

اهحال صإو هئاطخأ فاشك تساو syslog نيوكت (ACI) لوصولا يف مكحتلا هجاو يف

ةمدقملا

فاشك تساو هنم ققحتلاو (syslog) ماظنلا ليجست نيوكت ةيفيك دننتملا اذه فصري ريس يطغي وهو. Cisco Application Centric Infrastructure (ACI) يف اهحال صإو ليجستلا اذه ءاطخأ مكحت ةدحول (MO) رادمل نئاكل زارط مادختساب يجم انربلا ققحتلاو، لماكل نيوكتلا لمع لك يهم اهحال صإو ءاطخأ فاشك تسأ لمع قفدتو، قيبطتلا ءسايسل ءسايسألا ءينبلا. ءسايسألا دومعلو قاروالا تالوحمو APIC مكحت تادحو نم لكل

ةماع ءرظن

رماو دجوت ال، لقتسملا Cisco NX-OS® جمانرب سكع ىلع. ءسايس لماكلاب وه ACI Syslog ىلع ءزكت رمل ءسايسألا logging server وأ ءيفرطلا تالوحملا ىلع (CLI) رماوالا رطس هجاو APIC موقي يتلا APIC تاسايس لالخنم syslog نيوكت عيجم ذيفنت متي. تاقيبطتلا اءاقلت ءانب ءدقع لك ىلإ اهءفدب

ءيسئلرلا تانوكملا


ءيلال ءرادملا تانئاكل نم ACI يف syslog يعرفلا ماظنلا ءاشنإ مت

- مكحتت syslog. تاهجو عيجملا ءولاع ءيواحل — Syslog (syslogGroup) ءهجو ءعومجم ىلع يوتحي نأ نكميو. تقولا متخ تاراخيو (NX-OS طمن وأ ACI) ءلاسرلا قيسنت يف مكحت ءدحو ءهجو، ءيلحم فلم ءهجو، رثكأ وأ ءدحو ءديعب ءهجو.
- ىلع ءيرادلل ءلحال يف مكحتت يتلا ءهجولا ءعومجم لءبات — syslog profile (syslogProf) (TCP أو UDP) لقنلا لوكونوربو ءعومجملا يوتسم.
- نع syslog مءاخ لثمى ءهجولا ءعومجم لءبات — Syslog Remote Destination (syslogRemoteDest) ءروطخلا ءيفصت لماعو ذفنملاو فيضملا مسا وأ مءاخلاب صاخلا IP يف مكحتتلا. ءعب مءاخلا ىلإ لوصول ءمءختسملا (EPG) ءرادلل ءياهن طاقن ءعومجمو syslog قفرمو.
- لئاسر ءباتك يف مكحتت يتلا ءهجولا ءعومجم لءبات — syslog مءيلحم (syslogFile) ءربم يلمع syslog ءانب ءدقع لك ىلع /var/log/external/messages يلمعلا ىلإ syslog.
- (قبقءت) لئاسرلا ءاونأ يف مكحتتلا. ءبقارملا ءسايسب قفرم — Syslog (syslogSrc) رءصم رعب ءهجولا ءعومجم ىلإ طباورلاو، ءروطخلا نم ىندألا ءحلاو (لمع ءسلج، ءاطخأ، ءاءأ ءقالع syslogRsDestGroup).

Syslog رءصم قفرم طاقن

يتل تانئاكل او دقعل ا يف مكحتت يتل ةبقارملا تاسايسل تاقاطن ةعبرأ ACI مدختسي
syslog لئاسر عاشناب موقت

- ةموظنملا قاطن ىلع قاطنلا - (monCommonPol، uni/fabric/moncommon) ةكرتشملا دصرلا ةسايس
ايئاقلت اهرشن متيو ثادحأل او لاطعأل ا عيمج ىلع قبطنت ةيساسأ ةبقارم ةسايس
مكحتل تادحو عيمجو (ةيسيسئرلا تالوحملاو ةيفرطلا تالوحملا) دقعل عيمج ىلع
رجأتسملاو لوصولو اوجيسنلل ةيمرهل تاجردتلا ةفاك يطفغي. ةينبلا يف (APICs)
ةماعلا ةسايسلا > ةبقارملا > تاسايسلا > ةينبلا تاسايس > ةينبلا يف دوجوم
syslog دلوي. ةينبلا قاطن - (monInfraPol، uni/infra/moninfra-default) ةينبلا ةبقارم ةسايس
حوارم جارداو لكيه تانوكمو تاقاطبو ةيويينب ذفانم: لكيهلا ىوتسم ىلع تانئاكل
ةيضارتفالا > ةبقارملا > تاسايسلا > ةينبلا تاسايس > Fabric يف دوجوم
ةينبلا) لوصولو قاطن - (monFabricPol، uni/fabric/monfab-default) لوصولو ةبقارم ةسايس
عسوم ةزهجأو لوصولو ذفانم: لوصولو هجاوت يتل تانوكملا syslog عاشناب. (ةيساسأل
> ةينبلا يف دجوي. (VM) يرهاظلا زاهجلا يف مكحتل ةدحو ثادحأو ةينبلا تالوصول
ةيضارتفالا > ةبقارملا تاسايس > تاسايسلا > لوصولو تاسايس
• عاشناب. رجأتسملا قاطن — (monEPGPo1، uni/tn-common/monepg-default) رجأتسملا ةبقارم ةسايس
فيرعت تافلومو، (EPGs) ةياهنلا طاقن تاعومجم: رجأتسملا قاطن تاذا تانئاكل لل syslog
ةبقارملا جهن > [رجأتسم] يف رجأتسم لك تحت هيلع روثلعلا مت. تامدخلو، تاقيبطتلا
> ييضارتفالا

 syslog نيوكتل اهب ىوصولو ادبلا ةطقن يه ةكرتشملا ةبقارملا ةسايس: ةظحالم
اهرشن متيو ةيمرهل تاجردتلا عيمج ربع ةينبلا ىوتسم ىلع ةيطغت رفوت اهنأل
جيسنلاو لوصولو ةبقارم تاسايس نيوكت نكمي. دقعل عيمج ىلا ايئاقلت
تالسلست يف تايوتسملا ددعتم مكحتل نم ديزمل ةماعلا ةسايسلا ىلا ةفاضلاب
قيضاً قاطن ىلا syslog ديقتل ةماعلا ةسايسلا نم ادب واً، ةنيعم نئاك ةيمره

Syslog ةلاسر قيسننت

ACI ىلع ةعومجملا قيسننت نييعت دنع RFC 3164 قيسننت ACI ل syslog لئاسر رعبتت
(يضارتفالا):

TIMESTAMP SOURCE %FACILITY-SEVERITY-MNEMONIC: Message-text

لائملا لىبس ىلع:

Apr 10 08:25:33 apic1 %LOG_LOCAL0-3-SYSTEM_MSG [F0022][soaking][inoperable][major][topology/pod-
1/node-1/.../fault-F0022] LDAP Provider unreachable

للىبس ىلع) ةايحل ةرود ةلاحو (ACI) لوصولو يف مكحتل ةهجاو اظخ زمر ةلاسرلا صن نمضتي

لئاسررلا لعجي امم ،رثأتملا نئاكلل (DN) زيمللا مسال او ءدشلاو (soaking retaining، cleared) لئاسررلا
اهسفنن اهسفنن فصت

لئاسررلا قيسنننل تاراخي ءثالث رفوتت

- رشننلا تاي لعم مظعمل هب يصوم RFC 3164 عم قفاوتم قيسننن — (يضا رتفال) ACI
- عقوتي syslog ياساسال ماظنل ناك اذا اذه مدختسا NX-OS. طمن قيسننن — NXOS
- NX-OS قيسننن لئاسرر
- عم RFC 5424 عم قفاوتم قيسننن — (ثدخال تارا دصلال او (APIC 5.2(8) نسمحلا لجال
- ءنسللا نمضتت يتلا ءنسمحلا ءينمزللا عب او طلا

ءروطخللا نييعت

لودللا حضوي .(ءروطخ لقال) 7 لىل (ءروطخ رثكال) 0 نم دحاو مقررنع ءرابع syslog ءروطخ لقق
يلودلا داحتال / ACI ءروطخ تاحل طصمو syslog ءروطخ تايوتسم ني بطيطختللا لئاللا
(ITU) تالاصتاللا:

فصولا	ACI / ITU يوتسم	Syslog ءروطخ
مادختسالل لباق ريغ ماظنلا	—	0 - ئراوطلال تالاح
يروف ءارجل داختل بولطم	جرح	1 - هيبنت
ءجرح ءلاح	ريبك	2 - ماه
طرش أطخ	فيفط	3 - أطخ
ريذحتللا ءلاح	ريذحت	4 - ريذحت
ءيمهأ تاذ نكلو ءيداع ءلاح	حوسمم / ددحم ريغ	5 - راطخال
طقف ءيمالعل ءلاسرر	—	6 - ءيمالعل
طقف ءاطخالل حيحصت جارخل	—	7 - ءاطخالل حيحصت

لقنللا تاراخي

دعبنع syslog لوكوتوربل لقن تالوكوتورب ءثالث (ACI) لوصولاي ف مكحتللا ءهجاو معدت

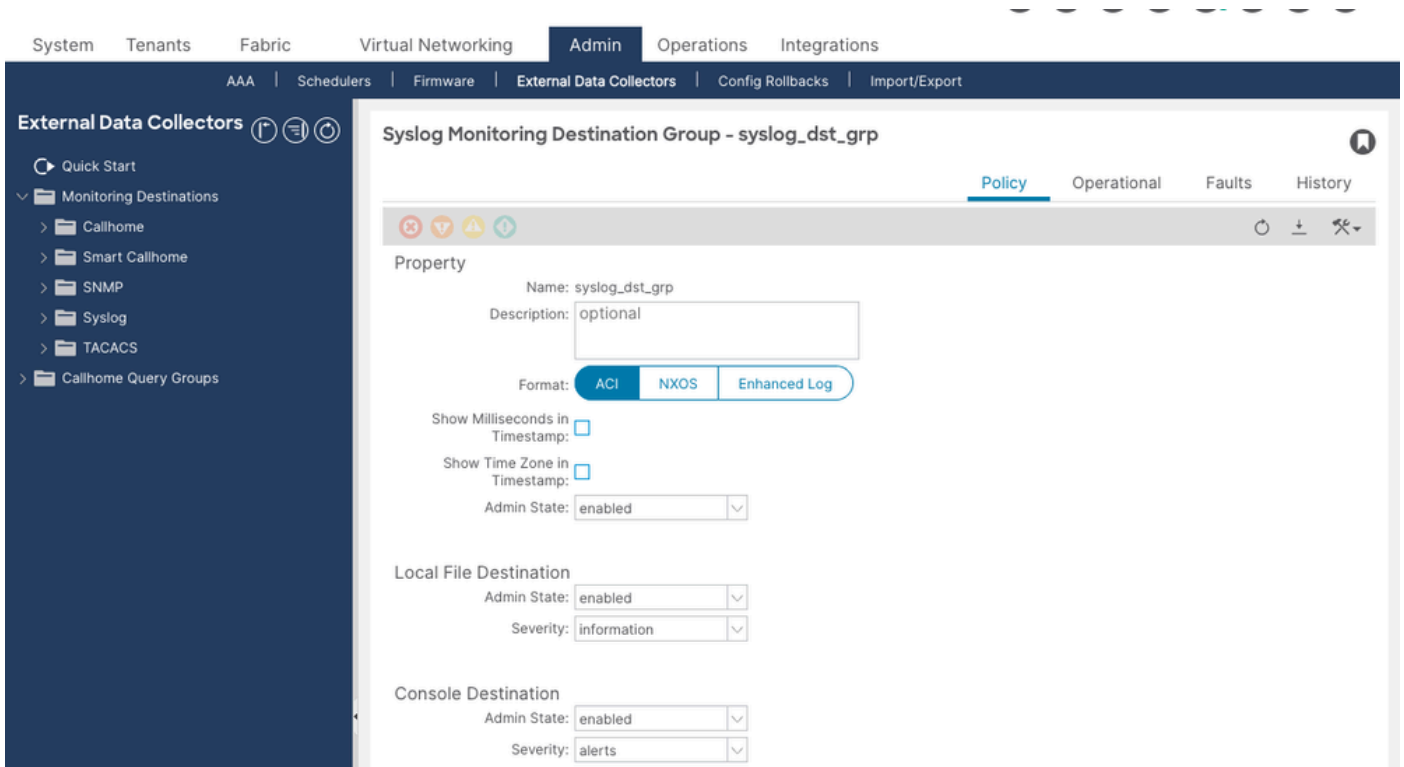
- نارينلل ياسايقلا ميلسنتلا APIC تارا دصلال عي مج يرفوتم — (يضا رتفال) UDP
- نايسننلاو
- ءيناكلما رفوي .ثدخال تارا دصلال او APIC نم 5.2(3) رادصلال نم رفوتم — TCP لوكوتورب
- لاصلال ءهجوم لقن ءيناكلما عم ءقوئوم لئاصوت
- رفشمللا لقنللا رفوي .ثدخال تارا دصلال او APIC نم 5.2(4) رادصلال نم رفوتم — SSL
- لئيمعك (لوحمللا و APIC) (ACI) لوصولاي ف مكحت ءمئاق ءدقع لك لمعت . TLS مادختساب
- Admin > يف APIC لىل مءاخلا ءداهش لئيمحت بجي . syslog مءاخ ب رءاص لاصلتا أدبتو TLS
- تاداهشلا عجارم > ماعللا حاتفملا ءرادا > ني مائللا AAA >

✎ ال رادصا إلى APIC ضفخ مت و SSL لقن مادختساب ةديعب ةهجو نيوكت مت اذا: ةظالم مدخل نكمي هنا نم دكأت UDP إلى ايئاقلت ديغتسي لقنللا لوكوتورب نإف، SSL معددي. يطايتح إءارجك UDP تالاصتإ لوبق اضيأ syslog

نيوكتلا

إلى ةياهنلا نم (ACI) لوصولا يف مكحتلا ةهجاول syslog نيوكتب مق ةيلاللا تاوطخللا مكحت زاهاج APIC لءاوس دح لىلع نم syslog forwarding تنكمت steps in order to ةياهنلا. يرقفلا دومعلا تالوحمو ةيكبشلا قاروالاو

ةومجم ةياغ syslog لءا قتلخ: 1 ةوطخللا



نأل، الءا اءه ءاشنإب مق. قيسنت يءبو syslog لئاسر لاسرا متي نيأ ةهءولا ةومجم دءت مءالاب ةومجملا هءه لىل ريشء ةقءاللا تاوطءللا يف انه نيوكت مت يءللا syslog رءاصم.

