Long-Term Data Retention with Veritas NetBackup

Microsoft Azure

This white paper provides a technical overview of Azure cloud as a long-term retention storage solution with Veritas NetBackup™. It highlights the overall solution architecture, components, integration points and walks you through configuring a CloudCatalyst media server using Azure Blob storage.

VERITAS
The truth in information.
# Cloud Object Storage with Veritas NetBackup and Microsoft Azure

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>3</td>
</tr>
<tr>
<td>SCOPE</td>
<td>3</td>
</tr>
<tr>
<td>SOLUTION ARCHITECTURE OVERVIEW</td>
<td>4</td>
</tr>
<tr>
<td>SOLUTION COMPONENTS</td>
<td>4</td>
</tr>
<tr>
<td>Azure Blob Storage</td>
<td>4</td>
</tr>
<tr>
<td>Blob Storage Access Tiers</td>
<td>5</td>
</tr>
<tr>
<td>Network Connectivity</td>
<td>5</td>
</tr>
<tr>
<td>SOLUTION INTEGRATION FLOW</td>
<td>6</td>
</tr>
<tr>
<td>STANDARD BACKUP TO AZURE BLOCK BLOB STORAGE (Hot, Cool, Archive)</td>
<td>6</td>
</tr>
<tr>
<td>TRADITIONAL DUPLICATION DATA FLOW</td>
<td>8</td>
</tr>
<tr>
<td>OPTIMIZED DUPLICATION TO THE CLOUD USING CLOUDCATALYST (DEDUPLICATION)</td>
<td>8</td>
</tr>
<tr>
<td>ACCESS APPLIANCE OPTIMIZED DUPLICATION (DEDUPLICATION) DATA FLOW TO –AZURE BLOB STORAGE</td>
<td>9</td>
</tr>
<tr>
<td>DISASTER RECOVERY USING AZURE</td>
<td>10</td>
</tr>
<tr>
<td>AUTO IMAGE REPLICATION (AIR) TO THE CLOUD – HYBRID CONFIGURATION</td>
<td>10</td>
</tr>
<tr>
<td>APPENDIX</td>
<td>12</td>
</tr>
<tr>
<td>AZURE</td>
<td>13</td>
</tr>
<tr>
<td>CREATION OF NETBACKUP CLOUDCATALYST STORAGE</td>
<td>14</td>
</tr>
<tr>
<td>CREATION OF STORAGE LIFECYCLE POLICY (SLP) DEFINITION</td>
<td>20</td>
</tr>
<tr>
<td>CREATION AND MODIFICATION OF THE BACKUP POLICY TO USE THE SLP</td>
<td>22</td>
</tr>
<tr>
<td>VALIDATE PROTECTION USING SLP</td>
<td>24</td>
</tr>
<tr>
<td>ABOUT VERITAS TECHNOLOGIES LLC</td>
<td>26</td>
</tr>
</tbody>
</table>

© 2020 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo and NetBackup are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
INTRODUCTION

EXECUTIVE SUMMARY

Cloud services play a critical role in helping organizations accelerate their digital transformation by offering scalability and flexibility without the big on-premises price tag. Some of the primary drivers for this move are to reduce the data center footprint and leverage the public cloud as the repository to safeguard long-term retention data from on-premises failures and malware attacks or to ensure regulatory compliance. Organizations are as responsible for data management in the cloud as they are on-premises—although how they accomplish it does differ. In a hybrid IT environment, proper data management is crucial to prevent operational expenditures (OpEx) and business risks from skyrocketing out of control. Microsoft Azure is the cloud of choice for many organizations worldwide.

Microsoft Azure Storage Services with Veritas NetBackup provides a compelling option for protecting and preserving data from on-premises challenges as well as for off-premises long-term retention. Storage optimization technologies such as compression and the Veritas Deduplication Engine reduce cloud egress and ingress costs and support for Blob storage access tiers help manage data based on cost and performance considerations.

Veritas Information Studio offers intuitive and flexible classification policies that can adapt to meet an organization’s changing needs. Robust file analysis aggregates metadata so organizations can better understand data type, ownership, access and age to determine areas of waste, risk and value. This process helps identify data that can be safely moved to the cloud to minimize risk and liability.

In addition, the Microsoft Azure Marketplace offers an Azure Resource Manager (ARM) Solution Template that allows organizations to deploy a NetBackup Linux virtual machine (VM) in just a few minutes using their existing license keys.

