

ESA ىلع TLS ل تاداهشلا دادع| لىلد عاشن|

تايوتحمل

[عمدقمل](#)

[ةيساسأل تابلطتم](#)

[تابلطتم](#)

[عمدختسمل تانوكمل](#)

[ةيساسأ تامولعم](#)

[ةيفيظو تابلطتمو ةماع ةرطن](#)

[ةصاخلا كتداهش رضأ](#)

[ةيلجال ةداهشلا ثيدحت](#)

[ايتاذ ةعقوملا تاداهشلا رشن](#)

[CSR و ايتاذ ةعقوم ةداهش عاشن](#)

[قدصم عجرم ىلا ايتاذ ةعقوملا ةداهشلا ريفوت](#)

[ESA ىلا ةعقوملا ةداهشلا ليمحت](#)

[ESA تامدخ عم مادختسالل ةداهشلا ديدحت](#)

[دراولا TLS](#)

[رداصل TLS](#)

[HTTPS](#)

[LDAPs](#)

[URL ةيفصت](#)

[ايطايتح \(تاداهشلا\) ةداهشلا وزاهجلا ةئيهت خسن](#)

[دراولا TLS طيشنت](#)

[رداصل TLS طيشنت](#)

[ESA ةداهشلا ئطاخلا نيوكتلا ضارعا](#)

[ةحصللا نم ققحتلا](#)

[بيوضرعتسم مادختساب TLS نم ققحتلا](#)

[ثلاثلا فرطلا تاودأ مادختساب TLS نم ققحتلا](#)

[اهجالص او عاطخأل فاشكتسا](#)

[ةطسوتمل تاداهشلا](#)

[بولطملا TLS لاصلتال لش فب ةصاخلا تامالعالا نيكمت](#)

[ديربلا تالجتس يف ةحجانلا TLS لاصلتال عقوم ديدحت](#)

[قلص تاذ تامولعم](#)

عمدقمل

يف مكحتلا مئوق طيشنتو TLS عم مادختسالل ةداهش عاشن| ةيفيك دنتسملا اذه حضوي Cisco ىلع اهجالص او عاطخأل فاشكتسا او عاطخأل فاشكتسا او رداصل / دراولا (TLS) لوصول ESA.

ةيساسأل تابلطتم

[تابلطتم](#)

دنتسمل اذهل ةصاخ تابللطتم دجوت ال

ةمدختسمل تانوكملا

ةني عم ةيدام تانوكموجمارب تارادصلإ يلع دنتسمل اذه رصتقي ال

ةصاخ ةيلم عم ةئي ب ي ف ةدوجوملا ةزهجالا نم دنتسمل اذه ي ف ةدراولا تامولعمل عاشنإ مت تناك اذإ. (يضا رتف) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجالا عيمج تادب رمأ يال لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تبش

ةيساسا تامولعمل

إلإ ةطقن نم ينورتكلإلا ديربلا لئاسر لاسرإل ةيصوصخلال ESA يلع TLS قي ب طت حيتي ةمدخ نم صاخ حاتفمو ةداهش داريتساب لوؤسملل حمسي وهو. ريفشتلا لالخنم ةطقن اي تاذة عقوم ةداهش مادختسإ وأ (CA) قدصملا عجرملا

ديربلا لقن لوكتوربلا STARTTLS قحلم ينورتكلإلا ديربلا نامأل Cisco AsyncOS معدي (TLS ربع نامأل SMTP) (SMTP) طيسبلا

إلإ عجرا، RFC 3207. يلع لوصحلل: [RFC 3207](#) عجملت

ةومجملا يوتسم يلع تاداهشلا تي ب ثت ةيفي ك دنتسمل اذه حضوي: **ةظحال** زاهجالا يوتسم يلع تاداهشلا قي ب طت نكمي. ESA يلع ةيزكرملا ةرادلا ةزيم مادختساب متي، يرخا ةرم هتفاضلإ تمت مثةومجملا ماظن نم زاهجالا ةلازا تمت اذإ، كلذ عم و، اضيأ زاهجالا يوتسم يلع تاداهشلا دق

ةيفيظو تابللطتمو ةماع ةرطن

بابسالا هذه نم يال زاهجالا يلع اي تاذة عقوم ةداهش عاشنإ لوؤسمل ديدي

- ةدراولا تاا داحملا الك) TLS مدختست يتلا يرخالأ MTAs عم SMTP تاا داحم ريفشتلا (ةرداصل او).
 - ربع (GUI) ةيموسرلا مدختسمل اةهجاو لإ لوصولل زاهجالا يلع HTTPS ةمدخ ني كمتل HTTPS.
 - اذإ، (LDAPs) نزولا ةيفي ف لي لدلا لإ لوصولل تالوكتوربلا لي مع ةداهش ك مادختسالل. لي مع ةداهش بل طتي LDAP مداخنك.
 - Rivest-Shamir-Addleman (RSA) جم انربو زاهجالا ني ب نمألا لاصلتالاب حامسلا لجا نم (DLP) تانايبال نادقف ةي امحل Enterprise Manager.
 - جماربالا نم ةمدقتملا ةي امحل تاديدهت ةكبش زاهجو زاهجالا ني ب نمألا لاصلتالاب حامسلا ل (AMP) ةراضلا Cisco.
- TLS تالاصلتإ عاشنإل اهمادختسإ نكمي حاضيإ ةداهش ب اقبسم ائيهه ESA يتأي

ملع يلع نك، نمأ TLS لاصلتإ عاشنإل ةيفاك ةي حاضيإل اةداهشلا نوكت امنيب: **ريذحت**

هنم ققحتلا نكمي لاصتا ريفوت عي طتست ال اهنأب.

