

eBook

Azure Storage Guidebook: Tips, Tricks, and Best Practices



Executive Summary

The Azure cloud has redefined the way enterprises consume and manage storage for their applications. Moving away from the constraints of block storage, applications now have many options to choose from: object storage, messaging queue storage, file storage, cold / hot tiers of storage, and more. There are additional benefits that cloud brings into the picture for storage: scalability to accommodate petabytes of data, agility of integrating with existing processes, and the benefits of pay-as-you-go model to name just a few.

Organizations are allocating approximately [30% of IT budgets](#) for cloud adoption and this underlines the trend of cloud adoption. It comes as no surprise that Gartner forecasted the cloud revenues to grow by 17% in 2020, with IaaS services comprising compute and storage services slated for 24% growth year over year.

This unprecedented growth rate compared to other services is attributed to the fact that modern applications have outgrown the constraints of legacy data centers. The need of the hour is for compute and storage services agile enough to meet the rapidly evolving application requirements.

Azure-based object, block and file storage solutions are preferred by SMB and enterprises alike due to the uncompromised quality and diverse set of features available to customers at the click of a button. However, understanding which is the right storage that fits the application and the best practices for each of these storage options in the cloud is complex enough to be considered a project in itself.

This guidebook will demystify these storage options and focus on the best practices to be followed while adopting Azure storage services for your enterprise workloads.

Table of Contents

Executive Summary	1
Understanding Cloud Storage Types in Azure	3-4
How to Make Best Use of Azure Cloud Storage	5
Scalability and High Availability	5
Performance	6-7
Security	8
Cost Control	9-10
Data Protection and Disaster Recovery	11
Get More from Azure Storage using Cloud Volumes ONTAP	12
Cloud Volumes ONTAP Case Studies	13
Boosting Innovation at Mellanox	13
Financial Services Company Meets Increased VDI Demands During Covid-19 Crisis	14
Optimizing the Cloud for Innovation at McKesson	15
Conclusion	16

Understanding Cloud Storage Types in Azure

Legacy on-premises storage systems are restricted to hard disks available to servers: either connected directly or over network. There is a new generation of born-in-the-cloud storage services that give a never-before-seen flexibility to how storage can be consumed by applications.

Let's explore some of the different storage types in Azure and where they would fit into your IT solution landscape.

- **Azure Blobs**

Azure Blob offers object storage for unstructured data. It is an ideal storage type for images or video files for websites. It can also be used as an inexpensive storage option for your backup, log, and archival data. Azure Blob is also widely used in data analytics applications, either independently or by integrating with Azure Data Lake storage service.

- **Azure Disks**

Azure Disks is the managed block storage service available in Azure. The service provides managed disks that can be attached to compute services such as virtual machines and containers in Azure. They are similar to the physical and virtual disks attached to on-premises machines, but with all underlying provisioning processes abstracted from the user.

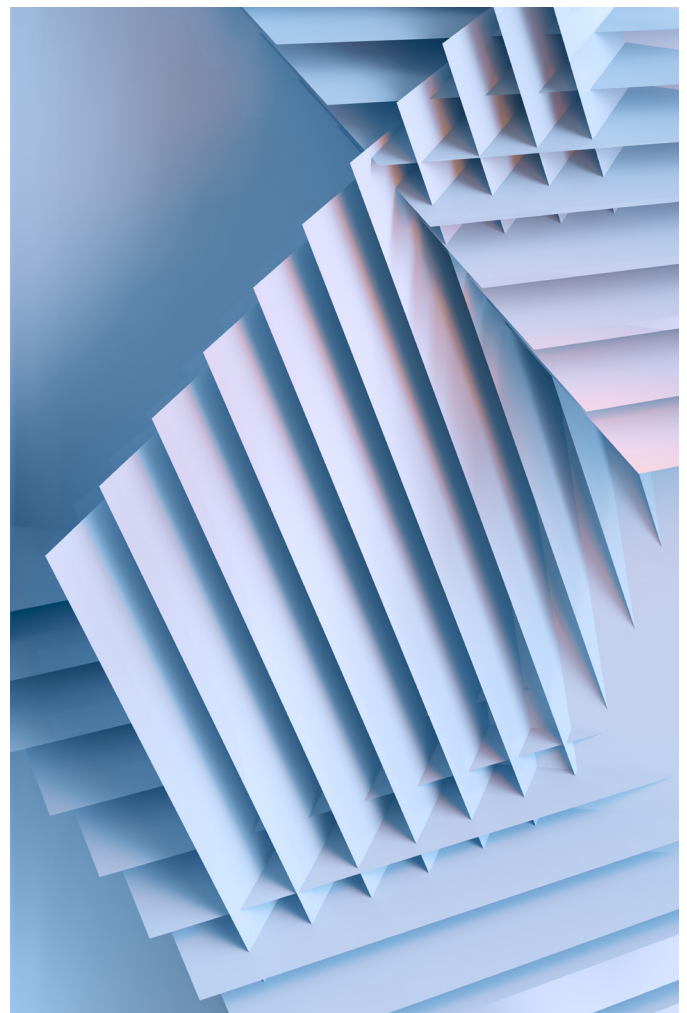
Customers can choose from HDD- or SSD-based disk SKUs depending on their application's specific storage requirements. There are four such SKUs available for customers: Standard HDD, Standard SSD, Premium SSD, and Ultra disk. Of these four options, Standard HDD is best suited for your non-critical data storage, Standard SSD best for lightly used applications and web services, and Premium SSD and Ultra Disks are suitable for production systems with high IOPS requirements.

