

فاشككتساو ةيچراخال TACACS م داوخ نيوكت ISE ىلع اهحالصاوا اهئااطخأ

تايتوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[نيوكتلا](#)

[ةكبش لىل يطيطختلا مسرلا](#)

[ISE نيوكت](#)

[ACS نيوكت](#)

[ةحصللا نم ققحتلا](#)

[اهحالصاوا ءاطخألا فاشككتسا](#)

ةمدقملا

مادختساب رشن ةيلمع يف يچراخال TACACS+ م داخ مادختسال ةزيملا دنتسملا اذه فصى
لجكوك (ISE) Identity Service Engine.

ةيساسألا تابلطتملا

تابلطتملا

- ISE ىلع ةزهجال ةرادل يساسألا مهفلا.
- ىلع قيبطتل لباقلا Identity Service Engine نم 2.0 رادصإلا ىل دنتسملا اذه دنتسي
2.0 نم ىلعأ Identity Service Engine نم رادصإ ي.

ةمدختسملا تانوكملا

م داخ ي اىل اعجرم نوكيل دنتسملا اذه يف ACS ىل اعجرم ي اىل ريسفت نكمي: **ةظالم**
م داخ ي اىل نيوكتلاو ACS ىل نيوكتلا فلختي دق، ك لذ عم و. يچراخ TACACS+
TACACS رخأ.

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإلا ىل دنتسملا اذه يف ةدراولا تامولعمل دنتست:

- Identity Service Engine 2.0

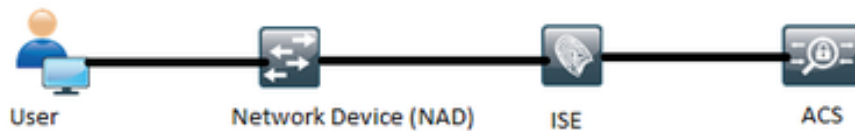
- لوصولاب مكحتلا ماظن (ACS) 5.7

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراولا تامولعمل عاشنإ مت
ت ناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسملا ةزهجال عيمج تادب
نيوكتلا يف رييغت يال لم تحملا ريثاتلل كمهف نم دكاتف، ةرشابم كتكتبش.

نېوكتال

ACS. لىل لىكولل TACACS+ تابلطل ISE نېوكت لىل مسقلا اذە دعاسى

ةكبشلل يطيختال مسرلا



ISE نېوكت

1. ةقداصل ملام ادختسا نكمىو ISE لىل ةددعتمال ةيخرال TACACS مداوخ نېوكت نكمى > لمعل زكارم لىل لقتنا، ISE لىل ةيخرال TACACS+ مداوخ نېوكت لجا نم. نىمدختس مال ةئبعت و ةفاضل قوف رقتنا. ةيخرال TACACS مداوخ > ةكبشلا دراوم > ةزهجال ةرادا ةيخرال مداخال لىل صافت.