نسخملا ينورتكلال دي رپلا ةداهش وأ [X.509](#) ةداهش ىلع لوصحلل Cisco ي صوت ةداهشلا نوكت .يشتابأ ةداهشب اضيا اهيل راشيو .(CA) قدصم عجرم نم (PEM) ةيصوصخلل ةعقوملا ةداهشلا نأل ايتاذ ةعقوملا ةداهشلا ىلع اهي فابو عرم قدصملا عجرملا نم ةدراولا نكمي لاصتا ريفوت نأ نكمي ال يتلاو ،اقباس ةروكذملا حاضيالا ةداهشلا ةلثامم ايتاذ هنم ققحتلا.

[RFC 1424](#) ىتح [RFC 1421](#) يف يفاضا لكشب PEM ةداهش قيسنت دي دحت مت :ةظحالم تيبت لثم) ةماعلا ةداهشلا ىلع طقف يوتحي نأ نكمي ةيواح قيسنت وه PEM حاتفملا ني مضتل ،ةلماك تاداهش ةلسلس وأ (CA /etc/ssl/certs) تاداهش تافلومو Apache ديربلل ةلشاف ةقيرط نم PEM مسالا .رذجل تاداهش و صاخلا حاتفملاو ماعلا base-64 ةمجرت وهو اطشن لازي ال هم دختسا يذلا ةيواحلا قيسنت نكلو ،نم ال ينورتكلال 1. ASN.1 X.509 حاتفملا 64.

ةصاخلا كتداهش رضحأ

ةداهشلا نوكت نأ وه بلطتملا نإف ،كلذ عمو ،ESA ىلع كصيخرت داريستسا رايخ ريفوت يابلأغ نولوؤسملا يوتحي ال .صاخلا حاتفملا قيسنتلا اذه نمضتي .PKCS#12 قيسنتب ESA ىلع ةداهشلا عاشنأب Cisco ي صوت ،ببسا اذهل .قيسنتلا اذهب ةرفوتم تاداهش ىلع CA .ةطساوب حيص لكشب اه عي قوتو

ةيواحلا ةداهشلا ثي دحت

ايتاذ ةعقوملا تاداهشلا رشن مسق ي طختب مقف ،لعفلاب ةدوجوم ةداهش ةيواحلا الص تهتنا اذا .ةدوجوملا ةداهشلا عي قوت دعاو دنتسملا اذهب

ينورتكلال دي رپلا نامأ زاوجب صاخلا Cisco دنتسم [يف ةداهش دي دحت](#) عجار :حيملت لي صافاتلا نم ديزم ىلع لوصحلل .

ايتاذ ةعقوملا تاداهشلا رشن

ريفوتو ،(CSR) ةداهش عي قوت بلطو ايتاذ ةعقوم ةداهش عاشنأ ةيفي ك مسقلا اذه حضوي ةداهشلا دي دحتو ،ESA ىلع ةعقوملا ةداهشلا لي محتو ،عي قوتلل CA ىل ايتاذ ةعقوم ةداهش (هتاداهش) هتداهشو زاوجل نيوكتل يطايتحال خسنلاو ،ESA تامدخ عم مادختس الل

CSR و ايتاذ ةعقوم ةداهش عاشنأ

certconfig رمال لخدأ ،رماوالا رطس ةهجاو ربع ايتاذ ةعقوم ةداهش عاشنأل

:ةيموسرلا مدختسملا ةهجاو نم ايتاذ ةعقوم ةداهش عاشنأل

- (GUI) ةيموسرلا مدختسملا ةهجاو نم ةداهش ةفاضل > تاداهشلا > ةكبشلا ىل لقتنا .1. زاوجل
- .ايتاذ ةعقوم ةداهش عاشنأل ةلدسنملا ةمئاقلا ىلع رقنا .2.

