THE DEFINITIVE GUIDE TO

Data Protection and Disaster Recovery on Enterprise Clouds

NUTANIX™

WHAT THIS BOOK COVERS

Many companies have failed to modernize data protection at the same pace as infrastructure and applications. By converging compute, storage, virtualization, and data protection, a Nutanix enterprise cloud delivers data protection without dedicated hardware or appliances, greatly simplifying your infrastructure, eliminating bottlenecks, streamlining management, and reducing costs.

This book examines important challenges and trends in availability and data protection, and explains how the simpler, more cost-effective approach taken by a Nutanix enterprise cloud can close the gap between where your data protection is today, and where it needs to be.

Version 0.1 / June 2016

TABLE OF CONTENTS

The State of Data Protection and Disaster Recovery

Businesses of all sizes are modernizing IT to increase productivity and reduce costs. Continued investments in infrastructure consolidation and virtualization have yielded significant benefits. Unfortunately, many businesses have not made the same investments in modernizing data protection as in other aspects of IT. With application uptime and availability becoming increasingly important, the result is a widening gap between the level of protection being delivered and the level of protection needed.

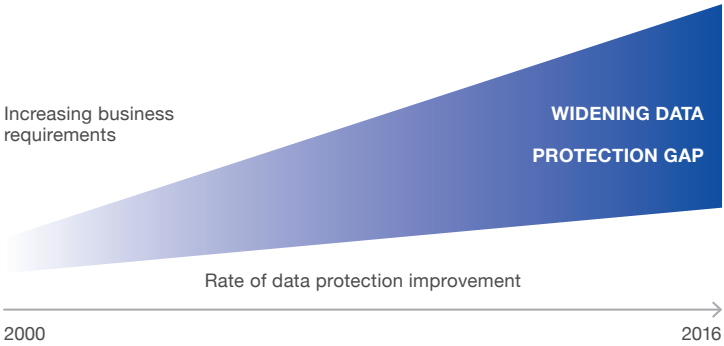

Figure 1:
Datacenters see a widening gap between the level of data protection provided and the level of protection required

Businesses of all sizes are discovering that enterprise clouds, built using predictable web-scale engineering and simple consumer-grade design, simplify IT, increase availability, and accelerate the entire IT environment—including data protection. This book examines data protection in Nutanix enterprise clouds.

DATA PROTECTION TRENDS

A number of factors make data protection more challenging than ever:

- **The amounts and types of stored data continue to grow.** And the diversity of places data is being stored—on servers, on desktops, on SAN and NAS storage, in multiple clouds—is growing with it.
- **Businesses are demanding a higher level of protection.** Applications of all types are seeing shrinking recovery time objectives (RTOs) and recovery point objectives (RPOs). In a recent Enterprise Strategy Group (ESG) survey, respondents said that two-thirds of services, on average, needed to be recovered in two hours or less.
- **The widespread adoption of virtualization has changed data protection.** Conventional unified backup solutions may not adequately address the needs of virtualized environments, forcing IT teams to change or add solutions. Providing protection in multi-hypervisor environments is a further complication. According to IDC, more than 72% of enterprises in 2015 were using more than one hypervisor, up from 59% in 2014.
- **There is no longer time for traditional data protection.** While the amount of data is increasing, the time available for data protection tasks is more and more limited. For many applications, the backup window has effectively shrunk to zero.

A number of additional factors muddle the data protection landscape:

- **Complexity.** Many enterprises rely on multiple data protection solutions, backup servers, appliances, and a variety of disk and tape media to address data protection needs.
- **Cost.** More data, longer retention periods, and complex data protection hardware and software add up to significant and growing costs.
- **Proliferating copies.** Copies of data are needed for backup, archival, disaster recovery (DR), analytics, development and test, and other purposes. A proliferation of copies leads to higher costs and inevitable challenges regarding what to keep and what to protect.

Many of the recent trends in data protection are in response to the challenges described above. Data protection modernization is closely tied to the following trends:

- **Snapshots.** There's almost no way to achieve an RPO of two hours or less (or meet shrinking backup windows) with traditional streaming backup methods. Space-efficient snapshots, which can be taken frequently without interrupting data access and which only consume storage as data changes, are becoming an essential part of data protection.
- **VM-centric protection.** Many companies continue to use traditional unified backup methodologies, even as more and more infrastructure is virtualized. However, by mid-2016 more organizations will be using VM-specific backup than unified backup.
- **Replication.** As with snapshots, replication is essential for meeting aggressive RTO and RPO goals. Asynchronous replication of data to one or more remote sites ensures that recovery can occur quickly if a primary datacenter goes offline for any reason. Synchronous replication can eliminate the chance of significant data loss from disasters, even when an entire datacenter is affected.
- **Cloud.** Almost everyone is looking at ways to leverage the cloud to decrease the cost and complexity of data protection and to reduce or eliminate tape. The cloud provides an unlimited pool of capacity, eliminating the need for provisioning and capacity planning for data protection. "Disk-to-cloud" and "disk-to-disk-to-cloud" models are popular.
- **Copy data management.** The final trend for 2016 involves limiting the number of full data copies that need to be stored and managed for backup, replication, and other needs. Snapshots or clones take the place of full copies, limiting storage consumption and simplifying data management.

[1] ESG Research Report: 2015 Trends in Data Protection Modernization, September, 2015.
[2] IDC QuickPoll Survey, IDC, 2014 & 2015.

DATA PROTECTION TERMINOLOGY

Not everyone defines every data protection term in the same way. This list defines the terms used in this book.

DATA PROTECTION. An overarching term that includes all the activities that protect data and application availability—backup/restore, replication, DR, etc.

BACKUP. The process of creating a copy of data. Traditionally, this consists of occasional full backups (all data copied) with regular, often nightly, incremental backups that copy only data that has changed since the previous backup.

RECOVERY TIME OBJECTIVE (RTO). The time allowed for recovery when an IT failure occurs. An RTO of one hour means an application or a data set will be back online within one hour after a failure.

RECOVERY POINT OBJECTIVE (RPO). The maximum amount of data you are willing to lose. An RPO of one hour means you will be able to restore an application or data set to a point no more than one hour prior to the outage or failure. The backup interval typically matches the RPO.

BUSINESS CONTINUITY. The full set of processes and procedures required to ensure that a business process can continue or be quickly restarted should a failure or disaster occur. A full business continuity plan may include provisions for personnel as well as infrastructure and applications. Infrastructure resilience, high availability, backup, and DR are all part of business continuity.

DISASTER RECOVERY (DR). The process of returning IT infrastructure and applications to an operational state following a disaster.

ARCHIVING. The process of storing data that is no longer being actively accessed for long-term retention.

REGULATORY COMPLIANCE. Adherence to the various laws, regulations, and guidelines to which a business is subject. Regulations often have a direct bearing on data protection requirements.

HIGH AVAILABILITY (HA). The process of ensuring that an application or set of applications can continue to run or be quickly restarted in the face of one or more failures.

REPLICATION. The process of copying data from a primary to a secondary location. Replication is most often used to ensure that important applications can be restarted should a failure or disaster take down a primary site. Asynchronous replication updates the secondary site at set intervals. Synchronous replication ensures that primary and secondary sites are always up to date, so no data is lost.

SNAPSHOT. A full or virtual data copy that preserves the state of the data at a specific point in time.

CLONE. A full or virtual copy of data that is writable; a clone is often a writable snapshot.

COPY DATA MANAGEMENT. The process of minimizing and managing the number of copies maintained of each data object. Data protection and other activities can result in the creation of huge numbers of data copies and consumption of excessive storage capacity. Technologies such as snapshots and clones can greatly reduce the number of full copies.

SECURITY FOR IT ENVIRONMENTS WITH STRINGENT COMPLIANCE REQUIREMENTS

Organizations that manage sensitive information—such as government agencies, healthcare facilities, and financial services companies—benefit from the built-in security features of the Nutanix architecture.

Nutanix software is hardened by default. It utilizes the principle of least privilege and delivers a true defense in depth model. Its custom security baseline is built off the requirements of the U.S. Department of Defense.

Nutanix combines features such as two-factor authentication and data-at-rest encryption with a security development life-cycle. This is integrated into product development to help meet the most stringent security requirements. Nutanix publishes custom security baseline documents, called security technical implementation guides (STIGs) that cover the entire infrastructure stack and prescribe steps to secure deployment in the field. Nutanix STIGs are based on common National Institute of Standards and Technology (NIST) standards that can be applied to multiple baseline requirements, e.g., for the DoD and PCI-DSS.

Nutanix STIGs are published in a machine-readable format, allowing for automated validation and ongoing monitoring of the security baseline for compliance. Nutanix has implemented security configuration management automation (SCMA) to efficiently check hundreds of security entities in the Nutanix STIGs, covering storage and built-in virtualization. Nutanix automatically reports log inconsistencies and reverts to the baseline. With SCMA, systems can self-heal from any deviation and remain in compliance.

Nutanix systems are certified across a broad set of evaluation programs to ensure compliance with the strictest standards. Nutanix is forging partnerships with leaders in the security industry to help you achieve your security goals.

Integrated Data Protection

A pioneer in delivering enterprise clouds, Nutanix removes the constraints of conventional data protection approaches. Nutanix converges compute, storage, virtualization, and data protection in a single infrastructure. Complex and expensive IT infrastructure is replaced with simple 2U appliances that combine compute and storage, scaling out one node at a time.

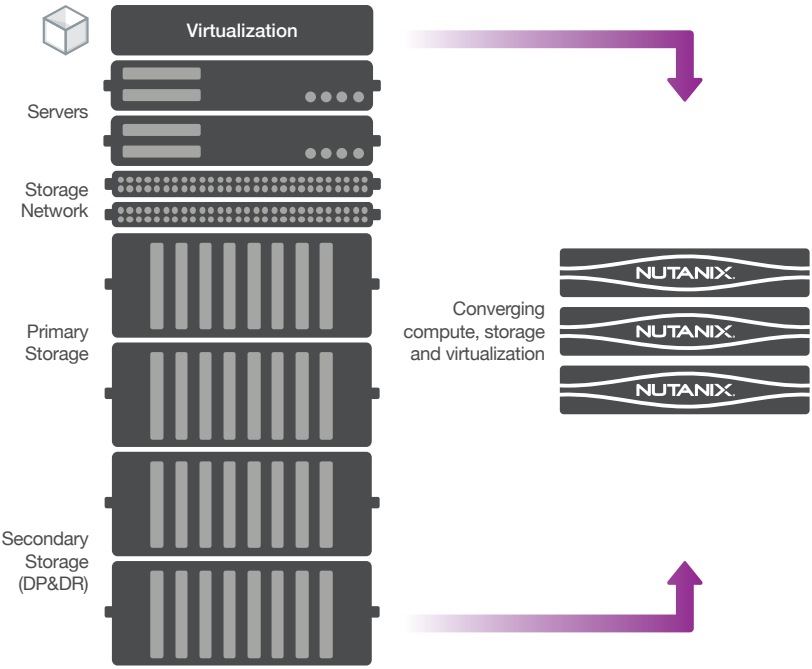

Figure 2:
Nutanix converges compute, storage, virtualization, and data protection functions in simple, scalable building blocks

Software innovation is what makes Nutanix systems unique. Nutanix software has two components: Acropolis and Prism. Nutanix Acropolis provides a distributed data plane with enterprise storage and virtualization services and the ability for applications to move seamlessly across hypervisors and cloud providers. Nutanix Prism provides a distributed management plane that uses advanced data analytics and heuristics to simplify and streamline common workflows, eliminating the need for separate management solutions for servers, storage networks, storage, and virtualization.

Nutanix software distributes all operating functions—including data protection—across a cluster. System resilience and overall performance increase as a cluster scales out, keeping pace with application and data growth.

Because a Nutanix system provides data protection without requiring separate dedicated hardware or appliances, it greatly simplifies your infrastructure, eliminates bottlenecks, streamlines management, and reduces costs.

Nutanix provides:

- Integrated, cross-hypervisor backup and DR with centralized consumer-grade management
- Flexible VM-centric policies to protect virtualized applications with different RPOs and RTOs
- Local, remote, and cloud backups
- DR based on asynchronous or synchronous replication

NUTANIX ENTERPRISE CLOUDS

You need the agility, simplicity, and pay-as-you-grow economics of the cloud, but you still rely on the security and control features of on-premises datacenter solutions like VMware. A Nutanix enterprise cloud gives your business the best of both worlds. You gain the agility advantages of the public cloud, including fast provisioning and fractional IT consumption, without sacrificing traditional datacenter virtues of tightly enforced security, predictable long-term costs, or the ability to satisfy demanding service-level agreements (SLAs).

CONVERGING DATA PROTECTION AND INFRASTRUCTURE

With the Nutanix approach to data protection, many customers find that they can eliminate reliance on third-party backup and DR products. Nutanix combines a highly resilient, scale-out infrastructure with highly efficient snapshot, cloning, and replication technologies to provide a higher level of data protection with less complexity and lower cost.

All Nutanix data protection functions are an integral part of the solution and are designed to be:

- **VM-centric.** All functions operate at the granularity of the virtual machine. Nutanix protection domains make it simple to group together VMs with similar data protection needs.
- **Multi-hypervisor and cross-hypervisor.** Nutanix provides native support for VMware vSphere, Microsoft Hyper-V, and Nutanix AHV (based on Linux KVM). Not only can you use data protection functionality with all three hypervisors, you can perform cross-hypervisor backup and DR to further optimize costs.
- **Simple to manage.** The complexity of data protection—with multiple solutions, devices, and interfaces—is a huge problem. Prism can be used to manage all Nutanix data protection functionality. A single consumer-grade interface can manage everything in a Nutanix environment.
- **Policy based.** Data protection is based on policies you define up front, allowing you to deliver the right level of data protection for every application and workload with ease.
- **Accessible via APIs.** Nutanix Acropolis provides full REST APIs that facilitate automation. Every action that can be performed from the Prism UI can be performed from PowerShell, scripts, or application programs.
- **Copy efficient.** Nutanix data protection and data reduction help you minimize the number of full data copies and, in the case of replication, the amount of bandwidth needed. This saves on space and cost, providing complete data protection while allowing you to quickly provision clones for analytics, dev/test, and other functions.

Figure 3:
Nutanix provides a continuum of capabilities that protect your applications and data at every level

DATA PROTECTION AT EVERY LEVEL

Backup and DR by themselves are not enough. Achieving maximum application availability requires a comprehensive approach to data protection that includes resiliency at every level and flexible technologies that combine to meet the needs of every workload.

Starting at the platform level and extending to the storage, virtualization, and management stacks, Nutanix has created a highly available, self-healing solution that delivers the right service levels for your applications and VMs—while reducing cost and management overhead. In a recent study of Nutanix customers, IDC found that unplanned downtime instances was reduced by 97% on average, and management overhead was reduced by 71% the customers' previous conventional deployments.

Nutanix offers a range of options that allow you to meet the RPOs and RTOs of different applications. Additionally, Nutanix solutions deliver data protection capabilities across hypervisors including VMware vSphere, Hyper-V, and Nutanix AHV. The sections that follow examine the resiliency, availability, and data protection capabilities of Nutanix enterprise clouds in detail.

ONE-CLICK NON-DISRUPTIVE UPGRADES

Unlike most other solutions on the market (both server and storage offerings), a Nutanix cluster allows software, hypervisor, and firmware upgrades through a simple and non-disruptive process that can be performed with a single click. If you've ever wasted a weekend in the datacenter, you'll understand the value immediately. Nutanix eliminates the need for planned downtime and takes the pain out of upgrade planning.

[3] Quantifying the Business Value of Nutanix Solutions, IDC, August 2015.

Built-In Infrastructure Resilience

Infrastructure resilience is the first line of defense for your data and applications. One of the things that differentiates Nutanix from conventional infrastructure with separately sourced servers, storage, and storage networks is that the platform is fault resistant, with no single points of failure and no bottlenecks. The system uses a shared-nothing architecture with data, metadata, and services distributed across all nodes within a cluster. It is designed to detect, isolate, and recover from failures; survive system hardware, software, and hypervisor issues; and maintain data availability.

The resiliency of the Nutanix web-scale architecture is the foundation for all Nutanix data protection functions.

TUNABLE REDUNDANCY

With Nutanix, tunable redundancy and erasure coding replace the HW-centric RAID technology of traditional storage. Each Nutanix data container—the equivalent of a VM datastore—is configured with a replication factor (RF) of two or three. An RF of 2 ensures that two copies of data are maintained at all times, allowing the cluster to survive the failure of a single node or drive. With an RF of 3, three copies of data are maintained across a cluster, providing resilience to two simultaneous failures. You can dynamically configure data redundancy based on application SLAs and the criticality of each data set.

Tunable redundancy provides continuous data availability for applications. In the event of a drive or node failure, data is automatically read from other nodes in the cluster. If the node does not come back online, all data on the affected node is automatically reconstructed to ensure full redundancy and data protection. Because the workload is spread across the cluster, the performance impact is small; the larger the cluster, the faster data is reconstructed and the smaller the impact of a failure. The system returns to full redundancy quickly and without intervention.

Tunable redundancy works in conjunction with Nutanix Erasure Coding-EC-X-which provides the same level of resilience but reduces storage capacity overhead.

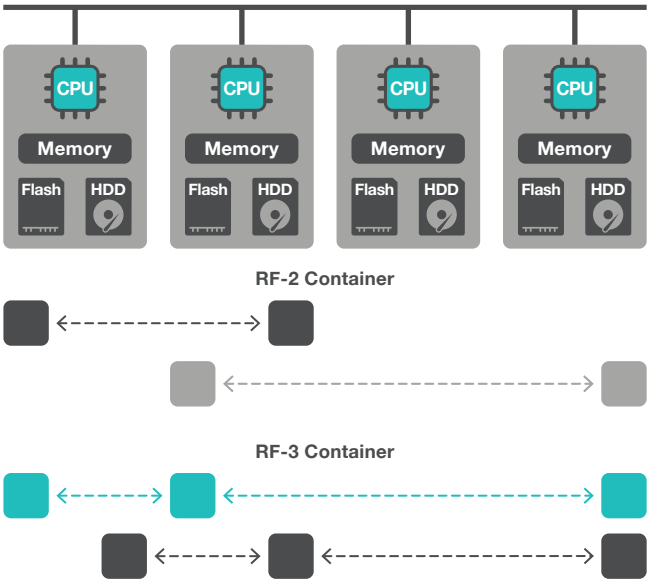

Figure 4:
Replication factor (RF) provides data resilience by placing data replicas on separate nodes

EC-X

Nutanix EC-X is an innovative erasure coding technology that provides resilience and increases usable capacity by up to 75%. EC-X reduces the capacity cost of storing two or three copies of data without taking away any of the resiliency benefits and with no impact on write performance. Nutanix systems use tunable redundancy for hot data and erasure coding for cold data.

Since coding and rebuilds are distributed across an entire cluster, EC-X is highly efficient with minimal computational overhead. This reduces vulnerability in the event of failures by speeding up rebuilds. EC-X also maintains data locality for high performance.

EC-X encodes a strip of data blocks on different nodes and calculates parity. In the event of a disk or node failure, parity is used to calculate missing data blocks. Each data block in a strip is on a different node and belongs to a different vdisk. The number of data and parity blocks in a strip is configured based on the number of failures a container must withstand.

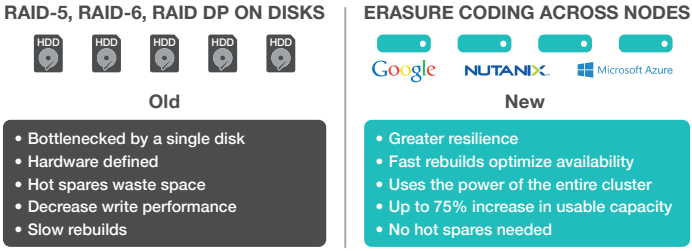

Figure 5:
EC-X provides greater resiliency without the limitations of RAID

SUPERIOR SUPPORT AND SERVICES

Nutanix has award-winning support, comprehensive global services, and innovative education solutions to help you run any workload at any scale. Nutanix Services can help you design the right data protection solution to keep your critical applications available and data properly protected.

INTEGRITY CHECKS

Nutanix software includes a variety of features to proactively identify and fix issues related to data consistency and integrity, bit rot failures, and hard disk corruption.

Detection of silent data corruption and repair of data consistency errors. The system scans data in the background and verifies it against the stored checksums in the distributed metadata store. If an error is detected, the bad data is rewritten using a good copy.

Automatic data integrity checks for every read. A checksum is computed for all data being read and compared with stored checksums.

Automatic isolation and recovery during drive failure. In the event of a drive failure, the system automatically replicates any data that is no longer redundant in order to ensure fault tolerance. During the failure and recovery process, both data and access to data are preserved.

AVAILABILITY DOMAINS

Availability domains offer even greater protection from hardware failures, allowing a Nutanix cluster to survive the failure of a node or block. Intelligent data placement combined with tunable redundancy ensures that a cluster can tolerate a node failure without losing access to any of its data. This is sometimes referred to as "node awareness."

Block awareness takes "node awareness" a step further by distributing data replicas across multiple blocks. (A block is a multi-node enclosure that may contain one, two, or four nodes.) If a block fails, there is at least one replica of all data on another block. A minimum of three blocks is needed for block awareness.

THE ADVANTAGE OF NUTANIX SELF-HEALING

If a conventional dual-controller storage system loses a drive, affected volumes run in degraded mode for a long period (possibly days or weeks) until the failed drive is reconstructed. Spare drives sit idle until there is a failure. If a storage system loses a controller, the workload on the other controller doubles. In either case, performance may noticeably suffer and time is of the essence when replacing the failed hardware.

If a drive inside a Nutanix cluster fails, active data is accessed from copies on other nodes, so the performance impact is minor; data redundancy is quickly restored in the background by re-establishing redundant copies of all data.

If a Nutanix node fails, workloads are restarted on other nodes. Data is accessed from copies on other nodes, and data redundancy is restored quickly in the background. The more nodes in a cluster, the more widely distributed the recovery work, and the more resilient the system. Self-healing reduces the urgency of replacing failed hardware.

VM-Centric Backup and Recovery

Regular backups are the second line of defense in data protection (after system resilience), and the only protection against user, administrator, and application errors that result in data being deleted or corrupted.

A Nutanix enterprise cloud provides three levels of backup and recovery. On-cluster Time Stream snapshots provide the first line of defense and the fastest and most convenient recovery from application problems or user errors. Remote backup lets you replicate snapshots to a remote location for longer-term retention and site-level resilience. Nutanix Cloud Connect provides remote backups to public cloud services such as Amazon Web Services and Microsoft Azure.

Using these capabilities, you can easily implement disk-to-disk, disk-to-cloud, or disk-to-disk-to-cloud backup models and tailor the number of backups you retain to your exact needs.

SELF-SERVICE FILE RESTORE

Nutanix backup includes self-service file restore, which allows users to recover individual files from within VM snapshots without an administrator. Self-service file restore is easy to set up and manage and in most cases eliminates the need to recover an entire VM.

CONVERGED LOCAL BACKUPS WITH NUTANIX SNAPSHOT

Backup remains one of the biggest challenges in virtual environments. Time Stream can create unlimited local backups-with VM- and application-level consistency-and recover data instantly to meet a wide range of backup and data protection requirements.

Time Stream uses VM-centric snapshots to provide production-level data protection without sacrificing performance. A redirect-on-write (ROW) algorithm dramatically improves system efficiency.

Other snapshot implementations rely on time-consuming data copies, or use copy-on-write (COW) algorithms that affect write performance and limit the number of snapshots that can be kept. The Nutanix approach avoids these limitations. Because Nutanix snapshots have access to all the storage capacity available on a cluster, you can store more snapshots for longer periods without worrying about the complexities of reserving space or maxing out individual LUNs or volumes. Many Nutanix customers add capacity-only nodes to accommodate long-term backups and archives.

Once a snapshot is created, it can be accessed without affecting production activity. You can back up a snapshot to tape for long-term retention, replicate it to another Nutanix cluster, or replicate it to the cloud.

NOT ALL SNAPSHOTS ARE CREATED EQUAL

Snapshots are a core Nutanix capability, so it is worth understanding how they work. When a snapshot is created, the base virtual disk (vdisk) becomes the snapshot while a new vdisk is created for reading and writing. Both vdisks have identical block maps, which map where data is physically stored. Each vdisk has its own block map, so accesses never have to traverse a long chain of snapshots.

When a write comes into the vdisk, the new data is written to a new location using a redirect-on-write algorithm. The block map of the read/write vdisk is updated, while the block map of the snapshot remains unchanged. Because additional storage is consumed only when data is changed or added, the process is extremely space efficient.

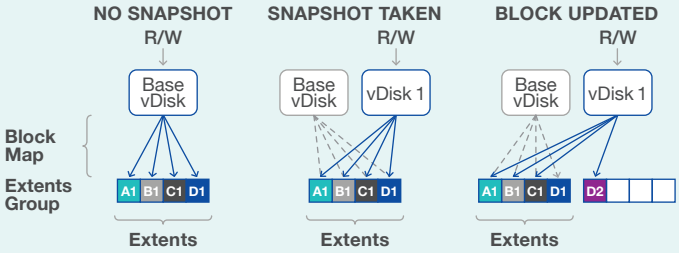

Figure 6:
Snapshots in DSF are extremely space efficient and don't impact performance

It's important to recognize that Nutanix snapshots benefit from the resiliency of the web-scale design. Each block in a snapshot is either stored multiple times or protected by erasure coding. Because data redundancy extends across multiple nodes, the chance that hardware failures will render a snapshot inaccessible are minimized. This means you can be confident replacing traditional backups with snapshots as a first line of defense.

INTEGRATED REMOTE BACKUP

Nutanix can efficiently replicate snapshots of individual VMs from a primary system to one or more secondary systems at different sites. Replication is flexible and bi-directional, enabling one-to-one, one-to-many, and many-to-one topologies. By supporting fan-out, fan-in, and multi-way replication, Nutanix allows you to create a flexible multi-master virtualization environment. VM snapshots can be asynchronously replicated or backed up to another datacenter on a user-defined schedule.

Only byte-level changes between snapshots of VMs are sent over the network to the remote cluster, and data is compressed to minimize WAN bandwidth consumption. Deduplicating data sent to remote sites can effectively cut the bandwidth required by as much as 75% versus host-based, full-copy backup solutions. Replication, like other system functions, is fully distributed across the nodes in a cluster, ensuring maximum replication performance.

The Prism interface provides a simplified view of all local and remote snapshots, allowing administrators to restore a VM from a snapshot with a single click. In case of disaster, you can fail over using the backup data copy at a secondary datacenter, providing a single replication stream for backup and DR.

IMPORTANT CONCEPTS FOR NUTANIX DATA PROTECTION

Protection domain. A group of VMs and/or files to be replicated together on a desired schedule so that protection policies can be applied on a per-application level. A protection domain can protect a full container or individual VMs and files.

Consistency group. A group of VMs and/or files that need to be protected in a crash-consistent manner so that they are in a consistent state when recovered. Related application or service VMs are typically collected in a consistency group.

Replication schedule. Defines the frequency of replication. For VMs, the snapshot schedule should be equal to the desired RPO.

Retention policy. Defines the number of local and remote snapshots to retain.

MULTI-HYPERVISOR AND CROSS-HYPERVISOR FLEXIBILITY

For environments running VMware vSphere and Nutanix AHV, VMs can be replicated across hypervisor boundaries. For example, you can run VMware in your production environment and Nutanix AHV in your DR/backup environment. Since your Nutanix solution includes AHV at no additional charge, this approach can significantly reduce virtualization licensing costs. You are free to choose the best hypervisor for each environment.

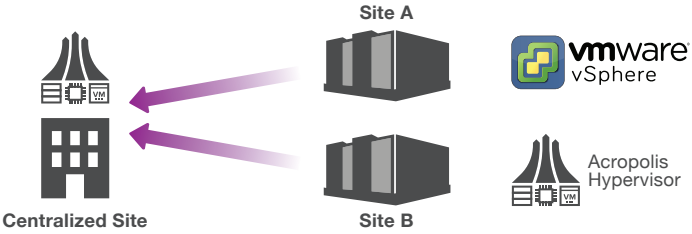

Figure 7:
Cross-hypervisor replication allows you to use different hypervisors at different sites

THE #1 CAUSE OF DATACENTER FAILURES IS...

Numerous studies have found that human error is the biggest cause of downtime—ahead of hardware, software, and facilities failures. Errors due to fatigue, lack of standard procedures, and "shortcuts" often trump more predictable human factors such as lack of training. You can protect against hardware and software failures, as explained elsewhere in this book, but eliminating operator error (sometimes comically referred to as PEBCAK or Problem Exists Between Chair and Keyboard) requires automation. You should always test your disaster preparedness plan to see where deficiencies exist—including human factors.

CLOUD CONNECT

Nutanix Cloud Connect lets you use public cloud services, such as Amazon Web Services (AWS) and Microsoft Azure, as a long-term backup destination for all types of workloads, making the public cloud a logical extension of your own datacenters.

Cloud Connect is integrated with a Nutanix system, allowing you to back up to and recover from the public cloud with a few clicks, just as you would with a remote Nutanix cluster. You can snapshot an individual VM, or a collection of VMs, to multiple geographically dispersed AWS and Azure regions. Recovery is the same as from a remote Nutanix site.

Cloud Connect for AWS provides a live Nutanix cluster in the cloud running on EC2 instances and using AWS Elastic Block Store for metadata and S3 storage for backups. For Microsoft Azure, the Nutanix software runs on Azure Compute, and storage is provided by Azure Page Blob. Data transfer is WAN optimized, reducing the storage footprint and network bandwidth by over 75%. Support for Amazon Virtual Private Cloud (VPC) and Azure Virtual Network (VNET) provides secure data transfers over an IP connection.

APPLICATION-CONSISTENT BACKUP

Snapshots on Nutanix systems are instantaneous and ideal for stateless applications, such as Web servers and other workloads able to recover from operating system or VM crashes. With other applications, such as databases or Microsoft Exchange, it may be desirable for the VM and/or application to be in a consistent state when a snapshot is created. There are three methods to create VM- and application-consistent backups:

Volume Shadow Copy Service. For Windows VMs, you can utilize the Microsoft Volume Shadow Copy Service (VSS) to quiesce the VM and supported applications, such as Microsoft Exchange and SQL Server, before taking a snapshot of the VM.

Multiple VMs can be grouped together in a Nutanix protection domain, enabling them to be operated upon as a single entity with the same RPO. This is useful when trying to protect complex applications such as Microsoft SQL Server applications.

Commvault. Commvault provides a deeply integrated solution to protect enterprise applications running on Nutanix. Commvault IntelliSnap technology collapses backup windows and accelerates restores with easy-to-use snapshot management for VMware, Microsoft Hyper-V, and AHV and can ensure application consistency across a wide range of virtualized applications, including Oracle; SAP; Microsoft SQL Server, Exchange, and SharePoint; and more.

API Integration. Any function that can be performed through Prism is also available through Acropolis REST APIs and a library of Nutanix-provided PowerShell commandlets. This means you can easily integrate Nutanix data protection functions with existing scripts that automate application backup or create new scripts or programs that incorporate Nutanix data protection.

For example, you could create a custom script using REST APIs to trigger a Nutanix cluster to take and replicate a snapshot of the group of critical VMs that make up an order-entry system based on the number of transactions being executed.

Disaster Recovery

Nutanix provides both asynchronous and synchronous replication options to support infrastructure recovery as part of a complete business continuity plan. With these integrated and simple-to-use capabilities, many Nutanix customers find they are able to provide online DR for many more applications than they could in the past.

REMOTE REPLICATION FOR DISASTER RECOVERY

Nutanix VM-granular replication makes it possible to create an affordable DR solution. Using protection domains, groups of related VMs can be replicated together. A group of VMs can be brought up on the secondary site with a single command if the primary site is down.

One of the biggest limitations of many replication solutions is the requirement that the primary and secondary sites have identical configurations. Nutanix clusters don't have these stringent configuration restrictions. This is especially useful for deployments with multiple remote sites using a centralized backup and DR strategy.

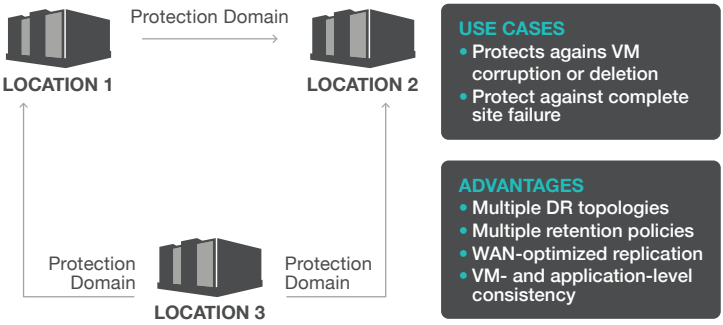

Figure 8:
Asynchronous replication provides remote backup and DR capabilities

METRO AVAILABILITY AND SYNCHRONOUS REPLICATION

For critical applications requiring zero RPO and near-zero RTO, Nutanix provides Metro Availability. Synchronous replication ensures continuous data availability across separate sites in a Metro Availability installation.

One of the main complaints with synchronous replication solutions is the complexity of deploying, monitoring, and managing them. Metro Availability is simple to set up and manage, and, because it doesn't rely on secondary solutions, it significantly simplifies DR.

Metro Availability can be set up bi-directionally between two sites connected over an IP-based metro area network. The only network requirement is a round-trip latency of less than five milliseconds, driven by guest OS requirements for acknowledging storage writes. Data is written synchronously to both sites, so it is always available to applications in the event a site fails or needs maintenance. You can non-disruptively migrate VMs between sites for planned maintenance events or other needs.

Failover isperformed at a storage container level, which means all VMs within a container will fail over to the secondary site. Nutanix and authorized partners can be engaged to create custom monitoring and failover scripts for specific situations.

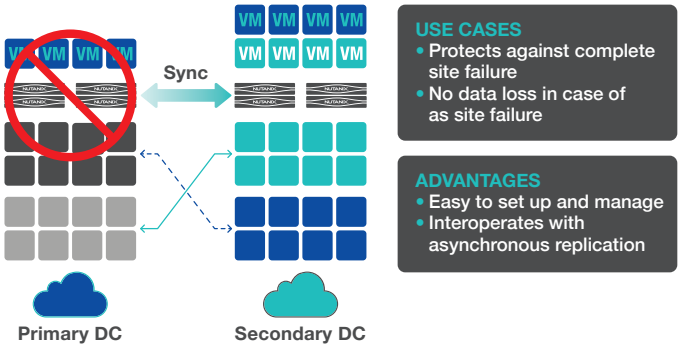

Figure 9:
Metro Availability provides synchronous replication between two data centers for DR with zero data loss

VIRTUALIZATION AND HIGH AVAILABILITY

Nutanix supports three hypervisors: Microsoft Hyper-V, VMware vSphere, and Nutanix AHV. You can utilize any of the HA capabilities supported by these hypervisors, such as vSphere HA or Hyper-V failover clustering, in your Nutanix environment.

Nutanix AHV provides native high availability for VMs. VM-HA works in conjunction with the resiliency built into the Nutanix platform. Out of the box, a Nutanix cluster running AHV automatically responds to node failures by restarting VMs on healthy nodes as long as a cluster has available capacity.

When VM-HA is explicitly enabled, the AHV software reserves failover capacity to ensure that HA is available to all powered-on VMs at all times. New VM power-on requests fail if the cluster does not have sufficient capacity to provide HA based on available memory.

The VM-HA software minimizes the need for configuration; it simply does “the right thing.” However, VM-HA also offers fine-grained control for advanced users. For instance, you can enable/disable VM-HA at a per-VM level, specify the relative priorities to restart VMs in case of a node failure, and specify the number of host failures to tolerate.

TEXAS A&M REDUCES RPO AND RTO TO AN HOUR OR LESS

The Information Technology Services (ITS) team of the Texas A&M University System Offices supports approximately 350 personnel, including the Office of the Chancellor and the Office of the Board of Regents. The ITS team switched to Nutanix in 2012 after organizational changes left them with too few staff to dedicate someone to managing a SAN.

Today, all System Offices servers run on Nutanix. This includes file servers, Microsoft SQL Server and Exchange, payroll, HR, accounting, and in-house applications.

ITS had been using a deduplication appliance for backups in its main location. If a disaster caused a server to go down, it could have taken weeks or months to restore full operation. With the addition of a second Nutanix cluster, ITS now has off-site backup and replication, reducing RPO and RTO to about an hour and greatly simplifying the DR plan. If a disaster occurs, all ITS has to do is turn on the replicated VMs at the off-site location.

Switching to a Nutanix enterprise cloud has delivered huge cost savings, especially when you include the increased productivity of the IT team. Even greater savings have resulted from a recent switch to Nutanix AHV. This eliminated hypervisor licensing costs as well as the need for separate software and a separate storage device to back up the virtual environment.

“The RPO and RTO have been reduced to about an hour or less, and the documented disaster recovery plan has been significantly simplified.”

Cary Tschirhart, Manager and ISO,
Information Technology Services
Texas A&M University System

Reducing Data Copies and Storage Consumption

Nutanix provides a variety of ways to decrease overall storage consumption and reduce the number of data copies you need, allowing you to implement a comprehensive copy data management strategy. Snapshots are extremely storage efficient and take the place of local backups in many circumstances.

Flexible deduplication and compression policies allow you to optimize the amount of primary storage consumed, and these savings are retained for secondary copies. These technologies have a big impact on the performance and efficiency of synchronous replication with Metro Availability.

SINGLE-STREAM BACKUP AND DISASTER RECOVERY

Traditional methods usually result in separate data copies for backup and DR. Nutanix integrated remote backups provide both backup and DR functionality in a single stream, saving storage space and WAN bandwidth. You can recover from a remote site to a primary site as necessary, or fail over to the remote site and restart operations there.

FLEXIBLE CLONING

Nutanix administrators can create clones, which are writable snapshots, of a base image in a matter of seconds. The result is a writable "copy" that consumes only incremental storage space. This capability can be integrated into scripts and programs to enable automation, and Nutanix provides full integration of cloning in popular offload capabilities, including the VMware API for Array Integration (VAAI) and Microsoft Offloaded Data Transfer (ODX), allowing copies to be created in seconds.

You can easily create clones of VMs and data sets for development, testing, analytics, and other uses. Clones replace full copies so that every developer and tester can have his or her own full environment to work in. Customers who have implemented remote backup and DR often use backups as the baseline for development and test processes, offloading the production environment and gaining greater leverage from their investment in Nutanix infrastructure.

LCUB CHOOSES NUTANIX FOR DR, PERFORMANCE, AND COST REDUCTION

The Lenoir City Utilities Board (LCUB) is one of the largest municipal utilities in Tennessee. LCUB's IT environment was running close to full capacity, making it very difficult to maneuver during peak demand or after a failure. In 2015, the team made the decision to purchase two Nutanix clusters to provide greater headroom and more flexibility.

LCUB has already experienced up to 20x faster performance and a two-thirds reduction in operating expenses. Because LCUB is a utility, downtime is not an acceptable option. Previously, upgrades would take a week or two to perform. With Nutanix, the IT team can perform non-disruptive upgrades on the fly without taking systems offline.

In Tennessee, disaster readiness includes preparing to recover from a direct hit by a tornado. A Nutanix enterprise cloud gives LCUB the ability to easily replicate data between clusters. A second datacenter is under construction to accommodate DR, and fiber optics are being put in place to connect all offices and substations. Nutanix replication will also enable LCUB to remain fully operational while bringing the new datacenter online.

To further improve monitoring, LCUB administrator William Jason Tuttle used the Acropolis REST API to create a smart-watch application. The application displays a variety of real-time statistics, including free space, memory utilization, and CPU utilization, on the team's Pebble watches.

"As our workflows become more dependent on technology, we must plan for the worst so that we are able to restore power and other lifesaving services in a timely manner after any catastrophic event."

William Jason Tuttlem Data Management and Administration, Lenoir City Utilities Board

Integration and Partnerships

Nutanix has put significant time and effort into making sure that the hypervisors, applications, and data protection solutions you depend on integrate with Nutanix solutions:

- **Offload.** Nutanix software integrates with popular offload capabilities, including VMware API for Array Integration (VAAI) and Microsoft Offloaded Data Transfer (ODX), to create clones in a matter of seconds with minimal overhead.

- **Data protection partners.** Nutanix provides support for vStorage API for Data Protection (VADP), application-level consistent snapshots using Volume Shadow Services (VSS), and VM-level backup for Hyper-V using VSS for SMB shares. This allows Nutanix backup and DR capabilities to integrate with third-party tools such as Commvault and VMware SRM. Commvault IntelliSnap integration combines Commvault backup capabilities with enterprise storage features from Nutanix.

- **REST APIs.** Prism management functionality is also accessible through Acropolis REST APIs and a library of PowerShell commandlets. API integration is ideal for next-generation Web-based applications or any team adopting a DevOps approach to IT.

- **Application validation.** Nutanix has invested in validating solutions for critical enterprise applications, including Microsoft SQL Server, Microsoft Exchange, Oracle, and SAP NetWeaver. This includes configuring applications to run optimally using both Nutanix and application-centric data protection.

Your Data Protection Checklist

As you now know, a Nutanix enterprise cloud delivers natively integrated data protection and continuous availability at the VM level, making it possible to meet the RPO and RTO of every application in your portfolio.

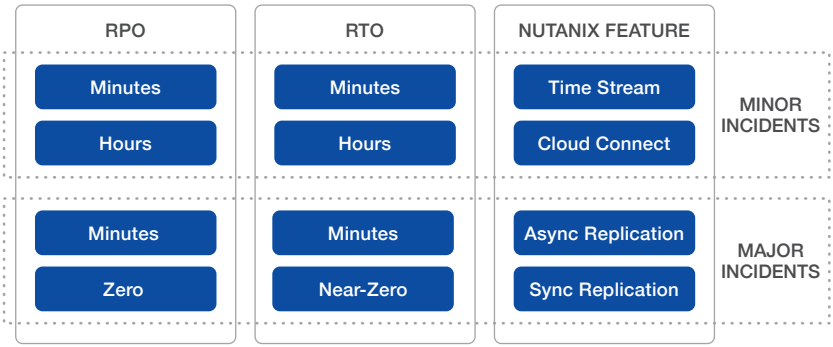

Figure 10:
Nutanix data protection options cover a wide range of RPOs and RTOs

While data protection requirements are trending up across the board, different applications can still have significantly different needs. This section provides guidance for common enterprise applications and infrastructure solutions. However, there are situations where you may need a higher degree of data protection to address operational requirements that others running the same application don't have. Consider these guidelines to be a starting point for thinking about your business requirements.

	REPLICATION FACTOR (RF)	SNAPSHOT INTERVAL	REPLICATION
Mission Critical	RF2 or RF3	1 hour	Synchronous (Nutanix) or application-based
Business Critical	RF2 or RF3	1-2 hours	Asynchronous (Nutanix) or application-based
General Virtualization	RF2	Daily	Asynchronous 2-4 hours
Application and Desktop Virtualization	RF2	File server with user data and infrastructure VMs: 1-2 hours	File server with user data and infrastructure VMs: 1-2 hours Golden image: daily

Table 1:
Nutanix general data protection guidelines

ENTERPRISE APPLICATIONS

TIER 0 AND TIER 1 DATABASES AND APPLICATIONS

These are the databases and associated applications that are mission critical to your organization.

Backup/restore. Mission-critical applications require regular backup (the more frequent the better) in addition to replication. Having regular backups allows you to quickly recover operations in the face of human errors or software bugs that corrupt data or take an application offline.

Disaster recovery. Whether you need synchronous replication or asynchronous replication depends on your RPO and RTO. For an RPO equal to zero, choose synchronous replication.

CUSTOM DATABASES AND APPLICATIONS

The applications in this class-developed in Java, .NET, and other languages-are considered important and are typically backed by relational database management solutions such as Microsoft SQL Server, MySQL, and PostgreSQL databases.

Backup/restore. These apps require regular backup. Taking snapshots every few hours is typical.

Disaster recovery. These applications require RPO and RTO of one hour or greater, making asynchronous replication the appropriate DR option.

MESSAGING AND COLLABORATION

This class of apps includes Microsoft Exchange and SharePoint, Avaya, and others.

Backup/restore. Apps such as Microsoft Exchange are business critical; the ability to recover individual mailboxes is highly desirable.

Disaster recovery. Resiliency is often built into the application. The Database Availability Groups (DAG) used by Exchange are one example. Snapshots can be important in other cases, such as reseeding DAG copies.

NEXT-GENERATION WEB-BASED APPLICATIONS

Enterprises are focusing efforts on Web-based application frameworks for development, often using NoSQL databases such as MongoDB and Cassandra. REST APIs may be used to integrate Nutanix data protection functions with an application.

Backup/restore. Backup and restore is an important defense against human errors and software bugs. For organizations doing continuous delivery (CD), snapshots and clones can provide a convenient way of rolling back changes if things don't go as expected.

Disaster recovery. Resiliency is often built into the application. Multiple instances of each application service are spread across a cluster and across locations.

APPLICATION AND DESKTOP VIRTUALIZATION

In organizations moving to application and desktop virtualization (VDI), the tendency is to continue providing the same level of data protection that was provided in the traditional desktop environment; organizations that don't back up physical desktops tend not to back up VDI.

An important caveat is that a failure in a VDI environment could idle a large number of employees; therefore, whether you protect user data or not, it's important to make sure the VDI environment itself is recoverable by backing up and possibly replicating databases, master images, etc.

Getting Started

We hope you're intrigued by the possibilities that Nutanix offers for keeping critical applications—including Oracle; SAP; and Microsoft SQL Server, Exchange, and SharePoint—up and running. Based on a foundation of resilient infrastructure, Nutanix provides integrated data protection to meet diverse needs for backup, replication, and DR. Nutanix helps you provide a higher level of data protection for important applications while reducing costs.

Ready to learn more about data protection and DR solutions for your organization? Contact us at info@nutanix.com, follow us on Twitter @nutanix, or send us a request at www.nutanix.com/demo to set up your own customized briefing and demonstration and see how validated and certified solutions from Nutanix can help your organization make the most of its enterprise applications.

Stay engaged with Nutanix experts and customers on the Nutanix Next online community (next.nutanix.com).

Nutanix makes infrastructure invisible, elevating IT to focus on the applications and services that power their business. The Nutanix enterprise cloud platform leverages web-scale engineering and consumer-grade design to natively converge compute, virtualization, and storage into a resilient, software-defined solution with rich machine intelligence. The result is predictable performance, cloud-like infrastructure consumption, robust security, and seamless application mobility for a broad range of enterprise applications. Learn more at www.nutanix.com or follow us on Twitter @nutanix.

T.855.NUTANIX (855.688.2649)
info@nutanix.com | www.nutanix.com | @nutanix