



Technical Report

Citrix Profile Management with Azure NetApp Files

Best practices guide

Frank Anderson, NetApp
Loay Shbeilat, Citrix
June 2021 | TR-4901

In partnership with



Abstract

The document covers guidance and best practices for using Citrix User Profile Manager to manage user profiles on Azure NetApp Files as the back-end storage location. The primary objective of this document is to provide you the necessary information to determine the best way to deploy User Profile Manager with Azure NetApp Files.

TABLE OF CONTENTS

Introduction	4
Azure NetApp Files	4
Service levels	4
Monitoring.....	5
Citrix Profile Management.....	7
Key features	7
Profile Management configuration	7
Monitoring.....	8
Test methodology	8
Test environment setup	9
Test runs	10
Test results	11
Throughput	12
Latency.....	14
Profile load time	15
Analysis of the results.....	16
Azure NetApp Files performance and capacity tiering.....	16
Service levels for Azure NetApp Files	17
Integrated data protection.....	18
Storage management and cost optimization	19
Conclusion	20
Where to find additional information	20
Version history.....	20

LIST OF TABLES

Table 1) GPO settings for Profile Management.....	7
Table 2) Static configurations during test runs.	8
Table 3) Testing variables and values.	8
Table 4) Test runs and variables.	10
Table 5) Average profile load times.....	16

LIST OF FIGURES

Figure 1) Read IOPS.....	5
Figure 2) Write IOPS.....	5

Figure 3) Average read latency.	6
Figure 4) Average write latency,	6
Figure 5) Average read throughput.	6
Figure 6) Average write throughput.	6
Figure 7) Test environment setup.	10
Figure 8) Test results – Read IOPS.	11
Figure 9) Test results – Write IOPS.	11
Figure 10) Test results – Total IOPS.	12
Figure 11) Test results – Read throughput (MBps).	13
Figure 12) Test results – Write throughput (MBps).	13
Figure 13) Test results – Total throughput (MBps).	14
Figure 14) Test results – Read latency (in milliseconds).	15
Figure 15) Test results – Write latency (in milliseconds).	15
Figure 16) Moving average over the previous minute of profile load time during test runs.	16
Figure 17) Azure NetApp Files performance and capacity tiering.	17
Figure 18) Throughput limits for each service level and examples.	18

Introduction

This document discusses the Citrix, Microsoft, and NetApp® components, describes test methodology, and reports the test results along with an analysis of the findings. It also provides guidance about key deployment decisions. Finally, additional information regarding securing, protecting, and migrating your user profile data is provided.

Azure NetApp Files

The Azure NetApp Files service is an enterprise-class, high-performance, low-latency, metered file storage service. It is publicly hosted Azure native, first-party portal service for enterprise NFS and SMB file services based on NetApp ONTAP® technology. Azure NetApp Files supports any workload type and is highly available by default. You can select service and performance levels and set up NetApp Snapshot™ copies through the service.

Azure NetApp Files is completely integrated into the Azure data center and portal. Customers can use the same comfortable graphical interface and API to create and manage shared files as with any other Azure service and hosted workload type, including Citrix. Azure NetApp Files provides NetApp enterprise-class storage and delivers many of the same data management capabilities:

- The ability to easily create and resize volumes.
- Adapting capacity and performance without downtime.
- Creating space-efficient storage Snapshot copies and clones in seconds.

The services are very valuable when used to optimize Citrix Virtual Apps and Desktops service (CVADS) on Azure.

Azure NetApp Files is a highly efficient file storage service from Azure. It can provide up to 450,000 IOPS per volume and submillisecond latency, capable of supporting extremely large scale of Citrix virtual apps and desktops deployments. You can adjust the bandwidth and change the service level of your Azure NetApp Files volumes on demand almost instantaneously without pausing I/O while retaining data plane access. This capability enables you to easily optimize your Citrix deployment scale for cost. You can also create space-efficient, point-in-time volume Snapshot copies without affecting volume performance. This capability makes it possible for you to roll back individual user data files using a copy from the `~snapshot` directory, or to instantaneously roll back the entire volume immediately using the volume revert capability. With up to 255 (rotational) Snapshot copies in place to protect a volume from data loss or corruption, administrators have many chances to undo what has been done.

Service levels

Azure NetApp Files has three different service levels with different costs and performance characteristics. Service levels are an attribute of a capacity pool. They are defined and differentiated according to the allowed maximum throughput for a volume in the capacity pool based on the quota that is assigned to the volume.

Supported service levels

Azure NetApp Files supports three service levels: Ultra, Premium, and Standard.

- **Ultra storage.** The Ultra storage tier provides up to 128MiBps of throughput per 1TiB of capacity provisioned.
- **Premium storage.** The Premium storage tier provides up to 64MiBps of throughput per 1TiB of capacity provisioned.
- **Standard storage.** The Standard storage tier provides up to 16MiBps of throughput per 1TiB of capacity provisioned.

Throughput limits

The throughput limit for a volume is determined by the combination of the following factors:


- The service level of the capacity pool to which the volume belongs.
- The quota assigned to the volume.
- The quality of service (QoS) type (auto or manual) of the capacity pool.






Monitoring





You can use Azure Monitor to view the key metrics on your Azure NetApp Files volumes to make usage adjustments accordingly. For storage monitoring, IOPS, throughput, and latency metrics should be closely observed. To enable these metrics, in the Azure portal select the storage account and then select Metrics from the Storage Account blade. The key metrics we used to monitor the performance of Azure NetApp Files during the test are as follows:

Read IOPS: The number of reads to the volume per second. To add this metric, click Add metric and set the scope to the volume name. Set the namespace to NetApp Volumes standard metrics then select Read IOPS as the metric and Avg as the aggregation type.

Figure 1) Read IOPS.


Avg Read iops for smb1 






 Add metric  Add filter  Apply splitting  Line chart 





Scope	Metric Namespace	Metric	Aggregation
 smb1	NetApp Volumes stand... 	Read iops 	Avg 

Write IOPS: The number of writes to the volume per second. To add this metric, click Add metric and set the scope to the volume name. Set the namespace to NetApp Volumes standard metrics then select Write IOPS as the metric and Avg as the aggregation type.

Figure 2) Write IOPS.


Avg Write iops for smb1 






 Add metric  Add filter  Apply splitting  Line chart 





Scope	Metric Namespace	Metric	Aggregation
 smb1	NetApp Volumes stand... 	Write iops 	Avg 

Average read latency: The average time for reads from the volume in milliseconds. To add this metric, click Add metric and set the scope to the volume name. Set the namespace to NetApp Volumes standard metrics then select Average read latency as the metric and Avg as the aggregation type.

Figure 3) Average read latency.


Avg Average read latency for smb1 






 Add metric  Add filter  Apply splitting  Line chart 





Scope	Metric Namespace	Metric	Aggregation
 smb1	NetApp Volumes stand... 	Average read latency 	Avg 

Average write latency: The average time for writes from the volume in milliseconds. To add this metric, click Add metric and set the scope to the volume name. Set the namespace to NetApp Volumes standard metrics then select Average write latency as the metric and Avg as the aggregation type.

