Backup VS Disaster Recovery – Why you need both

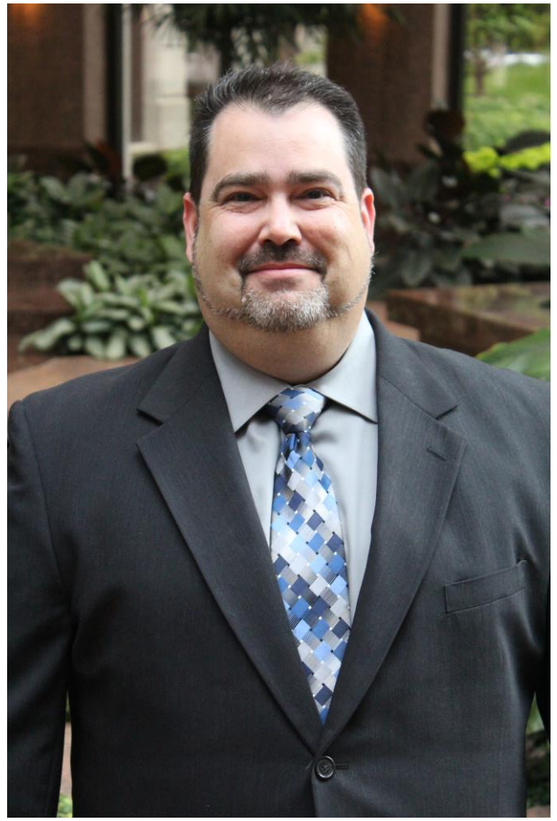
Mindsight℠
Formerly Tympani, Inc.
Technology. Transparency. Trust.

Agenda

- Data protection – past and present
- Disaster recovery vs backup
- What is right for your business
- Best practices
- Managed disaster recovery services

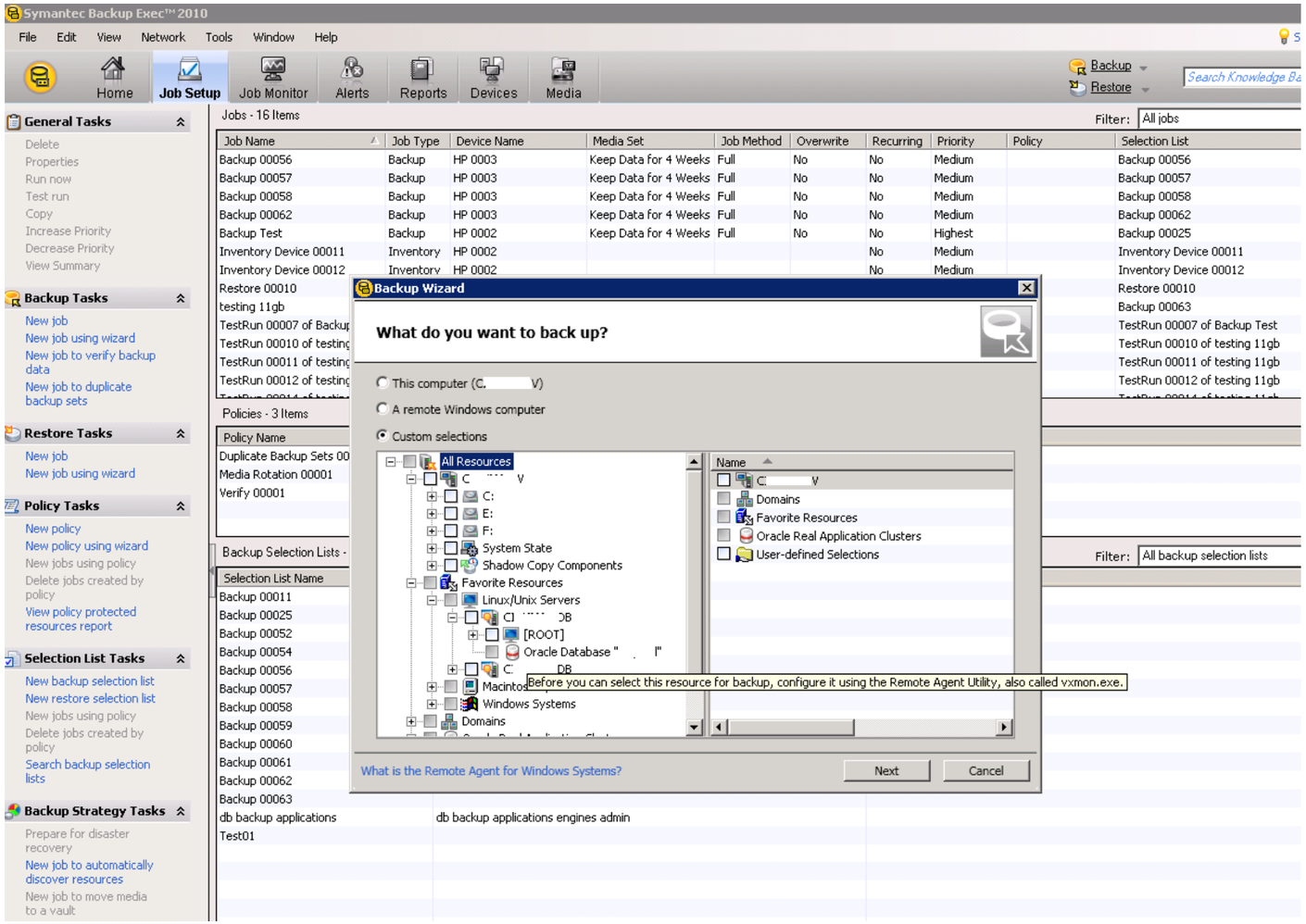
Jason Wankovsky
Mindsight CTO and VP of Consulting

- 20+ years of experience in IT management and executive leadership
- Focus on creation and delivery of high-value managed services
- Expertise in disaster recovery and backup solutions
- Experience as IT Manager and Consultant for mid-size and enterprise clients

