HPE Reference Architecture for HPE ProLiant for Microsoft Azure Stack data protection with Veritas NetBackup, HPE StoreOnce and Cloud Bank Storage
## Contents

- Executive summary .................................................................................................................................. 3
- Solution overview .................................................................................................................................. 4
- Solution components .............................................................................................................................. 5
  - HPE ProLiant for Microsoft Azure Stack .............................................................................................. 5
  - Hardware ........................................................................................................................................... 7
  - Software ........................................................................................................................................... 7
- Solution deployment considerations ....................................................................................................... 8
  - Azure Stack infrastructure protection ................................................................................................. 11
- Veritas NetBackup .................................................................................................................................. 12
  - Backup Use case 1 ................................................................................................................................. 13
  - Backup Use case 2 ................................................................................................................................ 14
- HPE StoreOnce ....................................................................................................................................... 15
  - HPE StoreOnce Catalyst ........................................................................................................................ 15
  - HPE StoreOnce Catalyst Plug-in for Veritas NetBackup ........................................................................ 16
  - Content Aware Backups for deduplication ............................................................................................ 16
  - Recovery Use case ................................................................................................................................. 19
- HPE Cloud Bank Storage for Hybrid IT data protection ........................................................................ 20
  - HPE Cloud Bank Storage configuration ............................................................................................... 21
  - HPE Cloud Bank Storage and Veritas NetBackup integration .............................................................. 23
    - Catalyst copy to Cloud Bank store ....................................................................................................... 24
    - Database restore directly from HPE Cloud Bank Storage .................................................................... 26
    - Database restore from Reverse catalyst copy .................................................................................... 26
    - Disaster recovery using HPE Cloud Bank Storage ............................................................................ 28
    - Archiving and long-term retention ...................................................................................................... 32
    - HPE Cloud Bank Storage encryption for security .............................................................................. 33
- Summary .................................................................................................................................................. 33
- Appendix A: Bill of materials ................................................................................................................ 34
- Resources and additional links .............................................................................................................. 36
**Executive summary**

Enterprises are under pressure to deliver public cloud-like experiences and services to their internal customers and business groups. There is a huge demand for hybrid cloud environments, as application developers and administrators in an organization look for a seamless cloud-like experience across their on-premises infrastructure and off-premises cloud. Many enterprises are trying to fill this gap and are making the leap to hybrid cloud as they try to balance between their differing needs of infrastructure and business. In addition to this huge change, enterprises also have to deal with other changes that range from cultural resistance to regulatory considerations.

Hewlett Packard Enterprise is helping customers to make this transformation with its hybrid cloud offering of HPE ProLiant for Microsoft® Azure Stack, which enables customers to deploy the right mix of private, public, and traditional IT on an open platform. HPE ProLiant for Microsoft Azure Stack is a pre-tested, factory-integrated Azure hybrid cloud solution, providing a consistent development, management, and security experience. Co-engineered by Hewlett Packard Enterprise and Microsoft, it delivers Azure-consistent software-defined Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) on HPE hardware in your data center. It runs Azure compatible workloads on-premises to meet security, compliance, cost, and performance requirements. The speed, agility, and simplicity provided by the Microsoft Azure public cloud when combined with the cost-effective and secure on-premises HPE ProLiant for Microsoft Azure Stack help provide the best of both worlds.

This hybrid cloud transformation requires organizations to protect the data on the on-premises Azure Stack cloud. Data is the core asset of all businesses. This data could be lost due to unexpected situations arising from hardware failure, human error, or natural disaster. Also businesses require all important data to be available throughout the day with zero or no downtime. Hence it is necessary for organizations to have a plan in place to protect data that resides on the on-premises cloud. HPE StoreOnce provides a backup appliance target that delivers fast backups and restores with efficient deduplication and enables copying backup stores to an object storage in the cloud with HPE Cloud Bank Storage. HPE StoreOnce integrates with key backup and recovery software such as Veritas NetBackup to provide higher levels of efficiency in data protection tasks.

HPE Cloud Bank Storage is a feature of HPE StoreOnce Systems, industry-leading data protection storage, that delivers highly efficient data transfer to your on-premises and off-premises cloud. The combination of HPE StoreOnce deduplication and cloud storage delivers low-cost, high-performance, and zero-risk long-term retention and archiving solutions. HPE StoreOnce System with Cloud Bank Storage gives you the benefits of object storage without changing your existing backup application environment. It also adds the protection of offsite backup data copies without having to invest in offsite facilities. Above all it enables cloud-based disaster recovery but without the high costs associated with the transfer of large amounts of data to the cloud.

Veritas is a leader in the backup and recovery market, with Veritas NetBackup being a leading product in this space. Veritas NetBackup 8 supports multiple cloud platforms. In this solution we demonstrate how customers who are standardized on or considering Veritas NetBackup as the backup software can benefit from using HPE StoreOnce with Cloud Bank Storage features and integration. With a cohesive solution from HPE and Veritas, customers can eliminate the complexity of point solutions and infrastructure management, physical and virtual, with a single, unified solution; modernize infrastructure with a converged backup platform; and improve productivity through centralized, policy-based management. The solution also allows for self-service capabilities that give IT staff better visibility and control of backup and recovery, and enables enterprises to transform faster to keep pace with business needs.

**Target audience:** This paper is intended for IT decision makers and administrators looking for an efficient backup and recovery solution for use with the HPE ProLiant for Microsoft Azure Stack hybrid offering. This paper discusses best practices and use cases for protection of data on HPE ProLiant for Microsoft Azure Stack using Veritas NetBackup and HPE StoreOnce with HPE Cloud Bank Storage.

A working knowledge of server architecture, networking architecture, storage design, and backup/recovery software is recommended.

**Document purpose:** The purpose of this document is to describe a Reference Architecture (RA) for data protection of the Microsoft workload deployed on HPE ProLiant for Microsoft Azure Stack.
Solution overview

HPE ProLiant for Microsoft Azure Stack is a hybrid cloud solution that allows organizations to run consistent Azure services in their data center and provides a simplified development, management, and security experience which is consistent with Microsoft Azure public cloud services. As organizations make the transformation to hybrid cloud, it is important to consider cloud-based data protection solutions rather than traditional hardware-dependent data protection solutions. This enables organizations to store vital data on-premises while moving less accessed data to cloud.

The production data on Microsoft Azure Stack needs to be protected for short term (to recover accidental data deletion or corruption) as well as long term (to handle site-level disaster situations) and archival (to address regulatory compliance and future reference) purposes.

