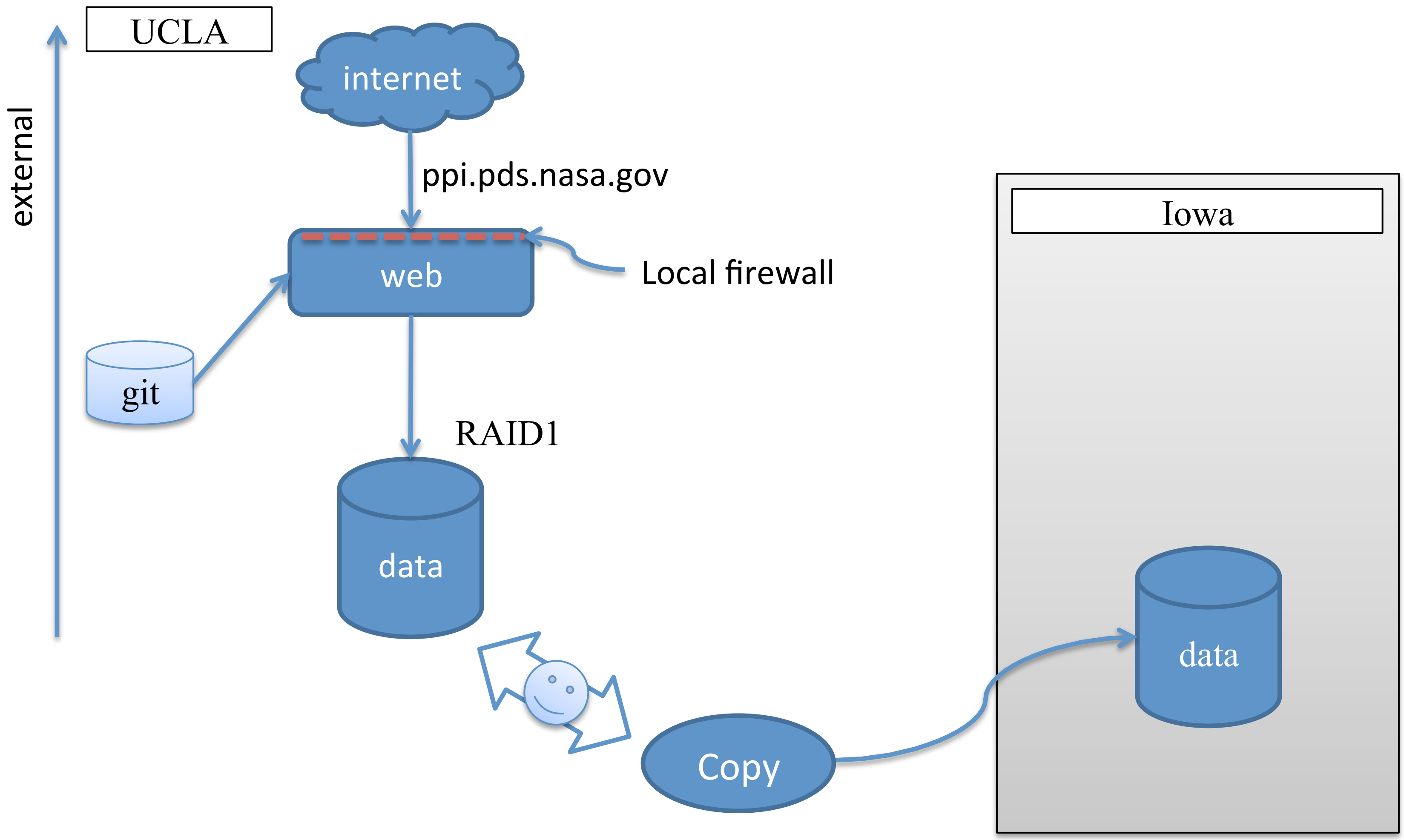
The New PPI Node Architecture

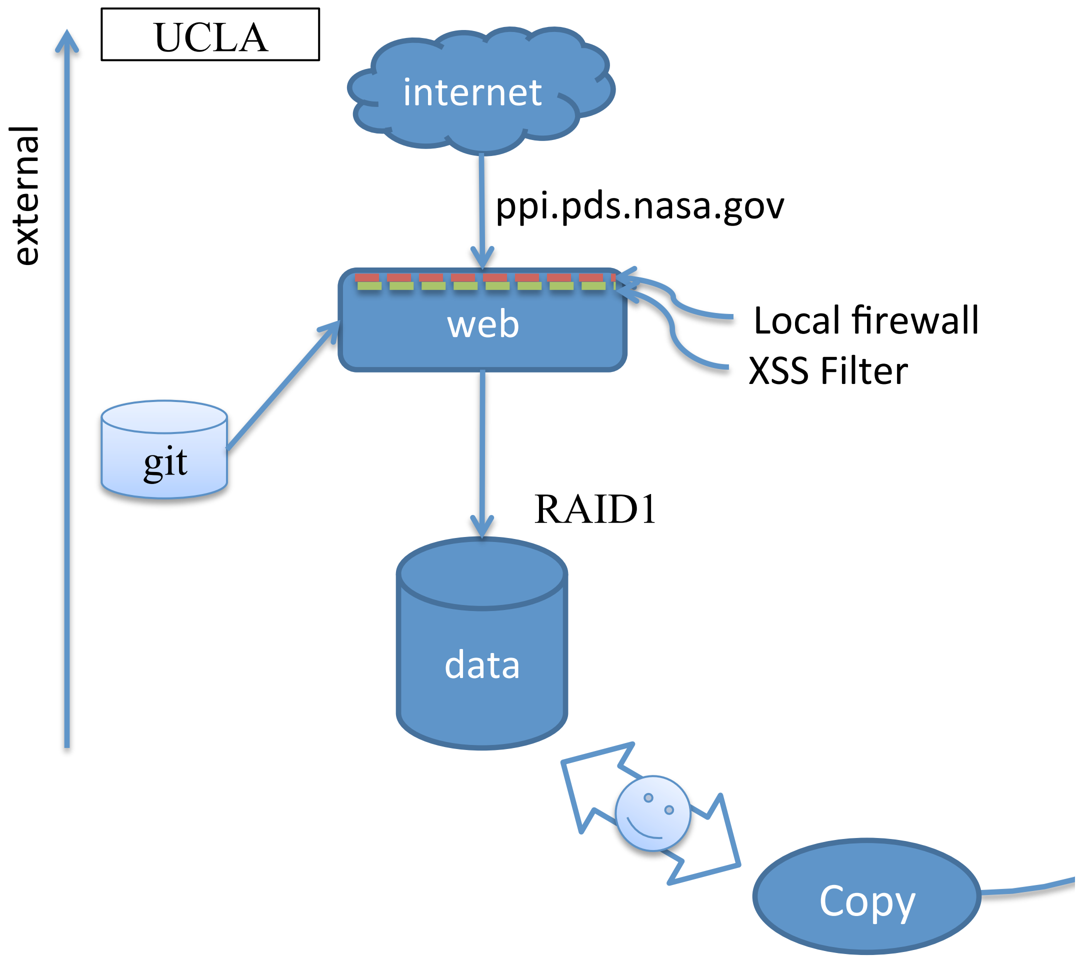
More secure, resilient and responsive

Todd King

In the Beginning… (9 months ago)



After XSS Incident... (6 months ago)



XSS Filter

- Disallows passing of HTML tags to services.
- Implemented as a filter servlet.
- Configurable.

Source available at:

https://github.com/igpp/servlet.git

Our Assessment

We needed a new architecture.

Our Goals

- Perform maintenance on servers while remaining fully operational
- Transparently upgrade and increase both storage and computational capacity
- Eliminate most single point failure risks
- Allow geographically separated redundancy
- Quicker response to critical events.

Technology Stack

- nginx reverse proxy server
- Tomcat application servers
- Solr search engine
- Redundancy (did I say redundancy)

with

- All user facing access through nginx reverse proxy.
- All content servers behind subnet firewall.
- Multiple security layers – fail safe assumptions

  i.e., fire walls at building, reverse proxy and each server.

With nginx you can…

Set security at access point (nginx)

- Load balance with multiple servers.
- Have automated recovery
  - Detection of off-line servers
  - Fail over to designated backup servers
  - Mark server off-line during servicing.
- Prevent common exploits
- Prevent access to files/folders
- Handle redirects up front.

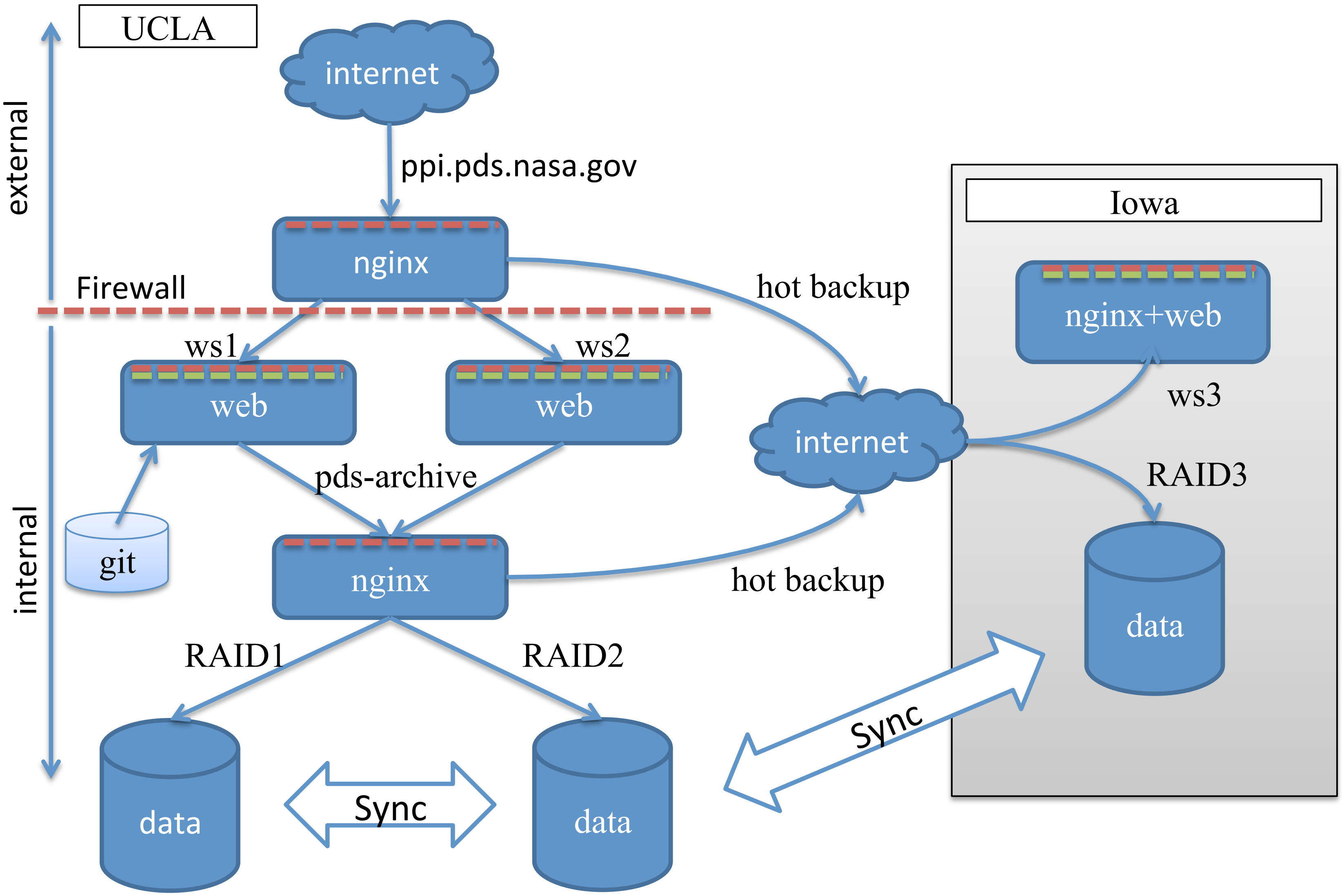
- Make all changes with live system.

```
$ nginx reload
```

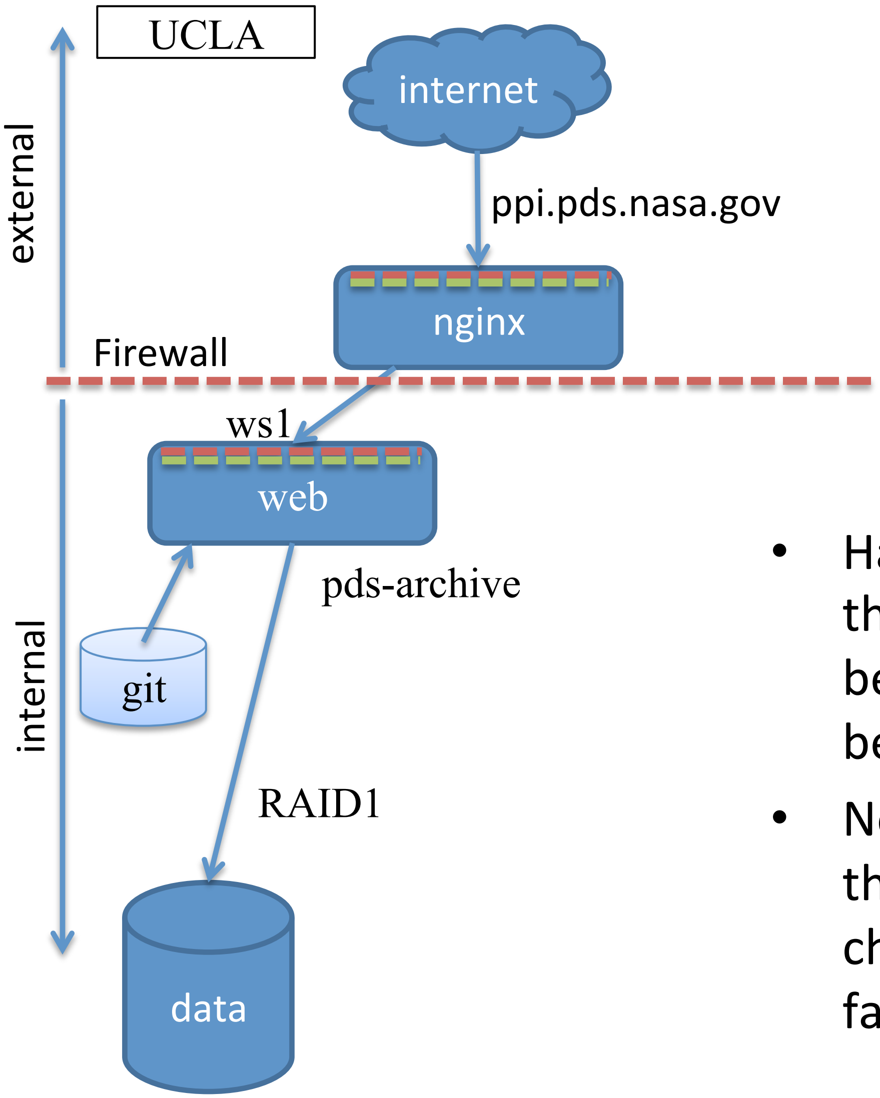
Sample Configuration

```
upstream ppi {
   ip_hash;
   server 192.168.1.1:8080;
   server 192.168.1.2:8080 weight=4 max_fails=3 fail_timeout=20;
   server ppi.physics.uiowa.edu backup;
 }

server {
   listen       80;
   server_name  ppi.pds.nasa.gov;

 # Protect from exploits: version snooping, ssl stripping, clickjacking, XSS
   server_tokens off;
   add_header Strict-Transport-Security "max-age=31536000; includeSubdomains;";
   add_header X-Frame-Options SAMEORIGIN;
   add_header X-Content-Type-Options nosniff;
   add_header X-XSS-Protection "1; mode=block";

   # prevent hidden files from being served
   location ~ /\.    { access_log off; log_not_found off; deny all; }
   location ~ /\_    { access_log off; log_not_found off; deny all; }

   # prevent common file exploit attempts
   location ~ /msadc { access_log off; log_not_found off; deny all; }
   location ~ /msadm { access_log off; log_not_found off; deny all; }
   location ~ \.dll$ { access_log off; log_not_found off; deny all; }

   location / {
      proxy_set_header X-Forwarded-Host $host;
      proxy_set_header X-Forwarded-Server $host;
      proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
      proxy_pass http://ppi;
   }
}
```

New Architecture



Phase 1 (Today)



Next Steps

- Hardware has been ordered and the rest of the architecture will be deployed as components become available.
- No one will notice as we build out the rest of the system since all changes will be behind the user facing nginx server.

תודה
Dankie
Gracias
Спасибо
شكراً
Merci
Takk
Köszönjük
Terima kasih
Grazie
Dziękujemy
Dėkojame
Ďakujeme
Vielen Dank
Paldies
Kiitos
Täname teid
谢谢
Thank You
Tak
感謝您
Obrigado
Teşekkür Ederiz
감사합니다
Σας Ευχαριστούμ
ขอบคุณ
Bedankt
Děkujeme vám
ありがとうございます
Tack