Emergency Preparedness

Creating a Disaster Recovery Plan for your Drupal Site

Keri Poeppe
Gorton Studios/NodeSquirrel.com
Twin Cities Drupal Camp 2014

NodeSquirrel

Hello!

Keri Poeppe
Product Manager, NodeSquirrel
Content Strategist, Gorton Studios
PM, Twin Cities Drupal Camp

gorton studios

NodeSquirrel

What can go wrong

- User Errors
- Bad Services
- Hackers
  - Intrusion
  - DDOS
- Success
  - The Reddit Hug/Slashdot Effect
- Natural Disasters

Been there, done that

- When things go wrong, clients call the people they know → YOU
- Big fail: Site database corrupted, backups were corrupted, lost weeks of volunteers' content
- Small fail: User installed modules on live site, website imploded

NodeSquirrel

Disaster Recovery Plans

A documented process to protect and recover from bad things.

3 Basic Features:

1. preventive measures
2. detective measures
3. corrective measures

NodeSquirrel

Typical advice

- Write down every possible scenario
- Write down the solution to every problem
- Practice!

Less intimidating

- Identify all the things that can fail
- Figure out how to replace them
- Practice!

Things that can fail

- Domain Registrar
- Authoritative Name Servers (DNS)
- Host Network
  - (load balancers, front end cache, solr)
- Web Server(s)
- Drupal and Modules
- Database(s)
- Uploaded Files

What do you need to do?

1. Preventive measures
2. Detective measures
3. Recovery measures

NodeSquirrel

	Prevent	Detect	Correct
Domain Registrar			
DNS			
Host Network			
Web Servers			
Drupal & Modules			
Database(s)			
Uploaded Files			

Prevent

- Drupal security best practices
- Content Delivery Network
- Hosted DNS
- Train your users
- Use good vendors (host, registrars etc.)

Drupal Security

- https://www.drupal.org/security/secure-configuration
- https://www.drupal.org/security
- File permissions on Apache
- https
- php module = BAD
- …and more

Content Delivery Network (CDN)

- Multiple copies of content on a distributed network of servers
- Serve up content based on geographic proximity
- Optimizes bandwidth, better performance
- Good for spikes in activity
- Protects from hackers, blocks IP addresses
- Prevent DDOS (intentional or unintentional)
- Display cached version of your site if down

NodeSquirrel

Options

- CloudFlare.com
- Incapsula.com
- Amazon Cloudfront

Hosted DNS

Using a third party service to manage your DNS

- Some protection from DDOS
- Better uptime (than cheap registrars)
- Actual redundancy

Hosted DNS Options

- Amazon Route 53
- dnsbycomodo.com
- dyn.com

Prevent

	Prevent	Detect	Recover
Domain Registrar	Good vendors		
DNS	Good vendors, DNS Host		
Host Network	Good vendors, CDN		
Web Servers	Good vendors, Security, CDN		
Drupal & Modules	Good vendors, Security, CDN, Train		
Database(s)	Security, CDN, Train		
Uploaded Files	Security, CDN, Train		

NodeSquirrel

Detective Measures

Don’t wait until your users tell you your site is down.

- Uptime monitors
- Application monitors

Uptime Monitors

Monitors pages, servers, ports.
Sends notifications for 404 errors or if unresponsive.
You set the monitoring schedule.

- Pingdom.com
- Uptimerobot.com
- Mon.itor.us

Application Monitors

- Checks the health of the server
  - Resource usage etc.
- Detect problems before they're critical
- Installed on your server

NodeSquirrel

Application Monitors Options

- New Relic
- Nagios
- Appneta
- Wormly
- Drupal Monitor

NodeSquirrel

Detect

	Prevent	Detect	Recover
Domain Registrar	Good vendors	Uptime Monitor	
DNS	Good vendors, DNS Host	Uptime Monitor	
Host Network	Good vendors, CDN	Uptime Monitor, App Monitor	
Web Servers	Good vendors, Security, CDN	Uptime Monitor, App Monitor	
Drupal & Modules	Good vendors, Security, CDN, Train	Uptime Monitor, App Monitor	
Database(s)	Security, CDN, Train	Uptime Monitor, App Monitor	
Uploaded Files	Security, CDN, Train		

NodeSquirrel

Recover

- The meat of the your plan
- Backups that you can use when needed

What you need to recover

- Host Network Configuration
- Server Configuration
- Drupal Code
- Drupal Database
- Drupal Uploaded Files

Server Configuration

- Changes rarely
- Not too hard to recover without backup
- Difficult to back up
- Ask your host
- Keep a record of custom configuration

NodeSquirrel

Drupal Code

- Changes rarely
- Sometimes possible to recover without backup
- Most of it is on drupal.org/github etc.
- Should be in a version control system
  - git, svn
- Automate Deployment (dploy.io)
- Backup and Migrate (v3)

NodeSquirrel

Database

- Changes frequently
- Impossible to recover without backup
- Easy to backup
- A few MB to a few GB
- Tools:
  - Backup and Migrate
  - phpMyAdmin export
  - MySQLDump

NodeSquirrel

Uploaded Files

- Change hourly or infrequently, depends on site
- Difficult-ish to recover without backup
- Pesky to back up
- Hundreds of MB+
- Restoring can be slow
- Tools:
  - Backup and Migrate (v3)
  - Rsync
  - Custom scripts

NodeSquirrel

Recover

	Prevent	Detect	Recover
Domain Registrar	Good vendors	Uptime Monitor	
DNS	Good vendors, DNS Host	Uptime Monitor	
Host Network	Good vendors, CDN	Uptime Monitor, App Monitor	Host Backup
Web Servers	Good vendors, Security, CDN	Uptime Monitor, App Monitor	Host Backup
Drupal & Modules	Good vendors, Security, CDN, Train	Uptime Monitor, App Monitor	Host Backup, Backup & Migrate, VCS, Code storage
Database(s)	Security, CDN, Train	Uptime Monitor, App Monitor	Host Backup Backup & Migrate, MySQLDump, phpMyAdmin
Uploaded Files	Security, CDN, Train		Host Backup Backup & Migrate, Rsync

NodeSquirrel

Levels of Drupal Backup

- Server
- Application
- Content

Server backup

- Provided by hosts
- Backs up config/db/code/files
- Slow to recover
- Dependant on host/sysop
- Best for total system failure
- Tend to be untested

NodeSquirrel

Application Backup

- Backup Drupal DB and Files
- Controlled by site owner/admin
- Recover in seconds
- No support tickets needed
- Best for user error and partial failure
- Tend to be more frequent

NodeSquirrel

Content Backup

- Per-node versioning (“revisions”)
- Recover specific nodes/entities
- Built in to Drupal core
- Best for: localized user error
- Not good for: Things that aren’t entities. Deletes.

NodeSquirrel

Backup Storage

NodeSquirrel

On Site / On Server

- Quickest Backup
- Quickest Recovery
- Good for small fails
- Not good for serious failure

NodeSquirrel

Offsite

- Slower to backup
- More effort to set up
- Available when your server is down

- Offsite backup options
  - NodeSquirrel
  - Amazon S3
  - FTP to another host
  - Email (DON'T DO THIS)
- Offsite backup from your host is NOT offsite

Document your services

Know who to contact and how to log-in in an emergency

Your written plan

- A list of 3rd party services with:
  - Login credentials
  - Account email
  - Support contacts
- A list of internal people responsible for recovery
- The location, type and frequency of every backup
- Store online and offline

NodeSquirrel

Store tech support contacts

- Web host, Registrar, DNS, CDN, etc.
- Don’t rely on the company’s ticketing system.
  – Also store email, phone, twitter
- Make sure vendors have current contact information for your organization.
- Don’t give vendors email addresses that are not checked.
- Store online and offline

NodeSquirrel

Questions?

NodeSquirrel

Your Plan

	Prevent	Detect	Recover
Domain Registrar	Good vendors	Uptime Monitor	
DNS	Good vendors, DNS Host	Uptime Monitor	
Host Network	Good vendors, CDN	Uptime Monitor, App Monitor	Host Backup
Web Servers	Good vendors, Security, CDN	Uptime Monitor, App Monitor	Host Backup
Drupal & Modules	Good vendors, Security, CDN, Train	Uptime Monitor, App Monitor	Host Backup, Backup & Migrate, VCS, Code storage
Database(s)	Security, CDN, Train	Uptime Monitor, App Monitor	Host Backup, Backup & Migrate, MySQLDump, phpMyAdmin
Uploaded Files	Security, CDN, Train		Host Backup, Backup & Migrate, Rsync

NodeSquirrel

Thanks!

NodeSquirrel