Booter 개발과 서버호스팅 프로젝트 중간 보고회

시행일 : 2016.11.21

www.symphonysoft.co.kr

발주업체:㈜제넷 시큐리티

시행업체:㈜심포니소프트

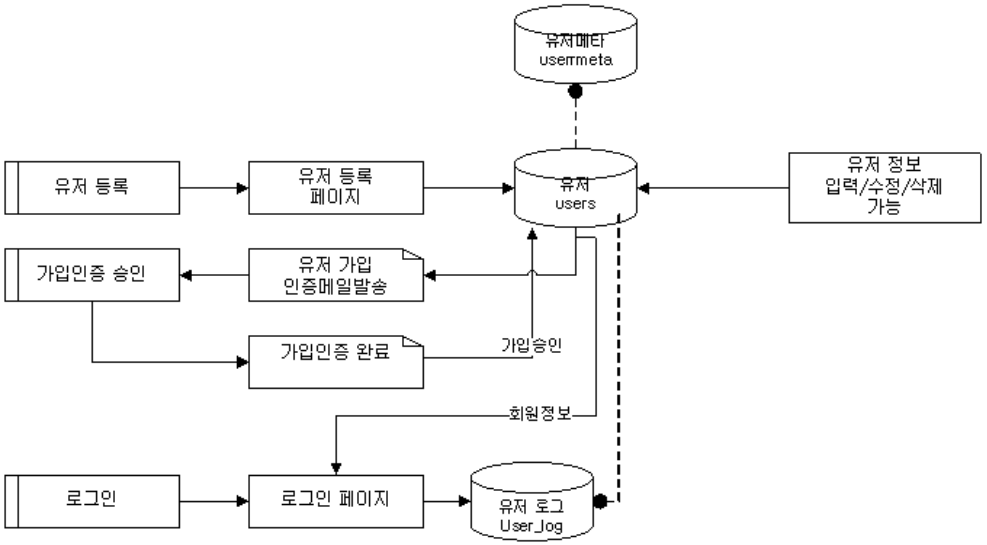
서울특별시 구로구 구로동 222-12 마리오 디지털 밸리 1006호

Tel. 02) 871-4134 Fax. 02-871-4155

❖목차

1. 1. Booter 개발 추가 및 수정 내역

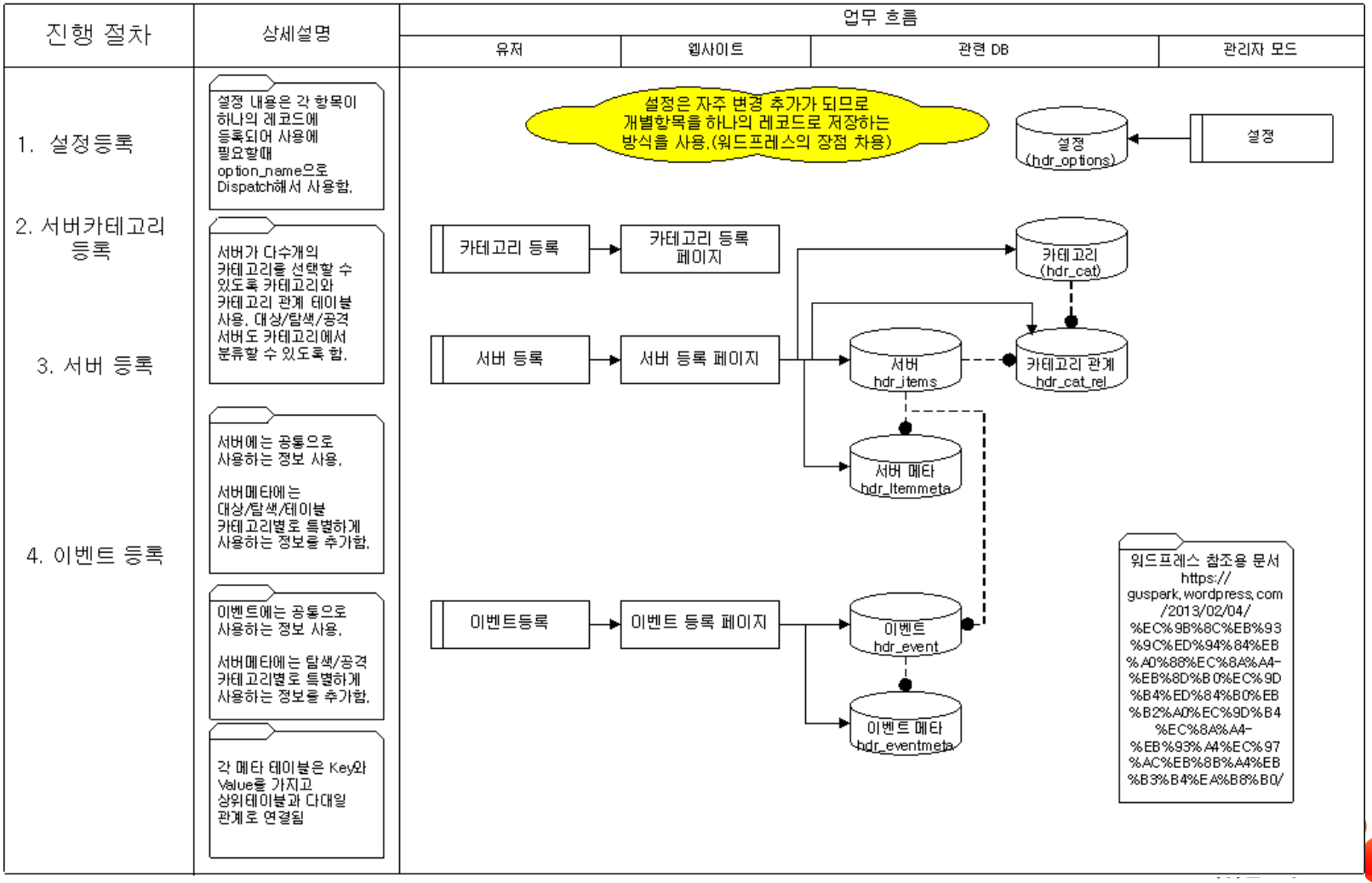
사용자 관리 흐름도	프로젝트 : 홈페이지 구성	고객 담당자 :	본사 담당자 :	작성일 :
	모듈 :	단위 :	:	:

진행 절차	상세설명	업무 흐름			
		유저	웹사이트 페이지	관련 DB Table	관리자 모드
1. 회원 등록	회원등록 정보는 (1)이메일 (2)패스워드 입력 받도록 함.				

(주)심포니소프트

1. 2. Booter 개발 추가 및 수정 내역

서버관리 테이블 다이어그램	프로젝트 : 홈페이지 구성	고객 담당자 :	본사 담당자 :	작성일 :
상품과 상품	모듈 :	단위 :	:	:

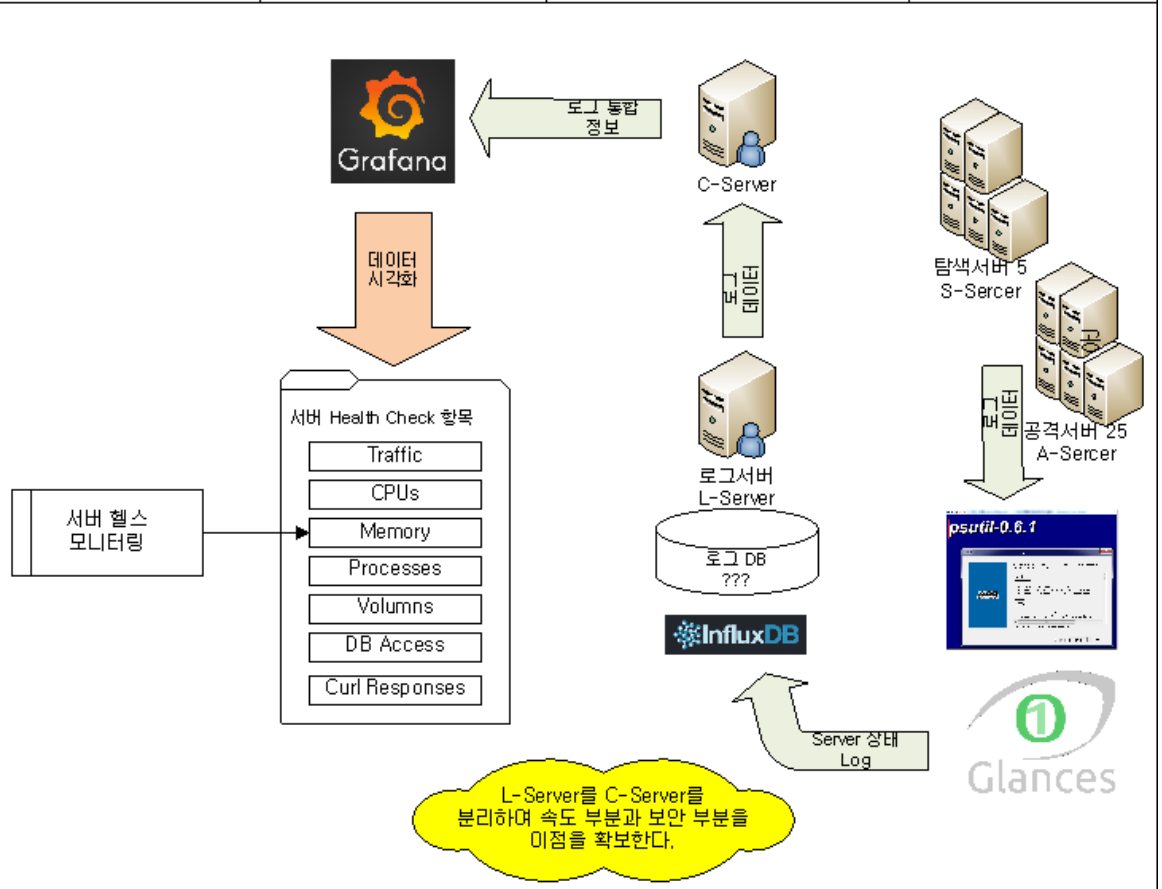


1. 3. 로그 서버를 통항 부하 분산 서버 기능도

웹 서버 모니터링과 마케팅 자동화

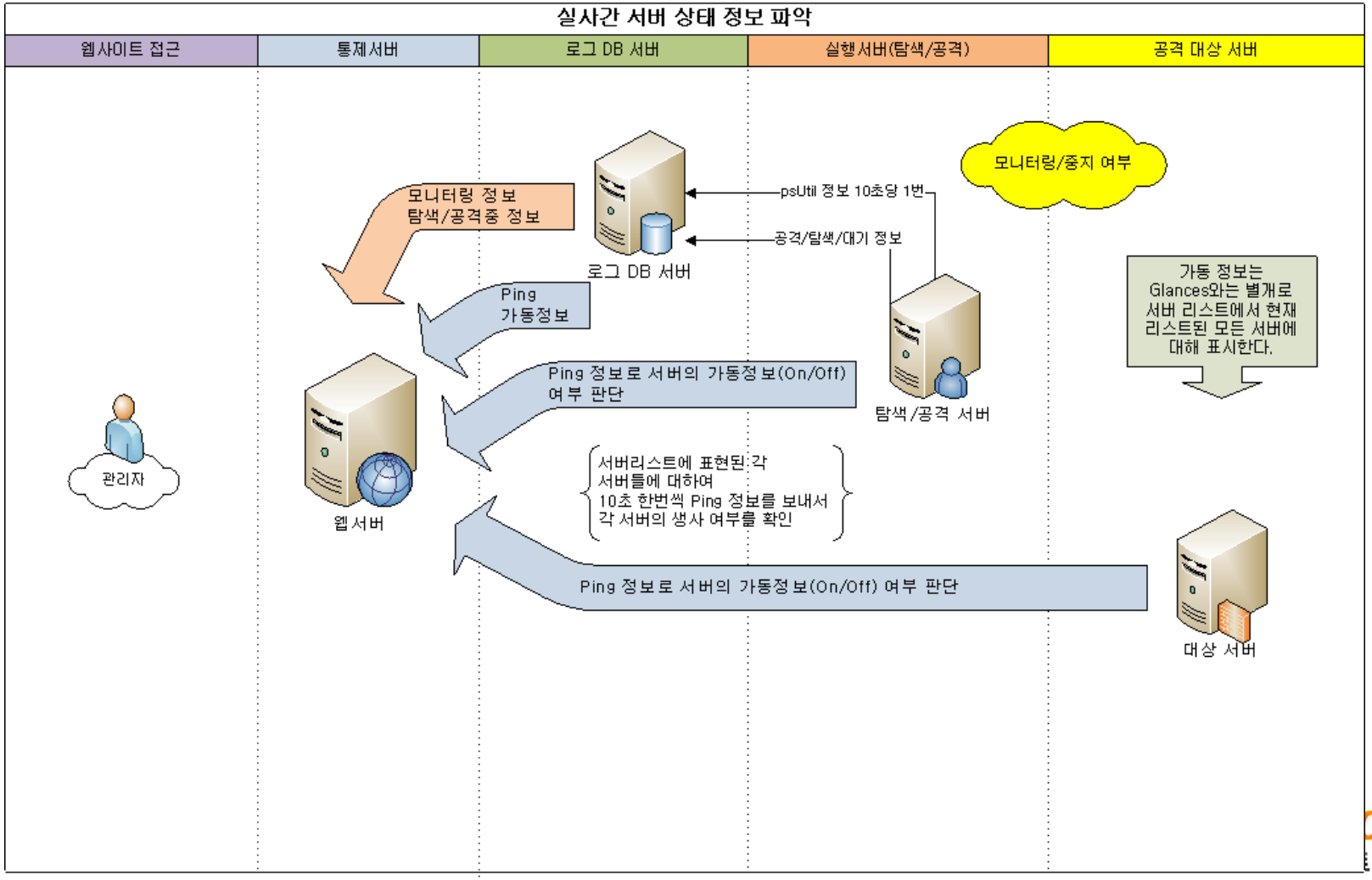
헬스 체크 로그 부하 분산 처리	프로젝트 : 홈페이지 구성	고객 담당자 :	본사 담당자 :	작성일 :
상품과 상품	모듈 :	단위 :	:	:

진행 절차	상세설명	업무 흐름
		유저 / 웹사이트 관리항목 / C-Server 관련 DB / 탐색/통제 서버
1. 30개의 서버 로그 트래픽	1. 30개의 서버에서 10초에 1번씩 서버의 헬스 체크 정보를 REST API 로 받음.	
2. Glances를 통해 DB에 직접 저장	2. Django ORM과 REST API에서 발생할 부하 예상으로 인하여 Log 정보 데이터를 Grances에서 로그서버로 기록하는 인터페이스를 직접 Query 하는 것을 변경하여 테스트함.	
3. 부하의 분산과 처리 속도 향상	3. 해당 내용 적용시 통제서버의 부하가 대폭 감소하며 30개이상의 서버가 로그정보를 보내오는 경우라도 문제없이 처리가 가능하리라 예상됨	
4. 로그서버는 특정 포트 이외에는 모두 차단하므로 보안 강화에 도움		

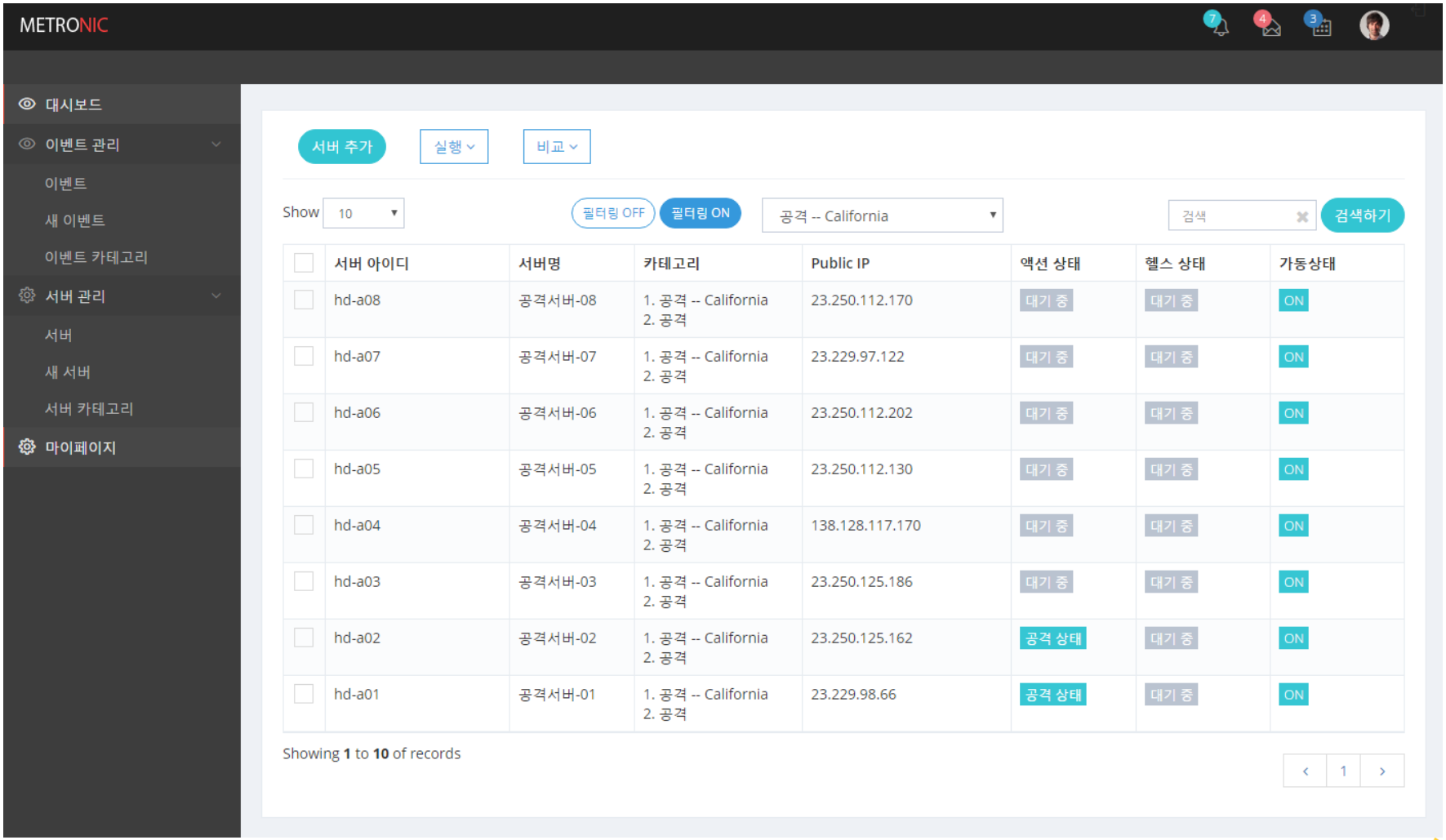


1.4. 서버 상태 정보 파악

히드라 서버 상태 정보 파악	프로젝트 : 히드라	고객 담당자 :	본사 담당자 :	작성일 :
	모듈 :	단위 :	:	:



1.5 관리자 메인 메뉴


METRONIC
대시보드
이벤트 관리
이벤트
새 이벤트
이벤트 카테고리
서버 관리
서버
새 서버
서버 카테고리
마이페이지
서버 추가
실행
비교
Show 10
필터링 OFF
필터링 ON
공격 -- California
검색
검색하기
서버 아이디
서버명
카테고리
Public IP
액션 상태
헬스 상태
가동상태
hd-a08 공격서버-08 1. 공격 -- California 2. 공격 23.250.112.170 대기 중 대기 중 ON
hd-a07 공격서버-07 1. 공격 -- California 2. 공격 23.229.97.122 대기 중 대기 중 ON
hd-a06 공격서버-06 1. 공격 -- California 2. 공격 23.250.112.202 대기 중 대기 중 ON
hd-a05 공격서버-05 1. 공격 -- California 2. 공격 23.250.112.130 대기 중 대기 중 ON
hd-a04 공격서버-04 1. 공격 -- California 2. 공격 138.128.117.170 대기 중 대기 중 ON
hd-a03 공격서버-03 1. 공격 -- California 2. 공격 23.250.125.186 대기 중 대기 중 ON
hd-a02 공격서버-02 1. 공격 -- California 2. 공격 23.250.125.162 공격 상태 대기 중 ON
hd-a01 공격서버-01 1. 공격 -- California 2. 공격 23.229.98.66 공격 상태 대기 중 ON
Showing 1 to 10 of records
1

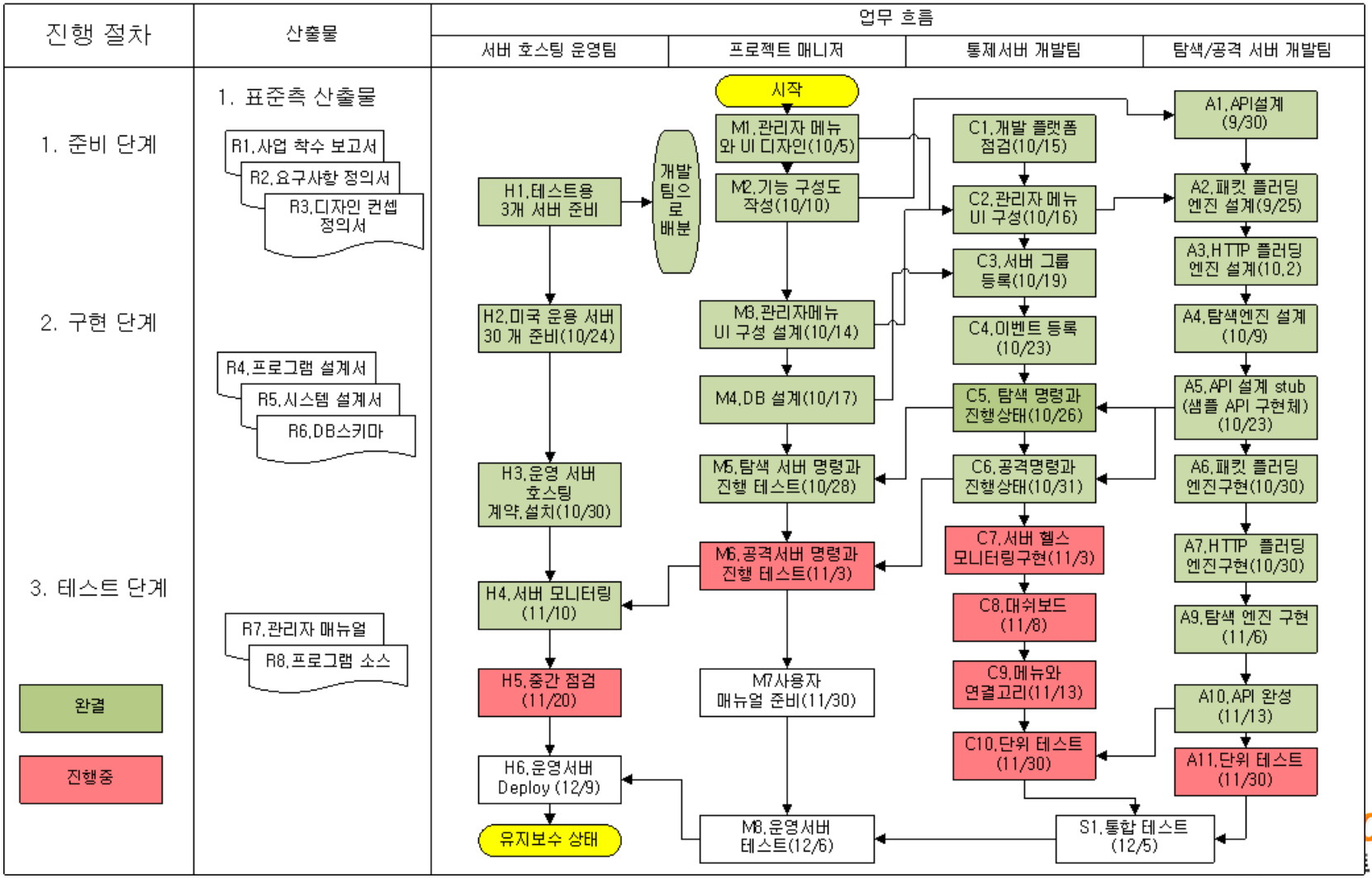
1.6 서버 헬스 체크 모니터링 그래프 예시

(주)심포니소프트

2. 개발와 서버호스팅 진척 상황

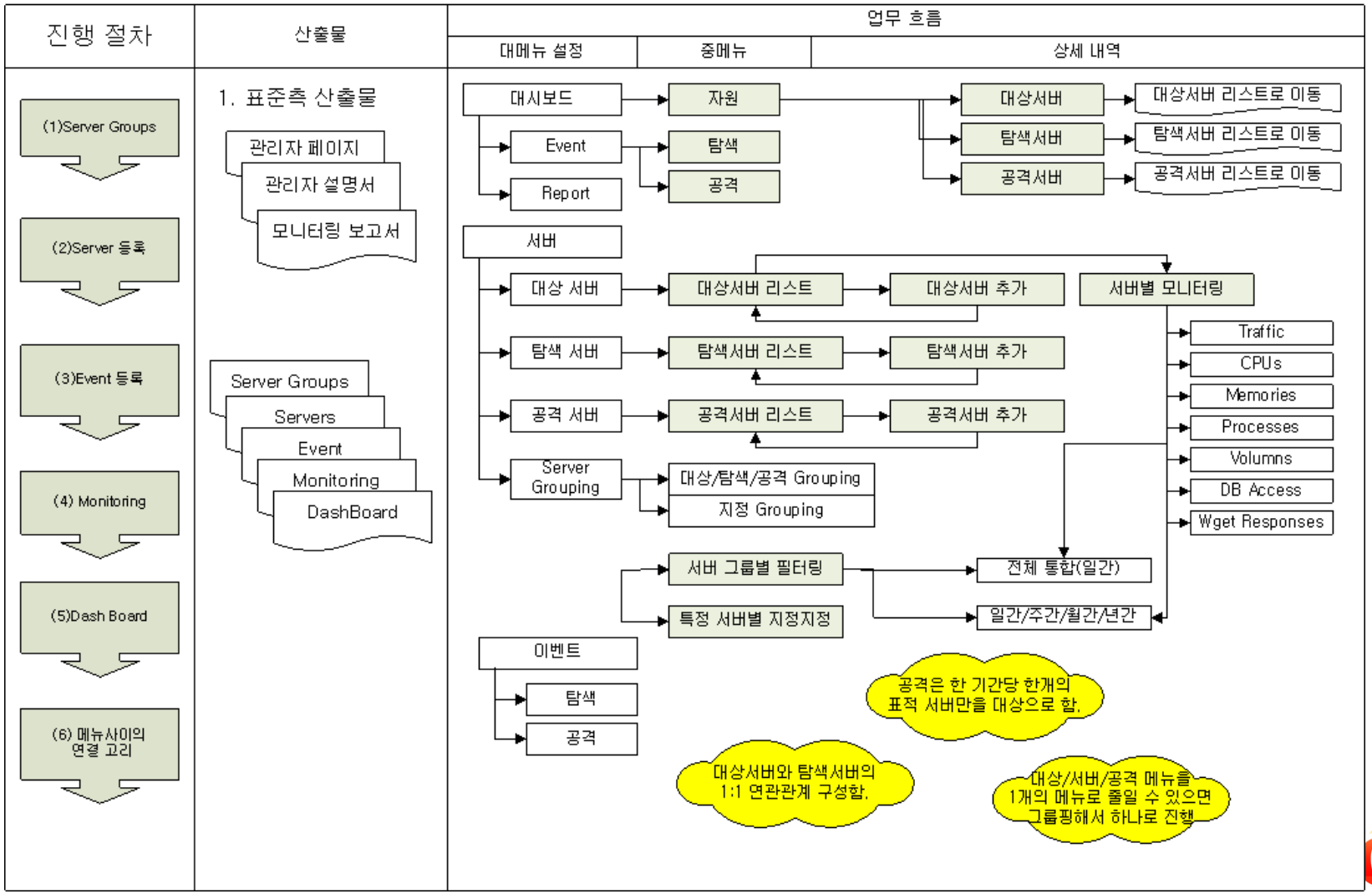
웹 서버 모니터링과 마케팅 자동화

통합 일정관리 및 보고서	프로젝트 : Booter개발/서버	고객 담당자 :	본사 담당자 :	작성일 :
심포니소프트	모듈 :	단위 :	:	:



3. 변경된 관리자 모드 메뉴

Booter 관리자 메뉴	프로젝트 : Booter와 서버호스팅	고객 담당자 :	본사 담당자 :	작성일 :
Jennet Security	모듈 : 실제 구성도	단위 :	:	:



4. 1. 서버 구성 내역

servers : 테이블

구분	서버코드	설치지역	IP	비밀번호	담당회사
1	hd-con	캘리포니아리전	52.52.192.155	k99614791	AWS
2	hd-log	캘리포니아리전	52.52.193.94	전서버가 동일하며 비밀번호로 ssh로그인 불가능함	AWS
3	hd-s01	노스버지니아리전	54.80.247.167		AWS
3	hd-s02	오하이오리전	52.15.134.167		AWS
3	hd-s03	캘리포니아리전	52.52.142.145		AWS
3	hd-s04	오레건리전	35.160.32.36		AWS
4	hd-a01	캘리포니아	23.229.98.66		ServerMania
4	hd-a02	캘리포니아	23.250.125.162		ServerMania
4	hd-a03	캘리포니아	23.250.125.186		ServerMania
4	hd-a04	캘리포니아	138.128.117.170		ServerMania
4	hd-a05	캘리포니아	23.250.112.130		ServerMania
4	hd-a06	캘리포니아	23.250.112.202		ServerMania
4	hd-a07	캘리포니아	23.229.97.122		ServerMania
4	hd-a08	캘리포니아	23.250.112.170		ServerMania
4	hd-a09	세인트루이스	209.126.66.32		Datasoft
4	hd-a10	세인트루이스	209.126.65.66		Datasoft
4	hd-a11	세인트루이스	209.126.68.102		Datasoft
4	hd-a12	세인트루이스	209.126.68.122		Datasoft
4	hd-a13	세인트루이스	209.126.68.142		Datasoft
4	hd-a14	세인트루이스	209.126.64.54		Datasoft
4	hd-a15	세인트루이스	209.126.65.30		Datasoft
4	hd-a16	세인트루이스	209.126.68.4		Datasoft
4	hd-a17	오하이오	67.219.150.202		DecicatedSolutions
4	hd-a18	오하이오	67.219.150.194		DecicatedSolutions
4	hd-a19	오하이오	67.219.150.142		DecicatedSolutions
4	hd-a20	오하이오	67.219.150.150		DecicatedSolutions
4	hd-a21	오하이오	67.219.150.158		DecicatedSolutions
4	hd-a22	오하이오	67.219.150.154		DecicatedSolutions
4	hd-a23	오하이오	67.219.150.146		DecicatedSolutions
4	hd-a24	오하이오	67.219.150.138		DecicatedSolutions
5	hd-t01	서울리전	115.68.185.231		스마일서브

4.2. 위치별 서버 구성 내역

캘리포니아 지역 서버 (8대)

System Hardware Configuration	
Processor:	Intel Xeon E3-1240v3, 3.4 GHz
RAM:	32 GB
Drive Configuration	
Primary Drive:	120 GB - Solid State Drive
Network Configuration	
Bandwidth:	100 Mbps Speed / 10 TB Bandwidth
IPv4 Addresses:	/29 IP Range (5 Usable IPs)
Datacenter Location:	Los Angeles, California (US West)
IPMI:	Free IPMI KVM Console
System Software Configuration	
Operating System:	CentOS 6 x64
Service Addons	
DDoS Protection:	1 Gbps - Enterprise DDoS Protection, All IP's Protected (Buffalo Only)

공격서버는 대용량 자료 저장기능이 필요없으므로 HDD 1TB 와 120GB SSD 의 선택 사양중 속도가 더 빠른 120GB SSD를 선택하였습니다.

(주)심포니소프트

4.2. 위치별 서버 구성 내역

루이지애나 서버 (8대)

Product/Service:
Dell PowerEdge C1100 Intel 8 Core 8 GB 2TB Dedicated Server With 1000 mbps Internet Port - Dell PowerEdge C1100 Intel 8 Core 8 GB 2TB Fully Managed Dedicated Server With 1000 mbps Internet Port Active
209.126.68.4[O004] 8 core 8 GB 2TB Linux

IP Address:
209.126.68.4

Operating System :
Centos 6 64 bit Free

Memory :
Default Memory

First Hard Drive :
2000 GB Hard Drive (Free Upgrade, a $30/month Value)

Second Hard Drive:
None

Third Hard Drive:
None

RAID Setup (Two Drives Needed):
No RAID

Internet Connection Port Speed :
1000 mbps Port (Free Upgrade, $30/month value)

Internet Bandwidth usage:
100 mbps Dedicated Bandwidth $30.00

4.3. 위치별 서버 구성 내역

오하이오 지역 서버 (8대)

- Server: 821B :Dell
- CPU :Intel Xeon 4 Core1x 2.0GHz E5335
- HDD :1x 500GB HDDNo Raid
- RAM :8GBRAM
- Bandwidth :10TB
- Location :OH, Columbus TIER-II
- Port Speed :1Gbps
- Operation System :Linux Centos 6.5

5. 공격 메소드 개발 내역

공격 정리

대분류	중분류	공격유형	정식 SIP	위변조SIP	TCP플래그	비고	지원여부	완성예정일	셀렉트이름
패킷플러딩	대역폭공격	UDP	O	O	N/A		O	-	UDP
		ICMP	O	O	N/A	임의의 ICMP type/code 공격 가능	O	-	ICMP
		ICMP-echo/req	-	-	N/A	SIP에 공격대상 서버 IP를 넣으면 Smurf 공격	O	-	ICMP-E/R
		ARP-Req			N/A	L2에서만 지원	O	-	ARP-REQ
	PPS 소비 공격	TCP	O	-	SYN	SYN > SYN/ACK > RST Stealth 공격	O	-	TCP/SYN
		TCP	O	O	ACK	ACK 공격	O	-	TCP/ACK
		TCP	O	O	RST	RST 공격	O	-	TCP/RST
		TCP	O	O	FIN	FIN 공격	O	-	TCP/FIN
		TCP	O	O	Random	모든 플래그를 매 패킷마다 랜덤으로 공격	O	-	TCP/RDM
	증폭 공격	DNS (UDP)	O	O	N/A	DNS 요청 플러딩 공격	O	-	AMP/DNA
		DNS (UDP)	O	O	N/A	DNS 요청 플러딩 공격에서 임의의 호스트 요청	O	-	AMP/DNS-A
		NTP (UDP)	O	O	N/A	NTP 요청 플러딩 공격	O	-	AMP/NTP

감 사 합 니 다

EconoQ
(주)심포니소프트