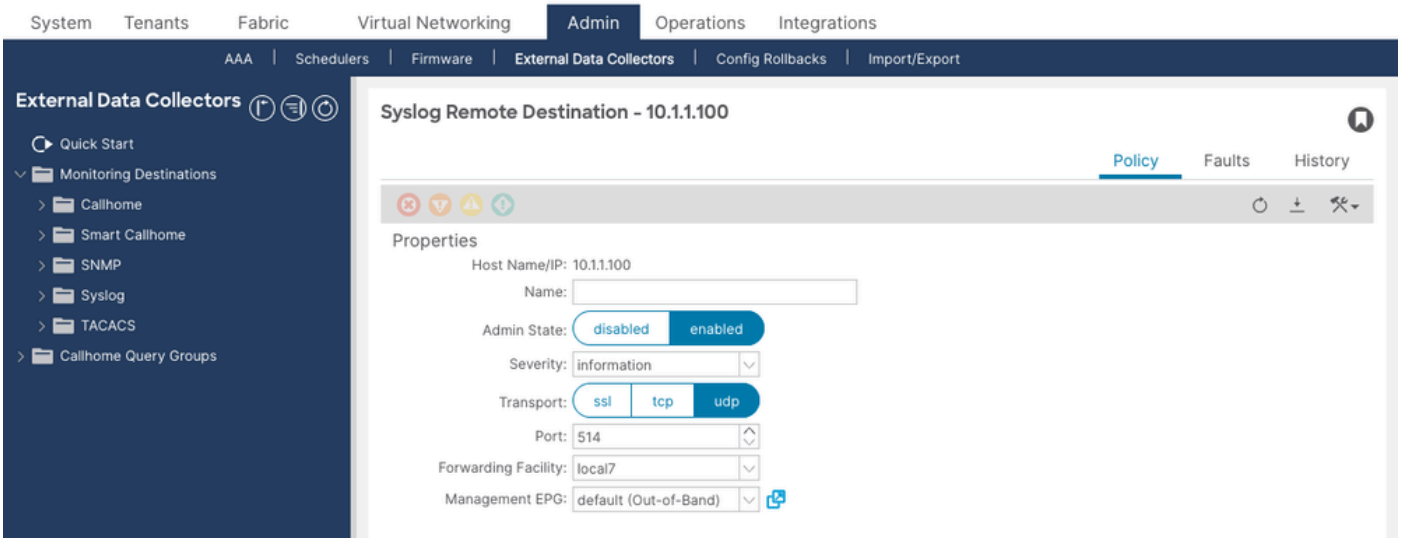
رءب رقنا Syslog. ءاهءولا ةبقارم > ةءراءللا ءانا يءللا ءيمءء تاوءأ > Admin لىل لءقءنا syslog. ةبقارم ةهجو ةومجم ءاشنإ دءو syslog قوف نم يءللا سءامللا

(ةومجملا فيءرءء فلم) لىل ءالءللا في يءللا ام نيوكتب مق، ءءالءملا في

- nxos. أو (RFC 3164 عم قفاوتم ،يضارتفالا) aci — قيسنتلا
- enabled. — ةرادلا ةلاح
- اهل لئاسر ةباتكب اذه موقى .(نستسم) enabled — يلحملا فلملا ةهجو لوؤسم ةلاح
- اهل صاؤ ةيلحملا اطاخال فاشكتسال يرورض وهو ةينب ةدق لك /var/log/external/messages
- هيل لوصولل لباق ريغ ديعبل مداخل نوكي ام دنع ىتح
- information. — يلحملا فلملا ةهجو ةروطخ
- disabled — مكحتلا ةدحو ةهجو ةرادلا ةلاح

ةديعب تاهجو عاشن ةقطنم يف + رقنا ،ةيناثلا ةحفصلا يف .(يلاللا) Next قوف رقنا دعب نع syslog مداخ ةفاضلا

ةديعب ةهجو ةفاضلا : 2 ةوطخال



راوح ةياغ ديعب create syslog ال يف لدان syslog ديعب لا تلاكش

- اذا . فيضملا مسا نم ال دب IP ناو نع مدختسا . syslog مداخ صاخال IP ناو نع — فيضملا
- ماظن مداخ لوصول ةيناكم نم دكأتلا كيلع بجيف ، فيضملا مسا مدختست تنك
- يتلا DNS مداوخ لشفت ناؤنكمي . (OOB) قاطنلا جراخ ةرادلا ةهجاو ربع (DNS) لاجملا مسا
- لئاسر عاشن دنع لجال يف قاطنلا لخاد لاصلتالا لالخ نم طقف اهيل لوصول نوكمي
- ةكبشلا عاطقنا ءانثا syslog
- enabled. — ةرادلا ةلاح
- اذه لئاسر مات يتلا ةروطخلل ىندألا دحلا وه اذه .(نستسم) information — ةروطخال
- ددحملا ديعبل مداخلا
- .(يضارتفا) 514 — ذفنم
- نيوكت مت يتلا قفرملا ةميقة قباطملا اذه نييعتب مق .(يضارتفالا) local7 — ءاشنم
- اههجو تو اهلو بقل كب صاخال syslog مداخ
- وأ (APIC 5.2(3) بلطتي) هب قوؤوملا ميلستلل tcp مدختسا .(يضارتفالا) udp — لقنلا
- (APIC) لئاسر اهليحت مت ةداهشو ثدحا وأ (APIC 5.2(4) بلطتي) رفسملا لقنلل ssl ، وأ ،(ثدحا)

- Management EPG — syslog مداخل إلى لوصولها هي تال EPG لإدارة وعومجم دح — لخاد لإدارة بلسنلاب: uni/tn-mgmt/mgmt-default/oob-default. ضيرعها يدرتال قاطنلا جراخ لإدارة لإغراف لإحلالا اذو نوكي الأ بجي. قاطنلا لإخاد بسانملا EPG دح، قاطنلا

زاجنإ كلذ دعبو، ok تقطقط

نوكي نأ نكمي. ههجولا وعومجم سفن إلى ددعتم ديعب تاهجو ةفاضإ كنكمي: ةظحالما ل. قنوليهست لوكونوربو فلتم ةروطخ دح ههجو لكل

ةساي س fabric monitore ل تحت ردصم syslog تق ل خ: 3 ةوطخال

The screenshot shows the configuration page for 'Callhome/Smart Callhome/SNMP/Syslog/TACACS'. The 'Monitoring Object' is set to 'ALL' and the 'Source Type' is set to 'Syslog'. The table below shows the configuration for the 'syslog' entry.

Name	Include	Min Severity	Destination Group
syslog	Audit logs Events Faults	warnings	syslog_dest_grp

ةينبلا ذفانم — ةينبلا نئاكل يمرهلا جردتال لل syslog نيوكتب ةوطخال هذه موقت ةوطخال) ةكرتشملا ةبقارملا ةساي س لمكي اذو. حوارملا جارداو لكيهلا تانوكمو تاقاطبلا او يمرهلا جردتالاب صاخلا مكحتال عم (4)

> ةيضارتفال > ةبقارملا > تاساي س > ةينبلا تاساي س > ةينبلا إلى لقتنا CallHome/Smart CallHome/SNMP/Syslog/TACACS.

syslog ردصم ءاشنإل + رقنا. syslog إلى ل ردصملا عون نييعتب مق، نميأل اعزجال ي

- Syslog-Source-Fabric لثم يفصو مسا — مسالا
- (ةلمالكلا ةيطغتلل هب صوي) information — ةروطخل نم ىندألا دحلا
- لكشب لمع ةسلج ةفاضاب مق .ءاطخألاو شادخالاو قيقدتلا نم ققحتلا — نيمضت جورخالو لوخدلا ليحست شادخال يرايتخا
- 1. ةوطخل يف اهؤاشنإ مت يتلا ةهجولا ةعومجمل دح — مدقألا ةعومجمل

لاسرا قوف رقنا

ماظنلا يوتسم ىلع syslog) ةكرتشملا ةبقارملا ةسايس نيوكت: 4 ةوطخل

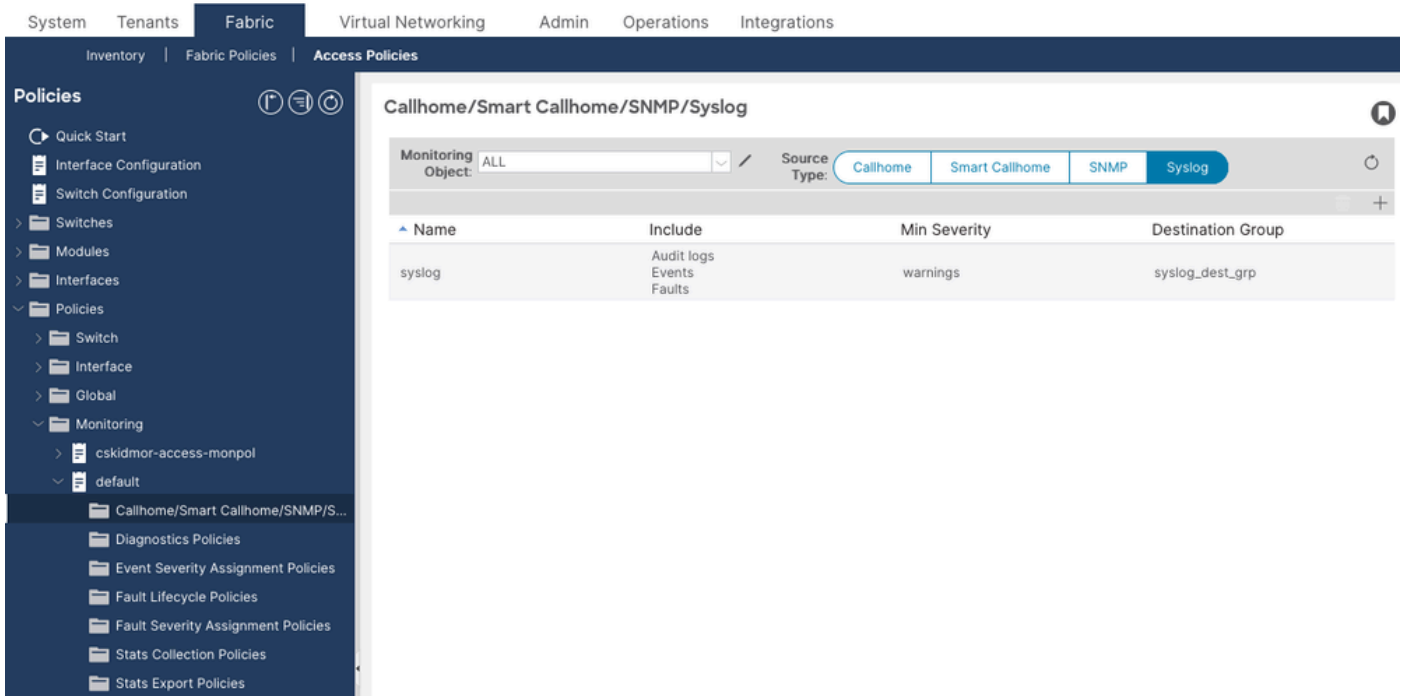
Name	Include	Min Severity	Destination Group
syslog	Audit logs Events Faults	warnings	syslog_dest_grp

اهرشن متي يتلا ماظنلا يوتسم ىلع syslog ةيطغت ةماعلا ةبقارملا ةسايس رفوت ماظنلل syslog ردصم ةوطخل هذه طبرت .ةينبلا يف مكحتلا تادحوو دقعل عيمج ىلا اياقلا ةهجولا ةعومجمل

لا تحت .ةماعلا ةسايسلا > ةبقارملا > تاسايسلا > ةينبلا تاسايس > ةينبلا ىلا لقتنا 1. ةوطخ يف قلخي ةعومجمل ةياغلا ىلا ردصم syslog ماظنلا تطبر ،مسق syslog

DN يف syslogRsSystemDestGroup MO رمألا ةكرتشملا تاسايسلا ماظنلا syslog ردصم مدختسي
uni/fabric/moncommon/systemsrc/rssystemDestGroup.

لوصولا ةبقارم ةسايس نمض Syslog ردصم ءاشنإ: 5 ةوطخل



ةزهجأو لوصول ذفانم — لوصول نئائك ليمرهال جردت لل syslog نيوكتب ةوطخال هذه موقت ةسايس لمكي اذهو (VM) يرهاطال زاهجال في مكحتال ةدحو شادحأو (FEX) ةينبل اسوم يمرهال جردت لل صاخال مكحتال عم (4 ةوطخال) ةكرتشمال ةبقارمل

> ةيضارتفال > ةبقارمل تاسايس > تاسايس > لوصول تاسايس > ةينبل الى لقتنا CallHome/SNMP/Syslog.

3: ةوطخال لثم تادادعال س فن نيوكتب مقو + رقنا syslog. لىل ردصملا عون نييعت

- Syslog-Source-Access، لاثملا لىبس لىل — مسالا
- information. — ةروطخال نم ىندال دحلا
- ءاطخال او شادحال او قيقدتال نم ققحتال — نيحضت
- ةهول ةعومجم س فن دح — مدقال ةعومجملا

لاسرا قوف رقنا

في مكحتال ةمئاق لىل جستل syslog ةلاسرة سايس طبض: (ةيرايتخا) 6 ةوطخال دقعال الى لوصول

System Tenants Fabric Virtual Networking Admin Operations Integrations

Inventory Fabric Policies Access Policies

Policies

- Quick Start
- Pods
- Switches
- Modules
- Interfaces
- Policies
 - Pod
 - Switch
 - Interface
 - Global
 - Monitoring
 - Fabric Node Controls
 - Fault Squelch Policies
 - Common Policy
 - Health Score Evaluation Policies
 - Stats Collection Policies
 - Syslog Message Policies
 - default
 - Callhome/Smart Callhome/SNMP/S...
 - Event Severity Assignment Policies
 - Fault Severity Assignment Policies
 - Fault Lifecycle Policy

System Messages Policy - default

Policy History

Properties

Description: Policy for system syslog messages

Handle Legacy System Messages: Drop Messages Forward Messages and Create Event Records Forward Messages

Facility Filters:

Facility	Severity
local2	alerts
local3	alerts
local4	alerts
local5	alerts
local6	alerts
local7	alerts
lpr	alerts
mail	alerts
news	alerts
syslog	information
user	alerts
uucp	alerts

مزحجلا تالجس ضفر وأ دقعلاب ةصاخلا لوصولا يف مكحتلا ةمئاقلا ءامسلا لىل ءءاب تنك اذا نىيىت بجىف ،دعب نع syslog مءاخ يف روهظلل (ACLLOG_PKTLOG_PERMIT / ACLLOG_PKTLOG_DENY) تامولعمل ءروطخ لىل syslog ءلاسرق فرم ءيىفصت لماع

> ءماعلا ءسايىسلا > ءبقارملا > تاسايىسلا > ءينبلا تاسايىس > ءينب لىل لقتنا قفرم دءء ،تأش نملا ءيىفصت لماع ءمئاق يف .ءيىضارءالا > Syslog ءلاسرق تاسايىس MO AT DN syslogFacilityFilter ءه اءه .information لىل ءروطخل ىنءالء ءءال نىىءو syslog uni/fabric/moncommon/sysmsgp/ff-syslog.

دقعلاب ءصاخلا (ACL) لوصولا يف مكحتلا ءمئاقلا ءامسلا تالجسل ءبسنلاب :ءظءالم بجى (1) :ءورء ءعبراً ءاىىسا بجى ،دعب نع syslog مءاخ لىل لوصولل ضفرل تالجسو ،تامولعمل ءىءىءبلا ءهءولا ءروطخ نوكء نأ بجى (2) ،تامولعمل syslog minSev رءصم نوكى نأ نىىءمء بجى (4) و ،تامولعمل syslog قفرمب صاخلا MinSev ءيىفصت لماع نوكى نأ بجى (3) ،ءءالءل ءورءل ءىمءب ءافول مءى امءنع .دقءلا ءيىفصت لماع لءءءل لىل ءهءءو نم سىل و) يف رءللا لءمءل نم (ACL) لوصولا يف مكحتلا ءمئاق لءس لئاسرأشءءءالءءم .الوأ ءقرولا لىل /var/log/external/messages يف رءظءا ءهءل ءللاب و ،(APIC) تاءءءءل ضفرمق :CoPP ءطساوب ءءءءم دقءلل لوصولا يف مكحتلا ءمئاق مزء لءس يف تالجسل ءضوب ءامسلا و (PPS) ءيىءالءل يف ءمزء 500 ل ءيىضارءالا تالجسل ءقرولءل ءيىءالءل يف ءمزء 300 ل ءيىضارءالا ءضولا

موءءم رىء ءراءءل ءوقء يف ءيىفصءلا لماع لىل ءهءءو لءءءسءل :ءظءالم ءوقء لىل ءطقف دقءلا لىءسء قىبءطء .ءىءوءلا ءءءاق رءش لءش فى ببسءىءو رءءسءملا تانايىب ءوئسم

نيوكتلا نم ققحتلا

رثك ألي سيئرلا ببسلا. اهالصلإو ةيلمعلا اطاخأ فاشكتسأ لبق نيوكتلا نم ققحت
جمانربلا أطخ وأ ةكبشلا سيلاو، ئطاخلا نيوكتلا وه ةدوقفملا syslog لئاسرل اعويش

فيصوتلاو ةهجو لا ةومجملا نم ققحتلا

اهصئاصخ نم ققحتلاو ةهجو لا ةومجم دوجو ديكأتل APIC لىل moquery -c syslogGroup ليغشت

<#root>

```
apic1#  
moquery -c syslogGroup  
Total Objects shown: 1  
# syslog.Group  
name : Syslog-Dest-Group  
dn : uni/fabric/slgroup-Syslog-Dest-Group  
format : aci <--- aci or nxos  
includeMilliseconds : yes  
includeTimeZone : yes  
remoteDestCount : 1 <--- must be ≥1; 0 means no remote dest added
```

moquery -c syslogProf م ادختساب (ةومجملا يوتسم لىل لوؤسم ةلاح) فيصوتلا نم ققحت م

<#root>

```
apic1#  
moquery -c syslogProf  
Total Objects shown: 1  
# syslog.Prof  
dn : uni/fabric/slgroup-Syslog-Dest-Group/prof  
adminState : enabled <--- must be enabled; disabled stops ALL forwarding for this group  
transport : udp  
port : 514
```

ليغشتب مق، قاعم اب صاخلا فيرعتلا فلم ةهجو ةومجم يلىل روثلل

<#root>

apic1#

```
moquery -c syslogProf -x 'query-target-filter=eq(syslogProf.adminState,"disabled")'
```

رظننا اننا ضغب syslog رورم ةكرح يا هيجوت ةداعاب موقت ال ةهجولا ةوومجم نا انه ةجيتننا ينعتو ةديعبلا ةهجولا لوؤسم ةلاح نع

ةديعبلا ةهجولا نم ققحتلا

ةديعب مداخل لك نيوكت نم moquery -c syslogRemoteDest ققحتلل ليغشتلا

<#root>

apic1#

```
moquery -c syslogRemoteDest
```

Total Objects shown: 1

```

# syslog.RemoteDest
dn          : uni/fabric/slogroup-Syslog-Dest-Group/rdst-10.1.1.100
adminState  : enabled <--- must be enabled
epgDn       : uni/tn-mgmt/mgmt-default/oob-default <--- must not be empty
operState   : unknown <--- normal; ACI does not probe syslog servers
severity    : information <--- lower values = less restrictive

```

اصاخ امامتها بلطت تامس ثالث كانه

- يا ددحملا ديعبلا مداخل اذه يقلتني ال، هليطعت ةلاح في enabled. نوكي مزال adminState: عيش.
- نم لسري نا نراق يا فرعي ال شامقلا ينعي epgDn غراف. اغراف نوكي ال بجي epgDn: شامقلا كرتي ةلاسر نم ام كلذل، رورم ةكرح syslog.
- ةهجاو موقت ال. ةلكشم يلا ريشت ال وةعقوتم ةميقلال هذه: فورعم ريغ: ليغشتلا ةلاح ةيناكم يلع لوصحلل لاعف لكشب syslog مداوخ صحفب (ACI) لوصولي فمكحتلا لوصول.

syslog رداصم نم ققحتلا

ةجيجصللا ةبقارملا جهن نمض رداصملا دوجو ديكتال moquery -c syslogSrc ليغشتلا

<#root>

apic1#

moquery -c syslogSrc

Total Objects shown: 2

```

# syslog.Src
dn      : uni/infra/moninfra-default/slsrc-Syslog-Source-Fabric <--- fabric monitoring policy (fa
minSev   : information <--- must match or be lower than remote dest severity
incl     : audit,events,faults

# syslog.Src
dn      : uni/fabric/monfab-default/slsrc-Syslog-Source-Access <--- access monitoring policy (ac
minSev   : information
incl     : audit,events,faults

```

ةبسانملا ةبقارملا تاسايس نمض رداصملا دوجو ديكأت:

- دقعل ايمج ةيطغتل ، ةكرتشملا ةبقارملا ةسايس — uni/fabric/moncommon تحت رداصم لكهلا يوتسم يلع تانئاكلل ةيمرهلا تالسلستلا ايمجو
- ةينبلا يوتسم يلع تانئاكلل ةينبلا ةبقارم ةسايس - uni/infra/moninfra-default تحت رداصم (لكهلا و تاقاطبلا و ةينبلا ذفانم)
- يوتسم يلع تانئاكلل ، لوصول ةبقارم ةسايس — uni/fabric/monfab-default تحت رداصم (ةيضارتفالا ةزهجالا يف مكحتلا تادحو ، FEX ، لوصول ذفانم) لوصول

ةماعلا ةبقارملا جهن ماظنل syslog رداصم طاابترا نم اضيا ققحت

<#root>

apic1#

moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup

Total Objects shown: 1

```

# syslog.RsSystemDestGroup
dn      : uni/fabric/moncommon/systemslsrc/rssystemDestGroup
tDn     : uni/fabric/slgroup-Syslog-Dest-Group <--- must point to your dest group

```

لماع ةروطخ نم ققحتف ، ابولطم دقعلل (ACL) لوصولا يف مكحتلا ةمئاق ليجست ناك اذا
moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog: مادختساب Syslog ةلاسرجهن قفرم ةيفصت

<#root>

apic1#

```
moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog
```

Total Objects shown: 1

```
# syslog.FacilityFilter
facility      : syslog
dn           : uni/fabric/moncommon/sysmsgp/ff-syslog
minSev      : information <--- must be information for ACL logs; default is warnings
```

يحمل لجسلا فلم نم ققحتلا

لئاسر عاشن| ديكأتل ةرشابم رثكألا ةقيرطالا AT /var/log/external/messages يحمل لجسلا فلملا دعي
هنم ققحت. لوصول لباق ريغ ديعبل مداخل نوكي امدنع ىتح، ةينب ةدقع يا ىلع syslog
يفرطحات فم APIC نم لك ىلع:

```
<#root>
```

```
apic1#
```

```
cat /var/log/external/messages | tail -20
```

```
Apr 10 08:25:33 apic1 %LOG_LOCAL0-3-SYSTEM_MSG [F0022][soaking][inoperable][major][topology/pod-1/node-1]
Apr 10 08:30:02 apic1 %LOG_LOCAL0-6-SYSTEM_MSG [F0022][retaining][inoperable][cleared][topology/pod-1/n
```

```
<#root>
```

```
leaf1#
```

```
cat /var/log/external/messages | tail -20
```

```
Apr 10 09:47:14 leaf1 %LOG_LOCAL0-6-SYSTEM_MSG [E4208077][oper-state-change][info][sys/ipv4/inst/dom-Pr
Apr 10 09:51:15 leaf1 %LOG_LOCAL0-6-SYSTEM_MSG [login,session][info][subj-[uni/userext/remoteuser-admin
```

ردصملا يف لئاسرلا عاشن| متي نلف، ةدقع ىلع هثيدحت متي ال وا اغراف فلملا اذه ناك اذا
ةداع| يف ةلكشملا نإف، لئاسر ىقلتي ال ديعبل syslog مداخل نكلو ىوتحم هب فلملا ناك اذا
ةلاسرلا عاشن| يف سي لو، (ةيامحل راج وا ةكبشلا وا ةهولاء ةومجم) هيجوتلا

syslog مداخل ىل لوصول ةينام نم ققحتلا

IP ىل لوصول ةينام نم ققحتلل syslog مداخل ىل APIC نم لاصتا رابتخا ليغشتب مق
ةرادإلا ةكبش ربع

```
<#root>
```

apic1#

```
ping -c 3 10.1.1.100
```

```
PING 10.1.1.100 (10.1.1.100) 56(84) bytes of data.  
64 bytes from 10.1.1.100: icmp_seq=1 ttl=251 time=0.8 ms  
64 bytes from 10.1.1.100: icmp_seq=2 ttl=251 time=0.8 ms  
64 bytes from 10.1.1.100: icmp_seq=3 ttl=251 time=0.8 ms
```

جراخ ةرادإل ا مادختسا VRF دي دحتل -v ةمالع عم iping مدختسا، يسيسئر دوماع وأ ةقروحاتفم نم
ةهوجل هنيي عت متي يرادإ EPG ي بسح، يددرتلا قاطنلا لخاد mgmt:inb وأ يددرتلا قاطنلا
syslog:

<#root>

leaf1#

```
iping -V management 10.1.1.100
```

```
PING 10.1.1.100 (10.1.1.100): 56 data bytes  
64 bytes from 10.1.1.100: icmp_seq=0 ttl=59 time=1.324 ms  
64 bytes from 10.1.1.100: icmp_seq=1 ttl=59 time=0.622 ms  
  
--- 10.1.1.100 ping statistics ---  
2 packets transmitted, 2 packets received, 0.00% packet loss  
round-trip min/avg/max = 0.622/0.973/1.324 ms
```

<#root>

leaf1#

```
iping -V mgmt:inb 10.1.1.100
```

```
PING 10.1.1.100 (10.1.1.100): 56 data bytes  
64 bytes from 10.1.1.100: icmp_seq=0 ttl=58 time=0.833 ms  
64 bytes from 10.1.1.100: icmp_seq=1 ttl=58 time=0.608 ms  
  
--- 10.1.1.100 ping statistics ---  
2 packets transmitted, 2 packets received, 0.00% packet loss  
round-trip min/avg/max = 0.608/0.72/0.833 ms
```

و UDP ذفنمب حامسلا دكؤي ال هنكلو IP لىل لوصولا ةينام إ حجانلا لاصتالا رابتخا دكؤي
syslog لوكوتوربو (ICMP) تنرتنإل ي ف مكحتلا لئاسر لوكوتورب مدختسي. TCP 514.
ةفلتخم تالوكوتورب

اهال صإو ءاطخال ا فاشكتسا

ديع بل مداخل ال syslog لئاسر لصت ال ام دن ع قيلاتل تارارقلا ةرچش مدختسأ

```
No messages at remote syslog server
|
└─ Step 1: Check /var/log/external/messages on APIC and a leaf
|   └─ File is EMPTY or not updating
|   └─ No messages are being generated at the source. Proceed to configuration checks:
|       └─ Is a syslogSrc configured and linked to the destination group?
|           └─ Is minSev set to information?
|               └─ Does incl include audit, events, and faults?
|                   └─ File HAS CONTENT (messages are generating locally)
|                       └─ Problem is in forwarding to the remote server. Continue to Step 2.
|                           └─ Step 2: Check syslogProf adminState
|                               └─ adminState = disabled → Enable it. This stops ALL forwarding from this group.
|                                   └─ Step 3: Check syslogRemoteDest adminState
|                                       └─ adminState = disabled → Enable it. This stops messages to this specific server.
|                                           └─ Step 4: Check syslogRemoteDest epgDn
|                                               └─ epgDn is empty → Set the correct Management EPG (OOB or in-band).
|                                                   └─ Step 5: Verify network reachability
|                                                       └─ Run on the APIC: ping -c 3 10.1.1.100
|                                                           └─ ping FAILS → routing/firewall issue; verify OOB routing table and firewall rules
|                                                               └─ ping SUCCEEDS → IP reachable; check firewall for UDP/TCP port 514 specifically

Messages from some nodes or object hierarchies are missing
└─ Check Common Policy – is it linked to the destination group?
    └─ Verify: moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup
        └─ Not linked → Configure Common Policy (Step 4) for fabric-wide coverage
            └─ Also check Fabric and Access policy sources for hierarchy-specific coverage

Messages arrive but important events are missing
└─ Check syslogSrc minSev AND syslogRemoteDest severity
    └─ Both must be information for full coverage; the more restrictive of the two applies
```

ةعئاشل تاهويرانيسل

ديع بل مداخل ال syslog لئاسر ي قلت متي مل: 1 ويرانيسل

ال لئاسر ي لصت ال نكلو، ةديع بل ةهوجل او syslog ةهجو ةومجم نيوكت مت: ةلكشم ال
تالخد ا لعل تالوحم ل او APIC لعل /var/log/external/messages ي لحمل فل مل يوتحي. ديع بل مداخل
ةثيدح.

نيوكتل صحت:

<#root>

apic1#

```
moquery -c syslogRemoteDest
```

```
# syslog.RemoteDest
host          : 10.1.1.100
adminState    : disabled <--- PROBLEM: remote destination is disabled
epgDn         : uni/tn-mgmt/mgmt-default/oob-default
```

ههوجلوا عاشنن مت اذا كلذ ثدحي نأ نكمي disabled. هه ةديعبلا ههوجلوا لوؤسم ةلاح: يرذجال ببسلا ادبأ ههنيكمت متي ملو ةنايصلل اناثأ اهليطعت مت اذا وأ، دصق نود ةلطمع اهكرت مت نكلو

مس] > Syslog > تاهوجلوا ةبقارم > ةيخراخلل تانايبلا عيجمحت تاودأ > Admin لىل لقتنا: لجلل لوؤسملا ةلاح نييعتو ةديعبلا ههوجلوا ريرحتب مق. [مداخل] > ةديعبلا تاهوجلوا > [ةومجملل نكمم لىل

Syslog ههوجلوا ةومجم فيرعت فلم ليطعت مت: يناثلا ويرانيسلل

ههوجلوا لوؤسم ةلاح نيكمت مت ولو ىتح ةدقع يأ نم لئاسر يأ هيجوت ةداعإ مت ال: ةلكشملا ةديعبلا

نيوكتل صحت:

<#root>

apic1#

```
moquery -c syslogProf -x 'query-target-filter=eq(syslogProf.adminState,"disabled")'
```

Total Objects shown: 1

```
# syslog.Prof
dn          : uni/fabric/slgroup-Syslog-Dest-Group/prof
adminState  : disabled <--- PROBLEM: group profile is disabled
transport   : udp
```

ال، اهليطعت دنعو. اهلمكأب ههوجلوا ةومجم يف ةرادالل syslogProf ةلاح مكحتت: يرذجال ببسلا ةيدرلل ةديعبلا ههوجلوا تالاح نع رظنلل ضغب ةدقع يأ نم لئاسر يأ هيجوت ةداعإ مت

مسار Syslog > تاهجول ةبقارم > ةيجراخال تانايبلا ةيمجت تاودأ > Admin لىل لقتنا: لجال
نكمم لىل لوؤسملا ةلاح نييعة و فيرعتلا فلم ريرحتب مق. [ةوومجملا

طبترم ريغ ةماعلا ةبقارملا جهن - ةدوقفملا ثادخال 3: ويرانيسللا

مداخالا لىل تانئاكل ةيمرهلا تاجردتلا وأ دقعل اضعب نم Syslog لئاسر لصت ال: ةلكشملا
"ةنبلا وأ لوصول ةبقارم جهن" نمض syslog رصم نيوكت مت ناو ىتح، ديعللا

نيوكتلا صحف:

<#root>

apic1#

```
moquery -d uni/fabric/moncommon/systemslsrc/rssystemDestGroup
```

Total Objects shown: 0

ةهجولا ةوومجمب طبترم ريغ ةكرتشملا ةبقارملا جهن ماظنل syslog رصم

يوتسم لىل syslog ةيطغت (uni/fabric/moncommon) ةكرتشملا ةبقارملا جهن رفوي: يرذجال ببسللا
مكحتلا تادحوو دقعل ةيمج لىل ةيئاقلت هرشن متي و ةيمرهلا تاجردتلا ةيمج ربع ةنبلا
ةيمرهلا تاجردتلا وأ ةددملا ةنبلا قباطت يتلا ثادخال ةيجوت ةداع متت، كلذ نودبو
(uni/infra/moninfra-default) ةنبلا ةبقارم ةساي س يطغت. طقف لوصول ةبقارم ةساي سل
(uni/fabric/monfab-default) لوصول ةبقارم ةساي س يطغتو، ةنبلا يوتسم لىل تانئاكل
اهمدقت يتلا ةنبلا قاطن لىل ةيطغتلا رفوت ال اهنكلو، لوصول يوتسم لىل تانئاكل
ةكرتشملا ةساي سل

ةماعلا ةساي سل > ةبقارملا > تاساي سل > ةنبلا تاساي س > ةنبلا لىل لقتنا: لجال
moquery -d عم تققد. ةوومجم ةيغال لىل رصم syslog ماظنلا تطبر، مسق syslog ل تحت
ةهجولا ةوومجم لىل tDn طاقنلا نأ uni/fabric/moncommon/systemslsrc/rssystemDestGroup

ةدوقفم ةعقوتملا لئاسرلا — ةيغالل ديقم ةروطخلا يوتسم 4: ويرانيسللا

لجس تالخدأ وأ ةيغال ةلثادخال نكلو، syslog مداخالا لئاسرلا اضعب لصت: ةلكشملا
ةريطخلا بويعلل يوس ىرت الو. ةدوقفم لمعلا ةسلج لىل لوخدلا ليحست ثادخال وأ قيقدتلا
ةيرهوجل او

نيوكتلا صحف:

apic1#

```
ping -c 3 10.1.1.100
```

```
PING 10.1.1.100 (10.1.1.100) 56(84) bytes of data.  
64 bytes from 10.1.1.100: icmp_seq=1 ttl=251 time=0.8 ms  
64 bytes from 10.1.1.100: icmp_seq=2 ttl=251 time=0.8 ms  
64 bytes from 10.1.1.100: icmp_seq=3 ttl=251 time=0.8 ms
```

م تي ام نيپ (لاصتال رابتخا) ICMP رمي . لصت ال syslog لئاسر نكلو ، لاصتال رابتخا حجني
UDP 514 ذفنم رطح

ةرادال اكبش نيپ (ACL) لوصول ايف مكحتال ةمئاق و اةي امحل رادج موقوي : يرذجل ا بسلا
UDP و ICMP . TCP لقن نيوكت مت اذا TCP 514 (و UDP 514 ذفنم رطح syslog م داخو
لك لسرت ، كلذى لى لة فاضال ابو . هب حومسم UDP 514 ن ICMP ريرمت دكؤي ال — نالقتسم
رادج موقوي . (OOB) قاطنل چراخ اهب صاخال IP ناوع نم ةرشابم syslog يسير قش و ةقرو
دقع نم أشنت يتل syslog مزح طاقساب APIC OOB IPs لوكوت وربل طقف حمسي يذلا ةي امحل
تال و حمل

قاطنل چراخ IP ناوع قاطن نم UDP/TCP 514 ذفنمب حمسي ةي امحل رادج نأ نم ققحت : ل حل
عيجو ، ةيفرطال تال و حمل ا عيجو ، APICs عيج كلذيف امب — ةينبال دقع عيجل (OOB)
لصت UDP 514 مزح تناك اذا ام syslog م داخ لى لة مزحل طاقتل دكؤي . يسيرللا دومعلا تال و حمل
ال مأ

لصت ال يتل دقل اب ةصاخال لوصول ايف مكحتال ةمئاق صفر/حامس تال جس : 8 ويراني سل

ACLLOG_PKTLOG_PERMIT /
ACLLOG_PKTLOG_DENY) مزحل تال جس صفر و دقل نذا لصي ال : ةلكشملا
syslog م داخ لى لة

نيوكتل صحف :

information: 1. هـ syslog ردصم ةروطخ نم ققحتال
<#root>

apic1#

```
moquery -c syslogSrc
```

```
# syslog.Src
```

```
minSev : information <--- must be information; any higher value drops ACL logs
```

information: 2. ةديعبال ةهول ةروطخ نم ققحت
<#root>

apic1#

```

moquery -c syslogRemoteDest
# syslog.RemoteDest
severity : information <--- must be information

```

3. information: وهو syslog لئاسر جهن قفرم ةيفصت لماع ةروطخ نم ققحتلا

```
<#root>
```

```
apic1#
```

```
moquery -d uni/fabric/moncommon/sysmsgp/ff-syslog
```

```
# syslog.FacilityFilter
```

```
facility : syslog
```

```
minSev : information <--- must be information; default is warnings which drops ACL logs
```

4. > نيرجات سمل الى لقتنا. دقعل ةيفصت لماع ىلع لجسلا هيچوت نيكمت نم ققحت

ديكأتو ةيفصتلا لماع > [عوضوملا] > عيضاوملا > [دقعل] > دوقعلا > [رجأت سمل]

ةلصللا يذحشرملا لاخدا ل لجسلا ضرعي تاهيچوتلا دومع

5. أشنت) يفرطال لوحمل الى ع (ACL) لوصولا يف مكحتلا ةمئاق تالجس عاشن! نم ققحت

(APIC) نم سيلو، ةقرولا نم لوصولا يف مكحتلا ةمئاق تالجس

```
<#root>
```

```
leaf1#
```

```
show logging ip access-list internal packet-log deny
```

```
<#root>
```

```
leaf1#
```

```
cat /var/log/external/messages | grep ACLLOG | tail -20
```

ةقرولا ىلع لجسلا عاشن! قلطي ال لجسلا هيچوت نإف، تالخد ACLLOG يف رهظت مل اذا

رورم ةكرح دجوت ال هنا وأ، حيحص لكش ب نوكم ريغ دقع هيچوت الى كلذ ري شي نأ نكمي

اهلچست لبق مزحلا طاقساب موقوي CoPP لدعم ديحت نأ وأ، دقعل الى لصت ةقباطم

(6) يوتسم informational syslog) لوصولا يف مكحتلا ةمئاق لجس ةروطخ يوتسم: يردجال بلسلا

وأ severity ةديعبل ةهوجل وأ minSev ردصملا — syslog ةلسلس يف ةيفصت لماع يف نييعت مت اذا

، هالع — (syslogFacilityFilterat uni/fabric/moncommon/sysmsgp/ff-syslog) syslog ةلسر جهن قفرم ةيفصت لماع

ةدقع كرت لبق تمص ب لوصولا يف مكحتلا ةمئاق لجس لئاسر طاقساب متي information

ةلنبل.

، ديعب ةيغال الى ع information الى تبثي، ردصم syslog ال information severity الى minSev تتبث: لجال

> ةسايس ةلسر syslog > ةماع ةسايس تحت الى minSev information حشرم قفرملا syslog تتبث

ال حمسي ةيامجال راج نأ تقق دو، حشرم دقعل الى ع تنكم نوكي هيچوت log ل تذكأ، ريصقت

مكحتلا ةمئاق نأل، APICs ل طقف سيل، ناو نع قاطن چراخ حاتفم ةقرولا نم رورم ةكرح syslog

حاتفملا نم لجس تلسرراً لوصولاب

(ACI) لوصول في مكحتللا هجاول syslog ةفيظو ىلع ةيلتلا ةفورعلملا جماربلا بوي ع رثوت

- ميسلست syslog فوقوي ةومجم ةياغ syslog ل يمست ةداع | — [CSCwj23752](#) id ق ب cisco
ثدحال تارادصل او 6.0(6c) رادصل APIC في تباث

ديصتلا ريعام

امدنع Cisco TAC عم كرتشاو في نم معد عمج

- ةومجم نم لك في ، ةينبالا دقع ىلع ايلحم `/var/log/external/messages` في syslog لئاسر رهظت متي و ، احيحص Management EPG نوكي و `enabled` ، ةديعبلا ةهجولا لوؤسم تالاحو ةهجولا راج صحف ريرمتو لاصلتالا رابتخا ةيلمع) ةكبشلا ىل لوصولا ةينام اديكات ديعبلا مداخللا ىل لصت ال لئاسرلا لازت ال نكلو ، (ةيامحلا
- دوجو مدع عم ، ىرخا دقع ىل لصت ال اهنكلو ةينبالا دقع ضعب نم Syslog لئاسر لصت ةساي سلا رشن في قاستا مدع دوجو ىل ريشي امم ، اهنب نيوكتلا في قرف
- فانئتسا متي ال نكلو ةديعبلا ةهجولا و ةهجولا ةومجم فيرعت فلم نيكمت ةداع مت نيوكتلا ريعت نم ةليلق قئاقد نوضغ في لئاسرلا
- لم تحت بعي دوجو ىل ريشي امم ، APIC ةيقرت دعب لوصولا نع syslog لئاسر تفتقوت جماربلا في

ةينفلا ةدعاسملا زكرم ةلاح حتف لبق اهيجمت متيس يتلا تانايبلا

- ةررضتم ةيقررو ةدقعو ررضتملا APIC نم بلطال بسح ينفلا معدلا
- هنم `moquery -c syslogGroupAPIC moquery -c syslogProf9 moquery -c syslogRemoteDest9 moquery -c syslogSrc` جتان
- كرتشملا جهنلا طابترا نم `moquery -d uni/fabric/moncommon/systems/src/rssystemDestGroup` ققحتلل جارخا
- ةرثاتم قاروا ةذوب نم ةرجش `/var/log/external/messages` نم ليد
- نيوانع نم لصت 514 UDP/TCP مزح تناك اذا ام دكوي يذلا syslog مداخل نم ةمزحلا طاقتلا ةيفيللا OOB

عجارملا

- [قرا دالا — 6.1\(x\) رادصل ، Cisco APIC لئاسرلا نيوكتلا ليد](#)
- [Cisco ACI ماظن لئاسر عجم ليد](#)
- [Cisco نم ماظنلا لئاسر و ثادجال او \(ACI\) لوصولا في مكحتلا ةمئاق عاڤخا قرا دالا ليد](#)
- [Cisco نم \(ACI\) لوصولا في مكحتلا ةهجاو دقع ليدل يمسرلا ريرقتلا](#)
- [اهجالص او ةئيط APIC مدختسم ةهجاو عاڤخا فاشكتسا](#)

