Carnegie Mellon

DevOps-Continuous Integration

Disaster Recovery

1

Carnegie Mellon University

Overview

- **Basic concepts**
- Data Strategies for Tiers 2-4
- Tier 1 Data Management
- Big Data
- Software in the Secondary Data Centers
- Fail Over

isr institute for SOFTWARE RESEARCH

2

Carnegie Mellon University

Terminology

- Disaster – event that makes a data center inoperable – flood, earthquake, tornado, power outage, etc
- Business continuity – keeping your business going in the event of a disaster
  - Involves customers, employees, protecting people and equipment
- Disaster Recovery – the IT portion of business continuity. Maintaining service to customers

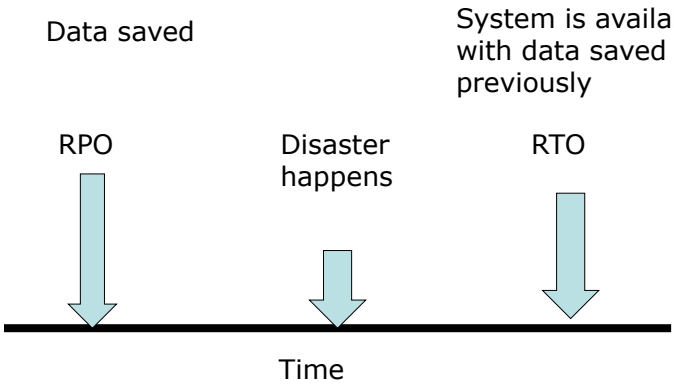
Carnegie Mellon University

Key measures per system

- RTO – recovery time objective
  - How long before system is in service again
- RPO – recovery point objective
  - How much data can be lost in the event of a disaster
- Will vary for each system in an organization

Carnegie Mellon University

Graphical representation



5

Carnegie Mellon University

Tiers

- Divide your systems into tiers based on RTO and RPO
  - Tier 1 (mission critical) – 15 minutes
  - Tier 2 (important support) - 2 hours
  - Tier 3 (less important support) - 4 hours
  - Tier 4 (everything else) - 24 hours

6

Carnegie Mellon University

Secondary data center

- When a disaster occurs, your data center will be out of operation for days/weeks/months
- You need a secondary (back up) data center

Carnegie Mellon University

Types of secondary data centers

- Warm – computing facilities in place but your software has not been loaded
- Hot – computing facilities in place with your software loaded and either executing or ready to execute. Current data not in data center
- Mirrored – computing facilities in place, current software in place and executing, data up to date.
- All secondary locations are geographically separated from primary data center

Carnegie Mellon University

Overview

- Basic concepts
- **Data Strategies for Tiers 2-4**
- Tier 1 Data Management
- Big Data
- Software in the Secondary Data Centers
- Fail Over

Carnegie Mellon University

Online or offline?

- Tiers 2-4 have recovery times in terms of hours
- Major decision is whether to keep data
  - Online – in a different region or availability zone or
  - Offline – on tape that is stored remotely from primary data center

Carnegie Mellon University

Considerations

- Volume of data
- Storage costs
- Encryption of data on tape
- Recovery time for tape from storage site
- Transfer time from online storage to secondary site

Carnegie Mellon University

Overview

- Basic concepts
- Data Strategies for Tiers 2-4
- **Tier 1 Data Management**
- Big Data
- Software in the Secondary Data Centers
- Fail Over

Carnegie Mellon University

Data in Tier 1

- RTO and RPO in minutes, not hours
- Data must be kept online and up to date in secondary data center
- Secondary data center must be mirrored.
- Database system can be used to keep transactional data consistent at both sites

Carnegie Mellon University

Non transactional Tier 1 data

- Non replicated data.
  - Session data may not be replicated
  - Requires user to log in again if disaster
- Slowly changing data
  - Static web pages, videos, other data changes only slowly
  - Can be kept up to date with configuration management system

Carnegie Mellon University

Overview

- Basic concepts
- Data Strategies for Tiers 2-4
- Tier 1 Data Management
- **Big Data**
- Software in the Secondary Data Centers
- Fail Over

Carnegie Mellon University

Big Data

- "Big Data" is a data set too large to back up
- Data is divided into groups – "shards"
- Each shard is replicated several times
  - For performance and availability reasons
  - Each shard is managed by database system that keeps replicas up to date

Carnegie Mellon University

Overview

- Basic concepts
- Data Strategies for Tiers 2-4
- Tier 1 Data Management
- Big Data
- **Software in the Secondary Data Centers**
- Fail Over

Carnegie Mellon University

Software in secondary data center

- Must be kept in alignment with software in primary data center
  - Version inconsistency may lead to behavioral inconsistency.
- Configuration management systems can work across data centers
- Deployment process for modified software should consider secondary data center

Carnegie Mellon University

Overview

- Basic concepts
- Data Strategies for Tiers 2-4
- Tier 1 Data Management
- Big Data
- Software in the Secondary Data Centers
- **Fail Over**

Carnegie Mellon University

Fail over

- Three activities to a fail over process
  - Trigger switch to secondary data center
  - Activate secondary data center
    - Involves ensuring data and software are up to date
  - Resume operations at secondary data center

Carnegie Mellon University

Trigger

- Manual or automatic
- In either case, the trigger is scripted so that it is a one button/command
- Automatic trigger should only be used with very short RTO
  - Requires data center failure detector that may have false positives
  - Any failover has business implications.

Carnegie Mellon University

Activate secondary data center

- Data and software must be brought up to date.
- If secondary data center is not mirrored, the last back up must be restored
- User requests sent to secondary data center
- Software is activated based on tiers

Carnegie Mellon University

Resume operations

- Make secondary data center be primary
- May need to locate a new secondary data center in case of disaster at currently operating center

Carnegie Mellon University

Testing fail over

- If you can afford down time, test during scheduled down time
- If no scheduled down time, then test using staging environment where care is taken to avoid corrupting production data base

Carnegie Mellon University

Summary

- RPO and RTO are basic measures to describe behavior in case of failure. Used to divide apps into tiers
- Secondary data center must be identified
- Tiers 2-4 can use back ups, either online or offline
- Tier 1 data has database support to keep copy at secondary data center up to date
- Software in secondary data center kept current with configuration management system
- Fail over is scripted and must be tested