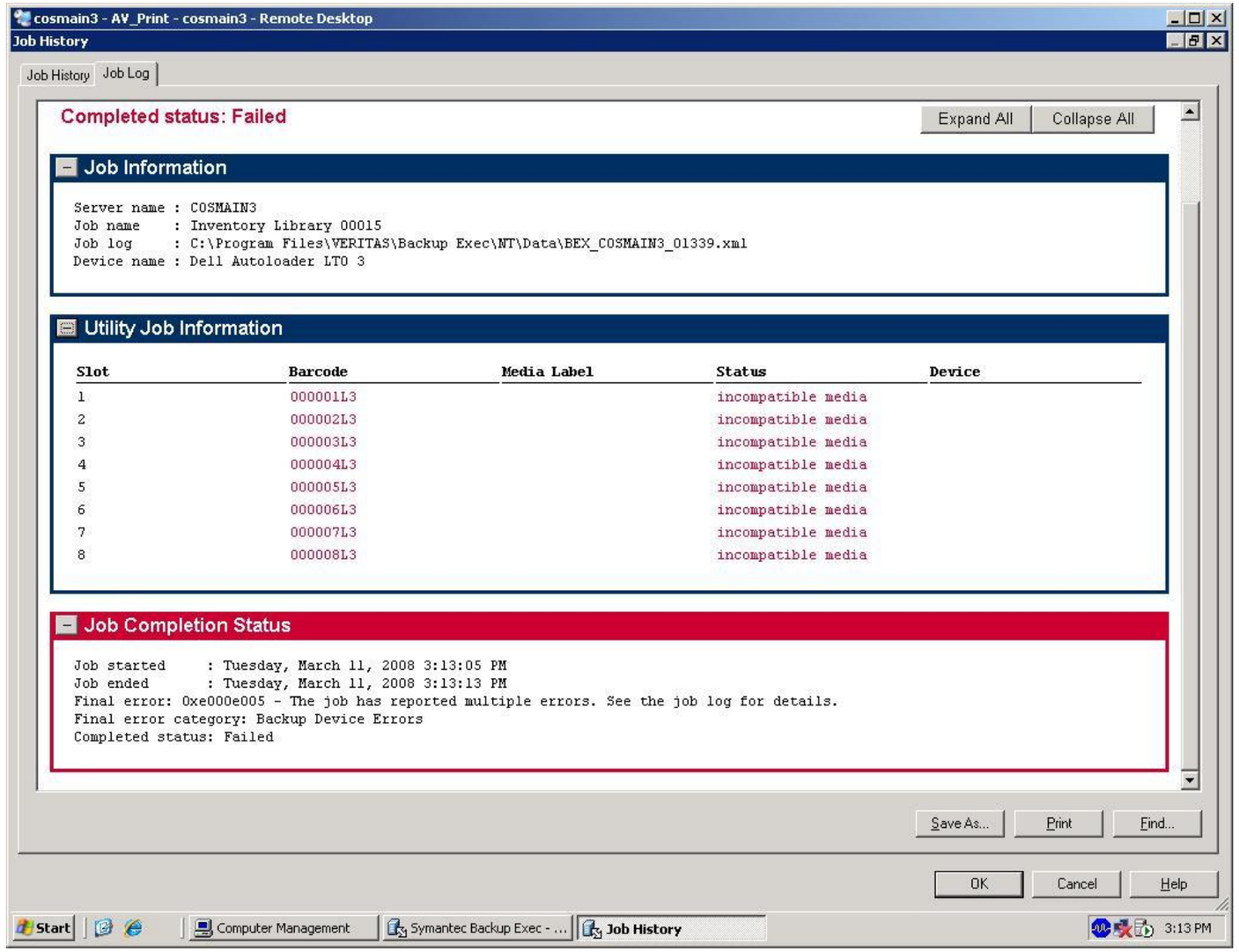


Data Protection Past and Present

Simple Creation of Jobs



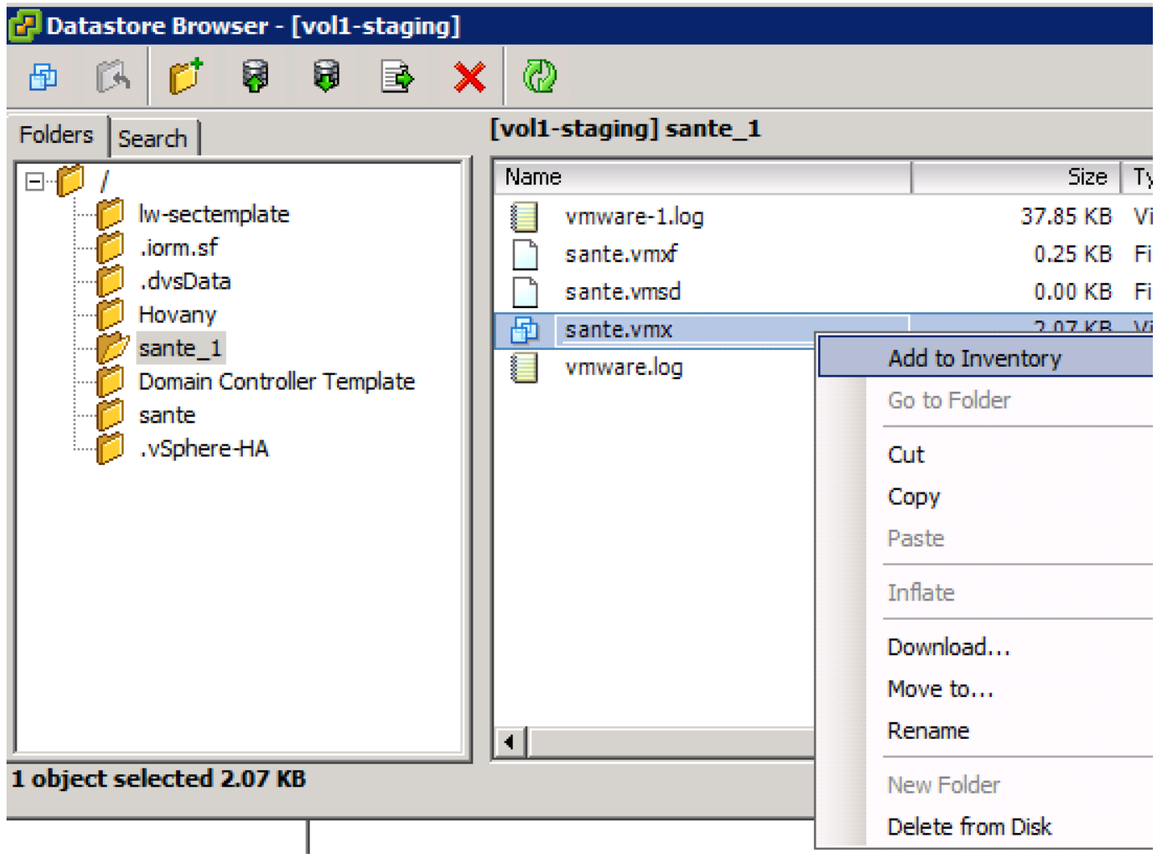
Troubleshooting Job Failures



Why Were Backups So Problematic?

- Agents running on bare metal servers unreliable
- Connection to backup targets an issue – WAN links
- Connection to tape library
- Upgrades to Library Firmware or Backup Software often broke backup jobs
- Required constant monitoring and testing – no time
- Selecting individual folders for backup
- Retaining permissions

What is Different about Modern Datacenters?



VS

Backup VS Disaster Recovery

How Disaster Recovery Differs from Backup

Disaster Recovery:

- A subset of business continuity
- Prepares for recovery or continuation of technology infrastructure - vital to an organization after a natural or human-induced disaster
- Systems or applications may be available but the end users may not be
- Disaster recovery ensures the data is available quickly after an outage

Backup:

- Copying and archiving of computer data so it can be used to restore the original after a data loss event
- Backup system contains at least one copy of all data worth saving
- Data storage requirements can be significant
- Organizing this storage space and managing the backup process can be a complicated undertaking

Why Do You Need Both?

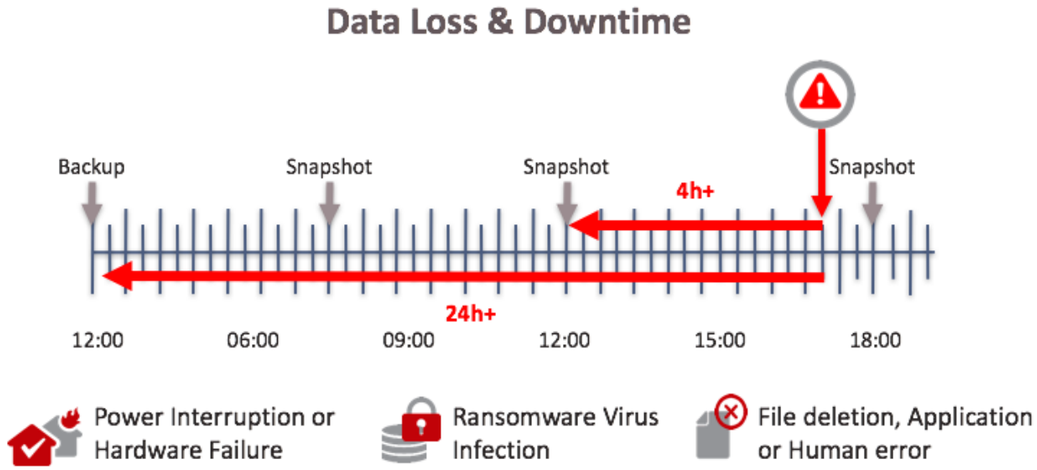
Backup: years of retention to meet internal and external compliance requirements, fewer recovery options

- Recovery takes a longer time, extending RPOs

Disaster Recovery: shorter retention, with many recovery options

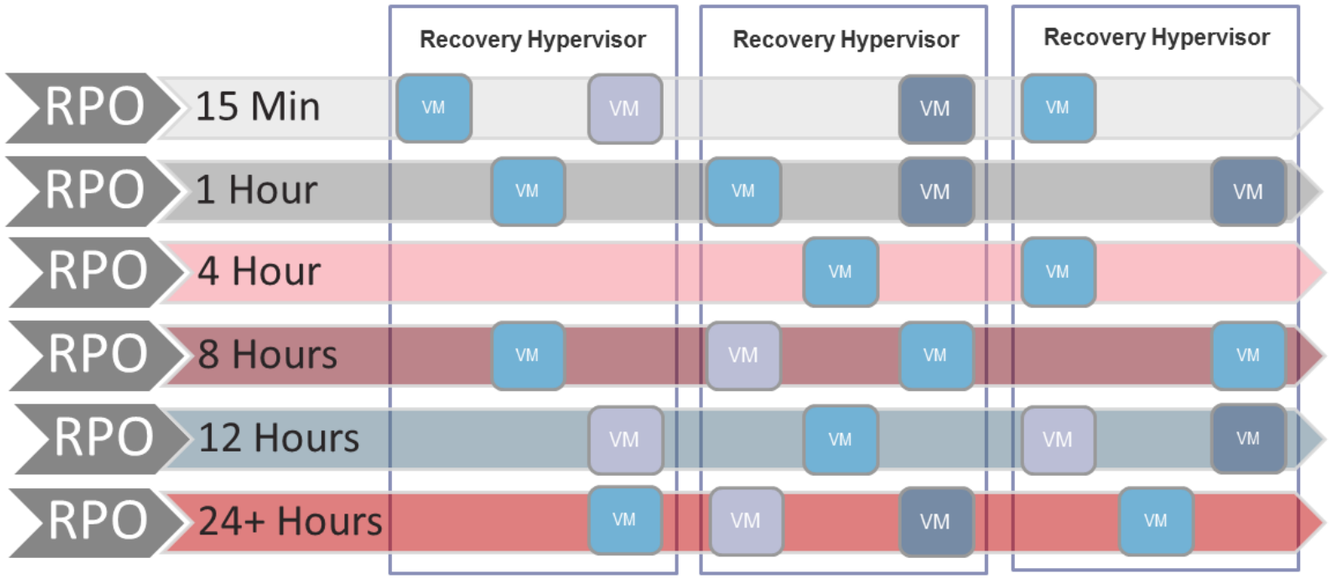
- Reduced RPO and RTO

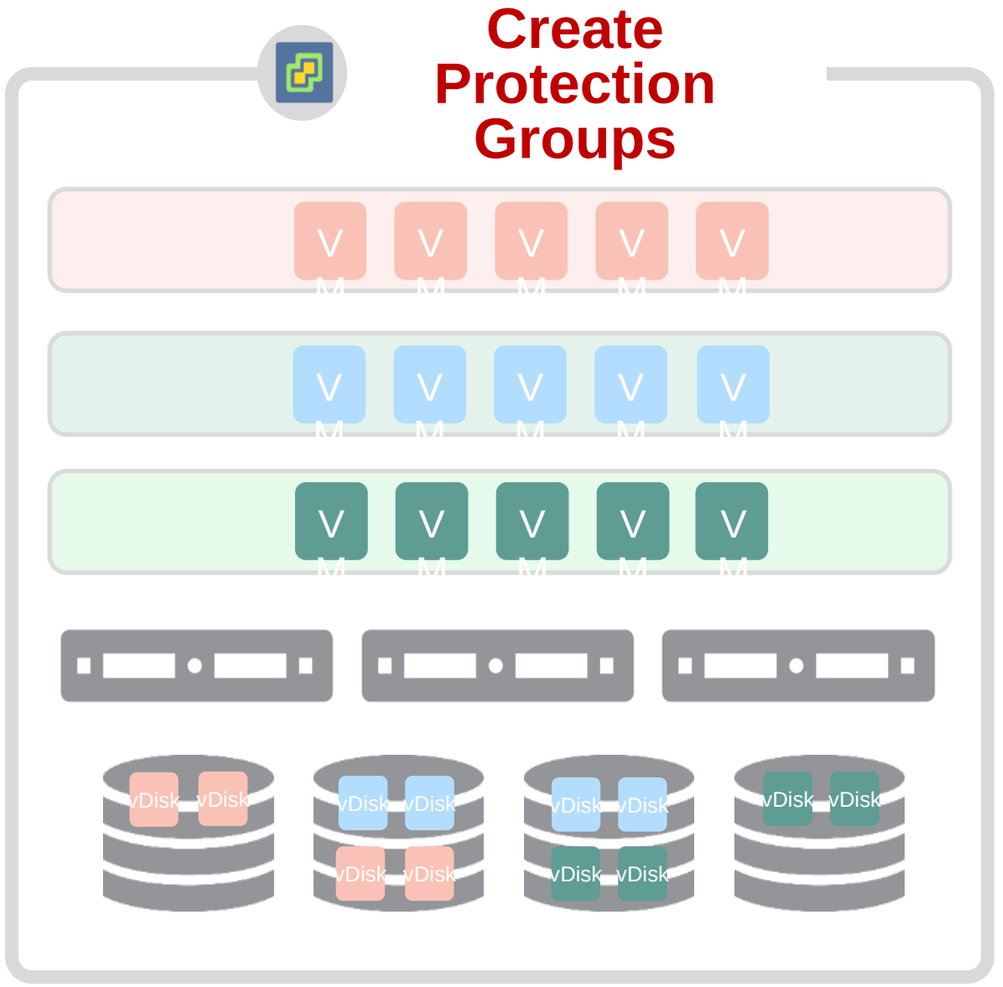
- Analysis of the businesses RPO and RTO needs, as well as the potential disaster to account for, will guide us on the method of recovery
- Lower RPO/RTO for your key applications will require the implementation of replication tools
  - Replication
    - Does NOT replace backup
    - Replicates corruption and data deletion



How Do I Know What I Need?

Assign RTO and RPO Needs by Application-Tiering





What is Right for My Business?

Defining a Sound Backup Strategy

- All business and all data need this!
- Needs to be consistent, reliable, tested and proven to work
- Needs to be constantly monitored; if an alert is detected, remediation needs to happen
- Second copy has to be sent offsite from the primary copy
  - Test the restore capabilities
  - In the event of a recovery from restore, you need to know that it will be successful to get you back to your last safe state

What Service Level is Required

Service Levels (Days / Hours / Minutes)

- Disaster Recovery delivers very aggressive service levels
  - — Recovery point objectives of seconds
  - — Recovery time objectives of minutes
- Backup delivers service levels that are better suited for a tier 3 application
  - — Can you lose 24 – 48 hours of data?
  - — Can the business survive without the application for 12/24/36 hours or more?

Define Application Requirements

Application Performance and Impact

- Disaster Recovery – The replication mechanism operates continuously and does not significantly impact the application
  - End-user productivity is not impacted
  - Revenue generating activities are not slowed
- Backup – The replication mechanism occurs at a set time(s) during the day and application performance slows
  - End-users notice a change in application performance
  - Backups usually occur in the overnight/early morning hours

DR Must Have:

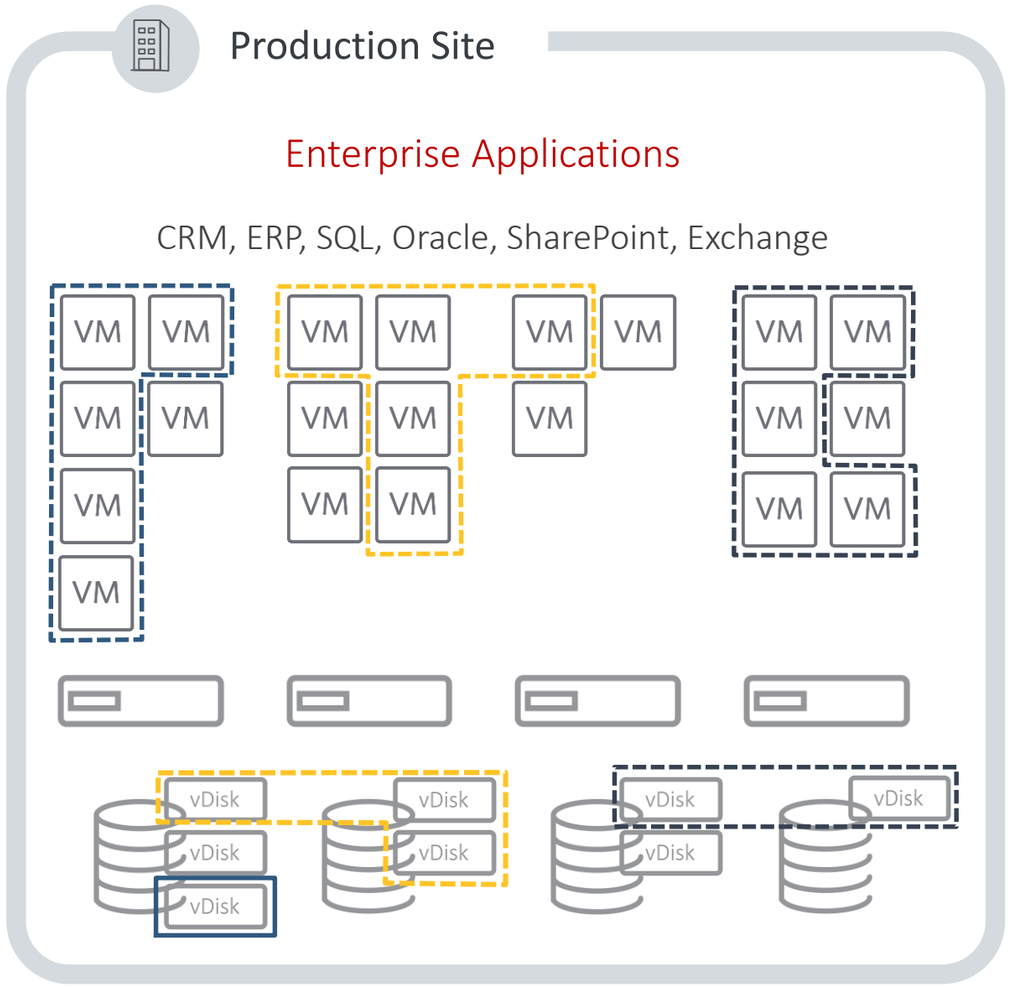
Automated Recovery

– Disaster Recovery should have minimal manual steps to ensure accuracy and speed

