ةيضارتفالا ةيباحسلا ةئيبلا لماكت ةكبشو ةمدقتملا ةيامحلاب ةصاخلا تاديدەتلا

تايوتحملا

<u>ةمدقملا</u> <u>ةىساسالا تابلطتملا</u> <u>تابلطتملا</u> ةمدختسملا تانوكملا <u>ةىساساً تامولعم</u> لماكتلا ةىن <u>لماكتلا لوح ةيساساً تامولعم</u> ءارجإلا SSL تاداەش ءاشنا ةداع <u>SSL تاداەش لىمحت</u> <u>اىتاذ ةعقوم تادىدەتال قكيش زاەجل ةفىظنال قەجاولا ىف قدوجومال قداەشلا</u> عجرم ليق نم تادىدەتلا قكيش زاەجل قفىظنلا قەجاولا ىف قدوجوملا قداەشلا عىقوت متى <u>(CA) ىسسۇم قدصم</u> لاثم ققحتلا <u>ةصاخلاا AMP ةباحس تانايب ةدعاق يف ةنيعلل يئاهنلا ريصملا ثيدحت ديكأت</u> ل<u>اثم</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>مل ،ةداەش لارات خامت مل ،حلاص رىغ فىضملا لوج AMP ل صاخلا قباحس لازاەج ىف رىدەت </u> API ج<u>اتفم رابتخا متي</u> <u>حلاص ريغ تاديدهت ةكبشل API حاتفم لوح AMP ل صاخلا ةباحسالا زامج يف ريذجت</u> ،(AMP) قمدق تمل القي المحل اب صراخل القك بش ل الزامج قطس اوب 95=< جئ اتن ل الجذامن مال تس المتي <u>ةنيعلل يئاەنلا ريصملا يف رييغت يأ ةظحالم متي ال نكلو</u> <u>قحلاص ريغ تاديدهت ةكبشل SSL قداهش لوج AMP ل صاخلا قباحسلا زاهج يف ريذجت</u> <u>تاداەشلاب قۆلەتملا دىدەتلا قكېش زاەج يە قدوجوملا تارىدەتلا</u> <u>قباطتم ريغ صاخ حاتفم نم دمتسملا ماعلا حاتفملا - ريذحت ةلاسر</u> <u>PEM ریغ یوتجم یلع صاخلا جاتفملا یوتحی - ریذجت ةلاسر</u> <u>صاخلا جاتفملا نم ماع حاتفم ءاشنا نكمي ال - ريذحت ةلاسر</u> مداخلا/ليمعلل قدصم عجرم قداهش تسيل - ريذحت قلاسر <u>ةلص تاذ تامولعم</u> ةمدقملا

نم ةمدقتملا ةيامحلل ةيرهاظلا ةصاخلا ةكبشلا لماكت لامكا ءارجا دنتسملا اذه فصي تاوطخ دنتسملا رفوي امك .تاديدهتلا نم ةيامحلا ةكبش زاهجو (AMP) ةراضلا جماربلا اهحالصاو لماكتلا ةيلمعب ةقلعتملا تالكشملا فاشكتساً.

.Cisco نم TAC سدنهم ،ايسراغ ودنامرأ ةطساوب ةمهاسملا تمت

ةي س اس أل ات اب لطت مل ا تاب لطت مل

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- اەليغشتو ةيضارتڧالا ةصاخلا AMP ةكبش ىلع لمعلا •
- ةيامحلا تاديدهت ةكبش ليغشتو لمعلا •

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- AMP Private Cloud، رادصإلاا 3.2.0
- 2.12.0.1 تاديدەتلا ةكبش زاەج •

يف ةصاخلا AMP ةكبش ةزهجأو تاديدهتلا ةكبش ةزهجأل ةحلاص قﺉاثولا نوكت :**قظحالم** يرهاظلا رادصإلا وأ زاهجلا.

. (). .

ةيساسأ تامولعم





لماكتلا لوح ةيساسأ تامولعم

- هباحس زاهج ةطساوب اهلاسرا مت يتلا تانيعلا "تاديدهتلا ةكبش" زاهج للحي صاخلا.
- ديدەتلا ةكبش زاەج ىلإ ايئاقلت وأ ايودي جذامنلا لاسرا نكمي.
- .ةصاخلا AMP ةباحس زاهج يف يضارتفا لكشب يئاقلتلا ليلحتلا نيكمت متي ال •
- .ةنيعلا ليلحت نم ةجردو اريرقت صاخلا AMP ةباحس زاهجل تاديدهتلا ةكبش زاهج رفوي •

- وأ ديزت ةنيع يأ نع "ةصاخلا AMP ةكبش" زاهج مالعإب (poke) "ةيامحلا ةكبش" زاهج موقي .ةجرد 95 يواست
- ةنيعلاا ىلع ةمالع عضو متي ،95 يواست وأ 95 نم ربكأ ليلحتلا نم ةجيتنلا تناك اذإ ةراضلا ءايشألا يف فرصتلاب AMP تانايب ةدعاق يف ةدوجوملا.
- تانيعلاا ىلع AMP Private Cloud ةكرش لبق نم يعجر رثأب فشكلا تايلمع قيبطت متي 95. يواست وأ نم ربكأ ةمالع ىلع يوتحت يتلا

ءارجإلا

دوجو نم ققحت .(دعب لماكت دجوي ال) ەنيوكتو تاديدەتلا ةكبش زاەج دادعإب مق.1 ةوطخلا رمألا مزل اذإ ،تيبثتو تاثيدحت.

(دعب لماكت دجوي ال) ةياهنلا طاقنب ةصاخلا ةباحسلل AMP نيوكتو دادعإب مق.2 ةوطخلا.

رتخاو **نيوكت** بيوبتلا ةمالع ددح ،تاديدەتلا ةكبش ةرادا مدختسم ةەجاو يف .3 ةوطخلا SSL.

.(PANDEM) ةفيظنلا ةهجاولل ةديدج SSL ةداهش ليمحتب مق وأ ئشنأ.4 ةوطخلا

SSL إعادة إنشاء شهادات

(SAN) يمكن إنشاء شهادة موقعة ذاتيا جديدة إذا لم يتطابق اسم المضيف للواجهة النظيفة مع الاسم البديل للموضوع في الشهادة المثبتة حاليا في جهاز الواجهة النظيفة. يولد الجهاز شهادة جديدة للواجهة، مما يشكل اسم مضيف الواجهة للشهادة التوقيع الذاتي SAN الحالي في حقل.

الخطوة 4.1. من عمود الإجراءات حدد (..) ومن القائمة المنبثقة حدد **إنشاء شهادة جديدة**.

الخطوة 4.2. في واجهة مستخدم شبكة التهديد، حدد **عمليات**، في الشاشة التالية حدد **تنشيط** واختر **إعادة التكوين**.

ايتاذ ةعقوم ةأشنملا ةداهشلا هذه :**ةظحالم**.

SSL تاداەش ليمحت

نكمي ،"تاديدەتلا ةكبش" زاەج فيظنت ةەجاول لعفلاب اەۋاشنإ مت ةداەش دوجو ةلاح يف زاەجلا ىل| ةداەشلا ەذە ليمحت.

