CPAC
CONTINGENCY PLANNING ASSOCIATION OF THE CAROLINAS

Cloud-Based Business Continuity and Disaster Recovery

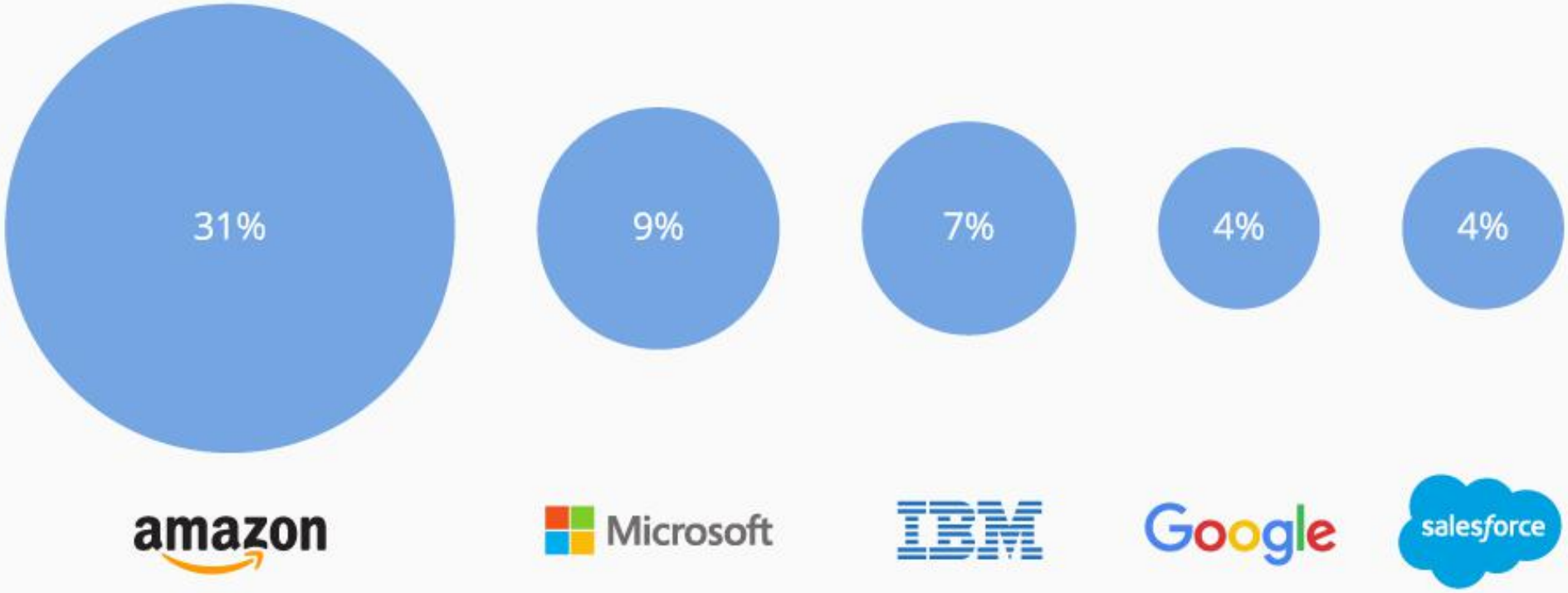
CPAC November 9, 2016 Meeting

Manuel W. Lloyd, ITIL® Certified
CEO, Manuel W. Lloyd Consulting®

- US Election
- Happy Birthday Marine Corps
- Happy Veteran’s Day

Top 5 Cloud Infrastructure Service Providers

Worldwide cloud infrastructure services market share in 2015*



* includes IaaS, PaaS, private & hybrid cloud services

Source: Synergy Research Group

Cloud Business Continuity and Disaster Recovery

- Cloud environments provide common elements to support the availability of workloads through its fabric and fabric management infrastructure.
- Availability targets in cloud environments can be achieved either through
  - the design of native workload availability constructs
  - the capabilities of the hosting cloud infrastructure
  - or a combination of both.
- Guidance on supporting BC/DR scenarios across public, private and hybrid cloud environments using each environment’s unique capabilities.

Cloud BC/DR Decision Points

- Data Location – The data within the application and the level of trust the organization has with the cloud services being provided for data. Data can be active or passive (data-at-rest) in nature.
- Failover Mechanism – The location of both the control point and the failover mechanism itself.
- Backup (and Restoration) - The mechanism used to back up the workload and the location of the associated backup data.

BC/DR Options – Private Cloud Only

- The organization leverages on-premises cloud constructs to host the data, failover mechanism and backup infrastructure
- Potential drivers for adopting this model include:
  - A requirement to control and manage the data on-premises
  - Incompatibility with public cloud offerings.

BC/DR Options – Public Cloud Only

- Leverages public cloud IaaS and PaaS constructs to support availability of the application or service
- Only public cloud capabilities are used for the data, failover mechanism and backup infrastructure.
- Potential drivers for adopting this model include:
  - Public cloud capabilities exceed those found on-premises
  - Lower costs

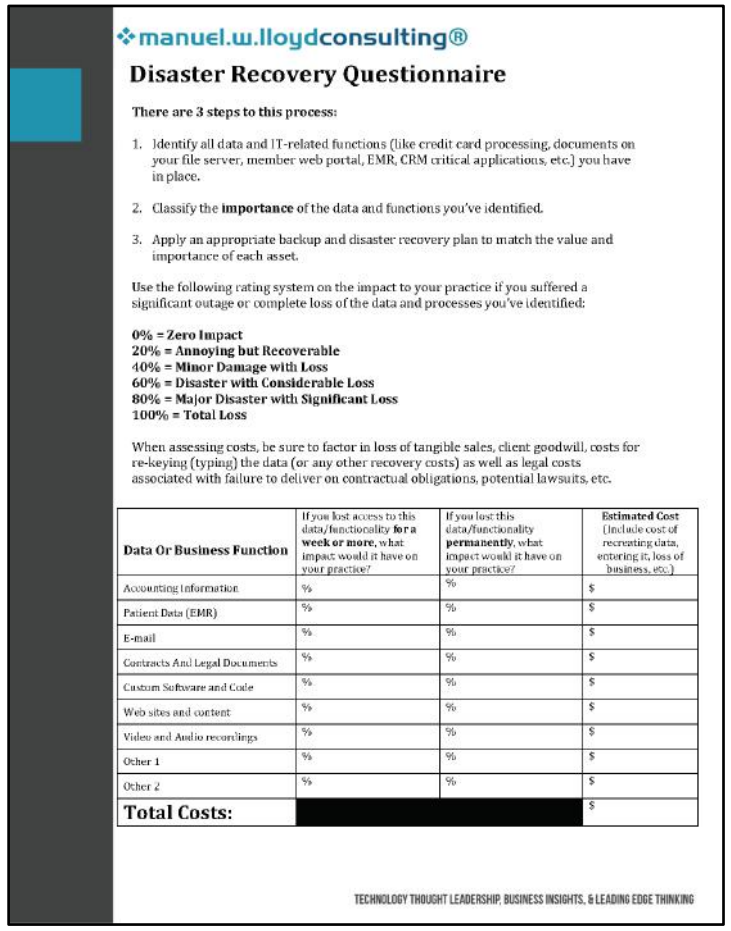
BC/DR Options – Hybrid Cloud

- Leverages a combination of public and private cloud constructs across three sub-models:
  - "Low Touch" - The workload's data and backup remain on-premises while failover mechanism is either hosted or controlled by the public cloud.
  - "Medium Touch" - The workload's live data remains on-premises while data-at-rest (backup) and the failover mechanism is either hosted or controlled by the public cloud.
  - "High Touch" – Leverages the traditional method of hybrid cloud deployment where a given workload's live data spans on-premises and public cloud infrastructures along with data-at-rest (backup) and the failover mechanism itself.

CPIF BC/DR Model

Native Private Cloud	Low Touch Hybrid Cloud	Medium Touch Hybrid Cloud	High Touch Hybrid Cloud	Native Public Cloud
Data, failover mechanism and backup leverage on-premises constructs	Data and backup remain on-premises while failover mechanism leverages public cloud capabilities	Active data remains on-premises while backup and failover mechanism leverages public cloud capabilities	Active data remains on-premises while passive data, backup and failover mechanism leverages public cloud capabilities	Data, failover mechanism and backup leverage public cloud constructs

Disaster Recovery Questionnaire



manuel.w.lloydconsulting®

Disaster Recovery Questionnaire

There are 3 steps to this process:

1. Identify all data and IT-related functions (like credit card processing, documents on your file server, member web portal, EMR, CRM critical applications, etc.) you have in place.
2. Classify the **importance** of the data and functions you've identified.
3. Apply an appropriate backup and disaster recovery plan to match the value and importance of each asset.

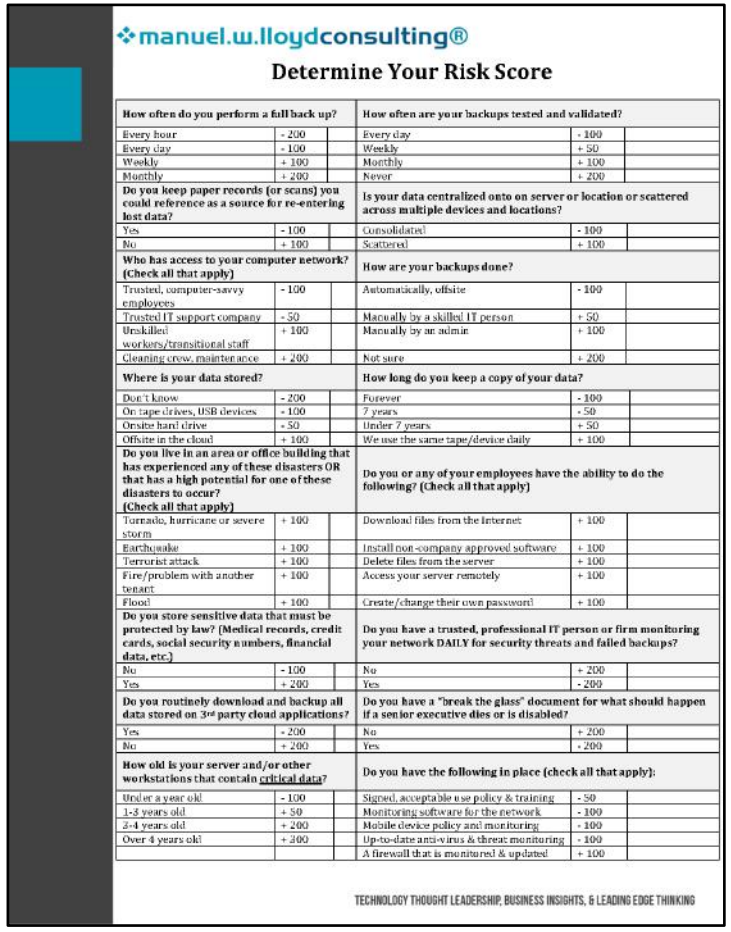
Use the following rating system on the impact to your practice if you suffered a significant outage or complete loss of the data and processes you've identified:

0% = Zero Impact
20% = Annoying but Recoverable
40% = Minor Damage with Loss
60% = Disaster with Considerable Loss
80% = Major Disaster with Significant Loss
100% = Total Loss

When assessing costs, be sure to factor in loss of tangible sales, client goodwill, costs for re-keying (typing) the data (or any other recovery costs) as well as legal costs associated with failure to deliver on contractual obligations, potential lawsuits, etc.

Data Or Business Function	If you lost access to this data/functionality **for a week or more**, what impact would it have on your practice?	If you lost this data/functionality **permanently**, what impact would it have on your practice?	**Estimated Cost** (Include cost of recreating data, entering it, loss of business, etc.)
Accounting Information	%	%	$
Patient Data (EMR)	%	%	$
E-mail	%	%	$
Contracts And Legal Documents	%	%	$
Custom Software and Code	%	%	$
Web sites and content	%	%	$
Video and Audio recordings	%	%	$
Other 1	%	%	$
Other 2	%	%	$
Total Costs:			$

TECHNOLOGY THOUGHT LEADERSHIP, BUSINESS INSIGHTS, & LEADING EDGE THINKING

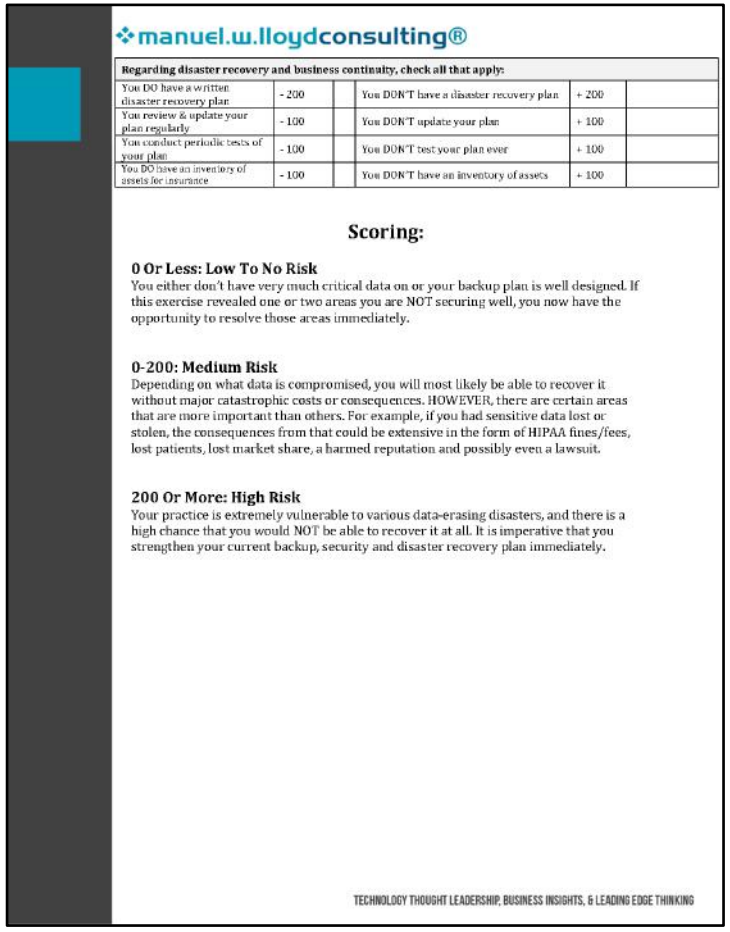


manuel.w.lloydconsulting®

Determine Your Risk Score

How often do you perform a full back up?			How often are your backups tested and validated?		
Every hour	- 200		Every day	- 100	
Every day	- 100		Weekly	+ 50	
Weekly	+ 100		Monthly	+ 100	
Monthly	+ 200		Never	+ 200	
Do you keep paper records (or scans) you could reference as a source for re-entering lost data?			**Is your data centralized onto on server or location or scattered across multiple devices and locations?**		
Yes	- 100		Consolidated	- 100	
No	+ 100		Scattered	+ 100	
Who has access to your computer network? (Check all that apply)			**How are your backups done?**		
Trusted, computer-savvy employees	- 100		Automatically, offsite	- 100	
Trusted IT support company	- 50		Manually by a skilled IT person	+ 50	
Unskilled workers/transitional staff	+ 100		Manually by an admin	+ 100	
Cleaning crew, maintenance	+ 200		Not sure	+ 200	
Where is your data stored?			**How long do you keep a copy of your data?**		
Don't know	- 200		Forever	- 100	
On tape drives, USB devices	- 100		7 years	- 50	
Onsite hard drive	- 50		Under 7 years	+ 50	
Offsite in the cloud	+ 100		We use the same tape/device daily	+ 100	
Do you live in an area or office building that has experienced any of these disasters OR that has a high potential for one of these disasters to occur? (Check all that apply)			**Do you or any of your employees have the ability to do the following? (Check all that apply)**		
Tornado, hurricane or severe storm	+ 100		Download files from the Internet	+ 100	
Earthquake	+ 100		Install non-company approved software	+ 100	
Terrorist attack	+ 100		Delete files from the server	+ 100	
Fire/problem with another tenant	+ 100		Access your server remotely	+ 100	
Flood	+ 100		Create/change their own password	+ 100	
Do you store sensitive data that must be protected by law? (Medical records, credit cards, social security numbers, financial data, etc.)			**Do you have a trusted, professional IT person or firm monitoring your network DAILY for security threats and failed backups?**		
No	- 100		No	+ 200	
Yes	+ 200		Yes	- 200	
Do you routinely download and backup all data stored on 3rd party cloud applications?			**Do you have a "break the glass" document for what should happen if a senior executive dies or is disabled?**		
Yes	- 200		No	+ 200	
No	+ 200		Yes	- 200	
How old is your server and/or other workstations that contain critical data?			**Do you have the following in place (check all that apply):**		
Under a year old	- 100		Signed, acceptable use policy & training	- 50	
1-3 years old	+ 50		Monitoring software for the network	- 100	
3-4 years old	+ 200		Mobile device policy and monitoring	- 100	
Over 4 years old	+ 300		Up-to-date anti-virus & threat monitoring	- 100	
			A firewall that is monitored & updated	+ 100	

TECHNOLOGY THOUGHT LEADERSHIP, BUSINESS INSIGHTS, & LEADING EDGE THINKING



manuel.w.lloydconsulting®

Regarding disaster recovery and business continuity, check all that apply:					
You DO have a written disaster recovery plan	- 200		You DON'T have a disaster recovery plan	+ 200	
You review & update your plan regularly	- 100		You DON'T update your plan	+ 100	
You conduct periodic tests of your plan	- 100		You DON'T test your plan ever	+ 100	
You DO have an inventory of assets for insurance	- 100		You DON'T have an inventory of assets	+ 100	

Scoring:

0 Or Less: Low To No Risk
You either don't have very much critical data on or your backup plan is well designed. If this exercise revealed one or two areas you are NOT securing well, you now have the opportunity to resolve those areas immediately.