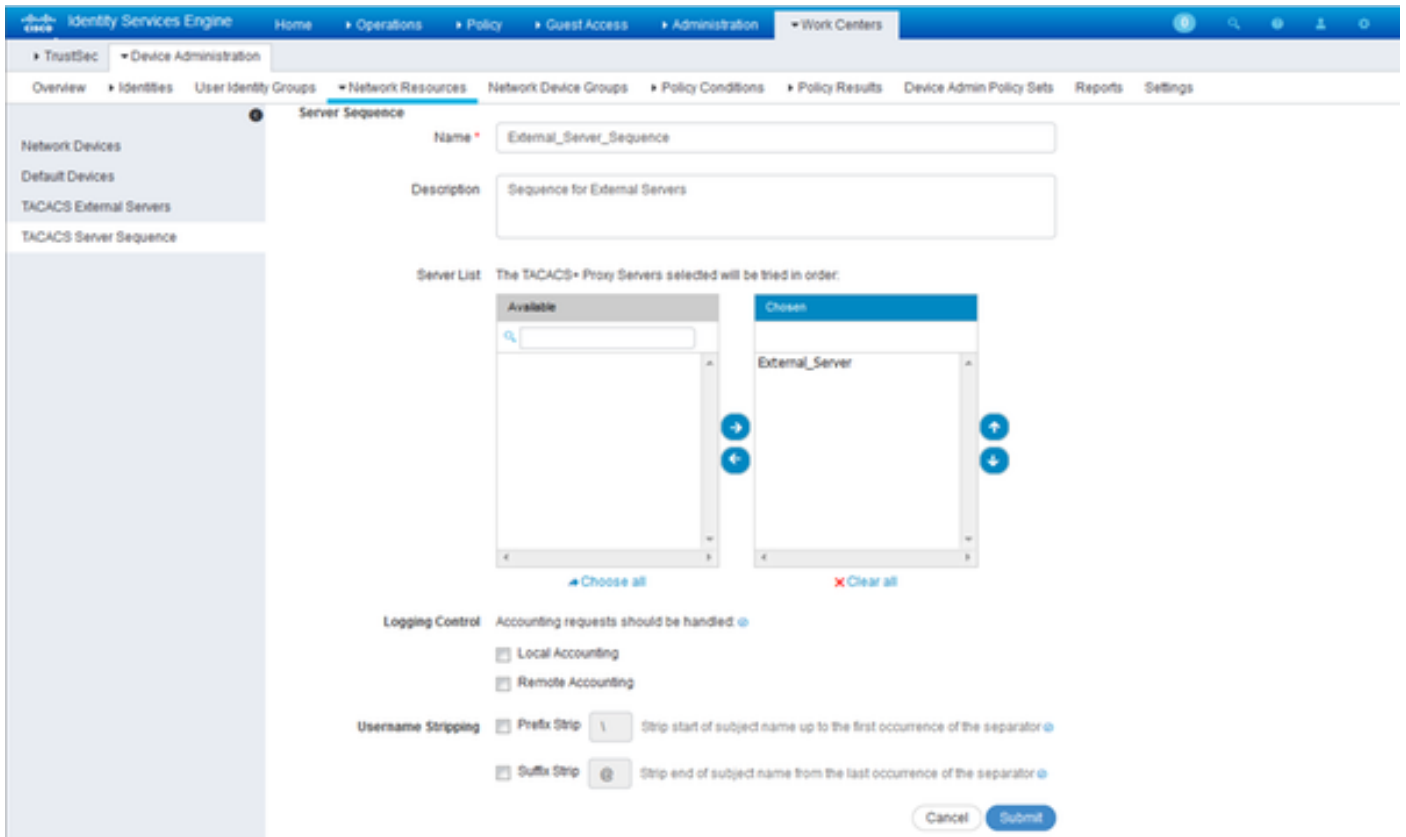
The screenshot shows the Cisco Identity Services Engine (ISE) configuration page for TACACS External Servers. The page is titled "TACACS External Servers > External_Server". The configuration fields are as follows:

- Name: External_Server
- Description: External TACACS Server
- Host IP: 10.127.196.237
- Connection Port: 49 (1-65,535)
- Timeout: 20 Seconds (1-999)
- Shared Secret: ***** (with a "Show Secret" button)
- Use Single Connect:

At the bottom of the page, there are "Cancel" and "Save" buttons.

ACS. فى مدختس مال رسلا هسفن وه مسقلا اذە فى رفوتمال كرتشمال رسلا نوكتى نأ بچى

2. مداخ لسلسلت فى هتفاضل بچى، هنىوكت مت يذلا ةيخرال TACACS مداخ مادختسال. لسلسلت لدان TACACS تلكش in order to. جهنل تاعومجم فى همدختسال TACACS قوف رقتنا. لسلسلت لدان TACACS > دروم ةكبش > ةرادا ةادأ > لمعل زكارم لىل لقتنا اذە فى اهمادختسال ةبولطمال مداخال رتخا لىل صافتال ةئبعت مق، ةفاضل لسلسلتال.