.**ةديدج ةداەش ليمحت** ددح ةقثبنملا ةمئاقلا نمو **(..)** ددح تاءارجالا دومع نم 4.1 ةوطخلا

يتلا صنلا تاعبرم يف PEM قيسنتب فدارملا صاخلا حاتفملاو ةداهشلا خسنا 4.2. ةوطخلا **ق**دا<mark>مش ةفاض ا</mark> ددحو ةشاشلا يلع رمظت.

ددح ةيلاتان المشاشل اليف ،**تايلمع** ددح ،ديدهتلا المكبش مدختسم قمجاو يف .4.3 قوطخلا المداعة المالي المنافع ا

رتخاو **لماكتلا تايلمع** ددح ،AMP Private Cloud Device Admin مدختسم ةهجاو يف .5 ةوطخلا ت**اديدەتلا ةكبش**.

ر**يرحت** ددح ،ديدەتلا ةكبش نيوكت ليصافت يف .6 ةوطخلا.

زاهجل ةفيظنلا ةهجاولاب صاخلا FQDN لخدأ ،تاديدهتلا ةكبشل فيضملا مسا يف .7 ةوطخلا تاديدهتلا ةكبش.

ةكبش زامجل ةفيظنلا ةمجاولا ةدامش فضأ ،تاديدمتلا ةكبشل SSL قدامش يف .8 ةوطخلا (ماندأ تاظحالملا رظنا) .تاديدمتلا

الشهادة الموجودة في الواجهة النظيفة لجهاز شبكة التهديدات موقعة ذاتيا

.SSL الخطوة 8.1. في واجهة مستخدم "إدارة شبكة التهديدات"، حدد **التكوين واختر**

الخطوة 8.2. من عمود الإجراءات حدد **(..)** ومن القائمة المنبثقة حدد **تنزيل الشهادة**.

في صفحة تكامل AMP الخطوة 8.3. قم بالمتابعة لإضافة الملف الذي تم تنزيله إلى الجهاز الخاص الظاهري من شبكة التهديدات.

يتم توقيع الشهادة الموجودة في الواجهة النظيفة لجهاز شبكة التهديدات من قبل مرجع مصدق (CA) مؤسسي

.الكاملة CA الخطوة 8.1. انسخ في ملف نصي شهادة الواجهة النظيفة لجهاز شبكة الحماية وسلسلة شهادات

. PEM قيسنتب يصنلا فلملا يف ةدوجوملا تاداهشلا نوكت نأ بجي :**قظحالم**

ةداەش :يە ةلماك تاداەشلا ةلسلس تناك اذإ THREAT_GRID_CLEAN_INTERFACE تەزام ئۇلىف ؛THREAT_GRID_CLEAN_INTERFACE يف حضوم ۋە امك ،يصنلا فلملا ةروصلا

-----BEGIN CERTIFICATE-----

Threat_Grid_Clean_Interface certificate PEM data

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

ROOT_CA certificate PEM data

-----END CERTIFICATE-----

ةداەش < Sub_CA ةداەش < ROOT_CA قداەش :يە ةلماك تاداەشلا ةلسلس تناك اذا يف حضوم وہ امك ،يصنلا فلملا ءاشناٍ مزليف ؛THREAT_GRID_CLEAN_INTERFACE . قروصلا

BEGIN CERTIFICATE							
Threat_Grid_Clean_Interface certifi	ta						
END CERTIFICATE							
BEGIN CERTIFICATE							
Sub_CA certificate PEM data							
END CERTIFICATE							
BEGIN CERTIFICATE							
ROOT_CA certificate PEM data							
END CERTIFICATE							
9. (API) API .							
API							
API Key	*******	*********	**** ● 唱				
Disable API Key 👔	True	False	Unset				
Can Download Sample	True	False	Unset				
Content Via API 👔							

ة ملعملا نأ مدختسملا دكؤي ،تاديدەتلا ةكبش نم باسحلا تادادعإ يف :**قظحالم** API Key قملعملا نأ مدختسملا ديغ مريغ True.

ظ**فح** ددح ،تارييغتلا ةفاك لامتكا دعب .10 ةوطخلا.

AMP. نم يرهاظلا ةباحسلا زاهج ىلع نيوكت ةداعا ةيلمع قيبطت .11 ةوطخلا

قكبش رتخاو **لماكتلا تايلمع** ددح ،صاخلا AMP قباحس زاهج مدختسم قهجاو نم .12 قوطخلا ت**اديدەتلا**.

مدختسمو ،يئاەنلا ريصملا ثيدحت ةمدخل URL ناونع ميق خسنا **ليصافتلا** نم .13 ةوطخلا ەذە مادختسإ متي .يئاەنلا ريصملا ثيدحت ةمدخ رورم ةملكو ،يئاەنلا ريصملا ثيدحت ةمدخ 17. ةوطخلا يف تامولعملا

.**CA تاداەش** رتخاو **نيوكت** ددح ،ديدەتلا ةكبش ةرادإ مدختسم ةەجاو يف .14 ةوطخلا

ةمدخ ةداهش ىلع تعقو يتلا CA ةداهش PEM قيسنتب خسنو **ةداهش ةفاضإ** ددح .15 ةوطخلا

هي شهادة AMP التي وقعت على شهادة تحديث الترتيب السحابي الخاص ل CA **ملاحظة**: إذا كانت شهادة A. مرجع مصدق فرعي، فكرر العملية حتى يتم تحميل جميع الشهادات المصدقة في السلسلة إلى **شهادات**

.الخاصة AMP الخطوة 16. في مدخل شبكة التهديدات، حدد إدارة وحدد إدارة تكامل سحابة

.الخطوة 17. في صفحة "خدمة مشاركة تحديث المصير النهائي"، أدخل المعلومات التي تم تجميعها في الخطوة 13.

- URL صاخلاا ةباحسلا زامجل يئامنلا ريصملا ثيدحت ةمدخب صاخلا FQDN : ل AMP.
- الماخلاا ةباحسلا زاهجل يئاهنلا ريصملا ثيدحت ةمدخ نم مدختسملا :مدختسملا AMP.
- . صاخلا AMP ةباحس زاهجل يئاهنلا ريصملا ثيدحت ةمدخل رورم ةملك :رورملا ةملك •

حاجنب لماكتلا لمعي نأ بجي ،حيحص لكشب تاوطخلا عيمج قيبطت مت اذإ ،ةلحرملا هذه يف.

ققحتلا

....

جاتنإ ةئيب يف قيبطتلل ةبسانم طقف 4 و 3 و 2 و 1 تاوطخلا نوكت :**قظحالم** الو لماكتلا لوح ديزملا ةفرعمل تامولعمك 5 ةوطخلا ريفوت متي .لماكتلا نم ققحتلل جاتنا ةئيب يف اهقيبطتب حصني.

1. AMP Private Cloud Device Admin UI > > Threat Grid ! .

eat Grid Con	guration Details	Edit
Hostname	cisco.com	
API Key	Q	
Threat Gri	I SSL Certificate	≓ Test Connection
Issuer	subca_tga_clean	
Subject	.cisco.com	
Subject		

tus
Integrations
Support

Threat Grid Connection test successful!

2. AMP .

CISCO AMP for Endpoints		armando garcia ~
Dashboard Analysis v Outbreak Control v Management v Accou	s ~ Search	٩
File Analysis	earch by SHA-256, File name, IP, Keywords ile Analyses to view	Q Submit File . ⊟ ⊞

ةباحسلا مكحت ةدحو **لـيلحت** نم ايودي اهلاسرا متي يتلاا تافلملا كاردا نم دكأت .3 ةوطخلا ةدحاو ةطقنب ريرقت عاجرا نمو ،"تاديدهتلا ةكبش" زاهج يف **تافلملا لـيلحت <** AMP ل ةصاخلا تاديدهتلا قكبش" زاهج قطساوب.

Case AMP for Endpoints			armando garcia ~
Dashboard Analysis - Outbreak Control - Management - Account	unts ~	Search	Q
File has been uploaded for analysis			×
File Analysis			
	Search by SHA-256, File name, IP,	Keywords	🔍 🔤 🏝 Submit File 📋 🕀
There are no	o File Analyses to view		
cisco AIVIP TOT Endpoints			armando garcia 🗸
Dashboard Analysis V Outbreak Control V Management V Acco	unts \sim	Search	Q
File Analysis			
	Search by SHA-256, File name, IP,	Keywords	Q 🕹 Submit File 🕀 🕀
glogg.exe (e309efdd0c2c3d25)		2021-01-31 0	06:16:55 UTC Report 24

ثيدحت ةمدخ ةداەش ىلع ةعقوملا (CAs) ةقدصملا تاداەشلا تيبثت نم دكأت .4 ةوطخلا تامج يف تاديدەتلا ةكبش زامج يف AMP ل صاخلا ةباحسلا زامجب ةصاخلا يئاەنلا ريصملا .

ةمالع عم ديدهتلا ةكبش زاهج قطساوب اهيلع قمالع عضو مت قنيع يأ نأ نم دكأت .5 قوطخلا دعب قراض راثآ قيأ عم لماعتلا عم قصاخلا AMP قباحس تانايب قدعاق يف اهليجست متي 95=< ديدهتلا قكبش زاهج قطساوب طاقن قنيعو ريرقتلا ميدقت.

مكحت ةدحو يف ةنيع 95=> ليجستو حاجنب يجذومنلا ريرقتلا يقلت ينعي ال :**قظحالم** رييغت مت منأ ةرورضلاب **فلملا ليلحت** بيوبتلا ةمالع AMP **نم** ةصاخلا ةباحسلا تعقو يتلا CAs تيبثت متي مل اذإ .AMP تانايب ةدعاق يف فلملل يئاهنلا ريصملا زاهج يف AMP صاخلا قباحسلا زاهجب قصاخلا يئاهنلا ريصملا ثيدحت قمدخ قداهش ىلع زاهج قطساوب تانيعلاو ريراقتلا يقلت متي ،**تاداهشلا تائيه** يف تاديدهتلا قكبش تاديدهتلا قكبش زاهج نم لئاسر يأ يقلت متي ال نكلو ،AMP ل صاخلا قباحسلا.

ةدعاق يف ةنيعل يئامنلا ريصملا رييغت ليغشتل يلاتلا رابتخال للمكامت :ر**يذحت** ناك .95=< ةمالع وذ فلم ىلع ةمالع عضوب Threat Grid زامج ماق نأ دعب AMP تانايب AMP قباحس زامج يف ةيلخادلا تايلمعلا لوح تامولعم ريفوت رابتخالا اذه نم ضرغلا رييغت ةيلمع ليغشتل .95=< نم ةنيع تاديدمتلا ةكبش زامج رفوي امدنع صاخلا قيبطت مادختساب قراضلا جماربلا ةاكام رابتخا فلم ءاشنا مت ،يئامنلا ريصملا Cisco يلغا مادختساب قراضلا عالا عرابي عنايي عنايي فل ماشن المت المائي المائي المائي المائي المائي المائي المائي 843862795bb4747984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995.

جاتناٍ ةئيب يف ةراض جمارب ةاكاحم رابتخإ فلم يأ ريجفتب حصني ال :**ريذحت**.

ةصاخلا AMP ةباحس تانايب ةدعاق يف ةنيعلل يئاهنلا ريصملا ثيدحت ديكأت

"" A	MP. 100 AM	P Private Clou	d Device Threat (Grid. >=95
AMP .	AMP >=95 .			
cisco AMP for	Endpoints		۲	? armando garcia ~
Dashboard Analysis ~	Outbreak Control V Management V	Accounts ~	Search	Q
File Analysis				
		Search by SHA-256	, File name, IP, Keywords Q	La Submit File
► xca.exe (63019d7c	a24c6c44)		2021-01-31 08:16:38	3 UTC Report _30
WinRAR.exe (9066f0	0bcf79d741e)		2021-01-31 06:17:05	5 UTC Report 80
▶ glogg.exe (e309efdd	d0c2c3d25)		2021-01-31 06:16:55	5 UTC Report 24
▼ malware3-8d3bbc79	95.exe(8d3bbc795aacc995)		2021-01-31 06:16:50	UTC Report 100
Fingerprint (SHA-256)	8d3bbc795aacc995			
File name	malware3-8d3bbc795.exe			
Threat Score	100			
	Name		Score	
			400	

:اذإ

• حاجنب لماكتلا لامكإ مت.

ايودي تافلملا لاسرا دعب **تافلملا ليلحت** يف تانيعلاو ريراقتلا جذامن ضرع متي • مث:

- فلملا ىلإ لاخدا ةفاضا متت ،95=< ةجردب ةيامحلا ةكبش زامج اميلإ ريشي ةنيع لكل /data/poked/poked.log قكبش زامج يف AMP .
- ة تيامحلاب قصاخلا ةكبشلا زاهج يف data/poked/poked.log/ ةحفصلا ءاشنإ متي ةيامحلام قام العالي المحلية الم المحتي الم العام العالي الم العالي الم العالي الم العالي الم العامي المحلي الم
- يئاەنلا ريصملا قصاخلا AMP قباحس يف قدوجوملا db_protect تانايب قدعاق لمحت ىلع يوتحت قنيعلا تناك اذإ امم دكأتلل تامولعملا ەذە مادختسإ نكمي .قنيعلل يلاحلا

ةجيتنلا ريفوتب "تاديدەتلا ةكبش" زامج ماق نأ دعب 3 ىلع يئاەنلا ريصملا. ل ةصاخلا ةباحسلا مكحت ةدحو يف **فلملا ليلحت** يف 95=< ةجردو جذومنلا ريرقت ضرع مت اذإ AMP، ةيلاتلا تاوطخلا قيبطتب مقف:

.صاخلا AMP ةباحس زاهج ىلإ SSH ربع لوخدلا لجس .1 ةوطخلا

ةنيعلل data/poked/poked.log/ يف لاخدإ دوجو نم دكأت .2 ةوطخلا.

روثعلا متي نلف ،تاديدهت ةكبش زاهج نم سدكم يأ ةصاخلا AMP ةباحس زاهج ملتسي مل اذا قروصلا يف حضوم وه امك ،ليلدلا يف وdata/poked/poked.log/ فلم ىلع.

[root@fireamp ~]# ls /data/poked/ poked_error.log [root@fireamp ~]#

.هؤاشنإ مت يذلا فلملا، 95=< ةمالع لوأ مالتسإ دعب /data/poked/ ليلدلا ةمئاق رهظت

.95=< ةجردب ىلوألا ةنيعلا مالتسإ دعب



دربم poked.log لا لخاد مەفي نأ نكمي ةكبش ديدەت لا ب دوزي ةادألا نم ةمولعم ةنيع.

يلاحلا يئاەنلا ريصملا دادرتسال SHA256 جذومن مادختساب رمألا اذه **ليغشتب مق** .3 ةوطخلا صاخلا AMP ةباحس زاهج تانايب قدعاق نم.

mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x لاثم

ليمحت لبق ةنيعلل يئاەنلا ريصملا ىلع لوصحلل تانايب ةدعاق مالعتسا رفوي ال ةروصلا يف حضوم وہ امك جئاتن ةيأ "تاديدەتلا ةكبش زامج" ىلإ ةنيعلا.

[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"

ريرقتلا مالتسا دعب ةنيعلل يئاەنلا ريصملا ىلع لوصحلل تانايب ةدعاق مالعتسا رەظي .ةراض ربتعت يتلاو 3 يئاەنلا ريصملا اەل يتلا ةنيعلا ،تادىدەتلا قكبش زاەج نم ةمالعلاو

<pre>[root@fireamp ~]# mysql -e "select hex(fingerprint), disposition_id</pre>	<pre>from protect.binaries where fingerprint=0x8d3bbc795bb47447984bf2842d3a0119bac0d79a15a59686951e1f7c5aacc995;"</pre>
hex(fingerprint)	disposition_id
* 8D3BBC795BB47447984BF2842D3A0119BAC0D79A15A59686951E1F7C5AACC995	* 3
↓	# **********

اهحالصإو ءاطخألا فاشكتسا

يرجي ،ةقييثولا نم ءزجلا اذه يفو .ةلمتحملا اياضقلا ىلإ رظنلا نكمي ،لماكتلا ةيلمع يفو اعويش لئاسملا رثكأ ضعب لوانت.

رابتخإ متي مل ،حلاص ريغ فيضملا لوح AMP ل صاخلا ةباحسلا زاهج يف ريذحت API حاتفم رابتخإ متي مل ،ةداهشلا

ضرع

ةكبشل SSL ةداەش رابتخإ رذعت ،حلاص ريغ تاديدەتلا ةكبش فيضم :ريذحتلا ةلاسر AMP ةكبش زاەج يف ەمالتسإ مت ،تاديدەتلا ةكبشل API حاتفم رابتخإ رذعت ،تاديدەتلا .**تاديدەتلا ةكبش < لماكتلا تايلمع** يف **لاصتالا رابتخإ رز** ديدحت دعب ةصاخلا

Connect Threat Grid Appliance to AMP for Endpoints Appliance

Threat Grid Connection test failed.

- Threat Grid host is invalid.
- Threat Grid SSL Certificate could not be tested.
- Threat Grid API key could not be tested.

لماكتلا يف ةكبشلا ىوتسم ىلع ةلكشم كانه.

اەب ىصوملا تاوطخلا:

- ة قايظنلا ةەجاولا ىل AMP ل صاخلا ةباحسلا زاەج مكحت ةدحو ةەجاو لوصو ةيناكمإ ديكأت تاديدەتلا ةكبش زاەجل.
- ة قكبش زاهج فيظنت ةهجاوب صاخلا FQDN لح هنكمي صاخلا AMP ةباحس زاهج نأ ديكأت تاديدهتلا.
- ةكبش زاهجو صاخلا AMP ةباحس زاهجل ةكبشلا راسم يف ةيفصت زاهج دوجو مدع نم دكأت تاديدەتلا.

AMP API

ضرع

ريغ تاديدهتلا ةكبشب صاخلا API ،تاديدهتلا ةكبش لاصتا رابتخإ لشف :ريذحتلا ةلاسر **تايلمع** يف **لاصتالا رابتخإ** رز ديدحت دعب صاخلا AMP ةباحس زامج يف همالتسإ متي ،حلاص **تاديدهتلا ةكبش < لماكتلا**.

Connect Threat Grid Appliance to AMP for Endpoints Appliance

Threat Grid Connection test failed.

Threat Grid API key is invalid.

API AMP.

اەب ىصوملا تاوطخلا:

نييعت متي مل ،تاديدهتلا ةكبش زاهج مدختسمب ةصاخلا باسحلا تادادعإ يف ديكأت •

```
. True ىلإ Disable API Key تمرلعمل
```

onset. وأ false دىلع Disable API Key ةملعملا نييعت بجي -

API



- ةرادإ ةباوب **لماكت تايلمع** يف ەنيوكت مت يذلا تاديدەتلا ةكبشل API حاتفم ديكأت يف مدختسملا تادادعإ يف API حاتفم سفن وه ،**تاديدەتلا ةكبش <** ةصاخلا AMP ةباحس تاديدەتلا ةكبش زاەج.
- تاديدەتلا ةكبشل (API) تاقيبطتلا ةجمرب ةەجاو حاتفم ظفح متي ناك اذإ ام ديكأت صاخلا AMP ةباحس زاەج تانايب ةدعاق يف ةحيحصلا.

ةيلاحلا تاديدەتلا ةكبشل API حاتفم ديكأت نكمي ،صاخلا AMP ةباحس زاەج رماوأ رطس نم ربع AMP ل صاخلا ةكبشلا زاەج ىلإ لوخدلا ليجستب مق .AMP زاەج يف ەنيوكت مت يذلا SSH حاتفم دادرتسال رمألا اذه ليغشتب مقو SSH تا

mysql -e "select tg_api_key, tg_login, api_client_id from db_smbe.businesses;" ةجمرب ةەجاو حاتفمل صاخلا AMP ةباحس زاەجب ةصاخلا تانايبلا ةدعاق يف حيحص لاخدا اذه تاديدەتلا ةكبش زاەجل (API) تاقيبطتلا.

[root@fireamp ~]# my	sql -e "select tg_api_key,	<pre>tg_login, api_client_id from db_smbe.businesses;"</pre>
+ tg_api_key	tg_login	api_client_id
mirt1if:	nnjae7 argarci2_samples-	user de4c23c64d3e36034bb7
[root@fireamp ~]#		

ةباحسلا زاهج يف ةرشابم ەنيوكت متي مل ديدەتلا ةكبش مدختسم مسا نأ نم مغرلا ىلع ەكاردا متي تاديدەتلا ةكبش مدختسم مسا نأ الإ ،لماكتلا نم ةوطخ يأ يف AMP ل ةصاخلا تاديدەتلا ةكبشل API حاتفم قيبطت مت اذا AMP تانايب ةدعاق يف tg_login ةملعملا يف .حيحص لكشب

ةكبشل (API) تاقيبطتالا ةجمرب ةهجاو حاتفمل AMP تانايب ةدعاق يف ئطاخ لاخدا اذه تاديدەتال.

