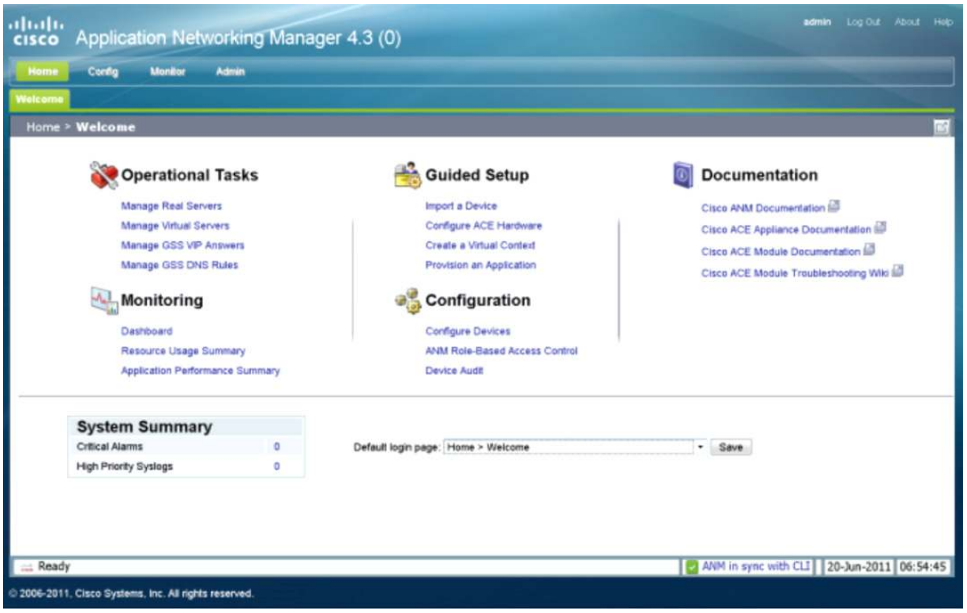
# Cisco Application Networking Manager 4.3

## Product Overview

Cisco® Application Networking Manager (ANM) software, part of the Cisco ACE Application Control Engine product family, is a critical component of any data center or cloud computing architecture that requires centralized configuration, operation, troubleshooting, and monitoring of Cisco data center networking equipment and services. Cisco ANM increases the operators' application network services awareness and capabilities while reducing the burden of operating and managing those services.




Cisco ANM can help you effectively manage multidevice data center network services by:

- Streamlining the deployment and ongoing maintenance of the Cisco ACE virtualized environment
- Simplifying the operations management and monitoring of real and virtual servers spanning the load-balancing infrastructure of Cisco ACE, Cisco CSS Content Services Switches, Cisco Content Switching Module (CSM), and Cisco Content Switching Module with SSL (CSM-S) devices
- Centralizing operations management of virtual IP answers and Domain Name System (DNS) rules for Cisco ACE and Cisco Global Site Selector (GSS) devices
- Integrating with VMware virtual data center environments and allowing you to configure Dynamic Workload Scaling (DWS) on Cisco ACE, thereby allowing administrators to easily navigate and use resources in a virtualized cloud environment
- Enabling integration with third-party or custom developed tools through a web services API

Cisco ANM is designed for data centers requiring a single point of management for their entire Cisco Application Delivery Controller (ADC) environment. Customers using Cisco ANM range from large enterprises including top Fortune 500 companies, to industry leaders in banking and finance, to public-sector organizations, to cloud and mobile service providers, to small and medium-sized enterprises.

## Features and Benefits

### Device Inventory and Service Configuration

Cisco ANM provides an easy-to-follow Guided Setup wizard that provide step-by-step guide to enable rapid creation and modification for immediate deployment of common services by operators of all skill levels (Figure 1). With Cisco ANM, network managers can create, modify, and delete all virtual contexts (partitions) of the Cisco ACE, control the allocation of resources among virtual contexts, and define and manage high availability. Within these virtual contexts, Cisco ANM enables configuration of load-balancing services, including application control lists (ACLs), real servers, server farms, sticky groups, Secure Sockets Layer (SSL) services and health monitoring, and the service bindings to the hosting Cisco Catalyst® 6500 Series Switch and Cisco 7600 Router VLAN interfaces for the Cisco ACE Module.

