CHAPTER 1

Overview of the Cisco Active Directory Agent

The Cisco Active Directory Agent (AD Agent) is a component that runs on a Windows machine; monitors in real time a collection of Active Directory domain controller (DC) machines for authentication-related events that generally indicate user logins; learns, analyzes, and caches mappings of IP addresses and user identities in its database; and makes the latest mappings available to its client devices.

Client devices, such as the Cisco Adaptive Security Appliance (ASA) and the Cisco IronPort Web Security Appliance (WSA), interact with the AD Agent using the RADIUS protocol in order to obtain the latest set of IP-to-user-identity mappings, in any one of the following ways:

- On-Demand—The AD Agent can respond to an on-demand query from the client device for a specific mapping.
- Bulk Download—The AD Agent can respond to a request from the client device for the entire set of mappings currently in its cache.

For both the on-demand and bulk-download methods, the request from the client device can be specially tagged to indicate that it also includes a request for notification regarding any subsequent updates.

For example, when a client device requests a basic on-demand query, the AD Agent will respond with the specific mapping that might have been found in its cache, and does not send any further updates about that mapping. On the other hand, if the on-demand query also includes a request for notification, the initial response from the AD Agent will be the same as before and if, at a later point in time, that specific mapping undergoes a change, then the AD Agent will proactively notify the requesting client device (as well as any other client devices that have registered for notification) about the change in that specific mapping.

Similarly, when a client device requests a basic bulk download, the AD Agent will transfer a snapshot of the session data containing all of the mappings currently found in its cache, and does not send any further updates. On the other hand, if the request is to register for replication, then the initial response from the AD Agent will be the same as before, and if, at a later point in time, the set of mappings undergoes any sort of change (new mappings added or certain mappings changed and so on), then the AD Agent will proactively notify the requesting client device (as well as any other client devices that have registered for replication) about these changes, relative to the snapshot that was previously sent.

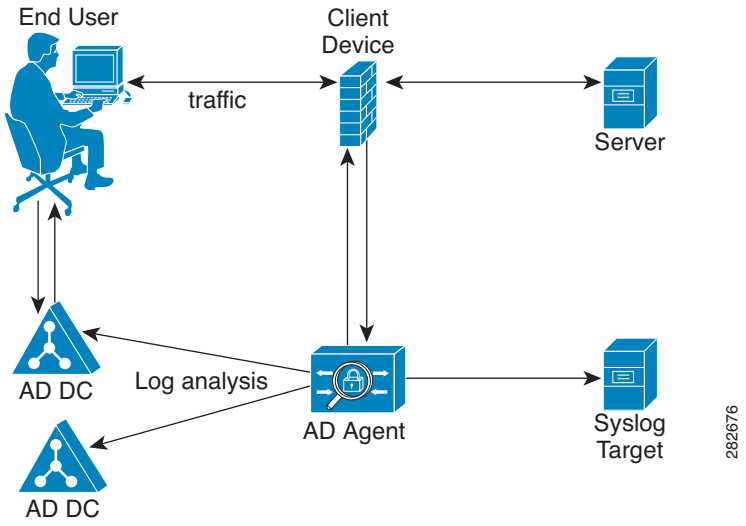
The IP-to-user-identity mappings that are discovered, maintained, and provided by the AD Agent can include not only IPv4 addresses, but also IPv6 addresses.

The AD Agent can send logs to one or more syslog servers.

The AD Agent will continue to function if any of the AD domain controllers or the client devices have failed. It will obtain information from other domain controllers. However, there is no failover for the AD Agent. The Cisco AD Agent internally contains a “watchdog” functionality that continuously monitors the Windows processes internal to the AD Agent, automatically restarting them if it detects that they have crashed.

Figure 1-1 illustrates the role of AD Agent in an example scenario.

Figure 1-1 AD Agent Used in a Solution



In this example, a user logs in from a computer and generates web traffic by requesting access to a server. The client device intercepts the web traffic and sends a RADIUS request to the AD Agent asking for the user who logged into the computer. The AD Agent, which has been maintaining the latest set of IP-to-user-identity mappings, sends the user information to the client device. The client device uses the the user identity information to determine whether or not to grant access to the end user.

The AD Agent interacts with the following components in a network:

- Client Devices
- Active Directory Domain Controller Machines
- Syslog Servers

Note AD Agent can support up to 100 client devices and 30 domain controller machines, and can internally cache up to 64,000 IP-to-user-identity mappings.

Client Devices

Client devices are responsible for actively retrieving (and/or passively receiving) the latest IP-to-user-identity mappings from the AD Agent.

A client device can retrieve these mappings from the AD Agent in the following ways:

- Query the AD Agent for each new IP
- Maintain a local copy of the entire user identity and IP address database

In addition to receiving the latest set of IP-to-user-identity mappings from the AD Agent, a client device can also send updates of mappings that it learns through other mechanisms to the AD Agent. For example, the ASA device updates the AD Agent with:

- new mappings learned during web authentication fallback (for IP addresses that the AD Agent could not map to user-identity)
- new mappings learned from VPN sessions
- mapping-removals associated with logoffs or disconnects learned from VPN/Cut-Through Proxy or through NetBIOS probing or MAC checking

These updates are sent as RADIUS Accounting-Request messages.

Note For information about configuring ASA devices to send notifications to the AD Agent, refer to the ASA end-user documentation.

Active Directory Domain Controller Machines

Though Active Directory is part of this solution, it is managed by Active Directory administrators. The reliability and accuracy of the data depends on the Active Directory domain controller's data. The AD Agent monitors, learns, and reads events from Active Directory domain controllers.

The AD Agent only monitors authentication events in which Kerberos is used to authenticate the user.

The events that the AD Agent monitors are usually triggered by logins, but can also be triggered by other activities such as:

- The use of the "runas" Windows command
- The use of the "net user" Windows command

The AD Agent is able to monitor up to 30 Active Directory domain controller machines, each running one of the following supported versions of Windows Server:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

Note Windows Server 2003 R2 is not supported.

It is important to verify that each and every Active Directory domain controller machine running Windows Server 2008 or Windows Server 2008 R2 has the appropriate Microsoft hotfixes installed, as detailed in "Active Directory Requirements" section on page 2-5. You must apply the hotfixes regardless of whether the AD Agent is installed directly on the domain controller machine, or monitoring the domain controller machine remotely.

Similarly, it is important to verify that the Audit Policy on each Active Directory domain controller machine allows for auditing of successful authentication attempts, as detailed in "Configuring AD Agent to Obtain Information from AD Domain Controllers" section on page 2-9.

The AD Agent can monitor domains that have a trust relationship with the domain to which the AD Agent machine is joined. The AD Agent supports the following Active Directory structures:

- Single forest, single domain
- Single forest, multiple domains
- Multiple forests

Syslog Servers

The AD Agent can forward logs containing administrative and troubleshooting information to one or more syslog servers. The contents of these logs are identical to that of the customer logs that are locally available on the AD Agent machine, in the C:\IBF\radiusServer\runtime\logs\localStore\ directory. The syslog mechanism allows this information to be distributed remotely, to any target machine running a syslog server and capable of receiving syslog messages.