IT SECURITY FOR LIBRARIES PART 3: DISASTER RECOVERY

BRIAN PICHMAN | EVOLVE PROJECT
@BPICHMAN ON TWITTER!

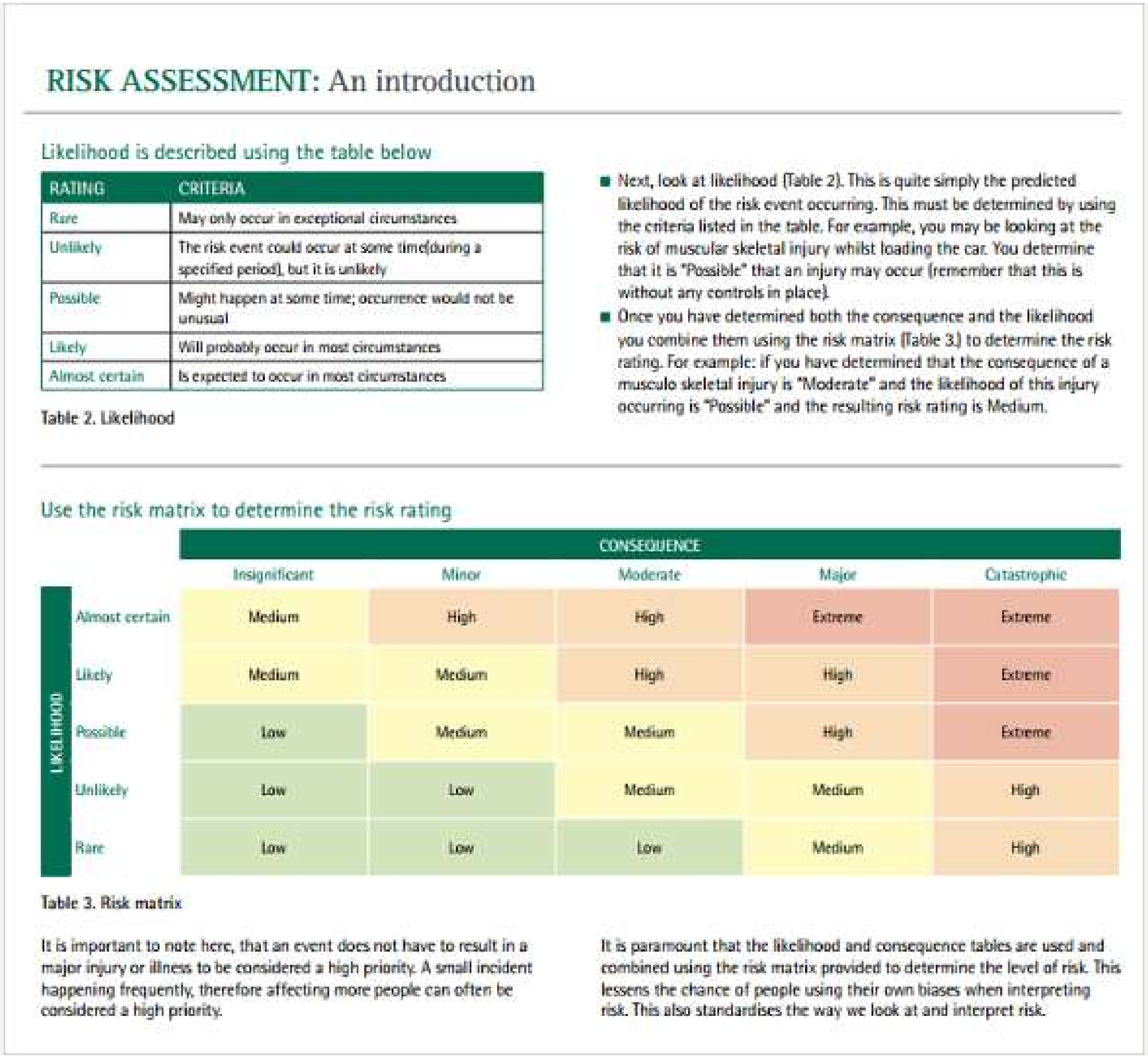
Our Disaster Recovery Plan Goes Something Like This...
HELP! HELP!

IDENTIFYING THREATS

- “Act of God”
  - Tornado, Flood, Fire
- ”Act of Evil”
  - Break-ins, Hacking, Physical Damage,Viruses
- “Act of Error”
  - Accidental Deletions, Hardware Failure, Software Glitches
- Loss of Services (could be caused by above)
  - Internet, Power, Heating/Cooling, Phone, Building Issues

RECOVERABLE RISKS

- Risks with Provided Services:
  - Internet
  - Phone
  - Power
- Risks with Created Data
  - Corruption
  - Loss
- Risk with Owned Systems
  - Errors or Corruption
  - Failure or Loss



RISK ASSESSMENT: An introduction

Likelihood is described using the table below

RATING	CRITERIA
Rare	May only occur in exceptional circumstances
Unlikely	The risk event could occur at some time(during a specified period), but it is unlikely
Possible	Might happen at some time; occurrence would not be unusual
Likely	Will probably occur in most circumstances
Almost certain	Is expected to occur in most circumstances

Table 2. Likelihood

- Next, look at likelihood (Table 2). This is quite simply the predicted likelihood of the risk event occurring. This must be determined by using the criteria listed in the table. For example, you may be looking at the risk of muscular skeletal injury whilst loading the car. You determine that it is "Possible" that an injury may occur (remember that this is without any controls in place).
- Once you have determined both the consequence and the likelihood you combine them using the risk matrix (Table 3.) to determine the risk rating. For example: if you have determined that the consequence of a musculo skeletal injury is "Moderate" and the likelihood of this injury occurring is "Possible" and the resulting risk rating is Medium.

Use the risk matrix to determine the risk rating

		CONSEQUENCE				
		Insignificant	Minor	Moderate	Major	Catastrophic
LIKELIHOOD	Almost certain	Medium	High	High	Extreme	Extreme
	Likely	Medium	Medium	High	High	Extreme
	Possible	Low	Medium	Medium	High	Extreme
	Unlikely	Low	Low	Medium	Medium	High
	Rare	Low	Low	Low	Medium	High

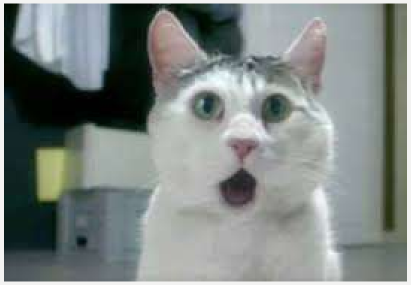
Table 3. Risk matrix

It is important to note here, that an event does not have to result in a major injury or illness to be considered a high priority. A small incident happening frequently, therefore affecting more people can often be considered a high priority.

It is paramount that the likelihood and consequence tables are used and combined using the risk matrix provided to determine the level of risk. This lessens the chance of people using their own biases when interpreting risk. This also standardises the way we look at and interpret risk.

A GOOD RECOVERY PLAN INCLUDES

- Monitoring
  - Systems need to be actively monitored
- Recoverable Backups and Systems
  - Systems need to have data backed up
- Redundancy
  - Systems need to be redundant to mitigate risk of device or service failure, having failover devices and services is important to ensure uptime.
- TESTING
  - I'm going to say this a few times.



"Risks need to be monitored so that management can act promptly if and when the nature, potential impact, or likelihood of the risk goes outside acceptable levels."

Author Norman Marks in "World Class Risk Management" (p. 179)

www.ERMInsightsbyCarol.com

COST OF DOWNTIME

- **RESEARCH HIGHLIGHTS:**
- Data loss and downtime costs enterprises $1.7 trillion[1]
- Companies on average lost 400%[2] more data over the last two years (equivalent to 24 million emails[3] each)
- 71% of IT professionals are not fully confident in their ability to recover information following an incident
- 51% of organizations lack a disaster recovery plan for emerging workloads[4]; just 6% have plans for big data, hybrid cloud and mobile
- Only 2% of organizations are data protection "Leaders"; 11% "Adopters"; 87% are behind the curve
- China, Hong Kong, The Netherlands, Singapore and the US lead protection maturity; Switzerland, Turkey and the UAE lag behind
- Companies with three or more vendors lost three times as much data as those with a single-vendor strategy

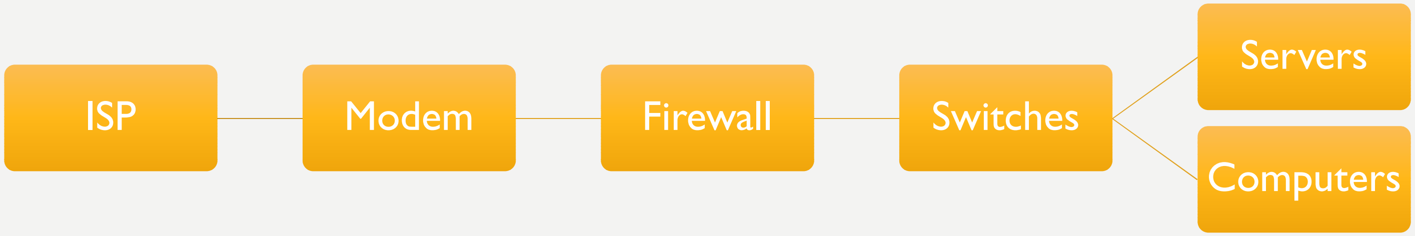
https://www.emc.com/about/news/press/2014/20141202-01.htm

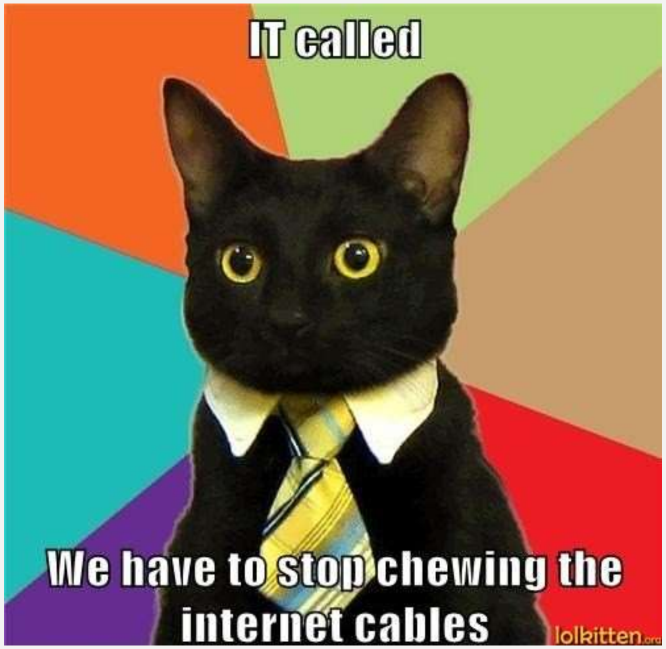
A DISASTER PLAN IS ABOUT

- Ensuring Redundancy and Recovery
- Planning and Preparation:
  - Risk Management
  - Risk Assessment
  - Risk Mitigation
  - Business Continuity
- If a Disaster Occurs:
  - Response
  - Relief
  - Recovery
  - Restoration

SERVICES: INTERNET AND PHONE

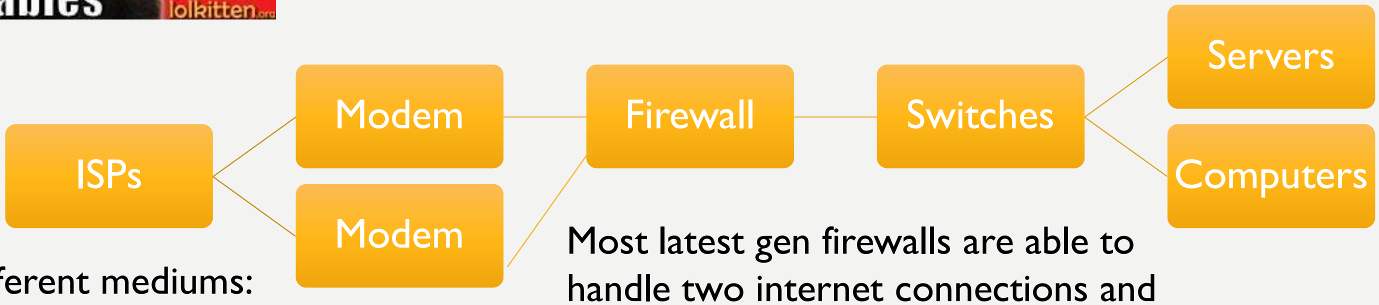
- Internet is a core component for day to day operations
  - Connecting to an ILS
- What makes up your connection to the outside world?
- ISP = Internet Service Provider





Having two different internet connections across two different modems will help mitigate risk of a Service Provider Failure

Other considerations include hardware failure and redundancy. Having a spare firewall (or using two firewalls to load balance) can help mitigate risk.



Usually pick two different mediums:

Cable
Telephone
Satellite
…

Most latest gen firewalls are able to handle two internet connections and “round-robin” and do “failover”

SERVICES: POWER

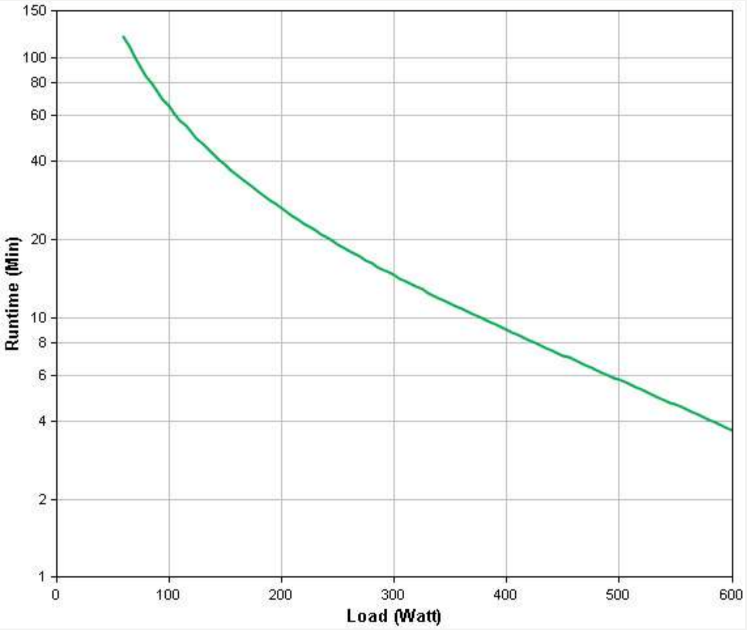
- Having Battery Power Supplies / UPS for your server and network equipment can help ensure uptime
  - Time for Generators to kick on
  - Gives you enough time to power down the machines versus an abrupt power loss.
- Have generators if your business requires you to have power in your building consistently.
  - If you are considered a shelter or a heating place it should be a requirement.

CHOOSING A BATTERY BACKUP-CONSUMPTION

- How much power does your devices consume?
  - You can do the math using server tools that measure consumption of power at peak times.
  - You can also get a watt meter and test average consumption over an extended period of time.
  - Some fancy rack mounted power strips have power consumption built in.

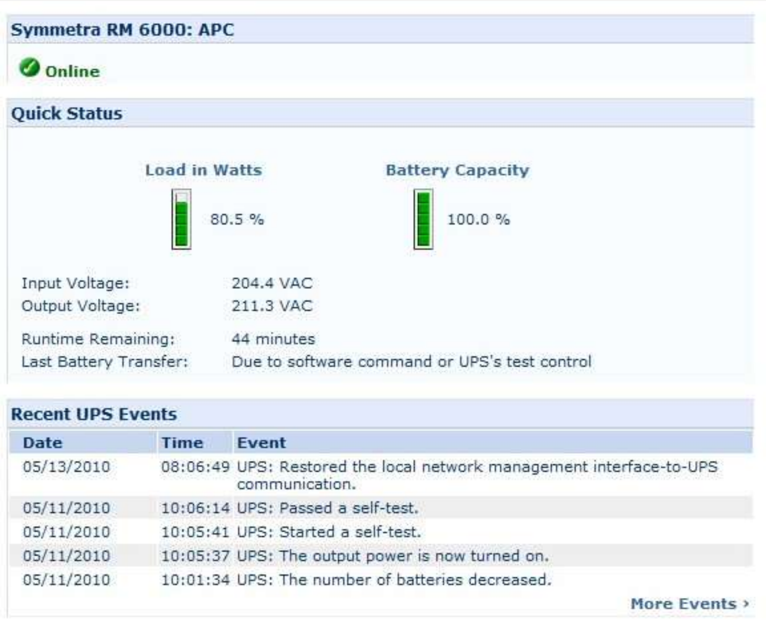
CHOOSING A BATTERY BACKUP-LOAD TIME

- You will want to make sure your UPS can power your network long enough to get what you need to get done (in terms of powering down) or length of time for the generator to kick in.



CHOOSING A BATTERY BACKUP- FEATURES

- Power supplies should be plugged into your network
  - To give you real time reporting of load (so you can add more UPSs if need)
  - To tell you battery health
  - Sending alerts at thresholds
    - Power Failure
    - Over usage
    - Battery is almost drained



Symmetra RM 6000: APC

Online

Quick Status

Input Voltage: 204.4 VAC
Output Voltage: 211.3 VAC

Runtime Remaining: 44 minutes
Last Battery Transfer: Due to software command or UPS's test control

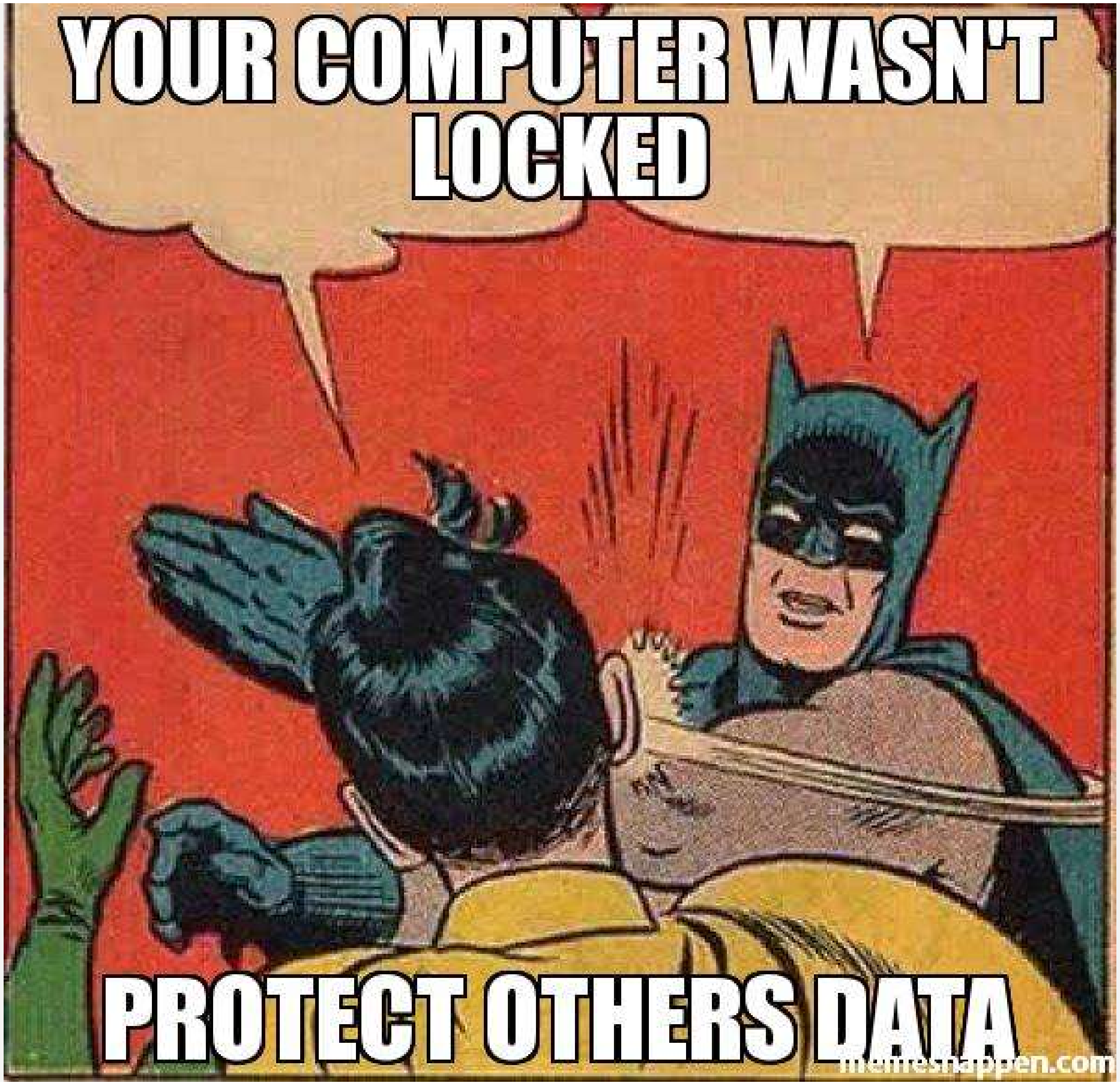
Recent UPS Events

Date	Time	Event
05/13/2010	08:06:49	UPS: Restored the local network management interface-to-UPS communication.
05/11/2010	10:06:14	UPS: Passed a self-test.
05/11/2010	10:05:41	UPS: Started a self-test.
05/11/2010	10:05:37	UPS: The output power is now turned on.
05/11/2010	10:01:34	UPS: The number of batteries decreased.

More Events ›

DATA IS EXPENSIVE

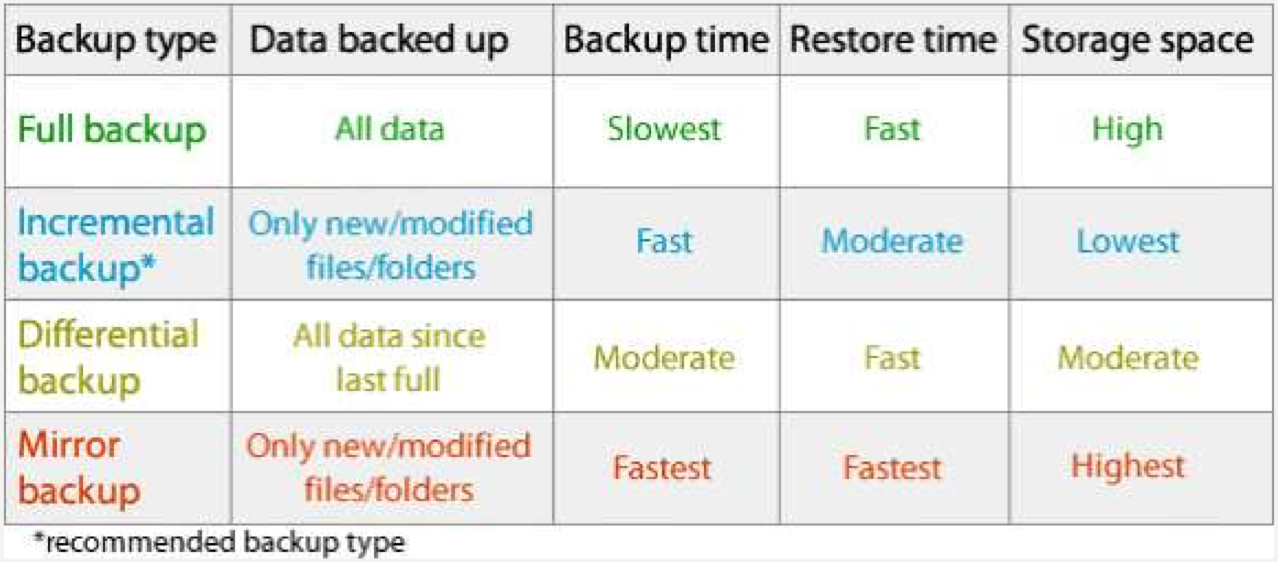
- Financial Records for 7 years
  - SOX (Sarbanes–Oxley Act of 2002)
- Cost of a "data record"
  - On average, the cost of such a record containing healthcare information is $363 (and also employee records are known to be this much if including social information
  - At the end of May 2015, the Ponemon Institute released its annual "Cost of Data Breach Study." Researchers estimated that the average cost of each lost or stolen record containing sensitive and confidential information was $154.
  - Verizon has the concept from a per-record perspective, claiming an average cost of just 58 cents for each lost or stolen file.


YOUR COMPUTER WASN'T LOCKED
PROTECT OTHERS DATA
memeshappen.com

WHAT CAN HAPPEN TO MY DATA?

- It can be corrupted!
  - Someone makes changes to a file. Accidental deletion, purposeful manipulation, script goes rouge.
  - Can impact system performance
- It can be lost!
  - Server goes down, disappears, etc.
  - Spreadsheets, employee files, payroll, flyers, data about events
  - Website Data, Catalog Data, Hosted Applications…gone!
  - Email!
- Hardware failure

WAYS TO BACK UP



Backup type	Data backed up	Backup time	Restore time	Storage space
Full backup	All data	Slowest	Fast	High
Incremental backup*	Only new/modified files/folders	Fast	Moderate	Lowest
Differential backup	All data since last full	Moderate	Fast	Moderate
Mirror backup	Only new/modified files/folders	Fastest	Fastest	Highest

*recommended backup type

CALENDAR

- Monthly Full Back Up
- Hourly/Daily Incremental Back Ups
- Weekly Differential

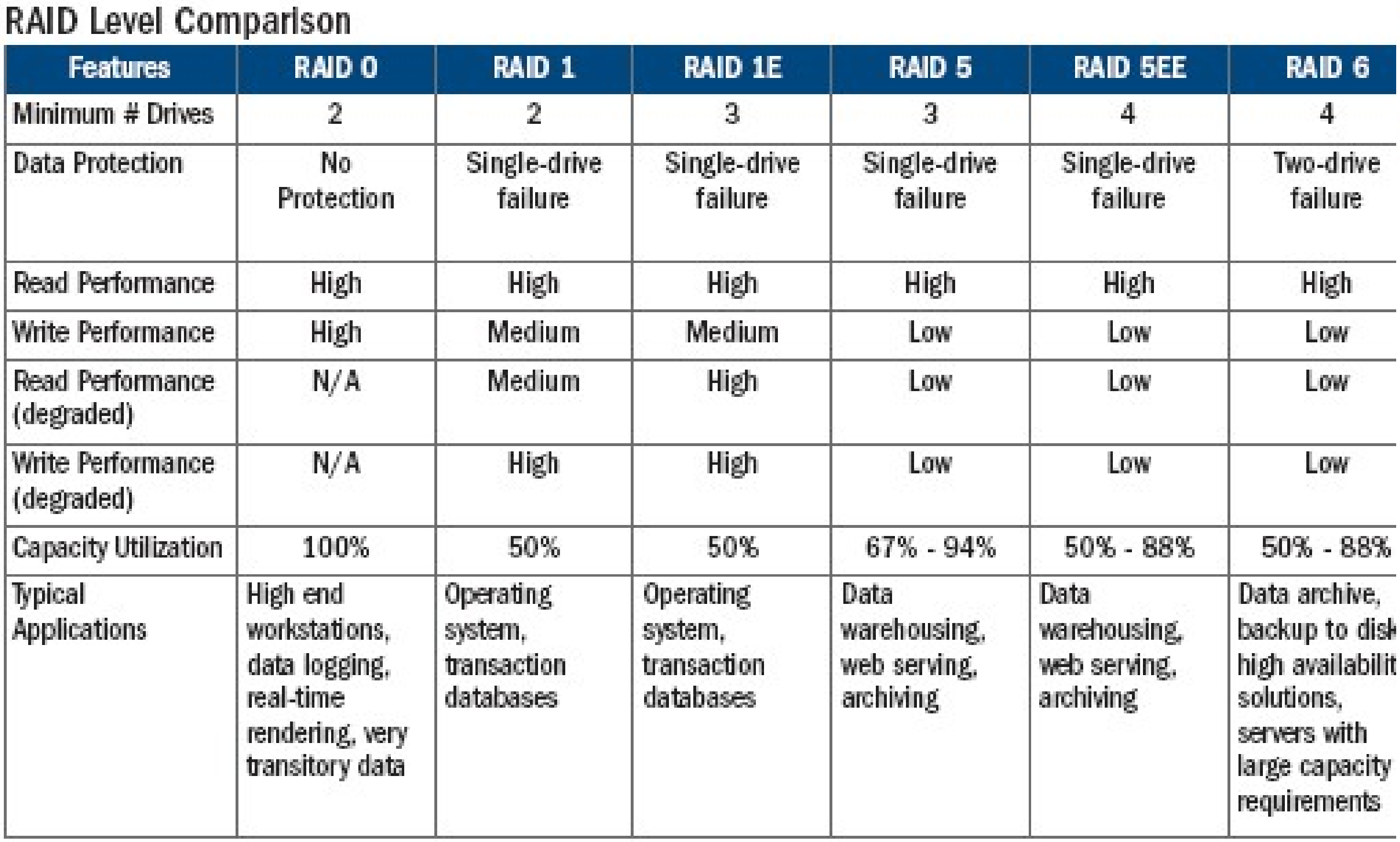
- Back Ups should also be stored off-site.
  - Either Weekly Differentials and/or Monthly Back Ups
  - This fixes the "what if the place was taken out a storm"

BACK UP MEDIUMS

Outdated Media:
USB Flash Drives
Optical Disks

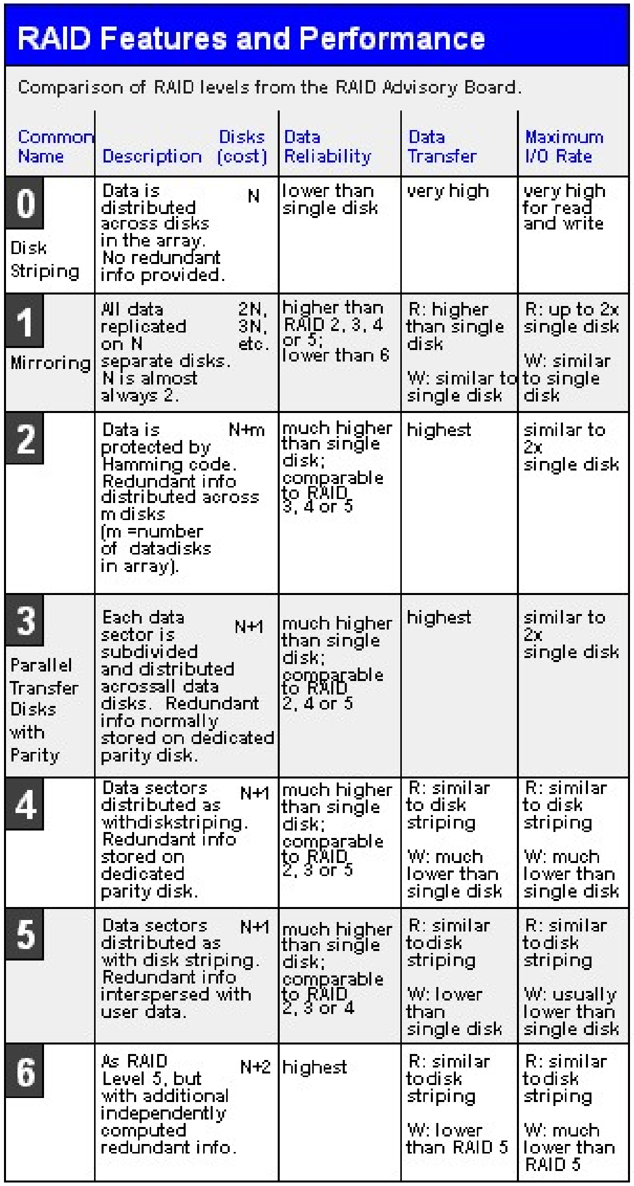
Type	Pros	Cons
External Drives*	Inexpensive Fastest media for backups Easily portable Readable on variety of computers	More fragile than other media Ruggedized versions available (pricey) May require special power supply
NAS (Network Area Storage)*	Backups are more automated and controlled. More Security. Can be remotely monitored with ease.	Can be more expensive depending on automation. Requires setup and network configurations. Bandwidth May require the NAS OS to read if NAS Hardware Failure
Tape Drives	Inexpensive Durable Easily portable Reliable	Expensive Compatibility issues May require additional software SLOW
Cloud	Off Premise by another group.	Expensive and less control of your "data"

*Solid State Drives would be more expensive but less risk of hardware failure (no mechanical parts)



RAID Level Comparison

Features	RAID 0	RAID 1	RAID 1E	RAID 5	RAID 5EE	RAID 6
Minimum # Drives	2	2	3	3	4	4
Data Protection	No Protection	Single-drive failure	Single-drive failure	Single-drive failure	Single-drive failure	Two-drive failure
Read Performance	High	High	High	High	High	High
Write Performance	High	Medium	Medium	Low	Low	Low
Read Performance (degraded)	N/A	Medium	High	Low	Low	Low
Write Performance (degraded)	N/A	High	High	Low	Low	Low
Capacity Utilization	100%	50%	50%	67% - 94%	50% - 88%	50% - 88%
Typical Applications	High end workstations, data logging, real-time rendering, very transitory data	Operating system, transaction databases	Operating system, transaction databases	Data warehousing, web serving, archiving	Data warehousing, web serving, archiving	Data archive, backup to disk high availabilit solutions, servers with large capacity requirements



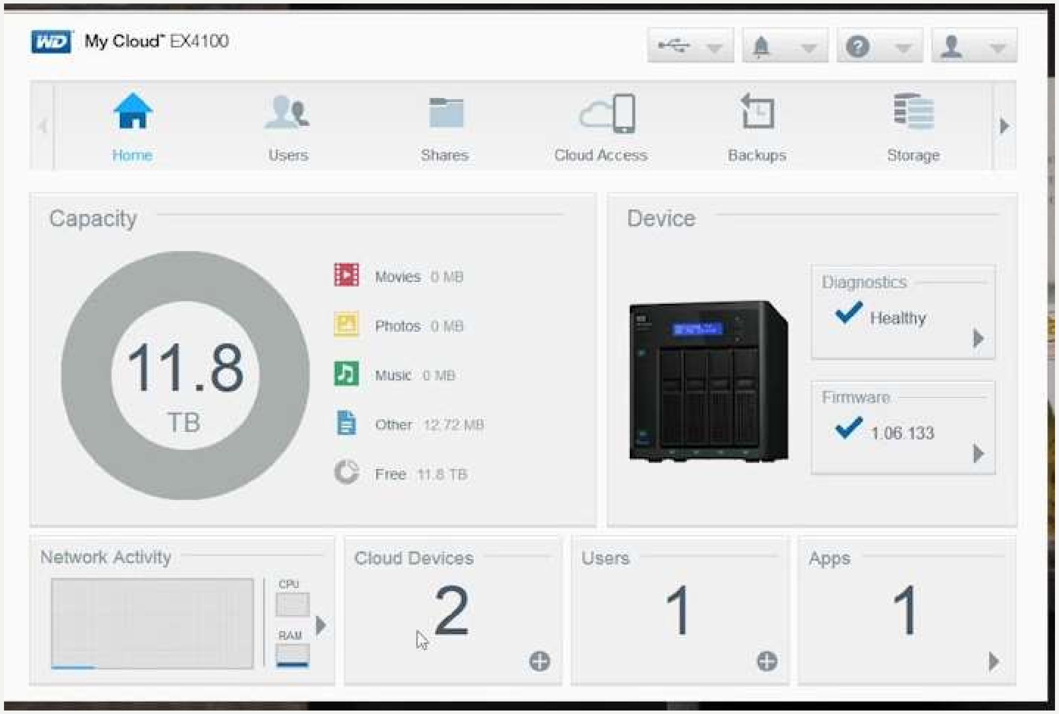
RAID Features and Performance

Comparison of RAID levels from the RAID Advisory Board.

Common Name	Description	Disks (cost)	Data Reliability	Data Transfer	Maximum I/O Rate
0 Disk Striping	Data is distributed across disks in the array. No redundant info provided.	N	lower than single disk	very high	very high for read and write
1 Mirroring	All data replicated on N separate disks. N is almost always 2.	2N, 3N, etc.	higher than RAID 2, 3, 4 or 5; lower than 6	R: higher than single disk W: similar to single disk	R: up to 2x single disk W: similar to single disk
2	Data is protected by Hamming code. Redundant info distributed across m disks (m =number of datadisks in array).	N+m	much higher than single disk; comparable to RAID 3, 4 or 5	highest	similar to 2x single disk
3 Parallel Transfer Disks with Parity	Each data sector is subdivided and distributed acrossall data disks. Redundant info normally stored on dedicated parity disk.	N+1	much higher than single disk; comparable to RAID 2, 4 or 5	highest	similar to 2x single disk
4	Data sectors distributed as withdiskstriping. Redundant info stored on dedicated parity disk.	N+1	much higher than single disk; comparable to RAID 2, 3 or 5	R: similar to disk striping W: much lower than single disk	R: similar to disk striping W: much lower than single disk
5	Data sectors distributed as with disk striping. Redundant info interspersed with user data.	N+1	much higher than single disk; comparable to RAID 2, 3 or 4	R: similar todisk striping W: lower than single disk	R: similar todisk striping W: usually lower than single disk
6	As RAID Level 5, but with additional independently computed redundant info.	N+2	highest	R: similar todisk striping W: lower than RAID 5	R: similar todisk striping W: much lower than RAID 5

DEVICES!

- "Personal Cloud Storage" devices
  - Western Digital EX series



Capacity

11.8 TB

Movies 0 MB

Photos 0 MB

Music 0 MB

Other 12.72 MB

Free 11.8 TB

Device

Diagnostics ✓ Healthy

Firmware ✓ 1.06.133

Network Activity

CPU

RAM

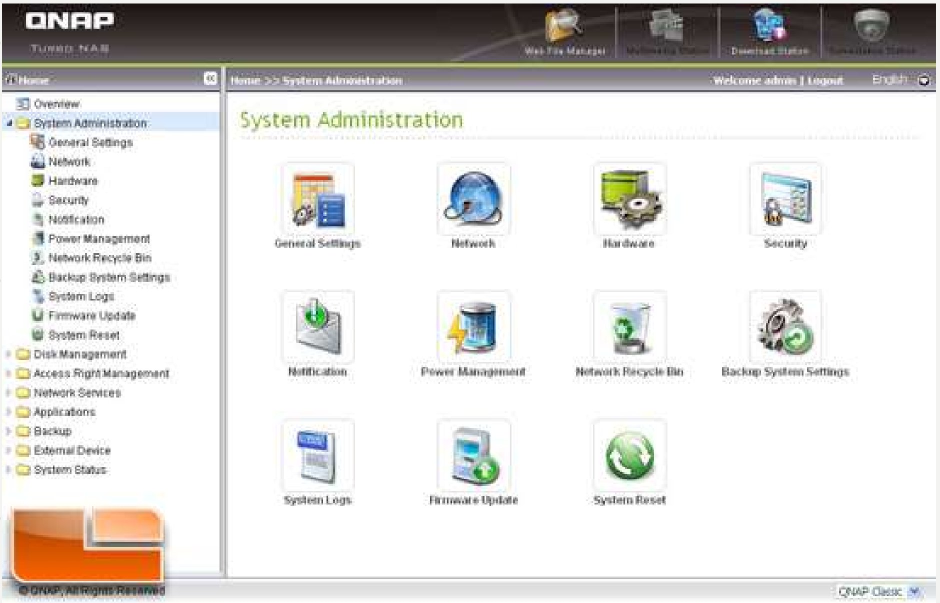
Cloud Devices 2

Users 1

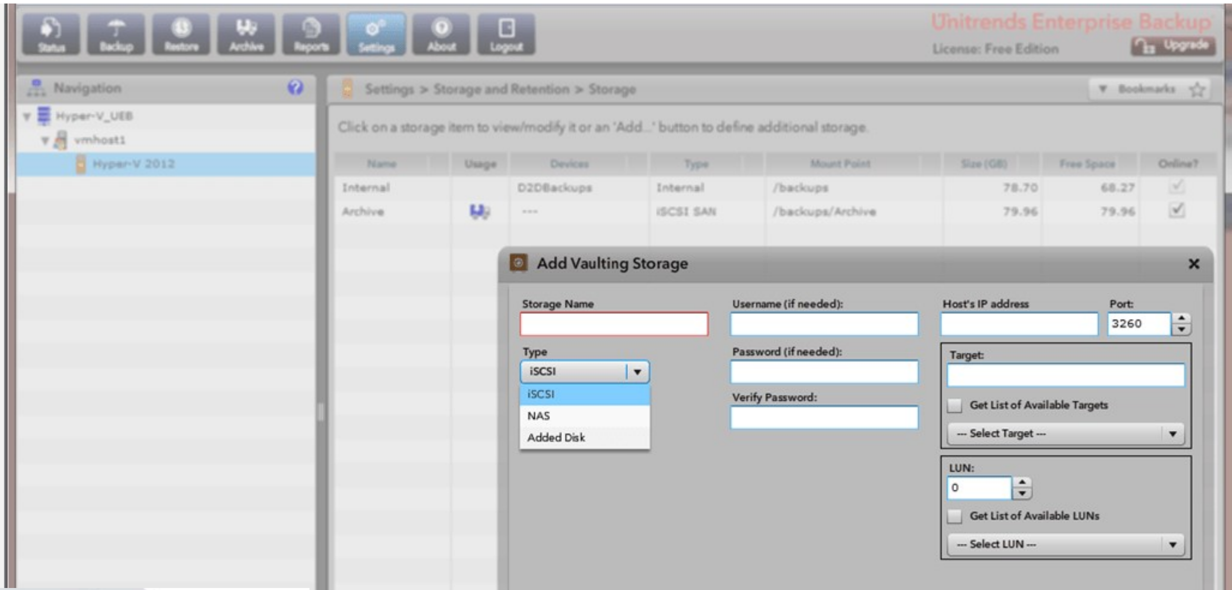
Apps 1

DEVICES!

- “Personal Cloud Storage” devices
  - QNAP



DEVICES!



License: Free Edition

Settings > Storage and Retention > Storage

Click on a storage item to view/modify it or an 'Add...' button to define additional storage.

Name	Usage	Devices	Type	Mount Point	Size (GB)	Free Space	Online?
Internal		D2DBackups	Internal	/backups	78.70	68.27	✓
Archive		---	iSCSI SAN	/backups/Archive	79.96	79.96	✓

Add Vaulting Storage

Storage Name

Type: iSCSI

Username (if needed):

Password (if needed):

Verify Password:

Host's IP address

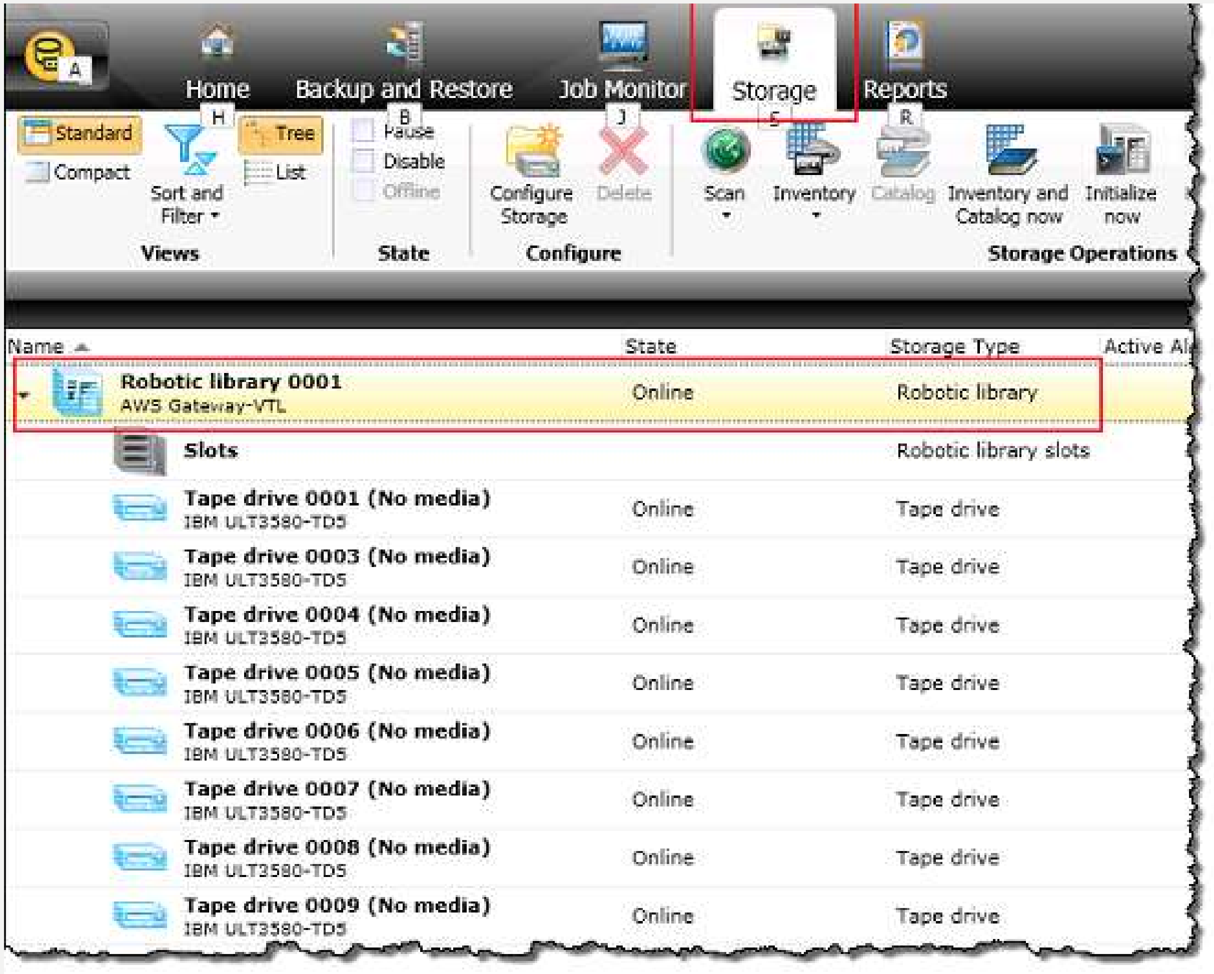
Port: 3260

Target:

LUN: 0

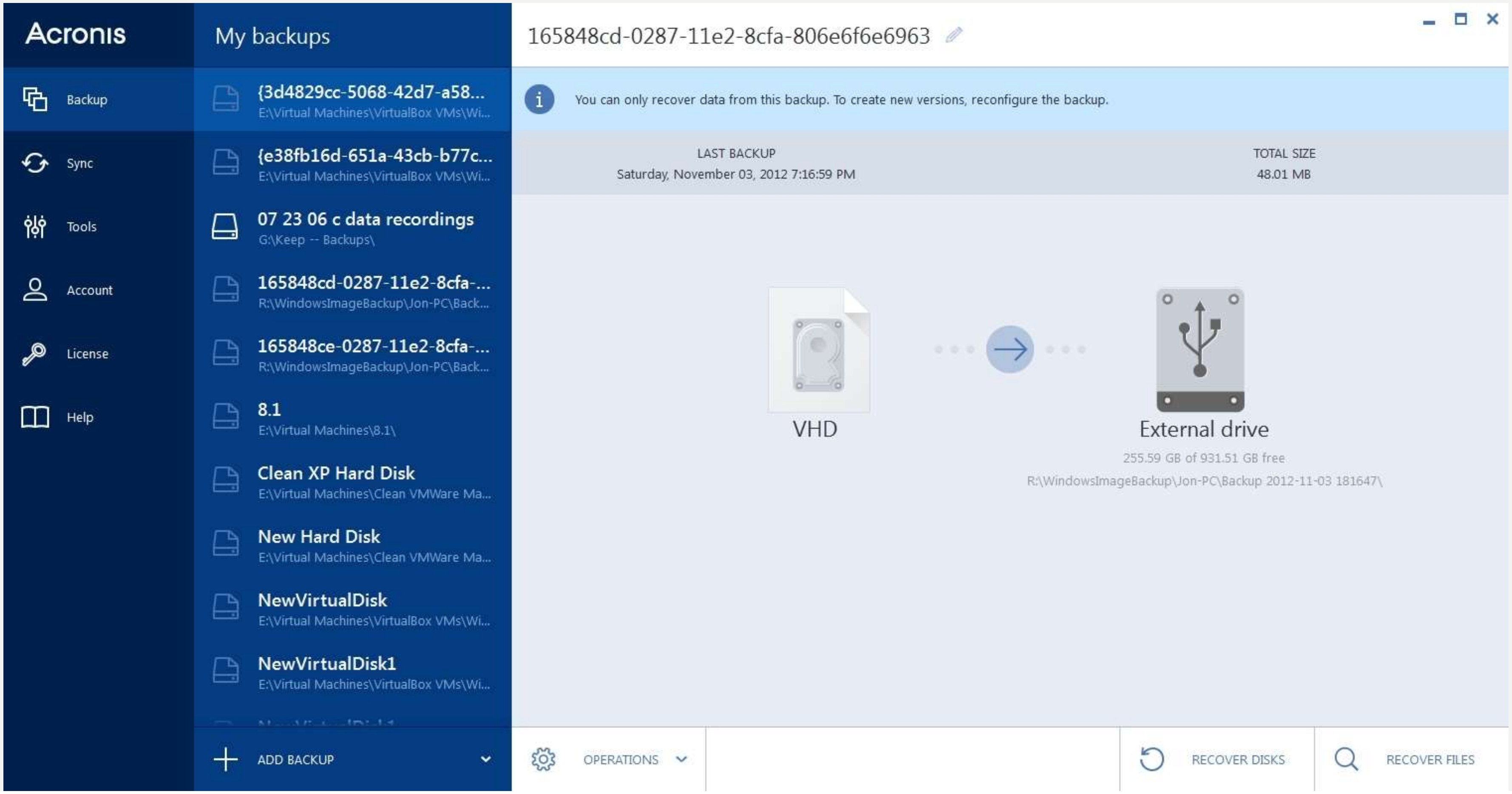
- Unitrends
  – Enterprise Level Back Up

SYMANTEC BACKUP EXEC



Name	State	Storage Type	Active Al
Robotic library 0001 AWS Gateway-VTL	Online	Robotic library	
Slots		Robotic library slots	
Tape drive 0001 (No media) IBM ULT3580-TD5	Online	Tape drive	
Tape drive 0003 (No media) IBM ULT3580-TD5	Online	Tape drive	
Tape drive 0004 (No media) IBM ULT3580-TD5	Online	Tape drive	
Tape drive 0005 (No media) IBM ULT3580-TD5	Online	Tape drive	
Tape drive 0006 (No media) IBM ULT3580-TD5	Online	Tape drive	
Tape drive 0007 (No media) IBM ULT3580-TD5	Online	Tape drive	
Tape drive 0008 (No media) IBM ULT3580-TD5	Online	Tape drive	
Tape drive 0009 (No media) IBM ULT3580-TD5	Online	Tape drive	

ACRONIS BACK UP



165848cd-0287-11e2-8cfa-806e6f6e6963

{3d4829cc-5068-42d7-a58...
E:\Virtual Machines\VirtualBox VMs\Wi...

{e38fb16d-651a-43cb-b77c...
E:\Virtual Machines\VirtualBox VMs\Wi...

07 23 06 c data recordings
G:\Keep -- Backups\

165848cd-0287-11e2-8cfa-...
R:\WindowsImageBackup\Jon-PC\Back...

165848ce-0287-11e2-8cfa-...
R:\WindowsImageBackup\Jon-PC\Back...

8.1
E:\Virtual Machines\8.1\

Clean XP Hard Disk
E:\Virtual Machines\Clean VMWare Ma...

New Hard Disk
E:\Virtual Machines\Clean VMWare Ma...

NewVirtualDisk
E:\Virtual Machines\VirtualBox VMs\Wi...

NewVirtualDisk1
E:\Virtual Machines\VirtualBox VMs\Wi...

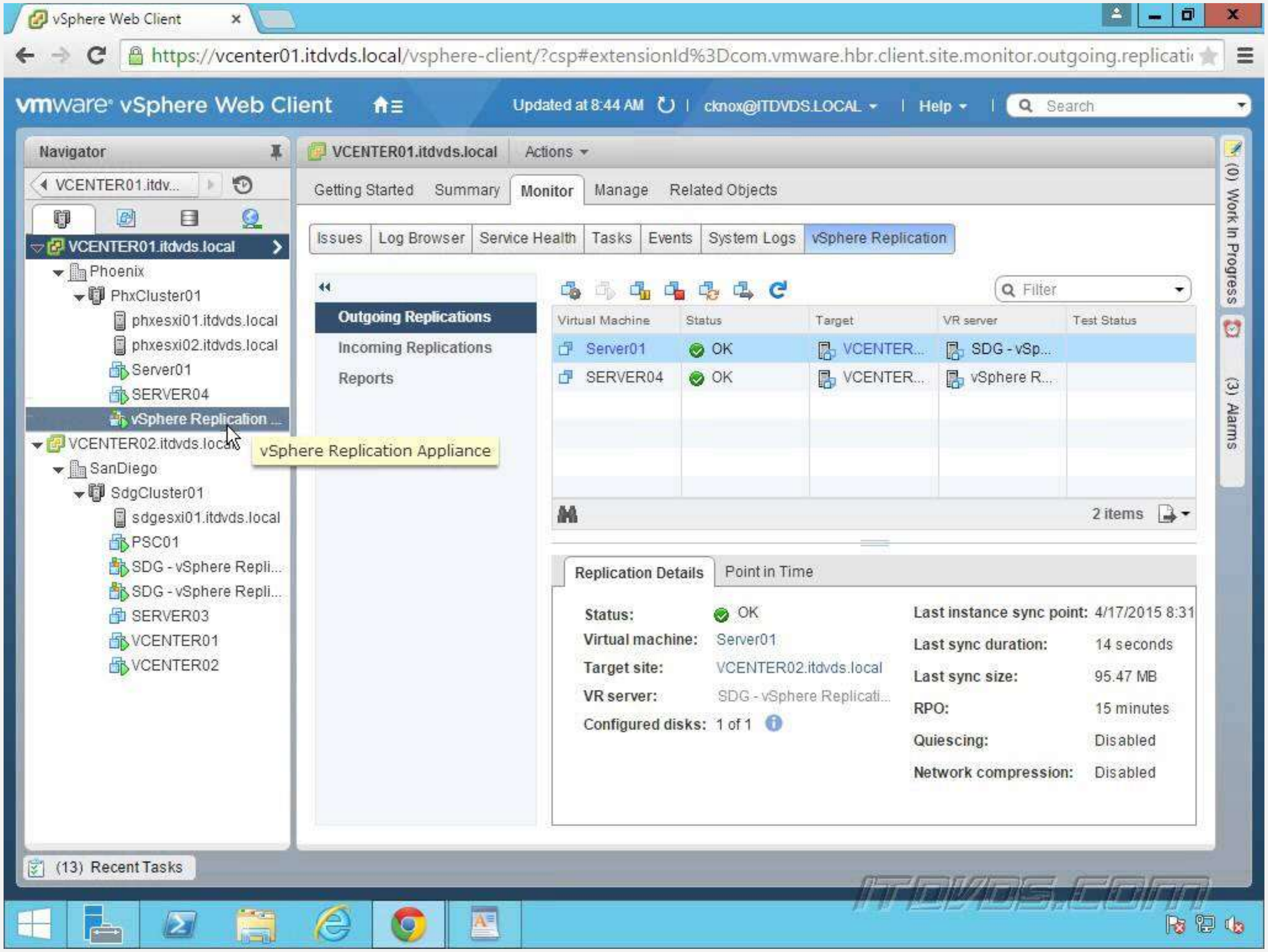
You can only recover data from this backup. To create new versions, reconfigure the backup.

LAST BACKUP	TOTAL SIZE
Saturday, November 03, 2012 7:16:59 PM	48.01 MB

255.59 GB of 931.51 GB free
R:\WindowsImageBackup\Jon-PC\Backup 2012-11-03 181647\

REPLICATION

- You can also replicate your servers (with all of its data) to multiple locations.
  - This isn’t the best for protecting of “corrupted” data
    - IE Crypto Locker
  - However this offers redundancy!
- Replication is running the exact same server environment on different:
  - Hardware (preferred)
  - VM (less preferred)



Virtual Machine	Status	Target	VR server	Test Status
Server01	OK	VCENTER...	SDG - vSp...	
SERVER04	OK	VCENTER...	vSphere R...	

Status: OK

Virtual machine: Server01

Target site: VCENTER02.itdvds.local

VR server: SDG - vSphere Replicati...

Configured disks: 1 of 1

Last instance sync point: 4/17/2015 8:31

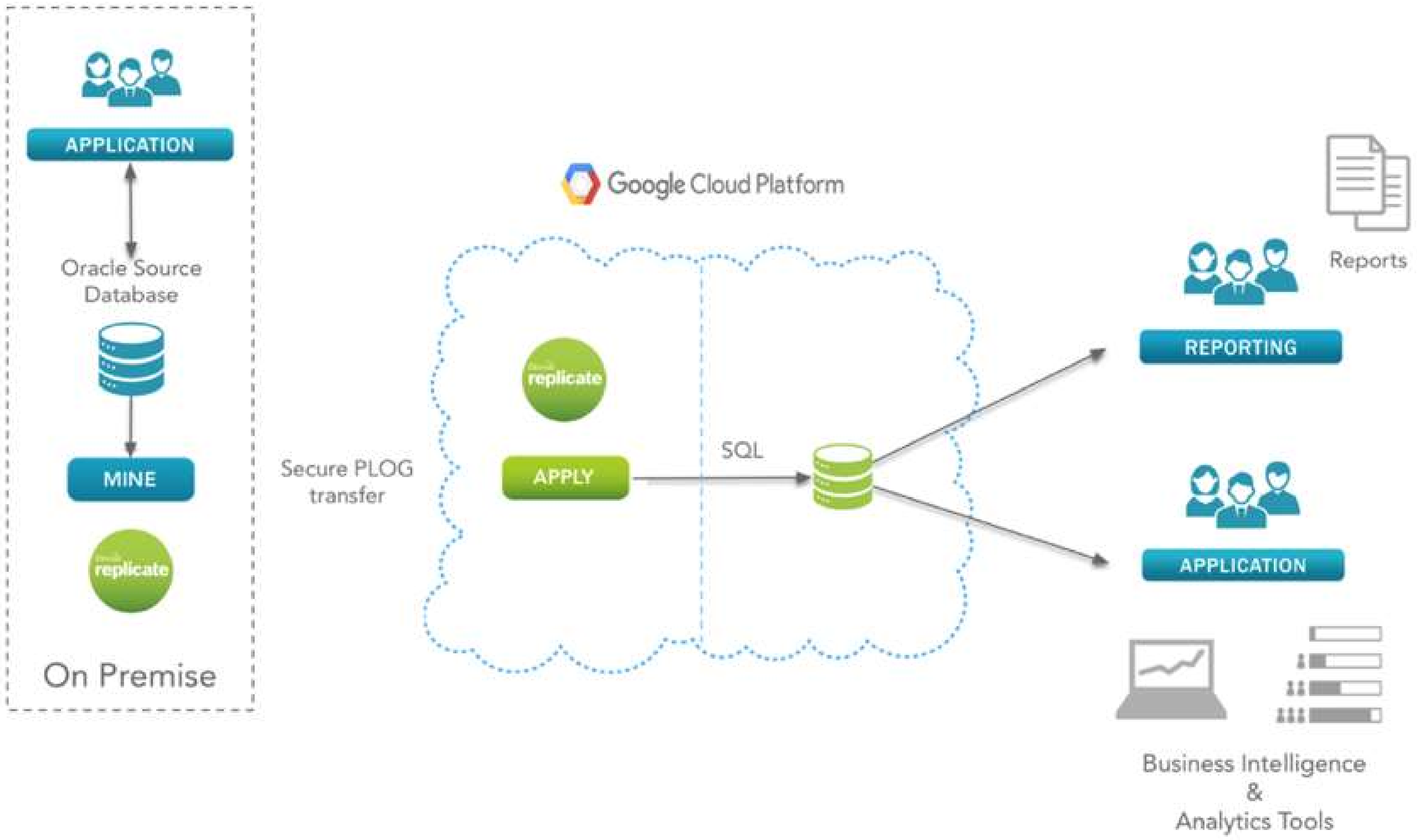
Last sync duration: 14 seconds

Last sync size: 95.47 MB

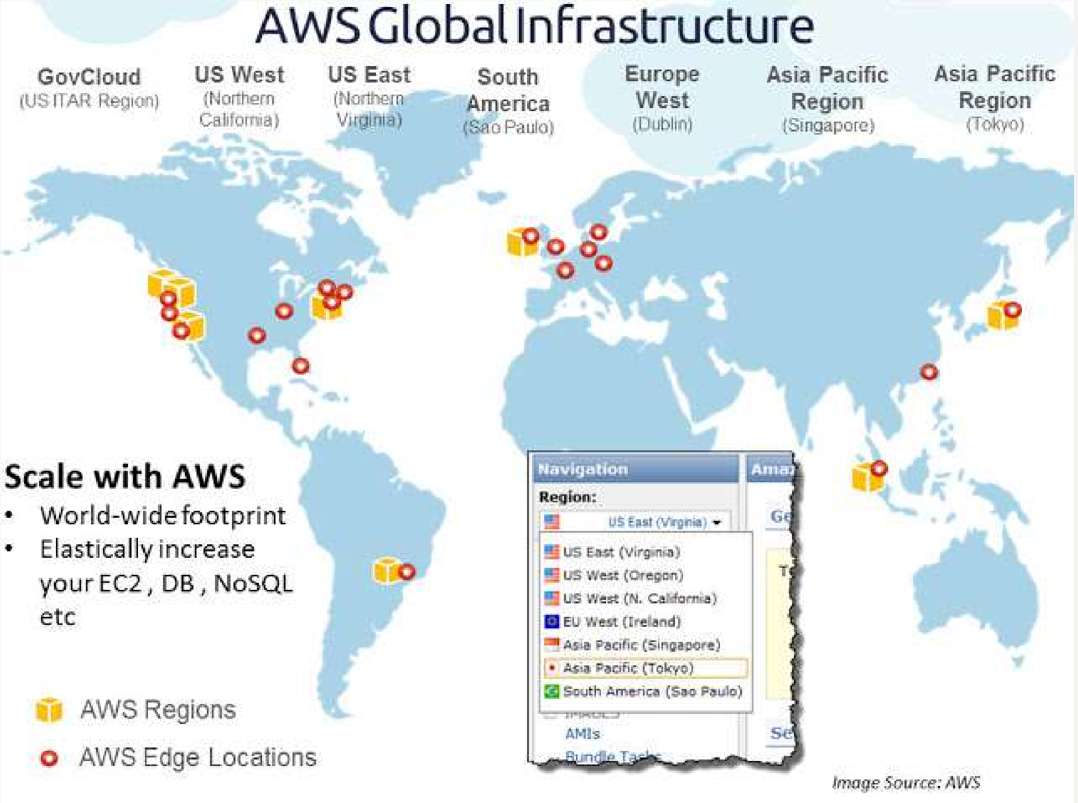
RPO: 15 minutes

Quiescing: Disabled

Network compression: Disabled



https://cloud.google.com/sql/docs/mysql/replication/



AWS Global Infrastructure

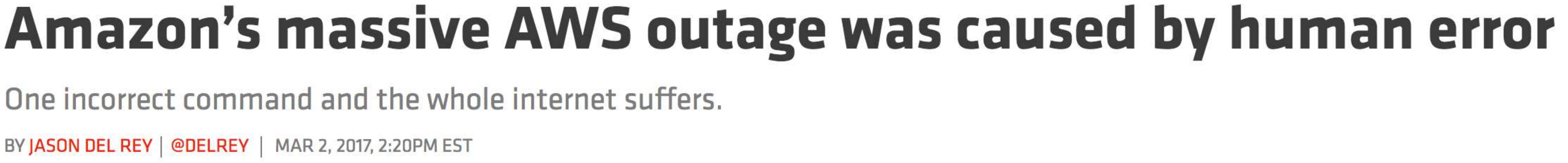
Scale with AWS

- World-wide footprint
- Elastically increase your EC2 , DB , NoSQL etc

🟨 AWS Regions

○ AWS Edge Locations

Image Source: AWS



Amazon’s massive AWS outage was caused by human error

One incorrect command and the whole internet suffers.

BY JASON DEL REY | @DELREY | MAR 2, 2017, 2:20PM EST

http://www.recode.net/2017/3/2/14792636/amazon-aws-internet-outage-cause-human-error-incorrect-command

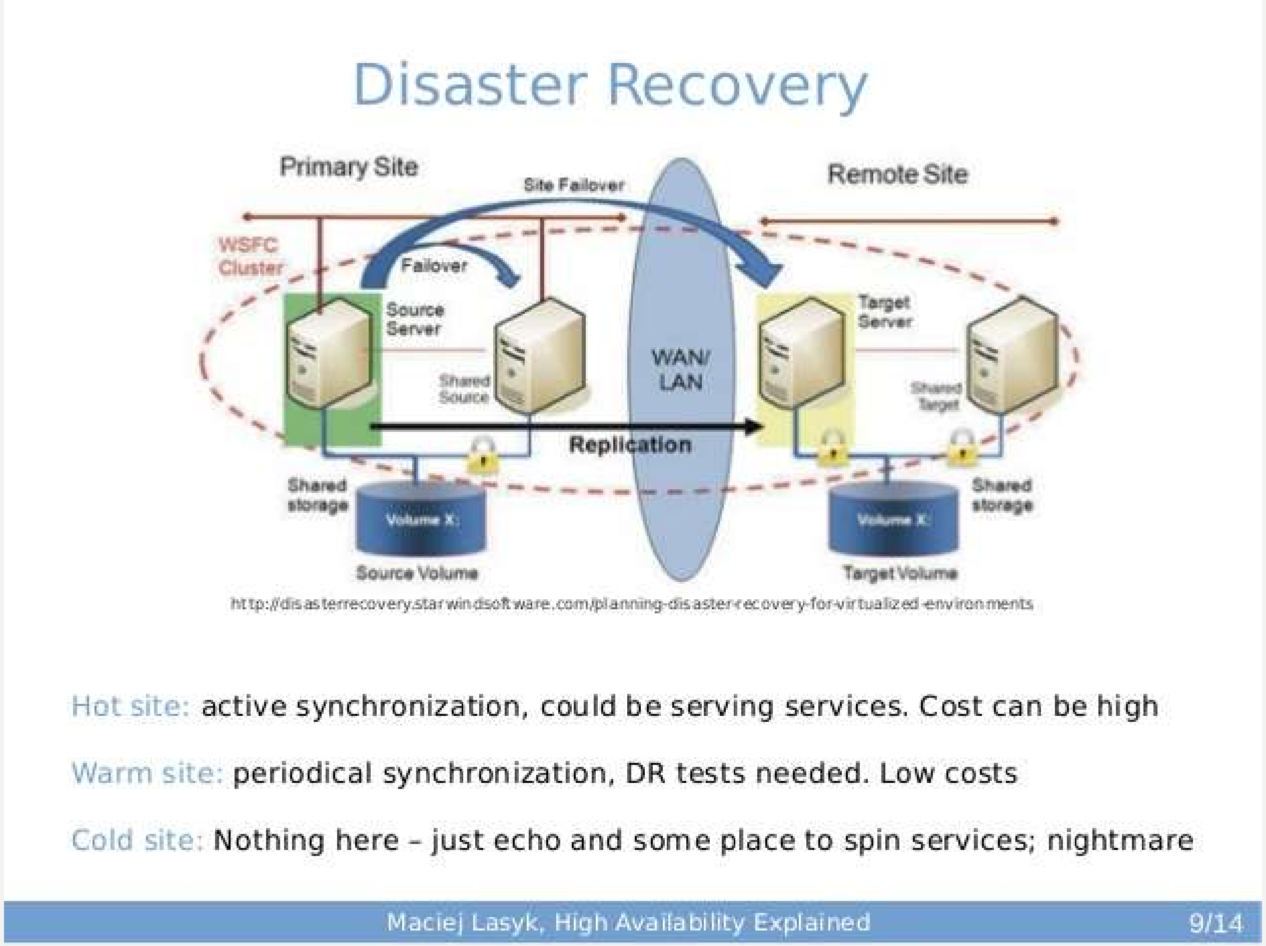
DATA CENTERS

- Host your environment in someone else's data center
  - Latisys
  - RackSpace
- You rely on them to provide redundancy and security
  - However, if your network is down, you have no way to connect to the data center.

APPLICATION HOSTING AND BACK UP

- Two Layers
  - Server Front End: Runs the "pretty" stuff like windows, graphics, and public facing display.
  - Server Back End: Usually a "database".
- It is harder to replicate databases, so most people will replicate front ends (for load balancing) and back up the databases.

HIGH AVAILABILITY



Disaster Recovery

http://disasterrecovery.starwindsoftware.com/planning-disaster-recovery-for-virtualized-environments

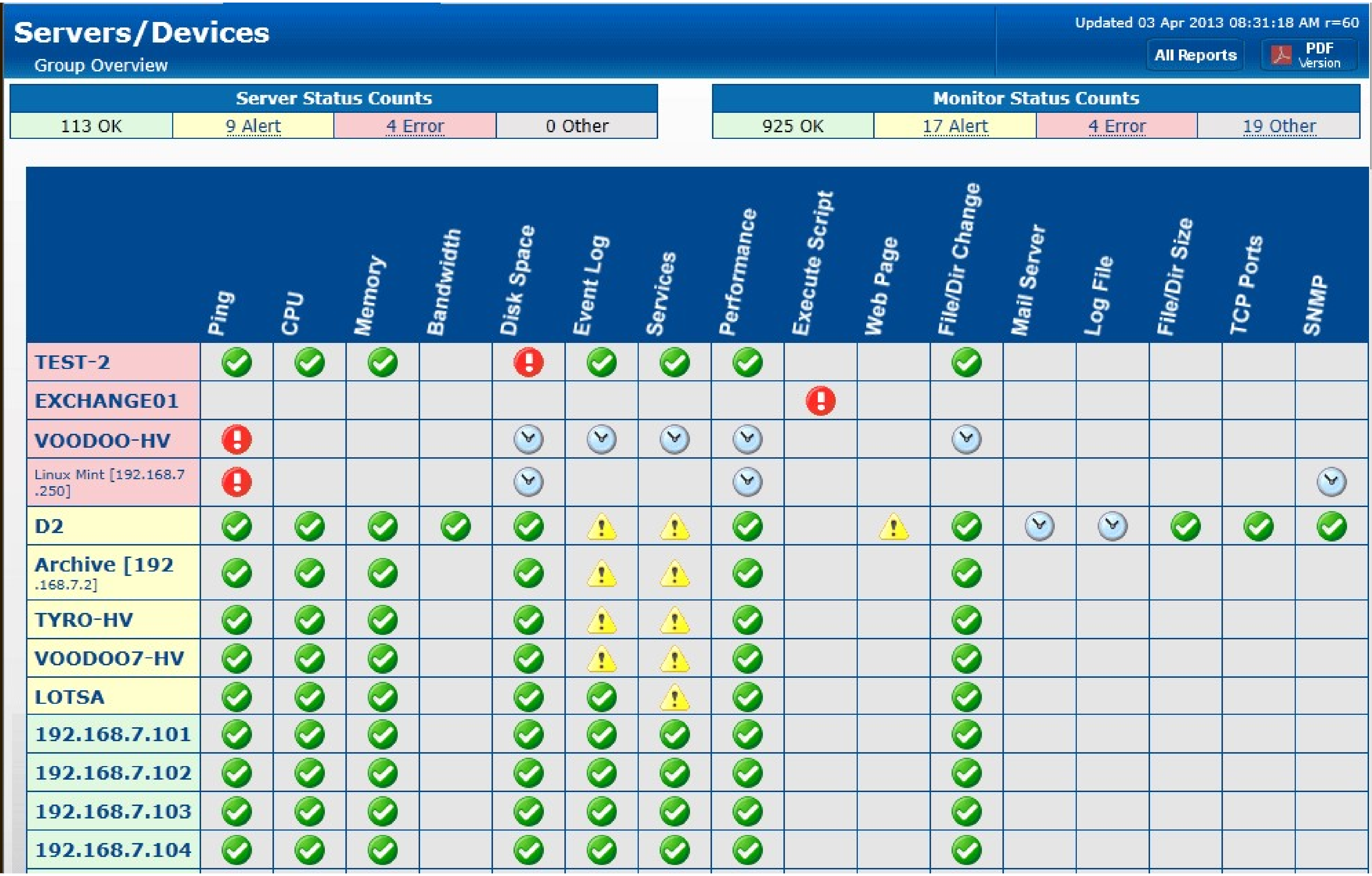
Hot site: active synchronization, could be serving services. Cost can be high

Warm site: periodical synchronization, DR tests needed. Low costs

Cold site: Nothing here – just echo and some place to spin services; nightmare

MONITORING IS IMPORTANT

- Monitor your servers to prevent issues before they happen. Things to monitor for:
  - Network Drops (means it can be device failure or network issue)
  - Temperature of Devices (prevent overheating)
  - Server Processes (if a server is running to high for too long something could be wrong)
  - Storage Space (running out of space can corrupt an entire system)
  - Memory Usage
  - Database Errors



Servers/Devices

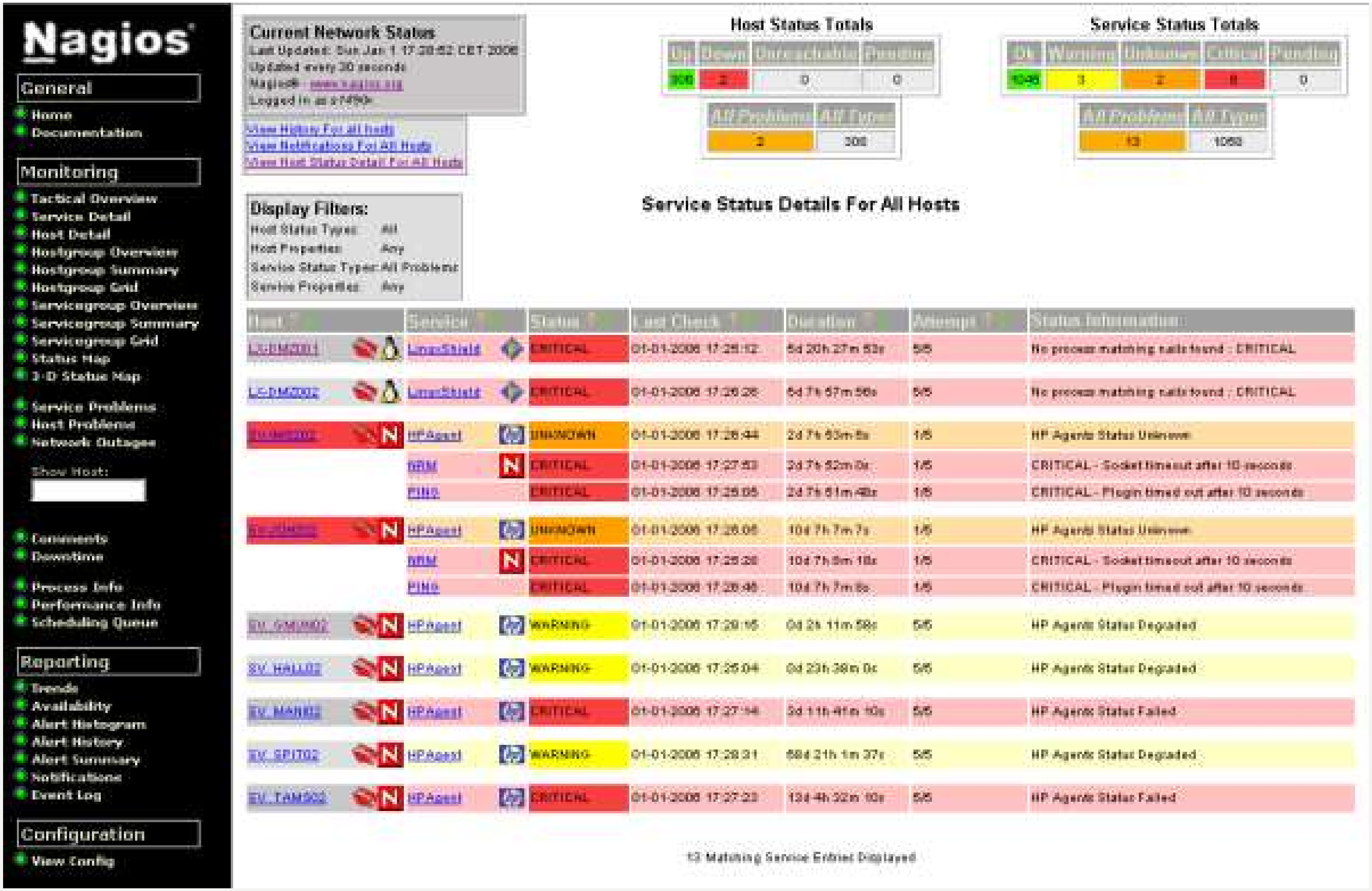
Group Overview

Updated 03 Apr 2013 08:31:18 AM r=60

Server Status Counts			
113 OK	9 Alert	4 Error	0 Other

Monitor Status Counts			
925 OK	17 Alert	4 Error	19 Other

	Ping	CPU	Memory	Bandwidth	Disk Space	Event Log	Services	Performance	Execute Script	Web Page	File/Dir Change	Mail Server	Log File	File/Dir Size	TCP Ports	SNMP
TEST-2	✓	✓	✓		❗	✓	✓	✓			✓					
EXCHANGE01									❗							
VOODOO-HV	❗				🕒	🕒	🕒	🕒			🕒					
Linux Mint [192.168.7.250]	❗				🕒			🕒								🕒
D2	✓	✓	✓	✓	✓	⚠	⚠	✓		⚠	✓	🕒	🕒	✓	✓	✓
Archive [192.168.7.2]	✓	✓	✓		✓	⚠	⚠	✓			✓					
TYRO-HV	✓	✓	✓		✓	⚠	⚠	✓			✓					
VOODOO7-HV	✓	✓	✓		✓	⚠	⚠	✓			✓					
LOTSA	✓	✓	✓		✓	✓	⚠	✓			✓					
192.168.7.101	✓	✓	✓		✓	✓	✓	✓			✓					
192.168.7.102	✓	✓	✓		✓	✓	✓	✓			✓					
192.168.7.103	✓	✓	✓		✓	✓	✓	✓			✓					
192.168.7.104	✓	✓	✓		✓	✓	✓	✓			✓					



General
- Home
- Documentation

Monitoring
- Tactical Overview
- Service Detail
- Host Detail
- Hostgroup Overview
- Hostgroup Summary
- Hostgroup Grid
- Servicegroup Overview
- Servicegroup Summary
- Servicegroup Grid
- Status Map
- 3-D Status Map
- Service Problems
- Host Problems
- Network Outages

Show Host:

- Comments
- Downtime
- Process Info
- Performance Info
- Scheduling Queue

Reporting
- Trends
- Availability
- Alert Histogram
- Alert History
- Alert Summary
- Notifications
- Event Log

Configuration
- View Config

Current Network Status
Last Updated: Sun Jan 1 17:28:52 CET 2006
Updated every 30 seconds
Nagios® - www.nagios.org
Logged in as s74[illegible]

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
300	2	0	0

All Problems	All Types
2	300

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
1046	3	2	8	0

All Problems	All Types
13	1060

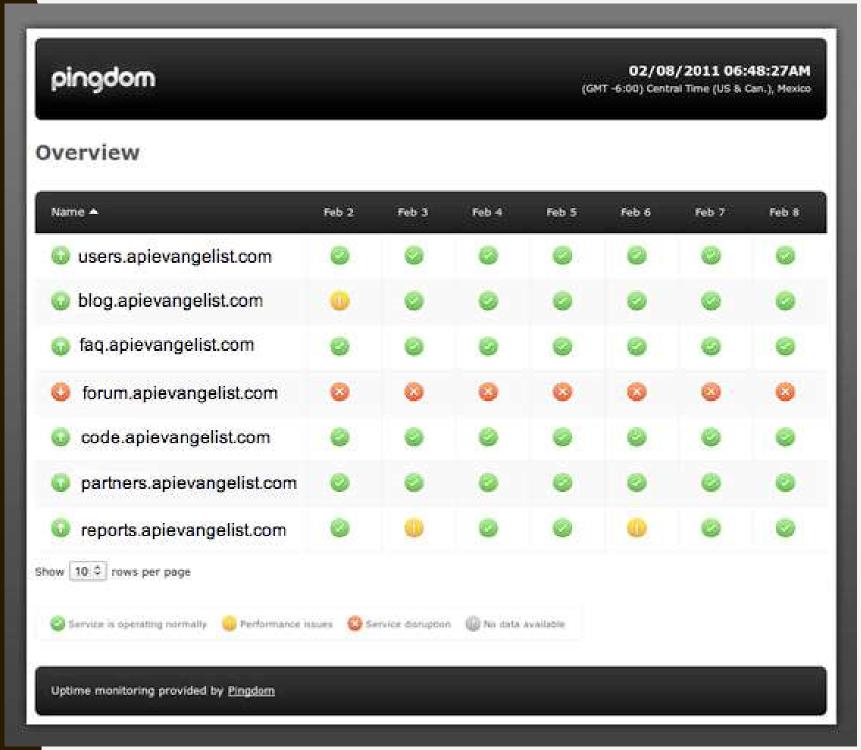
Display Filters:
Host Status Types: All
Host Properties: Any
Service Status Types: All Problems
Service Properties: Any

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
LX-DMZ001	LinuxShield	CRITICAL	01-01-2006 17:25:12	5d 20h 27m 53s	5/5	No process matching nails found : CRITICAL
LX-DMZ002	LinuxShield	CRITICAL	01-01-2006 17:26:26	5d 7h 57m 56s	5/5	No process matching nails found : CRITICAL
[illegible]	HPAgent	UNKNOWN	01-01-2006 17:26:44	2d 7h 53m 8s	1/5	HP Agents Status Unknown
	NRM	CRITICAL	01-01-2006 17:27:53	2d 7h 52m 0s	1/5	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	01-01-2006 17:25:05	2d 7h 51m 48s	1/5	CRITICAL - Plugin timed out after 10 seconds
[illegible]	HPAgent	UNKNOWN	01-01-2006 17:26:05	10d 7h 7m 7s	1/5	HP Agents Status Unknown
	NRM	CRITICAL	01-01-2006 17:25:20	10d 7h 8m 18s	1/5	CRITICAL - Socket timeout after 10 seconds
	PING	CRITICAL	01-01-2006 17:26:46	10d 7h 7m 8s	1/5	CRITICAL - Plugin timed out after 10 seconds
SV_GMUN002	HPAgent	WARNING	01-01-2006 17:20:15	0d 2h 11m 58s	5/5	HP Agents Status Degraded
SV_HALL02	HPAgent	WARNING	01-01-2006 17:25:04	0d 23h 38m 0s	5/5	HP Agents Status Degraded
SV_MAN02	HPAgent	CRITICAL	01-01-2006 17:27:14	3d 11h 41m 10s	5/5	HP Agents Status Failed
SV_SPI702	HPAgent	WARNING	01-01-2006 17:28:31	68d 21h 1m 37s	5/5	HP Agents Status Degraded
SV_TAM002	HPAgent	CRITICAL	01-01-2006 17:27:23	13d 4h 32m 10s	5/5	HP Agents Status Failed

13 Matching Service Entries Displayed

PINGDOM



pingdom

02/08/2011 06:48:27AM
(GMT -6:00) Central Time (US & Can.), Mexico

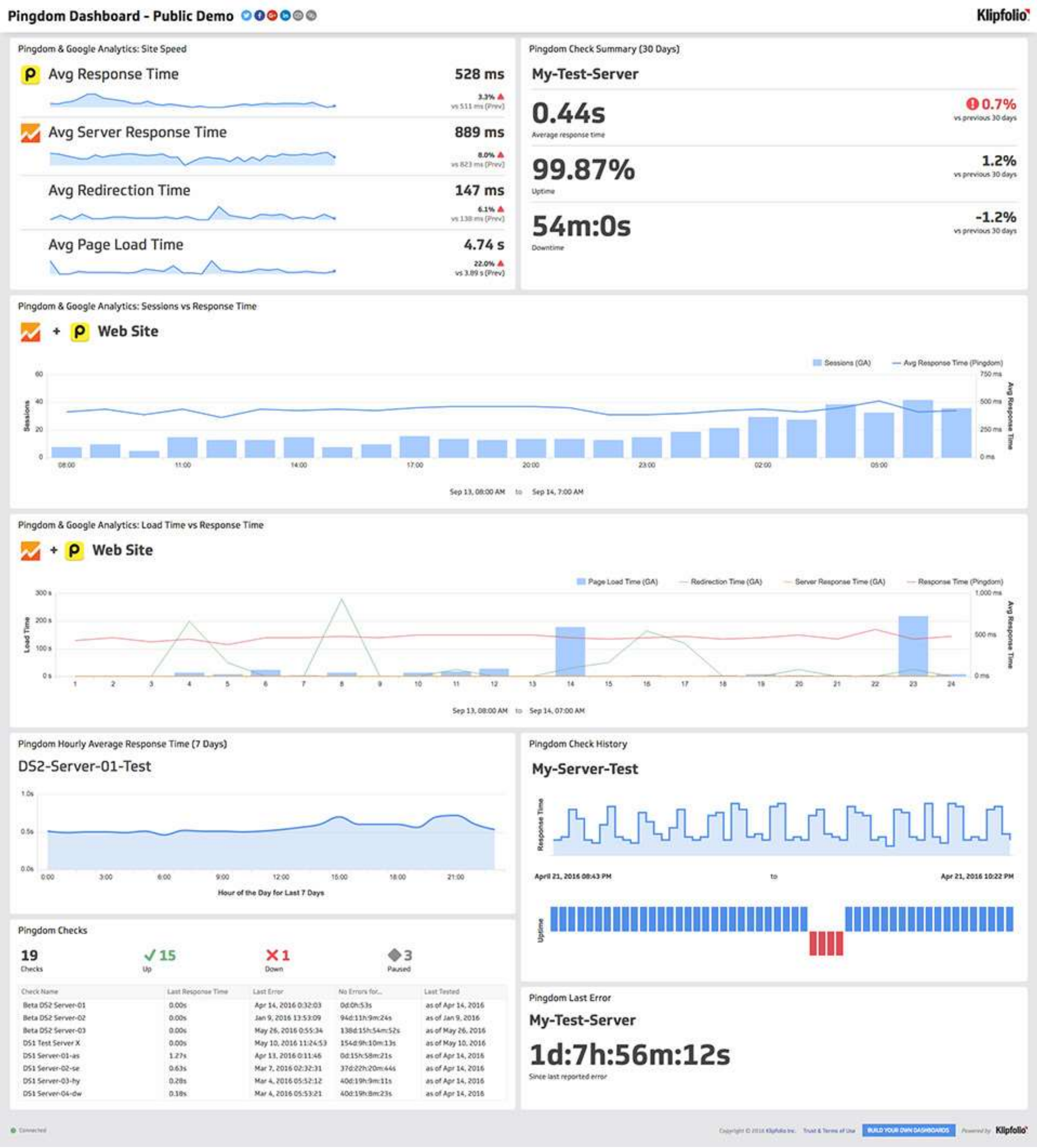
Overview

Name ▲	Feb 2	Feb 3	Feb 4	Feb 5	Feb 6	Feb 7	Feb 8
↑ users.apievangelist.com	✓	✓	✓	✓	✓	✓	✓
↑ blog.apievangelist.com	!	✓	✓	✓	✓	✓	✓
↑ faq.apievangelist.com	✓	✓	✓	✓	✓	✓	✓
↓ forum.apievangelist.com	✗	✗	✗	✗	✗	✗	✗
↑ code.apievangelist.com	✓	✓	✓	✓	✓	✓	✓
↑ partners.apievangelist.com	✓	✓	✓	✓	✓	✓	✓
↑ reports.apievangelist.com	✓	!	✓	✓	!	✓	✓

Show 10 rows per page

✓ Service is operating normally ! Performance issues ✗ Service disruption ○ No data available

Uptime monitoring provided by Pingdom



Pingdom Dashboard - Public Demo Klipfolio

Pingdom & Google Analytics: Site Speed

Avg Response Time	528 ms	3.3% ▲ vs 511 ms (Prev)
Avg Server Response Time	889 ms	8.0% ▲ vs 823 ms (Prev)
Avg Redirection Time	147 ms	6.1% ▲ vs 138 ms (Prev)
Avg Page Load Time	4.74 s	22.0% ▲ vs 3.89 s (Prev)

Pingdom Check Summary (30 Days)

My-Test-Server

0.44s Average response time	❶ 0.7% vs previous 30 days
99.87% Uptime	1.2% vs previous 30 days
54m:0s Downtime	-1.2% vs previous 30 days

Pingdom & Google Analytics: Sessions vs Response Time

+ Web Site

Sep 13, 08:00 AM to Sep 14, 7:00 AM

Pingdom & Google Analytics: Load Time vs Response Time

+ Web Site

Sep 13, 08:00 AM to Sep 14, 07:00 AM

Pingdom Hourly Average Response Time (7 Days)

DS2-Server-01-Test

Pingdom Check History

My-Server-Test

April 21, 2016 08:43 PM to Apr 21, 2016 10:22 PM

Pingdom Checks

19	✓ 15	✗ 1	◆ 3
Checks	Up	Down	Paused

Check Name	Last Response Time	Last Error	No Errors for...	Last Tested
Beta DS2 Server-01	0.00s	Apr 14, 2016 0:32:03	0d:0h:53s	as of Apr 14, 2016
Beta DS2 Server-02	0.00s	Jan 9, 2016 13:53:09	94d:11h:9m:24s	as of Jan 9, 2016
Beta DS2 Server-03	0.00s	May 26, 2016 0:55:34	138d:15h:54m:52s	as of May 26, 2016
DS1 Test Server X	0.00s	May 10, 2016 11:24:53	154d:9h:10m:13s	as of May 10, 2016
DS1 Server-01-as	1.27s	Apr 13, 2016 0:11:46	0d:15h:58m:21s	as of Apr 14, 2016
DS1 Server-02-se	0.63s	Mar 7, 2016 02:32:31	37d:22h:20m:44s	as of Apr 14, 2016
DS1 Server-03-hy	0.28s	Mar 4, 2016 05:52:12	40d:19h:9m:11s	as of Apr 14, 2016
DS1 Server-04-dw	0.18s	Mar 4, 2016 05:53:21	40d:19h:8m:23s	as of Apr 14, 2016

Pingdom Last Error

My-Test-Server

1d:7h:56m:12s

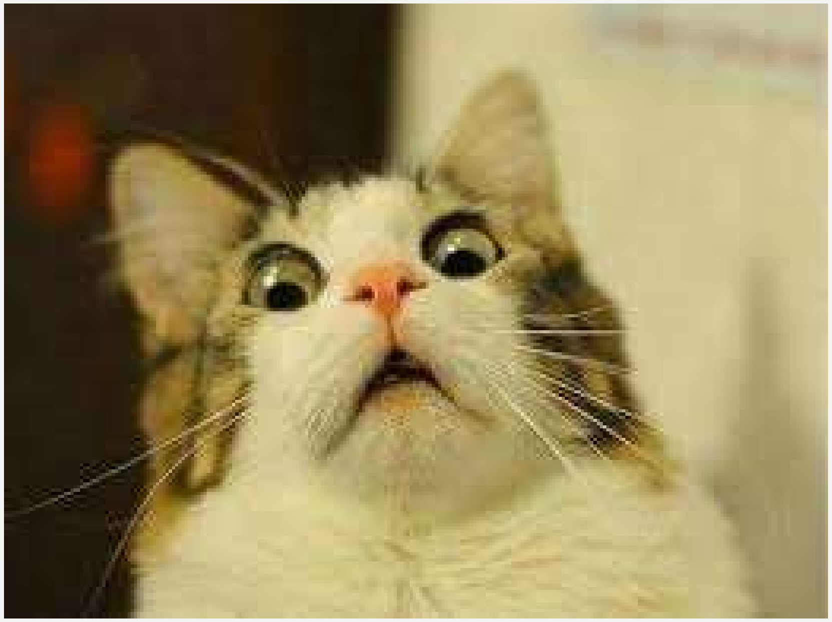
Since last reported error

● Connected

Copyright © 2016 Klipfolio Inc. Trust & Terms of Use BUILD YOUR OWN DASHBOARDS Powered by Klipfolio

TEST YOUR PLAN

- Test Your Back Ups
  - Do a recovery on a different server to ensure accuracy and time how long it takes to recover
- Test Your Redundancy
  - Remove a network, server, and determine if fail over occurs.
  - Time these!
- Test Test Test.

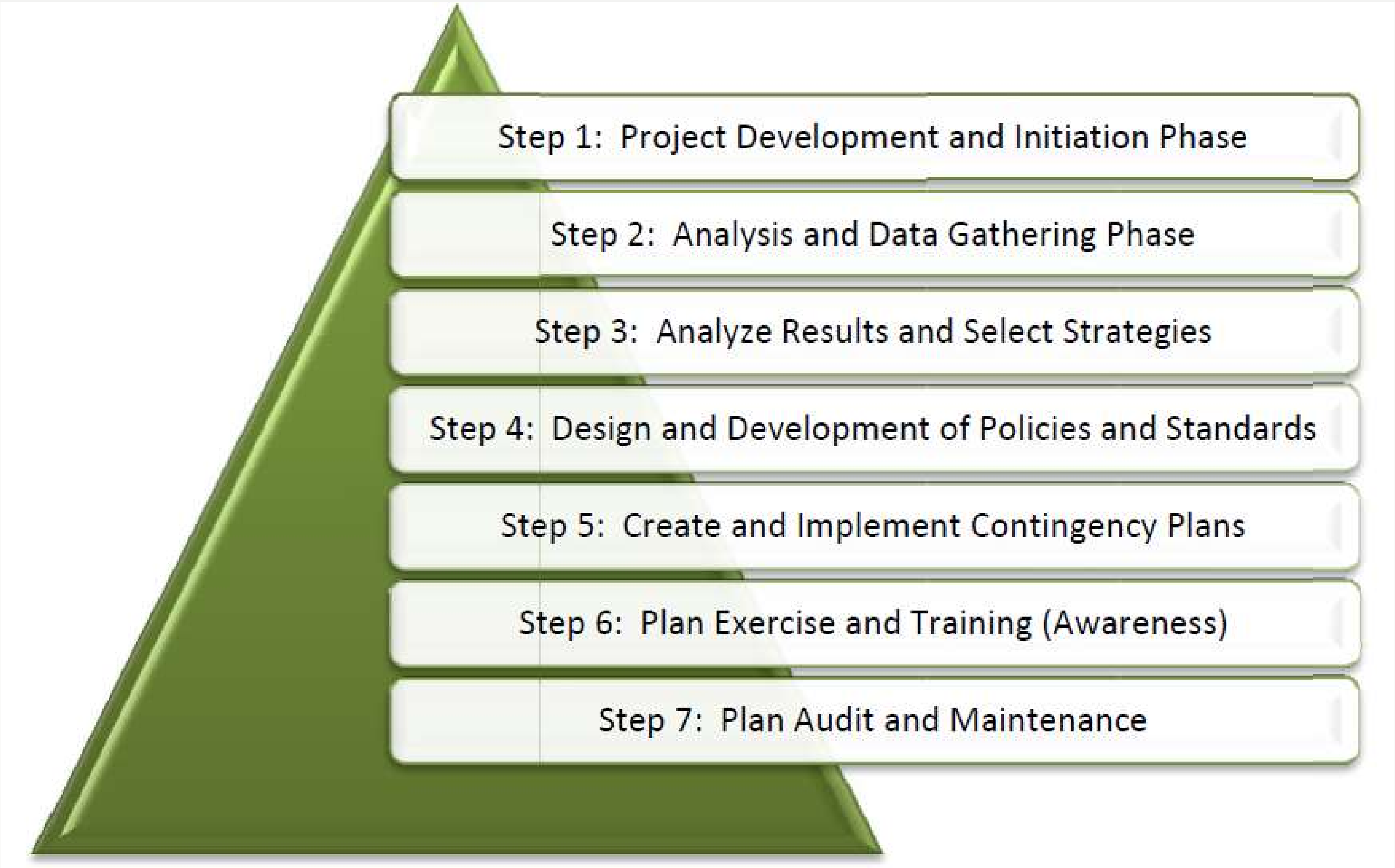


DIFFERENCES BETWEEN…

- An Emergency Response Plan
  - What to do immediately if an incident occurs.
- Business Continuity Plan
  - Address the immediate response AND short and long term continued performance of essential business functions

- While you make your disaster plan, you should work to mitigate as many risks, and then plan for the risks you couldn't mitigate.

LAYOUT OF A “DISASTER PLAN”



Step 1: Project Development and Initiation Phase

Step 2: Analysis and Data Gathering Phase

Step 3: Analyze Results and Select Strategies

Step 4: Design and Development of Policies and Standards

Step 5: Create and Implement Contingency Plans

Step 6: Plan Exercise and Training (Awareness)

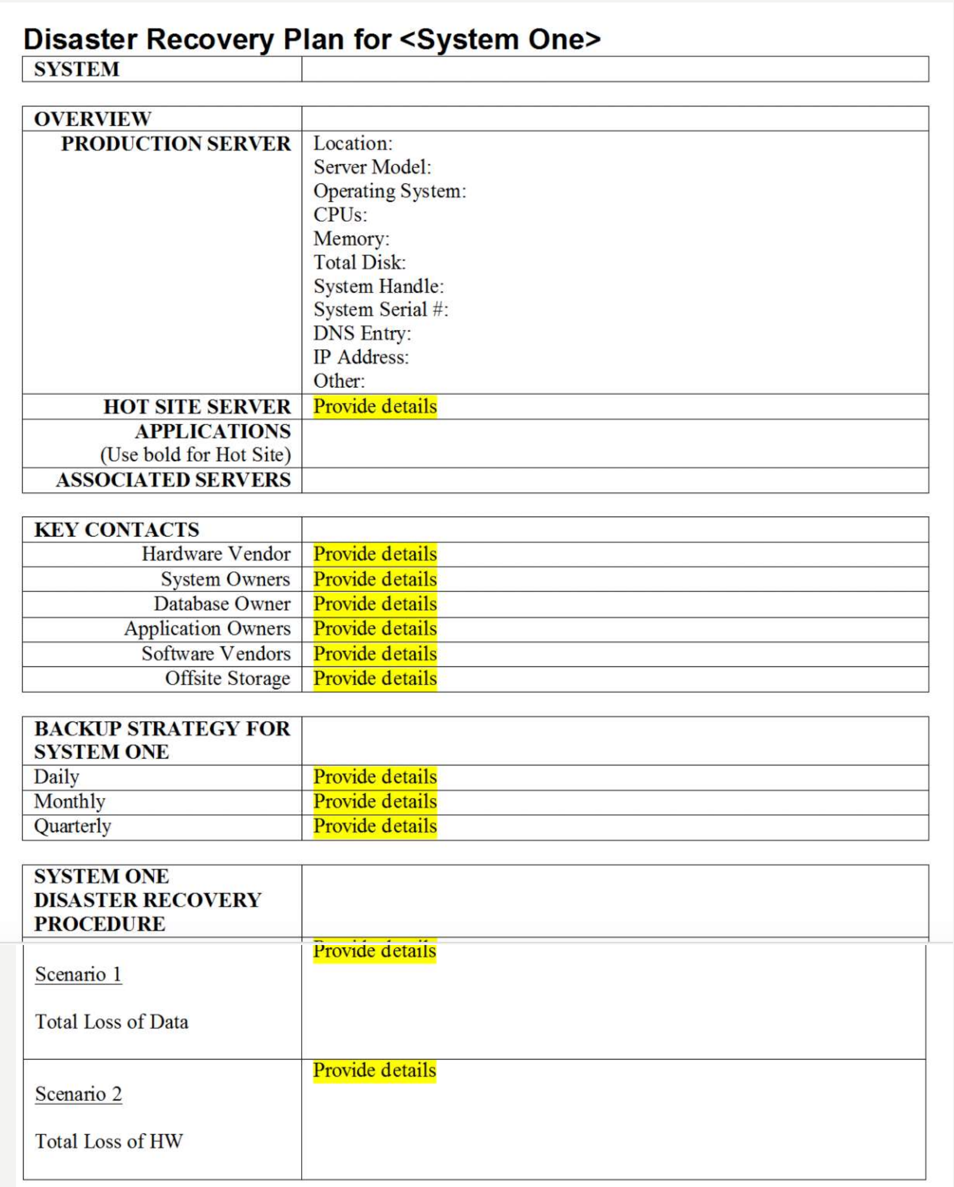
Step 7: Plan Audit and Maintenance

TO RECAP

- Risk Assessments to determine what the risks are and how to handle them.
  - Using the risk matrix; determine how much effort will be needed (and at what costs)
- Plans in place if there is some sort of failure.
  - Using the options presented, what makes the most sense to you?
  - Who are the contacts?
- Test.
  - Most important part of the entire disaster recovery process.

LINKS!

https://view.officeapps.live.com/op/view.aspx?src=http://cdn.ttgtmedia.com/searchDisasterRecovery/downloads/SearchDisasterRecovery_IT_DisasterRecoveryTemplate.doc



Disaster Recovery Plan for <System One>

SYSTEM	

OVERVIEW	
PRODUCTION SERVER	Location: Server Model: Operating System: CPUs: Memory: Total Disk: System Handle: System Serial #: DNS Entry: IP Address: Other:
HOT SITE SERVER	Provide details
APPLICATIONS (Use bold for Hot Site)	
ASSOCIATED SERVERS	

KEY CONTACTS	
Hardware Vendor	Provide details
System Owners	Provide details
Database Owner	Provide details
Application Owners	Provide details
Software Vendors	Provide details
Offsite Storage	Provide details

BACKUP STRATEGY FOR SYSTEM ONE	
Daily	Provide details
Monthly	Provide details
Quarterly	Provide details

SYSTEM ONE DISASTER RECOVERY PROCEDURE	
Scenario 1 Total Loss of Data	Provide details
Scenario 2 Total Loss of HW	Provide details

STORIES

- Crypto Locker:
  - Brought a business to a halt for three days.
  - Email Access Missing Back Ups
- Server Failure on Accounting Server
  - Was right before tax season.
- SAN Failure
  - Brought entire business down when EMC drives failed and there was no alerting set up (on a RAID).

QUESTIONS

- Brian Pichman
- bpichman@evolveproject.org
- Twitter: @bpichman