ههجاول فيضم ال مساقباطي عئاشل مسال نأ نم دكأت، ةداهشل عاشنإب موقت ام دنع ميسلستلا ههجاول فيضم ال مساقباطي هنأ وأ، عامتسالا

نمض اهنيوكت مت يتلاو تصنم ل باب اهطبر متي يتلا ههجاول يه عامتسالا ههجاو اهنيوكت متي مل ام، ايئاق لت ميسلستلا ههجاو ديحت متي. ني عم تسمل > ةكبشلا deliveryconfig رمال مادختساب (CLI) رمال رطس ههجاو نم حي رص لكش ب

3. ةثالثل رصانعال ةقباطم نم ققحت، هنم ققحتلل لباق دراو لاصتال ةبسنلاب: ةيلاتلا:

MX لجسل (DNS) لاجم ال مساقباطي صاخلا فيضم ال مساقباطي

عئاشل مسالا

ههجاول فيضم مساقباطي

ةلباقب قلعتي امي TLS تالاصتلا يلع ماظنلا فيضم مساقباطي ال: ةظالم مدختسمل ههجاو نم ينم ال اي لعال ةيوازلا في ماظنلا فيضم مساقباطي. ققحتلا CLI sethostname رمال جارخا نم وأ، زاهلاب ةصاخلا (GUI) ةيموسرلا

، تاوطلال هذه لم تكت مل اذا CSR ري دصت لباق اهم ازلتلاو كتاريي غت لاسرا ركذت: ري دخت عجرم ال نم ةعقوم ال ةداهشلل نكمي الو، زاهلاب نيوكتب مزتلت ال ةديجل ال ةداهشل اناف. اهيلع اهقيا بطت وأ لع فلاب ةدوجوم ةداهش عيقوت قدصم ال

قدصم عجرم ال اي تاذ ةعقوم ال ةداهشل ري فوت

عيقوتلل قدصم عجرم ال اي تاذ ةعقوم ال ةداهشل لاسرال:

1. > ةداهشل مساقباطي > تاداهش > PEM قيسنتب ةكبش في يلحم بساح ال CSR ظفحا. ةداهشل عيقوت بلط لي زنت

2. عيقوتلل هيلع فرعتم قدصم عجرم ال اهواشنإ مت يتلا ةداهشل لاسرا.

3. ةطيسولا ةداهشل ال ةفاضلاب، X.509/PEM/Apache قيسنتب ةداهش بلطا. PEM قيسنتب ةداهش عاشنإب كلذ دعب قدصم ال عجرم ال موقبي

في [قدصم ال عجرم ال](#) لاقم عجار، قدصم ال عجرم ال يدوزمل ةمئاق يلع لوصحلل: ةظالم ايدي بيكيو

ESA ال ةعقوم ال ةداهشل لي محت

صاخات فم ةطساوب ةعقوم ال ةقووم ال ةماع ال ةداهشل عجارب قدصم ال عجرم ال موقبي نأ دعب ESA ال ةعقوم ال ةداهشل لي محتب مق

ههجاو وأ IP ههجاو HTTPS ةمدخ وأ صاخ وأ ماع لئاسر عزوم عم ةداهشل مادختسا كلذ دعب نكمي و ةهجول تالاجم ال ةرداصل ال TLS تالاصتلا عيمج وأ LDAP

ESA ال ةعقوم ال ةداهشل لي محت:

1. وأ PEM قيسنتب مدختسي همالتسا مت يذلا هب قووم ال ماع ال صيخرتلا نأ نم دكأت.

مادختسا كنكمي: **جيملت**. زاهجلا ىللى هليمحت لبق PEM ىللى هليوحت نكمي قيسنت
قيسنتلا ليوحتل، يناعم جمانرب يهو، [OpenSSL](#) تاودأ ةعومجم.
2. ةعقوملا ةداهشلا ليمحت:

تاداهشلا > ةكبشلا ىللى لقتنا

عيقوتلل قوصملا عجرملا ىللى اهلاسرا مت يتلا ةداهشلا مسالىل عرقنا

ةكبشلا نيزخت ةدحو وأ يلملا زاهجلا ىللى ةوجوملا فلملا ىللى راسملا لخدأ

نكمي. ةيلال ةداهشلا لدبتست اهنإف، ةديدل ةداهشلا ليمحت ب موقت امدنع: **ةظالم**
ايتاذ ةعقوملا ةداهشلاب ةطبترم ةطيسو ةداهش ليمحت اضيا

ةعقوملا ةداهشلا ليمحت دعب اهمازتلاو تاريخيغتللا لاسرا ركذت: **ريذحت**

ESA تامدخ عم مادختسالل ةداهشلا ديذحت

يتلا تامدخلل اهمادختسا كنكمي، ESA ىللى اهليمحتو اهعيقوتو ةداهشلا عاشنإ دعب نآلا
ةداهشلا مادختسا بلطتت

دراولا TLS

دراولا TLS تامدخل ةداهشلا مادختسالل ةيلالتلا تاوطخلل لمكأ:

1. **نيعمتسملا > ةكبشلا ىللى لقتنا**.
2. **يغصملا مساقوف رقنا**.
3. **ةداهشلا ةلدسنملا ةمئاقلا نم ةداهشلا مسادح**.
4. **لاسرا ىللى رقنا**.
5. **نييفااضا نيعمتسم يال ةجالحا بسح 4 ىللى 1 نم تاوطخلل ررك**.
6. **تاريخيغتللا ذيفنتب مق**.

