

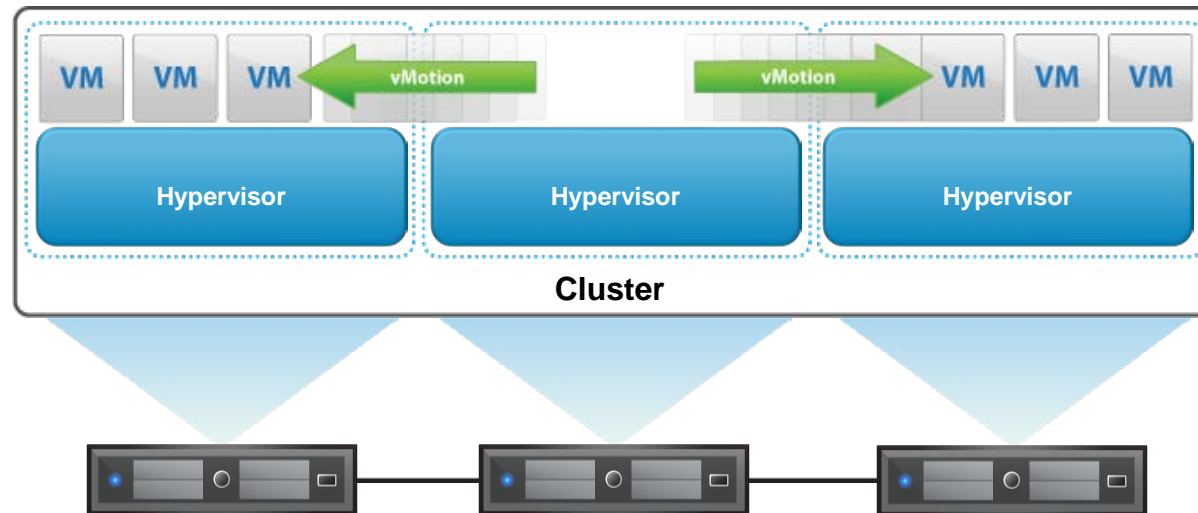
Lesson 1: Advanced Virtual Technologies – Live Migration

What is Live Migration?

Seamless migration of running virtual machines.

Zero downtime.

No loss of network data.



Pre-Requisites for Live Migration

Source and destination hosts must be able to run the virtual machine.

Accessibility to all storage that is used by the virtual machine.

Compatible CPUs.

Common network configurations.

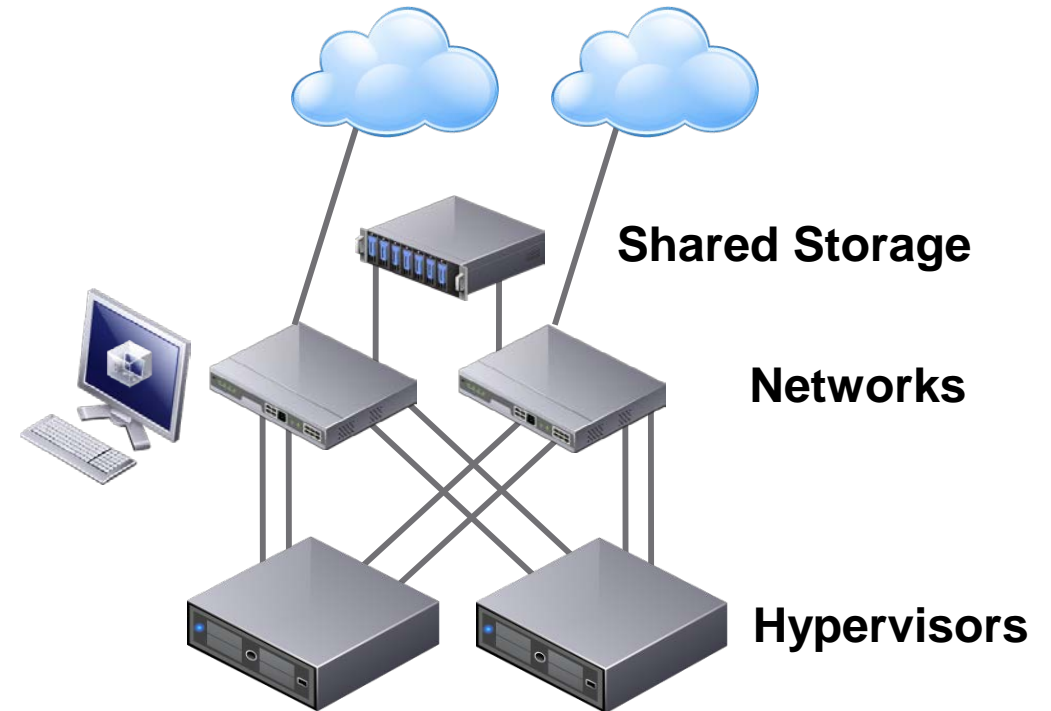
High capacity networks.

Compatible virtualization platform.

Live Migration Infrastructure

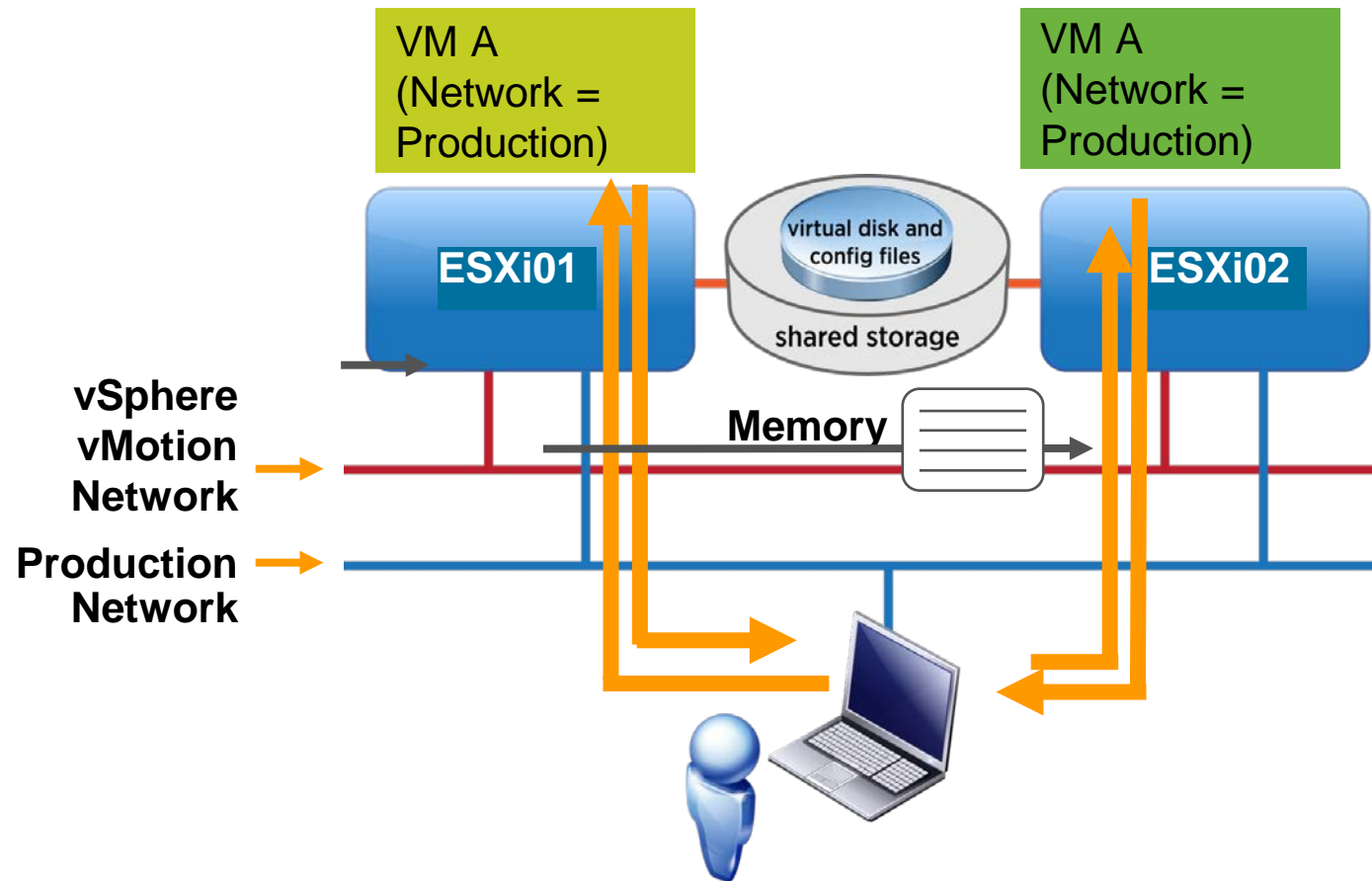
An infrastructure that enables live migration requires the following components:

- Compatible virtualization platform.
- Multiple hosts in a cluster with compatible CPUs.
- Common network configurations.
- High capacity network for migration data.



The Live Migration Process

The live migration process is a transfer of machine state between two hypervisors.



Live Migration Challenges and Issues

A fast, reliable network is required for synchronization.

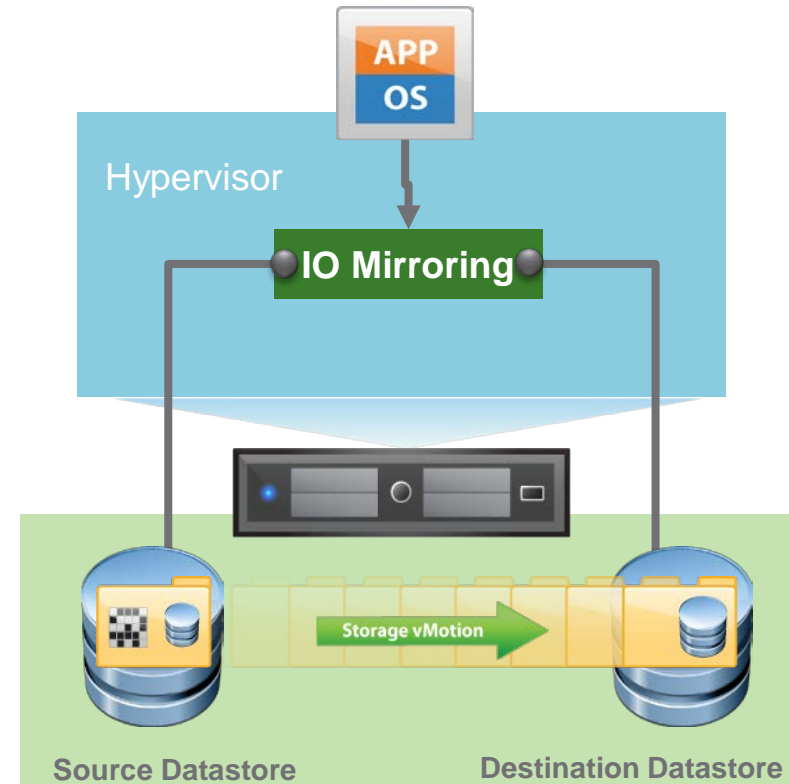
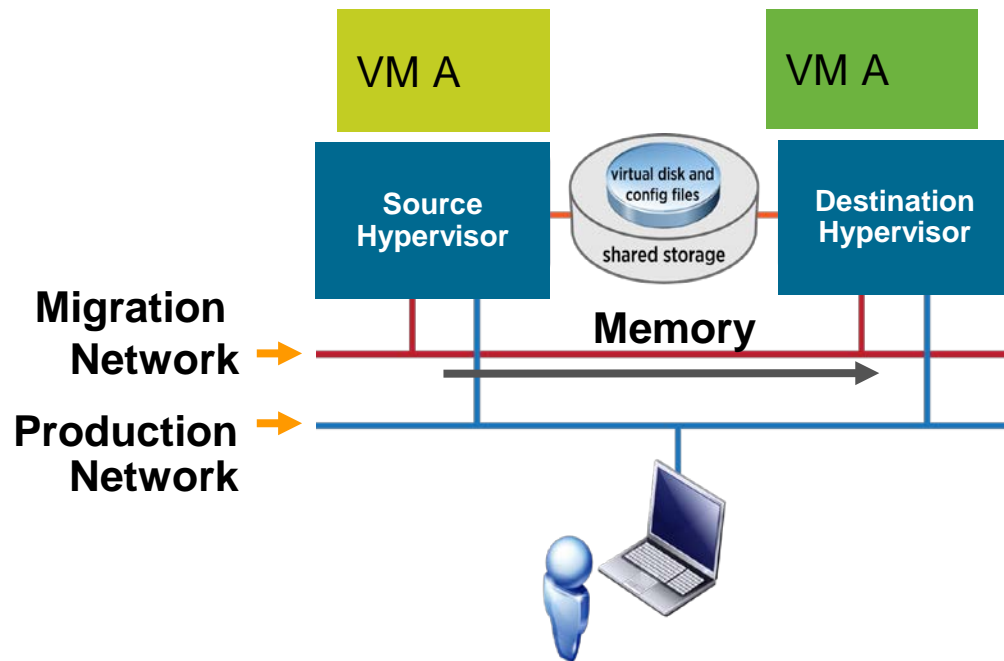
CPU compatibility is very strict.

Live migration that also migrates storage can take a long time.

There will be limits on the number of concurrent migrations.

The Role of Storage in Live Migration

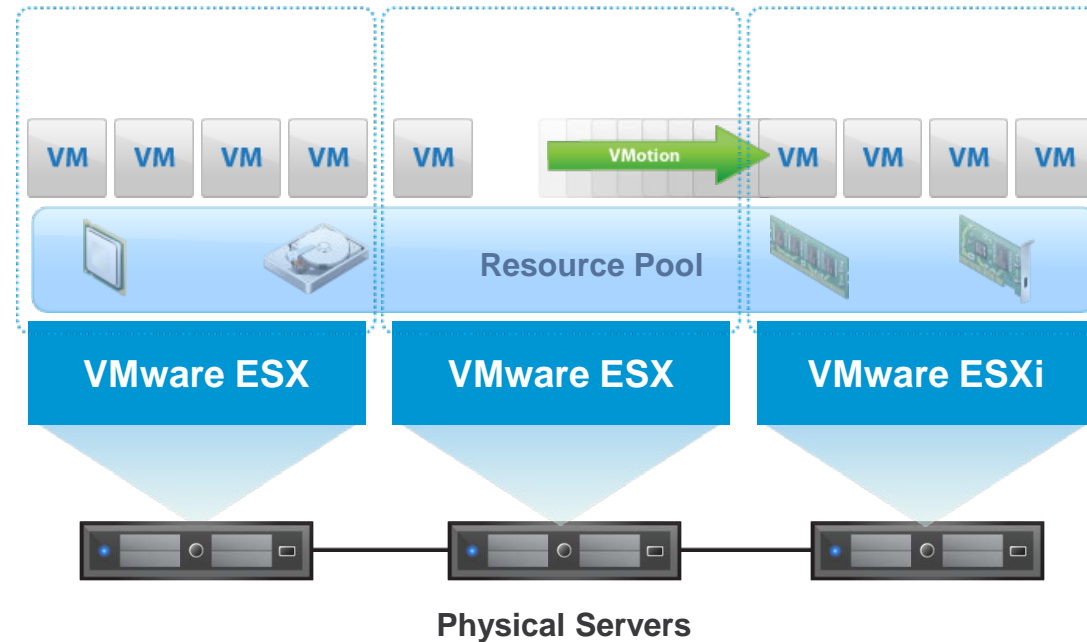
Platforms that support VMware vSphere® Storage vMotion®, no longer require virtual machines to run from shared storage. They do have higher demands on the live migration network though and can support fewer concurrent migrations.



Dynamic Load Balancing

VMware vSphere® Distributed Resource Scheduler™ uses a vSphere vMotion enabled cluster to load-balance systems in response to dynamic server load.

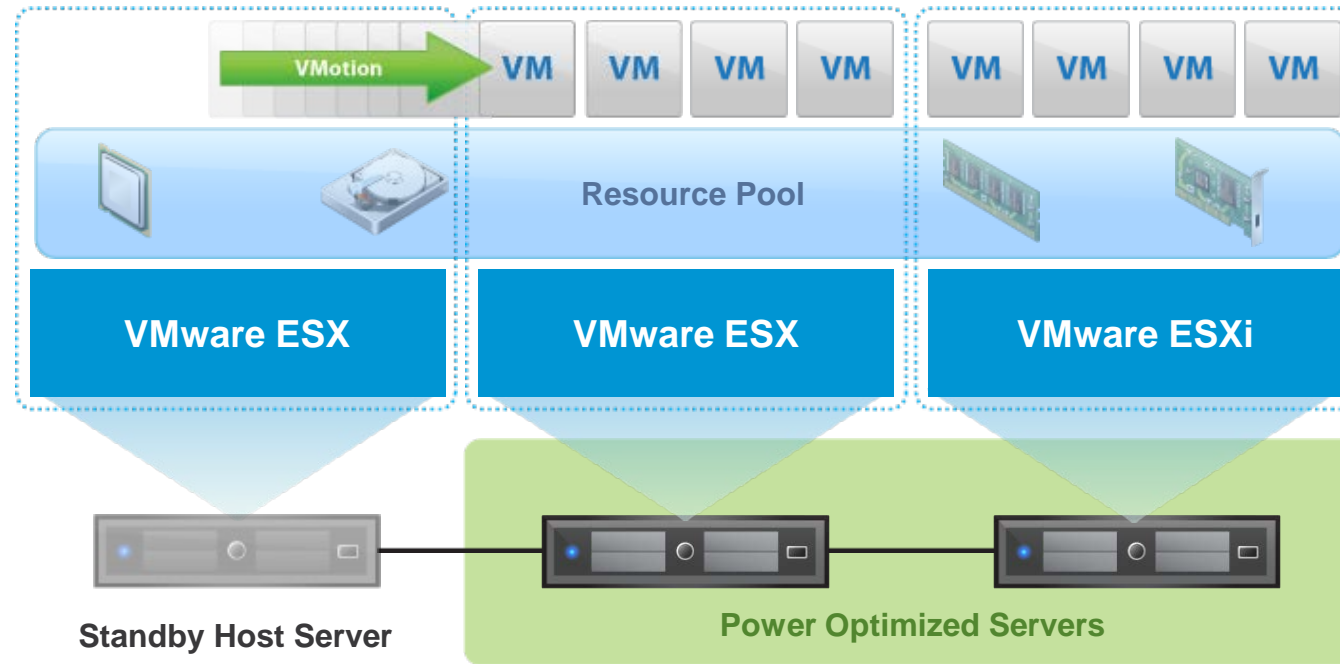
Load balancing ensures that resources are effectively utilized and minimises the impact on the remaining virtual machines in a cluster.



Dynamic Power Management

VMware vSphere® Distributed Power Management™ shuts down unused resources to save power and restarts nodes when demand increases again.

Hardware features are required that allow a system that is in a powered off state to be powered on.



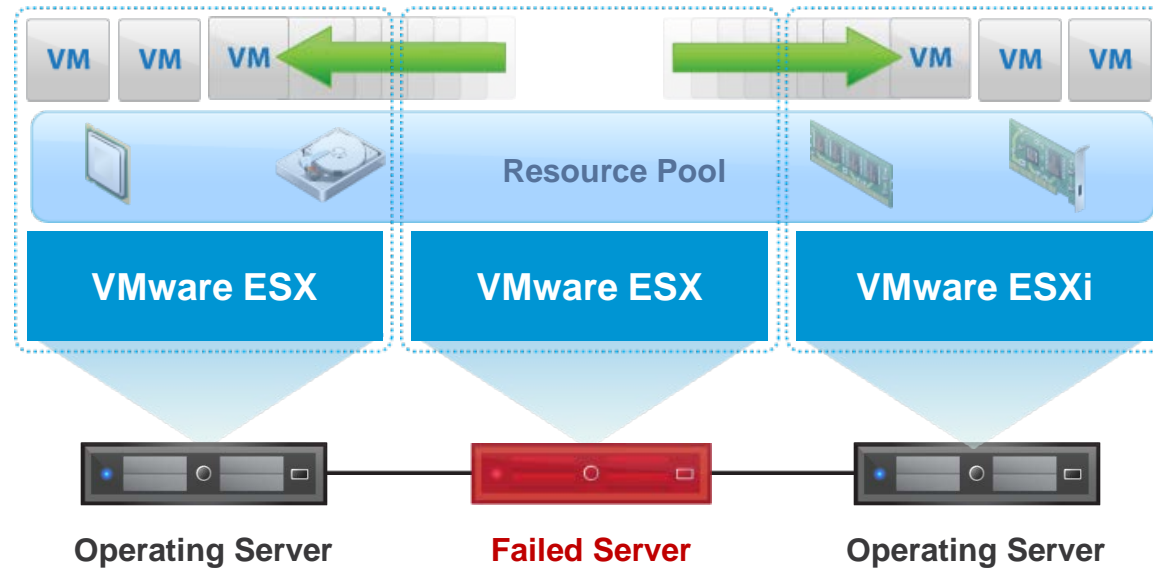
Lesson 2: Failover Technologies – High Availability and Fault Tolerance

High Availability

High availability allows systems to recover from a failure, or outage, to minimize the time the services they provide are unavailable.

In a server cluster, one server can take over the services provided by another in the case of a failure.

In a hypervisor cluster, the virtual machine running in one hypervisor will restart on another if the hypervisor it is running on fails.



The High Availability Failover Process

Nodes in the cluster monitor each other.

Nodes recognize cluster failure events.

Restart procedures and rules define the order and location of restarted virtual machines.

Nodes must be configured to recognize and respond to isolation.

High Availability Cluster Requirements

Shared storage is critical.

Common network configurations are necessary.

Sufficient spare capacity must be available.

Cluster management must have configured HA and the desired failure response behaviors.

Features and Benefits of High Availability

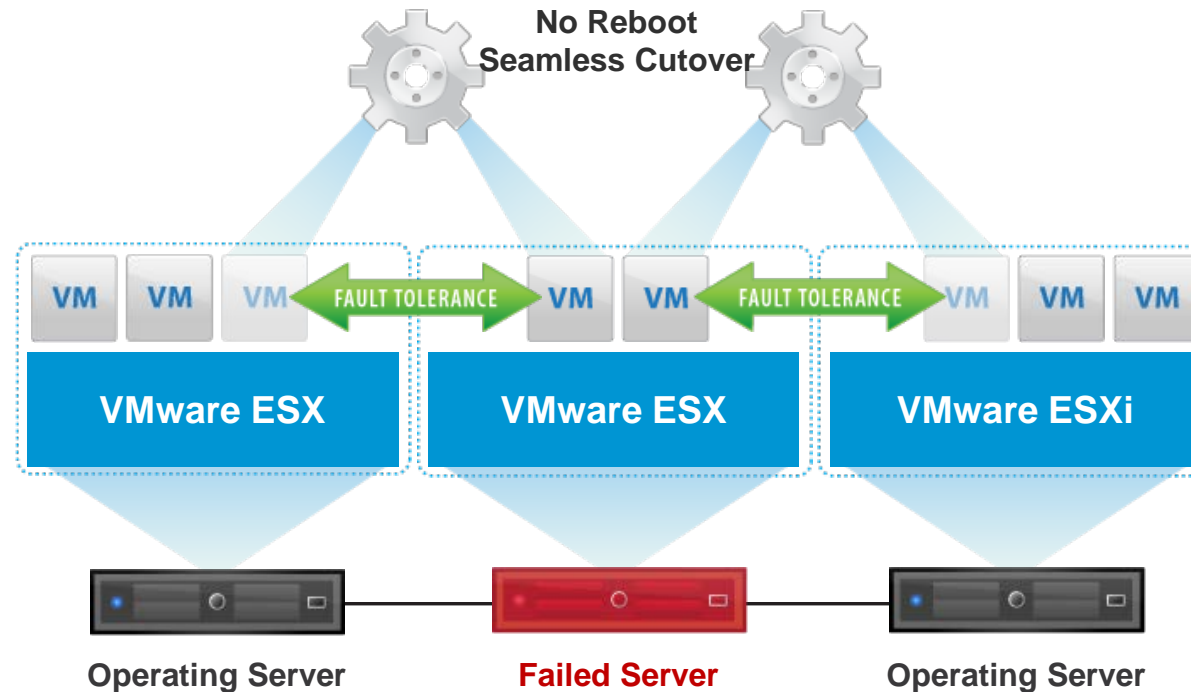
Automated restart of any service without administrator intervention.

Does not require custom solutions or dedicated clustering hardware for each solution.

The level of resilience can be adjusted to provide enhanced protection, for example, during maintenance.

Fault Tolerance

Two fully synchronized instances of a virtual machine are run on two separate hypervisors. If one hypervisor or virtual machine fails, the other continues to provide a service. Zero downtime is experienced.



Fault Tolerance Pre-Requisites

Shared storage must be used as the virtual machine runs simultaneously on separate hypervisors.

Storage for virtual machine files must be connected to both hypervisors.

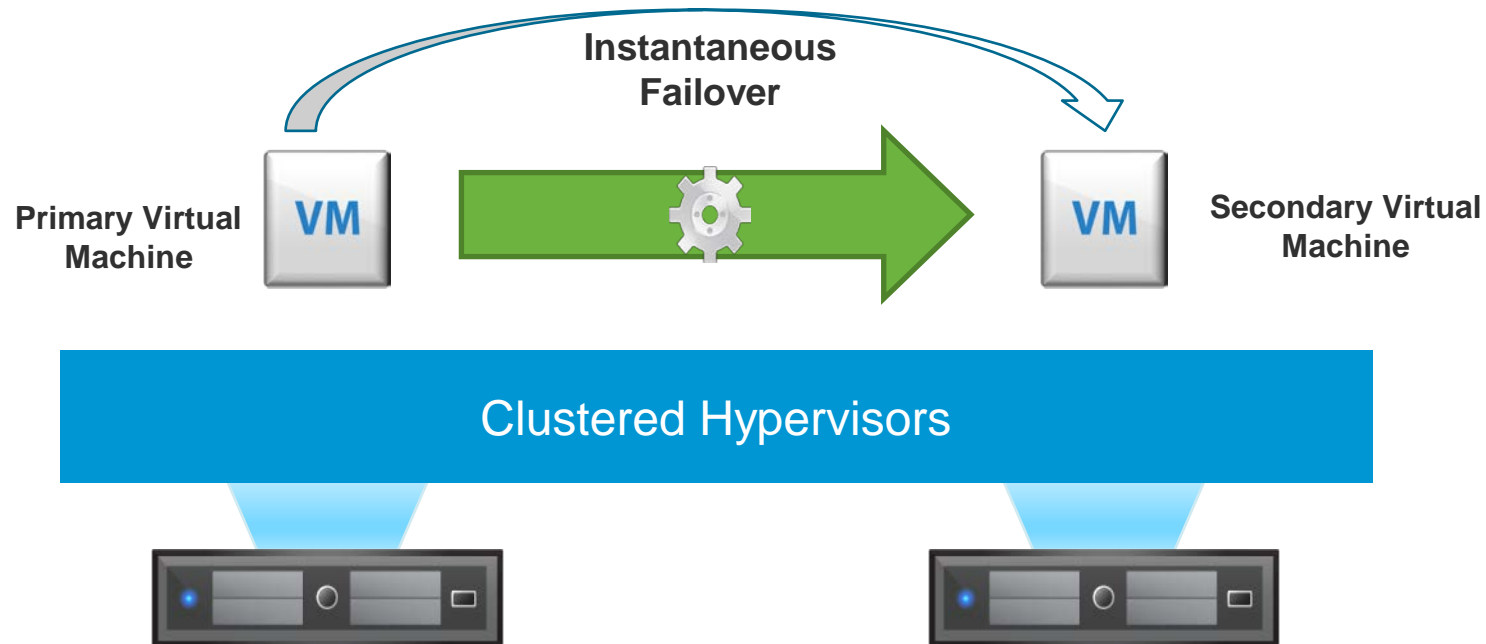
Reliable, high-bandwidth network connection.

CPU and RAM capacity.

Virtual machines are limited to one or two virtual CPUs.

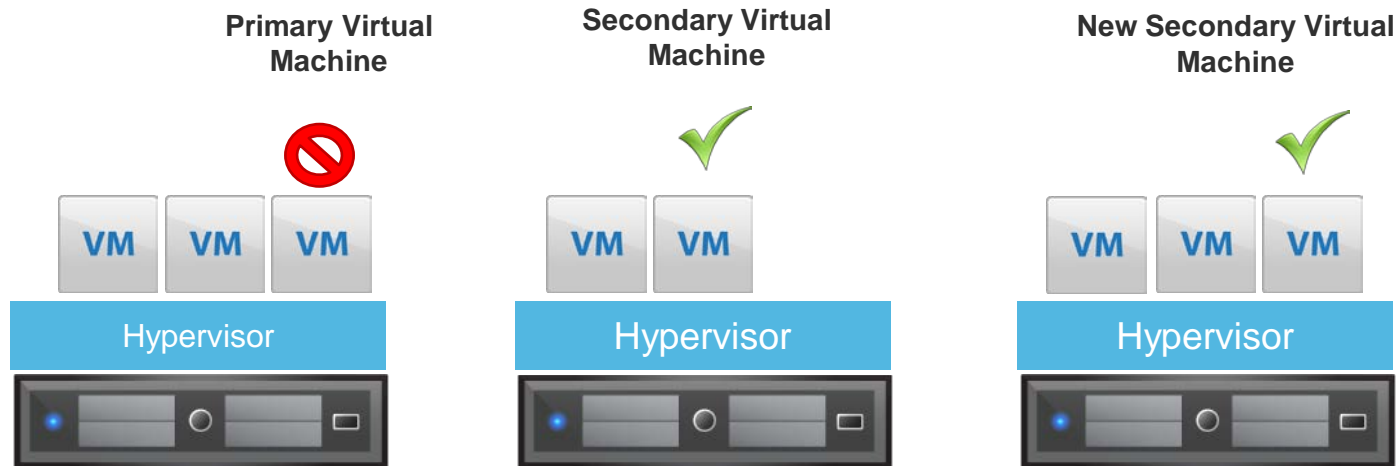
Fault Tolerance Operation

Fault tolerance starts up one virtual machine and then brings up the second instance. The synchronization process ensures the processor and memory state of both virtual machines remain in sync.



Fault Tolerance Failure Operation

The process that takes place when a failure occurs that affects one of the fault-tolerant lockstep machines differs dependant on whether the failure affects the primary or the secondary virtual machine.



Lesson 3: Snapshots – Point-in-Time Recovery

What are Snapshots?

Storage technique to provide access to a point-in-time version of a file, set of files, or file system.

Space efficient and very quick to create.

There are a number of techniques that differ in terms of performance impact and disk space requirements.

No impact on the live or current state.

Storage Technologies and Snapshots

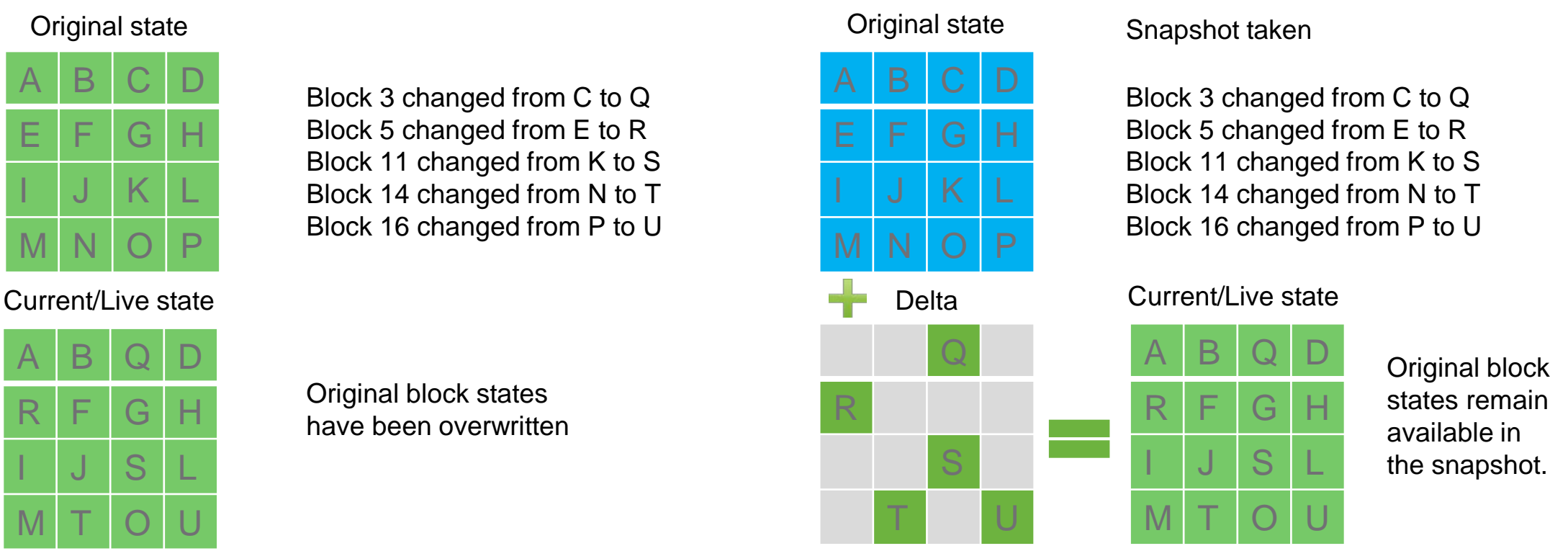
Snapshots are key features of SAN and NAS hardware arrays.

Some file systems support snapshots.

Hypervisors generally provide virtual machine snapshot capabilities.

Point-in-Time Checkpoints and Deltas

With a snapshot active (second diagram) the original disk is marked read-only. If a block changes, the new data is tracked in a delta disk. The delta disk, when combined with the original disk (now read-only), provides the current state of the system. The read-only copy can be used to roll back if necessary.



Rolling Data Back to a Point-in-Time

The main use of snapshots is to enable a disk to be reverted to an earlier point in time.

The administrator, or owner, can choose to roll back the file, set of files, or file system, to the snapshot.

Data changed since the snapshot was taken may be lost.

Some snapshot implementations allow for such data to be preserved in another snapshot.


The Impact of Snapshots

The presence of a snapshot has no effect on data unless a rollback is triggered.

Original state

A	B	C	D
E	F	G	H
I	J	K	L
M	N	O	P

Q,V,W,S,T,U written to disk

 Delta

		Q	
V			
	W	S	
Z	T		U

Current/Live state

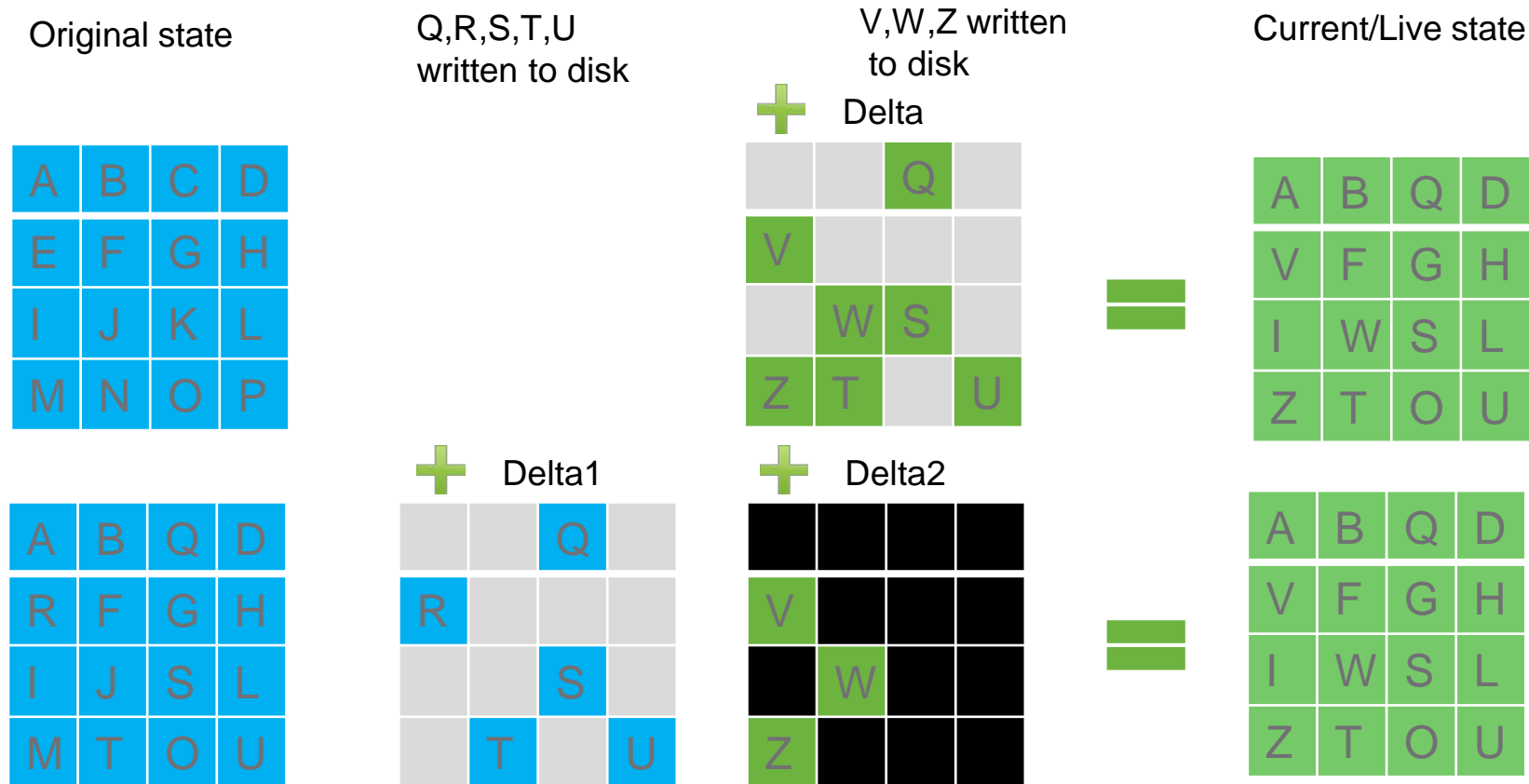
A	B	Q	D
V	F	G	H
I	W	S	L
Z	T	O	U

=

A	B	Q	D
V	F	G	H
I	W	S	L
Z	T	O	U

Multiple Snapshots

Multiple sequences of snapshots can be taken of the same system concurrently.

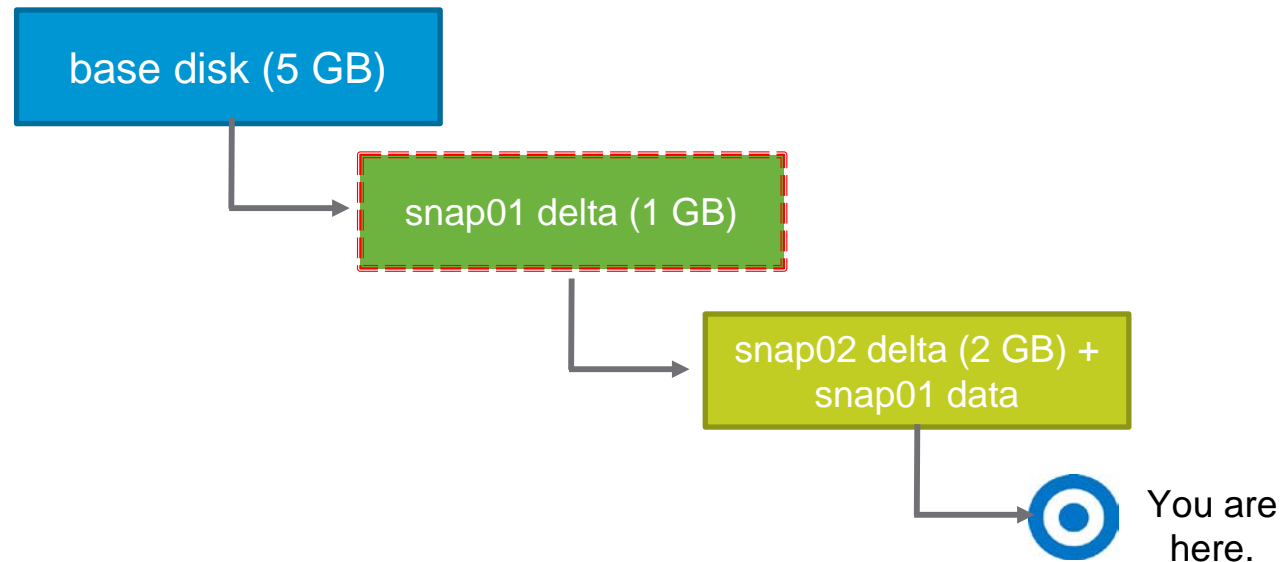


Snapshots Allow Virtual Machine States to be Rolled Back

Virtual machines are just a collection of files.

Virtual machine snapshots allow entire virtual machines to be rolled back quickly and easily.

Snapshots are efficient but cause virtual machine storage to grow so care must be taken.



Rolling Back a Virtual Machine Snapshot

A virtual machine snapshot always includes configuration and data files.

A virtual machine snapshot can also include the running virtual machine state, including CPU and RAM data.

Rolling back a storage-only snapshot that does not include the RAM and CPU state will restore a virtual machine to a powered off state.

Rolling back a snapshot that includes CPU and RAM will restore a running machine.

Snapshots that include the RAM and CPU state take more space and much more time to complete.

Snapshots are Short-Term Tools

Snapshots consume increasing amounts of space and should be avoided over long periods of time.

Snapshots should always be considered as short-term tools.

Snapshots are not independent of the system they protect so they must not be used instead of backups.

Snapshot Efficiency

Software-only snapshots incur some overhead.

Extra data must be read and written while snapshots are active.

Storage arrays provide dedicated hardware to improve snapshot performance.

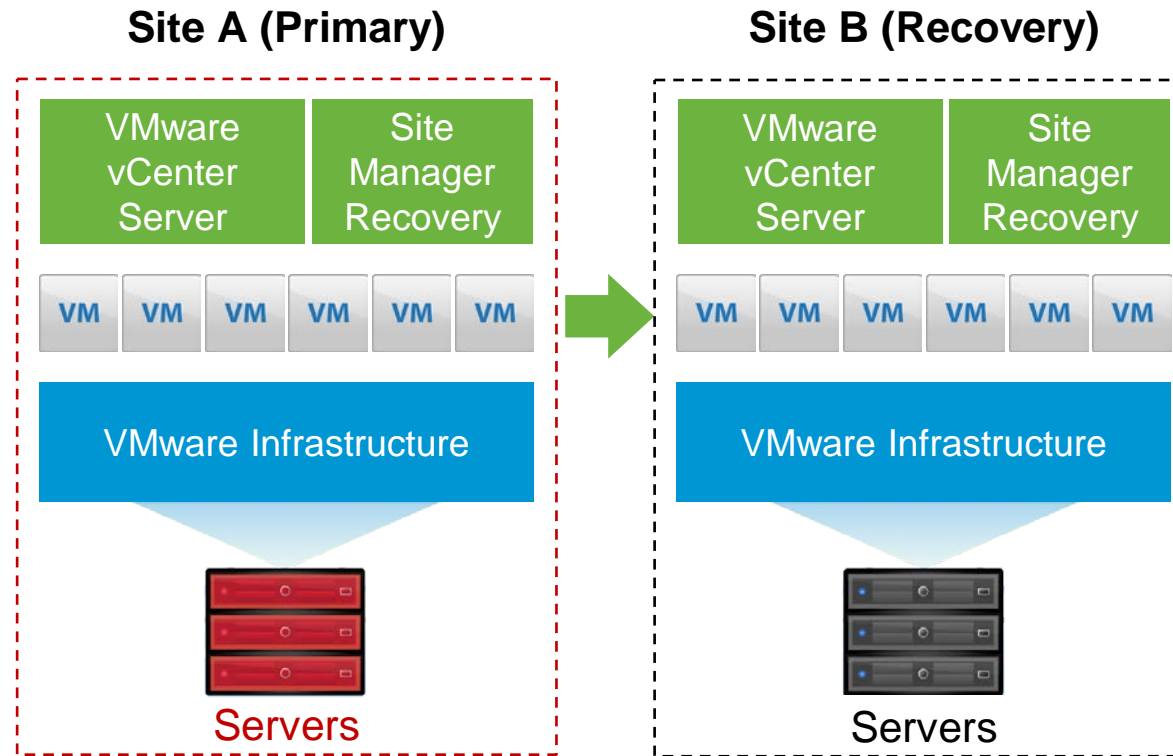


Lesson 4: Disaster Recovery and Business Continuity

Business Continuity and Disaster Recovery

Business continuity refers to plans and systems designed to deal with limited data or system losses.

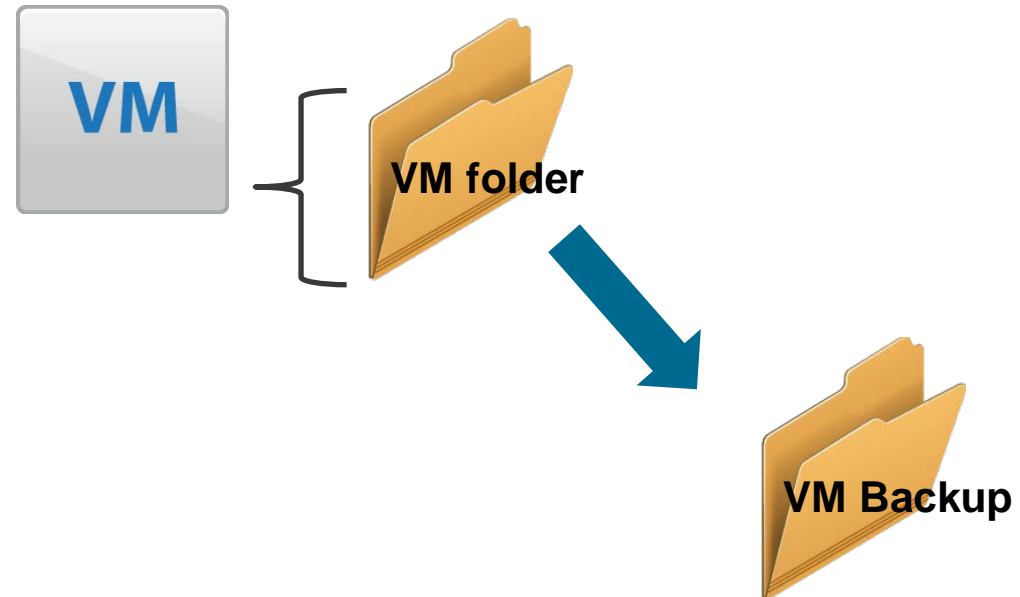
Disaster recovery refers to recovery that requires recovery when most or all infrastructure at a primary site has been lost.



Backing up Virtual Machines as Files

A virtual machine can be backed up by making a copy of its files.

Configuration file	<code>VM_name.vmx</code>
Swap files	<code>VM_name-*.vswp</code> <code>vmx-VM_name-*.vswp</code>
BIOS file	<code>VM_name.nvram</code>
Log files	<code>vmware.log</code>
Template configuration file	<code>VM_name.vmtx</code>
Disk descriptor file	<code>VM_name.vmdk</code>
Disk data file	<code>VM_name-flat.vmdk</code>
Raw device map file	<code>VM_name-rdm(p).vmdk</code>
Snapshot disk file	<code>VM_name-#####-delta.vmdk</code>
Snapshot data file	<code>VM_name.vmsd</code>
Snapshot state file	<code>VM_name-Snapshot#.vmsn</code>
Snapshot memory file	<code>VM_name-Snapshot#.vmem</code>
Suspend state file	<code>VM_name-*.vmss</code>
Suspended snapshot memory	<code>VM_name-*.vmem</code>



Data Consistency and Backing Up Running Virtual Machines

Running virtual machines have active disks.

Simple copies may result in corrupt disk data.

Shutting down applications allows for safe backups.

Application downtime is required for backup windows.

Data Consistency and Quiescing Disks

Backup solutions need to ensure that unwritten disk data is flushed out of any memory cache.

An agent inside the operating system of a virtual machine can ensure the virtual disk's application data is consistent.

In VMware environments this capability is one of the functions of VMware Tools™, which should be installed in all virtual machines.

Placing a disk into a temporary inactive state is referred to as quiescing.

Crash Consistency

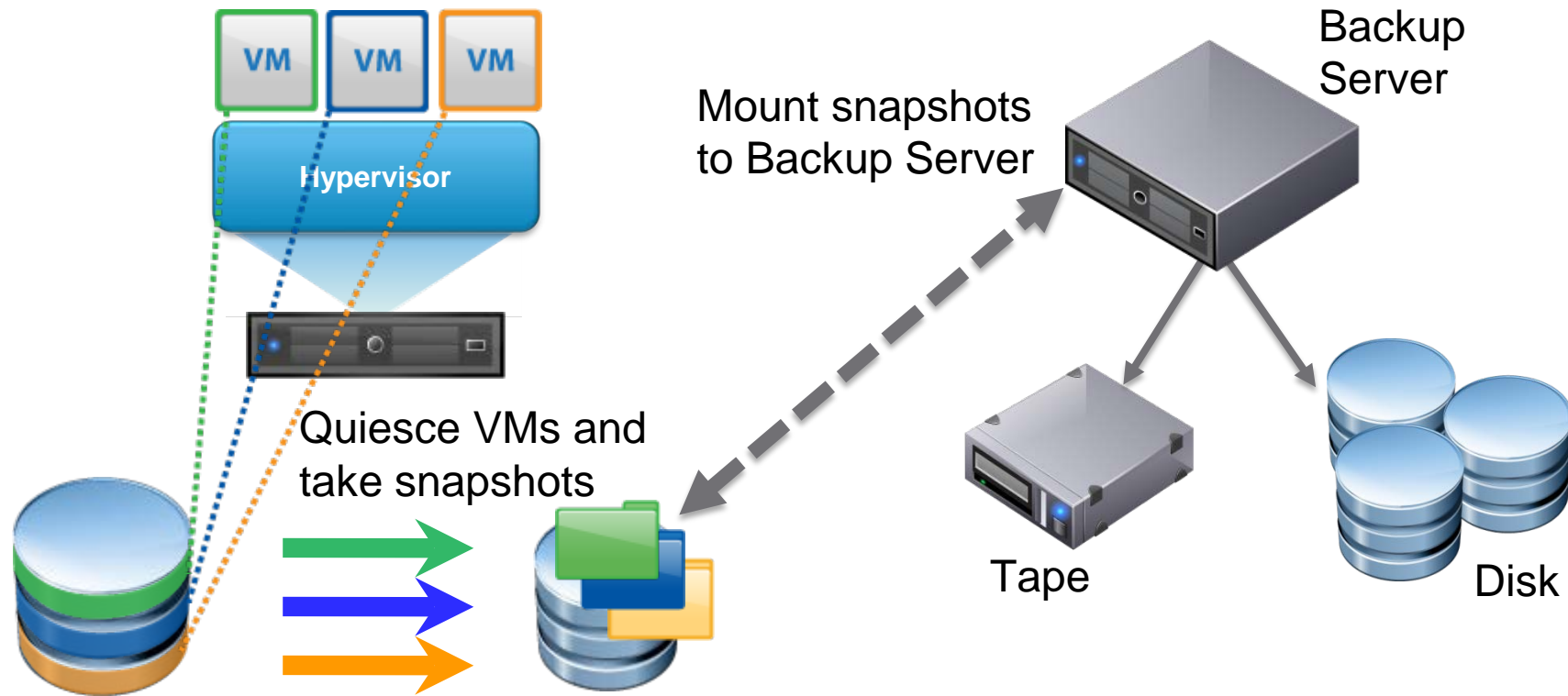
Crash consistent data avoids corruption of virtual machine file system data when a backup, or copy, is made of a running virtual machine's disks.

Quiescing in this way is not sufficient on its own as the virtual disks cannot be kept quiesced for long periods without interfering with applications.

Backup windows, where services are unavailable for many hours, are unacceptable for many modern solutions.

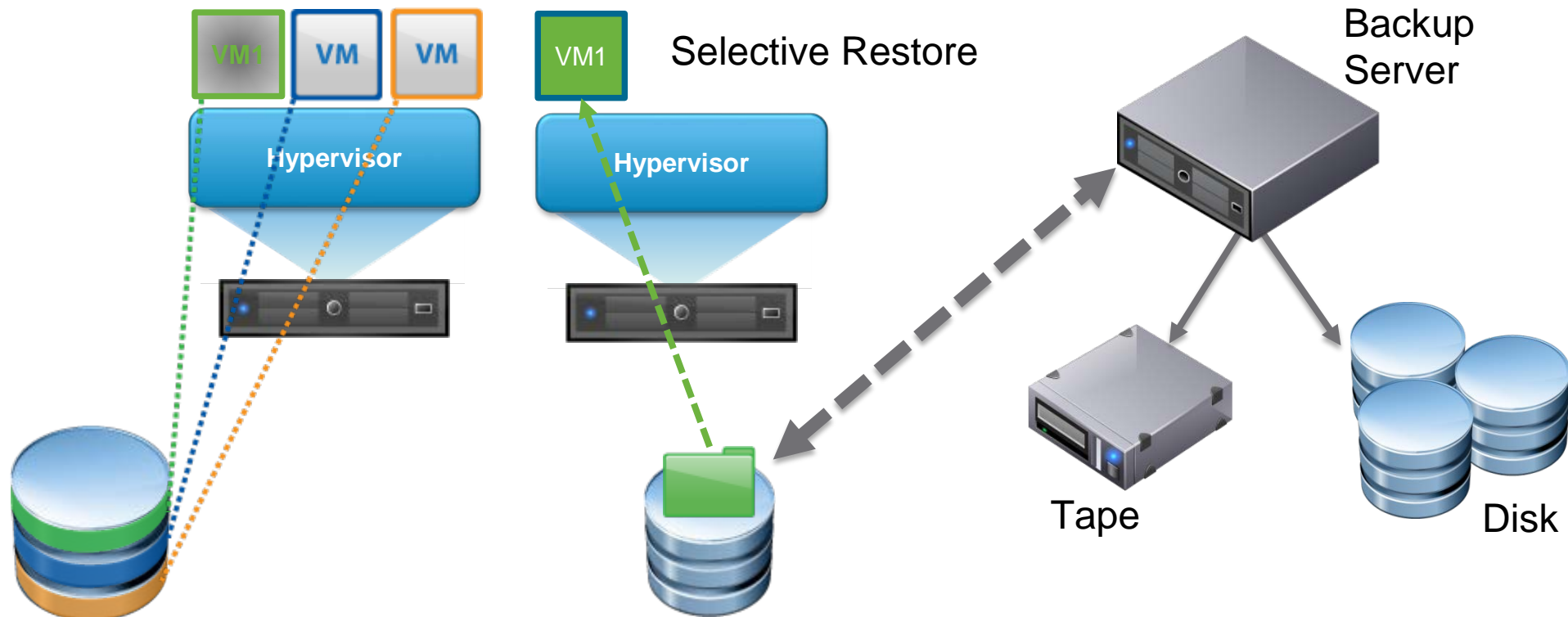
Snapshots and Backups

During a backup, a snapshot can be used to maintain read-only copies of the disks to be backed up. This allows the virtual machine, and its applications, to quickly return to full operation.



Selective Restore of Virtual Machine Data

Restoring partial data is easier in a virtual environment because the restore task can target a new, isolated virtual machine.



The role of Snapshots in Replication

Disaster recovery of virtual infrastructure requires the ability to make copies of virtual machines.

Backup based solutions are an option but the recovery time may be very long.

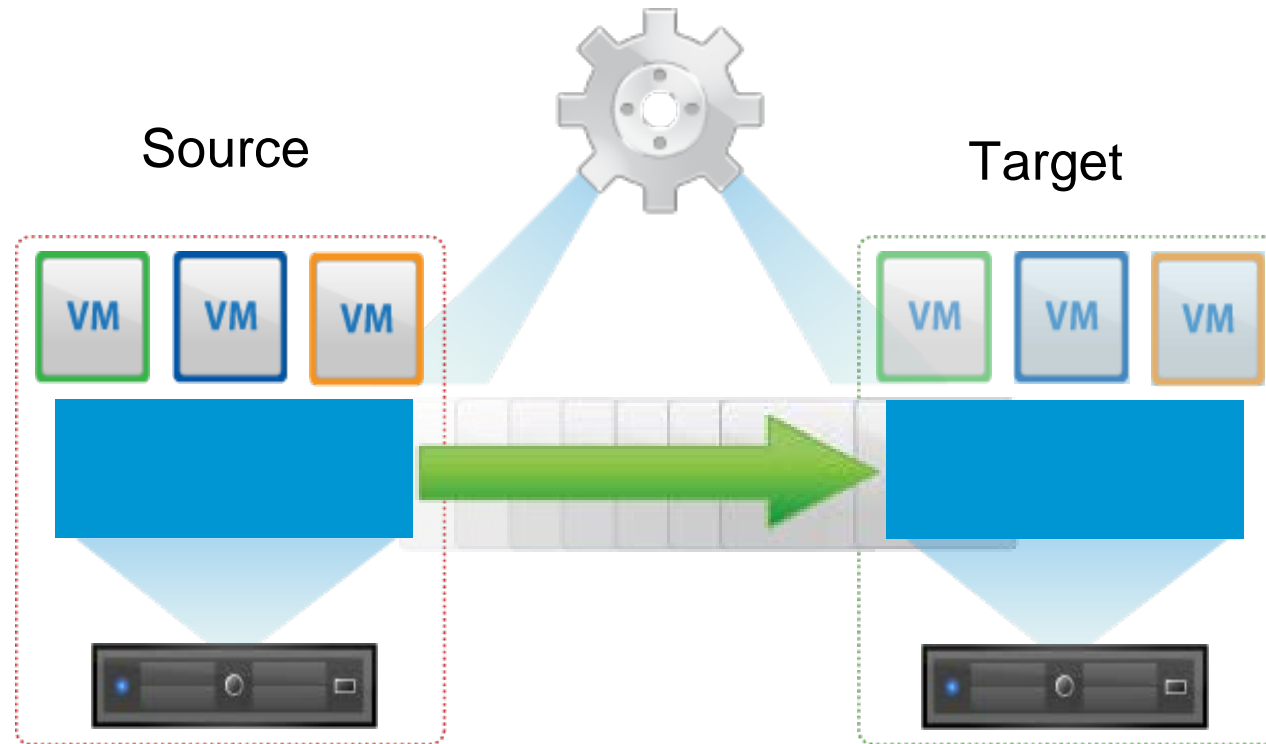
Replication of virtual machines and entire solutions is a better approach.

Replication of virtual machines is simpler than the replication of non-virtualized machines.

Replication can use snapshots and agents running inside virtual machines to ensure that replicated disks are consistent and not corrupt.

Automated Replication

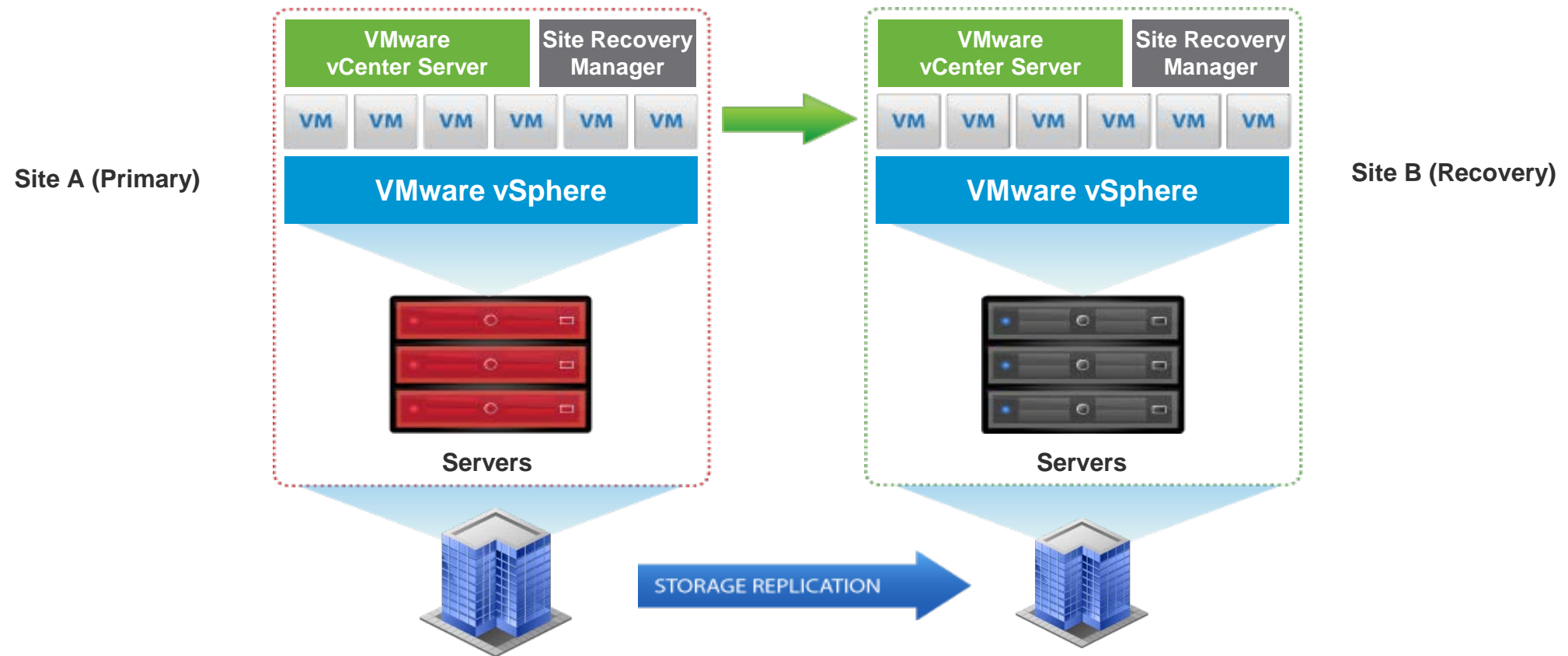
Automated replication enables organisations to implement robust disaster emergency plans. Virtual infrastructure makes it much easier to implement because everything is in software.



Orchestration of Replication

Powerful disaster recovery solutions viable with VMware Site Recovery Manager™.

Replication recovery plan restarts servers in a defined sequence.



Lesson 5: Cloud Disaster Recovery and Archiving

Traditional Business IT and the Cloud

Traditional IT infrastructure models do not map easily to the cloud.

Traditional IT solutions:

- Designed for a fixed capacity that changes slowly.
- Infrastructure must be able to cope with peak loads, requires idle capacity.

Cloud native solutions:

- Rely on automation to scale automatically and minimise costs at all time.
- Scale-out and scale-in as necessary.

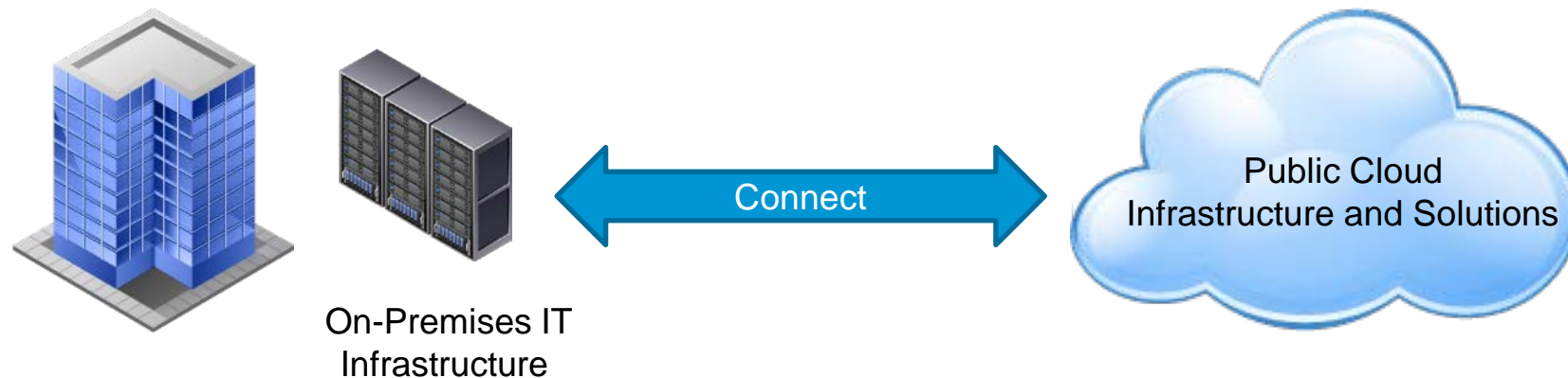
Existing IT solutions can be hard to move to a cost efficient cloud model.

Hybrid Cloud and the Transition to Cloud

Many organizations adopt a hybrid cloud approach rather than re-engineer core services:

- Maintain existing infrastructure as needed.
- Expand some existing services into the cloud where possible.
- Leverage the cloud for new solutions.

Core IT infrastructure hosted on-premises will be cost competitive for traditional applications. An effective hybrid solution can deliver the benefits of both on-premises solutions and cloud solutions.



Unified Management of Hybrid Clouds

Minimizing the range of management solutions in hybrid environments is a major concern.

Management tools are the key to productivity in IT administration.

Minimizing the number of IT administration consoles or tools is a priority.

Single-pane-of-glass management is ideal.

Hybrid cloud management consoles or tools that enable seamless integration of management of on-premises infrastructure and cloud is ideal.

Disaster Recovery

Cloud based disaster recovery and DRaaS solutions are easy to implement.

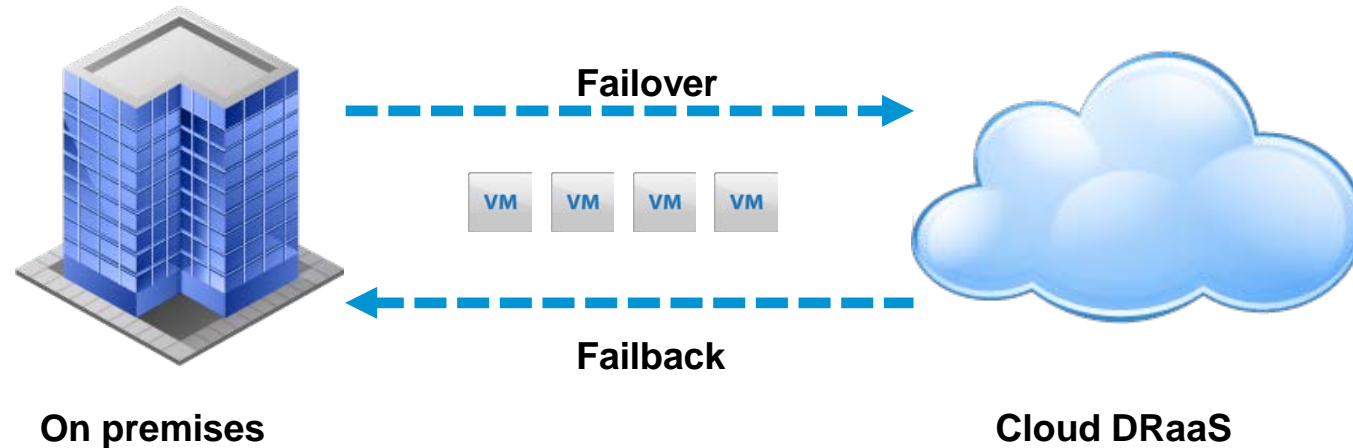
Cloud model matches disaster recovery planning very well.

Wholly owned disaster recovery capacity can be a very expensive solution.

Adjusting DR capacity over time is a challenge that the cloud can easily deal with.

Cloud storage solution models work well with disaster recovery.

Automation is key for disaster recovery.

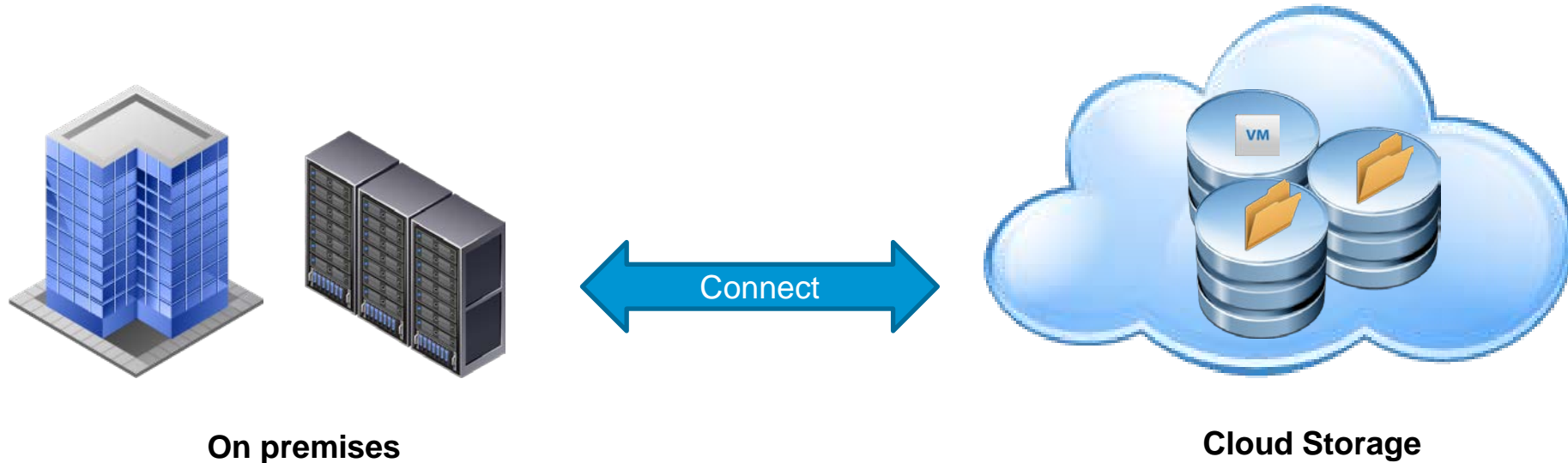


Off-Premises Archiving

Low-cost, archive-grade cloud storage can be used by most organizations.

Cloud storage provides excellent solutions for archive use cases.

Archiving supports the long-term retention of virtual machine images.



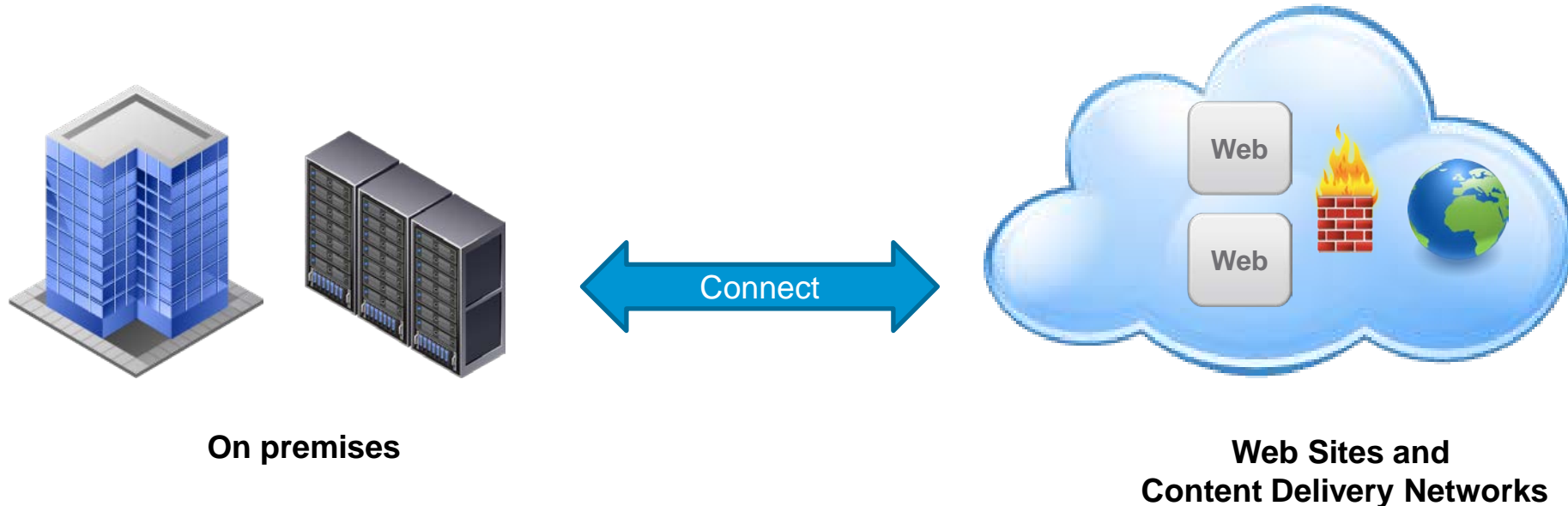
Separating Web Services from Core IT

The cloud can be used to isolate risky public services from core IT infrastructure.

Online business services, such as e-commerce, may be better handled by a cloud provider.

Cloud infrastructure benefits from high-end firewall and load balancing infrastructure and expertise.

Web presence at a scale that needs Content Delivery Network (CDN) services or Denial-of-Service (DoS) protection requires integration of those cloud services already.



Cloud Virtual Desktop Infrastructure

Cloud VDI provides organizations with rapidly scalable high performance user services.

Organizations that might have a sudden or short-term or need for additional end user desktop systems are a good match for cloud-based virtual desktops:

- Events organization companies.
- Emergency and disaster response teams.
- Political campaigns.
- Organizations with a high seasonal variability or that are highly mobile.
- Help desks and admin for retail businesses with seasonal trading peaks.
- Mobile sales workforces.

Organizations that have a need to provide a very secure, tightly managed, end-user computing environment but who do not have the expertise or resources to manage such an environment can benefit from cloud VDI.

The role of SaaS in the adoption of the Cloud

Many organizations are moving certain functions to the cloud through the SaaS route.

The adoption of SaaS solutions might be easier than migrating existing applications to IaaS.

The initial adoption of SaaS is likely to include some of the following core business IT services:

- Salesforce.com for CRM.
- Workday for HR management.
- Outlook.com or Gmail for email.
- Dropbox for storage and team collaboration.

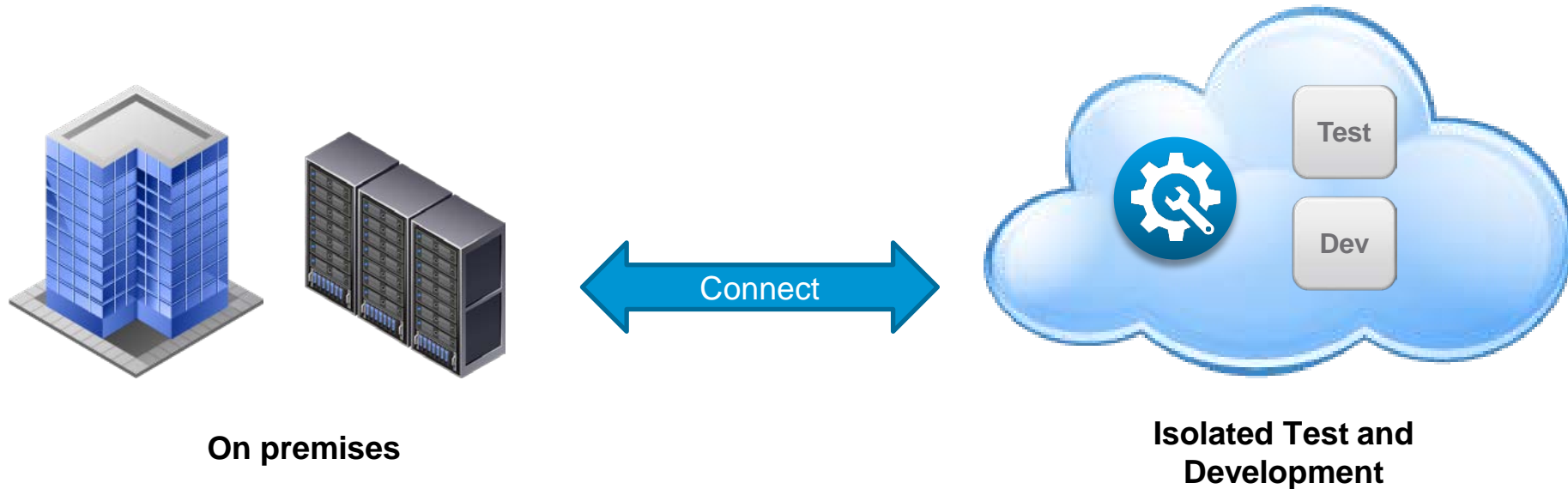


Cloud-Based Test and Development

Test and development are often the initial testing ground for adopting new technologies and platforms in an organization.

The cloud makes it easy to build safe, isolated sandboxes for test and development.

Systems administrators and DevOps teams can easily build test/integration phases into deployment procedures with the cloud.



Temporary Scaling

Temporary scaling accommodates temporary capacity requirements by scaling out to the cloud.

Provides temporary capacity through the cloud as an alternative to purchasing systems that will end up idle.

Responds to unplanned outages, or partial disasters, by opting for the cloud as a temporary workaround.

Providing Geographical Reach

Cloud solutions simplify the task of delivering data center level infrastructure close to remote locations or different jurisdictions.

Local VPN endpoints for an organization's global workforce.

Local CDN endpoints for websites.

Ensures customer data/services are securely provided within a fixed legal or geographical boundary.

