تكوين خادم SMTP لاستخدام AWS SES

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين **Secure Network Analytics Manager** (SNA) المطلوب إستخدامها **Amazon Web Services Simple Email Service** (AWS SES).

المتطلبات الأساسية

المتطلبات

توصي Cisco بمعرفة الموضوعات التالية:

- أس إس إس أو

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- **Stealthwatch Management Console v7.3.2**
- خدمات AWS SES كما هي موجودة في 25 مايو 2022 مع **Easy DKIM**

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهم للتأثير المحتمل لأي أمر.

التكوين

مراجعة تكوين AWS SES

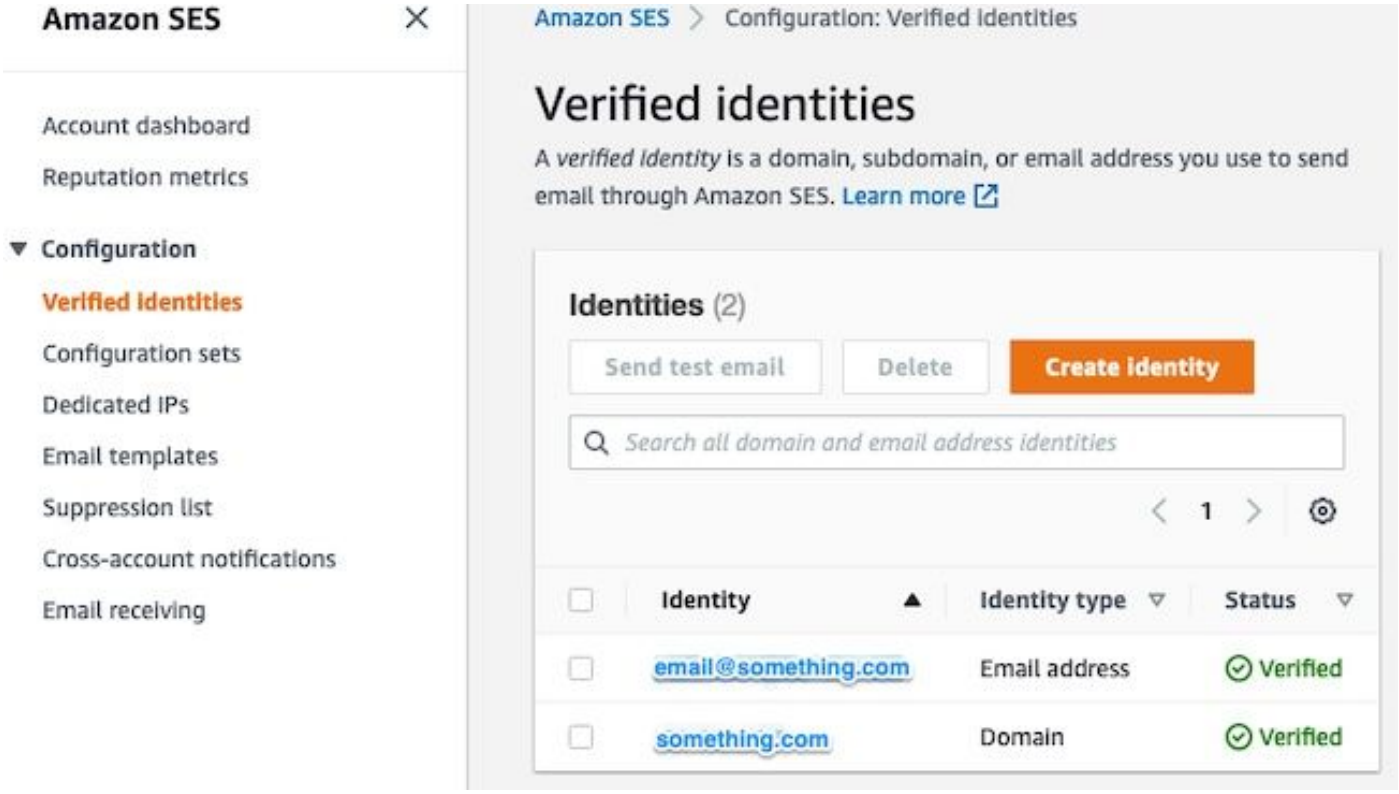
يلزم توفر ثلاث وحدات بت من المعلومات من AWS:

1. موقع AWS SES
2. اسم مستخدم SMTP
3. كلمة مرور SMTP

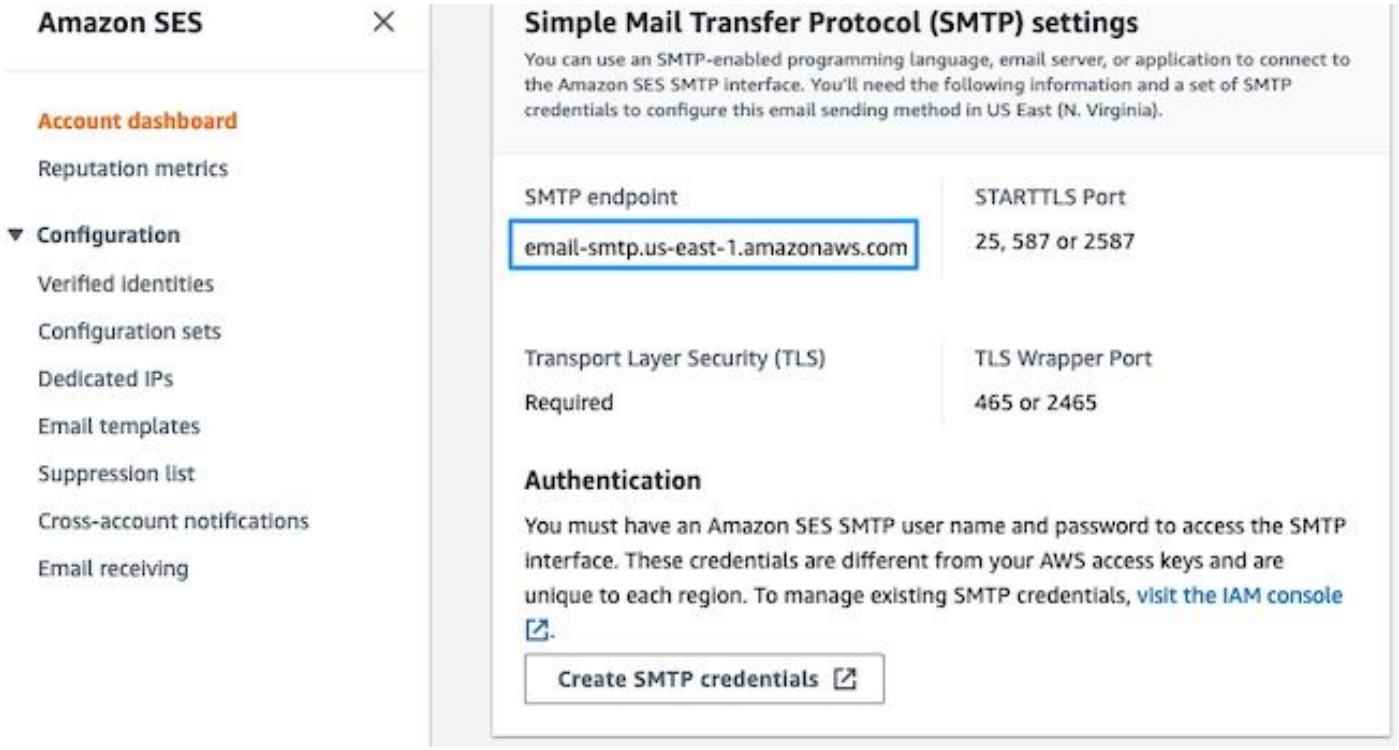
ملاحظة: AWS SES الموجود في المربع الرملي مقبول ولكن كن على دراية بالقيود المفروضة على بيئات وضع الحماية: https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html

في وحدة تحكم AWS، انتقل إلى **Amazon SES**، ثم حدد **Configuration** وانقر فوق **Verified Identities**.

يجب أن يكون لديك مجال تم التحقق منه. عنوان البريد الإلكتروني الذي تم التحقق منه غير مطلوب. ارجع إلى وثائق AWS https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure



لاحظ موقع نقطة نهاية SMTP. هذه القيمة مطلوبة لاحقا.



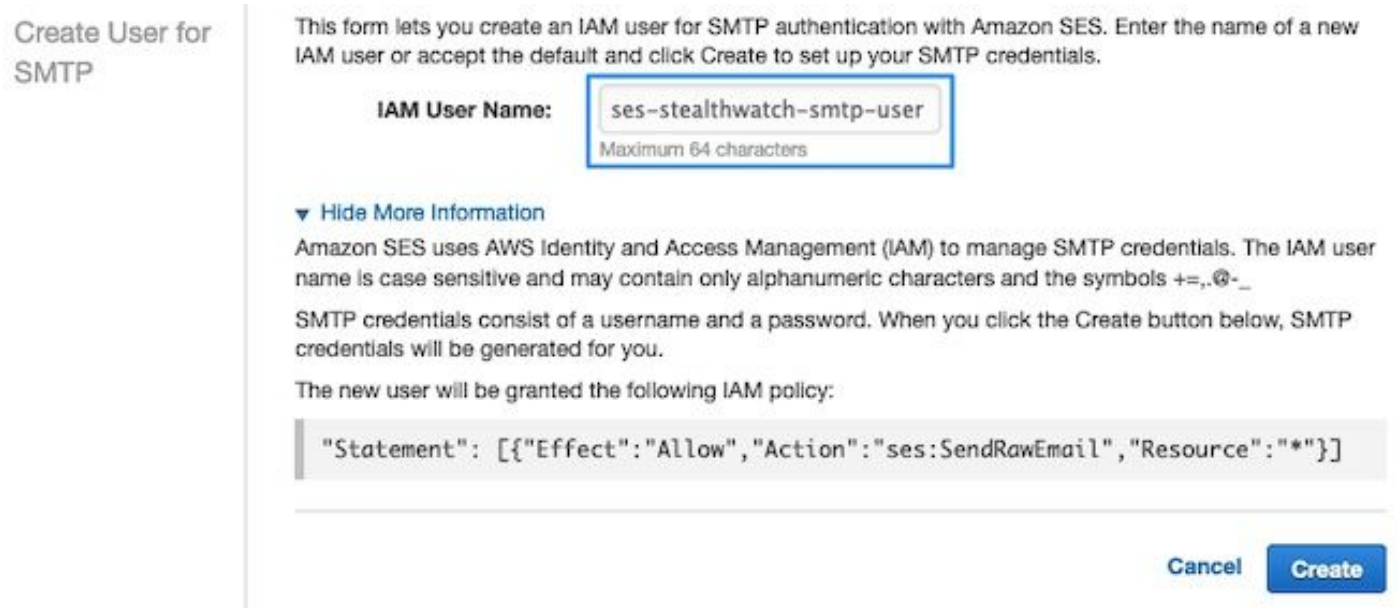
إنشاء بيانات اعتماد AWS SES SMTP

في وحدة تحكم AWS، انتقل إلى **Amazon SES**، ثم انقر **Account Dashboard**.

قم بالتمرير لأسفل إلى "**Simple Mail Transfer Protocol (SMTP) settings**" وانقر فوق **Create SMTP Credentials** عندما تكون مستعدًا لإكمال هذا التكوين.

لا يجب أن بيانات الاعتماد القديمة غير المستخدمة (حوالي 45 يومًا) خاطئة كبيانات اعتماد غير صحيحة.

في هذا النافذة جديد، قم بتحديث اسم المستخدم إلى أي قيمة وانقر **Create**.