رداصللا TLS

رداصللا TLS تامدخل ةداهشلا مادختسالل ةيلالتلا تاوطخلل لمكأ:

1. **ةهوجل يلمكحتللا رصانع > ديربلا تاسايس ىللى لقتنا**.
2. **ةيمومعلا تاداعلا مسق يفي.. ةيمومعلا تاداعلا ريرحت ىللى رقنا**.
3. **ةداهشلا ةلدسنملا ةمئاقلا نم ةداهشلا مسادح**.
4. **لاسرا ىللى رقنا**.

5. تاريخي غتال ذيفنتب مق

HTTPS

HTTPS تامدخل ةداهشال مادختسال ةيلالال تاوطلال لمكأ

1. IP تاهجاو > ةكبشال ال لقتنا
2. ةهجاوال مسال لعل رقتنا
3. HTTPS ةداهشال ةلدسنمال ةمئالال نم ةداهشال مسال ددح
4. لاسرا لعل رقتنا
5. ةيفاضا تاهجاو ال ةجالال بسح 4 ال 1 نم تاوطلال ررك
6. تاريخي غتال ذيفنتب مق

LDAPs

LDAPs ال ةداهشال تلمعتسا steps in order to اذه تمتأ

1. LDAP > ماظنللا ةرادا ال لقتنا
2. مسق دادع ةيلمع لماش LDAP ال يف ..دادع ةيلمع ررحي ةقطق
3. ةداهشال ةلدسنمال ةمئالال نم ةداهشال مسال ددح
4. لاسرا لعل رقتنا
5. تاريخي غتال ذيفنتب مق

URL ةيفصت

URL ةيفصت ةداهشال مادختسال

1. رماوال رطاس ةهجاو يف webSecurityConfig رمالا لخدا
2. ةبلاطمال هذه ال لوصولا دنع Y ديحت نم دكأت .رمالابلاطم ربع ةعباتمالاب مق

Do you want to set client certificate for Cisco Web Security Services Authentication?

3. ةداهشالاب نرتقمال مق رلا ددح
4. نيوكتال تاريخي غت ذيفنتل commit رمالا لخدا

ايطايحت | (تاداهشال) ةداهشال او زاهجال ةئيهت خسن

لمتكملة عداهشلا لمع ىلع زاهجلا نيوكت يوتحي .تقولا اذه يف زاهجلا نيوكت ظفح نم دكأت
اقبسمة فوصوملا تايلمعلا ربع هقيبطت مت يذلا

دربم ليكشت ةادألا تذقنا steps in order to اذه تمتأ

1. ضرعل يلحملا رتويبمكلا ىلا فلملا ليزنت > نيوكتلا فلم > ماظنلا ةرادا ىلا لقتنا
ظفح وأ

2. ةداهشلا ريصت:

تاداهشلا > ةكبشلا ىلا لقتنا

ةداهشلا ريصت ىلع رقنا

اهريصت دارملا ةداهشلا دح

ةداهشلا فلم مسا لخدأ

ةداهشلا فلم رورم ةملك لخدأ

ردصي ةقطاق

ةكبش زاهج وأ يلحم زاهج ىلا فلملا ظفح مق

ىلا ةدوعلا رمألا ءاغلا ىلع رقنا وأ تقولا اذه يف ةيفاضا تاداهش ريصت نكمي
تاداهشلا عقوم > ةكبشلا

فلملا ئشنني يذلاو، PKCS#12 قيسنتب ةداهشلا ةيلمعلا هذه ظفحت: **ةظحال**
رورملا ةملك ةيماح مادختساب هظفحي

دراولا TLS طيشنت

(GUI) ةيموسرلا مدختسملا ةهجاوب لاصتالاب مق، ةدراولا تاسلجلا عيملج TLS طيشنتل
مت يذلا دراولا ديربل عم تسملا ديربل قفدت تاسايس > ديربل تاسايس رتخاو، بيولل
ةيالاتا تاوطخلا لمكأ م، هنيوكت

1. اهل جهنلا ليذعت بجي ءاغصا ةدحو رتخأ.

2. هريحتل جهنلا مساب صاخلا طابترالا قوف رقنا.

3. TLS يوتسم نيبيعتل هذه ةقداصملا اوريفشنتلا تاراخي دحأ رتخأ، نامألا تازيم مسق يف
عم تسملا اوريبل قفدت جهنلا بولطملا

TLS مادختسا متي ال، راخلا اذه رايتخا دنع - فاقيا ل ديقي

لكلذ عمو. ESA ىلا ديبل MTA نم ضوافتلا TLS نكمي، راخلا اذه رايتخا دنع - لصف
يف SMTP ةلماعم رمتست، (220 ةباجتسا مالتسا لبق) دعب نع MTA ضوافت مل اذا
نم أشنت ةداهشلا تناك اذا امام ققحتلل ةلواحم يءارجا متي ال. (ةرفشملا ريغ) ولخلا

SMTP ةلماعم دوعت نلف ، 220 ةباجتسا يقلت دعب أطخ ثدح اذا .هب قووثوم قدصم عجرم ص.نلا حسم ىلا

ملا ESA ىلا ديعبلا MTA نم TLS ىلع ضوافتلا نكمي ،رايخلا اذو رايخا دنع - بولطم يلا لاسرا متي نلف ،ضوافتلا لشف اذا .لاجملا ةداهش نم ققحتلل ةلواحه ةيأ عارجا متي ربع ديربلا ميسلست متيسف ،ضوافتلا حجن اذا .لاصتالا لالخ نم ينورتكللا ديرب ةرفشم لمع ةسلج

4. لاسرا ىلع رقنا .

