CAMS 1.20-3100版本使用指导书

王雪梅　2006-02-23 发表

CAMS 1.20-3100版本使用指导书

关键词：CAMS EAD 新特性 升级

摘　要：本文详细描述了CAMS 1.20-3100版本的新增特性、遗留问题、规避措施和版本升级操作方法。

缩略语：

缩略语	英文全名	中文解释
表 1 CAMS	表 2 Comprehensive Access Management Server	表 3 综合访问管理服务器
表 4 EAD	表 5 Endpoint Admission Defense	表 6 端点准入防御

目 录

2 版本介绍

2.1 版本号

外部版本号：CAMS 1.20-3100
内部版本号：CAMS V100R002B03D100

上一发布版本外部版本号：CAMS 1.20-0390
上一发布版本内部版本号：CAMS V100R002B03D090

2.2 版本发布原因

本版本发布的原因是实现以下用户需求（与CAMS 1.20-0390版本相比）：

n　　EAD支持与国外主流防病毒软件的安全协同防御

EAD增加了与Symantec、TrendMicro、McAfee等国外主流防病毒软件的安全协同防御功能，可以检查以上防病毒软件是否运行正常，病毒库版本和扫描引擎版本是否合格。

注意：EAD与以上防病毒软件的协同防御是一种弱联动方式，不支持可控的认证时病毒查杀、自动升级、策略部署等协同功能。

n　　EAD支持对在线用户的桌面安全检查

EAD支持对在线用户的操作系统进行即时监控。管理员可以在CAMS管理台中对指定用户进行操作系统版本、进程列表、服务列表、共享目录列表、分区列表、屏保密码等信息进行即时检查。

n　　EAD支持对软件黑名单/白名单的界面定制

管理员可以在CAMS管理台进行软件黑名单/白名单等受控软件的界面定制。受控软件的定义包括软件名称和进程名称。

n　　CAMS支持基于用户的QoS Profile部署

QoS Profile是Quidway S3900/5600系列交换机对用户或业务的QoS进行控制的流控参数，可以通过Quidview网管平台进行配置和部署。

管理员可以在CAMS管理台中通过对服务的QoS属性的配置指定某种接入服务的QoS Profile，并通过服务与用户的关联动态控制用户接入网络时的流控策略。

管理员在配置服务的QoS属性时，可以手工输入已在交换机中设定的QoS Profile名称，也可以选择CAMS直接从Quidview中读取的QoS Profile配置。

注意：基于用户的QoS Profile部署只能与Quidway S3900/5600系列交换机配合使用。

n　　CAMS 可用性和易用性增强

l　　本版本在可用性和易用性上得到增强，具体的优化特性包括：

?　增加强制销户模式，即：在销户时如果选择强制销户模式，则将在线用户强制下线或删除后强制销户；

?　提供充负值的功能，并限制只有Admin以及具有“退费”权限的操作员可以进行此项操作；

?　批量修改时可修改用户失效时间；

?　账号维护页面增加在线和下线状态，提供对用户的强制下线和删除操作；

? 用户计费周期精确显示到秒；
? 增加可使用业务名登录用户自助服务页面的功能；
? 货币单位和显示可以进行配置；
? 在关于页面增加显示补丁版本信息的功能；
? 支持LDAP用户自动检测，发现LDAP服务器中的新增用户，并添加到预注册用户列表中。

n EAD支持与微软WSUS服务器协同的自动补丁管理

EAD增加了与微软WSUS补丁管理服务器的联动功能，可以在用户接入网络前与WSUS客户端/服务器协同进行补丁安装状态检查，并通过WSUS对未安装必要补丁的终端进行自动补丁升级。

n EAD支持与Windows域的统一认证

EAD认证功能可以与 Windows域用户认证无缝集成，在用户进行Windows域认证的同时，自动进行身份和EAD安全认证。

注意：CAMS 1.20-3100版本不提供DHCP组件。

3 版本存在问题与规避措施

3.1 启用EAD安全认证时的用户域名限制

问题描述：启用EAD安全认证时，用户名是否携带域名后缀，必须要求CAMS客户端、接入设备以及CAMS服务器在配置上保持一致，否则安全认证无法发起。

规避措施：启用EAD安全认证时，需注意在接入设备和CAMS服务器间保持相同的域名配置。

3.2 EAD安装/运行软件检查限制

问题描述：EAD进行安装/运行软件的合法性检查时，如果接入用户修改了软件名称，EAD将无法对该软件进行正确的安装/运行判断。

规避措施：无。Windows操作系统的限制，无法规避。可通过对在线用户的桌面安全状态检查功能查看运行软件名称。

3.3 WEB 认证二次地址分配问题

问题描述：用户使用WEB认证，并启用了二次地址分配时，如果用户浏览器使用的Java版本为JRE 1.5及以上时，将导致认证无法通过。

规避措施：可通过使用Portal 客户端进行认证来规避。

3.4 用户界面中的文字描述问题

问题描述： CAMS服务器和客户端部分界面中存在错别字和描述不够准确等文字问题。

规避措施：无。不影响产品功能的正常使用。

4 解决问题列表

无。

5 版本升级操作指导

参见《CAMS1.20-3100版本说明书》。