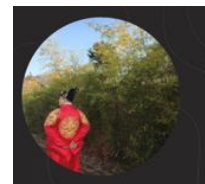


대규모 인프라를 운영하기 위한 15가지 정보

작성자 : Master SEO
topasvga@naver.com



작성자 소개

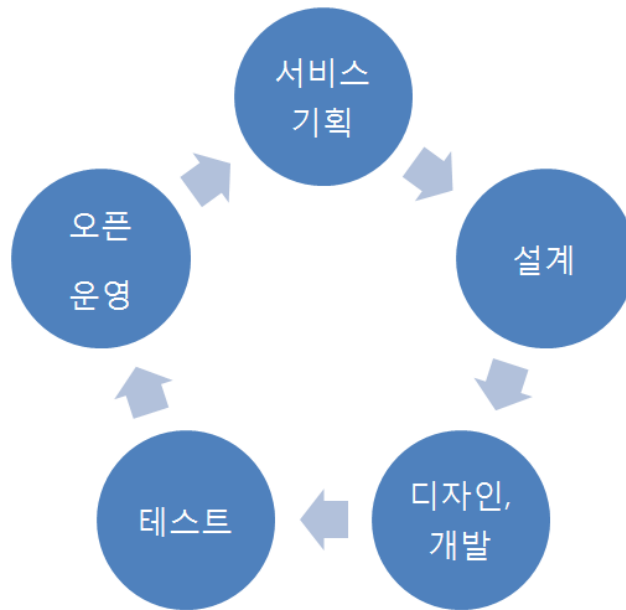


1. 대규모 인프라를 운영하기 위한 15가지 정보

시간	내용
10분	강사소개,WIFI공유,시설 소개
1시간	1.(입문) IT서비스는 어떻게 만들어지는가? 2. 온프레미스 인프라와 네트워크 알아보기 3. 대규모 네트워크 서비스망 4. DNS 구축과 구성 알아보기 5. CDN 서비스 이해와 CDN운영기술
1시간	6. 기술 플랫폼을 공부하고 적용하라! 7. 업무 요청 처리 시스템은 필수이다. 8. 서비스 코드, 자산관리, CMDB 알아야 한다. 9. 변경과 장애 관리시스템은 필수다 10. 모니터링 시스템과 장애 관리 조직 필요성
1시간	11. 전자금융거래법 통과와 PCI-DSS 취득하기 12.Facebook 페이스 북 서버와 OCP기술 보기 13. 온프레미스 IT 아키텍처 전문가 되기 1 14.IT 아키텍처 전문가 되기 2 15.IT 아키텍처 전문가 되기 3
계: 3시간	

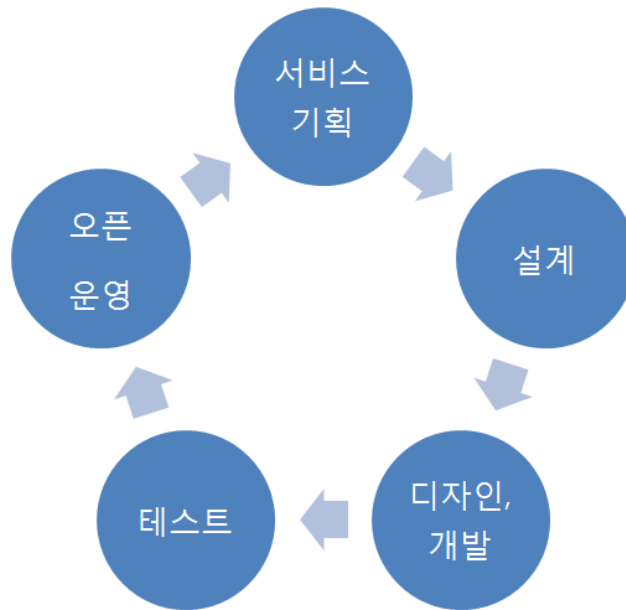
2. IT서비스는 어떻게 만들어지는가?

- IT인프라는 비즈니스 목적을 달성하기 위해 IT서비스를 만들고 운영하는 것이다.
- 다음은 신규 IT 서비스 오픈 프로세스 설명이다.
- 프로세스를 알아보고, 각 담당자가 하는 역할을 적어보았다.
- 5단계를 거쳐 만들어진다.
- [서비스 기획] => [설계] => [디자인, 개발] => [테스트] => [오픈/운영]



3. IT서비스는 어떻게 만들어지는가?

- IT인프라는 비즈니스 목적을 달성하기 위해 IT서비스를 만들고 운영하는 것이다.
- 다음은 신규 IT 서비스 오픈 프로세스 설명이다.
- 프로세스를 알아보고, 각 담당자가 하는 역할을 적어보았다.
- 5단계를 거쳐 만들어진다.
- [서비스 기획] => [설계] => [디자인, 개발] => [테스트] => [오픈/운영]



4. 서비스는 누가 만들어가나?



5. 서비스는 누가 만들어가나?

1) 서비스 기획

서비스가 할만한 것인지 분석하여 기획한다.

상위에서 과제를 제안하는 경우와 담당 기획자가 과제를 제안하는 2가지 경우가 있다.
프로세스를 거쳐 기획서를 심의하여 승인되면, 설계단계로 넘어간다.

담당 : 대부분 서비스 기획자는 사업부서 담당자.

2) 설계

구체적인 서비스 내용을 공유한다.

개발과 디자인과 협업하여하여 설계한다.

콘텐츠 수집, 법적 검토, 보안 점검, 마케팅 계획 등 여러 분야를 사전 검토와 준비를 해야 한다.

담당 : 기획자, 디자이너, 개발자, 인프라 담당자

3) 개발, 디자인 - 설계에 맞는 디자인, 개발을 진행한다.

담당: 개발자, 디자이너

6. 서비스는 누가 만들어가나?

4) 테스트

오픈전에 기능과 성능 테스트를 진행한다.

담당: 개발자, QA팀, 인프라 담당자

용어설명 : QA(Quality Assurance) , 제품 기획에서부터 릴리즈까지 전 과정의 품질을 관리

5) 오픈/운영

테스트가 완료되면 오픈하고 운영이 시작된다.

테스트 과정을 통과하면 서비스를 오픈하고 voc 체크하고 모니터링한다.

각 단계에서 산출물이 작성되고 , 승인을 통한 의사결정이 진행된다

담당: 전체 담당자 - 기획, 개발, 디자이너, QA, 인프라 담당자, 고객센터

* 용어설명 : VOC(Voice Of Customer- 고객의 소리) = 고객 불편사항 확인

7. 온프레미스 인프라와 네트워크 알아보기

- 나는 ISP, 네이버, 대기업, 중소기업에서 20년이상 인프라를 운영 했다.
- 내용 공유합니다.
- 온프레미스가 이후 클라우드에서 다른 용어로 불리우게 된다.
- 우선 온프레미스 인프라와 네트워크를 알아보자~
- 다음은 IT 서비스를 오픈해야 하는데 인프라를 잘 모르는 분들을 위한 글이다.
- 인프라에 대한 전체적인 개념을 알고 싶는데 마땅한 정보가 없는분
네이버처럼 대규모 인프라는 어떻게 운영되는지 알고 싶은분
- 개발은 외주를 주는데 서비스 서버에 포팅해야 하는데 어떻게 하는지 궁금하신분
- 궁금해하는 점들
 1. 서버가 어떻게 들어가 있는가?
 2. 네트워크 구성을 알고 싶다.
 3. 가상 서버는 뭐가 다른가?

8. 데이터 센터와 랙

1

데이터 센터는 서버, 네트워크 장비등을 수용하는 공간이다.

예) 서울 데이터 센터, 부산 데이터 센터, IDC (인터넷 데이터 센터)라고 부른다.

2

랙은 서버와 네트워크 장비를 수용하는 설비이다.

Data Center(IDC) 안에 전원을 공급받아 배치되어 있는 수용 장비이다.

서버, 네트워크 장비, 스토리지를 수용하고 있는 것이 랙이다.

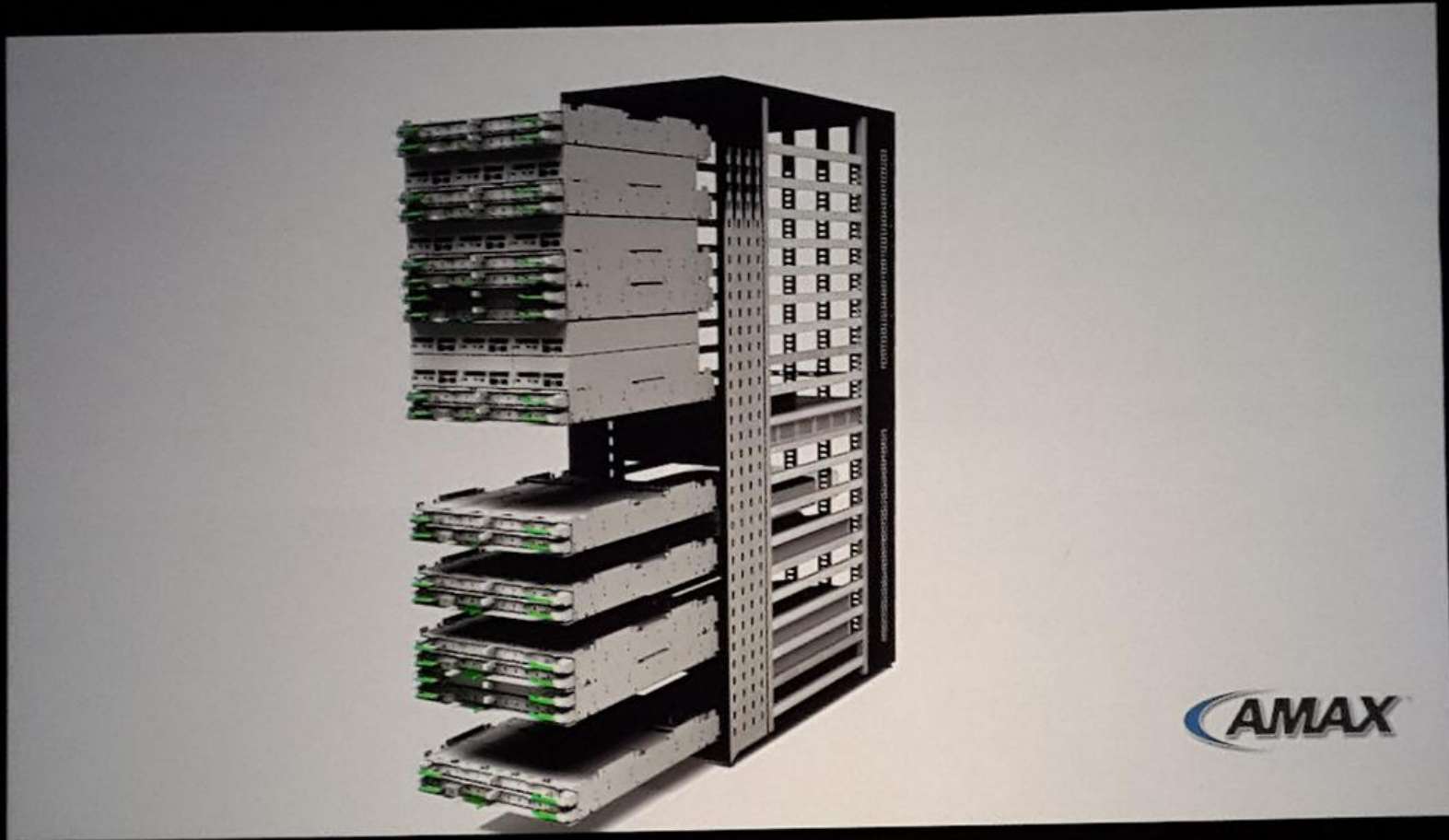
9. 데이터 센터와 랙



PHP, Memcache, MySQL
OEM servers & network
Leased data center space

10. 데이터 센터는 서버, 네트워크 장비등을 수용하는 공간이다.

랙에 서버는 다음과 같이 설치된다. 랙은 2개의 전원이 사용된다.
일반적으로 네트워크 장비나 서버가 2개의 전원을 제공하므로 2개 전원을 각각 연결한다.

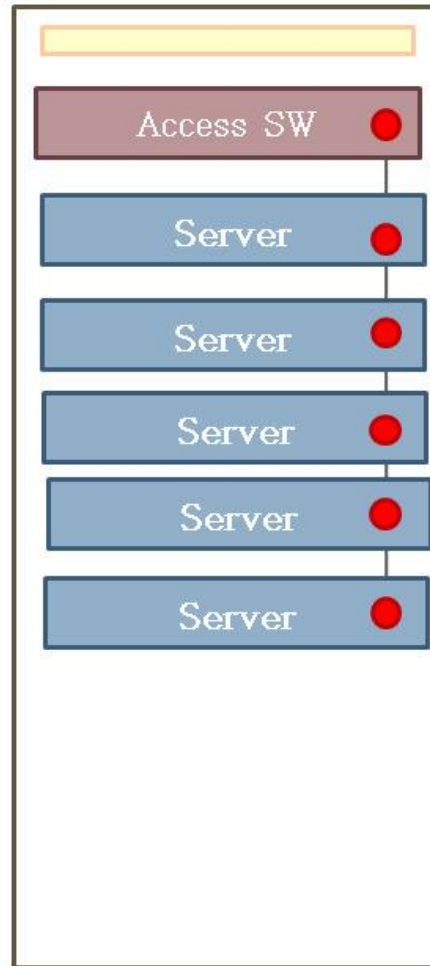


11. 랙은 서버와 네트워크 장비를 수용하는 설비이다.



12. 랙은 서버와 네트워크 장비를 수용하는 설비이다.

랙 배치를 보면, 보통 L2 스위치인 Access Switch가 있고, 서버들이 연결된다. Access Switch는 허브라고 보면 된다.



13. 네트워크와 보안 장비

1. L2 ?

서버가 연결되는 스위치로 Access Switch라고도 한다.
서버에 가장 근접해 있는 스위치

2. L3 ?

인터넷 회선이 연결되는 장비이다.
라우터 또는 L3 Switch가 사용된다.

3. L4 ?

서버를 이중화하도록 해주는 장비이다.
서버 로드 밸런싱 장비라고 한다.
SLB 장비라고도 부른다.

4. 보안장비

서버에 구축하기도 하고, 오픈라이언스로 일체 솔루션 장비가 도입되기도 한다.
방화벽, IDS (침입탐지시스템), IPS (차단 시스템) 등이 있다.

14. 서버

1. 서비스가 올라가는 장비

CPU , Memory , 디스크(HDD)를 가지고 있는 장비.
물리 서버와 가상 서버로 나누어진다.

2. 물리 서버

일반 물리적인 서버를 이야기한다.

서비스에는 웹, WAS, DB서버가 사용되는데, 주로 DB서버는 주로 물리 서버를 사용한다.

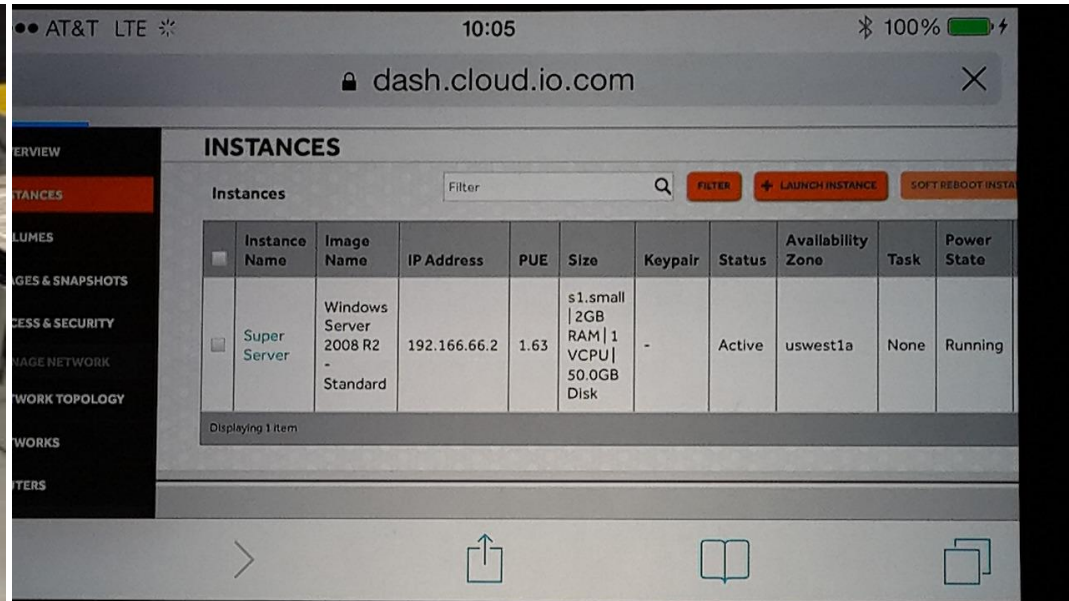
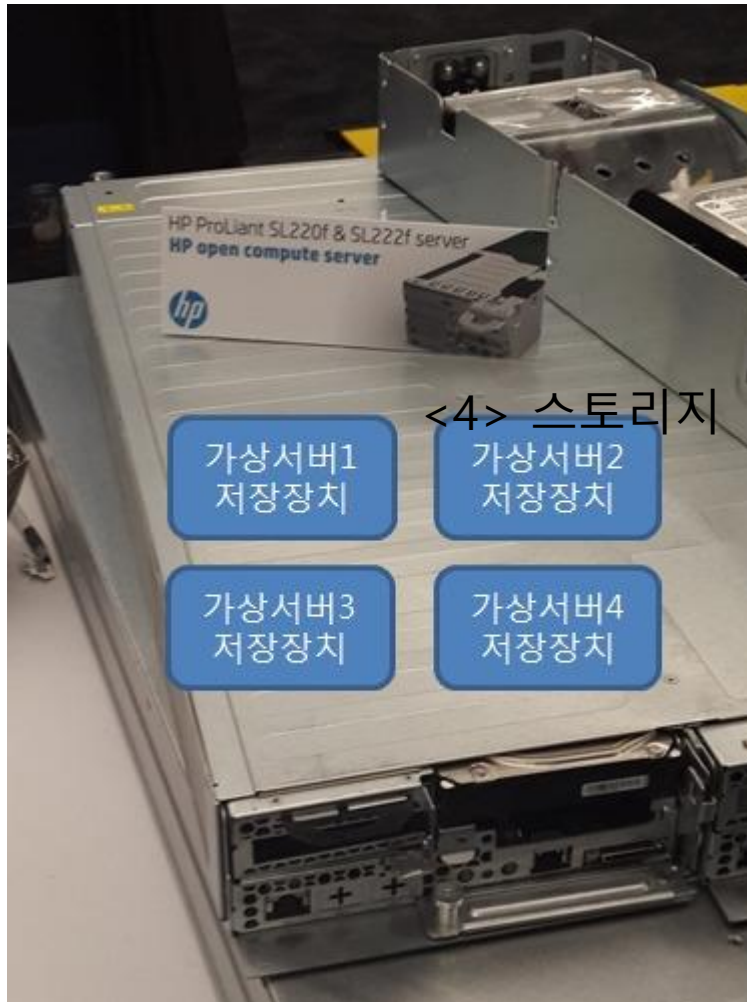
가상 서버는 물리 서버 안에 논리적으로 os(이미지)를 만들어 올린 것이다.

IO가 많은 DB들은 가상 서버에서 느린경우 물리 서버를 권장한다.



15. 가상 서버

주로 웹, 와스 서비스에 사용한다.

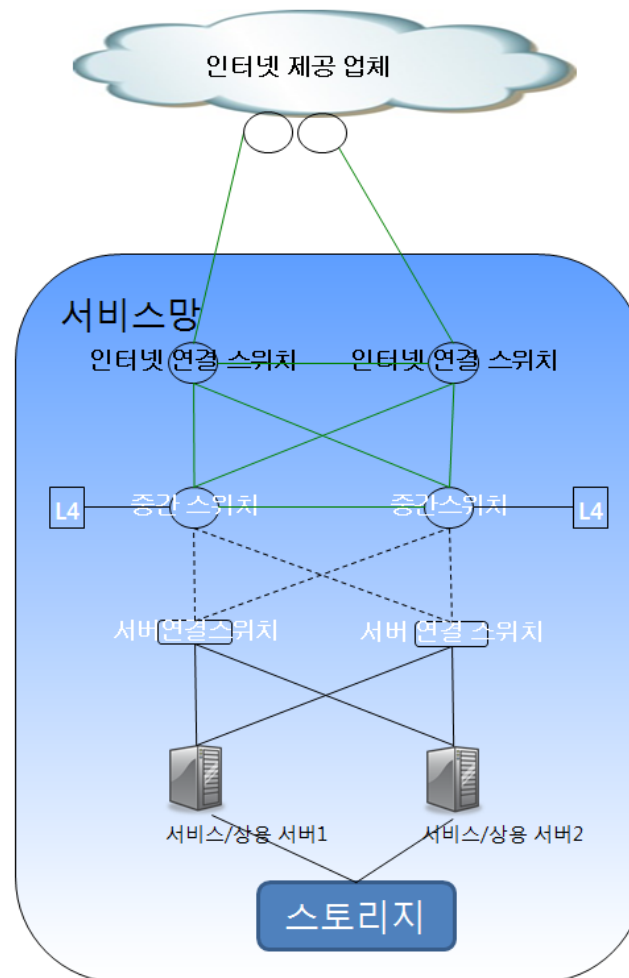


16. 스토리지1

NAS

웹서버에서 이미지를 같이 공유하고자 할 때 주로 사용한다.

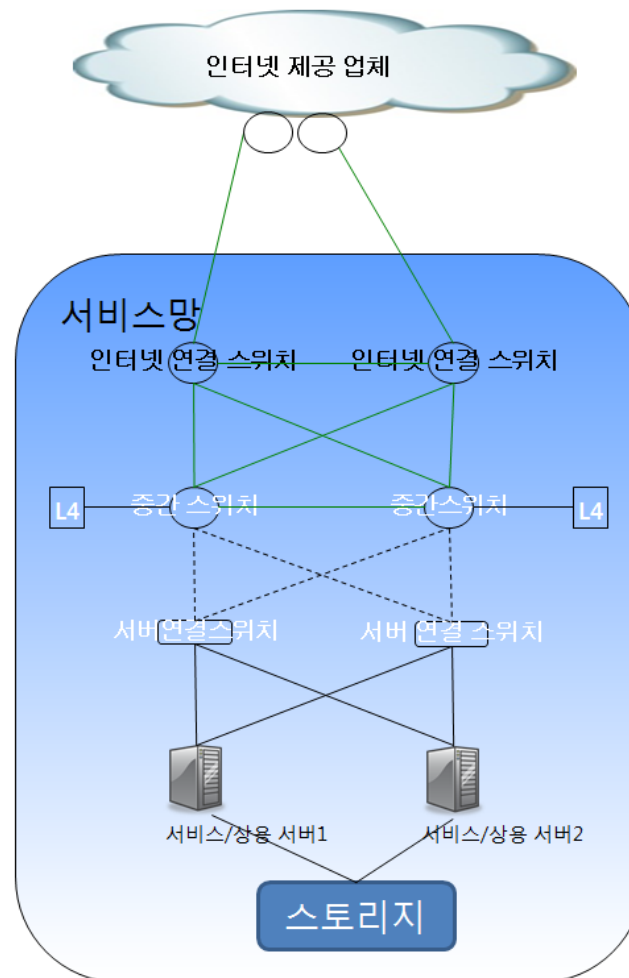
데이터 저장, 기기종 간에 데이터 공유할 때 사용



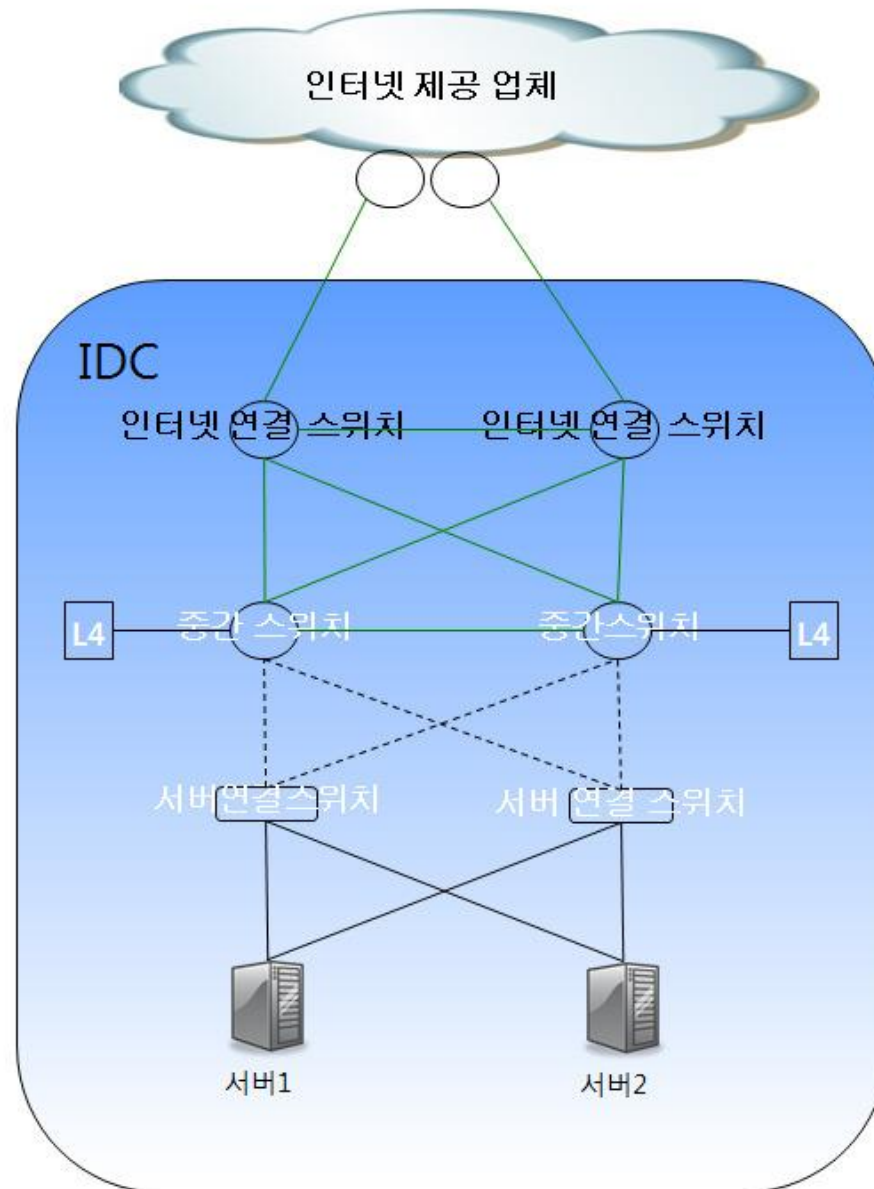
17. 스토리지2

SAN

높은 신뢰성, 빠른 전송, DB 이중화 시 사용된다.
고비용이 발생한다.

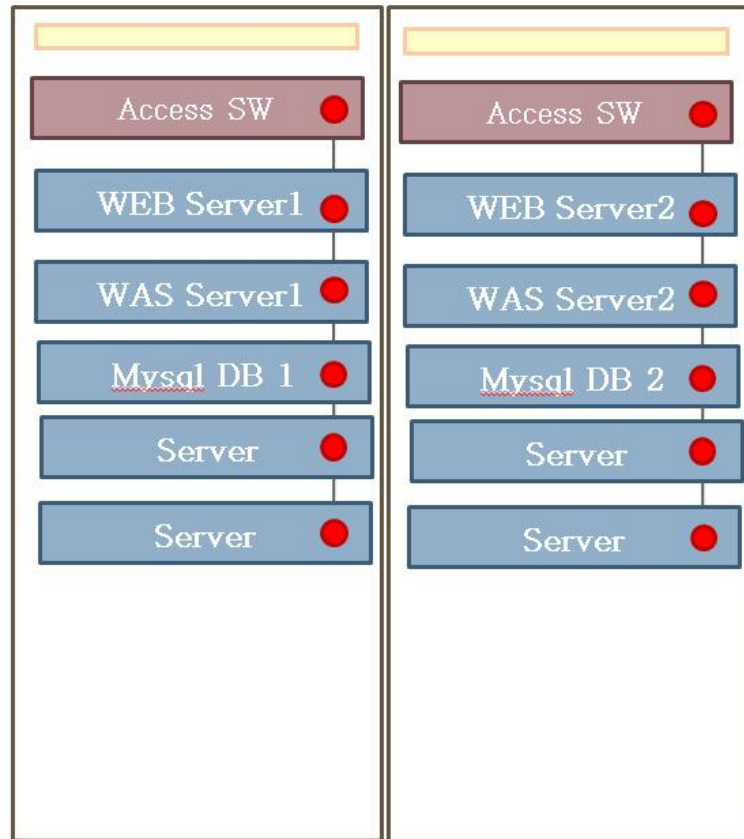


18. 인프라 구성



15. 서버 HW설치

랙에 서버 연결 스위치에 설치 된다.(L2 스위치 = Access SW라고 한다)
웹서버, WAS 서버, DB서버 이중화를 위해 물리적으로 2개 랙에 분산 배치하도록 한다.
스위치가 죽더라도 서비스가 계속되어야 하기 때문에 분산 배치를 한다.
전원은 이중화 되어 있으므로, 스위치나 서버도 이중화된 전원에 각각 연결한다.
전원은 1개 랙에 이중화 됨



16. OS 설치

Linux와 Windows가 설치된다.

Linux는 Rocky Linux가 주로 설치된다.

17. IT 서비스 오픈 전/후 문서화 해야 할 내용

1. 담당자 정보
2. 서비스 구성도
3. 서버 리스트, 서버 군별 특성
4. 연동 구성
5. 애플리케이션 정보 / 설정 최적화 확인
6. 데몬 재시작법
7. 모니터링 등록
8. 이중화 테스트
9. DB 백업

18. 대규모 네트워크 서비스망

장비

요즘은 라우터 대신 라우팅 기능을 포함한 L3 Switch로 구성된다.
L3 Switch를 라우터로 보면 된다.

