HPE GreenLake

Technical brief

Protect HPE VM Essentials using Veeam Agents

Executive summary

As many businesses reevaluate their virtualization strategy in response to software packaging updates, new technologies, and demands of AI workloads, reducing cost without adding more complexity to their existing environments is key. Using proven data protection technology helps keep things simple and avoids increasing the burden on system administrators. Veeam agent-based backup is a mature and well understood method of protecting data and workloads and can now be used to protect virtual environments in HPE VM Essentials.

By providing a single interface for kernel-based virtual machine (KVM) and VMware® environments, HPE VM Essentials Software, a new hypervisor offering from Hewlett Packard Enterprise, enables management of both HPE VM Essentials and VMware vSphere® and provisioning of workloads on-demand without any vendor lock-in. This way, customers can manage existing virtualized workloads, replatform to the HPE VM Essentials hypervisor, and experience a simple virtual machine (VM)-vending experience across both stacks thus reducing cost and complexity.

Due to the shared nature of underlying hardware, VMs can be the target for attackers to access critical data or propagate malware across a network. Protecting VMs becomes crucial since data compromised on one VM can possibly affect all VMs on the same host or network.

Veeam Backup & Replication software has a track record of offering secure backup, clean recovery, and data resilience for any workload and storage configuration. Its tight integration with the HPE storage and server portfolio offers customers a robust data protection solution. This data protection capability is now available on HPE VM Essentials with an agent-based backup approach.

This technical brief provides an overview of how HPE VM Essentials is protected by Veeam Backup & Replication software where the underlying storage infrastructure is HPE Alletra Storage MP B10000, HPE Alletra Storage MP dHCI, or HPE SimpliVity.

HPE VM Essentials Software

HPE VM Essentials is a new virtualization software solution that allows customers to provision and manage KVM and VMware-based VMs from a single intuitive interface. HPE VM Essentials includes the HPE VM Essentials KVM-based hypervisor but also supports your existing VMware licenses, providing ease of use, agility, and a unified VM-vending experience for HPE VM Essentials and VMware clusters. The KVM stack is ideal for those exploring alternatives to VMware, starting with non-mission-critical workloads such as test and development. With the solution's ability to support VMware vSphere, it provides a unified VM provisioning and management experience for HPE VM Essentials hypervisor and VMware vSphere VMs. This provides ease of use, agility, and a unified VM-vending experience for HPE VM Essentials and VMware clusters. Integration with IP Address Management (IPAM), DNS, and automation tools enables tedious provisioning steps to be automated to simplify the provisioning of VMs in HPE VM Essentials and VMware.

For an overview of HPE VM Essentials read the Solution Brief at paths.ext.hpe.com/r/a00144027-1 or watch a video introduction to HPE VM Essentials Software at youtube.com/watch?v=Ah1IC4tiwxI.

Figure 1 shows the dashboard of the HPE VM Essentials manager web-based interface.

