

# ISE ىلع لىجراخ لى syslog م داخ نى وكت

## تاىوت حمل

[قمدقم](#)

[قئسس اسأل تا بل طتم](#)

[تا بل طتم](#)

[قمدخت سمل تا نوكت](#)

[قئسس اسأل تامول عم](#)

[نى وكت](#)

[\(UDP Syslog\) دعب نع لىجستل فده نى وكت](#)

[ل ائتم](#)

[لىجستل تا ئف نمض دىعبل فدهل نى وكت](#)

[تا ئف ل مهف](#)

[اهال ص او اطاخ ل ا فاش كت س او قصل نم ق قحت](#)

## قمدقم

ISE ىلع لىجراخ لى syslog لىجراخ لى وكت نى فى قى وكت و اذ ف صى.

## قئسس اسأل تا بل طتم

### تا بل طتم

قئسس اسأل تا بل طتم لىجراخ لى وكت نى فى قى وكت و اذ ف صى:

- (ISE) قئسس اسأل تامول عم
- Syslog م داخ

### قمدخت سمل تا نوكت

قئسس اسأل تا بل طتم لىجراخ لى وكت نى فى قى وكت و اذ ف صى:

- Identity Services Engine (ISE) 3.3 رادصل
- Cisco Syslog Server v1.2.1.4

قئسس اسأل تا بل طتم لىجراخ لى وكت نى فى قى وكت و اذ ف صى. تا ئف ل مهف (ىضارتفا) حوسم نى وكت ب دنت سمل اذ ف قمدخت سمل اذ ف قى وكت نى فى قى وكت و اذ ف صى. رما لى لىجراخ لى وكت نى فى قى وكت و اذ ف صى.

## قئسس اسأل تامول عم

نبيعت متي و. تالجال ل عي مجت تاودا ة طساوب اهنيزختو ISE نم Syslog لئاسر عي مجت متي متي يتل تالجال ل نيزختب MnT موقت يتح دقل ة بقارمل هذه تالجال ل عي مجت تاودا اي لجم اهنيزخت.

فنصت. افاده ايمست يتلاو، ة جراخ ل syslog م داوخ نيوكت ب موقت، ايجراخ تالجال ل عي مجت ل اق بس م ة فرعم ة فل تخم تائف يف تالجال ل

يوتسمو افاده اب قلعتي اميف تائف ل ريرحت لال خ نم ليجست ل تاجرخم صي صخت كنكمي كلذ ل امو ة روطخ ل

## نيزخت ل

لجال لئاسر لاسرا متي يتل دع ب نع syslog م داخ فاده اءاش نال ب يولا ة ج او م ادخت سا كنكمي رايعمل اق فو ة دي عب ل syslog م داخ فاده ا ل لجال لئاسر لاسرا متي. اهل ل ماظن ل (RFC-3164 عجار) syslog لوكوتورب

(UDP Syslog) دع ب نع ليجست ل فده نيزخت



قوف رونا، Cisco ISE ل (GUI) ة موموسر ل م دختسم ل ة ج او يف

قوف رونا > دع ب نع ليجست ل فاده ا > Administration > System رتخ او () Menuicon ة فاضا

---

فده نيوكت :ةامسمل ةشاشلا ةطول ىلع اذه نيوكتلا لاثم دم تعي :ةظحالم  
دعب نع ليجستلا

- اذه مادختسا متي و ،ديعبلا syslog مداخل مسا لاخدا انه كنكمي ، Remote\_Kiwi\_Syslog ك مسا ةيفصو ضارغال مسالا
- ،كلذ عم و ؛مادختسالا دي ق syslog UDP ، اذه نيوكتلا لاثم في ، UDP syslog ك فدهلا عونلا :  
فدهلا عونلا ةلدسنملا ةمئاقلا نم تارايلخلا نم ديزملا نيوكت كنكمي

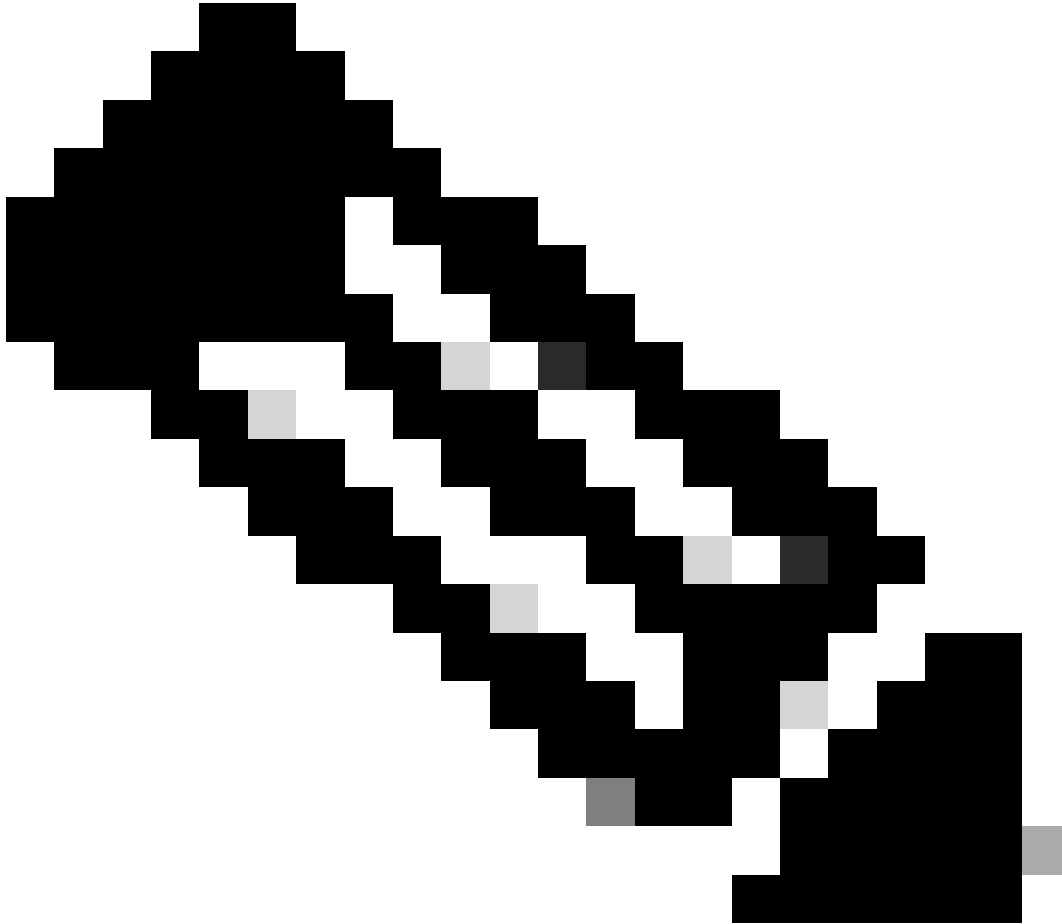
عيرسلا ليجستلا ةبس انملا ، UDP ربع syslog لئاسر لاسرال مدختسي : UDP syslog  
نزولا في فخو

تاينام عم ةيقو و ملافوي يذلاو ، TCP ربع syslog لئاسر لاسرال مدختسي : TCP syslog  
لاسرالا ةداعاو ءاطخال نم ققحتلا

TLS، ريفشت مادختساب TCP ربع اهلاسرلا متي يتلا syslog لئاسر ىلا ريشي :نمآلا syslog  
اهتيرسو تانايبلا لماكت نمضي امم

- Statusdrop ةلدسنملا ةمئاقلا نم Enabled راي تخا ك لي لع بجي ، نيكمتلا ةلاح

- ديدجل فدهلل زجوم فصولاخذ ايراي تخا ك نكمي ، فصولا
- يذلا هجولا مداخلل فيضملا مسا و IP ناوع ل اخاب موقت انه ، IP ناوع / فيضملا ليجستلل IPv4 و IPv6 تاقيسنت Cisco ISE معددي .تالجلال نيزختب موقوي



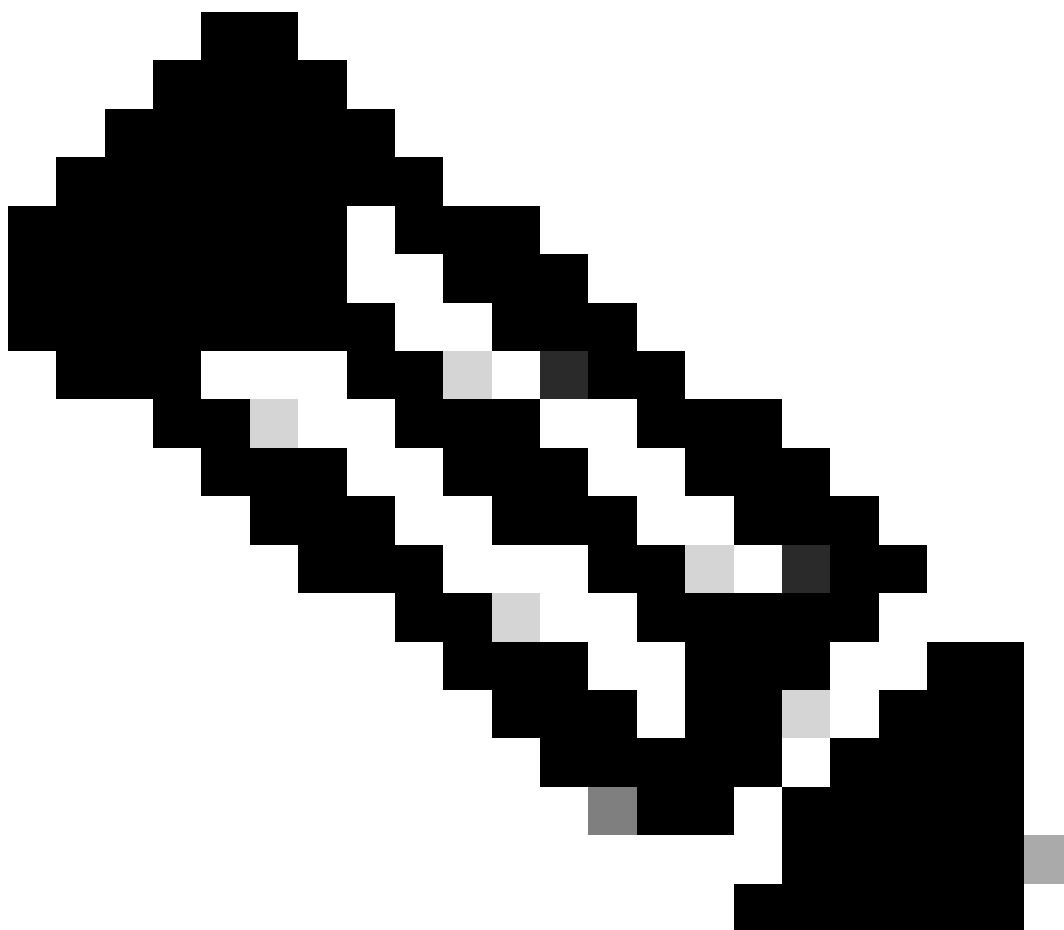
FQDN مادختساب syslog مداخل نيوكت ديترت تنك اذا هنأ ركذ يروضلا نم :ةظحالم نيزختلا نودب .ءادألا يلع ريثأتلل بنجتل DNS ل تقؤملا نيزختلا دادع ا بچي ف يلا syslog ةمزح لاسرا بچي ةرم لك في DNS مداخل نع ISE ملعتسي ، DNS ل تقؤملا ءادأ يلع ةدشب كلذ رثؤوي . FQDN مادختساب هن نيوكت مت يذلا دعب نع ليجستلا فده ISE.

ي:يلي ام يلع بلغتلل رشنلاب ةصاخلا PSN تاكبش عيمج ي service cache enable رمألا مدختسأ

لاشم

```
ise/admin(config)# service cache enable hosts ttl 180
```

- 
- UDP لءانيم ريصقتلا نوكي يا 514 ءانيم في عمئتسي لءان Kiwi syslog لا ،لاثم ليكشت اءه في ،514 as ءانيم رطء مءء نم ءكأت .65535 و 1 نيب ءميقي يا اءه ءفنملا مقر ربيغت نيمءءستملل نكمي ،كلء عمو .ءلاسر syslog ءميامء راءء يا لبق نم بولطملا ءفنملا .
  - ءءسنملا ءمءاقل نم ،ليءسءلل ءمءءسء بءي يءلا syslog قفرم زمر رايءءا كنكمي ،LOCAL6 ك قفرملا زمر LOCAL0 through Local7 يه ءءاصللا ءارايءلا .
  - ءءل نبيءء مءي .ءيءبلا لءسلا فءه لءاسر لولل صقألا ءءلا لاءءا انه كنكمي ،1024 ك لولل صقألا ءءلا ءءل نبيءء مءي .ءيءبلا 1024 لءل 200 نم مبيقلا ءوارءءو ،ISE 3.3 راءصءب ايضارءءا 1024 لءل لولل صقألا .
- 



هنأىلعلولوللصقألالدلالللدعتكنكمي،دعبنعليجستلالفدهىلإلعطتقملائسرللسرلابنجلت:نظالم 8192.

- عمو:فدهلااذللتاهيبنتنيمصتديجتمتيال،اذهنيوكتلالاثلثيف،اطيسبئاقبال،فدهلااذللتاهيبنتنيمصت

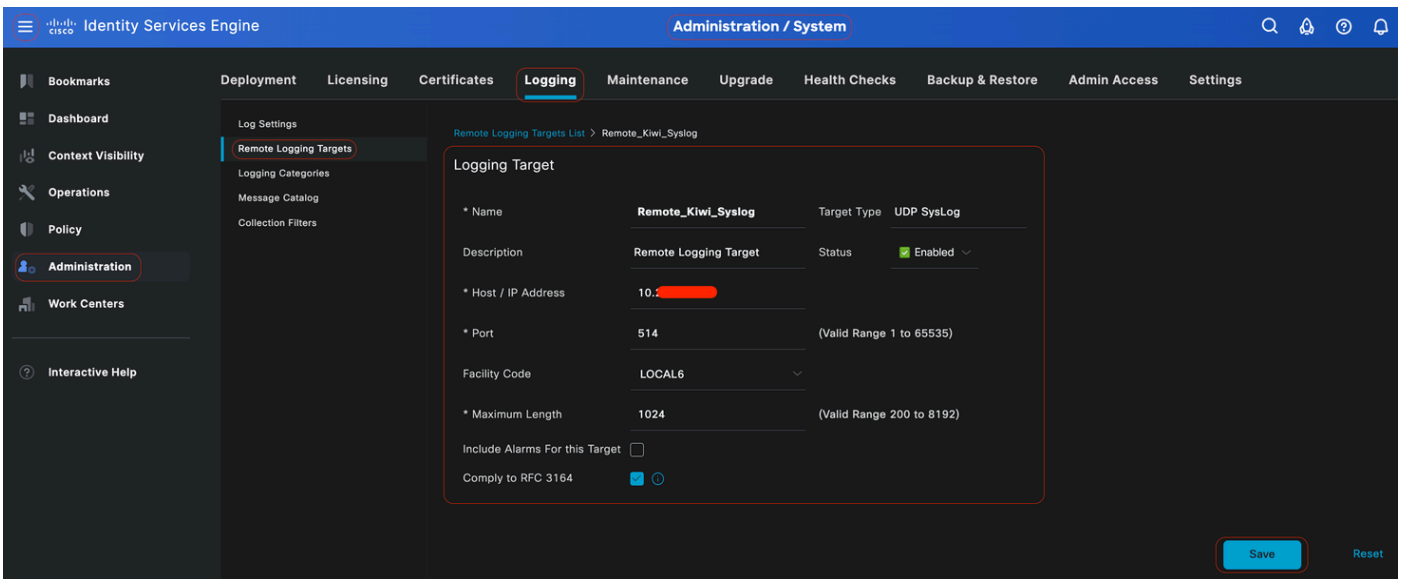
- متييتللسyslogلائسري( \{ } )، تاددحلمإف،هذيرايتخالالناخديجتدنع، RFC 3164 عمقفاوتلاديجتمت

- 

نظفقوقرقنا،نيوكتلالاهتنادرجمب

- 

ديكأتلابديرتله.مداخالاب(TCP/UDP)نمأريغلاصتاءاشن!تتخأدقل:ريذحتلالاذهضربماظنلالموقيس،ظفحلالدرجمب معنقوقرقنا،ةعابتمل



ديعبلالفدهلانيوكت

ليجستلالتائفنمصديعبلالفدهلانيوكت

ىللكذدعبجاتحت،كبصاخلالدعبنعليجستلالفدهنيوكتدرجمب. syslog فدهىلإللقيدتلاللباقأل Cisco ISE لسري قيقيدتلاللباقألألألهجوتدعالعدوصقلملائفلالىلإلدعبنعليجستلالفدهنييعت.

هذهلجسلاتائفنمألألتالجسءاشنإمتي.هذهلجسلاتائفنمئلكلليجستلالفادهانييعتلكلذدعبنكمي متييتللتامدخالالىلإداننسا ديعبلالس syslog مداخالىلألصلالتالجالسلالسرالانهنيوكتنكمي و PSN دقعنمطقف دقعلالهذهلأهنيوكت:

- 

تأجيل (AAA) تأجيل وقت العمل أو إيقاف العمل مؤقتاً

- 

تأجيل AAA تأجيل وقت العمل

- 

تأجيل تأجيل وقت العمل

- 

تأجيل MDM تأجيل وقت العمل

- 

تأجيل فرع تأجيل وقت العمل

- 

تأجيل Client Provisioning و Posture تأجيل وقت العمل

- 

تأجيل Client Provisioning و Posture تأجيل وقت العمل

- 

تأجيل تأجيل وقت العمل

تأجيل تأجيل وقت العمل لاسرير انيوكت نكمي ورش نل ايف دقعل ايمج نم هذه لجسلا تائف نم ثادحلأا تالجسءاشنإ م تي  
دعب نع syslog م داخ لى

- 

تأجيل تأجيل وقت العمل أو إيقاف العمل مؤقتاً

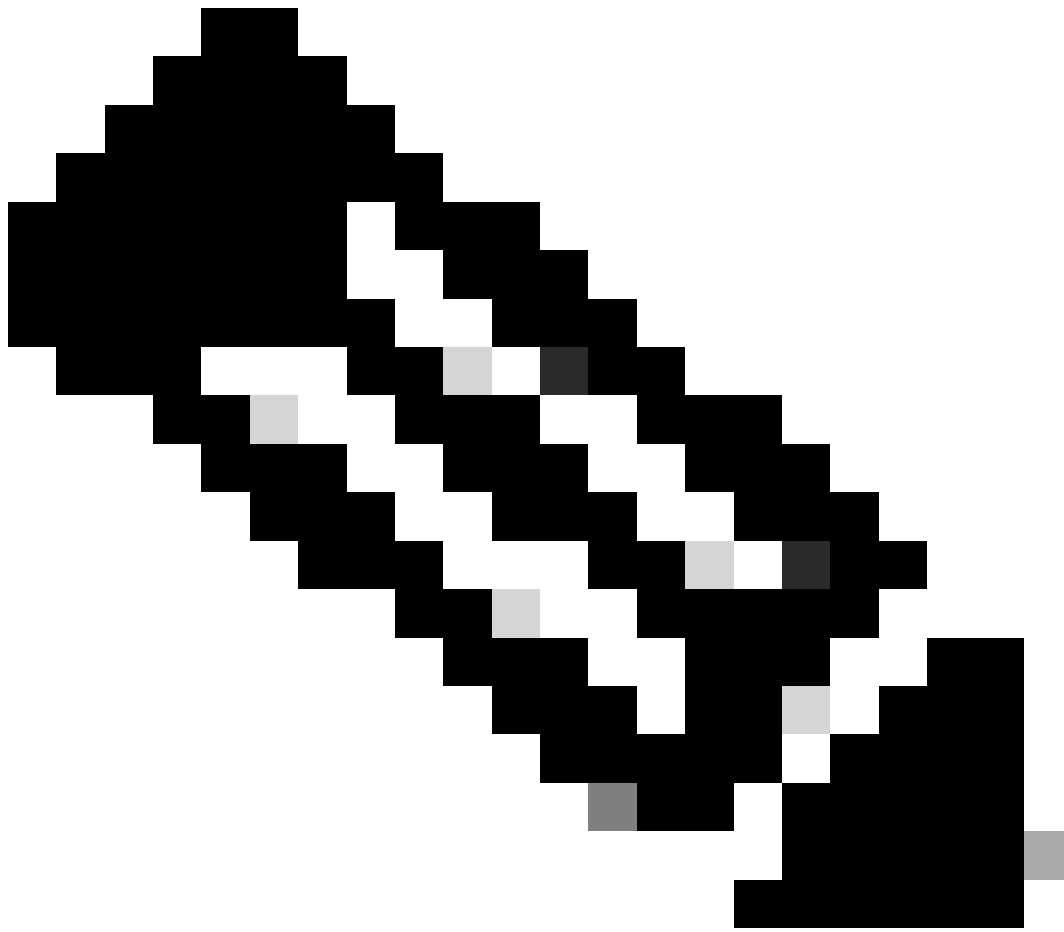
-

ماظننلا تااصي خشت

.

ماظننلا تااي ئاصح

ةكرح تالجس لاسررال ثالثللا تاائفلا هذهو ،ليجست تاائف عبرأ نمض ديعبلا فدهلا نيوكتب موقتس ،اذه نيوكتلا لاثم يف  
ISE لوؤسم ليجست رورم ةكرح لةائفلا هذهو ،RADIUS ةبساومو ةلشافلا تالواحملاو ،اهيرمت مت يتلا ةقداصملا :ةقداصملا رورم



دعب نع ليجستلا فده نيوكت :ةامسمل ةشاشلا ةطقول ىلع اذه نيوكتلا لاثم دمتعي :ةظالم





قوف رقنا، Cisco ISE (GUI) ةيموسرلا مدختسملا ةهجاو يف

يتلا ققداصملا تاي لمع) ةبولطملا ةئفلا قوف رقناو، ليجستلا تائف ليجستلا Administration>System> رتخاو () (Menuicon) رايخلال (RADIUS) ةبساحم و لشفلا تالواحم، اهريرمت مت

بسح اهبيرتول لئاسرلا ةيفصتب لوؤسملل حمسي امم، ةروطخ يوتسمب شح ةلاسرت: ليجستلا ةروطخ يوتسم-1 ةوطخلا لكشب ةميقلا هذه نبيعت متي، ليجستلا تائف ضعبل ةبسنلاب. بولطم وه امك ليجستلا ةروطخ يوتسم ددح. ةيولوالا نم ةيلاتلا ةروطخ تايوتسم دح رايخا كنكمي، ليجستلا تائف ضعبل ةبسنلاب. اهريرحت كنكمي الو، يضارثفا ةلدسنملا ةمئاقلا:

•

يلع مزاللا ءارجال داخا كليل بجي و Cisco ISE مادختسا كنكمي ال هنأ ينعي يوتسملا اذه. ئراوطلال يوتسم: تيمم روفلا.

•

جداف أطخ ةلاح يلا يوتسملا اذه ريشي: أطخ.

•

نم ديدعلل هنييعت مت يذلا يضارثفال يوتسملا وه اذه. ةماه نكلو ةيداع ةلاح يلا يوتسملا اذه ريشي: ريذحت ليجستلا تائف.

•

ةيمالع ةلاسرا يلا يوتسملا اذه ريشي: تامولعم.

•

ةيصيخشث أطخ ةلاسرا يلا يوتسملا اذه ريشي: اطخالل حيحصت.

PSNs ةطساوب اهؤاشن مت يتلا تالجلال نأ ينعمب. يلحملا ليجسلا ءاشن| هذه رايخالا ةناخ حيتي: يلحملا ليجستلا -2 ةوطخلا

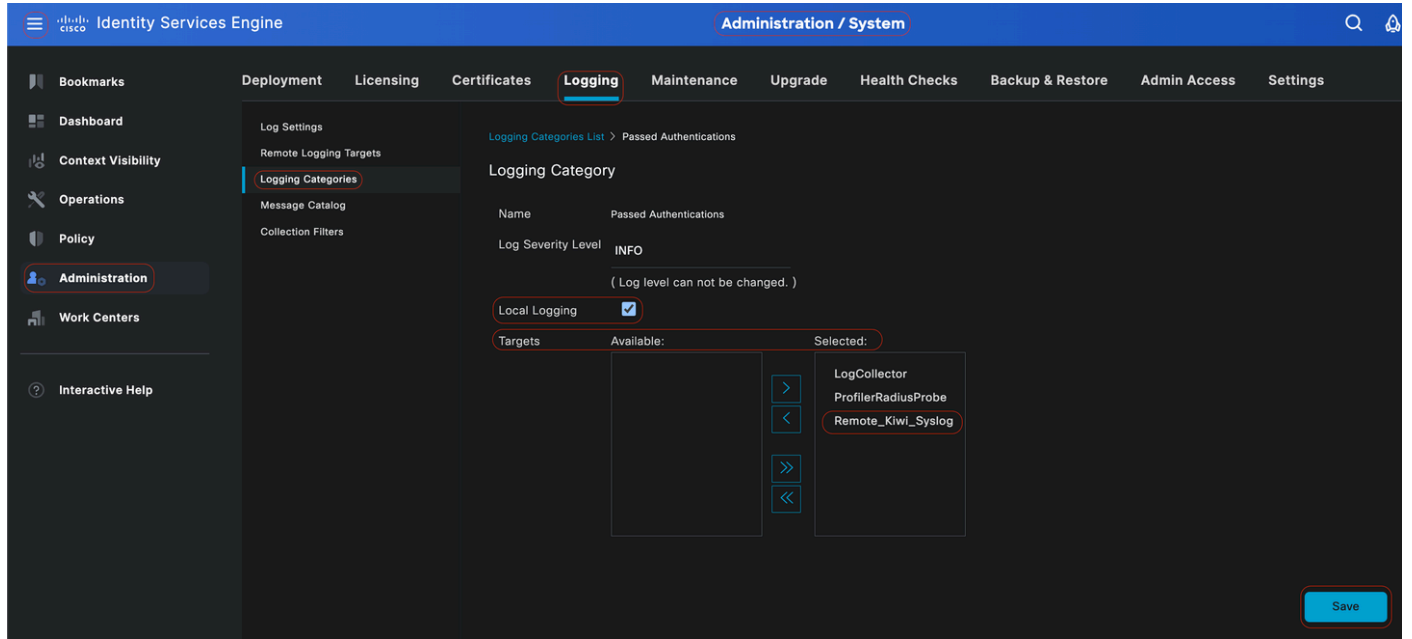
يضا رتفالال نيوكتلابل ظافتحالابل ي صون .اضيأ لجلسلا عاشنابل موقوي يذلا ددحملال PSN لىل ع اهظفح م تي

و AvailableArea نيبل فادهالال لىل قيرط نع لىل جست ةئفل فادهالال رايتخاب ةقطنملا هذه كل حمست :فادهالال -3 ةوطخلال رسيالال او نميالال مهسالال زومر مادختساب SelectAreas.

(مدختسملا لىل بق نم ةددحملال) ةيچراخلال او (اقبسم ةددحملال) ةيلا حملال ، ةدوچوملا لىل جستلا فادهالال لىل AvailableArea يوتحت

ةئفلل اهرايتخاب | مت يتل فادهالال ، ةيادبلال ي ف اغرافل نوكل يذلا ، Selectedarea ضرعي م ث

RADIUS ةبسا حمو ةلشاف تالواحم تائف نمض ديعلبال فدهالال ةفاضلال 3 ةوطخلال لىل 1 ةوطخلال نم ةوطخلال ررك -4 ةوطخلال



ةدوصقملا تائفلال لىل ةديعلبال فادهالال نييعت

وتلل هتفضأ يذلا ديعلبال فدهالال ةيؤر لىل ارداق نوكت نأ بچي . ةبولطملا تائفلال نمض ديعلبال فدهالال نأ نم دكأت -5 ةوطخلال

ةبولطملا تائفلال لىل نيعلمال Remote\_Kiwi\_Syslog ديعلبال فدهالال ةيؤر كنكمي ، هذه ةشاشلال ةطقل ي ف

Parent Category	Category	Targets	Severity	Local Log ...
<input type="radio"/>	AAA Audit	LogCollector	INFO	enable
<input type="radio"/>	Failed Attempts	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
<input type="radio"/>	Passed Authentications	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
<input type="radio"/>	AAA Diagnostics	LogCollector	WARN	enable
<input type="radio"/>	Administrator Authentication and Auth...		WARN	enable
<input type="radio"/>	Authentication Flow Diagnostics		WARN	enable
<input type="radio"/>	Identity Stores Diagnostics		WARN	enable
<input type="radio"/>	Policy Diagnostics		WARN	enable
<input type="radio"/>	RADIUS Diagnostics	LogCollector	WARN	enable
<input type="radio"/>	Guest	LogCollector	INFO	enable
<input type="radio"/>	MyDevices	LogCollector	INFO	enable
<input type="radio"/>	AD Connector	LogCollector	INFO	enable
<input type="radio"/>	TACADS Diagnostics	LogCollector	WARN	enable
<input type="radio"/>	ACI Binding	LogCollector	INFO	enable
<input type="radio"/>	Accounting	LogCollector	INFO	enable
<input type="radio"/>	RADIUS Accounting	LogCollector,ProfilerRadiusProbe,Remote_Kiwi_Syslog	INFO	enable
<input type="radio"/>	TACADS Accounting	LogCollector	INFO	enable
<input type="radio"/>	Administrative and Operational Audit	LogCollector,Remote_Kiwi_Syslog	INFO	enable
<input type="radio"/>	External MDM	LogCollector	INFO	enable
<input type="radio"/>	PassiveID	LogCollector	INFO	enable
<input type="radio"/>	Posture and Client Provisioning Audit	ProfilerRadiusProbe,LogCollector	INFO	enable
<input type="radio"/>	Posture and Client Provisioning Diagnostics	LogCollector	WARN	enable
<input type="radio"/>	Profiler	LogCollector	INFO	enable
<input type="radio"/>	System Diagnostics	LogCollector	WARN	enable
<input type="radio"/>	Distributed Management		WARN	enable
<input type="radio"/>	Internal Operations Diagnostics		WARN	enable
<input type="radio"/>	Licensing	LogCollector	INFO	enable
<input type="radio"/>	Threat Centric NAC	LogCollector	INFO	enable
<input type="radio"/>	System Statistics	LogCollector	INFO	enable

## تائفلال نم ققحتال

### تائفلال مهدف

kernel، لثم ةددتم تآشمن نم اهديلوت متي يتال ثدجال لئاسر نم ةفلتخم عاونأ كانه. ثدح ثودح دنع ةلأسر عاشنإ متي اذكهو، مدختسملأ يوتسم، يدربال.

تائفلأ يلمره لكشب اضيأ ثادحألا هذه ميظنت متي و"لائسارلا جولالتك" نمض عاطخألا هذه فينصت متي و.

تائفلال ضعب وأ ةئف يلع يوتحت ةئف يلع تائفلأ هذه يوتحت.

ةئفأل	ةئفأل
ةبسا حمل او ضي وفتلاو ةقداصل مالا قيقدت (AAA)	ةبسا حمل او ضي وفتلاو ةقداصل مالا قيقدت (AAA) ةلشاف تالوا حم اهري رمت مت يتال ةقداصل مالا
تاصيخشت AAA	تاصيخشت AAA

	<p>ضيوف تال او لوؤس مالا ةقداصم</p> <p>ةقداصم لاقفدت تاصيخشنت</p> <p>ةيوهال نزم تاصيخشنت</p> <p>ةسايسال تاصيخشنت</p> <p>RADIUS تاصيخشنت</p> <p>فيض</p>
ةبساحم	<p>ةبساحم</p> <p>RADIUS ةبساحم</p>
ةيوليغشنت لاقفدت تال او لوؤس مالا ةقداصم	ةيوليغشنت لاقفدت تال او لوؤس مالا ةقداصم
Client Provisioning و Posture قيقت	Client Provisioning و Posture قيقت
Client Provisioning و Posture تاصيخشنت	Client Provisioning و Posture تاصيخشنت
للحم	للحم
ماظنل تاصيخشنت	<p>ماظنل تاصيخشنت</p> <p>ةعزوم لاقفدت</p> <p>ةيلخادل تال مالا تاصيخشنت</p>
ماظنل تال تال تال	ماظنل تال تال تال

يلع هذه فيض لاقفدت تال او لوؤس مالا ةقداصم. فيض لاقفدت تال او لوؤس مالا ةقداصم هو Guest نأرت نأكنكمي، هذه ةشاش لاقفدت تال او لوؤس مالا ةقداصم. AAA تاصيخشنت يمس تال تال تال.

Identity Services Engine Administration / System

Deployment Licensing Certificates **Logging** Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Log Settings  
Remote Logging Targets  
Logging Categories  
**Message Catalog**  
Collection Filters

Export

Category Name	Message Class	Message Code	Message Text	Message Description	Severity
Guest	Guest	86001	Guest user has entered the guest portal login page	Guest user has entered the guest portal login page	INFO
Guest	Guest	86002	Sponsor: Guest user has entered the guest portal login page	Sponsor has suspended a guest user account	INFO
Guest	Guest	86003	Sponsor has enabled a guest user account	Sponsor has enabled a guest user account	INFO
Guest	Guest	86004	Guest user has changed the password	Guest user has changed the password	INFO
Guest	Guest	86005	Guest user has accepted the Use Policy	Guest user has accepted the use policy	INFO
Guest	Guest	86006	Guest user account is created	Guest user account is created	INFO
Guest	Guest	86007	Guest user account is updated	Guest user account is updated	INFO
Guest	Guest	86008	Guest user account is deleted	Guest user account is deleted	INFO
Guest	Guest	86009	Guest user is not found	Guest user record is not found in the database	INFO
Guest	Guest	86010	Guest user authentication failed	Guest user authentication failed. Please check your password and account permis...	INFO
Guest	Guest	86011	Guest user is not enabled	Guest user authentication failed. User is not enabled. Please contact your system ...	INFO
Guest	Guest	86012	User declined Access-Use Policy	Guest User must accept Access-Use policy before network access is granted	INFO
Guest	Guest	86013	Portal not found	Portal is not found in the database. Please contact your system administrator	INFO
Guest	Guest	86014	User is suspended	User authentication failed. User account is suspended	INFO
Guest	Guest	86015	Invalid Password Change	Invalid password change. Use correct password based on the password policy	INFO
Guest	Guest	86016	Guest Timeout Exceeded	Timeout from server has exceeded the threshold. Please contact your system adm...	INFO

## لئاسرلا جولتاتك

اهالصالو اعاطخالو فاشكتساو عحصلال نم ققحتال

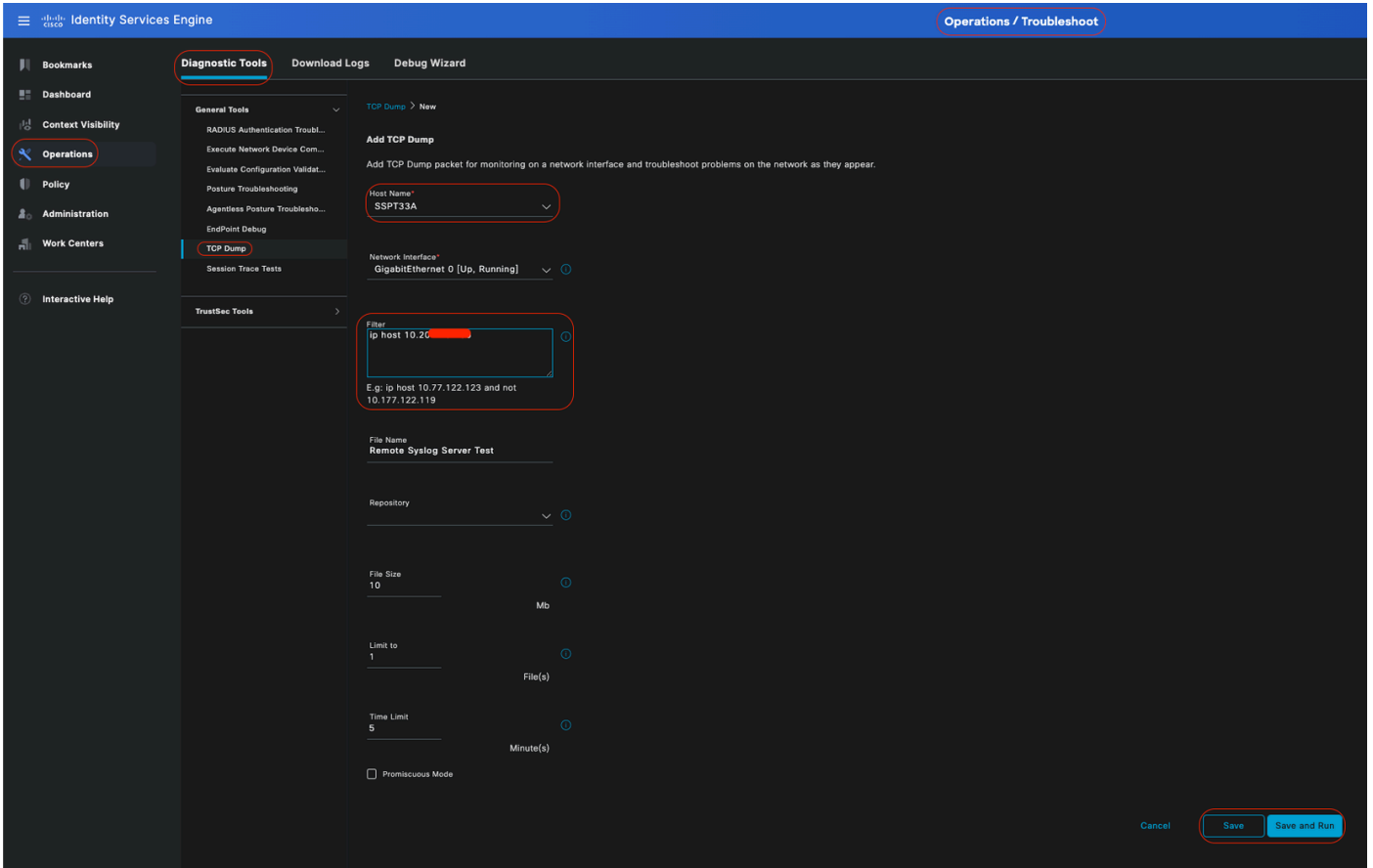
اهتحص نم ققحتالو اهلصالو اعاطخالو فاشكتسالو عوطخ عرسأ دعب نع ليجستال فده لباقم TCP غيرفتة ليمع عارجا دعيا  
ال ما لجسال اذاع لاسرلا متي ناك اذا ام ديكأتل

لئاسرلا هذه لاسرلا متي سو لجسال لئاسرلا عااشنا ب موقيسي PSN نأل مدختسمل قداصي يذال PSN نم طاقتلال ذخأ بجي  
ديعبل فدهال



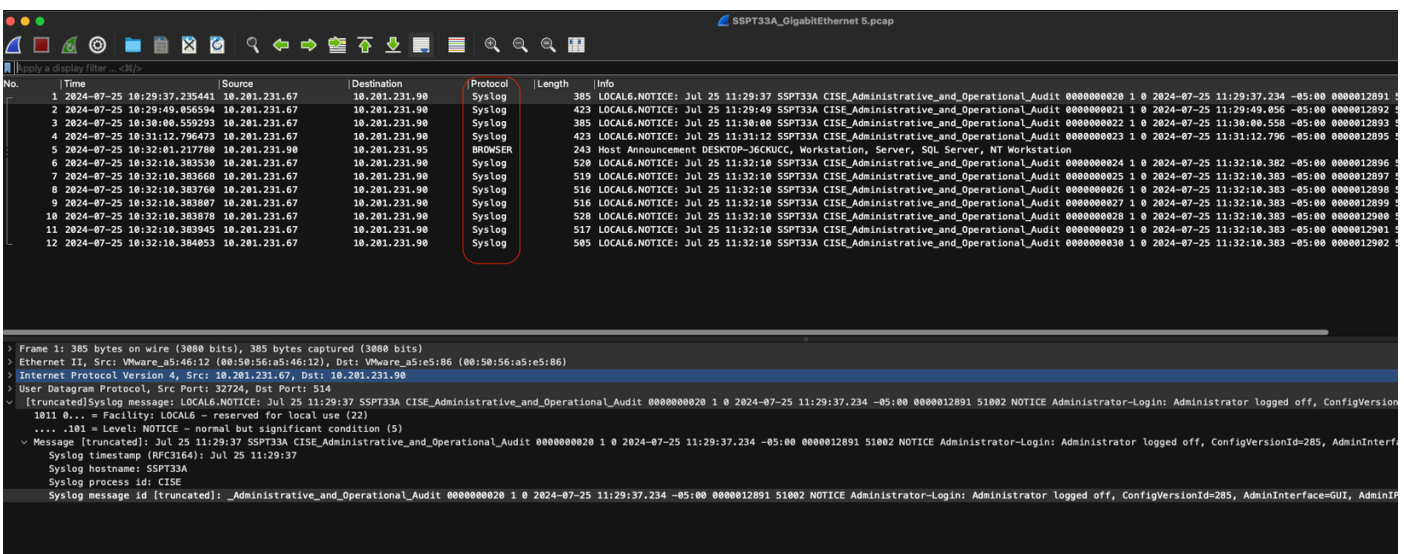
Menuicon قوف رقنا، Cisco ISE قوف موموسرلا مدختسمل اهه او يف  
ة. فاضا قوف رقنا TCP غيرفتا اهلصالو اعاطخالو فاشكتساو اذاع ليمع رتخاو

- ip فيضم ل <remote\_target\_ip\_address> ةفصت ل قح ةفاضو، رورملا ةكرح ةفصت بجي.
- PSN ةجالام ةقداصم نم طاقتلال طاقتلال بجي.



## تغريف TCP

ISE لوؤسم ليچست رورم ةكرحل Syslog لئاسر لئاسر اب ISE موقوي فيك ةيؤر كنكمي ،هذه ةشاشلا ةطقل يف



## Syslog رورم ةكرح

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ل ا ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
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 دن ت س م ل ا