

Cisco ACNS Software Release 5.0 Upgrade Planning

Overview

Cisco Application and Content Networking System (ACNS) Software Release 5.0 includes significant changes and enhancements from Cisco ACNS Software Release 4.2 affecting how customers store and distribute their content. This product bulletin gives an overview of important changes and outlines the new hardware and software that customers will need before upgrading from Cisco ACNS Software Release 4.2 to Release 5.0. Please refer to the full documentation and the Cisco ACNS Software Migration Guide for more in-depth information: http://www.cisco.com/en/US/products/sw/conntsw/ps491/tsd_products_support_install_and_upgrade.html

Customers who only use caching functions will not have to make many changes to their system to upgrade. Customers using the Content Delivery Network (CDN) features will need to migrate their content and follow the migration guide. If CDN customers do not follow the Migration Guide and just upgrade the equipment, the CDN will be non-functional.

Basic Changes in Cisco ACNS Software Release 5.0

- The Cisco Content Distribution Manager (CDM) no longer stores content

All content is pulled from a Web server or an FTP server (the origin server) and sent directly to the content engines. Certain content engines are designated as “root” content engines—responsible for acquiring content from the origin servers and then distributing the content to other content engines subscribed to the same channel of content. This means that you do not need to store content on the Cisco CDM—content resides on the origin server that is accessible to the root content engines. The protocols supported in Cisco ACNS Software Release 5.0 for acquisition are HTTP, HTTPS, or FTP.

- Routing and redirection are handled differently

With Cisco ACNS Software Release 5.0, you can now use edge-intercept methods—either Web Cache Communication Protocol (WCCP) supported on Cisco IOS® Software routers and switches or browser proxy configuration—to redirect clients to the best content engine, whether the content is demand-pulled or pre-positioned. Your router must support WCCP in order for you to use WCCP as an edge-intercept method. With edge-intercept methods, you do not need a content router. The CDM no longer redirects requests, so if you do not use WCCP or proxy configuration, you must use a content router.



- Content acquisition and distribution has changed

Instead of importing files into the CDM, the root content engines fetch files directly from an origin Web server or FTP server. Cisco ACNS Software Release 5.0 uses a manifest file to identify which files should be acquired from the origin server and then pre-positioned to the content engines. This manifest file is in Extensible Markup Language (XML) format and should be placed on a Web server or FTP server that the content engines can access. The CDM facilitates management and configuration, determining which root content engines get which manifest file based on the channels of content for which they are responsible. ACNS Software Release 5.0 uses a “root” CE to acquire content from the origin server. This root CE then distributes the content to other CEs based on the instructions in the manifest file. Many CDN installations will need to add a root CE in order to take advantage of the new content distribution system. The root CE should be placed in a location with good connectivity and close to the origin servers.

- The URL used to request content is significantly different

When using edge-intercept methods, the URLs used are the original URLs from the Web server—no change is required. When using content routing in Cisco ACNS Software Release 5.0, however, the URL on the Web server for pre-positioned content has changed. In Cisco ACNS Software Release 4.2, the URL pointed to the CDM that redirected requests to the appropriate content engine. In Cisco ACNS Software Release 5.0, all requests are sent to a content router that then issues the redirected requests to a content engine. Requests are directed to a content router using the Domain Name System (DNS). The content router becomes authoritative for a domain that is hosted by the Content Delivery Network. This means that all URLs referring to content served by the CDN must include the domain hosted by the content routers.

Required Software and Hardware

1. When you use Cisco ACNS Software Release 5.0 for pre-positioning content, you must first put that content on an origin Web server or FTP server that the content engines have access to. You need to deploy the server and ensure that it has sufficient capacity for all the content you want to put on the CDN. The CDN can pre-position content from more than one Web server or FTP server. You will need to place root content engines with sufficient network link speed to the origin server.
2. If you plan to use content routing (as opposed to WCCP or proxy configuration of clients), you need one or more content routers. Cisco recommends two or more (up to eight) for reliability and redundancy.
3. You need a Web server or FTP server to host the manifest file. This can be the same server used to host the content.
4. If you plan to use content routing, you need access to a DNS server. The content router will respond for a domain, but it must be configured as authoritative (NS records must return the IP address of the content router) in a higher-level DNS server. For example, if the domain `cdn.cisco.com` will serve content from the CDN, the DNS server for `cisco.com` must have an NS record identifying the content router as authoritative for `cdn.cisco.com`. Therefore, you need to have access to edit the DNS configuration of the higher-level DNS server (in this example, `cisco.com`).

Other Changes That May Be Required

You may need to change the URLs of Web sites that serve content from the CDN. If you are using content routing, you need to change all the URLs for pre-positioned content as described above. If you were using enterprise CDN (ECDN) pre-positioning in Cisco ACNS Software Release 4.2 and now plan to use WCCP or proxy configuration of browsers, you need to move content from the CDN to an origin server and rewrite the URL to use that origin server.

This is a brief overview of the hardware and software changes needed to migrate from Cisco ACNS Software Release 4.2 to Release 5.0. Please refer to the Cisco ACNS Software Migration Guide for more details.



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 Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 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 Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
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