0-200: Medium Risk
Depending on what data is compromised, you will most likely be able to recover it without major catastrophic costs or consequences. HOWEVER, there are certain areas that are more important than others. For example, if you had sensitive data lost or stolen, the consequences from that could be extensive in the form of HIPAA fines/fees, lost patients, lost market share, a harmed reputation and possibly even a lawsuit.

200 Or More: High Risk
Your practice is extremely vulnerable to various data-erasing disasters, and there is a high chance that you would NOT be able to recover it at all. It is imperative that you strengthen your current backup, security and disaster recovery plan immediately.

TECHNOLOGY THOUGHT LEADERSHIP, BUSINESS INSIGHTS, & LEADING EDGE THINKING

Appendix: BC/DR Concepts

Business Continuity/Disaster Recovery

Organizational Resiliency

Organizational Resiliency

1. **Crisis leadership** and effective communications
2. Critical **supply chains** and critical vendors
3. Business continuity management and the ability to **manage issues**
4. The **resilient workforce**
5. The larger **community**

Disaster Types

- Forecasted event - the impact can be foreseen (such as a weather system event such as a hurricane) and can be mitigated through prior planning.
- Un-forecasted event - the organization cannot provide a mitigation plan due to the immediate timing of the event itself (such as an earthquake or cyber security attack) or the realization of previously accepted risk factors.

Enterprise Risk Management (ERM)

- ERM looks at competitive threats, natural and manmade threats, regulatory changes and government and market changes
- ERM teams map out the forecasted impact of strategic mistakes
- For disasters, this team must understand how much damage (money, assets, and destroyed supply chains) the organization can withstand.

Common ERM Risk Areas

Risk Classification (SCC)	Risk Identification (MIT)
Disaster Risk	Storm, Tsunami
Financial Risk	Delayed payment, credit rating, currency devaluation
Human Resource Risk	Employee misconduct ,labor disputes, workplace accident and injury
Market Risk	Fierce competitor movement or failure of new product introduction
Environmental Risk	Disease, fires, contamination and leak
Distribution Risk	Transportation carrier failure
Security Risk	Terrorism and workplace security
Regulatory Risk	Regulatory change or government policy change
Operational Risk	Demand uncertainty, poor deliver, poor planning, bad customer service
Safety Risk	Workplace accident and injury
Supplier Risk	Supplier performance failure and rising material cost
IT Risk	Failure of software systems or loss of important data

Business Continuity

Forecasts, analyzes and mitigates specific threat vectors for targeted divisions in the organization to restore essential people, processes, technologies and supply chains to stabilize the organization in the event of a disaster.

Common Business Continuity Outputs

- Business Continuity Policy and Charter – A policy stating the strategy and executive support in the times of disaster.
- Risk Assessments – Identifies and analyze potential risks and threats to the overall organization's performance before a disaster event is realized.
- Business Impact Analysis - Analyzes and determines the impact of specific disasters on specific operational functions.
- Continuity Requirements – Determines specific continuity performance metrics for specific supply chains, systems and processes including desired recovery time objectives and recovery point objectives.

Disaster Recovery Plans

- Focuses on mitigating the impact of forecasted disasters on specific targeted systems and processes
- When no predefined recovery plan is available, the disaster recovery plan covers the roles and responsibilities for handling the disaster

Emergency Management Teams

- Manage the complexity of a disaster event providing:
  - Situational awareness
  - Impact analysis
  - Triaging mission teams
- Typically, response teams utilize the Incident Command System (ICS)

Regulation Examples and What They Mean

ISO 22301 and ISO 22313	Business Impact Analysis, Emergency Response, Strategies to continue products and services, Exercising and Testing, Coordination with External Agencies
ISO 9001	Customer Requirements, Management Responsibility, Resource Mgmt., Documentation, Metrics and Measurement Effectiveness
OHSAS 18001	OH&S Policy, OH&S Planning, Hazard Analysis, Pandemic Planning, Consultation & Communication, Operational Policies and Procedures
ISO 20000	Budgeting and accounting, Business relationship mgmt., Design and transition of services, Service Level Mgmt.
ISO 27001	Information Classification, Information Asset Mgmt., Access Controls, Human Resource Security, Vulnerability Mgmt.
Federal Information Security Management Act of 2002 (FISMA)	US Federal mandate to provide a comprehensive Information Security (INFOSEC) framework for US government systems, coordination with various law enforcement agencies, establishment of controls, acknowledgement of commercial products and software capabilities in the INFOSEC space. Section 3544 covers agency responsibilities including IT controls.
Sarbanes-Oxley Act of 2002 (SOX)	Section 404 recognizes the role of information systems Requires publicly traded companies to provide an annual review of their internal controls over financial reporting.
ISO 31000, ISO/IEC 31010, ISO/IEC Guide 73	Risk Management — Principles and Guidelines Risk management — Vocabulary Risk management — Risk assessment techniques

Disaster Response Protocol

Watch	Mobilize	Assess	Stabilize	Close

Incident

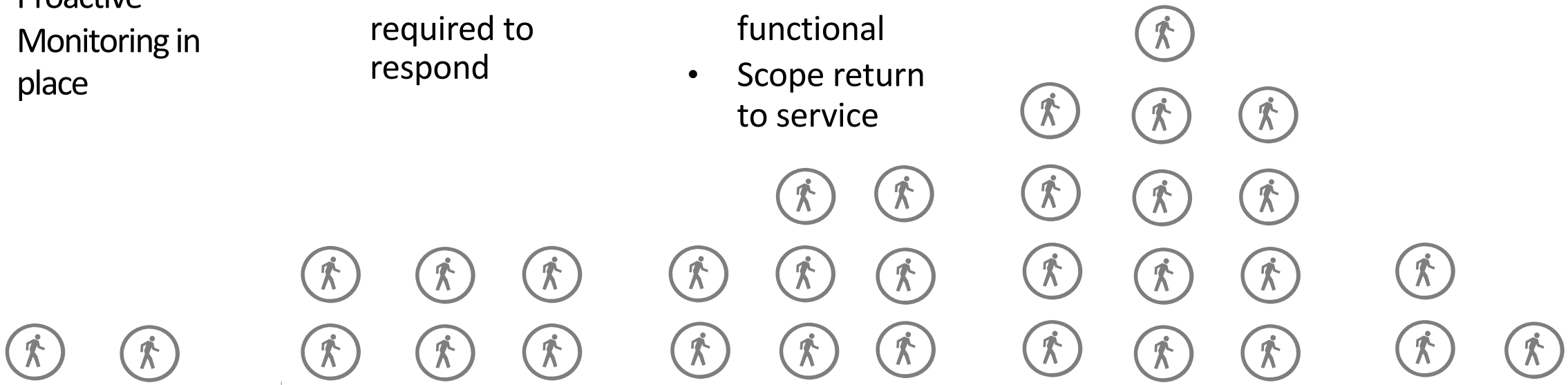
- Processes established
- Proactive Monitoring in place

- Bring together resources required to respond

- What is functional vs. non-functional
- Scope return to service

- Return to service

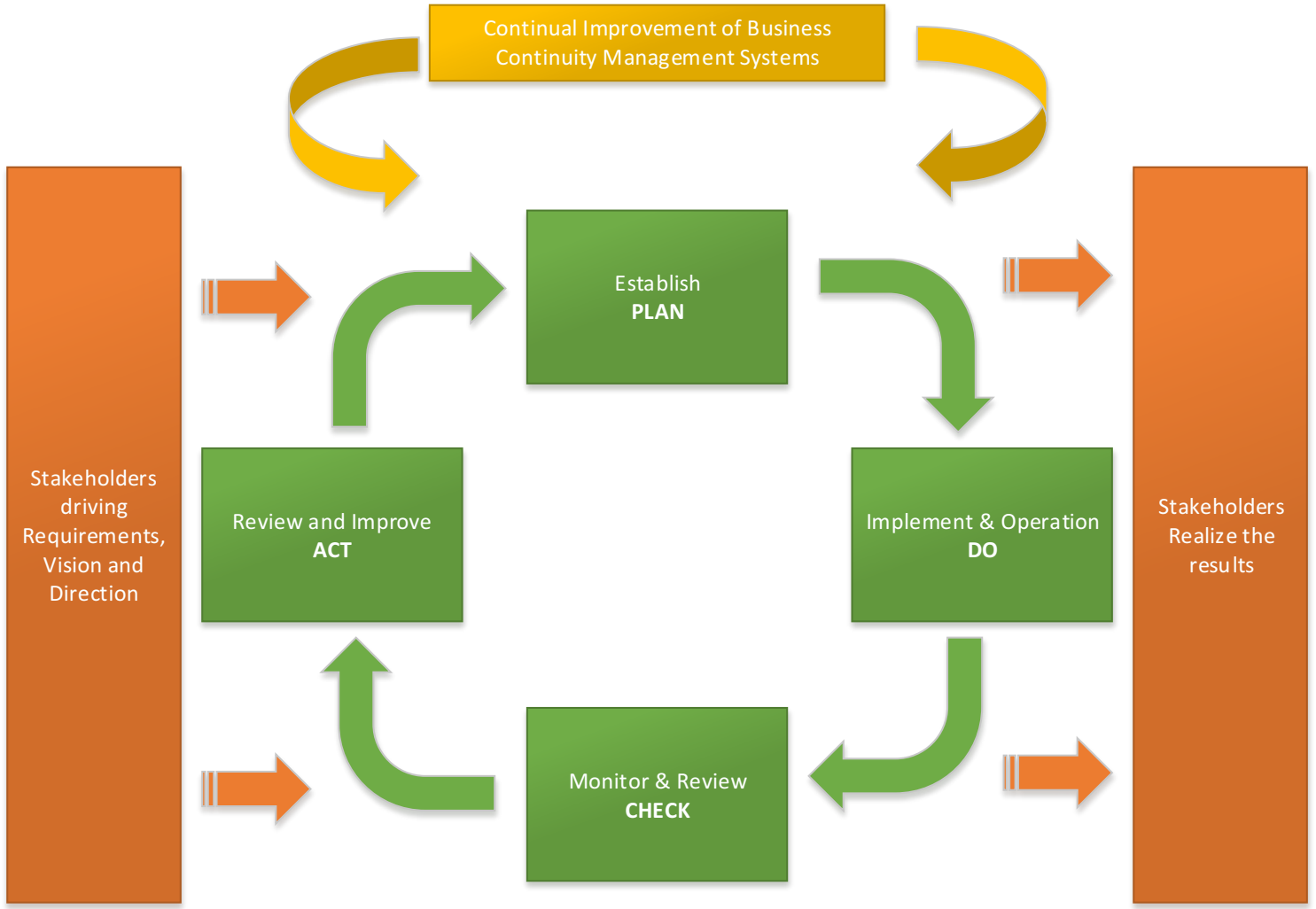
- After-Action



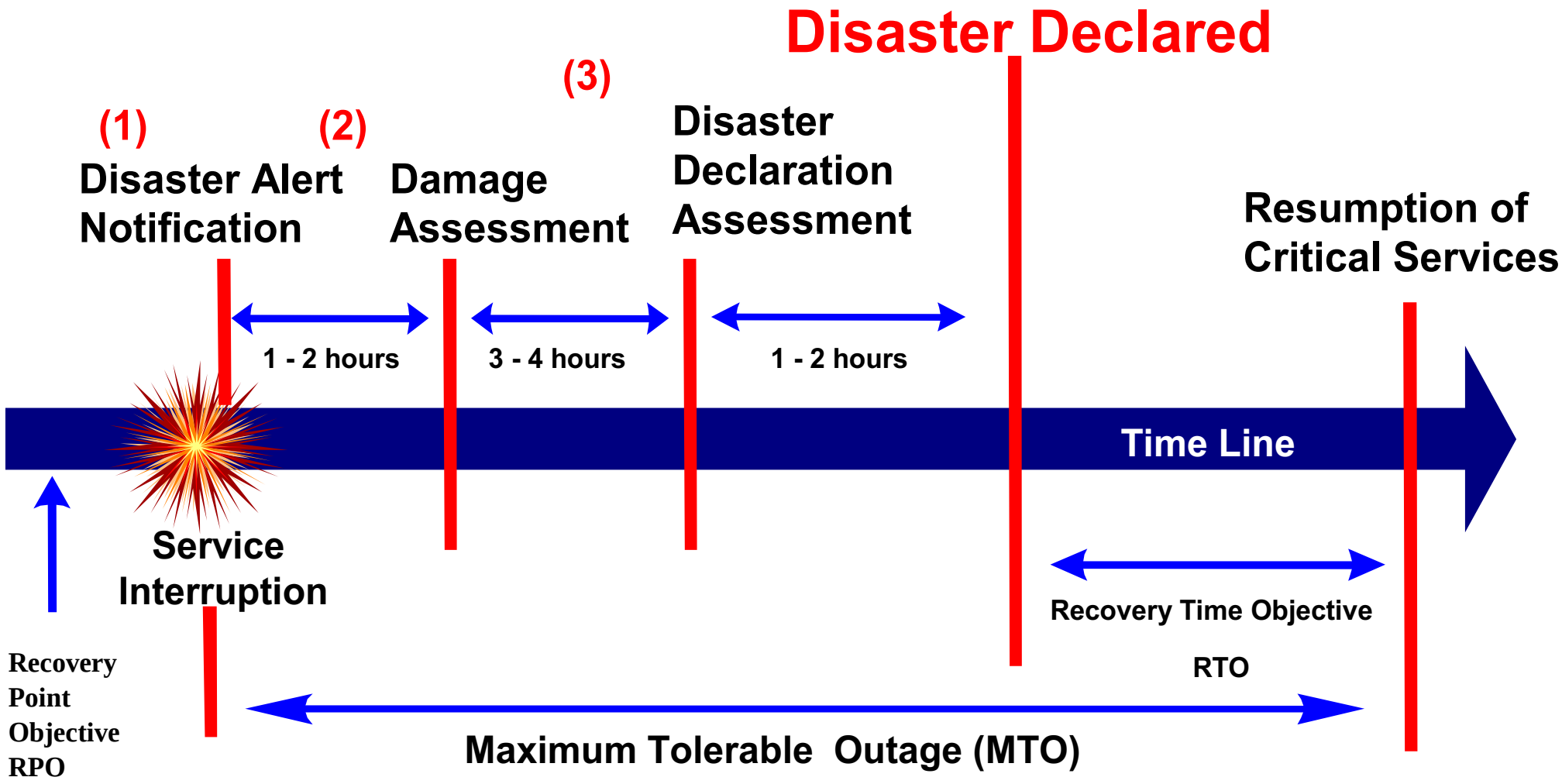
Plan-Do-Check-Act (PDCA) Model

PDCA

- ISO 22301 standard
- The PDCA promotes BC/DR as a perpetual commitment of execution including processes, technology, organizational “muscle memory” and executive commitment
- Not a product or technology, it is a process-based effort.



50,000 Foot View



RPO/RTO

Recovery Point Objective (RPO)

The maximum amount (in time) of data that can be lost in case of a disruption.
Answers the question: *"To what point in time can I recover?"*

RPO/RTO

Recovery Time Objective (RTO)

The maximum amount of time it will take from the disruption to bring back the business functions according the agreements including data.

Technical Dependency Analysis (TDA)

- Examines the application(s) and supporting infrastructure that a process depends on to determine, at a minimum, the following:
  - Recovery Time Capability (RTC), or;
  - Recovery Time Estimate (RTE), if they haven’t been tested ;
  - Recovery Point Capability (RPC), or ;
  - Recovery Point Estimate (RPE), if they haven’t been tested

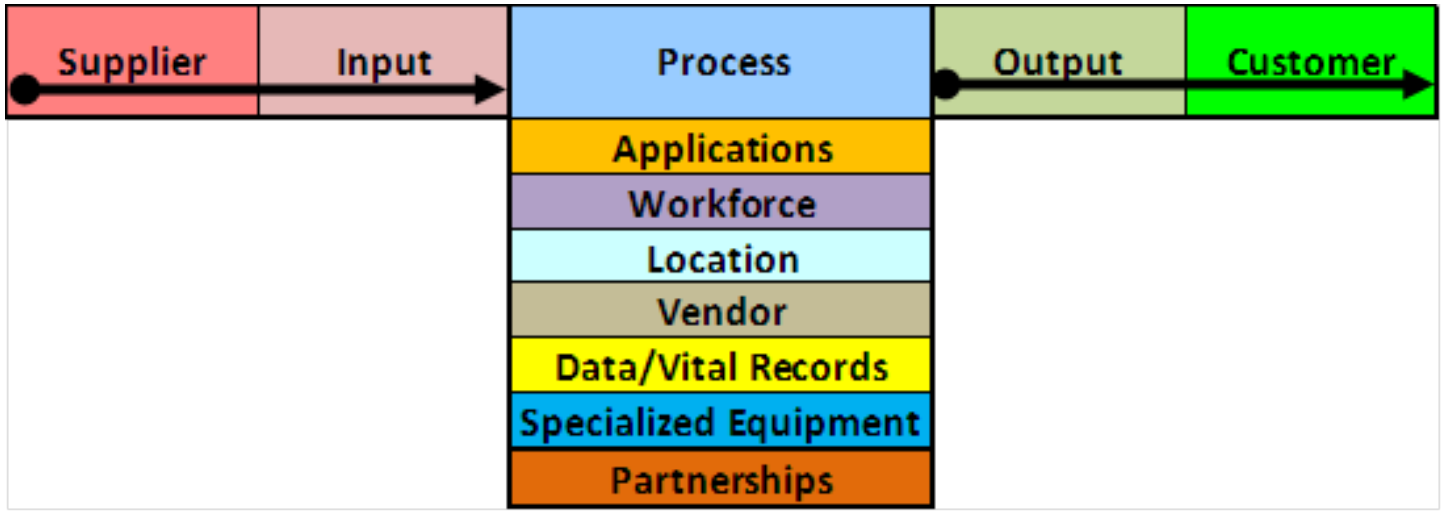
Technical Dependency Analysis (TDA)

- Recovery Time Estimate - the technical dependency has not been proven through a test and the RTC has not been validated.
- Recovery Time Capability - the technical dependency has been proven through a test and may or may not meet the RTO requirement.
- Recovery Point Estimate - the technical dependency has not been proven through a test and the RPC has not been validated.
- Recovery Point Capability - the technical dependency has been proven through a test and may or may not meet the RPO requirement.