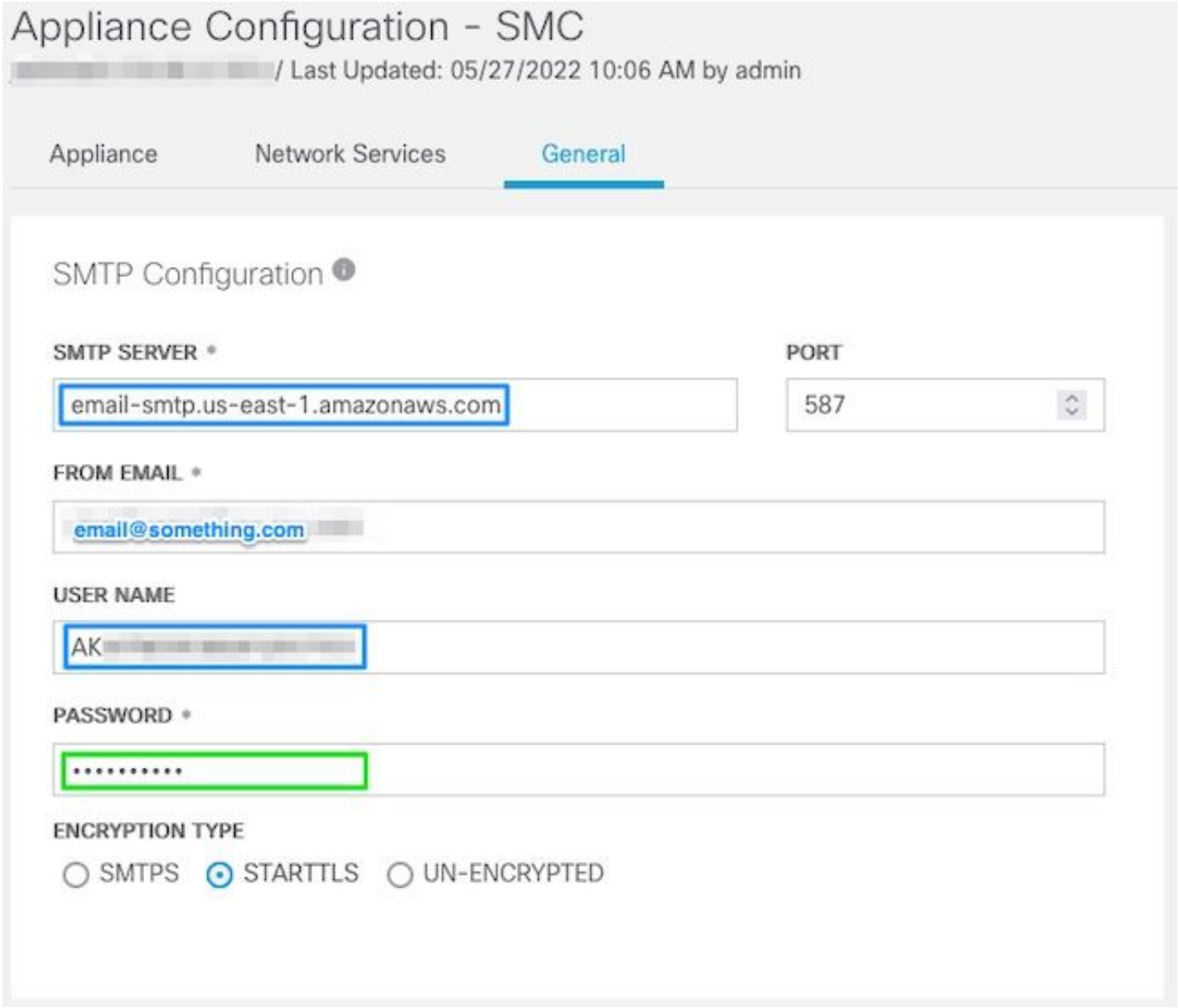


عندما تعرض الصفحة بيانات الاعتماد، قم بحفظها. إبقاء علامة تبويب المستعرض هذه مفتوحة.

