White Paper

Geo-Redundancy for Cisco Prime Collaboration Assurance and Analytics

Geo-Redundancy: Your key to Cisco Prime Collaboration Continuity

You've invested in an advanced, feature-rich communications platform. And thanks to Cisco Prime™ Collaboration Assurance and Analytics, you're able to gather critical data from that system and diagnose service-quality issues before they become real problems. But even the most sophisticated platform can be affected by unexpected failures. Natural disasters. Power outages. They can take a system down and keep you from delivering on your commitments to customers. This white paper provides an overview and links to resources on how to avoid downtime and "disaster-proof" your communications, even in the face of catastrophic events. It all hinges on geographical redundancy (geo-redundancy).

Simply put, geo-redundancy means running multiple instances of an application in geographically separate data centers. This practice provides application and service continuity and helps ensure that a major storm in one part of the country, for example, won't shut down your operations.

Cisco Prime Collaboration Assurance and Analytics requires geo-redundancy to prevent service failures during natural disasters or massive system outages such as power failures. The secret to geo-redundancy for Cisco Prime Collaboration Assurance and Analytics is VMware vSphere replication.

What Is VMware vSphere Replication?

VMware vSphere replication is a data protection and disaster recovery solution that provides host-based, asynchronous replication of virtual machines (VMs). It is fully integrated with VMware vCenter server and the VMware vSphere web client. And because it uses a cold standby approach with manual failover, it copies only changed blocks to the recovery site and uses very little bandwidth. vSphere replication can:

- Use a "seed copy" of virtual machine data during initial synchronization
- Help ensure efficient network usage by tracking changed disk areas and replicating only deltas

You can get further details on VMware vSphere replication by visiting http://www.vmware.com/files/pdf/vsphere/VMware-vSphere-Replication-Overview.pdf.

System Requirements

Cisco Prime Collaboration Assurance and Analytics itself does not require any special configuration to enable VMware vSphere replication. To enable the host-based replication in your virtual appliance environment, you need:

- VMware vSphere replication, distributed as a 64-bit virtual appliance and packaged in the ova format
- Dual-core CPU, 10-GB and 2-GB hard disks, and 4 GB of RAM
- ESXi host on a VMware vCenter server (5.x or later) - this is a virtual appliance deployed using the OVF deployment wizard

Details on system requirements are available under the vSphere Replication System Requirements at http://pubs.vmware.com/vsphere-replication-60/index.jsp.

You can also find general VMware requirements for Cisco Prime Collaboration Assurance and Analytics in the Install and Upgrade Guides at http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-installation-guides-list.html.

VMware vSphere Replication Configuration

To install the VMware vSphere replication appliance, refer to “Installing vSphere Replication” at http://pubs.vmware.com/vsphere-replication-60/topic/com.vmware.ICbase/PDF/vsphere-replication-60-admin.pdf.

Replication for Cisco Prime Collaboration Assurance and Analytics

To bring up a secondary VM, you will need to install the primary Cisco Prime Collaboration Assurance and Analytics instance at the source site and perform replication to the target site. Get further details in “Replicating Virtual Machines” at http://pubs.vmware.com/vsphere-replication-60/topic/com.vmware.ICbase/PDF/vsphere-replication-60-admin.pdf.

Performing a Recovery with vSphere Replication

1. At any point in time, if your primary instance goes down, perform VM recovery to the target site. Learn more in “Performing a Recovery with vSphere Replication” at http://pubs.vmware.com/vsphere-replication-60/topic/com.vmware.ICbase/PDF/vsphere-replication-60-admin.pdf.

   Note: If you want to test or perform a recovery operation in a normal situation when there is no catastrophic event, be sure that the primary VM is in a powered-off state.
2. Once the secondary VM is powered on, you can choose to retain the same or a different IP address for the VM, depending on the type of network. If the target site is in a different network, you should change the network configuration, such as IP address, gateway, and Network Time Protocol (NTP).
3. To change the IP address of your Cisco Prime Collaboration Assurance server, follow the directions at http://docwiki.cisco.com/wiki/Troubleshooting_Cisco_Prime_Collaboration#How_to_change_IP_Address_on_the_Prime_Collaboration_Assurance_Server.3F.
4. Change the default gateway and NTP to meet network requirements.

Once you have completed all of the network configurations, the secondary server is ready to be launched.

Cisco Prime Collaboration Assurance and Analytics Licensing Behavior for Geo-Redundancy

Cisco Prime Collaboration Assurance and Analytics is a licensed software product that is secured to the MAC address of the virtual machine. When a virtual machine is powered on, the VMware workstation guarantees that VMs are assigned unique MAC addresses within a given host system.

There are two methods of assigning MAC addresses: static MAC allocation and dynamic MAC allocation. Static MAC allocation is recommended, because it enables you to guarantee matching MAC addresses between the secondary and primary VMs. This immediately allows the secondary VM to reuse the primary VM’s Cisco Prime Collaboration Assurance and Analytics license. Dynamic MAC allocation will not guarantee matching MAC addresses between primary and secondary VMs. As a result, the secondary VM will require a new Cisco Prime Collaboration Assurance and Analytics license. License requests require lead time, and can prolong downtime during failover. For this reason, dynamic MAC allocation is not recommended.

Assigning a Static MAC Address

To assign a static MAC address, please refer to http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc%2FGUID-E5C514B3-32CC-4033-AA16-FAD9B07CC3A4.html.

In this scenario, the MAC address does not change for the recovered secondary VM. That means there is no change in the license validity during any further operation.

Obtaining a New License in Dynamic MAC Allocation

To obtain a new license after dynamic MAC allocation, you will need to open a case with the Cisco® Technical Assistance Center (TAC) or Global Licensing Operations (GLO) team and request the geo-redundant license for Cisco Prime Collaboration Assurance and Analytics. Be sure to have on hand your sales order (SO) number and end-customer name (if applicable) to facilitate the entitlement verification. You will also need to include your VM MAC address for the redundant server. GLO will escalate this to the product manager, if needed, to verify the entitlement and will then issue the generic redundant license.

We highly recommend that you use static MAC addressing if you wish to avoid the lead time of license generation and related processes each time the redundant server is activated.

Setting Up Devices for Management in Cisco Prime Collaboration Assurance and Analytics in a Geo-Redundant Environment

You must configure all endpoints, application managers, call processors, multipoint switches, and network devices with protocols such as HTTP, Simple Network Management Protocol (SNMP), Java Telephony API (JTAPI), command-line interface (CLI), and Cisco Discovery Protocol to manage them in Cisco Prime Collaboration Assurance and Analytics.

For supported software versions, refer to http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-collaboration/products-device-support-tables-list.html.

For information on how to configure devices on the network before managing them in Cisco Prime Collaboration Assurance and Analytics, visit http://docwiki.cisco.com/wiki/Setting_up_Devices_for_Prime_Collaboration_Assurance#Required_Protocols_for_the_Devices.

Any change in the Cisco Prime Collaboration Assurance and Analytics server IP address demands changes in device settings as well. We recommend maintaining the same IP address for both primary and secondary Assurance and Analytics servers to minimize the need for reconfiguration on devices.

If this is not possible, we recommend you use a DNS name, instead of an IP address, that maps to the A-names of the primary and secondary Cisco Prime Collaboration Assurance and Analytics VMs whenever possible. In this way, the same DNS name can be used to reach both VMs. An example could be the Cisco Unified Communications Manager billing server configuration.

Also, in some cases, such as SNMP community strings, you can configure device settings with both primary and secondary Cisco Prime Collaboration Assurance and Analytics VM IP addresses.

If any of the above cases are not possible, the better alternative is to wait for the secondary Cisco Prime Collaboration Assurance and Analytics VM to come up and then reconfigure the device settings in order to successfully manage the devices in the secondary Assurance and Analytics server upon recovery.

We also recommend that you reconfigure SNMP trap destinations and syslog receivers only once the secondary server is up, to avoid unnecessary flow of data packets.

No special action is required in the cases of HTTP, JTAPI, and CLI.

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.

Printed in USA C11-735844-00 09/15