WX系列AC 本地认证使用User Profile不同场景应用举例

wlan接入 User Profile **王森森** 2012-06-27 发表

WX系列AC 本地认证使用User Profile不同场景应用举例

一、特性介绍:

User Profile（用户配置文件）提供一个配置模板，能够保存预设配置（一系列配置的集合）。用户访问设备时，需要先进行身份认证。在认证过程中，认证服务器会先匹配用户名和密码，匹配成功后再将与用户绑定的User Profile名称下发给设备，设备会立即启用User Profile里配置的具体内容。只有用户名和密码匹配，并且User Profile下的配置均应用成功，设备才认为用户通过了认证。因此，当用户通过认证上线后，其访问行为将受到User Profile的限制。当用户下线时，系统会自动禁用User Profile下的配置项，从而取消User Profile对用户的限定。因此，User Profile适用于限制上线用户的访问行为，没有用户上线（可能是没有用户接入、或者用户没有通过认证、或者用户下线）时，User Profile是预设配置，并不生效。

二、配置基于SSID的用户接入控制

在有用户临时需要接入网络时，需要临时为用户建立一个来宾账户，通过基于SSID的接入控制可以达到访问限制的目的，即限制来宾用户只能在指定的SSID登录。SSID的接入控制可以通过在User Profile下配置允许接入的SSID来实现。

场景一：通过配置本地用户的授权属性User Profile实现

本地用户的授权属性在用户组和本地用户视图下都可以配置，且本地用户视图下的配置优先级高于用户组视图下的配置。用户组的配置对组内所有本地用户生效。

在本地用户视图下配置步骤（以802.1X本地认证为例）：

system-view

[AC] user-profile profile01

[AC-user-profile-profile01] wlan permit-ssid h3c-test01

[AC-user-profile-profile01] quit

[AC] user-profile profile01 enable

[AC] local-user test

[AC-luser-test] password simple test

[AC-luser-test] authorization-attribute user-profile profile01

[AC-luser-test] service-type lan-access

[AC-luser-test] quit

结果验证:

802.1X用户只有接入SSID” h3c-test01”时成功通过认证。

场景二：通过配置本地用户组的授权属性User Profile实现

在本地用户组视图下配置步骤（以802.1X本地认证为例）：

system-view

[AC] user-profile profile01

[AC-user-profile-profile01] wlan permit-ssid h3c-test01

[AC-user-profile-profile01] quit

[AC] user-profile profile01 enable

[AC] user-group group01

[AC-ugroup-group01] authorization-attribute user-profile profile01

[AC-ugroup-group01] quit

[AC] local-user test

[AC-luser-test] password simple test

[AC-luser-test] group group01

[AC-luser-test] service-type lan-access

[AC-luser-test] quit

结果验证：

802.1X用户只有接入SSID” h3c-test01”时成功通过认证。

场景三：通过配置ISP域的授权属性User Profile实现

对于802.1X认证、Portal认证和MAC地址认证，缺省认证ISP域为system域，而system域缺省认证方法为local，所以通过配置ISP域的授权属性User Profile同样对本地用户生效。

在ISP域视图下配置步骤（以802.1X本地认证为例）：

system-view

[AC] user-profile profile01

[AC-user-profile-profile01] wlan permit-ssid h3c-test01

[AC-user-profile-profile01] quit

[AC] user-profile profile01 enable

[AC] domain system

[AC-isp-system] authorization-attribute user-profile profile01

[AC-isp-system] quit

[AC] local-user test

[AC-luser-test] password simple test

[AC-luser-test] service-type lan-access

[AC-luser-test] quit

结果验证：

802.1X用户只有接入SSID” h3c-test01”时成功通过认证。

三、配置基于AP的用户接入控制

无线接入服务的提供者希望能控制客户端在无线接入网中的接入位置。这里的接入位置目前主要指客户端所接入的AP。基于某些策略考虑（如安全性或者计费等因素），提供无线接入服务的机构希望通过特定的AP接入策略，以使不同的client通过不同的AP访问网络。AP接入策略可以通过用户在User Profile下配置客户端关联的AP组，这样就可以确保客户端只能通过授权的AP访问网络资源。

场景一：通过配置本地用户的授权属性User Profile实现

本地用户的授权属性在用户组和本地用户视图下都可以配置，且本地用户视图下的配置优先级高于用户组视图下的配置。用户组的配置对组内所有本地用户生效。

在本地用户视图下配置步骤（以802.1X本地认证为例）：

system-view

[AC] wlan ap-group 1

[AC-ap-group1] ap ap01

[AC-ap-group1] quit

[AC] user-profile profile01

[AC-user-profile-profile01] wlan permit-ap-group 1

[AC-user-profile-profile01] quit

[AC] user-profile profile01 enable

[AC] local-user test

[AC-luser-test] password simple test

[AC-luser-test] authorization-attribute user-profile profile01

[AC-luser-test] service-type lan-access

[AC-luser-test] quit

结果验证：

802.1X用户只有接入特定AP”ap01”时成功通过认证。

场景二：通过配置本地用户组的授权属性User Profile实现

在本地用户组视图下配置步骤（以802.1X本地认证为例）：

system-view

[AC] wlan ap-group 1

[AC-ap-group1] ap ap01

[AC-ap-group1] quit

[AC] user-profile profile01

[AC-user-profile-profile01] wlan permit-ap-group 1

[AC-user-profile-profile01] quit

[AC] user-profile profile01 enable

[AC] user-group group01

[AC-ugroup-group01] authorization-attribute user-profile profile01

[AC-ugroup-group01] quit

[AC] local-user test

[AC-luser-test] password simple test

[AC-luser-test] group group01

[AC-luser-test] service-type lan-access

[AC-luser-test] quit

结果验证：

802.1X用户只有接入特定AP”ap01”时成功通过认证。

场景三：通过配置ISP域的授权属性User Profile实现

对于802.1X认证、Portal认证和MAC地址认证，缺省认证ISP域为system域，而system域缺省认证方法为local，所以通过配置ISP域的授权属性User Profile同样对本地用户生效。

在ISP域视图下配置步骤（以802.1X本地认证为例）：

system-view

[AC] wlan ap-group 1

[AC-ap-group1] ap ap01

[AC-ap-group1] quit

[AC] user-profile profile01

[AC-user-profile-profile01] wlan permit-ap-group 1

[AC-user-profile-profile01] quit

[AC] user-profile profile01 enable

[AC] domain system

[AC-isp-system] authorization-attribute user-profile profile01

[AC-isp-system] quit

[AC] local-user test

[AC-luser-test] password simple test

[AC-luser-test] service-type lan-access

[AC-luser-test] quit

结果验证：

802.1X用户只有接入特定AP”ap01”时成功通过认证。

说明：

1、配置基于SSID的用户接入控制同样适用于802.1X本地认证、Portal本地认证（请与本地Portal区别）、MAC地址本地认证。

2、配置基于AP的用户接入控制同样适用于802.1X本地认证、Portal本地认证（请与本地Portal区别）、MAC地址本地认证。

3、可根据不同的应用场景选择不同的认证方式和用户接入控制策略。