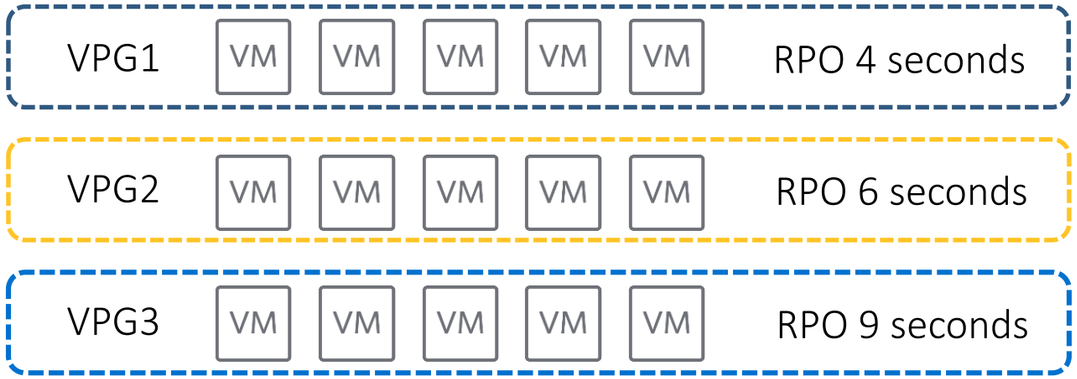
Reverse Protection

– Disaster Recovery should deliver the ability to replicate back to the production site for simple failback when possible

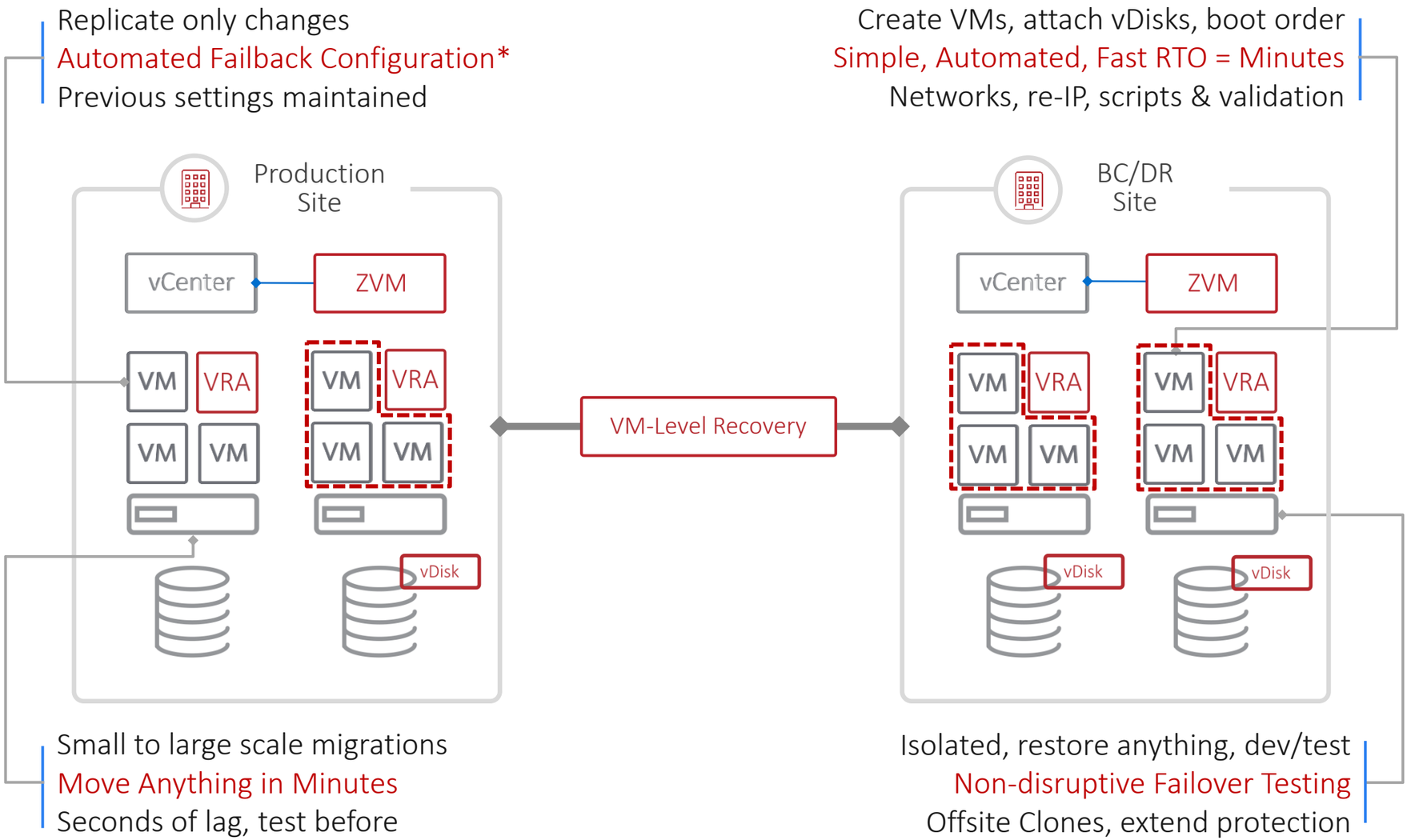
DR Must Have: Consistent Protection and Recovery



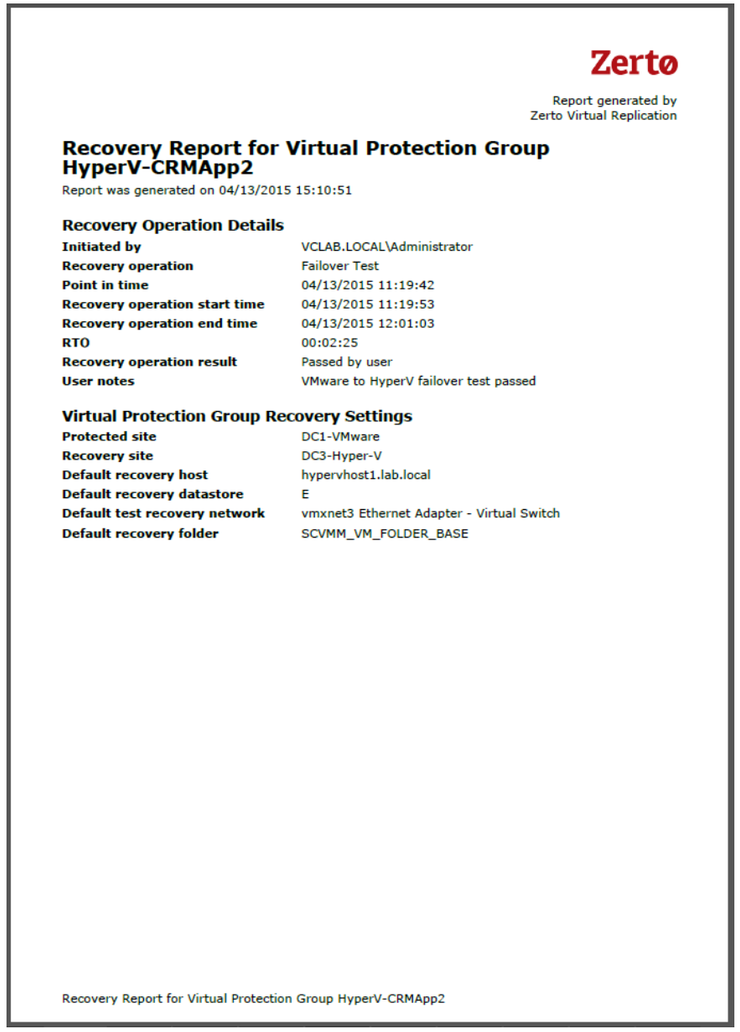
- LUN Consistency Group evolved = Virtual Protection Group
- Simple, scalable, protection & recovery of VMs, not LUNs
- Protect all VMs & recover multi-VM application stacks together
- Point in time recovery, write ordering & consistency
- Pre-configure recovery settings, network etc, prioritize VPGs
- Support virtualization features vMotion, svMotion, HA etc