- **Azure Files**

Azure Files is the managed SMB file share service in Azure, parallel to file shares on-premises. Azure Files file shares can be mounted to Windows, Linux, and MacOS machines that support the SMB protocol. The service is widely adopted by organizations looking forward to replacing their existing file servers during cloud adoption using cloud native service.

- **Azure NetApp Files**

Azure NetApp Files (ANF) is a fully managed cloud service with Azure portal integration and access via REST API and Azure SDKs. Customers can seamlessly migrate and run applications in the cloud without worrying about procuring or managing storage infrastructure.



Azure Files eliminates the need for ongoing administration of multiple file servers in the cloud for shared file requirements. In hybrid deployments, Azure Files can be complemented with the Azure File Sync service, which replicates and caches file share data nearest to the location where it is used, i.e. either on-premises or in the cloud. Azure Files are commonly used when performing lift and shift cloud migrations of applications that have a dependency on file shares. It can also be used to store shared data such as application settings, diagnostics logs, and tools.

Azure NetApp Files makes it easy for enterprise to migrate and run complex, performance-intensive and latency-sensitive applications with no code-change. ANF is widely used as the underlying service in Migration of POSIX compliant Linux and Windows applications, SAP HANA, Databases, HPC infra and apps, and web-apps.

In addition to these four storage services, Azure also provides other two storage services: Azure Queues and Azure Tables. The Azure Queues service is used for storing messages that are shared between application components which can be accessed over HTTP or HTTPS calls. Azure Tables is used for storing structured NoSQL data in the cloud for applications handling schemaless data.



Azure Storage: Quick Hits

- **Azure Blob**
inexpensive object-based storage suitable for archive, infrequently used active data, backup.
- **Azure Disk**
a managed premium block-based storage for high performance workloads such as applications.
- **Azure Files**
offers file shares managed by Azure over the SMB protocol to serve the needs of databases, applications, and more.
- **Azure NetApp Files**
Run performance-intensive and latency-sensitive Linux and Windows file workloads in Azure.



How to Make Best Use of Azure Cloud Storage

Once the right storage solution is identified for your workload, the next step is to deploy them as per the best practices recommended for the service. Microsoft has documented these best practices extensively for different types of Azure cloud storage; however, it's important to align these best practices with the target use cases in order to implement the best fit solution.

Scalability and High Availability

Like all other Azure services, cloud storage also has scalability targets defined by Microsoft. These scalability targets include the number of storage accounts per region/subscription, supported ingress, egress, and request rates, and more that should be taken into consideration while planning which storage services are right for your application in Azure.

Multi-tenancy

Consider the situation with multi-tenancy. In this case, data isolation is paramount, and as such customers tend to opt for multiple storage accounts, thereby exhausting the scalability limit of their storage accounts per region or subscription. To avoid this situation, the recommended best practice is to use Azure Blob storage and apply RBAC roles at the container level. This helps improve the security of your application in Azure by protecting it against unauthorized data access and usage.

Storage throughput

Another use case where multiple storage accounts are used is when there is a possibility that ingress/egress, capacity, or IOPS limits won't meet the application requirements. The default limits can be increased by contacting Azure support. If it still doesn't meet the application scalability requirements, multiple storage accounts can be considered. This helps in meeting your application storage throughput requirements, whether they fall within the storage scalability limits or not.

Bandwidth

To overcome bandwidth limitations, customers can use client-side compression of data, which compresses data before sending data to the cloud storage account. If the constraints still exist, it is recommended to switch from object storage to block storage solutions, as block storage supports higher IOPS. These best practices help to meet the performance targets associated with your applications and ensure smooth customer experience.