SCOPE

This document provides technical detail to help you understand how NetBackup and Azure cloud storage can help solve long-term retention needs for IT organizations. It describes the solution’s components and some configuration options. For additional detail, we recommend reviewing Microsoft Azure and Veritas product documentation for installation, configuration and administration of the respective solution components.

NOTE: This document is updated periodically. If you downloaded a local copy of this document, please get the latest version from this link.
SOLUTION ARCHITECTURE OVERVIEW

Figure 1 depicts a high-level overview of the Veritas data protection solution with Azure cloud storage for long-term retention. An integral part of this solution is the use of Information Studio to provide information on the data residing on-premises to help organizations make decisions about the lifecycle of the data. A report generated by Information Studio assists users in making informed decisions about which data to store on-premises or send to the cloud and/or defining the storage lifecycle policies of the data. For instance, the lifecycle of backup data can first reside on-premises on a NetBackup Appliance or Build Your Own Server (BYOS) for the short term, then move to Veritas Access Appliances for mid-term retention and finally to Azure Blob storage for long-term retention and disaster recovery. NetBackup provides broad support for different Blob storage accounts and access tiers. These access tiers differ in terms of cost, usage, restore time, availability and other services.

Figure 1. A high-level overview of NetBackup with Azure Cloud Access Tiers.

SOLUTION COMPONENTS

Azure Blob Storage

Azure Storage Accounts offers four access tiers for Blob storage - Premium, Hot, Cool and Archive to house object storage data in Azure cloud. These storage objects are securely accessed using a REST (REpresentational State Transfer) API communicating via the http protocol. The Archive type of Blob storage is a great alternative to tape when it comes to long-term retention. Azure also offers different connectivity options based on desired transmission performance and cost.

NetBackup uses a built-in Azure cloud connector to connect to with Blob storage. This connector is based on our OpenStorage Technology (OST) plugin architecture and is automatically installed on all NetBackup servers — master, media and CloudCatalyst media servers. OST enables tighter integration of disk-based storage platforms with NetBackup using plug-ins developed in-house or by storage vendors.
Blob Storage Access Tiers

NetBackup can back up and retrieve data from the following Blob storage access tiers:

- **Hot**—For frequently accessed data.
- **Cool**—For infrequently accessed data that is stored at least for 30 days.
- **Archive**—Mainly for archival or long-term retention of data that is rarely accessed and stored for at least 180 days.

Support for these access tiers with NetBackup is available in all Azure locations. In addition, NetBackup also supports the above access tiers within Azure Government locations. Encryption is provided using the NetBackup Key Management Service (KMS). In addition, Azure Storage transparently encrypts all stored data using 256-bit Advanced Encryption Standard (AES) encryption and complies with Federal Information Processing Standards (FIPS) 140-2 standards.

Deciding to which Azure Blob access tier you should send backup images is usually based on several factors, including restore time, cost and NetBackup feature support. NetBackup can use Blob Hot, Cool or Archive access tiers like a regular disk pool or use CloudCatalyst to efficiently send deduplicated data to Hot or Cool access tiers. Table 1 provides a comparison of each of the Azure Blob access tiers based on these factors. Refer to Azure Storage Service documentation for additional information on access tiers.

**Table 1. Comparison of Azure Blob access tiers supported by NetBackup**

<table>
<thead>
<tr>
<th>Azure Blob Access Tier</th>
<th>Restore Time with NetBackup</th>
<th>Cost**</th>
<th>CloudCatalyst</th>
<th>Accelerator</th>
<th>Minimum Storage Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hot</td>
<td>milliseconds</td>
<td>$$$$</td>
<td>Supported</td>
<td>Supported</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Cool</td>
<td>milliseconds</td>
<td>$$</td>
<td>Supported</td>
<td>Supported</td>
<td>30 days</td>
</tr>
<tr>
<td>Archive</td>
<td>3–15 hours</td>
<td>$</td>
<td>Not Supported</td>
<td>Not Supported</td>
<td>180 days</td>
</tr>
</tbody>
</table>

** The "s" represents a simple cost view. For exact pricing, please refer to Block Blob pricing for Azure.**

Network Connectivity

The speed of backups and restores is highly dependent on the type of network connectivity. Azure offers multiple connectivity options to its global locations from on-premises data centers:

- **Internet** - Basic Internet connectivity to Azure offered by Internet service providers (ISPs).
- **VPN Gateway** - Enables creation of encrypted cross-premises connections to your virtual network from on-premises locations.
- **Virtual WAN** - A networking service that allows you to establish connectivity between your global sites to and through Azure.
- **ExpressRoute** - Connection between an on-premises environment to the Azure cloud facilitated by a connectivity provider. These connections do not go over the public Internet and address some typical challenges such as speed (bandwidth and throughput), network congestion and/or contention.
SOLUTION INTEGRATION FLOW

All data goes through a lifecycle from being created, read, modified, moved to other tiers of storage and eventually expired or deleted once it’s no longer of use. When data is actively used, it resides in primary storage and is backed up to secondary storage for protection. When data or backup data is infrequently accessed, organizations move it to cheaper storage on-premises and/or off-premises. Understanding data in terms of usage, age, type and if it contains personally identifiable information (PII), is non-business or is subject to regulatory compliance is crucial in determining where to move that data across storage platforms or different tiers of storage on-premises or off-premises.

NetBackup manages the lifecycle of data using storage lifecycle policies (SLPs). NetBackup backup policies and/or SLPs define the path or flow of data. You can define lifecycle policies to send data either to a single target or to an SLP. An SLP defines the lifecycle objectives of the data from backup to duplication to varying storage types and/or replication to different locations. As previously mentioned, data is sent to Azure Blob storage using the built-in OST-compatible cloud connector installed on CloudCatalyst or the media server. The solution integration flows described in this section includes:

- Backup to Azure Block Blob and Azure Archive storage.
- Traditional duplication to Azure.
- Optimized duplication (deduplication) to the cloud using CloudCatalyst.
- Optimized duplication (deduplication) to the cloud from an Access Appliance.

STANDARD BACKUP TO AZURE BLOCK BLOB STORAGE (Hot, Cool, Archive)

With NetBackup, the simplest way to move data to object storage is to use the standard cloud connector interface, which lets you configure a cloud object storage target in Microsoft Azure or Microsoft Azure GovCloud. The standard interface assists with writing data to Block Blob Hot or Cool access tiers. (See Figure 2.)

* Protect on-premises and cloud-based workloads with the same methods.

* Source and target can be converged master and storage or separate instances.

Figure 2. Standard backup to cloud object storage using NetBackup.
In addition, NetBackup helps you move data to Azure Archives. When writing to an Azure Archive, you must use the Hot access tier. Image data and metadata is written to a Hot access tier and object data comprising image fragments are reclassified to the Archive tier. (See Figure 3.)

![Figure 3. Backing up data to Azure Hot and Archive storage tiers using NetBackup.](image)

Restoring data from an Azure Archive tier requires a retrieval operation where data is recalled from the Archive tier to a Hot tier. Once the image fragments are available in the Hot tier, they’re read by the NetBackup media server and data is sent to the client for restore purposes. Once the restore is complete, the image fragments in the Hot tier are moved back to Archive tier. (See Figure 4.)

![Figure 4. Restoring data from an Azure Archive tier using NetBackup.](image)

This functionality enables a straightforward, easy implementation of a cloud storage target that can be written to from any master or media server. Standard charges apply based on data ingress and egress charges, as documented on the [Azure Storage pricing page](https://azure.microsoft.com/pricing/).
TRADITIONAL DUPLICATION DATA FLOW

For data that doesn’t benefit from deduplication, backup data is duplicated from the media server to Azure storage classes using the NetBackup OST plug-in installed by default on the media server. Pictured below in Figures 15 and 16 are examples of the data flow from NetBackup to Hot or Cool Azure Blob access tiers. The traditional duplication flow is similar to the optimized duplication (deduplication) without the use of CloudCatalyst.

The traditional flow for sending data to Hot or Cool Azure Blob access tiers involves the data being initially stored on an advanced disk (copy 1) on a NetBackup media server for short- to mid-term retention and then copied to Azure Blob storage (copy 2) for long-term retention. You can do restores from either the advanced disk (copy 1, the default) or from Azure Blob (copy 2), as shown in Figure 5.

Figure 5. Traditional duplication from NetBackup to and from Azure Hot or Cool access tiers.

When sending data to an Azure Archive, metadata is stored using Hot (online) tier and data is stored in Azure Archive (offline) tier within the storage account. This is represented in in Figure 6. Restoring Azure Archive access tier data requires rehydrating the data first to an online tier prior to retrieval from NetBackup.

Figure 6. Traditional duplication from NetBackup to and from Azure Blob storage access tiers.

