

AWS SESを使用するためのSMTPサーバの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[AWS SES設定のレビュー](#)

[Aws SES SMTP認証情報の作成](#)

[SNAマネージャSMTP設定の設定](#)

[AWS証明書の収集](#)

[応答管理の電子メールアクションの構成](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Secure Network Analytics Manager (SNA)を使用する Amazon Web Services Simple Email Service (AWS SES)。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AWS SES

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Stealthwatch Management Console v7.3.2
- AWS SESサービスは2022年5月25日に提供され、Easy DKIM

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

AWS SES設定のレビュー

AWSから3ビットの情報が必要です。

1. AWS SESロケーション
2. SMTPユーザ名
3. SMTPパスワード

注：サンドボックスにあるAWS SESは許容されますが、サンドボックス環境の制限に注意してください。<https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html>

AWSコンソールで、Amazon SESを選択し、Configuration をクリックし、 Verified Identities.

確認済みのドメインが必要です。確認された電子メールアドレスは必要ありません。AWSのドキュメント<https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure>

The screenshot shows the Amazon SES console interface. On the left is a navigation menu with 'Configuration' expanded and 'Verified Identities' selected. The main content area is titled 'Verified identities' and includes a description: 'A verified identity is a domain, subdomain, or email address you use to send email through Amazon SES. Learn more'. Below this is a section for 'Identities (2)' with buttons for 'Send test email', 'Delete', and 'Create Identity'. A search bar is present with the placeholder text 'Search all domain and email address identities'. A table lists two identities:

<input type="checkbox"/>	Identity	Identity type	Status
<input type="checkbox"/>	email@something.com	Email address	Verified
<input type="checkbox"/>	something.com	Domain	Verified

SMTPエンドポイントの場所をメモします。この値は後で必要になります。

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
<input type="text" value="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](#).

Aws SES SMTP認証情報の作成

AWSコンソールで、Amazon SESをクリックし、Account Dashboard.

下にスクロールして「Simple Mail Transfer Protocol (SMTP) settings」をクリックし、Create SMTP Credentials この設定を完了する準備ができたなら、

古い未使用のクレデンシャル (約45日) では、無効なクレデンシャルとしてエラーが発生しないようです。

この新しいウィンドウで、ユーザ名を任意の値に更新し、Create.

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:
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


ページにクレデンシャルが表示されたら、保存します。このブラウザタブは開いたままにしておきます。

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

SNAマネージャSMTP設定の設定

Cisco Unified Communications Managerにログインし、SNA Manager、およびopen SMTP Notifications セクションの「EULA not accepted」を確認します。

1. 開く Central Management > Appliance Manager.
2. ポリシーの横の [レポート (Report)] Actions アプライアンスのメニュー。
3. 選択 Edit Appliance Configuration.
4. 次のいずれかを選択します。 General tab.
5. 下にスクロールして SMTP Configuration
6. AWSから収集した値を入力します SMTP Server:これはSMTPエンドポイントの場所で、SMTP Settings AWS SES Account Dashboard pagePort:25、587、または2587と入力します。From Email:このフィールドには、IPアドレスを含む AWS Verified DomainUser Name:これは、Review AWS SES Configuration セクションの「EULA not accepted」を確認します。Password:これは、Review AWS SES Configuration セクションの「EULA not accepted」を確認します。Encryption Type:[STARTTLS]を選択します ([SMTPS]を選択した場合は、ポートを465または2465に編集します) 。
7. 設定を適用し、SNA Manager ネットワークに戻る UP 状態 Central Management

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証明書の収集

SSHセッションを確立し、SNA Managerルートユーザとしてログインします。

次の3つの項目を確認します

- SMTPエンドポイントの場所を変更します(email-smtp.us-east-1.amazonaws.comなど)。
- 使用するポートを変更します(たとえば、STARTTLSのデフォルトは587)。
- コマンドにはSTDOUTが含まれず、完了時にプロンプトが返されます

STARTTLS (デフォルトポート587) の場合 :

```
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
```

SMTPS (デフォルトポート465) の場合 :

```
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
```

pem拡張子が付いた証明書ファイルは、このディレクトリではなく、現在の作業ディレクトリに作成されます (pwdコマンドの出力/最終行)

```
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
```

Cisco IOSソフトウェアリリース12.1Tで作成された **SNA Manager** 選択したファイル転送プログラム (Filezilla、winscpなど) を使用してローカルマシンにアクセスし、これらの証明書を **SNA Manager trust store** イン **Central Management**.

1. 開く **Central Management > Appliance Manager**.
2. ポリシーの横の [レポート (Report)] **Actions** アプライアンスのメニュー。
3. 選択 **Edit Appliance Configuration**.
4. 次のいずれかを選択します。 **General tab**.
5. 下にスクロールして **Trust Store**
6. 選択 **Add New**
7. それぞれの証明書をアップロードします。ファイル名を **Friendly Name**

応答管理の電子メールアクションの構成

Cisco Unified Communications Managerにログインし、 **SNA Manager**をクリックし、 **Response Management** セクションの「EULA not accepted」を確認します。

1. 次のいずれかを選択します。 **Configure** 画面上部のメインリボンのタブ
2. 選択 **Response Management**
3. **Response Management** ページ、選択 **Actions tab**
4. 選択 **Add New Action**
5. 選択 **Email**この電子メールアクションの名前を指定します受信者のメールアドレスを[To]フィールドに入力します (AWS SESで確認されたドメインに属している必要があります)。件名は何でもかまいません。

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:

Subject:

Body:

+ Alarm Variables Preview

Test Action

6. クリック Save

確認

Cisco Unified Communications Managerにログインし、 SNA Managerをクリックし、 Response Management セクション :

1. 次のいずれかを選択します。 Configure 画面上部のメインリボンのタブ
2. 選択 Response Management
3. Response Management ページ、選択 Actions tab
4. 省略記号を Actions で設定した電子メールアクションの行の列 Configure Response Management Email Action を選択し、 Edit.
5. 選択 Test Action 設定が有効であれば、成功メッセージが表示され、電子メールが配信されます。
電子メールヘッダーの中で、 amazonsesは" Received」 フィールドとamazonsesに加え、 ARC-Authentication-Results (AAR) Chain

Success!

You've successfully sent your test email.

Close

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

6. テストに失敗した場合は、画面上部にバナーが表示されます。トラブルシューティングセクションに進みます

トラブルシューティング

「/lancope/var/logs/containers/sw-reponse-mgmt.log」ファイルには、テストアクションのエラーメッセージが含まれています。最も一般的なエラーと修正を表に示します。表に示されているエラーメッセージは、エラーログ行の一部に過ぎないことに注意してください

エラー

SMTPSendFailedException:554 Message rejected:メールアドレスが確認されていません。IDがリージョンUS-EAST-1のチェックに失敗しました。
{email_address}

AuthenticationFailedException:535認証資格情報が無効です

SunCertPathBuilderException:要求されたターゲットへの有効な証明パスが見つかりません

SSLルーチン : tls_process_ske_dhe:dhキーが小さすぎます

その他のエラー

修正

SNA ManagerSMTP設定の「From Email」をAWS SES検証済みドメインに属する電子メールに更新する

セクション「AWS SES SMTP認証情報の作成」SNA Manager SMTP設定の設定」を繰り返します

AWSから提示されたすべての証明書がSNA Manager信頼ストアにあることを確認します。アクションの実行時にパケットキャプチャを実行して、サーバ側から提示された証明書を信頼ストアの内容と比較します。

別紙を参照

TACケースを開いて確認する

付録:DHキーが小さすぎます。

これはAWS側の問題です。DHEとEDHの暗号を使用する場合（ログが詰まる可能性がある）、1024ビットキーを使用し、SNAマネージャがSSLセッションの続行を拒否します。コマンド出力には、DHE/EDH暗号が使用されている場合のopenssl接続からのサーバの一時キーが表示されます。

```
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
```


唯一の回避策は、SMCでrootユーザとしてコマンドを使用してすべてのDHEおよびEDH暗号を削除することです。AWSはECDHE暗号スイートを選択し、接続が成功します。

```
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
```

関連情報

- <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>
- [テクニカル サポートとドキュメント - Cisco Systems](#)