

CA Spectrum® Active Directory and Exchange Server Manager

Solution Guide

Release 9.2.2



This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following products:

- CA Spectrum® (CA Spectrum)
- CA Spectrum® Virtual Host Manager (Virtual Host Manager)
- CA SystemEDGE
- CA eHealth® Performance Manager (CA eHealth)
- CA Virtual Assurance for Infrastructure Managers (CA Virtual Assurance)
- CA Spectrum® Report Manager (Report Manager)

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At <http://ca.com/support>, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at <http://ca.com/docs>.

Contents

Chapter 1: About Active Directory and Exchange Server Manager 7

ADES Manager Features	7
System Requirements	8
Supported Technologies.....	8
Active Directory Overview	8
Exchange Server Overview	10
Solution Architecture	11

Chapter 2: Getting Started 13

Planning Your ADES Manager Implementation.....	13
Environment Management Considerations	14
Host Modeling	14
Supporting Changes to Your Active Directory and Exchange Server Environments	19
Understanding ADES AIM Technology	19
Installing ADES Manager Components.....	21
Discovery and Modeling	22
Discover and Model Your Active Directory and Exchange Server Environment	23
Models Created for ADES Manager	29

Chapter 3: Viewing Your Active Directory and Exchange Server Environments 31

Explorer View	32
Topology View	35
Support for Virtual Machines.....	36
Information Subviews	36
ADES Host Manager (ADES AIM) Subviews.....	37
Individual Host Subviews	40
Locator Searches	42
Event Reports	43

Chapter 4: Maintaining Your ADES Manager Environment 45

Controlling Polling Intervals	45
Updating ADES AIM Configuration Options	46
Updating Your Managed Environment.....	46
Discovery Process for Updating Your Modeled Environment	46

How to Update Your Modeled Environment	47
Modifying ADES Manager Host Management and Models.....	49
Deleting ADES Manager Models	49

Chapter 5: Alarms and Fault Isolation **51**

ADES Manager Alarms.....	51
ADES Manager Fault Isolation	51
Proxy Management	52
Alarm Correlation.....	54
ADES Manager Fault Management Scenarios	54

Appendix A: Troubleshooting **57**

SystemEDGE Host Not Modeled as ADES Host Manager	57
Duplicate Models Created After Discovery	58
Multiply Managed Alarms	59
Connections Do Not Appear in Topology	60
ADES Managed Hosts Container Not Created	60
Host Not in ADES Managed Hosts Container	61
Unable to Update Attribute	61
Host Subview is Empty	62
Changes in Environment Not Reflected in CA Spectrum.....	62
ADES Manager Updates are Slow.....	63

Glossary **65**

Index **69**

Chapter 1: About Active Directory and Exchange Server Manager

CA Spectrum Active Directory and Exchange Server Manager (ADES Manager) is a CA Spectrum feature that models and monitors your Microsoft Active Directory and Microsoft Exchange Server environments. ADES Manager provides an enterprise-wide view of your Active Directory and Exchange Server environments, showing topology as well as the logical relationships between servers. ADES Manager also provides visibility into key Active Directory and Exchange Server metrics and helps you pinpoint and effectively troubleshoot problems by applying unique fault isolation techniques to your Active Directory and Exchange Server environments.

ADES Manager is intended for CA Spectrum administrators who want to monitor Active Directory and Exchange Server hosts.

This section contains the following topics:

[ADES Manager Features](#) (see page 7)

[System Requirements](#) (see page 8)

[Supported Technologies](#) (see page 8)

[Solution Architecture](#) (see page 11)

ADES Manager Features

CA Spectrum ADES Manager features include:

- Automated device discovery and modeling. ADES Manager automatically creates models and connections for all managed Active Directory and Exchange Server hosts.
- A distributed solution that can handle scaling. Domain management can be distributed across multiple SpectroSERVERs.
- Identification of Active Directory and Exchange Server hosts in the topology.
- Hierarchical representation of Active Directory and Exchange Server environments.
- Dedicated ADES Manager views that provide visibility into data specific to Active Directory and Exchange Server environments.
- Enhanced fault management. ADES Manager recognizes and suppresses symptomatic alarms and aids fault isolation with proxy management.
- Locater searches specific to Active Directory and Exchange Server.

System Requirements

Active Directory and Exchange Server Manager is an application that works within CA Spectrum when all required components are available and configured properly. ADES Manager requires the following components:

- CA Spectrum 9.2.2 or later
- A dedicated host machine with:
 - CA SystemEDGE 5.x or later
 - Active Directory and Exchange Server AIM (ADES AIM) r12.7 with latest PTFs, or later

Important! The ADES AIM must be the only AIM installed on the CA SystemEDGE host. The CA SystemEDGE host itself cannot be a host in your Active Directory and Exchange Server environment.

Note: For CA SystemEDGE host and ADES AIM requirements, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Supported Technologies

CA Spectrum Active Directory and Exchange Server Manager supports the following product versions and technologies:

Active Directory for Windows Server 2008, Windows Server 2008 R2

- Active Directory Domain Services (AD DS) Server Role

Exchange Server 2007, 2010

- Hub Transport Server Role
- Mailbox Server Role

The following sections provide more information about these technologies.

Active Directory Overview

Active Directory is a directory service that provides administrators the ability to control, manage, and discover network resources throughout the organization. Using Active Directory, you can efficiently manage users, computers, groups, printers, applications, and other directory-enabled objects from one secure, centralized location. CA Spectrum ADES Manager helps you to manage and monitor your Active Directory environment so that you can achieve increased levels of availability of your network resources.

An Active Directory implementation can vary in size from a small number of objects to millions of objects. It enables administrators to centrally manage enterprise-wide network information from a repository that is globally replicated. Once information has been added to Active Directory, it is available throughout the entire enterprise.

Active Directory uses server roles to assign different functions to different servers, and a single server may fulfill several roles at once. The following server roles are available for Active Directory:

Active Directory Certificate Services (AD CS)

Allows you to create, distribute, and manage customized public key certificates.

Active Directory Domain Services (AD DS)

Stores directory data for all objects in your network and manages communication between users and domains, including authentication requests and directory searches.

Active Directory Federation Services (AD FS)

Provides secure identity technologies to authenticate users for access to resources.

Active Directory Lightweight Directory Services (AD LDS)

Provides support for directory-enabled applications without the restrictions of AD DS.

Active Directory Rights Management Services (AD RMS)

Protects your digital information from unauthorized use by identifying the rights that a user has to a file.

Important! CA Spectrum ADES Manager supports the AD DS server role only. The following section provides additional information on this role.

Active Directory Domain Services (AD DS)

Active Directory Domain Services provide the central location of the directory where configuration information, authentication requests, and information about all the objects in your network are stored. The basic internal structure of the Active Directory is a hierarchical arrangement of objects.

The following describes components of the Active Directory structure which are used in CA Spectrum ADES Manager:

Forest

An Active Directory container structure that contains a collection of Active Directory objects, their attributes, and attribute syntax. A forest is at the highest level of the logical structure. It is a collection of domain trees (see definition on page 66) sharing a common global catalog, directory configuration, directory, schema and logical structure.

Domain

An Active Directory container structure that contains a collection of objects that share a common set of policies, name, and security database. A domain is at the lowest level of the logical structure of an entire network and is identified by its domain name.

Domain Controller

A host that is running AD DS. There are typically multiple domain controllers that host Active Directory within a domain, and you can manage your network resources from any domain controller within your domain.

Exchange Server Overview

Exchange Server is a back-end product that provides messaging services (such as email, calendar, and contacts) to its end users. With email and messaging as business-critical tools, your Exchange Server implementation must be able to support a highly available messaging environment. CA Spectrum ADES Manager helps you to manage and monitor your Exchange Server environment so that you can achieve increased levels of reliability.

Exchange Server provides the underlying infrastructure to support a messaging system. This includes the database to store email data, the transport infrastructure to move the data from one place to another, and access points to access email data from a number of different clients. Exchange Server uses server roles to assign these different functions to servers throughout the enterprise, and you choose which roles each server supports. You can install only the roles you need, split server functions across multiple servers, and install more than one role on a single machine.

The following server roles are available in Exchange Server:

Mailbox

Provides email storage (including user mailboxes), advanced scheduling services, and supports public folders. Continuous replication technology provides a reliable failover mechanism in the event of failure. In Exchange 2007, continuous replication failover is at the server level; with Exchange 2010 and the introduction of database availability groups (DAGs) (see definition on page 66), failover is at the database level.

Client Access

Handles how users connect to Exchange by supporting functions such as Outlook, POP3, and web services such as calendar sharing.

Hub Transport

Handles email flow and routing. All messages are delivered through this role, regardless of whether they are being delivered locally or remotely.

Unified Messaging

Integrates your phone system with your email, handling automated call routing and directing voicemails to the user's mailbox.

Edge Transport

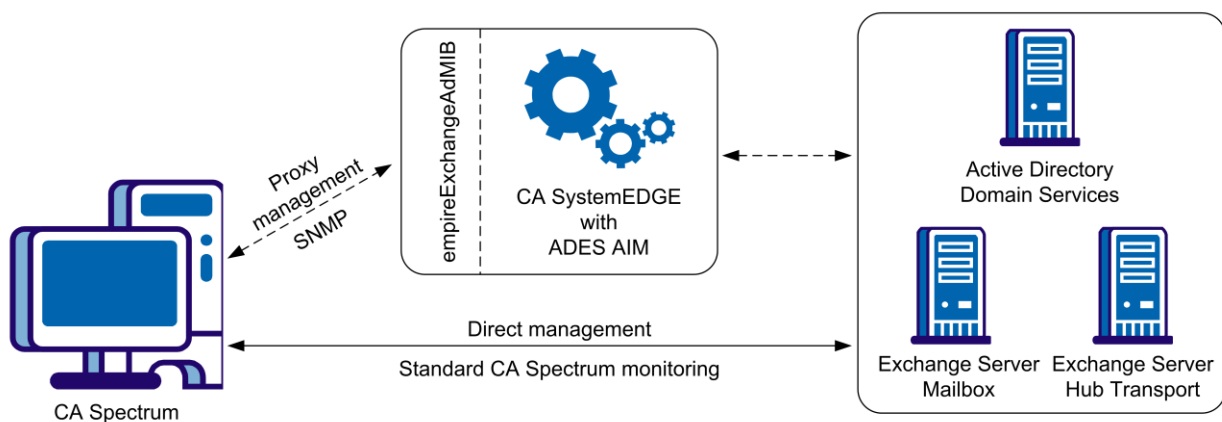
Supports antispam and antivirus functions for inbound and outbound messaging.

Important! CA Spectrum ADES Manager supports the Mailbox Server and Hub Transport Server roles only.

Solution Architecture

The purpose of CA Spectrum ADES Manager is to monitor your Active Directory and Exchange Server environments seamlessly as an integral part of your network, while providing additional data that is specific to the supported server roles. To accomplish this, CA Spectrum gathers information about your Active Directory and Exchange Server hosts using two different methods. As with other CA Spectrum managed devices, ADES Manager uses standard CA Spectrum monitoring methods. In addition, ADES Manager also retrieves specialized information from an alternate (proxy) manager, the Active Directory and Exchange Server AIM (ADES AIM).

The ADES AIM is a specialized CA SystemEDGE Application Insight Module (AIM), which is an extension of the CA SystemEDGE agent and resides on its own host. This host is referred to as the Active Directory and Exchange Server Host Manager (ADES Host Manager). The ADES AIM obtains data from Active Directory and Exchange Server hosts that is specific to the Active Directory and Exchange Server role technologies. This data is then written to a CA-developed MIB (empireExchangeAdMIB) and is accessed by CA Spectrum using SNMP requests. This solution allows other SNMP clients, such as CA eHealth, to utilize the ADES AIM. Each ADES AIM can support multiple domains, and ADES Manager can support multiple AIMs either within a single SpectroSERVER or distributed across multiple SpectroSERVERs.



Note: For information about how the ADES AIM operates, such as how it communicates with the Active Directory and Exchange Server hosts and how many hosts each AIM can support, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Chapter 2: Getting Started

This section describes how to plan for and install ADES Manager.

Follow these steps:

1. [Plan your ADES Manager implementation](#) (see page 13).
2. [Install ADES Manager components](#) (see page 21).
3. [Discover and model your Active Directory and Exchange Server environments](#) (see page 22).

Planning Your ADES Manager Implementation

The purpose of ADES Manager is to monitor your Active Directory and Exchange Server environments. ADES Manager is highly scalable and can monitor hundreds of servers using multiple AIMs and distributed SpectroSERVERs. There are different ways to configure your ADES Manager implementation for performance, geographical, and logical purposes. Understanding the various configuration and management options provides for a more efficient ADES Manager implementation.

Before setting up your ADES Manager, review the following:

- [Environment Management Considerations](#) (see page 14)
- [Host Modeling](#) (see page 14)
- [Supporting Changes to Your Active Directory and Exchange Server Environments](#) (see page 19)
- [Understanding ADES AIM Technology](#) (see page 19)

Environment Management Considerations

When setting up ADES Manager to monitor your Active Directory and Exchange Server environments, you specify how to organize the management of your environments. With a small environment, you can have a single ADES AIM managing all of your Active Directory and Exchange Server hosts in a single domain in a single location on one SpectroSERVER. In a complex environment, you might have multiple ADES AIMs managing different host subsets from multiple domains in different geographic locations split across multiple SpectroSERVER landscapes.

Although organizational specifications can be changed at any time, knowing the available configuration management options allows for a better initial setup.

Consider the following points when setting up your ADES Manager environment:

- A single ADES AIM can manage hosts from one or more domains.
- One or more ADES AIMs can manage a single domain.
- Domain management can be distributed across multiple SpectroSERVERs using multiple ADES AIMs. Multiple ADES AIMs can also be supported within a single landscape.
- A host should be managed by one ADES AIM only. If a host fulfills multiple roles, the roles should all be managed by the same ADES AIM.

When deciding how to distribute host management, consider the number and location of hosts in your environment. Performance can be affected by the number of hosts managed by an ADES AIM as well as the geographic proximity of the AIM to the monitored environment. For best performance, management of the environment should be sized and balanced appropriately.

Note: Domain-level management is controlled on the ADES AIM and not in CA Spectrum. For information on domain specification, load balancing, and sizing guidelines, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Host Modeling

As with any other network element supported in CA Spectrum, you must discover and model your Active Directory and Exchange Server hosts in order to monitor them. ADES Manager uses different types of discovery when modeling your ADES environment:

- Discovery by the ADES AIM (ADES AIM Discovery)
- Discovery within CA Spectrum (ADES Manager Discovery)

ADES Manager relies on the ADES AIM to discover and provide information about available Active Directory and Exchange Server hosts in the specified domains and then uses this information to model each host individually in CA Spectrum.

Note: Information used for the ADES Manager feature is gathered primarily from the ADES AIM. Additional information may be gathered directly from the hosts.

The following topics provide more details about the modeling process.

Note: Procedures for discovering and modeling your environment are provided in [Discovery and Modeling](#) (see page 22).

What is Modeled

Any host in the specified domain or domains that supports any of the supported roles is discovered during ADES AIM Discovery and made available for management in CA Spectrum. Supported server roles include Active Directory Domain Services, Exchange Server Hub Transport, and Exchange Server Mailbox. If a machine only has roles that are not supported, it will not be included in the list of available ADES hosts and, accordingly, will not be modeled. Of the available hosts, not all will necessarily be modeled in CA Spectrum; only those hosts designated by the CA Spectrum administrator to be managed by CA Spectrum ADES Manager will be discovered and modeled in CA Spectrum.

Note: You can specify in the ADES AIM to monitor Active Directory only, Exchange Server only, or both technologies. When monitoring a single technology only, only those hosts having a supported role in that technology are included as available hosts. You can also specify in the ADES AIM to automatically manage all newly-available hosts, in which case all newly-available hosts having any of the supported roles will be modeled automatically in CA Spectrum. Functionality provided by the AIM is described more in [Understanding ADES AIM Technology](#) (see page 19).

Models that are created during ADES Manager Discovery are placed in the topology in an ADES Managed Hosts container specific to the ADES AIM and are visible in the ADES hierarchy. If a host that is part of an Active Directory or Exchange Server environment has already been modeled in your CA Spectrum-managed network prior to ADES Manager Discovery, it will not be modeled again nor will the original model be moved in the topology during ADES Manager Discovery. Although the model will not be reflected in the ADES Managed Hosts container in the topology view automatically, it is included in the Active Directory and Exchange Server Manager hierarchy. In certain cases, you can move the host model into the ADES Managed Hosts container manually.

Note: Active Directory and Exchange Server host models can also be moved out of the ADES Managed Hosts container. Additionally, this container is not limited to Active Directory and Exchange Server hosts; other devices can be moved into the container if the administrator considers the inclusion to be logical. If the container is destroyed, all models in the container (except for models in a global collection) are moved to the Lost and Found (LostFound). This includes any models that are moved manually into the container and may not necessarily be Active Directory or Exchange Server hosts.

Modeling Methods

Hosts in the Active Directory and Exchange Server environment are modeled as SNMP-managed elements when possible. SNMP-capable modeling supports enriched device monitoring that can provide additional value to your ADES Manager solution. If an SNMP agent is not installed on the host, it is modeled as an ICMP (Pingable) device.

The following sections provide additional details about how Active Directory or Exchange Server hosts are modeled:

- [Model Naming](#) (see page 17)
- [IP and MAC Address Determination](#) (see page 17)

Model Naming

When Active Directory and Exchange Server hosts are modeled, the model name assigned in CA Spectrum depends on the type of modeling used, as follows:

- For SNMP modeling, CA Spectrum automatically attempts to supply a name for the model using standard CA Spectrum naming conventions. Automatic naming is controlled at the SpectroSERVER level as indicated by the Model Naming Order field on the SpectroSERVER Control view for the VNM model.
- For ICMP (Pingable) modeling (when not a virtual device), CA Spectrum uses the host name provided in the ADES AIM.

Important! For ICMP (Pingable) modeling, model names set by CA Spectrum Virtual Host Manager take precedence over ADES Manager.

The administrator can modify the name of an Active Directory or Exchange Server host model at any time. As with other managed network elements, CA Spectrum automatically updates the model name using established naming rules, which can replace the user-defined value. To retain a user-defined value, you must lock the model name.

Note: You can modify and lock the model name using the following model attributes: Model_Name (0x1006e) and Lock_Model_Name (0x12a52).

IP and MAC Address Determination

When Active Directory and Exchange Server hosts are modeled, the IP and MAC addresses assigned in CA Spectrum depend on the type of modeling used, as follows:

- For SNMP modeling, CA Spectrum automatically attempts to determine the addresses by querying the resident SNMP agent.
- For ICMP (Pingable) modeling (when not a virtual device), CA Spectrum uses the addresses provided by the ADES AIM.

Important! For ICMP (Pingable) modeling, addresses set by CA Spectrum Virtual Host Manager take precedence over ADES Manager.

If neither SNMP modeling nor Virtual Host Manager can supply a valid IP or MAC address, the ADES AIM value is used.

Host Management and Multiple ADES AIMs

An Active Directory or Exchange Server host should be managed by a single ADES AIM. If a host is inadvertently managed by multiple ADES AIMs, expect the following behavior:

- If the managing ADES Host Managers are in a single landscape, duplicate models are not created for the Active Directory or Exchange Server host. ADES Manager recognizes when a host is already managed by another ADES AIM and issues an alarm on the Active Directory or Exchange Server host.
- If the managing ADES Host Managers exist across multiple landscapes, duplicate models will exist.

Important! Managing a single host by multiple ADES AIMs can introduce performance issues. For more information, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Hosts Managed by Virtual Host Manager and ADES Manager

When a host is managed by both CA Spectrum Virtual Host Manager and ADES Manager, model parameters that are set by Virtual Host Manager (such as model name, IP address, and MAC address) are used.

When the ADES Host Manager is a virtual machine, the ADES Managed Hosts container is created a level above where the ADES Host Manager is modeled.

Additionally, if an Active Directory or Exchange Server host is a virtual machine, it remains in its physical host container.

Important! A virtual machine cannot be moved from its physical host container. An Active Directory or Exchange Server host that is a virtual machine is not reflected in the ADES Managed Hosts container.

Supporting Changes to Your Active Directory and Exchange Server Environments

After the initial modeling of your Active Directory and Exchange Server environments in CA Spectrum, changes to the environment are not automatically detected. You must start ADES AIM discovery manually to recognize and model any subsequent changes.

The ADES AIM performs its discovery of the Active Directory and Exchange Server environments when the AIM starts up, and CA Spectrum models the environment accordingly. After the initial ADES AIM discovery, you must start an ADES AIM discovery manually for the ADES AIM to recognize any changes in the Active Directory and Exchange Server environment, which CA Spectrum then automatically reflects in its modeled environment.

Because of the potentially large size of the Active Directory and Exchange Server environments, dynamic updates would be expensive to maintain. The manual start process also allows the administrator to address many environment changes at the same time in a controlled time frame.

Note: For information about updating your modeled ADES environment, see [Updating ADES Environment](#) (see page 46).

Understanding ADES AIM Technology

ADES Manager uses the ADES AIM for discovery, modeling, and monitoring of your Active Directory and Exchange Server environments. This section describes functionality that is controlled and provided by the ADES AIM, which you should be aware of prior to setting up your ADES Manager implementation. After initial setup, configurations can be modified. Some settings can only be changed directly in the ADES AIM, while others can be changed from within CA Spectrum.

Note: This section describes features of the ADES AIM at a high level. For detailed information, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

The section includes the following topics:

- [Discovery Options for the ADES AIM](#) (see page 20)
- [Polling by the ADES AIM](#) (see page 21)

Discovery Options for the ADES AIM

This section describes the ADES AIM Discovery options. These options are defined in the ADES AIM and control what hosts in your Active Directory and Exchange Server environments are discovered and how they are initially managed. The main settings on the ADES AIM are:

Domain name

Controls what domains to monitor.

Management entity

Controls what technologies to monitor: Active Directory, Exchange Server, or both. This setting is specified on a per-domain basis.

Management mode

Controls how discovered hosts are initially monitored: domain-based or host-based. This setting is specified on a per-domain basis.

The following describes how these settings work together and are used by CA Spectrum ADES Manager.

When you install and configure an ADES AIM, you provide the names of one or more domains to manage and specify by domain whether to manage Active Directory hosts, Exchange Server hosts, or both.

Using the specified domain names, the ADES AIM queries the Global Catalogs to retrieve all Active Directory and/or Exchange Server hosts (based on your setting) and identifies roles configured on each server. The ADES AIM then uses the respective roles of each host to determine if the host qualifies for inclusion as an available host.

For each domain, you also specify whether the ADES AIM should initially manage (domain-based management) or not manage (host-based management) newly-discovered hosts in the domain. Domain-based management identifies and automatically manages all new hosts that serve the requested technology within the domain, while host-based management identifies but does not manage all new hosts by default. Domain-based management is generally used with domains that are small enough to be managed by a single AIM, while host-based management is generally used with domains that are large enough to be managed by multiple ADES AIMs.

Note: Using host-based management, you must specify manually within CA Spectrum which hosts to manage. See [Specify Hosts to Manage by ADES Manager](#) (see page 26).

Polling by the ADES AIM

The ADES AIM polling interval indicates how often the ADES AIM queries the managed hosts for information. The default value is 300 seconds with a minimum value of 30 seconds. The interval must be a multiple of 30 seconds.

The ADES AIM polling interval can be modified from within CA Spectrum. For more information, see [Updating ADES AIM Configuration Options](#) (see page 46).

Important! CA Spectrum uses its own polling interval to control how often to poll the ADES AIM. For more information on polling intervals used by ADES Manager, see [Controlling Polling Intervals](#) (see page 45).

Installing ADES Manager Components

ADES Manager is included in all CA Spectrum extraction keys. When you install CA Spectrum, the ADES Manager components are automatically installed and available for use. However, ADES Manager is not operable until you also install and configure the CA SystemEDGE agent and ADES AIM. To manage your Active Directory and Exchange Server environment properly, CA Spectrum must be able to contact the CA SystemEDGE agent (which has the ADES AIM loaded); and, the AIM must be able to communicate with your Active Directory and Exchange Server hosts.

To install ADES Manager properly, the administrator must complete these tasks:

- Install the CA SystemEDGE agent and load and configure the ADES AIM, specifying the domain or domains to monitor. Note the following:
 - The CA SystemEDGE agent and ADES AIM must be installed on a Windows host that:
 - Is a member server in one of the domains to be monitored, with a trust relationship to the remaining domains.
 - Does not have any Active Directory or Exchange Server roles.
- The ADES AIM must be the only AIM installed on the CA SystemEDGE host.
- The ADES AIM can monitor the domain using various configurations. The ADES AIM can be configured to monitor Active Directory hosts, Exchange Server hosts, or both; and to use either domain-based (see definition on page 66) or host-based (see definition on page 66) management mode.

Important! The CA SystemEDGE agent and ADES AIM should *not* be installed on a host that will be managed by ADES Manager.

Note: For more information about ADES AIM functionality at a high level, see [Understanding ADES AIM Technology](#) (see page 19). For details about installing the CA SystemEDGE agent and ADES AIM, see the *CA Virtual Assurance for Infrastructure Managers Installation Guide* and *CA Virtual Assurance for Infrastructure Managers Administration Guide*, respectively.

- Install CA Spectrum with ADES Manager included.

Important! The SpectroSERVER should not be installed on a machine that will be managed by ADES Manager.

Note: For specific installation instructions, see the *Installation Guide*.

You can now discover and model your Active Directory and Exchange Server environment in CA Spectrum. See [Discovery and Modeling](#) (see page 22).

More information:

[Discovery Options for the ADES AIM](#) (see page 20)

Discovery and Modeling

After you have installed the necessary components, you have to discover and model any hosts that are to be managed before you can begin using ADES Manager to monitor your Active Directory and Exchange Server environments. The following types of discovery are used:

- Discovery on the ADES AIM (ADES AIM Discovery)
- Standard CA Spectrum Discovery
- Discovery within CA Spectrum of Active Directory and Exchange Server hosts to be managed (ADES Manager Discovery)

ADES Manager relies on the ADES AIM discovery to collect information about available Active Directory and Exchange Server hosts in the specified domains and, through ADES Manager Discovery, uses this information to model each Active Directory or Exchange Server host individually. Models are placed in the hierarchy and in ADES Managed Hosts containers in the topology. Using standard CA Spectrum logic, connections are established between the hosts and the upstream devices that are modeled during standard CA Spectrum Discovery.

This section provides the following topics:

- [Discover and Model Your Active Directory and Exchange Server Environment](#) (see page 23)
- [Models Created for ADES Manager](#) (see page 29)

Discover and Model Your Active Directory and Exchange Server Environment

The following steps are necessary to discover and model your Active Directory and Exchange Server environments:

1. [Let ADES AIM Discovery run.](#) (see page 23)
2. [Run a standard CA Spectrum Discovery to model the ADES Host Manager and connecting devices.](#) (see page 24)
3. [If necessary, upgrade the CA SystemEDGE model](#) (see page 26).
4. [Specify hosts to manage by ADES Manager](#) (see page 26).
5. [Let ADES Manager Discovery run.](#) (see page 27)

ADES AIM Discovery

ADES AIM Discovery occurs automatically when you set up the ADES AIM on the ADES Host Manager, as described in [Installing ADES Manager Components](#) (see page 21). The following describes the ADES AIM Discovery process and is provided for reference only. No action is required.

ADES AIM Discovery works as follows:

1. After the ADES AIM is installed correctly, the ADES AIM queries the Global Catalogs to retrieve all Active Directory and/or Exchange Server hosts for the configured domains and identifies roles configured on each host. Hosts that have one or more supported roles are made available for management by CA Spectrum ADES Manager. The management entity setting is also used to include only those hosts having a supported role for the configured technology (Active Directory, Exchange Server, or both).
2. Using the specified management mode, the ADES AIM sets all hosts as managed (domain-based management (see definition on page 66)) or not managed (host-based management (see definition on page 66)) by default.
3. The ADES AIM immediately begins polling all hosts that are set as managed to gather information about their respective server role function.
4. After the initial discovery, you must start ADES AIM Discovery manually to detect any subsequent changes to the environment. For more information, see [Updating Your Managed Environment](#) (see page 46).

Note: The ADES AIM stores a list of available hosts and their managed settings. On a restart of the ADES AIM, this host list is read in and any host that still resides in the Active Directory and Exchange Server environment retains its previous managed setting.

Run CA Spectrum Discovery to Model the ADES Host Manager and Connecting Devices

After the ADES Host Manager has been set up and ADES AIM Discovery has started, the ADES Host Manager and any connecting devices need to be modeled. You can use standard CA Spectrum Discovery to:

- Model the ADES Host Manager, which must be modeled with a read/write community string.
- Model the necessary upstream routers and switches of your Active Directory and Exchange Server environments so that connections from the Active Directory and Exchange Server hosts can later be established.

Important! It is not recommended to specify Active Directory and Exchange Server hosts to be modeled. Active Directory and Exchange Server hosts are discovered and modeled automatically during ADES Manager Discovery.

Note: This procedure is performed by an administrator only.

Follow these steps:

1. Open the Discovery console.

Note: Before modeling, prepare by gathering the correct community strings, IP addresses, and port numbers for any SNMP agents that run on a nonstandard port.



2. Click  (Creates a new configuration) in the Navigation panel.

The Configuration dialog opens.

3. Specify a name and location for the new configuration, and click OK.

The Configuration dialog closes.

4. Enter individual IP addresses or the beginning and ending IP addresses in the IP/Host Name Boundary List fields and click Add.

Note: Verify that the range of IP addresses includes all ADES Host Managers and the interconnecting switches and routers.

5. Configure SNMP Information.

Important! The ADES Host Manager must be modeled with a read/write community string. If you are modeling the ADES Host Manager in this Discovery, verify that its community string is placed appropriately in the ordered list. Alternatively, you can change the community string for the ADES Host Manager to its read/write value after the discovery.

6. Configure your Modeling Options as follows:

- a. Select the 'Discover and automatically model to CA Spectrum' option.

- b. Click the Modeling Options button.

The Modeling Configuration dialog opens.

- c. Click the Protocol Options button.

The Protocol Options dialog opens.

- d. Select the ARP Tables for Pingables option, and click OK.

The Protocol Options dialog closes.

- e. Click OK to close the Modeling Configuration dialog.

7. (Optional) Click the Advanced Options button in the Advanced Options group, add any nonstandard SNMP ports, and click OK.

The Advanced Options dialog closes.

8. Enter any additional values needed in the Discovery console to model your connecting devices and ADES Host Managers, and click the Discover button.

Models are created and added to your network topology in CA Spectrum for the following:

- Active Directory and Exchange Server Host Manager (ADES Host Manager).

Note: If the Discovery process did not assign the read/write community string to this model, use the CA Spectrum Modeling Information subview for the model to update this setting.

- The upstream switches and routers that connect the hosts in your Active Directory and Exchange Server environment to your network.

When these models exist in CA Spectrum, ADES Manager Discovery can begin.

Note: Instead of using standard CA Spectrum Discovery, you can manually model your ADES Host Manager by IP address or host name. If you do, model the upstream devices first (since modeling the ADES Host Manager automatically triggers an ADES Manager Discovery). Modeling in the proper order allows for the correct creation of connections in the topology between your Active Directory and Exchange Server hosts and the remainder of your network. For more information on how to perform a Discovery or manually discover by IP address or host name, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Upgrade the CA SystemEDGE Host Model (If Necessary)

If the CA SystemEDGE host was modeled in CA Spectrum before the ADES AIM was loaded on the agent, the existing CA SystemEDGE host (Host_systemEDGE) model is not compatible with ADES Manager. You must upgrade the model so that ADES Manager can access the ADES AIM capabilities in CA SystemEDGE.

To upgrade the CA SystemEDGE host model, right-click the model and select Reconfiguration, Reconfigure Model.

The CA SystemEDGE host model is upgraded to support the ADES AIM.

Note: You can also send a reconfigure model action to the CA SystemEDGE agent via CLI. For instructions to send a reconfigure model action to the CA SystemEDGE agent, see *Modeling and Managing Your IT Infrastructure Administrator Guide*.

Specify Hosts to Manage by ADES AIM

Hosts must be set as "managed" to be modeled in CA Spectrum. When using domain-based management (see definition on page 66), all hosts are set initially to be managed; with host-based management (see definition on page 66), all hosts are set initially to not be managed. Use the Universal Host Table (UHT) view in CA Spectrum to specify hosts to manage, as described in this section.

Using host-based management, you can distribute the management of hosts in a domain across multiple ADES AIMs for load balancing. The UHT contains all available hosts in all domains for which the ADES AIM is configured and lets you specify hosts for management. A host should only be managed by a single ADES AIM.

Important! Managing a single host by multiple ADES AIMs can introduce performance issues. For more information, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Note: Although these settings can also be set using MIB Tools or another MIB browser, it is recommended that you use the UHT view provided in CA Spectrum.

When a host is set to be managed, it appears in the Managed Host Table (MHT) view in CA Spectrum. The MHT contains the subset of UHT hosts for which the ADES AIM is polling for Active Directory and Exchange Server metrics. The MHT resides in the ADES AIM, and ADES Manager uses the MHT as its basis for creating, deleting, or updating Active Directory and Exchange Server host models.

Note: Only users with the appropriate privileges can modify host management. For more information, see the *Administrator Guide*.

Follow these steps:

1. Select the ADES Host Manager model. The model has a device type of 'Active Directory and Exchange Server Host Manager.'

Note: The host must have been modeled with a read/write community string.

The Component Detail panel displays information for the selected ADES Host Manager.

2. In the Information tab in the Component Detail panel, expand the Active Directory and Exchange Server (ADES) Management, Host Management, Universal Host Table subview.

The Universal Host Table lists all hosts that are available for management by this ADES AIM. The table also indicates the server roles defined for each host.

3. Select one or more hosts in the table, and click Manage or Do Not Manage to specify whether the hosts are managed by this ADES AIM.

Note: When working with a large number of hosts, undock the Universal Host Table subview to enable expansion of the table view. You can also use shift-click and control-click to control your host selection, as follows:

- To select a consecutive group of hosts, click the first host, press and hold down the Shift key, and then click the last host.
- To select non-consecutive hosts, press and hold down the Ctrl key, and then click each host that you want to select.

A check mark is displayed in the Managed column for any host that is managed by this ADES AIM. Each managed host exists in the MHT, as displayed by the Managed Host Table view.

Note: For information about moving a host from the management of one ADES AIM to another, see [Modifying ADES Manager Host Management and Models](#) (see page 49).

More information:

[Environment Management Considerations](#) (see page 14)

[Understanding ADES AIM Technology](#) (see page 19)

ADES Manager Discovery

ADES Manager Discovery is the modeling within CA Spectrum of any required ADES Manager components. These components include any managed Active Directory and Exchange Server hosts. Modeling the ADES Host Manager automatically triggers an ADES Manager Discovery.

After the initial modeling of the ADES Host Manager, anytime you add or delete a host in the Universal Host Table subview for management by CA Spectrum ADES Manager, ADES Manager Discovery runs automatically to update the modeling within CA Spectrum. It also runs automatically whenever an ADES AIM Discovery runs and effects changes in the Managed Host Table.

The following description explains the entire ADES Manager Discovery process and is provided for reference. No action is required.

ADES Manager Discovery works as follows:

1. After CA Spectrum models a CA SystemEDGE host and detects the presence of the ADES AIM, the following actions occur:
 - a. When the ADES AIM is detected, the device type of the CA SystemEDGE host changes to 'Active Directory and Exchange Server Host Manager'.
 - b. An application model that can run ADES AIM Discovery is created.
 - c. An ADES Managed Hosts container is created to contain any new Active Directory or Exchange Server host models for this ADES AIM.
2. With communication between CA Spectrum and the ADES AIM established, the CA Spectrum host-modeling process begins automatically. ADES Manager uses information from the MHT (see definition on page 67) in the ADES AIM to determine which hosts should be modeled. For each host to be modeled, if a model does not exist, a new host model is created. If an SNMP agent exists on the host, an SNMP-capable host model is created; otherwise, an ICMP (Pingable) model is created.
3. New Active Directory or Exchange Server host models appear in the Active Directory and Exchange Server Manager hierarchy in the Explorer view and are placed into the ADES Managed Hosts container for the ADES AIM in the topology view. Connections to any upstream devices are made.

Important! If a host is already modeled in your CA Spectrum-managed network prior to ADES Manager discovery, it will not be modeled again nor will the original model be moved in the topology. However, it is still included in the Active Directory and Exchange Server Manager hierarchy.

Note: You can also manually control whether a host is managed using the Universal Host Table (see definition on page 67). Modifying the UHT adds or deletes the host in the Managed Host Table, which triggers the modeling process. An ADES AIM Discovery can also add or remove host models from the MHT, which also triggers the modeling process.

More information:

[Host Modeling](#) (see page 14)

[Specify Hosts to Manage by ADES AIM](#) (see page 26)

Models Created for ADES Manager

ADES Manager provides several models to represent the components of your Active Directory and Exchange Server environments. Understanding the following basic models can help you to better understand Discovery and how the models relate to one another.



Active Directory and Exchange Server Host Manager (ADES Host Manager)

Model Type: Host_systemEDGE

Represents the host that contains the ADES AIM. The ADES AIM monitors the Active Directory and Exchange Server hosts in your environment. Successful creation of this model indicates that all requisite intelligence to support ADES Manager has been installed on the ADES Host Manager. This model has a device type of Active Directory and Exchange Server Host Manager.



<ADES_Host_Manager_name> Managed Hosts

Model Type: ADESHostContainer

Initially contains newly-created host models that are managed by the named ADES AIM. You can add or remove models from the container, but you cannot destroy the container itself. When possible, this container model is created alongside the ADES Host Manager model. If a managed host has already been modeled elsewhere in your CA Spectrum-managed network, it will not be modeled again nor will the original model be moved into this container. This includes a host that is being managed by another ADES AIM. If a host is managed by multiple ADES AIMs in the same landscape, it is included in the ADES Managed Hosts container for the first ADES AIM to model it only.

Note: The following pertains to virtual machines:

- If the ADES Host Manager is a virtual machine, the container is placed in the same topology as the associated Virtual Host Manager physical host container model.
- Active Directory and Exchange Server hosts that are virtual machines and managed by Virtual Host Manager are not placed into the ADES Managed Hosts container.



Active Directory and Exchange Server Host

Represents an Active Directory or Exchange Server host.

Note: If a host is managed by multiple ADES AIMs residing in different SpectroSERVERs of a multi-landscape environment, duplicate models will exist. For more information, see [Duplicate Models Created After Discovery](#) (see page 58).

For information about changing your modeled environment, including modifying host management by ADES AIM or deleting ADES Manager models, see [Maintaining Your ADES Manager Environment](#) (see page 45).

Chapter 3: Viewing Your Active Directory and Exchange Server Environments

The purpose of ADES Manager is to provide visibility into your Active Directory and Exchange Server environments. This visibility allows you to easily identify the function or role each host plays as well as the logical relationships between the players. Most importantly, when a problem occurs in your environment you can pinpoint its cause.

ADES Manager provides several methods for viewing your Active Directory and Exchange Server environments, as follows:

- Logical relationships are indicated by the Explorer tab's Active Directory and Exchange Server Manager hierarchy in the Navigation panel. Examples of hierarchy nodes include forests, domains, and roles.
- A graphical topology view helps you group like-managed Active Directory and Exchange Server hosts together as well as visualize the connections between the hosts.
- Customized Information views in the Component Detail panel provide details that are specific to Active Directory and Exchange Server technologies.
- Customized searches provide a quick way to find hosts by using Active Directory and Exchange Server metrics.
- Customized icons for individual models provide status and model type information at a glance and are integrated throughout the ADES Manager feature.

Understanding each of these methods can help you to monitor your Active Directory and Exchange Server environments more efficiently, allowing you to troubleshoot issues and optimize performance more effectively.

This section contains the following topics:

[Explorer View](#) (see page 32)

[Topology View](#) (see page 35)

[Information Subviews](#) (see page 36)

[Locator Searches](#) (see page 42)

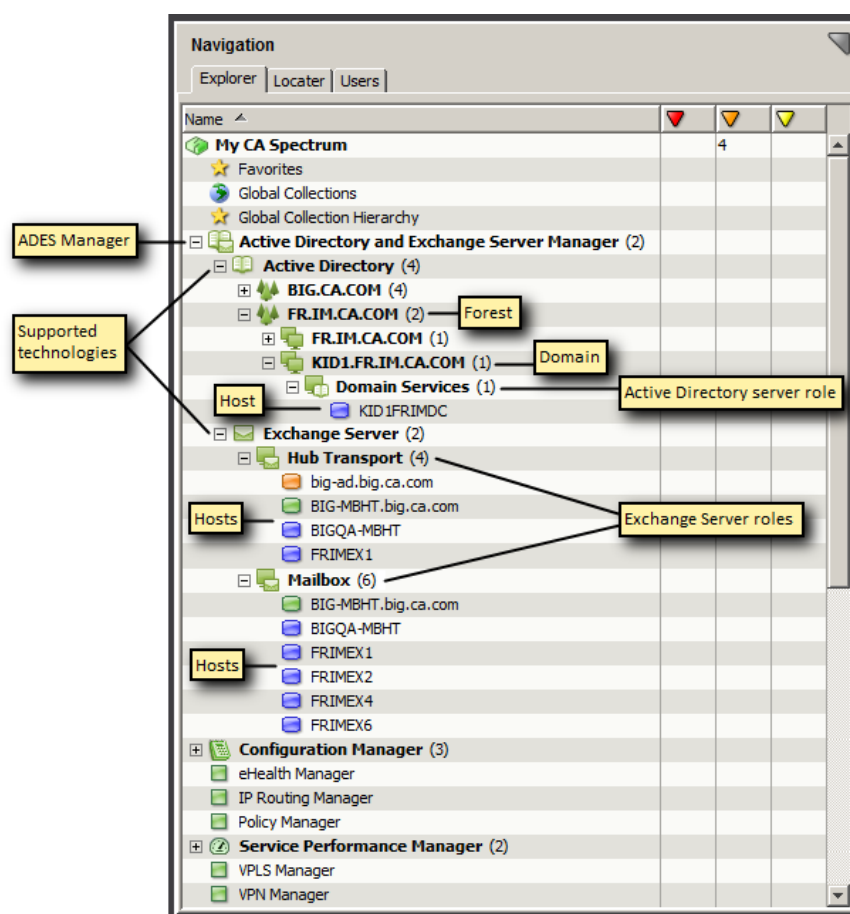
[Event Reports](#) (see page 43)

Explorer View

On the Explorer tab of the Navigation panel, the Active Directory and Exchange Server Manager node provides a hierarchical tree structure that helps you to visualize the logical organization of your managed Active Directory and Exchange Server environments. Distinctive icons distinguish the technologies, forests, domains, hosts, and roles used in your managed environment.

Using this information, you can see how the hosts are logically arranged as well as which functions or roles are supported by each host in your environment.

The following image is an example of the ADES Manager hierarchy:



The following nodes form the hierarchy:

Active Directory and Exchange Server Manager

Active Directory and Exchange Server Manager is the root node for the Active Directory and Exchange Server environments that are currently managed. Because ADES Manager is a distributed manager that handles multiple landscapes, the node appears above the landscape level.

Expanding the Active Directory and Exchange Server Manager node displays the technologies that are supported, as follows.

Note: Only technology, forest, domain, or role nodes that contain at least one managed host in their sub-hierarchy are displayed.

Active Directory

The Active Directory node structure displays all managed hosts that support the Active Directory Domain Services (AD DS) server role. For each host, the forest and domain to which it belongs are also presented, as depicted in the following diagram:

```
[ - ] Active Directory
    [ - ] Forest 1
        [ - ] Domain 1
            [ - ] Domain Services
                . Host 1
                . Host 2
                . Host 3
            [+] Domain 2
        [+] Forest 2
```

Note: Although there are other Active Directory server roles, CA Spectrum ADES Manager supports the AD DS server role only.

The hierarchy under the Active Directory node represents the logical relationships between the following components:

■ Forest

The forest node represents the forest (see definition on page 66) to which the domains with managed hosts belong.

■ Domain

The domain node represents the domain (see definition on page 66) to which the managed hosts belong. Its name is derived from the Domain Name System (DNS) name.

■ **Domain Services**



The Domain Services node represents the Active Directory Domain Services (AD DS) server role. All hosts displayed within this node structure support the AD DS server role.

■ **Host**

All hosts that appear within the Active Directory node structure support the AD DS server role. Such hosts are referred to as domain controllers (see definition on page 66).

Note: For more information, see [Active Directory Overview](#) (see page 8).

Exchange Server



The Exchange Server node structure displays all managed hosts that function in the Hub Transport or Mailbox server roles. Hosts can satisfy multiple roles and, as a result, may appear more than once. The format of the Exchange Server node structure is as follows:

```
[ - ] Exchange Server
  [ - ] Hub Transport
    . Host 4
    . Host 5
  [ - ] Mailbox
    . Host 1
    . Host 3
    . Host 4
    . Host 5
    . Host 6
```

Note: Although there are other Exchange Server roles, CA Spectrum ADES Manager supports the Hub Transport and Mailbox server roles only.

The hierarchy under the Exchange Server node represents the logical relationships between the following components:

- **Hub Transport**

The Hub Transport node represents the Exchange Server Hub Transport server role. All hosts displayed within this node structure support the Hub Transport server role.

- **Mailbox**

The Mailbox node represents the Exchange Server Mailbox server role. All hosts displayed within this node structure support the Mailbox server role.

- **Host**

All hosts that appear within the Hub Transport node structure support the Hub Transport server role, and all hosts that appear within the Mailbox node structure support the Mailbox role. If a host supports multiple roles, it appears multiple times in the hierarchy.

Note: For more information, see [Exchange Server Overview](#) (see page 10).

Topology View

The Active Directory and Exchange Server hosts in your managed Active Directory or Exchange Server environment are modeled, organized, and integrated into the Universe topology view. This graphical representation helps you to visualize the structure of your managed environment, including connections between Active Directory and Exchange Server hosts and other elements of your network.

Host models that are created during ADES Manager Discovery are placed in the topology in an ADES Managed Hosts container specific to the ADES AIM. When possible, this container model is created alongside the corresponding ADES Host Manager model.

If a managed host has already been modeled in your CA Spectrum-managed network prior to ADES Manager discovery, it will not be modeled again nor will the original model be moved into the ADES Managed Hosts container in the topology during ADES Manager Discovery. This includes a host that is being managed by another ADES AIM within the same landscape. If a host is managed by multiple ADES AIMs in the same landscape, it is included in the ADES Managed Hosts container for the first ADES AIM to model it only.

Active Directory and Exchange Server host models can be moved out of the ADES Managed Hosts container. Additionally, this container is not limited to Active Directory and Exchange Server hosts; in certain cases, you can move other host models into the ADES Managed Hosts container manually if the administrator considers the inclusion to be logical.

Although you can add or remove models from the container, you cannot destroy the container itself directly. The ADES Managed Hosts container is only destroyed when an ADES Host Manager model is deleted. If the container is destroyed, all models in the container (except for models in a global collection) are moved to the Lost and Found (LostFound). This includes any models that are moved manually into the container and may not necessarily be Active Directory or Exchange Server hosts.

Important! The contents of an ADES Managed Hosts container may not be a comprehensive reflection of the hosts managed by the corresponding ADES AIM. If a host has already been modeled in the landscape, the host will not be modeled again nor will the original model be moved into the ADES Managed Hosts container in the topology.

More information:

[What is Modeled](#) (see page 15)

[Hosts Managed by Virtual Host Manager and ADES Manager](#) (see page 18)

[Deleting ADES Manager Models](#) (see page 49)

Support for Virtual Machines

CA Spectrum attempts to create the ADES Managed Hosts container at the same level as the ADES Host Manager; however, special handling applies when components are virtual machines, as follows:

- If the ADES Host Manager is a virtual machine, the ADES Managed Hosts container is placed in the same topology as the parent Virtual Host Manager physical host container model for the ADES Host Manager.
- Active Directory and Exchange Server hosts that are virtual machines and managed by Virtual Host Manager are not placed into the ADES Managed Hosts container. They reside in their physical host container model permanently.

Information Subviews

Customized views in the Component Detail panel provide detailed information about the components in your Active Directory and Exchange Server environments. You can view information specific to your managed Active Directory and Exchange Server environments by:

- [ADES Host Manager \(ADES AIM\)](#) (see page 37)
- [Individual Host](#) (see page 40)

ADES Host Manager (ADES AIM) Subviews

Using views provided at the ADES Host Manager (ADES AIM) level, you can view the following information:

- Information specific to the ADES Host Manager such as agent version, polling interval, and ADES AIM Discovery status. You can also control certain options in the ADES AIM from these views, including polling interval and initiation of an ADES AIM Discovery.
- Information about hosts that are available for management and those that are actually being managed by the ADES AIM. You can also control which hosts to manage by the ADES AIM.
- Consolidated information about all hosts in your Active Directory and Exchange Server environments that are managed by this single ADES AIM. Views at the ADES AIM level combine information from all hosts that are managed by the AIM. From this perspective, for example, you can see collectively all hosts that serve a supported role, a list of domain controllers, or a list of all mailbox databases that reside on hosts that are managed by an ADES AIM.

The following describes how to view information for an ADES Host Manager (ADES AIM).

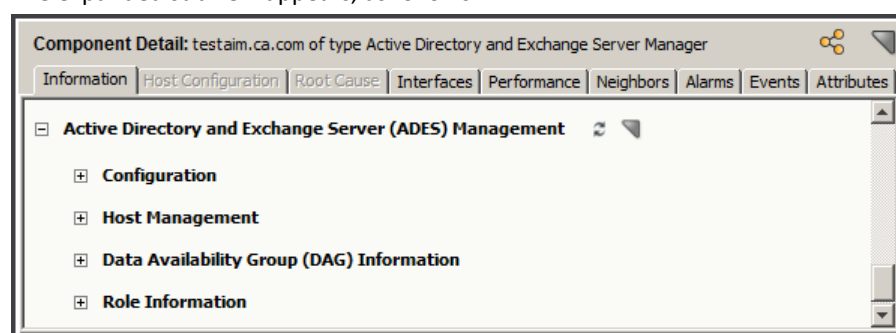
Follow these steps:

1. Select the ADES Host Manager model. The model has a device type of 'Active Directory and Exchange Server Host Manager.'

The Component Detail panel displays information for the selected ADES Host Manager.

2. In the Information tab in the Component Detail panel, expand the Active Directory and Exchange Server (ADES) Management subview.

The expanded subview appears, as follows:



Active Directory and Exchange Server (ADES) Management Subviews - ADES Host Manager (ADES AIM)

The following subviews are available at the ADES Host Manager (ADES AIM) level.

Note: When viewing host information using the ADES Host Manager subviews, the Host Name that appears reflects the name as provided by the ADES AIM. This value may differ from the model name chosen by CA Spectrum and which appears in the hierarchy and topology views. For more information on how CA Spectrum assigns model names for ADES Manager, see [Model Naming](#) (see page 17).

Configuration

Provides information specific to the ADES Host Manager, including:

- Agent identification, version, and status details.
- ADES AIM polling interval and Windows Event settings. This view also lets you modify these settings, as described in [Updating ADES AIM Configuration Options](#) (see page 46).
- Date and time when the ADES AIM inventory was last updated.
- Date and time when the last ADES AIM Discovery was performed. This view also lets you initiate a new ADES AIM Discovery, as described in [Updating Your Managed Environment](#) (see page 46).

Host Management

Provides information about available hosts and whether they are currently managed by this ADES AIM.

Universal Host Table

Lists all hosts that are available for management by this ADES AIM and the server roles defined for each host. This table also lets you control which hosts are managed.

For more information about the Universal Host Table, see [Specify Hosts to Manage by ADES AIM](#) (see page 26).

Managed Host Table

Lists all hosts that are managed by this ADES AIM. Unlike the Universal Host Table, which lists all hosts that *can* be managed by this AIM, the Managed Host Table lists those that are *actually* managed. The read-only Managed Host Table also provides AIM-specific polling and status information for each host.

For more information about the Managed Host Table, see [Specify Hosts to Manage by ADES AIM](#) (see page 26).

Data Availability Group (DAG) Information

Provides read-only information about the DAGs (see definition on page 66) that any of the Mailbox hosts that are managed by this ADES AIM are members of. Various subviews are provided, each presenting DAG-related information from a different perspective, including:

- General DAG configuration details such as originating and witness server information, compression and encryption used, and other replication details.
- Database information including active or passive copy status, issued error messages, latest snapshots and other backup details.
- Organizational information for DAG hosts and networks.

Role Information

Provides read-only information specific to each of the supported server roles. For the Domain Services role, all domain controllers are included in the views whether managed or not. For other roles, only hosts that are managed by this ADES AIM are included.

Note: A subview table contains data only when at least one host satisfying the above criteria exists. Otherwise, the table is empty.

Domain Services

Lists all domain controllers in the Global Catalogs accessed by this ADES AIM and also provides any domain controller replication information, such as source and destination servers and synchronization information.

Note: Although all domain controllers are reported, some of them may not be managed by the ADES AIM.

Hub Transport

Provides detailed information about each transport server such as identification of the originating server, external IP addresses that are used, and DNS servers that should be used. Locations of connectivity, message tracking, routing table, and server statistics log files are also provided. Details that are specific to Exchange Server 2010 are grouped separately.

Mailbox

Provides lists of all mailbox databases and mailbox server hosts managed by this ADES AIM. Mailbox host information includes details such as Exchange version, number of mailboxes hosted, name of organizational unit, and locations of log and data files. Details that are unique to Exchange Server 2007 (such as clustering support) or Exchange Server 2010 (such as DAG support) are grouped separately.

Individual Host Subviews

You can view information for individual hosts in your managed Active Directory and Exchange Server environments. Views for individual hosts provide information that is specific to all the server roles that are provided by the host, such as real-time LDAP activity metrics for Active Directory hosts or DAG information for Mailbox hosts.

The following describes how to view information for an individual host that is monitored by ADES Manager.

Follow these steps:

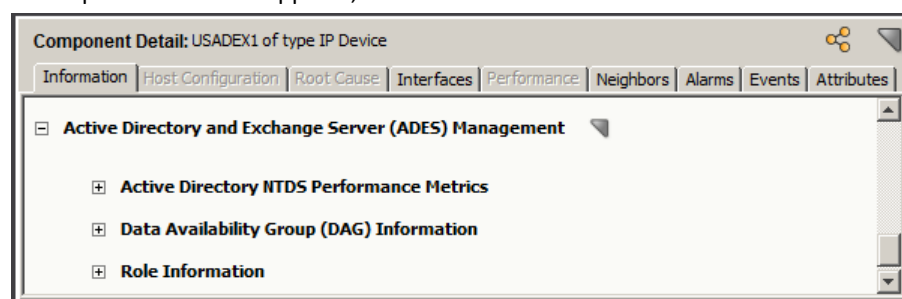
1. Select the model for a host that is managed by ADES Manager. The model exists under the Active Directory and Exchange Server Manager hierarchy in the Explorer tab of the Navigation panel.

Note: You can also select the host using any of the standard CA Spectrum methods, such as from a list (for example, in the Contents panel, List tab) or in the topology.

The Component Detail panel displays information for the selected Active Directory or Exchange Server host model.

2. In the Information tab in the Component Detail panel, expand the Active Directory and Exchange Server (ADES) Management subview.

The expanded subview appears, as follows:



Active Directory and Exchange Server (ADES) Management Subviews - Individual Hosts

The following subviews are available for individual hosts.

Note: When viewing host information using the individual host subviews, the referenced host names that appear reflect the names as provided by the ADES AIM. These values may differ from the model names chosen by CA Spectrum and which appear in the hierarchy and topology views. For more information on how CA Spectrum assigns model names for ADES Manager, see [Model Naming](#) (see page 17).

Active Directory NTDS Performance Metrics

(For Domain Services hosts) Provides performance data on activities such as LDAP operations, object updates and replication, and authentication requests.

Data Availability Group (DAG) Information

(For Mailbox hosts) Provides read-only information about the DAG (see definition on page 66) that the selected Mailbox host is a member of. Information includes active or passive status, data center activation mode, and other DAG-related details.

Role Information

Provides read-only information specific to each of the supported server roles, as follows.

Note: A subview table contains data only when the host supports the respective role.

Domain Controller

Provides general domain identification information, such as full domain name and IP address, and any replication information, such as source and destination servers and synchronization information.

Hub Transport Host Inventory

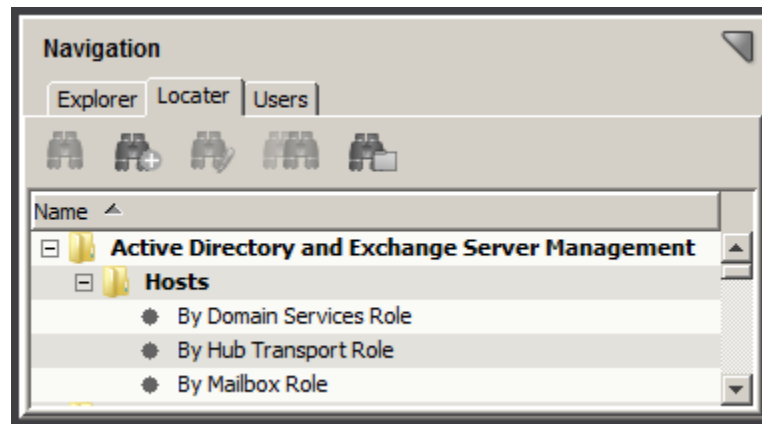
Provides detailed transport server information such as the external IP address that is used and DNS servers that should be used. Locations of connectivity, message tracking, routing table, and server statistics log files are also provided.

Mailbox Host Inventory

Provides mailbox host information that includes details such as Exchange version, number of mailboxes hosted, name of organizational unit, and locations of log and data files. Details that are unique to Exchange Server 2007 (such as clustering support) or Exchange Server 2010 (such as DAG support) are grouped separately.

Locator Searches

You can use preconfigured searches to quickly locate entities in the CA Spectrum database that are related to the Active Directory and Exchange Server technologies. The searches are grouped under the Active Directory and Exchange Server Management folder in the Locator tab of the Navigation panel, as shown:



The following searches are specific to Active Directory and Exchange Server technologies:

Hosts

Locates all hosts modeled in the CA Spectrum database that have been identified as serving the specified role in one of the following searches:

- By Domain Services Role
- By Hub Transport Role
- By Mailbox Role

Note: Only users with the appropriate privileges can access Active Directory and Exchange Server Management searches. For more information, see the *Administrator Guide*.

Event Reports

To help you monitor your Active Directory and Exchange Server environments, you can create event reports. Event reports gather information that helps you make informed decisions about your Active Directory and Exchange Server environment entities. Using the correct event filters, you can base these reports on any of the various management events generated for your Active Directory or Exchange Server environment entities in CA Spectrum.

To report on ADES Manager events, the following event filter file is included with Report Manager:

- ADES-events-filter.xml

Note: For more information about using Report Manager to generate event reports from these codes, see the *Report Manager User Guide*. For information about using the predefined event filter files to generate reports, see the *Report Manager Installation and Administration Guide*.

Chapter 4: Maintaining Your ADES Manager Environment

This section contains the following topics:

[Controlling Polling Intervals](#) (see page 45)

[Updating ADES AIM Configuration Options](#) (see page 46)

[Updating Your Managed Environment](#) (see page 46)

[Modifying ADES Manager Host Management and Models](#) (see page 49)

[Deleting ADES Manager Models](#) (see page 49)

Controlling Polling Intervals

Polling intervals control how often information is obtained from managed devices. To keep data for your managed Active Directory and Exchange Server environments current, CA Spectrum ADES Manager uses polling intervals set on the following components:

■ ADES AIM

The ADES AIM polling interval indicates how often the ADES AIM queries the managed hosts for information.

The ADES AIM polling interval exists in the ADES AIM but can be modified from within CA Spectrum. The default value is 300 seconds with a minimum value of 30 seconds. The interval must be a multiple of 30 seconds.

For information on how to update the ADES AIM polling interval from within CA Spectrum, see [Updating ADES AIM Configuration Options](#) (see page 46).

■ ADES Host Manager model

The polling interval on the ADES Host Manager model determines how often CA Spectrum polls the ADES AIM. The default value is 300 seconds with a minimum value of 30 seconds. This setting is available on the CA Spectrum Modeling Information view for the Active Directory and Exchange Server Host Manager (Host_systemEDGE) model.

Updating ADES AIM Configuration Options

ADES Manager uses the ADES AIM for discovery, modeling, and monitoring of your Active Directory and Exchange Server environments. Certain functionality is controlled and provided by the ADES AIM exclusively. Some ADES AIM settings can only be changed directly in the AIM (such as what domains are managed), while others can be changed from within CA Spectrum (such as the ADES AIM polling interval). This section describes how to change certain ADES AIM settings from within CA Spectrum.

Note: For detailed information about all ADES AIM parameters, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

Follow these steps:

1. Select the ADES Host Manager model that supports the ADES AIM. The model has a device type of 'Active Directory and Exchange Server Host Manager.'

The Component Detail panel displays information for the selected ADES Host Manager.
2. In the Information tab in the Component Detail panel, expand the Active Directory and Exchange Server (ADES) Management, Configuration subview.

The expanded Configuration subview appears.
3. Update ADES AIM polling and Windows Event parameters as appropriate.

Updating Your Managed Environment

After the initial, automatic modeling of the Active Directory and Exchange Server environments, you must initiate ADES AIM Discovery manually to update CA Spectrum with any subsequent changes. Due to the potentially large size of the Active Directory and Exchange Server environments, dynamic updates would be expensive for the ADES AIM to maintain. After ADES AIM Discovery completes, ADES Manager Discovery begins automatically, modeling changes in the environment as detected by the ADES AIM.

The following sections describe this process:

- [Discovery Process for Updating Your Modeled Environment](#) (see page 46)
- [How to Initiate Discovery](#) (see page 47)

Discovery Process for Updating Your Modeled Environment

Discovery for ADES Manager consists of two phases:

1. Discovery by the ADES AIM identifies changes to your Active Directory and Exchange Server environment as reflected in the Global Catalogs and makes these hosts available for management in the ADES AIM.

2. Discovery by ADES Manager uses the environment information gathered by the ADES AIM and the settings defined in the ADES AIM to update the CA Spectrum modeled environment. When a new host is detected in a Global Catalog, the ADES AIM first determines whether the host is available to manage based on the management entity for its domain. If so, the ADES AIM then examines the management mode for its domain. Based on the management mode, the following occurs:
 - In domain-based management (see definition on page 66), the host is set automatically to be managed. CA Spectrum models and begins monitoring the new host automatically.
 - In host-based management (see definition on page 66), the host is set automatically to not be managed. You must explicitly specify to manage the host using the Universal Host Table before CA Spectrum models and subsequently begins monitoring the new host.

Note: The determination of whether a host is managed or not managed applies to *newly-detected* hosts only. A host that was previously detected in a Global Catalog and identified by the ADES AIM as available to manage retains its previous managed setting.

The next section describes how to update your CA Spectrum modeled environment.

How to Update Your Modeled Environment

The following steps describe how to update your modeled environment, which begins with initiating an ADES AIM Discovery.

Note: Only users with the appropriate privileges can initiate ADES AIM Discovery. For more information, see the *Administrator Guide*.

Follow these steps:

1. Select the ADES Host Manager model that supports the ADES AIM. The model has a device type of 'Active Directory and Exchange Server Host Manager.'

The Component Detail panel displays information for the selected ADES Host Manager.

2. In the Information tab in the Component Detail panel, expand the Active Directory and Exchange Server (ADES) Management, Configuration subview.

The expanded Configuration subview appears and displays information about when the last ADES AIM Discovery was run.

Last Agent Inventory Update

Indicates the last time that an ADES AIM Discovery was performed or the last time a change was made to the ADES AIM inventory, which is used for CA Spectrum modeling. Editing host management in the Universal Host Table is a direct way to alter the ADES AIM inventory.

Last ADES AIM Discovery of Hosts

Indicates the last time that an ADES AIM Discovery was performed.

3. Click Run.

Important! Running an ADES AIM Discovery can require significant system resources on the ADES Host Manager.

The ADES AIM Discovery begins. Any change detected in your Active Directory and Exchange Server environment causes the following:

- Updates the forest, domain, and host information in the ADES AIM inventory.
- Updates the 'Last Agent Inventory Update' and 'Last ADES AIM Discovery of Hosts' timestamp values.
- Triggers an ADES Manager Discovery in CA Spectrum to reflect any changes in your modeled environment.

Note: If you are using host-based management and new hosts are introduced, you must specify to manage the hosts. See [Specify Hosts to Manage by ADES AIM](#) (see page 26).

Modifying ADES Manager Host Management and Models

When making changes in your modeled environment, consider the following:

- When a host is managed by multiple ADES AIMs in a given landscape, it is only included in the ADES Managed Hosts container for the first ADES AIM that modeled it. If you remove the host from management by the first ADES AIM, it remains in its original container even though the host is still managed by the second ADES AIM. To move the host to the ADES Managed Hosts container for the second ADES AIM (or any other location in the topology), you must manually move (cut and paste) the model.
- When a managed host is removed from management by an ADES AIM, the host is moved from the ADES Managed Hosts container to the Lost and Found (LostFound), except in the following cases:
 - The host is being managed by another ADES AIM.
 - The host is in a global collection.
- When the IP or MAC address for a host model that is managed by ADES Manager is modified, connections to any connecting devices are automatically updated.

Deleting ADES Manager Models

Consider the following regarding deleting models in your CA Spectrum modeled environment:

- You can delete host models from your CA Spectrum modeled environment; however, you cannot manually delete forests, domains, and roles. These models are automatically deleted by an ADES Manager Discovery when no longer needed. If you delete a host model that is still managed by an ADES AIM, a new host model is created on the next ADES Manager Discovery. When this happens, any customizations made to the original model are lost.
- Active Directory or Exchange Server hosts that are managed by Virtual Host Manager adhere to all the standard modeling behaviors of virtual machines and consequently cannot be deleted from the topology.
- When an ADES Host Manager model is deleted, the corresponding ADES Managed Hosts container is destroyed. All models in the container (except for models in a global collection) are moved to the Lost and Found (LostFound). This includes any models that are moved manually into the container and may not necessarily be Active Directory or Exchange Server hosts.

Chapter 5: Alarms and Fault Isolation

This section describes the alarms generated by ADES Manager and explains how ADES Manager handles fault isolation.

This section contains the following topics:

[ADES Manager Alarms](#) (see page 51)

[ADES Manager Fault Isolation](#) (see page 51)

ADES Manager Alarms

To alert you to problems within your monitored Active Directory and Exchange Server environments, ADES Manager generates alarms for the following conditions:

- Active Directory or Exchange Server proxy communication lost, which indicates that updated Active Directory or Exchange Server metrics can no longer be obtained.
- ADES Host Manager (ADES AIM) down or communication lost

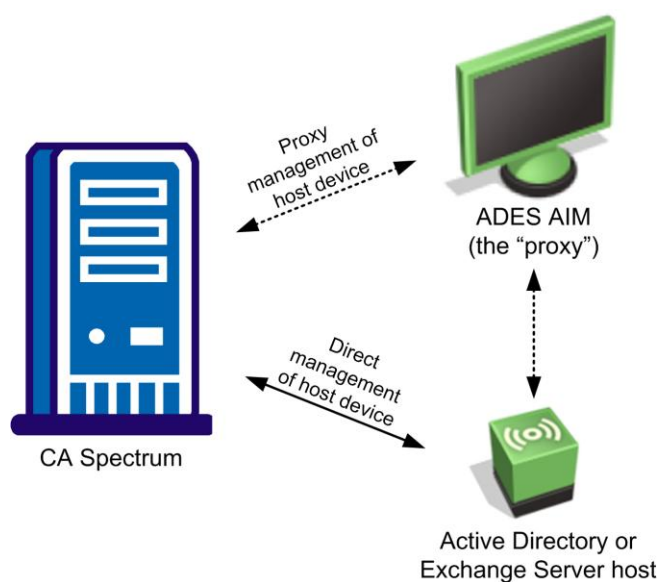
ADES Manager Fault Isolation

The goal of fault isolation is to narrow down the root cause of a networking problem so that you can quickly troubleshoot, identify, and correct the problem. Because problems with a single device can cause several other devices in your network to generate events, deciding which devices are the root cause of an alarm can be challenging. For example, losing contact with the ADES Host Manager means that you have also lost proxy communication with all the Active Directory and Exchange Server hosts it manages. As a result, alarms are generated for the ADES Host Manager and each of its managed hosts. Sifting through potentially hundreds of simultaneously produced alarms manually to pinpoint the problem could be a tedious and error-prone process. Using fault isolation techniques, ADES Manager significantly simplifies the troubleshooting process by automatically correlating these alarms to identify a single root cause.

Proxy Management

Hosts that are managed by the ADES AIM provide a unique management opportunity because they provide CA Spectrum an alternate management perspective in addition to standard device monitoring methods. Along with gathering information directly from a device, CA Spectrum also simultaneously gathers Active Directory and Exchange Server metrics such as server role information for your managed hosts from the ADES AIM. The ADES AIM serves as a "proxy" from which CA Spectrum gathers information specific to the Active Directory and Exchange Server technologies. Management of a device by way of an alternate source (such as the AIM) in addition to or in place of the device itself is called *proxy management*.

Note: The ADES AIM is not a Proxy Model as defined by CA Spectrum Modeling Information. For information about models designated as a Proxy Model, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.



This dual management perspective is handled by standard CA Spectrum fault management in two ways:

- **Proxy management alarms**—By using the ADES AIM for management, proxy-related alarms can be generated. These alarms are unique because they alert you when acquisition of Active Directory or Exchange Server metrics through the proxy is affected, not the state of the device or direct (SNMP) management. It is important to know when contact through the proxy is lost because you could be missing important server role information about your environment. Proxy management alarms are of major severity and are not clearable by the user.

- **Proxy unavailable** - When CA Spectrum cannot communicate with the ADES AIM, a proxy unavailable alarm is generated on the ADES Host Manager model.

The following text is used for the proxy unavailable alarm:

ACTIVE DIRECTORY AND EXCHANGE SERVER MANAGER UNAVAILABLE

- **Proxy lost** - When CA Spectrum cannot obtain information about the managed host by way of the proxy, then a proxy lost alarm is generated. This can happen when CA Spectrum cannot communicate with the ADES Host Manager model, which automatically generates a proxy unavailable alarm as well as a proxy lost alarm for each of its managed hosts, or when the ADES AIM cannot successfully communicate with the managed host. The following text is used for the proxy lost alarm:

ACTIVE DIRECTORY AND EXCHANGE SERVER HOST PROXY LOST

A proxy lost alarm is generated only for hosts that are managed by ADES Manager; if the host is removed from management by the proxy, the respective proxy management alarms are cleared. If a host is managed by more than one ADES AIM, multiple proxy lost alarms are generated for the managed host, one per ADES Host Manager model.

Note: A host should be managed by a single ADES AIM only.

- **Enhanced contact lost alarms**—Standard CA Spectrum alarms that indicate loss of contact with the ADES Host Manager contain additional correlation of ADES Manager proxy management alarms. These proxy management alarms indicate loss of Active Directory and Exchange Server metrics acquisition.

The following text is used for the contact lost alarm:

DEVICE HAS STOPPED RESPONDING TO POLLS

Alarm Correlation

Using standard CA Spectrum fault management and additional proxy information, ADES Manager automatically correlates the alarms to identify a single root cause. Proxy unavailable alarms on an ADES Host Manager model are correlated to any of the following alarms on the model to pinpoint the true root cause:

- Contact lost
- Maintenance
- Hibernation
- Management lost

In addition, the proxy lost alarms, which are automatically generated (one for each managed host) upon creation of a proxy unavailable alarm, are correlated to the proxy unavailable alarm

Note: You can find out more about alarms that are correlated or symptomatic by using the Impact tab for the alarm.

The scenarios presented in the next section provide additional details about alarms that are generated, what they indicate, and how they are correlated.

ADES Manager Fault Management Scenarios

The following scenarios describe how ADES Manager attempts to determine the root cause in different fault management situations.

Scenario: Contact between CA Spectrum and ADES AIM is lost

When CA Spectrum cannot communicate with ADES AIM, CA Spectrum loses information about the Active Directory and Exchange Server environment the AIM manages. To isolate the problem, ADES Manager determines the root cause as follows:

1. When CA Spectrum cannot communicate with the ADES AIM, a proxy unavailable alarm is generated on the ADES Host Manager model. This can happen, for example, when the device is in maintenance or hibernation mode. The reason for unavailability is identified through the event producing the alarm.

Note: Proxy management alarms are generated even when their models are in maintenance mode and are not visible in the Alarm view by default.

2. Because CA Spectrum cannot obtain information from the ADES AIM about any of the hosts it manages, proxy lost alarms are generated for each of the hosts managed by this AIM.
3. The proxy lost alarms are correlated to the proxy unavailable alarm as symptoms, which indicate that the proxy unavailable alarm is the root cause.

4. If CA Spectrum cannot communicate with the ADES Host Manager, one of the following standard CA Spectrum communication impairment alarms is also generated:
 - Contact lost
 - Maintenance
 - Hibernation
 - Management lost
5. Finally, the proxy unavailable alarm is correlated to the standard communication alarm forming a three-tiered hierarchy of alarm correlation: communication – proxy unavailable – proxy lost. Only the top-level communication alarm indicating the reason why CA Spectrum cannot communicate with the ADES AIM is visible to the user and indicates the root cause.

Scenario: Contact between ADES AIM and Active Directory or Exchange Server host is lost

If the ADES AIM loses contact with one of the Active Directory or Exchange Server hosts that it manages, Active Directory and Exchange Server metrics for that host can no longer be obtained, creating outdated or "stale" values in the ADES AIM. As a result, a proxy lost alarm is generated for the host.

Scenario: Active Directory or Exchange Server host is down

When an Active Directory or Exchange Server host is down, CA Spectrum uses information from both the proxy and directly from the host, as follows:

1. Because management of the device by the ADES AIM is lost, a proxy lost alarm is generated.

Note: Although a host should be managed by a single ADES AIM only, if the host is inadvertently managed by multiple ADES AIMs, multiple proxy lost alarms are generated, one for each managing ADES Host Manager model.
2. Through direct or standard CA Spectrum fault management, a contact lost alarm is generated for the managed host.

Both the contact lost alarm and proxy lost alarm are visible to the user, indicating that the proxy and direct methods of communication to the host are impacted.

Appendix A: Troubleshooting

This section contains the following topics:

[SystemEDGE Host Not Modeled as ADES Host Manager](#) (see page 57)

[Duplicate Models Created After Discovery](#) (see page 58)

[Multiply Managed Alarms](#) (see page 59)

[Connections Do Not Appear in Topology](#) (see page 60)

[ADES Managed Hosts Container Not Created](#) (see page 60)

[Host Not in ADES Managed Hosts Container](#) (see page 61)

[Unable to Update Attribute](#) (see page 61)

[Host Subview is Empty](#) (see page 62)

[Changes in Environment Not Reflected in CA Spectrum](#) (see page 62)

[ADES Manager Updates are Slow](#) (see page 63)

SystemEDGE Host Not Modeled as ADES Host Manager

Symptom:

After I model the SystemEDGE host with the ADES AIM installed, the created model is not configured as an ADES Host Manager. I am using the ADES AIM r12.7 with the latest PTFs installed (or later).

Solution:

The ADES AIM must complete its initialization and must have a ready status before CA Spectrum recognizes it as an ADES Host Manager. If you model the SystemEDGE host after the agent starts but before the ADES AIM finishes loading, the host is not modeled correctly.

To convert the existing SystemEDGE host model to an ADES Host Manager, perform the following procedure.

Follow these steps:

1. Wait for the ADES AIM to complete its initialization and reflect a ready status.

You can use MIB Tools or another MIB browser to query the SystemEDGE host and view the `exchAdAgentStatus` variable in the `empireExchangeAdMIB` MIB. A value of "ready" indicates that initialization is complete.

Note: For more information on MIB Tools, see *Certification Guide*.

2. Right-click the SystemEDGE host (Host_systemEDGE) model and select Reconfiguration, Reconfigure Model.

The SystemEDGE host model is reconfigured as an ADES Host Manager.

More information:

[Upgrade the CA SystemEDGE Host Model \(If Necessary\)](#) (see page 26)

Duplicate Models Created After Discovery

Symptom:

After ADES Manager Discovery runs, I see duplicate models in the ADES Manager hierarchy for some of the hosts in my modeled environment.

Solution:

A host should be managed by a single ADES Host Manager. If a host is inadvertently managed by multiple ADES Host Managers residing in different landscapes, duplicate models are created. One host model is created for each landscape where a ADES Host Manager is managing the host.

To resolve duplicate models:

1. Search for the host in each landscape. If a host is present:
 - a. Use the Universal Host Table subview to unmanage the host in each ADES Host Manager in the landscape.
 - b. (optional) After modifying the UHT subview, reconfigure the corresponding ADES Host Manager device to expedite its unmanagement process.
2. Repeat step 1 for every ADES Host Manager across all landscapes except one.

More information:

[Host Management and Multiple ADES AIMs](#) (see page 18)

[Specify Hosts to Manage by ADES AIM](#) (see page 26)

Multiply Managed Alarms

Symptom:

I do not see duplicate hosts in my ADES Manager hierarchy, but I am getting an alarm on an Active Directory or Exchange Server host with the title "ACTIVE DIRECTORY AND EXCHANGE SERVER HOST MULTIPLY MANAGED".

Solution:

A host should be managed by a single ADES Host Manager. If a host is inadvertently managed by multiple ADES Host Managers residing in the same landscape, this alarm is generated.

To avoid multiply managed alarms:

1. Locate the landscape in which the host resides, and do the following:
 - a. Use the Universal Host Table subview to unmanage the host in each ADES Host Manager in the landscape.
 - b. (optional) After modifying the UHT subview, reconfigure the corresponding ADES Host Manager device to expedite its unmanagement process.
2. Repeat step 1 for every ADES Host Manager except for one.

The alarm automatically clears when the Active Directory or Exchange Server host is managed by a single ADES Host Manager.

More information:

[Host Management and Multiple ADES AIMs](#) (see page 18)

[Specify Hosts to Manage by ADES AIM](#) (see page 26)

Connections Do Not Appear in Topology

Symptom:

My Active Directory and Exchange Server hosts are not showing connections to other devices in the OneClick topology view.

Solution:

To produce the connections between your Active Directory and Exchange Server hosts and the rest of the modeled environment, any connecting devices must be modeled before the Active Directory and Exchange Server hosts are modeled. When discovering and modeling your environment, a standard CA Spectrum Discovery should be run first to model upstream routers and switches. Then, ADES Manager Discovery can run, creating models and connections for the Active Directory and Exchange Server components.

To create connections for managed hosts:

1. Verify that devices such as routers and switches that are upstream from your Active Directory and Exchange Server environment are modeled. If not, run a standard CA Spectrum Discovery to model these connecting devices.
2. If the connecting devices are modeled after your Active Directory and Exchange Server environment is modeled, run Discover Connections on each of the affected devices.

Note: For information on Discover Connections, see the *Modeling and Managing Your IT Infrastructure Administrator Guide*.

More information:

[Discover and Model Your Active Directory and Exchange Server Environment](#) (see page 23)

ADES Managed Hosts Container Not Created

Symptom:

I have modeled an ADES Host Manager, but I do not see a corresponding ADES Managed Hosts container being created for it.

Solution:

CA Spectrum ADES Manager requires ADES AIM r12.7 or later. Verify that ADES AIM r12.7 or later is running on the ADES Host Manager.

More information:

[System Requirements](#) (see page 8)

[Installing ADES Manager Components](#) (see page 21)

[Upgrade the CA SystemEDGE Host Model \(If Necessary\)](#) (see page 26)

Host Not in ADES Managed Hosts Container

Symptom:

My ADES Managed Hosts container was created but, when I look inside, an expected Active Directory or Exchange Server host is not there.

Solution:

Active Directory or Exchange Server hosts that were modeled prior to ADES Manager Discovery are not moved in the topology when brought into management by ADES Manager. To locate the expected host, look in other possible locations in the landscape for the model. In particular, if the Active Directory or Exchange Server host is a virtual machine, it is located in the physical host container.

More information:

[What is Modeled](#) (see page 15)

[Hosts Managed by Virtual Host Manager and ADES Manager](#) (see page 18)

[Topology View](#) (see page 35)

Unable to Update Attribute

Symptom:

I get the following error when I try to manage or unmanage an Active Directory or Exchange Server host in the Universal Host Table subview:

Unable to update attribute exchAdUniversalHostManagedByAgent. No response from the device.

Solution:

The ADES Manager Host must be modeled with a read/write community string. If not, you cannot update the model. To resolve this problem, change the community string of the ADES Host Manager to its read-write value. The SNMP Community String is located on the CA Spectrum Modeling Information subview for the ADES Host Manager model.

More information:

[Run CA Spectrum Discovery to Model the ADES Host Manager and Connecting Devices](#)
(see page 24)

Host Subview is Empty

Symptom:

A role-specific subview for my Active Directory or Exchange Server host does not contain any data.

Solution:

A role-specific subview contains data only when the host supports the respective role. Verify that the host supports the role whose data the subview is displaying. Subviews for unsupported roles are empty. For mailbox servers, also verify that the host supports the correct Exchange version, 2007 or 2010; the subview for the unsupported version is empty.

More information:

[Individual Host Subviews](#) (see page 40)

Changes in Environment Not Reflected in CA Spectrum

Symptom:

When I modify my Active Directory or Exchange Server environment by adding or removing a host, the change is not reflected in my modeled CA Spectrum environment.

Solution:

An ADES AIM Discovery must be run manually before the environment change is detected by the ADES AIM and subsequently modeled in CA Spectrum. To update your modeled environment in CA Spectrum, initiate the ADES AIM Discovery process manually, which will trigger ADES Manager Discovery and reflect any changes in CA Spectrum.

More information:

[Updating Your Managed Environment](#) (see page 46)

ADES Manager Updates are Slow

Symptom:

The data specific to the Active Directory and Exchange Server technologies is not updating as frequently as I expect it to.

Solution:

Data update delays in CA Spectrum ADES Manager may be due to ADES AIM performance issues. Performance can be affected by the number of hosts managed by the ADES AIM as well as the geographic proximity of the ADES AIM to the monitored environment. These factors can contribute to long poll times.

To improve performance by the ADES AIM:

1. Verify that the polling interval is set appropriately.
2. If the polling interval is set as expected, the ADES AIM may be overloaded or located too far from the managed hosts. Check that the recommended limits and configuration for the ADES AIM are adhered to.

Note: For information on load balancing and sizing guidelines for the ADES AIM, see the *CA Virtual Assurance for Infrastructure Managers Administration Guide*.

More information:

[Controlling Polling Intervals](#) (see page 45)

[Environment Management Considerations](#) (see page 14)

Glossary

Active Directory Domain Services (AD DS) server role

The *Active Directory Domain Services (AD DS) server role* stores directory data for all objects in your network and manages communication between users and domains, including authentication requests and directory searches.

ADES AIM Discovery

ADES AIM Discovery is the process performed by the ADES AIM to identify hosts in Active Directory and Exchange Server environments. ADES AIM Discovery uses the Global Catalogs to extract information based on configurations set by the user that specify domain name, management entity (Active Directory, Exchange Server, or both) and management mode (domain-based or host-based). Hosts identified by ADES AIM Discovery are made available to CA Spectrum for management.

ADES Host Manager

Active Directory and Exchange Server Host Manager (ADES Host Manager) is the CA Spectrum model that represents a host that contains the ADES AIM. Successful creation of this model indicates that all requisite intelligence to support ADES Manager has been installed on the host.

ADES Manager Discovery

ADES Manager Discovery is the modeling within CA Spectrum of Active Directory and Exchange Server hosts that are to be managed by ADES Manager. It also includes the modeling of any other required components for ADES Manager. ADES Manager Discovery obtains information about the hosts that are determined as available for management by ADES AIM Discovery.

application insight module (AIM)

The CA SystemEDGE agent provides a plug-in architecture through which it can load optional *application insight modules (AIMs)* when it initializes. AIMs are functional extensions to the SystemEDGE agent.

available host

An *available host* is an Active Directory or Exchange Server host that has been identified by ADES AIM Discovery based on user specifications and qualifies for management by CA Spectrum ADES Manager.

database availability group (DAG)

A *database availability group (DAG)* is a cluster of Exchange Mailbox servers used for continuous replication, providing failover at the database level. The databases on any of the DAG members can be replicated to the other DAG members. At any given time, the database is active on one DAG member only, while the databases on the other DAG members are passive. A passive database can then be activated in the event of failure. The DAG feature was introduced in Exchange 2010.

domain

A *domain* is an Active Directory container structure that contains a collection of objects that share a common set of policies, name, and security database. A domain is at the lowest level of the logical structure of an entire network and is identified by its domain name.

domain controller

A *domain controller* is a host that is running AD DS. There are typically multiple domain controllers that host Active Directory within a domain, and you can manage your network resources from any domain controller within your domain.

domain tree

A *domain tree* is an Active Directory container structure that contains a collection of one or more domains in a network.

domain-based management

Domain-based management is a configuration option in the ADES AIM where all newly-discovered, available hosts in the domain are automatically managed by default. Domain-based management is generally used with domains that are small enough to be managed by a single ADES AIM.

forest

A *forest* is an Active Directory container structure that contains a collection of Active Directory objects, their attributes, and attribute syntax. A forest is at the highest level of the logical structure. It is a collection of domain trees sharing a common global catalog, directory configuration, directory, schema and logical structure.

host-based management

Host-based management is a configuration option in the ADES AIM where all newly-discovered, available hosts in the domain are automatically not managed by default. Host-based management is generally used with domains that are large enough to be managed by multiple ADES AIMS.

Hub Transport server role

The Exchange Server *Hub Transport server role* handles email flow and routing. All messages are delivered through this role, regardless of whether they are being delivered locally or remotely.

Mailbox server role

The Exchange Server *Mailbox server role* provides email storage (including user mailboxes), advanced scheduling services, and supports public folders. Continuous replication technology provides a reliable failover mechanism in the event of failure. In Exchange 2007, continuous replication failover is at the server level; with Exchange 2010 and the introduction of database availability groups (DAGs) (see definition on page 66), failover is at the database level.

managed host

A *managed host* is an Active Directory or Exchange Server host that is managed by CA Spectrum ADES Manager, as reflected by the Managed Host Table. The ADES AIM polls all managed hosts for Active Directory and Exchange Server metrics. Management of a host can be controlled by using the Universal Host Table view in CA Spectrum.

Managed Host Table (MHT)

The *Managed Host Table (MHT)* contains all hosts that the ADES AIM is managing (polling for Active Directory and Exchange Server metrics). Whereas the Universal Host Table contains all hosts that *can* be managed by an AIM, the Managed Host Table contains those that are *actually* managed. The MHT table resides on the ADES AIM and is viewable in CA Spectrum. ADES Manager uses the MHT as its basis for creating, deleting, or updating Active Directory and Exchange Server host models.

management entity

Management entity is a configuration option in the ADES AIM on a per-domain basis that controls what technologies to monitor by the ADES AIM: Active Directory, Exchange Server, or both.

management mode

Management mode is a configuration option in the ADES AIM that controls monitoring of the Active Directory and Exchange Server environments on a per-domain basis. Domain-based monitoring automatically manages all newly-discovered Active Directory and Exchange Server hosts in the domain. Host-based monitoring automatically does not manage all newly-discovered Active Directory and Exchange Server hosts in the domain.

proxy management

Proxy management is the act of managing network devices using an alternate management source in place of or in addition to the device itself. For example, CA Spectrum can manage Active Directory or Exchange Server hosts by contacting them directly or through the ADES AIM.

server role

A *server role* is the primary duty that a server performs. Active Directory and Exchange Server use server roles to assign specific functions to specific hosts.

Universal Host Table (UHT)

The *Universal Host Table (UHT)* contains all hosts that are available for management by an ADES AIM. Using the Universal Host Table view in CA Spectrum, you can control which hosts are managed by CA Spectrum ADES Manager.

Index

A

- Active Directory • 8
 - Domain Services • 9
 - overview • 8
- ADES AIM • 8
 - configuration • 14, 20, 21, 37, 45, 46
 - discovery • 14, 20, 22, 23, 37, 47
 - overview • 11, 19, 52
 - polling • 21, 45
- ADES Host Manager model • 24, 29, 45
- ADES Managed Hosts container • 15, 29, 35, 49
 - container not created • 60
 - host not in container • 61
- ADES Manager
 - discovery • 14, 22, 27
 - features • 7
 - hierarchy • 32
 - installing • 21
 - overview • 7, 11
 - planning for • 13
 - searching • 42
 - solution architecture • 11
 - subviews • 36
 - system requirements • 8
 - topology • 35
 - viewing • 31
- ADES-events-filter.xml • 43
- alarms • 51
 - correlation • 54
 - fault isolation • 51, 54
 - multiply managed • 59
 - proxy management • 52
- attribute, unable to update • 61

C

- CA SystemEDGE • 8, 37
 - installing • 21
 - modeling • 24, 26
 - overview • 11
 - upgrade host model • 26
- connections • 49, 60
 - connections do not appear • 60
 - discover and model • 24
- contacting technical support • 3

- customer support, contacting • 3

D

- Data Availability Group (DAG) • 10, 37, 40
- deleting models • 49
- discovery • 22, 24, 46
 - ADES AIM Discovery • 14, 22, 23
 - ADES Manager Discovery • 14, 22, 27
 - connecting devices • 24
- domain • 9, 20, 32
- domain controller • 9, 40
- Domain Services • 8, 9, 11, 32, 37, 40, 42
- domain-based management • 20, 23, 46
- duplicate models • 58

E

- empireExchangeAdMIB • 11
- environment
 - maintaining • 45, 49
 - management considerations • 14, 18
 - modifying • 49
 - updating • 19, 46, 47, 49, 62
- event reports • 43
- Exchange Server • 8
 - overview • 10

F

- forest • 9, 32

G

- Global Catalog • 23, 46

H

- hibernation • 54
- hierarchy • 32
- host management • 26, 37
- host-based management • 20, 23, 46
- Hub Transport • 8, 10, 11, 32, 37, 40, 42

I

- ICMP • 16, 17
- installation • 21
- IP address • 17, 49

L

Locater searches • 42

M

MAC address • 17, 49

Mailbox • 8, 10, 11, 32, 37, 40, 42

maintenance • 54

Managed Host Table (MHT) • 26, 27, 37

management mode • 20, 23

MIB • 11

modeling • 15, 22

- deleting models • 49

- duplicate models • 58

- methods • 16

- model naming • 17

- models created • 24, 27, 29

P

performance • 63

polling • 21, 45

proxy management • 11, 52

R

Report Manager, event reports • 43

S

scenarios, fault isolation • 54

searches • 42

server roles

- Active Directory Domain Services • 9

- Exchange Server Hub Transport • 10

- Exchange Server Mailbox • 10

SNMP • 16, 17, 24

solution architecture • 11

subviews • 36

- empty • 62

- for ADES Host Manager • 36

- for individual hosts • 40

support, contacting • 3

system requirements • 8

T

technical support, contacting • 3

topology • 35, 49

- connections do not appear • 60

troubleshooting • 57

- ADES Managed Hosts container not created • 60

ADES Manager updates are slow • 63

changes in environment not reflected in CA

- Spectrum • 62

connections do not appear in topology • 60

duplicate models created after discovery • 58

host not in ADES Managed Hosts container • 61

host subview is empty • 62

multiply managed alarms • 59

unable to update attribute • 61

U

Universal Host Table • 26, 37

update environment • 19, 46, 47, 49, 62

V

Virtual Host Manager • 18, 35, 49