



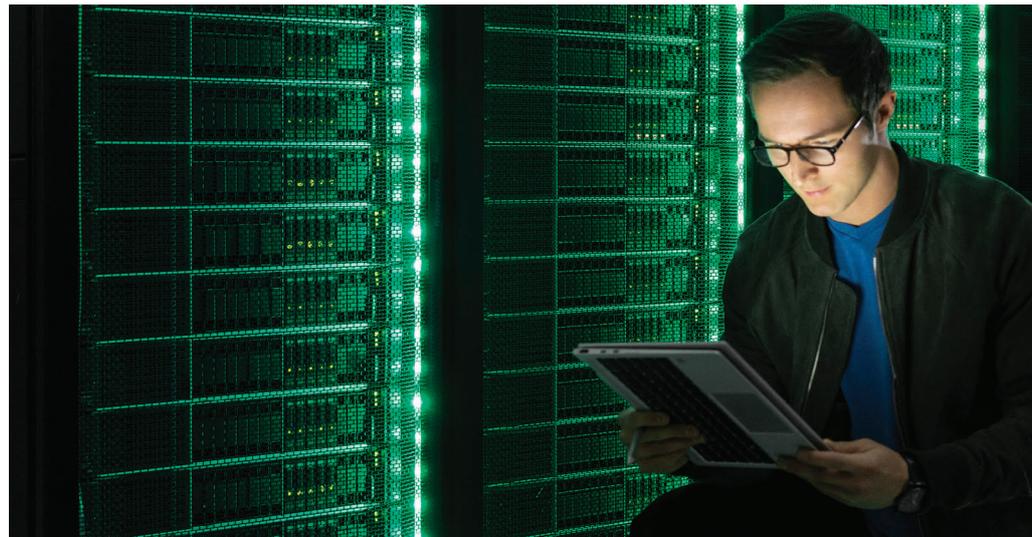
DATA PROTECTION FOR MICROSOFT AZURE STACK HUB

Commvault Complete Backup and Recovery for HPE ProLiant for Microsoft Azure Stack Hub

Why Commvault Complete for HPE ProLiant for Microsoft Azure Stack Hub?

- Fully protects all data including VMs and BLOBs, and applications across Microsoft Azure Stack Hub, Azure, and all other environments in a single solution
- Simplifies migration of a full VM from an outside hypervisor or cloud providers to Azure Stack Hub
- Enables DR for an Azure Stack Hub VM between Azure Stack Hub scale units

Protecting infrastructure and tenant data resources on Microsoft Azure Stack Hub and beyond



MICROSOFT AZURE IN THE DATA CENTER

HPE ProLiant for Microsoft Azure Stack Hub enables an on-premises deployment of Microsoft Azure Stack Hub that mirrors the functionality of Microsoft Azure cloud. Co-engineered by Hewlett Packard Enterprise and Microsoft, it incorporates compute, storage, and networking in an Azure on-premises instance. The advantage of this approach is to deliver the speed, agility, and simplicity of a public cloud but with the characteristics of an on-premises cloud.

DATA PROTECTION CHALLENGES ON MICROSOFT AZURE STACK HUB

The success of HPE ProLiant for Microsoft Azure Stack Hub has led users to embrace the solution for their most ambitious and business-critical workloads. At the same time, human beings—and the world at large—can throw some pretty serious challenges at even the most stable infrastructure. Data protection has thus become an essential requirement for users of Microsoft Azure Stack Hub. Commvault addresses this need by offering protection against human errors, programmatic errors, and malicious insiders. It mitigates data risks threatened by hackers and malware, as well as natural disasters and power outages.

Solution brief

Natively, Microsoft Azure Stack Hub protects the core platform software and infrastructure resources. This is the data that keeps Azure Stack Hub itself functioning. It includes services and microservices such as Azure Resource Manager (ARM), the Key Vault store of cryptographic keys and other secrets, Compute Resource Provider (CRP), Network Resource Provider (NRP), Storage Resource Provider (SRP), and so forth. The Azure Stack Hub admin portal provides built-in capabilities that protect this data restore in the event of an outage.