OPTIMIZED DUPLICATION TO THE CLOUD USING CLOUDCATALYST (DEDUPLICATION)

NetBackup CloudCatalyst is required when sending deduplicated data to either the Azure Blob Hot or Cool access tiers supported by NetBackup. The access and storage costs vary inversely, depending on the access tier of the Azure storage account. The NetBackup CloudCatalyst solution combines the performance and flexibility of NetBackup with powerful data deduplication technology to better leverage the cloud for storing backups for disaster recovery or long-term data retention. By ensuring backup data remains optimized while in transit to the cloud and at rest in the cloud, the NetBackup CloudCatalyst solution greatly reduces cost and increases performance when using cloud storage. CloudCatalyst allows organizations to send backup data to cloud object storage in deduplicated form. CloudCatalyst can process optimized backup images from existing media server deduplication pool (MSDP) volumes or directly from a client for transfer to an Azure Block Blob storage target. The Hot and Cool tiers of Azure BlockBlob storage have been certified for use with NetBackup CloudCatalyst as well.
When using MSDP volumes as the source, the CloudCatalyst server does not rehydrate or remove optimization from deduplication. This end-to-end deduplication is a significant difference in how the CloudCatalyst solution operates compared to other solutions on the market today. The CloudCatalyst server allows direct recovery of data from the CloudCatalyst server without first passing through another media server. Using CloudCatalyst provides the highest level of functionality and cost savings when using object storage. (See Figure 7.)

![CloudCatalyst Diagram]

### Figure 7. Optimized data duplication with NetBackup CloudCatalyst to and from Azure Blob object storage access tiers.

In Figure 7, client data is backed up and deduplicated to an MSDP storage target residing on a media server for short- or mid-term retention. This deduplicated data is sent to CloudCatalyst, which caches the data for performance and then uploads the unique data to Blob storage for long-term retention. It’s best to do the deduplication on a separate media server instead of on CloudCatalyst because it allows CloudCatalyst to use all its resources mainly for caching and transferring the data to Blob storage. For restores, data goes through a similar path but in the reverse direction. By default, if the data is still on the media server, then it’s restored from the media server. When restoring data from Blob storage, however, NetBackup will first check for the requested data in the CloudCatalyst cache and if it exists in the cache, send it back from the cache. If data isn’t in the CloudCatalyst cache, it’s retrieved from Blob storage and then passed to CloudCatalyst to recover the data on the client.

### ACCESS APPLIANCE OPTIMIZED DUPLICATION (DEDUPLICATION) DATA FLOW TO –AZURE BLOB STORAGE

In some scenarios, the Access Appliance is in the data path for on-premises mid-term or long-term retention prior to sending data off-premises. When using Access data deduplication with NetBackup, you can duplicate data to the cloud using NetBackup SLP policies and CloudCatalyst. The SLP would specify to duplicate the data from the Access Appliance to CloudCatalyst to send the data to the cloud. Figure 8 shows this approach of sending data to the cloud from Access data deduplication. In this example, deduplicated data is sent to the Access Appliance from the media server, which then does an optimized duplication of the data to the cloud via CloudCatalyst. The role of the media server during the optimized duplication to cloud is to control and orchestrate transfer between the Access Appliance and CloudCatalyst. The actual I/O is between the Access Appliance and CloudCatalyst. You can do a restore either from the Access Appliance (copy 2) or from the Azure copy in the cloud (copy 3). The data path from CloudCatalyst to the Hot or Cool Blob storage access tiers is the same as described in the previous sections. By default, copy 1 is used for restores unless you specify restoring from different copies.

© 2020 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo and NetBackup are trademarks or registered trademarks of Veritas Technologies or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
Cloud Object Storage with Veritas NetBackup and Microsoft Azure

![Diagram of Cloud Catalyst and Azure Blob storage tiers]

**Figure 8.** The Access Appliance data deduplication path to Azure Blob Hot or Cool storage tiers via CloudCatalyst.

Figure 9 shows a sample view of data in an Azure storage account for a traditional duplication. Backup images and associated header information are stored in a directory structure. Each directory contains the image properties, block map file and the actual backup image. The header directory contains the header information, the properties of the header information and the block map file for the header. The NetBackup Azure Cloud plug-in breaks the backup image up into fixed object sizes. With encryption, there is one key per OST image, so there will be additional directories and objects related to the keys.

![Table of backup data without deduplication]

**Figure 9.** A sample view of data backed up to the Azure Blob Archive access tier.

**DISASTER RECOVERY USING AZURE**

**AUTO IMAGE REPLICATION (AIR) TO THE CLOUD – HYBRID CONFIGURATION**

Another option to get data into the cloud would be to use a hybrid model where part of the environment is in the data center and another part is running as a cloud-based service. This setup would use AIR functionality to provide automation and optimization to deliver the data to the cloud for mobility and disaster recovery. (See Figure 10.)
This concept is very simple and ties into a number of these use cases. An organization configures a NetBackup master and media server with MSDP the data center and also configures a master and media server with MSDP in Azure. From there, Auto Image Replication automatically sends data from MSDP in the data center to MSDP or CloudCatalyst in Azure. Metadata is encapsulated as part of the data transfer, so the import into the Azure NetBackup domain is near instantaneous after the data is copied. Organizations have been using this model for global DR protection, such as moving data from a data center in San Francisco to a data center in London, for quite a while. Leveraging this technology for a cloud target is no different—for NetBackup, it’s just another AIR target. This option is ideal for an organization that wants an off-site DR copy of the data and it’s also a good way to migrate to the cloud from a NetBackup perspective.
This section provides an example of how to configure NetBackup to send data to Azure cloud storage as well as how to use the report from Veritas Information Studio within example scripts to generate a backup policy. Because this is only a sample deployment, please refer to the Azure and Veritas product documentation for definitive and specific installation, administration and configuration details.

This example uses a BYOS NetBackup environment that consists of master server, media server and CloudCatalyst server configured as shown in Figure 21.

Figure 21. Sample configuration of NetBackup and NetBackup CloudCatalyst with Azure Blob storage.

This example assumes you’ve configured and installed the Information Studio and NetBackup components. It also assumes you’ve already created the MSDP. The example consists of the following main steps:

1. Create a storage account and note down the access keys from the Azure portal.
2. Create a NetBackup cloud storage server, enable CloudCatalyst and use an Azure Cool access tier as a target.
3. Create an SLP definition where backup and deduplication are done on a media server and placed in an MSDP, then duplicated to the cloud storage server (Cool access tier) identified in the previous step.
4. Create a backup policy and modify the backup policy to use the SLP.
5. Run a manual backup.
6. Verify backup and duplication.
7. Generate the *.csv report using Information Studio’s GUI based on preconfigured filters.
8. Extract the file path from the report and create file paths that can be fed into NetBackup backup policies.
9. Use a script to create a backup policy defined above to include the file paths from the report.
Log on to the Azure portal and create a storage account for use with NetBackup. You’ll use the access keys to configure the Azure CloudCatalyst storage server within NetBackup. Storage accounts that support Hot or Cool access tiers and Block blobs are a requirement for configuring CloudCatalyst.

1. Log on to the Azure portal. Click on the main menu icon, hover over Storage accounts, then click the Create button. On the next page, click the + Add button to create a storage account and select the Azure subscription.

2. Select additional values for creating the Storage Account:
   - Choose an existing Resource Group or create a new one.
   - The Storage account name must be globally unique across all of Azure and contain only lowercase letters or numbers.
   - Select the Azure Location and set the Performance as Standard; this selection lets NetBackup create Block Blobs.
   - Choose an Account kind that supports Hot or Cool access tiers.
   - Under Replication, Azure lets you select the storage redundancy type to provide different levels of durability.
   - Note that CloudCatalyst supports only Hot or Cool access tiers.

If you need to do additional fine tuning, choose the Next button to configure Networking, Tags or other Advanced settings. To use the defaults, click the Review + create button to display a summary of selected values. Once the input settings are verified, a green bar indicates successful validation.

Click the Create button at the bottom of the page to initiate creation of the storage account.
3. Locate the nbstorhot storage account we just created.
   Choose Access keys from the menu on the left. Of the two keys—key1 and key2—select one value for configuration.
   Use the copy buttons/icons on the right to minimize errors when entering these values into the NetBackup cloud storage wizard.

CREATION OF NETBACKUP CLOUDCATALYST STORAGE

In this example, NetBackup is configured to send data to the Azure Cool access tier via CloudCatalyst.

1. Log on to the NetBackup administration console. Click on Configure Cloud Storage Server and then click Next.

2. Select Microsoft Azure as the Storage API type; then select Microsoft Azure as the Cloud storage provider.
3. Configure the cloud storage server:
   - Enter a **storage server name** for the **CloudCatalyst server**; this name should **not** be resolvable on the network.
   - For **Media server name**, from the dropdown list, choose a Linux media server supported for CloudCatalyst. This media server should not have any existing CloudCatalyst or MSDP configuration present.
   - Designate an empty volume on this media server as the **CloudCatalyst Cache Directory**.
   - Enter the values for the storage account and access key identified previously in Step 3 of the Azure section of this Appendix and then click **Next**.
4. Select **ACCOUNT_ACCESS_TIER** as the preferred access tier for Microsoft Azure and then click **Next**.

5. Azure data at rest is encrypted by default; however, the option to enable encryption using the NetBackup Key Management Server is available. Click **Next** to advance to the next screen where you can review the options selected for CloudCatalyst configuration. Clicking **Next** once more begins the CloudCatalyst storage server configuration.
6. Once you’ve completed the cloud storage server configuration, the following dialog box appears. Click **Next** to launch the Disk Pool Configuration Wizard. Click the **Add New Volume** button to create a cloud volume in the storage account for NetBackup data.
On the next screen, enter a **Container name** and click **Add**. Select the newly created container you just added and click **Create**.

7. Select the newly created volume and click **Next**. Enter the **Disk Pool name** and click **Next**. Review the **Disk Pool Configuration Summary** and click **Next**.
8. After you’ve created the disk pool, click **Next** to continue with storage unit creation, then click **Next** followed by **Finish**.
CREATION OF STORAGE LIFECYCLE POLICY (SLP) DEFINITION

In this example, you’ll create an SLP to first back up data to an MSDP and then to the CloudCatalyst storage server you created in the previous section. This example assumes you've already configured an MSDP on another media server in the environment.

1. Right-click on Storage Lifecycle Policies under NetBackup Management > Storage and select New Storage Lifecycle Policy.

2. Enter the Storage lifecycle policy name LTR-msdp-2-cloud. Click Add and select the Operation to be Backup. Select the Destination storage to be the MSDP storage unit (for example, msdp-stu-onprem-copy). Click OK to finish adding the first storage destination.

3. Click Add again. In the next pane, select the Operation to be Duplication and the Destination storage to be the CloudCatalyst...
4. Click **Ok** and the defined SLP appears on the right-side pane.
CREATION AND MODIFICATION OF THE BACKUP POLICY TO USE THE SLP

This section describes how to create a backup policy and then modify the backup policy attribute to use the SLP you defined in the previous step.

1. Click on Policies on the left pane and then right-click on the right pane and select New Policy. Enter the Policy name, place a check in Use Policy Configuration Wizard and click OK. Follow the wizard.

2. Select the policy type. In this example, we’ve selected Standard. Enter the client information in next screen and click Next.

3. Select the Backup Selection List and click Next. In the next screen, select the Backup Type and click Next.
4. Enter the **Frequency and Retention** from the dropdowns. Click **Next** and **Next**.
5. Double-click on the new created policy, select the **Attributes** tab and modify the attribute **Policy storage** to use the SLP you created in the previous section.

VALIDATE PROTECTION USING SLP

Validation of the configuration involves running a manual backup that would follow the SLP defined in the previous section. Based on the policy, it will first do a backup and place the deduplicated data on the MSDP. Afterward, it will duplicate the data to the cloud.

1. Right-click on the backup policy and select **Manual Backup**. Click **Ok**.
2. Click on Activity Monitor on the left-side pane. Wait for the backup and duplication job to finish.

3. Log on to the Azure portal, select Storage accounts, then choose the nbstor storage account, the container (or cloud volume named) azr-cc-nb82media-svr used to store NetBackup data.

ADDITIONAL INFORMATION FOR AZURE Solution Templates

WHITEPAPER – NetBackup Guidelines for AZURE deployments
DISCLAIMER

THIS PUBLICATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTEES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. VERITAS TECHNOLOGIES LLC SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS PUBLICATION. THE INFORMATION CONTAINED HEREIN IS SUBJECT TO CHANGE WITHOUT NOTICE.

No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

ABOUT VERITAS TECHNOLOGIES LLC

Veritas Technologies empowers businesses of all sizes to discover the truth in information—their most important digital asset. Using the Veritas platform, customers can accelerate their digital transformation and solve pressing IT and business challenges including multi-cloud data management, data protection, storage optimization, compliance readiness and workload portability—with no cloud vendor lock-in. Eighty-six percent of Fortune 500 companies rely on Veritas today to reveal data insights that drive competitive advantage. Learn more at http://www.veritas.com/or follow us on Twitter at @veritastechllc.