DR Must Have: Disaster Recovery Automation



DR Must Have: Testing Recovery and Reporting



Zerto

Report generated by
Zerto Virtual Replication

Recovery Report for Virtual Protection Group HyperV-CRMApp2

Report was generated on 04/13/2015 15:10:51

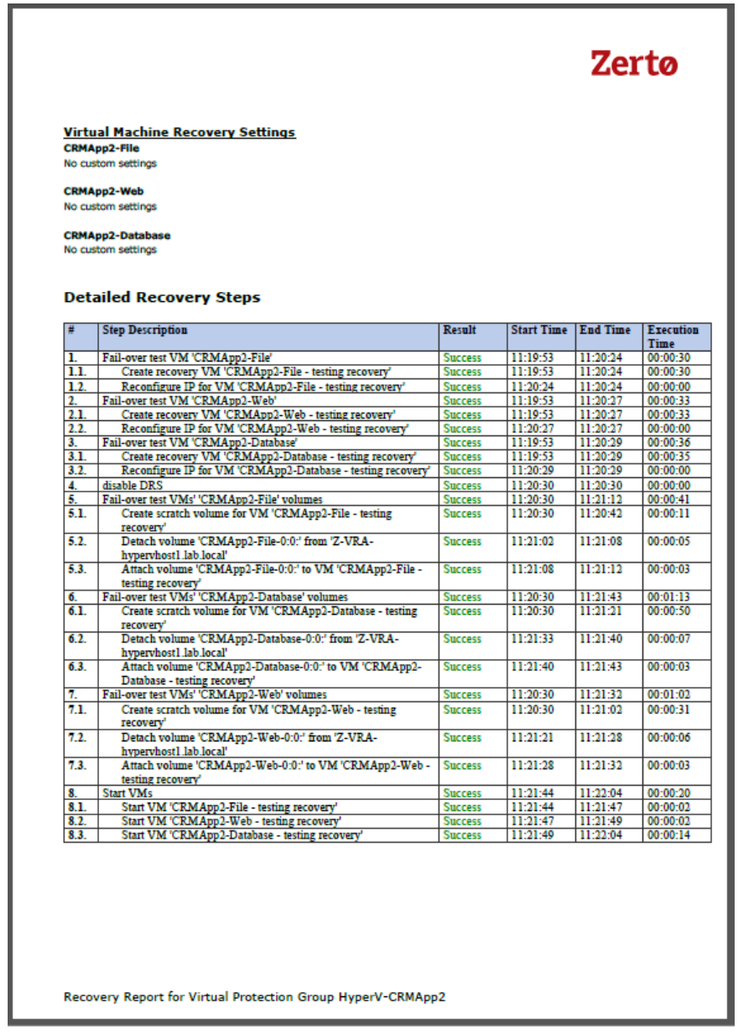
Recovery Operation Details

Initiated by	VCLAB.LOCAL\Administrator
Recovery operation	Failover Test
Point in time	04/13/2015 11:19:42
Recovery operation start time	04/13/2015 11:19:53
Recovery operation end time	04/13/2015 12:01:03
RTO	00:02:25
Recovery operation result	Passed by user
User notes	VMware to HyperV failover test passed

Virtual Protection Group Recovery Settings

Protected site	DC1-VMware
Recovery site	DC3-Hyper-V
Default recovery host	hypervhost1.lab.local
Default recovery datastore	E
Default test recovery network	vmxnet3 Ethernet Adapter - Virtual Switch
Default recovery folder	SCVMM_VM_FOLDER_BASE

Recovery Report for Virtual Protection Group HyperV-CRMApp2



Zerto

Virtual Machine Recovery Settings

CRMApp2-File
No custom settings

CRMApp2-Web
No custom settings

CRMApp2-Database
No custom settings

Detailed Recovery Steps

#	Step Description	Result	Start Time	End Time	Execution Time
1.	Fail-over test VM 'CRMApp2-File'	Success	11:19:53	11:20:24	00:00:30
1.1.	Create recovery VM 'CRMApp2-File - testing recovery'	Success	11:19:53	11:20:24	00:00:30
1.2.	Reconfigure IP for VM 'CRMApp2-File - testing recovery'	Success	11:20:24	11:20:24	00:00:00
2.	Fail-over test VM 'CRMApp2-Web'	Success	11:19:53	11:20:27	00:00:33
2.1.	Create recovery VM 'CRMApp2-Web - testing recovery'	Success	11:19:53	11:20:27	00:00:33
2.2.	Reconfigure IP for VM 'CRMApp2-Web - testing recovery'	Success	11:20:27	11:20:27	00:00:00
3.	Fail-over test VM 'CRMApp2-Database'	Success	11:19:53	11:20:29	00:00:36
3.1.	Create recovery VM 'CRMApp2-Database - testing recovery'	Success	11:19:53	11:20:29	00:00:35
3.2.	Reconfigure IP for VM 'CRMApp2-Database - testing recovery'	Success	11:20:29	11:20:29	00:00:00
4.	disable DRS	Success	11:20:30	11:20:30	00:00:00
5.	Fail-over test VMs' 'CRMApp2-File' volumes	Success	11:20:30	11:21:12	00:00:41
5.1.	Create scratch volume for VM 'CRMApp2-File - testing recovery'	Success	11:20:30	11:20:42	00:00:11
5.2.	Detach volume 'CRMApp2-File-0:0:' from 'Z-VRA-hypervhost1.lab.local'	Success	11:21:02	11:21:08	00:00:05
5.3.	Attach volume 'CRMApp2-File-0:0:' to VM 'CRMApp2-File - testing recovery'	Success	11:21:08	11:21:12	00:00:03
6.	Fail-over test VMs' 'CRMApp2-Database' volumes	Success	11:20:30	11:21:43	00:01:13
6.1.	Create scratch volume for VM 'CRMApp2-Database - testing recovery'	Success	11:20:30	11:21:21	00:00:50
6.2.	Detach volume 'CRMApp2-Database-0:0:' from 'Z-VRA-hypervhost1.lab.local'	Success	11:21:33	11:21:40	00:00:07
6.3.	Attach volume 'CRMApp2-Database-0:0:' to VM 'CRMApp2-Database - testing recovery'	Success	11:21:40	11:21:43	00:00:03
7.	Fail-over test VMs' 'CRMApp2-Web' volumes	Success	11:20:30	11:21:32	00:01:02
7.1.	Create scratch volume for VM 'CRMApp2-Web - testing recovery'	Success	11:20:30	11:21:02	00:00:31
7.2.	Detach volume 'CRMApp2-Web-0:0:' from 'Z-VRA-hypervhost1.lab.local'	Success	11:21:21	11:21:28	00:00:06
7.3.	Attach volume 'CRMApp2-Web-0:0:' to VM 'CRMApp2-Web - testing recovery'	Success	11:21:28	11:21:32	00:00:03
8.	Start VMs	Success	11:21:44	11:22:04	00:00:20
8.1.	Start VM 'CRMApp2-File - testing recovery'	Success	11:21:44	11:21:47	00:00:02
8.2.	Start VM 'CRMApp2-Web - testing recovery'	Success	11:21:47	11:21:49	00:00:02
8.3.	Start VM 'CRMApp2-Database - testing recovery'	Success	11:21:49	11:22:04	00:00:14

Recovery Report for Virtual Protection Group HyperV-CRMApp2

Regulatory Compliance

- GDPR
- PCI
- ISO
- SOX
- HIPAA
- SEC

Managed DR Services

Disaster Recovery as a Service

- Procuring outcome of recoverability through preparedness & testing
  - — Application/Service Tiering
  - — Days / Hours / Minutes
- Recovering critical applications at an alternate DR site for anywhere access by users performing functional testing
- 72 hour user application test time AFTER your IT team agrees recovery is a success!
- Documentation for compliance
- DR site resources reserved for time of need or disaster

Defining DRaaS Roles and Responsibilities

Disaster Recovery as a Service

- DRaaS takes DR one step further – offloads failover availability management, testing and execution of event mitigation to Mindsight
- In a DRaaS environment, the replication of your virtual or physical infrastructure takes place in our data centers
- The DRP policies, procedures, and actions are clearly defined by both your organization and Mindsight
- Our team conducts regular testing of failovers scenarios; in the event of an actual emergency, we perform your failover
- The entire DRaaS service is wrapped in a predefined Service Level Agreement (SLA) specifically written to achieve your businesses operating objectives

Backup: Your “Days” Scenario

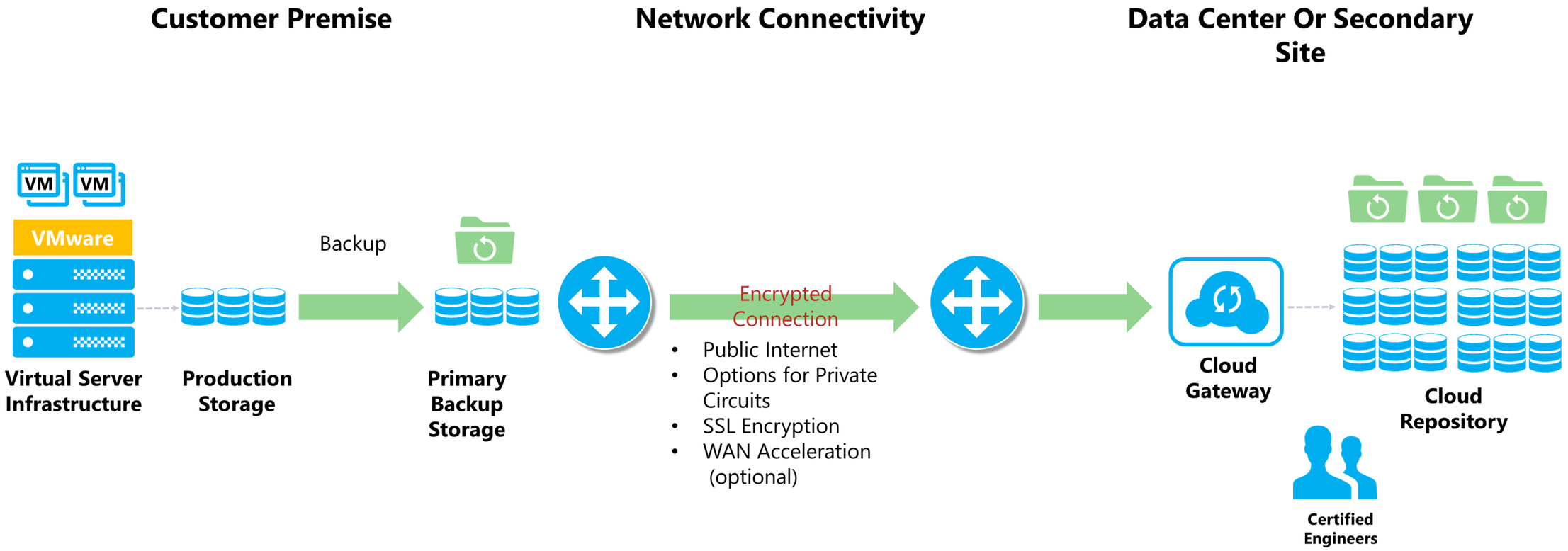
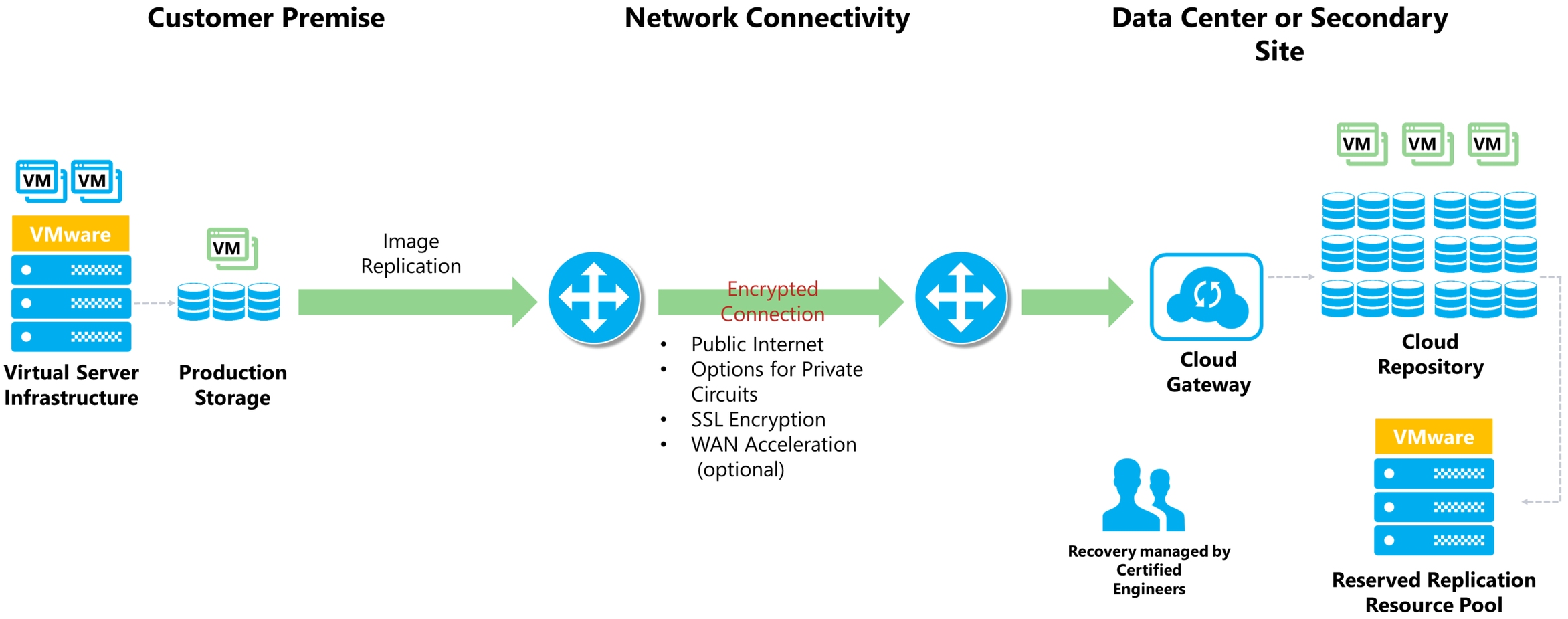
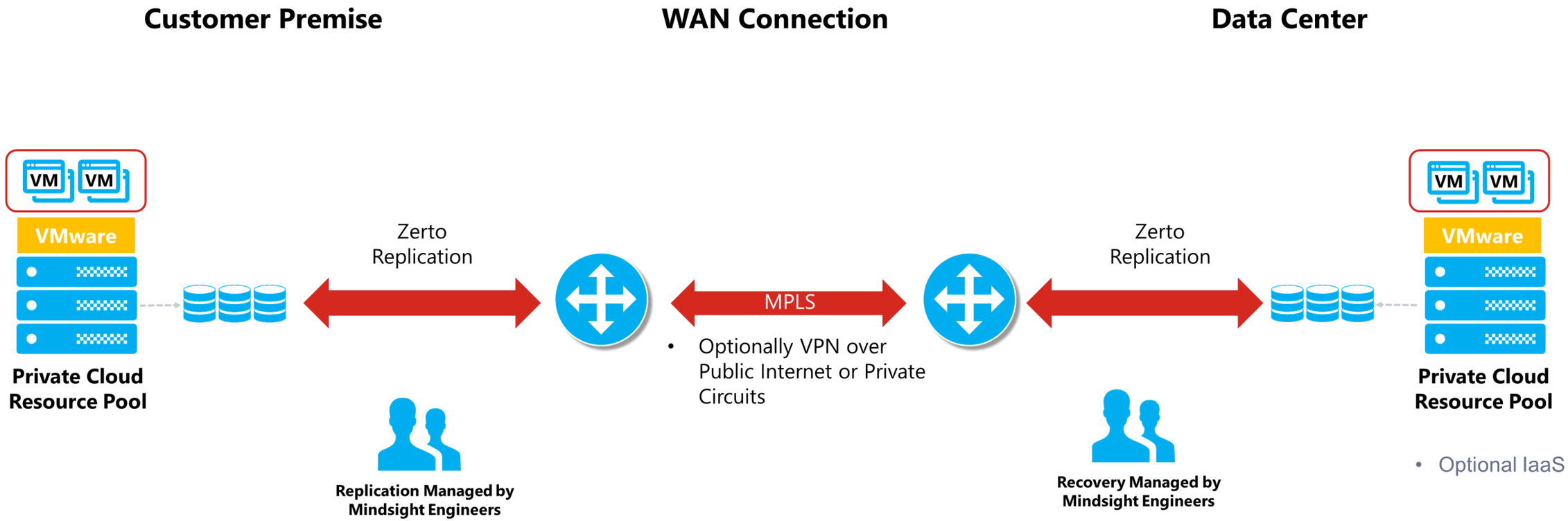


Image Replication: Your “Hours” Scenario



Data/System Replication: Your “Minutes” Scenario

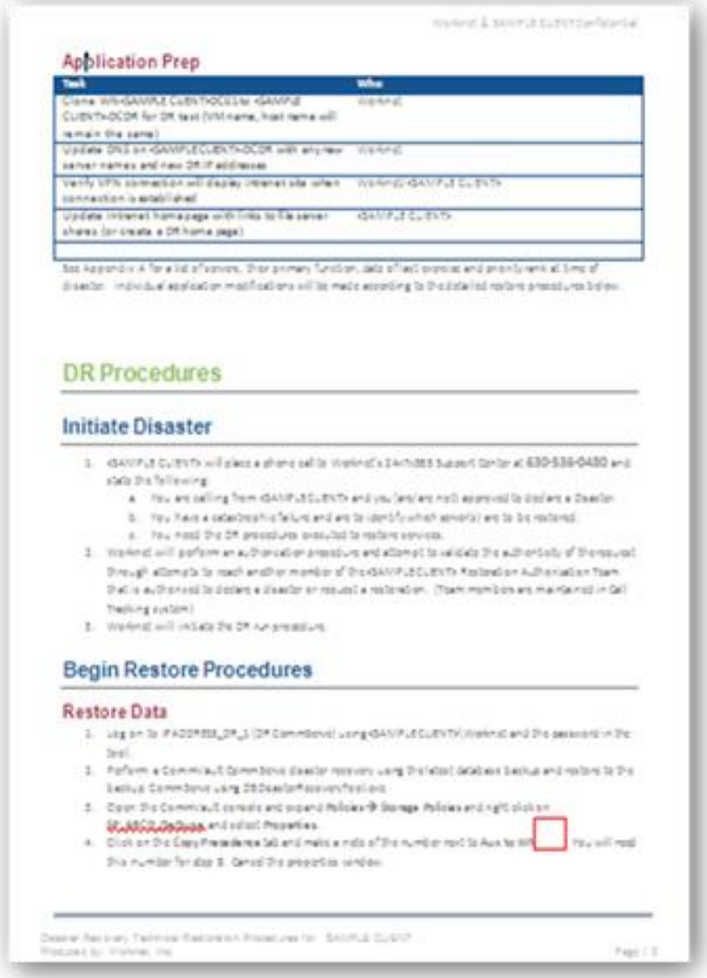


None of This Matters Without a Plan AND Testing!

Sample Project Plan Outline

Managed Disaster Recovery - Documentation

Step-by-Step DR Technical Recovery Procedures



Application Prep

Task	Who
Clone WIN-SAMPLECLIENTHOCO1 to <SAMPLE CLIENT>-DCDR for DR test (VM name, host name will remain the same)	Wishmid
Update DNS on <SAMPLECLIENT>-DCDR with any new server names and new DR IP addresses	Wishmid
Verify VPN connection will display internal site when connection is established	Wishmid/<SAMPLE CLIENT>
Update internal homepage with links to file server shares (or create a DR home page)	<SAMPLE CLIENT>

See Appendix A for a list of servers, their primary function, data affect in case and prioritization in case of disaster. Individual application modifications will be made according to the detailed restore procedure below.

DR Procedures

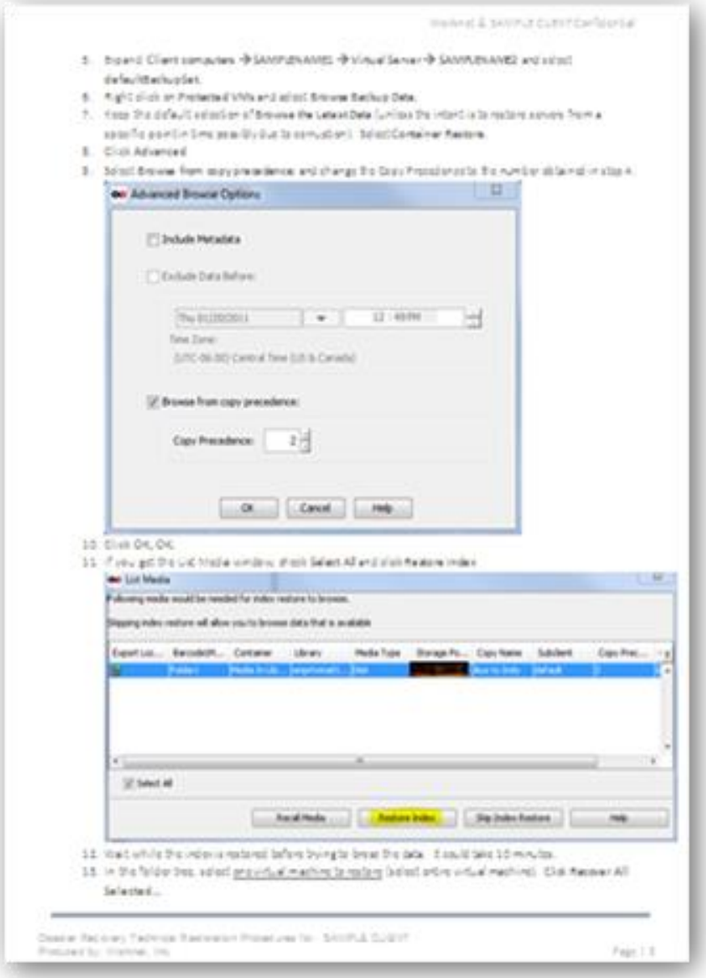
Initiate Disaster

1. <SAMPLE CLIENT> will place a phone call to Wishmid's Switch55 Support Center at 630-536-0400 and state the following:
   a. You are calling from <SAMPLE CLIENT> and you/are not approved to declare a Disaster
   b. You have a catastrophic failure and are to identify which server(s) are to be restored
   c. You need the DR procedure executed to restore services.
2. Wishmid will perform an authorization procedure and attempt to validate the authenticity of the request through attempts to reach another member of the <SAMPLE CLIENT> Restoration Authorization Team that is authorized to declare a disaster or request a restoration. (Team members are maintained in Call Tracking system)
3. Wishmid will initiate the DR run procedure.

Begin Restore Procedures

Restore Data

1. Log on to IP ADDRESS_DR_1 DR CommServe using <SAMPLECLIENT\Wishmid> and the password in the Vault.
2. Perform a CommVault CommServe disaster recovery using the latest database backup and restore to the backup CommServe using DRDisasterRecoveryTool.exe.
3. Open the CommVault console and expand Policies→ Storage Policies and right click on [redacted] and select Properties.
4. Click on the Copy Precedence Tab and make a note of the number next to Auxiliary. You will need this number for step 8. Cancel the properties window.



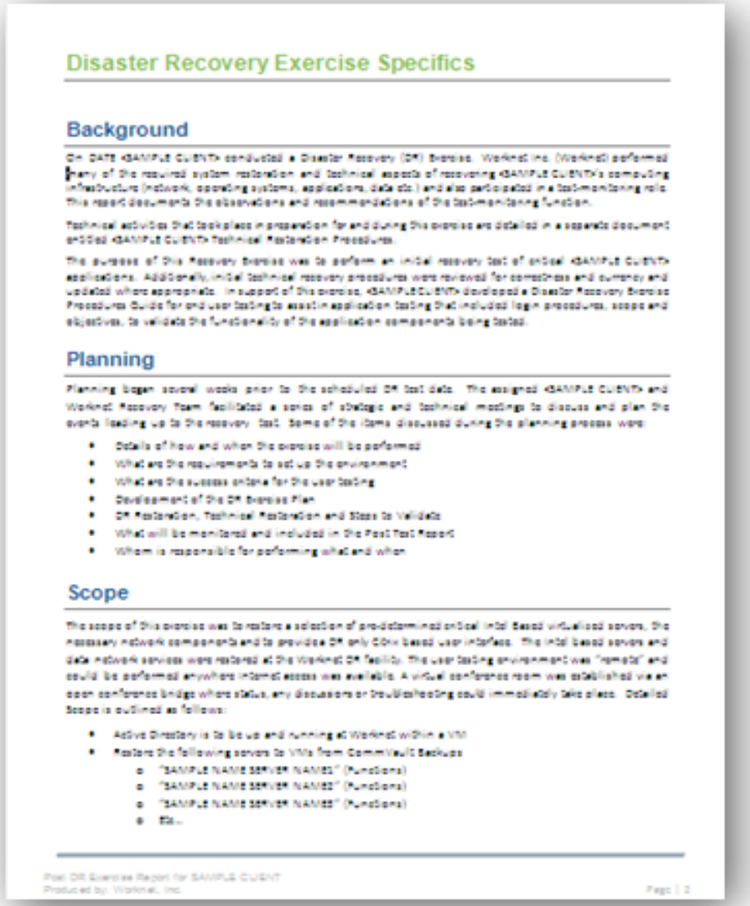
5. Expand Client computers → SAMPLENAME1 → Virtual Server → SAMPLENAME2 and select defaultBackupSet.
6. Right click on Protected VMs and select Browse Backup Data.
7. Keep the default selection of Browse the Latest Data (unless the intent is to restore servers from a specific point in time possibly due to corruption). Select Container Restore.
8. Click Advanced.
9. Select Browse from copy precedence and change the Copy Precedence to the number obtained in step 4.

10. Click OK, OK.
11. If you get the List Media window, click Select All and click Restore Index.

12. Wait while the index is restored before trying to browse the data. It could take 10 minutes.
13. In the folder tree, select one virtual machine to restore (select entire virtual machine). Click Recover All Selected...

Managed Disaster Recovery - Documentation

DR Exercise Report and Recovery Time Achieved



Disaster Recovery Exercise Specifics

Background

On DATE <SAMPLE CLIENT> conducted a Disaster Recovery (DR) Exercise. Workinet Inc. (Workinet) performed many of the required system restoration and technical aspects of recovering <SAMPLE CLIENT>'s computing infrastructure (network, operating systems, applications, data etc.) and also participated in a testmonitoring role. This report documents the observations and recommendations of the testmonitoring function.

Technical activities that took place in preparation for and during this exercise are detailed in a separate document entitled <SAMPLE CLIENT> Technical Restoration Procedures.

The purpose of this Recovery Exercise was to perform an initial recovery test of critical <SAMPLE CLIENT> applications. Additionally, initial technical recovery procedures were reviewed for correctness and currency and updated where appropriate. In support of this exercise, <SAMPLE CLIENT> developed a Disaster Recovery Exercise Procedures Guide for end user testing to assist in application testing that included login procedures, scope and objectives, to validate the functionality of the application components being tested.

Planning

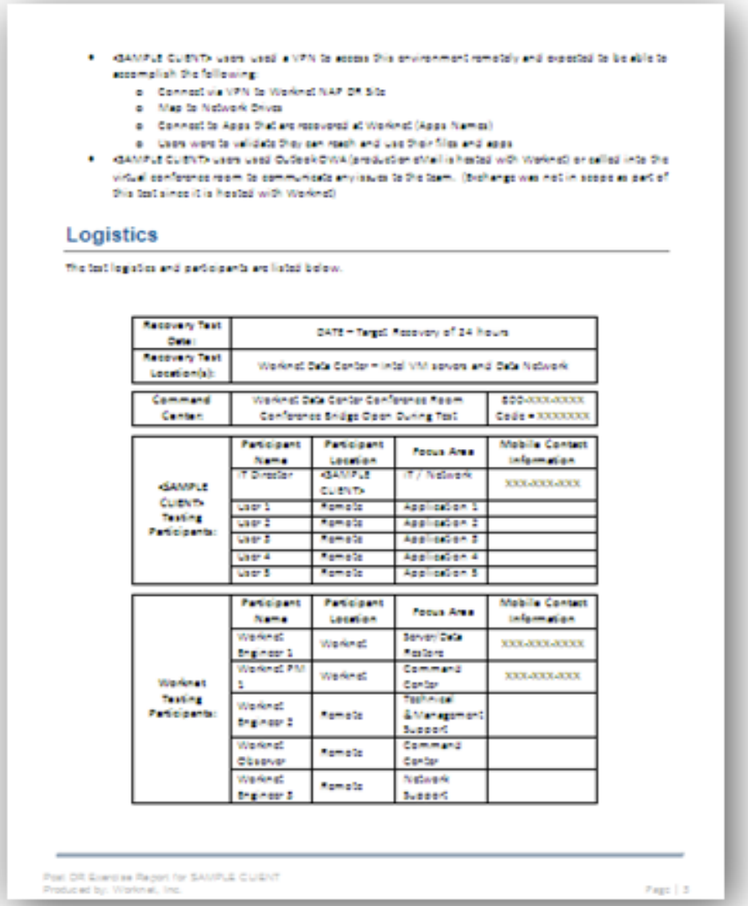
Planning began several weeks prior to the scheduled DR test date. The assigned <SAMPLE CLIENT> and Workinet Recovery Team facilitated a series of strategic and technical meetings to discuss and plan the events leading up to the recovery test. Some of the items discussed during the planning process were:

- Details of how and when the exercise will be performed
- What are the requirements to set up the environment
- What are the success criteria for the user testing
- Development of the DR Exercise Plan
- DR Restoration, Technical Restoration and Steps to Validate
- What will be monitored and included in the Post Test Report
- Whom is responsible for performing what and when

Scope

The scope of this exercise was to restore a selection of pre-determined critical Intel Based virtualized servers, the necessary network components and to provide DR only Citrix based user interface. The Intel based servers and data network services were restored at the Workinet DR facility. The user testing environment was "remote" and could be performed anywhere internet access was available. A virtual conference room was established via an open conference bridge where status, any discussions or troubleshooting could immediately take place. Detailed Scope is outlined as follows:

- Active Directory is to be up and running at Workinet within a VM
- Restore the following servers to VMs from CommVault Backups
  - "SAMPLE NAME SERVER NAME1" (Functions)
  - "SAMPLE NAME SERVER NAME2" (Functions)
  - "SAMPLE NAME SERVER NAME3" (Functions)
  - Etc..



- <SAMPLE CLIENT> users used a VPN to access this environment remotely and expected to be able to accomplish the following:
  - Connect via VPN to Workinet NAP DR Site
  - Map to Network Drives
  - Connect to Apps that are recovered at Workinet (Apps Names)
  - Users were to validate they can reach and use their files and apps
- <SAMPLE CLIENT> users used Outlook OWA (production email is hosted with Workinet) or called into the virtual conference room to communicate any issues to the team. (Exchange was not in scope as part of this test since it is hosted with Workinet)

Logistics

The test logistics and participants are listed below.

Recovery Test Date:	DATE – Target Recovery of 24 hours			
Recovery Test Location(s):	Workinet Data Center – Intel VM servers and Data Network			
Command Center:	Workinet Data Center Conference Room Conference Bridge Open During Test			800-XXX-XXXX Code = XXXXXXX
<SAMPLE CLIENT> Testing Participants:	Participant Name	Participant Location	Focus Area	Mobile Contact Information
	IT Director	<SAMPLE CLIENT>	IT / Network	XXX-XXX-XXX
	User 1	Remote	Application 1	
	User 2	Remote	Application 2	
	User 3	Remote	Application 3	
	User 4	Remote	Application 4	
	User 5	Remote	Application 5	
Workinet Testing Participants:	Participant Name	Participant Location	Focus Area	Mobile Contact Information
	Workinet Engineer 1	Workinet	Server/Data Restore	XXX-XXX-XXXX
	Workinet PM 1	Workinet	Command Center	XXX-XXX-XXX
	Workinet Engineer 2	Remote	Technical & Management Support	
	Workinet Observer	Remote	Command Center	
	Workinet Engineer 3	Remote	Network Support	

A Critical Piece to Ensure Your Insurance will Not Fight Your Claim – DR Exercise & Recovery Results Achieved Documentation.

Yet Often Overlooked!

Gotchas!

Managed Disaster Recovery as a Service

- Bandwidth constrained environments with a high rate of change are challenging
  - — Will stretch the RPO from seconds to minutes and potentially hours
- SaaS solutions DR capabilities need to be checked and lined up with your RPO and RTO goals
  - — This can increase the SaaS cost
- Complex networks add to the importance of planning and must be paid attention to and accounted for in advance of DR
  - — Actually makes testing more complex and difficult than a “real” disaster

Thank You!

Jason Wankovsky - Mindsight

jwankovsky@gomindsight.com

630.981.5039