[root@fireamp ~]# mysql -e	"select tg	_api_key, tg_login, api_client_id from db_smbe.businesses;"
tg_api_key	tg_login	api_client_id
thisisanwrongapikey	NULL	de4c23c64d3e36034bb7
[root@fireamp ~]#		

tg_login NULL. AMP .

ةيامحلاب صاخلا ةكبشلا زاهج ةطساوب 95=< جئاتنلا جذامن مالتسإ متي ةنيعلل يئاهنلا ريصملا يف رييغت يأ ةظحالم متي ال نكلو ،(AMP) ةمدقتملا

ضرع

لااسرا دعب "تاديدەتلا ةكبش" زامج نم حاجنب تامالعلاا نم ةنيع 95=< و ريراقتلا يقلت متي AMP ةكبش زامج يف ةنيعلل يئاەنلا ريصملا يف رييغت يأ كاردا متي ال نكلو ،ةنيع ةصاخلا.

اەب ىصوملا تاوطخلا:

• ىوتحم يف SHA256 ةنيعلا تناك اذإ صاخلا AMP ةباحس زامج يف دكأت /data/poked/poked.log.

ىلع روثعلا مت اذا SHA256 يف /data/poked/poked.log، ديكأتل رمألا اذه ليغشتب مقف /data/poked/poked.log تانايب ةدعاق يف يلاحلا ةنيعلل يئاهنلاا ريصمل

mysql -e "select hex(fingerprint), disposition_id from protect.binaries where fingerprint=0x

لخدم ىلاٍ ةحيحصلا AMP ل ةصاخلا ةيباحسلا ةئيبلا لماكت رورم ةملك ةفاضاٍ نم دكأت • AMP ل قصاخلا قيباحسلا قئيبلا لماكت قراداٍ < قراداٍلا يف تاديدهتلا ةكبش زاهج قراداٍ

.ةصاخلا AMP ةباحس ةرادإ ةباوب

Step 2: Threat Grid Portal Setup								
 Go to the Threat Grid Appliance Portal. Navigate to the Manage AMP for Endpoints Integration page on the Threat Grid appliance. Add the Service URL, User, and Password from the section below. 								
Details	Details							
Service URL	https://dupdateamp3.argarci2-lab.com/							
User disposition_update_user								
Password	ペ ew236 xJYfPK	I)	Change Password					

ةيامحلا ةكبش زاهج يف مكحتلا ةدحو ةباوب.

cisco	Threat Grid	Submit Sample	Dashboard	Samples	Advanced Search Beta	Reports	Indicators	Administration	~	
		Disposition	Update Syn	dication	Service					
		Service URL		User	r	Passwo	ord		Action(s)	
				dis	position_update_user				Edit	Remove
				dis	position_update_user				Edit	Remove
				dis	position_update_user				Edit	Remove
				dis	sposition_update_user				Edit	Remove
				dis	position_update_user				Edit	Remove
		https://dupda	ateamp3.argarci2	-lat dis	position_update_user	ew23	6 xJ	YfPK	Save	Cancel
				dis	position_update_user				Edit	Remove

ةزهجأ ريصم ثيدحت ةمدخ ةداهش ىلع ةعقوملا (CAs) ةقدصملا تاداهشلا تيبثت ديكأت • ما تاداهش يف تاديدهتلا ةكبش ةزهجأ ةرادإ لخدم يف AMP نم ةصاخلا ةباحسلا CA.

ريصم ثيدحت ةمدخ ةداەشب ةصاخلا تاداەشلا ةلسلس تيبثت بجي ،يلاتلا لائملا يف ىلع AMP ل صاخلا يباحسلا زاەجلا AMP يل .ديدەتلا ةكبش زاەج يف **CA تاداەش** يف Sub_CA و RootCA تيبثت بجي ،يلاتلابو

ةصاخلا AMP ةباحس ةرادإ لخدم يف تاداهشلا تاطلس.

il c	iii) isco	S AMP for	Endpoints	Private Cloue	d Administration Por	tal	Support	Announcements	? H	elp	🕞 Lo	gout	
1	*	Configuration -	Operations -	Status -	Integrations -	Support -					2	•	
	e	3 Sanity Check F	ailing										

Certificate Authorities are used by your Private Cloud device to verify SSL certificates and connections.

	Add C	Certific	cate Authority	
Certificate				(click to collapse)
Issuer	rootca_vpc			
Subject	rootca_vpc			
Validity	2020-11-15 00:00:00 UTC	-	2025-11-14 23:59:59 UTC	
Certificate				(click to collapse)
Issuer	rootca_vpc			Download
Subject	subca-dus			
Validity	2020-12-05 12:01:00 UTC	-	2023-12-05 12:01:00 UTC	Delete

:تادىدىتارا تائىش تر ادا قىباوب نارىيارى Cisco Threat C Threat Grid Appliance Home Configuration Status Operations Support

Configuration	CA Certificates	
Authentication	Details	Validity
CA Certificates	Subject: CN=rootca_vpc Issuer: CN=rootca_vpc	2020-11-1 Valid for alr
Change Password	Fingerprint: 66:BF:EB:63:36:9F:AC:E9:39:AD:76:A4:0E:5A:57:B1:45:B9:FD:A4:FD:63:7E:5A:11:FF:47:AA:CC:1E:FF:F2	
Clustering	Sub	-03-0
Date and Time	Fing	for ab
Email	Sut	-03-2
Integrations	lssu Find	for ab
License		07.0
Network	Issu	for ov
Network Exit	Fing	
NFS	Sub Issu	-03-0 for ab
Notifications	Fing	
SSH	Subject: CN=subca-dus	2020-12-0 Valid for alr
SSL	Fingerprint: 51:D5:74:9A:6C:44:4B:1A:E9:45:93:CB:B6:7C:3A:EB:7B:BB:BD:04:51:4D:79:8E:D4:23:35:92:C0:17:9D:5C	vana ror an
Syslog		
	Add Certificate Lookup Certificate	
	disposition_update_user	Edi

disposition_update_user https://dupdateamp3.argarci2-lab ew236 xJYfPK disposition undate user

ريغ تاديدەت ةكبشل SSL ةداەش لوح AMP ل صاخلا ةباحسلا زاەج يف ريذحت ةحلاص

ضرع

ةداەش" :ريذحتلا ةلاسر يقلت متي SSL ةباحسلا زاەج يف ،"ةحلاص ريغ تاديدەتلا ةكبشل SSL قداەش" :ريذحتلا قلاسر يقلت متي ت**اديدەتلا ةكبش < لماكتلا تايلمع** يف **لاصتالا رابتخإ** رز ديدحت دعب AMP ل صاخلا.



- Threat Grid SSL Certificate is invalid.
- Threat Grid API key could not be tested.

اەب ىصوملا تاوطخلا:

• لبق نم اهعيقوت مت يتلا Threat Grid ةهجاو يف ةتبثملا ةداهشلا تناك اذإ ام ديكأت يسسؤم قدصم عجرم.

تايلمع ىلإ فلم لخاد ةلماكلا تاداەشلا ةلسلس ةفاضإ بجيف ،CA ةطساوب اەعيقوت مت اذإ **ةكبشل SSL ةداەش** يف **تاديدەتلا ةكبش <** ةصاخلا AMP ةباحس ةزەجأ ةرادإ ةباوب **لماكت** ت**اديدەتلا**.

Threat Grid Configuration Details				
Hostname	cisco.com			
API Key	Q,			
Threat Gric				
Issuer	subca_tga_clean			
Subject	cisco.com			
Validity	2020-11-24 00:00:00 UTC - 2021-11-23 23:59:59 UTC	J		

ايلاح ةتبثملا ةيامحلا ةكبش زاهج تاداهش ىلع روثعلا نكمي AMP Private Cloud، ايلاح ةتبثملا ةيامحلا يف: /opt/fire/etc/ssl/threat_grid.crt .

تاداەشلاب ةقلعتملا دىدەتلا ةكبش زاەج يف ةدوجوملا تارىذحتلا

قباطتم ريغ صاخ حاتفم نم دمتسملا ماعلا حاتفملا - ريذحت ةلاسر

ضرع

زاهج يف همالتساٍ متي ،قباطم ريغ صاخ حاتفم نم دمتسملا ماعلا حاتفملا : ةهجاو يلإ قداهش قفاضإ قلواحم دعب ديدهتلا قكبش.

```
ululu
cisco
```

e Home

Support

```
Upload SSL certificate for PANDEM
Configuration
                              Certificate (PEM)
Authentication
                               hvcNAQELBQADggEBAKXz8oIDWacWY5V0XSHWrQIMULAMNAE8OZIXNkuByG6vvhj
CA Certificates
                               P
                               JkgjjU9xKrke5LCr+trWnr+qjZlc4ecVCm8FXBWUtr8BjHcimbHUbZlVLYp6WDxO
Change Password
Clustering
                               HMS37fv44R9Cir4pjUz0bc61HS4wo5PAfUyjPtO1Dy0dHia4zE3pH4X3D9rzQYYd
Date and Time
                               CI6KJpevCJzFvoQW3ahTZoxr4F11I5wO3XcH41Q=
Email
                               -----END CERTIFICATE-----
Integrations
                              Private Key (PEM)
License
                               wZfa8sZJp30zivJRtvBioPnwmPpNZzhqIW3cC90ASaRSXeU+4c+HmUknahEHJNn8
                               IJbkA4UJQgWgeD4QKOj8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqlXsBKDCHjYo
Network
                               g+H0NxIdl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFTbHIZO
Network Exit
NFS
                               /8E/D+jdT8zhA3aWNXADf8b9xjIRE324TFAfJf73a59g27y7d96tCa1PFaMOiXGc
                               nY2D9lwNsni5uk1lHL2SojLtVx8BYqw98w0uuBOmqZZVNprSparsyw==
Notifications
                               -----END RSA PRIVATE KEY-----
SSH
                              public key derived from private key does not match
SSL
Syslog
                                Add Certificate
                                                 Cancel
```

يف نوكملا ماعلا حاتفملا عم قباطتي ال صاخلا حاتفملا نم ردصملا ماعلا حاتفملا ةداەشلا.

اەب ىصوملا تاوطخلا:

ةداەشلا يف ماعلا حاتفملا قباطي صاخلا حاتفملا ناك اذإ ام ديكأت •. سألاو لماعملا نوكي نأ بجيف ،ةداەشلا يف ماعلا حاتفملا قباطي صاخلا حاتفملا ناك اذإ يف ةميقلا سفن ەل لماعملا ناك اذإ ام ديكأت يفكي ،ليلحتلا اذەل .عيشلا سفن ماعلا ةداەشلا يف ماعلا حاتفملاو صاخلا حاتفملا.

ادأ مدختسأ .1 ةوطخلا OpenSSL حاتفملا عن من الله عنه من الله عنه من الله عنه من عالما عنه من عنه من الماعل. مداهشلا عن من عوك مت عذل ماعل.

```
$ openssl x509 -noout -in certificate.cert | openssl md5
(stdin)= d41d8cd98f00b204e9800998ecf8427e
$
$
$
$ openssl rsa -noout -in private-key.key | openssl md5
(stdin)= d41d8cd98f00b204e9800998ecf8427e
```

```
PEM ريغ ىوتحم ىلع صاخلا حاتفملا يوتحي - ريذحت ةلاسر
```

زاهج يف همالتسإ متيو ،PEM ريغ ىوتحم ىلع صاخلا حاتفملا يوتحي :ريذحتلا ةلاسر ةمجاو ىلإ ةدامش ةفاضإ ةلواحم دعب ديدهتلا ةكبش.

Threat Grid	Appliance Home Configuration Status Operations Support
Configuration Authentication CA Certificates Change Password Clustering	Upload SSL certificate for PANDEM Certificate (PEM)
Date and Time Email Integrations	NIgQT03qqfX7Zh5wKY4BrTWxOpNBodUcl0KxzODPWYZqUUjpeKcjyUkj2L6fY0OV
License Network Network Exit	wZfa8sZJp30zivJRtvBioPnwmPpNZzhqlW3cC90ASaRSXeU+4c+HmUknahEHJNn8 IJbkA4UJQgWgeD4QKOj8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqlXsBKDCHjYo g+H0NxIdl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFTbHIZO
NFS Notifications SSH	/8E/D+jdT8zhA3aWNXADf8b9xjlRE324TFAfJf73a59q27y7d96tCa1PFaMOiXGc nY2D9lwNsni5uk1lHL2SojLtVx8BYqw98w0uuBOmqZZVNprSparsyw== END RSA PRIVATE KEY
SSL Syslog	Add Certificate Cancel

.ةفلات صاخلا حاتفملا فلم لخاد PEM تانايب

اەب ىصوملا تاوطخلا:

```
•
.صاخلا حاتفملا ةمالس نم ققحتلل OpenSSL ةادأ مدختسأ .1 ةوطخلا
```



عم لكاشم ىلع روثعلا مت ەنأ ينعي اذەف ،**RSA OK حاتفم** وە OpenSSL رمألاا جارخإ نكي مل اذإ حاتفملا لخاد PEM تانايب.