Azure Stack infrastructure backup can only protect the configuration data of Microsoft Azure Stack. Hence for protecting production data, an enterprise backup application such as Veritas NetBackup should be used. Veritas NetBackup can perform backup of data that run on Microsoft Azure Stack onto an on-premises HPE StoreOnce appliance and eventually into the Azure Cloud using HPE Cloud Bank Storage.

This solution is comprised of HPE ProLiant for Microsoft Azure Stack deployed on four HPE ProLiant DL380 Gen9 servers. After successful deployment of Microsoft Azure Stack, it is registered with Azure public cloud. Microsoft Windows Server® 2016 virtual machines running Microsoft SQL Server 2016 and a Windows File Server were deployed on Azure Stack. One additional Windows® virtual machine was created outside Azure Stack for the Veritas NetBackup master server, as shown in figure 1.

HPE StoreOnce 3520 System was used as the backup target and HPE Cloud Bank Storage was configured using Azure Blob storage for long term retention, archival, and disaster recovery purposes. HPE StoreOnce Catalyst stores, the device types stored on HPE StoreOnce, were created and configured to use as storage devices in the Veritas NetBackup master server. Storage Lifecycle Policies (SLP) were created to copy the data to the HPE Cloud Bank Storage automatically in a deduplicated and compressed manner. Figure 1 shows the architecture diagram for the solution.

![Figure 1. Azure Stack data backup to HPE StoreOnce and to Azure Cloud via HPE Cloud Bank Storage](image)

1 The NetBackup server that provides administration and control for backups and restores for all clients
Solution components

HPE ProLiant for Microsoft Azure Stack
HPE ProLiant for Microsoft Azure Stack is an integrated solution which quickly transforms on-premises data center resources into flexible hybrid cloud services that provide a simplified development, management, and security experience that is consistent with Microsoft Azure public cloud services. Some of the most notable features of HPE ProLiant for Microsoft Azure Stack are:

- Delivers Microsoft Azure services consistently across your data center
- Provides a consistent development environment that simplifies the developer experience
- Provides a highly configurable solution that meets your workload requirements
- Offers fast time-to-value and implementation with factory integration
- Offers HPE value added services to deliver a proven Azure hybrid cloud

For further information on the HPE ProLiant for Microsoft Azure Stack solution, visit hpe.com/us/en/solutions/cloud/azure-hybrid-cloud.html

Figure 2 shows an HPE ProLiant for Microsoft Azure Stack deployed on four HPE ProLiant DL380 Gen9 servers residing above the optional KVM switch. The HPE ProLiant for Microsoft Azure Stack solution consists of a scale unit that can be configured with a minimum of 4 nodes to maximum 12 nodes. This scale unit is managed by Azure Stack Resource Manager which is a control plane that manages all the resources in the Azure Stack environment. It controls compute, storage, networking, security, and other infrastructure services on Azure Stack.
The Management node is hosted on an HPE ProLiant DL360 Gen9 server. This Management node serves as a Hardware Lifecycle Host, and hosts HPE OneView, which is a powerful infrastructure automation tool that proactively manages compute, storage, and networking to meet the needs of workloads running on Azure Stack. The Management node also hosts HPE Insight Remote Support software to monitor the health of the HPE ProLiant for Microsoft Azure Stack hardware. Figure 3 shows the HPE OneView overview of HPE ProLiant for Microsoft Azure Stack host servers and figure 4 shows the Azure Stack administration console view of the host servers.

Figure 3. HPE OneView shows the layout of HPE ProLiant for Microsoft Azure Stack hardware

Figure 4. Azure Stack Administration showing the host servers
For detailed information on HPE ProLiant for Microsoft Azure Stack, refer to the QuickSpecs at,  

**Hardware**

Below is the list of hardware components used for this solution.

Hardware configuration for HPE ProLiant for Microsoft Azure Stack:

- 4 x HPE ProLiant DL380 Gen9 with Microsoft Azure Stack Node, each with:
  - 1 x HPE Smart Array P840/4G Controller
  - 2 x HPE DL380 Gen9 Intel Xeon E5-2683v4 Processor Kit
  - 16 x HPE 32GB Dual Rank x4 DDR4-2400 Registered Memory Kit
  - 10 x HPE 6TB SATA 6G Midline 7.2K LFF (3.5in) HDD
  - 4 x HPE 1.92TB SATA 6G Mixed Use LFF (3.5in) SSD
- 2 x HPE FlexFabric 5900AF 48XG 4QSFP+ Switch (ToR switches)
- 1 x HPE FlexFabric 5900AF 48G 4XG 2QSFP+ Switch (Management switch)
- 1 x HPE ProLiant DL360 Gen9 8SFF CTO Server (Hardware lifecycle host)
  - 1 x HPE Smart Array P440ar/2GB Controller
  - 2 x HPE DL360 Gen9 E5-2620v4 Processor Kit
  - 4 x HPE 16GB Single Rank x4 DDR4-2400-Registered Memory Kit
  - 4 x HPE 600GB 12G SAS 10K 2.5in SC ENT HDD
  - 1 x HPE Ethernet 10Gb 2P 546FLR-SFP+ Adapter

Hardware configuration for HPE StoreOnce 3520:

- 1 x HPE StoreOnce 3520 System with 24 TB of RAW disk storage
- 8 x 10Gb Ethernet ports per controller
- 4 x 1Gb Ethernet
- 1x 10 GbE network interface card
- 12 x 2 TB disks

**Software**

Below is the list of software components used for this solution.

- Microsoft Azure Stack software
- Veritas NetBackup 8.1 (for data backup and recovery)
- HPE Cloud Bank Storage with Azure Blob storage (for data replication into public cloud)
- Microsoft Windows Server 2016 Datacenter evaluation version (downloaded from Azure Marketplace)
- Microsoft SQL Server 2016 Developer evaluation edition

Once the HPE ProLiant for Microsoft Azure Stack is registered to Microsoft Azure public cloud, Marketplace on Azure public cloud, hosting many published templates, will be available for download onto the Azure Stack Marketplace. These templates can be deployed directly on Azure Stack.

To learn more about Azure Marketplace, refer to https://azuremarketplace.microsoft.com/en-us/marketplace
Solution deployment considerations

Management of the HPE ProLiant for Microsoft Azure Stack solution is done via two portals, one that is available for user activity and the other for administrator activities. The administrator portal has more features, such as the ability to create quotas, plans and offers for subscribers, as well as providing more secure administration features compared to the user portal.

In this solution, all tenant VMs running on HPE ProLiant for Microsoft Azure Stack were deployed through the administrator portal.