Redundancy

Azure storage offers data replication capabilities through locally-redundant storage (LRS), geo-redundant storage (GRS), and zone-redundant storage (ZRS), where multiple copies of data are stored across Azure regions, geographies, or availability zones respectively to ensure resiliency. While it is important to select the highest resiliency level offered by GRS (across regions) for production workloads assured by an SLA of 99.99999999999999% (16 nines) development and test environments can be configured to use LRS replication type to reduce the overall cost of the solution. This will help in achieving the most stringent storage resiliency and improve availability SLAs for your Azure workloads.



Performance

The performance of your workloads depends on the performance of the storage where the data resides. Consider the following best practices for getting the best performance outcomes from Azure storage.

- **Storage tier**

Azure offers two performance tiers for block and file storage: Premium and Standard. They are differentiated by the usage of HDD and SSD drives in the backend for Standard and Premium tiers respectively. Premium tier is costlier and can be considered in scenarios where high throughput, low-latency storage is required—such as for production databases, machine learning workloads, data analytics, e-commerce applications, etc. Standard storage, on the other hand, serves as a cost-effective storage with acceptable performance levels for use cases involving large data sets like images and videos, backup and archival data, and bulk data processing. Choosing the right storage tier helps in achieving the fine balance between performance and cost optimization for storage in Azure.

- **VM Network bandwidth**

All Azure VM SKUs have a supported bandwidth and storage throughput associated with them. While attaching high throughput premium disks to Azure VMs, it should be ensured that the throughput supported by the disk is not throttled by what is supported by the VM. The same consideration is applicable for network bandwidth also. For example, VMs accessing blob storage accounts over network should not be throttled by the supported bandwidth for the selected SKU. Choosing the right VM Network bandwidth configuration will help enhance the application performance by enabling it to benefit from the full potential of underlying storage.

- **Latency management**

When there are multiple dependent resources in an architecture, they can be placed in the same Azure regions to reduce network latency and deliver better performance. As inter-region bandwidth usage is free, it will also help in reducing the overall cost. When the storage content is being accessed from multiple geographies, Azure Content Delivery Network (CDN) can be leveraged to cache data in Point of Presence (POP) locations to reduce access latencies. This will noticeably improve user experience as data loads faster and information is made accessible to customers without delays.

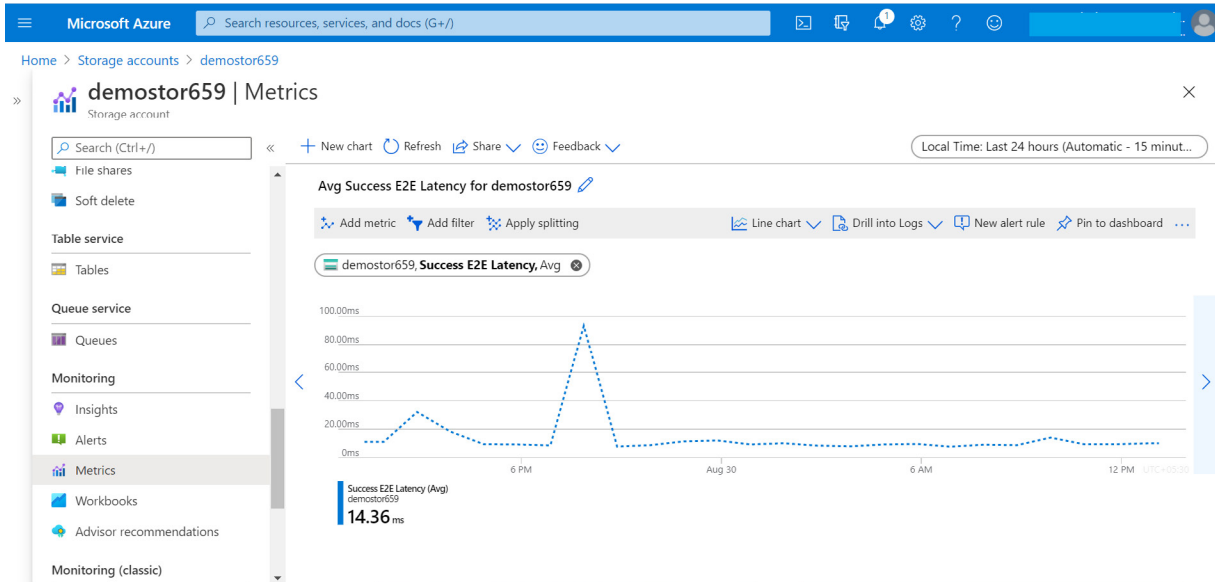
- **Monitor and optimize**

In addition to implementing the above best practices for performance, customers should also look at identifying the right signals for monitoring performance of storage and latency. This will help in identifying bottlenecks and optimize the deployments further.

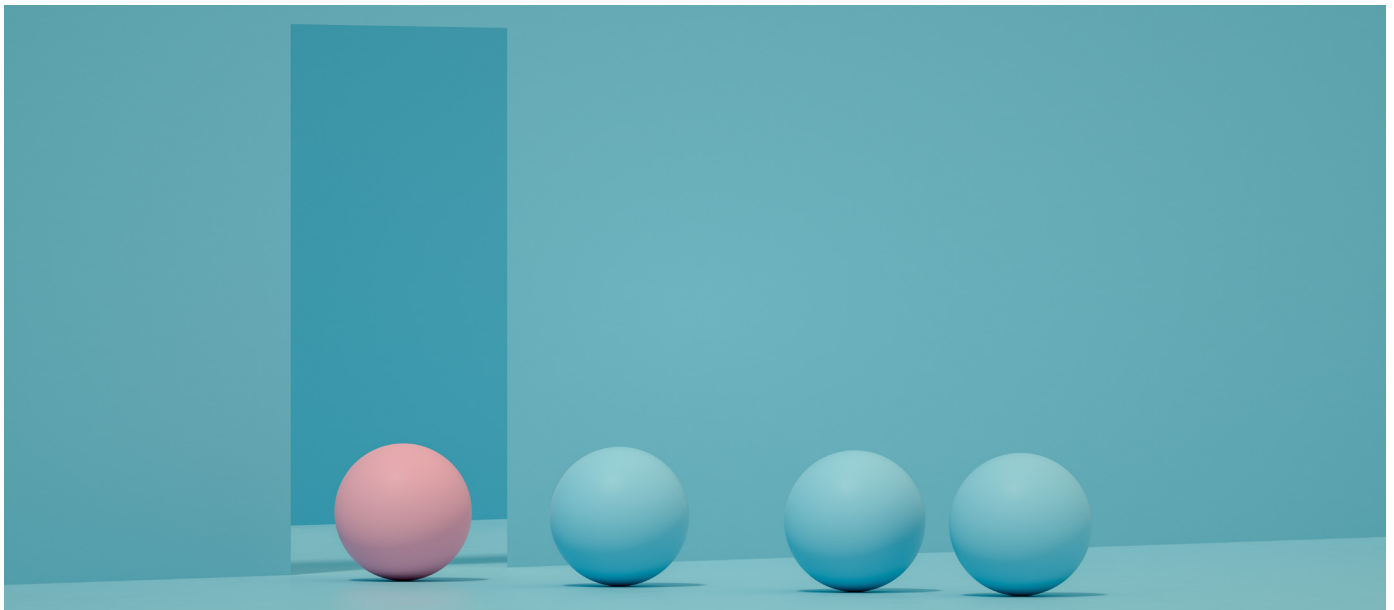


Azure Content Delivery Network

By bringing data closer to users, Azure Content Delivery Network (CDN) makes it possible to increase the user experience by cutting download time, optimizing bandwidth usage, and increasing performance. This makes websites and applications faster, easier to use, and operate.



Azure storage latency monitoring



Security

Security management of storage accounts include configurations to be done at the control plane and data plane.

Access control

At the control plane, the principle of least privilege should be applied using restricted Azure RBAC roles, provisioning administrators or users with limited access to perform only the activities they need to do. Regularly rotating storage keys is another best practice to adhere to for storage accounts. The access can be further restricted with the use of SAS tokens, which ensure secure communication over HTTPS using a SAS token for a limited period of time.

Network layer protection

Additional security can be enforced by limiting access to storage accounts from specific networks using firewalls or services using [Azure service tags](#). Azure Private Link can be used to keep the communication to Azure storage restricted to resources within a VNET. The traffic remains in the Azure backbone network and is hence secured.

Security at-rest and in-transit

Security of data in transit can be ensured by enabling the “Secure transfer required” option for storage accounts, which permits only HTTPS communication. Encryption of data-at-rest is enabled by default for Azure storage. The process is FIPS 140-2 compliant and is done transparently using 256-bit AES encryption. The default process is to use Microsoft-managed keys for encryption. Customers can also choose to bring their own encryption keys and integrate them with Key Vault or other key stores.

Azure Security Center recommendations

Azure Security Center provides security recommendations based on Azure storage best practices from Microsoft. To ensure holistic security of the storage services used by applications, customers should review these recommendations and follow the remediation guidelines.

Azure Private Link

Azure Private Link works as a direct and restricted link between Azure and a user’s virtual network, or other private assets or partner services. By limiting the exposure points of data to the public internet, Azure Private Link makes network connections more secure and easier to use.

The screenshot shows the Azure Security Center interface. The top navigation bar includes the Microsoft Azure logo and a search bar. Below the navigation bar, the breadcrumb path is 'Home > Security Center'. The main heading is 'Security Center | Data & storage'. A search bar is present with the text 'Search (Ctrl+/)'. The left sidebar contains a navigation menu with categories: 'Security policy', 'Regulatory compliance', 'RESOURCE SECURITY HYGIENE', 'Recommendations', 'Compute & apps', 'Networking', 'IoT Hubs & resources', 'Data & storage' (highlighted), 'Identity & access', 'Security solutions', 'ADVANCED CLOUD DEFENSE', 'Adaptive application controls', and 'Just in time VM access'. The main content area shows a table of storage accounts under the heading 'SQL Information Protection'. The table has columns for 'Name', 'Total', and 'Severity'. All accounts listed have a severity of 'None'.

Name	Total	Severity
teststor1110	None	None
sqlbkupstor1	None	None
demostore511	None	None
demostor707	None	None
demostor659	None	None
dataupload101	None	None
csgcc6c06d7a64ax425exb50	None	None
csg10032000c8d98f45	None	None
csg10032000e990b4a	None	None

Security Center storage view

Cost Control

With petabytes of data moving to the cloud, managing the costs of cloud storage requires careful planning and adherence to recommended guidelines to ensure storage economy.

- **Storage tiering**

Azure Blob storage offers hot, cool, and archive tiers to store data in a cost-effective manner based on their usage. Hot tier has higher storage cost but lower access charges. Plan to use hot access tier storage for your frequently accessed production data to minimize the access charges. The costs for storing on cool access are considerably lower, however, they do come with higher access charges than those on the hot access tier. Archive tier is the cheapest storage tier available in Azure. It is recommended to leverage this storage tier for use cases such as long-term archival data sets. Planning the right storage tier for your application data can help in long term cost benefits. For example, 5 TB of data stored in the archival tier will incur a monthly storage cost of \$5.07 only, while the same data in the cool and hot tier will incur charges of \$77.82 and \$106.50, respectively.

- **Storage Lifecycle Management**

Storage lifecycle management helps to automatically tier data to cool and archive tier based on the access patterns. Customers can opt in for storage lifecycle management to optimize the storage cost based on data usage.

- **Azure Cost Management**

Azure Cost Management service helps to review cost distribution of storage accounts and delete/consolidate them based on usage. The service provides detailed views of accumulated costs, usage trends, and a breakdown of costs used by different storage options, i.e. disks, blobs, files, etc. The service also helps to define budgets, monitors usage against the budget, and generates alerts on overages. Customers can leverage Azure Cost Management service for review and optimization of overall Azure cloud storage charges.

- **Azure Advisor**

This service helps to reduce cloud costs by monitoring your environment for unused/idle and underutilized resources. Azure Advisor provides prescriptive cost-reduction guidance for resizing underutilized VMs, deleting unused VMs, moving managed disks snapshots to Standard storage as well as opportunities for storage cost reduction through ephemeral OS disk. The service also monitors usage patterns and provides guidance on possible cost savings through reserved capacity purchase. These recommendations from Azure Advisor help you keep your cloud storage usage and costs under control.



Microsoft Azure | Search resources, services, and docs (G+)

Home > Advisor

Advisor | Cost

Subscriptions: Pay-As-You-Go

All types | Active | No grouping

Total recommendations: 2 | Recommendations by impact: 1 High impact, 1 Medium impact, 0 Low impact | Impacted resources: 2 | Potential yearly savings: 968 USD

For more cost management and optimization capabilities, visit Azure Cost Management

Impact	Description	Quick fix	Potential yearly savings	Impacted resources	Last updated
High	Right-size or shutdown underutilized virtual machines	Quick fix	932.08 USD	1 Virtual machine	8/29/2020, 06:48 PM
Medium	Delete Public IP address not associated to a running Azure resource	Quick fix	35.71 USD	1 Public IP address	8/30/2020, 12:30 PM

Are these recommendations helpful?

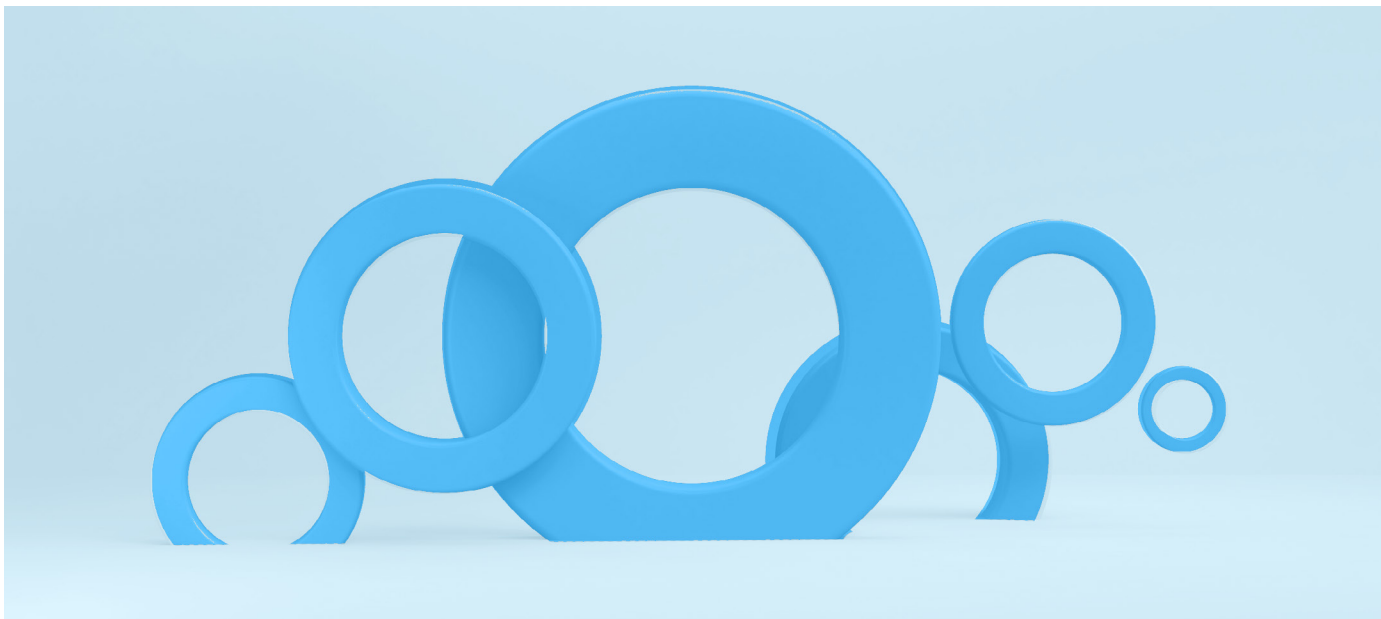
Azure advisor cost recommendations

⚡ Azure Advisor: Quick Hits

- Finds unused/underutilized resources
- Deletes unused VMs
- Moves snapshots to Standard storage
- Monitors and recommends cost optimization

⚡ Azure Cost Management: Quick Hits

- Reviews and reports on costs per storage service
- Recommends deletion or consolidation
- Alerts on usage overages and budget thresholds



Data Protection and Disaster Recovery

Data, irrespective of whether it is stored on-premises or in the cloud, should always be protected from corruption or loss in order to ensure business continuity. Azure offers a number of services to help with data protection and disaster recovery (DR).

- **Cloud-based backup**

Azure Backup is a cloud-based backup solution that can be used to protect data in your VM disks and Azure file shares. The backups are application-consistent by default for Windows VMs and can be configured using pre/post-scripts for Linux.

Azure Backup is a service that can be easily used by customers to protect workloads hosted in the cloud with minimal and no configuration overhead. It is also a cost-efficient solution as you need to pay only for the instances being backed up and also the underlying storage based on usage.

- **Disaster Recovery**

Azure Site Recovery (ASR) is a complete DR solution that protects hybrid workloads from planned and unplanned failures by replicating the data continuously to Azure storage. ASR is application aware and offers near-real time protection for your workloads by enabling a DR site in the cloud. It is an active passive solution that continuously replicates on-premises data to cloud storage. It is recommended to create failover plans that reflect your application architecture for centrally orchestrated failovers when the source environment becomes unavailable due to disasters or planned maintenance.

- **Data Migration**

ASR can also be leveraged for migrating data from on-premises environments to Azure in cloud adoption scenarios, however it needs additional ecosystem of tools and services to be deployed to manage the data transfer.

Azure Backup and ASR incurs cost for each instance being protected along with the storage charges. While integrating ASR and Azure backup to your BC/DR strategy, ensure that the cost aspects are also taken into account along with the prioritization of applications for recovery.



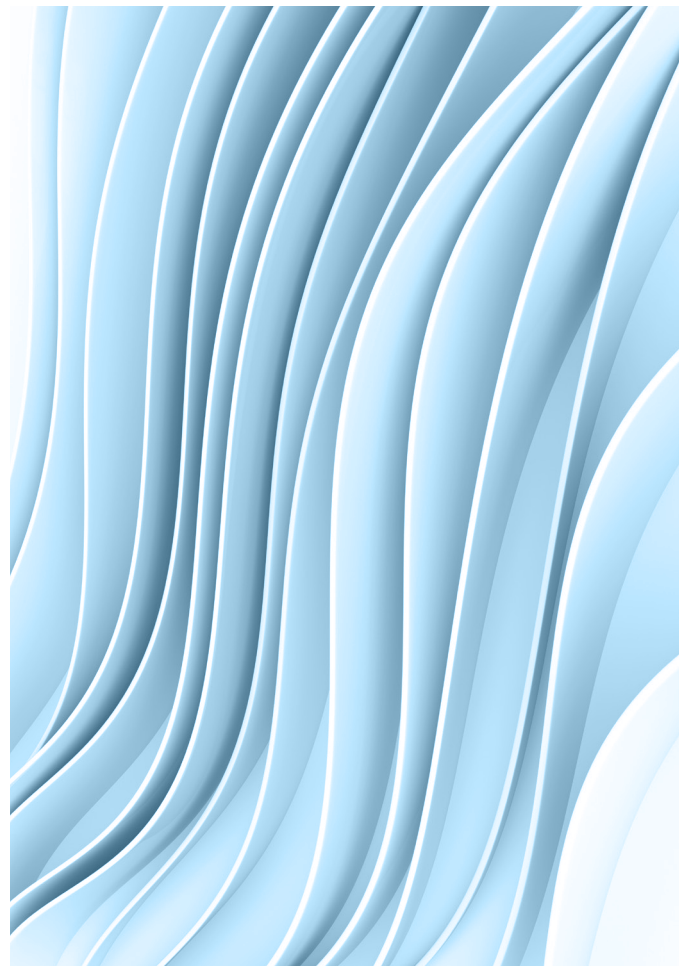
Get More from Azure Storage using Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP delivers enterprise-grade data management capabilities in Azure, bringing the power of the trusted ONTAP storage platform to Azure. The service complements the native storage services and provides a flexible and agile method of configuring and consuming storage for workloads in Azure. Cloud Volumes ONTAP helps you to manage your deployments across hybrid cloud environments seamlessly from a single management pane, thereby reducing administrative overhead.

Cloud Volumes ONTAP helps to reduce storage cost, increase usage efficiency of storage all the while easing the administrative process of Hybrid and on-premises storage management. Some of the features of the service that makes it a preferred storage solution among customers in Azure include:

- **Multiprotocol Access**
Access to storage over protocol of choice—NFS/ CIFS/ iSCSI—allows the same storage service to be configured and used for file share as well as block storage use cases.
- **High Availability**
Ensure redundancy through a highly available dual node configuration.
- **Storage Efficiency**
Proprietary data deduplication, compression, and thin provisioning help to reduce the storage footprint and costs.
- **Data Mobility**
[SnapMirror® data replication](#) seamlessly transfers data from on-premises or other clouds storage to Azure, avoiding vendor lock-in. SnapMirror also helps to set up and continuously synchronize DR environments to Azure.
- **Data protection**
[NetApp Snapshot™ technology](#), creates point-in-time backup copies which are storage efficient and application consistent.

- **High Performance**
Enhanced storage throughput through features like WAFL and cloud data caching, best suited for performance intensive production workloads.
- **Data Tiering**
Tiering data from Azure Disk block storage to object storage automatically to reduce the storage charges and optimize usage.
- **Security and Safety**
Cloud Volumes ONTAP augments and integrates with Azure storage features like encryption at-rest and in-transit, VNET integration for perimeter security and ransomware protection.
- **Compliance**
AI-driven Cloud Compliance add-on scans all your data in Azure in order to map, identify, and report on sensitive private data that could fall under regulatory scope of GDPR, CCPA, and other data privacy legislation.



Cloud Volumes ONTAP Case Studies

Cloud Volumes ONTAP is trusted by thousands of customers all over the world to deliver storage management services for mission critical workloads. Let us look at some of the success stories in Azure where organizations leveraged Cloud Volumes ONTAP to boost their cloud adoption journey.

Boosting Innovation at Mellanox

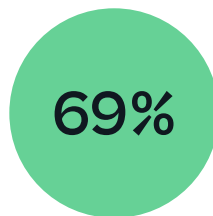


Mellanox Technologies develops networking products, catering to a customer base of enterprise computing, network security, and the finance industry. They were looking for easy integration with on-premises storage, while ensuring reliability, scalability, and cost effectiveness of deployment in the cloud. Mellanox adopted Cloud Volumes ONTAP in production for storing data including MongoDB, production logs, and more.

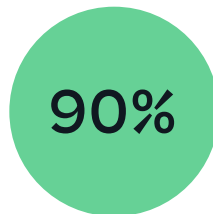
The benefits that Mellanox gained from Cloud Volumes ONTAP were manifold, and included the following:

- Centralized NFS file shares access from all Mellanox locations.
- Leveraged storage efficient data clones for test and development environments using NetApp FlexClone® technology.
- Reduced cloud bills by automatically tiering infrequently-used production data to Azure Blob storage.
- Achieved BC/DR goals by replicating data to the cloud using [SnapMirror®](#) technology.
- Centralized policy configuration and management of data across hybrid environments using unified console of NetApp Cloud Manager

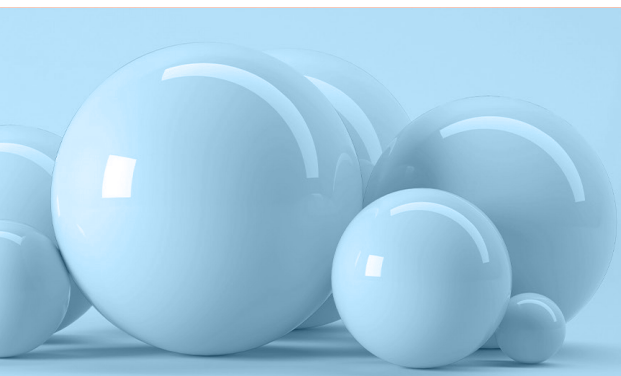
The Mellanox success story



storage reduction



of cold DR data tiered



[Read the full case study here →](#)

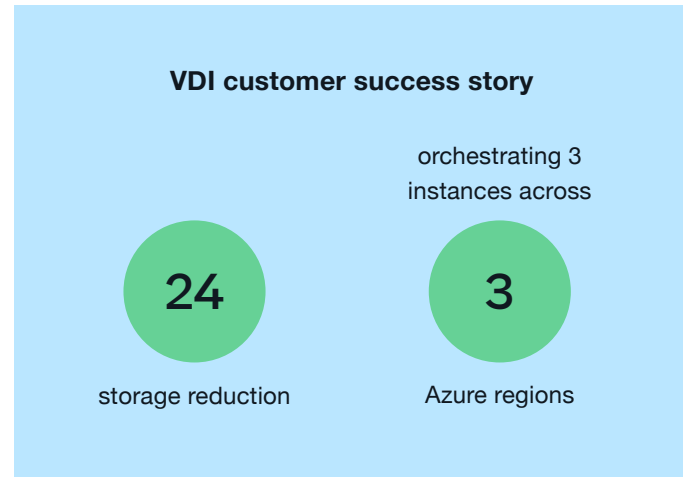
Financial Services Company Meets Increased VDI Demands During Covid-19 Crisis

A US financial advisory company had to ramp up their on-premises VDI deployment to meet the increasing VDI demand during Covid-19 crisis as its global workforce of thousands of employees started working from home overnight.

The VDI solution was already using on-prem NetApp storage for SMB/CIFS file shares. Over a period of 24 hours, the IT team was able to burst out the environment to Azure by deploying Cloud Volumes ONTAP instances, replicating data from on-premises volumes to Cloud Volumes ONTAP, and configuring the VDI solution in the cloud.

The quick turnaround of the solution helped the company achieve the following:

- Agility to scale up and meet increased VDI requirements on-demand in an extremely short period of time.
- Quick and secure transfer of data to cloud with no reconfiguration or reformatting through SnapMirror data replication.
- continued protection of data in the cloud using point-in-time incremental backup using NetApp Snapshot technology.



**Read the full
blog post on this
case study here**

[Read now](#)



Optimizing the Cloud for Innovation at McKesson



McKesson is the largest healthcare company in the US, distributing one third of North America's medicine supply. With a renewed focus on innovation, companies in the healthcare industry like McKesson require the highest level of technological support to drive their discoveries and products. McKesson had been relying on a private cloud infrastructure that couldn't keep up with those demands and saw that it was time to move to the cloud. They did so with the help of NetApp and Cloud Volumes ONTAP.

With a focus on developing applications to drive their healthcare innovations, McKesson relies on Cloud volumes ONTAP to:

- Orchestrate data replication and mobility across its hybrid deployment with SnapMirror NetApp Cloud Manager.
- More IT flexibility and responsibility, allowing developers and business units to get products to market faster.
- Provide seamless, automatic disaster recovery failover and failback.
- Reduce their overall cloud data storage costs.

McKesson customer success story



Lower cloud storage costs



Faster time to delivery

[Read the full case study here →](#)

Conclusion

Implementation of best practices is paramount to ensure optimal return on investment in Azure cloud storage. Enhancing the Azure cloud storage landscape by leveraging Cloud Volumes ONTAP is another best practice that helps towards this end. The enterprise class data management features of Cloud Volumes ONTAP, along with a deployment aligned with Azure storage best practices will help you achieve your cloud storage efficiency goals. A best fit solution for both cloud-only and hybrid deployments, Cloud Volumes ONTAP enhances the availability, security and performance of cloud storage while reducing the cloud storage costs significantly.

**Sign up for a
free trial now to
learn about the
advanced data
management
capabilities of
Cloud Volumes
ONTAP**

Start now



Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 1994–2020 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

NA-000-1220