Continuity of Operations: The Applications Angle

Most federal managers think continuity of operations means “resilience.” But just what resilience means is subject to interpretation. For example, is resilience continued network operations in the event of a failure? Is it uninterrupted access to network applications and data if the data center becomes unavailable? Is resilience the ability to use communications systems if lines go down? Or, is it the workforce’s ability to work productively from alternate locations, like home, if they are prevented from traveling to the office?

In fact, meeting the government Continuity of Operations (COOP) requirements means all of the above: network resilience, applications resilience, communications resilience, and workforce resilience. And, they all build on one another: Network resilience is required for applications resilience and applications resilience is required for communications and workforce resilience.

In this article, we will focus on what it means to build applications resilience, which becomes vital in situations as diverse as fire, flood, server failure, power failure, virus infection, and physical destruction of the data center. Agencies can choose from several approaches to replicating application data from the primary to the backup data center. The decision affects how up to date the backup data is, how far away the remote data center can be located, and costs.

Choosing the Right Strategy

Not long ago, the most prevalent approach to applications resilience was to create tape backups and transport the tapes to the backup data center by vehicle. Today, that approach is being largely replaced by network-based backups over wide-area networks, from a storage device at the primary data center to a storage device at the backup data center. Why? The old process of fully restoring a database from tape can take hours – days, in many cases – not the seconds or minutes needed for COOP compliance. Backup tapes also can become lost or damaged.

Choosing the right network-based replication strategy for a given application depends on how much information the agency can afford to lose. An hour’s worth of loss might be acceptable for a Microsoft Outlook e-mail database, but even five minute’s worth might be too much for a Border Patrol application because it might mean the loss of hundreds of border-crossing records.

Agencies whose backup applications need to be up to date within seconds, such as the Department of Homeland Security and the Federal Emergency Management Agency, can use a technique called synchronous replication. Every change to an application record is copied to the backup disk before the next change is recorded. Therefore, the backup application database is always perfectly in sync with the primary database. Synchronous replication has two drawbacks, however. One is that the backup data center must be within 50 to 100 miles of the primary site or else application performance slows to unacceptable levels. The other is that it requires very high bandwidth, which can increase costs.

Agencies whose applications are not so time-sensitive can use a technique called asynchronous replication, which does not require waiting for each application record to be replicated before registering the next record. This technique works over any distance, costs less because it requires less bandwidth, and is easier to implement.

Some agencies blend both replication techniques, reserving the more expensive synchronous replication for the most critical applications. “The question is whether losing less data is worth the higher costs,” says Steve Picot, regional manager for Federal Data Center at Cisco®. “The answer varies among agencies and even for different applications within the same agency.”

But identifying which applications are mission-critical is not always as straightforward as it seems, according to John Speicher, market development manager for federal government at Cisco Systems®. “It’s easy for agencies to identify their core business applications, such as citizen tax records for the Internal Revenue Service and health records for the Department of Veterans Affairs,” he says. “But if a burning building is evacuated, then an HR application might suddenly become critical because it contains the badge-reader data that indicates whether any employees still remain in the building.” Therefore, agencies need to carefully consider which applications are critical in various emergency scenarios.

Security: Protecting Application Data from Desktop to Backup Site

No matter which application replication strategy an agency chooses, security precautions are needed to prevent snooping on or altering application data in transit between data centers. Cisco storage solutions, for example, encrypt application data with the 256-bit Advanced Encryption Standard (AES).

Arguably, it is during disaster that government’s access to up-to-date information becomes most important. Proven disk-to-disk replication strategies address a critical element of COOP: providing employees with uninterrupted access to mission-critical application data even if the data center fails. To learn more, visit: http://www.cisco.com/web/strategy/government/agencies_coop.html.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

CG/LW10072 01/06

Printed in the USA