The tenant, however, is responsible for all other data protection, an approach which aligns with the standard two-tier security model of the cloud. Tenant resources data is everything that runs on Azure Stack Hub. It might be infrastructure-as-a-service (IaaS) data, platform-as-a-service (PaaS) configurations, virtual machines (VMs), databases, user data, binary large objects (BLOBs), etc. Essentially, Azure Stack Hub is a self-protecting infrastructure. Data protection requires separate services, and the better integrated those services are with the core platform, the easier and more complete the protection process is.

THE COMMVAULT COMPLETE SOLUTION FOR HPE PROLIANT FOR MICROSOFT AZURE STACK HUB

Commvault Complete for HPE ProLiant for Microsoft Azure Stack Hub provides comprehensive data protection. It is the same solution used internally by Microsoft for Office products, Xbox/Xbox Live, and Microsoft Azure Business Units. Through the

use of agents and Commvault HyperScale technology, Commvault Complete protects VMs. It enables backup and recovery of BLOB storage. Agents are available for all major operating systems, applications, and databases. Backups from Azure Stack Hub can be stored on any target supported by Commvault, including disk, tape, or dozens of cloud providers.

Backup and disaster recovery

Commvault Complete offers sophisticated backup and disaster recovery (DR) capabilities for HPE ProLiant for Microsoft Azure Stack Hub. The Commvault approach is comprehensive. It covers DR for VMs on one Azure Stack Hub scale unit to another Azure Stack Hub scale unit using Live Sync. The solution can also provide DR between multiple Azure Stack Hub subscriptions. It enables recovery of BLOB storage data as well as guest files and granular restore at the file and folder level.

The Commvault solution makes it possible to replicate data and VMs across Azure Stack Hub instances in multiple geographies. For example, if you are running Azure Stack Hub in California, you could replicate it to a backup instance in New Mexico. The solution is able to support your recovery point objectives (RPOs) and recovery time objectives (RTOs). With these capabilities, it has the potential to align well with business continuity plans.

Full VM and data migration

Data management processes sometimes require the migration of VMs from one Azure Stack Hub instance to another. To do this in a way that keeps uptime and availability to a maximum, Commvault Complete enables you to migrate VMs in their entirety, with all of their underlying configuration information. With such a capability provided by Commvault's agentless Virtual Server Agent (VSA), you can migrate VMware® and Azure VMs to Azure Stack Hub VMs. This solution can also enable migration of databases such as Microsoft SQL Server that are running on HPE ProLiant for Microsoft Azure Stack Hub.

Integrating Commvault Complete for Azure Stack Hub across the enterprise

HPE ProLiant for Microsoft Azure Stack Hub invariably runs in parallel with a wide

assortment of other enterprise technologies. To keep IT operations operating efficiently, Commvault Complete supports multiple types of software and infrastructure in addition to those running on Azure Stack Hub. It supports Azure Active Directory (AAD) and Active Directory Federation Service (ADFS) Azure Stack Hub configurations in a connected or non-connected environment. Commvault Complete can protect data across all bare metal instances, hypervisors, and so forth through a single point of control.

Why you need Commvault Complete for HPE ProLiant for Microsoft Azure Stack Hub?

Deploying Commvault Complete for HPE ProLiant for Microsoft Azure Stack Hub delivers a number of benefits to the enterprise. These include:

- Providing protection of data and software on HPE ProLiant for Microsoft Azure Stack Hub beyond its built-in capabilities.
- Extending data protection across the entire enterprise, including Azure Stack Hub.
- Making data protection more administratively efficient, with full VM migration and a single solution protecting data on Azure Stack Hub and Azure cloud subscriptions, as well on a wide range of other on-premises infrastructure elements.
- Providing full native integration with HPE StoreOnce Catalyst including Cloud Bank Storage, therefore extending the protection capabilities across the data center and supporting your hybrid cloud program goals and initiatives.
- Offering hyperscale reference design. Commvault and HPE have collaborated to offer a highly scalable hyperconverged data-protection solution built on HPE Apollo and HPE ProLiant server platforms. This solution is supported by a reference design program built on tested, validated, and documented architectures.

LEARN MORE AT

hpe.com/cloud/azure-stack-hub

Make the right purchase decision.
Contact our presales specialists.



Chat



Email



Call



Get updates

**Hewlett Packard
Enterprise**

© Copyright 2019–2020 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.

Active Directory, Azure, Microsoft, SQL Server, Xbox, and Xbox Live are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All third-party marks are property of their respective owners.

a00072601ENW, October 2020, Rev. 1