IBM's Always On Architecture

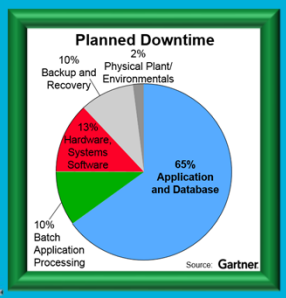
#zerodowntime

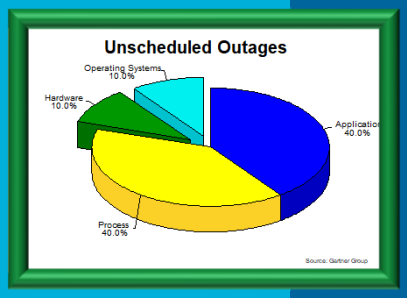
Presented by Dale McInnis, STSM, Hybrid Data Management Tech Sales
dmcinnis@ca.ibm.com @dalemmcinnis
Originally presented by
Herbie Pearthree, STSM, Acting CTO GTS Continuous Availability Hybrid Cloud Services
hpear3@us.ibm.com @herbiepear3

Agenda

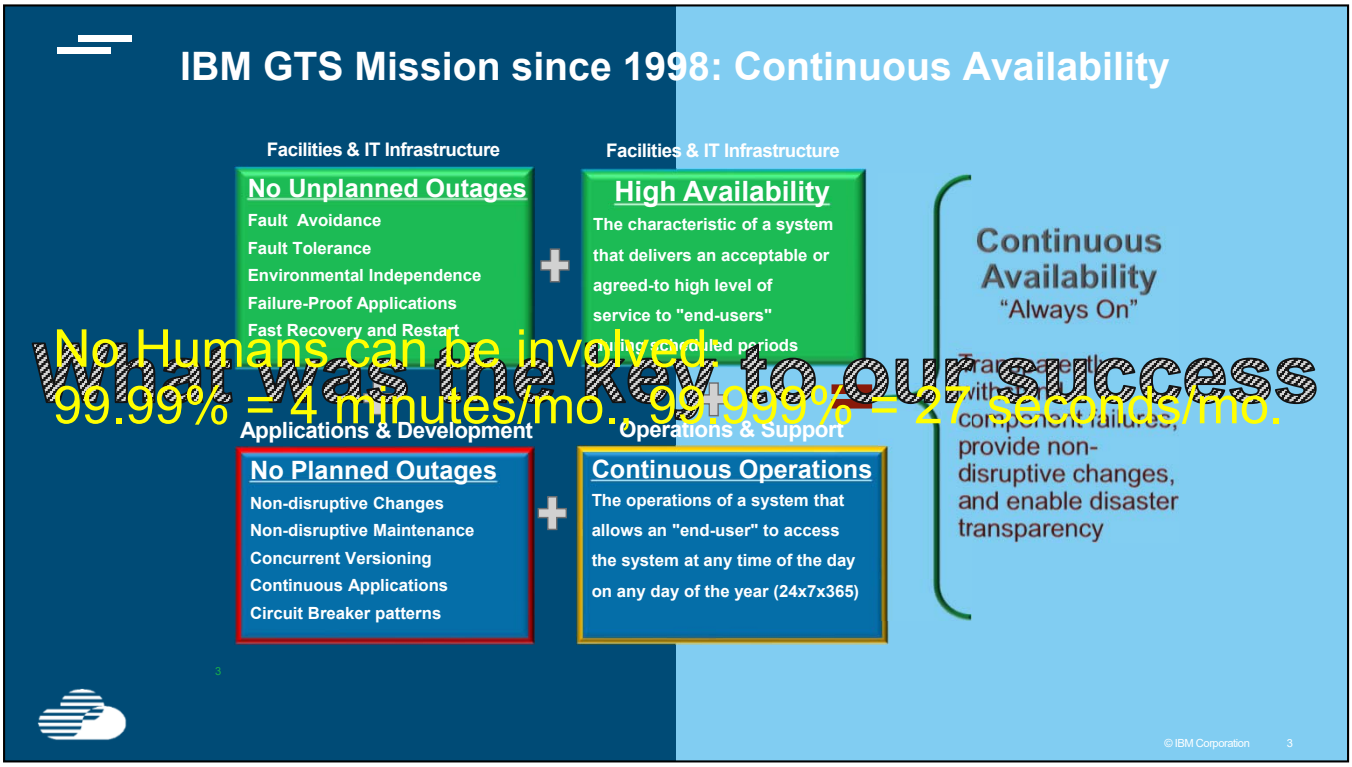
- Introduction
- Why Always On
- Always On Concepts
- Always on Journey

The Challenge: Get rid of these blockers!





© IBM Corporation



IBM GTS

Continuous Availability Services organization. In 1998, this organization was chartered from

their initial founding with the sole guiding principle of continuous availability. The mission was

clear and simple, failure was not an option after some visible failures occurred when trying to

rely on HA patterns and technologies and the reactive matrix delivery model. This new team

was given the continuous availability mission and left to design, implement, and manage the

Continuous Availability solution and the operational model. They were advised to question

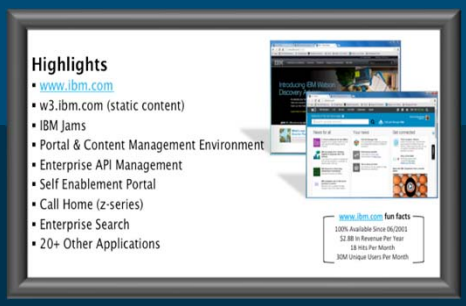
everything and empowered to change pattern solutions and operational processes to make

them more agile (within the constraints of audit and governance).

Our Internal Customers with Always On History

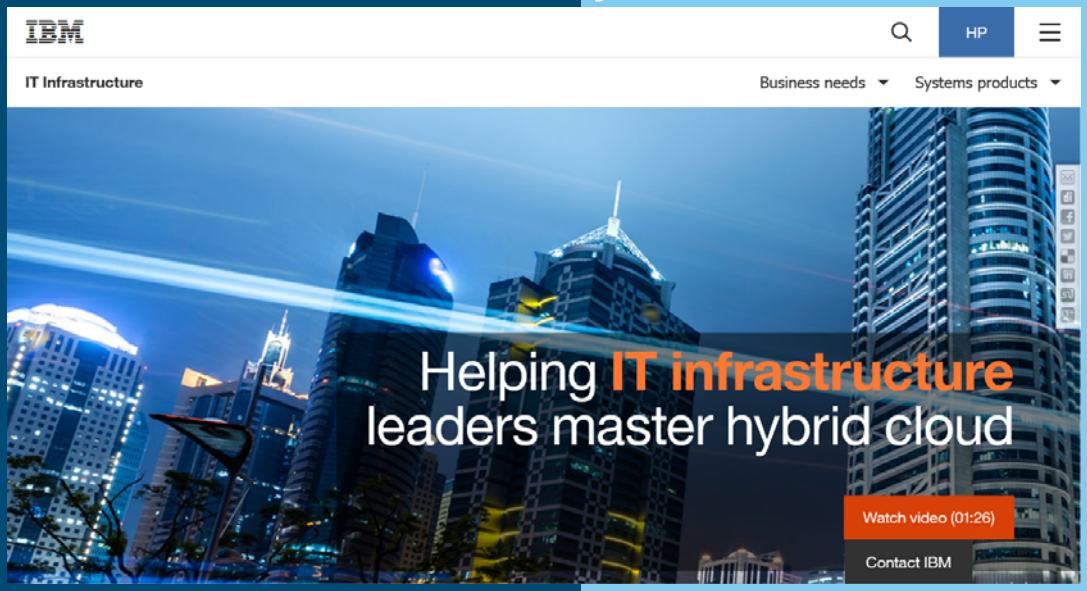
- **IBM Worldwide Sponsorship Marketing (25%) – where we push the "bleeding edge" while still guaranteeing Always On**
  - **e.g. The Masters, Wimbledon, etc.**
- **IBM CIO Digital Channels (75%) – benefit from the above "bleeding edge" efforts**
  - **e.g. www.ibm.com, Support Portal, SSO, APIgw, etc.**

With the expansion of IBM Digital Services (www.ibm.com, IBMaaS) the demand for continuous availability, continuous operations and continuous deployment increases the demand for always on platform services and operational method.



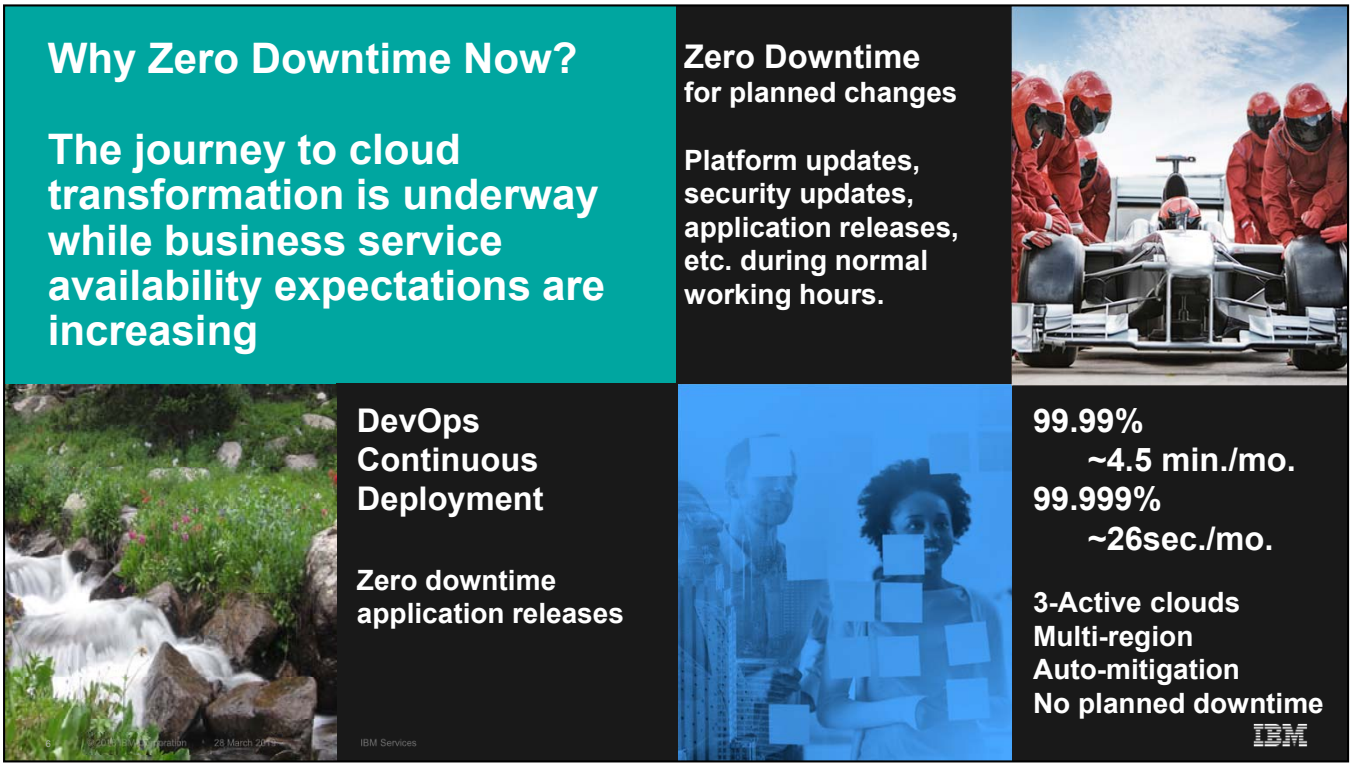
© IBM Corporation

www.ibm.com – Always-on since June 2001



For ibm.com, $1.8M USD per hour attributable to our corporate portal

© IBM Corporation



Why Always On now?

Many businesses have realized their web and mobile channels have become mission critical to their business. Their consumers have evolved to expect to be able to do business whenever they want, whatever time of day or day of week it is. Concurrently, businesses are expecting dev and ops teams to move at the speed of business.

Many CIO's are challenging their organizations to not only be more agile, but to also increase business service availability up into the realm to 4 and 5 nines. Consider the fact that 4 nines (99.99%) means there can be no more than 4 and a half minutes of planned or unplanned downtime a month. This also means that there can be no human involved in service recovery, therefore applications and the cloud platform must be designed in a way that enables the service to automatically bypass failed components and even failed clouds without requiring human intervention.

Everything breaks, we plan on it

Multi-region is a must-have
(unless you like recovery time)

Running the business service active in multiple-cloud availability zones and regions enables auto-mitigation of even disastrous regional failures, such as fires, floods and fools (bad operators or miscreants).

It also allows zero downtime for planned changes by changing only one cloud availability zone and region at a time.

$$ParallelAvailability = 1 - \left(\prod_{i=1}^{N} (1 - ComponentAvailability_i) \right)$$

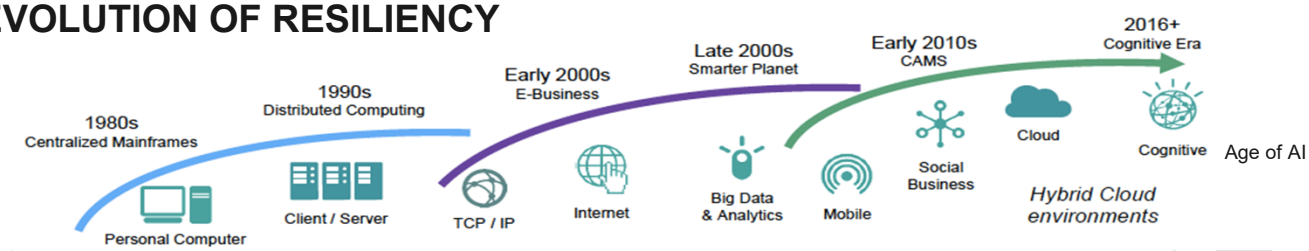
The importance in planning for availability is planning for failure. In order to mitigate failure within a data center or cloud region, it's important to embrace high availability methods within each data center (availability zone) or cloud region and include identical workloads in availability zones and regions.

Through using multi-region patterns, even the loss of an entire cloud region is automatically bypassed using global traffic management systems (like Akamai).

Why are our Clients asking for Always On?

Because their customers are always on

EVOLUTION OF RESILIENCY



Resiliency has become a business priority triggered by the need for "always on" service and for data protection.
With the growing complexity of hybrid environments, clients are looking for new solutions.

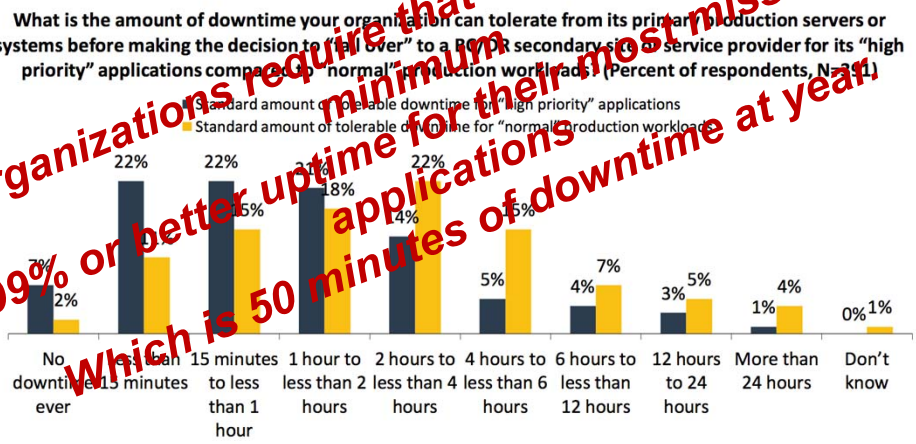
RTO* Trend	"Wave 1" Early 1989 – 2006	"Wave 2" Early 2007 - 2012	"Wave 3" Early 2012 – 2016+	"The next Wave"
	Time →			
	Weeks - Days	*Days - Minutes*	*Hours - Seconds*	*Minutes – Zero downtime*
	✓ **Infrastructure Recovery**	✓ **Cloud Recovery**	✓ **Resiliency for Business Process, Application, Data, & Compute**	✓ **Software Defined Resiliency**
	▪ Focus on recovery of systems & data ▪ Tape-based backup ▪ IT drives need for backups	▪ Focus on recovery of systems, data & applications ▪ Disk-based backup / replicas ▪ Regulations drive need for Disaster Recovery	▪ Customer expectations for "Always On" drives need for continuous availability ▪ Recovery of Applications up to business process ▪ Continuous replication ▪ Hybrid / Cloud Resiliency ▪ Automation	▪ Dynamic / cognitive orchestration & provisioning ▪ Continuous replication ▪ Backup & Recovery built in by software vendor ▪ Managing disparate backup & recovery environments as one ▪ Preventive Analytics ▪ Resiliency for IoT

9

*RTO : Recovery Time Objective

Over 50% of organizations said that their maximum tolerance for downtime was between 15 minutes to less than 1 hour for High Priority applications (and 28% said the same for normal applications)

Figure 1. Amount of Downtime Organizations Can Tolerate for Primary Production Systems Before Failing Over to BC/DR Site: High Priority Applications vs. Normal Applications



Source: Enterprise Strategy Group, 2016.

10

64% of organizations require that their databases deliver a minimum of 99.99% or better uptime for their most mission critical applications Which is 50 minutes of downtime at year.

Why Now? Resiliency events are front page news.

- **JUNE 2016 – Amazon AWS Sydney Availability Zone**
  - Last night's outage to an Amazon Web Services Sydney availability zone is prompting some of AWS' biggest local customers to reconsider their architectures to mitigate future damaging downtime.
- **JULY 2016 – Southwest Airlines** Computer Outage
  - Nationwide, the airline said more than 250 flights have been canceled for Friday – making the total number of canceled flights since Wednesday more than 1,000.
  - Outage will cost the airline between **$54 million and $82 million** in lost revenue and increased costs. Revenue losses including missed bookings, refunded tickets, canceled flights and vouchers will total at least $25 million. Additional costs including employee overtime, transportation, hotel and meal accommodations for stranded travelers and crew and other expenses will tally to between $28 million and $57 million.
- **AUGUST 2016 –** Power outage takes down **Delta** Data Center
  - Delta Chief Financial Officer Paul Jacobson said on a conference call with investors that the airline expected a $150 million drop in pretax income due to a power outage that shut down computer systems in August. The incident forced Delta to cancel 2,300 flights over three days and highlighted airlines' fragile technology infrastructure.

SOUTHWEST

Estimated

-$54 to $82 M

DELTA

Estimated

-$150 M

IBM Internal Use Only

http://www.datacenterknowledge.com/archives/2016/01/14/verizon-data-center-outage-delays-jetblue-flights/

http://www.cleveland.com/travel/index.ssf/2016/07/southwest_airlines_computer_ou.html

http://www.wfaa.com/news/local/southwest-airlines-computer-outage-costs-could-reach-82m/296158194

https://www.thestreet.com/story/13675074/1/delta-outage-will-mean-a-120-million-loss-and-more-humility-analyst-says.html

TRADITIONAL THINKING

IBM Resiliency Services provides standardized High Availability and Disaster Recovery solutions today, where planned and unplanned downtime cause digital service disruption, impacting both financial obligations and brand.

- **High Availability**
  - Protects against infrastructure outages within a data center
  - ***Does not protect against data center failures***
- **Disaster Recovery**
  - Protects against large-scale infrastructure and data center outages.
  - ***Requires some level of downtime*** *while systems are recovered* – dependent on the solution. Near-zero downtime solutions are most expensive.
  - *Data loss is dependent on solution.* Near-zero data loss solutions are most expensive.
  - ***Requires extensive program management, maintenance, annual testing.***

Move from Disaster Recovery To Disaster Avoidance

12

IBM has proven that we can deliver Always-On for www.ibm.com and major events (e.g. The Masters), and we can now make this available as a standardized, modular service from Resiliency Services

Craig Coffey, Resiliency Services Leader, Asia Pacific

- "Continuous Availability has become an **increasingly regular topic with banks and manufacturing firms** who are beginning to see the intangible impacts of an outage as more significant than the monetary ones."

VP IT Architecture Emirates Airlines

- "Don't talk to me about Disaster Recovery, we can't afford that much downtime" (paraphrased from conversation with Herbie Pearthree)

CIO REA Group Nigel Dalton – post Sydney AWS outage

- Multi AZ and ultimately, multi-region, with some smart architecture for deployment is key to cloud resilience today

13

REFERENCE
USE CASES

What are the Always On Concepts?

It's a combination of people, process, IT and resilient applications

Always On methods are based on people, process, apps and IT.

The apps provide resiliency!

Psst…the IT is the easy part

- **PEOPLE:** Manage end-to-end operations as **one focused team** aligned to the business service vs. technology silos
- **PaaS:** Design a Continuously Available Platform with **patterns** that fit the business application requirements (RPO & RTO)
- **Business Application:** Mandate resilience in architected **patterns** that **fit the platform**
- **Process & Governance**: Ensure business, development, and operational processes are integrated, agile, and focused on the availability of the service – know how it works, know how it fails

What is the most Challenging aspect?

© IBM Corporation

THINK DIFFERENTLY - DIGITAL FORMS OF ENGAGEMENT DRIVING DEMAND FOR ALWAYS-ON SERVICES

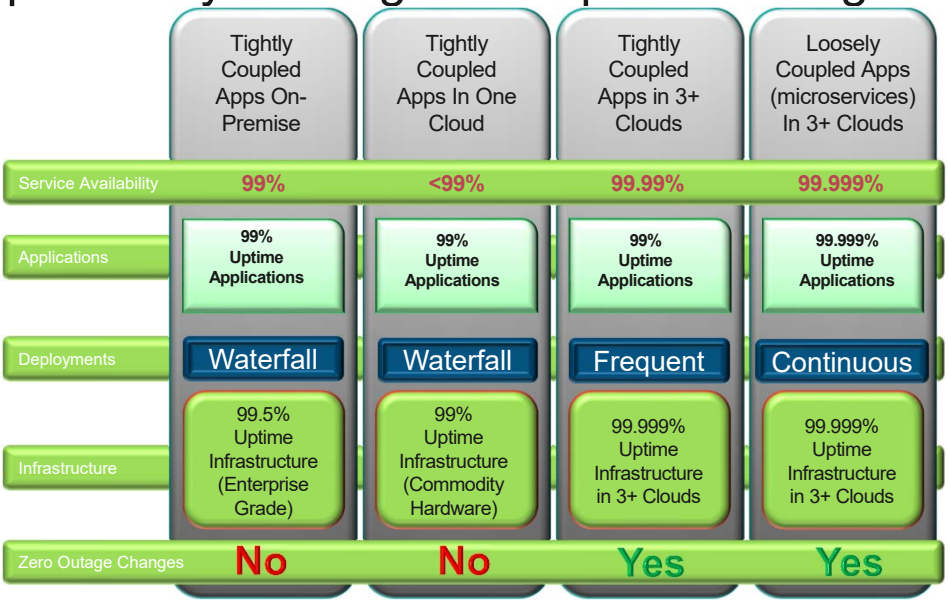
THINK DIFFERENTLY

Consider **deploying** cloud enabled and cloud native SoE workloads in **two or more regions**. This pattern enables disaster avoidance rather than disaster recovery, allowing for digital services availability even with an entire region being down. Enterprises also gain greater agility required of dev/ops processes including Continuous Deployments with zero downtime.

ALWAYS-ON

Protects against large-scale infrastructure and data center outages.
Zero downtime. Near-zero data loss.
Reduced program management requirements.

The Cloud doesn't make an application agile or resilient, the app does by running in multiple cloud regions



Enabling the IT platform

is as straightforward as implementing the three enabling technologies:

Global traffic management, which intelligently routes users to one of the service "clouds"

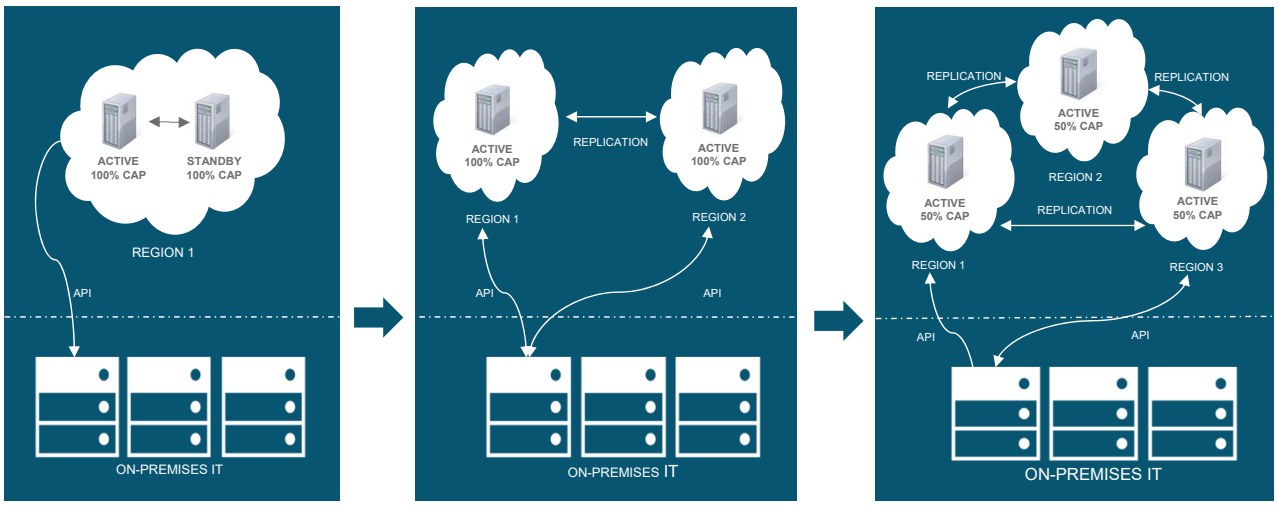
Non-persistent application data grid where sessions and non-persistent data can be

replicated across "clouds"

Guaranteed application level data replication, which enables data to persist in all clouds

whether it fits the requirements of Atomicity, Consistency, Isolation, and Durability (ACID)

Always On Hybrid Cloud Approach



Production Capacity	200%	200%	150%
Platform Availability	99.5%	99.999%	99.99999%
Failure Impact	100%	50%	33%
Maintenance Windows	Yes	Sometimes	No

3-Active "Always On" Method born in IBM in 1998

(Also common with the "Internet generation" companies e.g. Amazon, Facebook, Google, Netflix, etc.)

People and Process – The Most Challenging

- Proactive End to End Fully Managed Model
- Technical Leaders Responsible for the Business Service
- Dedicated SME staff aligned to business services
- Global distributed staff for 24x7x365 coverage
- Virtual Colocation for efficient communications
- Daily Change Management calls, Agile Delivery, Continuous Operations

IT Technology – The Easy Part!

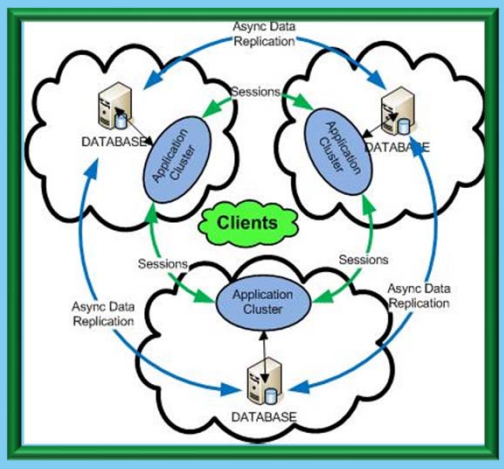
- Platform as a Service designed for Always On
- Identical in all 3 locations – all live
- Automated and end-to-end monitored
- No HA takeover, all components live

Enabling Technologies not in HA Solutions:

- Global Traffic Management
- Application Session Replication Grid (if sessions)
- Bidirectional Peer-to-peer Logical Data Replication

Application Developers Must Think Differently

- Platform mandates Non-Functional Requirements
- Think "Integrate across the WAN" – decouple apps
- Non-destructive updates/releases/schema changes
- Embrace eventual Data Consistency
- Must Generate Unique Indexes/Keys/etc.
- Explicit SQL required for data conflict remediation



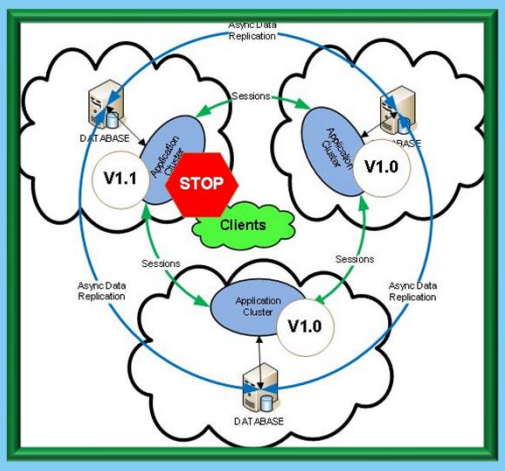
3-Active Platform as a Service
Always On, Continuous Operations
150% Compute, Memory & Network

© IBM Corporation

3-Active Continuous Operations Delivery – Concurrent Versioning

Zero Downtime Changes
One cloud at a time while the others provide the business service

Zero Downtime Change Process
- Same person(s) perform change everywhere – two person rule
- Technical lead orchestrates change
- De-advertise first service site from world
- Silence service alerts from this site
- Perform changes:
  - Non-destructive schema updates
  - Non-destructive app deploys
- Perform QA with health-check app
- Second person verifies QA
- IF Anything found wrong, leave down for problem determination and remediation
  - If app issue, back out to previous
- Un-ACK alerts for service
- Advertise site back to the world
- **AT THIS TIME WE HAVE 2 VERSIONS LIVE – "SNAP" method can mitigate**
- Go to next site, repeat, next site, complete



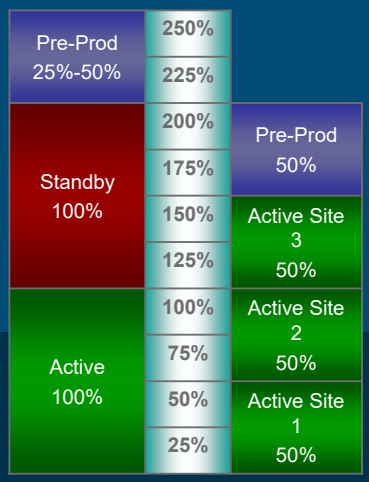
Non-disruptive releases make this possible

© IBM Corporation

Wait, What? 3 is Cheaper than 2?

When compared to a traditional active standby environment, 3-Active improves cost performance through the more efficient utilization of available resources. Compared to 2-Active, less cost and less risk.

	Active / Standby	2-Active	3-Active
Production cpu/ mem/ network capacity	>200%	>200%	>150%
Production Capacity with Out of Region DC	>200%	300%-600%	>150%
Platform Availability	99.5%	99.999%	99.99999%
Availability during Planned Changes	99.5%	99.5%	99.999%
Failure Impact	100%	50%	33%
Disaster Recovery Time	Hours to Days	0 to seconds in region, hours to days OoR	0 in region to seconds OoR
Incident Response	Manual Failover	Automatic Bypass in region else manual	Automatic Bypass
Maintenance Windows	YES	Sometimes	No



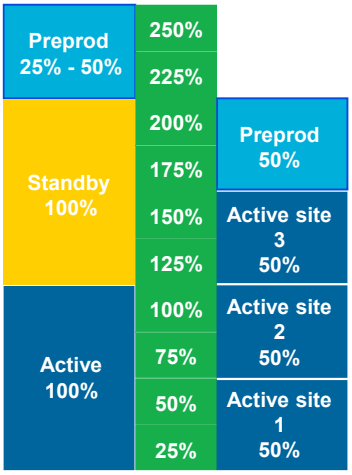
NOTE: Storage capacity does not follow the 50% rule

© IBM Corporation

Why 3-active for continuous availability?

	Active/ standby	2-active	3-active
Production cpu/mem/ network capacity	>200%	>200%	>150%
Production capacity with out-of-region DC	>200%	300% - 600%	>150%
Platform availability	99.5%	99.999%	99.99999%
Availability during planned changes	99.5%	99.5%	99.999%
Failure impact	100%	50%	33%
Disaster recovery time	Hours to days	0 to seconds in region, hours to days OOR	0 in region to seconds OOR
Incident response	Manual failover	Automatic bypass in region else manual	Automatic bypass
Maintenance windows	Yes	Sometimes	No
Recovery Point Objective	0	0 in region	> 0 Out of region

NOTE: Storage does not follow the 50 percent capacity rule



Cost efficiency
When compared to a traditional active/standby environment or even active/active, 3-active improves cost performance through the more efficient utilization of platform resources.

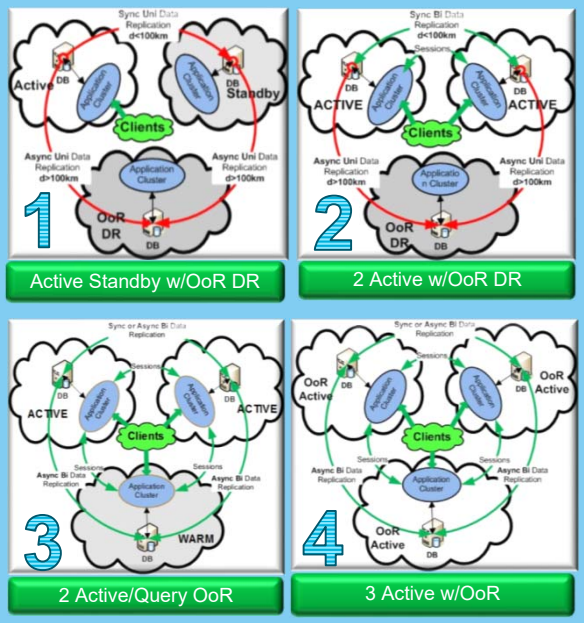
Flexibility #zerodowntime:
With 3-active, changes can be performed one cloud at a time while serving the business service live from the other two clouds with full capacity.

Locality: Business services run from clouds closest to your clients.

SOR data consistency:
For data that requires absolute data consistency and a recovery point objective (RPO) of zero, two clouds must be in region within synchronous distances where all data writes occur. The third out-of-region (OOR) cloud can be used for local data reads, batch jobs, analytics and meets disaster recovery (DR) governance requirements.

Assess & Design the Application's Resiliency Pattern

Architecture	Description
#1) Active Standby Metro / OoR DR 300%? Capacity	• **HA**: 100% Active, 100% Standby, <100% DR • **RTO** = minutes within metro, hours to days for OoR DR • **DATA**: Sync block level replication, async DR • **RPO=0?**
#2) 2 Active Metro / OoR DR 300%? Capacity	• **nCA**: <100% Active, <100% Active, <100% DR • **RTO** = seconds within metro, hours to days for OoR DR • **DATA:** sync block level replication, async DR • **RPO=0?**
#3) 2 Active Metro / OoR Query 300%? Capacity	• **nCA**: <100% Active, <100% Active, <100% Standby • **RTO** = seconds within metro, minutes to hours to warm OoR • **DATA**: sync block level or async logical replication within region, async logical replication OoR • **RPO=0 to seconds OoR**
#4) 3 Active OoR (or 2-Active metro, Active OoR) 150% Capacity	• **CA**: 50% Active, 50% Active, 50% Active • RTO = seconds to minutes •**DATA:** async logical replication write everywhere • **RPO = 0 to seconds OoR** •**RISK** = Eventual Data Consistency



Patterns 3 & 4 Include out of Region and rely on application level data replication, not storage level data replication

© IBM Corporation

#1 This is the standard and traditional Active/Standby with OoR DR model. It provides only HA. Often, the Active/Standby pair is within the same data center and therefore provides no

protection from a data center catastrophe (FFF: Fires, Floods, or Fools).

#2 typically seen in the mature financial sector where continuous availability is required during business hours and the RPO=0 or data consistency requirements are ACID.

Planned changes can be performed in off hours, because mature organizations can shorten the planned outage duration using staggered deployments and upgrades.

The active pair is within synchronous distance (typically < 40 km (24.8 miles)) allowing writes to occur on both sides of the Active/Active pair (GDPC/GDPS)

#3 more mature version of the previous Active/Active with OoR DR pattern. This is most likely as far as we can take an organization whose data policies require RP0=0 and ACID consistency requirements and DR requirements. DR scenario, it is instead integrated into day-to-day operations and can be

used for analytics, reporting, batch processing, read only queries, and in fact might be used as an Active component when maintenance is required on a component affecting both the Active pairs within the Metro

#4 This is the 3-Active model (Figure 7) that has been used to keep IBM.com always on since June 2001 and fully uses business service parallelism, which is also referred to as *“N+2” resiliency*. The key business decision enabling this pattern is that of eventual data consistency. Data can be written to any of the three “clouds”; it is captured at the source; and it is applied to its two peers with a replication delay based on the distance between the data centers.

Active Standby with Out of Region DR
High Availability within Metro

People and Process: RTO minutes to days

- Silo or matrix based delivery model
- Reactive – Incident Management and Service Restoration
- Legacy Change Management Process
- Disaster must be declared to switch to OoR

IT Technology Overview – Old and Proven

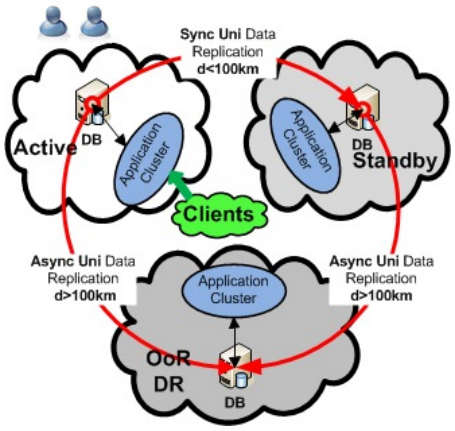
- Standard HA Methods
- Active Standby Pair can be in same DC or Metro
- Standby often used for dev/test/preprod!
- HA and IP takeover for OoR DR

Enabling Technologies

- Block Level Sync and Async Replication

Applications

- No Changes required



Active Standby Metro Pair with OoR DR
Capacity > 250%

24

This is the standard and legacy active/standby with Out of Region DR model. Often, the Active/Standby is within the same datacenter posing very high DR recovery times. Variants include the standby datacenter being in a different datacenter within a metro distance. Clients often use the standby datacenter for dev/test/pre-production increasing the recovery time if primary datacenter or any component failure brings down the active service. Much human effort is required to support this model. Incident management involves critical situations and service restoration, often not finding true RCA.

Active Active with Out of Region DR
Near Continuous Availability within Metro

People and Process: RTO seconds to days

- Matrix based delivery model plus business aligned support model needed for Continuous Operations
- Reactive & Proactive – Incident Management and Service Restoration, Auto-mitigation possible
- Legacy Change Management Process
- Disaster must be declared to switch to OoR

IT Technology Overview

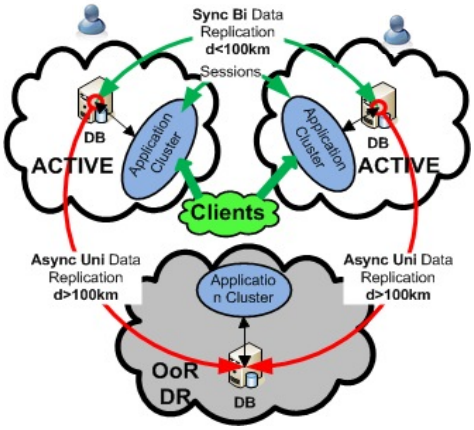
- Standard HA Methods plus sync & async replication
- Active Active Pair can be in same DC or Metro
- HA and IP takeover for OoR

Enabling Technologies

- Global Traffic Management
- Block or Logical level Sync and Async Replication
- Metro & Global GDPS/GDPC & "Q-Replication"

Applications

- Middleware Grid for session management
- May implement dual commit
- May implement logical bidirectional data replication



Active Active Metro pair with OoR DR
Capacity > 250%

25

This is the common pattern typically seen in the Financial Sector where Continuous Availability is required during business hours, and planned changes are managed in the traditional way – aka near Continuous Availability. Proactive Services Management thru the business application must be enabled. A focused support model is required for the platinum and gold applications (business services).

Active Active with Out of Region Query/Warm Near Continuous Availability Global

People and Process: RTO seconds to minutes

- Business Aligned focused support model
- Proactive Service Management: auto-bypass vs restoration where possible
- Agile Change Management Process
- No Disaster Recovery required

IT Technology

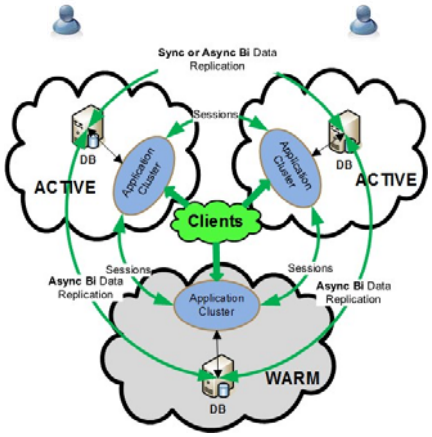
- Sync & Async logical replication
- Active Active Pair can be in same DC or Metro
- No DR – OoR used for RO, batch, reporting, analytics, and live during change of Metro pair

Enabling Technologies

- Global Traffic Management
- Block and Logical level Sync and Async Replication – Consistent writes go to metro pair
- Metro & Global GDPS/GDPC and "Q-Replication"

Applications

- Middleware Grid for session management
- App or technology may implement dual commit
- Logical bidirectional replication may mandate application mitigation and changes
- Application may implement "soft locks" to use OoR



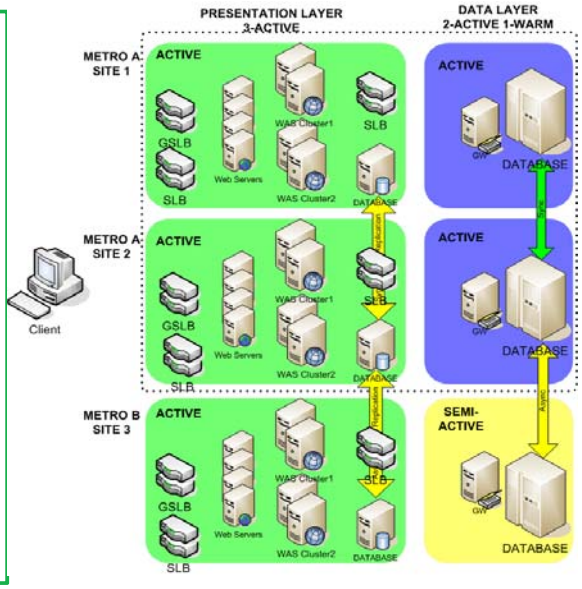
Active Active Metro pair with OoR Query/Warm Capacity > 250%

This is as far as we could take the Financial Sector where Continuous Availability is required as is absolute data consistency. Absolute data consistency requires metro distances of no more than 40km, or significant application enhancement to mitigate data consistency issues across the OoR distance (soft locks with timeout pre-write). Proactive Services Management thru the business application must be enabled. A focused support model is required for the platinum and gold applications (business services).

Hybrid: 3-Active Application Tier
2-Active Metro/1 Warm OoR Data Tier

RPO=0 Data Layer
Absolute data consistency
- **Writes only occur in 2-Active metro**

- **3-Active Presentation Layer**
  - Site 1 read/writes site 1 Database
  - Site 2 read/writes site 2 Database
  - Site 3 read/writes site 1 or site 2 DB
- **Site 1 and Site 2 are within 70km**
  - Synchronous Replication
  - GDPS / GDPC Hyperswap Mgr
  - Active-Active DB2
- **Site 3 – Geographically Remote**
  - Asynchronous Replication
  - DB2 LUW HADR
  - InfoSphere Replication Server
    - Parallel MQ transport reduces latency
  - Data Layer has multiple uses
    - Query/Warm Standby
    - Planned changes in Metro A
    - Batch Processing
    - Reporting
    - Partitioned Active



27

Another perspective on a 3-Active presentation and business logic tier where we gain the benefit of 3-Active zero outage changes for everything besides the data tier. In this model, **absolute data consistency is guaranteed as the writes only happen in the 2-Active data tier**. Note the semi-active OoR database can be used for query purposes, integrated into the change process when needing to bring down the metro data tier.

There can of course be many variations on how to do this. **The data tier can be exposed as a service, with write requests routed to the write master, and reads routed to the local replicas**, users can be partitioned so they stay in Metro A or Metro B and do their writes on either but never both, Advanced application load balancing can be used to route all writes to the write pair in metro A, etc.

3-Active "Always On" Method born in IBM in 1998

People and Process – The Most Challenging

- Proactive End to End Fully Managed Model
- Technical Leaders Responsible for the Service
- Dedicated SME staff aligned to business services
- Global distributed staff for 24x7x365 coverage
- Virtual Colocation for efficient communications
- Daily Change Management calls, Agile Delivery, Continuous Operations

IT Technology – The Easy Part!

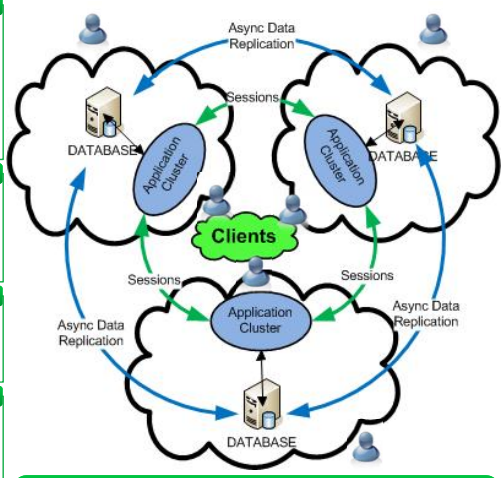
- Platform as a Service designed for Always On
- Identical in all 3 locations – all live
- Automated and end-to-end monitored
- No HA takeover, all components live

Enabling Technologies not in HA Solutions:

- Global Traffic Management
- Application Session Replication Grid
- Bidirectional Peer-to-peer Logical Data Replication

Application Developers Must Think Differently

- Platform mandates Non-Functional Requirements
- Think "Integrate across the WAN"
- Non-destructive updates/releases/schema changes
- Eventual Data Consistency
- Must Generate Unique Indexes/Keys/etc.
- Explicit SQL required for data conflict remediation
- Application may implement "soft locks" to mitigate data conflicts



3-Active Platform as a Service
Capacity 150%

28

This is the 3-active model that's been used to keep IBM.com always on since June 2001. Agile People and processes managing the end to end service. Technical leads aligned to the service interface with the client and the delivery teams to ensure business goals are met while orchestrating the zero outage changes. Staff is distributed globally as changes are done during normal business hours for all (follow the sun model). The technology is fairly straight forward, a platform designed from the ground up to enable continuous business services. No HA exists, all clouds are identical in all components, nearly everything is automated to ensure consistency.

Enabling technologies are the same as going two active with an out of region warm site – **global traffic management, clustered apps across the WAN, logical data bidirectional peer-to-peer replication.**

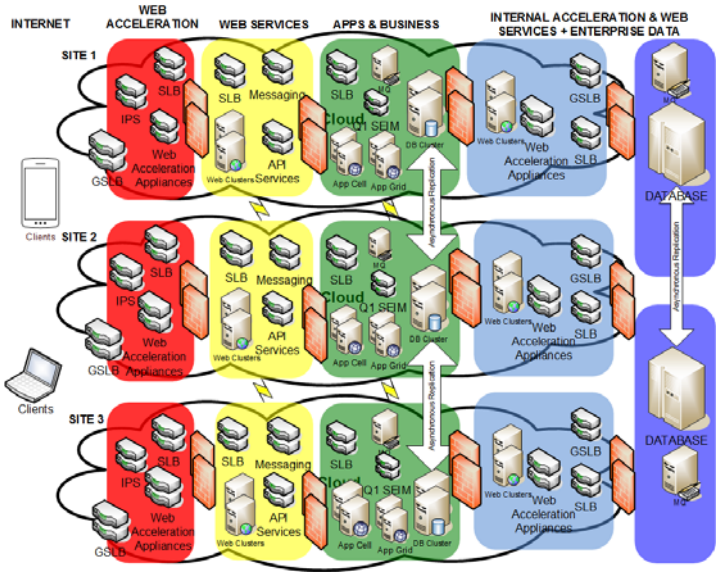
The risk in enabling the out of region cloud to be integrated into the read-write data layer is data conflicts. The logical replication (Q-Replication) can apply basic business rules to conflict remediation, though your conflict potential increases with the latency between sites and the volume of writes.

Applications must adapt and change to this, they must be uncoupled as they must be with 2-Active. Given the latency is a physics problem which cannot be broken, **the mitigation of data conflicts should be handled at the application layer**. Similar to sync methods of locking databases, applications must establish a "soft lock" mechanism to mitigate latency if this is required by the business. This means the **application checks for a soft lock prior to a write, if none, it sets a soft lock with a time to live on it prior to any data write, then waits the worst case**

replication delay before releasing the soft lock.

“3-Active” Resilient Architecture – www.ibm.com

- Platform as a Service
- www.ibm.com and other mission critical applications are 2/3 our business
- 1/3 business is IBM’s World Wide Sponsorship Marketing where we prove IBM’s technologies at The Masters, Wimbledon, etc.
- All Services Live in all sites – svc parallelism
- Applications designed to benefit from the platform architecture
- All components identical
- Nearly all tasks automated
- Failures automatically bypassed (mostly)



29

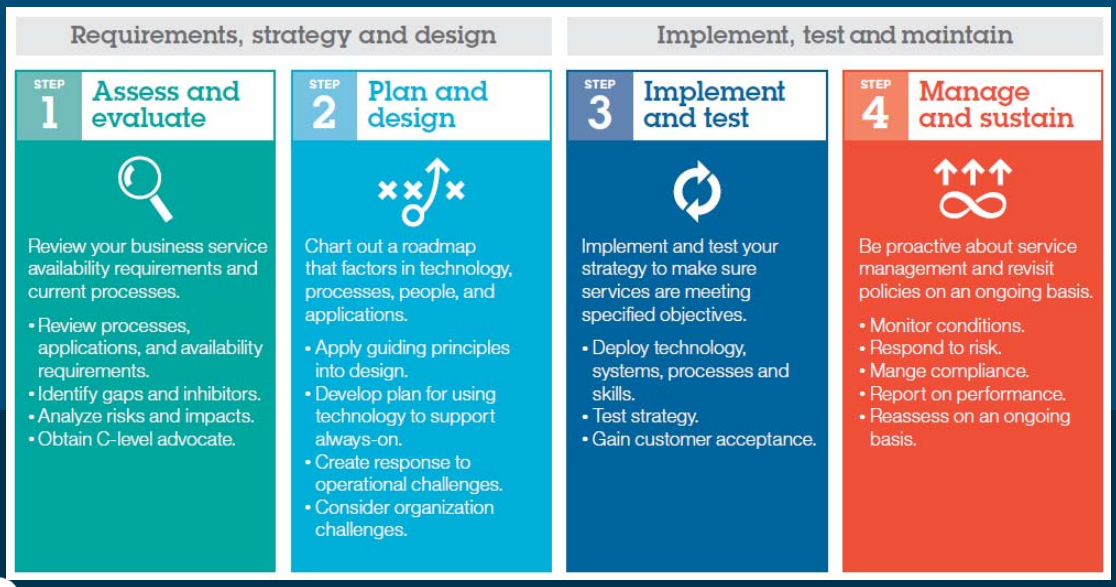
Here’s a high level component diagram. To note, all components are active in all 3 clouds at all times, except during planned and unplanned maintenance. NOTE: In the blue on the right, you’ll see some of our back office components where they’re configured in a dual-site active/warm method. We did this as most of the planned changes are done at either the presentation or business logic tiers shown as our web and app tiers, so we gain the benefit of zero outage changes for the things that change the most. The back office, which houses IBM’s massive client software/hardware/entitlement database, benefits by reducing it’s maintenance window down from an 8 hour change window to a 4 minute cutover for planned maintenance – in other words, 4 nines.

The Journey to Always On

It's a combination of people, process, IT and resilient applications

The Journey to Always On

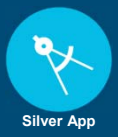
Follow these four steps to build an always-on platform aligned to your business goals.

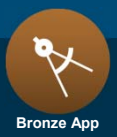


© IBM Corporation

Assess and Evaluate the Business Service Requirements

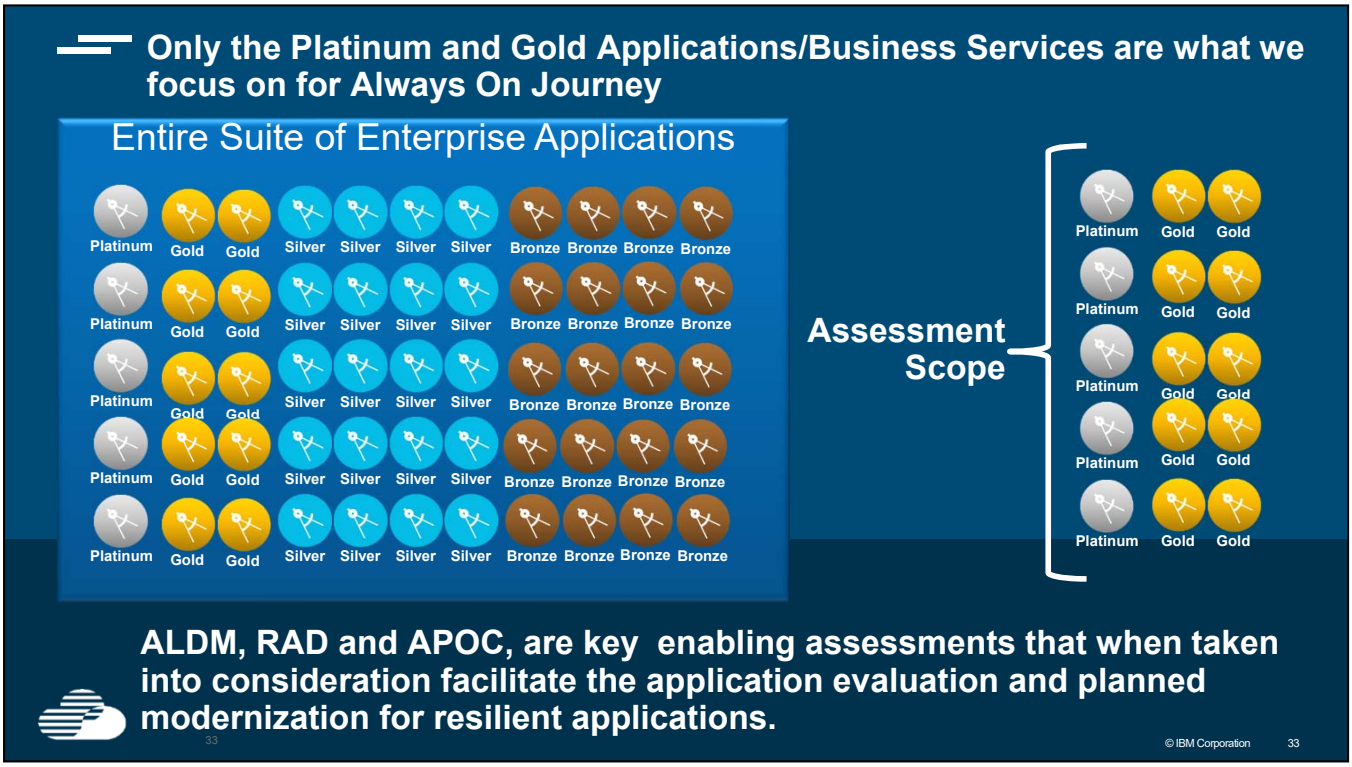
Business Criteria	Platinum <5% Continuous Availability "Always On"	Gold <5% Near Continuous "Almost Always On"	Silver 20-40% High Availability "Usually On"	Bronze 50-70% Moderate Availability
Business Function	✓ Targeted to applications & business functions that, if unavailable, will result in either financial or legal penalties based on regulatory restrictions	✓ Targeted to business applications and functions that present a potentially broad impact across the internal organization	✓ Targeted to applications that support analysis of business functions	✓ Targeted to non-critical, back-end, offline business functions
Business Impact	✓ Typically assigned to the **5-10%** of applications that drive revenue & profits	✓ During critical processing windows, must be available	✓ Typically backend processes with minimal impact to higher class services	✓ Typically less desirable methods are available to achieve same business function to support tolerance for extended outages
Tolerance for Downtime	✓ Ability to provide continuous availability 24x7x365	✓ Ability to provide constant availability within a defined processing window with availability requirements reduced outside the window	✓ Ability to provide consistent availability within a defined processing window	✓ Availability desired but not mandated with extended outages tolerated by business
Component Failure Impact	✓ Component and regional failures will not cause disruption in service	✓ Component failures should not present a disruption in service	✓ Redundancy at the subcomponent level limits outages based on a single subcomponent failure	✓ Potential outages due to single points of failure inherent within technology & application design
Maintenance and Change Impact	✓ Maintenance & changes required to be concurrent and/or staggered, with no interruption to service	✓ Maintenance & changes required to be concurrent or predefined outage window for change introduction	✓ Maintenance & changes require predefined outage window where changes can be introduced	✓ Maintenance & changes require a liberal outage window where changes can be introduced





Continuous Operations Required!

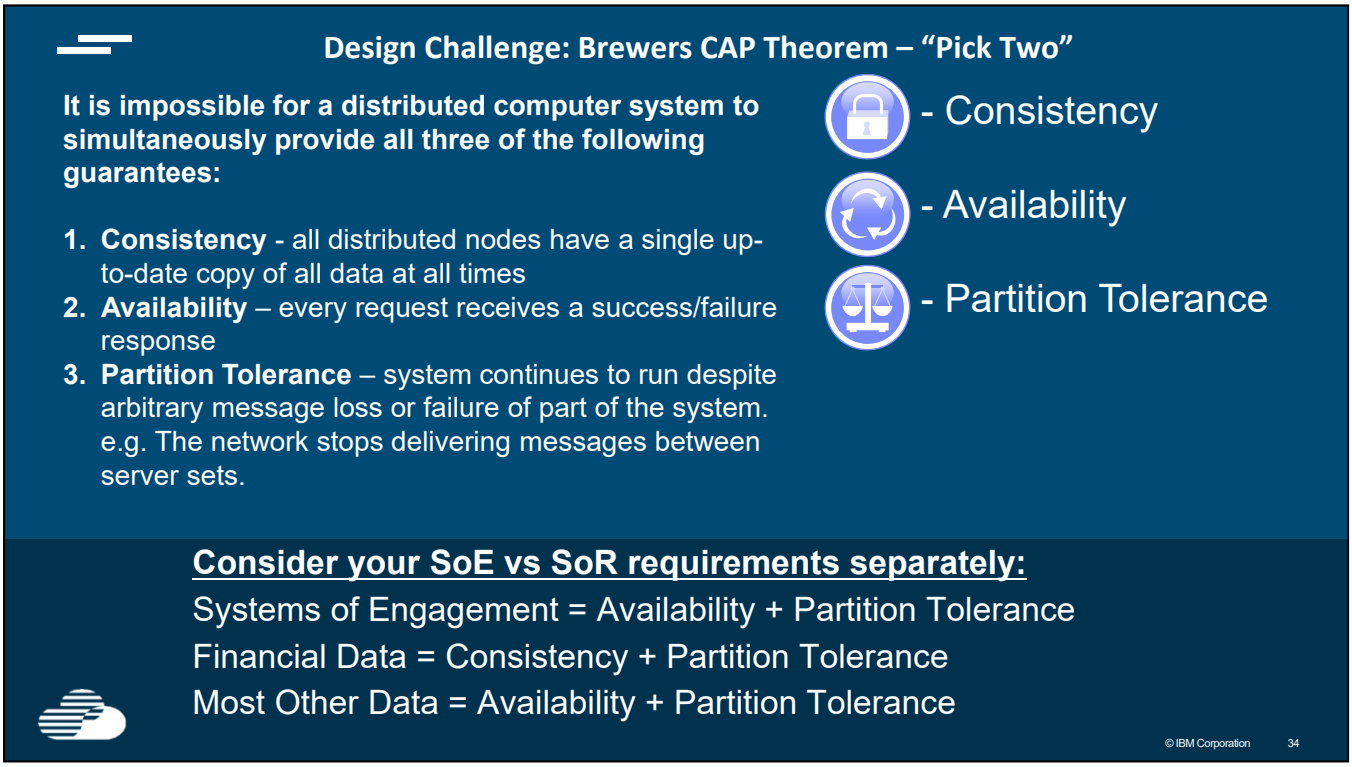
© IBM Corporation



ALDM- Analytics for Logical Dependency Mapping

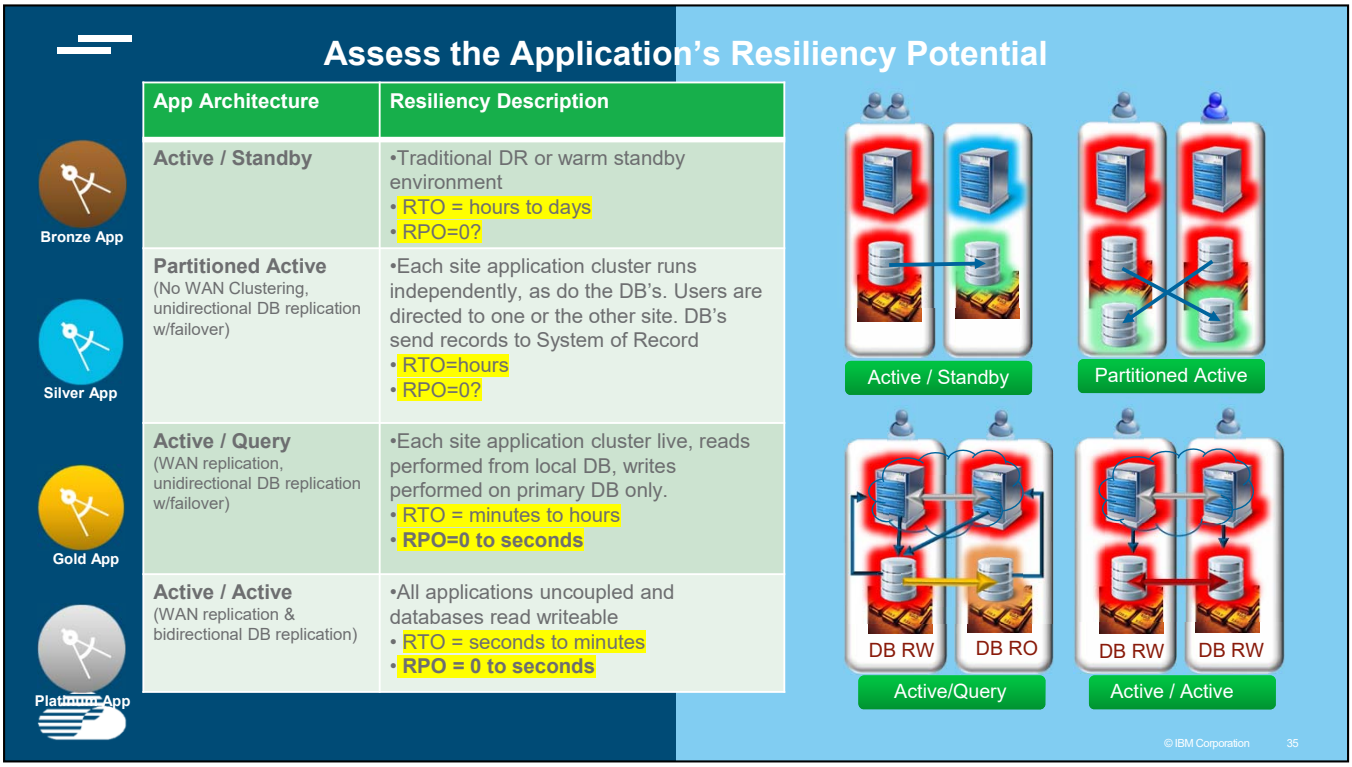
RAD – Rational Application Developer

APOC - Awesome Procedures on Cypher



Brewers CAP Theorem on distributed systems limits the technology solution to providing only two of the three guarantees:

- **Consistency**: All distributed nodes have a single up-to-date copy of all data at all times.
- **Availability**: Every request receives a success/failure response.
- **Partition tolerance**: System continues to run despite arbitrary message loss or failure of part of the system. For example, the network, stops delivering messages between server sets.



Active/Standby is the traditional architecture since the first IT failure

Partitioned Active is one step beyond Active/Standby in that both "clouds" can be used

with users directed to one or the other "cloud" and there are no application changes

required.

Asymmetric Active or Active/Query means that only one read/write database (also known

as *systems of record*) exists with the replicas being used for read-only workloads.

Active/Active means that all "clouds" provide the same service, with data reads and writes

at any "cloud" synchronized. This method provides transparent fault tolerance, even at the

"cloud" level.

Always On Guiding Principles (1)

1. **Core Principles** – transparently withstand component failures, provide non-disruptive changes, and enable disaster transparency
2. **Think Differently** – legacy architectural practices no longer apply
3. **KISS** – Keep It Simple Stupid, complexity adds obfuscation and prolonged service recovery
4. **Concurrent Versioning** – non-disruptive changes is the ability to run two versions at once
5. **Continuous Operations** – design in platform concurrency to enable non-disruptive changes
6. **Design each "cloud" identically** – best practices should be followed per "cloud", then interconnect
7. **Fail Small** – everything breaks, minimize the impact in design
8. **Virtualize Nearly Everything** – Virtualization provides flexibility and mobility, both essential
9. **Automate Nearly Everything** – avoid human error and inconsistency
10. **Design For Failure – know how it works, know how it breaks** and how to mitigate it's impact
11. **Applications Must be Designed for Failure** – fail gracefully, minimize impact to consumer
12. **Avoid HA Takeover – service parallelism** (clustering) is more reliable and faster
13. **Availability is provided by peer "clouds"** – failure in one "cloud" doesn't impact the others, the fault domain is isolated to each "cloud", service is still functional in the other(s)
14. **Share Nothing** – each cloud must be able to provide the business service independently, perhaps with reduced capacity (contingency planning enables critical functions during capacity reduction)

© IBM Corporation

Always On Guiding Principles (2)

15. **Availability Zones** – CA, near CA, and HA environments have their own architectural requirements and change windows, keep them separate, share nothing
16. **Add Global Traffic Management** – routes consumers to the best "cloud" to consume the service. Domain Name Service based, closely coupled with SLB and DNS services
17. If application must maintain state across "clouds**", use in memory application grid** – fast & tolerant and sessions must be small to take advantage of this technology, else don't use sessions beyond individual "cloud"
18. **Add Application Level Data Replication** – capture and apply changes to all peers. In order to provide fast failover or transparent service bypass, logical data replication is required to avoid human tasks. Bi-directional peer-to-peer allows writes anywhere, but OoR induces eventual data consistency.
19. **Never stretch a cluster across "clouds"** – extends fault domain beyond individual cloud
20. **Include Out of Region** – must mitigate 3-F's (Fire, Flood, and Fools) outside region, integrate it into your change practices
21. **Don't Forget Security** – the "Fools" can cause unexpected damage
22. **Don't Forget Performance Engineering** – Development must embrace performance engineering. Business must make development and operations aware of any planned media events that may bring "flash mobs" very early. Applications must be efficient. IT must be sufficient.

These guiding principles build upon the many guiding principles common in HA and DR design and are here to guide practitioners beyond core HA design.

© IBM Corporation

Always On New Technologies Deeper Dive

In order to run resilient clouds, we need to introduce:

- **Global Traffic Management**
  - Resolve www.ibm.com to the best responding clouds IP addresses
- **Session Grid**
  - I put these items in my cart and hopped clouds, cart's still full
- **Data replication**
  - Create, Read, Update, Delete data anywhere and everywhere
- **Ops Dashboard**
  - Business service XYZ is spitting errors in cloud 2, bypass it

- ✓ Global Traffic Management
  - ✓ Sends end user to the best cloud using Domain Name Service
- ✓ Session Grid
  - ✓ If Apps not session-less, need session grid to synchronize
- ✓ Application Level bi-directional, multi-master, peer-to-peer async data replication
  - ✓ Synchronize data
- ✓ "Single pane of glass" perspective of all cloud transactions and errors

© IBM Corporation

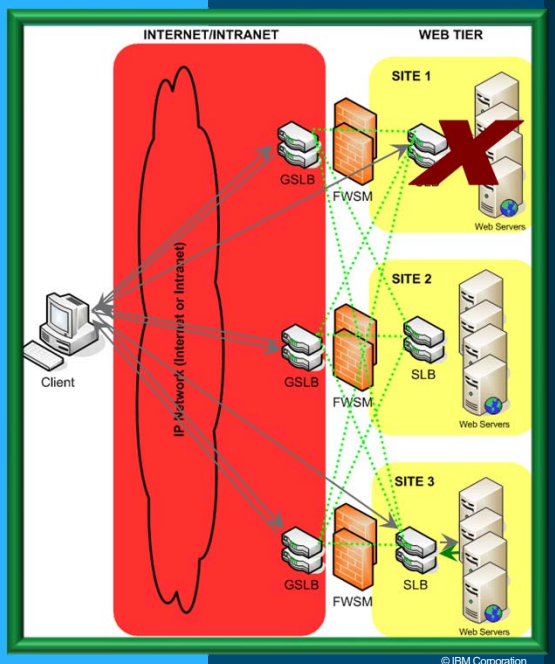
Global Traffic Management

DNS based Global Traffic Management (aka GTM/GSLB)

- GTM/GSLB determines best site based on metrics gained from itself and SLBs
  - Health Check
  - Response Time
  - Concurrent Sessions/Session Capacity
  - Geographic Preference
  - Session Availability, etc.
- DNS based, end user gets to best responding site, can customize rules for consumer or application needs, bypasses failed site and applications automatically – very short TTL

Externalized Geographic Load Balancing

- Global Traffic Management Service
  - E.g. Akamai, Dyn, FastLY, etc.
- Features similar to GTM/GSLB
- Must provide metrics via web page

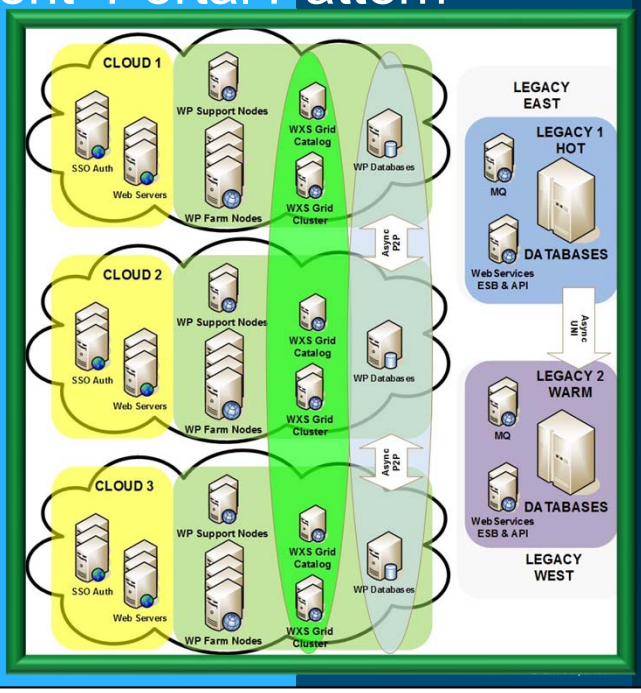


© IBM Corporation

Elastic and Resilient Portal Pattern

Portal was one of the most difficult platforms to solve the resiliency and scalability challenge…

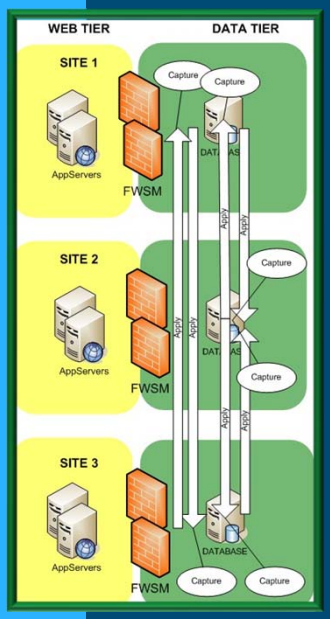
- **Each Cloud has Portal Support Nodes and Portal Farm Nodes**
- **Portal Farm nodes are easily cloned from support nodes for rapid elasticity**
- **Session Grid keeps sessions in sync**
  - E.g. WebSphere Extreme Scale, DB2, Oracle Coherence, Redis, etc.
- **Portal Databases are synchronized asynchronously with InfoSphere Replication Server in peer-to-peer**
- **Local databases hold non-sensitive data, Legacy databases are where the sensitive & secure data resides, access via web services, IEB, API's, MQ, etc.**



Write anywhere & everywhere DB

Resilient & Prioritized Asynchronous Data Replication (InfoSphere Replication Server)

- There is a delay with asynchronous replication and varies based on object sizes, applications may mitigate this to avoid data inconsistencies and conflicts
  - Define delay, debate pros & cons of soft locks
- Primary key on every user table to be replicated
- Identity columns must be set to GENERATED BY DEFAULT (instead of GENERATED ALWAYS)
- Primary keys must be generated such that they are guaranteed to be unique across sites
  - Change the PK into a composite key, adding a site_ID column to the existing PK.
  - Offset identity/sequence values across sites (start at 1, 2, 3 respectively, increment by 3)
- Explicit SQL required for queue replication (fields added for conflict resolution)
  - i.e. insert into department (dept_id, dept_name) values (1, 'App Team')
  - instead of: insert into department values (1, 'App Team')

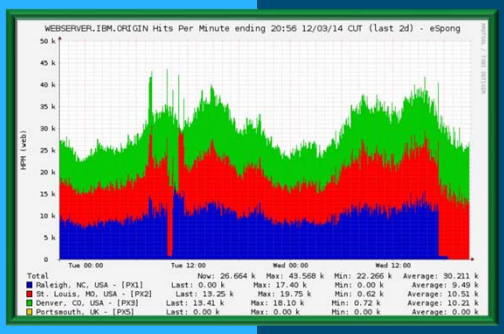


© IBM Corporation

Operations Single Panes of Glass

Operations must have an integrated view of the health of all systems and business services, in all clouds

- Monitor the IaaS, PaaS, from inside and outside
  - •Inside: Tivoli, Nagios, Ganglia, etc.
  - •Outside: Keynote, Dynatrace, etc.
- All applications/micro-services must have a "healthcheck" service verifying functionality and dependencies – circuit breaker pattern highly recommended
- Application Performance Monitoring is key to the health of business services
  - •IBM APM, AppDynamics, New Relic, etc.
- Real-time log collection and Insights
  - •Splunk, Elastisearch+ Logstash+ Kibana (ELK), etc.



© IBM Corporation

Questions?

Dale McInnis dmcinnis@ca.ibm.com
Herbie Pearthree hpear3@us.ibm.com

IBM RedPapers and Redbooks for more Always On Multi-Active Concepts
(Google "IBM Always On Redpapers"):
- "Always On: Assess, Design, Implement and Manage Continuous Availability"
http://www.redbooks.ibm.com/abstracts/redp5109.html?Open
- The Value of Active-Active Sites with Q Replication for IBM DB2 for z/OS An Innovative IBM Client's Experience
http://www.redbooks.ibm.com/abstracts/redp5140.html?Open

Assessment Offerings:
ALDM (Application Discovery & Dependency Mapping) https://w3.gsar.ibm.com/services/gsar/gda/sbb_details.xhtml?id=198
RAD (Resilient Architecture Design) for IT Infrastructure
https://w3-03.ibm.com/tools/cm/iram/assetDetail/generalDetails.faces?guid={E165A380-BF03-D415-D99D-05365A442683}&v=1.0&submission=false
APOC (Application Performance Optimization Consulting)
https://w3-03.ibm.com/tools/cm/iram/assetDetail/generalDetails.faces?guid=E8F68785-C147-47F9-27B7-21CA47102688&v=1.0&submission=false

Application Modernization – Cloud Native Application Design
- Top 9 Rules for Cloud Applications - Kyle Brown, IBM Distinguished Engineer , Bluemix
http://www.ibm.com/developerworks/websphere/techjournal/1404_brown/1404_brown.html

- "Going Cloud Native" – a great article with links on how to modernize services and organizations
http://CloudNative.online

© IBM Corporation