

ANM Data Center Strategy for Disaster Recovery (DR)



ANM Product Releases: ANM Version 2.0 and later

ACE Product Releases: All versions supported by ANM

Author: David Muñoz, Cisco Systems, Inc.

Last Update: March 24, 2010

Introduction and Summary

Application Networking Manager (ANM) is the multi-device Provisioning, Monitoring and Operations tool for Cisco Application Control Engine (ACE).

When a Disaster Recovery (DR) datacenter is provisioned, it is advantageous to add ANM to the DR site so that Provisioning, Monitoring and Operations of ACE devices is not impaired due to a failover event.

This guide describes how to configure a “Shadow” server for ANM that allows failover operation of the ANM in a DR site. This solution operation uses a backup-copy-restore mechanism to maintain a standby version of ANM where a WAN link separates the two ANM instances. For operation of ANM using High-Availability (HA) mode within the same datacenter, please consult the ANM Installation Guide.

Native Product Capability & Behavior



The ACE Device itself is the primary authority for Device Configuration as far as ANM is concerned. Therefore, if you configure ANM to Automatically Synchronize, the ANM will stay up-to-date with the ACE devices it manages. ANM discovers changes to ACE devices by watching the ACE configuration counter. In addition, ANM regularly polls the ACE devices to update operations status and monitoring information. This behavior can be exploited in order to implement a Disaster Recovery (DR) strategy as documented herein.

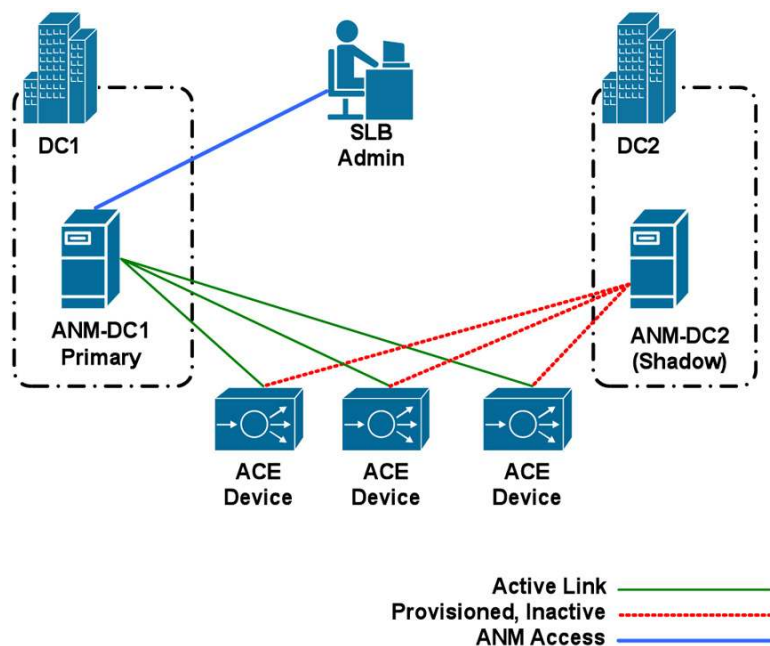
ANM Version 2.0 and later has the following characteristics that affect your Disaster Recovery (DR) strategy:

- ANM High Availability (HA) installation requires ANM servers to be within the same Layer 2 network. - i.e two servers must be on the same subnet.
- ANM-HA Supports Primary/Secondary configuration - Secondary server is a hot standby device.
- A given ACE device can be managed by two independent ANM servers.
- ANM pushes small changes to the device for each operation performed - these operations are similar to a “configlet” concept.
- ANM discovers configuration change events by monitoring the ACE device’s configuration sequence counter.
- When a configuration change is discovered, ANM will read and parse all the configuration text in a given context.
- ANM auto synchronization for the ACE device copies the configuration bits from the ACE device to the ANM.

Note: This behavior is critical to DR operations because the ACE device itself is the authoritative store for device configuration.

DR Strategy: Backup Datacenter with “Shadow” ANM Server

In this scenario, you install two copies of ANM; one in your primary Datacenter (ANM-DC1) and the other in your Disaster Recovery (DR) Datacenter (ANM-DC2). An illustration of the DR arrangement is shown below.



You configure ANM-DC1 as you like, importing all your ACE devices and adding RBAC settings for your users. You make sure you have ANM-DC1 configured to “auto-sync” your ACE devices. After you finish initial configuration of ANM-DC1 and import the devices, you backup the database and then restore it to ANM-DC2.

ANM-DC2 will auto-sync with the devices when it becomes active and hence becomes a “shadow” server for configuration of the existing ACE devices. You do not need to leave the backup ANM server active because it will re-sync with the ACE devices upon activation. Periodically, you repeat the backup-copy-restore to ANM-DC2 device to ensure all the Administrative settings and new imports are reflected on ANM-DC2.

All normal operations are performed using ANM-DC1 unless a failover to the DR site occurs and ANM-DC2 must be used.

