RBAC 技术白皮书

Copyright © 2019 紫光恒越技术有限公司 版权所有，保留一切权利。
非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。
除紫光恒越技术有限公司的商标外，本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。本文中的内容为通用性技术信息，某些信息可能不适用于您所购买的产品。

目 录

1 概述 ····· 1
1.1 产生背景 ····· 1
1.2 技术优点 ····· 1
2 RBAC技术实现 ····· 1
2.1 概念介绍 ····· 1
2.1.1 用户账户 ····· 1
2.1.2 动作 ····· 1
2.1.3 命令属性 ····· 1
2.1.4 特性 ····· 2
2.1.5 特性组 ····· 2
2.1.6 用户角色 ····· 2
2.1.7 权限规则 ····· 2
2.1.8 资源控制策略 ····· 3
2.2 运行机制 ····· 3
2.2.1 用户与角色的关联 ····· 3
2.2.2 基于角色的用户权限控制 ····· 3
3 Comware实现的技术特色 ····· 4
3.1 丰富的系统预定义角色 ····· 4
3.2 灵活的用户权限控制 ····· 6
3.2.1 支持不同粒度的权限规则配置 ····· 6
3.2.2 对文件系统访问的控制 ····· 7
3.2.3 多种方式为用户授权角色 ····· 7
3.2.4 用户角色的切换 ····· 8
4 典型组网应用 ····· 8
4.1 RBAC典型组网应用 ····· 8

1 概述

1.1 产生背景

随着网络技术的高速发展，大型数据中心技术尤其是网络虚拟化技术的广泛应用对网络设备的管理提出了更高的要求。传统的基于用户优先级的权限控制技术已经无法适应日新月异的网络应用。为了应对新的技术挑战，引入了 RBAC（Role-Based Access Control，基于角色的访问控制）权限管理模型——一种已经广泛应用于各种管理系统的权限管理模型。在 RBAC 中，操作权限与角色之间建立关联，再通过在角色与用户之间建立关联来完成对用户的授权，大大提高了权限控制的灵活性。

1.2 技术优点

在传统的基于用户优先级的权限控制模型中，用户的权限和用户级别静态绑定，用户具有的权限完全由系统预定义确定。在 RBAC 模型中，系统管理员可以通过配置将特定功能的操作权限赋予自定义的用户角色，从而灵活地控制用户权限。另外，RBAC 增加了对系统资源访问权限的控制，可以限定用户对 VLAN、接口、VPN 实例、安全域和地区标识的访问。

另外，由于权限与用户的分离，RBAC 具有以下特点：

- 管理员不需要针对用户去逐一指定权限，只需要预先定义具有相应权限的角色，再将角色赋予用户即可。因此 RBAC 更能适应用户的变化，提高了用户权限分配的灵活性。
- 由于角色与用户的关系常常会发生变化，但是角色和权限的关系相对稳定，因此利用这种稳定的关联可减小用户授权管理的复杂性，降低管理成本。

2 RBAC技术实现

2.1 概念介绍

2.1.1 用户账户

Comware 系统支持通过创建用户账户来对用户进行身份验证和授权。用户账户分为设备管理用户和网络接入用户两类。设备管理类用户，用于登录设备，对设备进行配置和监控；网络接入类用户，用于通过设备接入网络，访问网络资源。RBAC 功能用来控制设备管理类用户对设备的操作权限。

2.1.2 动作

是指用户对系统的一次操作。例如通过命令行或者 SNMP 协议对系统进行功能配置，通过基于 Web 的用户界面查看设备运行状态等。

2.1.3 命令属性

根据操作性质的不同可分为读、写和执行三种属性。

- 读属性：表示仅对系统配置信息和运行状态信息进行查看；

- 写属性：表示对系统进行配置；
- 执行属性：表示可以执行特定的程序（如 ping 命令调用 ping 程序完成探测功能），并对系统运行状态不产生影响。

2.1.4 特性

与一个功能相关的所有命令的集合，例如 OSPF 特性包含了所有 OSPF 的配置、显示及调试命令。

2.1.5 特性组

一个或者多个特性的集合。其主要目的是为了方便管理员对用户权限进行配置。

2.1.6 用户角色

用户角色是一组权限规则和多种类型的资源控制策略的集合。权限规则定义了允许用户执行的动作和拒绝执行的动作；资源控制策略分别定义了允许用户可以操作的接口、VLAN、VPN 实例、安全域和地区标识。

2.1.7 权限规则

权限规则具体定义了用户角色的执行权限，一个用户角色可以拥有多条权限规则。权限规则可以分为以下几类：

- 基于命令特征字符串的权限规则：此类规则由命令关键字与通配符组成，用于控制与之匹配的命令是否有权限被执行。如果设置为允许执行（**permit**），并且用户被授权用户角色包含这个规则时，此用户有权限执行此命令。如果是设置为拒绝时（**deny**），用户没有权限执行此命令。
- 基于特性的权限规则：此规则可以控制特性包含的命令是否有权限被执行。特性中每条命令均具有动作属性，所以在定义基于特性的权限规则时，可以精细地控制所包含的读命令或者写命令能否被执行。
- 基于特性组的权限规则：此规则和基于特性的权限规则类似，区别是一个特性组中包含了一个或者多个特性。
- 基于 Web 菜单的权限规则：此规则可以控制指定的 Web 菜单是否允许被操作。Web 菜单对应的用户界面中的各种控件具有动作属性，所以在定义此类规则时，可以精细地控制 Web 菜单中所包含的读控件或者写控件能否被操作。
- 基于 XML 元素的权限规则：此规则可以控制指定的 XML 元素的 XPath 是否允许被操作。与 Web 菜单相似，XML 元素的 XPath 对应的用户界面中的各种控件具有动作属性。定义此类规则时，可以精细地控制读控件或者写控件能否被操作。
- 基于 SNMP OID 的权限规则：此规则可以控制指定的 OID 是否允许被 SNMP 访问。

一个用户角色中可以定义多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户的权限是这些规则中定义的操作的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。其中，OID 规则遵循最长匹配，相同长度的匹配规则中编号大的有效。

2.1.8 资源控制策略

资源控制策略规定了用户对系统资源的操作权限。在用户角色中可定义四种类型的资源控制策略：接口策略、VLAN 策略、VPN 策略、安全域策略和地区标识策略，它们分别定义了用户允许操作的接口、VLAN、VPN 实例、安全域或者地区标识。

2.2 运行机制

2.2.1 用户与角色的关联

角色与用户的关联是通过为用户赋予角色建立的。将有效的用户角色成功授权给用户后，登录设备的用户才能以各角色所具有的权限来配置、管理或者监控设备。根据用户登录设备时采用的不同认证方式，可以将为用户授权角色分为 AAA 方式和非 AAA 方式。

- AAA 方式：用户登录设备后所拥有的用户角色由 AAA 功能进行授权。
  - 如果对用户采用本地授权方式，则授权的用户角色是在本地用户中设置的。
  - 如果对用户采用远程服务器授权，则可以在远程服务器上灵活地配置授权方案，可以实现单个用户或者一组用户的角色关联。
- 非 AAA 方式：用户登录后所拥有的用户角色是用户线下配置的用户角色。

2.2.2 基于角色的用户权限控制

当系统获得用户的授权角色后，将根据角色名称读取系统配置并依据角色中的权限规则和资源控制策略为其生成两个表，分别是权限规则表和资源控制策略表。

- 权限规则表项的组成元素包括：规则编号、权限（允许/禁止）、规则类型（命令/Web/XML/SNMP）、动作属性（读/写/执行）、规则内容。
- 资源控制策略表项的组成元素包括：资源类型（VLAN/接口/VPN/安全域/地区标识）、权限（允许/禁止）、资源标识（VLAN 编号/接口名称/VPN 名称/安全域名称/地区标识）。

每个登录到系统中的用户都具有上述两个权限控制表，用户只能执行权限控制表内规定的操作。

当用户通过命令行或者其他配置工具对系统进行操作时，系统将查找该用户的权限控制表来判断用户的当前操作是否被允许。资源控制策略表项需要与权限规则表项相配合才能生效。下面以执行某条配置命令为例，详细描述具体处理过程：

(1) 用户输入配置命令，例如：**`vlan`** 1。

(2) 系统读取到用户的输入后，查找该用户对应的权限规则表：

   a. 按照规则编号从大到小查找。

   b. 判断规则类型，如果不是命令规则，则跳过该表项；否则，继续进行下一步处理。

   c. 将字符串“vlan 1”与规则中的正则表达式内容进行匹配，如果不匹配，继续查找下一条规则；否则，得到该表项对应的权限（允许/禁止）。

(3) 如果步骤（2）中的匹配结果为允许执行，则查找资源控制策略表。因为 **`vlan`** 1 命令操作的对象是 VLAN 资源，所以查找该用户 VLAN 类型的资源控制表项，如果 VLAN 1 在允许的列表中，则允许用户执行 **`vlan`** 1；否则，返回禁止执行，并提示用户“Permission denied.”。

(4) 如果步骤（2）中的匹配结果为禁止执行，则提示用户“Permission denied.”。

3 Comware实现的技术特色

3.1 丰富的系统预定义角色

Comware提供了丰富的系统预定义角色，用户可以直接使用这些预定义角色来对设备进行权限控制。系统预定义的用户角色名和对应的权限如 表 3-1 所示。这些用户角色缺省均具有操作所有系统资源的权限，但具有不同的系统功能操作权限。

表3-1 系统预定义的用户角色名和对应的权限

用户角色名	权限
network-admin	可操作系统所有功能和资源（除安全日志文件管理相关命令之外）
network-operator	• 可执行系统所有功能和资源的相关显示命令（除 **display history-command all**、**display security-logfile summary** 等命令，具体请通过 **display role** 命令查看） • 可执行切换 MDC（Multitenant Device Context，多租户设备环境）视图的命令 • 如果用户采用本地认证方式登录系统并被授予该角色，则可以修改自己的密码 • 可执行进入 XML 视图的命令 • 可允许用户操作所有读类型的 Web 菜单选项 • 可允许用户操作所有读类型的 XML 元素 • 可允许用户操作所有读类型的 OID
mdc-admin	可操作该MDC所有功能和资源（除安全日志文件管理相关命令之外），但不包括操作仅缺省MDC支持，非缺省MDC不支持的功能的权限
mdc-operator	• 可执行该 MDC 所有功能和资源的相关显示命令（除 **display history-command all**、**display security-logfile summary** 等命令，具体请通过 **display role** 命令查看），但不包括仅缺省 MDC 支持，非缺省 MDC 不支持的功能的相关 **display** 命令的执行权限 • 如果用户采用本地认证方式登录系统并被授予该角色，则可以修改自己的密码 • 可执行进入 XML 视图的命令 • 可允许用户操作所有读类型的 Web 菜单选项 • 可允许用户操作所有读类型的 XML 元素 • 可允许用户操作所有读类型的 OID

用户角色名	权限
level-*n* (*n* = 0～15)	• level-0：可执行命令 **ping**、**tracert**、**ssh2**、**telnet** 和 **super**，且管理员可以为其配置权限 • level-1：具有 level-0 用户角色的权限，并且可执行系统所有功能和资源的相关显示命令（除 **display history-command all** 之外），以及管理员可以为其配置权限 • level-2～level-8 和 level-10～level-14：无缺省权限，需要管理员为其配置权限 • level-9：可操作系统中绝大多数的功能和所有的资源，且管理员可以为其配置权限，但不能操作 **display history-command all** 命令、RBAC 的命令（Debug 命令除外）、MDC、文件管理、设备管理以及本地用户特性。对于本地用户，若用户登录系统并被授予该角色，可以修改自己的密码 • level-15：具有与 network-admin 角色相同的权限（不支持 MDC、Context 的设备） • level-15：在缺省 MDC 中，具有与 network-admin 角色相同的权限；在非缺省 MDC 中，具有与 mdc-admin 角色相同的权限（支持 MDC 的设备） • level-15：在缺省 Context 中，具有与 network-admin 角色相同的权限；在非缺省 Context 中，具有与 context-admin 角色相同的权限（支持 Context 的设备）
security-audit	安全日志管理员，仅具有安全日志文件的读、写、执行权限，具体如下： • 可执行安全日志文件管理相关的命令 • 可执行安全日志文件操作相关的命令，例如 **more** 显示安全日志文件内容；**dir**、**mkdir** 操作安全日志文件目录等 以上权限，仅安全日志管理员角色独有，其它任何角色均不具备 该角色不能被授权给从当前用户线登录系统的用户
guest-manager	来宾用户管理员，只能查看和配置与来宾有关的Web页面，没有控制命令行的权限
context-admin	可操作该Context所有功能和资源（除安全日志文件管理相关命令之外）
context-operator	• 可执行该 Context 所有功能和资源的相关 **display** 命令（除 **display history-command all**、**display security-logfile summary** 等命令，具体请通过 **display role** 命令查看） • 如果用户采用本地认证方式登录系统并被授予该角色，则可以修改自己的密码 • 可执行进入 XML 视图的命令 • 可允许用户操作所有读类型的 Web 菜单选项 • 可允许用户操作所有读类型的 XML 元素 • 可允许用户操作所有读类型的 OID

用户角色名	权限
system-admin	系统管理员，具有部分Web页面菜单的读、写、执行权限，具体如下： ● 对概览菜单具有读、写、执行权限 ● 对监控菜单下的系统日志菜单具有读、写、执行权限 ● 对系统菜单具体权限如下： ○ 对管理员和角色菜单仅有读权限 ○ 对其它子菜单菜单具有读、写、执行权限 系统管理员角色目前仅实现Web页面功能，命令行只有**ping**和**tracert**的权限，具体权限请通过**display role**命令查看 该角色不能被授权给从当前用户线登录系统的用户
security-admin	安全管理员，具有大部分Web页面菜单的读、写、执行权限，具体如下： ● 对策略、对象和网络菜单具有读、写、执行权限 ● 对监控菜单具体权限如下： ○ 对系统日志、操作日志子菜单无读、写、执行权限 ○ 对于其他子菜单拥有读、写、执行权限 安全管理员角色目前仅实现Web页面功能，命令行只有执行**ping**和**tracert**命令的权限，具体权限请通过**display role**命令查看 该角色不能被授权给当前用户线登录系统的用户
audit-admin	审计管理员，仅具有对监控菜单下的操作日志子菜单具有读、写、执行权限 审计管理员角色目前仅实现Web页面功能，命令行只有执行**ping**和**tracert**命令的权限，具体权限请通过**display role**命令查看 该角色不能授权给当前用户线登录系统的用户

3.2 灵活的用户权限控制

3.2.1 支持不同粒度的权限规则配置

1. 基于命令特征的规则

当需要限制用户对符合某些特征的命令的权限时，可以配置基于命令特征的规则。规则由允许/禁止（**permit/deny**）关键字及命令匹配字符串（*command-string*）定义是否允许执行一条命令或者与指定命令关键字相匹配的一组命令。

2. 基于特性的规则

当需要限制用户对某个功能的整体操作权限时，可以配置基于特性的规则。规则由允许/禁止（**permit/deny**）关键字、特性名称（*feature-name*）以及该特性中命令的类型（读/写/执行）定义是否允许执行一个特性中包含的指定类型的命令。当不指定特性名称时，将理解为指定所有特性。

3. 基于特性组的规则

当需要限制用户对某些功能的整体操作权限时，可以配置基于特性组的规则。规则由允许/禁止（**permit/deny**）关键字、特性组名称（*feature-group-name*）以及该特性组中命令的类型（读/写/执行）定义是否允许执行一个特性组中的特性包含的指定类型的命令。

4. 基于 Web 菜单的权限规则

当需要限制用户对 Web 界面上某菜单项的权限时，可以配置基于 Web 菜单的规则。规则由允许/禁止（**permit**/**deny**）关键字，Web 菜单选项的 ID 路径以及该菜单中控件的操作类型（读/写/执行）定义是否允许操作一个 Web 菜单中包含的指定类型的控件。如果不指定 Web 菜单项，则对所有 Web 菜单项生效。

5. 基于 XML 路径的权限规则

当需要限制用户对 XML 路径的权限时，可以配置基于 XML 路径的规则。规则由允许/禁止（**permit**/**deny**）关键字，XML 路径描述符以及控件的操作类型（读/写/执行）定义是否允许操作一个 XML 路径中包含的指定类型的控件。如果不指定 XML 路径，则对所有 XML 路径生效。

6. 基于 OID 的权限规则

当需要限制用户通过 SNMP 对 OID 的权限时，可以配置基于 OID 的规则。规则由允许/禁止（**permit**/**deny**）关键字、OID（*oid-string*）以及对该 OID 的操作类型（读/写/执行）定义是否允许执行一个或所有指定类型的 OID。

3.2.2 对文件系统访问的控制

通过配置基于文件系统特性的规则，可以控制用户在命令行界面对文件系统的访问权限。例如：定义规则 **rule** *rule-num* **permit read feature filesystem**，可以允许用户在命令行界面仅拥有读文件系统的操作权限。

需要关注的是：

- 访问文件系统的命令，受基于文件系统特性规则以及具体命令规则的双重控制。
- 对于 FTP 用户，规则中对文件系统读、写属性的控制将影响 FTP 用户的上传和下载权限。
- 对于需要将输出信息重定向到文件中保存的命令，只有在用户角色被授权了文件系统写权限后才允许执行。

3.2.3 多种方式为用户授权角色

1. 为远程 AAA 认证用户授权角色

对于通过远程 AAA 认证登录设备的用户，由 AAA 服务器的配置决定为其授权的用户角色。如果用户没有被授权任何用户角色，将无法成功登录设备。为此，系统提供了一个缺省用户角色授权功能。使能该功能后，用户在 AAA 服务器没有为其授权角色的情况下，将具有一个缺省的用户角色。该缺省用户角色可以通过配置来指定。

RADIUS 服务器上的授权角色配置与服务器的具体情况有关，请参考服务器的配置指导进行；HWTACACS 服务器上的授权角色配置必须满足格式：roles="*name1 name2 namen*"，其中 *name1*、*name2*、*namen* 为要授权下发给用户的用户角色，可为多个，并使用空格分隔。

2. 为本地 AAA 认证用户授权角色

对于通过本地 AAA 认证登录设备的用户，由本地用户配置决定为其授权的用户角色。由于本地用户缺省拥有一个用户角色，如果要赋予本地用户新的用户角色，请确认是否需要保留这个缺省的用户角色，若不需要，请删除。但需要注意的是，一个本地用户至少必须拥有一个用户角色。

3. 为非 AAA 认证用户授权角色

对于不使用 AAA 认证登录设备的非 SSH 用户，由用户线的配置决定为其授权的用户角色。通过 publickey 或 password-publickey 方式认证登录的 SSH 用户，由同名的设备管理类本地用户配置决定为其授权的用户角色。

3.2.4 用户角色的切换

Comware 系统提供了 **super** 命令用于切换当前登录用户的角色，从而满足用户临时提升/降低自身权限的需求。

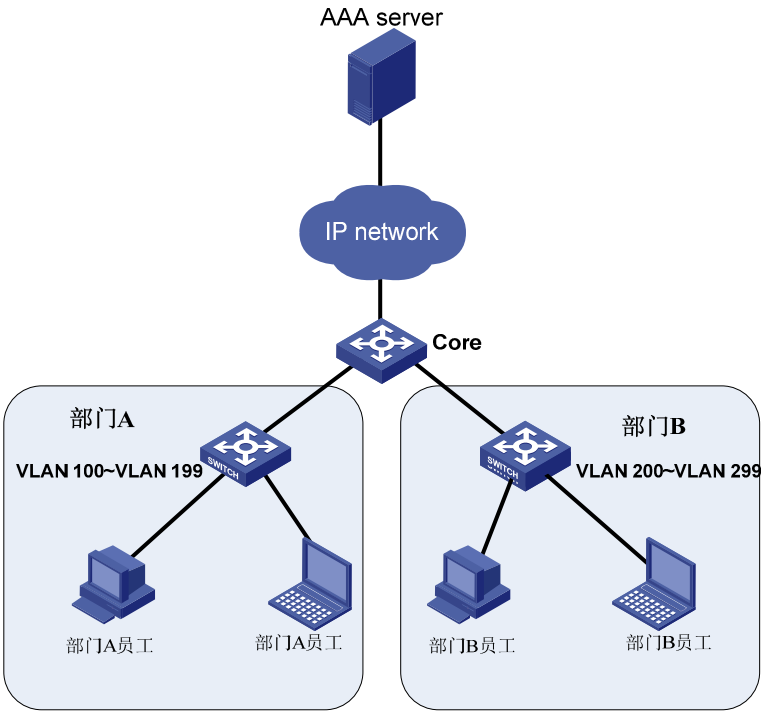
切换用户角色是指在不退出当前登录、不断开当前连接的前提下修改用户的用户角色，改变用户所拥有的命令行权限。切换后的用户角色只对当前登录生效，用户重新登录后，又会恢复到原有角色。

- 为了防止对设备的误操作，通常情况下建议管理员使用较低权限的用户角色登录设备、查看设备运行参数，当需要对设备进行维护时，再临时切换到较高权限的用户角色。
- 当管理员需要暂时离开设备或者将设备暂时交给其它人代为管理时，为了安全起见，可以临时切换到较低权限的用户角色，来限制其他人员的操作。

4 典型组网应用

4.1 RBAC典型组网应用

图4-1 RBAC 典型应用组网图



某企业内部为隔离部门间流量将不同 VLAN 划分给不同的部门使用，并允许各部门网络管理员在 Core 设备上部署 QoS 流量控制策略。另外，为了防止部门网络管理员操作 Core 设备的其它的配置，可以采用 RBAC 对各部门网络管理的权限进行控制。

具体的权限管理需求如下：

- 部门网络管理员角色为 depart-admin，该角色具有 QoS 流量控制策略相关功能的配置权限。
- 部门 A 资源控制角色为 departA-resource，该角色具有操作 VLAN 100~VLAN 199 的操作权限；
- 部门 B 资源控制角色为 departB-resource，该角色具有操作 VLAN 200~VLAN 299 的操作权限。

在 AAA 服务器上为部门 A 管理员授权角色 depart-admin 和 departA-resource，为部门 B 管理员授权角色 depart-admin 和 departB-resouce 角色。这样，即可通过 RBAC 实现权限的精细控制。