تكوين SNA Manager SMTP

تسجيل الدخول إلى **SNA Manager**، و مفتوحة **SMTP Notifications** قسم

1. فتح **Central Management > Appliance Manager**.
2. انقر فوق **Actions** قائمة الجهاز.
3. تحديد **Edit Appliance Configuration**.
4. حدد **General** علامة تبويب.
5. تمرير ألأسفل إلى **SMTP Configuration**
6. إدخال القيم التي تم تجميعها من AWS **SMTP Server**: اذه وه موقع نقطة نهاية SMTP الذي تم تجميعه من **SMTP Settings** من **AWS SES Account Dashboard** صفحة**Port**: أدخل 25 أو 587 أو 2587**From Email**: يمكن تعييني اذه إلى أي عنوان بريد إلكتروني يحتوي على **AWS Verified DomainUser Name**: اذه وه اسم مستخدم SMTP الذي تم تقديمه في الخطوة ألأخيرة في **Review AWS SES Configuration** قسم**Password**: هذه هي كلمة مرور SMTP التي تم تقديمها في الخطوة ألأخيرة في **Review AWS SES Configuration** قسم**Encryption Type**: حدد STARTTLS (إذا قمت بتحديد SMTPS، فقم بتحرير المنفذ إلى 465 أو 2465)
7. تطبيق الإعدادات وانتظار **SNA Manager** للعودة إلى **UP** والية في **Central Management**



تجميع شهادات AWS

إنشاء جلسة SSH إلى **SNA Manager**، والدخول كمستخدم جذري.

مراجعة هذه العناصر الثلاثة

- تغيير موقع نقطة نهاية SMTP (على سبيل المثال email-smtp.us-east-1.amazonaws.com)
- غير المينا يستعمل (مثل تقصير من 587 ل STARTTLS)
- الأوامر ليس لها STDOUT، يتم إرجاع المطالبة عند الاكتمال

ل STARTTLS (المنفذ الافتراضي 587):

```
openssl s_client -starttls smtp -showcerts -connect email-smtp.us-east-1.amazonaws.com:587 <<<
"Q" 2>/dev/null > mycertfile.crt awk 'split_after == 1 {n++;split_after=0} /-----END
CERTIFICATE-----/ {split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt for i in `ls -t1
*.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert*
mycertfile.crt
```

بالنسبة ل SMTPS (المنفذ الافتراضي 465):

```
openssl s_client -showcerts -connect email-smtp.us-east-1.amazonaws.com:465 <<< "Q" 2>/dev/null
> mycertfile.crt awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
{split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt for i in `ls -t1 *.pem`; do cp $i
$(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert* mycertfile.crt
```

الدليل اذه نم ذخأت ال ،يلاحلا لمعلا ليلد يف PEM قحلم تاذ تاداهشلا تافلم ءاشنإ متي (ريخألا رطسلا / PWD رمأ نم جارخإ)

```
sna_manager:~# openssl s_client -starttls smtp -showcerts -connect email-smtp.us-east-
1.amazonaws.com:587 <<< "Q" 2>/dev/null > mycertfile.crt
sna_manager:~# awk 'split_after == 1 {n++;split_after=0} /-----END CERTIFICATE-----/
{split_after=1} {print > "cacert" n ".pem"}' < mycertfile.crt
sna_manager:~# for i in `ls -t1 *.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}'
$i).pem ; done ; rm -f cacert* mycertfile.crt
sna_manager:~# ll
total 16
-rw-r--r-- 1 root root 1648 May 27 14:54 Amazon.pem
-rw-r--r-- 1 root root 1829 May 27 14:54 AmazonRootCA1.pem
-rw-r--r-- 1 root root 2387 May 27 14:54 email-smtp.us-east-1.amazonaws.com.pem
-rw-r--r-- 1 root root 1837 May 27 14:54 StarfieldServicesRootCertificateAuthority-G2.pem
sna_manager:~# pwd
/root
```

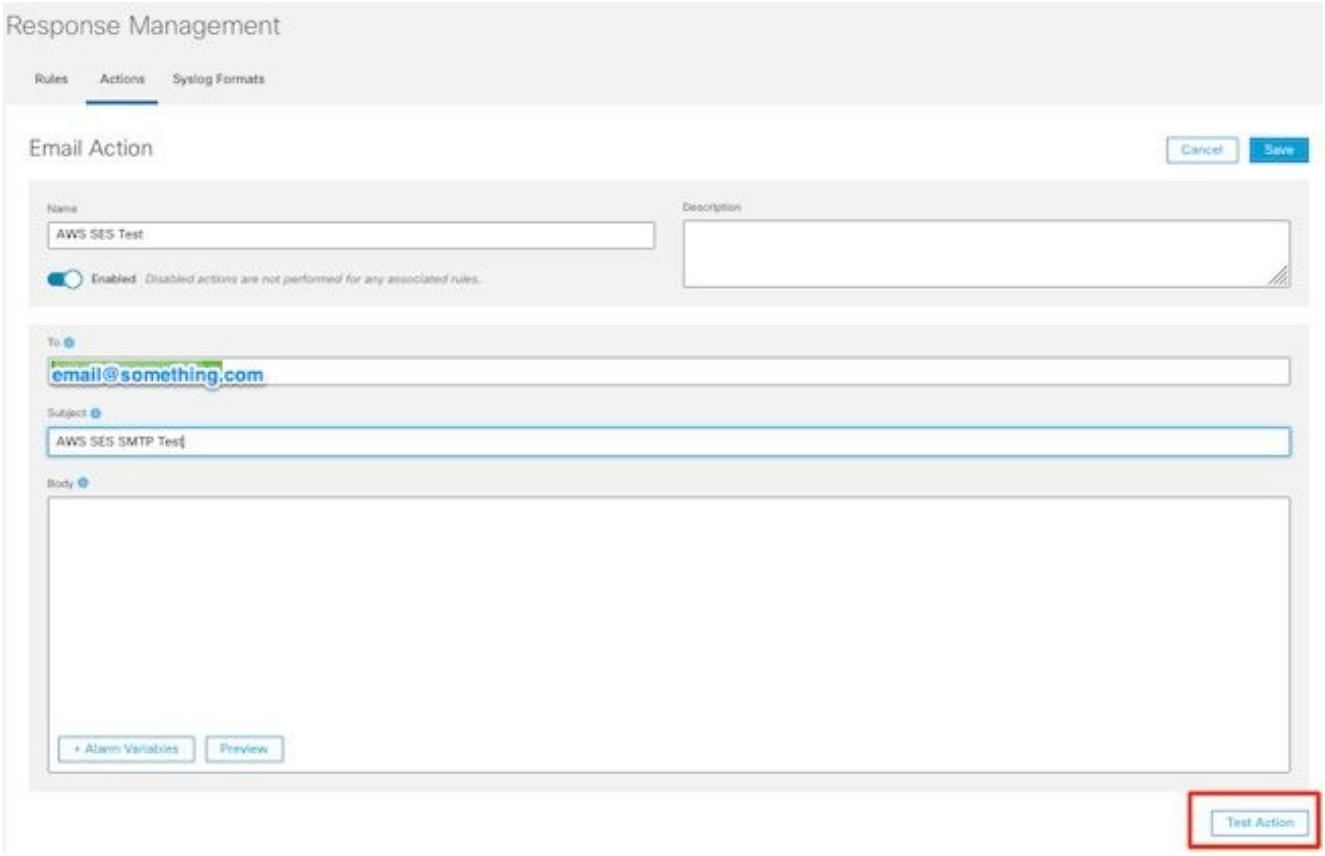
مادختساب كيدل يلحملا زاهجلا ىلإ **SNA Manager** ىلع اهؤاشنإ مت يتلا تافلملا ليزنتب مق جمانرب لقن تافلملا يذلا هراتخت (Filezilla، WinSCP، امو ىلإ كلذ)، ةفاضإو هذه تاداهشلا ىلإ **SNA Manager trust store** يف **Central Management.**

1. حتف **Central Management > Appliance Manager.**
2. انقر قوف **Actions** ةمئاق زاهجلا.
3. ديدحت **Edit Appliance Configuration.**
4. ددح **General** ةمالع بيوبت.
5. ريرمت لفسأل ىلإ **Trust Store**
6. ديدحت **Add New**
7. مق ليمحتب لك ةداهش، ىصوم مادختساب مسا فلملا ك **Friendly Name**

تكوين إجراء البريد الإلكتروني لإدارة الاستجابة

تسجيل الدخول إلى **SNA Manager**، ويفتح ال **Response Management** مسق

1. ددح **Configure** ةمالع بيوبت يف الشريط الرئيسي على طول الجزء العلوي من الشاشة
2. ديدحت **Response Management**
3. نم عقوم **Response Management** ةحفص، ديدحت **Actions** ةمالع بيوبت
4. ديدحت **Add New Action**
5. ديدحت **Email**ريفوت مسا لإجراء البريد الإلكتروني اذهلخدأ ناونع البريد الإلكتروني للمستلم يف الحقل "إلى" (ظحال نأ اذه بجي نأ يمتني إلى المجال الذي مت التحقق هنم يف AWS SES)الموضوع نكمم نوكي يأ ةجاح.

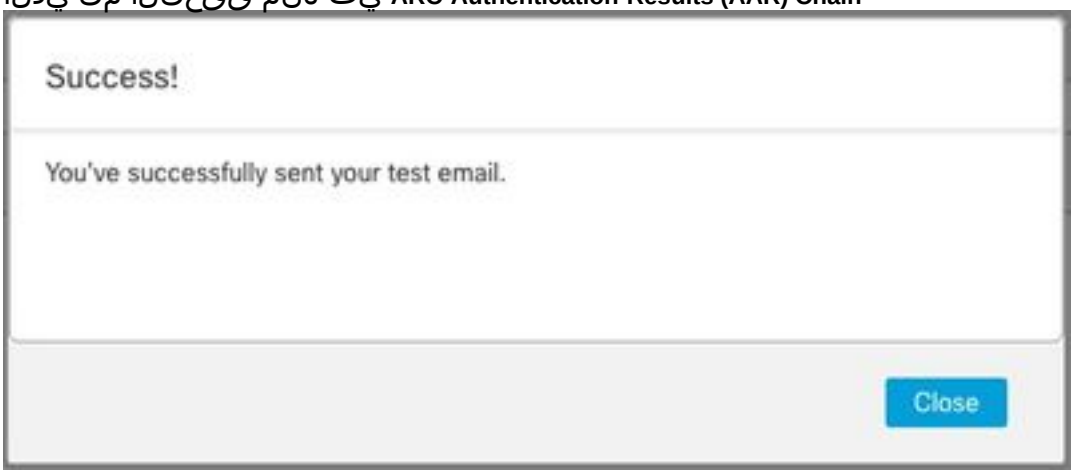


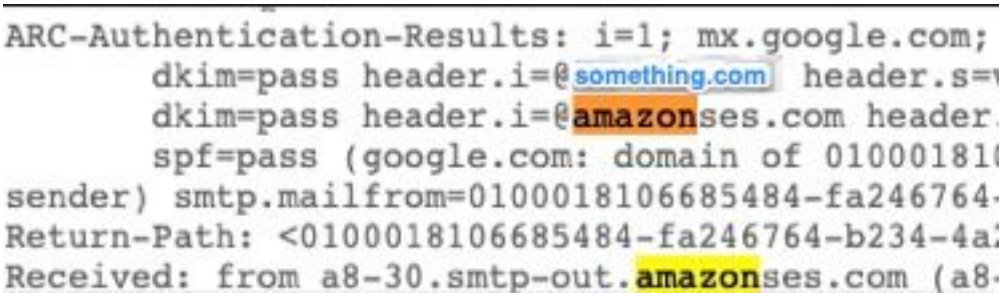
6. انقر **Save**

التحقق من الصحة

تسجيل الدخول إلى **SNA Manager**، ويفتح ال **Response Management** القسم:

1. حدد **Configure** عالمة تبويب في الشريط الرئيسي على طول الجزء العلوي من الشاشة
2. تحديد **Response Management**
3. من موقع **Response Management** صفحة، تحديد **Actions** عالمة تبويب
4. حدد القطع الناقص في **Actions** عمود لصف إجراء البريد الإلكتروني الذي قمت بتكوينه في **Configure Response Management Email Action** مقطع، وحدد **Edit**.
5. تحديد **Test Action** وإذا كان التكوين صحيحا، يتم تقديم رسالة نجاح ويتم تسليم بريد إلكتروني.
   في رأس البريد الإلكتروني، يتم عرض الأمر في " **Received**"المجال، والأذهان، مع المجال الذي تم التحقق منه في **ARC-Authentication-Results (AAR) Chain**





6. إذا لم يتم تقديم شعار في أعلى الشاشة - انتقل إلى قسم أستكشاف الأخطاء وإصلاحها

استكشاف الأخطاء وإصلاحها

يحتوي الملف على رسائل الخطأ الخاصة /lancope/var/logs/containers/sw-reponse-mgmt.log يعرض الأمر
بإجراءات الاختبار. الخطأ الأكثر شيوعا، والإصلاح مدرج في الجدول.
لاحظ أن رسائل الخطأ المدرجة في الجدول هي مجرد جزء من سطر سجل الأخطاء

الخطأ	إصلاح
SMTPSendFailedException: تم رفض 554 رسالة: لم يتم التحقق من صحة عنوان البريد الإلكتروني. فشلت المحاولات في التحقق من المنطقة US-EAST-1: {email_address}	قم بتحديث "من البريد الإلكتروني" في تكو SNA ManagerSMTP إلى بريد إلكتروني يتم المجال الذي تم التحقق من AWS SES
AuthenticationFailedException: بيانات اعتماد المصادقة 535 غير صالحة	تكرار الأقسام إنشاء بيانات اعتماد AWS SES SNA Manager SMTP وتكوين تكوين SMTP
SunCertPathBuilderException: تعذر العثور على مسار شهادة صالح للهدف المطلوب	تأكد من أن جميع الشهادات المقدمة من AWS مو في المخزن الموثوق بإدارة SNA - قم بإجراء الت الحزم عند **إجراء الاختبار** وتتم مقارنة الشهادات المقدمة من جانب الخادم للثقة بمحتويات المخ
نهج SSL:tls_process_ske_dhe:dh مفتاح صغير جدا	انظر الإضافة
أي خطأ آخر	فتح حالة مركز المساعدة الفنية للمراجعة

إضافة: مفتاح DH صغير جدا.

هذه مشكلة جانبية لـ AWS، حيث أنهم يستخدمون مفاتيح 1024 بت عند إستخدام شفرات SSL. تعرض SNA مدير يرفض متابعة جلسة (ذات إمكانية الوصول إلى logAm) و DHE و EDH مخرجات الأمر مفاتيح درجة حرارة الخادم من اتصال OpenSSL عند إستخدام شفرة DHE/EDH.

```
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587 -
cipher "EDH" <<< "Q" 2>/dev/null | grep "Server Temp"
Server Temp Key: DH, 1024 bits
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587 -
cipher "DHE" <<< "Q" 2>/dev/null | grep "Server Temp"
Server Temp Key: DH, 1024 bits
sna_manager:~# openssl s_client -starttls smtp -connect email-smtp.us-east-2.amazonaws.com:587
<<< "Q" 2>/dev/null | grep "Server Temp"
Server Temp Key: ECDH, P-256, 256 bits
```

الحل الوحيد المتاح هو إزالة جميع شفرات DHE و EDH باستخدام الأمر حيث يقوم المستخدم الجذري على SMC، ويقوم AWS بتحديد مجموعة شفرة ECDHE وينجح الاتصال.

```
cp /lancope/services/swos-compliance/security/tls-ciphers /lancope/services/swos-compliance/security/tls-ciphers.bak ; > /lancope/services/swos-compliance/security/tls-ciphers ; echo "TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_256_GCM_SHA384:TLS_AES_128_CCM_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:AES256-GCM-SHA384" > /lancope/services/swos-compliance/security/tls-ciphers ; docker restart sw-response-mgmt
```

معلومات ذات صلة

- https://docs.aws.amazon.com/ses/latest/dg/setting-up.html
- https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure
- https://docs.aws.amazon.com/ses/latest/dg/smtp-credentials.html
- https://docs.aws.amazon.com/ses/latest/dg/smtp-connect.html
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).