Attributs RADIUS pris en charge sur le contrôleur LAN sans fil

Contenu

Introduction

Ce document explique la liste d'attributs RADIUS pris en charge sur le contrôleur LAN Sans fil (WLC) qui sont envoyés au serveur de RAYON dans l'Access-demande, honoré dedans Access-recevez, et introduit des demandes de comptabilité. Ceci inclut également les attributs de constructeur-particularité.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Méthodes de sécurité sans fil
- authentification basée sur rayon

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Attributs RADIUS pris en charge sur le contrôleur LAN sans fil

Des attributs RADIUS sont utilisés pour définir les éléments spécifiques d'Authentification, autorisation et comptabilité (AAA) dans un profil utilisateur, qui est enregistré sur le démon de RAYON. Cette section répertorie les attributs RADIUS actuellement pris en charge sur le contrôleur LAN Sans fil.

- **Qualité de service** — Si actuel dans un RAYON Access recevez, la valeur niveau QoS ignore la valeur de QoS spécifiée dans le profil WLAN.
- **ACL** — Quand l'attribut de liste de contrôle d'accès (ACL) est présent dans le RAYON Access recevez, le système s'applique l'Acl-nom à la station client après qu'elle authentifie. Ceci ignore n'importe quel ACLs qui sont assignés à l'interface.
- **VLAN** — Quand un Interface-nom ou la VLAN-balise VLAN est présente dans un RAYON Access recevez, le système place le client sur une interface spécifique.
- **ID de WLAN** — Quand l'attribut d'ID de WLAN est présent dans le RAYON Access recevez, le système s'applique l'ID de WLAN (SSID) à la station client après qu'elle authentifie. L'ID de WLAN est envoyé par le WLC dans tous les exemples de l'authentification excepté IPsec. En cas d'authentification Web, si le WLC reçoit un attribut d'ID de WLAN dans la réponse d'authentification du serveur d'AAA, et de elle n'apparie pas l'ID du WLAN, authentification est rejeté. D'autres types de méthodes de Sécurité ne font pas ceci.
- **Valeur DSCP** — Si actuel dans un RAYON Access recevez, la valeur DSCP ignore la valeur DSCP spécifiée dans le profil WLAN.
- **802.1p-Tag** — Si actuel dans un RAYON Access recevez, la valeur 802.1p ignore le par défaut spécifié dans le profil WLAN.

Remarque: La caractéristique VLAN prend en charge seulement le filtrage MAC, le 802.1X, et le Protocole WPA (Wi-Fi Protected Access). La caractéristique VLAN ne prend en charge pas l'authentification Web ou l'IPsec. La base de données locale du filtre d'adresses MAC du système d'exploitation a été étendue pour inclure le nom d'interface. Ceci permet aux filtres d'adresses MAC locaux pour spécifier qui relient le client devraient être assignés. Un serveur distinct de RAYON peut également être utilisé, mais le serveur de RAYON doit être défini utilisant les menus Security.

Niveau QoS

L'attribut niveau QoS indique le niveau de qualité de service à appliquer au trafic du client mobile dans la matrice de commutation, aussi bien qu'au-dessus de l'air. Cet exemple affiche un résumé du format niveau QoS d'attribut. Les champs sont transmis de gauche à droite.

```
0                   1                   2                   3

0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
|     Type      |  Length       |            Vendor-Id

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

     Vendor-Id (cont.)          | Vendor type   | Vendor length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|                           QoS Level                           |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

•Type - 26 for Vendor-Specific

•Length - 10

•Vendor-Id - 14179

•Vendor type - 2

•Vendor length - 4

•Value - Three octets:

–3 - Bronze (Background)

–0 - Silver (Best Effort)

–1 - Gold (Video)

–2 - Platinum (Voice)

Acl-nom

L'attribut d'Acl-nom indique le nom d'ACL à appliquer au client. Un résumé du format d'attribut d'Acl-nom est affiché ici. Les champs sont transmis de gauche à droite.

```
 0                   1                   2                   3

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|     Type      |  Length       |            Vendor-Id

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

     Vendor-Id (cont.)          | Vendor type   | Vendor length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|        ACL Name...

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

•Type - 26 for Vendor-Specific

•Length - >7

•Vendor-Id - 14179

```
•Vendor type - 6

•Vendor length - >0

•Value - A string that includes the name of the ACL to use for the client
```

Interface-nom

L'attribut d'Interface-nom indique que l'interface VLAN un client doit être associée à. Un résumé du format d'attribut d'Interface-nom est affiché ici. Les champs sont transmis de gauche à droite.

```
 0                   1                   2                   3

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|     Type      |  Length       |            Vendor-Id

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

     Vendor-Id (cont.)          |  Vendor type  | Vendor length |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|    Interface Name...

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-

•Type - 26 for Vendor-Specific

•Length - >7

•Vendor-Id - 14179

•Vendor type - 5

•Vendor length - >0

•Value - A string that includes the name of the interface
the client is to be assigned to.
```

Remarque: Cet attribut fonctionne seulement quand le filtrage MAC est activé ou si le 802.1X ou le WPA est utilisé comme stratégie de sécurité.

VLAN-balise

L'attribut de VLAN-balise indique l'identification groupe pour une session percée un tunnel par détail, et est également connu comme attribut de Tunnel-Private-Group-ID.

Cet attribut pourrait être inclus dans le paquet de demande d'accès si le demandeur de tunnel peut prédéterminer le groupe qui résulte d'une connexion particulière et si est inclus dans le paquet d'acceptation d'accès si cette session de tunnel doit être traitée comme si il appartient à un groupe privé particulier. Des groupes privés peuvent être utilisés pour associer une session percée un tunnel avec un groupe particulier d'utilisateurs. Par exemple, il peut être utilisé pour faciliter l'acheminement des adresses IP non inscrites par une interface spécifique. Il devrait être inclus en paquets de Comptabilité-demande qui contiennent des attributs d'Acct-État-type avec des valeurs de début ou d'arrêt et qui concernent une session percée un tunnel.

Un résumé du format d'attribut de Tunnel-Private-Group-ID est affiché ici. Les champs sont

transmis de gauche à droite.

```
 0                   1                   2                   3

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

|      Type     |    Length     |     Tag       |   String...

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

•Type - 81 for Tunnel-Private-Group-ID.

•Length - > = 3

•Tag - The Tag field is one octet in length and is intended to provide a means of grouping attributes in the same packet which refer to the same tunnel. If the value of the Tag field is greater than 0x00 and less than or equal to 0x1F, it should be interpreted as indicating which tunnel (of several alternatives) this attribute pertains. If the Tag field is greater than 0x1F, it should be interpreted as the first byte of the following String field.
•String - This field must be present. The group is represented by the String field. There is no restriction on the format of group IDs.

Attributs de tunnel

Si l'uns des d'autres attributs RADIUS (niveau QoS, Acl-nom, Interface-nom, ou VLAN-balise) sont retournés, les attributs de tunnel RFC 2868 doivent également être retournés.

RFC 2868 définit des attributs de tunnel de RAYON utilisés pour l'authentification et l'autorisation, et RFC 2867 définit des attributs de tunnel utilisés pour la comptabilité. Là où les prises en charge de l'agent d'authentification de 802.1X d'IEEE perçant un tunnel, un tunnel obligatoire peuvent être installées pour le suppliant en raison de l'authentification.

En particulier, il pourrait être desirable de permettre un port à placer dans un VLAN particulier, défini dans le 802.1Q d'IEEE, basé sur le résultat de l'authentification. Ceci peut être utilisé, par exemple, pour permettre à un hôte sans fil pour rester sur le même VLAN qu'il déplace dans un réseau campus.

Le serveur de RAYON indique typiquement le VLAN désiré en incluant des attributs de tunnel dans l'Access-recevoir. Cependant, l'authentificateur de 802.1X d'IEEE pourrait également fournir un signe quant au VLAN à assigner au suppliant en incluant des attributs de tunnel dans l'Access-demande.

Ces attributs de tunnel sont utilisés pour l'affectation VLAN :

- Tunnel-Type=VLAN (13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

Le VLANID est 12-bits, est une valeur entre 1 et 4094, et est inclus. Puisque le Tunnel-Private-Group-ID est de la chaîne de type comme défini dans RFC 2868 , pour l'usage avec le 802.1X d'IEEE, la valeur entière VLANID est encodée comme chaîne.

Quand des attributs de tunnel sont envoyés, il est nécessaire de compléter le champ Tag. Ceci est noté dans RFC 2868 , la section 3.1 :

- Le champ Tag est un octet de longueur et est destiné pour fournir des moyens des attributs de groupement dans le même paquet qui se rapportent au même tunnel. Les valeurs valides pour ce champ sont 0x01 par 0x1F (inclus). Si la zone Tag est inutilisée, elle doit avoir pour valeur zéro (0x00).
- Pour l'usage avec les attributs de Tunnel-Client-point final, de Tunnel-Serveur-point final, de Tunnel-Private-Group-ID, de Tunnel-Affectation-ID, de Tunnel-Client-Auth-ID ou de Tunnel-Serveur-Auth-ID (mais pas le Tunnel-type, le Tunnel-Support-type, le Tunnel-mot de passe, ou la Tunnel-préférence), un champ de balise de plus grand que 0x1F est interprété comme le premier octet du prochain champ de chaîne. Pour des informations détaillées sur le format référez-vous à la section 3.1 RFC 2868.
- Àmoins que des types alternatifs de tunnel soient fournis, (par exemple, pour les authentificateurs de 802.1X d'IEEE qui pourraient prendre en charge le Tunnellisation mais pas les VLAN), il est seulement que les attributs de tunnel spécifient un tunnel simple. En conséquence, où on le désire seulement pour spécifier le VLANID, le champ Tag devrait être placé à zéro (0x00) dans tous les attributs de tunnel. Là où des types alternatifs de tunnel sont fournis, vous devriez choisir des valeurs de balise entre 0x01 et 0x1F.

Syntaxe pour la configuration des attributs WLC sur des serveurs de RAYON

Les VSAs de Cisco Airespace sur le Cisco Access Registrar

Cisco CNS Access Registrar est un policy server Rayon-conforme, d'accès conçu pour prendre en charge la livraison du cadran, un RNIS, et un nouveau service comprenant le DSL, un câble avec le Telco-Return, une radio et une voix sur ip. Pour des informations détaillées sur le Cisco Access Registrar référez-vous à la page de support de Cisco Access Registrar.

C'est la syntaxe qui doit être utilisée sur le Cisco Access Registrar pour définir les attributs WLC.

- **Définit des attributs RADIUS d'Airespace :**
```
Description = str:[0]
Name = str:[0]Airespace
Type = str:[0]SUB_ATTRIBUTES
VendorID = int32:[0]14179
VendorTypeSize = str:[0]8-bit
```
- **Définit l'ID de WLAN pour l'utilisateur :**
```
Description = str:[0]
Max = int32:[0]4294967295
Min = int32:[0]0
Name = str:[0]Airespace-WLAN-Id
SubAttribute = int32:[0]1
Type = str:[0]UINT32
```
- **Définit le niveau de QoS pour un utilisateur :**
```
Description = str:[0]
Max = int32:[0]3
Min = int32:[0]0
Name = str:[0]Airespace-QoS-Level
SubAttribute = int32:[0]2
Type = str:[0]ENUM
0 = str:[0]Silver
1 = str:[0]Gold
2 = str:[0]Platinum
```

```
3 = str:[0]Bronze
```

- **Définit la valeur DSCP des paquets d'un utilisateur :**
```
Description = str:[0]
Max = int32:[0]4294967295
Min = int32:[0]0
Name = str:[0]Airespace-DSCP
SubAttribute = int32:[0]3
Type = str:[0]UINT32
```
- **Définit la balise 802.1p :**
```
Description = str:[0]
Max = int32:[0]4294967295
Min = int32:[0]0
Name = str:[0]Airespace-802.1P-Tag
SubAttribute = int32:[0]4
Type = str:[0]UINT32
```
- **Définit l'interface à laquelle l'utilisateur est tracé :**
```
Description = str:[0]
Max = int32:[0]253
Min = int32:[0]0
Name = str:[0]Airespace-Interface-Name
SubAttribute = int32:[0]5
Type = str:[0]STRING
```
- **Définit l'ACL qui est appliqué :**
```
Description = str:[0]
Max = int32:[0]253
Min = int32:[0]0
Name = str:[0]Airespace-ACL-Name
SubAttribute = int32:[0]6
Type = str:[0]STRING
```

Les VSAs de Cisco Airespace sur le rayon libre divisent

Le fichier de dictionnaire d'Airespace pour le serveur libre de RAYON est disponible dans le répertoire d'installation sous le **partage de** nom du répertoire. Le nom du fichier est dictionary.airespace.

Remarque: Le fichier de dictionnaire pourrait être différent pour des versions antérieures. Les exemples donnés dans ce document sont de version 1.1.6 libre de RAYON.

```
# -*- text -*-
#
#As found on the net.
#
#$Id: dictionary.airespace,v 1.3.2.1 2005/11/30 22:17:19 aland Exp $
#
VENDORAirespace14179

BEGIN-VENDORAirespace
ATTRIBUTEAirespace-Wlan-Id1integer
ATTRIBUTEAirespace-QOS-Level2integer
ATTRIBUTEAirespace-DSCP3integer
ATTRIBUTEAirespace-8021p-Tag4integer
ATTRIBUTEAirespace-Interface-Name5string
ATTRIBUTEAirespace-ACL-Name6string

VALUEAirespace-QOS-LevelBronze3
VALUEAirespace-QOS-LevelSilver0
VALUEAirespace-QOS-LevelGold1
VALUEAirespace-QOS-LevelPlatinum2


END-VENDOR Airespace
```

Le dictionnaire spécifique de constructeur pour des Produits d'Airespace est inclus dans le fichier

de dictionnaire disponible sous le même répertoire. Le nom du fichier est dictionnaire.

```
# -*- text -*-
#
# Version $Id: dictionary,v 1.93.2.5.2.10 2007/04/08 14:42:06 aland Exp $
#
#DO NOT EDIT THE FILES IN THIS DIRECTORY
#
#
#Use the main dictionary file (usually /etc/raddb/dictionary)
#for local system attributes and $INCLUDEs.
#
#
#
#This file contains dictionary translations for parsing
#requests and generating responses.  All transactions are
#composed of Attribute/Value Pairs.  The value of each attribute
#is specified as one of 4 data types.  Valid data types are:
#
#text       - printable, generally UTF-8 encoded (subset of 'string')
#string     - 0-253 octets
#ipaddr     - 4 octets in network byte order
#integer    - 32 bit value in big endian order (high byte first)
#date       - 32 bit value in big endian order - seconds since
#     00:00:00 GMT,  Jan.  1,  1970
#ifid       - 8 octets in network byte order
#ipv6addr   - 16 octets in network byte order
#ipv6prefix - 18 octets in network byte order
#
#FreeRADIUS includes extended data types which are not defined
#in the RFC's.  These data types are:
#
#abinary - Ascend's binary filter format.
#octets  - raw octets, printed and input as hex strings.
#  e.g.: 0x123456789abcdef
#
#
#Enumerated values are stored in the user file with dictionary
#VALUE translations for easy administration.
#
#Example:
#
#ATTRIBUTE  VALUE
#---------------   -----
#Framed-Protocol = PPP
#7= 1(integer encoding)
#

#
#Include compatibility dictionary for older users file. Move
#this directive to the end of this file if you want to see the
#old names in the logfiles, INSTEAD OF the new names.
#
$INCLUDE dictionary.compat

#
#Include the RFC dictionaries next.
#
#For a complete list of the standard attributes and values,
#see:
#http://www.iana.org/assignments/radius-types
#
$INCLUDE dictionary.rfc2865
```

```
$INCLUDE dictionary.rfc2866
$INCLUDE dictionary.rfc2867
$INCLUDE dictionary.rfc2868
$INCLUDE dictionary.rfc2869
$INCLUDE dictionary.rfc3162
$INCLUDE dictionary.rfc3576
$INCLUDE dictionary.rfc3580
$INCLUDE dictionary.rfc4372
$INCLUDE dictionary.rfc4675
$INCLUDE dictionary.rfc4679

#
#Include vendor dictionaries after the standard ones.
#
$INCLUDE dictionary.3com
$INCLUDE dictionary.3gpp
$INCLUDE dictionary.3gpp2
$INCLUDE dictionary.acc
$INCLUDE dictionary.airespace $INCLUDE dictionary.alcatel $INCLUDE dictionary.alteon $INCLUDE
dictionary.alvarion $INCLUDE dictionary.aruba $INCLUDE dictionary.ascend $INCLUDE dictionary.asn
$INCLUDE dictionary.bay $INCLUDE dictionary.bintec $INCLUDE dictionary.cablelabs $INCLUDE
dictionary.cabletron $INCLUDE dictionary.cisco # # The Cisco VPN300 dictionary is the same as
the altiga one. # You shouldn't use both at the same time. # #$INCLUDE dictionary.cisco.vpn3000
$INCLUDE dictionary.cisco.vpn5000 $INCLUDE dictionary.cisco.bbsm # # And finally the server
internal attributes. # $INCLUDE dictionary.freeradius.internal # # Miscellaneous attributes
defined in weird places that # don't really belong anywhere else... # ATTRIBUTE Originating-
Line-Info 94 string # As defined in draft-sterman-aaa-sip-00.txt ATTRIBUTE Digest-Response 206
string ATTRIBUTE Digest-Attributes 207 octets # # # Integer Translations # VALUE Service-Type
Voice 12 VALUE Service-Type Fax 13 VALUE Service-Type Modem-Relay 14 VALUE Service-Type IAPP-
Register 15 VALUE Service-Type IAPP-AP-Check 16 VALUE Framed-Protocol GPRS-PDP-Context 7 VALUE
NAS-Port-Type Wireless-CDMA2000 22 VALUE NAS-Port-Type Wireless-UMTS 23 VALUE NAS-Port-Type
Wireless-1X-EV 24 VALUE NAS-Port-Type IAPP 25 VALUE Framed-Protocol PPTP 9
```

Les VSAs de Cisco Airespace sur le serveur de RAYON de Microsoft IAS

Pour les informations sur la façon dont configurer un serveur de Service d'authentification Internet de Microsoft (MS IAS) pour prendre en charge les attributs de particularité de constructeur de Cisco Airespace (les VSAs) lisez les VSAs de Cisco Airespace sur l'exemple de configuration du serveur RADIUS de MS IAS

Les VSAs de Cisco Airespace sur le serveur de Cisco Secure ACS

L'engine de solution de version 4.0 de Cisco Secure Access Control Server, prend en charge beaucoup d'attributs de Remote Access Dial-In User Service (RAYON) qui incluent des attributs de Cisco Airespace.

ACS ne peut pas offrir le support partiel de l'IETF. Par conséquent, quand vous ajoutez un périphérique de Cisco Airespace (dans la configuration réseau), il active automatiquement tous les attributs IETF. Cette table donne à Cisco Airespace des attributs pris en charge par Cisco ACS.

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
1	Aire-WLAN-Id	Name of the user being authenticated.	Integer	Outbound	No
2	Aire-QoS-Level	Enumerations: 3: Bronze 0 : Silver 1 : Gold 2 : Platinum	Integer	Outbound	No
3	Aire-DSCP	—	Integer	Outbound	No
4	Aire-802.1P-Tag	—	Integer	Outbound	No
5	Aire-Interface-Name	—	String	Outbound	No
6	Aire-ACL-Name	—	String	Outbound	No

Les périphériques de Cisco Airespace prennent en charge quelques attributs IETF pour le réseau d'identité de 802.1x :

- Tunnel-type (64)
- Tunnel-Support-type (65)
- Tunnel-Privé-Groupe-id (81)

Afin de configurer un attribut spécifique à envoyer pour un utilisateur, vous devez assurer cela :

- Dans la section de configuration réseau, vous devez configurer l'entrée de client d'AAA qui correspondent au périphérique d'accès qui accorde l'accès au réseau à l'utilisateur pour utiliser un grand choix de RAYON qui prend en charge l'attribut que vous voulez envoyé à l'AAA le client.
- Dans la section de configuration d'interface, vous devez activer l'attribut de sorte qu'il apparaisse aux pages de profil d'utilisateur ou de groupe d'utilisateurs. Vous pouvez activer les attributs à la page qui correspondent à la variété de RAYON qui prend en charge l'attribut. Par exemple, l'attribut de session-timeout de RAYON IETF (27) apparaît à la page du RAYON (IETF).**Remarque:** Par défaut, des attributs RADIUS de par-utilisateur ne sont pas activés (ils n'apparaissent pas dans la page de configuration d'interface). Avant que vous puissiez activer des attributs sur une base par utilisateur, vous devez activer l'option d'attributs du Par-utilisateur TACACS+/RADIUS sur la page options avancée dans la section de configuration d'interface. Après l'activation des attributs de par-utilisateur, une colonne d'utilisateur apparaît comme désactivé dans la page de configuration d'interface pour cet attribut.
- Dans le profil que vous utilisez pour contrôler des autorisations pour l'utilisateur — dans l'utilisateur ou le groupe éditez les pages ou la page composante partagée d'autorisation

RADIUS — vous devez activer l'attribut. Quand vous activez cet attribut, il fait envoyer ACS l'attribut au client d'AAA dans le message d'Access-recevoir. Dans les options qui sont associées avec l'attribut, vous pouvez déterminer la valeur de l'attribut qui est envoyé au client d'AAA.

Référez-vous à la section d'attributs RADIUS du guide utilisateur pour le pour en savoir plus de l'engine 4.0 de solution de Cisco Secure ACS.

Vérifiez et dépannez

Quand l'utilisateur se connecte au WLAN un user-id et mot de passe, le WLC passe les qualifications au serveur de RAYON qui authentifie l'utilisateur contre aux conditions et au profil utilisateur configurés. Si l'authentification de l'utilisateur est réussie, le serveur de RAYON renvoie un RAYON reçoivent la demande qui contient également les attributs RADIUS configurés pour cet utilisateur. Dans cet exemple, la stratégie QoS de l'utilisateur est retournée.

Vous pouvez émettre le **debug aaa toute la** commande d'**enable** afin de voir la séquence d'opérations qui se produisent pendant l'authentification. Voici un exemple de sortie :

```
(Cisco Controller) >debug aaa all enable Wed Apr 18 18:14:24 2007: User admin authenticated Wed
Apr 18 18:14:24 2007: 28:1f:00:00:00:00 Returning AAA Error 'Success' (0) for mobile
28:1f:00:00:00:00 Wed Apr 18 18:14:24 2007: AuthorizationResponse: 0xbadff97c Wed Apr 18
18:14:24 2007: structureSize.....70 Wed Apr 18 18:14:24 2007:
resultCode.....0 Wed Apr 18 18:14:24 2007:
protocolUsed.....0x00000008 Wed Apr 18 18:14:24 2007:
proxyState..... 28:1F:00:00:00:00-00:00 Wed Apr 18 18:14:24 2007: Packet
contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-Type..... 0x00000006
(6) (4 bytes) Wed Apr 18 18:14:24 2007: AVP[02] Airespace / WLAN-Identifier..... 0x00000000 (0)
(4 bytes) Wed Apr 18 18:14:24 2007: User admin authenticated Wed Apr 18 18:14:24 2007:
29:1f:00:00:00:00 Returning AAA Error 'Success' (0) for mobile 29:1f:00:00:00:00 Wed Apr 18
18:14:24 2007: AuthorizationResponse: 0xbadff97c Wed Apr 18 18:14:24 2007:
structureSize.....70 Wed Apr 18 18:14:24 2007:
resultCode.....0 Wed Apr 18 18:14:24 2007:
protocolUsed.....0x00000008 Wed Apr 18 18:14:24 2007:
proxyState..... 29:1F:00:00:00:00-00:00 Wed Apr 18 18:14:24 2007:
Packet contains 2 AVPs: Wed Apr 18 18:14:24 2007: AVP[01] Service-Type.....
0x00000006 (6) (4 bytes) Wed Apr 18 18:14:24 2007: AVP[02] Airespace / WLAN-Identifier.....
0x00000000 (0) (4 bytes) Wed Apr 18 18:15:08 2007: Unable to find requested user entry for User-
VLAN10 Wed Apr 18 18:15:08 2007: AuthenticationRequest: 0xa64c8bc Wed Apr 18 18:15:08 2007:
Callback.....0x8250c40 Wed Apr 18 18:15:08 2007:
protocolType.....0x00000001 Wed Apr 18 18:15:08 2007:
proxyState..... 00:40:96:AC:E6:57-00:00 Wed Apr 18 18:15:08 2007:
Packet contains 8 AVPs (not shown) Wed Apr 18 18:15:08 2007: 00:40:96:ac:e6:57 Successful
transmission of Authentication Packet (id 26) to 172.16.1.1:1812, proxy state 00:40:96:ac:e6:57-
96:ac Wed Apr 18 18:15:08 2007: 00000000: 01 1a 00 68 00 00 00 00 00 00 00 00 00 00 00 00
...h..... Wed Apr 18 18:15:08 2007: 00000010: 00 00 00 00 01 0d 55 73 65 72 2d 56 4c 41
4e 31 ......User-VLAN1 Wed Apr 18 18:15:08 2007: 00000020: 30 02 12 fa 32 57 ba 2a ba 57 38 11
bc 9a 5d 59 0...2W.*.W8...]Y Wed Apr 18 18:15:08 2007: 00000030: ed ca 23 06 06 00 00 00 01 04
06 ac 10 01 1e 20 ..#..... Wed Apr 18 18:15:08 2007: 00000040: 06 57 4c 43 32 1a 0c 00
00 37 63 01 06 00 00 00 .WLC2....7c..... Wed Apr 18 18:15:08 2007: 00000050: 01 1f 0a 32 30 2e
30 2e 30 2e 31 1e 0d 31 37 32 ...20.0.0.1..172 Wed Apr 18 18:15:08 2007: 00000060: 2e 31 36 2e
31 2e 33 30 .16.1.30 Wed Apr 18 18:15:08 2007: 00000000: 02 1a 00 46 3f cf 1b cc e4 ea 41 3e 28
7e cc bc ...F?.....A>(~.. Wed Apr 18 18:15:08 2007: 00000010: 00 e1 61 ae 1a 0c 00 00 37 63 02
06 00 00 00 03 ..a.....7c..... Wed Apr 18 18:15:08 2007: 00000020: 06 06 00 00 00 01 19 20 37
d0 03 e6 00 00 01 37 .....7.....7 Wed Apr 18 18:15:08 2007: 00000030: 00 01 ac 10 01 01 01
c7 7a 8b 35 20 31 80 00 00 .....z.5.1... Wed Apr 18 18:15:08 2007: 00000040: 00 00 00 00 00
1b ..... Wed Apr 18 18:15:08 2007: ****Enter processIncomingMessages: response code=2 Wed Apr
18 18:15:08 2007: ****Enter processRadiusResponse: response code=2 Wed Apr 18 18:15:08 2007:
00:40:96:ac:e6:57 Access-Accept received from RADIUS server 172.16.1.1 for mobile
```

```
00:40:96:ac:e6:57 receiveId = 0 Wed Apr 18 18:15:08 2007: AuthorizationResponse: 0x9802520 Wed
Apr 18 18:15:08 2007: structureSize.....................114 Wed Apr 18 18:15:08 2007:
resultCode.....................0 Wed Apr 18 18:15:08 2007:
protocolUsed.............0x00000001 Wed Apr 18 18:15:08 2007:
proxyState..... 00:40:96:AC:E6:57-00:00 Wed Apr 18 18:15:08 2007: Packet
contains 3 AVPs: Wed Apr 18 18:15:08 2007: AVP[01] Airespace / QOS-Level..... 0x00000003 (3)
(4 bytes) Wed Apr 18 18:15:08 2007: AVP[02] Service-Type.................. 0x00000001 (1) (4
bytes) Wed Apr 18 18:15:08 2007: AVP[03] Class..... DATA (30 bytes) Wed Apr 18
18:15:08 2007: 00:40:96:ac:e6:57 Applying new AAA override for station 00:40:96:ac:e6:57 Wed Apr
18 18:15:08 2007: 00:40:96:ac:e6:57 Override values for station 00:40:96:ac:e6:57 source: 48,
valid bits: 0x3 qosLevel: 3, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1
dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1 vlanIfName: '', aclName: ' Wed Apr 18
18:15:12 2007: AccountingMessage Accounting Start: 0xa64c8bc Wed Apr 18 18:15:12 2007: Packet
contains 13 AVPs: Wed Apr 18 18:15:12 2007: AVP[01] User-Name..... User-
VLAN10 (11 bytes) Wed Apr 18 18:15:12 2007: AVP[02] Nas-Port.....
0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[03] Nas-Ip-Address.....
0xac10011e (-1408237282) (4 bytes) Wed Apr 18 18:15:12 2007: AVP[04] NAS-
Identifier..... 0x574c4332 (1464615730) (4 bytes) Wed Apr 18 18:15:12 2007:
AVP[05] Airespace / WLAN-Identifier..... 0x00000001 (1) (4 bytes) Wed Apr 18 18:15:12 2007:
AVP[06] Acct-Session-Id..... 4626602c/00:40:96:ac:e6:57/16 (29 bytes) Wed Apr 18
18:15:12 2007: AVP[07] Acct-Authentic..... 0x00000001 (1) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[08] Tunnel-Type..... 0x0000000d (13) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[09] Tunnel-Medium-Type..... 0x00000006 (6) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[10] Tunnel-Group-Id..... 0x3230 (12848) (2 bytes) Wed Apr 18
18:15:12 2007: AVP[11] Acct-Status-Type..... 0x00000001 (1) (4 bytes) Wed Apr 18
18:15:12 2007: AVP[12] Calling-Station-Id..... 20.0.0.1 (8 bytes) Wed Apr 18 18:15:12
2007: AVP[13] Called-Station-Id..... 172.16.1.30 (11 bytes)
```

Cet utilisateur prouve que l'utilisateur est authentifié. Puis, des valeurs de priorité d'AAA sont retournées avec le RAYON reçoivent le message. Dans ce cas, vous voyez que l'attribut de QoS est retourné avec le RAYON reçoivent le message. Par conséquent, l'utilisateur est donné la stratégie QoS du bronze qui ignore la valeur de QoS par défaut réglée pour ce SSID.

Informations connexes

- Exemple de configuration d'attributs VSA Cisco Airespace sur un serveur Radius IAS Microsoft
- Guide de configuration du contrôleur LAN sans fil Cisco, version 4.1
- Page de prise en charge du mode sans fil
- Support et documentation techniques - Cisco Systems