SIPOC

SIPOC

- Six Sigma methodology
- SIPOC stands for *supplier, inputs, processes, outputs,* and *customers*
- Often used to assist groups in understanding the interrelationships of their processes and how work is currently performed within each process



Dependency Categories

- Supplier
- Input
- Location
- Application
- Vendor
- Data and Vital Records
- Specialized Equipment
- Partnership
- Output
- Customer

BC/DR Planning Challenges

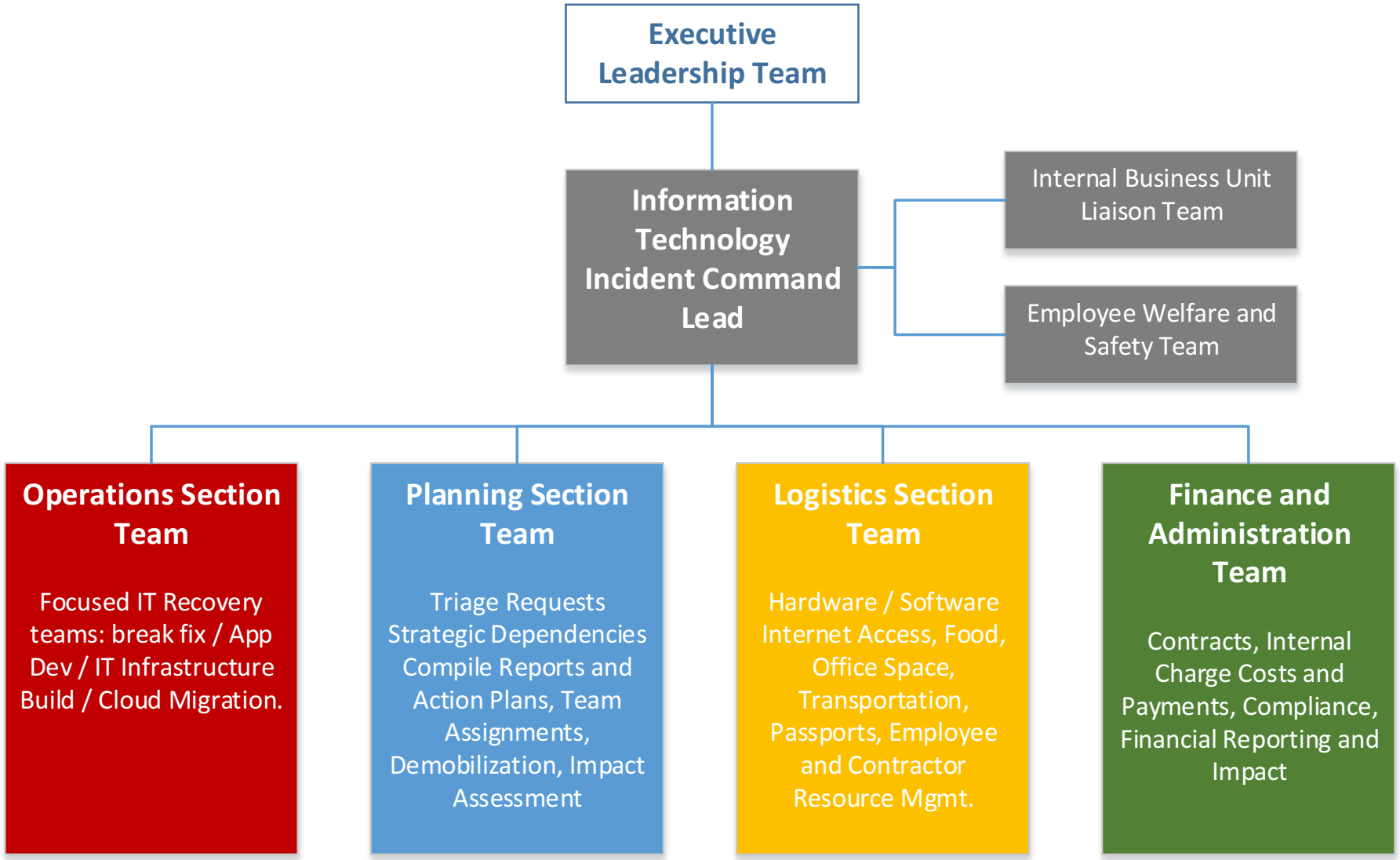
Disaster recovery plans often result in failure

- There are a variety of reasons for this:
  - Too much complexity
  - Too much specialized human involvement
  - Decisions by consensus
  - Lack of testing (this brings out the missing details)
  - Lack of real world disaster management experience by the planning team

Incident Command System

- Emergency Response requires a clear command model with focused teams to quickly rebuild the organization effectively
- ICS is an internationally recognized operational command and control model to mobilize, access and triage the crisis
  - Responsibly orchestrates all available talent while working with critical partners, government organizations and key stakeholders.

ICS Model for Disaster Management

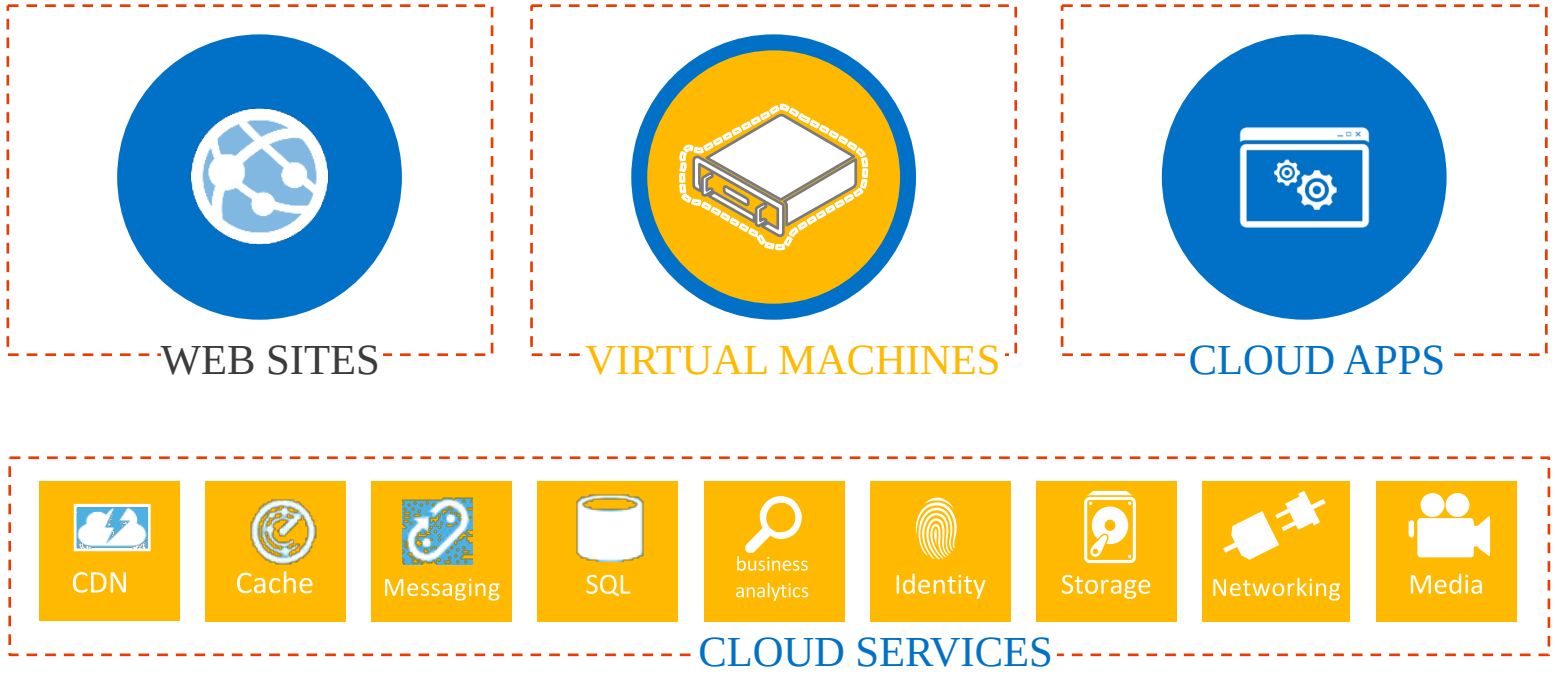


IT Restoration Mission Classification

- Break/Fix missions
  - Repair and restore of existing IT assets
  - Examples include restoring an existing application or service from backup.
- Complex missions
  - Major rebuild of key IT assets.
  - Examples include setting up new emergency cloud services, rapidly building applications or addressing significant cyber-attacks while in crisis.

Planning BC/DR For Cloud Environments (Geekspeak)

Delivering on the Consistency Promise



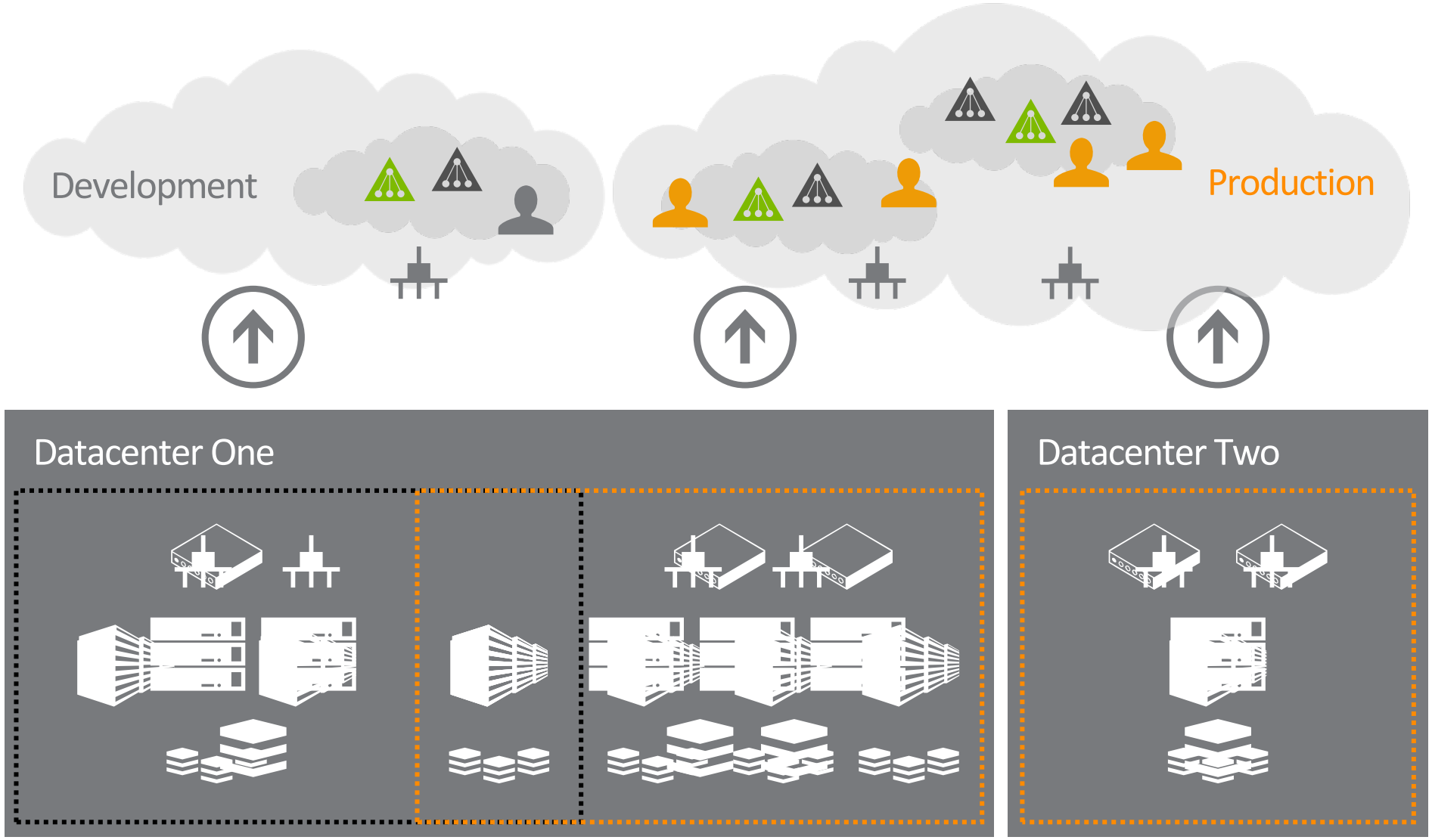
Consistency is about enabling applications to run and be managed.

A service provider can offer consistency in one or more scenarios, applications, and services.

Stateless and Stateful Workloads

- Stateful
  - Rely on the infrastructure to provide availability
  - Do not have the constructs within the application or service to manage their own state in a cloud environment
  - Stateful resource pools provide virtual machine resiliency through availability constructs such as Live Migration
- Stateless
  - Rely on the application or service to provide availability
  - Contain the constructs within the service to continue service during outages
  - Stateless resource pools do not offer availability services and rely on the underlying service or application to provide resiliency and can operate during failures with diminished capacity

Private Clouds



- Standardized services
- Delegated capacity
- Cloud abstraction
- Logical and standardized
- Diverse infrastructure

Development

Production

Hypervisor High Availability & Resiliency

Robust, reliable & resilient infrastructure foundation for running continuous services

Provide flexibility for application-level resiliency

Simplify infrastructure maintenance

Provide granular solutions for enabling disaster recovery

Integration with cloud services

Failover Clustering

Online Backup

NIC Teaming

Hyper-V Replica with Extended Replication

Guest Clustering

Shared VHDX

Site Recovery Service

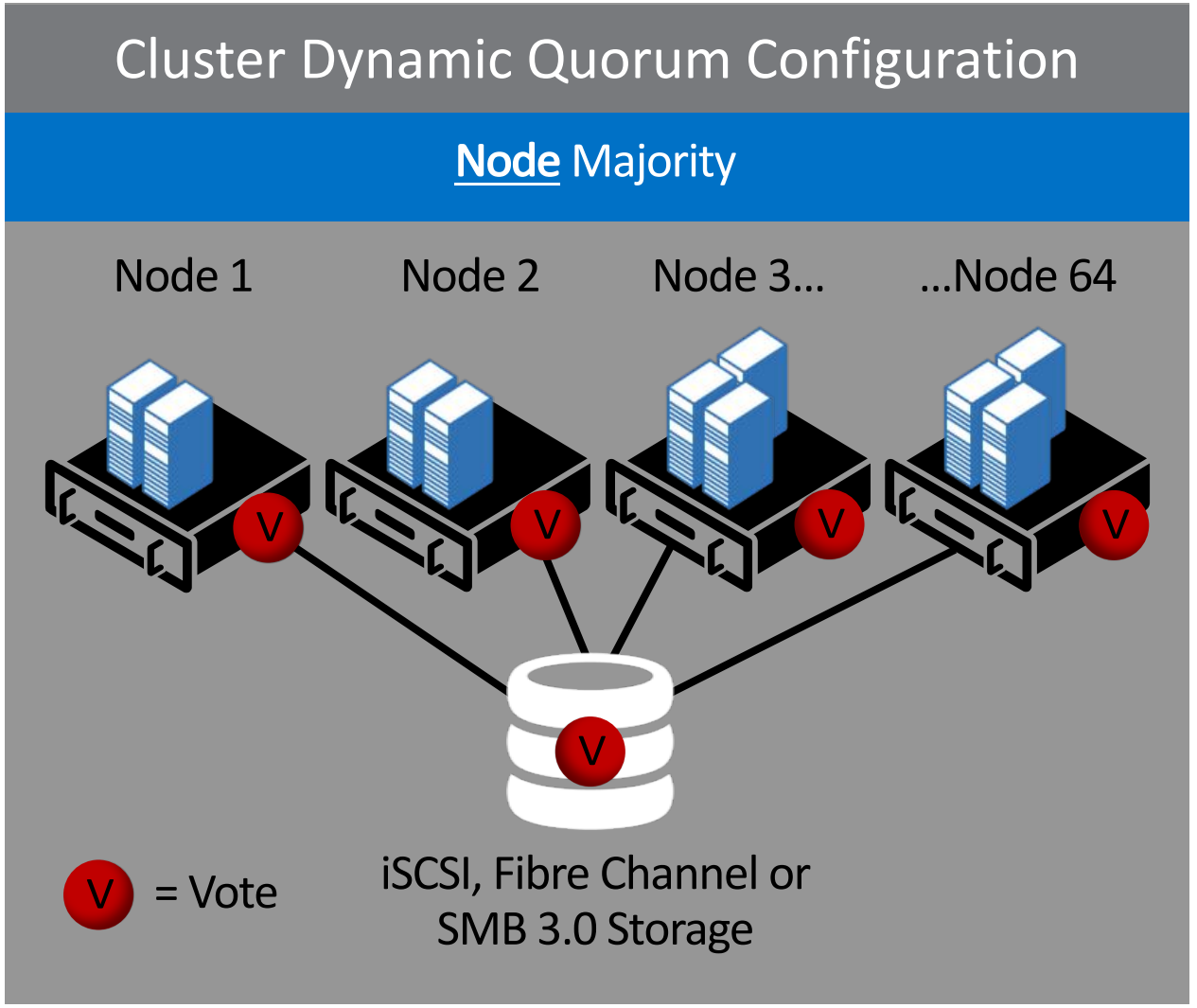
Failover Priority & Affinity Rules

Cluster Aware Updating

Failover Clustering

Integrated Solution for Resilient Virtual Machines

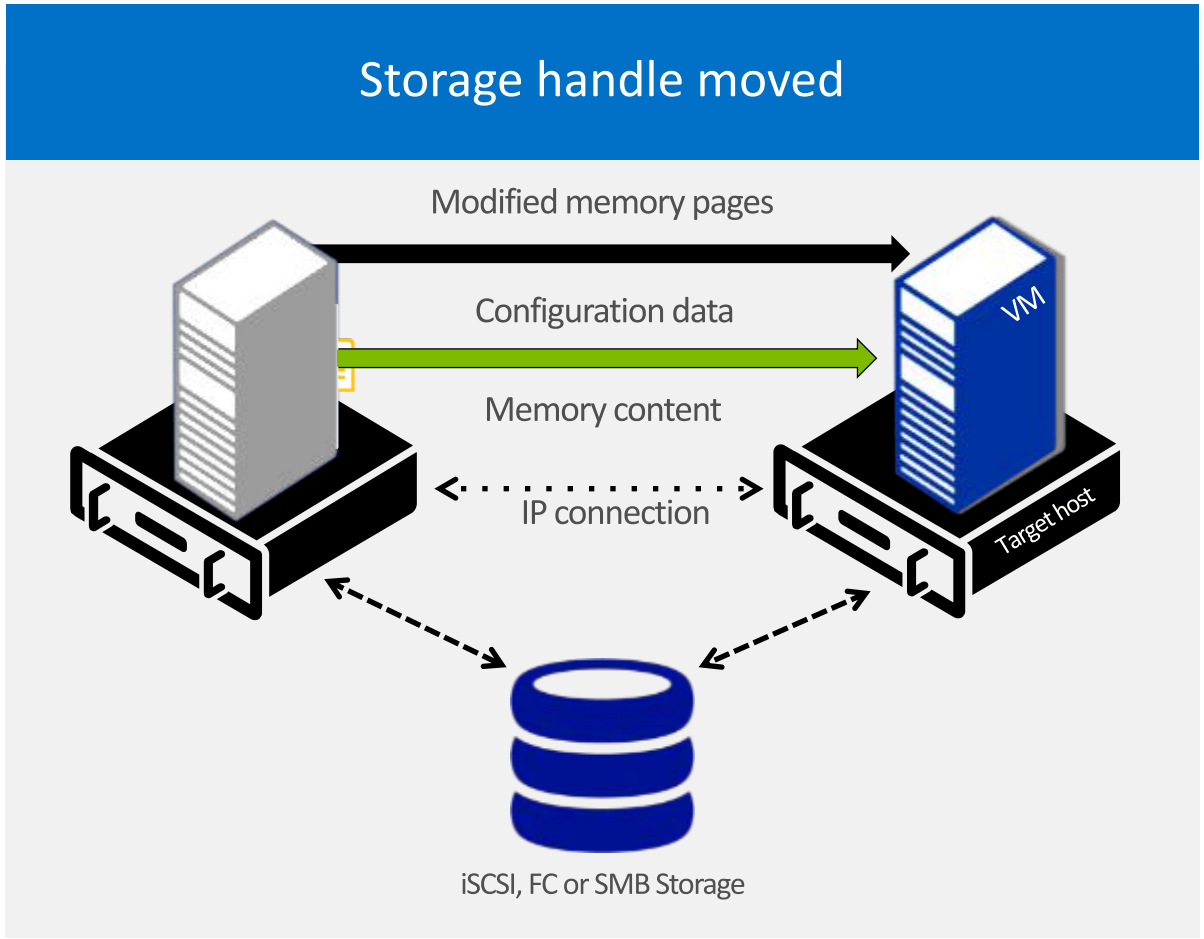
- Massive scalability with support for 64 physical nodes and 8,000 VMs
- VMs automatically failover and restart on physical host outage
- Enhanced Cluster Shared Volumes
- Cluster VMs on SMB 3.0 Storage
- Dynamic Quorum and Witness
- Reduced AD dependencies
- Drain Roles – Maintenance Mode
- VM Drain on Shutdown
- VM Network Health Detection
- Enhanced Cluster Dashboard



Hyper-V Live Migration

Faster, Simultaneous Migration of VMs Without Downtime

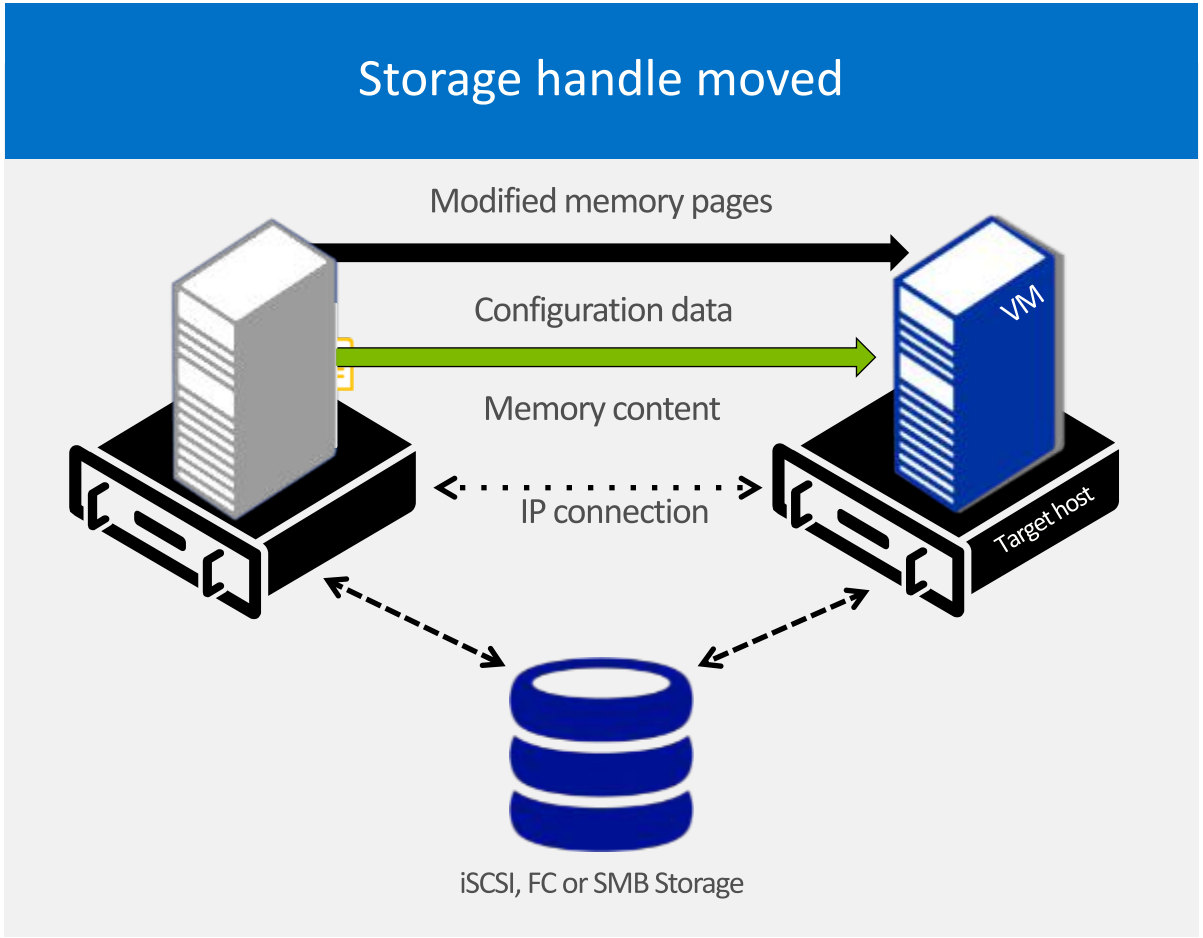
- Faster live migrations, taking full advantage of available network
- Simultaneous Live Migrations
- Supports flexible storage choices – iSCSI, Fibre Channel or SMB for VM's files
- Requires Failover Clustering if using iSCSI/Fibre Channel Storage
- No Failover Clustering required if virtual machine resides on SMB 3.0 File Share
- Can be triggered via PowerShell



Hyper-V Live Migration Compression

Intelligently Accelerates Live Migration Transfer Speed

- Utilizes available CPU resources on the host to perform compression
- Compressed memory sent across the network faster and decompressed on target host
- Operates on networks with less than 10 gigabit bandwidth available
- Enables a 2X improvement in Live Migration performance
- Enabled by default but will only operate if there is spare CPU available to compress the VM memory.

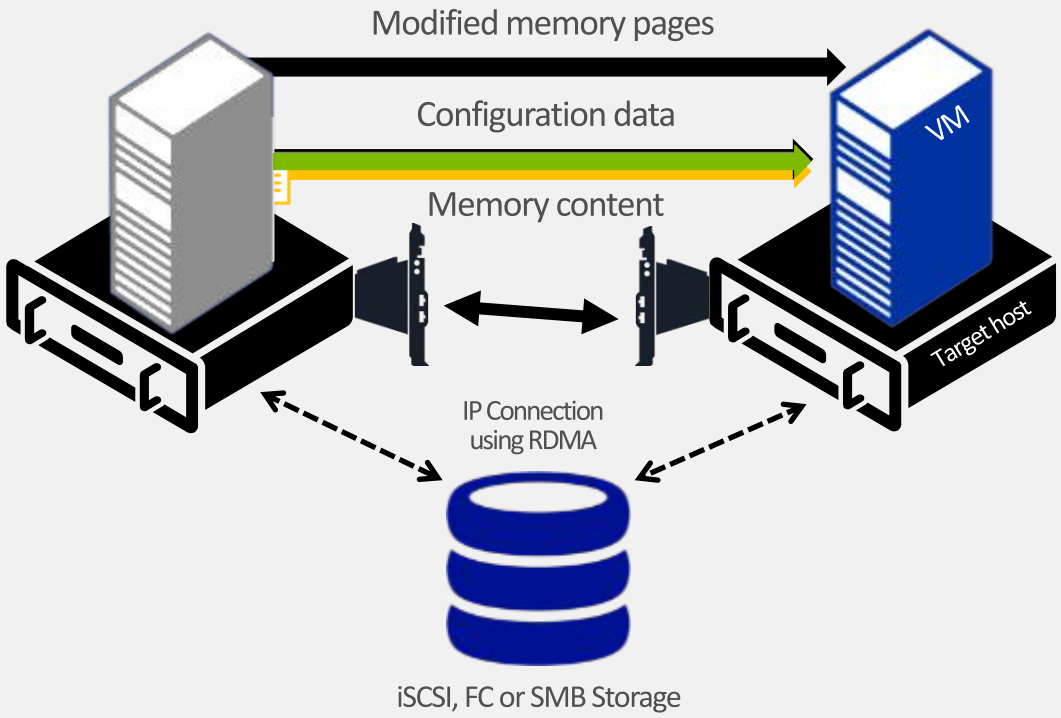


Hyper-V Live Migration over SMB

Harness RDMA to Accelerate Live Migration Performance

- SMB Multichannel uses multiple NICs for increased throughput and resiliency
- Remote Direct Memory Access delivers low latency network, CPU utilization & higher bandwidth
- Supports speeds up to 56Gb/s
- Windows Server 2012 R2 supports RoCE, iWARP & Infiniband RDMA solutions
- Delivers the highest performance for Live Migrations
- Cannot be used with Compression

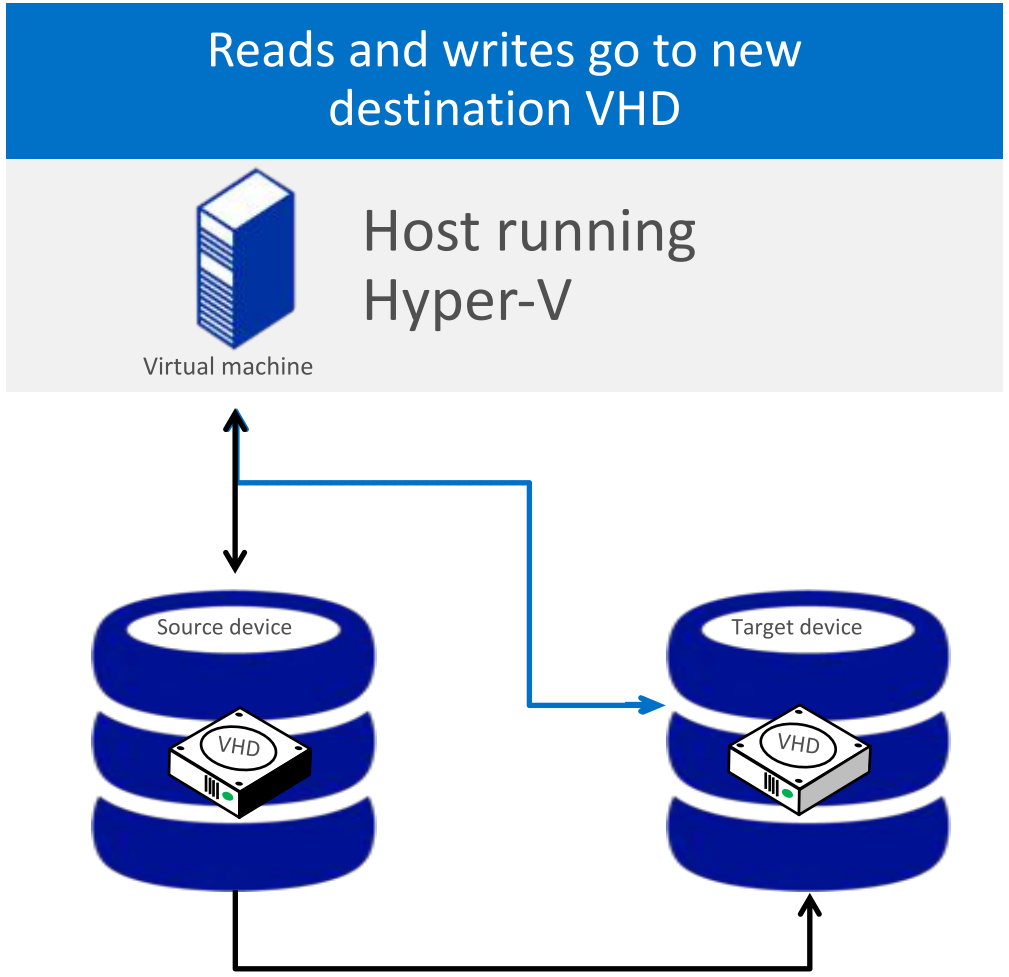
Storage handle moved



Hyper-V Storage Live Migration

Increased Flexibility through Live Migration of VM Storage

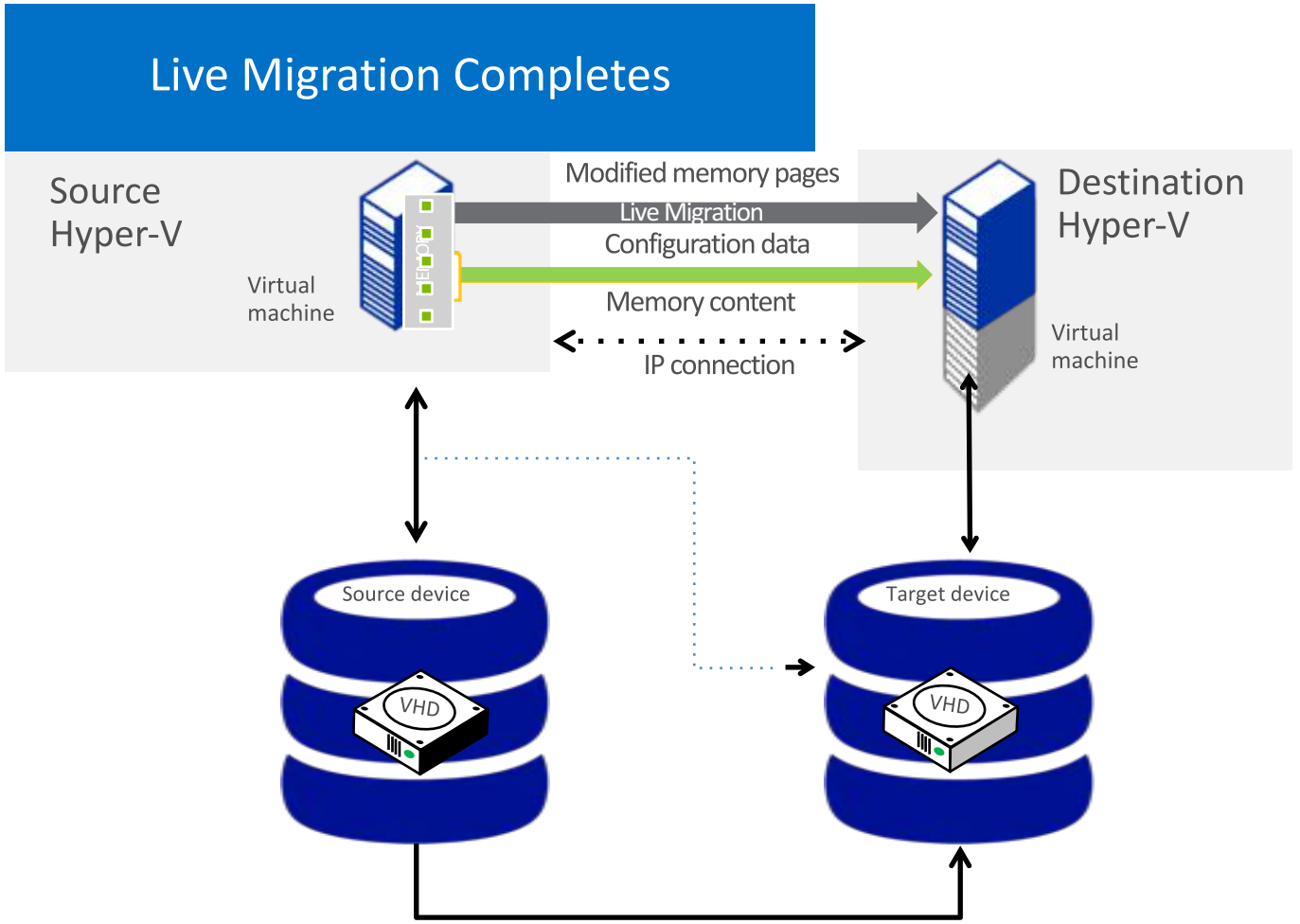
- Move virtual hard disks attached to a running virtual machine
- Manage storage in a cloud environment with greater flexibility and control
- Move storage with no downtime
- Update physical storage available to a virtual machine (such as SMB-based storage)
- Windows PowerShell cmdlets



