Optimize Your Azure Environment

Prepare, migrate and protect assets with the Veritas Enterprise Data Services Platform.

VERITAS

Veritas and Microsoft have been leading the industry for over three decades. When it comes to pairing the right data management solution with Microsoft's Azure infrastructure, there is nothing better for the job than the Veritas Enterprise Data Services Platform. With solutions deployable directly from the Azure Marketplace, you can quickly and easily spin up the Veritas data management portfolio and put it to work to ensure all Azure assets are protected, highly available and understood. This approach allows organizations to harness the power of Microsoft Azure without fear of human error, regulatory compliance, ransomware or disaster interrupting their business.

The journey to achieve a cloud, hybrid cloud or even multicloud strategy can seem complex. What applications do you run in the cloud? What data should you migrate to the cloud? What data should you clean out of your environment prior to migration? If you're already in the cloud, how can you optimize your current strategy? There are so many details to consider, but Veritas is here to provide some guidance.

If you're looking for ways to analyze, migrate and protect your applications, data and workloads in Azure or if you're already deployed in Azure, this brief is for you. We'll cover how the Veritas Enterprise Data Services Platform complements Azure offerings and how they work together to provide a seamless experience in the cloud.

PREPARE

Whether you're at the beginning of your journey and deciding in what capacity you'd like to adopt Azure or you've already deployed in Azure, visibility and insight into your data and infrastructure is a crucial first step. Understanding where areas of waste, risk and value are in your environment lets you optimize costs, address compliance and ensure mission-critical data doesn't get buried when you need it most.

Data

When it comes to getting a handle on your data, you can rely on Veritas Data Insight. Data Insight supports metadata visibility, classification, permission visibility and file auditing from a variety of data sources, both on-premises and in the cloud. This solution helps you better understand the risk hiding in your file systems by triangulating critical intelligence from metadata attributes, content classification and user behavior, enabling better management of unstructured data. It can also automate the discovery of sensitive information with our integrated Classification Engine, allowing you to tackle compliance regulations or security threats with confidence. You can also use this information to mitigate exposure of critical data by detecting the location of this data and, if stored improperly, using insights from inferred ownership to identify the proper owner, who can then remediate the issue.

With data growing at a rapid pace, it's crucial to understand what important information you have and where it lives. Data Insight gives you the power to prioritize classification of petabytes of files with the help of artificial intelligence. To further increase performance, Data Insight lets you scale-out scanning and classification operations both in the cloud and on-premises, allowing it to run closest to

where the data resides. Regardless of where the scan and classification operations run, the data is centralized into a single UI, providing an enterprise view of your data landscape. And with the rise in ransomware, data protection and threat mitigation are a high priority for organizations of all sizes. Data Insight can identify anomalous behaviour such as unusual read, write and rename activity trends or unnatural user behavior and deliver this information via custom reports. These reports allow organizations to identify the location of potential ransomware, accounts that might be compromised and ransomware-infected systems.

Infrastructure

Just like information, knowing what hardware and infrastructure is in your environment is a key first step in making progress on your cloud journey. Business budgets are often held hostage by the need to purchase more hardware, cool more data centers and chase down shadow IT before organizations can even consider the next step in cloud adoption. Becoming aware of the challenges of knowing what you have, what you're using and what you need can make the transition to Azure a painless one. Veritas is helping address these challenges with APTARE™ IT Analytics.

APTARE is the only IT analytics software to offer unified insights for all major storage, backup and virtual infrastructures through a single plane of glass in both on-premises and multicloud environments. Only APTARE can provide unified visibility, insights and control of your hardware and infrastructure. It includes advanced analytics to help minimize risk and identify utilization and resource consumption, which paves the way for data center optimization. When it's time to make the move to Azure, APTARE allows you to do it confidently, knowing what you have, where you're going and what you need at your endpoint.

APTARE also offers support for Azure resources, so once you prep and migrate a data center, you maintain the same level of absolute visibility and control over your newly adopted cloud resources. Today, APTARE can help provide insights into Azure's compute stack, including disk, table and queue resources and bring complete visibility into Azure storage with deep reporting and insights on Azure Blob.

MIGRATE

Once you have a handle on your data and your infrastructure, you need the ability to easily move that data to, from and between clouds. Migrating systems between an on-site data center and an Azure environment poses challenges that in most cases cannot be completely resolved with native Azure configuration options. Veritas Resiliency Platform is designed to integrate with Azure to address these challenges by providing additional functionality and automation. It also offers standardized support across both physical and virtual systems, giving you the flexibility to enable bidirectional hybrid cloud migration between multi-platform on-site data centers and the Azure cloud.

As we mentioned in the previous section, visibility into your data and workloads is key. When making the decision to move workloads between sites, visibility into system status is critical. Resiliency Platform provides several reporting options that can help you understand the data synchronization status, system inventory, activity history and risk profile of your environment. You can run reports in real time that are stored in the Resiliency Platform database where you can access them on demand for historical analysis. You can also export reports and use them for auditing purposes and to prove compliance with corporate standards.

With Resiliency Platform, availability management goes beyond simply replicating data between sites. In addition to managing bidirectional replication of data between on-site systems and Azure without requiring data format conversion, Resiliency Platform can manage several other actions: the automation of DNS updates, network mappings between sites and starting entire applications at the new site during migration or failover—all with a single click. And when it comes to the migration of your applications, Resiliency Platform lets you easily configure and manage resiliency for multi-system applications based on application-level requirements and dependencies.

One of the last—and arguably most crucial—steps in a migration is your migration plan. On paper, getting workloads A, B and C from Site 1 to Site 2 and potentially back to Site 1 sounds great in theory, but how do you actually execute it? Resiliency Platform provides the ability to create a custom automated workflow consisting of a specific set of tasks. This workflow can include tasks such as starting, stopping, migrating and taking over a resiliency group or Virtual Business Service (VBS). You can also include a rehearsal as part of a resiliency plan. This rehearsal is executed in an isolated, non-production network segment either on-site or in an Azure virtual network to ensure systems are working properly prior to migration. You can run these rehearsals by using snapshots of production data that are then attached to temporarily provisioned systems used for testing purposes. Resiliency Platform also manages the cleanup of the rehearsal environment when it's no longer needed.

Sending data from on-premises to Azure using a third-party gateway appliance

The appliance performs deduplication before the changed blocks are forwarded on to the cloud via Azure Storage APIs. This solution will work with any Azure-compatible gateway that presents itself as a disk target to Veritas NetBackup™, allowing data to be deduplicated for the given environment. Unlike NetBackup MSDP Cloud, third-party deduplication appliances are not compatible with MSDP (media server deduplication pool), which requires the data to be rehydrated prior to sending to the gateway device.

PROTECT

Ensuring your data is adequately protected regardless of location is vital, which is why Veritas has partnered with Microsoft to offer a robust backup and recovery experience both to and in the cloud.

Organizations often have a mix of on-premises and cloud environments. If you want to move data to the cloud, NetBackup can orchestrate the movement of various workloads to the cloud to be stored in places such as Azure Blob Storage Hot, Cool or Archive access tiers for additional protection. For resources that already exist in the cloud, you can deploy NetBackup from the Azure Marketplace and use it to protect these resources the same way as protecting physical resources in a data center. This strategy avoids the cost and performance impact of sending data back to the data center for backups.

NetBackup and cloud restore options

Restores of data in the cloud are as simple as in a local data center. The backup admin has full use of the web UI to recover data. The storage access tier (Hot, Cool or Archive) the admin selects affects the restore performance, with restore from the Hot tier being similar to that of on-prem recovery in a data center.

Deduplication

Let's talk efficiency. To better leverage the cloud for storing backups for DR or long-term data retention, consider deduplication. With the power of deduplication, you can ensure backup data remains optimized while in transit to the cloud and while at rest in the cloud, greatly reducing cost and increasing performance when using cloud storage. This functionality is delivered via NetBackup MSDP Cloud and is available with the 8.3 release. NetBackup MSDP Cloud can process optimized backup images from existing MSDP volumes or directly from a client for transfer to an Azure Block Blob Storage target. The Hot and Cool tiers of Azure Block Blob Storage have been certified for use with NetBackup MSDP Cloud as well. And when using MSDP volumes as the source, the data does not rehydrate or remove optimization from deduplication. This end-to-end deduplication is a significant difference in how the MSDP Cloud operates compared to other solutions in the market today. Using MSDP Cloud will provide the highest level of functionality and cost savings when using object storage.

Cloud tiering

NetBackup MSDP Cloud support provides a flexible, scalable, high-performing, easy-to-configure solution that lets you leverage cloud storage more efficiently. Data is stored directly to cloud targets with deduplication. You can configure one MSDP storage server to support multiple storage targets, including one local storage target and zero or more cloud storage targets. You can move data to local and multiple cloud targets simultaneously. The cloud targets can be from the same or different providers—either public or private—and can be added on demand after the MSDP server is configured and active. Multiple cloud targets can coexist in a single storage server with multiple buckets that are distributed to one or more cloud providers. The data and metadata for local storage and multiple cloud targets are isolated to support multi-tenant use. Optimized deduplication is supported within one MSDP server scope so data can be stored to local storage first and then duplicated to cloud targets using the same MSDP server. DR from the cloud targets is enhanced and straightforward.

Backup in the cloud

In addition to sending data to the cloud for DR or tape elimination, developing a solution that is completely cloud native is also desirable. This approach is known as infrastructure as a service (IaaS), and many organizations find that running workloads entirely in the cloud is more cost-effective and offers the ability to provision virtual machines (VMs), with the VM and all storage in Azure. When protecting Azure-based workloads, minimizing data movement to on-premises infrastructure by also running NetBackup in the cloud is an important cost consideration.

Organizations typically still require backups of these workloads to protect from corruption and malicious activity such as ransomware. Azure VMs function similar to a data center using a hypervisor environment for VMs, so there are built-in safeguards to improve data availability; however, failures and corruption can still occur. NetBackup in Azure IaaS works exactly like NetBackup in a data center. You can provision a NetBackup Master and Media Server from the Azure Marketplace using Azure Resource Manager (ARM) or manually deploy them in a BYO fashion.

For cloud native workload protection, you can launch NetBackup CloudPoint from the Azure Marketplace and add it to the NetBackup configuration. NetBackup CloudPoint provides cross-cloud functionality and management from the NetBackup UI. CloudPoint allows automated protection for cloud native virtual instances, volumes and PaaS applications from an easy-to-use, central location. (See Figure 1.)

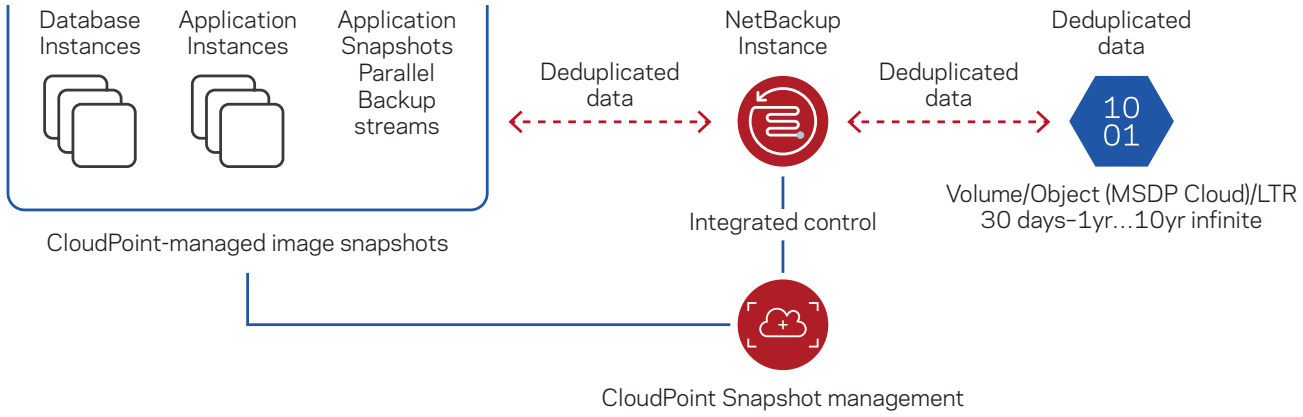

Figure 1. An overview of the workload protection process in Azure using NetBackup CloudPoint and MSDP Cloud.

Disaster recovery using Azure

One option to get data into the cloud is to adopt a hybrid model where part of the environment is in the data center and a second part is running in the cloud. Such a setup lets you duplicate and send a storage-optimized data stream from a data center to the cloud using Auto Image Replication (AIR) technology.

This concept is very simple and ties into a number of these use cases. Configure a NetBackup Master and Media Server with MSDP in the data center and a Master and Media Server with MSDP in Azure. From there, an AIR process can be used to automatically send data from MSDP in the data center to MSDP or MSDP Cloud in Azure. The transferred data's metadata is encapsulated in the transfer, so the import into the Azure NetBackup domain is near-instantaneous after the data is copied. Organizations have been using this model for global DR protection, like moving data from a data center in San Francisco to a data center in London, for a while. Leveraging this technology for a cloud target is no different for NetBackup—it's just another AIR target.

This option is ideal for organizations that want an off-site DR copy of the data. It's also a good way to migrate to the cloud from a NetBackup perspective. Veritas offers additional solutions like Veritas Resiliency Platform, which automates workload migration to the cloud and can integrate with NetBackup. This method is a perfect blend of creating dual instances of a workload for test/dev/QA while maintaining the original data in the data center. Resiliency Platform can also orchestrate workload recovery.

Organizations can also use Veritas InfoScale™ Enterprise and Azure integration to build a resilient infrastructure within Azure or one that allows on-premises systems to failover and replicate to Azure. It's also possible to design a topology using InfoScale that enables infrastructure to failover and replicate between Azure and other public clouds. Plus, you can use InfoScale to migrate data from on-premises systems to public clouds like Azure.

To simplify the configuration of high availability, InfoScale Enterprise ships with an array of agents that integrate into various third-party applications in addition to agents explicitly written to integrate with Azure. Integration with Azure means being able to conduct operations such as provisioning disks, registering IPs with DNS or provisioning VMs with RESTful APIs. (See Figure 2.)

InfoScale Enterprise provides agents that bind to Azure RESTful APIs to enable operations that make your applications highly available. For example, let's say you have two nodes in an InfoScale cluster in Azure. The expectation is that if one node fails, your enterprise service will failover to the second node to maintain availability. The InfoScale agents that integrate with Azure resources such as Disk, IP and DNS would be disconnected from the failed node and reconnected to the failover node. When your failed node recovers, InfoScale would then reconnect these resources.

Leveraging NetBackup image sharing for migration and DR

Starting with version 8.3, NetBackup extended the image sharing capability when using MSDP Cloud to write to Azure Blob Storage. Cloud tier support for MSDP is also new in this version.

This new functionality essentially makes the data in the storage container self-descriptive for reuse by an instance other than the one that initially wrote it. The only data needed to access the data is the storage account name and the necessary authorization.

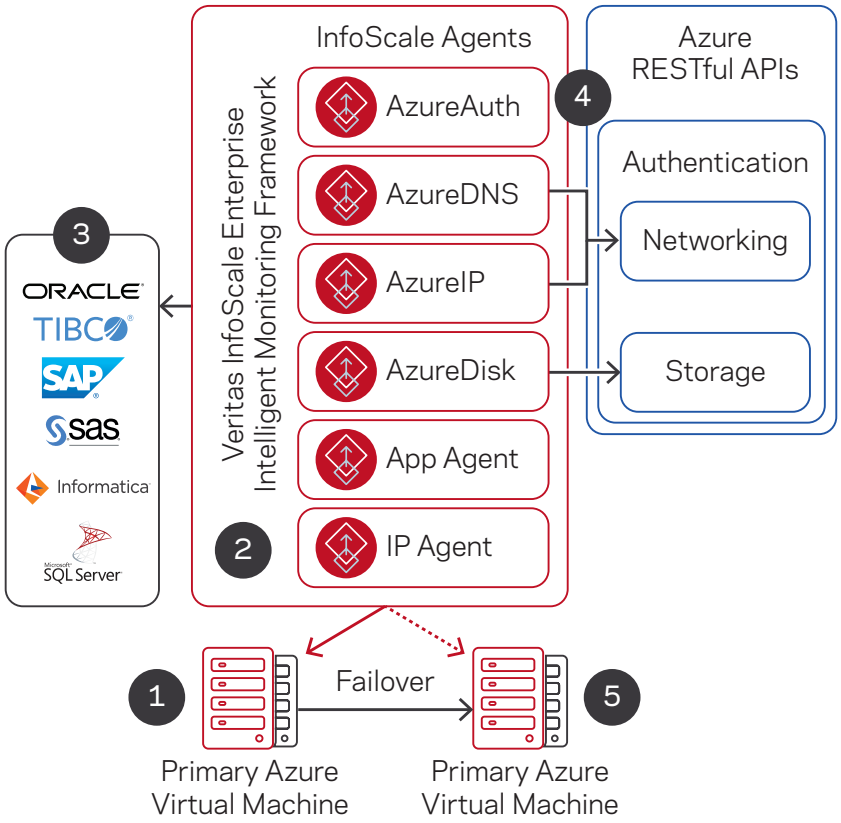

Figure 2. An overview of the failover process to Azure using InfoScale Enterprise.

Using image sharing, you can launch an on-demand NetBackup instance from the ARM Solution Template from the Azure Marketplace and attach it to the existing MSDP Cloud bucket. The new instance will be able to read the bucket data from within the cloud infrastructure and leverage image data to restore workloads in the cloud. (See Figure 3.)

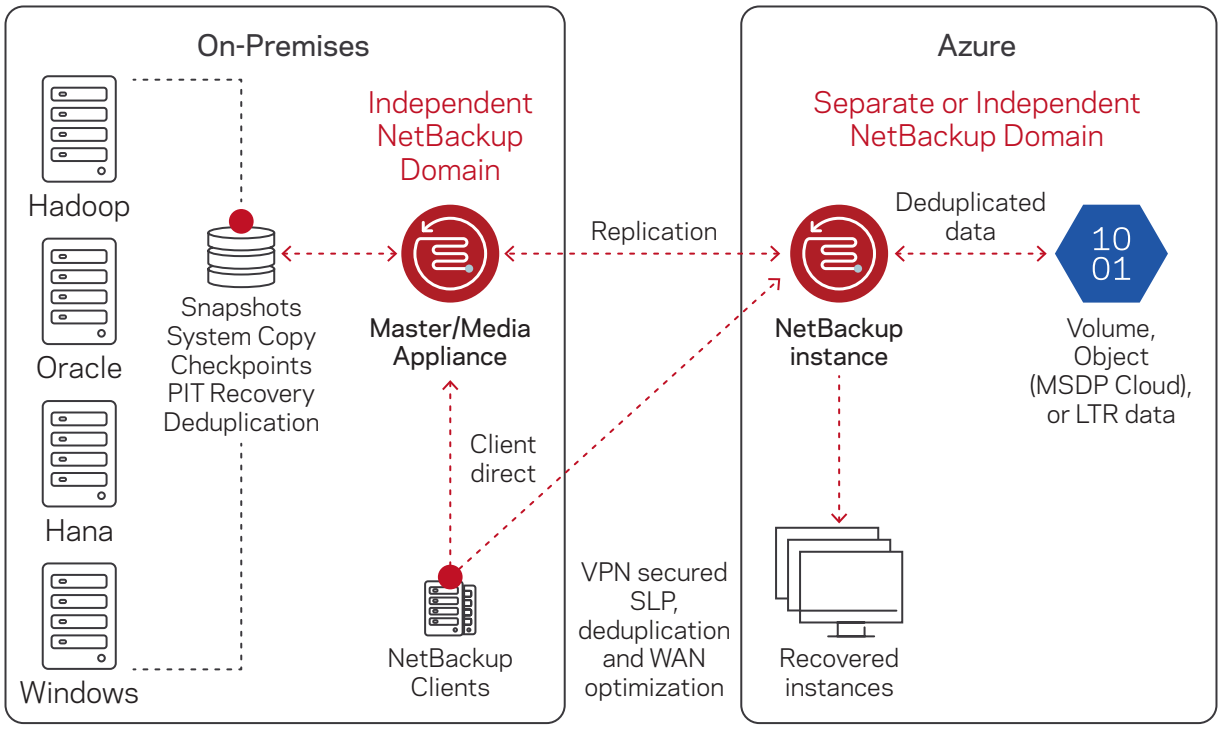

Figure 3. An overview of the failover process to Azure using NetBackup and MSDP Cloud.

For more advanced migrations of complex environments and their infrastructures, Resiliency Platform integrates with NetBackup to orchestrate recovery and migration operations with push-button simplicity.

To learn more about how the Veritas Enterprise Data Services platform can help optimize your Azure environment, please reach out to the Cloud Alliance team at azure.cloud@veritas.com.

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

2625 Augustine Drive, Santa Clara, CA 95054
+1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

VERITAS

V1083 8/20