Figure 4) Average write latency,


Avg Average write latency for smb1 






 Add metric  Add filter  Apply splitting  Line chart 





Scope	Metric Namespace	Metric	Aggregation
 smb1	NetApp Volumes stand... 	Average write latency 	Avg 

Average read throughput: The average throughput for reads from the volume in MiB/s. To add this metric, click Add metric and set the scope to the volume name. Set the namespace to NetApp Volumes standard metrics then select Average write latency as the metric and Avg as the aggregation type.

Figure 5) Average read throughput.


Avg Read throughput for smb1 






 Add metric  Add filter  Apply splitting  Line chart 





Scope	Metric Namespace	Metric	Aggregation
 smb1	NetApp Volumes stand... 	Read throughput 	Avg 

Average write throughput: The average throughput for writes from the volume in MiB/s. To add this metric, click Add metric and set the scope to the volume name. Set the namespace to NetApp Volumes standard metrics then select Average write latency as the metric and Avg as the aggregation type.

Figure 6) Average write throughput.

Avg Write throughput for smb1 

 Add metric  Add filter  Apply splitting  Line chart 

Scope	Metric Namespace	Metric	Aggregation
 smb1	NetApp Volumes stand... 	Write throughput 	Avg 

Citrix Profile Management

The use of Citrix Profile Management greatly enhanced the end-user experience during our testing. Citrix Profile Management is designed to remove profile bloat and significantly speed log-in times, while reducing profile corruption. Citrix Profile Management is a feature of CVADS.

Key features

The key features of Citrix Profile Management that provide a great end-user experience when Azure NetApp Files is used for the back end storage are as follows:

Profile streaming: Files and folders contained in a profile are fetched from the user store to the local computer only when they are accessed by users after they have logged in. Profile streaming significantly reduces the log in time by reducing the amount of data that is copied down to the local profile at user login. This setting is enabled by default and decreases the amount of IOPS and throughput incurred by Azure NetApp Files; therefore, reducing costs and improving login time.

Active write-back: Files and folders that are modified can be synchronized to the user store in the middle of a session before logout. Usually, these mid-session writes occur about every 5 minutes. Enabling this setting provides Azure NetApp Files with a more consistent stream of write traffic, instead of having it all hit at logout. This frequent write-back resolves the “last writer wins” issue when users are accessing their profile from multiple devices simultaneously.

Large file handling: To improve login performance and to process large-size files, a symbolic link is created instead of copying files in this list. You must configure the paths where the files are stored but you can use wildcards. This setting is a must-have when using the transactional tier and highly recommended for the premium tier.

Profile Management configuration

For the testing, each of the Citrix hosts had the Multi-session OS Virtual Delivery Agent (VDA) 2006 installed. During installation, on the Additional Components window, both the Citrix User Profile Manager and Citrix User Profile Manager Windows Management Instrumentation (WMI) Plugin were enabled.

The Group Policy Object (GPO) settings for Profile Management listed in Table 1 were configured, and the GPO was assigned to all the Citrix hosts being used for the tests.

Table 1) GPO settings for Profile Management.

GPO setting	Value
Active write back	Enabled
Active write back registry	Enabled
Enable profile management	Enabled
Path to user store	\\<ANFSMBVOL>\upmprofiles\%username%
Customer Experience Improvement Program	Disabled
Enable Default Exclusions List – Directories	Enabled
Enable Default Exclusions List – Registry	Enabled
Delete locally cached profiles at logout	Enabled
Local profile conflict handling	Delete local profile
Large File Handling – files to be created as symbolic links	OSTFolder*.ost PSTFolder*.pst

Monitoring

Monitoring the performance can be done through the Citrix Director. The key metric to watch for performance is the profile load time. The profile load time provides the number of seconds it takes for the user's profile to load into the Citrix session. Profile load time includes the amount of time it takes to copy the user's profile down from the profile storage, in this case from Azure NetApp Files. The user profile load time has a significant effect on the user experience and profile load times of greater than 30 seconds usually result in a poor user experience. The profile load time is available through the Citrix Director. From Citrix Cloud Virtual Apps and Desktops Service, select Monitor > Trends > Logon Performance as shown in the following tabs:



The profile load time is available by hovering over the time period being monitored or viewed in the table below the chart.

Test methodology

The primary goal was to assess Azure NetApp Files under a load and determine for a specific workload condition how an SBM-based volume would perform with Citrix Profile Management configured on the Citrix hosts. The settings listed in Table 2 were kept static during the test runs.

Table 2) Static configurations during test runs.

Static configuration	Value
Number of users	1,000
File Share Quota	7TiB
Folder Redirection	Enabled for desktop, documents, and pictures
Large File Handling	4GB OST file updated with Citrix Profile Management large file enabled
Login Rate	1,000 users per hour or one login every 3.6 seconds
User Profile Size	4.7GB, 400 files

The following test variables in Table 3 were decided on after assessing performance during a wide variety of test runs of different configurations:

Table 3) Testing variables and values.

Variable	Values to test
Azure NetApp Files SL	Standard
Files updated per hour	20,000 files 40,000 files 60,000 files 80,000 files 100,000 files

To simulate many users with few resources, we designed a test that used a custom PowerShell script which randomly updated various files stored either in the user's redirected folder (87.5%) or in the user's local profile (12.5%). This script when run by a single-user would be updating between 20 and 100 files

(depending on the number of files per hour to update) in the session along with updating the 4GB OST file stored in the local profile folder. To control the launch rate and provide random wait times during the session, we used LoginVSI for test framework. The random waits helped prevent the predictable spikes in network traffic caused by users logging on simultaneously and helps simulate a better workload. The user would log in and access the required files before logging off. To ensure that any logout traffic was excluded from the results, all users were logged on and the files accessed before any user logged off. The graphs show the metrics from the first 1 hour of the test while users were logging on.

