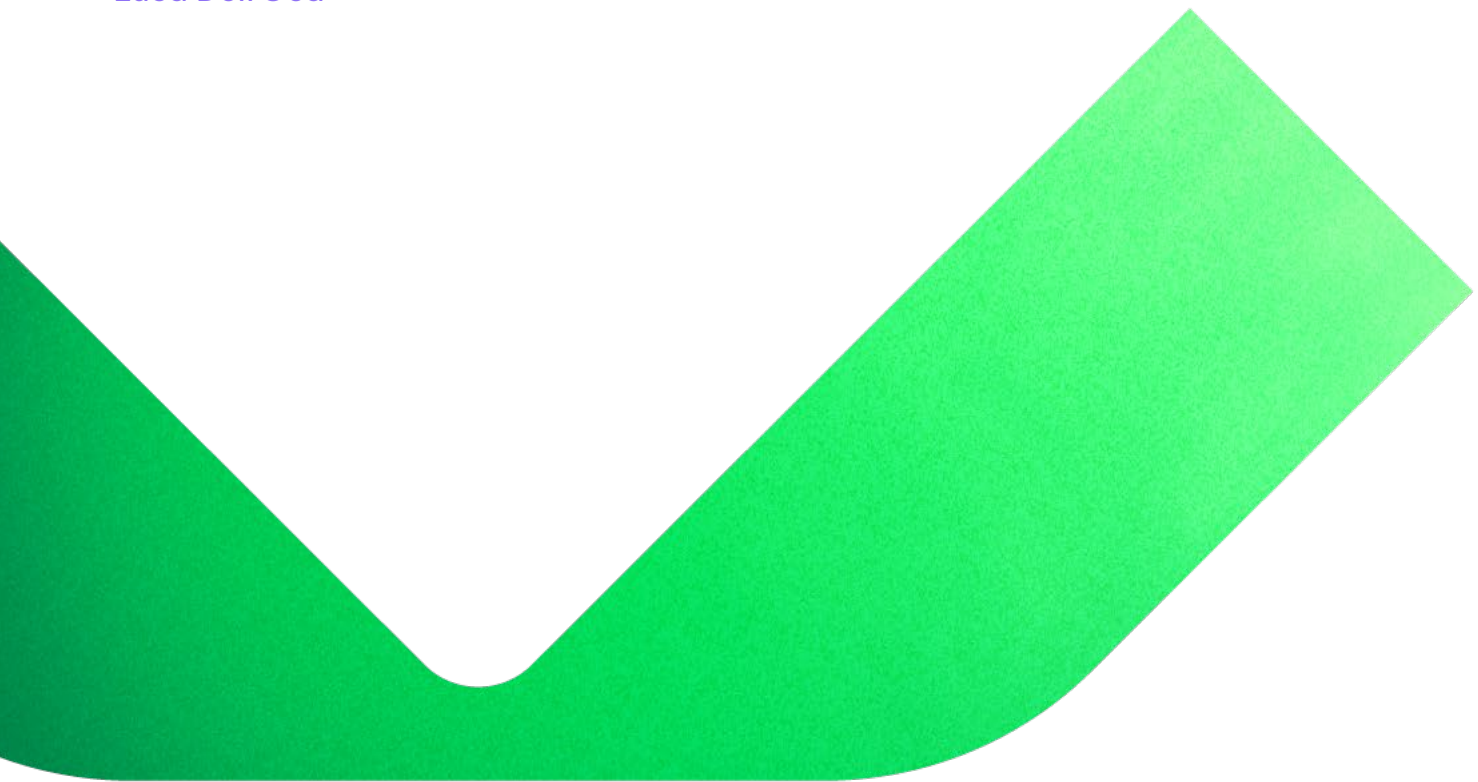




One-Two-Many Portals

Artem Philippov
Luca Dell'Oca





Contents

Introduction	3
Portals	4
Enterprise Manager	5
Management of VBR installations	6
Veeam Backup Enterprise Manager 1	6
Provide access only to restore scope.	7
Restore scope 2	7
Server Administrator to Restore Guest Files	9
Self-Service File Restore Portal 3	9
Backup and Restore Self-Service for VMware vSphere	10
vSphere Self-Service Backup Portal 4	10
Backup and Restore Self-Service for VMware Cloud Director	12
Veeam Self-Service Backup Portal for Cloud Director 5	12
Veeam Cloud Connect Failover Portal 7	15
Veeam Service Provider Console and its friends	16
Veeam Backup & Replication Servers	18
Veeam Agents	20
Microsoft 365 management	21
Cloud Connect Failover	23
Final considerations	26



Introduction

For over a decade, here at Veeam we have dedicated ourselves to enhancing our product portfolio, creating a tailored fit for small businesses, medium-sized enterprises, and service providers. Each segment faces unique challenges while maintaining a focus on its distinct specialties. Small businesses seek simplicity and efficiency, while the core requirements for medium-sized enterprises include stability and comprehensive technology coverage. In contrast, scalability, and the ability to manage operations at scale are crucial cornerstones for both Enterprises and Service Providers.

Based on our extensive field experience, we have observed that Enterprises and Service Providers often share common ground, learning effective strategies from each other to achieve their respective goals. This whitepaper aims to illuminate the subject of managing Veeam Solutions at scale, based on experience we got from our clients.



Portals

 **portal**¹
/'pɔ:tl/

noun

noun: **portal**; plural noun: **portals**

1. a website or web page providing access or links to other sites.

Isolated ROBO architecture, Role-based access control, Self-service requirements, single pane of glass.

Those terms are in the top of the list, for any solution architect working for a scalable solution.

Originally most of Veeam Solutions came in the form of .NET software, based on Windows-based applications. The obvious downside was a requirement for direct access to a terminal server, where the application console was installed. This situation was bringing some security concern, as any direct access to a backend infrastructure is not an option in sensitive environments. For such cases, the best solution is to use a portal that sits in between the user and the infrastructure.

That was one of the core reasons for the first portal we had in our product: Veeam Enterprise Manager.

That was the first step. A decade later, the needs of sharing secure and flexible access to the backup infrastructure brought us more than 15 portals.

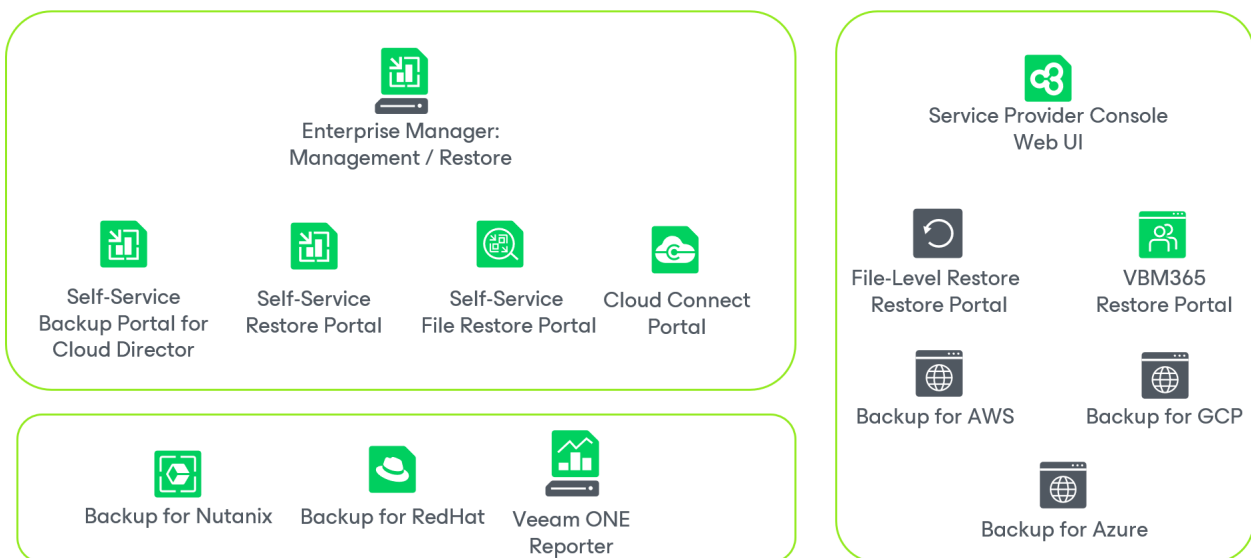


Figure 1. Portals available in the Veeam portfolio

If you've been gradually ramping up with Veeam products, use cases and interconnections can be obvious. However, it's a great challenge if you face it without a proper background. One of the key goals of this document is to classify the use cases/requirements in the Service Provider/Enterprise infrastructure and map them to the related product portal.



Enterprise Manager

Enterprise Manager was the first portal to provide Web-based access for backup management. Currently, there are 6 core use cases of this portal, which are connected to specific endpoints.

Portal	Main Use Case	URL
1. VBEM (classic)	Manage multiple VBR servers connected over LAN	<a href="https://<host>:9443">https://<host>:9443
2. Restore	Provide access only to restore operators	<a href="https://<host>:9443">https://<host>:9443
3. File Restore	Provide access to Server Administrator to Restore Guest Files	<a href="https://<host>:9443/selfrestore">https://<host>:9443/selfrestore
4. Self-Service Backup (vSphere)	Tenant self-service for IaaS based on VMware vSphere	<a href="https://<host>:9443/backup">https://<host>:9443/backup
5. Self-Service Backup for Cloud Director	Tenant self-service for IaaS based on VMware Cloud Director	<a href="https://<host>:9443/vcloud/<OrgName>">https://<host>:9443/vcloud/<OrgName>
6. VCD Plug-in	= VCD SSP within the VCD UI (iframe)	<a href="https://<vcd>/tenant/<OrgName>/plugins/<id>/veeam/portal">https://<vcd>/tenant/<OrgName>/plugins/<id>/veeam/portal
7. Cloud Connect	Tenant self-service DR failover based on VCC-R	<a href="https://<host>:6443">https://<host>:6443

We are not covering all the capabilities of EM, as they are explained in the technical guide. On the contrary, we are focusing on scenarios that we see mostly used in the field.



Management of VBR installations

Veeam Backup Enterprise Manager¹



Licence
management



Centralized API access
to VBR installations



Encryption Keys
Management

Most of the tasks related to the Enterprise manager can be split into 3 wide groups:

- **Management:** everything related to configuration, monitoring, and reporting of servers
- **Backup:** configuration of backup tasks
- **Restore:** recovery of the data, stored in backup repository

The initial core capabilities of the Enterprise manager for VBR installations were around **reporting and alarm management**. However, with the parallel development of Veeam ONE and Veeam Service Provider console native EM functionality became limited.

License management is still a valid use case, however, only when usage of the Service Provider Console is not possible. Otherwise, the latter is a preferable option, due to fewer port requirements and a greater number of management options.

On another hand, when building automation or reporting – **Enterprise Manager API** gives better flexibility and a greater number of calls and low-level details than Veeam Service Provider Console and Veeam Backup and Replication API. Nevertheless, there's no strict recommendation of which one to use, and the decision must be made based on the specific project requirements.

Encryption key management (the ability to decrypt the data if you have lost or forgotten the password used for data encryption or if a KMS server used for data encryption is not available) is the unique capability of the Enterprise manager. Due number of recent attacks, making silent changes of encryption passwords – it's highly recommended to use the protection option.



Provide access only to restore scope.

Restore scope²



The principle of least privilege



Application owner access



Self-service without job management

Even if a self-service backup portal is available for VMware (we are discussing it later) - which provides job management and restore capabilities – it doesn't support other platforms. Many service providers are protecting alternative platforms (Hyper-V, Nutanix AHV, Physical servers, File Shares) and still have a requirement to provide self-service capabilities to other departments, offices, or customers.

To cover this scenario, it's recommended to configure backup jobs using VBR Console directly and expose restore capabilities using Veeam Backup Enterprise Manager restore scope. The same approach can be implemented for service desk or application owners, which require only restore functionality, without any access to the job management itself.

The configuration of the restore scope is done through Enterprise Manager WebUI, by creation of additional role and assigning objects and restore permissions to it (Fig. 2)

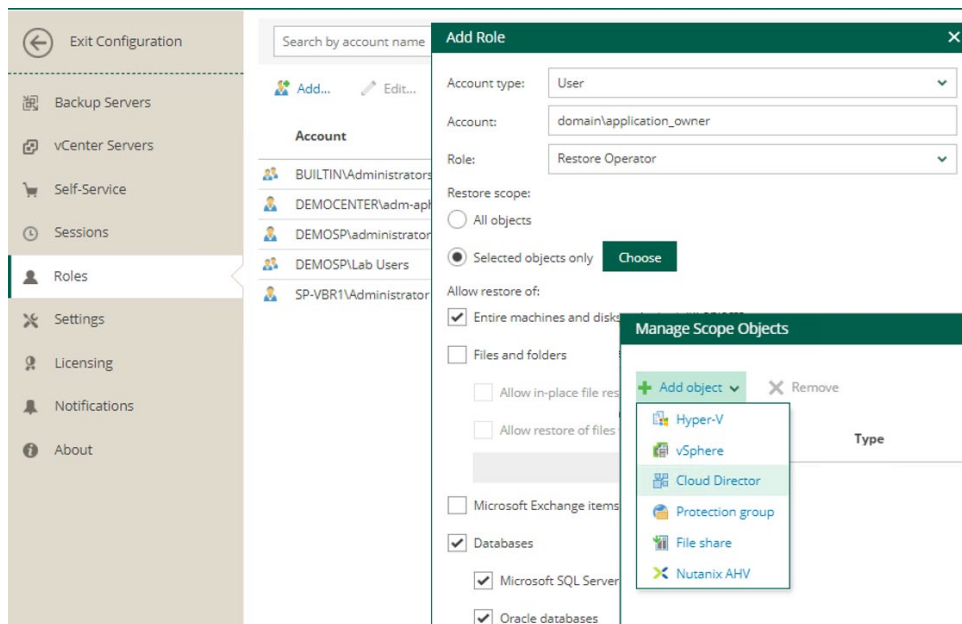


Figure 1. Configuration of restore scope.



In such a scenario, it's recommended to configure backup jobs using VBR Console directly and expose restore capabilities using Veeam Backup Enterprise Manager restore scope.

After that, the customer/application owner can log in to the portal with their credentials and have limited visibility, according to the scope.

Machine	Backup Server	Job Name	Restore Points	Location	Path	Last Success
exch1	hq-vbr1.demolab...	VMware - Backup to XF...	18 points	XFS Repository	/veeam/xfs_repository/VMware - Backup to XFS R...	16 hours ago
exch1	hq-vbr1.demolab...	Backup Copy to Data D...	12 points	EMC Data Domain	ddboost://172.21.238.87:demo@/Backup Copy to...	16 hours ago
exch1	hq-vbr1.demolab...	GFS Backups to Tape	44 points	Not available	Tape	23 days ago
exch1	hq-vbr1.demolab...	Backup Copy to ExaGri...	13 points	ExaGrid	/home/svc-exagrid/demo/Backup Copy to ExaGri...	16 hours ago
exch1	hq-vbr1.demolab...	VMwareLinux - Backup...	1 point	Not available	Tape	133 days ago
exch1	hq-vbr1.demolab...	HPE StoreOnce Catalys...	20 points	HPE StoreOnce (S...	storeonce://172.21.238.195:demo_copy@VMwar...	16 hours ago

Figure 3. EM portal with Restore scope.



Server Administrator to Restore Guest Files

Self-Service File Restore Portal³



**No configuration
needed**



**Server administrator
access**



**File-level
restore**

The advantage of the previous approach lies in its broad spectrum of restoration capabilities, however at the cost of additional operational load. Managing an extensive array of applications and individual server administrators can make the creation of distinct roles nearly impractical. Moreover, there are situations where the backup administrator may prefer to delegate only the ability to perform file-level restores, such as in a VPS infrastructure.

In such scenarios, the most straightforward solution is the Self-Service File Restore Portal. If all its prerequisites are met, it seamlessly works out of the box. Users possessing local administrator rights on a Windows machine can effortlessly access the portal using the provided general URL³ and their respective accounts.

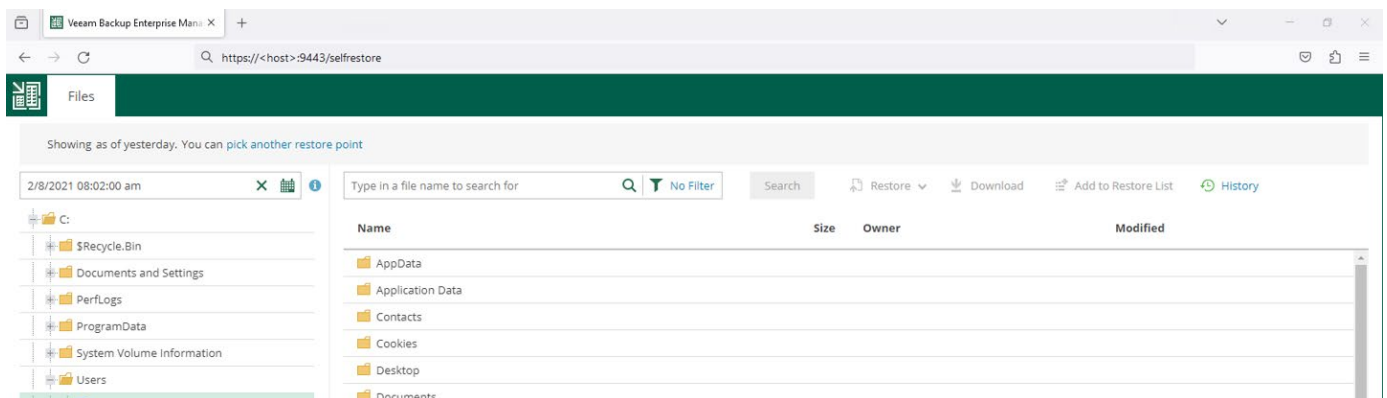


Figure 4. Guest Files Restore portal



Backup and Restore Self-Service for VMware vSphere

vSphere Self-Service Backup Portal⁴



Management of Backup Jobs



Recovery of VMs and Application data



Repository quotas

Service Providers (and Enterprise customers acting like Service Providers for their departments) often want to delegate not just the restore operations, but also the backup operations. After all, as the name IAAS implies, they offer (and operate) the underlying infrastructure, not the multitude of applications that all the tenants are going to execute on top of it.

When VMware vSphere is used as the underlying IaaS technology, the best solution is to use the vSphere Self-Service Backup Portal.

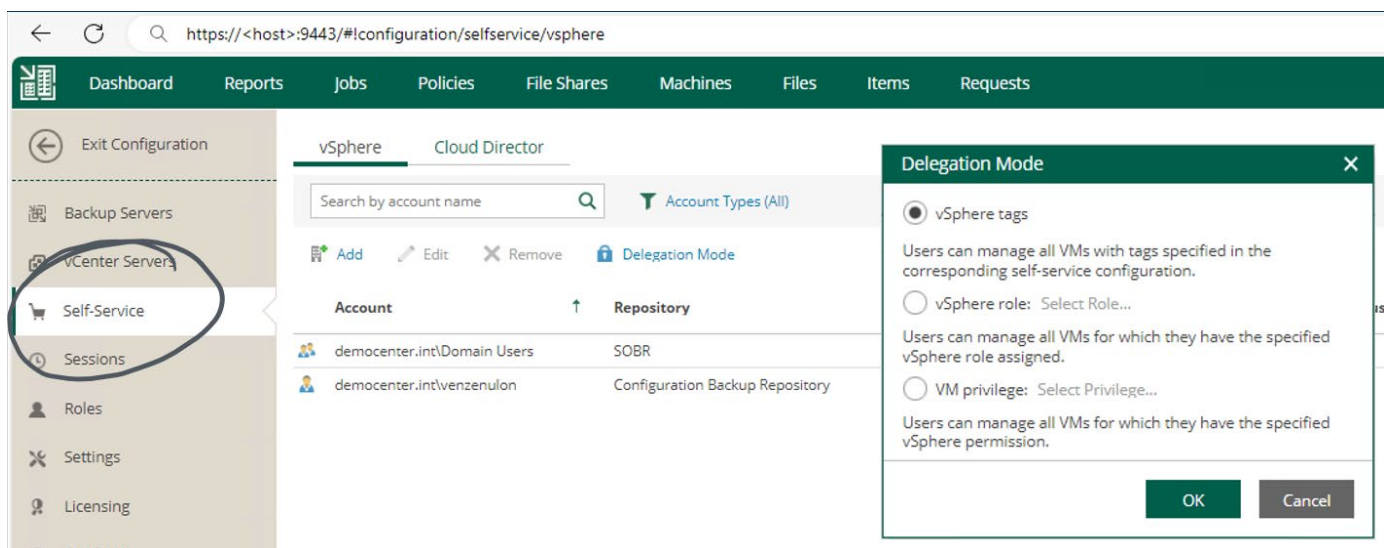


Figure 5. Initial configuration by Administrator



This portal empowers administrators to establish a secure and protected Self-Service environment. Portal administrators can determine which users have access to the environment and specify the level of access for each user/group. They can leverage multiple options such as vSphere tags, vSphere roles, or VM privilege. The enforcement of multitenancy is then achieved through one of the available delegation modes.

Figure 2. Organization configuration

For each group or user, administrators have the flexibility to designate the repository to be utilized, set the quota that can be consumed, define the level of freedom in job scheduling for each user, and outline the scope of their permissions.

The recommended approach is to configure multitenancy in a manner that allows tenants to use the same credentials for the IaaS vSphere platform. This ensures a seamless user experience across the board.

Tenants can operate completely within the portal, having a wide degree of freedom to configure the preferred policy to protect their virtual machines, deciding which machines to protect, the different options for application processing, and the frequency and retention, inside the limits imposed by the Quota assigned to them.

Restore operations can then be executed from the same portal, with options to recover an entire virtual machine (to an existing or new location), single files, and application items.

