Software robustness process improvements

D. Petravick

OSG Security Officer/FNAL

March 1, 2007

Services Offered

Server Description	grid service	Version	Short Service Description	TCP port(s)	UDP port(s)	protected by...
Main gateway, globus gatekeeper, condor master.	slapd		Grid info publisher	2135		none
	postgresql		Core Service - 3rd Party	5434	13706	self
	globus-job-manager	4.0.2	Batch system	40819:10:00		none
	mysqld	4.1.11-log	Core Service - 3rd Party	49151		iptables
	apache	2.2.0	Core Service - 3rd Party	80,8443		none
	condor master	6.8.3	Batch system	62532:15:00	62532:15:00	none
	condor schedd	6.8.3	Batch system	62532:15:00	62532:15:00	none
	condor collector	6.8.3	Batch system	9618	9618	none
	condor negotiator	6.8.3	Batch system	62532:15:00	62532:15:00	none
	condor startd	6.8.3	Batch system	62532:15:00	62532:15:00	none
	condor gridmanager	6.8.3	Batch system	62532:15:00	62532:15:00	none
	Condor gahp server	6.8.3	Batch system	62532:15:00	62532:15:00	none
	Condor shadow	6.8.3	Batch system	62532:15:00	62532:15:00	none
	xinetd services					
	globus gatekeeper	4.0.2	Batch system	2119		none
	gridftp	4.0.2	Batch system	2811,40000:49150		none
	Java apps	1.4.2_10-b03	Core Service - 3rd Party			
	MonaLisa	1.4.12	Monitoring system	9000:9003,35332	9000, 9003, 58884	iptables
VOMS authentication Server, VOMRS registration server	mysqld	4.1.11-log	Core Service - 3rd Party	49151		iptables
	apache	2.2.0	Core Service - 3rd Party	8443		none
	apache	2.2.0	Core Service - 3rd Party	8080		iptables
	edg-voms	1.6.10.2	Authentication System	15250:20:00		none
	Java apps	1.4.2_10-b03	3rd Party – Core service			
	tomcat	5.0.28	Core Service - 3rd Party	8893,5001		iptables
	tomcat	5.0.28	Core Service - 3rd Party	8085		self
	Vomrs	1.2	Authentication System			
	Voms-admin	1.2.10_r0	Authentication System			
GUMS authorization server	mysqld	4.1.11-log	Core Service - 3rd Party	49151		iptables
	apache	2.2.0	Core Service - 3rd Party	8443		none
	apache	2.2.0	Core Service - 3rd Party	8080		iptables
	Java apps	1.4.2_10-b03	3rd Party – Core service			
	tomcat	5.0.28	Core Service - 3rd Party	8893,5001		iptables
	tomcat	5.0.28	Core Service - 3rd Party	8085		self
	Gums	1.1.0	Authorization System			self
SAZ authorization server, MyProxy server, squid web cache.	mysqld	4.1.11-log	Core Service - 3rd Party	49151		iptables
	apache	2.2.0	Core Service - 3rd Party	8443		none
	apache	2.2.0	Core Service - 3rd Party	8080		iptables
	squid	2.6.9	Core Service - 3rd Party	3128		iptables
	myproxy-server	3.4	Authentication System	7512		none
	condor master	6.8.3	Batch system	62532:15:00	62532:15:00	none
	condor schedd	6.8.3	Batch system	62532:15:00	62532:15:00	none
	condor startd	6.8.3	Batch system	62532:15:00	62532:15:00	none
	Java apps	1.4.2_10-b03	3rd Party – Core service			
	saz	2.0	Authorization System	8888		iptables
	tomcat	5.0.28	Core Service - 3rd Party	8893,5001		iptables
	tomcat	5.0.28	Core Service - 3rd Party	8085		self

One site

- Applies IDS to reduce exposure of computers to "scanning" behavior.
- Perimeter defenses viewed as an element of defense in depth.
  - Site should survive if this defense fails.
- Scans to avoid soft chewy center.
  - nmap -sS -p 1-65535 -A -P0 -T4 --osscan_limit --osscan_guess --host_timeout 40m --max-retries 0 IPADDRESS
  - "That scan will try to scan all 65,535 ports. For every port that is open, it will aggressively try to determine the service that is listening on that port."
  - As well as nessus (14,110 Nessus plugins are used)

One site -- Observer A

- Observer -- "malaise", and sometimes subtle to track.
  - (repeatable) Kills popular web server and servlet container on port 8893
  - (repeatable Causes popular job manager to use all memory on the machine
    - linux starts killing processes
    - Often leads to the crash of the machine.

One site -- Observer B

- In the past we've experienced application crashes, hangs, and memory leaks when the security scanners have hit our grid service machines. Specifically, we've seen our ***popular web server and servlet container*** become unresponsive while the number of java threads increases to around 75 as well as the ***popular job manager*** consume all available memory on a machine causing the Linux Kernel out-of-memory (OOM) killer to start randomly killing applications.

- Services that have, so far, been resilient to our scans include the voms and myproxy servers.

One site

- Subject to audits that include assessment using scanning tools inside its perimeter.
  - Can take some comfort that most treats are not grid aware.
  - But non grid specific tools break the as-deployed grid services.

What is the roadmap…

- For a successful ubiquitous deployment.
  - Do we have expectations for Level of effort for a secure deployment?
  - Platform: So configurable it's not configurable.

Diligences required?

- Service Provider: Understand problem well enough to file a problem report.
- Software Provider: Do something "reasonable" while software is in test.
- Grid
  - OSG: VDT adds scanning to its test bed.
  - Tabulate experience
  - Feed back to suppliers.

Mini-workshop.

- Is there a statement/can we make a statement about how robust a service ought to be? (how precise of a statement can we make to the development community)
  - Extremes
    - MUST survive trivial scan
    - But no need to exceed hardness of platform?
  - Ideas
    - The "environment in the Wild"
    - What prudent site officers do?