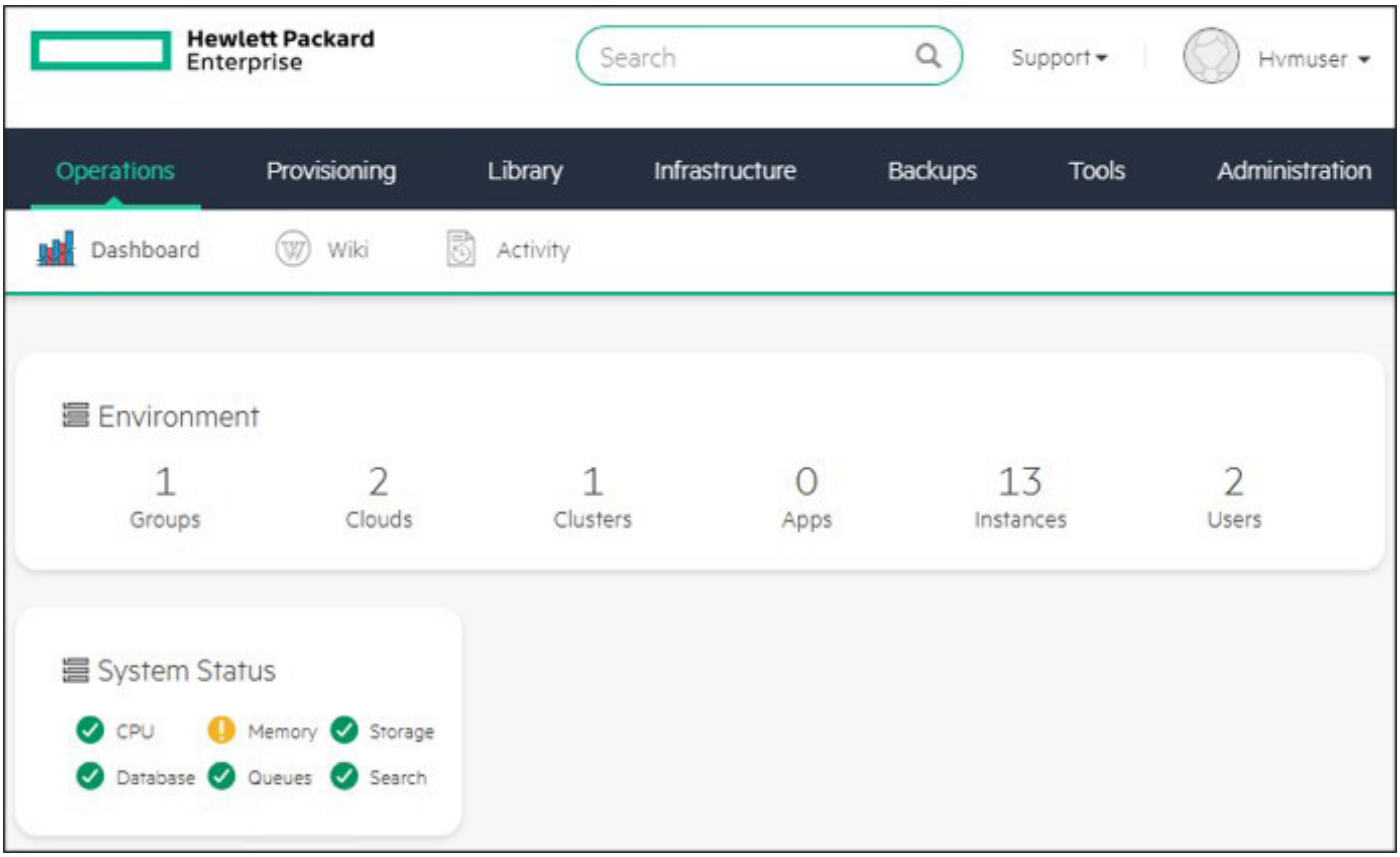

Figure 1. HPE VM Essentials web-based interface

In HPE VM Essentials, VMs are provisioned by creating a resource or service, which may include several VMs. New VMs are provisioned by launching the **Create Instance** wizard from the **Provisioning → Instances** page of the HPE VM Essentials user interface.

Veeam Backup & Replication

Veeam Backup & Replication provides secure backup, clean recovery, and data resilience for any workload and any storage configuration. HPE and Veeam engineers have conducted functional testing using a physical Windows Server running Veeam Backup & Replication. This server was configured with all necessary Veeam roles, including the backup server, proxy, and repository. In addition to this server, an HPE VM Essentials cluster was set up, containing the source VMs to be backed up. The goal of testing was functional validation; scaling and performance were outside the scope of this test.

The VMs in the HPE VM Essentials cluster were protected using Veeam Protection Groups. These groups are configured to protect workloads using Veeam Agents. During the setup of the protection group in the Veeam user interface, the backup schedule is configured. Once the protection group has been created, servers can be manually added to it as shown in Figure 2. When the protection group settings are saved, the Veeam Agent is automatically installed on the designated servers.

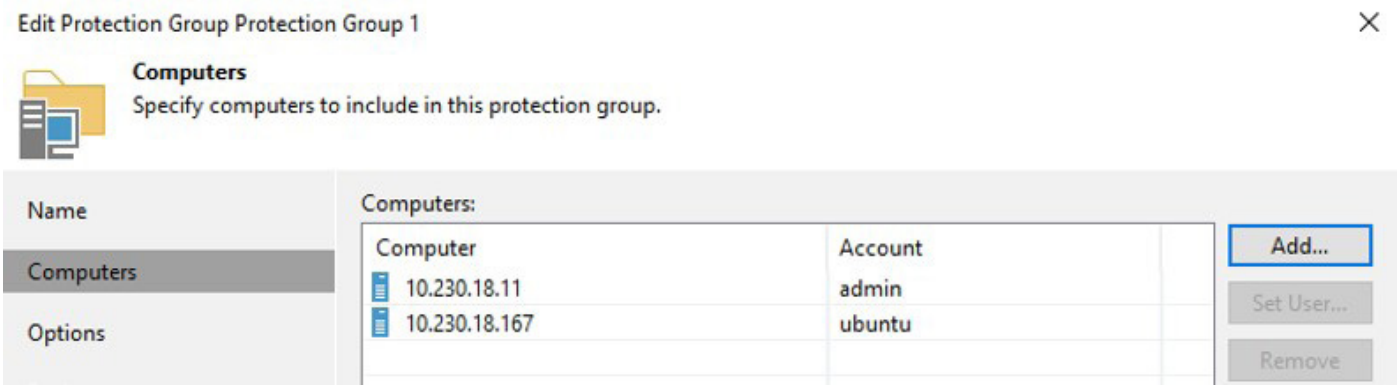

Figure 2. Adding servers to a Veeam Protection Group

After adding servers to the protection group, they must be included in a backup job. When the backup job is run, the Veeam agent-based backup runs on VMs hosted in HPE VM Essentials cluster just as it would on a physical server.