**Note**

It is necessary to register the HPE ProLiant for Microsoft Azure Stack to Microsoft Azure public cloud. This is required to download published templates from Azure public cloud Marketplace.

In this RA, we deployed Veritas NetBackup master server and the HPE StoreOnce backup appliance outside of the Azure Stack solution. Table 1 shows a list of ports opened up on the firewall to facilitate network traffic between the tenant VMs, NetBackup master server, and StoreOnce.

<table>
<thead>
<tr>
<th>Veritas NetBackup Ports</th>
<th>StoreOnce Catalyst operations Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>VERITAS_PBX-1556</td>
<td>Command protocol-9387</td>
</tr>
<tr>
<td>VNETD-13724</td>
<td>Data protocol-9388</td>
</tr>
<tr>
<td>BPCD-13782</td>
<td></td>
</tr>
<tr>
<td>Deduplication spool-id-10082</td>
<td></td>
</tr>
<tr>
<td>Deduplication spad -10102</td>
<td></td>
</tr>
</tbody>
</table>

We created inbound security rules for these ports within an Azure Stack network security group; this is necessary to establish communication between tenant VMs and the NetBackup master server, as shown in figure 5.

![Figure 5. Microsoft Azure Stack Inbound security rules created under the Network security group of the Microsoft SQL VM](image-url)
Note
It is very important that the name resolution works before you install and configure Veritas NetBackup master server and media/client servers.

The high-level configuration steps for the backup environment deployed on HPE ProLiant for Microsoft Azure Stack are as follows:

- Log in to the Azure Stack administrative portal.
- Deploy Microsoft Windows Server 2016 using the downloaded Windows template, for acting as a Windows File Server.
- Deploy Microsoft workload, that is, SQL Server 2016.
- Install and configure Veritas NetBackup master server on a Windows 2016 server outside of Azure Stack. This is to simulate the actual customer scenarios.
- Configure a NetBackup storage unit using HPE StoreOnce Catalyst stores for target storage for the backup.
- Configure a Storage Lifecycle Policy to copy data from the local Catalyst store to the HPE Cloud Bank Storage, which is created using Azure Blob storage in this RA.

Figure 6 shows Windows virtual machines deployed on HPE ProLiant for Microsoft Azure Stack through the administrator portal. Microsoft SQL Server and a Windows File Server were installed and configured on Windows 2016 virtual machines.

For the purpose of testing granular backup and restore of data, a small TPC-C database of size ~10GB was hosted on SQL Server.

Figure 6. Microsoft workloads deployed on HPE ProLiant for Microsoft Azure Stack

2 TPC Benchmark C is an online transaction processing (OLTP) benchmark
Figure 7 shows Microsoft SQL Server Management Studio showing a tpcc database configured and the Disk Usage for the same.
Azure Stack infrastructure protection

Backup

It is necessary to back up the configuration data of Azure Stack so that Azure Stack can be restored in the event of any failure. Each Azure Stack installation contains an instance of the service. You can use backups created by the service for the re-deployment of the Azure Stack Cloud to restore identity, security, and Azure Resource Manager data. The Azure Stack infrastructure backup functionality available within Microsoft Azure Stack is used to perform this backup. An external file share accessible from Azure Stack is required to store the infrastructure backups.

Under the administration section of the Microsoft Azure Stack, select “Infrastructure Backup” and then “Backup controller settings”, specify the external file share location which is created in the HPE StoreOnce NAS share, credentials to access the file share, and encryption key as shown in figure 8. The key needs to be saved in a separate location as it will no longer be visible through the interface once set for the first time.

For more information, refer to: https://docs.microsoft.com/en-my/azure/azure-stack/azure-stack-backup-infrastructure-backup

Figure 8. Microsoft Azure Stack – Backup controller settings
After successful configuration of the infrastructure backup, confirm the backup completed in the administration portal, and verify the State is Succeeded, as shown in figure 9. This infrastructure backup data can be used to redeploy Azure Stack in the event of any failure.

Figure 9. Microsoft Azure Stack infrastructure backup contents

**Restore**

In the case of disaster or complete data loss or corruption, re-deployment of Azure Stack may be required. Azure Stack infrastructure backup functionality will be used for restoring the configuration data. During re-deployment, you can specify the storage location and credentials required to access backups. In this restore, there is no need to specify any services that need to be restored. Infrastructure Backup Controller injects the control plane state as part of the deployment workflow.

For more information, refer to: https://docs.microsoft.com/en-my/azure/azure-stack/azure-stack-backup-recover-data

**Note**

It is not possible to initiate an Azure Stack infrastructure backup using Veritas NetBackup at the present time.

**Veritas NetBackup**

Veritas NetBackup delivers unified data protection for mid-market to enterprise customers and is designed to protect the largest and most complex heterogeneous environments—cloud, virtual, and physical applications across the enterprise—anywhere the data resides. To learn more about NetBackup, visit veritas.com/netbackup

For more information, refer to: veritas.com/support/en_US/article.000127661

In this solution for data protection for Azure Stack, we have tested two Veritas NetBackup deployment use cases, which are:

- Media server installed and configured inside Azure Stack tenant VMs (see below Backup Use case 1)
- Media server installed and configured outside Azure Stack tenant VMs (see below Backup Use case 2)

In the case of media server outside of tenant VMs, the master server will act as a media server itself.
Media server installed outside Azure Stack would be the preferred model for most customers as Azure Stack infrastructure is added into their existing data center infrastructure, and hence the Azure Stack tenant VMs act as additional NetBackup clients in the existing NetBackup master server domain.

**Backup Use case 1**

One VM running Microsoft SQL Server and another VM running Windows File Server were deployed on HPE ProLiant for Microsoft Azure Stack. Both the Microsoft SQL Server VM and the Windows File Server VM were installed with Veritas NetBackup media server software. These media servers, using the HPE StoreOnce Catalyst Plug-in for Veritas NetBackup, will perform the deduplicated low-bandwidth content-aware catalyst backup to the HPE StoreOnce Catalyst store. Veritas NetBackup master server is installed and configured on a Windows 2016 server outside of Azure Stack. Separate backup policies were created to take backups. HPE StoreOnce Catalyst stores were created and configured as storage units in the NetBackup master server.

Figure 10 shows the media server installed and configured inside Azure Stack tenant VMs.

![Figure 10. Veritas NetBackup backup/restore architecture with media server installed inside Azure Stack tenant VMs](image-url)
Figure 11 shows that the Veritas NetBackup storage unit is configured with NetBackup media server inside Azure Stack. "Keepbackupvmsql" is the hostname for the Azure Stack tenant VM running Microsoft SQL and NetBackup media server.

Backup Use case 2

Figure 12 shows a combined NetBackup master and media server installed and configured outside Azure Stack. NetBackup client software was installed in the tenant VMs. In this case NetBackup client will push the backup data to the media server, and the media server, using the HPE StoreOnce Catalyst Plug-in for Veritas NetBackup, will perform the deduplicated low-bandwidth content-aware catalyst backup to the HPE StoreOnce Catalyst store. In this case since the deduplication is not happening at the tenant VM-level, the performance impact on the tenant VMs is reduced.
Figure 13 shows the Veritas NetBackup storage unit was configured with media server outside of Azure Stack. “netbackup” server is the NetBackup master server configured outside of Azure Stack.

![Image of storage unit configuration](image)

Figure 13. Veritas NetBackup storage unit configured with media server outside Azure Stack

**HPE StoreOnce**

HPE StoreOnce addresses the needs of all types of customers from entry level to large-scale enterprises. HPE StoreOnce Systems deliver scale-out capacity and performance to keep pace with shrinking backup windows, reliable disaster recovery, simplified protection of remote offices, and rapid file restore to meet today’s SLAs. The models vary by capacity and connectivity protocol. One could start by purchasing a single HPE StoreOnce base unit or couplet and then expand with additional couplets as well as expansion shelves. We have used an HPE StoreOnce 3520 System in this Reference Architecture. These units deliver cost-effective, scalable disk-based backup with deduplication, and optional copying of backup stores to lower cost object storage on-premises or in the cloud via Cloud Bank Storage for long-term data retention and archival. HPE StoreOnce also provides a replication target device for up to 50 remote or branch offices.

**HPE StoreOnce Catalyst**

HPE StoreOnce Systems with StoreOnce Catalyst are disk-based deduplication solutions providing seamless backup and recovery from the smallest remote sites to the largest enterprises. HPE StoreOnce Systems with StoreOnce Catalyst provide a single, high-performance backup architecture that spans the entire enterprise.

HPE StoreOnce Systems use Low Bandwidth Primary Transfer Policies, also known as source-side deduplication. These low bandwidth policies leverage HPE StoreOnce Catalyst source-side deduplication technology. This is the preferred option for copying backups directly to remote HPE StoreOnce Systems and Cloud Bank Storage stores; and, it achieves the highest level of aggregated backup throughput, both on and off site. Figure 14 shows the Catalyst store configured for content-aware Microsoft SQL Server backup and Windows File Server backup.

**Note**

If HPE StoreOnce Catalyst operations pass through a firewall, the network administrator must open (TCP) ports 9387 (Command protocol) and 9388 (Data protocol).
HPE StoreOnce Catalyst Plug-in for Veritas NetBackup

The HPE StoreOnce Catalyst Plug-in for Veritas NetBackup delivers tight integration between HPE StoreOnce Systems and Veritas NetBackup software through the StoreOnce Catalyst interface. The plug-in allows StoreOnce Systems to be managed as OpenStorage Technology (OST) devices and support of the OST features with StoreOnce Catalyst backup targets.

This plug-in allows NetBackup-managed movement of deduplicated data across the enterprise, from one HPE StoreOnce System to another or to the cloud. This high efficiency is enabled by the HPE StoreOnce Catalyst interface, which offers multiple advantages for backup to disk compared to traditional NAS and virtual tape interfaces. HPE StoreOnce Catalyst software dramatically improves the performance, function, and integration of backup applications such as Veritas NetBackup. HPE StoreOnce Catalyst delivers deduplication on an appliance server, media server, or dedicated appliance. Because it uses the same deduplication algorithm globally, data can be moved between platforms without rehydration. HPE StoreOnce Catalyst allows better utilization of advanced, disk-based storage solutions while increasing efficiency and performance.

Content Aware Backups for deduplication

The HPE StoreOnce Catalyst Plug-in for Veritas NetBackup version 4.0.2 introduces a feature called Content Aware Backups. When this feature is enabled, the plug-in identifies backups of well-structured data (primarily Microsoft SQL Server, Oracle, and SAP HANA® databases). The plug-in optimizes the deduplication algorithms to detect and align chunking around the well-structured data instead of using variable block chunking. This reduces the CPU requirements for processing the backup, increases deduplication ratios, and improves backup throughput. The plug-in processes backups of other data types using variable block chunking as usual. Figure 14 shows the HPE StoreOnce Catalyst Plug-in for Veritas NetBackup architecture.

The Content Aware Backups feature can be globally enabled during plug-in installation. You can also enable the feature for specific storage servers or logical storage units by editing the plug-in configuration file (plugin.conf). Only enable Content Aware Backups for new plug-in installations, or for new logical storage units in an existing installation.

For more information, refer to: https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=StoreOnceForVERITAS
Separate Catalyst stores were created in HPE StoreOnce, one for the Microsoft SQL Content Aware Backup and another for the Windows File Server backups as shown in figure 15.

Figure 15. HPE StoreOnce Catalyst stores created as target for different application backups

Separate NetBackup storage units were created for the above Catalyst stores and were used in the backup policies to take backups as shows in figure 16.

Figure 16. Veritas NetBackup – backup policies showing storage units
The steps below were followed to protect the workloads running on Microsoft Azure Stack tenant VMs:

- Install NetBackup media server or client software on Windows virtual machines deployed on HPE ProLiant for Microsoft Azure Stack.
- Add media/client servers into the existing NetBackup master server domain.
- Create a Catalyst store in HPE StoreOnce and add that as a storage unit.
- In the NetBackup Administration console, select policy type MS-SQL-Server, and browse the NetBackup client to discover the running SQL instance. Policy of type MS-Windows is used to protect the Windows File Server.
- Incremental backups were scheduled for every 15 minutes and a full backup was scheduled once per day.

Figure 17 shows the Microsoft SQL database backup policy. In the Attributes tab, specify the policy type and policy storage; in the Instances and Databases tab, specify to protect the SQL instances; and, in the Backup Selections tab, specify the object type. We are describing only Microsoft SQL backup/restore as the Windows File Server backup/restore is a pretty straightforward activity.

**Figure 17.** Veritas NetBackup Backup policy for SQL backup
Recovery Use case
The steps listed below were followed to recover the SQL database:

- From the Windows Start menu, select Programs ➔ Veritas NetBackup ➔ NetBackup Agents ➔ NetBackup MS SQL Client.
- From the NetBackup MS SQL Client Window, go to File, and select “Restore SQL Server objects”.

In the Restore Microsoft SQL Server Objects dialog box, in the left pane, select the database instance and backup which you want to restore. Select the necessary restore options, and click “Restore” as shown in figure 18.

