

AWS SES مَادخْتَسَال SMTP مَادخْ نِيوَكْت

تَايَوْتَحْمَلَا

[قَمْدَقْمَلَا](#)

[قَسِيسَاسَالَا تَابَلَطْتَمَلَا](#)

[تَابَلَطْتَمَلَا](#)

[قَمْدَخْتَسْمَلَا تَانوَكْمَلَا](#)

[نِيوَكْتَلَا](#)

[AWS SES نِيوَكْت قَعَجَارْم](#)

[AWS SES SMTP دَامْتَعَا تَانَايَبْ عَاشِنَا](#)

[SNA Manager SMTP نِيوَكْت](#)

[AWS تَادَاهَشْ عِيْمَجْت](#)

[قَبَاچْتَسَالَا قَرَادَالْ نِيوَرْتَكَلَلَا دِيرْبَلَا عَارچَا نِيوَكْت](#)

[قَحْصَلَا نَمِ قَقْحْتَلَا](#)

[اَهْخَالِصْ اَوْ عَاطْخَالَا فَاشْكْتَسَا](#)

[قَلِصْ تَاذْتَامَوْلَعْم](#)

قَمْدَقْمَلَا

اهْمَادخْتَسَا بَوْلَطْمَلَا Secure Network Analytics Manager (SNA) نِيوَكْت قِيْفِيَكْ دَنْتَسْمَلَا اذَهْ حَضْوِي Amazon Web Services Simple Email Service (AWS SES).

قَسِيسَاسَالَا تَابَلَطْتَمَلَا

تَابَلَطْتَمَلَا

قِيْلَاتَلَا تَاعَوْضَوْمَلَا قَعْرَعْمَبْ Cisco يَصْوْت:

- سَا سَا سُوْأْ

قَمْدَخْتَسْمَلَا تَانوَكْمَلَا

قِيْلَاتَلَا قِيْدَامَلَا تَانوَكْمَلَاوَجْمَارْبَلَا تَارَادِصَالَا اذَهْ قِيْفِيْدَرَاوَلَا تَامَوْلَعْمَلَا دَنْتَسْت:

- Stealthwatch Management Console v7.3.2
- Easy DKIM عم 2022 وَيَام 25 قِيْفِيْدَوْجَوْمِ يَهْ اَمَكْ AWS SES تَامَدْخْ

قِصَاخْ قِيْلَمَعْمِ قِيْبْ قِيْفِيْدَوْجَوْمَلَا قَزَهْجَالَا نَمِ دَنْتَسْمَلَا اذَهْ قِيْفِيْدَرَاوَلَا تَامَوْلَعْمَلَا عَاشِنَا مِتْ تَنَاكْ اذَا. (يَضَارْتَفَا) حَوْسْمَمِ نِيوَكْتَبْ دَنْتَسْمَلَا اذَهْ قِيْفِيْمَدْخْتَسْمَلَا قَزَهْجَالَا عِيْمَجْ تَادَبْ رَمَا يَالْ لَمْتَحْمَلَا رِيثَاتَلَلْ كَمَهْفْ نَمِ دَكَاتْفْ، لِيغَشْتَلَا دِيْقْ كَتْكَبْشْ.

نِيوَكْتَلَا

AWS SES نِيوَكْت قَعَجَارْم

Amazon SES ×

Simple Mail Transfer Protocol (SMTP) settings

You can use an SMTP-enabled programming language, email server, or application to connect to the Amazon SES SMTP interface. You'll need the following information and a set of SMTP credentials to configure this email sending method in US East (N. Virginia).

SMTP endpoint	STARTTLS Port
email-smtp.us-east-1.amazonaws.com	25, 587 or 2587
Transport Layer Security (TLS)	TLS Wrapper Port
Required	465 or 2465

Authentication

You must have an Amazon SES SMTP user name and password to access the SMTP interface. These credentials are different from your AWS access keys and are unique to each region. To manage existing SMTP credentials, [visit the IAM console](#).

[Create SMTP credentials](#)

إشارة SMTP AWS SES دامت عا تانايب عاشن

Account Dashboard رقنا مث Amazon SES، لى لقتنا، AWS مكحت ةدحوي

Create SMTP قوف رقناو "Simple Mail Transfer Protocol (SMTP) settings" لى لفسأل ريرمتلاب مق نيوكتل اذ لامكإل ادعتسم نوكت امدنع Credentials.

دامت عا تانايبك ةئطاخ (اموي 45 يلاوح) ةمدختسمل ريغ ةميدقلا دامت عالا تانايب نأ ودبي ال ةححص ريغ.

Create رقناو ةميقق يلى لى مدختسمل مسا شيحتب مق، ديدج ةذفان اذ ي.

Create User for SMTP

This form lets you create an IAM user for SMTP authentication with Amazon SES. Enter the name of a new IAM user or accept the default and click Create to set up your SMTP credentials.

IAM User Name: ses-stealthwatch-smtp-user

Maximum 64 characters

Hide More Information

Amazon SES uses AWS Identity and Access Management (IAM) to manage SMTP credentials. The IAM user name is case sensitive and may contain only alphanumeric characters and the symbols +=, @- _

SMTP credentials consist of a username and a password. When you click the Create button below, SMTP credentials will be generated for you.

The new user will be granted the following IAM policy:

```
"Statement": [{"Effect": "Allow", "Action": "ses:SendRawEmail", "Resource": "*"}]
```

Cancel

Create

هذه ضرعتسمل بيوبت ةمالع اقبإ. اهظفح مق، دامت عالا تانايب ةحفصلا ضرعت امدنع ةحوتفم.

Create User for SMTP

✔ Your 1 User(s) have been created successfully.

This is the only time these SMTP security credentials will be available for download. Credentials for SMTP users are only available when creating the user. For your protection, you should never share your SMTP credentials with anyone.

▼ Hide User SMTP Security Credentials

 ses-stealthwatch-smtp-user

SMTP Username: AK

SMTP Password: BC

Close

Download Credentials

SMTP SNA Manager نيوكت

مسق SMTP Notifications ةحوتفم و ، SNA Manager لى لوخدلا لىجست

1. حتف Central Management > Appliance Manager.
2. زاهجلا ةمئاق Actions قوف رقنا.
3. دىجت Edit Appliance Configuration.
4. بىوبت ةمالع General ددح.
5. SMTP Configuration لى لفسأل ريرمت.
6. يذلا SMTP ةياهن ةطقن عقوم وه اذه AWS SMTP Server نم اهعيجت مت يتلا ميقل لاخدا
أو 587 أو 25 لخدأ Port ةحفص AWS SES Account Dashboard نم SMTP Settings نم هعيجت مت
AWS Verified لىع يتحتي ينورتكلل ديرب ناو نع يلى اذه نييعت نكمي From Email: 2587
يف ةريخألا ةوطخلال يف هميدقت مت يذلا SMTP مدختسم مسا وه اذه Domain User Name
يف اهميدقت مت يتلا SMTP رورم ةملك يه هذو Password: مسق Review AWS SES Configuration
تمق اذا) STARTTLS ددح Encryption Type: مسق Review AWS SES Configuration يف ةريخألا ةوطخلال
SMTPS، مقف دىجتب (2465 أو 465 لى ذفنملا ريرحتب مقف، SMTPS دىجتب
7. Central Management يف ةيالو UP لى ةدوعلل SNA Manager راطت ناو اتاداعللا قىببطت.

Appliance Configuration - SMC

/ Last Updated: 05/27/2022 10:06 AM by admin

Appliance

Network Services

General

SMTP Configuration ⓘ

SMTP SERVER *

email-smtp.us-east-1.amazonaws.com

PORT

587

FROM EMAIL *

email@something.com

USER NAME

AK

PASSWORD *

ENCRYPTION TYPE

SMTPS STARTTLS UN-ENCRYPTED

AWS تاداهش عي مجت

ي رذج مدخت سمك لوخدلاو، SNA Manager ىلى SSH ةسلج عاشنإ

ةثالثل رصانعلا هذ ةعج ارم

- ل اثملا لى بس ىلع (SMTP ةياهن ةطقن عقوم ري ي غت email-smtp.us-east-1.amazonaws.com)
 - ل STARTTLS ل 587 نم ري صقت ال ثم) لمعت سي اني مالا ري غ
 - لامتك ال دن ع ةبلاطملا عاجرا متي، STDOUT اهل سيل رماوالا
- ل STARTTLS (587 ي ضارثفالا ذفنملا):

```
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 -tl
*.pem`; do cp $i $(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF}' $i).pem ; done ; rm -f cacert*
mycertfile.crt
```

ل SMTPS (465 ي ضارثفالا ذفنملا) ةبسنلاب

```
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 -tl *.pem`; do cp $i
$(awk -F "CN=" '/s:/ {gsub(/ /,x ); print $NF} ' $i).pem ; done ; rm -f cacert* mycertfile.crt
```

ليلدلا اذه نم ذخأت ال ،يالحال لمعلال ليلدي في PEM قحلم تاذا تاداهش للافلم عاشن ا متي
(ريخأل رطس ل / PWD رمأ نم جارخا)

```
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 -tl *.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 كيديدل يلحلمل زاوجل ال ال SNA Manager لعل اهؤاشن ا متي تلافلمل ليزنتب مق
ال ا تاداهش لاهذه ةفاضو ،(ك لذل امو ، WinSCP ، Filezilla) هراتخت يذلا تلافلمل لقن جم انرب
Central Management في SNA Manager trust store

1. حتف Central Management > Appliance Manager.
2. زاوجل ةمئاق Actions قوف رقنا .
3. ديدحت Edit Appliance Configuration.
4. بيبوت ةمالع General ددح .
5. Trust Store للافلسأل ريرمت .
6. ديدحت Add New
7. Friendly Name ك فلفلمل مسا مادختساب ي صوم ، ةداهش لك ليلمحتب مق .

ةباجتسالال ةرادال ي نورتكللال ديربال اراج نيوكت

مسق Response Management لاحتفيو ، SNA Manager للافلمل ليلوخلال ليجست

1. ةشاشلال نم يولعل اعزلال لوط لعل يسيسيرللا طيرشلال في بيبوت ةمالع Configure ددح .
2. ديدحت Response Management
3. بيبوت ةمالع Actions ديدحت ، ةحفص Response Management عقوم نم .
4. ديدحت Add New Action
5. ي نورتكللال ديربال ناو نع لخدأ اذه ي نورتكللال ديربال اراجل مسا ريفوت Email ديدحت .
نم ققحتلال مت يذلا لاجملا ال ا يمتني نأ بجي اذه نأ طحال) "ال" لقلال في ملتسملل
ةجاج ي نوكي نكمم عوضومل (AWS SES في

Response Management

Rules Actions Syslog Formats

Email Action

Cancel Save

Name

AWS SES Test

Description

Enabled Disabled actions are not performed for any associated rules.

To

email@something.com

Subject

AWS SES SMTP Test

Body

+ Alarm Variables

Preview

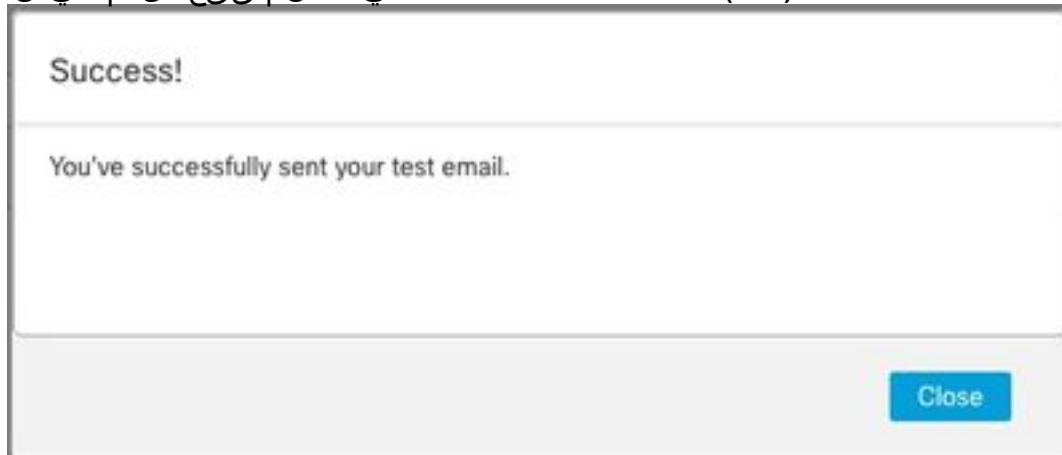
Test Action

6. Save رقنا.

ةحصلا نم ققحتلا

مسقلا Response Management لاحت فيو، SNA Manager لى لوخدلا ليجست

1. ةشاشلا نم يولعل اعزلال لوط لىع يسئيرلا طيرشلا في بيوبت ةمالع Configure دح.
2. Response Management ديدحت.
3. بيوبت ةمالع Actions ديدحت، ةحفص Response Management عقوم نم.
4. نينوكتب تمق يذلا ينورتكللال ديربلا ءارجا فصل دومع Actions في صقانلا عطقلا دح. Edit دحو، عطقم Configure Response Management Email Action في.
5. ديرب ميلست متي و حاجن ةلاس رر م يدقت متي، احيحص نينورتكللا ناك اذو Test Action ديدحت لىنورتكللا لاجملا عم، ناهذالو، لاجملا "Received" في نوزامال ضرع متي، ينورتكللال ديربلا سار في لاجملا ARC-Authentication-Results (AAR) Chain في هنم ققحتلا مت يذلا



```
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@something.com header.s=
dkim=pass header.i=@amazon.es.com header.
spf=pass (google.com: domain of 01000181
sender) smtp.mailfrom=0100018106685484-fa246764-
Return-Path: <0100018106685484-fa246764-b234-4a
Received: from a8-30.smtp-out.amazon.es.com (a8-
```

6. فاشكتسأ مسق ىلإ عبات - ةشاشلا ىلعأ ي ف راعش مي دقت متي ، رابتخالأ حجني مل إذا .
اهحالصإو ءاطخالأ

اهحالصإو ءاطخالأ فاشكتسا

ةصاخلا أطلخال لئاسر ىلع فلملا يوتحي `/lancope/var/logs/containers/sw-reponse-mgmt.log` رمأل ضرعي
لودجلا ي ف جردم حالصإو ، اعويش رثكالأ أطلخال . رابتخالأ تاءارجإب
ءاطخالأ لجس رطس نم عزج درجم يه لودجلا ي ف ةجردملا أطلخال لئاسر نأ طخال

أطلخال

SMTPSendFailedException: مل :ةلاسر 554 ضفر مت
ي.نورتكلإلإ ديربلا ناو نع ةحص نم ققحتلا متي
US-ةقطنملا نم ققحتلا ي ف تايوهلا تلشف
EAST-1: {email_address}

AuthenticationFailedException: دامتعا تانايب
ةحلصا ريغ 535 ةقداصملا

SunCertPathBuilderException: راسم ىلع روثعلا رذعت
بولطملا فدهلل حلصا ةداهش

ادج ريغص حاتفم `SSL:tls_process_ske_dhe:dh` جهن

رخأ أطلخي

حالصإ

وكت ي ف "ي نورتكلإلإ ديربلا نم" شي دحتب مق
ممتني ي نورتكلإلإ ديرب ىلإ SNA Manager SMTP
AWS SES نم ققحتلا مت يذلا لاجملا

AWS SES دامتعا تانايب ءاشنإ ماسقأل راركت
SNA Manager SMTP ني وكت ني وكتو SMTP

و AWS نم ةمدقملا تاداهشلا عيمج نأ نم دكأت
تلا ءارجإب مق - SNA ةرادإب قوئوملا نزخملا ي ف
تاداهشلا ةنراقم متي و رابتخالأ ءارجإ دنع مزحلا
ملا تايوتحمب ةقثلل مداخل بناج نم ةمدقملا

ةفاضال رظنا

ةعجارملا ةينفلا ةدعاسملا زكرم ةلاح حتف

ادج ريغص DH حاتفم :ةفاضا

تارفش مادختسا دنع تب 1024 حيتافم نومدختسي مهنأ شيح ، AWS ل ةيبناج ةلكشم هذه
ضرعت SSL. ةسلج ةعباتم SNA ري دم ضفريو (logAm لىل لوصولا ةيناكمإ تاذ) EDH و DHE
DHE/EDH ةرفش مادختسا دنع OpenSSL لاصتا نم مداخل ةقراخ ةجرد حيتافم رمأل تارجم

```
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
```

مدختسملا موق ي شيح رمأل مادختساب EDH و DHE تارفش عيمج ةلازا وه حاتملا ديحولال
ل. لاصتال حجنيو ECDHE ةرفش ةوعومج دي دحتب AWS موقيو ، SMC ىلع يردجلا


```
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
```

ةلص تاذا تامولعم

- <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>
- [تادنتس مل او ينقت لا م عدلا - Cisco Systems](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق م ق د ن و ك ت ن ل ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م م چ ر م . ة ص ا خ ل م ه ت غ ل ب
Cisco مچرت م ا م د ق م م ي ت ل ا ة م ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا م ا د ا د ع و چ ر ل ا ب م ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت م ل و ئ س م
Systems (ر ف و ت م ط ب ا ر ل ا) م ل ص ا ل ا م ي ز م ل چ ن ا ل ا دن ت س م ل ا