5. اذا ،تقولا اذو ي ف يرايخا قىلعت ةفاضلا كنكمي .تاريخيغتللا ذيفنت رزلا قوف رقنا .ابولطم كلذنا

6. تاريخيغتللا ظفحل تاريخيغتللا ذيفنت قوف رقنا .

اهترتخا يتلا TLS تاداعلا مادختساب يغصملا باب صاخلا ديربلا قفدت جهن شيحت نالا متي

لاجم نم ةعومجم ديحت نم لصي نا دراولا تاسلجلا TLS طشن steps in order to اذو تمتأ

1. > ديربلا تاسايس رتخاو بيولا ربع (GUI) ةيموسرلا مدختسمللا ةهجاوب لاصتالاب مق . HAT ىلع ةماع ةرطن

2. ةبسانملا "نيلسرمللا ةعومجم" ىلا (لسرمللا) لسرملاب صاخلا IP/FQDN ةفاضلا .

3. تمق يتلا نيلسرمللا ةعومجم نرتقملا ديربلا قفدت جهنل TLS تاداعلا ريحت . ةقباسلا ةوطخلا ي ف اهل يدعتب

4. لاسرا ىلع رقنا .

5. اذا ،تقولا اذو ي ف يرايخا قىلعت ةفاضلا كنكمي .تاريخيغتللا ذيفنت رزلا قوف رقنا .ابولطم كلذنا

6. تاريخيغتللا ظفحل تاريخيغتللا ذيفنت قوف رقنا .

اهترتخا يتلا TLS تاداعلا ب نيلسرمللا ةعومجملا ديربلا قفدت جهن شيحت نالا متي

ESA ةجلاعم ةيفيك لوح تامولعمللا نم ديزم ىلع لوصحلل ةلاقملا هذه ىلا عجرا :**حيملت** [ESA؟ ف ةداهشلا نم ققحتلل ةيمزراوخللا يه ام](#) : TLS نم ققحتلل

رداصللا TLS طيشنت

ةيموسرلا مدختسمللا ةهجاوب لاصتالاب مق ،ةرداصللا لمعلا تاسلجلا TLS طيشنت لجا نم ةيلاتلا تاوطخلا لمكأ م ،ةهجولا ي ف مكحتلا رصانع > ديربلا تاسايس رتخاو ،بيولل (GUI)

1. ةياع فيضي ةقطق .

2. ةهجولا لاجم ةفاضلا .

3. TLS عون نيكمتل تاراخيلا هذه دحا رتخاو ةلدسنملا ةمئاقلا رقنا ، TLS معد مسق ي ف :هنوك متيس يذلا

ههجاو لا نم ةرداصل الالاصتال TLS لىل ضوافتلا متي ال ،رايخلا اذه رايخا دنع - none لاجملل MTA لىل .

MTA (MTA) لىل ESA ههجاو نم TLS لىل ضوافتلا متي ،رايخلا اذه رايخا دنع - **لضفم** ةلماعم رمتست ،(220 ةباجتسا يقلت لبق) TLS ضوافت لشف اذا ،كلذ عمو . لاجملل تناك اذا امم ققحتلل ةلواحم ي اارجا متي ال . (رفشملا سيولو) حوضولا ي SMTP دوعت نلف ،220 ةباجتسا يقلت دعب اطح ثدح اذا . ةقث قدصم عجرم نم أشنت ةداهشلا صنلا حسم لىل SMTP ةلماعم .

(تآ) MTA لىل ESA ههجاو نم TLS لىل ضوافتلا متي ،رايخلا اذه رايخا دنع - **بولطم** نلف ،ضوافتلا لشف اذا . لاجملا ةداهش نم ققحتلل ةلواحم ةي اارجا متي مل . لاجملل ميلاست متيسف ،ضوافتلا حجن اذا . لالاصتالا لالخ نم ينورتكلل ديرب ي لاسرا متي . ةرفشم لمع ةسلج ربع ديربلا .

MTA لىل ESA نم TLS لىل ضوافتلا متي ،رايخلا اذه رايخا دنع - **Preferred-Verify** هذه نإف ،ةلاجال هذه يفو . لاجملا ةداهش نم ققحتلا زاهجلا لواحيو ،لاجملل (تاقافاتالا) :ةنكمم ةثالثل جئاتنلا

ةسلج ربع ديربلا ميلاست متي . ةداهشلا نم ققحتلا متي و TLS لىل ضوافتلا متي . ةرفشم لمع

ربع ديربلا ميلاست متي . ةداهشلا نم ققحتلا متي مل نكلو ، TLS لىل ضوافتلا متي . ةرفشم لمع ةسلج

ديربلا ةلاسرا ميلاست متي . ةداهشلا نم ققحتلا متي ملو ، TLS لالاصتا اارجا متي مل TLS لىل ضوافتلا متي ،رايخلا اذه رايخا دنع - **Required-Verify** . يداع صنب ينورتكللا هذه يفو . لاجملا ةداهش نم ققحتلا بلطتو ،لاجملل (تاقافاتالا) MTA لىل ESA نم :ةنكمم ةثالثل جئاتنلا هذه نإف ،ةلاجال

ةلاسرا ميلاست متي . ةداهشلا نم ققحتلا متي و ، TLS لالاصتا لىل ضوافتلا متي . ةرفشم ةسلج ربع ينورتكللا ديربلا

عجرم ةطساوب ةداهشلا نم ققحتلا متي ال نكلو ، TLS لالاصتا لىل ضوافتلا متي . ةرفشم ةداهشلا ميلاست متي مل . ةقث قدصم

ديربلا ميلاست متي مل نكلو ، TLS لالاصتا لىل ضوافتلا متي ال

4. ههجاو لاجملل ههجاو *مكحت رصانع* لىل ةبولطم ةيفاضا تاريخي غت ي اارجا مق .

5. لاسرا لىل رونا .

6. اذا ،تقولا اذه ي رايخا قيعت ةفاضلا كنكمي . تاريخي غتلا ذيفنت زولا قوف رونا . ابولطم كلذ ناك

7. تاريخي غتلا ظفحل تاريخي غتلا ذيفنت قوف رونا .

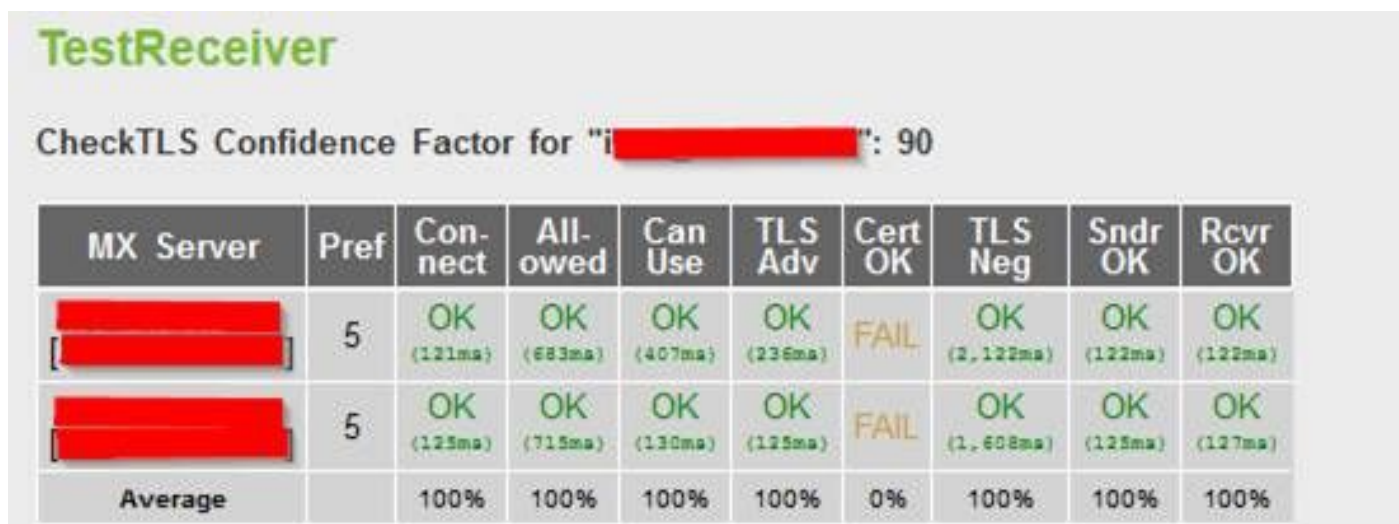
ESA ةداهشل ئطاخال نيوكتلا ضارعا


```

// email / test To:
250 STARTTLS
[000.344] We can use this server
[000.344] TLS is an option on this server
[000.344] -->STARTTLS
[000.384]<-- 220 Go ahead with TLS
[000.385] STARTTLS command works on this server
[000.558] Connection converted to SSL
SSLVersion in use: TLSv1.2
Cipher in use: ECDHE-RSA-AES256-GCM-SHA384
Certificate 1 of 3 in chain: Cert VALIDATED: ok
Cert Hostname VERIFIED (rocdn-mx-01.cisco.com = rocdn-mx-01.cisco.com | DNS:rocdn-mx-01.cisco.com | DNS:rocdn-inbound-a.cisco.com | DNS:rocdn-inbound-b.cisco.com | DNS:rocdn-inbound-c.cisco.com | DNS:rocdn-inbound-d.cisco.com | DNS:rocdn-inbound-e.cisco.com | DNS:rocdn-inbound-f.cisco.com | DNS:rocdn-inbound-g.cisco.com | DNS:rocdn-inbound-h.cisco.com | DNS:rocdn-inbound-i.cisco.com | DNS:rocdn-inbound-j.cisco.com | DNS:rocdn-inbound-k.cisco.com | DNS:rocdn-inbound-l.cisco.com | DNS:rocdn-inbound-m.cisco.com | DNS:rocdn-inbound-n.cisco.com)
Not Valid Before: Oct 3 12:35:32 2018 GMT
Not Valid After: Oct 3 12:45:00 2020 GMT
subject= /C=US/ST=CA/L=San Jose/O=Cisco Systems, Inc./CN=rocdn-mx-01.cisco.com
issuer= /C=US/O=HydrantID (Avalanche Cloud Corporation)/CN=HydrantID SSL ICA G2
Certificate 2 of 3 in chain: Cert VALIDATED: ok
Not Valid Before: Dec 17 14:25:10 2013 GMT
Not Valid After: Dec 17 14:25:10 2023 GMT
subject= /C=US/O=HydrantID (Avalanche Cloud Corporation)/CN=HydrantID SSL ICA G2
issuer= /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2
Certificate 3 of 3 in chain: Cert VALIDATED: ok
Not Valid Before: Nov 24 18:27:00 2006 GMT
Not Valid After: Nov 24 18:23:33 2031 GMT
subject= /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2
issuer= /C=BM/O=QuoVadis Limited/CN=QuoVadis Root CA 2
[000.831] -->EHLO www6.CheckTLS.com
[000.874]<-- 250-rocdn-inbound-c.cisco.com
250-8BITMIME
250 SIZE 33554432
[000.874] TLS successfully started on this server
[000.874] -->MAIL FROM:<test@checktls.com>
[000.915]<-- 250_sender <test@checktls.com> ok
[000.915] Sender is OK
[000.916] -->QUIT
[000.957]<-- 221 rocdn-inbound-c.cisco.com