You can either restore to the same database or you can create a template and move to a different database.

![NetBackup MS SQL Client restore options](image)

Figure 18. NetBackup MS SQL Client restore options
HPE Cloud Bank Storage for Hybrid IT data protection

HPE Cloud Bank Storage is a feature of HPE StoreOnce Systems, industry-leading data protection storage, that delivers highly efficient data transfer to and storage in the cloud. The combination of the HPE StoreOnce deduplication and cloud storage delivers low-cost, high-performance, and zero-risk long-term-retention solutions. HPE Cloud Bank Storage lets you leverage the economics, agility, and flexibility of the cloud for modernized data protection. You can natively, reliably, and cost-effectively move backup data to a public, private, or hybrid cloud, enabling long-term retention and reliable disaster recovery that is simple and efficient. HPE Cloud Bank Storage has the following benefits:

- **Economic**
  - Cloud Bank Storage is everything you need to manage large volumes of long-term backup data. It protects more than 100 petabytes of data at 20-times lower cost than other cloud services

- **Efficient**
  - Intelligent deduplication reduces cloud storage and access costs

- **Flexible**
  - Protect data on-premises and off-premises with public and private cloud services by purchasing an HPE Cloud Bank Storage license and pointing it at either Amazon Web Services (AWS), Microsoft Azure, or even your own private cloud with Scality RING
  - Broad-ecosystem of supported ISVs (Veritas NetBackup, Backup Exec, Micro Focus Data Protector), StoreOnce Catalyst Application plug-ins (Oracle RMAN, Microsoft SQL, and SAP HANA) and HPE Recovery Manager Central (RMC)

- **Simple**
  - Single management point for copy control utilizing the existing backup application

- **Robust**
  - Cloud Bank Storage delivers robust offsite protection that can be combined with cloud-based disaster recovery

- **Reliable**
  - Mitigate risk with simple, encrypted, and reliable cloud disaster recovery solutions. HPE Cloud Bank Storage moves data not only to cloud storage but also from the cloud and back to the local HPE StoreOnce System

- **Secure**
  - All data can be encrypted for secure transmission and storage in the cloud

HPE Cloud Bank Storage configuration

In order to create Cloud Bank stores, a valid Azure public cloud subscription and a valid HPE Cloud Bank Storage license are required. HPE StoreOnce firmware version 3.18.0 or later is required to use the HPE Cloud Bank Storage feature.

Create a Blob storage account in Azure public cloud with the relevant subscription, and create a container inside the storage account. See figures 19 and 20.

![Create storage account](image)

**Figure 19.** Microsoft Azure public cloud - Creating a Storage account with Account kind “Blob storage”

![Create new container](image)

**Figure 20.** Microsoft Azure public cloud - Creating a new Container inside the storage account

After the successful creation of the Blob storage in Microsoft Azure public cloud, go to the HPE StoreOnce Management Console, and click Create Catalyst store.
A page similar to figure 21 will appear. Check the box next to Cloud Bank Storage, and select the Cloud Service Provider from the dropdown list, then provide the necessary details of the Blob storage and the container which was created in Azure public cloud, and click Create. Now you are ready to do a backup to the HPE Cloud Bank Storage.

**Figure 21.** Creating a new HPE Cloud Bank Storage store in HPE StoreOnce using Microsoft Azure Blob storage
HPE Cloud Bank Storage and Veritas NetBackup integration

Figure 22 shows an overview diagram of Microsoft Azure Stack protected with HPE Cloud Bank Storage for long-term retention, archival, and disaster recovery. NetBackup master server initiates a backup to the local Catalyst store and then a duplicate backup copy to the Cloud Bank store.

Figure 22. Protecting tenant VMs running Microsoft workloads to HPE Cloud Bank Storage in Azure public cloud
HPE Cloud Bank Storage Catalyst copy is configured using a Storage Lifecycle Policy (SLP) in NetBackup. For the backup destination, the storage unit created using the local HPE StoreOnce System is selected. For the copy destination, the storage unit that was created using HPE Cloud Bank Storage, in this case a Microsoft Azure Blob storage is selected, as shown in figure 23. Update the Policy Storage attribute of the NetBackup policy with this lifecycle name.

The following sections describe the different HPE Cloud Bank Storage use cases.

The steps below were followed to back up the workloads running on tenant VMs to the HPE Cloud Bank Storage.

- Install NetBackup media server or client software on Windows virtual machines deployed on HPE ProLiant for Microsoft Azure Stack.
- Add NetBackup media/client servers into the existing NetBackup master server domain.
- Create a local Catalyst store and a Cloud Bank store in HPE StoreOnce and add that as a storage unit in NetBackup master server.
- Configure a Storage Lifecycle Policy to copy the data from the local Catalyst store to the Cloud Bank store, which is created using Azure Blob storage for this environment.
- Create backup policies to protect the Microsoft SQL database and Windows File Server, and select the respective SLP under policy storage.

**Catalyst copy to Cloud Bank store**

HPE Cloud Bank Storage stores are designed for use as Catalyst copy targets. In this use case, the customer directs backups to a regular Catalyst store, then for long-term backup data retention, a copy job is run to copy the backup data to the Cloud Bank store.
It sends only unique data to the cloud which is already deduplicated at the StoreOnce; this will reduce the storage capacity requirement in the cloud.

Figure 24 shows the backup jobs and the duplication (copy) jobs from the Veritas NetBackup Activity monitor screen.

![Figure 24. Veritas NetBackup management console - backup jobs and duplication (copy) jobs](image)

Figure 25 shows a Cloud Bank report from the HPE StoreOnce Management Console for the Catalyst copy to the Cloud Bank store.

![Figure 25. Cloud Bank report from the HPE StoreOnce Management Console](image)

HPE Cloud Bank Storage has an advanced compression algorithm that provides much better dedupe than the local StoreOnce which over time saves a lot of cloud related costs. Figure 25a shows the Dedupe Ratio comparison between the Local Catalyst store and the Cloud Bank store.

![Figure 25a. HPE StoreOnce GUI shows the Dedupe Ratio comparison between Local Catalyst store and the Cloud Bank store](image)
In the case of accidental deletion of the local backup or expired backup, we can do either a direct restore from the Cloud Bank store or restore to the local Catalyst store using Reverse catalyst copy.

**Database restore directly from HPE Cloud Bank Storage**

In this case all data to be restored are read from the Cloud Bank store, which involves many transactions at the cloud thus increases cloud billing. If you copy data from Cloud Bank Storage to the local StoreOnce (Reverse catalyst copy) and then do a restore, only deduplicated data will be copied from the cloud and will save cost.

Figure 26 shows the download statistics (top graph) and the get requests statistics (bottom graph) from the Cloud Bank store.

Figure 26. Cloud Bank report for download and get requests statistics from the HPE StoreOnce Management Console

**Database restore from Reverse catalyst copy**

Reverse catalyst copy is nothing but copying the backup back to the local StoreOnce from the Cloud Bank store. In this case a duplicate job will be initiated form the NetBackup console. The advantage of doing this is that only the deduplicated data will be copied back, hence saving the bandwidth as well as the “get” request to the cloud. Over time this reduces cloud billing.

Hence it is always beneficial to do a Reverse catalyst copy from the cloud back to on-premises for faster and more economical restore.
Figure 27 shows the Cloud Bank statistics for direct restore from Cloud Bank Storage and Reverse catalyst copy to the local Catalyst store. The first spike in both graphs is for direct restore from Cloud Bank Storage and the second spikes are Reverse catalyst copy. The top graph shows the bandwidth utilization and the bottom graph shows the get request.

Figure 27. Cloud Bank report – comparing results for direct restore from Cloud Bank Storage and Reverse catalyst copy in terms of Bandwidth utilization (top graph) and Get request (bottom graph)
Disaster recovery using HPE Cloud Bank Storage

Investing in and managing an owned off-site location that prevents the business from coming to a halt in the event of a site outage, ransomware threat, or natural disaster is cost-prohibitive for many businesses. The high costs associated with the transfer of large amounts of data to the cloud also remains a barrier.

Low-cost, high-capacity object storage in a public, private, or hybrid cloud is an ideal storage option for disaster recovery. This has become easy with new features of HPE Cloud Bank Storage, namely, Disconnecting, and Multi-Reader functionalities.

In the case of disaster recovery:

- Install a new StoreOnce Appliance (can be a VSA).
- Re-connect to the HPE Cloud Bank Storage by entering the credentials and encryption key.
- Create a new local Catalyst store.
- Re-configure Veritas NetBackup Server.
- Configure the storage device in the NetBackup Server.
- Initiate an inventory job.

NetBackup will identify all the backups automatically and we can initiate Catalyst copy to the local store and Restore Data to either the original locations or to different locations.

In case of a DR drill:

- Connect the Cloud Bank Storage from another StoreOnce by entering the credentials and encryption key.
- Create a new local Catalyst store.
- Configure Veritas NetBackup Server.
- Configure the storage device in the NetBackup Server.
- Initiate an inventory job.
- Verify the data by restoring to a dummy database.

Restoring the database or files is possible only using Veritas NetBackup. As mentioned in an earlier section, NetBackup will auto detect the backup contents from the connected stores and can initiate a restore either directly from the Cloud Bank store or from Reverse catalyst copy.

Disconnecting Cloud Bank stores

Disconnecting a Cloud Bank store removes the store from a StoreOnce System and leaves the data in the cloud in a read/write state. This allows a Cloud Bank store to be migrated between StoreOnce Systems or used to test Connect functionality.

Navigate to the StoreOnce → StoreOnce Catalyst → Stores → Catalyst Store Details tab, select the Cloud Bank Catalyst store and Disconnect.

Note

When you disconnect a Cloud Bank store from a StoreOnce System:

- If the store is encrypted, be sure that you have exported the Encryption Key before disconnecting. The key is required for Connect (Read Only) or Connect (Read Write) on another system.
- For the first 24 hours, you can only connect to the store Read Only. If you do not Connect (Read Write) to this store within 60 days after disconnecting, the store no longer permits connections from any StoreOnce System. The data can no longer be recovered by yourself and you'll need to contact HPE customer support for the recovery.
Figure 28 shows disconnecting a Cloud Bank store using the HPE StoreOnce GUI for testing disaster recovery.

**Figure 28.** Disconnecting a Cloud Bank store using the HPE StoreOnce GUI

Connect (Read Write) to a Cloud Bank store adds an existing Cloud Bank store to a StoreOnce System. After connection, the store is online and available to accept backups. This procedure allows you to migrate a Cloud Bank store between StoreOnce Systems, or to recover it after a disaster.

Connecting to a Cloud Bank store from another HPE StoreOnce in the case of disaster is shown in figure 30. Read-only operation is enabled within 24 hours. You can restore from the read-only Cloud Bank store to the local StoreOnce, and, if required, after 24 hours, you can re-connect to the store as read-write, as shown in figure 31.

**Multi-Reader Cloud Bank stores**

Multi-Reader functionality allows additional StoreOnce Systems to access data in the Cloud Bank store while the primary StoreOnce System is still attached to it. This can be used for checking compliance, for data mining, and for disaster recovery. This can be across geographies and the data can be accessed in read-only mode.

Navigate to StoreOnce ➔ StoreOnce Catalyst ➔ Stores, and click Connect, provide the necessary information regarding the Cloud Service provider, and click OK, as shown in figures 29 and 30.
## Cloud Bank Storage Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Service Provider</td>
<td>Azure</td>
</tr>
<tr>
<td>Storage Account Name</td>
<td>sreenivaru</td>
</tr>
<tr>
<td>Access Key</td>
<td>Example: MyStorageAccount</td>
</tr>
<tr>
<td>Use Proxy</td>
<td></td>
</tr>
<tr>
<td>Container Name</td>
<td>dr-container</td>
</tr>
</tbody>
</table>

(*) Required Value

---

Figure 29. Connecting a Cloud Bank store using the StoreOnce management GUI

## Catalyst Store Details

- **Status**: Connected
- **UID**: 7415947990098057435
- **StoreOnce Serial Number**: CZ36083K0101
- **Store Name**: dr-container
- **Store Description**: Catalyst Store 3
- **Number of Items**: 0
- **User Bytes**: 0 B
- **Disk Bytes**: 2.1 KB
- **Creation Date/Time**: 10:30 2018/01/30
- **Last Accessed Date/Time**: 10:54 2018/01/30
- **Store Version**: 3
- **Encrypted**: [ ]

Connect (Read Write) is disabled because the Catalyst Store was connected to a StoreOnce System within the last 24 hours

---

Figure 30. Connecting a Cloud Bank store from another HPE StoreOnce with Read-Only access
### Catalyst Store Details

<table>
<thead>
<tr>
<th>Status:</th>
<th>Disconnected</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID:</td>
<td>7415947990098057435</td>
</tr>
<tr>
<td>StoreOnce Serial Number:</td>
<td>CZ36053K0101</td>
</tr>
<tr>
<td>Store Name:</td>
<td>DR-container</td>
</tr>
<tr>
<td>Store Description:</td>
<td>Catalyst Store 3</td>
</tr>
<tr>
<td>Number of Items:</td>
<td>0</td>
</tr>
<tr>
<td>User Bytes:</td>
<td>0 B</td>
</tr>
<tr>
<td>Disk Bytes:</td>
<td>2.1 KB</td>
</tr>
<tr>
<td>Creation Date/Time:</td>
<td>10:30 2018/01/30</td>
</tr>
<tr>
<td>Last Accessed Date/Time:</td>
<td>10:28 2018/02/01</td>
</tr>
<tr>
<td>Store Version:</td>
<td>3</td>
</tr>
<tr>
<td>Encrypted:</td>
<td>✔</td>
</tr>
</tbody>
</table>

#### Figure 31
Connecting a Cloud Bank store from another HPE StoreOnce with Read-Write access.

#### Figure 32
Multi-Reader Cloud Bank store accessed from two different HPE StoreOnce Systems with Read-Only access.
Archiving and long-term retention

Many IT companies cannot delete backup data in order to comply with legal requirements or for future restores. This drives the need to retain vast datasets for years or decades, as data ages and access is infrequent, it can be moved to even more cost-efficient storage for archiving or extended retention. This data is protected for future access and is readable via any StoreOnce System. The Cloud Bank Storage Detach Option addresses this requirement.

Detaching a Cloud Bank store

Detaching a Cloud Bank store uses Cloud Bank Storage Detach Capacity licenses. Once detach is complete, the Cloud Bank Storage Detach Capacity license is reduced by the store size in the cloud. This operation removes the store from a StoreOnce System and leaves the detached store in a read-only state. The equivalent value of Detach Capacity that is used is released from the Cloud Bank Storage Read/Write Capacity. The available Read/Write Capacity is ready for new or existing Cloud Bank stores.

Navigate to the StoreOnce → StoreOnce Catalyst → Stores → Catalyst Store Details tab, select the Cloud Bank Catalyst store and Detach, as shown in figure 33.

**Note**

When you detach a Cloud Bank store from a StoreOnce System:

- If the store is encrypted, be sure that you have exported the Encryption Key before detaching. The key is required for Connect (Read Only) on another system.
- Detaching is only possible if there is enough Detach Capacity licenses on the StoreOnce System.

---

**Figure 33.** Detaching a Cloud Bank store using the HPE StoreOnce management GUI
Once detached, Connect (Read Write) is no longer possible. No further data can be written to this store from a StoreOnce System. However, the container permissions in the cloud service provider remain unchanged. Figure 34 shows connecting to a detached store in read-only mode.

### Catalyst Store Details

<table>
<thead>
<tr>
<th>Status:</th>
<th>Detached</th>
</tr>
</thead>
<tbody>
<tr>
<td>UID:</td>
<td>8786190461080561700</td>
</tr>
<tr>
<td>StoreOnce Serial Number:</td>
<td>999546088101</td>
</tr>
<tr>
<td>Store Name:</td>
<td>detach-attach</td>
</tr>
<tr>
<td>Store Description:</td>
<td>Catalyst Store 7</td>
</tr>
<tr>
<td>Number of Items:</td>
<td>2</td>
</tr>
<tr>
<td>User Bytes:</td>
<td>74.1 MB</td>
</tr>
<tr>
<td>Disk Bytes:</td>
<td>33.2 MB</td>
</tr>
<tr>
<td>Creation Date/Time:</td>
<td>10:35 2018/01/18</td>
</tr>
<tr>
<td>Last Accessed Date/Time:</td>
<td>10:49 2018/01/18</td>
</tr>
<tr>
<td>Store Version:</td>
<td>3</td>
</tr>
<tr>
<td>Encrypted:</td>
<td>☑</td>
</tr>
</tbody>
</table>

⚠️ Connect (Read Write) is disabled because the Catalyst Store is in a detached state

### Figure 34. Connecting to a Detached Cloud Bank store using the HPE StoreOnce management GUI

**HPE Cloud Bank Storage encryption for security**

HPE Cloud Bank Storage lets you reduce risk with simple, encrypted, and reliable cloud disaster recovery. Encryption is a recommended setting for Cloud Bank stores and is selected by default when creating the Cloud Bank store and you cannot change that later. Cloud Bank stores use the same encryption process as regular Catalyst stores with keys stored on the StoreOnce System or in an external key manager.

All encryption keys written to the object store are encrypted with a key encryption key (KEK) – this is only stored locally or in a central key manager (ESKM).

The object storage credentials are also stored encrypted on the StoreOnce System. If there is no central key manager and you are restoring/recovering to a different StoreOnce System, the encryption key (KEK) and its password must be entered.

For more information on HPE StoreOnce Security with ESKM, refer to: https://h20195.www2.hpe.com/V2/GetDocument.aspx?docname=a00000438enw

**Summary**

Protection of HPE ProLiant for Microsoft Azure Stack, providing Azure public cloud functionality on-premises, is critical. Organizations are investing in hybrid cloud to address differing needs of their infrastructure and business. The necessity to protect some data on-premises while moving other data directly to cloud requires cloud-aware data protection solutions.

Veritas NetBackup along with HPE StoreOnce and HPE Cloud Bank Storage can back up Azure Stack data to both a local Catalyst store and to off-premises Azure Blob storage. This data protection solution provides an easy, cost effective, long retention, and efficient backup method to protect the data on HPE ProLiant for Microsoft Azure Stack.
This Reference Architecture describes solution testing performed in January 2018.

## Appendix A: Bill of materials

### Note

Part numbers are at time of testing and subject to change. The bill of materials does not include complete support options or other rack and power requirements. If you have questions regarding ordering, please consult with your HPE Reseller or HPE Sales Representative for more details: [hpe.com/us/en/services/consulting.html](http://hpe.com/us/en/services/consulting.html)

### Table A-1. Bill of materials

<table>
<thead>
<tr>
<th>Qty</th>
<th>Part number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Q2851A</td>
<td>HPE DL380 Gen9 with Microsoft Azure Stack Node</td>
</tr>
<tr>
<td>4</td>
<td>817953-L21</td>
<td>HPE DL380 Gen9 Intel Xeon E5-2683v4 (2.1GHz/16-core/40MB/120W) FIO Processor Kit</td>
</tr>
<tr>
<td>4</td>
<td>817953-B21</td>
<td>HPE DL380 Gen9 Intel Xeon E5-2683v4 (2.1GHz/16-core/40MB/120W) Processor Kit</td>
</tr>
<tr>
<td>64</td>
<td>805351-B21</td>
<td>HPE 32GB (1x32GB) Dual Rank x4 DDR4-2400 CAS-17-17-17 Registered Memory Kit</td>
</tr>
<tr>
<td>4</td>
<td>768856-B21</td>
<td>HPE DL380 Gen9 3LFF Rear SAS/SATA Kit</td>
</tr>
<tr>
<td>40</td>
<td>861750-B21</td>
<td>HPE 6TB SATA 6G Midline 7.2k LFF (3.5in) SC 1yr Why 512e HDD</td>
</tr>
<tr>
<td>8</td>
<td>875519-B21</td>
<td>HPE 480GB SATA 6G Read Intensive M.2 2280 3yr Why Digitally Signed Firmware SSD</td>
</tr>
<tr>
<td>16</td>
<td>875480-B21</td>
<td>HPE 1.92TB SATA 6G Mixed Use LFF (3.5in) SCC 3yr Why Digitally Signed Firmware SSD</td>
</tr>
<tr>
<td>4</td>
<td>761874-B21</td>
<td>HPE Smart Array P840/4GB FBWC 12Gb 2-ports Int FIO SAS Controller</td>
</tr>
<tr>
<td>4</td>
<td>779799-B21</td>
<td>HPE Ethernet 10Gb 2-port 566FLR-SFP+ Adapter</td>
</tr>
<tr>
<td>4</td>
<td>878783-B21</td>
<td>HPE Universal SATA HHHL 3yr Why M.2 Kit</td>
</tr>
<tr>
<td>8</td>
<td>720482-B21</td>
<td>HPE 800W Flex Slot Titanium Hot Plug Power Supply Kit</td>
</tr>
<tr>
<td>4</td>
<td>BD505A</td>
<td>HPE iLO Advanced 1-server License with 3yr Support on iLO Licensed Features</td>
</tr>
<tr>
<td>4</td>
<td>P8831A</td>
<td>HPE OneView w/o iLO including 3yr 24x7 Support 1-server FIO LTU</td>
</tr>
<tr>
<td>1</td>
<td>Q2852A</td>
<td>HPE DL380 Gen9 with Microsoft Azure Stack Management Node</td>
</tr>
<tr>
<td>1</td>
<td>818172-L21</td>
<td>HPE DL360 Gen9 Intel Xeon E5-2620v4 (2.1GHz/8-core/20MB/85W) FIO Processor Kit</td>
</tr>
<tr>
<td>1</td>
<td>818172-B21</td>
<td>HPE DL360 Gen9 Intel Xeon E5-2620v4 (2.1GHz/8-core/20MB/85W) Processor Kit</td>
</tr>
<tr>
<td>4</td>
<td>805349-B21</td>
<td>HPE 16GB (1x16GB) Single Rank x4 DDR4-2400 CAS-17-17-17 Registered Memory Kit</td>
</tr>
<tr>
<td>4</td>
<td>872477-B21</td>
<td>HPE 600GB SAS 12G Enterprise 10K SFF (2.5in) SC 3yr Why Digitally Signed Firmware HDD</td>
</tr>
<tr>
<td>1</td>
<td>764442-B21</td>
<td>HPE DL360 Gen9 Low Profile PCIe Slot CPU2 Kit</td>
</tr>
<tr>
<td>1</td>
<td>749974-B21</td>
<td>HPE Smart Array P440ar/2GB FBWC 12Gb 2-ports Int FIO SAS Controller</td>
</tr>
<tr>
<td>1</td>
<td>779799-B21</td>
<td>HPE Ethernet 10Gb 2-port 566FLR-SFP+ Adapter</td>
</tr>
<tr>
<td>2</td>
<td>720482-B21</td>
<td>HPE 800W Flex Slot Titanium Hot Plug Power Supply Kit</td>
</tr>
<tr>
<td>1</td>
<td>871147-B21</td>
<td>Microsoft Windows Server 2016 (16-core) Standard FIO Not Pre-installed English SW</td>
</tr>
<tr>
<td>1</td>
<td>BD505A</td>
<td>HPE iLO Advanced 1-server License with 3yr Support on iLO Licensed Features</td>
</tr>
<tr>
<td>1</td>
<td>P8831A</td>
<td>HPE OneView w/o iLO including 3yr 24x7 Support 1-server FIO LTU</td>
</tr>
<tr>
<td>1</td>
<td>JG510A</td>
<td>HPE 5900AF 48G 4XG 2QSFP+ Switch</td>
</tr>
<tr>
<td>2</td>
<td>JC772A</td>
<td>HPE 5900AF 48XG 4QSFP+ Switch</td>
</tr>
<tr>
<td>Qty</td>
<td>Part number</td>
<td>Description</td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Backup Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>BB922A</td>
<td>HPE StoreOnce 3520 12TB System</td>
</tr>
<tr>
<td>1</td>
<td>BB926A</td>
<td>HPE StoreOnce 10GbE Network Card</td>
</tr>
<tr>
<td>1</td>
<td>BB887A</td>
<td>HPE StoreOnce 2000/3000 Catalyst LTU</td>
</tr>
<tr>
<td>1</td>
<td>Q8J92AAE</td>
<td>HPE StoreOnce Cloud Bank Storage Read/Write for Gen3 Systems 1TB E-LTU</td>
</tr>
<tr>
<td>1</td>
<td>Q8J93AAE</td>
<td>HPE StoreOnce Cloud Bank Storage Detach for Gen3 Systems 1TB E-LTU</td>
</tr>
<tr>
<td>Others</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>P9K40A</td>
<td>HPE 42U 600x1200 Enterprise G2 Shock Pallet</td>
</tr>
<tr>
<td>4</td>
<td>AF521A</td>
<td>HPE Intelligent Modular 8.3kVA/CS8265C 40A/208V Outlets (6) C19</td>
</tr>
</tbody>
</table>
Resources and additional links

HPE Reference Architectures
hpe.com/info/ra

HPE ProLiant for Microsoft Azure Stack QuickSpecs

HPE ProLiant for Microsoft Azure Stack

HPE ProLiant for Microsoft Azure Stack (Microsoft partner site)


HPE StoreOnce: hpe.com/storage/storeonce

HPE Cloud Bank Storage

HPE Servers
hpe.com/servers

HPE Storage
hpe.com/storage

HPE Networking
hpe.com/networking

HPE Technology Consulting Services
hpe.com/us/en/services/consulting.html

To help us improve our documents, please provide feedback at hpe.com/contact/feedback.