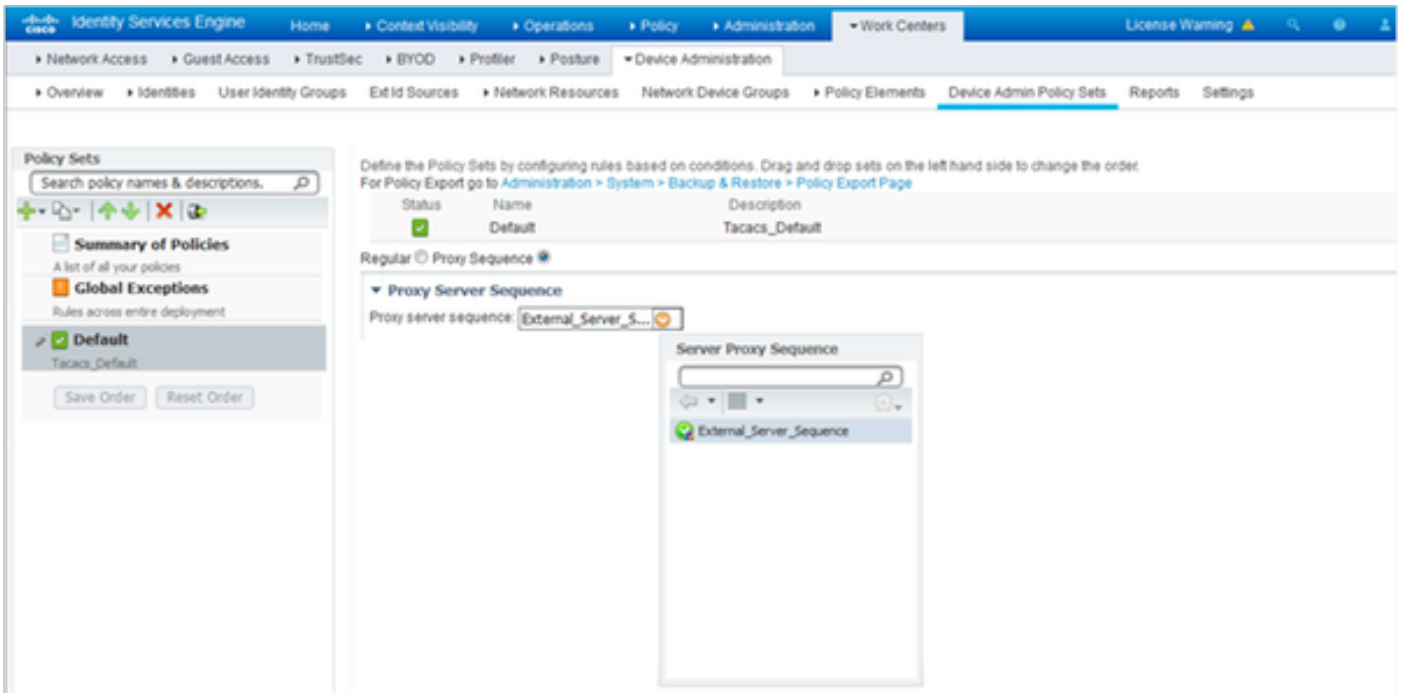


ةيرعتو وليجستللا في مكحتلا .نيرخا نيرايخ ريفوت مت ،مداخلا لسلسلتا لىل افاضالاب
مدختسملامسا

أ ISE لىل عايلحم ةبسااحملا تابلط ليجستللا اما ارايخ ليجستللا في مكحتلا يطعي
اضيا ةقداصملا عم لماعتا في ذللا يجراخلا مداخلا لىل ةبسااحملا تابلط ليجستللا