Hyper-V Shared-Nothing Live Migration

Complete Flexibility for Virtual Machine Migrations

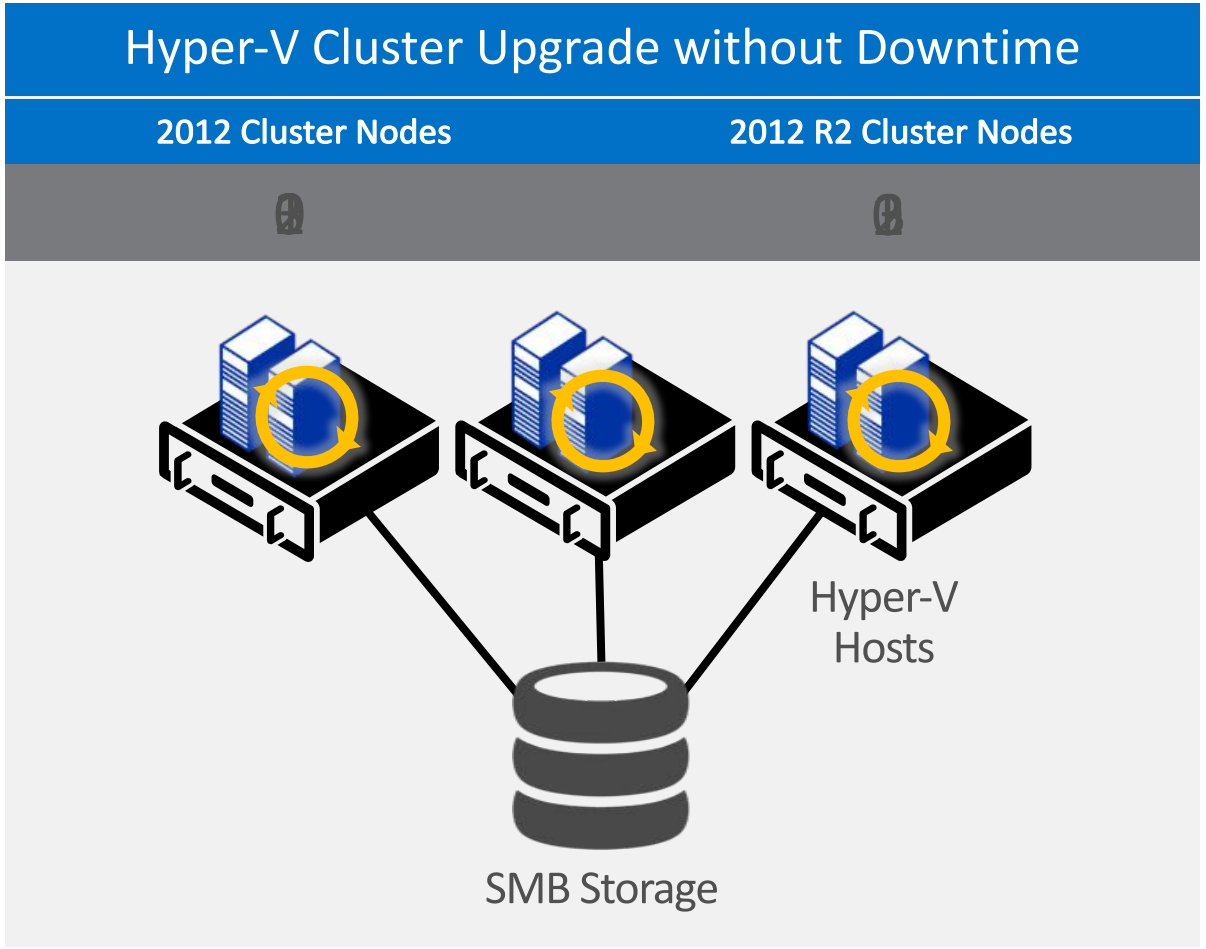
- Increase flexibility of virtual machine placement & increased administrator efficiency
- Simultaneously live migrate VM & virtual disks between hosts
- Nothing shared but an ethernet cable
- No clustering or shared storage requirements
- Reduce downtime for migrations across cluster boundaries



Hyper-V Live Migration Upgrades

Simplified upgrade process from 2012 to 2012 R2

- Upgrade from Windows Server 2012 Hyper-V to Windows Server 2012 R2 Hyper-V with no VM downtime
- Supports Shared Nothing Live Migration for migration when changing storage locations
- If using SMB share, migration transfers only the VM running state for faster completion
- Automated with PowerShell
- One-way Migration Only



Hyper-V Replica

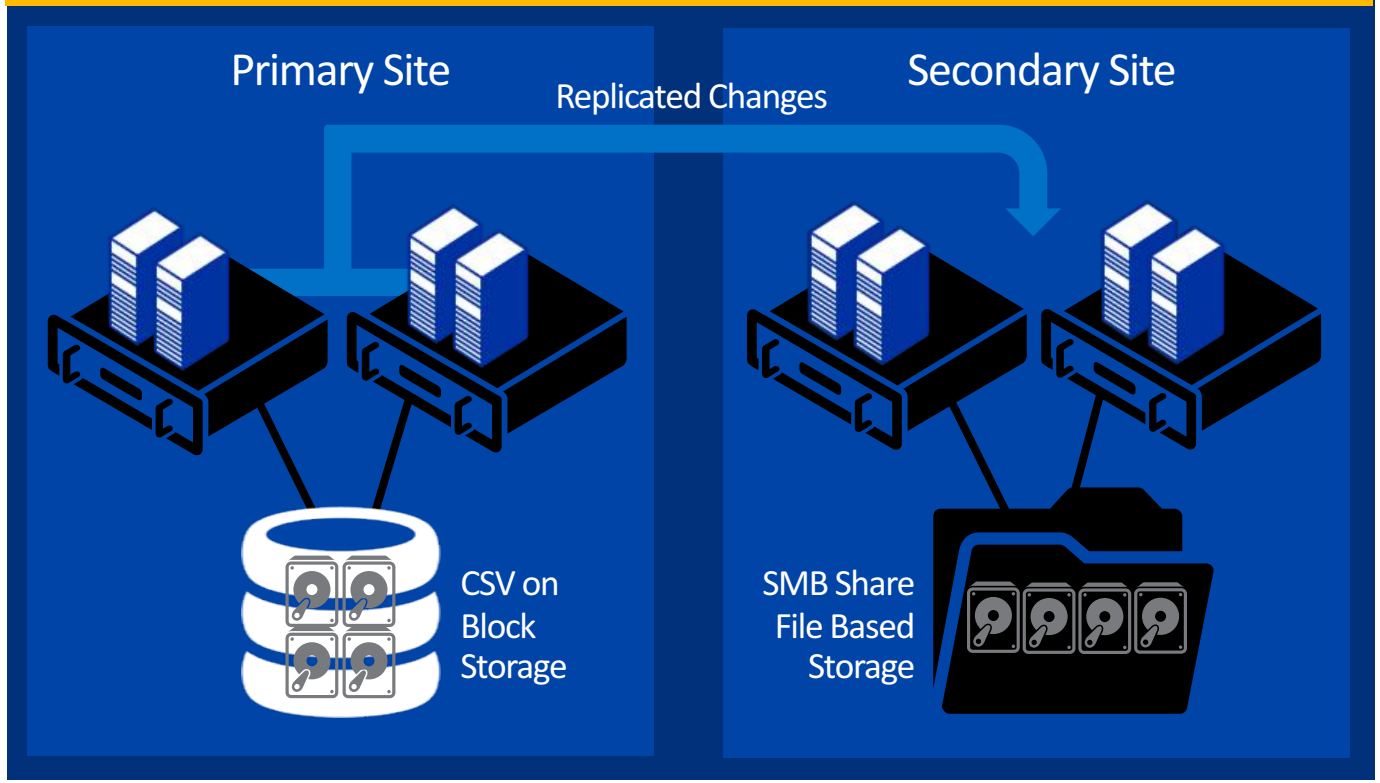
Replicate Hyper-V VMs from a Primary to a Replica site

- Affordable in-box business continuity and disaster recovery
- Configurable replication frequencies of 30 seconds, 5 minutes and 15 minutes
- Secure replication across network
- Agnostic of hardware on either site
- No need for other virtual machine replication technologies
- Automatic handling of live migration
- Simple configuration and management

Once Hyper-V Replica is enabled, VMs begin replication

Once replicated, changes replicated on chosen frequency

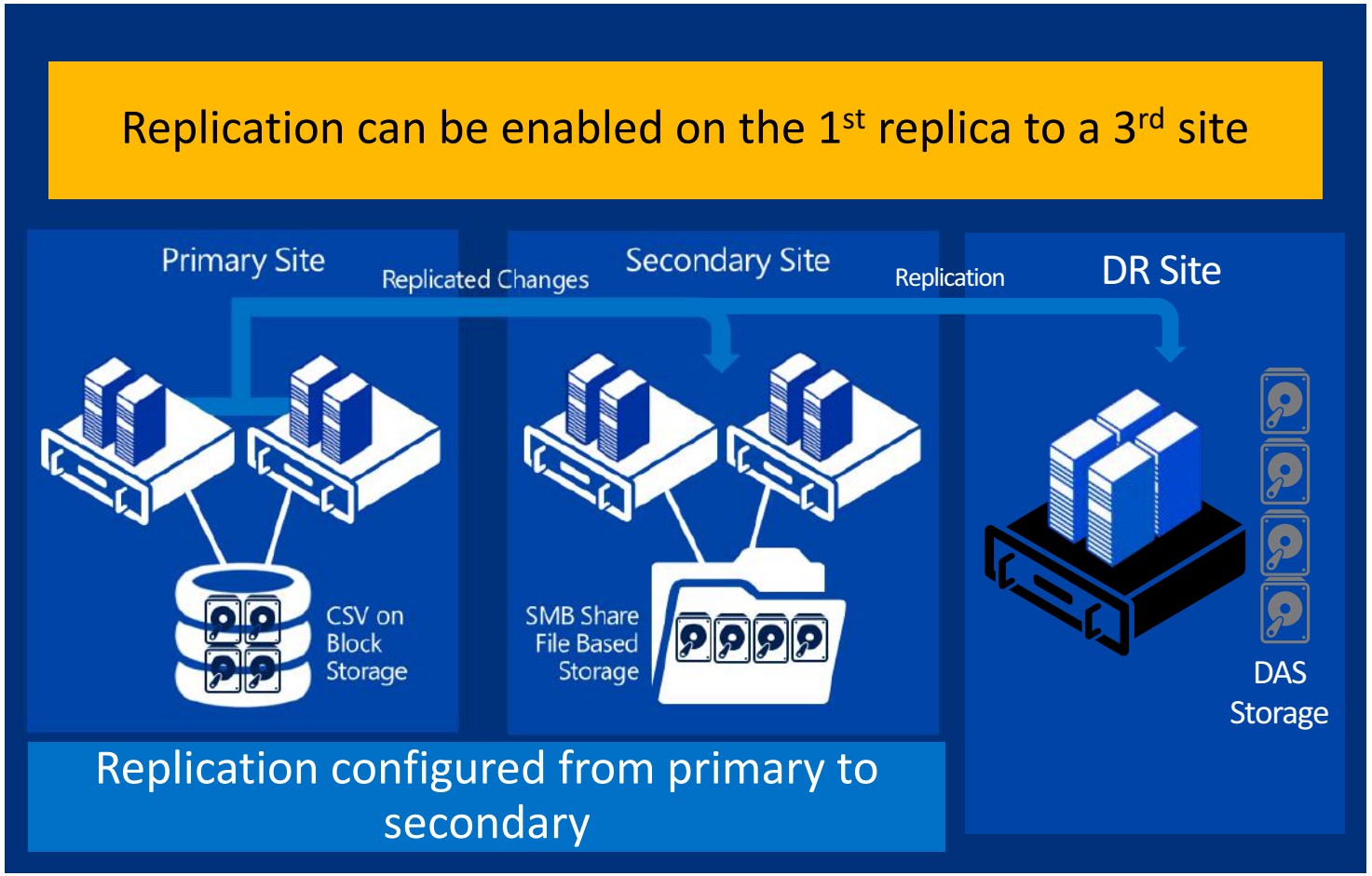
Upon site failure, VMs can be started on secondary site



Hyper-V Replica | Extended Replication

Replicate to 3rd Location for Extra Level of Resiliency

- Once a VM has been successfully replicated to the replica site, replica can be replicated to a 3rd location
- Chained Replication
- Extended Replica contents match the original replication contents
- Extended Replica replication frequencies can differ from original replica
- Useful for scenarios such as SMB -> Service Provider -> Service Provider DR Site



Hybrid Cloud

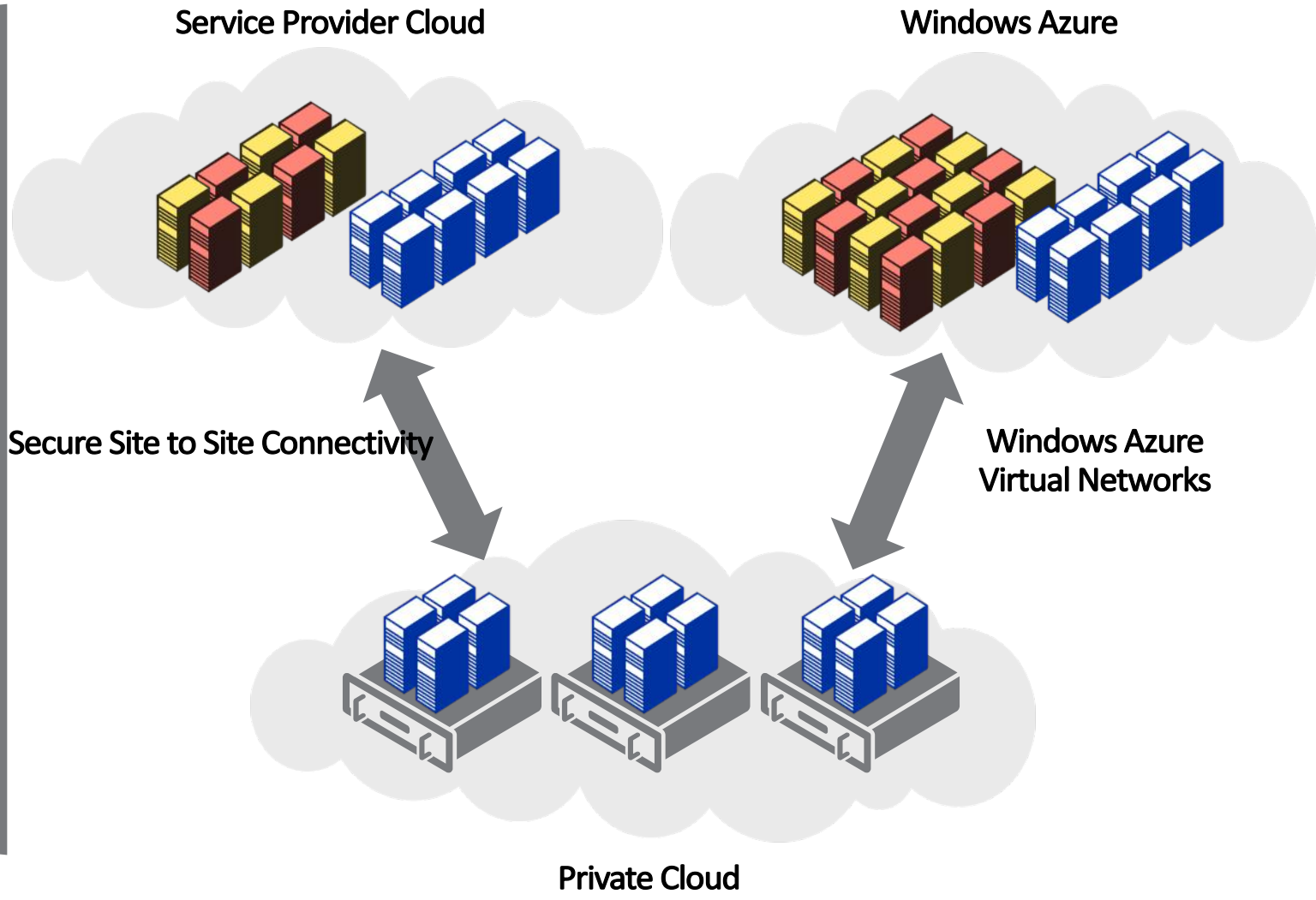
Utilize External Capacity through Seamless Integration

As customers grow, and look to scale their infrastructure, multiple options exist for deployment of workloads

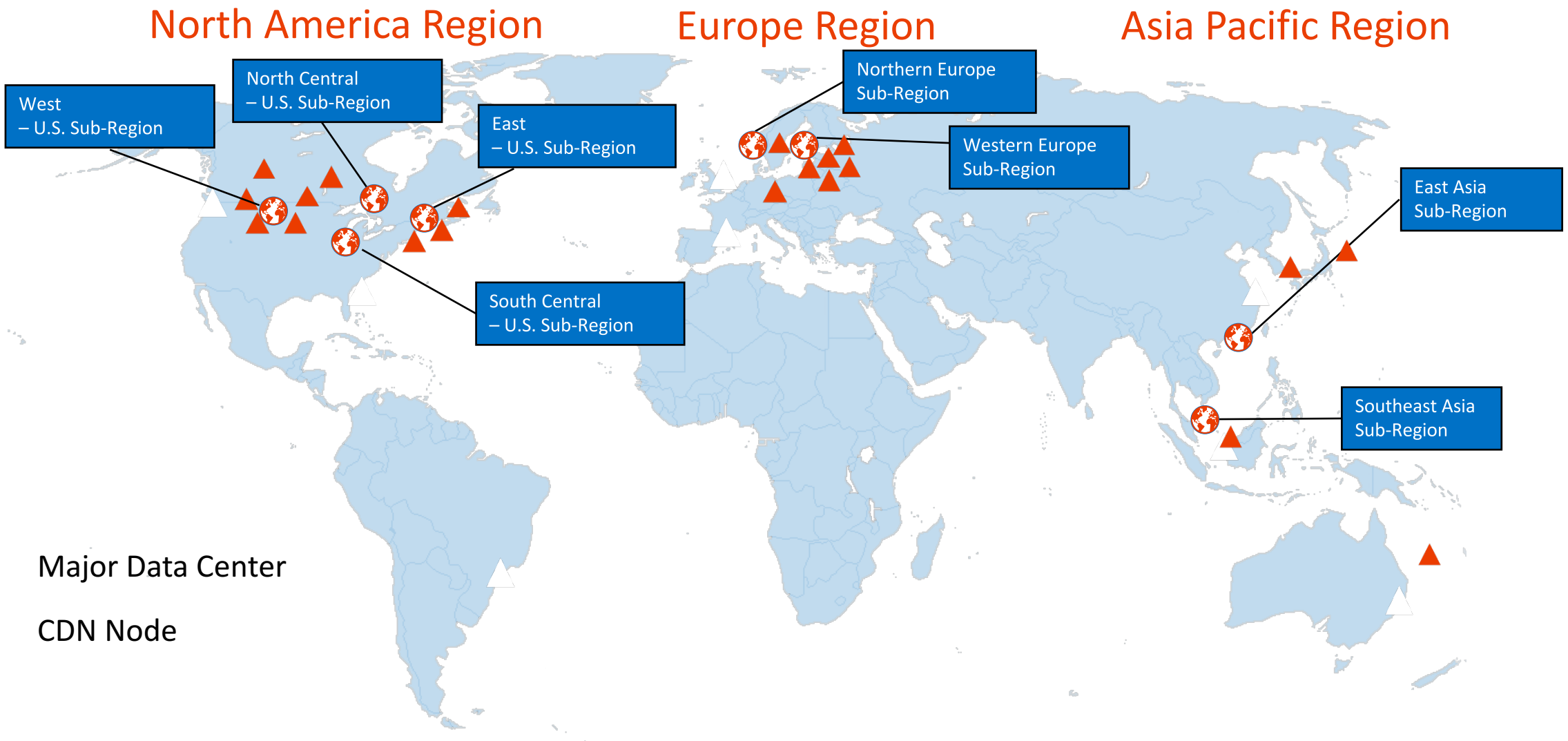
Private Cloud – Utilize and optimize existing on premise capacity

Connect to Service Providers – establish secure connectivity and harness Service Provider capacity for workloads

Connect to Windows Azure – utilize the Windows Azure Virtual Networks to provide seamless connectivity into Windows Azure and an extension to your own network.



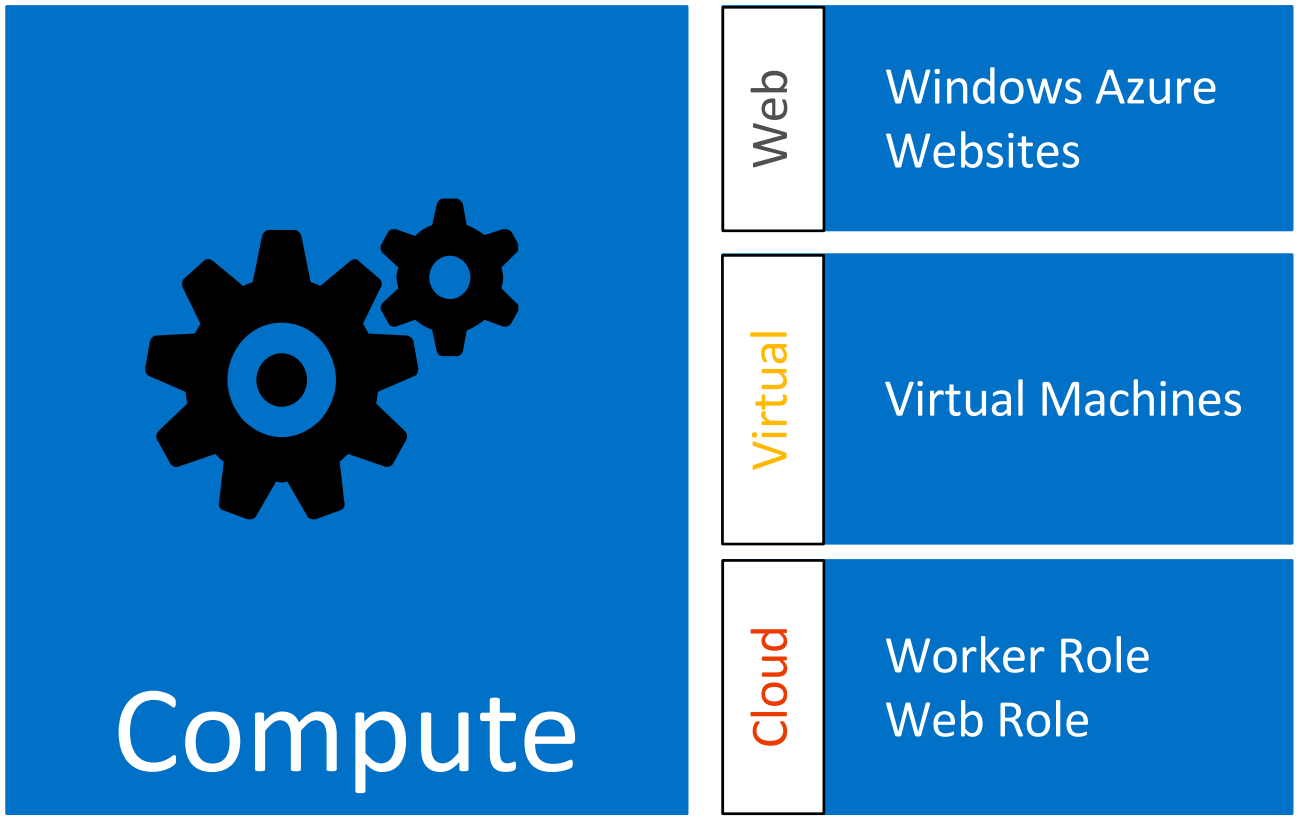
Windows Azure Global Presence



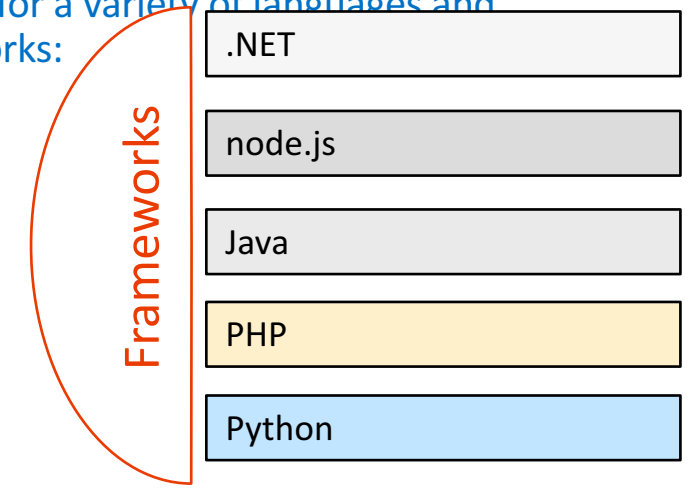
West US, North Central US, South Central US, East US, Northern Europe, Western Europe, East Asia, Southeast Asia, and 24 Edge CDN Locations

Windows Azure Compute

Flexible IaaS and PaaS based hosting options for Cloud, Web, and Virtual Workloads.



- **Features:**
  - 99.95 percent monthly SLA
  - Support for Windows and Linux virtual machines
  - Fault Isolation
  - Elastic Capacity
  - Open source support (Git, and so forth)
  - First class .NET support
  - Support for a variety of languages and frameworks:



Windows Azure Infrastructure Services

Integrating Public Cloud IaaS with On Premise Infrastructure

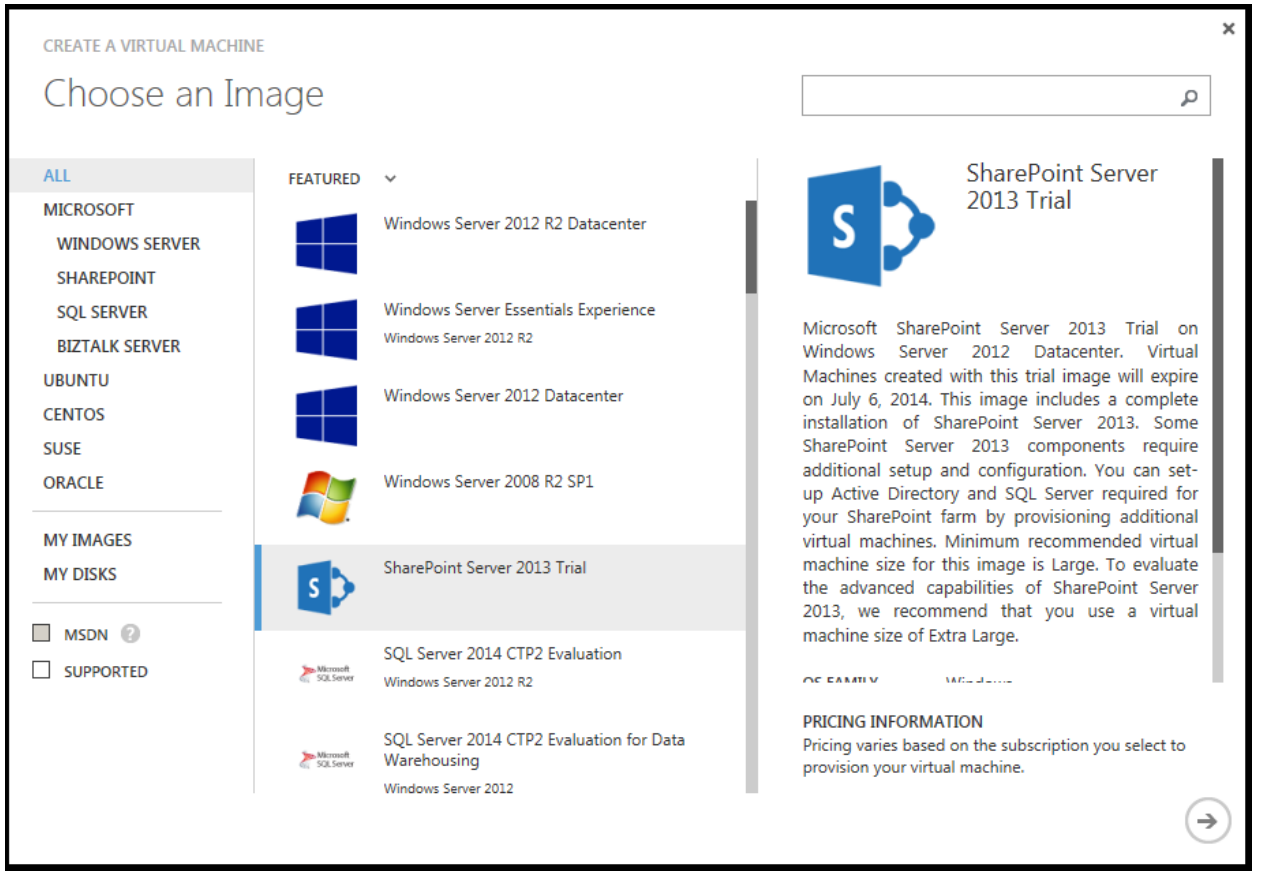
Azure Infrastructure Services – Spin up new Windows Server and Linux VMs in minutes and adjust usage as your needs change

Extend Your Datacenter – Virtual Network technology securely connects to your datacenter with a 99% SLA

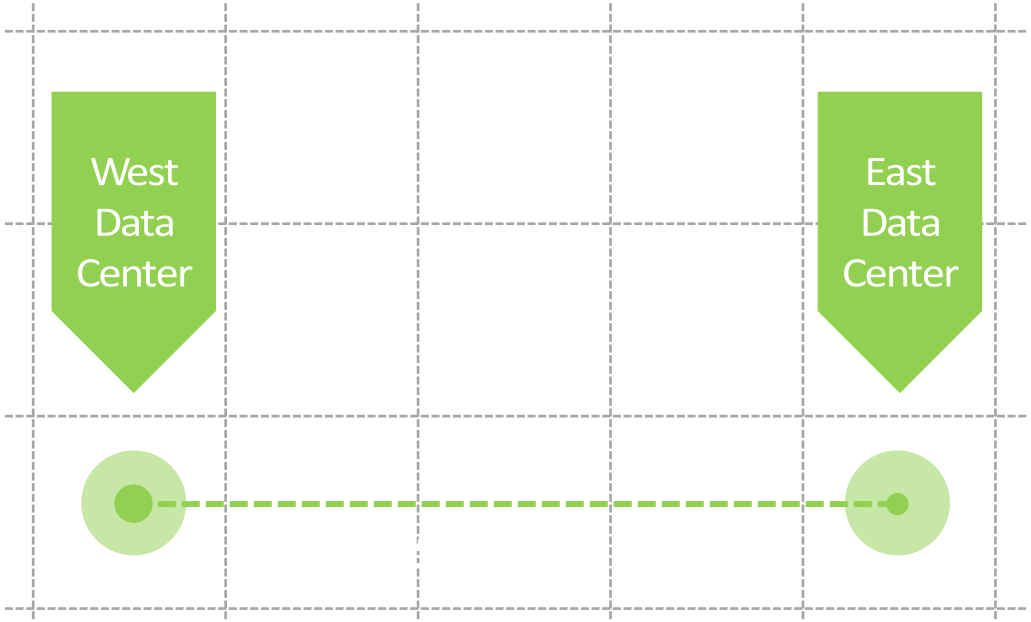
Rich Interface – Intuitive experience for creating and managing virtual machines through the browser

Integrated – Use App Controller to deploy and manage apps and services on Azure

Combined Templates – Use existing Azure images, or upload your own using App Controller