```

CheckTLS.com لشرح لثلاث



مل متي ق قحت التا م في ض م س ا نم ق قحت التا م تي مل رارق

دومع في ة ع ق و ت م ل ا ة ج ي ت ن ل ل ا ف ، م ا د خ ت س ا ل ا د ي ق ا ي ت ا ذ ع ق و م ل ا ق د ص م ن ا ك ا ذ ا : ة ظ ح ا ل م "ل ش ف" يه "ق ف ا و م".

نم ق قحت ف ، ل ش ف ي ل ا ز ي ا ل T L S - v e r i f y ن ا ك و م ا د خ ت س ا ل ا د ي ق ة ع ق و م ل ا C A ة د ا ه ش ت ن ا ك ا ذ ا ر ص ا ن ع ل ا ه ذ ه ة ق و ب ا ط م :

- ة د ا ه ش ل ل ع ئ ا ش ل ل م س ا ل ا .
- (ة ج ا و ل > ة ك ب ش ل ل > (G U I) ة ي م و س ر ل ل م د خ ت س م ل ا ة ج ا و ي ف) ف ي ض م ل ا م س ا .
- T e s t R e c e i v e r ل و د ج ي ف M X م د ا خ د و م ع و ه ا ذ ه : M X ل ج س ف ي ض م م س ا .

ل ا ة ع ب ا ت م ل ا ب م ق ف ، ع ا ط خ ا ل ا د ه ا ش ت و ق د ص م ل ا ع ج ر م ل ا ن م ة ع ق و م ة د ا ه ش ت ي ب ث ت م ت ا ذ ا ا ه ا ل ص ا و ة ل ك ش م ل ا ف ا ش ك ت س ا ة ي ف ي ك ل و ح ت ا م و ل ع م ي ل ع ل و ص ح ل ل ي ل ا ت ل ا م س ق ل ا .

اهال صإو ااطخأل فاشكتسا

ESA ىلع اهال صإو اىس اسأل TLS ااطخأ فاشكتسا ةىفك مسقلا اذه حضوي

ةطسوت مالا تاداهشلا

نم ال دبة ىلجال تاداهشلا شىدحت متي ام دنع ةصاخ، ةطيسولا تاداهشلا ةفعاضم نع شحبا مت وا تريغت دق ةطيسولا (تاداهشلا) ةداهشلا نوكت نا لم تحملل نم. ةديج ةداهش عاشنا نم ديدعلل لىمحتب تماق دق ةداهشلا نوكت نا لم تحملل نم، حىحص ريغ لكشبا اهطبر ققحتلاو ةداهشلا لسلسلست يى لكاشم ثودح لىل ك لذى دوى نا نكمي. ةطيسولا تاداهشلا اهنم.