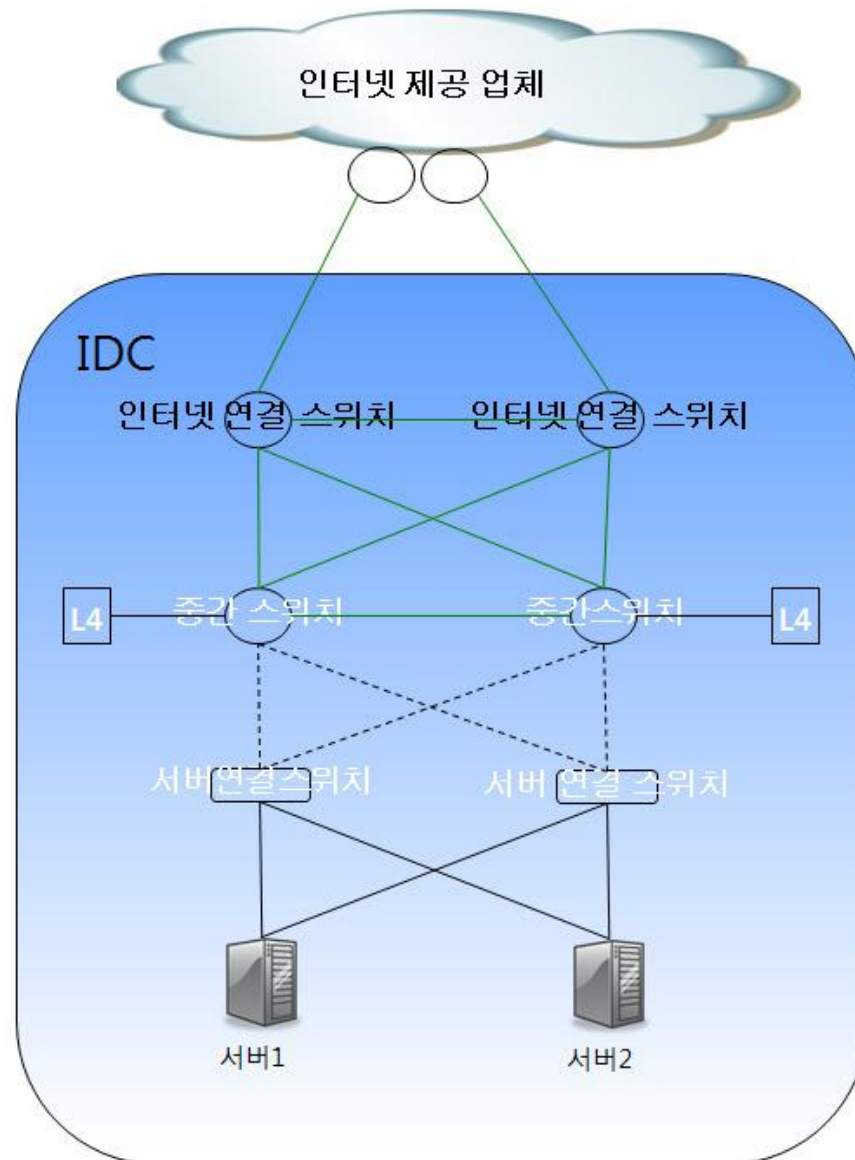
네트워크 레이어

대부분 3 계층 구조로 구축된다.

상세구조

1. 인터넷 연결 스위치 = L3
2. 중간 스위치 = L3
3. 서버 연결 스위치 = L2
4. L4 스위치 = 대규모 처리를 위해 일반적으로 DSR구성을 한다.
// DSR는 다이렉트 서버 리턴, L4를 거치지 않고 바로 데이터를 리턴 한다.

19. 대규모 네트워크 서비스망



20. 서비스망내에서 구분

서비스망 내에서의 네트워크 구성.

1) 서비스망은 WEB 영역, WAS 영역과 DB 영역으로 구분한다.

2) WEB 영역은 DMZ 라고도 하며, 외부에서 접속가능한 영역이다.

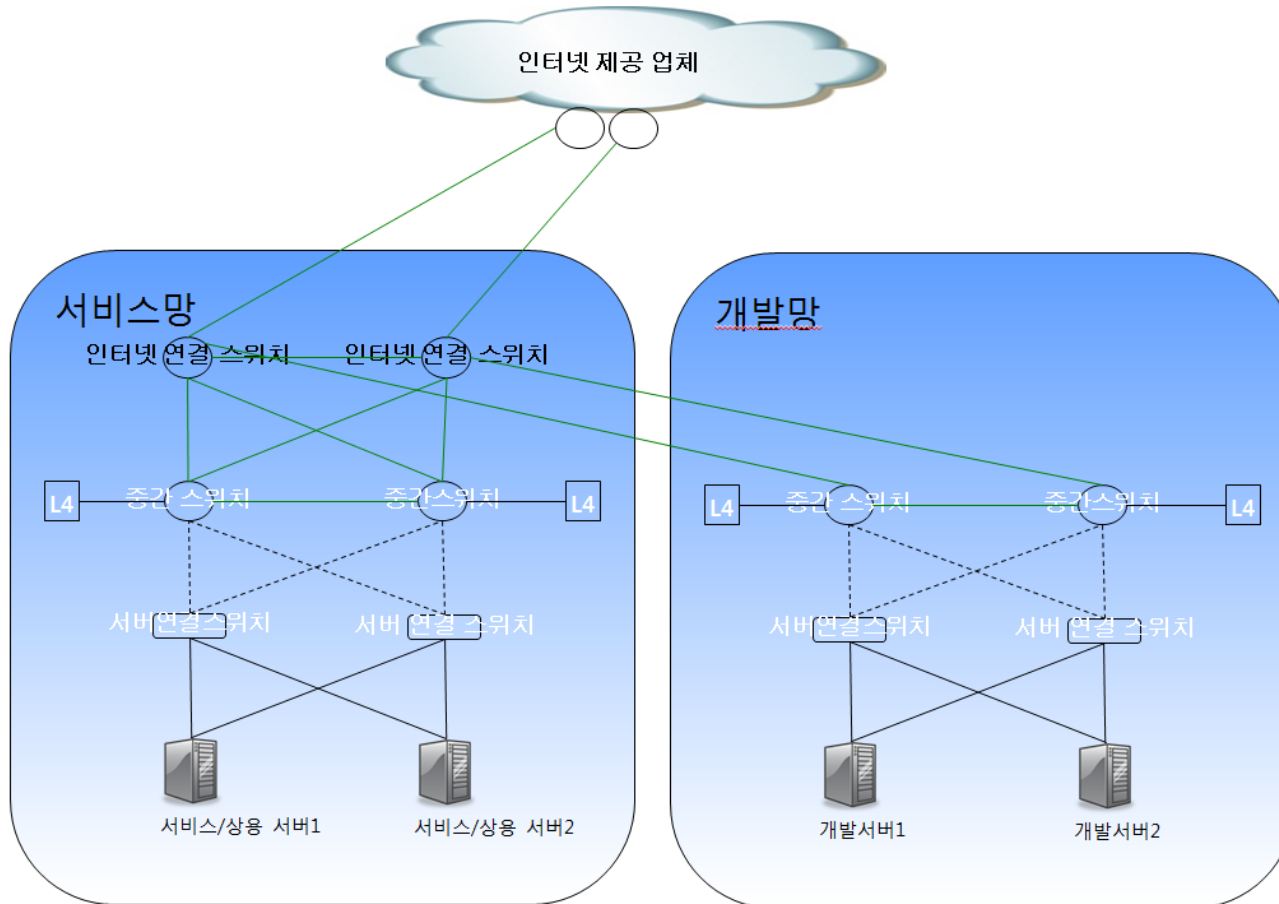
전자금융거래법에서는 외부에서 직접 접속하는 DMZ Zone(WEB Zone)와 외부에서 직접 접속할 필요 없는 네트워크(DB)는 구분해 구성해야 한다고 되어 있다.

3) DB는 사설 IP로 보안관리상 인터넷이 안되는 영역으로 구성한다.

21. 망 구분

1. 대규모 네트워크 운영하는 기업에서는 네트워크 망이 분리 되어 있다.
2. 서비스망과 개발망, 2개로 구분해 운영한다.

보안을 위해 인터넷 연결 스위치 앞단에 보안장비들이 구축되어 있다.
개발망은 저렴한 스위치 장비로 구축하여 비용절감을 한다.



22. 스테이징은 서비스망에 놓아, 실서비스와 거의 동일

개발망에 놓기도 한다.

스테이징 서버 위치는 회사 정책으로 정한다.

서비스망 or 개발망 어디로 할지 결정해 운영하면 된다.

단지, 스테이징 서버에 개인정보가 있으면 서비스망에, 개인정보가 없다면 개발망에 놓는 것을 권장한다.

개인정보 유출되면 망한다.

23. DNS 구축과 구성 알아보자

네트워크만큼이나 중요하고 장애가 생기면 전체 서비스가 멈추는 것이 DNS 서비스이다.
초기 구축 시 아키텍처 설계가 아주 중요한 시스템이다.

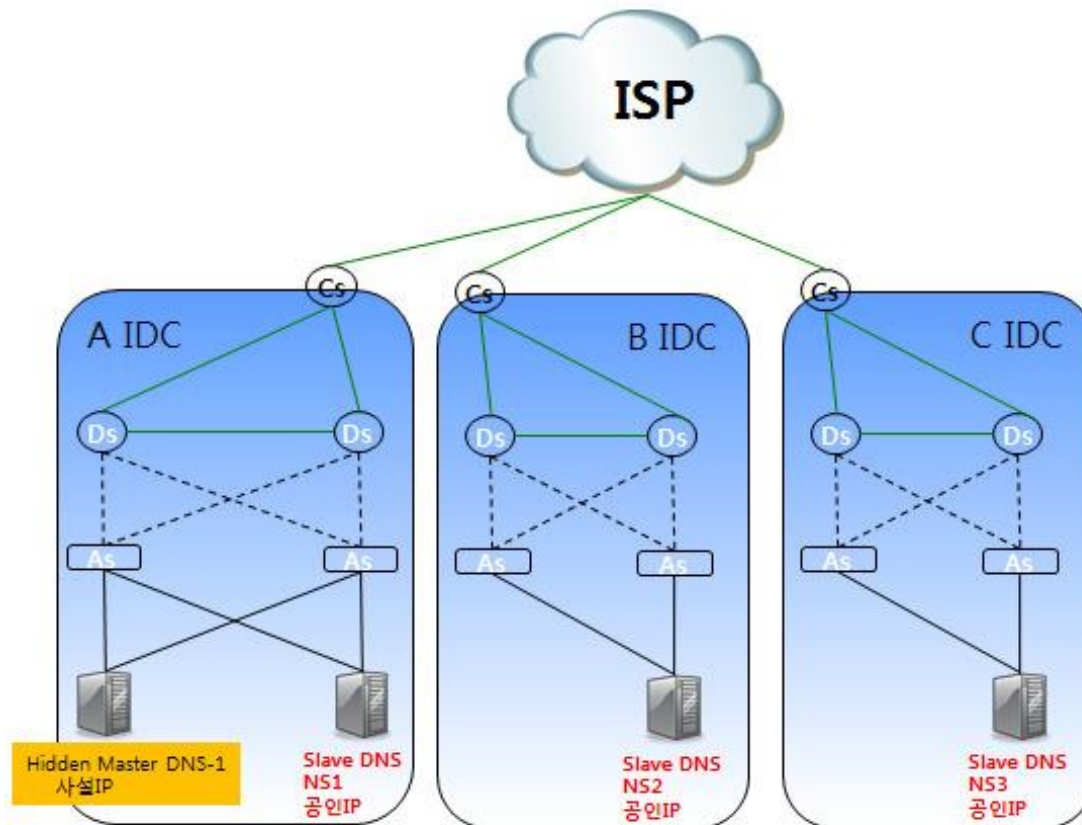
- <1> DNS 구축하기
- <2> DNS 네임서버 몇 대가 정답일까?
- <3> DNS 구축시 추가로 고려해야 하는 것
- <4> 네임서버 구성은 어떻게 하는 게 좋을까?
- <5> 기업별 네임서버수는 도메인을 넣어보면 알 수 있어요 ^^

24. DNS 구축하기

1

DNS는 네임서버와 Cache DNS 2종류가 있다.

여기서는 도메인을 관리하는 DNS 네임서버 구축법에 대해 설명한다.
Cache DNS는 서버나 PC가 DNS로 지정하는 DNS서버이다.



25. DNS 네임서버 몇 대가 정답일까?

1

DNS 네임서버는 일반적으로 2대는 기본으로 구축해야 한다.
1대 운영하다 장애가 생기면 전체 서비스가 중지되기 때문이다.

2

그럼 2대가 정답인가?

대규모 서비스를 운영하는 기관은 보통 3~5대로 구축해서 운영하고 있다.

네이버는 3개 세트, Google은 4개 세트로 운영하고 있다.

보이는 네임서버가 3~5개라는 것이다.

보이는 것 1개 네임서버로 표시된다.

그러나, 실제로 L4 VIP를 사용해 서버는 여러 대이다.

26. Google 네임서버를 보자 ~

4개이다.

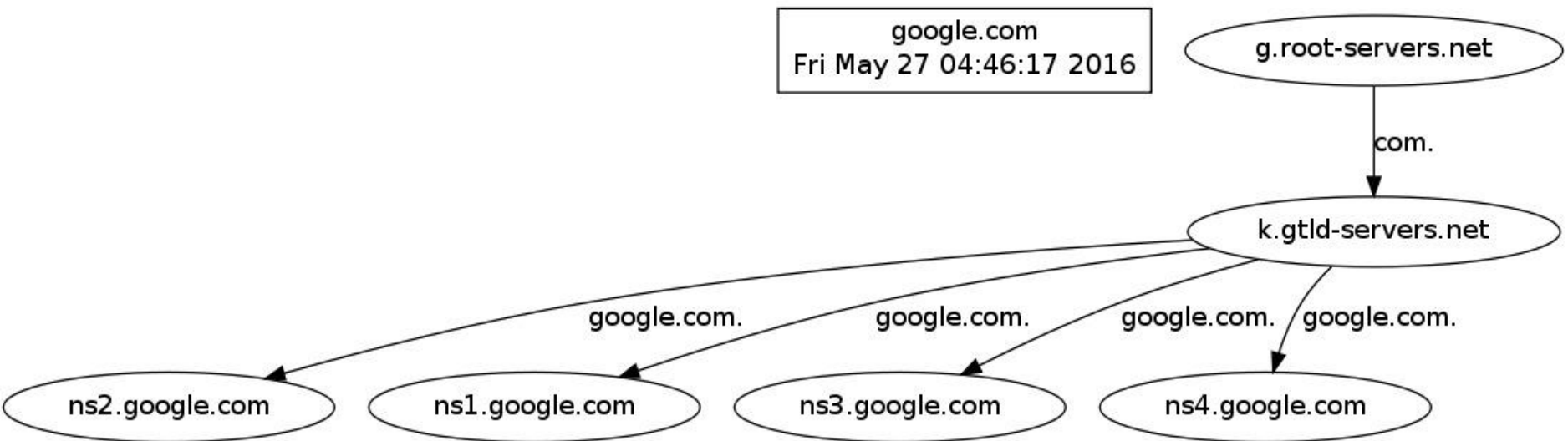
대표 IP가 4개이라는 것이다.

4곳의 위치에 있다.

서버가 4대라는것이 아니다.

대표 IP가 4개는 로드밸런서이다.

로드 밸런서 아래에 DNS서버 수백대가 있다.



27. DNS 구축 시 추가로 고려해야 하는 것

1

대규모 서비스 운영 시 초기 구축 시 고려해야 하는 사항 몇 가지를 적어본다.
필수는 아니고 권고사항이다. 회사마다 사정이 다 틀리기 때문이다. ^^

2

네임서버는 2대 이상으로 운영해야 한다. 3대~5대

3

DNS 서버 2대를 서로 다른 네트워크 장비에 연결해야 한다.

4

다른 네트워크 IP 블록을 가져야 한다.

5

물리적으로 서로 다른 IDC에 구축한다.

6

DDOS 공격받으므로 앞단에 방화벽이 있는 구성을 권장한다.

28. 네임서버 구성은 어떻게 하는 게 좋을까?

1

보안상 Master는 Hidden으로 사설 IP로 구성한다.

2

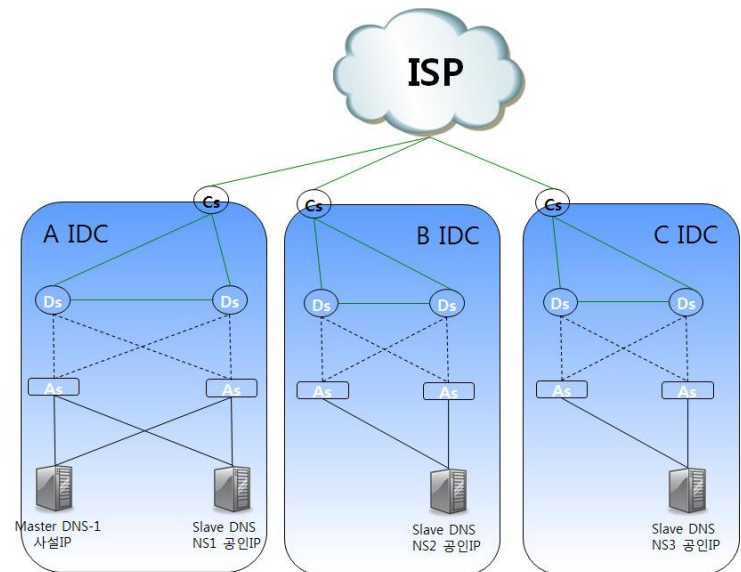
Slave는 공인 IP로 네임서버로 구성한다. 예) NS1 , NS2 , NS3

3

참고

1) 네임서버는 Master와 Slave로 구성된다.

2. Master만 정보를 변경할 수 있으며, Master 정보가 변경되면 Slave는 정보를 업데이트해 가는 방식으로 운영된다.



29. 기업별 네임서버수는 도메인을 넣어보면 알 수 있어요 ^^

구글? 페이스북? 애플? 아마존? 이 궁금하면 도메인을 넣으세요~

<http://www.zonecut.net/dns/>

30. CDN 서비스 이해와 운영 기술

콘텐츠를 잘 운영하기 위한 것 중 하나인 CDN에는 어떤 서비스가 있고, 어떤 기술이 있는지 보자.

<1> CDN 이란?

<2> 콘텐츠 종류는?

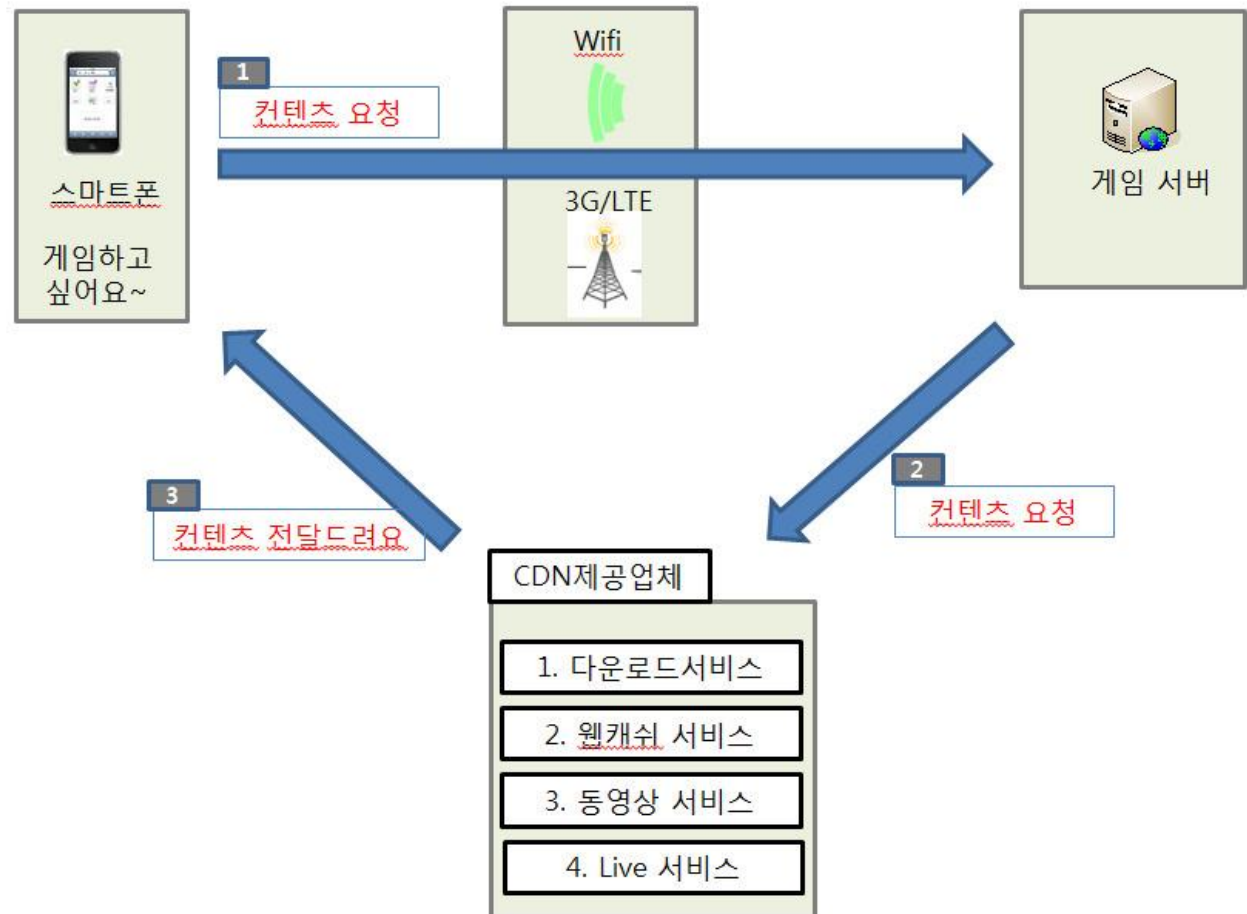
<3> CDN을 왜 쓸까?

<4> CDN에는 어떤 종류의 서비스가 있는지 알아보자

<5> CDN 기술

31. CDN이란?

콘텐츠를 배달하는 네트워크



32. 콘텐츠 종류는?

게임 콘텐츠, 만화, 영화, 뮤직, 이미지, 동영상, 라이선스 서비스 콘텐츠 등이 있다.

게임 다운로드

만화, 이미지 등 영상

33. CDN을 왜 쓸까?

- 대규모 서비스를 운영하다 보면, IDC의 로컬 회선이나 네트워크만 가지고 서비스하기가 힘들다.
- 사용자에게는 더 빠른 서비스와 안정적인 서비스 제공이 필요하다.
- CDN을 이용하면 사용자 입장에서 가장 가까운 데서 다운로드하게 되므로 빠르게 하기 위해 쓴다.
- 로컬 회선을 사용은 것보다 비용절감 효과가 있을 때 사용하게 된다.
- 게임 콘텐츠나 이미지 등을 로컬 회선으로 다운로드하기 힘들 만큼
- 데이터가 클 경우 사용한다.

34. CDN에는 어떤 종류의 서비스가 있는지 알아보자

대표적인 CDN 서비스 4가지

다운로드 서비스

웹캐시 서비스

동영상 서비스

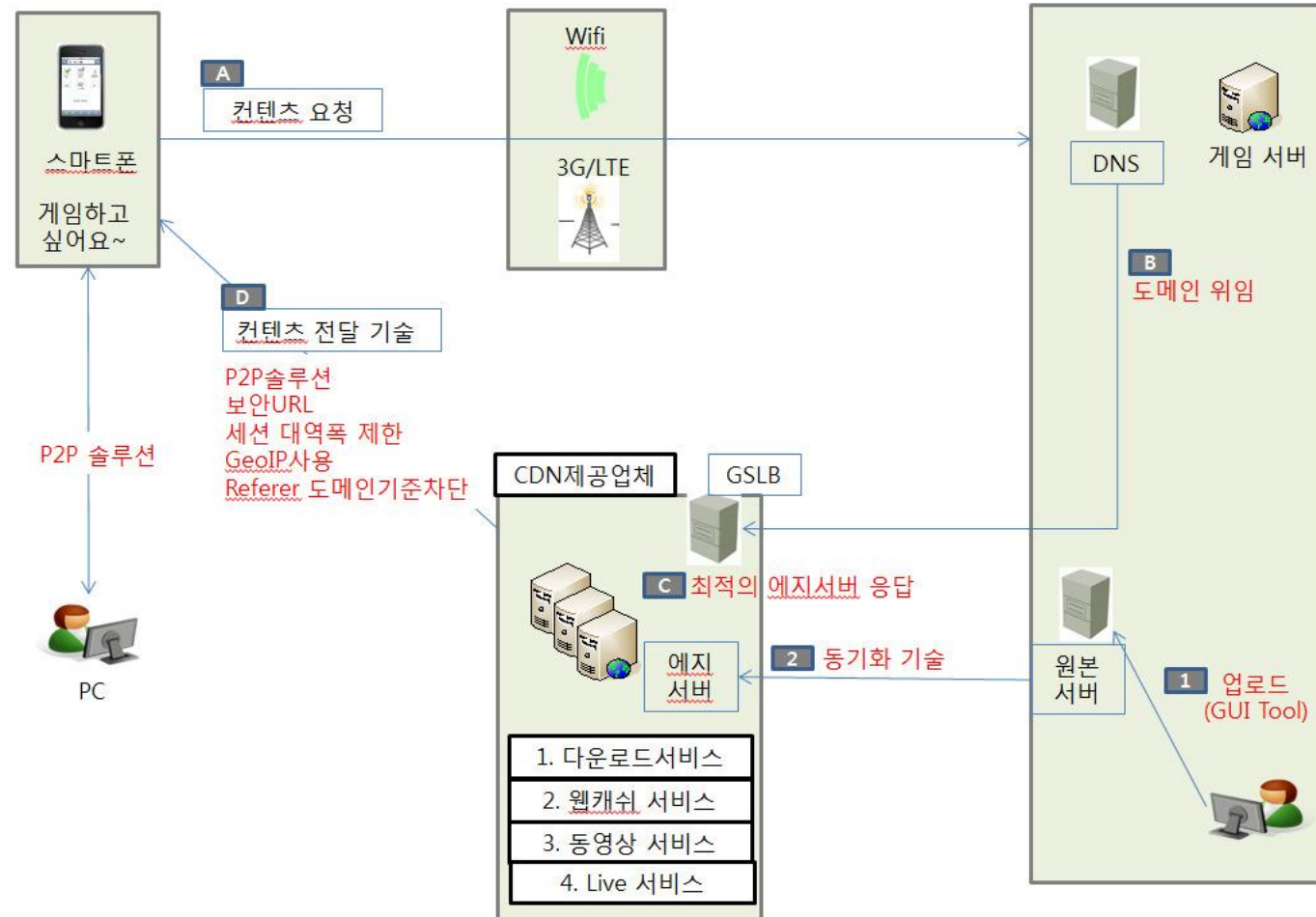
LIVE 서비스

요즘은 라이브 서비스 많이 사용한다.

쇼핑몰등 라이브 방송

35. CDN 기술

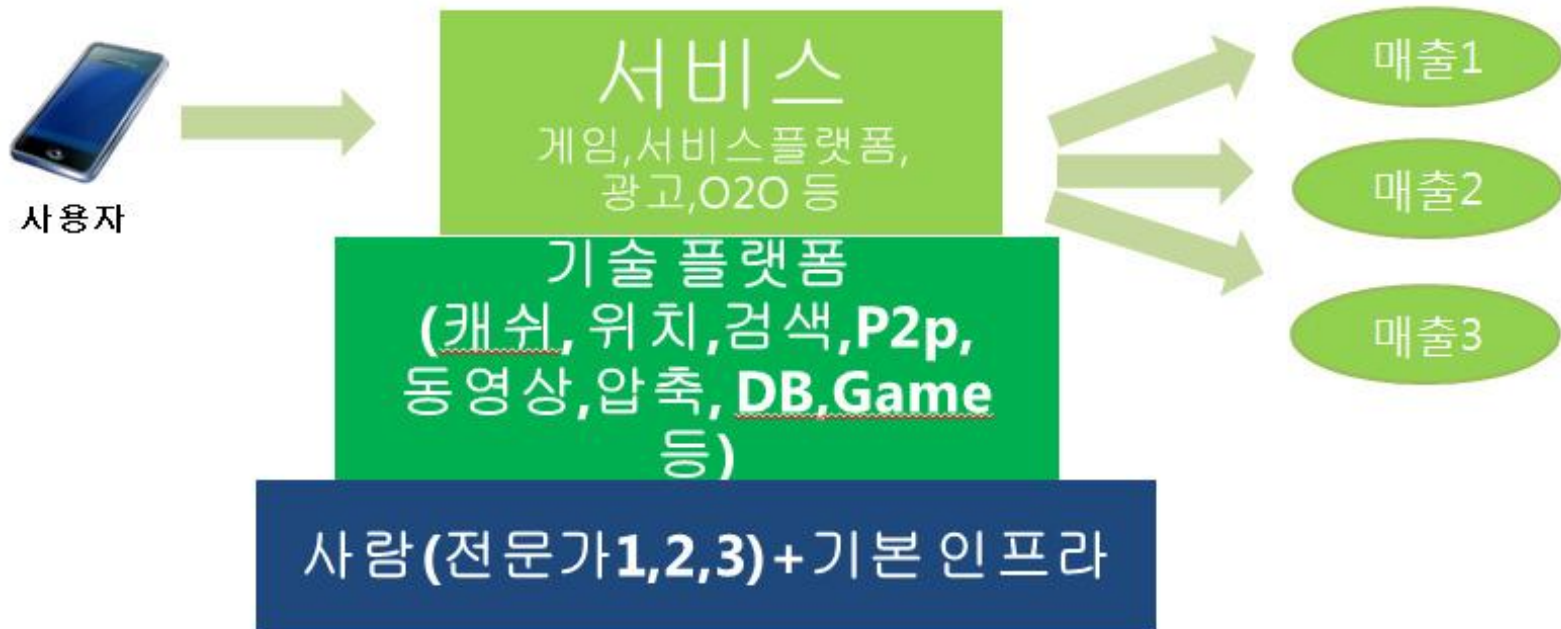
DNS 운영기술 / GSLB 최적의 에지 서버 응답기술 / 콘텐츠 업로드 툴 / 동기화 기술
P2P 솔루션 기술 / 보안 URL 기술 / 세션 대역폭 제한 기술 / GeoIP사용 국가별 차단 기술 /
Referer 도메인 기준 차단 기술 / 콘텐츠 압축기술 / 글로벌 가속 서비스 / https 전송기술 등이 사용된다.



36. 기술 플랫폼을 공부하고 적용하라!

대규모 서비스를 운영하기 위한 핵심 기술인 기술 플랫폼에 대해 간단히 소개하고자 한다.

대규모 서비스하는 곳에서는 기술 플랫폼이 있었다.
지금 클라우드로 이야기하면, Pass와 SaaS 서비스에 해당된다.



37. 기술 플랫폼이란?

1. 사용자가 서비스를 제공받는데 차별화된 서비스를 제공하기 위한 기술들을 얘기한다.

좀 더 빠르고 좋은 서비스를 제공할 수 있게 하는 기술들이다.

2. 구글이 회사를 인수하는 조건중 하나는 내가 하루에 2번 이상 해당 서비스를 이용하는가? 가 있다고 한다.

매출이 많은 기업을 인수하는 것도 아니다.

사용자 입장에서 하루에 2번 이상 들어가는 서비스~

서비스가 좋아야 하는데, 그 서비스의 기반이 되는 부분이 기술 플랫폼 들이다.

3. 기술 플랫폼 예)

응답이 빠르고 이미지가 빨리 뜨게 하는 캐시

사용자 위치를 파악해 최적화된 서비스를 제공하는 위치기술

모르면 검색해서 찾을 수 있게 하는 검색 기술

생동감 넘치는 영상을 최적화해서 제공하는 동영상 압축 기술

성능을 높이는 DB기술, 각종 게임 기술 플랫폼 등이다.

38. 사람이 필요한 기술 플랫폼

1
전문가가 필요하다.
IT서비스는 사람이 만들고 사람이 운영한다.
회사에 핵심 전문가 몇 명만 있어도 매출엔 이상이 없다.
해당 인원이 1명당 100을 하는 경우도 있다.

2
회사에 전문가 10명은 양성하라~
그 전문가들이 사내에서 또 전문가를 만들어 내면,
다양한 10개 서비스에 대해 빠르게 대응하고 서비스를 키울 수 있다.
이것이 회사가 직원을 Care 해야 하는 이유이다.

39. 업무 요청 처리 시스템은 필수다.

현황

일반적으로 업무 요청은 메일로 많이 하게 된다.

하지만 메일이 많이 오게 되는 경우는 누락이 되어 답변을 못하게 되는 경우가 있다.

문제점

중소기업에서는 메일이나 사내 메신저로 처리가 가능하다.

하지만, 하루에 수십 통의 메일이 오는 경우, 회신을 하다 보면 수백 통의 메일이 날아다니게 된다.

이 경우 처리에 누락이 생길 수밖에 없다.

개선 방향

대규모 인터넷 업무처리를 하는 기업들에서는 업무 요청 처리 시스템으로 접수를 받아 누락 없이 처리하고 있다.

이를 프로세스적으로 해결하기 위해 '업무 요청 처리 시스템'을 만들고 사용하게 된다.

40. 업무 요청 처리 시스템중 하나인 JIRA 좋다!

The screenshot displays the JIRA web interface. At the top, there's a navigation bar with 'JIRA' logo, 'Dashboards', 'Projects', 'Issues', 'Agile', and a 'Create' button. A search bar is on the right. Below the navigation bar, there's a 'Search' section with a 'Save as' button and filters for 'Project: All', 'Type: All', 'Status: All', 'Assignee: All', and 'Contains text'. A 'More' button and 'Advanced' link are also present. On the left, a sidebar shows a list of tasks under 'Order by', including 'MA-9 New Task 1 (Medini Analyze -> ...)', 'MA-8 Task for Test 1', 'MA-7 Test Task 1', 'MA-5 Medini Analyze -> JIRA test4', 'MA-4 Medini Analyze -> JIRA test3', 'MA-3 Medini Analyze -> JIRA Test2', 'MA-2 Medini Analyze -> JIRA Test1', and 'MA-1 Ticket'. The main content area shows the details of 'New Task 1 (Medini Analyze -> JIRA)'. It includes a toolbar with 'Edit', 'Comment', 'Assign', 'More', 'Start Progress', 'Done', and 'Admin'. The 'Details' section shows 'Type: Task', 'Priority: Medium', 'Status: TO DO (View Workflow)', and 'Resolution: Unresolved'. The 'Description' section contains the text: 'Severity를 기존의 1에서 2로 변경' and 'Navigate the following link to the related element platform/resource/Airbag/his/_TqZ7UG3kEeGyZ5eYIZakUA.ha#_6A5TEG36EeGyZ5eYIZakUA'. The 'Activity' section shows 'All', 'Comments', 'Work Log', 'History', and 'Activity' tabs, with a message: 'There are no comments yet on this issue.' On the right, the 'People' section shows 'Assignee: Unassigned (Assign to me)', 'Reporter: chungshinhoon@gmail.com', 'Votes: 0', and 'Watchers: 1 (Stop watching this issue)'. The 'Dates' section shows 'Created: 1 minute ago' and 'Updated: 1 minute ago'. The 'HipChat discussions' section has a link: 'Do you want to discuss this issue? Connect to'.

41. 업무 요청 처리 시스템중 하나인 JIRA 좋다!

1. 업무 요청 처리 시스템에 등록되면,
누락 없이 처리를 하는 기반이 마련되는 것이다.
요청 담당자는 업무에 맞는 처리를 하면 된다.
2. 인프라의 업무 요청은 6가지 정도는 필수다.
 - 1) 서버에 대한 업무 요청
 - 2) DB에 대한 업무 요청
 - 3) 네트워크에 대한 업무 요청
 - 4) 스토리지 업무 요청
 - 5) 보안에 관련한 업무 요청
 - 6) 기타 업무 요청
3. 프로세스
프로세스는 뒷단의 처리자가 필요한 내용만 전달하면 된다.

42. 서비스 코드, 자산관리, CMDB 알아야 한다.

네이버와 대기업을 거치며 경험한 인프라 운영 경험을 공유한다.

좋은 레퍼런스로 참고되었으면 해서 적어본다.

많은 기업이 큰 회사는 인프라가 잘 되어 있으리라 생각하지만, 실제로 들여다보면 사람에 의존하거나 관리가 되지 않는 기업이 많다.

대규모 시스템을 잘~ 운영하기 위한 3가지 시스템에 대해 이야기해보려 한다.

<1> 서비스 코드

<2> 자산 관리시스템

<3> CMDB

43. 서비스 코드

서비스 코드는 서비스명을 관리하는 시스템이다.
서비스가 정의되어야 인프라는 그다음에 따라가는 것이다 ~~

서비스코드	서비스 소개	사업부서	개발부서	서비스 생성일
카카오게임서비스 > 슈퍼스타 테니스	테니스 게임			
카카오게임서비스 > <u>프렌즈</u> 맞고	<u>고스돌</u> 게임			
카카오게임서비스 > <u>프렌즈런</u>	달려가며 아이콘 먹는 게임			

44. 서비스 코드

서비스 코드는 4가지 정도로 이용된다.

1) 서비스 상태를 한눈에 알 수 있다.

서비스명이 뭔지, 언제 생성되었는지, 개발부서, 사업부서가 누구인지 등 관리된다.

2) 사업부서, 개발부서와 운영부 서간에 커뮤니케이션 용도(서비스 이름)로 사용된다.

3) 운영비용에 대해서는 각 사업부에 배부되는데 이때, 해당 서비스 = 해당 사업부로 매칭이 가능하므로 해당 사업부에 잘 배부가 된다.

4) 서비스 코드와 CMDB매칭을 통해 해당 서비스를 하는데 들어가는 인프라서버수등을 한눈에 알 수 있다.

45. 자산 관리시스템

서버 구매 후 자산이 어디 있는지 관리하는 시스템이다.

서비스 정의된 다음에 이제 서버를 사면 관리가 되어야겠지요~

자산은 나중에 감사 대상이 된다.

구매했는데 어디 있나요???

회계시스템과 자산 관리시스템은 연계되어야 한다.

일반적으로 서버, 네트워크 장비, 스토리지, 기타 설비가 구매된다.

구매 시 서버도 1대만 구매가 되는 게 아니고 여러 대 구매된다.

구매 기안은 1건이라 해당 장비들과 모두 매핑하는 게 중요하다.

자산관리번호	자산유형	사용상태	위치

46. CMDB

1
Configuration Management Database

구성관리 데이터 베이스
운영 DB를 이야기한다.

2
인프라 운영을 하기 위한 가장 기본적인 정보를 가진 시스템이다.
자산 정보를 기반으로 실제 운영을 하기 위한 모든 정보를 가지고 있는 DB이다~
서버, 네트워크, 스토리지 장비 리스트라고 보면 된다.

자산관리번호	자산유형	사용상태	위치	<u>호스트명</u>	IP

47. CMDB는 6가지 정도로 활용이 된다.

1) 자산관리

장비가 어디에 있는지 해당 서버를 물리적 위치를 기록한다.
자산은 회계 감사의 중요한 부분이 된다.

2) 실제 운영시 사용

인프라 운영에 대한 모든 기본 정보가 기록되어 운영에 활용된다.
서버 사양, 담당자 정보, 설치 시기, 유지보수 정보 등

3) 사용 비용 배부에도 사용된다.

해당 서버를 어느 부서에서 요청해 설치되었는지 확인되어, 운영비용도 해당 부서에 배부하게 된다.

48. CMDDB는 6가지 정도로 활용이 된다.

4) 보안 부분에서도 많이 요청이 된다.

해당 서버에 어떤 애플리케이션이나 라이브러리가 설치되어 있는지 필드 만들어 관리하기도 한다.

5) 모니터링

대상에 대해서도 누락이 없는지 해당 리스트로 점검을 할 수 있다.

6) 자료 요청 대응

해당 데이터를 다운로드하여 EXCEL 피벗 기능을 이용하면 원하는 인프라 정보는 대부분 얻을 수 있다 ^^

49. 변경과 장애 관리 시스템은 필수다

- 작업에 대해 공유하고, 같이 모니터링하기 위한 '변경관리 시스템'
- 장애를 빠르게 전파하여 빠른 장애처리를 하기 위한 '장애 전파 프로세스'
- 장애이력 관리와 장애 후 개선, 재발방지를 진행하는 '장애 관리 시스템'에 대해 이야기하도록 하겠다.
- ISMS-P나 전자금융거래업에서 장애 이력과 조치내역 완료에 대해 제출하는 게 필수다!
- 대규모 서비스를 운영하기 위해서는 필수 법적 요건이다

50. 변경관리시스템

1

개발부서나 인프라 부서에서 작업에 대해, 유관 서비스 담당자들에게 서로 공유가 되도록 하는 시스템.

2

변경작업에 대해 공유가 됨으로 서비스 장애 시 원인이 빠르게 확인되어 조치될 수 있다.

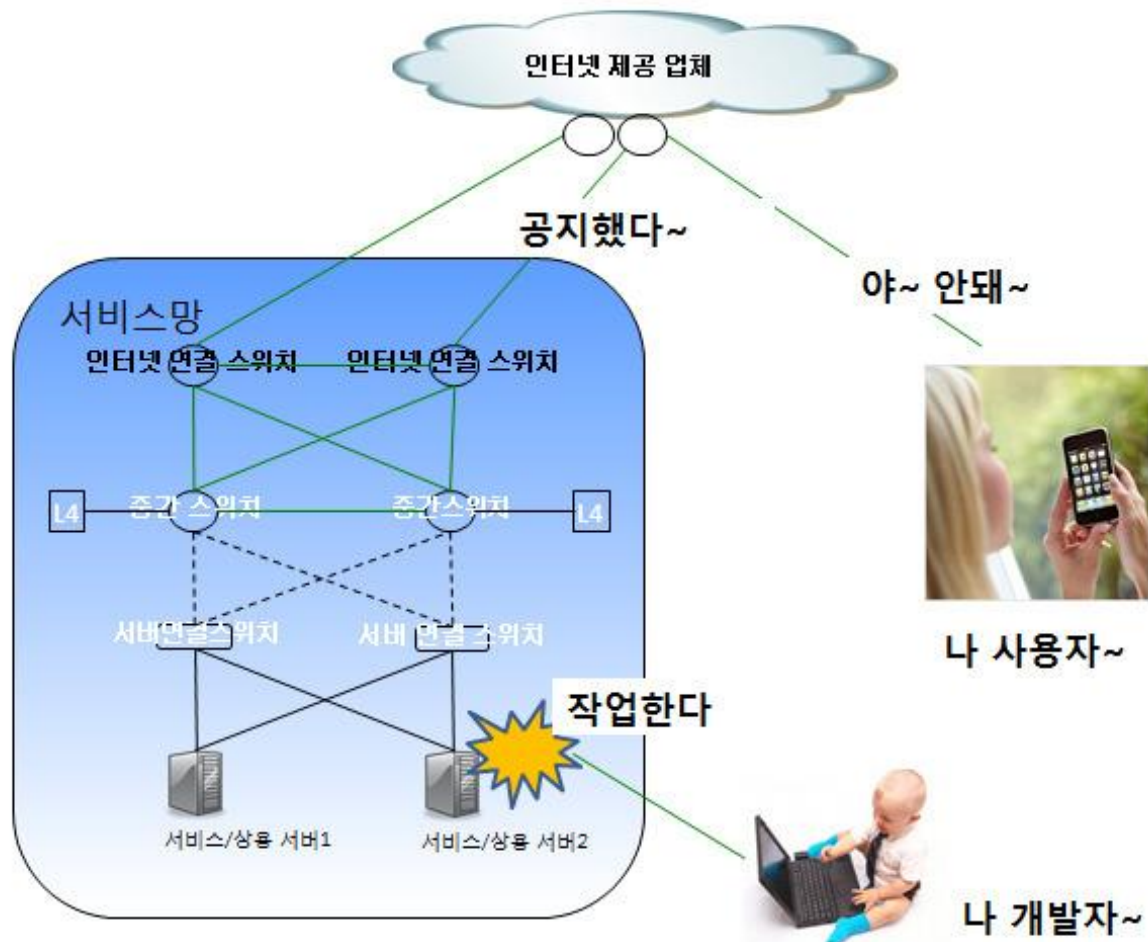
작업하는 서비스의 서비스코드를 지정하면,
해당 서비스 관련 모든 부서 담당자에게 동시에 공유되는 시스템.

예를 들어, A게임서비스 작업을 한다고 서비스코드를 지정하고, 예정 작업을 등록한다.

해당 서비스코드 담당자로 등록되어 있는 인원에게 자동 공유된다.

변경관리시스템에 등록을 하면 Outlook으로 일정 공유되면 변경작업 인지가 쉬웠다.

51. 변경관리시스템



52. 장애 전파 프로세스

1

장애 발생 시 담당자에게 SMS전파하여 빠른 장애처리가 되도록 하는 시스템.

2

프로세스

- 1) 서비스모니터링 시스템을 이용해 24시간 모니터링 중인 근무자가 이벤트 인지
- 2) 실제 장애인지 PC나 스마트폰으로 재현테스트
- 3) 서비스 장애 발생로 확인되면, 장애전파 시스템을 통해 담당자(사업/개발/인프라/유관부서)에게 전파
- 4) 전파받은 개발/인프라 담당자는 원인을 찾아 서비스복구가 되도록 조치한다.

3

역할

- 1) 24시간 모니터링하는 인원은 장애 발생/진행경과/조치완료에 대해 전파되도록 해야 한다.
- 2) 각 담당자는 장애 전파시스템에 본인 담당 서비스에 대해서는 본인이 직접 담당자로 등록한다.
장애처리 시스템에 해당 서비스에 대해 개발, 인프라 담당자 직접 수정할 수 있도록 되어 있어야 한다.
- 3) 장애관리담당자는 모든 서비스에 담당자가 지정되도록 공지를 하여 담당자 관리가 되도록 해야 한다.

53. 장애 관리시스템

1

장애 발생 후 장애 이력관리와 장애 후 개선 결과 입력하는 시스템.

2

목적

- 1) 장애 후 미팅은 장애원인을 파악하고, 동일 장애가 발생되지 않도록 개선하는 것을 목적으로 해야 한다.
- 2) 장애관리담당자는 장애 후 개선필요 부분에 대해 각 담당자에 티켓으로 할당하여 결과를 받도록 한다.
- 3) 장애관리자는 장애 이력과 개선결과 꼭 확인하도록 한다. 장애관리는 내부/외부기관의 감사 대상.
- 4) 전자금융거래법(이하 전금법)에서는 중요장애의 경우는 금감원에 보고하도록 되어 있다.

54. 모니터링 시스템에 대한 구분

모니터링은 서버 모니터링과 서비스 모니터링 2가지가 있다.

1) 서버모니터링

서버 여러 대중 1대라도 죽는 경우 모니터링하는 것을 말한다.

2) 서비스 모니터링

사용자 입장에서 서비스가 안 되는 경우 모니터링하는 것을 말한다.

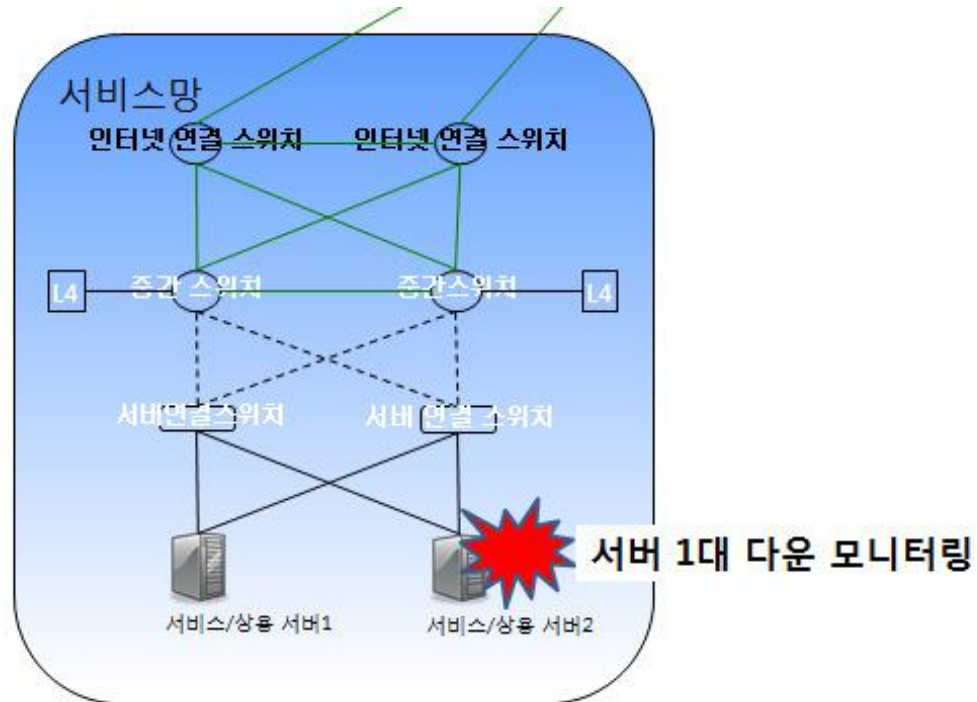
일반 기업은 서버 모니터링을 하고 있으나, 서비스 모니터링 부분이 부족한 경우가 많다.

왜냐하면, 서비스 모니터링하기 위해서는 전담 모니터링 조직과 전용 모니터링툴, 개발부서의 많은 지원이 필요하기 때문이다.

서버를 모니터링하는 것과 서비스를 모니터링하는 것은 다르다.

55. 서버 모니터링

1. 서버 여러 대중 1대라도 죽는 경우 모니터링하는 것을 서버 모니터링이라 한다.



56. 대규모 네트워크 서비스망

2

용어 통일

서버가 전원문제등으로 다운될 시 '서버 1대 다운이 발생했다' 또는 '서버 1대 폴트(Fault)가 발생했다'라고 이야기하기로 하자.

서버 장애가 발생했다고 하지 말자.

장애는 서비스가 안 된 경우 장애라고 하도록 하자.

3

모니터링 인원

IDC에 24시간 근무하는 OP근무자가 서버 물리적인 다운이나 애플리케이션 다운을 모니터링한다.

4

모니터링 툴

이를 모니터링하는 툴은 주로 자빅스, 나기오스, 자체개발 에이전트 등을 사용한다.

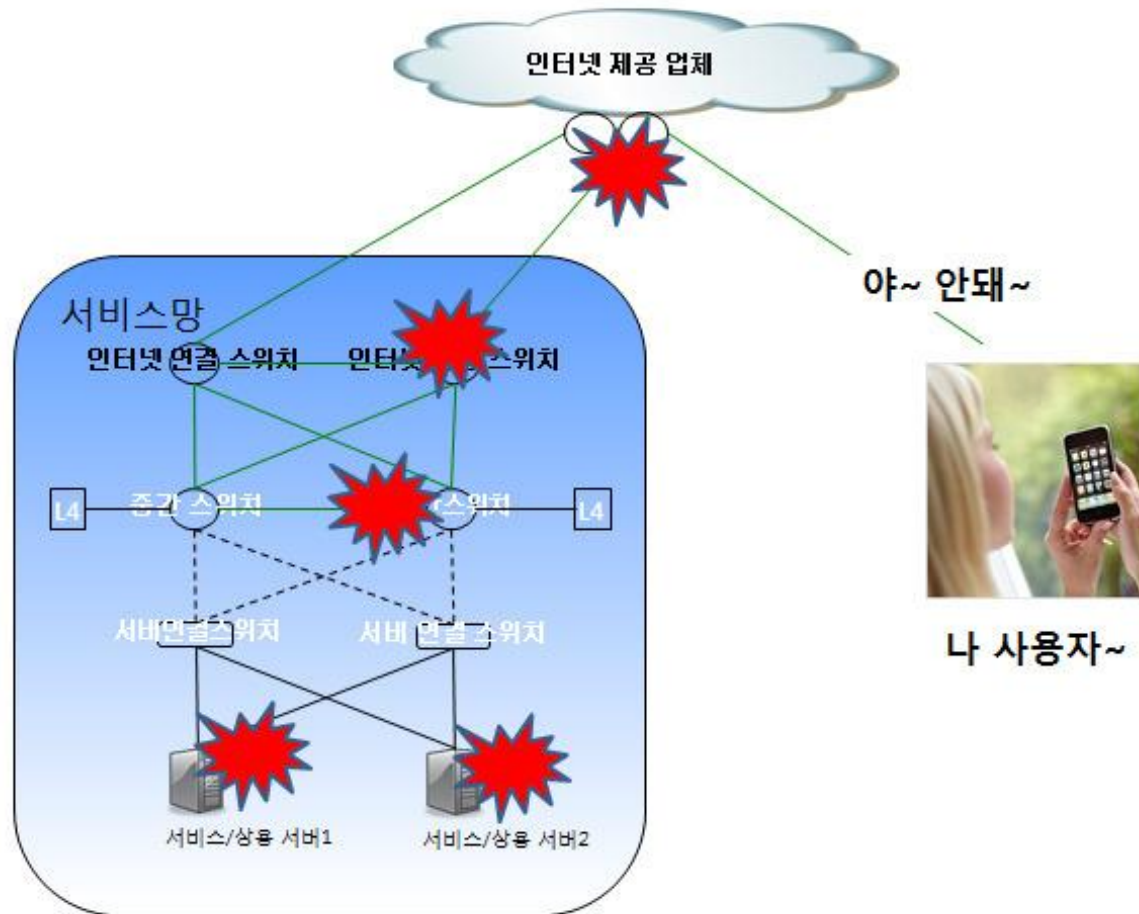
보통 서버에 에이전트를 설치하는 방식을 사용한다.

자빅스(Zabbix) <http://www.zabbix.com/>

57. 서비스 모니터링

서비스 모니터링은?

사용자 입장에서 서비스가 안되는 것을 모니터링하는 것을 서비스 모니터링이라고 한다.



58. 서비스 모니터링

2

서비스 모니터링 예)

- 1) 네트워크장비나 스토리지가 죽어 사용자가 정상 서비스를 받지 못하는 경우
- 2) 애플리케이션 성능장애로 사용자가 정상 서비스를 받지 못하는 경우
- 3) 서버 2 대중 2대가 다 죽어 사용자가 정상 서비스를 받지 못하는 경우

3

모니터인원

- 1) 일반 회사는 24시간 근무하는 IDC OP근무자가 서버와 서비스 모니터링을 같이 한다.
- 2) 대규모 시스템을 운영하는 회사는 전담 서비스 모니터링 조직이 24시간 집중모니터링한다.

4

모니터링 툴

- 1) '서비스 전용 모니터링'툴을 사용한다.
Topaz와 아르고스 등과 같이 사용자단부터 서버까지 모니터링을 하는 툴이용한다.

59. 장애관리 조직 필요성

1

서비스 모니터링과 장애전파 조직은 대부분 사업부 요청으로 만들어진다.

장애가 생겨도 모르고, 조치도 제대로 되고, 장애보고서도 제대로 정리가 안되고, 다음 장애가 안 일어나게 되는지 확인이 힘들기 때문에, 이를 대신해주는 조직이 필요하다.

장애가 반복되면 요청은 더 자주 일어나게 된다.

2

장애가 반복되는 이유

근원적인 조직문제나 비용 문제는 해결하지 않고, 사람이 무조건 해주기를 바라기 때문에 장애는 반복된다.

프로세스적으로 기능적으로 개선이 필요하다.

근본 이유를 찾아내고 재발방지 되지 않도록 개선하는 것이 장애관리 조직의 일이 되기도 한다.

60. 전자금융거래법 통과와 PCI-DSS취득하기

핀테크시대 필수 감사 금감원의 전자거래금융법 감사
PCI-DSS인증 취득
9개 카드사 제휴에 대한 경험을 요약한다.

전자금융거래법이나 PCI-DSS 등은 개인이 잘해서 되는 업무는 아니다.
단지, 개인이 미리 알고 미리 준비하면 한결 수월하게 처리가 될 수 있다.
업무 부서로는 보안부서, 사업부서, 개발부서, 개인정보보호부서, 인사부서, IDC 물리 인프라 관리자,
서버담당자, DB담당자, 네트워크 담당자, 백업 담당자, IDC시설 관리회사(호스팅업체 자료)등 회사의 거의 모든 부서가 대응해야만 잘 처리되는 부분이다.

점검을 받고 나면, 다시 작업해야 하는 부분과 기존 자료를 사용해도 되는 부분이 구분되는 노하우를 얻을 수 있다 ^^

50%는 전금법 내용으로 커버된다.

감사는 항상 급박하고 긴장된 시간을 보내게 되지만, 증거를 사전에 만들어 놓으면 급박함은 줄일 수 있다.

감사에 문제가 되면 과징금, 회사 임원에 대한 징계까지 갈 수 있는 사항이니 미리미리 준비하자~

크게 지적을 안 받으면 성공이다!!

61. 전자거래금융법(이하 전금법) 무사 통과하기

전금법 점검 프로세스

- 1) 사전 자료를 제출한다.
- 2) 방문 심사를 받는다.
- 3) 심사결과가 나온다.
- 4) 결과에 대해 다른 부분은 증적자료로 소명을 한다.
- 5) 지적사항에 대해 개선을 진행한다.
- 6) 개선사항을 다시 보고한다.
- 7) 완료

62. 전자금융거래법 보다 힘든 PCI-DSS 인증 획득하기

1

정의 : 결제 카드 산업(PCI) 데이터 보안 표준

심사 : 글로벌 인증 심사이다.

법규 : PCI 3.2를 따른다(2016년 기준), 엄청 많은 양의 자료와 증거를 요구한다.

일정 : 1년간 진행된다.

2. 진행

1) PCI 3.2를 기준으로 각 담당자와 인터뷰가 진행된다.

2) 갭(GAP)에 대한 분석 보고서가 나온다.

3) 개선한다.

4) 증적자료를 제출한다.

5) 심사를 받는다.

3. 특이사항

서버에 파일의 변경이 일어났을 때 감시하는 기능까지 요구하는 부분이 있다.

파일 변경감시하는 오픈소스를 이용하여 해결하면 된다.

4. 참고사이트 PCI DSS

https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

63. Payment 사업을 위한 9개 카드사 제휴 하기

1

대상 서비스
xxx-Pay 서비스

2

대응

1) 국내 9개 카드사를 제휴하기 위해 해당 기관의 심사 요청에 맞춰 대응해야 한다.

카드사마다 양식이 틀리다. 양식은 좀 통일시켜줬으면 좋겠다.

PPT 몇 백장 작성해 달라는 곳도 있고 --

대부분은 방문하여 심사를 한다.

1곳은 와서 심사를 받으라고 해서 갔다.

2) 카드사별 중점으로 보는 사항들이 있다.

카드사마다 중요하게 보는 게 다르다. 담당자 전공이 다르기 때문이다.

인적 보안문제를 중요시하는 곳도 있다.

3) 전자금융거래법 기준을 충족하면 크게 무리는 없다.

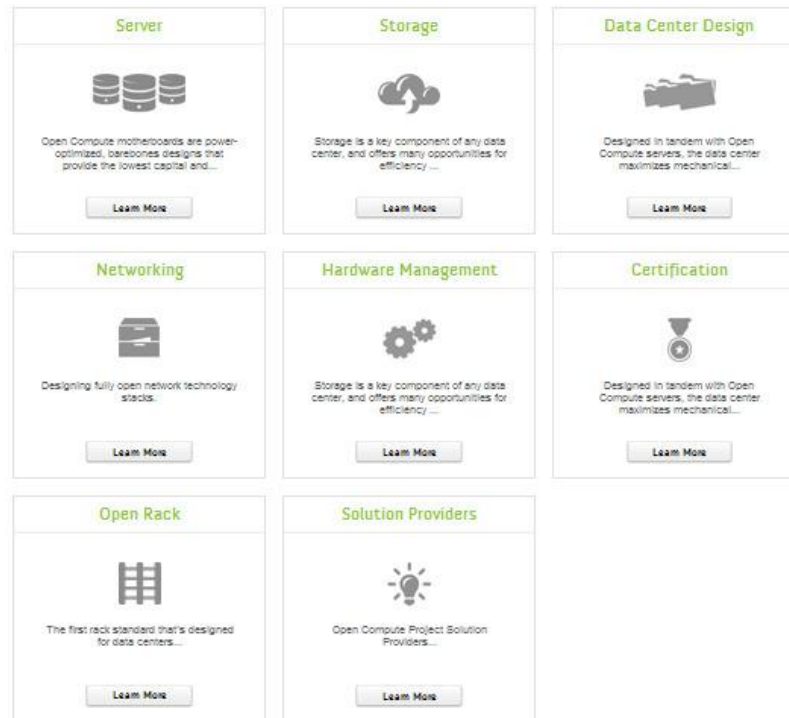
내용은 전자금융 거래법과 다를 게 없는데 양식만 다르다.

64. Facebook서버와 OCP기술 보기

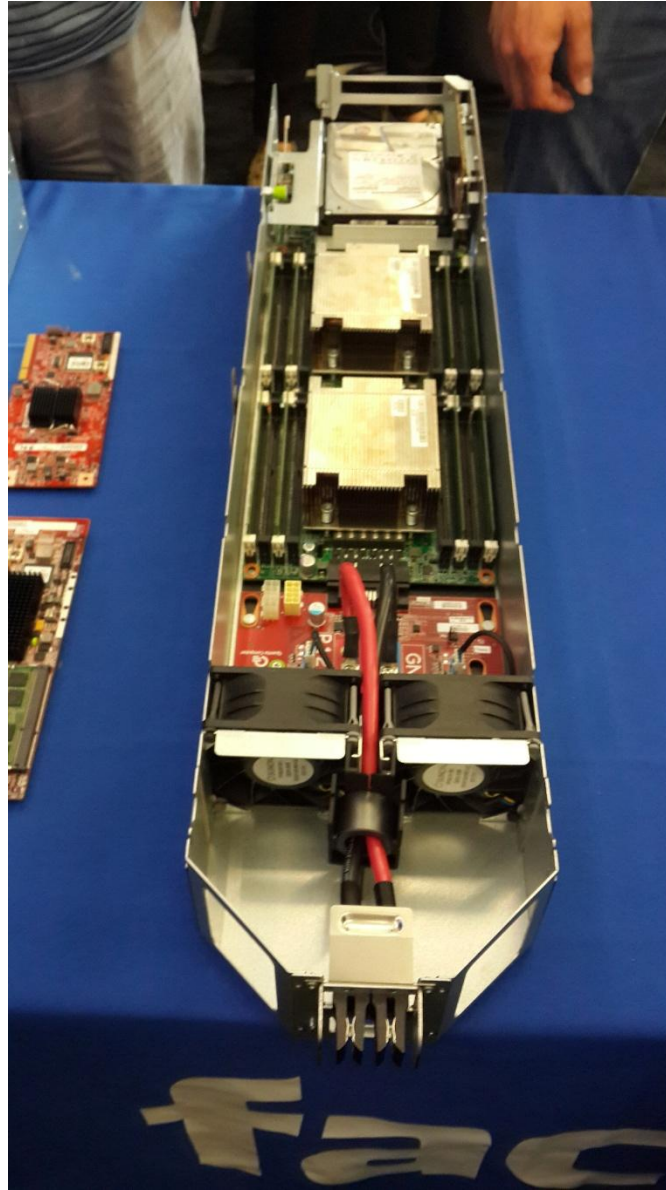
OCP (Open Compute Project)는?

Facebook이 주도하여, 사용자가 원하는 인프라를 공급자가 만들어 제공하도록 하는 프로젝트이다.

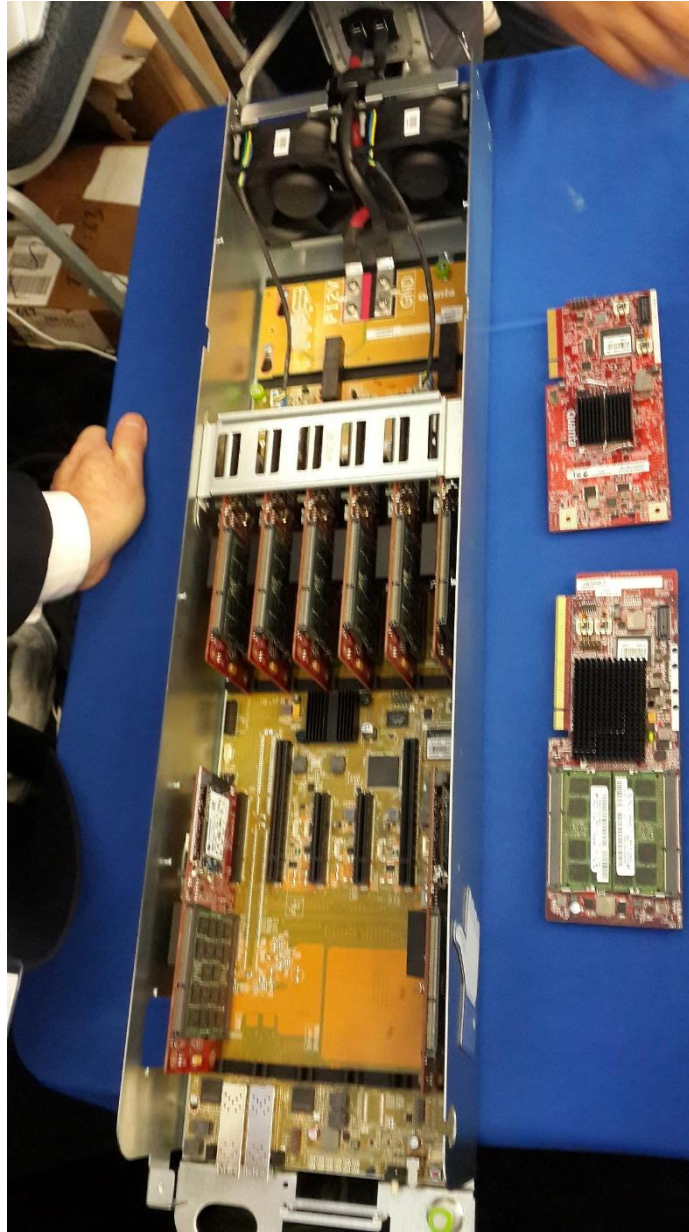
대상은 서버, 스토리지, 랙당 모든 인프라가 포함된다.



65. Facebook서버와 OCP기술 보기



66. Facebook서버와 OCP기술 보기



67. 대규모 네트워크 서비스망

네이버 인프라 운영 7년 , 대규모 인프라 운영 경험을 공유합니다.

운영 노하우입니다.

중소기업에서는 어떻게 하면 좋을지 적어봅니다.

- <1> 가상서버는 OS,WEB/WAS,어플리케이션,DB설치된 이미지를 준비하라.
- <2> 네트워크장비 L4를 이용하여 디폴트 이중화 하라.
- <3> L7 Check설정을 통해 WAS,DB장애까지 모니터링하라.
- <4> 웹 Cache등 기술플랫폼을 적용하라.
- <5> CDN을 활용하라~
- <6> MySQL DB 이중화를 MMM을 활용하라
- <7> 사용자가 늘어 DB성능이 부족한 경우 , Slave Read-Only DB를 사용하여 분산 한다.
- <8> 주간단위로 인프라 리뷰 시간을 가져라.
- <9> 회사 핵심 서비스는 데이터센터 이중화를 하라.
- <10> GSLB기능을 이용해 서비스 안정성을 높여 보자.
- <11> 대형 장애가 발생할 경우는 대비하여 , 미리 장애 공지 페이지 서버들을 준비하라.
- <12> 정기점검검시에 사용자가 필수 서비스는 계속 사용할수 있도록 Read-Only DB를 활용하자

68. 가상서버는 OS,WEB/WAS,어플리케이션,DB설치된 이미지를 준비하라.

1

문제점

OS설치후, WEB/WAS설치, 어플리케이션 설치,DB설치등에 시간이 많이 걸린다. 이벤트등이 생기면 20대 정도 늘려야하는데 시간이 부족하다.

2

해결방안

OS,WEB/WAS,어플리케이션,DB를 한서버에 설치하고 그 이미지를 만들어두고 재사용한다.

3

성과

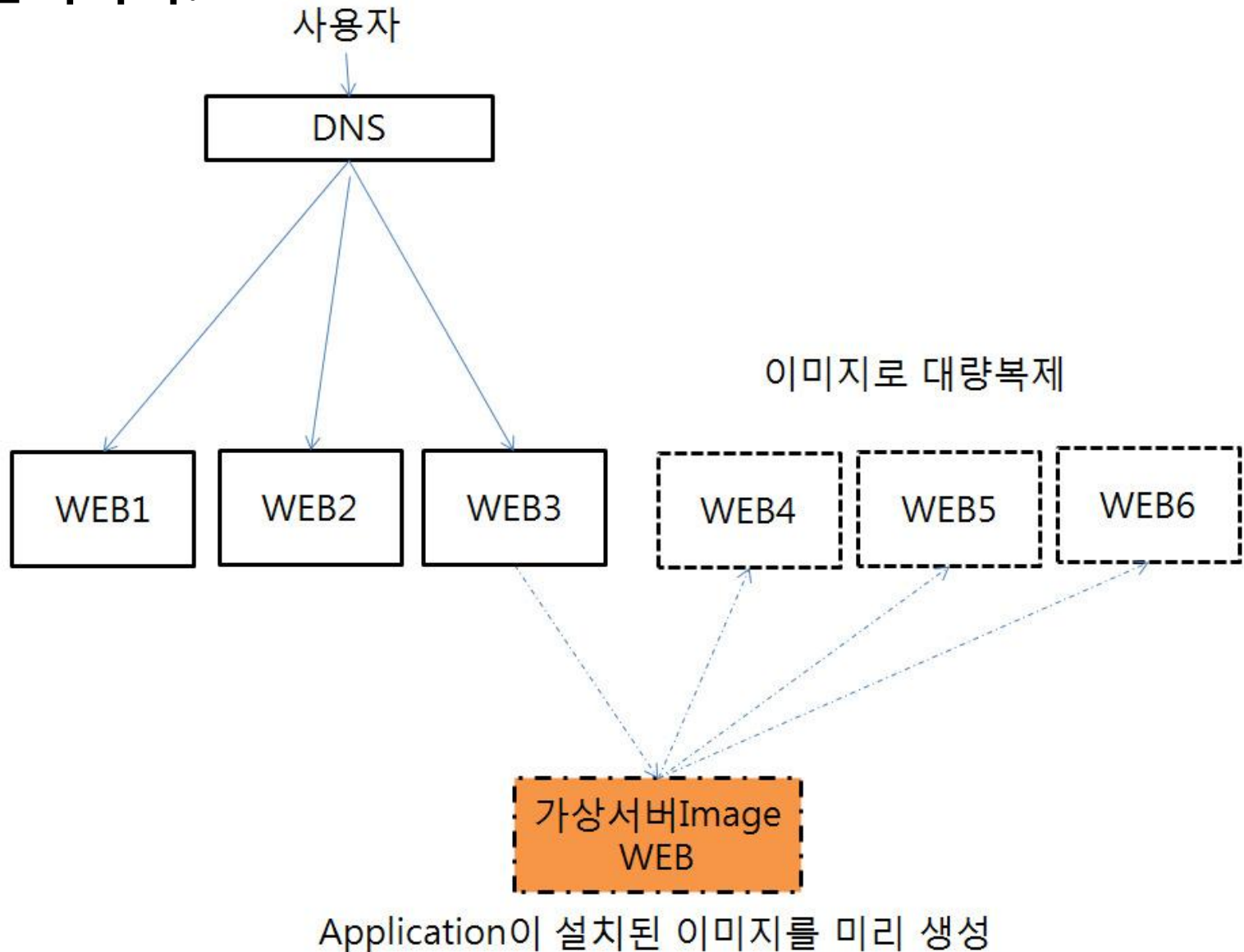
해당 이미지는 보안점검도 미리 받아 , 나중에 따로 보안점검을 받는데 시간을 낭비하지 않도록 한다.

표준OS와 표준WEB/WAS, 설치위치등 사전에 표준이 정해져있어야한다. 이미지 관리가 필수이다.

4

중소기업에서는 설치가 많지 않으므로 그냥 OS설치, 스크립트를 이용한 보안 패치를 차이는 없다^^

69. 가상서버는 OS,WEB/WAS,어플리케이션,DB설치된 이미지를 준비하라.



70. 네트워크장비 L4를 이용하여 디폴트 이중화 하라.

1

문제점

서버 1대로 운영중 서버 장애시 서비스가 중지됨

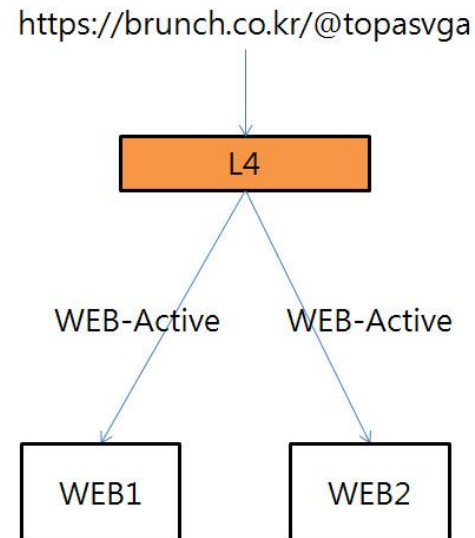
2

해결방안

서버는 2대이상으로 구축하고, 네트워크 L4장비를 이용해 서비스를 이중화 하라.

서버는 24시간 켜놓는 장비라 언제든지 고장 날수 있다.

1대 고장이 난다고 서비스가 중지되면 안된다.



71. L7 Check설정을 통해 WAS,DB장애까지 모니터링하라.

1. 문제점

L4를 쓰더라도 WAS장애시 Fail-over가 되지 않는다.

2. 해결방안

L7 Check설정으로 WAS,DB오동작까지 모니터링하여 Fail-over를 한다.

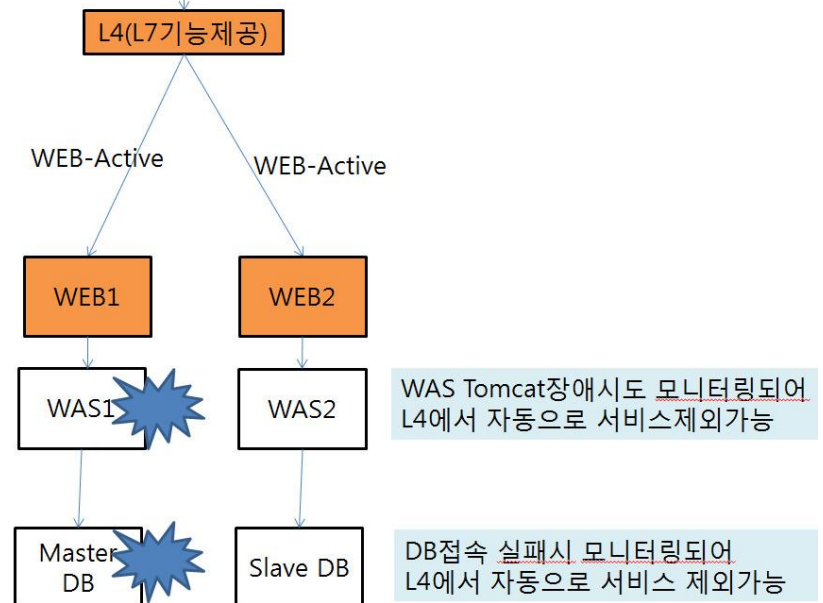
L4에서 WEB서버 장애는 잘 모니터링 되고 Fail-over가 되지만, WAS 안된다.

L7 Check 설정을 통해 해결을 한다.

WEB에서 WAS를 모니터링하는 부분을 만들어 L4에서 모니터링한다.

L4가 L7 Check를 지원해야 하며, L4장비 부하가 늘어나므로 장비 성능고려를 반영해야 한다.

<https://brunch.co.kr/@topasvga>



72. 웹 Cache등 기술플랫폼을 적용하라.

1

문제점

이벤트등으로 급격히 트래픽이 늘어나는 경우
웹서버 부하가 늘어나 서비스지연이 발생한다.

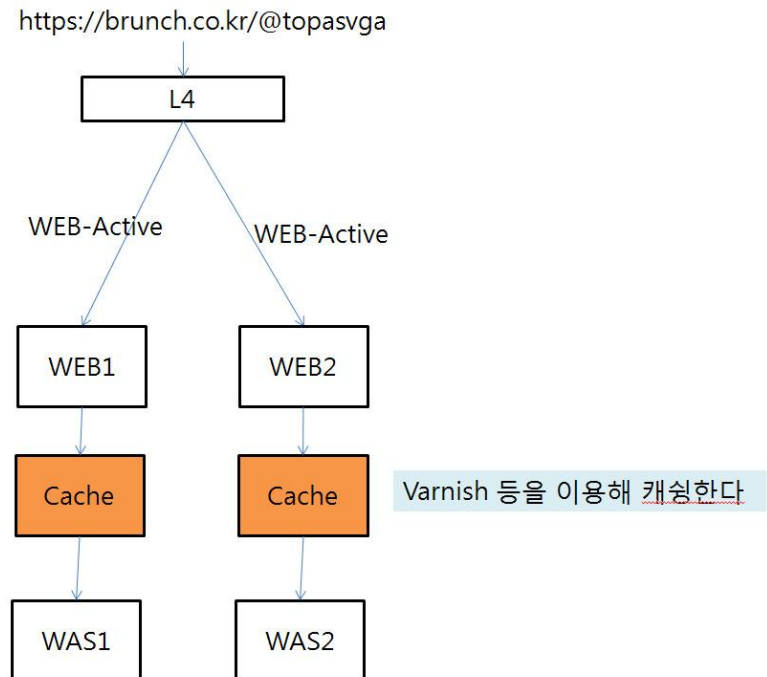
2

해결방안

Web과 Was사이에 Cache기술플랫폼을 적용하여 부하를 감소시킨다.

적용사례: 네이버에서 대선사이트 운영시 Varnish 적용

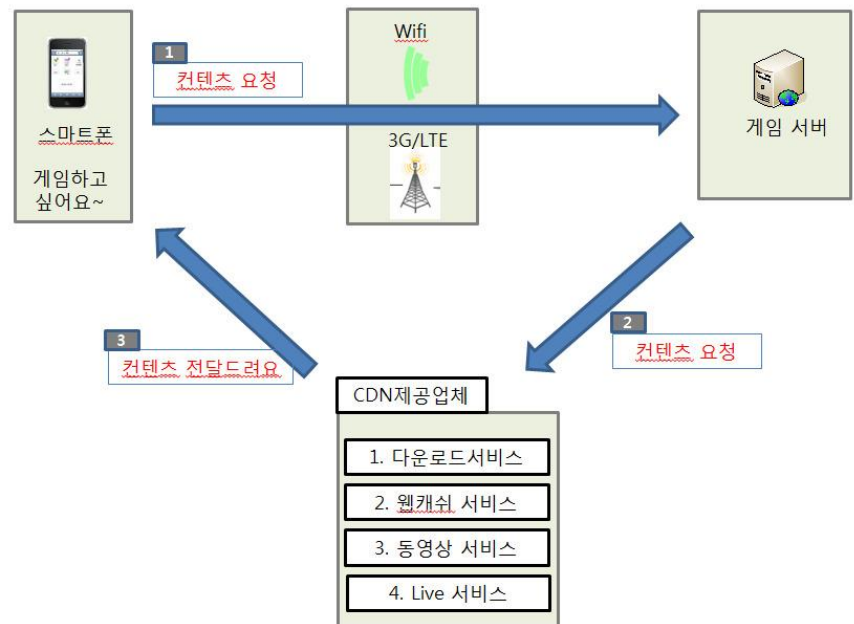
<http://d2.naver.com/helloworld/352076>



73. CDN을 활용하라~

1
문제점
사용자가 콘텐츠를 빠르게 받지 못한다.

2
해결방안
CDN서비스를 이용해 사용자가
가까운 네트워크에서 콘텐츠를 받도록 한다.



74. MySQL DB 이중화를 MMM을 활용하라

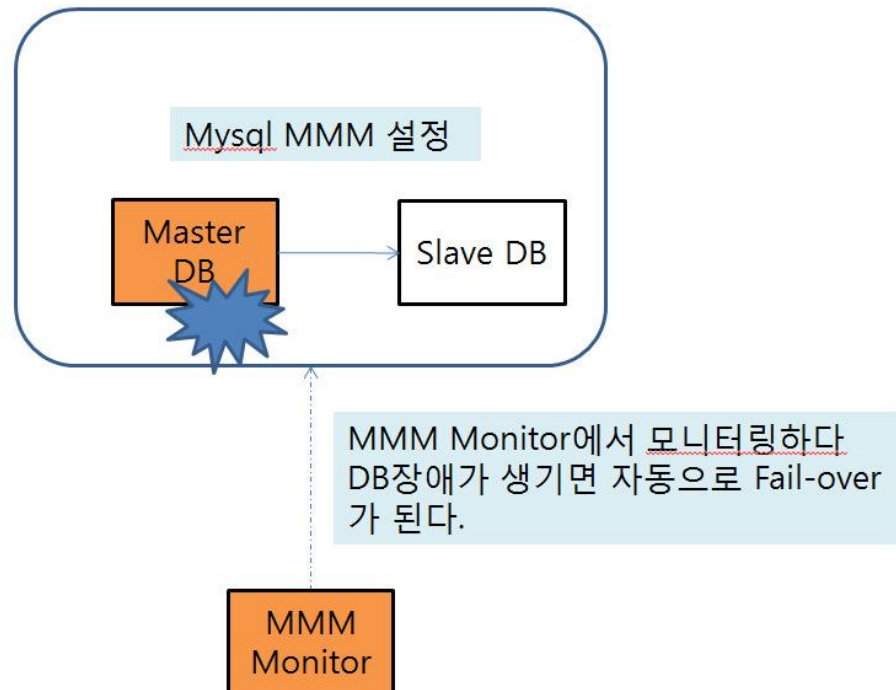
문제점

Mysql MasterDB 가 장애 발생하는 경우 서비스가 중지 된다.

해결방안

Mysql MMM(Mysql Multi-Mmaster) 설정하여,
DB가 자동 Fail-over되도록 한다.

<http://mysql-mmm.org/doku.php>



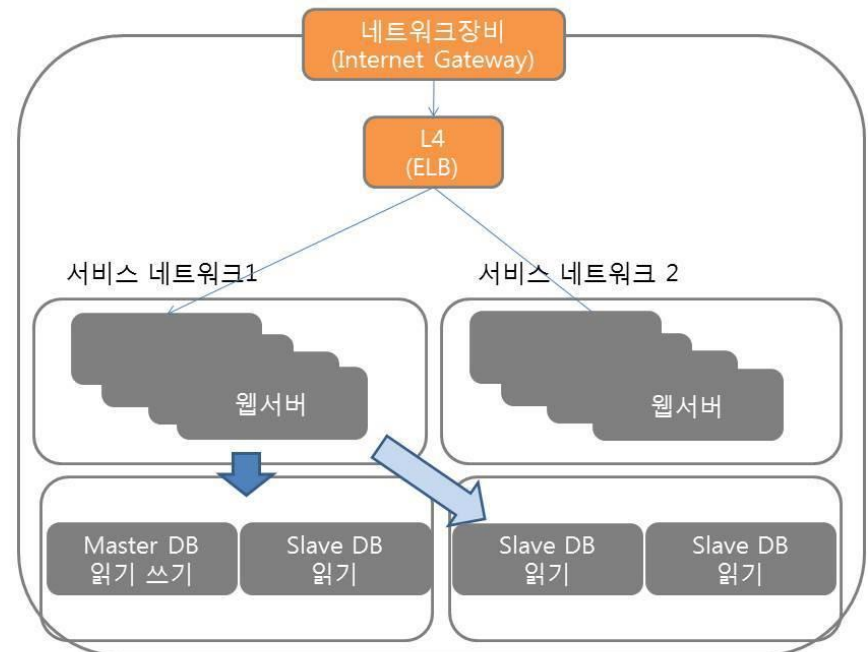
75. 사용자가 늘어 DB성능이 부족한 경우 , Slave Read-Only DB를 사용하여 분산 한다.

문제점

사용자가 늘어 DB HW를 업그레이드(Scale-UP)해야 하는데,
HW슬롯이 없어 증설이 불가하여 서비스가 느려지는경우 발생

해결방안

어플리케이션에서 읽기기능은 Slave DB를 바라보도록 변경하여
Master DB로 집중되는걸 분산하여 해결 한다.



76. 주간단위로 인프라 리뷰 시간을 가져라.

문제점

서비스오픈후 서버 사용률이 높아져 장애로 이어지고 있다.

해결방안

주간단위로 모니터링 리뷰하며, 사용량이 부족한경우 증설하여 장애를 예방할수 있다.

모니터링 시스템의 데이터를 이용한다.

Zabbix의 Screen기능으로 주요서비스 WEB,WAS,DB의 CPU,MEM,DISK,SWAP,.

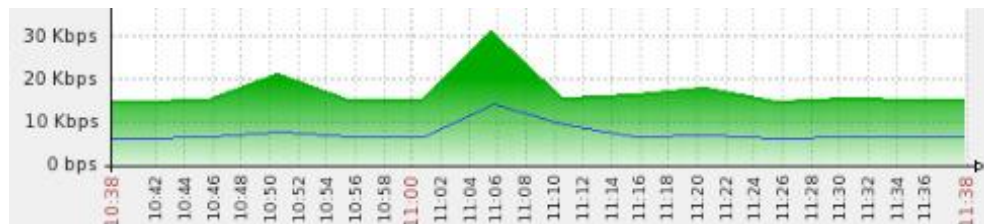
네트워크 트래픽을 주간단위로 리뷰하라.

트래픽 변경이 왜 생겼는지 사업,개발팀과 커뮤니케이션 하여 성능을 개선하라.

WEB,WAS,DB용 표준서버를 각각 사전에 정의하고,

DB경우 좀 넉넉하게 정의하라.

DB용량 부족한 경우, 전체 서비스장애로 이어진다.



77. 회사 핵심 서비스는 데이터센터 이중화를 하라.

문제점

회사의 핵심서비스인데, IDC랙 전원이 나가거나 화재의 경우, 서비스 전체적으로 안되는 경우가 발생한다.

해결방안

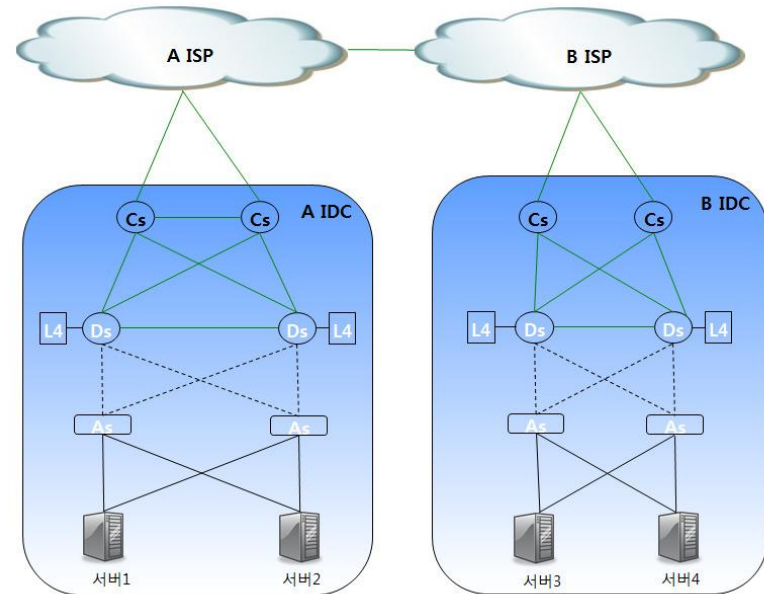
DNS와 L4를 이용해 IDC이중화 한다.

GSLB장비 또는 AWS Route53을 이용해 IDC이중화 한다.

Read가 많은 뉴스서비스의 경우 IDC이중화가 가능하다.

Write가 되는 서비스의 경우는 IDC이중화가 쉽지 않다.

(데이터 동기화에 대한 고민이 필요하다.)



78. GSLB기능을 이용해 서비스 안정성을 높여 보자.

일반적인 회사는 DNS만 이용해 서비스를 운영한다.
대기업이나 대형 포털은 GSLB장비를 이용해 서비스 안정성을 높이고 있다.

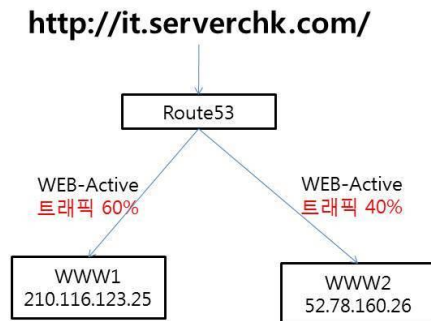
문제점

DNS서버만 운영하여 글로벌 서비스에 제약이 있다.

해결방안

GSLB장비나 AWS Route 53의 GSLB기능을 이용하여,
다양한 DNS 서비스가 되도록 한다.

AWS Route53 GSLB기능 사용법 <https://brunch.co.kr/@topasvga/28>



79. 대형 장애가 발생할 경우는 대비하여 , 미리 장애 공지 페이지 서버들을 준비하라.

문제점

대형 장애가 발생되고 해결에 시간이 길어질 경우, 사용자에게 오류페이지가 장시간 보여진다.

해결방안

장애시 긴급 점검중이라는 페이지가 보여지도록 미리 준비한다.

장애공지용 서버군을 외부에 구축한다.

장애가 길어지면 DNS에서 해당서비스 도메인을 장애공지용 서버팜으로 전환
장애공지용 서버팜에서는 *.도메인명.com으로 유입이 되면 특정 장애공지 페이지를 보여주도록 설정한다.

장애공지팜은 외부에 두어야 한다.

대형 포털에서는 미리 장애 대비 공지 서버들을 준비하고 있다.

AWS S3 와 route53을 이용해서도 가능하다.

80. 정기점검시에 사용자가 필수 서비스는 계속 사용할 수 있도록 Read-Only DB를 활용하자

문제점

정기점검을 하면 매번 서비스가 모두 중지된다.

해결방안

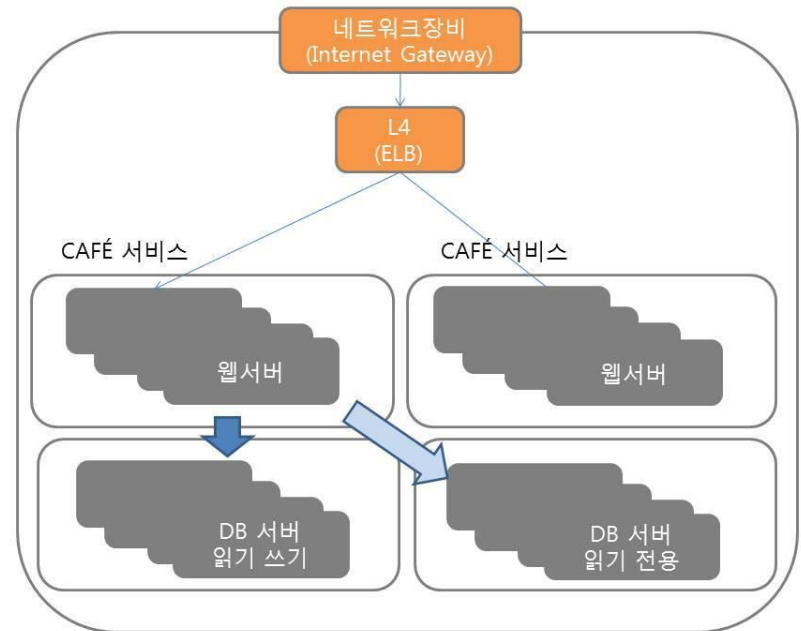
정기점검시에도 사용자에게 필수기능인 읽기 기능은 제공되도록 한다.

Read OnlyDB를 사용하여 읽기기능은 작업중에도 제공한다.

게시판서비스의 경우 쓰기를 막는다.

대형포털 정기 점검시 사용하고 있다.

주기적인 서비스관리는 쉽게 따라할수 있지만
비용이 들어가는 부분은 고려가 필요하다.
해당 기업의 규모와 특성에 맞게 가면 된다.



감사합니다.