クラウドコンピューティング基礎論

第３回

創造情報•小林克志

ikob@acm.org

Outline

1. Administravia
2. Homework review
3. Reliability in general
   - Availability, MTTF, MTBF, Bus tub curve..
4. Reliability in cloud service
   1. Service Level Agreement (SLA)
   2. Redundancy
   3. Availability zone and region

Course Outline

1. Administrivia
2. Cloud computing
3. Service reliability
4. Distributed data stores
5. Global services
6. Datacenter networkings (1)
7. Datacenter networkings (2)
8. Network performance
9. User experiences
10. Network latencies
11. Advanced topics

Class Information

- Provided by Web page:

  http://www.ci.i.u-tokyo.ac.jp/~ikob/lecture/2018-fcloud

- Includes report submissions/roll calls/materials.

- An authorization is required for access:
  User: cloud
  Pass: cloud!2018

Outline

1.Administravia

2.Homework review

3.Reliability in general

- Availability, MTTF, MTBF, Bus tub curve..

4. Reliability in cloud service

- Service Level Agreement (SLA)
- Redundancy
- Availability zone and region

1 May 2019

- What will be happen in Japan ?
  - Switch Japanese-“era”-name (元号).

法令標準XMLスキーマ（案）に関する意見の募集結果について

平成29年５月

総務省行政管理局

行政情報システム企画課

別紙

法令標準XMLスキーマ(案)に関する御意見及びこれに対する考え方

NO	項目	お寄せいただいた御意見	御意見に対する考え方
1	元号	法令標準XMLスキーマ参考資料において、法令のカラムにて整備される属性として、元号が予定されているが、電算処理を行うにあたっては西暦についても属性として記載が行われることが望ましいのではないか。	法令の公布日等については、官報で和暦にて公布されることから、その情報を属性の値としています。 また、ご意見にもあるとおり、和暦/西暦のどちらで表示するかに関してはアプリケーションに依存するものと考えています。
2		「年号」の属性の英語名が「year」であることは、西暦表記との誤解を招く可能性があるのではないか。	
3		Era(元号)属性を廃止する 年月日を和暦/西暦のどちらで表示するかはXMLの処理側に委ねることであり、data型で年月日が指定されていれば元号は機械的に判定できるものである。また元号改正の度に法令標準XMLスキーマを改訂するのは本質的ではない。	

XML スキーマ案より

```
<xs:attribute name="Era" use="required">
   <xs:simpleType>
     <xs:restriction base="xs:token">
       <xs:enumeration value="Meiji"/>
       <xs:enumeration value="Taisho"/>
       <xs:enumeration value="Showa"/>
       <xs:enumeration value="Heisei"/>
     </xs:restriction>
   </xs:simpleType>
 </xs:attribute>
```

「総務省：法令標準ＸＭＬスキーマ（案）に関する意見の募集について」より

Outline

1.Administravia

2.Homework review

3.Reliability in general

- Availability, MTTF, MTBF, Bus tub curve..

4. Reliability in cloud service

- Service Level Agreement (SLA)
- Redundancy
- Availability zone and region

Today’s assignment

- With Japanese government support, RIKEN provides high-performance computing system as known as “K (京)” computer.

1. Is “K computer” is a cloud computing service in terms of NIST definition ?
    - If your student ID is odd : Tell reason why it is “cloud computing” service.
    - Otherwise (or ID is even) : Tell reason why it is NOT “cloud computing” service.
2. If “K computer” is cloud computing service. Which service model is K-computer ? Which deployment model is K ? Tell reason why this service and deployment models fit to it.

- Submit your answers in Japanese or English via the course web.
- NIST：http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- K-computer :
    - System: http://www.aics.riken.jp/en/k-computer/system
    - Guide for applicants : http://www.hpci-office.jp/pages/e_k_guidance

本日の課題

- 理化学研究所は「京」コンピュータとしてしられる高性能コンピューティングサービスを提供している。

1. 「京」は NIST 定義によるクラウドコンピューティングに該当するか？

    - 学績番号が奇数：クラウドコンピューティングに該当する理由を述べよ。
    - それ以外（番号が偶数）：クラウドコンピューティングに該当しない理由を述べよ。

2. 「京」がクラウドコンピューティングとして、いずれのサービスモデルに該当するか？いずれの展開モデルに該当するか？サービスモデル、展開モデルに適合する理由を述べよ。

- 講義 web から日本語か英語で回答すること。
- NIST：http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
- K-computer :
    - System: http://www.aics.riken.jp/en/k-computer/system
    - Guide for applicants : http://www.hpci-office.jp/pages/e_k_guidance

Outline

1.Administravia

2.Homework review

3.Reliability in general

- Availability, MTTF, MTBF, Bus tub curve..

4. Reliability in cloud service

- Service Level Agreement (SLA)
- Redundancy
- Availability zone and region

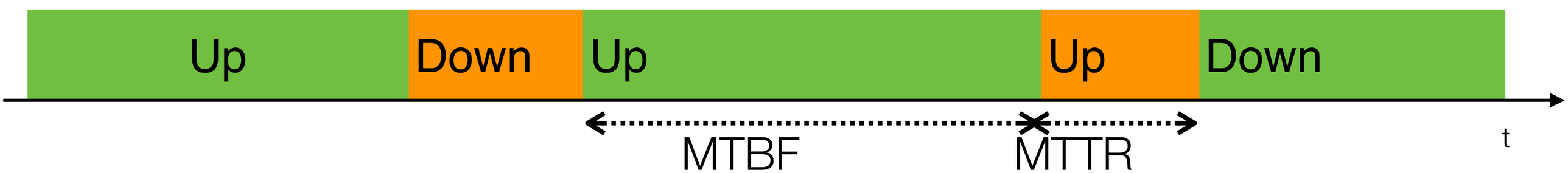
Indices of reliability

1. Classic definition, for predictions.
   A = MTBF / (MTBF + MTTR)
   Mean Time Between Failure (MTBF),Mean Time To Recover(MTTR)

2. Actual, to evaluate services, such for 24hr 7days service.
   A = Uptime / (Uptime + Downtime)

3. In fact, on Service Level Agreement (SLA) evaluation.
   A = Uptime / (Uptime + Unplanned Downtime)

   • excluding planned down time



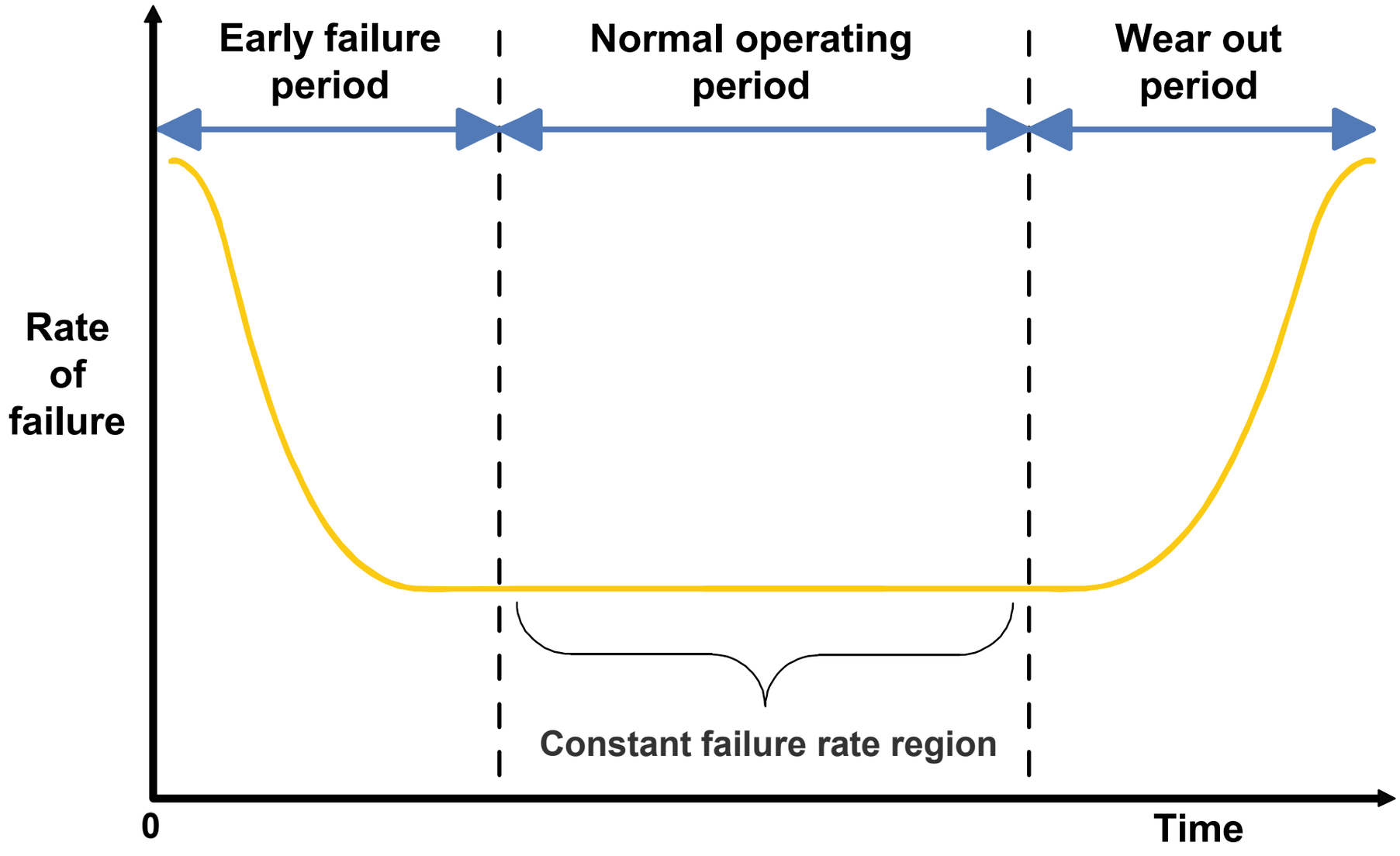
Availability in nines notation

- Availability is often specified in nines notation, e.g., four-nines stands for 99.99%.
- In fact, real-system failure rates are not constant. It depends on a lot of factors, such as, working time, environment, production lot.

Nines	%	Down time in a year
Two	99	4 days
Three	99.9	9 hrs
Four	99.99	1 hrs
Five	99.999	5 min.
Six	99.9999	30 sec.
Seven	99.99999	3 sec.

Availability of real-systems

Figure 1 *– Bathtub curve to illustrate constant rate of failures*



W. Torell and V. Avelar, “Mean Time Between Failure: Explanation and Standards”, APC White paper, 2004

Availability of HDD

“…at moderate temperature ranges it is likely that there are other effects which affect failure rates much more strongly than temperatures do.”

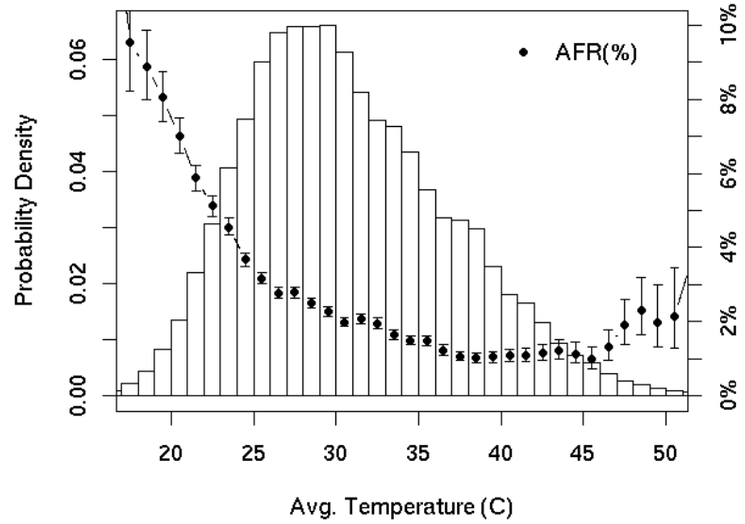


Figure 4: Distribution of average temperatures and failures rates.

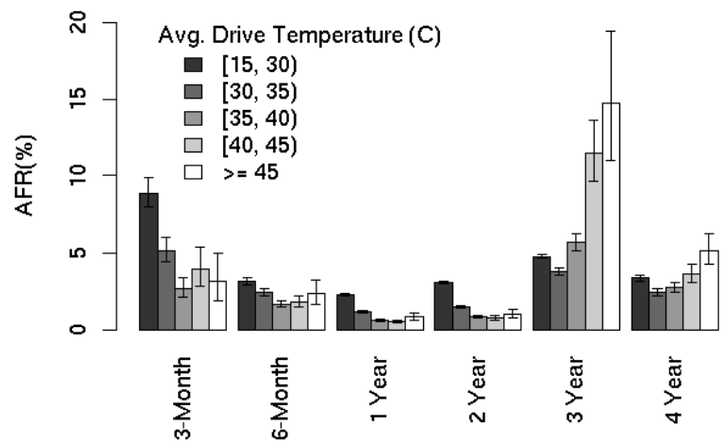


Figure 5: AFR for average drive temperature.

Pinheiro, Eduardo, *et al.* "Failure Trends in a Large Disk Drive Population." FAST. Vol. 7. 2007.

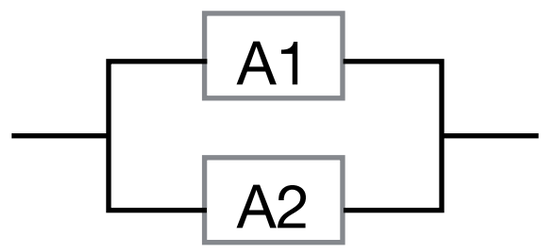
Evaluate system availability with multi-components

- Model the systems with interconnection of components.
  - Two components, x and y, are operating:
    - in series, if a part failure causes inoperable, e.g., RAID 0. The availability is :

$$A_{series} = A_1 A_2$$

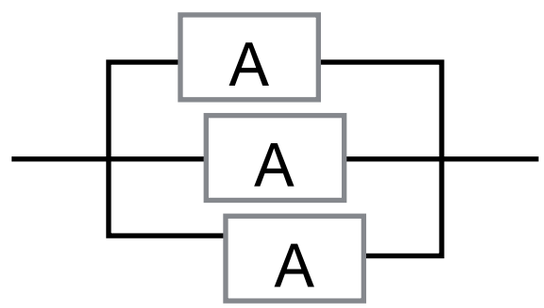
    - in parallel, if a part failure is taken over other part, RAID 1. The availability is :

$$A_{parallel} = 1 - (1 - A_1)(1 - A_2)$$



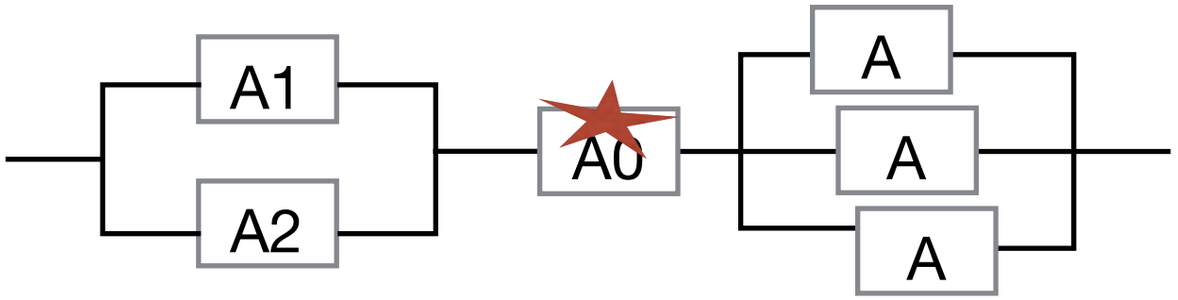
- In general case, i.e., partial operation,
  - when up to n components failure of q in total, can be taken over others, RAID 5,6

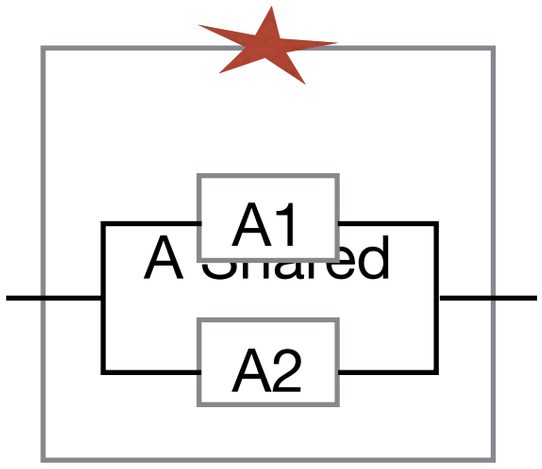
$$A_{partial} = \sum_{p=0}^{n} C(p,q) A^{q-p} (1 - A)^p$$



Single Point Of Failure / Shared Risk

- Should be eliminated or minimized at system design.
  - Component level redundancy is effective but not perfect.
- Risk assessment conducted for “entire system”
  - Internal: Servers, Storage, DC networks, Application
  - External: WAN, ISP, External services, Power grid, Building
  - Temporal: HW supply, Software support
  - Combinational: Version mismatch





SPOF/Shared Risk

On real-systems ….

- Deal with “failback” as well as failover, either automatically or manually.
- Active - Stand bye / Active - Active ?
-

More than 10hrs service disruption.

Microsoft Corporation

Azure status history | Microsoft Azure

Microsoft Azure

Search MY ACCOUNT PORTAL

Why Azure Solutions Products Documentation Pricing Partners Blog Resources Support FREE ACCOUNT

March 2017

3/31 RCA – Cooling Event – Japan East – Additional Information

Summary of impact: Between 11:28 UTC and 22:16 UTC on March 31 2017, a subset of customers in Japan East region may have experienced unavailability of Virtual Machines (VMs), VM reboots, degraded performance or connectivity failures when accessing those resources or/and service resources dependent upon Storage service in this region.

As a part of standard monitoring, Azure Engineers received alerts for availability drops for this region. Engineers identified the underlying cause was due to an error in the safe power recovery procedure followed by a failure within the power distribution system that was running at N+2. One RUPS (rotary uninterruptible power supply) in the N+2 parallel line up failed and resulted in being unable to supply power to the cooling system in this datacenter. As a consequence of the cooling system going down, some resources were automatically shutdown to avoid overheating and ensure data integrity and resilience. The first failure within the power distribution system that was running at N+2 occurred at 11:28 UTC, and the Facility Service Provider promptly responded and initiated the safe power recovery procedure.
There was an error in the safe power recovery procedure and one of the cooling systems was incorrectly shutdown at 12:40 UTC. As a result of this, some areas in the facility lost the cooling function and temperatures inside the facility went up and passed safe thresholds.

Between 12:45 UTC and 13:12 UTC, Azure engineers and the Facility Service Provider received multiple overheating alerts due to overheating event at the facility, and started using outside airflow to force cool the datacenter.

At 13:46 UTC, Microsoft site services personnel were onsite with the Facility Service Provider and restarted the cooling system air handlers as well as continued using outside airflow to force cool the datacenter. At the same time, Azure engineers prepared to bring systems back online when cooling was restored to the datacenter.

At 15:24 UTC, the Facility Service Provider confirmed that the cooling systems were restored successfully. Temperatures for some impacted area in the inside the datacenter returned to safe operational thresholds.

At 16:08 UTC, a thorough health check was completed after RUPS system and cooling systems were restored at 15:24 UTC, any suspects or failed components were replaced and isolated due to damages by overheating. Suspected and failed components are being sent for analysis.

At 16:53 UTC, Engineers confirmed that approximately 95% of all switches/network devices have been restores successfully. Power up processes began on impacted scale units that host Software Load Balancing (SLB) services and the control plane.

At 17:16 UTC, majority of the core infrastructure was brought online, Networking Engineers began restoration of Software Load Balancing (SLB) services in a controlled process to help programming to establish a quorum promptly.

Once SLB was up and running, Engineers confirmed that majority of services were recovered automatically and successfully at 18:51 UTC. Residual impacts with Virtual Machines were found. Engineers investigated and continued to recover impacted Virtual Machines to bring them

Rotary Uninterruptible Power Supply.
The image is unrelated to the trouble in the article.

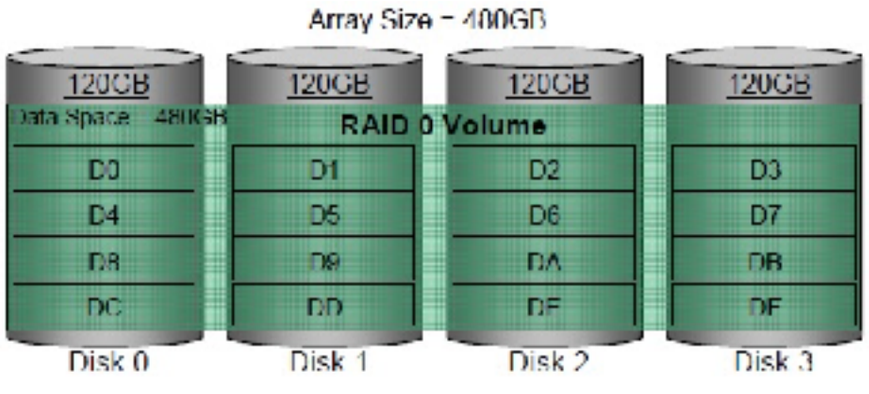
Hard Disk Drive (HDD) & Disk Array

HGST Deskstar T7K500
http://www.hgst.com より

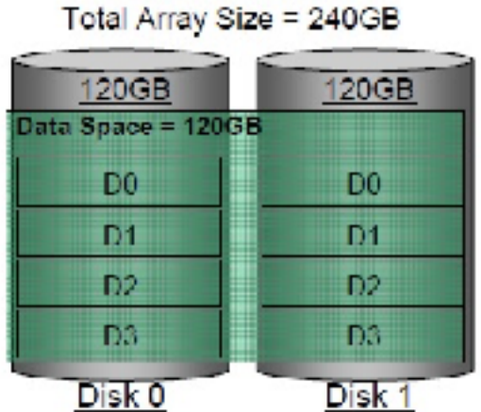
http://www.dell.com より

Redundant Arrays of Independent/ Inexpensive Disks (RAID)

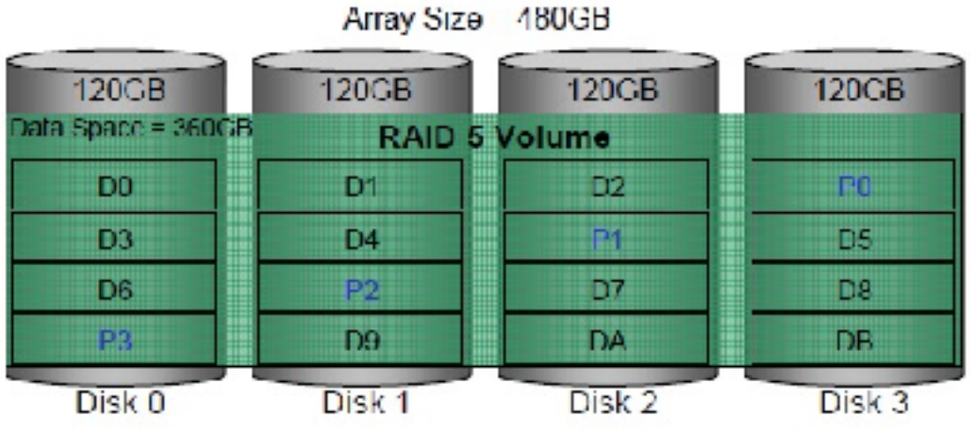
RAID 0 (striping, no redundancy)



RAID 1 (mirroring)

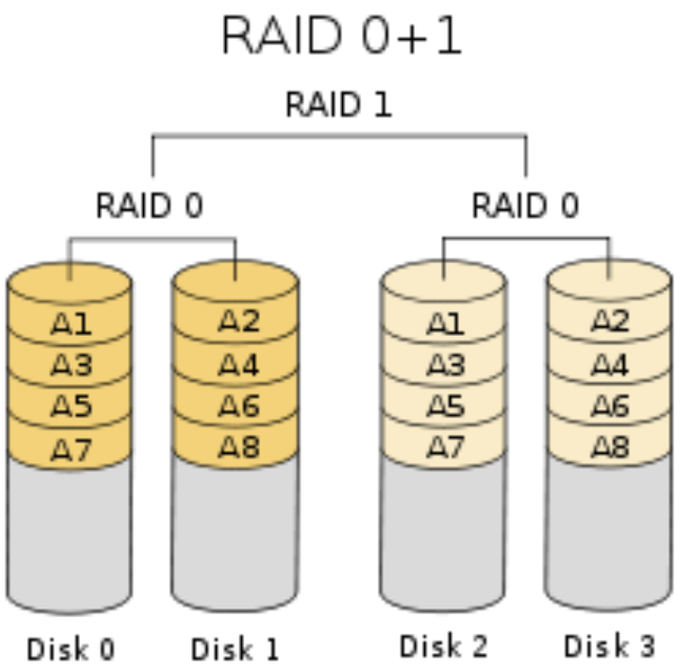


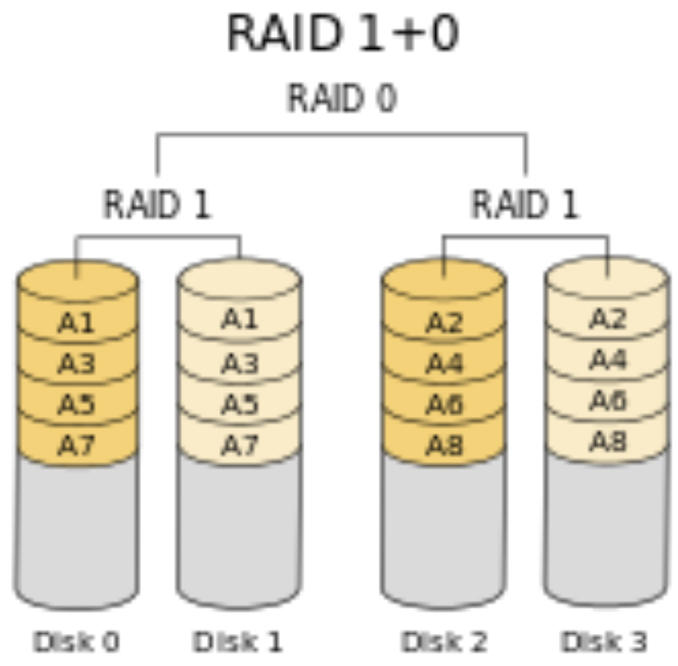
RAID 5 (striping with parity)



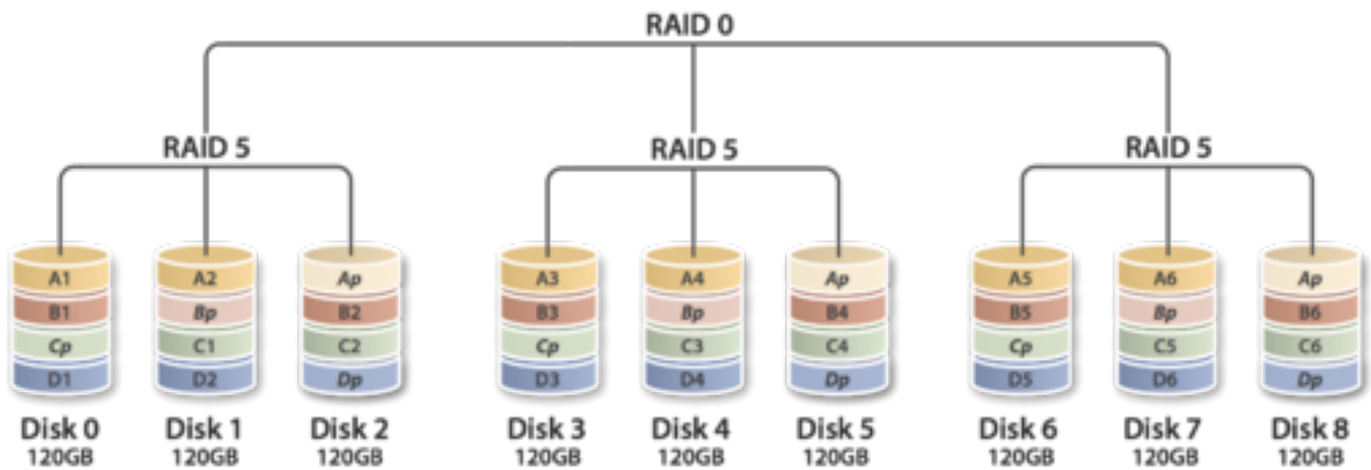
http://www.intel.com/support/chipsets/imsm/sb/CS-009337.htm

Nested RAID configs





RAID 50



Wikipedia より

Outline

1.Administravia

2.Homework review

3.Reliability in general

- Availability, MTTF, MTBF, Bus tub curve..

4. Reliability in cloud service

- Service Level Agreement (SLA)
- Redundancy
- Availability zone and region

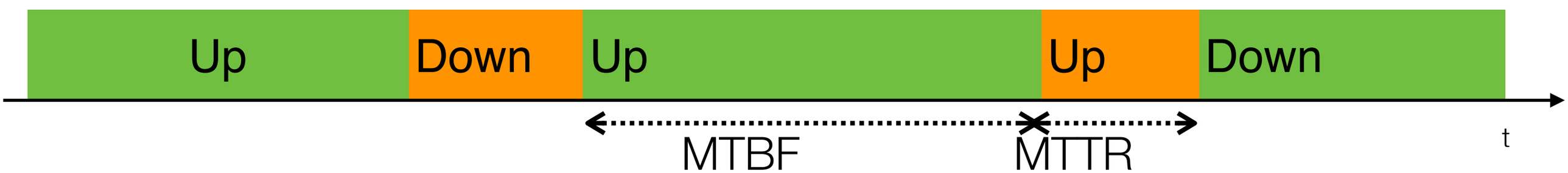
Indices of reliability

1. Classic definition, for predictions.
   A = MTBF / (MTBF + MTTR)
   Mean Time Between Failure (MTBF),Mean Time To Recover(MTTR)

2. Actual, to evaluate services, such for 24hr 7days service.
   A = Uptime / (Uptime + Downtime)

3. In fact, on Service Level Agreement (SLA) evaluation.
   A = Uptime / (Uptime + Unplanned Downtime)

   • excluding planned down time



Service Level Agreement (SLA)

- Is used in legal contract between the provider and client.
    - The result of compromise between cost and reliability.
    - If the service cannot achieves the contracted SLA level, the provider pays back fee for downtime, or with penalty.
        - Note: In most cases, the providers never compensate entire losses, caused by the service down.
- Typical SLAs as:
    - Cloud service : 99.5% availability (AWS, MS Azure)
    - Internet Service Provider : 100%, Packet delay of < 25ms. (IIJ)
    - TELCO line : Payback with penalty according down-time.

Service Level Agreement (SLA)

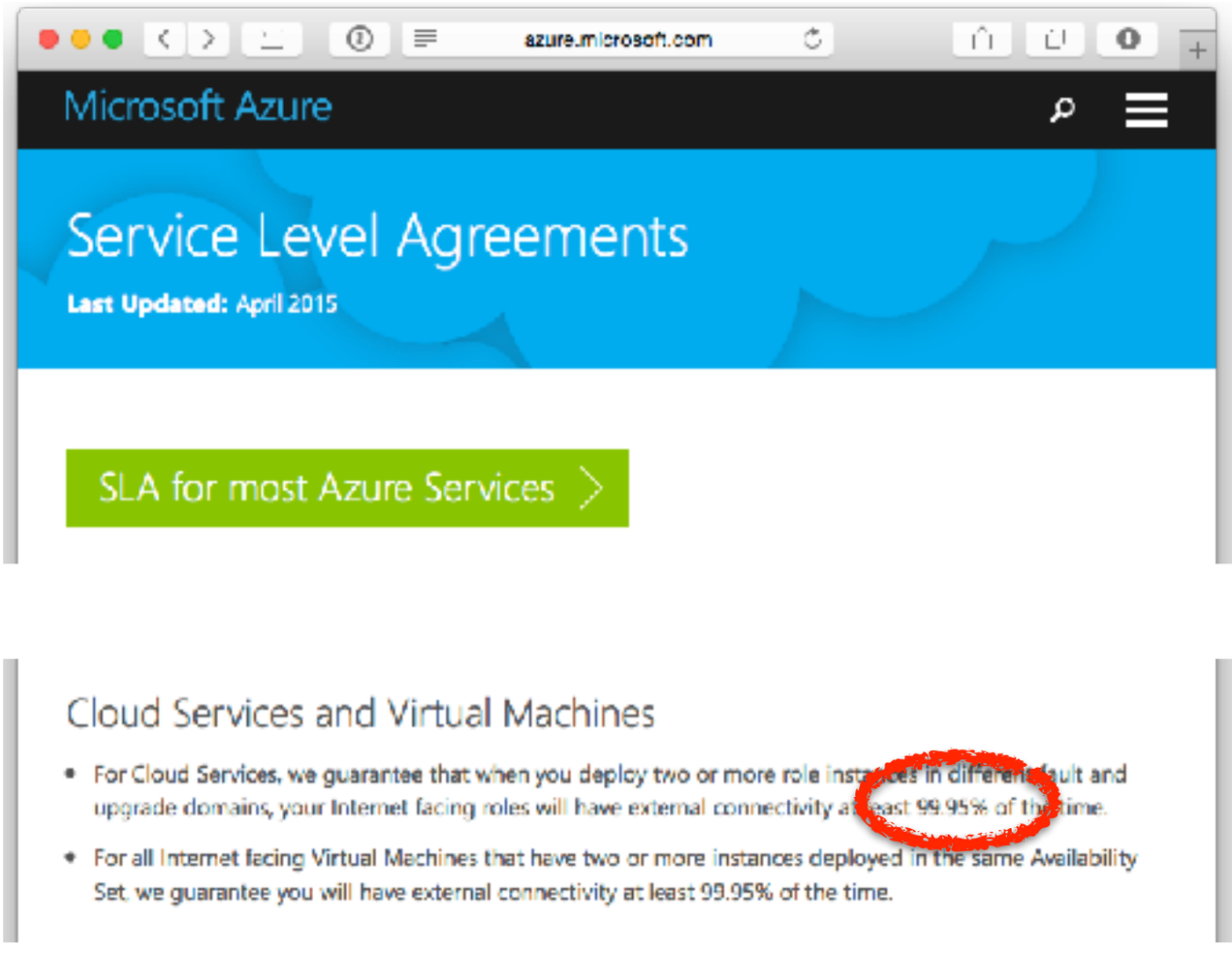
Amazon EC2 Service Level Agreement

Effective Date: June 1, 2013

This Amazon EC2 Service Level Agreement ("SLA") is a policy governing the use of Amazon Elastic Compute Cloud ("Amazon EC2") and Amazon Elastic Block Store ("Amazon EBS") under the terms of the Amazon Web Services Customer Agreement (the "AWS Agreement") between Amazon Web Services, Inc. ("AWS", "us" or "we") and users of AWS' services ("you"). This SLA applies separately to each account using Amazon EC2 or Amazon EBS. Unless otherwise provided herein, this SLA is subject to the terms of the AWS Agreement and capitalized terms will have the meaning specified in the AWS Agreement. We reserve the right to change the terms of this SLA in accordance with the AWS Agreement.

Service Commitment

AWS will use commercially reasonable efforts to make Amazon EC2 and Amazon EBS each available with a Monthly Uptime Percentage (defined below) of at least 99.95%, in each case during any monthly billing cycle (the "Service Commitment"). In the event Amazon EC2 or Amazon EBS does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.



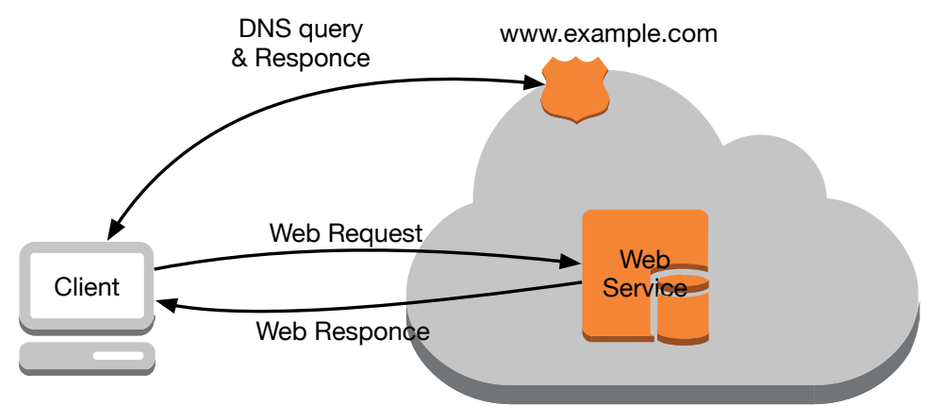
mazon, "Amazon EC2 Service Level Agreement", June 1, 2013 Microsoft, "Microsoft Azure Service Level Agreements", April, 2015

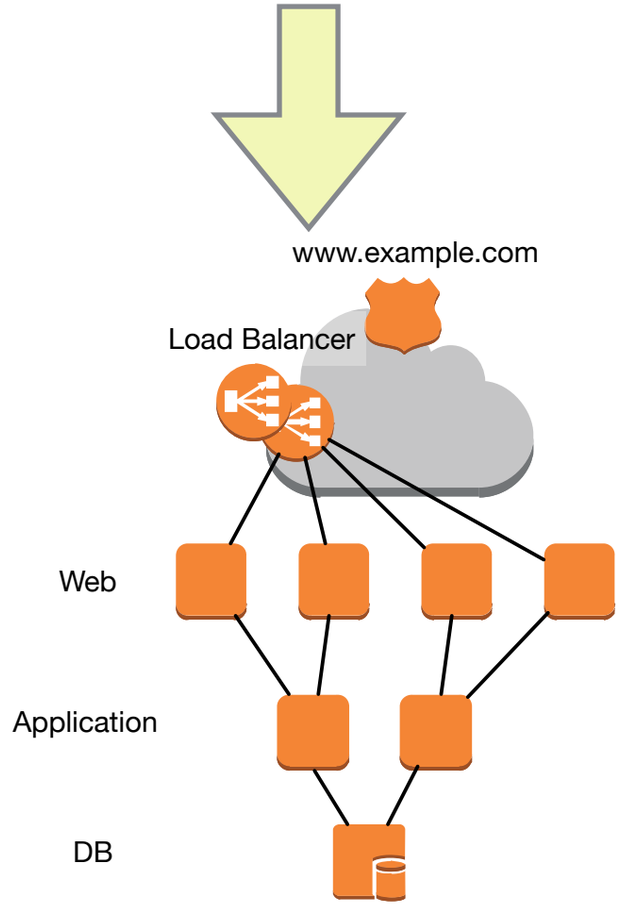
A simple Web to scalable architecture.

- Simple Web architecture, such as static contents delivery with a single Web server, is out of date.

- Today's web services are required
  - Availability : avoid service disruption.
  - Scalability : Support huge number of customers, 100M or more.
  - High level UX : smooth end-to-end user experience.

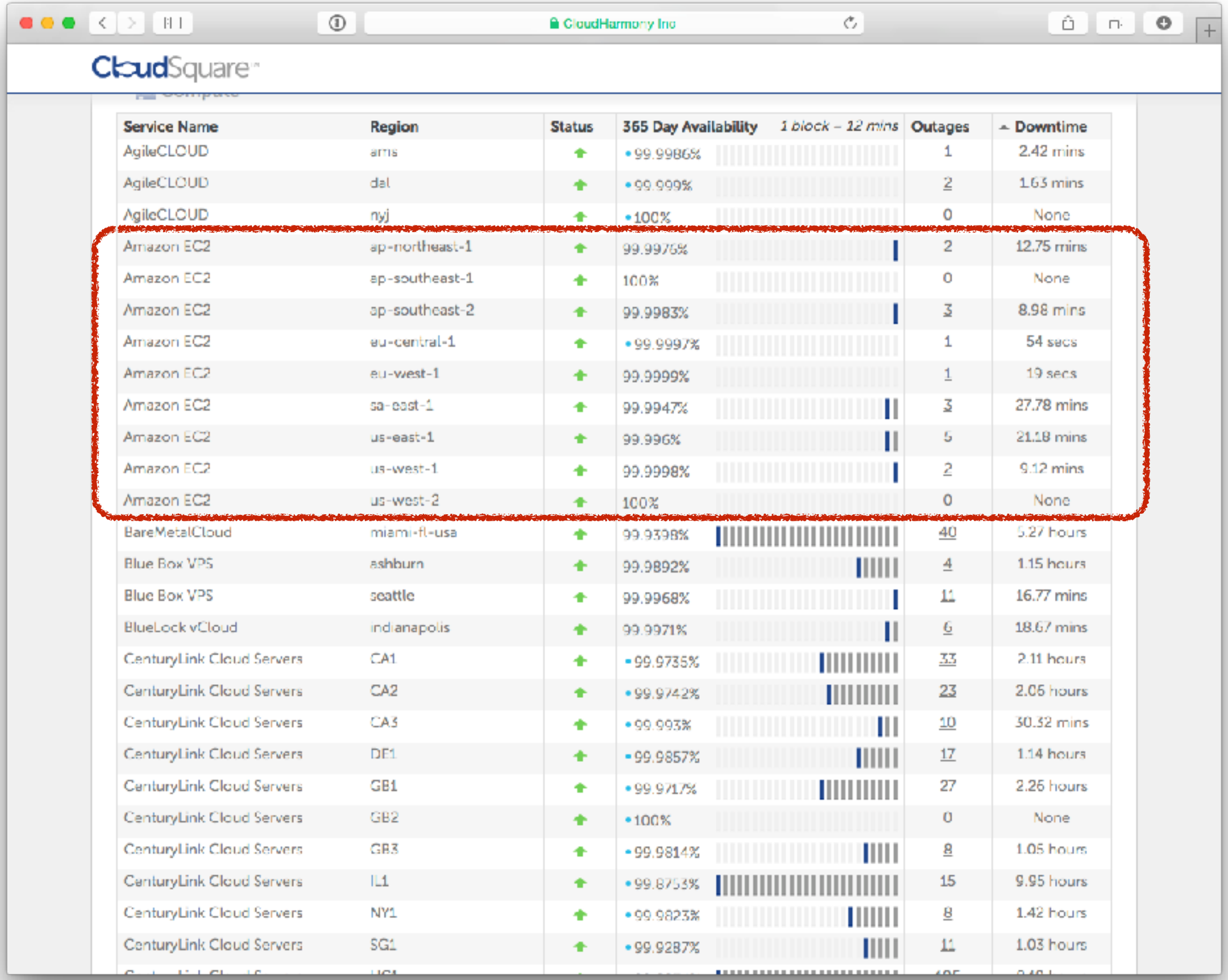
- A scalable Web architecture:
  - Three-tier : Web + Application + DB





Availability in Cloud computing

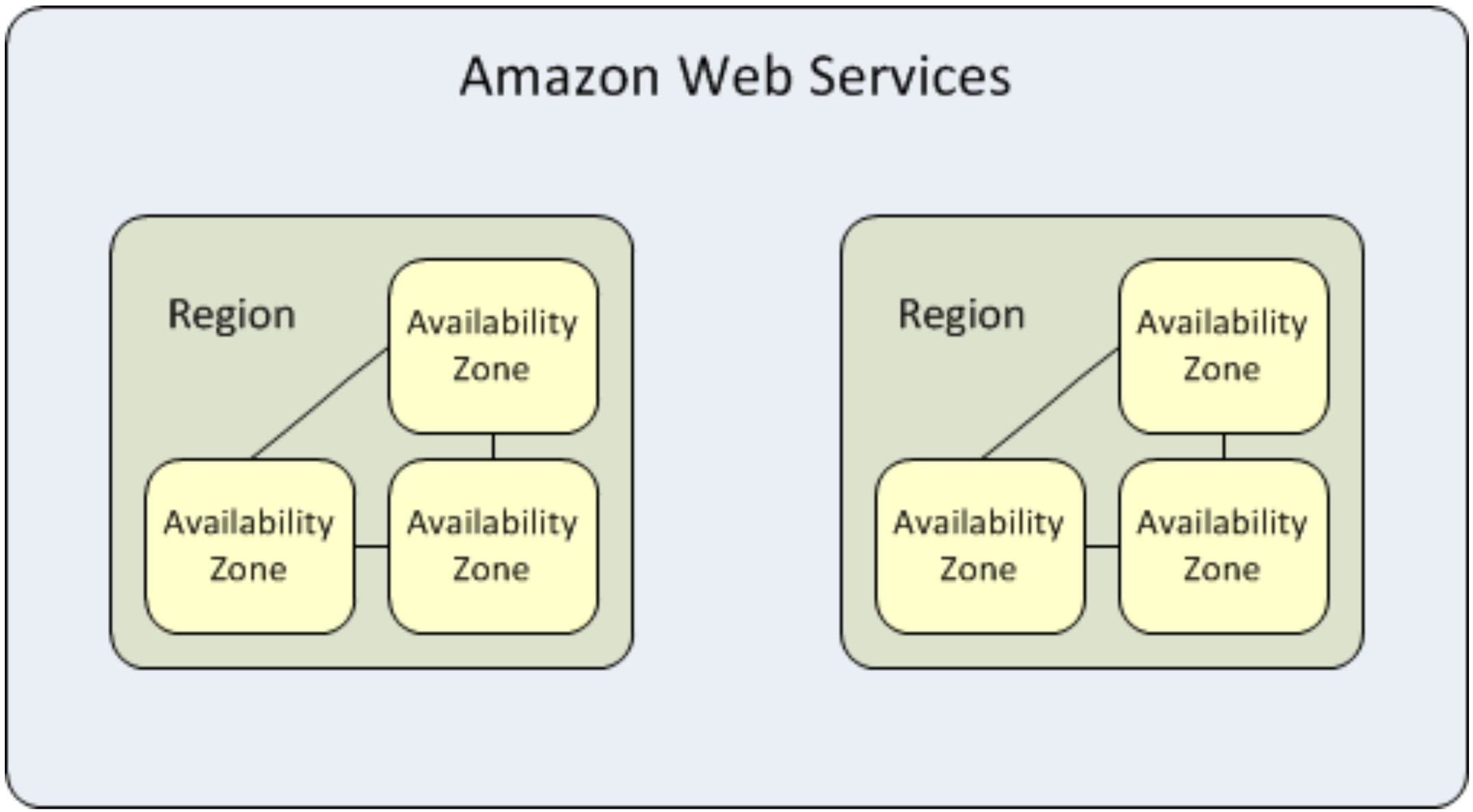
- Availability is a key factor to choose because service outage impact is critical.
    - Outages lead the worst user experience.
    - Customers switch competitive services.
    - Outage even due to maintenance, the duration should be minimized, or zero.
- However, 100% available IaaS/SaaS is impossible or expensive. High availability should be achieved by service provider itself, as well as performance scale-out.


CloudHarmony Inc
CloudSquare
Service Name
Region
Status
365 Day Availability
1 block = 12 mins
Outages
Downtime
AgileCLOUD
ams
99.9986%
1
2.42 mins
AgileCLOUD
dal
99.999%
2
1.63 mins
AgileCLOUD
nyj
100%
0
None
Amazon EC2
ap-northeast-1
99.9976%
2
12.75 mins
Amazon EC2
ap-southeast-1
100%
0
None
Amazon EC2
ap-southeast-2
99.9983%
3
8.98 mins
Amazon EC2
eu-central-1
99.9997%
1
54 secs
Amazon EC2
eu-west-1
99.9999%
1
19 secs
Amazon EC2
sa-east-1
99.9947%
3
27.78 mins
Amazon EC2
us-east-1
99.996%
5
21.18 mins
Amazon EC2
us-west-1
99.9998%
2
9.12 mins
Amazon EC2
us-west-2
100%
0
None
BareMetalCloud
miami-fl-usa
99.9398%
40
5.27 hours
Blue Box VPS
ashburn
99.9892%
4
1.15 hours
Blue Box VPS
seattle
99.9968%
11
16.77 mins
BlueLock vCloud
indianapolis
99.9971%
6
18.67 mins
CenturyLink Cloud Servers
CA1
99.9735%
33
2.11 hours
CenturyLink Cloud Servers
CA2
99.9742%
23
2.05 hours
CenturyLink Cloud Servers
CA3
99.993%
10
30.32 mins
CenturyLink Cloud Servers
DE1
99.9857%
17
1.14 hours
CenturyLink Cloud Servers
GB1
99.9717%
27
2.26 hours
CenturyLink Cloud Servers
GB2
100%
0
None
CenturyLink Cloud Servers
GB3
99.9814%
8
1.05 hours
CenturyLink Cloud Servers
IL1
99.8753%
15
9.95 hours
CenturyLink Cloud Servers
NY1
99.9823%
8
1.42 hours
CenturyLink Cloud Servers
SG1
99.9287%
11
1.03 hours

Region and Availability zone/set

- Are provided by cloud service providers, incl. AWS, MS Azure, to meet requirements as :
    - More than one dedicated cloud sub-systems for redundancy in order to achieve high-availability services because:
        - All nodes in a DC cluster could share risks.
        - Customer does not know underlying system.
- All services must follow government / regional policy and regulations, e.g., personal data from EU.

AWS region and zone

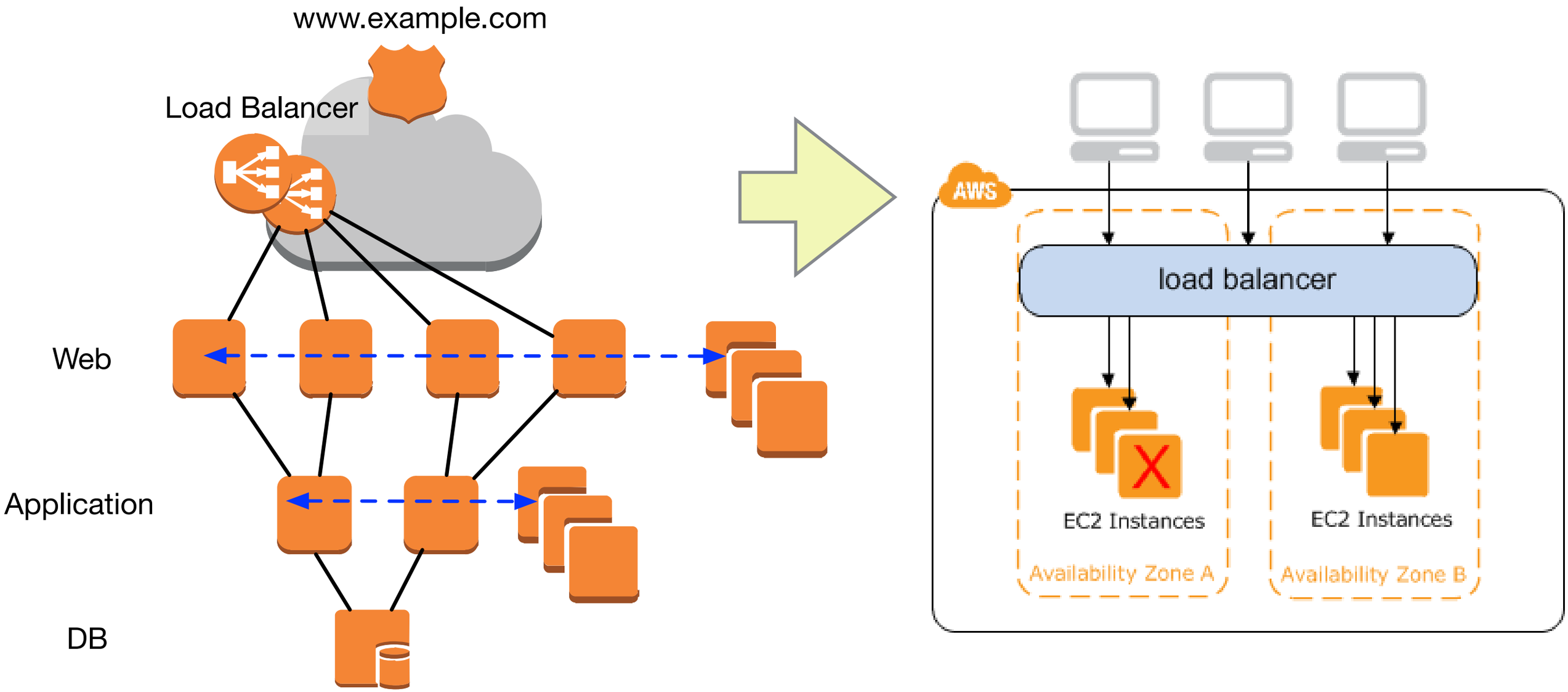


Amazon, “Amazon Elastic Compute Cloud: User Guide for Linux”, March, 2015.

Why “Availability zone” is not sufficient, or “Region” is required ?

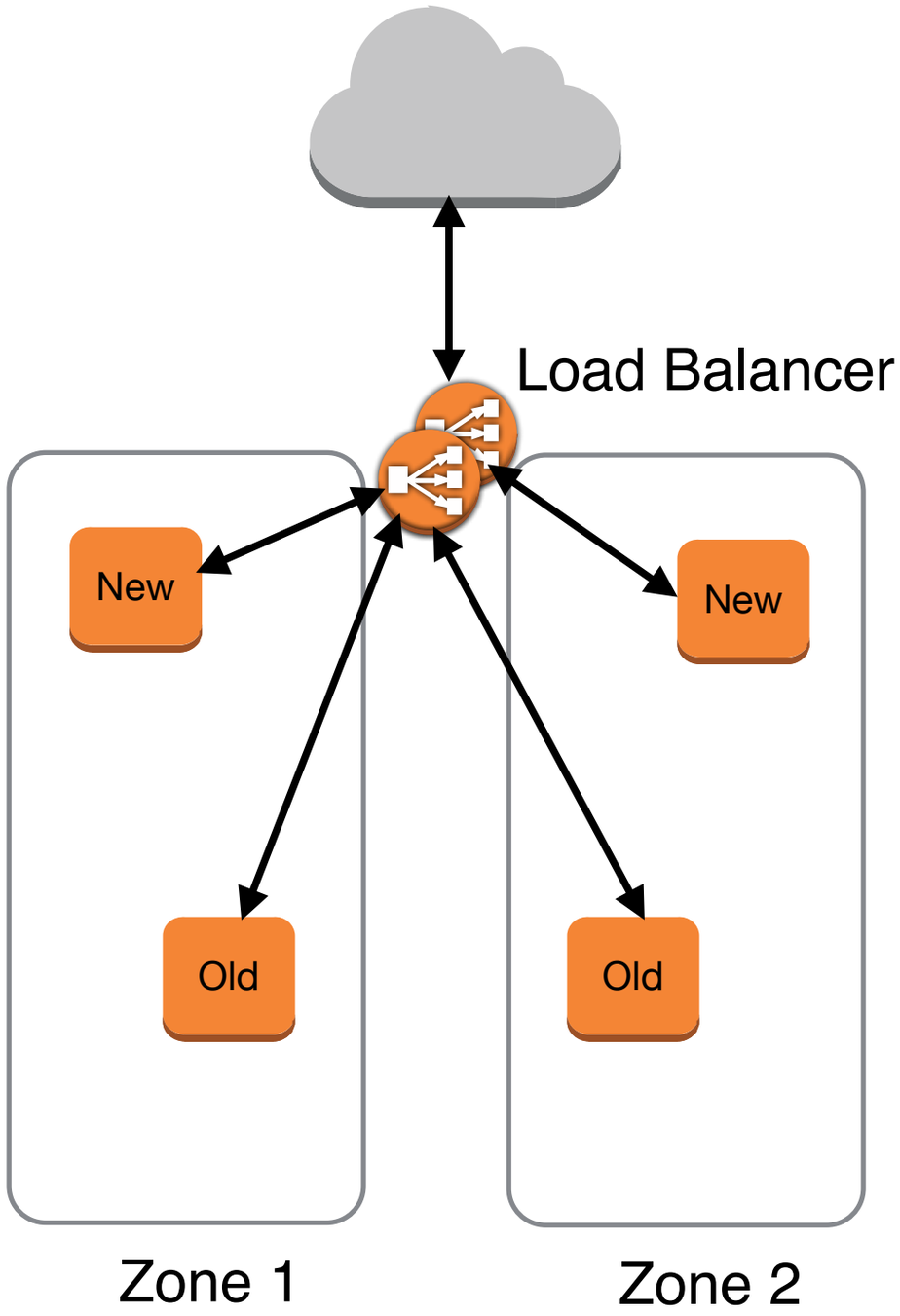
- Single location approaches even with more than one availability zones cannot reduce geographical / country risks, such as:
  - Engineering : Disaster, Infrastructure trouble e.g., telco. circuit cut, power outage
  - Not engineering : Law / Regulation depend on countries.
- “Region” also contributes :
  to improve customer experiences reducing network latencies.

3-tier Web architecture and scalability



“Elastic Load Balancing Developer Guide”, Amazon Web Services, 2016

Immutable infrastructure and disposable components in service upgrade scenario



Today’s Assignment

- MS provides Azure Cloud Services, an IaaS, which offers Service Level Agreement (SLA) as 99.95% uptime. This SLA is applied when customers deploy two or more role instances in different fault and upgrade domains.

  Your Web service deployed on MS Azure is required 99.95% availability as well as Cloud Services. Therefore, the service configuration is a redundant that the applications run on different domains’ instances.
  Each application program is expected service down for maintenance, such as, to apply security patch, at least one per month.

- How long downtime is allowed at the monthly maintenance without any critical impact(*) on the availability ?

(*) Discussion about “critical impact” is welcome.

- Submit your answers in Japanese or in English via the course web.

本日の課題

- MS は Azure Cloud Services を 99.95% の可用性を SLA として提供している。この SLA の適用要件として、複数のドメインで 2つ以上のインスタンスの稼働が求められている。

- Azure 上に展開した Web サービスでは Cloud service と同等の可用性が求められている。
  したがって、2 つのアプリケーションプログラムを異なるドメインのインスタンスで稼働させる冗長構成とした。
  それぞれのプログラムではセキュリティパッチなどメンテナンスのため月間 1 回の停止が見込まれる。

- 可用性に深刻な影響を与えない月例メンテナンスに許される停止時間は？

  (*) 「深刻な影響」の考察があってもよい。

- 講義 Web フォームから記入すること。

Wikipedia より