بولطم TLS لاصتا لشفب ةصاخلا تامالعال ني كمت

لاجم لىل لئاسرلا مىلست دنع TLS ضوافت لشفب اذا هيبنت لاسرلا ESA نيوكت كنكمي TLS تاضوافم لهجولا لاجملا مسالى هيبنتلا ةلاسريوتحت. TLS لاصتا بلطتي يقلت لهطبض مت نىذل نىم لتسملا عىم لىل هيبنتلا ةلاسرا ESA لسري. ةلشافلا ماطنلا هيبنت عاونال رىذحتلا ةروطخ يوتسم تاهيبنت

لاجم لكل هنىعت نكمي ال ك لذل، يمومع دادع اذه: **ةظالم**

TLS لاصتا تاهيبنت ني كمتلا ةيلاتلا تاوطخلا لمكأ:

1. ةهجولا يى م كحتلا رصانع > دىربلا تاساىس لىل لقتنا.
2. ةماعلا تاداعلا رىرت لىل رقنا.
3. بولطم TLS لاصتا لشفب دنع هيبنت لاسرلا راي تخاللا ةناخ ددح.

صاخلا (CLI) رماوال رطس ةهجاو رما م ادختساب دادعلا اذه نيوكت اضيأ كنكمي: **حىملت دادعاب**

اهم ادختسا رذعت نكلو، ام لاجملا اهل TLS دوجو مزلي يىتلا تالىثملا لىجستب ESA موقت امك طورشلا هذه نم يى اءاىتسا دنع اذه شدى. زاهجلا دىرب تالجتس يى:

- (ESA نم *EHLO* رمال مه فى مل، لاثملا لىبس لىل) *ESMTP* دىعبلا *MTA* معدي ال.
- يىتلا تاقحلملا ةمئاق يى نكى مل *STARTTLS* رمال نكلو، *ESMTP* دىعبلا *MTA* معدي *EHLO* ةباجتسا يى اهنع نلعا.
- ESA لسرا ام دنع اطق عم تباجتسا اهنكلو، *STARTTLS* دادتما نع ةدىعبلا *MTA* تنلعا *STARTTLS* رمال.

دىربلا تالجتس يى ةحجانلا TLS لاصتا تاسلج عقوم دىدحت

ىرخالا ةماهلا تاءارجلال لىل ةفاضلاب، دىربلا تالجتس يى TLS تالاصتا لىجست متي تاسورىفلا ةحفاكبم ةصاخلا ماكأل او، ةىفصتلا تاءارجا لثم، لئاسرلاب ةطبت رملال لاخدا دجوي، حججان TLS لاصتا دوجو ةلح يى. مىلستلا تالواجمو، اهىف بوغرملا ريغ لئاسرلاو

TLS لاخدا لشفاف TLS لاصتا جتنني، لثامم وحن ىلعو. ديربلا تالجس يف ئشان TLS ح/جن كلت ميلاست متي مل، لجسلا فلم يف نرتقم TLS لاخدا ةلاسرا نكي مل اذا. لشفاف TLS لاصتا ربع ةلاسرا.

[ESA](#) ل لئاسرا ريضم ديحتل Cisco دنننسم ىل عجرا، ديربلا تالجس مهفل: **جيملت**

(لابقتسالا): ديعلبلا فيضملا نم حجنا TLS لاصتا ىلع لاثم يلي امي فو

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address 10.0.0.1 reverse dns host mail.example.com verified yes
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS - 1.1
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

(لابقتسالا): ديعلبلا فيضملا نم لاصتا لشفاف TLS نم لاثم انه

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address 10.0.0.1 reverse dns host mail.example.com verified yes
Mon Apr 16 18:59:13 2018 Info: ICID 590052584 ACCEPT SG UNKNOWNLIST match sbrs[2.1:10.0] SBRS 2.7
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 TLS failed: (336109761, 'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

(ميسلاستالا): ديعلبلا فيضملا حجنا للافاف TLS لاصتا ىلع لاثم يلي امي فو

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 10.0.0.1 port 25
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

(ميسلاستالا): ديعلبلا فيضملا للافاف TLS لاصتا لشفاف ىلع لاثم يلي امي فو

```
Mon Apr 16 00:01:34 2018 Info: New SMTP DCID 40986669 interface 192.168.1.1 address 10.0.0.1 port 25
Mon Apr 16 00:01:35 2018 Info: Connection Error: DCID 40986669 domain: domain IP:10.0.0.1 port: 25 details: 454-'TLS not available due to temporary reason' interface: 192.168.1.1 reason: unexpected SMTP response
Mon Apr 16 00:01:35 2018 Info: DCID 40986669 TLS failed: STARTTLS unexpected response
```

ةلص تاذا تامولعم

- [يئاهنلا مدختسمللا ةلدا - Cisco](#) نم ينورتكلالا ديربلا نامأ زااج
- [يئاهنلا مدختسمللا ةلدا - Cisco](#) نم ىوتحملا نامأ قراا زااج
- [Cisco Systems](#) - تادنننسملا و ينقتلا معدلا

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل 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 ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ئ ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا