Protecting and Managing Oracle® Workloads in Microsoft® Azure NetApp Files (ANF) using Commvault® Software

Best Practices

June 2021

Table of Contents

Introduction

Enterprises continue to embrace Microsoft® Azure as their cloud provider of choice to run large numbers of database and other application workloads. Flexibility, elasticity, cloud economics, and the ability to rapidly build new applications fuel this decision by combining existing apps with Azure services like Azure Machine Learning, Azure Internet of Things (IoT), and others. This trend is unbroken, and database workloads are an excellent example of rapidly growing workloads.

Oracle® Workloads in Azure

While new PaaS offerings like Azure SQL Server or Azure Cosmos DB are gaining market share quickly, Azure also proves to be very attractive for IaaS deployments of Oracle workloads. They are running Oracle on Azure memory-optimized VMs, like the E-Series v4, for all kinds of memory and CPU-intensive Oracle-based applications and workloads. However, many enterprise customers considering these solutions rely on NetApp storage and the ONTAP® software with its NFS services to run their on-premises mission-critical Oracle environment. This method is proven, secure and stable, and includes significant advantages in rapid and impact-free backup, cloning, and disaster recovery based on NetApp Snapshot™ technology. These benefits are now available through Azure NetApp Files (ANF), NetApp's enterprise file storage in Azure, and Microsoft's first-party service built on NetApp technology.

Many of the same customers also rely on Commvault software for application-consistent Oracle protection and automated NetApp Snapshot orchestration, allowing them to manage large environments very efficiently, be prepared for disasters and meet their SLAs.

This best practice guide details how you can leverage Commvault software for migrating your Oracle landscape to Azure and for backup and disaster recovery of Oracle on ANF. Whether you have a standalone Oracle database or an SAP on Oracle setup, Commvault can meet your data protection and data management needs. Please note that this guide does not address every possible situation, and users should always be aware of the technical and configuration guidance provided by each of their vendors. Commvault is not responsible for the performance of any applications, solutions, or infrastructure that is provided by other companies.

Commvault and Microsoft Partnership

Commvault has delivered industry-leading data management solutions on Microsoft's robust, secure infrastructure for nearly two decades. With Microsoft as our foundation partner, we designed a single platform that unifies and automates our intelligent data services across all the operating systems and applications your organization relies on daily. Together with Microsoft, we simplify the way you store, protect, optimize, and use your data.

Commvault has supported Microsoft Azure since 2008. We deliver unmatched depth and breadth of support for Azure compute and storage that uniquely positions our joint customers to benefit from the best practices of thousands of clients. In recent years, Commvault and Microsoft have expanded and strengthened this relationship through enterprise solutions for SAP HANA and Oracle. Commvault has also entered a new solution area with Metallic™ SaaS-based data protection offerings, discussed later in this guide.

Commvault Software and Microsoft Azure

Commvault Software Overview

Commvault's intelligent data services platform is an enterprise-level integrated solution providing data management and protection, data security, data compliance and governance, data transformation, and data insights. It delivers unparalleled advantages and benefits of a genuinely holistic approach to protecting, managing, and accessing data while providing infinite scalability and unprecedented control of data and information.

Commvault Software Architecture

A **Commvault CommCell® environment** (figure 1) is the logical grouping of all software components for the intelligent data services platform. A CommCell environment contains one CommServe® host, one or more MediaAgents, and one or more clients.

The **CommServe** host is the central management component of the CommCell environment. It coordinates and executes all CommCell operations, maintaining a Microsoft SQL Server database that contains all configuration, security, and operational history for the CommCell environment. There can be only one CommServe host in a CommCell environment.

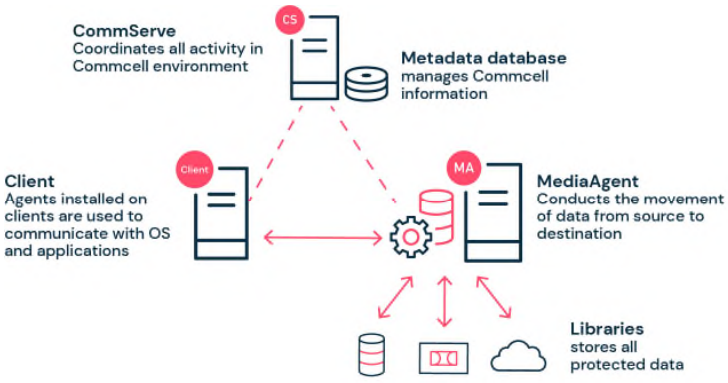

Figure 1 - Commvault CommCell Environment

The **MediaAgent** is the data transmission manager in the CommCell environment and provides high-performance data movement and manages data storage libraries. The CommServe server coordinates MediaAgent tasks. For scalability, there can be multiple MediaAgents in a CommCell environment.

A **client** is a logical grouping of software agents that facilitate the protection, management, and movement of data associated with the client.

An **agent** is a software module installed on a client computer to protect a specific type of data. Different agent software is available to manage various data types on a client, for example, Linux file system data and Oracle databases.

The Virtual Server Agent, or VSA, is a specialized agent that protects hypervisor and cloud resources.

Commvault's Integration with Azure

The primary integration point with Azure is through Commvault's Virtual Server Agent (VSA). You can use the VSA to perform the following tasks for Azure VMs:

- Backup and recover Azure virtual machines using either the Azure Classic or the Azure Resource Manager deployment model. You can restore complete virtual machines or guest files and folders
- Seamlessly convert backups of Amazon, Hyper-V, and VMware virtual machines to Azure virtual machines (Azure Classic or Azure Resource Manager)
- When performing a restore from a backup of an Azure VM, you can choose to restore a VM disk and attach it to a different VM that already exists
- Replicate Azure virtual machines to create and maintain warm recovery sites for virtual machines running critical business applications

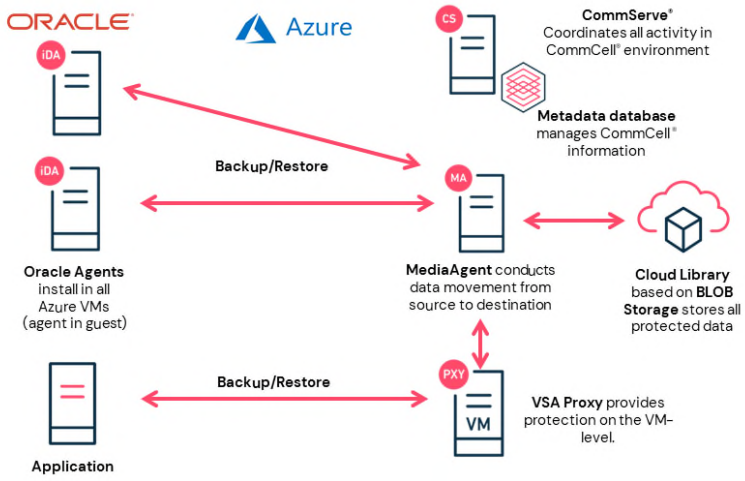

Figure 2 - Sample Commvault architecture with Oracle on Azure

Commvault handles data management and data protection operations through the CommCell Console. Use the CommCell Console to configure a virtualization client and other entities used to support operations.

A virtualization client instance is the access point for an Azure subscription and is used to back up complete Azure virtual machines. You must define a VSA agent instance for each Azure subscription. If a database or application runs inside the VM on the Linux OS, the VSA approach is not enough, as it guarantees crash-consistent backups only. For database workloads, we need application-consistent backups. Therefore, we use the "agent-in-guest" approach with the respective Commvault database agent installed inside the VM. This approach applies specifically to VMs running Oracle databases. VMs running Oracle application instances can be protected using the agentless VSA approach.

When you create a virtualization client instance or proxy, Commvault software automatically creates an Azure instance, a so-called backup set, and a default subclient to protect all virtual machines. You can create additional subclients to perform separate protection operations for different groups of virtual machines. For example, a different subclient can be made for other guest operating systems and use the default subclient to protect any remaining virtual machines that user-defined subclients do not cover.

Commvault's VSA agent can perform full, incremental, subsequent full, or synthetic full backups of virtual machines and restore entire virtual machines, disks, or guest files and folders at a granular level.

Another essential integration with Azure is available on the storage level. Commvault can leverage Azure Blob Storage as a secondary storage tier. Cloud libraries are built using Azure Blob storage containers. We recommend you use multiple containers in a single cloud library to enable Commvault's load-balancing capabilities and to easily increase storage capacity as needed. Azure Blob Storage provides centralized data access, better failover capabilities, and reduces the day-to-day storage administration tasks. Depending on the underlying Azure storage account type, Commvault can also leverage Azure geo-redundant storage (GRS) to build disaster recovery concepts across Azure regions. To achieve this, you need to provision RA-GRS Blob storage containers to build the cloud library.

As the data gets transferred over the network, protecting data integrity is crucial for any cloud storage implementation. Azure Blob Storage protects the integrity of the data using the following features:

- By default, data is transferred through secured channels using HTTPS protocol.
- If selected, data encryption can further encrypt the data providing data protection during network transfer and storage.

Commvault's deduplication feature identifies and eliminates redundant data in the backup, thereby reducing the volume of data stored in the cloud and the bandwidth required for data transfer. Enabling compression reduces the data footprint even further.

Commvault solution for Azure Oracle workloads

Once you have deployed the Commvault Oracle agent, it can auto-discover all databases running in each Azure VM. New Oracle instances will then become available in the Commvault Command Center™ user interface. Auto-discovery applies both to single-instance and containerized Oracle deployments.

Streaming vs. Snapshot Protection

One option for protecting Oracle instances in Azure is via streaming data transfer utilizing Oracle RMAN across Azure networks to the configured MediaAgent, where it gets written to a cloud library. Alternatively, it is also possible to install a MediaAgent directly into the hosting Oracle VM and share the cloud library. This way, all database nodes can back up their local data in parallel to blob storage, enabling high-speed backups and restores. However, note that the online backup process itself causes a specific database/application performance impact that will last for the entire duration of the backup job.

A more advanced way for protecting Oracle databases is by using storage-level snapshots, which has the following additional advantages:

- Minimal Oracle impact as the backup takes just seconds, compared to taking hours when streaming
- Ability to drive backup windows to zero, which is an enormous benefit for large mission-critical production systems
- Fast restores allowing you to meet aggressive RTO targets

IntelliSnap® implements Commvault's integration with storage-level snapshots. IntelliSnap operations are fully application-aware and very versatile as it currently supports many on-premises storage vendors like NetApp, alongside cloud storage. It also provides fully automated snapshot lifecycle management and cloning of databases and applications.

Azure NetApp Files

Commvault IntelliSnap in Azure supports Oracle databases running on Azure NetApp Files (ANF). Customers can achieve high-performance, better manageability, and reliability of the Azure NetApp File service combined with Commvault's automated snapshot orchestration. Like in an on-premises environment, it is possible to automate the creation of snapshot copies for the Oracle database running on ANF. Once its lifetime has expired, Commvault software automatically deletes both backup metadata and the snapshot itself. You can also copy snapshots to Azure Blob Storage for creating secondary copies with different retention times. Those snapshot copies can be made automatically on a proxy host (for offloading production), including an Oracle-level consistency check. You can also leverage Blob containers of different types for cost-efficient long-term storage or automatically replicate the data to a different Azure region to serve disaster recovery or other regulatory purposes.

IntelliSnap also supports Oracle configurations running on Azure Managed Disks, including simple disk configurations and Logical Volume Manager (LVM) volumes. At the backup time, IntelliSnap automatically creates a snapshot for each disk hosting the database volume, which typically takes a few minutes after the database is in backup mode. When a snapshot revert operation initiates, ANF creates new disks (clones) from the snapshots. It then recreates and mounts the original LVM volume to replace the original volumes to the destination VM.

Regardless of the underlying Azure storage technology, Commvault helps eliminate Oracle application impact and dramatically reduces recovery time - from hours to minutes. Another benefit is that the entire process can be streamlined and managed via the modern, web-based Commvault Command Center user interface, which provides a consistent and straightforward user experience and enables the backup admin to support the Oracle DBA team.

Restores start with selecting a recovery point, determining if the restore job will run from a streaming backup or a snapshot. As backups and snapshots can have multiple copies (which can reside in different places) in Commvault (Figure 2), there is also an option to select from which copy to restore. Various levels of granularity are selectable: full database, single tablespace or datafile, single tables, control file, or archive log. Restores will either go back to the same instance/database or be easily redirected to alternate nodes/VM and can optionally include Oracle full or point-in-time (PIT) recovery. Rapid, in-place restores are available for Oracle databases using ANF (based on NetApp SnapRestore® software), or Azure Managed Disk setups. Alternatively, you can configure a restore to run from a mounted snapshot via RMAN or file-based copy.

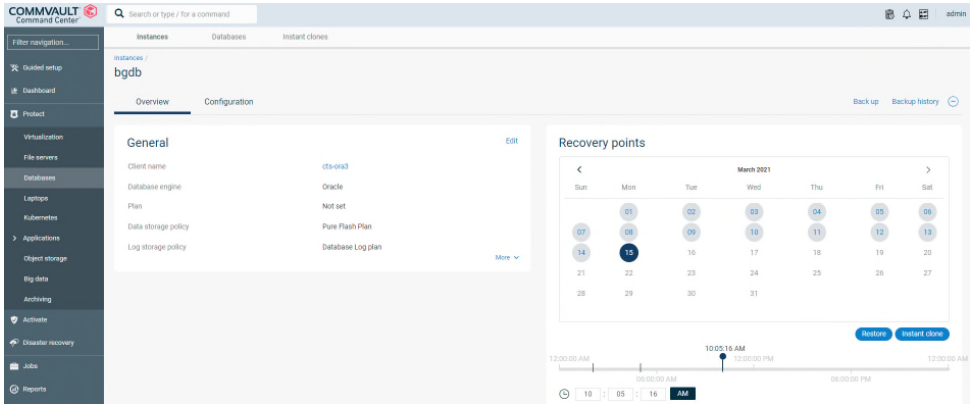

Figure 3 – Commvault Command Center: Choose from multiple recovery points

Cloning

During day-to-day operations, there is often a need to create one-off database copies. Examples of this are training environments or special-purpose test systems that you may need to copy from production or test databases. Setup and decommissioning of these one-off copies need to be quick and easy. It is also possible to create Oracle database copies based on cloned IntelliSnap snapshots. Clones can either be attached to the original Oracle VM or a different one and assigned a lifetime attribute. Once its lifetime has expired, the software automatically decommissions the clone, avoiding costly data sprawl. Oracle cloning is available both for Managed Disk and ANF configurations.

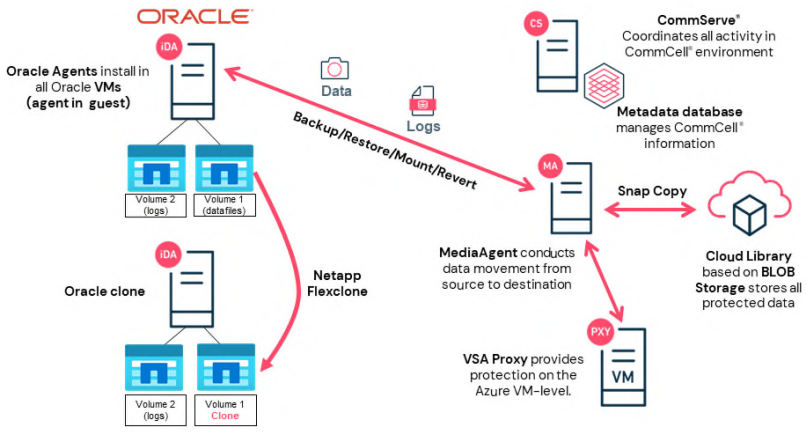

Figure 4 - Example of cloning architecture

Disaster Recovery

Being prepared for a disaster is not limited to on-premises. Disasters can also happen in the cloud. Therefore, it has become common practice to distribute data environments across multiple Azure regions. If one region goes down, you can start the Oracle and application services in the disaster recovery (DR) region. For building a meaningful Azure DR concept, you should ask yourself these critical questions:

- How can I replicate my Oracle and application data between Azure Regions?
- How can I meet my Service Level Agreements (SLAs)?

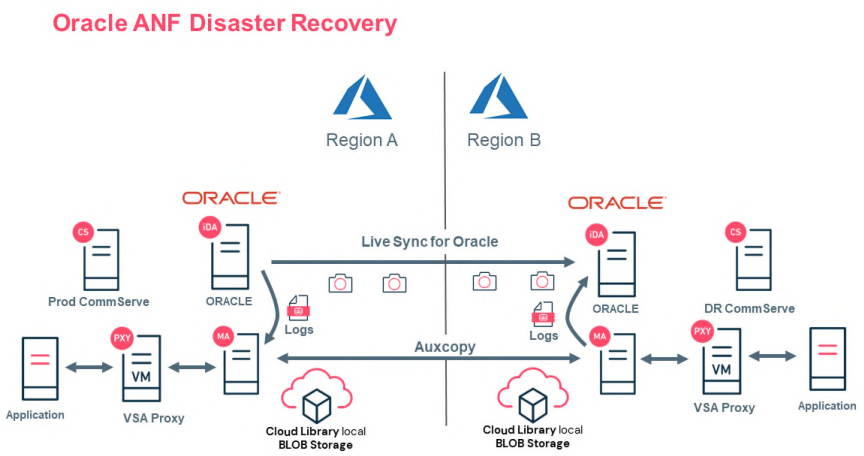

Figure 5 - Oracle ANF Disaster Recovery Model

The simplest way for replicating streaming backups or snapshots of both Azure VMs and Oracle to another region is by leveraging Commvault's built-in auxiliary or aux copy operation (Figure 5). This copy can leverage Commvault's deduplication, compression, and encryption technologies, which helps reduce network bandwidth, blob storage consumption and enforcing data security. Performing an aux copy requires a MediaAgent and a second cloud library available in the DR region. At DR time, you can provision new VMs, and restore application and Oracle data from the replicated copy. These restores run in streaming mode and can take a while, depending on the data amounts.

A second option for replicating the backup data is to leverage Azure geo-redundant blob storage containers (like RA-GRS) to build a cloud library shared between multiple regions. This way, Azure is replicating the data, and the second cloud library is no longer needed. Regarding recovery time objectives (RTO) and recovery point objectives (RPO) for Oracle and application data, there is no significant difference compared to aux copy.

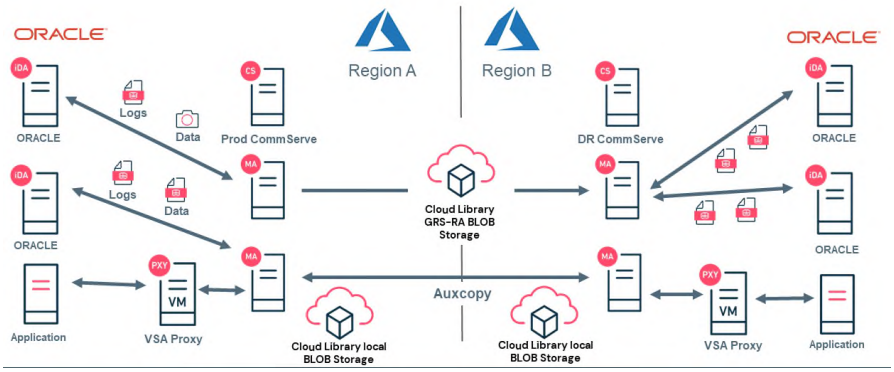

Figure 6 - Example Commvault DR configuration using Azure geo-redundant blob storage containers

Oracle Data Replication

For disaster recovery of critical production systems with minimal RTO and RPO, database and VM replication technologies play an essential role. For instance, you can run Oracle DataGuard for log shipping to the DR region. Commvault is fully integrated with Oracle DataGuard and provides freedom of choice between backing up from the primary or secondary copy. DataGuard is typically used for the most critical production systems and requires DBA involvement to set it up. However, Commvault provides an alternative solution. If you don't have – or want – DataGuard but want to implement Oracle replication on a broad scale, you can use Commvault's Live Sync feature to replicate Oracle databases. Because Commvault backs up all archive logs by default, the idea is to implement log shipping through Commvault. This process starts with a full backup of an Oracle database, followed by incremental backups to be restored on the target. Once the source and destination are almost in sync, only archive logs are shipped and applied to the target database. Achievable RPO can be as little as 5 minutes. The failover time determines the RTO.

A similar solution, replication of Virtual Machines, allows replicating Azure VMs where VM-level incremental backups are shipped to the DR region and applied to target VMs. For example, VM replication could improve DR times for Oracle E-Business Suite application VMs.

Migrating Oracle workloads to Azure

Commvault software also helps migrate Oracle workloads to Azure by leveraging the technologies described in the previous section. In this scenario, a Commvault deployment runs on-premises where backup data gets stored in a tape or disk library. For instance, there is an Azure connection via Express-Route, alongside at least one MediaAgent and a cloud library in Azure. Based on this setup, you can create Azure-based copies of an Oracle database and log backups via aux copy. For best results, start with a full Oracle backup followed by incremental and log backups to help minimize downtime for the switchover.

Suppose the on-premises Oracle environment is virtualized and protected by a Commvault VSA agent. In that case, you can directly create a new Azure VM from the aux copy via a VM conversion restore. Commvault automatically converts the VM backup during this restore, including all Oracle database and application data. This method is efficient and convenient as it allows automated migration of a large amount of VMs. We advise you to shut down Oracle right before the last incremental VM backup is taken for database consistency and, because these two migration scenarios require some downtime, recommended they only be used for development, test, and sandbox environments. We also recommend you enable Commvault deduplication and compression features to minimize the data footprint. Additionally, you can enable Commvault data encryption for in-flight security.

You may want to consider leveraging Commvault Live Sync for Oracle databases for critical production systems or landscapes. After creating the baseline in Azure via full and incremental backups, you can enable log shipping. Once the secondary system has caught up, you can stop the production environment. Then, after applying the final set of archive logs, you can open the Azure-based system as the new production environment. Unlike the previous methods, this one requires minimal downtime.

Metallic™ Database Backup for Oracle

As enterprises increasingly adopt Oracle to speed business process transformation and modernize IT, they need options that deliver peace of mind to ensure the protection of their mission-critical data against the threat of data loss or attack. Metallic™ delivers enterprise-grade data protection as a simple cloud-delivered SaaS solution. With Metallic™ Backup as a Service (BaaS), you can rest easy knowing your mission-critical Oracle data and workloads are safe and recoverable, now and in the future, whatever your cloud strategy holds.

Metallic™ Database Backup for Oracle provides support for Oracle running on-premises or in the cloud. BaaS means your environment is up in minutes with reduced management, automatic updates, no infrastructure and offers a powerful option to reduce TCO.

Metallic™ SaaS offerings are built on and optimized for Microsoft Azure and support all current Oracle versions on Windows, Linux, and Azure VM. In addition to Oracle, Metallic™ also supports SAP HANA databases.

Summary and Conclusion

Azure NetApp Files is a fully managed service built for simplicity, performance, and compliance that will take your business, applications, and workflows to the cloud faster and more securely than ever before. The service combines the best of NetApp's 26+ years of patented data management and storage knowledge with all the forward-looking capabilities of Azure cloud, making it a perfect solution for Oracle IaaS deployments.

To have a complete, well-rounded solution ready for production and daily operations, you need cloud migration, data protection, and disaster recovery. Commvault can help migrate your on-premises Oracle database by providing options for critical and non-critical deployments. Commvault's integration with NetApp storage and advanced snapshot orchestration delivers low-impact backup and recovery of Oracle environments, both on-premises and with Azure NetApp Files. Also, because Commvault integrates deeply with Oracle and Microsoft Azure, you can continue using

this proven on-premises solution for Oracle protection after migrating to ANF, ensuring you also meet your SLAs in the cloud.

Finally, Commvault can help you help build, orchestrate, and automate disaster recovery of Oracle in Azure NetApp Files in Azure. The additional option of Metallic™ Database Backup for Oracle provides you with complete flexibility and optimization, ensuring the ability to match the best solution to your specific needs, with the ability to modify your approach based on changing business and IT infrastructure needs.

The recommendations in this document are based on our experience in working with customers, and while these are generally applicable to most customers, individual environments and use cases can differ. Users remain solely responsible for the configuration and operation of their systems. If you would like to discuss any of these specific recommendations with a Commvault technical resource, please contact your partner account team.