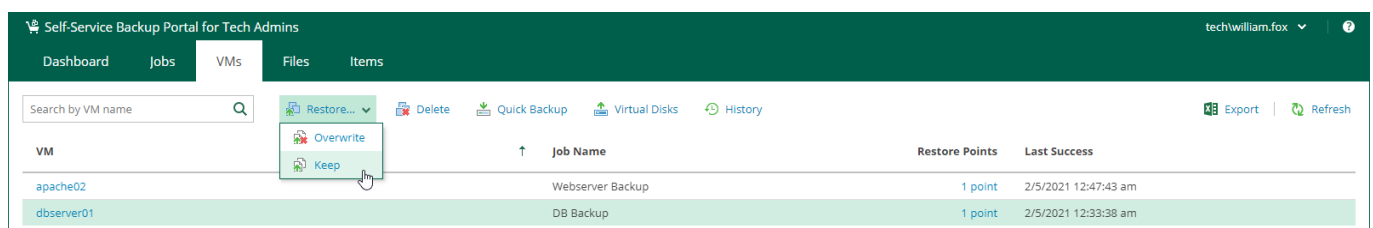


Figure 3. Self-Backup portal restore capabilities

Keep in mind that in an IaaS environment network isolation is a common scenario. Files level restore in network-less mode (over VIX) is heavily limited by the VIX transfer rate (2Mb/Sec). Application items level restoration without a network connection to the guest VM is not possible. For the list of required ports visit the user guide.



Backup and Restore Self-Service for VMware Cloud Director

Veeam Self-Service Backup Portal for Cloud Director⁵



Management of Backup Jobs



Recovery of VMs and Application data



Repository quotas

For Service Providers offering IAAS services, VMware has a great solution: VMware Cloud Director (VCD). VCD offer some capabilities that make it a great fit:

- Native multi-tenancy
- abstraction of the infrastructure
- embedded networking services
- single web interface

Veeam has a dedicated portal to allow self-service operations for tenants of VCD, that natively supports Cloud Director to guarantee:

1. Complete self-service capabilities for both backup and restore operations of tenants
2. Control of storage consumption and backup frequency by the Service Provider
3. All the operations have to happen inside the same interface *
4. Single sign-on to access both the main interface and the Data Protection solution *

Our focus in this discussion centers on scenarios requiring both requirements #1 and #2. In cases where #3 and #4 are also necessary, providers can leverage the Veeam Cloud Director Self-Service plugin. Further details on this additional topic will be explored in the following chapter; however, it's important to note that both options for Veeam Cloud Director share the same underlying technology. The core capability of the integration with VCD is the support for native authentication and authorization:

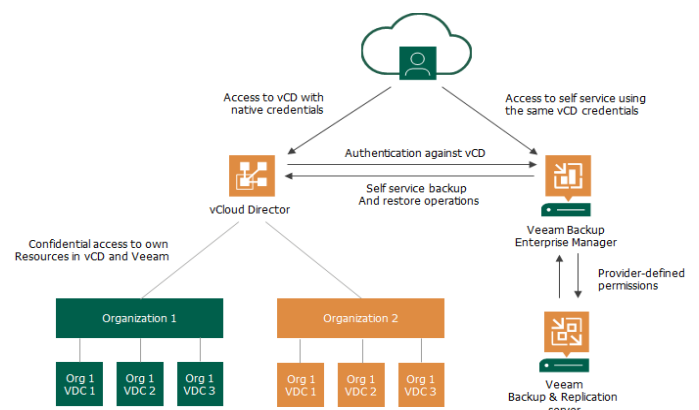


Figure 4. Cloud Director porta authentication



- Users are transparently identified by VCD, Veeam uses a pass-through authentication.
- Multi-tenancy is read from Veeam and applied to all the operations: there is no need to configure any permission, as Organizations and their users are natively recognized.

Also, Veeam supports all the native objects of VCD: vApps and their metadata are recognized and protected, and this information is available during the restore operations.

The backend management of the Veeam Self-Service Backup Portal for Cloud Director similar to the version designed for vSphere. Administrators, initially, can determine the VCD Organizations for which the service should be made available. Subsequently, mirroring the process explained in the vSphere version of this portal, administrators can tailor the settings for each tenant. This includes decisions on the target repository, the allocated storage quota, and the available scheduling options.

The screenshot shows the 'Organization configuration for Cloud Director Portal' interface. It features a navigation menu on the left with options like 'Exit Configuration', 'Backup Servers', 'vCenter Servers', 'Self-service', 'Sessions', and 'Roles'. The main content area is titled 'vSphere Cloud Director' and includes a table with columns: Organization, Repository, Friendly name, Priority, Quota, and Used. The table contains three rows of configuration data.

Organization	Repository	Friendly name	Priority	Quota	Used
organization01	Backup Repository 1	Repository 2	Normal	100 GB	0
organization01	Default Backup Repository	Repository 1	Normal	100 GB	31.9 GB
Other vCloud organizations	Backup Repository 1	Repository 2	High	1 TB	Not available

Figure 9. Organization configuration for Cloud Director Portal

Once an Organization has been granted authorization to access the Veeam portal, any user with Organization Admin privileges can log in and utilize the portal for creating backup jobs or restoring VMs and files, all in a fully self-service manner.

The screenshot shows the 'Self-Service Backup Portal for Organization01' interface. It features a navigation menu with 'Dashboard', 'Jobs', 'VMs', 'Files', and 'Items'. The main content area is titled 'VMs' and includes a search bar and a table with columns: VM, vApp, Job Name, Restore Points, Last Success, and Repository. The table contains two rows of VM data. A context menu is open over the first row, showing options: Instant Recovery, Entire VM Restore, Restore vApp, Virtual Disks, and Delete.

VM	vApp	Job Name	Restore Points	Last Success	Repository
vm01	vApp01	vApp01 Backup	3 points	8/1/2022 01:03:11 pm	Repository01
vm2	vApp02	vApp02 Backup	1 point	8/1/2022 01:19:32 pm	Repository01

Figure 10. Restore capabilities for Cloud Director Portal



Veeam Plug-in for VMware Cloud Director⁶

For an even more smooth, seamless, and integrated experience, Veeam offers the Veeam Plug-in for VMware Cloud Director, a component that can be exposed directly into the VMware Cloud Director interface:

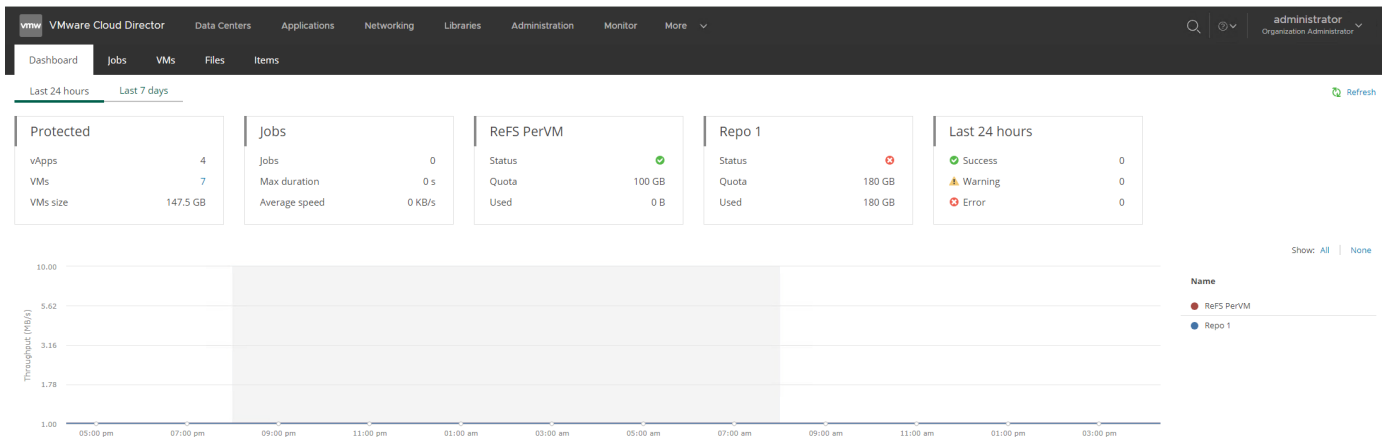
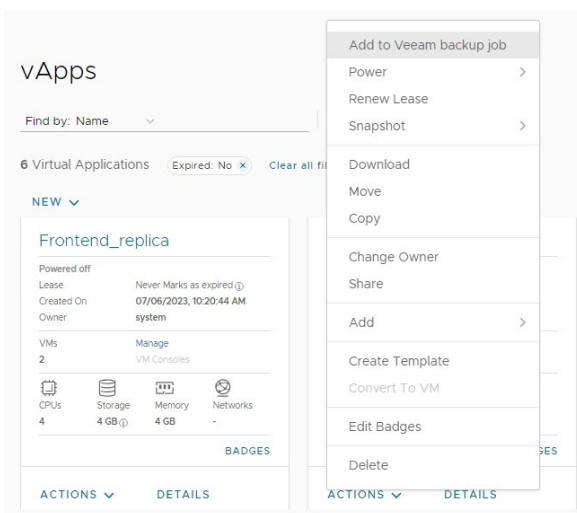


Figure 11. Plug-in for VMware Cloud Director

The set of functionalities remains consistent with the Veeam Self-Service Backup Portal for Cloud Director, given that they share the same platform. However, a notable distinction exists: the plug-in is integrated directly into the VMware Cloud Director interface. This integration offers several significant advantages:

- Passthrough authentication from VCD to Veeam: any login mechanism configured in VCD will be used by Veeam, without any additional login screen
- Tenants don't need to jump from one interface to the other
- Veeam operation directly available in VCD Actions menu





Veeam Cloud Connect Failover Portal⁷



Failover Execution



Self-service



Veeam Cloud Connect

Tenants create their failover plans from their local installation of Veeam Backup & Replication, and they are then stored in Veeam Cloud Connect. In this way, if the tenant installation is lost, the Failover Plan is not lost. But if the whole Veeam installation at the tenant side is lost, how can the tenant execute the failover plan?

That's when the Veeam Cloud Connect Failover Portal comes into play. It can be accessed via a web interface using the Cloud Connect credentials, and its simple interface allows to do only one but very important operation: execute one of the saved Failover Plans.

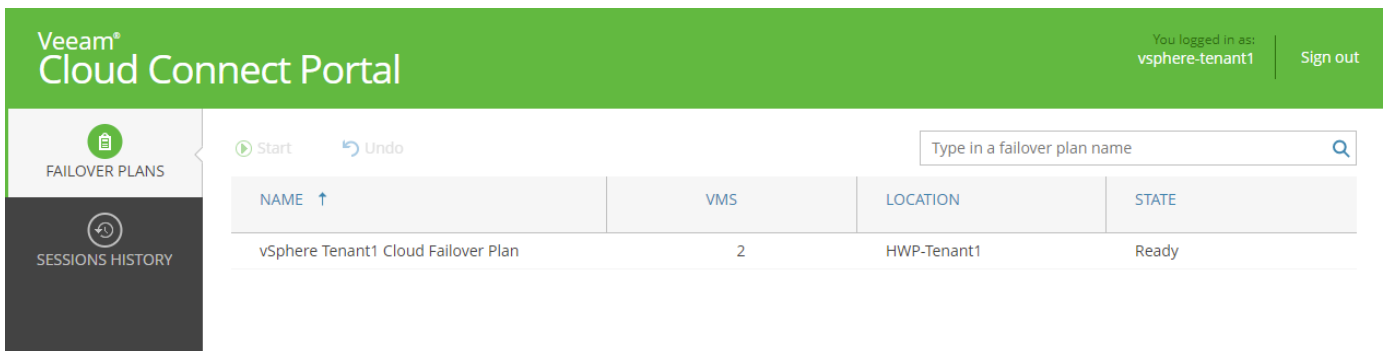


Figure 12. EM Cloud Connect Portal

The interface shows the progress of the plan execution and outputs the result.

This functionality is also available in the Veeam Service Provider Console (VSPC), so some service providers may prefer to avoid using this portal and expose this functionality in VSPC together with all the many others that are available.



Veeam Service Provider Console and its friends.

As previously discussed, Veeam Enterprise Manager effectively addresses management challenges for Veeam Backup and Replication servers. However, the evolution of the Veeam platform has prompted service providers and enterprise clients to adopt a variety of products beyond Veeam Backup and Replication.

This diversification, coupled with the expansion of infrastructure and heightened network security requirements, has presented a significant challenge in terms of central management, configuration, and monitoring for such multifaceted environments. This challenge was the catalyst for the inception of the Veeam Service Provider Console.

Presently, the Veeam Service Provider Console serves as a comprehensive solution, offering a unified view (single pane of glass) for multiple products and use cases. It effectively addresses the complexity of managing diverse products within a growing and dynamic Service Provider or Enterprise infrastructure.

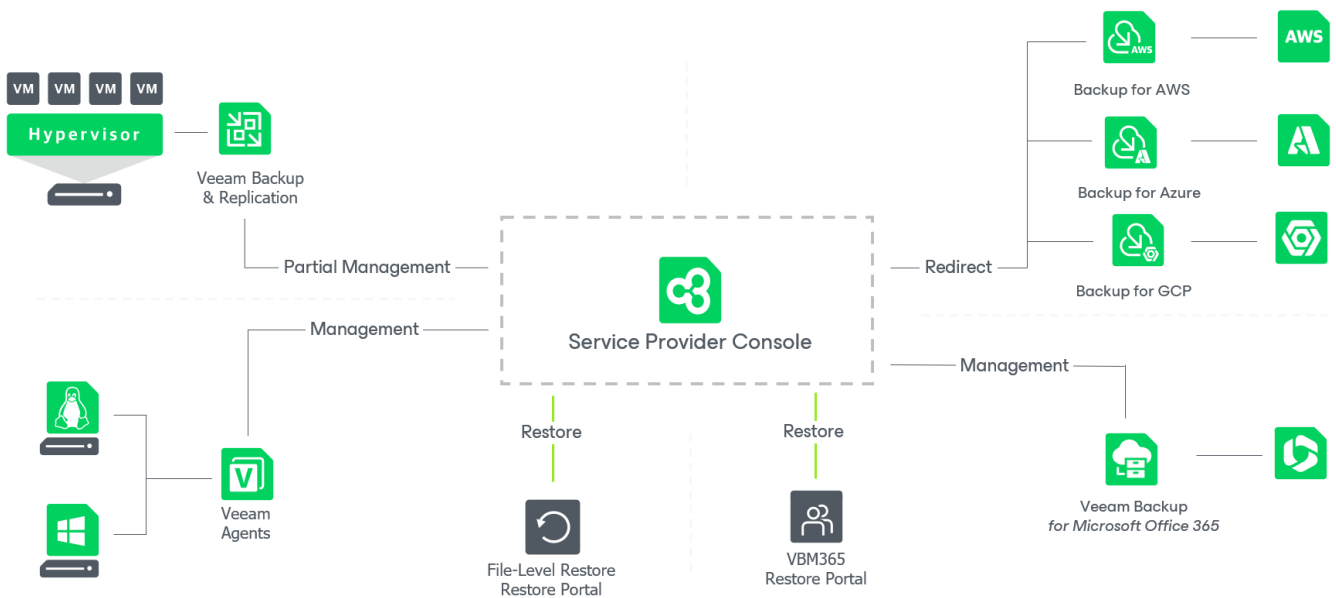


Figure 13. Veeam Service Provider Console use-cases map

Utilizing this system, a global backup administrator/manager gains the ability to efficiently allocate and oversee individual licenses throughout the entire infrastructure, extending to remote offices. The entire communication process operates through a single port connection, significantly streamlining management in a distributed environment.



In addition to providing access through the Web UI, the system acts as a "proxy" for a variety of API calls across all manageable products. However, not all calls are routed through the VSPC (Service Provider Console). Therefore, for specific tasks, it is recommended to utilize the API of each product rather than relying solely on the VSPC API. The decision should be made based on a case-by-case scenario, taking into consideration the specific requirements of each task.

Even when seeking direct access to the individual products managed by the console, the Service Provider Console can always function as a high-level monitoring and alarm management tool. However, for more granular monitoring and analytics, it is advisable to leverage the Veeam ONE solution.

Nevertheless, while the Service Provider Console proves to be a valuable tool for scaled environments, it necessitates Veeam Cloud Connect deployment. It's important to note that enterprise customers seeking to utilize this feature must obtain special approval for the appropriate license.

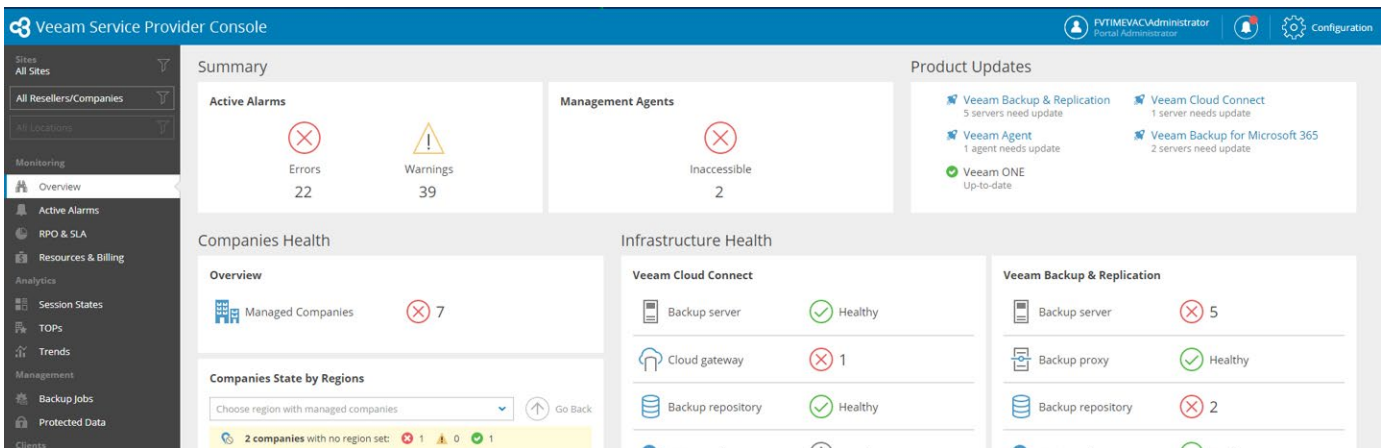


Figure 14. Veeam Service Provider Console Dashboard



Veeam Backup & Replication Servers



Deployment and update



Job management (start, stop, retry)



Restore

As previously mentioned, the Veeam Service Provider Console offers powerful capabilities for centralized monitoring and oversight of various components within an infrastructure, including Veeam Backup and Replication nodes. This extends further with the use of remote dedicated management agents, unlocking additional use-case scenarios for the console.

In contrast to Enterprise Manager, there's no requirement for a wide range of open ports, as the communication link is initiated by the management agent located on the remote Veeam Backup and Replication (VBR) server. In practical terms, this allows the VBR server to be positioned behind a firewall without the need for incoming connections, a common scenario in Enterprise Remote Office/Branch Office (ROBO) setups.

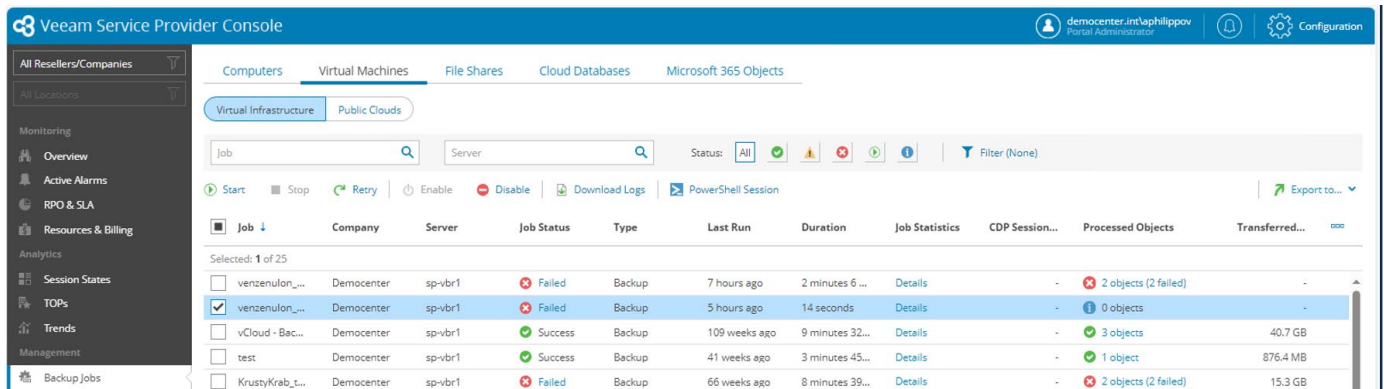


Figure 15. VSPC Backup job management

Given that the VSPC management agent is a standalone product, it serves a dual purpose by facilitating the deployment and updating of the Veeam Backup and Replication instance itself. However, this simplicity comes with some limitations in terms of backup job management. Unfortunately, it's not possible to create or modify configurations for jobs on a remote VBR server, and the management options are restricted to start/stop and retry functionalities. Furthermore, there are no restore capabilities available for VBR within the VSPC management agent. These missing features should be addressed through either the VBR Console itself or Veeam Enterprise Manager. To ease the remote management of complex situations, the underlying Cloud Connect allows administrators to create a "reverse tunnel" connection to start either a Veeam windows client session, or a Windows Remote Desktop session towards the remote Veeam server itself.



The screenshot shows the Veeam Cloud Connect interface. At the top, there is a toolbar with icons for 'Add Tenant', 'Edit Tenant', 'Download', 'Disable Tenant', 'Manage Subtenants', 'Delete', 'Report', 'Remote Console', and 'Remote Desktop'. Below the toolbar is a navigation pane on the left with a tree view containing 'Cloud Connect', 'Cloud Gateways', 'Gateway Pools', 'Tenants', 'Backup Storage', 'Replica Resources', 'Replica org VDCs', 'Last 24 Hours', 'Running (1)', and 'Success'. The main area on the right has a search bar with 'tena' and a table of tenant connections.

Name	Backups ↑	Replicas	Servers	Workstations	Type
tenant1	6	0	0	0	Standalone

Figure 16. Tunnel connections through Veeam Cloud Connect

Finally, another interesting feature is the execution of Powershell commands on the remote VBR server, directly from the VSPC console:

The screenshot shows the Veeam Service Provider Console interface. At the top, there are tabs for 'Discovered Computers', 'Backup Agents', 'Backup Servers', 'ONE Servers', and 'Microsoft 365 Backup Servers'. Below the tabs is a search bar for 'Hostname' and a 'Type' dropdown set to 'All'. Below the search bar are buttons for 'Collect Data', 'Server Actions', 'Delete Agent', and 'PowerShell Session'. Below the buttons is a table of backup servers.

<input checked="" type="checkbox"/>	Company	Application Status	Hostname	Available Updates
Selected: 1 of 1				
<input checked="" type="checkbox"/>	CloudSP-tenant1	Healthy	sp-vbr1	Up-to-date

Figure 17. Tunnel connections through Veeam Service Provider Console



Veeam Agents



Deployment and update



Job Management



File-Level Restore

In SMB/Mid-size infrastructure Veeam Backup and Replication can be used for distribution and configuration of Veeam Backup agents. However, on a scale (100+ agents) same challenge as for virtual infrastructure are valid: role-based access control, task delegation, and secure network communication. Network communication usually plays the core role here, specifically in case of end-user

If basic restore delegation can be achieved by Enterprise Manager Restore2 and File Restore3 portals, the rest is possible only using Veeam Service Provider Console.

A backup administrator, even without a direct connection, can initiate deployment and update for backup agents and automatically assign a preconfigured/customized template of a backup job through the Veeam Service Provider Console portal.

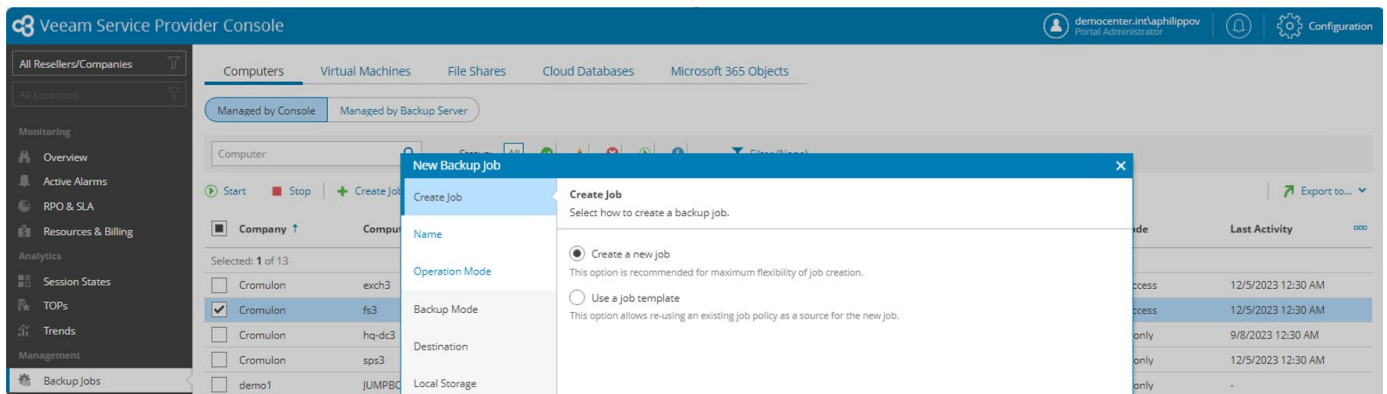


Figure 18. Veeam Service Provider Console — Agent Backup Job

After that file level recovery can be delegated to a Location Administrator (office administrator), limited to one or more company locations. The key point is that Windows/Linux/macOS are supported, and the restore can be done back to the original machine.



Microsoft 365 management



**Multitenant
Architecture**



**Job
Management**



**Restore
portal**

Veeam Backup for Microsoft 365 is a dedicated solution to manage the data protection of Microsoft 365 data. It has a powerful Web Interface that can be used by administrators and end users to fulfill their daily tasks. But what happens when a service provider has tens of hundreds of these deployments, and needs to control them all? Again, Veeam Service Provider Console to the rescue.

VSPC allows service providers and their tenants to manage multiple installations of Veeam Backup for Microsoft 365 jobs and monitor multiple Veeam Backup for Microsoft 365 servers.

Administrators can install the VSPC management agents into all the different VB365 servers, to control them in a single place in the console:

Company	Application Status	Hostname	Available Updates
CloudSP	Running	sp-vbm1	Up-to-date

Figure 19. Microsoft 365 server management

It's possible to check their status, retrieve logs, and be notified of available upgrades. For each server, administrators can also create new jobs and control all backup (and backup copy) jobs

Job	Server	Job Type	Last Run	Job Status	Repository	Next Run
Test schedule	allowe-company	SP-VBM1	-	Stopped	allowe-M365x56945273-rep01	-
allowe-M365x56945273-archive...	allowe-company	SP-VBM1	1 hour ago	Success	allowe-M365x56945273-rep01	12/17/2023 8:00 AM
allowe-M365x56945273-onedri...	allowe-company	SP-VBM1	1 hour ago	Success	allowe-M365x56945273-rep01	12/17/2023 8:00 AM
allowe-M365x56945273-mail-n...	allowe-company	SP-VBM1	10 hours ago	Success	allowe-M365x56945273-rep01	12/16/2023 11:00 PM
allowe-M365x56945273-mail-n...	allowe-company	SP-VBM1	10 hours ago	Success	allowe-m365x56945273-immut...	-
BTE demo all	btedemo	SP-VBM1	17 weeks ago	Warning	tellierbaptiste-M365B620749	-
pvereecken-M365x38893979-c...	CloudSP	SP-VBM1	7 hours ago	Failed	pvereecken-M365x38893979-c...	12/17/2023 1:00 AM

Figure 20. Microsoft 365 job management



Tenants can control their VB365 services directly from the VSPC interface, without the need to open the dedicated interface of the appliance. This allows them to spend less time jumping from one interface to the other, while all the Veeam-powered services are available in one single console.

Operations like job creation, job management, job monitoring, and protection status of the different items, can all be completed from the VSPC interface:

Restore Portal... | Export to...

<input type="checkbox"/>	Name	Type	Latest Restor...	Backup Copies	Restore Points	Licensed	ooo
Selected: 1 of 49							
<input type="checkbox"/>	Adele Vance	User	1 hour ago	4	23	Yes	
<input type="checkbox"/>	Alex Wilber	User	1 hour ago	4	23	Yes	
<input type="checkbox"/>	All Company	Group	10 hours ago	4	7	-	
<input type="checkbox"/>	Allan Deyoung	User	1 hour ago	4	23	Yes	
<input type="checkbox"/>	Ask HR	Group	10 hours ago	4	7	-	
<input type="checkbox"/>	CEO Connection	Group	10 hours ago	4	7	-	
<input checked="" type="checkbox"/>	Christie Cline	User	1 hour ago	4	23	Yes	
<input type="checkbox"/>	Communicatio...	Group	10 hours ago	4	7	-	
<input type="checkbox"/>	Conf Room Ad...	User	10 hours ago	4	7	No	
<input type="checkbox"/>	Conf Room Ba...	User	10 hours ago	4	7	No	

Figure 21. Microsoft 365 backup management

One additional and powerful option is, finally, the direct access to the Restore Portal. By selecting the resource we want to restore, we can easily hit the top-left button and reach immediately the VB365 restore portal:

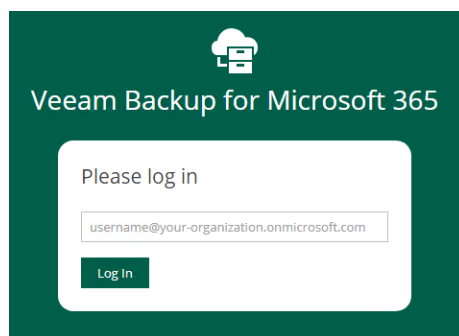


Figure 22. Microsoft 365 restore portal



Cloud management



Failover plan management



Monitoring



Enterprise Manager Cloud Connect

As discussed previously, Veeam Service Provider Console (VSPC) is designed for the comprehensive management of multiple resources, often dispersed across various locations, all through a unified interface. These external resources encompass Veeam Backup and Replication (VBR) servers, agents, VB365 servers, as well as the diverse Cloud Appliances offered within the Veeam portfolio. This includes support for all three major and endorsed Hyperscale's.

Administrators can control the status of all the managed appliances:

Hostname	Address	Version	Company	Platform	Appliance Status	Remote UI Access	Appliance Deployment	Description
ay-azure-ayvbr...	https://ay-azur...	5.1.0.75	My Company	Microsoft Azure	Healthy	Not applic...	Not applicable	Created by AYV...
ay-google-ayvb...	https://34.159...	4.0.0.1082	My Company	Google Cloud	Healthy	Not applic...	Not applicable	Created by AYV...

Figure 23. Cloud Appliances management

And if an operation requires direct access to the Cloud appliance interface, they can easily do it using the dedicated button.

Both administrators and tenants can create, edit, remove, enable, and disable backup policies, that are then executed by the remote appliance. Once they are created, they can monitor their status.

The different protected workloads are then visible in the respective area of the "Protected Data" for virtual machines, file shares, and cloud databases. From this point, restore operations are also possible:



Virtual Machines Data Backup Cloud Databases Microsoft 365 Objects

Virtual Infrastructure **Public Clouds**

VM

Restore

- Instance Restore
- Volume Restore
- File-Level Recovery

	Backup Appliance	Platform	File-Level Re...	Company	Source Size	
<input type="checkbox"/>	linuxfreetier	maxvcspne1	Amazon Web Services	-	vcspaws	8.0 GB
<input type="checkbox"/>	linuxfreetier	maxvcspne1	Amazon Web Services	-	vcspaws	8.0 GB
<input type="checkbox"/>	win-freetier	maxvcspne1	Amazon Web Services	-	vcspaws	30.0 GB
<input checked="" type="checkbox"/>	win-freetier	maxvcspne1	Amazon Web Services	-	vcspaws	30.0 GB
<input type="checkbox"/>	win-freetier	maxvcspne1	Amazon Web Services	-	vcspaws	30.0 GB

Figure 24. Cloud Appliances restore.



Cloud Connect Failover



Failover plan management



Monitoring



Enterprise Manager Cloud Connect

We previously talked about the Veeam Cloud Connect Failover Portal. As said in that part of this document, the same functionality is available inside the Veeam Service Provider Console:

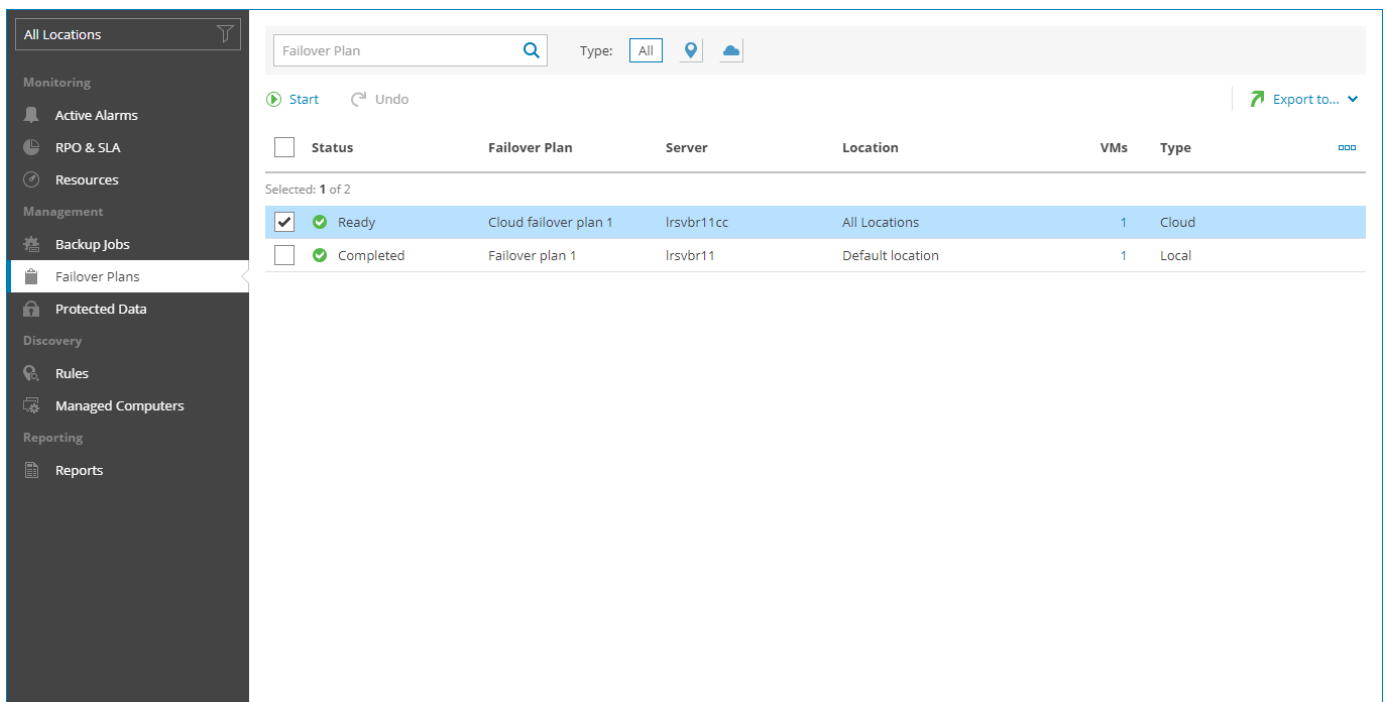


Figure 25. Failover Plans management.

This allows tenants to execute their Failover Plans from the same interface they use to manage and consume all the other Veeam services. For Administrators, this means they can offer this service without the need to expose another additional interface (the previously described Veeam Cloud Connect Failover Portal).



Final considerations

In this document we walked you through the many portals that are available in the Veeam portfolio. We explained the scenario for which they are designed, their usage, advantages.

As you noticed, over time Veeam developed different powerful solutions, each of them aiming at a specific use case. We understand that sometimes a large set of options may confuse people (like a pizza restaurant with too many flavors?), but having many choices help to select the perfect tool for the given scenario.

We believe that with this paper we have guided you through the choice of the correct portal during your Veeam design, to help you to maximize the use of our technology.