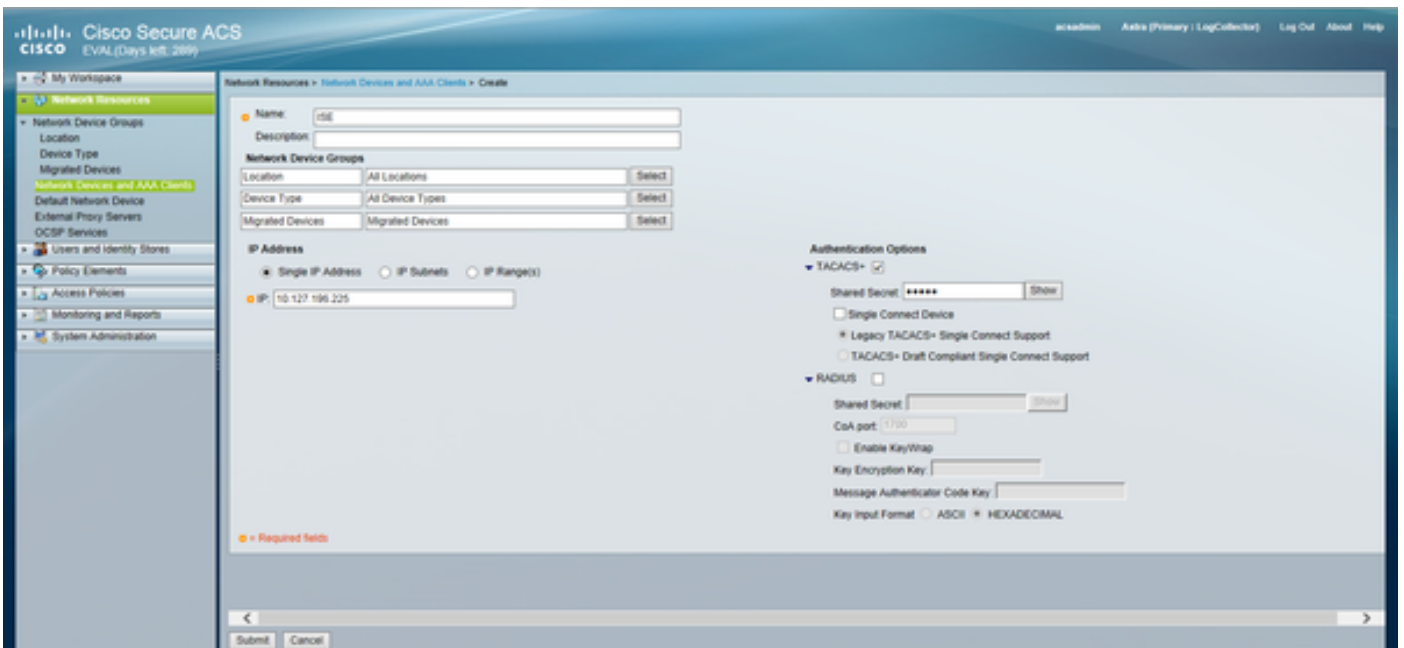
لبق ددحم ديدحت قيرط نع ةقحلالا وأ ةئدابلا بطشل مدختسملامسا ديخت مادختسا متي
يجراخ TACACS مداخلا لىل بلطلا هيجوت ةداعا

3. جهنلا تاعومجم نيوكت بجي ،هنيوكت مت يذلا يجراخلا TACACS مداخلا لسلسلتا مادختسالا
مادختسالا تاسايسالا تاعومجم نيوكتل .هؤاشن مت يذلا لسلسلتا مادختسالا
ةرادا تاسايسالا تاعومجم > ةزهجالا ةرادا > لمعلا زكارم لىل لقتنا ،يجراخلا مداخلا لسلسلتا
ليكولا لسلسلتا لوقي يذلا يكلسالا رزلا ليدبت .[تاسايسالا ةعومجم دح] > ةزهجالا
هؤاشن مت يذلا يجراخلا مداخلا لسلسلتا رتخا