**Figure 1.** Cisco ANM Guided Setup


Cisco ANM Guided Setup allows you to quickly perform the following tasks:

- Establish communication between Cisco ANM and Cisco ACE devices
- Configure Cisco ACE devices that are new to the network by establishing network connectivity in either standalone or high-availability deployments
- Create and connect to a Cisco ACE virtual context
- Set up a load-balancing application from Cisco ACE to a group of back-end servers

You can perform all these configuration tasks from the Cisco ANM GUI, eliminating the need to use the Cisco ACE command-line interface (CLI).

Advanced users can go directly to the configuration forms without using Guided Setup. They can use the Cisco ANM expert mode, where they can implement even the most intricate service configurations while still gaining the security and error reduction offered by performing these tasks through the Cisco ANM GUI and using building block-based configuration management.

Additional device and service configuration features include:

- Cisco ANM global building blocks, which accelerate deployment of common configuration components and support the standardization of those configurations for devices, virtual contexts of devices, and services
- Discovery of all chassis, modules, appliances, virtual contexts, and service definitions across a large number of systems for systems established prior to Cisco ANM deployment

## Securely Delegated Operations Management

Cisco ANM secure delegation capabilities allow application and server administrators to perform their management tasks as defined by their roles and privileges, such as taking one or more real servers in or out of service, with options for graceful shutdown and cleared connections. Administrators can take servers out of service without needing to know the type of network device that is supporting their servers (Cisco ACE, Cisco CSS, Cisco CSM, or Cisco CSM-S), the network topology, or other network operations.

Cisco ANM also supports secure delegation of SSL key and certificate credentials maintenance to application and server administrators. This capability empowers the responsible application and server administrators to perform self-management, alleviating unnecessary burden on the network services team and reducing the risk of errors in key and certificate administration. This secure delegation extends to expiration date listings for certificates and keys and certificate expiration alarms, helping ensure the security of this sensitive information.

For clusters of Cisco GSS devices, Cisco ANM enables centralized operations to activate and suspend virtual IP answers and DNS answer groups for global load balancing across one or more clusters of Cisco ACE real servers (Figure 2).

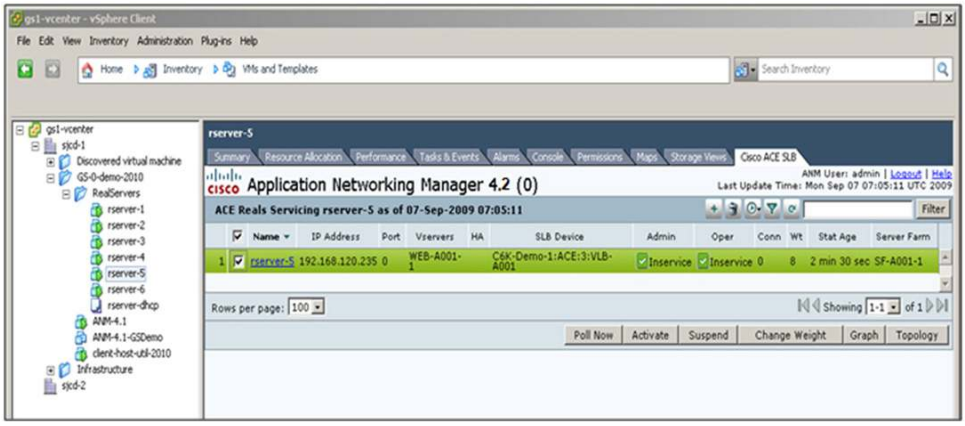
**Figure 2.** Cisco ANM Securely Delegated Operations


On a single screen, operators can monitor the administrative and operational state of all their servers (server health) and the number of connections active on the servers (server use), including servers that are high-availability peers. For administrators who manage large numbers of devices, these displays include the capability to toggle filters on and off for any displayed data elements and custom configuration options, with a customization feature common to almost all Cisco ANM displays.

## Cisco ACE Access in the Virtual Data Center

Cisco ANM offers enhanced integration into the VMware virtual data center environment. Application and server administrators using VMware vCenter to manage their VMware environment can use the Cisco ACE Server Load Balancing (SLB) tab in vCenter vSphere Client to add, delete, activate, and suspend traffic and change load-balancing weights for servers benefiting from Cisco ACE load-balancing services. From within VMware vCenter, administrators have access to the real-server monitoring graphs, which can greatly enhance administrators' knowledge of the true operations of their applications in real time (Figure 3).

**Figure 3.** Cisco ANM VMware vCenter Plug-In




Through the Cisco SLB tab in VMware vCenter (enabled by Cisco ANM), administrators can:

- Accelerate implementation by using Cisco ANM discovery tools to automate importation and mapping of virtual machines to existing Cisco ACE real servers
- Control the way that Cisco ANM associates virtual machines and real servers
- Create real servers within Cisco ANM based on information about virtual machines
- See virtual machines created in VMware vCenter so that they can make appropriate updates to the Cisco ACE configuration: for example, administrators can create and map new real servers

Cisco ANM also lets administrators configure DWS, which is a Cisco ACE feature that permits on-demand access to remote resources, such as VMware virtual machines that you own or lease from an Internet service provider (or cloud service provider). This feature uses Cisco Nexus® 7000 Series Switches with Cisco Overlay Transport Virtualization (OTV), which is a Cisco Data Center Interconnect (DCI) technology used to create a Layer 2 link over an existing IP network between geographically distributed data centers.

As with all Cisco ANM functions, you can perform these tasks only on those elements for which the system administrator has granted access rights. Therefore, although application and server administrators can be allowed to manage the appropriate portions of the application-delivery services for their servers, they cannot see or make changes to the underlying application-delivery services or to the Cisco ACE devices themselves.

### Web Services API for Operations

The Cisco ANM web services API provides a programmable interface for system integrators to integrate the Cisco ACE product family with custom or third-party management applications. The Cisco ANM web services API supports the most common operations for the Cisco ACE Module, Cisco ACE appliance, Cisco GSS, Cisco CSS, Cisco CSM, and Cisco CSM-S, including operations to:

- List devices and virtual contexts
- List server farms and real servers
- List associations of VMware virtual machines and Cisco ACE, Cisco CSS, Cisco CSM, and Cisco CSM-S real servers
- List all virtual IP answers configured on the specified Cisco GSS
- Add and remove real servers from Cisco ACE server farms
- Activate and suspend real servers for participation in load balancing
- Activate and suspend Cisco GSS answers and DNS rules
- Change real-server weight for load-balancing algorithms

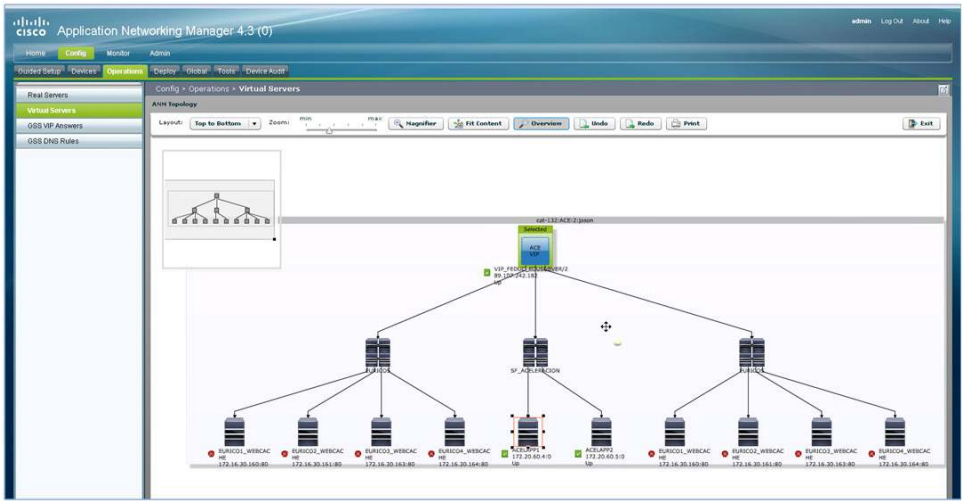
### Network Service Toplogy Visualization

Cisco ANM provides topology maps of the application services network, allowing you to better visualize and understand the flow of traffic through Cisco ACE application networking services (Figure 4). Now when you perform operations and monitoring tasks in Cisco ANM you can visually navigate maps of the network services topology (with panning and zooming) and quickly find, view, and print any set of interest to you. By selecting elements shown on these maps, you can learn:

- Information about Cisco GSS DNS rules, answer groups, and virtual IP answers
- Information about Cisco ACE virtual server and real server
- Information about VMware virtual machine relationships
- Detailed information about each real server and VMware virtual machine that is displayed

The topology mapping tools are also available to authorized VMware vCenter users from the Cisco SLB tab in VMware vCenter.

**Figure 4.** Cisco ANM Topology Map



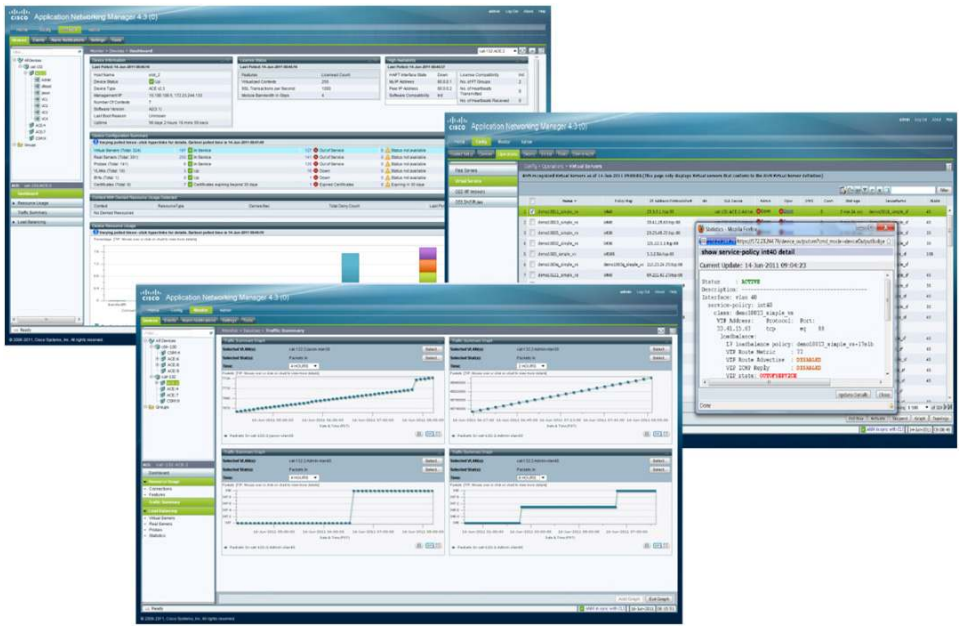

## Monitoring Dashboards with Real-Time and Historic Graphing

Cisco ANM provides up-to-date information about the health and state of all devices, virtual contexts, and applications managed by Cisco ANM. It provides this information through real-time monitoring dashboards. These dashboards enable operations staff to see the most useful information at a glance, to quickly and easily perform more in-depth analysis and accelerate troubleshooting and problem resolution.

Cisco ANM monitoring includes dashboards at the systemwide top level for all managed devices, and for Cisco ACE Modules and Cisco ACE appliances it provides dashboards at the device and virtual context levels. These dashboards display health, use, and performance data for such elements as devicewide traffic, context resource allocation and use, load-balancing statistics, and real-server use. For instance, the Cisco ACE device-level dashboard includes the Context with Denied Resource Usage Detected table, which lists all contexts for which a resource request was denied after the maximum limit for the resource was reached, enabling the operator to track virtual contexts that may need additional resources allocated.

Cisco ANM stores historical data for a selected list of statistics calculated over the last 1-, 2-, 4-, 8-, or 24-hour or month interval. Operators can view this historical data as a statistical graph. Figure 5 shows an example of historic graphing, as well as portions of a top-level dashboard and a context-level dashboard.

**Figure 5.** Cisco ANM Monitoring Dashboards and Graphs



Additional monitoring features include:

- Export of graphed data in JPEG picture file or Microsoft Excel file format for archival or other purposes
- Health and performance dashboards that include top-N and alarm and event graphs and tables
- Support for multiple levels of monitoring views for Cisco ACE, Cisco CSS, Cisco CSM, and Cisco CSM-S devices

### Event Logging and Threshold-Crossing Alerts

Cisco ANM provides a dedicated event view of syslog and Simple Network Management Protocol (SNMP) trap events collected from Cisco ACE Modules and Cisco ACE appliances. Cisco ANM monitoring dashboards display the most recent five critical events with an option to open an event view to display all events.

Within Cisco ANM, you can define threshold-crossing alerts that span multiple devices and virtual services so that you can monitor health, availability, fault-tolerant status, use, and resource capacity with both crossing and clearing notifications generated through an SNMP trap or an email message, or both. For example, an SNMP trap notification can be generated to inform an enterprise event management system of abnormal use rates for a particular application, while both an SNMP trap and alarm email (which could be configured to a pager) can be generated whenever a critical application server fails to respond to the Cisco ACE.

### SSL Certificate Monitoring

In addition to the previously described capability to securely delegate the management of SSL certificates and keys, Cisco ANM provides a global list of all certificates used by the managed Cisco ACE, which is available in the monitoring dashboards. The dashboards show the total count of SSL certificates and the count of SSL certificates that are valid, expired, or expiring within 30 days. At each dashboard level, a hyperlink leads to a view of the SSL certificates list based on the selection, displaying the certificate name, device name, days until expiration, expiration date, and date that the certificate was evaluated to determine the days until expiration. As with all elements, the user's display is limited to those elements that the user has rights to view.

In addition to health and use threshold-crossing alerts, Cisco ANM can be configured to monitor the certificate expiration status and to generate warning alerts (using SNMP traps and email) prior to the expiration date of the SSL certificate (usually annually).

With these two features, the staff responsible for renewal of the certificates and related keys can acquire and put in place the necessary updates in a timely manner, thus avoiding service interruption due to expired certificates and key pairs.

### Data Export for Planning

Cisco ANM provides an optional statistical data export facility so that you can identify baselines and trends as well as perform capacity planning based on application networking services use and performance over time. To simplify data management, the Cisco ANM server manages database disk use, performing such tasks as purging exported data according to user-defined rules and providing notifications when disk-use thresholds are reached.

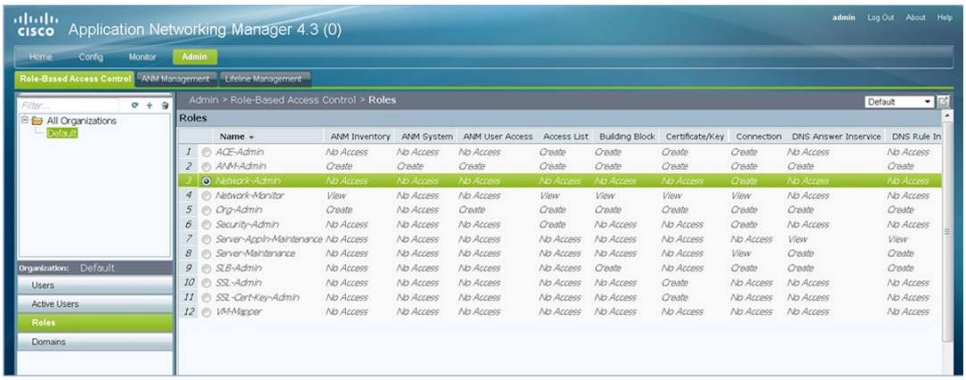
### Highly Detailed Role-Based Access Control and Secure Access

Cisco ANM uses an administrator-defined role-based access control (RBAC) security model that facilitates delegation of authority and responsibility for operations, administration, and monitoring of the managed devices, including activation and suspension of selected load-balanced servers. The Cisco ANM administrator can define with high specificity the tasks and options that are available to individual users or user groups.

RBAC is used to administratively authorize users to access network resources, such as virtual contexts of Cisco ACE devices, content networking and load balancing, and SSL services, as well as individual application services. This feature eliminates unnecessary overhead among network administrators, network-operations-center (NOC) staff, systems operators, and server managers, enabling faster service deployment, simplifying the IT workflow, and reducing configuration errors.

RBAC allows each virtual context in Cisco ACE to be managed by the appropriate business or IT team. Using Cisco ANM, you can create an unlimited number of administratively defined domains within each virtual context, providing even more detailed control over resources within that virtual context or spanning multiple virtual contexts. Similarly, Cisco ANM administrators can define and assign user roles that specify which of 34 defined actions you can take against the network resources you can reach, such as configuration, editing and modification, and device and service monitoring. A set of predefined roles is provided with the product to accelerate implementation and provide examples that administrators can tailor to their specific needs (Figure 6).

**Figure 6.** Cisco ANM Monitoring Dashboards and Graphs



Used in combination, domains and roles let you control access and allow tasks based on the application, business department, or user. For example, network managers can be allowed to configure all operation variables, whereas the application and server owners can be allowed only to monitor and take specific virtual servers in and out of service for maintenance, preventing risk to other IT configurations.

