

رADIUS كېلىش رايونى قاتارلىق سىياسەت

تایوت حملہ

مقدمہ

تظحو ل يتلا ضارعا

عَبْقَارِ مِلِّل RADIUS زَاهِجْ عَاداً 1.

2. Msglogs راجع ٻڌائڻ ۽ RADIUS راجع ٺاهڻ ۽ WLC رٿ 2.

3. AAA عا ط خ أ ل ا ح ي ح ص ت

4. بيجتي سي الوادج لوغشم RADIUS مداخل

تاس رام مل لاض فاً ط پ ض

WLC پنجاه طباض

ةمدقملا

رشنل تاي لمعل ةي ساسأل ني وكتل تاداشرا ىل ةرصتخم ةماع ةرطن دنتسمل اذه مدقي (WLC) ةي كللسال ةي لم ةكبشلا يف مكحتل ةدحولثم قاطنل ةعساو ةي كللسال لوصول يف مكحتل مداخ وأ Cisco نم (ISE) ةي وهل تامدخ كرحم مادختساب RADIUS عم AireOS ركبك ةي نف لي صافت تاذ رخأ تادنتسم ىل دنتسمل اذه ريشي Cisco نم (ACS) نملال

تظحول يتل اضارعالا

فصلي. هذه (AAA) عېساحمل او ضيوف تال او عقد اصم الراي هنا ؤلا ح تاع م ا ج ل ا تائيب هجاوت ام ؤءاع ؤئيب ل هذه في اهتدهاشم متت يتل ؤءات عمل تال ج سل / ا ضار ؤال مسقل اذه

1. رقبہ اور ملل RADIUS زاہج عاذاً

ةقداصم للالواحمل نم ديدعل عم اريبك اريخأت Dotx لي مع هجاوي

نع شحب لل (RADIUS م داوخ > تاي ئاصح | > عبقارم : GUI) show radius auth statistics رمل آل مدخ تسأ
ءاهتنا تالاح و ضفرل او ةل و احم الم ةءاع | تاي لمم نم ةري ب ةءاع نع صاخ لك شب شحبا . لك اشمل
الاثم لي امي ف . ةلهمل

```

Server Index..... 2
Server Address..... 192.168.88.1
Msg Round Trip Time..... 3 (msec)
First Requests..... 1256
Retry Requests..... 5688
Accept Responses..... 22
Reject Responses..... 1
Challenge Responses..... 96
Malformed Msgs..... 0

```

```

Bad Authenticator Msgs..... 0
Pending Requests..... 1
Timeout Requests..... 6824
Unknowntype Msgs..... 0
Other Drops..... 0

```

نوع ثحب:

- (10% نم رثكأ نوكت الأ بجي) ىلوالأ بللطلأ ةبسن: ةيلالال ةلواحلل ةداعإ
- ةبسنلأ لوبق: يلالال ضفرلأ
- (5% نم رثكأ نوكت الأ بجي) ىلوالأ بللطلأ ةبسن: ةيلالال ةلهم

يلي امم ققحتف، لكاشم كانه تناك اذا

- حيحص ريغ لكشب مهنويوكت مت عالمع
- ةيلحملل ةكبشلل ي ف مكحتلأ رصنع ني ب ةكبشلل ىلأ لوصولل ةيناكلما تالكشم
- RADIUS مداخلو (WLC) ةيكلساللأ
- ،مادختسالل دي ق تناك اذا، ةيفللأل ةياملل تاناي ب ةدعاقو RADIUS مداخل ني ب لكاشملل
- Active Directory (AD) عم لثم

2. Msglogs ىل عئلتمم RADIUS راطتنا ةمئاق WLC ىرت

راظتنا ةمئاق لوح ةلاسزلل هذه ةيكلسالل ةيلحملل ةكبشلل ي ف مكحتلأ ةدحو ىقللت
RADIUS:

```

Univ-WISM2-02: *aaa QueueReader: Dec 02 14:25:31.565: #AAA-3-3TXQUEUE_ADD_FAILED:
radius_db.c:889 Transmission queue full. Que name: Radius queue. Dropping
sessionpackets.
host = x.x.x.x.

```

3. AAA ءاطخالأ حيحصت

ةلاسزلل هذه AAA ءاطخالأ حيحصت ضرعي

```

*aaaQueueReader: Dec 02 21 09:19:52.198: xx:xx:xx:xx:xx:xx Returning AAA Error
'Out of Memory' (-2) for mobile xx:xx:xx:xx:xx:xx

```

AAA مداخل ىلأ لوصولل رذعتي. ةلومحملل ةزهجالل (-5) AAA أطخ ةلهم AAA ءاطخالأ حيحصت عجري
ل. يملل ليوخت ءاغلأ هعبتيو

4. بيحتسي الو ادج لوغشم RADIUS مداخل

لجسلل ماظنل ةينمزلل بكارتل يلي امي فو

```

0 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
1 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
2 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
3 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
4 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 unavailable
5 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 failed to respond to request
  (ID 22) for client 68:96:7b:0e:46:7f / user 'user1@univ1.edu'
6 Wed Aug 20 15:29:57 2014 User Larry_Dull_231730 logged Out. Client MAC:84:a6:c8:
  87:13:9c, Client IP:198.21.137.22, AP MAC:c0:7b:bc:cf:af:40, AP Name:Dot1x-AP
7 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
  (ID 183) for client 48:d7:05:7d:93:a5 / user ' user2@univ2.edu '
8 Wed Aug 20 15:28:42 2014 RADIUS auth-server x.x.x.x:1812 unavailable
9 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
  (ID 154) for client 40:0e:85:76:00:68 / user ' user1@univ1.edu '
10 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 available
11 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 unavailable
12 Wed Aug 20 15:28:41 2014 RADIUS server x.x.x.x:1812 failed to respond to request
  (ID 99) for client 50:2e:5c:ea:e4:ba / user ' user3@univ3.edu '
13 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
14 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
15 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 failed to respond to request
  (ID 30) for client b4:18:d1:60:6b:51 / user ' user1@univ1.edu '
16 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
17 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
18 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
19 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable

```

تاسرامال لضفا طبض

WLC بناج طبض

- لمعي 802.1X ليمع اناثتسا لعجا - (EAP) عسوتمال عقداصمال لوكوتورب
- 802.1X ل ماع لكشب عالعمل اناثتسا نيكم ت
- ةيكلساللا ةيلحمل 802.1X تاكبش ىلع ليمعلا اناثتسا نييعتب مق
- لقالا ىلع ةيئاث 120 ىلإ (WLANs)
- [ىلع 802.1X ليمع اناثتسا](#) يف حضوم وه امك EAP تيقتو تادحو نييعتب مق
- [AireOS WLC](#) لاقم

- لقالا ىلع يئاوث ةسمخ ىلع RADIUS لاسرا ةداعا تارتف طبضا
- لقالا ىلع تاغاس ينامث ىلإ لمعلا ةسلج ةلهم نييعت
- نأ فرصتلا ءوسل دحاو بلاطمل حمسي ال يذلاو، ديدشلا لشفلا زواجت لي طعتب مق
- RADIUS مداوخ نيب WLC لشف يف ببستي
- كئالمعل عيرسلا نمآلا لواجتلا نيوكتب مق
- 2 Wi-Fi Protected Access نومدختسي Microsoft Windows EAP عالمع نأ نم دكأت

تقوم ال نيزختل ا ماذختس ا مهنكمي ى تح (AES) مدقتم ال ري فشتل ا راي عم (WPA2) (OKC) يزاهتن ال ا حت فم لل

◦ مه ب ة صا ال WLAN ة كبش ن ع Apple iOS ا لم ع ل ص ف ع ي ط ت س ت ت ن ك ا ذا
ك لت WLAN ة كبش ى ل ع 802.11r ن ي ك م ت ك ن ك م ي ف

◦ ة ي ل ح م ة كبش ي ا ل (CCKM) Cisco ن م ة ي ز ك ر م ل ا ح ي ت ا ف م ل ا ة ر ا د ا ن ي ك م ت ب م ق
ي ا ى ل ع CCKM ن ي ك م ت ب م ق ت ا ل ا ه ن ك ل و 792x ف ت ا و ه م ع د ت (WLAN) ة ي ك ل س ا ل
ن و ل ي م ي م ه ن ا ل ، Android و Microsoft Windows ا لم ع م ع د ي (SSID) ة م د خ ة و م ج م ف ر ع م
(ة ي ل ا ك ش ا CCKM ت ا ق ي ب ط ت د و ج و ى ل ا

◦ WLAN EAP ة كبش ي ا ل (SKC) ق ص ا ل ا ل ا حت ف م ل ل ت ق و م ل ن ي ز خ ت ل ن ي ك م ت ب م ق
Android ا لم ع و ا / و X (Mac OS) م ا ق ي ف Macintosh ل ي غ ش ت ل ا م ا ط ن م ع د ت

ن م ا ل ا ل ا و ج ت ل ا و 802.11 (WLAN) ة ي ك ل س ا ل ا ة ي ل ح م ل ا ة كبش ل ا ر ب ع ل ا و ج ت ل ا ع ج ا ر
ت ا م و ل ع م ل ن م د ي ز م ى ل ع ل و ص ح ل ل CUWN ى ل ع ع ي ر س ل ل ا

ر ي غ ي س ي ئ ر ل ا حت ف م ل ل ت ق و م ل ن ي ز خ ت ل ا ة ر ك ا ذ م ا ذ خ ت س ا ب ق ا ر : ة ط ح ا ل م
show pmk-cache ر م ا ل ا م ا ذ خ ت س ا ب ة و ر ذ ل ا ت ا ق و ا ي ف ك ب ص ا خ ا ل (PMK) م ي ك ح ل ا
و ا PMK ل ت ق و م ل ن ي ز خ ت ل ا ة ر ك ا ذ م ج ح ل ى ص ق ا ل ا د ح ل ا ى ل ا ت ل ص و ا ذا all.
SKC ل ي ط ع ت ى ل ا ج ا ت ح ت ن ا ل م ت ح م ل ن م ف ، ا ه ن م ت ب ر ت ق ا

◦ ن م DHCP/HTTP ط ي م ن ت م ا ذ خ ت س ا ك ي ل ع ف ، ط ي م ن ت ل ا ع م ISE م د خ ت س ت ت ن ك ا ذا
ة ب س ا ح م ة م ز ح ي ف ت ا ف ل م ل ا ا ش ن ا ت ا ن ا ي ب ن ي م ص ت ى ل ا ي د و ي ا ذ ه و WLC ب ن ا ج
ة ط ق ن ت ا ن ا ي ب ع ي م ج ل و ص و ن م ص ي ا م م ، ل ا م ح ا ل ا ة ن ز ا و م ة ل و ه س ب م س ت ت RADIUS
ا ه س ف ن (PSN) ة م ا ع ل ا ت ا م د خ ل ا ة كبش ى ل ا ة ي ا ه ن ل ا

◦ ت ا م د خ ل ا ه ي ل ا ة ج ا ح ب ن ك ت م ل ا م ة ت ق و م ل ا ة ب س ا ح م ل ا ل ي غ ش ت ف ا ق ي ا ن م د ك ا ت
ى و س ف ي ص ت ا ل ة ت ق و م ل ا ة ب س ا ح م ل ا ن ا ف ا ل و . ت ي ا ب ل ا ى ل ا ة د ن ت س م ل ا ة ر ت و ف ل ا
ة ي ف ا ض ا ة د ئ ا ف ة ي ا ن و د ل م ع ل م ح

◦ WLC ز م ر ل ل ض ف ا ل ي غ ش ت

م دا خ ل ا ب ن ا ج ن م RADIUS ة ف ل ا و م

◦ ل و ح ن ي و ك ت ل ل ة ل ب ا ق RADIUS م د ا و خ م ط ع م ن و ك ت . ل ي ج س ت ل ا ل د ع م ل ي ل ق ت
ر ا ي ت خ ا ل و و س م ل ل ن ك م ي ، ISE و ACS م ا ذ خ ت س ا ة ل ا ح ي ف . ه ن ز خ ت س ي ذ ل ا ل ي ج س ت ل ا
ا ذا ة ل ث م ا ل ا د ح ا ن و ك ي د ق و . ة ب ق ا ر م ل ا ت ا ن ا ي ب ة د ع ا ق ى ل ا ا ه ل ي ج س ت م ت ي ت ل ا ت ا ئ ف ل ا
ل ث م ر خ ا ق ي ب ط ت م ا ذ خ ت س ا ب ا ه ض ر ع و RADIUS م د ا خ ن م ة ب س ا ح م ل ا ت ا ن ا ي ب ل ا س ر ا م ت
ISE ى ل ع . ا ي ل ح م ت a n a y b a ل ة د ع ا ق ى ل ا T a n a y b a ل ة ب ا ت ك ب ك ل ذ د ع ب م ق ت a l f ، syslog
ض ا ر غ ا ل ه ل ي ط ع ت ب ج ي ن ا ك ا ذا . ت ا ق و ا ل ا ل ك ي ف ا ن ك م م ي ق ب ي ل ج س ل ا ح ب ك ن ا ن م د ك ا ت
> ل ي ج س ت ل a > م ا ط ن ل a > ة ر ا د ا ل ا ى ل ا ك ل ذ د ع ب ل ق ت ن ا ف ، ا ه ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا
ة ط ق ن ى ل ع ت ب ك ل ا ل ي ط ع ت ل ي ف ا ف ت ل a ل a ت ب ك ل ا ر ا ي خ م د خ ت س ا و ع ي م ج ت ل a ت ا ح ش ر م

نكمي، ثدحألا تارادصلإاو ISE نم 1.3 رادصلإا يف. دحاو مدختسم وأ ةيدرف ةياهن
قرشأبملا ةقداصلما لجس يف ةياهن ةطقن قوف نميألا سواملا رزب رقنلا
اضيأ عمقلا ليطعتل

◦ لوصولو لوكوتورب، AD) ضفخنم ةيفلخلا ةقداصلما إىل لوصولو نمز نأ نم دكأت
مدختست تنك اذا. ((Rivest، Shamir، Adleman (RSA)، LDAP) نزولا فيفخ ليلىلإ
لوصولو نمز ةبقارم لجأ نم ةقداصلما صخلم ريراقت ليغشت نكمي، ISE وأ ACS
نمزلوصولو نمز طسوتم نم لكل ةبسنلاب مداخلك ساسأ يلع مداخلكل
نكمي يذلا ةقداصلما لدعم لق، ام بلط ةجلاعم تقو لاطاملكو. يصولأ لوصولو
ةباجتسإ إىل يلاعلا لوصولو نمز عجري، تقولا نم 95%. هتجلاعم ISE وأ ACS ل
ةيفلخ تانايب ةدعاق نم ةئيطب

◦ يمحمل عسوتملا ةقداصلما لوكوتورب رورم ةملك ةلواحم ةداعإ تايلمع ليطعت
قفن لخاد رورملا ةملك لاخدا ةلواحم ةداعإ تايلمع ةزهجألا مظعم معدت ال. (PEAP)
ةداعإو زاهجلا ةباجتسإ فاقإ يف EAP مداخل نم ةلواحملا ةداعإ ببستت كلذل، PEAP
ةينمزل ةلهملا ءهتنا تالاح يف ببستي اذهو. ةديج EAP لمع ةسلجب هليغشت
اهيلى لوصولو متي نل ليملعلا تءانثتسإ نأ ينعي امم، صفرلا نم الدب EAP ل

◦ هنكلو ةيمهألا غلاب ارمأ سيل اذهو. ةمدختسملا ريغ EAP تالوكوتورب ليطعت
مادختسإ عيطتسي ال ليملعلا نأ نمضي و EAP لدابت إىل ةءافكلا ضعب فيضي
دوصقم ريغ وأ فيعض EAP بولسأ

◦ عيرسلا لاصتالا ةداعإو PEAP ةسلج فانئتسإ نيكمت

◦ ئطاخ نيوكت اذه. كلذل ةجاح كانه نكت مل اذا نالعلإا إىل MAC ةقداصلما لاسرا مدع
اهدض ةقداصلما اب ISE موقى يتلا لاجملا ب مكحتلا تادحو يلع لمحل ديذي عئاش
طسوتم نم ديزتو تقولا كلهتست ةيبلس شحب تايلمع إىل هذه يدؤت ام ابلاغو
لوصولو نمز

◦ (ددحم ISE) كلذ قبطنى امثي زاهجلا رعشتسم مدختسأ

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا