Configura server SMTP per l'utilizzo di AWS SES

Sommario

Introduzione

Questo documento descrive come configurare **Secure Network Analytics Manager** (SNA) da utilizzare **Amazon Web Services Simple Email Service** (AWS-SES).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AWS-SES

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- **Stealthwatch Management Console v7.3.2**
- Servizi AWS SES esistenti al 25 MAGGIO 2022 con **Easy DKIM**

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Verifica configurazione AWS SES

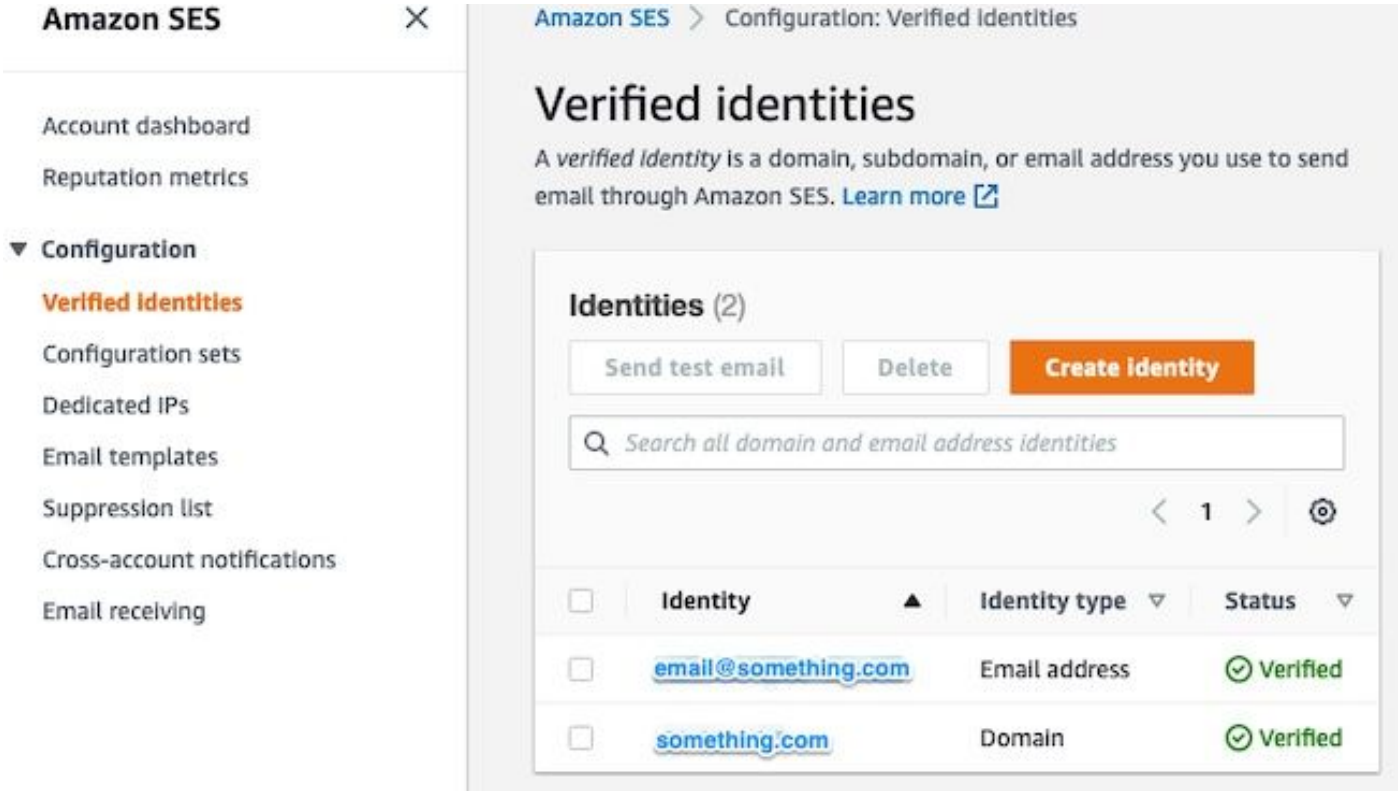
Sono richiesti tre bit di informazioni da AWS:

1. Percorso AWS-SES
2. Nome utente SMTP
3. Password SMTP

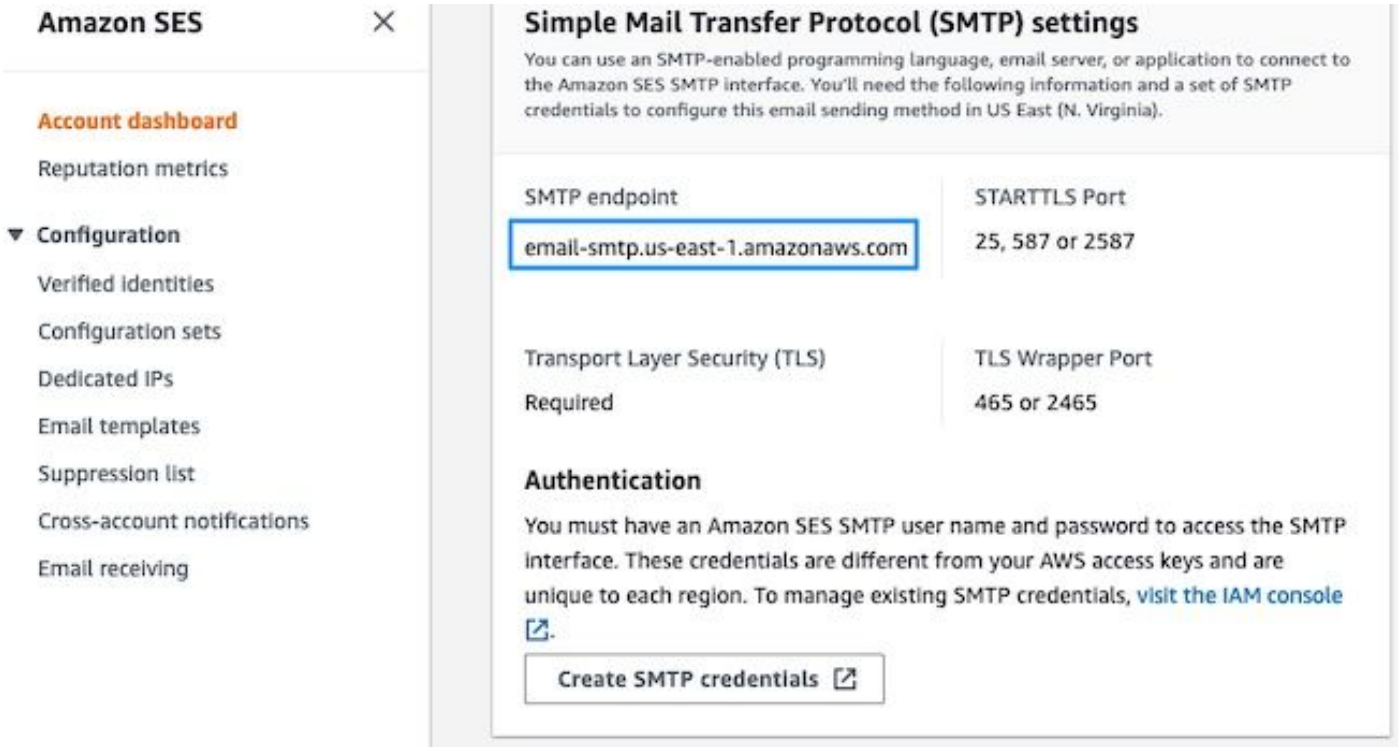
> **Nota:** AWS SES, situato nella sandbox, è accettabile, ma è necessario essere consapevoli delle limitazioni per gli ambienti sandbox: https://docs.aws.amazon.com/ses/latest/dg/request-production-access.html

Nella console AWS, passare a **Amazon SES**, quindi selezionare **Configuration** e fare clic su **Verified Identities**.

Ènecessario disporre di un dominio verificato. Non è necessario un indirizzo di posta elettronica verificato. Fare riferimento alla documentazione di AWS https://docs.aws.amazon.com/ses/latest/dg/creating-identities.html#verify-domain-procedure



Annotare il percorso dell'endpoint SMTP. Questo valore è necessario in seguito.



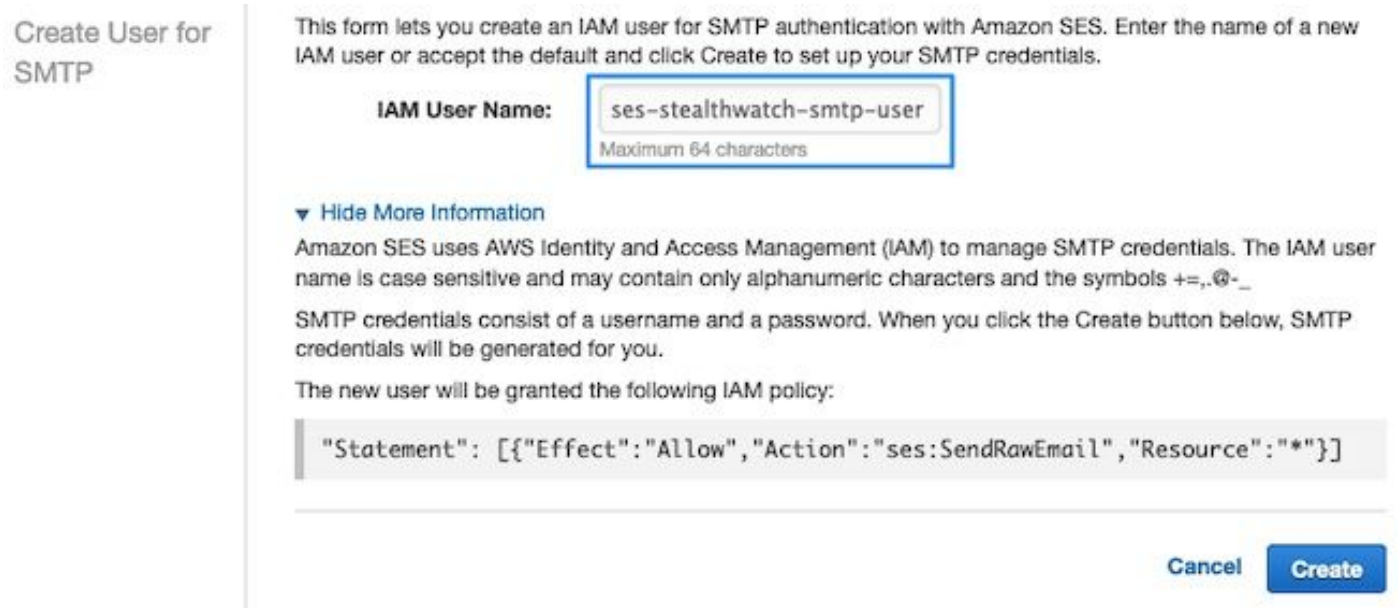
Crea credenziali SMTP AWS SES

Nella console AWS, passare a **Amazon SES**, quindi fare clic su **Account Dashboard**.

Scorrere verso il basso fino a visualizzare "**Simple Mail Transfer Protocol (SMTP) settings**" e fare clic su **Create SMTP Credentials** per completare la configurazione.

Le credenziali non utilizzate meno recenti (circa 45 giorni) non sembrano essere errate in quanto non valide.

In questa nuova finestra, aggiornare il nome utente a qualsiasi valore e fare clic su **Create**.

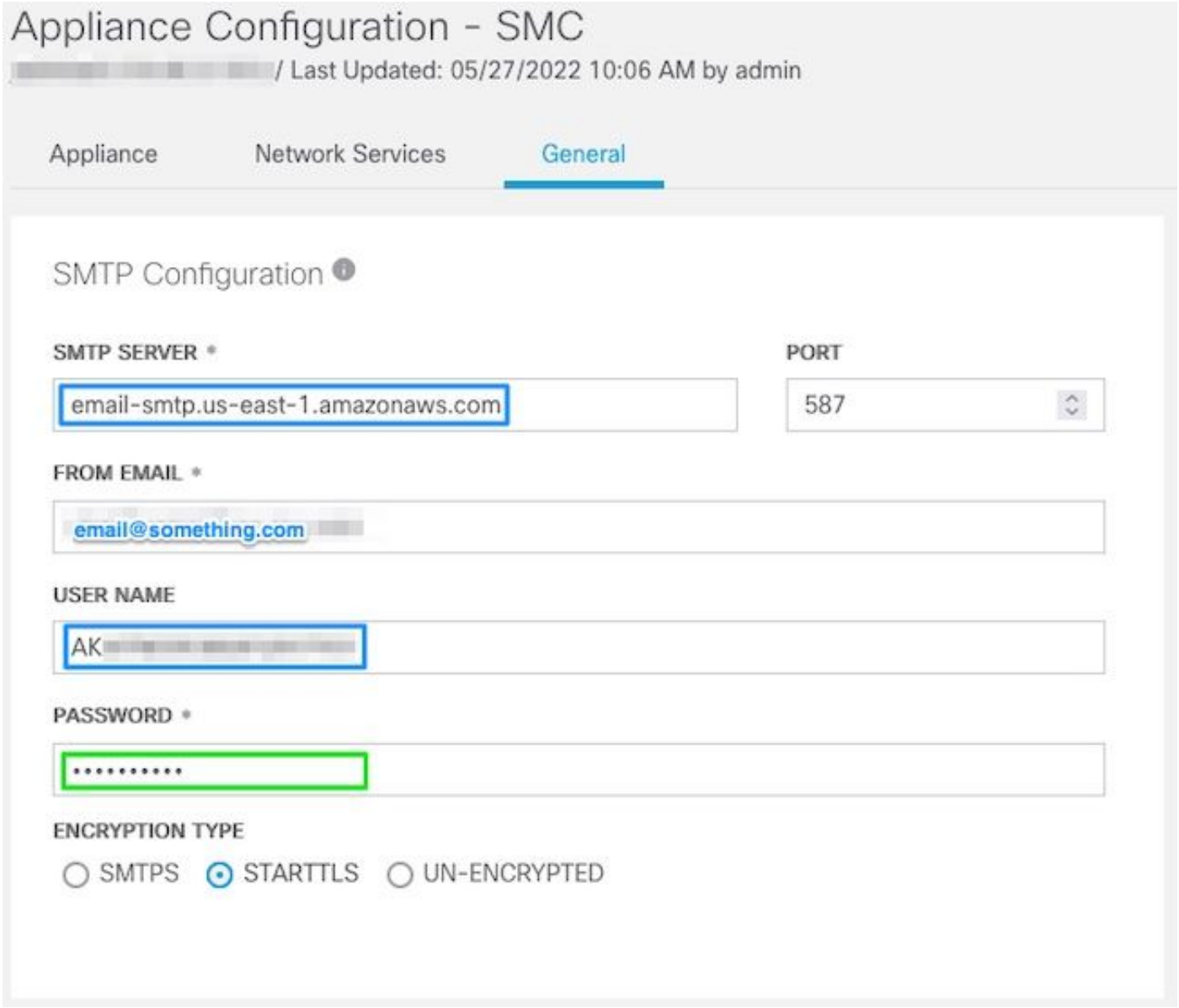


Quando la pagina presenta le credenziali, salvarle. Tieni aperta la scheda del browser.

Configurazione della configurazione SMTP di SNA Manager

Accedi a **SNA Manager**e aperto **SMTP Notifications** sezione

1. Open (Aperto) **Central Management > Appliance Manager**.
2. Fare clic sul pulsante **Actions** per l'accessorio.
3. Seleziona **Edit Appliance Configuration**.
4. Selezionare il **General** .
5. Scorri verso il basso fino a **SMTP Configuration**
6. Immettere i valori raccolti da AWS **SMTP Server**: Percorso dell'endpoint SMTP raccolto dal **SMTP Settings** dal **AWS SES Account Dashboard** pagina**Port**: Immettere 25, 587 o 2587**From Email**: Può essere impostato su qualsiasi indirizzo di posta elettronica contenente **AWS Verified DomainUser Name**: Si tratta del nome utente SMTP visualizzato nell'ultimo passaggio della **Review AWS SES Configuration** sezione**Password**: Si tratta della password SMTP presentata nell'ultimo passaggio della **Review AWS SES Configuration** sezione**Encryption Type**: Selezionare STARTLS (se si seleziona SMTPS, modificare la porta su 465 o 2465)
7. Applicare le impostazioni e attendere **SNA Manager** per tornare a un **UP** stato in **Central Management**



Raccolta certificati AWS

Stabilire una sessione SSH per **SNA Manager**e accedere come utente root.

Rivedi questi tre elementi

- Modificare la posizione dell'endpoint SMTP (ad esempio email-smtp.us-east-1.amazonaws.com)
- Modificare la porta utilizzata (ad esempio, impostare 587 per STARTTLS)
- I comandi non hanno STDOUT, il prompt viene restituito al completamento

Per STARTTLS (porta predefinita 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
```

Per SMTPS (porta predefinita 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
```

I file di certificato con estensione pem vengono creati nella directory di lavoro corrente, non accettare questa directory (output da comando pwd / ultima riga)

```
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
```

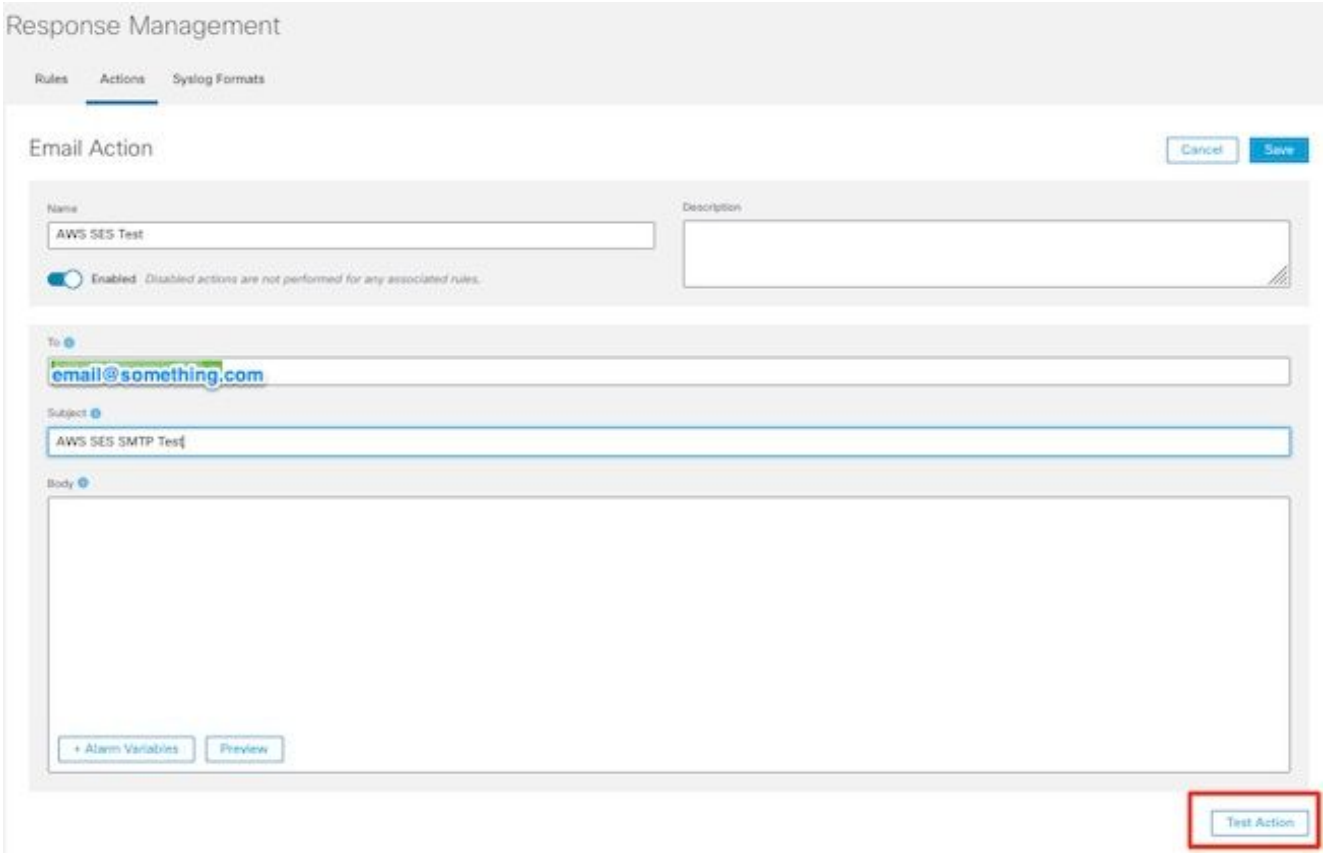
Scarica i file creati in **SNA Manager** sul computer locale con il programma di trasferimento file desiderato (Filezilla, winscp, ecc.) e aggiungere questi certificati al **SNA Manager trust store** in **Central Management**.

1. Open (Aperto) **Central Management > Appliance Manager**.
2. Fare clic sul pulsante **Actions** per l'accessorio.
3. Seleziona **Edit Appliance Configuration**.
4. Selezionare il **General** .
5. Scorri verso il basso fino a **Trust Store**
6. Seleziona **Add New**
7. Caricare ogni certificato, si consiglia di utilizzare il nome file come **Friendly Name**

Configura azione e-mail di Response Management

Accedi a **SNA Manager**e aprire la **Response Management** sezione

1. Selezionare il **Configure** sulla barra multifunzione principale nella parte superiore dello schermo
2. Seleziona **Response Management**
3. Dal **Response Management** selezionare **Actions** scheda
4. Seleziona **Add New Action**
5. Seleziona **Email**Specificare un nome per l'azione di posta elettronicaImmettere l'indirizzo e-mail del destinatario nel campo "A" (notare che deve appartenere al dominio verificato in AWS SES)Il soggetto può essere qualsiasi cosa.

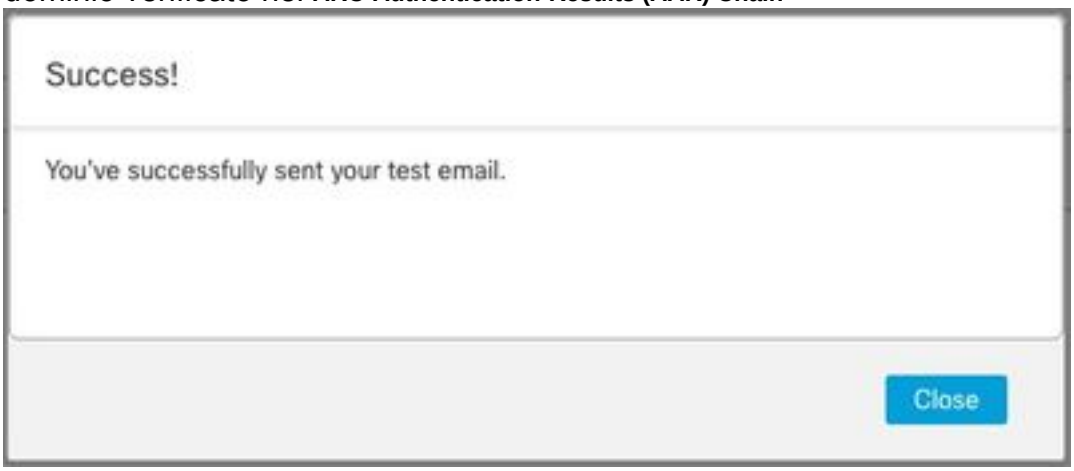


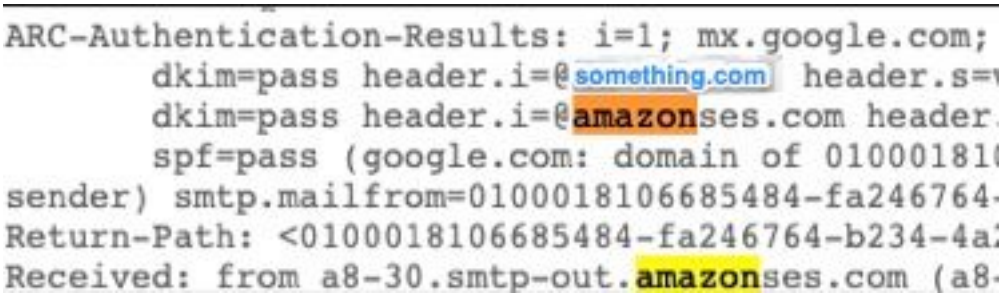
6. Clic **Save**

Verifica

Accedi a **SNA Manager**e aprire la **Response Management** sezione:

1. Selezionare il **Configure** sulla barra multifunzione principale nella parte superiore dello schermo
2. Seleziona **Response Management**
3. Dal **Response Management** selezionare **Actions** scheda
4. Selezionare i puntini di sospensione nella **Actions** per la riga dell'azione e-mail configurata nel **Configure Response Management Email Action** e selezionare **Edit**.
5. Seleziona **Test Action** e se la configurazione è valida, viene visualizzato un messaggio di operazione riuscita e viene recapitata un'e-mail.
   Nell'intestazione email amazonses è mostrato nella " **Received**" e amazonses, insieme al dominio verificato nel **ARC-Authentication-Results (AAR) Chain**





6. Se il test ha avuto esito negativo, nella parte superiore dello schermo viene visualizzato un banner - passare alla sezione Risoluzione dei problemi

Risoluzione dei problemi

OSPF (Open Shortest Path First) **/lancope/var/logs/containers/sw-reponse-mgmt.log** contiene i messaggi di errore per le azioni di test. L'errore più comune e la correzione viene elencata nella tabella.
I messaggi di errore elencati nella tabella sono solo una parte della riga del log degli errori

Errore	Fix
SMTPSendFailedException: 554 Messaggio rifiutato: Indirizzo di posta elettronica non verificato. Identità non sottoposte a controllo nella regione US-EAST-1: {indirizzo_posta_elettronica}	Aggiornare "From Email" (Da e-mail) nella configurazione SMTP di SNA Manager su un messaggio di posta elettronica appartenente al dominio verificato di AWS SES
EccezioneAutenticazioneNonRiuscita: Credenziali di autenticazione 535 non valide	Ripetere le sezioni Creare credenziali SMTP AWS SES e configurare la configurazione SMTP di SN Manager
Eccezione SunCertPathBuilder: impossibile trovare un percorso di certificazione valido per la destinazione richiesta	Confermare che tutti i certificati AWS presentati s trovino nell'archivio attendibile di SNA Manager - eseguire l'acquisizione dei pacchetti quando vien eseguita l'**azione di test** e confrontare i certificati presentati sul lato server con il contenuto dell'arc attendibile
routine SSL:tls_process_ske_dhe:chiave dh troppo piccola	Cfr. addendum
Qualsiasi altro errore	Apri richiesta TAC per revisione

Appendice: Chiave DH troppo piccola.

Questo è un problema del lato AWS, in quanto usano chiavi a 1024 bit quando si usano cifrari DHE ed EDH (suscettibili logjam) e SNA Manager rifiuta di continuare la sessione SSL. Il risultato del comando mostra i tasti temp del server dalla connessione openssl quando vengono utilizzati i cifrari 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
```

L'unica soluzione disponibile è rimuovere tutte le cifrature DHE ed EDH con il comando come utente root su SMC, AWS seleziona una suite di cifratura ECDHE e la connessione riesce.

```
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
```

Informazioni correlate

- 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
- Documentazione e supporto tecnico – Cisco Systems