Solution Characteristics

- Two Datacenters: DC1 Primary, DC2 is the DR-Standby
- ANM is installed in both DC1 and DC2
- ANM-DC1 is used for regular operations
- ANM-DC2 is activated and used during failover conditions
- Backup-and-restore-to-Shadow operation must be performed on a regular basis (daily, weekly, etc.)

Configuration Steps

1. Configure ANM in the primary DC1 (ANM-DC1)
2. Add regular Non-HA ANM licenses for managing ACE Devices.
3. Import your ACE Devices to ANM-DC1.
4. Configure RBAC settings, Auto Sync settings and any other administrative settings for ANM-DC1. Administrative Changes are only made to ANM-DC1. These changes include:

- Device Import
- RBAC administration
- Anything under the “Admin” tab
- Monitor Alarm Notifications and Settings

Note: Rule of thumb is that any changes which affect ANM itself should be done on the primary to minimize maintenance.

5. Install a new copy of ANM at the DR Datacenter. This new copy is ANM-DC2
6. Install ANM-High Availability (ANM-HA) licenses on ANM-DC2
7. Copy the backup file to the ANM host for ANM-DC2.

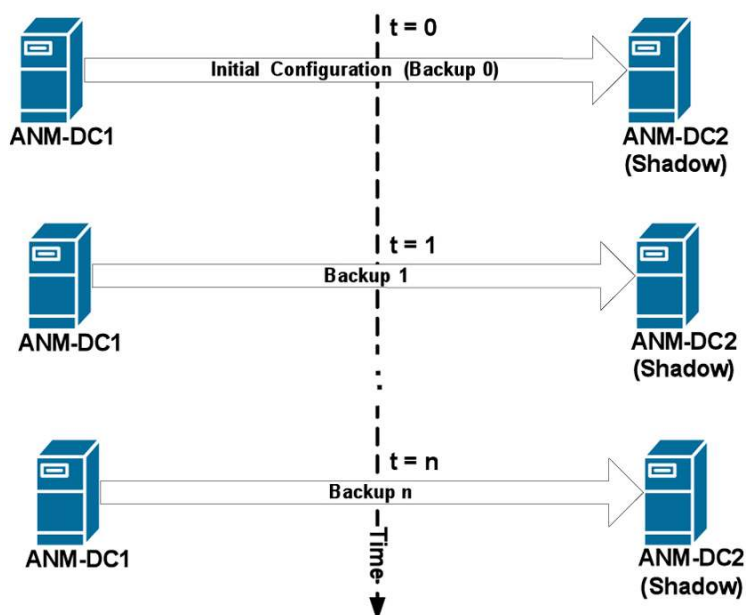
Note: Use a secure copy mechanism such as sftp.

8. Restore the backup file to ANM-DC2 in order to make ANM-DC2 a clone of ANM-DC1.

Note: This process will not copy performance data to the backup ANM in DC2. Performance data is not copied by the ANM backup tool.

Scheduled Operations - Synchronizing Primary and DR Site

For this scheme to work effectively, you must periodically update the DR Site's copy of ANM (ANM-DC2). The arrangement is shown below.



Administrative changes to ANM-DC1 will not automatically be reflected on ANM-DC2. For example, if you add a new user to ANM-DC1, that user will not automatically appear in ANM-DC2. In addition, if you add a new Device to ANM-DC1 that device will not be automatically added to ANM-DC2. Only a Backup and Restore operation from ANM-DC1 to ANM-DC2 will bring the ANM servers into complete sync.

The Synchronization steps are as follows:

1. Backup ANM-DC1 creating a file such as anm-dc1-backup.bak

Example using “bash” shell from the Linux command line:

```
# cd /opt/CSCOanm/bin
# ./anm-tool backup /tmp/anm-dc1-backup.bak
Backing up ANM information to /tmp/anm-dc1-backup.bak (this may take a while)
ANM backed up to /tmp/anm-dc1-backup.bak
Finished
```

2. Copy the backup file to the ANM host for ANM-DC2.

Note: Make sure you use a secure copy mechanism such as sftp.

3. Restore the backup file to ANM-DC2 in order to make ANM-DC2 a clone of ANM-DC1.

4. Optional: Stop the ANM server in DC2 to prevent unnecessary configuration sync.

```
[root@localhost bin]# ./anm-tool stop
Stopping services
Stopping monit services (/etc/monit.conf) ... (0)
Stopping monit ... Stopped
Stopping heartbeat ... Stopped
```

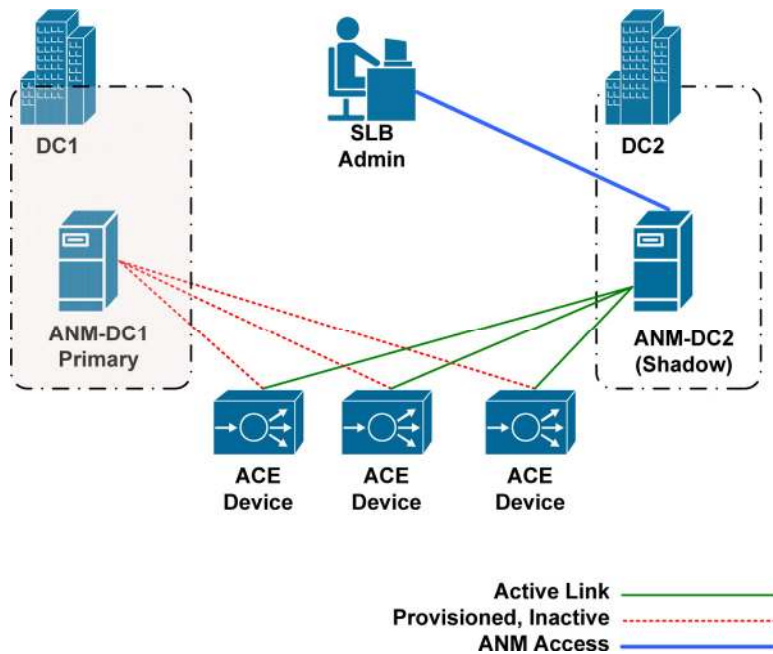
Note: This action is benign because the configuration is stored in the ACE device. When ANM-DC2 starts, it will begin to Auto-Sync to those devices.

Automation of ANM Shadow Synchronization

Automation can be accomplished using a script and a scheduler like the Linux ‘cron’ facility. Cron allows you to schedule such an operation with whatever frequency you deem appropriate. Any number of languages may be used to effect such automation such as Bash, Perl, Python, Ruby or Expect. Specific implementation is beyond the scope of this document.

Failover Operations

An illustration of the DR Failover scenario is below. The SLB Admin uses ANM-DC2 to perform operations for Application delivery since the primary ANM-DC1 is not available.



During failover, the following events occur:

1. An event causes ANM-DC1 to go off-line.
2. If ANM-DC2 is off-line, the ANM-Admin enables the ANM and checks server status

```
[root@localhost bin]# ./anm-tool start
```

```
Starting services
```

```
Starting monit ...Starting monit daemon with http interface at [*:2812]
Started
```

```
[root@localhost bin]# ./anm-tool info
```

```
The monit daemon 4.8.1 uptime: 0m
```

Process 'dcm'	running
Process 'dal'	running
Process 'ip-disc'	running
Process 'licman'	running
Process 'anm-fw-mon'	running
Process 'mysql'	running
System 'localhost.localdomain'	running

```
Java Processes:
```

licman	: Running (27407)	[2010-03-26 14:21:57]
dcm	: Running (27401)	[2010-03-26 14:21:57]

```
dal          : Running (27405) [2010-03-26 14:21:57]
ip-disc      : Running (27402) [2010-03-26 14:21:57]
```

Other Processes:

```
anm-fw-mon: Running (27412) [2010-03-26 14:21:57]
mysql      : Running (27467) [2010-03-26 14:21:58]
```

```
[root@localhost bin]#
```

3. SLB admins login to ANM-DC2 and perform regular SLB admin duties on the ACE devices.

Note: If any administrative changes are made (as described in the Configuration Steps above) to ANM, then a backup-and-restore operation will be required to put the administrative changes back onto ANM-DC1.

Restore to Primary Operations

Once connectivity to the primary DC (DC1) is re-established, the following events occur:

1. ANM-DC1 is restored to operational Condition
2. If administrative changes were made to ANM-DC2, then those changes need to be propagated back to ANM-DC1 using the backup/restore routing outlined earlier. The following steps perform this function:
 - Backup ANM-DC2 creating a file such as anm-dc2-backup.bak

Example using "bash" shell from the Linux command line:

```
cd /opt/CSCOanm/bin
./anm-tool backup /tmp/anm-dc2-backup.bak
```

 - Copy the backup file to the ANM host for ANM-DC1.

Note: Use a secure copy mechanism such as sftp.

 - Restore the backup file to ANM-DC1 in order to synchronize ANM-DC1.
3. Resume SLB admin operations and ANM admin operations using ANM-DC1

Caveats

Performance Data is not migrated by the process above. Backup and Restore utilities do not copy performance data.

If you choose to leave the Shadow server active during non-failover times then ANM-DC2 will read and parse the whole context every time a change is made to that context on ANM-DC1. Depending on the configuration size, configuration complexity and load of your ACE devices, this could cause undesired traffic and control plane loading.

As stated above, ANM's auto-synchronization function only acts upon ACE devices that are already imported to ANM. It does not reflect newly imported devices or contexts, nor any CSS, CSM, CSM/S or GSS managed devices. Only the Backup and Restore operation described above will accomplish The addition of new devices on the DR site (ANM-DC2). Therefore it is very important to have regular backup & restore operations to keep the shadow ANM (ANM-DC2) up-to-date with the primary server (ANM-DC1).

For More Information

For more information about the Cisco ACE product family, visit

<http://www.cisco.com/go/ace>

For the ANM Installation Guide, visit

http://www.cisco.com/en/US/products/ps6904/prod_installation_guides_list.html

For more information about Application Networking Services, go to:

<http://www.cisco.com/en/US/products/hw/contnetw/index.html>

or contact your local account representative.



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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Printed in USA

C07-677671-00 06/11