All user access to Cisco ANM is secured. Between the user's web browser and the Cisco ANM server, 128-bit full encryption SSL2 is used, so that authorized users can transparently monitor, activate, and configure Layer 4 through 7 services remotely, even through firewalls. During login to Cisco ANM, users are authenticated either by local accounts created on Cisco ANM or (preferably) remotely by TACACS+, RADIUS, or Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory remote authentication.

### Cisco ACE Checkpoint Management and Centralized Backup and Restore

The Cisco ACE includes a checkpoint configuration feature at the context level to create configuration snapshots. The Cisco ACE stores the checkpoint for each context in a hidden directory in flash memory. These saved checkpoints can be applied to the Cisco ACE context to cause the running configuration to revert to the configuration in effect at the time the checkpoint was created.

For all Cisco ACE devices, Cisco ANM provides checkpoint management as a means to create configuration snapshots and subsequently apply those snapshots to quickly roll back the configuration to that contained in a selected snapshot. You can also use Cisco ANM to view the configuration stored in each saved checkpoint.

Checkpoints can protect the Cisco ACE system if a problem arises after configuration modification, especially when a complex set of configuration changes has been made in a short period of time. Instead of having to reboot and reconstruct a good working configuration on a Cisco ACE after unsuccessful modification of the running configuration, operators can more rapidly recover using a Cisco ACE checkpoint. Using the Cisco ANM checkpoint feature, operators can create a copy of a known stable running configuration before making modifications. Thereafter, if the modifications to the running configuration result in problems, the operator can use the checkpoint to roll back the configuration to the previous stable configuration in moments.

Cisco ANM provides centralized backup and restore features that can create a backup of the running configuration for one or more entire Cisco ACE devices, including the licenses, scripts, checkpoints, certificates, and keys (if they are exportable). Backup can be performed for one, many, or all contexts, on one, many, or all Cisco ACE Modules running the required software release, once or on daily, weekly, or monthly schedules. This global backup and copy capability allows operators to back up the configuration and dependencies of multiple Cisco ACE devices simultaneously or copy existing backup configuration files from disk0 of multiple Cisco ACE devices to a remote server.

## Additional Features

### Discovery and Device Management

- IP and network discovery (using ping sweep, IP range, and Cisco Discovery Protocol)
- Credential discovery (using Secure Shell [SSH] Protocol, TACACS, and SNMP)
- Layer 2 and 3 connectivity
- Chassis, module, and appliance discovery (physical inventory and logical)
- Device import through add and delete operations
- Management of device access credentials

### Global

- Configurable homepage for quick access to, or saved direct login to, commonly used task pages
- Logging of user activity for actions taken in Cisco ANM by users (who did what, when, and from where)
- RBAC role and domain support
- Debugging tool, proving a snapshot of running Cisco ANM system and Cisco ACE configurations
- Support for system failover and high availability

## Product Specifications

Table 1 lists the product specifications for Cisco ANM 4.3.

**Table 1.** Product Specifications

| Product Parameter | Specification |
|---|---|
| **Product compatibility** | Cisco ACE Module (ACE10-6500-K9, ACE20-MOD-K9, and ACE30-MOD-K9) installed in Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Cisco ACE 4710 Application Control Engine, Cisco CSS, Cisco CSM, Cisco CSM-S, and Cisco GSS as specified in the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html. |
| **Protocols** | **For web client:**<br>• Use HTTP or HTTPS.<br>• For additional information, refer to the "Supported Web Browser" section of the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html.<br>**For communication with managed devices:**<br>Refer to the specifications in the "Cisco ANM Ports Reference" section of the Installation Guide for Cisco Application Networking Manager 4.3 available at http://www.cisco.com/en/US/products/ps6904/prod_installation_guides_list.html. |
| **Reliability and availability** | Cisco ANM High Availability is a configuration option for implementing Cisco ANM servers in a highly available active and standby mode. In this configuration, the active Cisco ANM server maintains a stateful synchronization with the standby Cisco ANM server so that if the active server fails, or if an administrative action failover occurs, the standby server can transparently take over operations. |

### System Capacity

Cisco ANM is designed to support up to 50 Cisco ACE devices for full management; up to 40 Cisco CSS, Cisco CSM, and Cisco CSM-S devices for delegated activation and suspension of real and virtual servers with monitoring; and up to 3 clusters of Cisco GSS devices. The exact number of devices supported depends on the scale of operations on each device. For Cisco ACE devices, this value is weighted by the number of virtual contexts per Cisco ACE and the number of configured components and services within each virtual context (servers, server farms, and health-monitoring probes) and the complexity of service configurations. For other devices, the value is weighted by the number of real and virtual servers (Cisco CSS, Cisco CSM, and Cisco CSM-S) and by the number of virtual IP answers, DNS rules, and cluster sizes (Cisco GSS).

### System Requirements

Cisco ANM can be run in two ways:

- As a virtual machine: Cisco ANM Virtual Appliance for VMware
- As an application on a dedicated server: Cisco ANM for Red Hat Enterprise Linux (RHEL)

Cisco ANM Virtual Appliance for VMware is run as a virtual machine in a VMware vSphere 4.0 or 4.1 environment. There is no change to the Cisco ANM user's web interface, nor does the use of this appliance affect the way that Cisco ANM manages network devices. When deployed, this appliance is nearly identical to Cisco ANM run on a standalone Linux server; it is a complete computing system, including the application and operating system and an interface similar to the Cisco IOS® Software interface for administration functions such as backing up and restoring the system and configuring SNMP properties.

In terms of data center design, a Cisco ANM virtual appliance is interchangeable with Cisco ANM for RHEL. This interchangeability makes the appliance easy to deploy and scale; provides more efficient use of hardware resources; and eliminates the need to acquire, install, and maintain the operating system separately.

The installation files for Cisco ANM Virtual Appliance for VMware are provided in the same package as those for Cisco ANM Server for RHEL 32- and 64-bit solutions.

Table 2 lists the system requirements for Cisco ANM Virtual Appliance for VMware, and Table 3 lists the system requirements for Cisco ANM for RHEL.

**Table 2.** System Requirements for Cisco ANM Virtual Appliance for VMware

| Description | Specification |
|---|---|
| **Virtual machine requirements** | • VMware vSphere 4.0 or 4.1<br>• 2-GB RAM minimum; 4-GB RAM recommended<br>• 128-GB minimum disk space |
| **Client hardware requirements** | As specified in the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html |
| **Client software requirements** | As specified in the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html |

**Table 3.** System Requirements for Cisco ANM for Red Hat Enterprise Linux

| Description | Specification |
|---|---|
| **Server hardware requirements** | • A dedicated Linux server for Cisco ANM<br>• Generic PC with equivalent of 3-GHz Pentium III CPU performance (dual processor and dual-core CPUs are supported)<br>• 2-GB RAM minimum, 4-GB RAM recommended as minimum for optimum performance<br>• 120-GB minimum hard drive or fixed storage<br>• CD-ROM drive<br>• One 100-Mbps Ethernet interface for single Cisco ANM configuration; two full-duplex interfaces for Cisco ANM High Availability configuration |
| **Server software requirements** | • RHEL 5 (base server) Update 3 (5.3) 32-bit or 64-bit Server Edition (Linux 2.6 kernel)<br>• RHEL 5 (base server) Update 4 (5.4) 32-bit or 64-bit Server Edition (Linux 2.6 kernel)<br>• RHEL 5.5 (base server) Update 5 (5.5) 32-bit or 64-bit Server Edition (Linux 2.6 kernel)<br>• The instructions provided in the Installation Guide for Cisco Application Networking Manager 4.3, available at http://www.cisco.com/en/US/products/ps6904/prod_installation_guides_list.html. |
| **Client hardware requirements** | As specified in the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html |
| **Client software requirements** | As specified in the Supported Devices table for Cisco ANM available at http://www.cisco.com/en/US/products/ps6904/products_device_support_tables_list.html |

## Ordering Information

Cisco ANM Versions 4.3, 4.2, and 4.1 are offered for order at no charge, but they do require licensing. You must order the Cisco ANM server software license to receive the license necessary to install the product for production use, and Cisco Software Application Support (SAS) requires a separate purchase.

Table 4 provides ordering information. To place an order, visit the Cisco Ordering homepage.

**Table 4.** Ordering Information

| Part Number | Description |
|---|---|
| **ANM-SERVER-40-K9** | Postal delivered ANM Server Software license |
| **L-ANM-SERVER=40-K9** | Electronically delivered ANM Server Software license |

## Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco Services programs help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, please refer to Cisco Technical Support Services and Cisco Advanced Services.

## For More Information

For more information about Cisco ANM, please visit http://www.cisco.com/go/anm or contact your local Cisco 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.**





Printed in USA C78-678118-00 06/11