Release Notes for Cisco Context Directory Agent, Release 1.0

Revised: February 10, 2014, OL-26298-01

Contents

These release notes describe the role of the Cisco Context Directory Agent in an identity-based solution, its limitations and restrictions (caveats), and related information. These release notes supplement the Cisco Context Directory Agent documentation that is included with the software, and cover the following topics:

Introduction

Unlike traditional security mechanisms, Cisco's security gateways such as ASA-CX, WSA, ASA and the Cloud-based CWS service, provide security to networks based on the context of the entity requiring access. While traditional network and content security gateways used to rely on the entity's IP address only to determine if it should pass the security gateway or not, today's Cisco products allow to take into account much additional information, and make decisions based on the complete context of the network entity, such as the user currently using it, what operating system it uses, what location is it in, and so on.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Security administrators write policies using reference to this context, and when network traffic hits the security gateway, it needs to check what is the context of the originating (and sometimes, also the destined) IP address.

Cisco Context Directory Agent (CDA) is a mechanism that maps IP addresses to usernames in order to allow security gateways to understand which user is using which IP address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to).

CDA runs on a Cisco Linux 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.

Starting with patch 2, CDA can now receive information from Cisco Identity Services Engine (ISE) and Cisco Secure Access Control Server (ACS) in order to map users that do not directly login into Active Directory. CDA acts as a syslog server, receiving syslog messages from ISE and ACS, and populates the mapping table using network login information derived from ISE and ACS.

CDA supports ISE 1.1.x and 1.2 and ACS 5.3, and 5.4 only.

Client devices, such as the Cisco Adaptive Security Appliance (ASA) and the Cisco IronPort Web Security Appliance (WSA), interact with the Cisco CDA 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 Cisco CDA can respond to an on-demand query from the client device for a specific mapping.
- **Full Download**—The Cisco CDA can respond to a request from the client device for the entire set of mappings currently in its cache.

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

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

Integration with ISE/ACS allows consumer devices such as ASA-CX and WSA to make security decisions for a large portion of network endpoints, including those that are not domain members. CDA passes the information to the consumer devices in the same format whether the user/domain information was received from a Windows domain controller event log or through integration with ISE/ACS.

Note WSA currently supports deriving user information only about authentications performed by ISE/ACS against an Active Directory domain. WSA does not provide permission to users authenticated against other databases within ISE such as the local user database.

CDA can support up to 80 domain controller machines, and can internally cache up to 64,000 IP-to-user-identity mappings. It supports up to 100 Identity consumer devices. It processes 1000 IP-to-user-identity mappings per second (input and output).

Context Directory Agent Requirements

See the *Installation and Configuration Guide for Context Directory Agent, Release 1.0* for information on the Context Directory Agent Requirements.

Context Directory Agent License Information

See the *Open Source Used in Cisco Active Directory Agent 1.0* document for the Context Directory Agent licence information,

Important Notes

For the Cisco Context Directory Agent to function properly in an identity-based solution, you must ensure that:

- Hardware requirements are met. See http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda_install.html#wp1053078 for more information.
- Firewall exceptions, if required, are configured on the AD Agent machine and the AD domain controller machines. See http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda_install.html#wp1053513 for more information.
- Active Directory requirements are met. See http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda_install.html#wp1053829 for more information.
- A supported version of Cisco ISE/ACS, if required, is installed on a machine in your deployment.
- Network and firewalls between ISE/ACS and CDA allow syslog traffic (either UDP or TCP, as configured on both ISE/ACS and CDA) to flow from ISE/ACS to CDA. This is applicable only if you have installed Cisco CDA 1.0, Patch 2.

Installing the Context Directory Agent Software

See the *Installation and Configuration Guide for Context Directory Agent, Release 1.0* for information on how to install and configure the Active Directory Agent.

Open Caveats in Cisco Context Directory Agent Release 1.0

Table 1 Open Caveats in Cisco Context zDirectory Agent Release 1.0

Caveat	Description

CSCty64187	**Symptom** Attempting to create a log backup file results in the following error message:
	`% ERROR: Bad hashed password.`
	Conditions This issue occurs when you attempt to create a log backup file with a hashed password. For example:
	`backup-logs logs repository local password hash 1q2w3e4r`
	Workaround Use a text (non hashed) password.

CSCtx13593	**Symptom** Cannot install Cisco CDA application via network interfaces 2 or 3. **Conditions** This issue occurs if the connectivity to the repository hosting the Cisco CDA application bundle is via network interfaces 2 or 3 of the machine. Fetching the file fails with a timeout. **Workaround** Install the Cisco CDA application via network interfaces 0 or 1.
CSCtx13800	**Symptom** In Cisco CDA CLI, you cannot use % within a password. **Conditions** This issue occurs when you attempt to set or change a password that contains the % character. **Workaround** Use a password without %.
CSCtz47312	**Symptom** The Cisco CDA GUI may not reflect changes made to the administrator list in the other concurrent GUI sessions when clicking the Refresh icon. **Conditions** When the administrator list is open in one Cisco CDA GUI session, and some change is made to the administrator list in another concurrent GUI session of the same Cisco CDA, clicking the refresh icon in the Cisco CDA GUI does not reflect those change in the administrator list. **Workaround** Use the browser refresh button to refresh the display, or go to the Home page (Cisco CDA Dashboard) and then go back to the system administrators page.

Table 1 Open Caveats in Cisco Context zDirectory Agent Release 1.0 (continued)

Caveat	Description
CSCtw78043	**Symptom** DC status in the Cisco CDA Dashboard might show as down during the first few minutes after Cisco CDA is connected. **Conditions** When cisco CDA connects to the Active Directory DC, it retrieves login history from the DC. While history is being retrieved, the DC status might show as down. This may last for several minutes, depending on history size and system load. **Workaround** The issue is transient and the DC status is updated as soon as history retrieval is complete. Click the refresh icon to update the display. Hence, the workaround provided here is not mandatory. It is possible to avoid this issue by setting the following registry keys on the domain controller: • HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}\InProcServer32\ThreadingModel Change the default value “Apartment” to “Free”. On 64 bit Domain Controllers, the following key should also be similarly changed: • HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}\InProcServer32\ThreadingModel Restart the WMI service on the DC for the changes to take effect.
CSCtx67710	**Symptom** Cisco CDA does not receive identity mappings from an Active Directory 2008R2 DC, even though the DC shows as connected, and the user login events show up in the DC security audit log. **Conditions** This issue might occur under rare conditions. Clearing logs on the DC multiple times is one way to trigger the issue. **Workaround** Restart the WMI service on the DC to restore normal operation of the system. A Hotfix is available from Microsoft to address the root cause of this defect. The WMI process stops sending events to WMI clients from a Windows 7-based or Windows Server 2008 R2-based server, http://support.microsoft.com/kb/2705357

Resolved Caveats in Cisco Context Directory Agent Release 1.0 Patch 1

The Cisco Context Directory Agent 1.0, Patch 1 now supports Windows Active Directory, version 2012.

Table 2 lists the caveats that are resolved as part of this patch.

Table 2 Resolved Caveats in Cisco Context Directory Agent Release 1.0 Patch 1

Caveat	Description
CSCud69408	CDA needs to support user with non-admin privileges when connecting to Windows Domain Controller. Refer to the *Installation and Configuration Guide for Context Directory Agent, Release 1.0* for more information.
CSCud69418	CDA to support NTLMv2 for the connection with Windows Domain Controller.
CSCud69438	Log records are not displayed in the log table after CDA is installed on VMware.
CSCtz47312	Refresh in Administrators screen does not work.
CSCtz21543	Tool tips on mouse over for Green/Red status icons.

Resolved Caveats in Cisco Context Directory Agent Release 1.0 Patch 2

Table 3 Resolved Caveats in Cisco Context Directory Agent Release 1.0 Patch 2

Caveat	Description
CSCuj16952	CDA bundle compressed zip greater than 4GB fails
CSCue46013	Potential to gain shell with root privileges
CSCug29400	Potential to run arbitrary commands as root from CLI
CSCUI91348	CDA GUI is not usable in Chrome version 30 and Firefox 25
CSCUG77225	Populates mapping tables with non existent usernames
CSCuj16936	Certificate is invalid after one year, CDA self signed certificate expires after 1 year
CSCuj16989	Creating a bundle takes logs but not database itself
CSCuf93569	CDA establishes connection to remote site
CSCui21212	Mappings table is not populated in IE 7,8,9
CSCuj39335	Upgrade apache commons version
CSCuj38832	While expanding one of the fields, the table disappears
CSCuj41148	Please fix how CDA presents installed patches from GUI
CSCuj45367	GUI is vulnerable to XSS via User Supplied Input
CSCuj45353	Odd number of single quotes (‘) makes AD server list invisible

Table 3 Resolved Caveats in Cisco Context Directory Agent Release 1.0 Patch 2

Caveat	Description
CSCuj63255	TCP vulnerability CVE-2011-3188
CSCuj63264	TCP vulnerability
CSCul80311	Help button is missing
CSCul41560	Client side filtering of various fields in the GUI is easily bypassed
CSCum28731	Show secret is not working with IE / FF
CSCuj45358	XSS vulnerability in CDA Mappings page
CSCuj45347	Proper role check not present for admin pages, allows priv. escalation

Open Caveats in Cisco Context Directory Agent Release 1.0, Patch 2

s

Table 4 Open Caveats in Cisco Context Directory Agent Release 1.0, Patch 2

Caveat	Description
CSCum52734	**Symptom** You cannot use SFTP protocol type when configuring repository via CLI on Cisco CDA 1.0, patch 2 due to security update applied in patch 2. **Conditions** This issue occurs when you try to configure repository using the sftp: server protocol. **Workaround** Use other available repositories, such as FTP, NFS,TFTP, DISK.

Documentation Updates

Table 5 Updates to Release Notes for Cisco Context Directory Agent, Release 1.0

Date	Description
Jan 2014	Added/ updated the following section: • "Introduction" section on page 1 • "Important Notes" section on page 3 • "Resolved Caveats in Cisco Context Directory Agent Release 1.0 Patch 2" section on page 6 • "Open Caveats in Cisco Context Directory Agent Release 1.0, Patch 2" section on page 7
Feb 2013	Added "Resolved Caveats in Cisco Context Directory Agent Release 1.0 Patch 1" section on page 6
June 2012	Updated CSCtx67710
June 2012	Cisco Context Directory Agent, Release 1.0

Related Documentation

Release-Specific Documentation

Table 6 lists the product documentation available for the AD Agent, Release 1.0, patch 1.

Table 6 Product Documentation for Cisco Context Directory Agent, 1.0, patch 1

Document Title	Location
Installation and Configuration Guide for Cisco Context Directory Agent, Release 1.0	http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html
Release Notes for Context Directory Agent, Release 1.0	http://www.cisco.com/en/US/docs/security/ibf/cda_10/release_notes/cda10_rn.html
Open Source Licenses used in Context Directory Agent, Release 1.0	http://www.cisco.com/en/US/docs/security/ibf/cda_10/open_source_doc/open_source.pdf

Other Related Documentation

Links to Adaptive Security Appliance (ASA) 5500 Series Release 8.4.2 documentation and Ironport Web Security Appliance (WSA) documentation are available on Cisco.com at the following locations:

- Cisco ASA 5500 Series Adaptive Security Appliances Page

  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
- Cisco Ironport Security Management Appliances Page

  http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.