Automating the backup tasks

The **Create Instance** wizard of HPE VM Essentials includes an **Automation** page. By completing this optional configuration step, users can create a task that automates adding new VMs to the appropriate Veeam Protection Group. This helps ensure the new VMs are included in existing backup schedules. To implement this functionality, the user would create a bash or PowerShell script that interacts with Veeam to add the VM being provisioned into the desired protection group. That script would be created as part of a new automation task under **Library** → **Automation** → **Tasks** in the HPE VM Essentials UI. The task name would then be selected from the drop-down list in the **TASK** field under the **Automation** section on this page.

The **Automation** page also includes a section labeled **Backups** as shown in Figure 3.

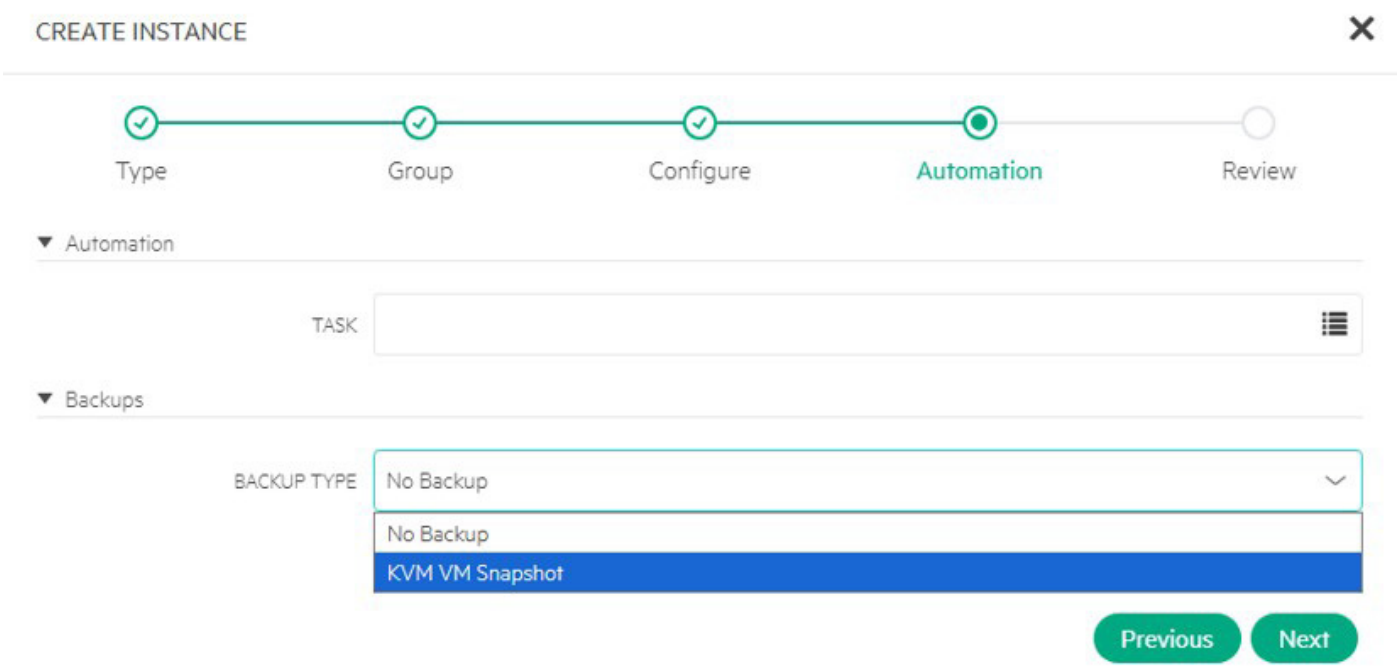

Figure 3. The Automation page of the Create Instance wizard in HPE VM Essentials

It is important to note that in HPE VM Essentials, the term backup equates to VM Snapshots, as highlighted in blue in Figure 3. This KVM VM Snapshot uses the native functionality of HPE VM Essentials and is not integrated with Veeam. These snapshots are not proper backups by themselves, but can be used to facilitate a backup. While snapshots are a good first step in creating a restore point for the VMs, they do not adequately protect a production environment. For VMs to be fully protected, it is necessary to have a solid backup strategy, which includes a robust backup solution such as Veeam Backup & Replication. Veeam strongly recommends adhering to the 3-2-1-1-0 backup rule for a robust data protection solution that can help protect against all threats:

3—Have at least three copies of all data. This should include the primary (production) data and at least two backups

2—Data should be kept on at least two different types of storage media

1—At least one copy should be kept off-site

1—One copy should be offline, air-gapped, or immutable

0—Veeam SureBackup should be used to verify that backups can be recovered with zero errors

Conclusion

The functional test of Veeam's backup strategies within an HPE VM Essentials environment was completed successfully. Protection groups in Veeam Backup & Replication can be used effectively to protect VMs in HPE VM Essentials by making use of Veeam Agents.

Learn more at

HPE.com/us/en/HPE-VM-Essentials.html

HPE.com/us/en/alliance/Veeam.html

Visit **HPE.com**

Chat now (sales)

© Copyright 2025 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

PowerShell and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. VMware vSphere and VMware are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All third-party marks are property of their respective owners.

a50012338ENW, Rev. 3

Hewlett Packard Enterprise