:ذئدنعف ،OpenSSL رمألا يف لكاشم ىلع روثعلا مت اذا

ال مأ ةدوقفم صاخلا حاتفملا لخاد PEM تانايب تناك اذإ ام ديكأت • نأ نكمي .افرح 64 نم ةنوكملا رطسألا يف صاخلا حاتفملا فلم لخاد PEM تانايب ضرع متي .ةدوقفم تانايبلا تناك اذإ ام فلملا لخاد PEM تانايبل عيرسلا يرصبلا صحفلا رهظي فلملا يف ىرخألا رطسألا عم هتاذاحم متت ال ةدوقفملا تانايبلا وذ رطسلا \$ cat wrong-private-key.key ----BEGIN PRIVATE KEY--MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCvfIytwkf9UIc5 DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52 Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/PW4fE /JNGbMIU/d1DDuzxfgGze0viztT90rpCbZyQP2r+sGxa0KM0c3AEgK/pYA7aCv/G P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTIcI2q/vH/i0WeIgAv10aGuBC0eg <----NwOgPyY3XI8g7 1HA6/VsM10NHKT4EhvSks WXZW1XhNAgMBA tU9huSCL7t4BF7VpSeKXM Uh4/Vrdg1TYXf s7k0sCwmhKUaMAcTYAnrg 17ttvLvX3zweLCEXsDXK6 fINIJto/x0azh mdhzCQSTBfYbM {4M7HiocsbkLjijScTFYQ JqSwA5BEgqeH3 ngd4kJ6ddAaSjQS7sJxaf WtVHzbVDqJ+rb 3gQDePpxacxGRZLXfja3s SU+TvjNWQGcUs a8y8ZQd01qPZrV0Z6Mym2 i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2x0Cy51K5KsfDPa/SrbhDkxZty0SG 1CgVLEycQ5t1xt16qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRLPxeCS CbcflDYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn g7LG+bcJIQKBgHFn/ZziDtrkSzJSN6fVGPhJHCUtI+yZRuBkkz/8ohv1Rf+En+VY 90G0GBq/MEBZy3TV+SUYfPX1S09e0DDYNQToKsfpUh00vu00JeIGSm+E6jFApNeg QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTY1GD7ZAoGASHku b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0 SxuwKWoARshnMsDvsTYWofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmblpAYS DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd V3Pq4IWaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o a+IQn0Y41zLJ22ScgyFzEQ== -----END PRIVATE KEY-----

، **صاخ حاتفم** تاملكلا **أدبتو** ،ةلصاو 5 ب أدبي صاخلا حاتفملا يف لوألا رطسلا نأ ديكأت • .ةلصاو 5 ب يەتنيو

.لاثم

—صاخلا حاتفملا ءدب—

،صاخلا حاتفملا ءاەناٍ تاملك ،ةلصاو 5 ب أدبي صاخلا حاتفملا يف ريخألا رطسلا ديكأت • .ةلصاو 5 ب يەتنيو

لاثم.

—صاخلا ةياەنلا حاتڧم—

.صاخ حاتفم لخاد ةدوجوملا تانايبلاو PEM قيسنت حيحصت .لاثم

\$ cat correct-private-key.key -----BEGIN PRIVATE KEY-----MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCvfIytwkf9UIc5 DluK9PTbKvDrShgn8/Cen9wXEUDIBNahlFiZvwZb/5FL+I1ry/P0WKJMiXRhLQ52 Y0oogQsuDTw79Moa6xXYLKq1P5QRIV6tQQDNiHUoHFNSLkoo0H0ubkDtGo/PW4fE /JNGbMIU/d1DDuzxfgGze0viztT9OrpCbZyQP2r+sGxaOKM0c3AEgK/pYA7aCv/G P6rGkHc/ViM1NTuWVIWdIcLgTUX0DeHLjTIcI2q/vH/i0WeIgAv10aGuBC0egVDU NwOgPyY3XI8g7H 4HA6/VsM10NHKT4EhvSks WXZW1XhNAgMBAA tU9huSCL7t4BF7VpSeKXM Uh4/Vrdg1TYXfB s7k0sCwmhKUaMAcTYAnrg fINIJto/x0azhe 47ttvLvX3zweLCEXsDXK6 mdhzCQSTBfYbM4 R4M7HiocsbkLjijScTFYQ JqSwA5BEgqeH3a hgd4kJ6ddAaSjQS7sJxaf WtVHzbVDqJ+rb9 BgQDePpxacxGRZLXfja3s SU+TvjNWQGcUsX a8y8ZQd0lqPZrV0Z6Mym2 i5S+/LS4jHB5hcCfnZpL4M0zHYvX+HPuGHm2x0Cy51K5KsfDPa/SrbhDkxZty0SG 1CgVLEycQ5t1xt16qiBLKNmtrQKBgQDKI+BTMrHFYD50gPcBZyGXVhmSyHcZOP9k OosXngeKtpdqL8Ck/H2QftFpOAFoHQxD/tiJA6E1eK9HfVnsq9+xbCU1fRLPxeCS CbcflDYBwaMn8Ywp9PfZKPgu/gI3XIUWT6T0LcBGtdspYDEbApvYA091PoS0vcBn g7LG+bcJIQKBgHFn/ZziDtrkSzJSN6fVGPhJHCUtI+yZRuBkkz/8ohv1Rf+En+VY 9QG0GBq/MEBZy3TV+SUYfPX1SQ9eQDDYNQToKsfpUh0QvuQ0JeIGSm+E6jFApNeg QauT9x0TkVDP1bP5LFkTMG27Brzr9oG95F45hrZ0gW0D+w7YdTY1GD7ZAoGASHku b4XoeNS1771hUg5w27qR9q+LC+8EmiHnRrNxDsnCZd7zGfQw7MKbQDdFQdfQUvyn FBDKFsrLRT1rJVDGJe2ZNaE/QmE20AVNs7PG3UBYx/RxhYV/60smGGsXz10Mn+A0 SxuwKWoARshnMsDvsTYWofmlSMwTlMmCKpbTiiECgYBi8ZjgsdFv2NtYlmblpAYS DHiErbldtVumF42Tax+fucqUrdB3LZo6FjagvPy+LBjA3VjtRYkDjQmstvxD5jfd V3Pq4IWaocGU8RQUJY5L6rmw+y1s6Z+iNkIcPeZtWidSgP+NZa1xvhfj8XeL560o a+IQn0Y41zLJ22ScgyFzEQ== ----END PRIVATE KEY-----

صاخلا حاتفملا نم ماع حاتفم ءاشنإ نكمي ال - ريذحت ةلاسر

ضرع

ةكبش زاهج يف اهيقلت مت ،صاخلا حاتفملا نم ماع حاتفم ءاشناٍ نكمي ال :ريذحتلا ةلاسر ةهجاو ىلاٍ قداهش ةفاضاٍ ةلواحم دعب ديدهتلا.

```
cisco
```

Threat Grid Appliance

Home

Support

Upload SSL certificate for PANDEM Configuration Certificate (PEM) Authentication AN **CA Certificates** BgkqhkiG9w0BAQsFAAOCAQEAsCQ1iOkPkLj6A1R94eueZ64zCYGuf8wg0z2S9Kle epjqQobaJadl3WTh7LMHuxHZP02YZJIO/QjUQ/8uLk1sG7rVE5ROe/Ev9OvjL5nF **Change Password** Clustering wbTboJukREZOyiBoQDPcSWhQe8j3FEtJIf9yfv2bthOFQQ+Lf3BU4ZPiXPVEtuUL **Date and Time** 7FIP0kjC/33s5ZWpC8OzCmdPvFgx//JbpWr1glIYVs1uYg== Email ----END CERTIFICATE--Integrations Private Key (PEM) License -----BEGIN RSA PRIVATE KEY-----MIIEpAIBAAKCAQEAucb3AU15P91Ym/PvHva/xKBCbLeY7+jQJGO7wm7eruX3KTZY Network EE9N6qn1+2YecCmOAa01sTqTQaHVHJdCsczgz1mGalFl6Xinl8lJl9i+n2NDlcNr XBVPvCUs5fnH2cZwKGTen/NDJhnyC5Dlb17RLy7Y+wxhMiyRCHH3aZ3l0Mpl1k4X **Network Exit** NFS cjSc9W8Fy/CDXbX27KncS4qWe91phsKXq0jo7wIDAQABAoIBAFrH8EHRsvNTXY5v **Notifications** yCSwXQtfaLYpjXGGqdduaPzdlrlCrCGWbbgimKeYQByGTU9v7vXAx2EAh57lzvb2 SSH cannot generate public key from private key SSL Syslog Add Certificate Cancel

.صاخلا حاتفملا فلم لخاد ةيلاحلا PEM تانايب نم ماعلا حاتفملا ءاشناٍ نكمي ال

```
اەب ىصوملا تاوطخلا:
```

1. OpenSSL .

openssl rsa -check -noout -in

عم لكاشم ىلع روثعلا مت ەنأ ينعي اذەف ،**RSA OK حاتفم** وە OpenSSL رمألاا جارخإ نكي مل اذإ تانايب.

openss1 rsa -in حجان ماع حاتفم ريدصتو ماعلا حاتفملا ريدصت لشف .لاثم.



PEM تانايب زيمرت كف رذعت :ليلحتلا يف أطخ - ريذحت ةلاسر

ضرع

زاهج يف اهيقلت مت ،PEM تانايب زيمرت كف رذعت :ليلحتلا يف أطخ :ريذحتلا ةلااسر .قمجاو يلإ قداهش قفاضإ قلواحم دعب "ديدهتلا قكبش"

CISCO Threat Grid	Appliance Home Configuration Status Operations Support
ConfigurationAuthenticationCA CertificatesChange Password	Upload SSL certificate for PANDEM Certificate (PEM) AN BgkqhkiG9w0BAQsFAAOCAQEAsCQ1iOkPkLj6A1R94eueZ64zCYGuf8wg0z2S9KIe epjqQobaJadl3WTh7LMHuxHZP02YZJIO/ <u>QjUQ</u> /8uLk1sG7rVE5ROe/Ev9OvjL5nF
Clustering Date and Time Email	wbTboJukREZOyiBoQDPcSWhQe8j3FEtJIf9yfv2bthOFQQ+Lf3BU4ZPiPVEtuUL 7FIP0kjC/33s5ZWpC8OzCmdPvFgx//JbpWr1gIIYVs1uYg==END CERTIFICATE
Integrations License	parse error: PEM data could not be decoded Private Key (PEM)
Network Network Exit	wZfa8sZJp30zivJRtvBioPnwmPpNZzhqlW3cC90ASaRSXeU+4c+HmUknahEHJNn8 IJbkA4UJQgWgeD4QKOj8cQKBgQCIZmRmL7H7d1avaPzbEIA0kYnlqlXsBKDCHjYo g+H0Nxldl8zU5HYFab9LO361thYO+OBwd3EGhbQ2u7CeinFp8Y7mQuqQNFTbHIZO
NP3 Notifications SSH	/8E/D+jdT8zhA3aWNXADf8b9xjIRE324TFAfJf73a59q27y7d96tCa1PFaMOiXGc nY2D9lwNsni5uk1IHL2SojLtVx8BYqw98w0uuBOmqZZVNprSparsyw==
SSL Syslog	Add Certificate Cancel

تانايب .ةداەشلا فلم يف ةدوجوملا ةيلاحلا PEM تانايب نم قداەشلا زيمرت كف رذعتي PEM تانايب .قداەشلا فلم يف قدوجومل

.ةداەشلا فلم لخاد PEM تانايب نم ةداەشلا تامولعم دادرتسإ نكمي ناك اذإ ام ديكأت •

.PEM تانايب فلم نم صيخرتلا تامولعم ضرعل OpenSSL ةادأ مدختسأ .1 ةوطخلا

openss1 x509 -in تانايب تناك اذإ PEM تامولعم ليمحت OpenSSL تامولعم ليمحت المدنع أطخ رهظيسف ،ةفلات الت ةداهشلا.

.ةداەشلا فلم يف PEM تانايب فلت ببسب ةداەشلا تامولعم ليمحت ةلواحم تلشف .لاثم

\$ openssl x509 -in wrong-certificate.cert -text -noout
unable to load certificate
140159319831872:error:09091064:PEM routines:PEM_read_bio_ex:bad base64 decode:../crypto/pem/pem_lib.c:929:

مداخلا/ليمعلل قدصم عجرم ةداەش تسيل - ريذحت ةلاسر

ضرع

يف اهمالتسإ متي ،مداخ/ليمع قيدصت عجرم ةداهش سيل :ليلحتلا يف أطخ :ريذحتلا ةلااسر عجرملا تاداهش < نيوكتلا</mark> ىلإ قدصم عجرم ةداهش ةفاضإ ةلواحم دعب "ديدهتلا ةكبش" زاهج قدصملا.

cisco Threat Grid	Appliance Home Configuration Status Operations Support
Configuration	CA Certificates Certificate (PEM) Ir2MrtEmB8vuU3CzLqSnC3iFRYF9bbwiQTW/AqMBAAGiDzANMAsGA1UdDwQEAwIC
CA Certificates	jDANBgkqhkiG9w0BAQsFAAOCAQEAY3b0+QmLE0Ri7q3iHUSK3cGcWhCrWIF5z3OR
Clustering	w6yBX1YrWKICWS0mT8K/3mscEbUvyjALFRvoGccYLII3wboaB8ZLxysEL6Nw7r+5
Date and Time Email	L2wj6R2hS8e7dzJzHbsp+1icL/w7MAuFRWKTA0j7gEbKmYj+0Q== END CERTIFICATE
Integrations	not a client/server CA cert
License	
Network	Add Certificate Cancel
Network Exit	
NFS	
Notifications	
SSH	
SSL	
Syslog	

.حيحص :CA ك CA ةداهش يف "ةيساسألا دويقلا" قحلملا ةميق فيرعت متي مل

ةادأ مادختساب ديكأتلا CA: ىلع ةيساسألا دويقلا قحلم ةميق نييعت مت اذإ OpenSSL ةادأ مادختساب ديكأتلا قداهش يف حيحص CA.

.PEM تانايب فلم نم صيخرتلا تامولعم ضرعل OpenSSL ةادأ مدختسأ .1 ةوطخلا

.**ةيساسألا دويقلا** قحلمل ةيلاحلا ةميقلا نع ةداەشلا تامولعم يف ثحبا .2 ةوطخلا

.تاديدەتلا ةكبش زاەج ةطساوب لوبقم CA ل ةيساسألا ديقلا ةميق .لاثم



ةلص تاذ تامولعم

- <u>نيوكتلا ةلدأ ةيامحلا ةكبش زامج</u> •
- <u>Cisco نم ةراضلا جماربلا نم ةمدقتملا ةيامحلاب ةصاخلا ةيضارتفالا قيباحسلا ةادألا</u> (<u>Cisco نم قراضلا جماربلا م</u> <u>قينفلا تاظحالملاو نيوكتلا قلثماً</u>
- <u>Cisco Systems تادنتسملاو ينقتلا معدلا</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما