Cisco Context Directory Agent 版本说明（1.0 版）

修订日期：2016 年 8 月 22 日，OL-26298-01

目录

本版本说明介绍 Cisco Context Directory Agent 在基于身份的解决方案中的角色、该软件的局限性和限制（注意事项），以及各种相关信息。本版本说明是对软件随附的 Cisco Context Directory Agent 文档的补充。本文档包含以下主题：

美洲总部：
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

简介

与传统安全机制不同，思科安全网关（如 ASA-CX、WSA、ASA 和基于云的 CWS 服务）能够根据请求访问的实体的上下文信息，来保护网络安全。传统网络和内容安全网关通常仅依靠实体的 IP 地址来确定是否允许该实体通过安全网关。但是现在，思科产品却可以将更多信息考虑在内，并根据网络实体的完整上下文信息做出决策，例如：该实体正在被用户使用、该实体所使用的操作系统，该实体所在的位置等等。安全管理员可以创建引用这些上下文信息的策略，以便在网络流量进入安全网关时，检查源 IP 地址的上下文信息（有时也可以检查目标 IP 地址的上下文信息）。

Cisco Context Directory Agent (CDA) 是将 IP 地址映射到用户名的机制，可使安全网关了解用户在网络中使用的 IP 地址，以便安全网关根据这些用户（或用户所在的组）做出决策。

CDA 在 Cisco Linux 计算机上运行。它能够实时监控一组 Active Directory 域控制器 (DC) 计算机，捕捉通常可表明用户登录活动的身份验证相关事件。CDA 还能学习和分析 IP 地址与用户身份的映射关系，并将这些信息缓存到其数据库中。不仅如此，CDA 还能将向客户端设备提供最新的映射关系。

从 Patch 2 开始，CDA 能够接收来自思科身份服务引擎 (ISE) 和思科安全访问控制服务器 (ACS) 的信息，以便映射未直接登录到 Active Directory 的用户。CDA 可作为系统日志服务器，用于接收来自 ISE 和 ACS 的系统日志消息，并使用来自 ISE 和 ACS 的网络登录信息填写映射表。

CDA 仅支持 ISE 1.1.x、1.2、1.3 和 2.0，以及 ACS 5.3、5.4、5.6、5.7 和 5.8。

为了获得最新的 IP 与用户身份映射，客户端设备（如思科适应安全设备 [ASA] 和 Cisco IronPort 网络安全设备 [WSA]）会使用 RADIUS 协议，通过以下方式与思科 CDA 进行交互：

- **按需**：思科 CDA 可以响应客户端设备对特定映射的单次按需查询。
- **完整下载**：思科 CDA 可以响应客户端设备对缓存中当前保存的全部映射的查询请求。

CDA 可与网络中的以下组件交互：

- 客户端设备
- Active Directory 域控制器计算机
- 系统日志服务器/客户端

通过与 ISE/ACS 集成，CDA 可以帮助 ASA-CX 和 WSA 等消费类设备对大部分网络端点（包括非域成员设备）做出安全决策。无论消费类设备是通过 Windows 域控制器事件日志接收用户/域信息，还是通过集成 ISE/ACS 来接收用户/域信息，CDA 都会以相同的格式将信息传送给消费类设备。

CDA 可最多支持 80 台域控制器计算机，并在内部缓存最多 64000 个 IP 与用户身份映射。它最多支持 100 台具有独立身份的消费类设备，每秒可处理最多 1000 次 IP 与用户身份映射（输入和输出）。

Context Directory Agent 的要求

如需详细了解 Context Directory Agent 的要求，请参阅 *Context Directory Agent 版本 1.0 安装和配置指南*。

Context Directory Agent 许可证信息

有关 Context Directory Agent 许可证的详细信息，请参阅 *Cisco Active Directory Agent 1.0 中使用的开源许可证*。

重要说明

为了确保 Cisco Context Directory Agent 在基于身份的解决方案中正常运行，您必须确保做到以下几点：

- 满足硬件要求。有关详细信息，请参阅 http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda_install.html#wp1053078。
- 必要时，为网络和 AD 域控制器计算机配置防火墙例外。有关详细信息，请参阅 http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda_install.html#wp1053513。
- 满足 Active Directory 要求。有关详细信息，请参阅 http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda_install.html#wp1053829。
- 必要时，在您部署的机器上安装受支持的思科 ISE/ACS 版本。
- ISE/ACS 和 CDA 之间的网络和防火墙应允许系统日志流量（可以是在 ISE/ACS 和 CDA 上配置的 UDP 或 TCP 流量）从 ISE/ACS 流向 CDA。此要求仅适用于已安装思科 CDA 1.0 Patch 2 或更高版本的用户。

Context Directory Agent 软件的安装

有关如何安装和配置 Active Directory Agent 的详细信息，请参阅 *Context Directory Agent 版本 1.0 安装和配置指南*。

Cisco Context Directory Agent 版本 1.0 中未解决的注意事项

表 1　Cisco Context Directory Agent 版本 1.0 中未解决的注意事项

注意事项	说明

CSCty64187	**症状**　在尝试创建日志备份文件时，会导致出现以下错误消息：
	`% ERROR: Bad hashed password.`
	条件　如果尝试使用散列密码创建日志备份文件，则会出现此问题。例如：
	`pmbu-ibf-pip10/admin# backup-logs aaa repository nfs password hash $1$Hzq51M3/$plfaaOB0PyW6Ia0UStvfo/`
	`% ERROR: Bad hashed password.`
	解决方法　使用文本密码，而不要使用散列明文密码。

CSCtx13593	**症状**　无法通过网络接口 2 或 3 安装思科 CDA 应用。 **条件**　如果通过计算机的网络接口 2 或 3 连接托管思科 CDA 应用捆绑包的存储库，则会出现此问题。获取文件的操作会因为超时而失败。 **解决方法**　通过网络接口 0 或 1 安装思科 CDA 应用。
CSCtx13800	**症状**　在思科 CDA CLI 中，不能使用包含 % 字符的密码。 **条件**　如果尝试在设置或更改密码时使用 % 字符，则会出现此问题。 **解决方法**　使用不含 % 字符的密码。
CSCtz47312	**症状**　点击刷新图标时，思科 CDA GUI 可能不会反映出在其他并发 GUI 会话中对管理员列表所做的更改。 **条件**　如果在一个思科 CDA GUI 会话中打开管理员列表，而在此期间，同一思科 CDA 上的另一个并发 GUI 会话对该管理员列表进行了更改，那么在该思科 CDA GUI 中点击刷新图标不会体现出另一个 GUI 会话中对管理员列表所做的更改。 **解决方法**　使用浏览器的刷新按钮刷新显示内容，或者转到思科 CDA 控制面板“主页”，然后再返回系统管理员页面。

表 1　Cisco Context Directory Agent 版本 1.0 中未解决的注意事项（续）

注意事项	说明
CSCtw78043	**症状**　在连接思科 CDA 后的前几分钟内，思科 CDA 控制面板的 DC 状态可能会显示为关闭。 **条件**　CDA 在连接到 Active Directory DC 后，会检索 DC 中的登录历史记录。在检索历史记录期间， DC 状态可能会显示为关闭。这可能持续几分钟时间，具体取决于历史记录的数量和系统负载。 **解决方法**　历史记录检索完成后，DC 状态会相应更新，此问题也会随之消失。点击刷新图标可更新显示内容。因此，下述解决方法可以不必执行。 通过设置域控制器的以下注册表项，可以避免此问题： • HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}\InProcServer32\ThreadingModel 将默认值从 “套件” (Apartment) 改为 “自由” (Free)。 在 64 位域控制器中，也需要对以下注册表项执行相似的更改： • HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}\InProcServer32\ThreadingModel 重启 DC 上的 WMI 服务，使更改生效。
CSCtx67710	**症状**　虽然 Active Directory 2008R2 DC 显示为已连接，且 DC 安全审核日志中也显示出用户登录事件，但思科 CDA 接收不到来自 DC 的身份映射。 **条件**　此问题只会在极少数情况下发生。例如，多次清除 DC 上的日志便有可能触发此问题。 **解决方法**　重启 DC 上的 WMI 服务，可使系统恢复正常。 安装 Microsoft 修补程序可从根本上解决此问题。此修补程序位于 http://support.microsoft.com/kb/2705357，可使 WMI 进程停止从运行 Windows 7 或 Windows 2008 R2 的服务器向 WMI 客户端发送事件。

Cisco Context Directory Agent 版本 1.0 (Patch 1) 中已解决的注意事项

Cisco Context Directory Agent 1.0 Patch 1 现支持 Windows Active Directory 2012 版。

表 2 列出了 Patch 1 中已解决的注意事项。

表 2　Cisco Context Directory Agent 版本 1.0 (Patch 1) 中已解决的注意事项

注意事项	说明
CSCud69408	在连接到 Windows 域控制器时，CDA 需要为具有非管理员权限的用户提供支持。有关详细信息，请参阅 *Context Directory Agent 版本 1.0 安装和配置指南*。
CSCud69418	对于使用 Windows 域控制器的连接，CDA 要能支持 NTLMv2。
CSCud69438	当 CDA 安装在 VMware 环境中时，日志表中不显示日志记录。
CSCtz47312	在管理员屏幕中，刷新操作无效。
CSCtz21543	将鼠标悬停在绿色/红色状态图标上，会显示工具提示。

Cisco Context Directory Agent 版本 1.0 (Patch 2) 中未解决的注意事项

表 3　Cisco Context Directory Agent 版本 1.0 (Patch 2) 中未解决的注意事项

注意事项	说明
CSCum52734	**症状** 由于思科 CDA 1.0 Patch 2 中应用的安全更新，在 CDA 1.0 Patch 2 中通过 CLI 配置存储库时无法使用 SFTP 协议类型。 **条件** 如果使用 SFTP 服务器协议配置存储库，则会出现此问题。 **解决方法** 使用 FTP、NFS、TFTP 和 DISK 等其他可用存储库。

Cisco Context Directory Agent 版本 1.0 (Patch 2) 中已解决的注意事项

表 4　Cisco Context Directory Agent 版本 1.0 (Patch 2) 中已解决的注意事项

注意事项	说明
CSCuj16952	将 CDA 捆绑包压缩为大于 4GB zip 文件会失败
CSCue46013	有可能通过根权限获得 Shell 访问权限
CSCug29400	有可能以根用户的名义通过 CLI 运行任意命令
CSCUI91348	CDA GUI 在 Chrome 版本 30 和 Firefox 25 中无法使用
CSCUG77225	使用不存在的用户名填充映射表
CSCuj16936	证书在一年后失效，CDA 自签名证书在一年后到期
CSCuj16989	使用日志而非数据库创建捆绑包
CSCuf93569	CDA 与远程站点建立连接
CSCui21212	在 IE 7、8、9 中，CDA 不填充映射表
CSCuj39335	升级 Apache Commons 版本
CSCuj38832	展开表格中的一个字段时，表格消失
CSCuj41148	修复了 CDA 在 GUI 中显示已安装补丁的方式
CSCuj45367	GUI 很容易受到通过用户输入发起的 XSS 攻击
CSCuj45353	单引号 (‘) 数量为奇数会导致 AD 服务器列表不可见
CSCuj63255	TCP 漏洞 CVE-2011-3188
CSCuj63264	TCP 漏洞
CSCul80311	“帮助”(Help) 按钮缺失
CSCul41560	在 GUI 中，客户端对各种字段的筛选操作很容易被忽略
CSCum28731	在 IE/FF 中，显示密码功能无效
CSCuj45358	CDA 映射页面存在 XSS 漏洞
CSCuj45347	对于管理员页面，没有正确的角色检查机制，可能导致权限权限

Cisco Context Directory Agent 版本 1.0 (Patch 3) 中已解决的注意事项

表 5　Cisco Context Directory Agent 版本 1.0 (Patch 3) 中已解决的注意事项

注意事项	说明
CSCul00096	磁盘已满问题
CSCuo41459	如果域中启用了至少一个 DC，则向消费类设备报告的域状态为“启用”
CSCum52734	支持 SFTP 存储库
CSCun10631	Windows Server 2012 R2 对 CDA 的支持
CSCuo01498	只能获取成功操作的历史记录

Cisco Context Directory Agent 版本 1.0 (Patch 4) 中已解决的注意事项

表 6　Cisco Context Directory Agent 版本 1.0 (Patch 4) 中已解决的注意事项

注意事项	说明
CSCur84288	CVE-2014-4263 Diffie-Hellman 公共密钥验证不充分
CSCuo61907	commons-fileupload 升级到版本 1.3.1
CSCur36448	CDA 不支持在用户名中使用美元符号 ($)（非末尾）
CSCum30446	CDA 用户登录有效期：将数值范围增加到最少 72 小时
CSCuq35289	不支持使用在用户名中使用撇号
CSCur56397	SSLv3 POODLE 漏洞
CSCur56385	Bash 漏洞修复 (Shellshock)

Cisco Context Directory Agent 版本 1.0 (Patch 5) 中已解决的注意事项

表 7　Cisco Context Directory Agent 版本 1.0 (Patch 5) 中已解决的注意事项

注意事项	说明
CSCut61989	如果 WSA 设备发送多个并行请求，CDA 的响应会出现延迟。
CSCuw13663	如果域控制器在配置的时间段内未使用所需的数据做出响应，CDA 会丢弃域控制器发出的请求。

文档更新

表 8　Cisco Context Directory Agent 版本说明（1.0 版）的更新历史

日期	描述
2015 年 10 月	添加了 “Cisco Context Directory Agent 版本 1.0 (Patch 5) 中已解决的注意事项” 部分（第 8 页）
2014 年 12 月	添加了 “Cisco Context Directory Agent 版本 1.0 (Patch 4) 中已解决的注意事项” 部分（第 8 页）
2014 年 7 月	添加了 “Cisco Context Directory Agent 版本 1.0 (Patch 3) 中已解决的注意事项” 部分（第 8 页）
2014 年 1 月	添加/更新了以下部分： • “简介” 部分（第 2 页） • “重要说明” 部分（第 3 页） • “Cisco Context Directory Agent 版本 1.0 (Patch 2) 中已解决的注意事项” 部分（第 7 页） • “Cisco Context Directory Agent 版本 1.0 (Patch 2) 中未解决的注意事项” 部分（第 6 页）
2013 年 2 月	添加了 “Cisco Context Directory Agent 版本 1.0 (Patch 1) 中已解决的注意事项” 部分（第 6 页）
2012 年 6 月	更新了 CSCtx67710
2012 年 6 月	Cisco Context Directory Agent 版本 1.0 发布

相关文档

版本特定文档

表 9 列出与 CDA 版本 1.0 相关的产品文档。

表 9　Cisco Context Directory Agent 1.0 的相关产品文档

文档标题	位置
Cisco Context Directory Agent 版本 1.0 安装和配置指南	http://www.cisco.com/en/US/docs/security/ibf/cda_10/Install_Config_guide/cda10.html
Context Directory Agent 版本 1.0 版本说明	http://www.cisco.com/en/US/docs/security/ibf/cda_10/release_notes/cda10_rn.html
Context Directory Agent 版本 1.0 中使用的开源许可证	http://www.cisco.com/en/US/docs/security/ibf/cda_10/open_source_doc/open_source.pdf

其他相关文档

自适应安全设备 (ASA) 5500 系列版本 8.4.2 文档和 Ironport 网络安全设备 (WSA) 文档的链接可在 Cisco.com 的以下位置找到：

- 思科 ASA 5500 系列自适应安全设备页面
  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html
- Cisco IronPort 安全管理设备页面
  http://www.cisco.com/en/US/products/ps10155/tsd_products_support_series_home.html

获取文档和提交服务请求

有关如何获取文档、提交服务请求和收集更多信息的详情，请参阅每月的*思科产品文档更新*（其中会列出所有最新版及修订版思科技术文档），网址为：

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

通过 RSS 源的方式订阅*思科产品文档更新*，相关内容将通过阅读器应用直接发送至您的桌面。RSS 源是一项免费服务，思科目前支持 RSS 2.0 版本。

本文档需结合“相关文档”一节中列出的文档共同使用。