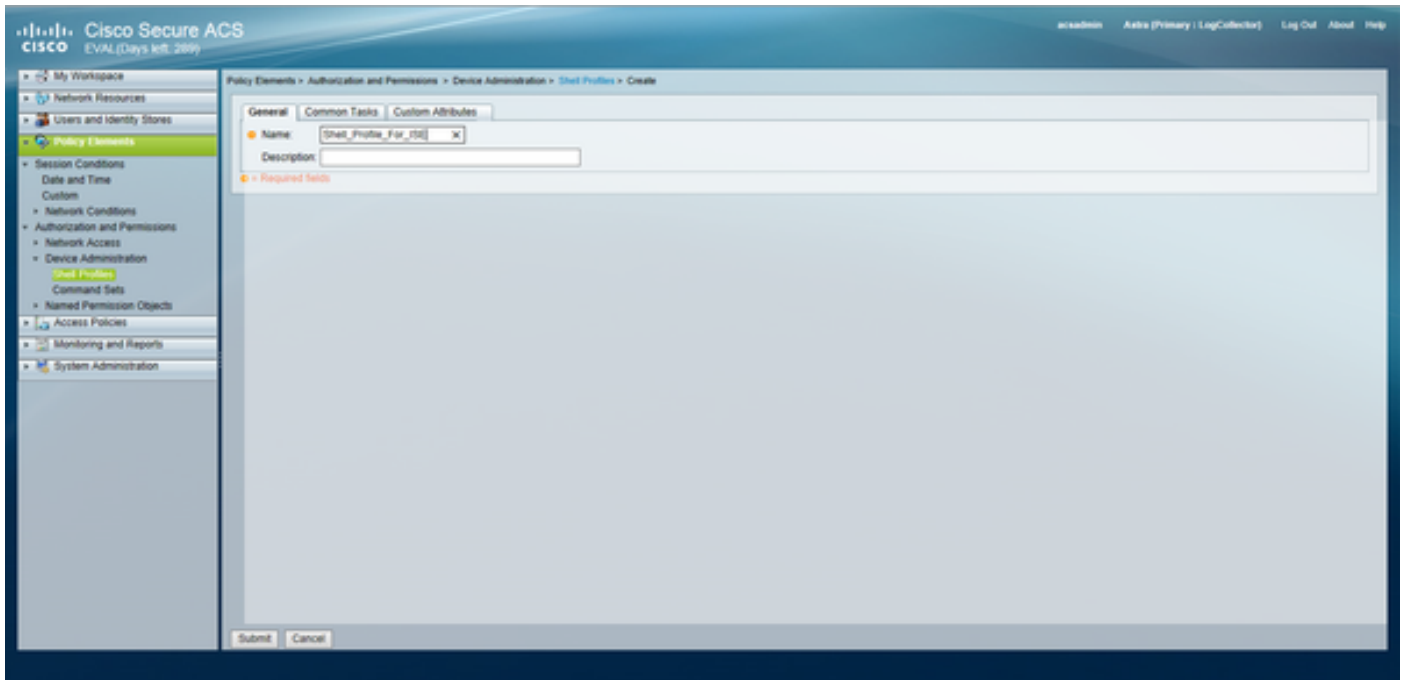


ACS نيوكت

ISE نيوكتل TACACS ب ل ط ل اس ر اب موقيس رخأ ةكبش زاهج درجم ISE دعي ، ACS ل ةبسن ل اب قوف رقنا AAA ءالمعو ةكبش ل ا ءزهجأ > ةكبش ل ا دراوم ل ا ل قتنا ، ACS ي ةكبش زاهجك ل ع هنيوكت مت امك كرتشم ل ا رس ل ا سفن مادختساب ISE م داخ ل ا ل صافات ةئبع ءو ءاشن ل ISE.



رم او ال ا ءاعوم جم و shell ءاف ي صوت و ءدوجوم ل ا ACS ل ع ءزهجأ ل ا ءراد ا ءامل عم نيوكت ب مق > ءزهجأ ل ا ءراد ا > ءانوذال او ل ي و ختل ا > جهنل ا رصانع ل ا ل قتنا ، Shell ءاف ي صوت نيوكتل ءص صخمل ا ءامل سل او ءكرتشم ل ا مامل او م سال ا نيوكت و ءاشن ل ا قوف رقنا Shell ءاف ي صوت ءاب ل ط ل ل ا قفو ء.



> زاهجلا قراد | > تانوذالاولي وختلا > جهنلا رصانع ىلا لقتنا ،رماوالا تاعومجم نيوكتل
بـلـطـمـلـا بـسـح لـيـصـاـفـتـلـا ةئبـعـتـو ءاـشـنـا قـوـف رـقـنا .رـمـاـوـالـا تـاعـومـجـم

General
 Name: Status:

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions
 Protocol:

Results
 Service:

دع اوق نيوكتل. تاب لطلتم لل اق فو ةمدخل دي دحت ةدع اق يف ةددحم لل لوصول ةمدخ نيوكتل مق
 > يضارت فال زاehl لوؤسم > لوصول تامدخ > لوصول تاسايس لى ل لقتنا ، لوصول ةمدخ
 دع اوق نيوكتل نمي . ةقداصم لل هم ادختس ا مزلي يذلا ةي وهال نزم دي دحت نمي شيح ةي وهال
 زاehl لوؤسم > لوصول تامدخ > لوصول تاسايس لى ل لقتنال لالخ نم لي وختل
 ضي وفتل > يضارت فال

كلذو ةني عم ةزهج أب ةصاخال shell تاهجاوولي وختل تاسايس نيوكتل فلتيخي دق : ةظالم
 دننتسم الا اذه قاطن جراخ

ةحصلا نم ققحتل

جيحص لكشب لمعي نيوكتل نا نم دكأتلل مسقلا اذه مدختس ا

لى ل ديؤيس ACS و ISE نيوكتل يف أطخ ي ا. ACS و ISE نم لك لىل ةحصلا نم ققحتل نمي و
 ةقداصم لل تاب لطل ةجل اع م لىل و تيس يذلا يساسا ل م داخال وه ACS . ةقداصم لل لش ف
 امب . تاب لطل ليكوك لمعي امك ، هنم و ACS م داخ هاجت ةي لوؤسم لل ISE لمحتي و ، ضي وفتل او
 نا نمي لي وختل بلط و ةقداصم لل نم ققحتل ل ا ف ، ني م داخال الك لالخ نم ربعت ةمزل نا

نېم داخال الك ىل ع متې.

ل صي يلات ل ا ب و ACS س ي ل و TACACS م داخ ك ISE م ا د خ ت س ا ب ة ك ب ش ل ل ا ة ز ه ج ا ن ي و ك ت م ت ي ة ج ا ح ب ب ل ل ط ل ا ن ا ك ا ذ ا م ISE ر ر ق ي ، ا ه ن ي و ك ت م ت ي ت ل ا د ع ا و ق ل ل ا ل ا ا د ا ن ت س ا و ، ا ل و ISE ل ل ب ل ل ط ل ا ل ل ع TACACS Live ت ا ل ج س ي ف ا ر ج ا ل ا ا ذ ه ن م ق ق ح ت ل ا ن ك م ي . ي ج ر ا خ م دا خ ل ل ا ه ه ي ج و ت ة د ا ع ل ل ISE.

ة ر ش ا ب م ل ا ت ا ل ج س ل ا > TACACS > ت ا ي ل م ع ل ا ل ل ل ق ت ن ا ، ISE ل ل ع ة ر ش ا ب م ل ا ت ا ل ج س ل ا ض ر ع ل ن ي ع م ب ل ط ل ل ي ص ا ف ت ة ع ج ا ر م ن ك م ي و ة ح ف ص ل ا ه ذ ه ل ل ع ة ر ش ا ب م ل ا ر ي ر ا ق ت ل ا ة د ه ا ش م ن ك م ي ة . م ه ا ل ا ي ذ د ح م ل ا ب ل ل ط ل ا ك ل ذ ب ق ل ع ت م ل ا ة ر ب ك م ل ا ة س د ع ل ل ز م ر ق و ف ر ق ن ل ا ب

Steps

- 13020 Get TACACS+ default network device setting
- 13013 Received TACACS+ Authentication START Request
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - Network Access.Protocol
- 15006 Matched Default Rule
- 13064 TACACS proxy received incoming request for forwarding.
- 13065 TACACS proxy received valid incoming authentication request.
- 13063 Start forwarding request to remote TACACS server.
- 13074 Finished to process TACACS Proxy request.
- 13020 Get TACACS+ default network device setting
- 13014 Received TACACS+ Authentication CONTINUE Request
- 13064 TACACS proxy received incoming request for forwarding.
- 13065 TACACS proxy received valid incoming authentication request.
- 13071 Continue flow (seq_no > 1).
- 13063 Start forwarding request to remote TACACS server.
- 13074 Finished to process TACACS Proxy request.

ل ي غ ش ت ل ا ء د ب ة ب ق ا ر م > ر ي ر ا ق ت ل ا و ة ب ق ا ر م ل ا ل ل ل ق ت ن ا ، ACS ل ل ع ة ق د ا ص م ل ا ر ي ر ا ق ت ض ر ع ل ة ب س ا ح م ل ا و ض ي و ف ت ل ا و ة ق د ا ص م ل ا ل و ك و ت و ر ب > ر ي ر ا ق ت ل ا و ة ب ق ا ر م ل ا > ر ي ر ا ق ت ل ا ض ر ا ع و ة ن و ق ي ا ق و ف ر ق ن ل ا ب ن ي ع م ب ل ط ل ل ي ص ا ف ت ة ع ج ا ر م ن ك م ي ، ISE ل ل م . TACACS ة ق د ا ص م > ة م ه ا ه ل ي ذ ل د ح م ل ا ب ل ل ط ل ا ك ل ذ ب ق ل ع ت م ل ا ة ر ب ك م ل ا ة س د ع ل ل

Steps
Message
Received TACACS+ Authentication START Request
Evaluating Service Selection Policy
Matched rule
Selected Access Service - Default Device Admin
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
TACACS+ will use the password prompt from global TACACS+ configuration.
Returned TACACS+ Authentication Reply
Received TACACS+ Authentication CONTINUE Request
Using previously selected Access Service
Evaluating Identity Policy
Matched Default Rule
Selected Identity Store - Internal Users
Looking up User in Internal Users IDStore - external
Found User in Internal Users IDStore
Authentication Passed
Evaluating Group Mapping Policy
Evaluating Exception Authorization Policy
No rule was matched
Evaluating Authorization Policy
Matched Default Rule
Returned TACACS+ Authentication Reply

اهحال صاوا عااطخاا فاشكتسا

اهحال صاوا نيوكتلا عااطخاا فاشكتسا ال اهم ادختسا كنكمي تامولعم مسقلا اذ رفوي

1. اا ريشت انا ف، لكشلا يف ءحضوملا ااطخالا لاسر ISE ىلع ريرقتلا ليصافت ترهظاا اذ. اا (NAD) ءكبشلا زاا و ISE ىلع هنيوكت مت حلص ريغ كرتشم رس

Message Text

TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. مدختسملا لوصو صرف متي نكلو ISE ىلع بلطل ءقداصم ريرقت دووو مدع ءلاا يف. رومأ ءدع ىلا ءداع كلذ ريشي، ءكبشلا زاا ىلا انا

- ISE مداخ ىلا هسفن بلطل لصي مل.
- ىلا TACACS+ نم بلط يا ااقسا متيسف، ISE ىلع ءزهالا ءرادا صخش ليطعت مت اذ. Live تالاس و ا ريراقتلا يف كلذ سفن ىلا ريشت تالاس يا ضرع متي نل. تم صب ISE ظحالو ريرحت قوف رقنا. [ءدقءلا دء] > رشن > ماظن > ءرادا ىلا لقتنا، كلذ نم ققحتلل وه امك ءماعلا تاداءءلا بيوبتلا ءمالع لفسا "ءزهالا ءرادا ءمدخ نيكم ت رايءخال ءناخ ISE ىلع "ءزهالا ءرادا" لمعت يكل هءه رايءخال ءناخ نم ققحتلا بءي. لكشلا يف ءحضوم

Personas

Administration Role **PRIMARY** Make Standalone

Monitoring Role PRIMARY Other Monitoring Node

Policy Service

Enable Session Services Include Node in Node Group None

Enable Profiling Service

Enable Threat Centric NAC Service

Enable SXP Service Use Interface GigabitEthernet 0

Enable Device Admin Service

Enable Passive Identity Service

pxGrid

- عي مج طاقس ا متيسف ،هتي حالص دم ا هتنا دعب ادوجوم زا هجلا ةرادا صيخرت نكي مل اذا ل ةيموسرلا مدختسملا هجاويف تالجس يا ضرع متي ال .تم صب TACACS+ تابلط زا هجلا ةرادا صيخرت نم ققحتلل صيخرت > ماظن > ةرادا ل لقتنا .هسفن

Licenses How do I register/modify or lookup my licenses?

License File	Quantity	Term	Expiration Date
EVALUATION.lic			
Base	100	90 days	22-Jan-2017 (43 days remaining)
Plus	100	90 days	22-Jan-2017 (43 days remaining)
Apex	100	90 days	22-Jan-2017 (43 days remaining)
Wired	100	90 days	22-Jan-2017 (43 days remaining)
Device Admin	Uncounted	90 days	22-Jan-2017 (43 days remaining)

- ISE، لىل عيحص ريغ ةكبش زا هجل IP نيوكت مت اذا وا ةكبش ل زا هج نيوكت متي مل اذا ،متي الولىم عمل ا ةباجتسا يا لاسرا متي مل .تم صب ةمزحل طاقسا اب ISE موقيسف TACACS+ ل ISE كولس يفي ريغت اذهو .ةيموسرلا مدختسملا هجاويف تالجس يا ضرع لىم ع وا فورعم ريغ ةكبش زا هج نم عاج ب لطلال ناب مل عي يذلا ACS كولسب هت نراقم دنع AAA.
- اذه نم ققحتلل نكمي . ISE لىل دع ت مل ةباجتسال نكلو ACS لىل بلطلال لصو لكشلا يفي حضورم وه امك يفاضلا يوتحمل رصمب ةقلعتم ل ريراقتلا نم ويرانيسلا وا ISE ل هنيوكت مت يذلا ACS لىل عاج لاص ريغ كرتشم رسب بسب كلذ نوكي ام ةداعو ACS ل هنيوكت مت يذلا ISE لىل

Steps
Message
Received TACACS+ Authentication START Request
Invalid TACACS+ request packet - possibly mismatched Shared Secrets

- صاخلا IP ناو نع نيوكت متي مل وا ISE نيوكت متي مل اذا يتح ةباجتسال لاسرا متي نل ةظحال نكمي ،عاطقلا اذه لثم يفي .ةكبش ل زا هج نيوكت يفي ACS لىل ISE ةرادا هجاوب ACS لىل لكشلا يفي ةلاسرلا

Steps
Message
Received TACACS+ packet from unknown Network Device or AAA Client

- لىل ريراقت يا ةدهاشم متي ال نكلو ACS لىل حجان ةقداصم ريراقت لىل عالطالال مت اذا

اذه نم ققحتلا نكمي. ةكبشلا يف ةلكشم كلذ نوكي دق ف، مدختسم لا صرف م تي و ISE عي مجتل. ةرورضلا ةيفصتلا لم اوع مادختساب ISE ىلع ةمزح طاقنتلا لال خ نم ءارجإلا تاودأ > اءحالصإو ءاطخألا فاشكتسأ > تايلمعلا ىلإ لقتنا، ISE ىلع ةمزح طاقنتلا TCP. ءيرفت > ةماع تاودأ > صيخشتلا

TCP Dump

Monitor the packet headers on the network and save to a file (up to 5 Minutes)

Status Stopped Start

Host Name

Network Interface

Promiscuous Mode On Off

Filter

Example: 'ip host helios and not iceberg'

Format

Dump File Last created on Fri Dec 09 20:51:18 IST 2016
File size: 9,606 bytes
Format: Raw Packet Data
Host Name: tornado
Network Interface: GigabitEthernet 0
Promiscuous Mode: On

3. بلطالنا اءا كلذ ينع ي دق ف، ACS ىلع سي ل نكل و ISE ىلع ريراقتلا ضرع نكمي ناك اءا. اءا نكمي يتلا و ISE ىلع تاسايسلا تاعومءم ل ءاطخ نيوكت ببسب ACS ىلإ لصي مل ةلكشم ببسب و ISE نع يليصفتلا ريرقتلا ىلإ ادانتسا اءحالصإو ءاطخألا فاشكتسأ ACS ىلع ةمزح طاقنتلا ةطساوب اءديحت نكمي ةكبشلا يف

4. نم اعونمم مدختسم لا لازي ال نكل و ACS و ISE نم لك ىلع ريراقتلا ىلع ءالطالما مت اءا. يتلا و ACS ىلع لوصول تاسايس نيوكت يف ةلكشم بلاءلا يف نيوكت اءنا ف، لوصول و ACS. لوح يليصفتلا ريرقتلا ىلإ ادانتسا اءحالصإو ءاطخألا فاشكتسأ نكمي ةكبشلا زاى ىلإ ISE نم ةءئاعلا رورملا ءءرب ءامسلا

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء عمة ف نمة دختسمل معد و تمة مة دقتل ةر شبل او
امك ةق قة نوك ت نل ةللأل ةمچرت لصف أن ةظحال مة چرئ. ةصاخل مة تغلب
Cisco ةلخت. فرتمة مچرت مة دقئ ةل ةل ةفارتحال ةمچرتل عم لالحل وه
لإمءاد عوچرلاب ةصؤت و تامچرتل هذه ةق دن ةه ةل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزئلچنل دن تسمل