Test environment setup

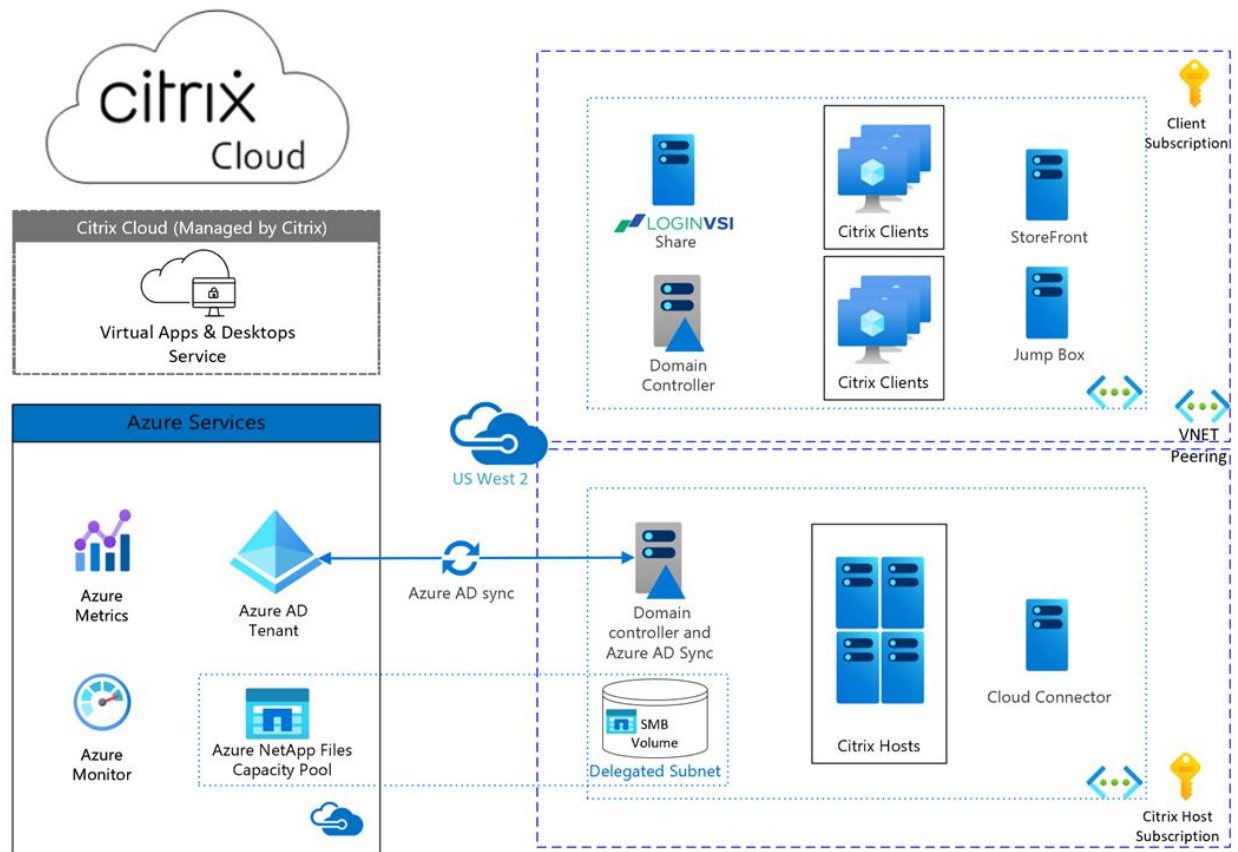
To reach the need for 100,000 files to be tested, the environment was designed to support 1,000 user sessions logging on within a 60-minute window. We did not want any of the test infrastructure or the Citrix host servers to become a hindrance, so the host servers were deliberately oversized to move any performance issues to the Azure NetApp Files share. See Figure 7.

We had two peered virtual networks configured in the Azure US West 2 region. One virtual network contained the LoginVSI infrastructure used to manage the sessions and report on progress. The other virtual networks contained the 30 Citrix hosts running on a Standard FS16_v2 instance with 1TB Premium SSD drive. The Citrix servers hosted the sessions that required user profiles to be loaded from and written to Azure NetApp Files. Citrix Profile Management was configured by GPO to be enabled and to use the Azure NetApp Files SMB share as the path store.

A NetApp storage account was created along with a Capacity Pool configured to the Standard Service Level set to 7TiB capacity. One SMB volume was provisioned for the user share set to 7TiB capacity providing a maximum throughput of 112MBps. The default user profile had 400 files ranging in size from 85KB to 5225KB plus a single 4GB OST file used for large-file testing. Total user profile size was approximately 4.7GB.

Citrix Cloud was used to manage the machine catalogs and the delivery groups. A local StoreFront server was used for enumeration. The 30 Citrix hosts were running Windows Server 2016 with the Citrix Multi-session OS Virtual Delivery Agent (VDA) 2006. The Citrix StoreFront server and the Citrix Cloud Connectors were on the subnet with the LoginVSI infrastructure, the Citrix hosts resided on a different subnet.

Figure 7) Test environment setup.



Test runs

Based on the variables identified earlier, the test matrix shown in Table 4 was run. Performance data was gathered from Azure Monitor and Citrix Director for each of the runs.

Table 4) Test runs and variables.

Run name	ANF service level	Volume quota	Files updated
ANF-Standard-20k	Standard	7TB	20,000
ANF-Standard-40k	Standard	7TB	40,000
ANF-Standard-60k	Standard	7TB	60,000
ANF-Standard-80k	Standard	7TB	80,000
ANF-Standard-100k	Standard	7TB	100,000

After the warm-up test run, each test run consisted of the following steps:

1. Restart the Citrix host servers.
2. Set the PowerShell script to the number of files to be updated per test case (20k, 40k, 60k, 80k, 100k).
3. Configure the test run to launch all 1,000 user sessions within 60 minutes.
4. Launch the test.
5. Record the start date and time.
6. Each session runs at least 60 minutes before logging off.

7. Record the stop date/time after all sessions are logged off.
8. Gather Azure NetApp Files data for key metrics.
9. Gather Citrix Director data for Logon Performance.

Test results

The test results are shown in Figure 8, Figure 9, and Figure 10, and are best displayed by categorizing them by key metrics discussed earlier: IOPS, Throughput, Latency, and Profile Load Time.

Figure 8) Test results – Read IOPS.

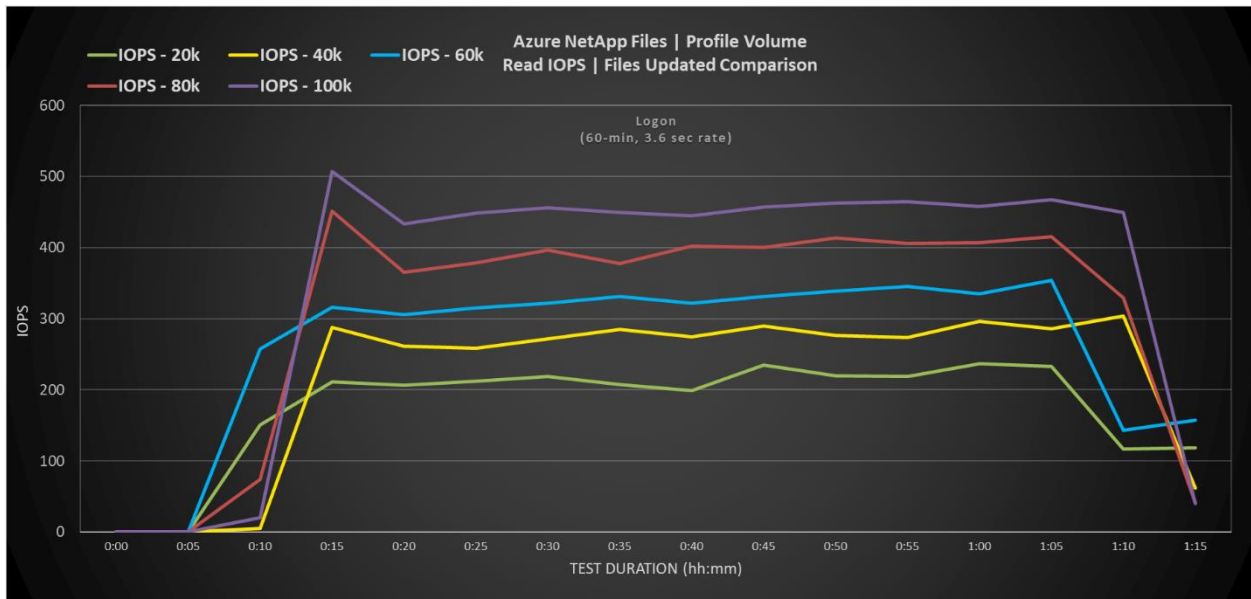


Figure 9) Test results – Write IOPS.

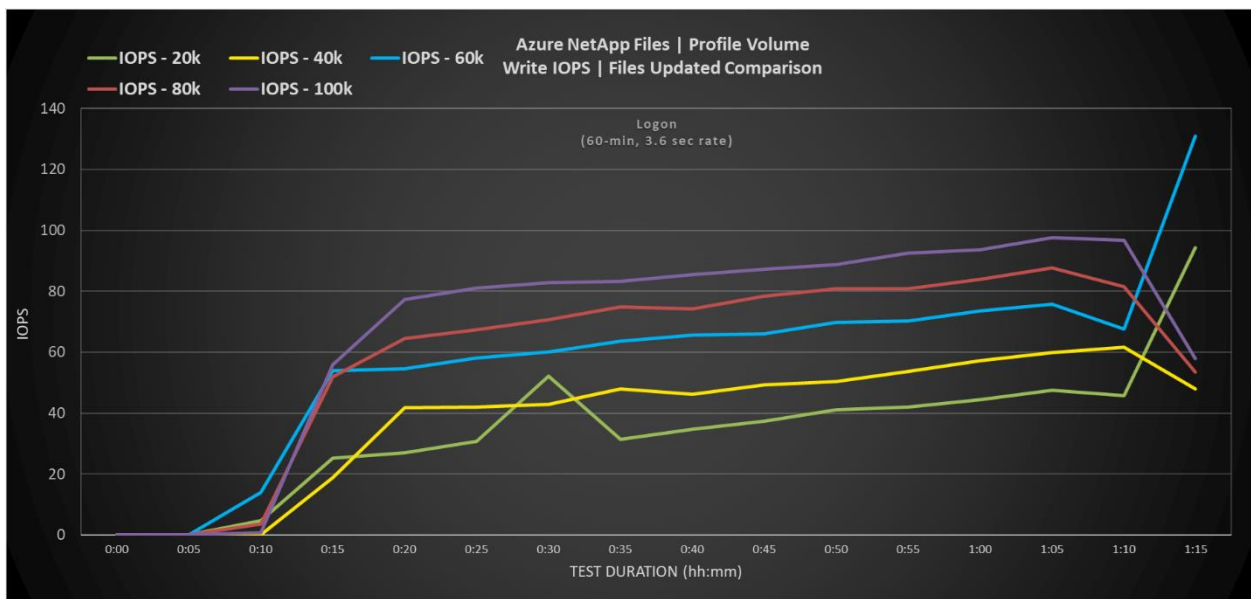
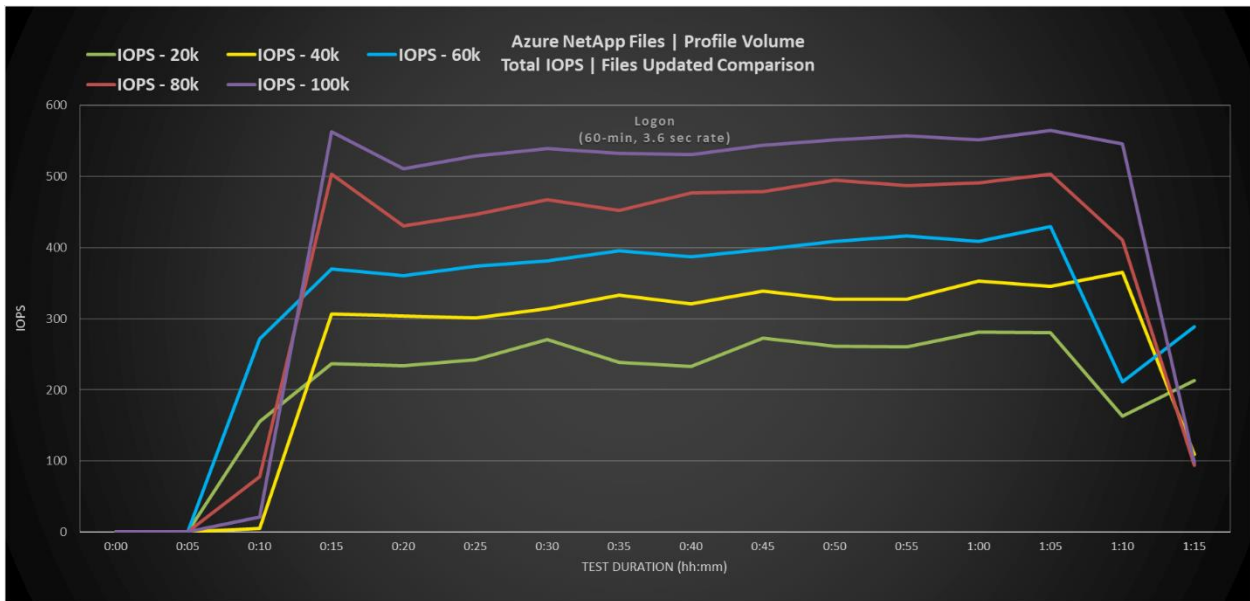


Figure 10) Test results – Total IOPS.



Read, write, and total IOPS are recorded as part of the Azure NetApp Files metrics. The preceding charts show a consistent amount of IOPS, relative to each test scenario, being used across all test runs. The total average input/output operations per second measured under 600. The consistent and incremental results are expected because the test was only varying the number of files touched using a single file share. The files themselves were the same amount and variety for every user profile.

Because Azure NetApp Files supports up to 450,000 Read IOPS and 130,000 Write IOPS in the configuration for the test, the IOPS required by our workload is well within the limits. This capability suggests that Azure NetApp Files can support several times this workload before IOPS would become the limiting factor.

Throughput

Throughput is currently not available as part of the Azure NetApp Files metrics found in the Azure Portal, however, this option is planned for the near future. Figure 11, Figure 12, and Figure 13 show the read, write, and total throughput consumed for Azure NetApp Files during testing. The read throughput is higher than write because Citrix Profile Manager is scanning the full profile at login and only changing a portion of the files. If profile streaming was not enabled as part of Citrix Profile Manager, then the entire profile would be read and copied down to each local host accessed. As the number of files updated during the test run increases, the throughput usage also increases. This behavior is because the entire file is streamed down to the local host, changed, and actively written back to the user share.

The throughput capacity is within the provisioned amounts of 112MiBps bound to the capacity pool and volume that provides the user store. Azure NetApp Files can process a maximum of 4500MiBps reads and 1500MiBps writes to accommodate the workload well beyond the demand of this testing exercise.

Figure 11) Test results – Read throughput (MBps).

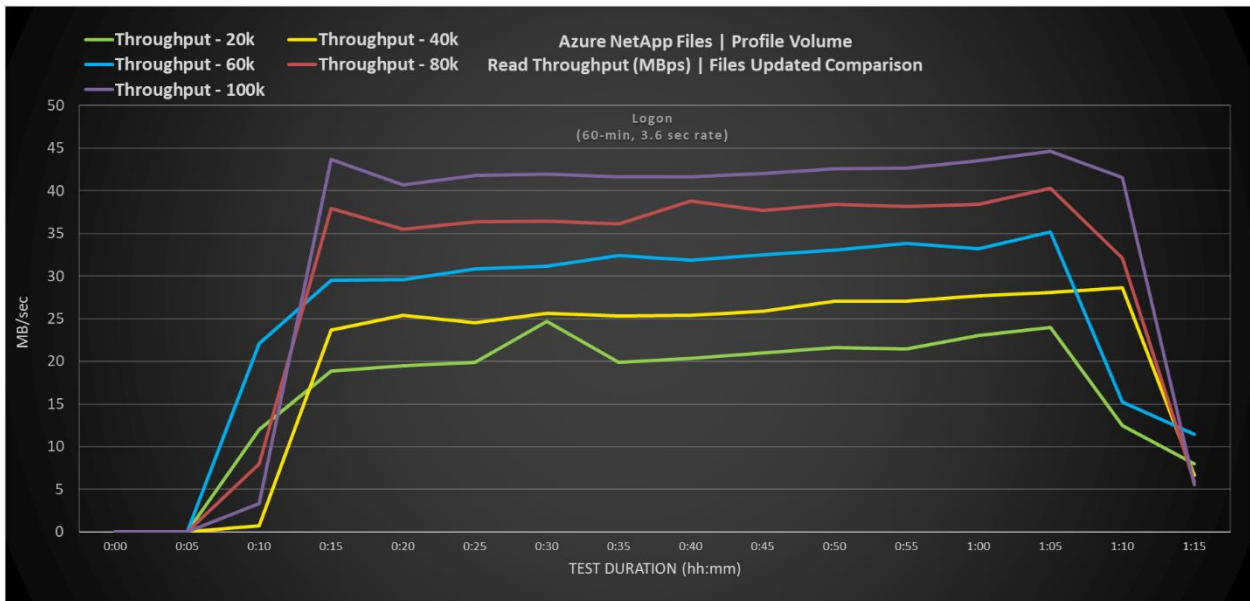


Figure 12) Test results – Write throughput (MBps).

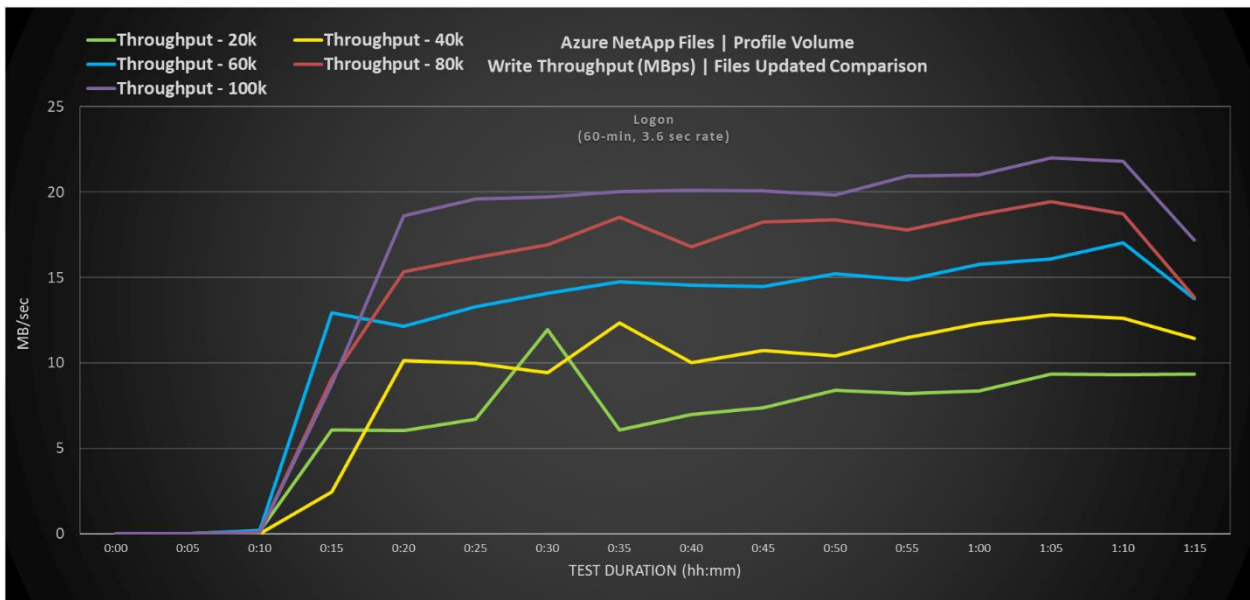
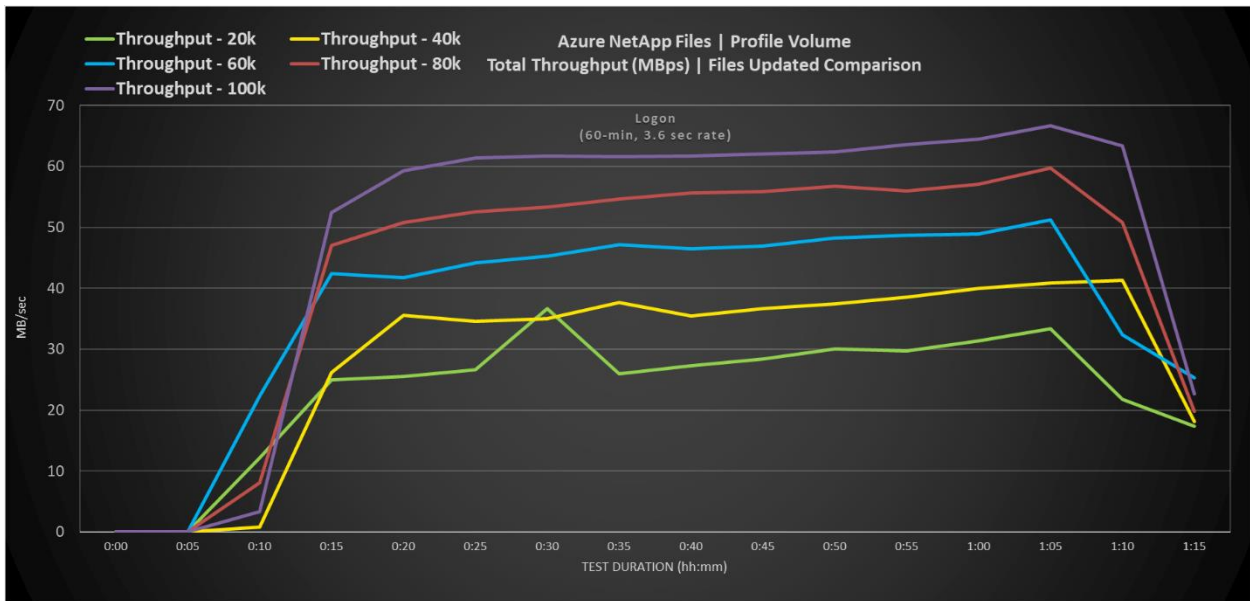


Figure 13) Test results – Total throughput (MBps).



Like the IOPS consumption pattern observed, throughput usage increased as expected based on the number of files updated per test scenario. The peak total amount of throughput recorded was slightly higher than 60MiBps during the 100,000 files touched test run providing for plenty of headroom to scale out the workload. Thus, theoretically doubling the users without needing to alter the capacity pool nor volume sizing.

These results are writing to the 4GiB OST files across the user sessions, but that file is not copied down to the local hosts because Large File Handling was enabled throughout testing. The writes to the OST files are made directly on the Azure NetApp Files share, much like how folder redirection functionally works.

Latency

Latency is available as part of the Azure NetApp Files metrics. Latency is a measure of the time required for a subsystem or a component in that subsystem to process a single storage transaction or data request. For storage subsystems, latency refers to how long it takes for a data request to be received, for the data to be found, and accessed from the storage media.

Figure 14 and Figure 15 illustrate the read and write latency performance pertaining to the test runs. Storage latency is a direct contributor of user experience with high amounts of latency resulting in long logon/logoff times and slow user operations such as loading data in an application.

Figure 14) Test results – Read latency (in milliseconds).

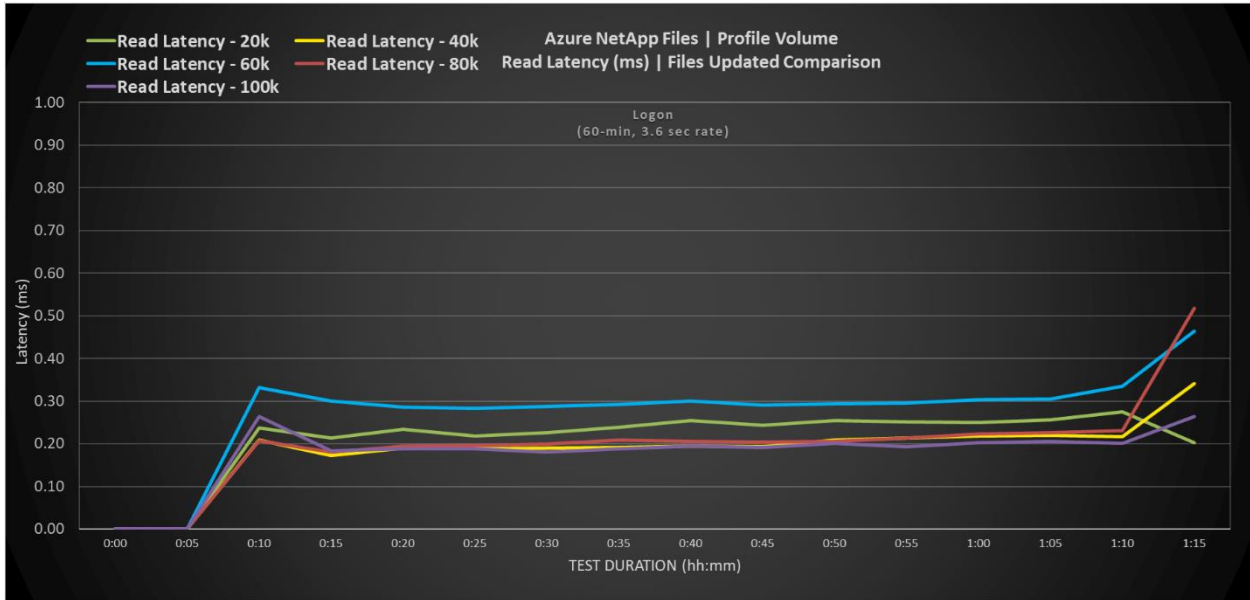
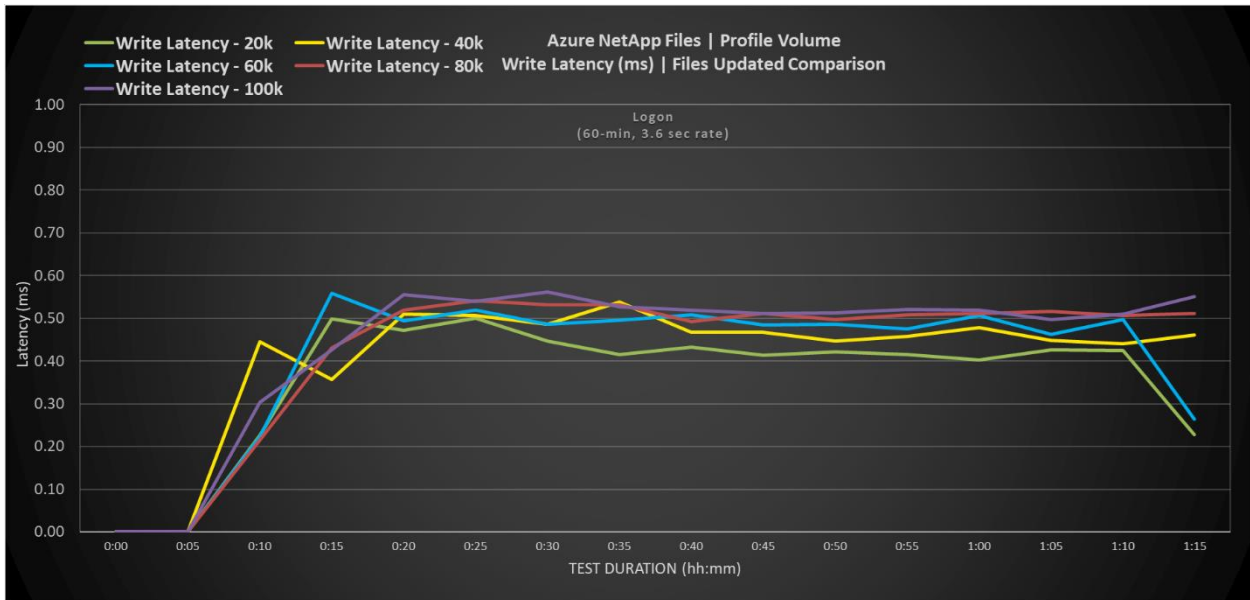


Figure 15) Test results – Write latency (in milliseconds).



As shown, Azure NetApp Files reported less than 1 millisecond (1ms) of latency throughout all testing scenarios. The latency stays within a reliable, consistent range of 0.2 through 0.3ms for reads and 0.4 through 0.5ms for writes with no erratic usage spikes to note. Latency performance has a direct correlation to profile load times where the later users logging on during a ramp period can be impacted. These results are discussed further in the section titled, “Profile load time.”

Profile load time

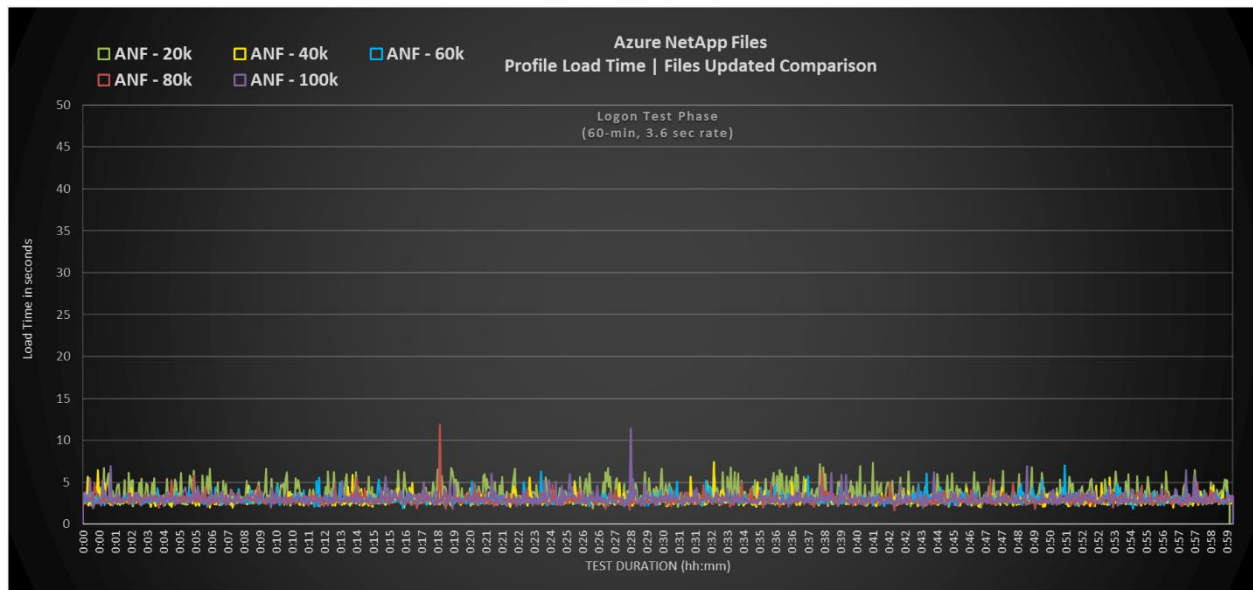
Profile load time is part of the Citrix Director trend analysis. Table 5 provides a brief overview of the average profile load times based on the run data collected from Citrix Director. Figure 16 shows a moving average over the previous minute for the profile load time for the users during the test runs.

Table 5) Average profile load times.

Run name	Average profile load time (in seconds)
ANF-Standard-20k	3.57
ANF-Standard-40k	2.80
ANF-Standard-60k	2.96
ANF-Standard-80k	2.92
ANF-Standard-100k	3.06
Variability	0.07
Overall Average	3.06

The profile load time metric (as shown in Figure 16) does not represent the entire login duration and excludes the following times: brokering, authentication, GPO, login scripts, and interactive session.

Figure 16) Moving average over the previous minute of profile load time during test runs.



The profile load times observed across all test runs are exceptionally low with only two outlier spikes to note. The results are consistent throughout with only a small degree of variability for all test scenarios proving Azure NetApp Files' reliability. Above all performance traits of Azure NetApp Files, ultra-low latency has a direct correlation to profile load times (as shown) and other application and user operations concerning storage resulting in a good or poor user experience. Irrespective of which service level is selected, Azure NetApp Files delivers the same latency performance given capacity and bandwidth requirements are met.

Analysis of the results

Azure NetApp Files does a superb job of managing and hosting end-user profiles and home directories. The results of the validation indicate with the tested workload Azure NetApp Files provides consistent and reliable performance at various load levels.

Azure NetApp Files performance and capacity tiering

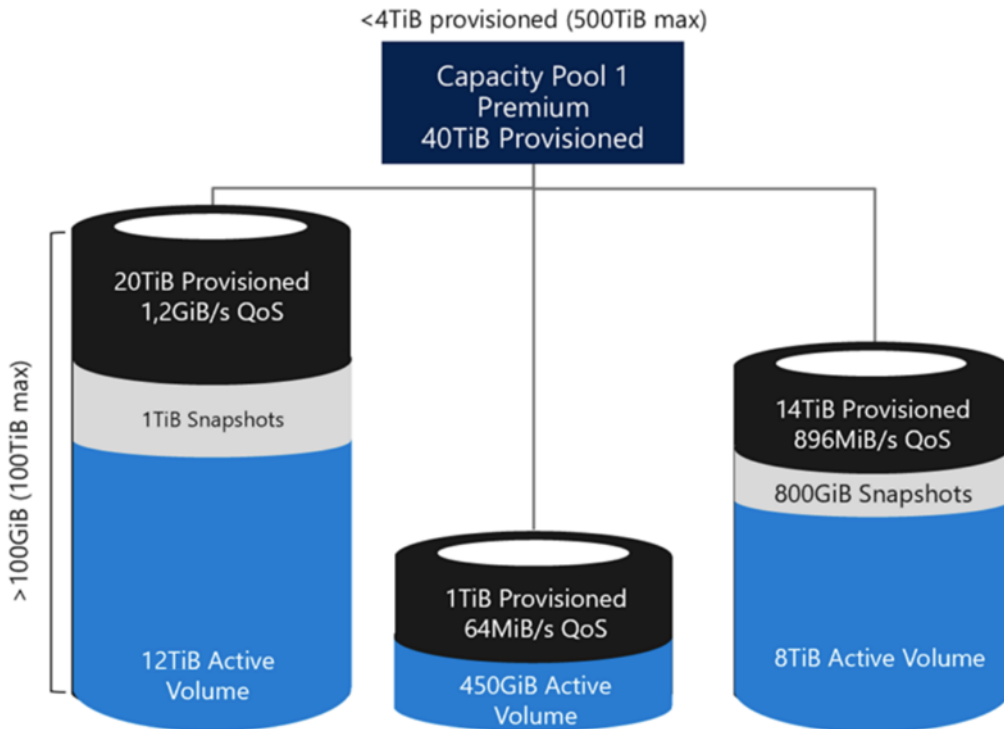
To understand how to optimize Azure NetApp Files' capacity regarding performance and costs, we need to take a closer look at how Azure NetApp Files is provisioned.

Azure NetApp Files volumes are allocated from a capacity pool the customer must provision in their Azure NetApp Files storage account. Each capacity pool is assigned:

- To a service level that defines the overall performance capability.
- The initially provisioned storage capacity for that capacity pool.

Figure 17 illustrates the Azure NetApp Files performance and capacity tiering.

Figure 17) Azure NetApp Files performance and capacity tiering.



The performance of a volume is based on the capacity pool service level, along with the number of TiBs provisioned for that volume. Customers can dynamically grow and shrink the volumes and pool capacity, manage performance, and manage capacity. Billing is based on the provisioned capacity pool, on an hourly base. Each of the service levels available has an associated cost per provisioned capacity and includes a QoS level that defines the overall maximum throughput per provisioned space. For example, a 10TiB provisioned single capacity pool with premium service level provides an overall available throughput for all volumes in this capacity pool of 10x 64MBps, so 640MBps, or 40,000 (16K) resp. 80,000 (8K) IOPS. For more information, see [Cost model for Azure NetApp Files](#).

Within a capacity pool, each volume is provisioned with a specific quota between 100GB up to the maximum volume size. This quota defines the maximum throughput/IOPs for this volume.

Service levels for Azure NetApp Files

Service levels are an attribute of a capacity pool. Service levels are defined and differentiated according to the allowed maximum throughput for a volume in the capacity pool based on the quota that is assigned to the volume.

Supported service levels

Azure NetApp Files supports three service levels: Ultra, Premium, and Standard.

- Ultra storage. This tier provides up to 128MiBps of throughput per 1TiB of volume quota assigned.
- Premium storage. This tier provides up to 64MiBps of throughput per 1TiB of volume quota assigned.
- Standard storage. This tier provides up to 16MiBps of throughput per 1TiB of volume quota assigned.

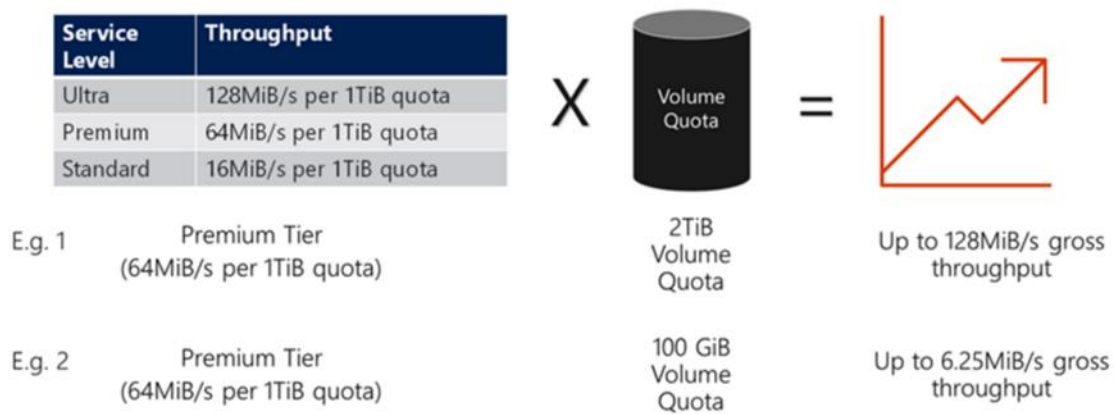
Throughput limits

The throughput limit for a volume is determined by the combination of the following factors:

- The service level of the capacity pool to which the volume belongs.
- The quota assigned to the volume.

This concept is illustrated in Figure 18.

Figure 18) Throughput limits for each service level and examples.



- In example 1, a volume from a capacity pool with the Premium storage tier that is assigned 2TiB of quota is assigned a throughput limit of 128MiB/s (2TiB * 64MiBps). This scenario applies regardless of the capacity pool size or the actual volume consumption.
- In example 2, a volume from a capacity pool with the Premium storage tier that is assigned 100GiB of quota is assigned a throughput limit of 6.25MiBps (0.09765625TiB * 64MiBps). This scenario applies regardless of the capacity pool size or the actual volume consumption.

For more information about the service levels, see [Service levels for Azure NetApp Files | Microsoft Docs](#).

Integrated data protection

Data protection is a critical part of any environment. The large part of a data protection strategy is ensuring that data can be restored quickly after any corruption or loss. The data protection architecture is defined by business requirements. These requirements include factors such as the speed of recovery, the maximum permissible data loss, and backup retention needs. The data protection plan must also consider various regulatory requirements for data retention and restore operation.

Small changes in data protection and recovery policies can have a significant effect on the overall architecture of storage, backup, and recovery. It is critical to define and document standards before starting design work to avoid complicating a data protection architecture. Unnecessary features or levels of protection lead to unnecessary costs and management overhead, and an initially overlooked requirement can lead a project in the wrong direction or require last-minute design changes. By using Azure NetApp Files, customers can implement comprehensive data protection for their user data and profiles by using Azure NetApp Files' ONTAP storage-based Snapshot copies.

The key benefits of the Azure NetApp Files storage-based Snapshot copies include:

- Snapshot copies can be created and kept on the service (for example, inside the original volume) with no performance effect on the storage service.
- Because these copies are created on the storage system, they do not consume database resources and no data needs to be copied out.
- Recovery from a data Snapshot copy is much faster than recovery from a data backup, resulting in aggressively short recovery time objectives (RTOs) (down to minutes).
- Snapshot copies and restores are near-instantaneous, enabling frequent creation, which means even shorter RTO because only a few log backups need to be applied after restoring a recently created Snapshot copy.

For more information, see the [introduction about Azure NetApp Files snapshots](#).

Storage management and cost optimization

Dynamic service level

You can change the service level of an existing volume by moving the volume to another capacity pool that uses the service level you want for the volume. This in-place service-level change for the volume does not require that you migrate data. It also does not affect access to the volume.

This functionality enables you to meet your workload needs on demand. You can change an existing volume to use a higher service level for better performance, or to use a lower service level for cost optimization. For example, if the volume is currently in a capacity pool that uses the Standard service level and you want the volume to use the Premium service level, you can move the volume dynamically to a capacity pool that uses the Premium service level.

The capacity pool that you want to move the volume to must already exist. The capacity pool can contain other volumes. If you want to move the volume to a brand-new capacity pool, you need to create the capacity pool before you move the volume.

Manual QoS capacity pools

The QoS type is an attribute of a capacity pool. Azure NetApp Files provides two QoS types of capacity pools – auto (default) and manual.

In a manual QoS capacity pool, you can assign the capacity and throughput for a volume independently. For minimum and maximum throughput levels, see [Resource limits for Azure NetApp Files](#). The total throughput of all volumes created with a manual QoS capacity pool is limited by the total throughput of the pool. It is determined by the combination of the pool size and the service-level throughput.

In an auto QoS capacity pool, throughput is assigned automatically to the volumes in the pool, proportional to the size quota assigned to the volumes.

See [Storage hierarchy of Azure NetApp Files](#) and [Performance considerations for Azure NetApp Files](#) for considerations about QoS types.

Specifying manual QoS type

When you create a capacity pool, you can specify for the capacity pool to use the manual QoS type. You can also change an existing capacity pool to use the manual QoS type.

Setting the capacity type to manual QoS is a permanent change. You cannot convert a manual QoS type capacity pool to an auto QoS capacity pool.

Using the manual QoS type requires that you [register the feature](#).

Conclusion

You can enhance the performance of Citrix virtual desktop workloads with the Azure NetApp Files service. The service gives you total control over your application performance. It can meet extremely demanding applications and workload scenarios while optimizing storage cost. The combination of Citrix Profile Management with Azure NetApp Files provides a great benefit to your Citrix deployment in Azure.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp Product Documentation
<https://www.netapp.com/support-and-training/documentation/>
- Azure NetApp Files documentation
<https://docs.microsoft.com/azure/azure-netapp-files/>
- Citrix Virtual Apps and Desktops with Azure
<https://azure.microsoft.com/services/virtual-desktop/citrix-virtual-apps-desktops-for-azure/>
- Citrix Product Documentation
- Reference Architecture: Virtual Apps and Desktops Service - Azure
<https://docs.citrix.com/tech-zone/design/reference-architectures/virtual-apps-and-desktops-azure.html>
- How to Configure Citrix Profile Management
<https://support.citrix.com/article/CTX222893>

Version history

Version	Date	Document version history
Version 1.0	June 2021	Initial release.

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 © 2021 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

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.

TR-4901-0621