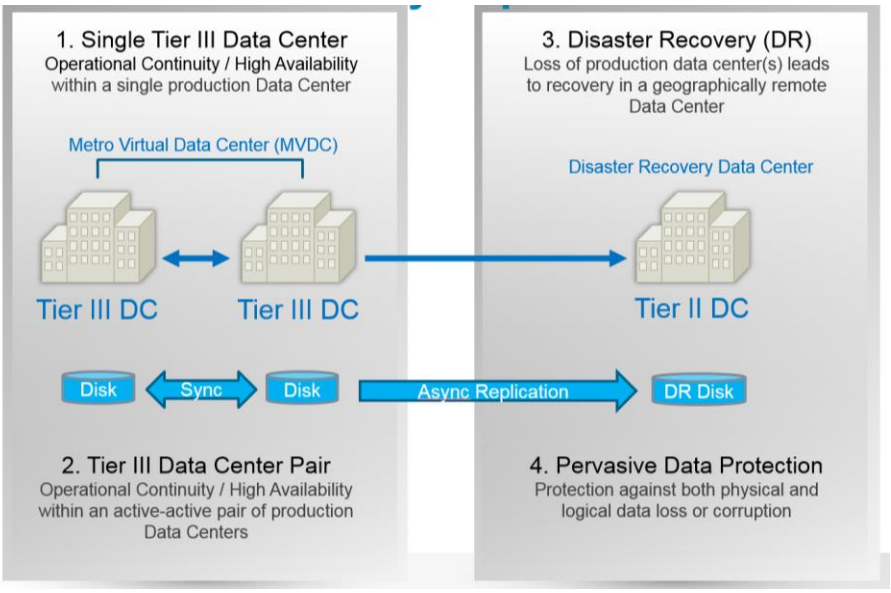
Cisco IT Methods

How Cisco IT Tested Data Center Failover

Introduction

Cisco revenues and reputation depend on our ability to continue operating during and after a major disaster. Our Texas Metro Virtual Data Center (MVDC) consists of two redundant data centers that can take over for each other with no downtime (Figure 1). If a major disaster takes down the MVDC, applications fail over to a data center in another region of the U.S. Ordinarily used for development and test, the remote data center can be quickly repurposed for production.

Figure 1. Cisco IT Resiliency



The Cisco® Risk Management and Resiliency Operations (RMRO) teams regularly test application failover. In December 2015, we became a frontrunner in testing data center failover. This article describes the readiness test we conducted to evaluate the processes and technology for simultaneously failing over our most critical IT services. Each service depends on multiple applications and databases. The test scenario was a fictitious solar superstorm that knocked out the power grid and the Internet in Texas. We established two success criteria: no downtime and full restoration in less than 48 hours. We exceeded the criteria, restoring services in eight hours with no production downtime.

Solution

Selecting the Applications for the Failover Test

Cisco's Chief Information Officer (CIO) asked senior leadership to identify critical services that must be restored on Day 1 of a disaster to prevent revenue loss. The leadership team identified 17 critical services. Examples include Employee Services and Supply Chain. IT determined which applications each service requires, and then selected for testing the subset of those applications that had to be running on Day 1. These applications were certified for disaster recovery, meaning that they had infrastructure in the disaster recovery data center and had been tested for failover.

Testing the Incident Management Process

We created a scenario—the fictitious solar superstorm—that would damage both the power grid and communications infrastructure. “We wanted the scenario to be as realistic as possible to set the scene and initiate the disaster recovery incident management process,” says Sal Pearce, Cisco IT manager.

Before the test, we validated the documented incident management process. “We walked through the process multiple times before the test to refine it,” says Sulbha Maske, Cisco IT risk manager. Here’s what happened on the day of the test:

- The RMRO teams contacted the regional IT group to check whether the disaster had affected IT. The regional IT group asked the local IT group whether all applications were operational. The answer: no, most critical applications were not operating.
- Concluding that failover was necessary, the regional IT group contacted the Cisco Incident Management (CIM) team, which is led by senior leadership.
- The CIM team escalated the decision about whether to invoke the disaster recovery process to the Executive Incident Management (EIM) team, which includes Cisco’s CIO and Chief Executive Officer (CEO).
- Our CIO decided that failover was necessary and instructed the IT Operations Command Center (ITOCC) to proceed.

Initiating Failover

After receiving the go-ahead, the ITOCC invoked the failover process:

- Pointed each application to the disaster recovery environment
- Brought up the application databases in the disaster recovery data center
- Brought up the applications in the disaster recovery data center
- Executed several transactions to confirm the application operated properly

ITOCC, application teams, technical teams, and management communicated throughout the test in Cisco Spark™ rooms. Immediately after the test the team brought down the applications and databases in the disaster recovery environment. Normal operations resumed in the MVDC.

Several Cisco solutions make failover possible. For example, Cisco Optical Network Switches (ONS) DWDM systems create a reliable, high-speed link between the data centers. If the MVDC network goes out, Cisco Global Site Selector and Cisco Virtual Routing and Forwarding (VRF) redirect traffic to the disaster recovery location. Using Cisco Unified Computing System™ and Cisco Nexus® switches in the data centers reduces space, power, and cooling costs.

Measuring Success

We set a goal to complete the failover test and resume normal operations within 48 hours. We were prepared to review progress at 45 hours and abandon the test if necessary. It wasn’t. “We exceeded our goals by bringing up the participating critical apps in less than eight hours,” says Mark Zelent, IT project manager. Individual services, such as the Cisco Product Catalog, were restored in approximately one hour.

We successfully restored all but a handful of applications in the disaster recovery environment. The few exceptions were coded in a way that prevented them from pointing to a different data center. “If we hadn’t done the test, we wouldn’t have known about this issue so that we could correct it,” says Maske.

Next Steps

In Cisco’s 2017 fiscal year beginning late July 2016, the team will test processes and technology in response to a cyber-attack scenario. As part of the test we will:

- Fail over more applications
- Work in close partnership with our Information Security (InfoSec) team
- Suspend the virtual machines used for development and test, allocating their capacity for production
- Perform load testing
- Automate database restoration

"We're working up to the ultimate test, which is to failover and then failback to the original data center," says Danny McKee, IT project manager.

Lessons Learned

Our Disaster Recovery teams offer the following suggestions to other companies planning to test data center failover:

- Expect glitches. "Failures are part of the learning process," says Maske. "It's good to find out about problems before a real disaster so that you can fix them."
- Create a dashboard that executives and IT can view to track live restoration status and progress.
- Decide beforehand how to communicate with the various teams. "Failing over one application affects relatively few people, but failing over an entire data center can affect thousands of people," says McKee. Based on our tests of the process, we decided to reduce the number of email distribution lists and to periodically confirm they contained the correct people.

For More Information

Read how Cisco IT designed a development data center that can be quickly repurposed for disaster recovery.

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described. Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties; therefore, this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**