Storage - Geo-Replication

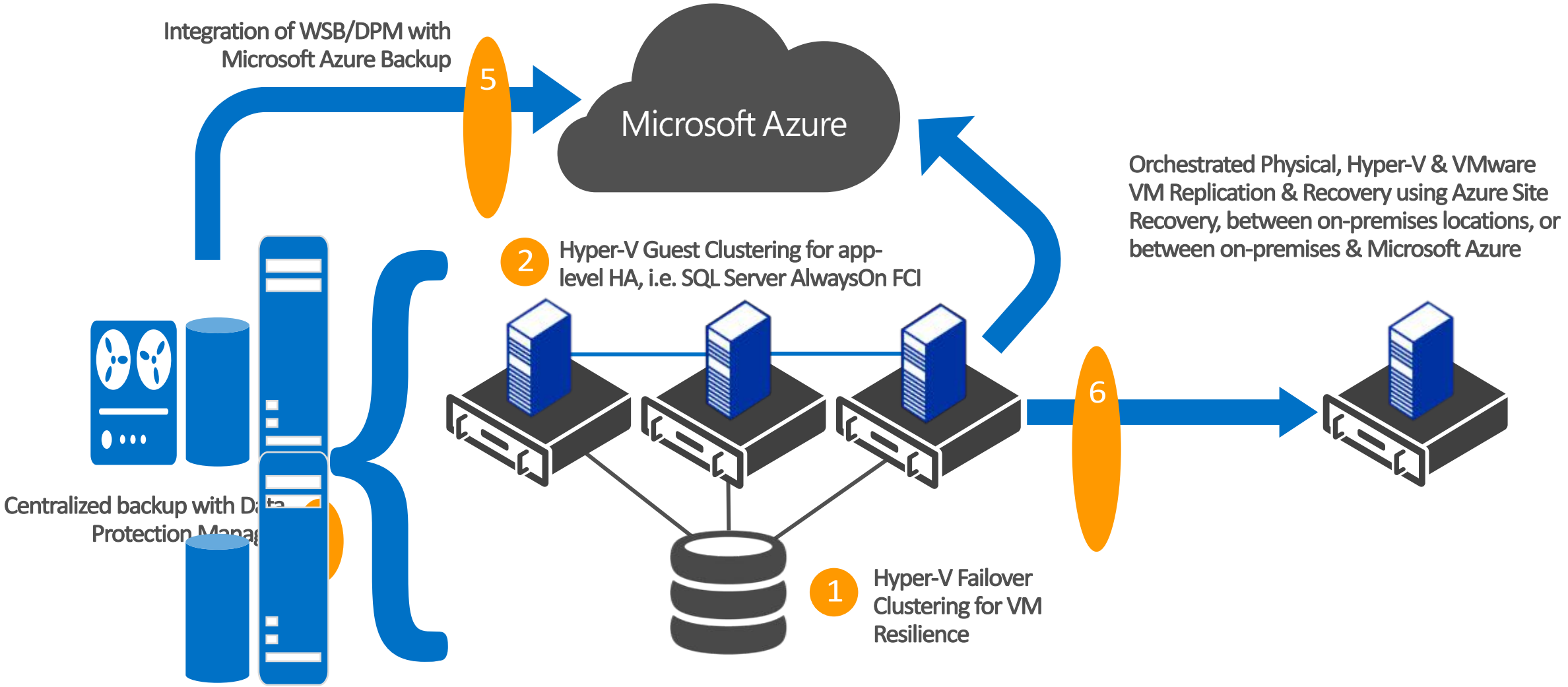


Continuous storage geo-replication

Windows Azure Storage

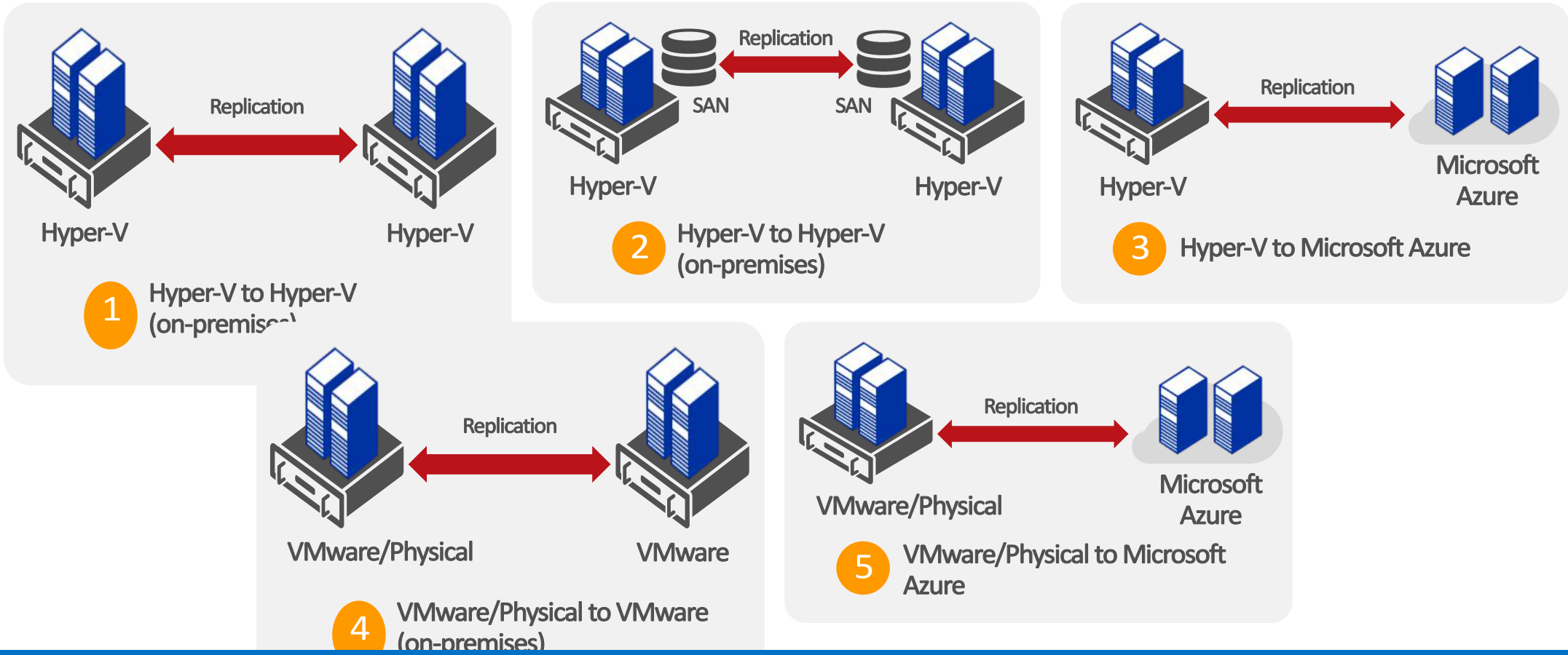
Microsoft Solutions

Breadth & depth solutions for business continuity & disaster recovery



Azure Site Recovery

One solution for multiple infrastructures

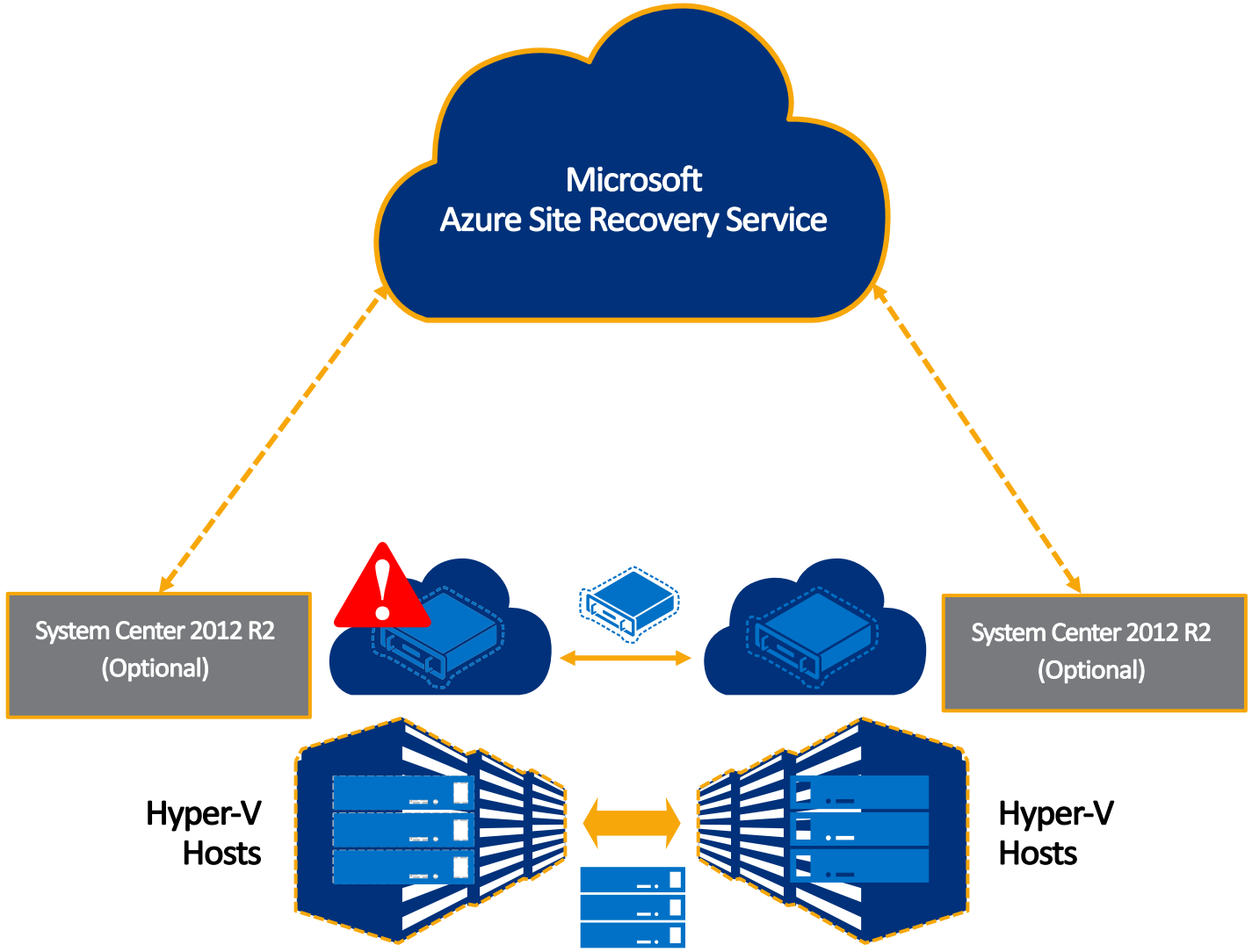


Protect important applications by coordinating the replication and recovery of private clouds across sites.
Protect your applications to your own second site, a HSP's site, or even use Microsoft Azure as your disaster recovery site

Azure Site Recovery Service

Orchestrate protection and recovery of private clouds

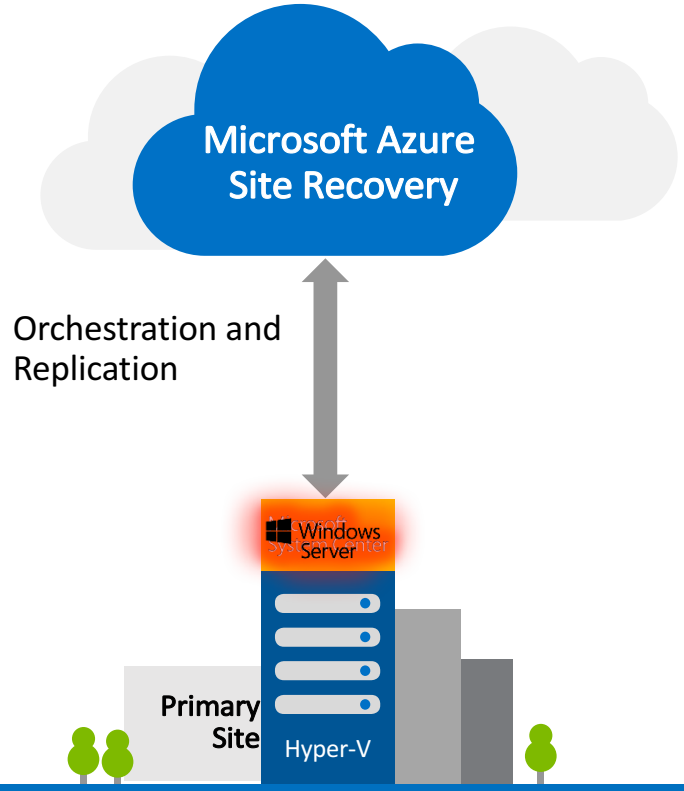
- Protect important services by coordinating replication and recovery of private clouds
- Automates replication of VMs within clouds between sites
- Hyper-V Replica provides replication, orchestrated by Azure Site Recovery Service
- Can be used for planned, unplanned and testing failover between sites
- Integrate with scripts for customization of recovery plans



ASR for SMBs to Azure

On-premises to Azure protection (Site-to-Azure)

October 2014



NEW December 2014

1. CUSTOMER TO *AZURE*
2. SMB TO *AZURE*

Key features include:

Automated VM protection and replication
Remote health monitoring
Near zero RPO

No-impact recovery plan testing
Customizable recovery plans
Minimal RTO – few minutes to hours

Orchestrated recovery when needed
Replicate to – and recover in – Azure
Heterogeneous physical and virtual support

Azure Site Recovery Service

Automated protection

Delivers on-going replication of virtual machines

Integrates with Hyper-V Replica and System Center Virtual Machine Manager technologies

Workload data remains in your network

Continuous health monitoring

Continuously and remotely monitors application availability

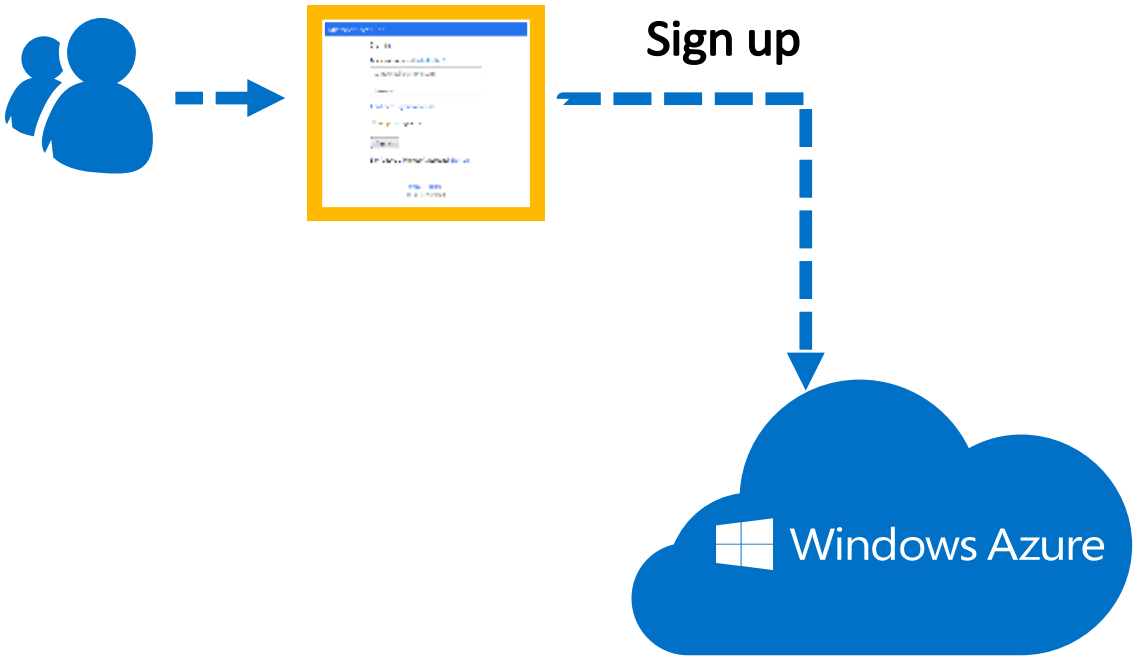
Orchestrated recovery

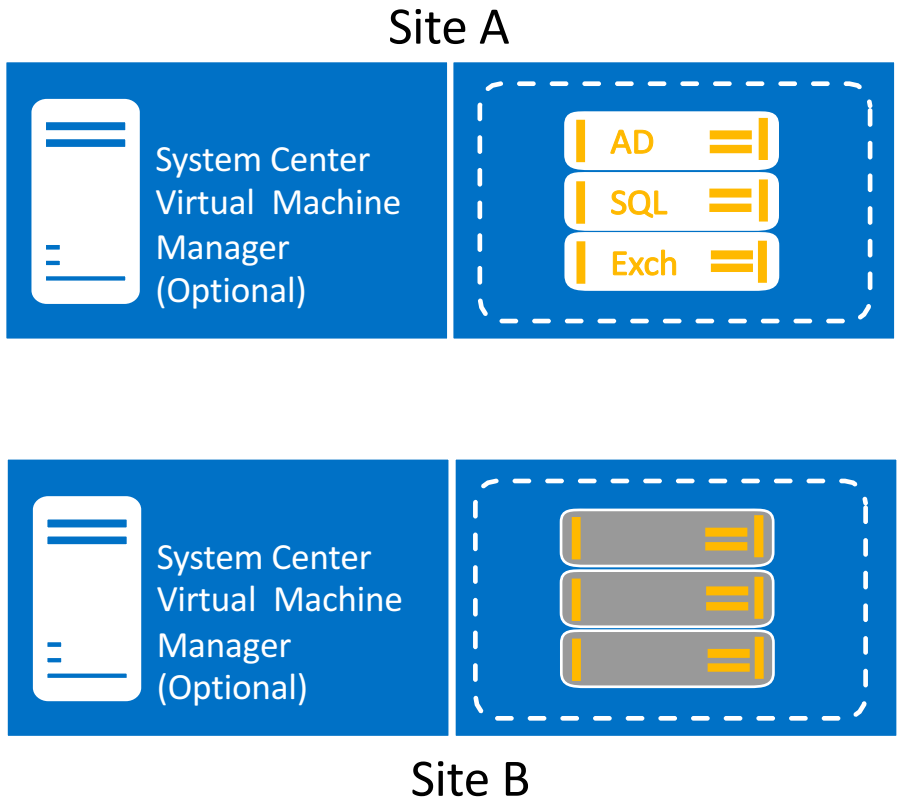
Orchestrates orderly recovery of virtual machines that compose multi-tier services

Offers customizable recovery plans

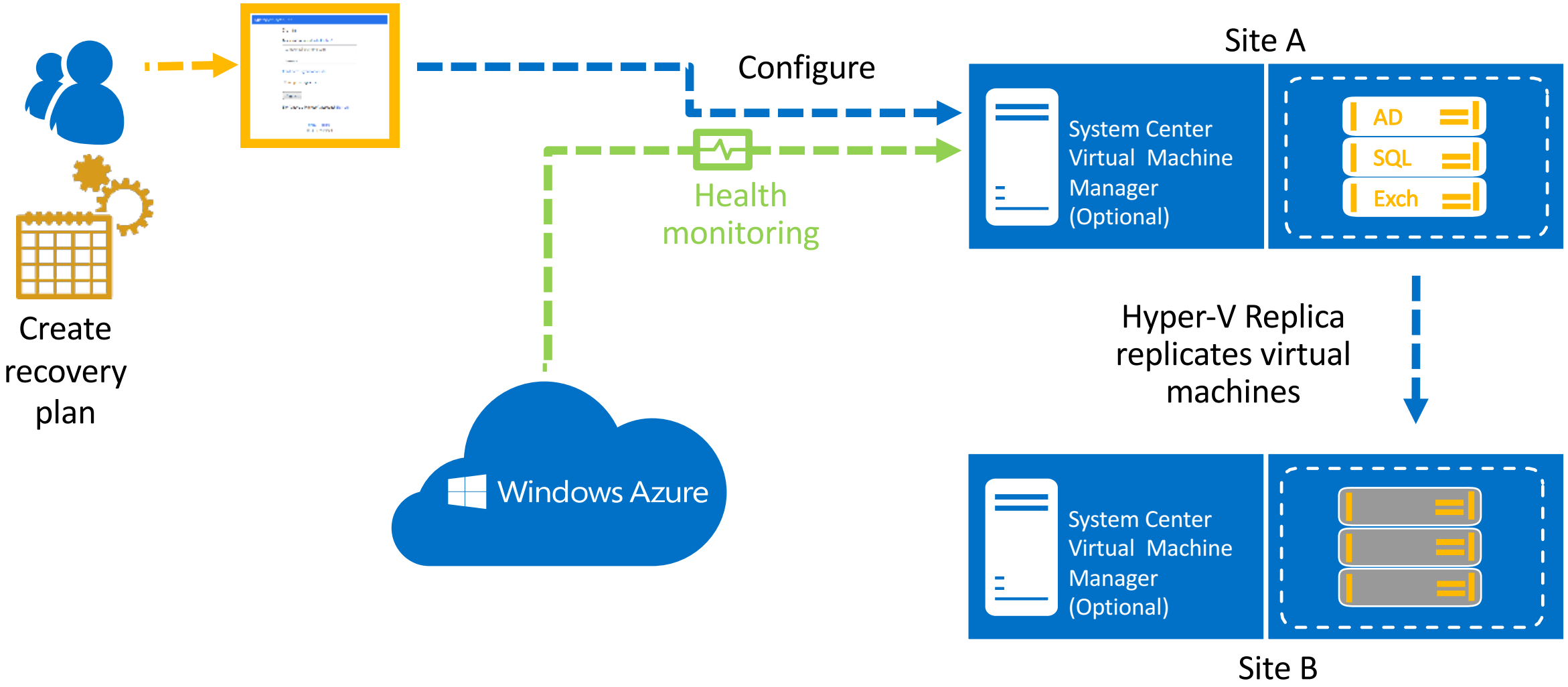
Simplifies recovery plan testing

How it works: configure

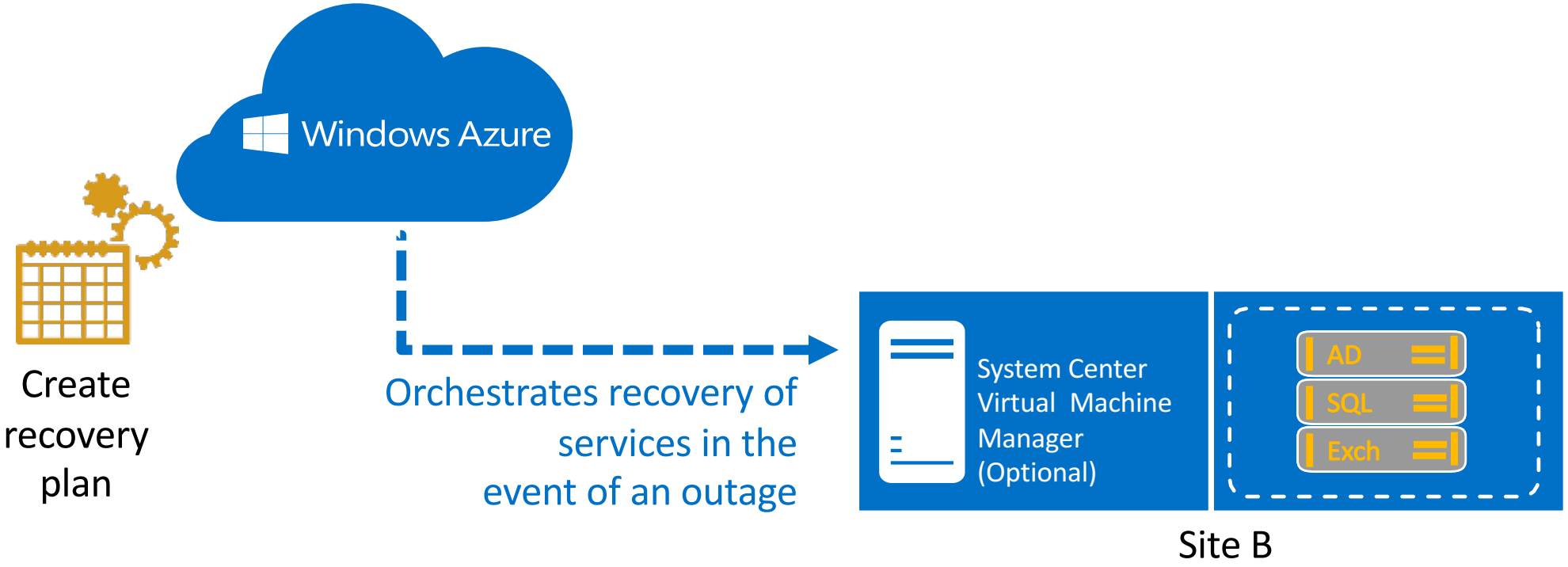




How it Works: Create Recovery Plan

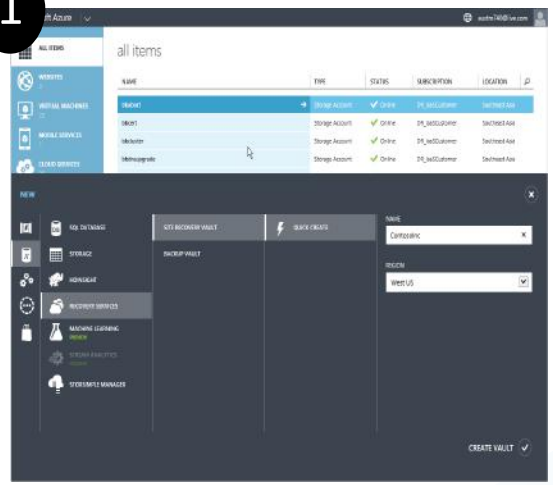


How it Works: Recover from Datacenter Failure



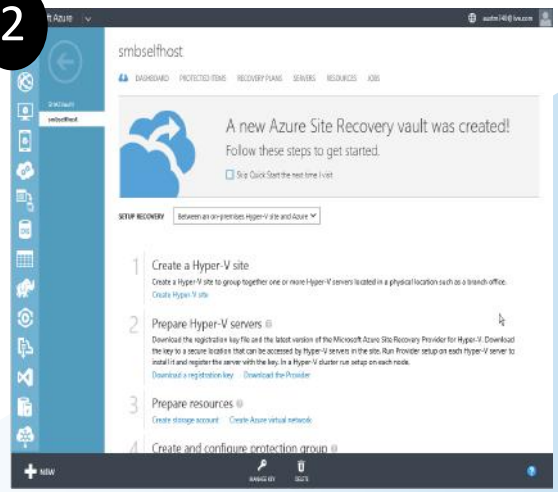
Summary

1



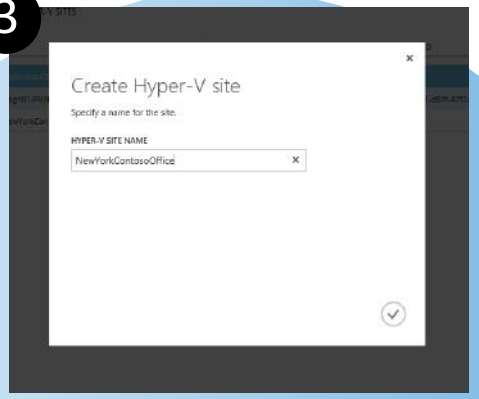
CREATE VAULT

2



QUICK START

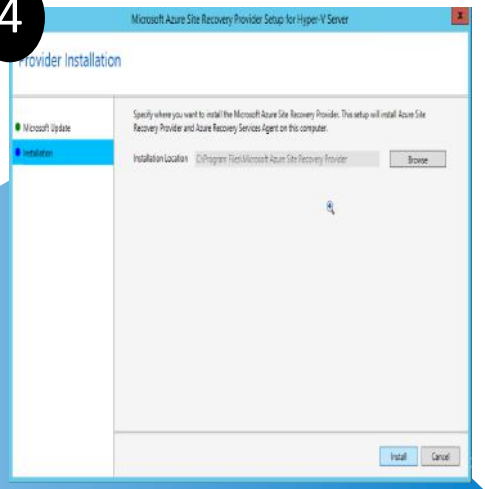
3



CREATE SITE

A group for servers to represent Site or Branch.

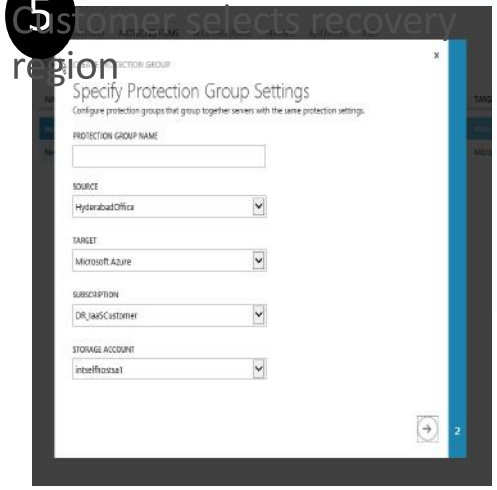
4



REGISTER

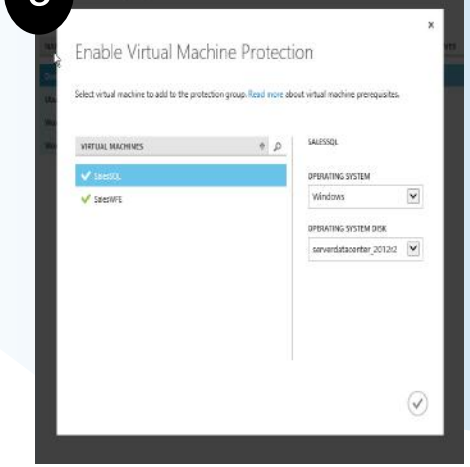
5

Customer selects recovery region



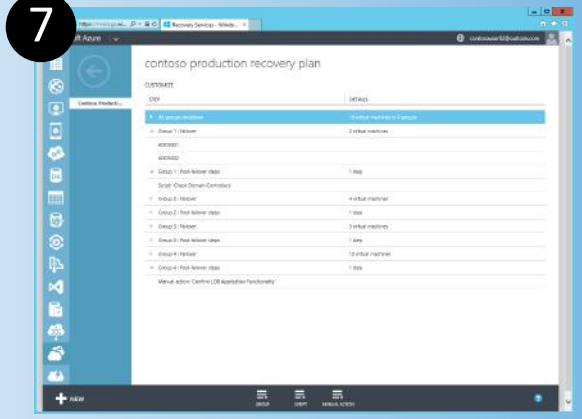
CONFIGURE PROTECTION

6



PROTECT VIRTUAL MACHINES

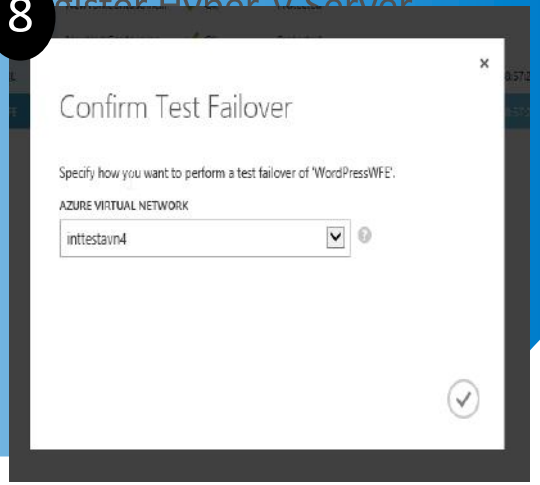
7



CREATE RECOVERY PLAN

Define DR Plan

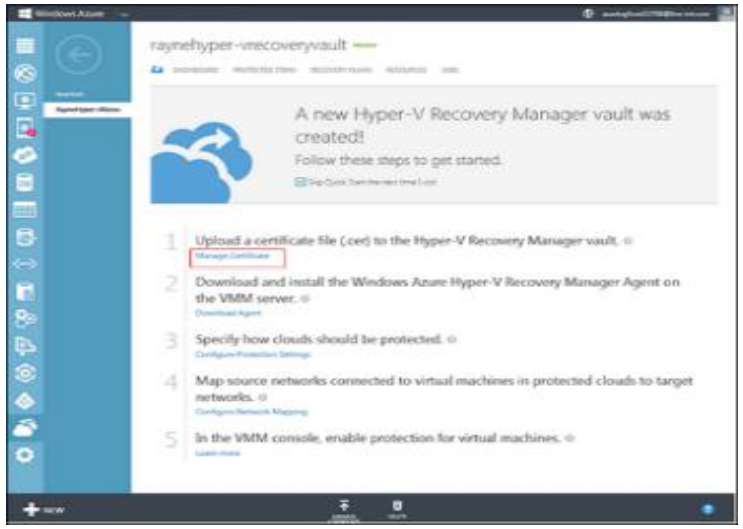
8

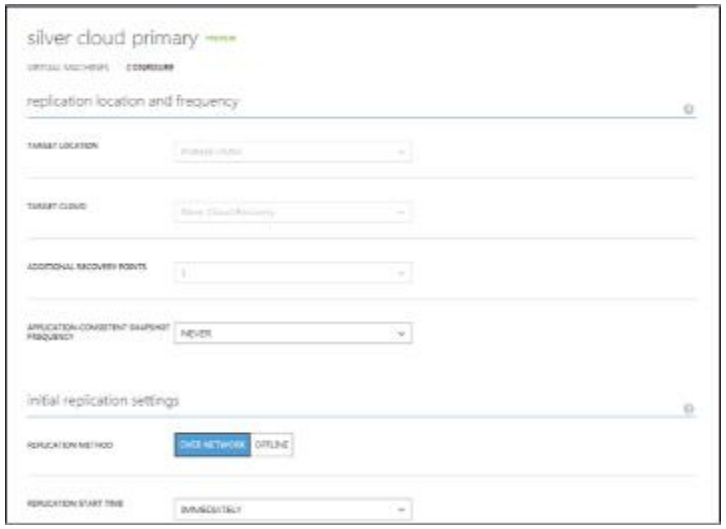


RUN DR DRILL

Flexible configuration options

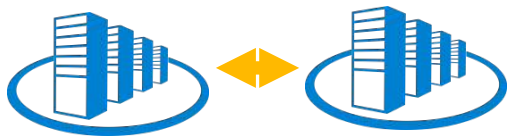
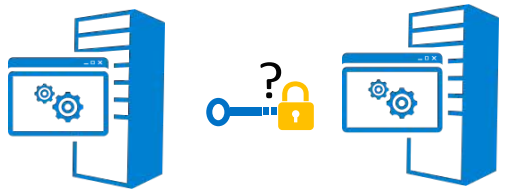
- Recovery plans are stored in Windows Azure as Cloud Services
- Select SCVMM clouds to protect
- Customize network mapping locally in SCVMM and failover same settings to a VNet in Azure
- Automatically enable replication of virtual machines
- Test recovery plans
- Monitor services





When to Choose Windows Azure Site Recovery Service?

If you:

Have a secondary site available	Use System Center Virtual Machine Manager (Optional)	Have currently unprotected workloads	Can benefit from reducing the impact of planned downtime at your primary data center
	Microsoft System Center		

When Azure Site Recovery Service May Not Fit

- The workload requires synchronous replication
- The workload data lives outside of a VHD
- The workload needs to recover physical servers
- The workload requires a solution outside or beyond Hyper-V Replica's capabilities

manuel.w.lloydconsulting

Manuel W. Lloyd, CEO
1213 Culbreth Drive
Wilmington, NC 28405
910.210.0485 ext. 101