

# نم ینورت کلالا دیربلا لئاسر ةجلاعم ةیفیک

## CTR

### تایوت حمل

ةمدقملا

ةیساسا تامولعم

ةمدختسملا تانوکملا

نیوکتلا

ققحتلا

قیقحتلا و ةرفوتملا مداوخللا ىلا لوصوللا ىلا اذانتسا CTR ةباوب ىلا لوصوللا 1. ةوطخللا ایدیتهت لكشت وأ ةراضهنا و دبى یتلا و اهمیلست مت یتلا لئاسرلا نم ققحت 2. ةوطخللا حضورم وه امك ةیلالاتلا رییاعملاب تاقحلملا نع شحبلانكمی. ةم و عدمل تاقحلملا مادختساب ةروصللا ىف:

ىف نیبم وه امك، ىلی امیف قیقحتلا و ةیلودلا ةطرشلا قیقحت ىلع لاثم 1-2 روصوللا:

ةروصللا ىف حضورم وه امك، ةلاسرلا حالصا لبق دراوولا ةبلع ىف هیلع لصحت ام اذه 2.2

تاءارجالا" نم ىأ ةمئاقلا تارایخ نم ددح، "Cisco ةلاسرفرعم" قوف رقنلا دنع 2.3 ةروصللا ىف حضورم وه امك، "ةم و عدمل ةیجالعلا

نكرلا ىف ةحجان ةقتببم ةذفان رهظتو "ةردابم مېدقت" دېدحت متی، لاثملا اذه ىف 2.4 ةروصللا ىف حضورم وه امك، نم ىالا ىلفسلا

نأ رهظت یتلا "mail log" تحت ةیلالاتلا تالچسلا ىلع عالطالا كنكمی، ESA ىف 2.5 ةیئاهنلا ةلاحلا و، ددجمل اءارجالا و، أدبى "CTR" حالصا

ىف نیبم وه امك، ةلاسرلا عوضوم ىف "اهحیصت مت یتلا ةلاسرلا" ةرابعلا درت 2-6 ةروصللا:

ىذلا ناوونعلا وه ESA/SMA ةدحو نیوکت دنع هبتكت ىذلا ینورت کلالا دیربلا ناوونع 2.7 وأ "هچوت ةداعا" رایخلا دېدحت دنع اهحالصا مت یتلا ینورت کلالا دیربلا لئاسر لبققتسى ةروصللا ىف حضورم وه امك، "فدح/هچوت ةداعا"

ESA/SMA نیب ةدېدجلا ةهجالل لئاسرلا بقرعت لیصافت ىلا ترظن اذا، ارىخأ 2.8 اهنأ ىلع "Last State" و "mail log" ىف اهیلع لوصوللا مت یتلا تالچسلا سفن ىرت نأ كنكمی ةروصللا ىف حضورم وه امك، "Remediated"

### ةمدقملا

تادیدهت لل ةباجتسالالا نم ینورت کلالا دیربلا لئاسر حالصا ةیفیک دنتسملا اذه حضورى Cisco (CTR) نم

### ةیساسا تامولعم

لائاسر نع شحبللا لوؤسملل كنكمی. OnDemand دیرب ةجلاعم معدل CTR قیقحت شېدحت مت لالخنم اهحالصا و OnPrem Exchange و O365 مدختسم دیرب بلع نم ةنیعم ینورت کلالا دیرب (SMA) نامألا ةرادا زاهج و (ESA) ینورت کلالا دیربلا نامأ زاهج

### ةمدختسملا تانوکملا

ةيلال ةيداملا تانوكمل او جماربل تارادصا اىل دنن سمل اذه يف ةدراولا تامولعمل دنن ستم:

- باسح CTR
- نم نامالا تامدخ لدابت Cisco
- ESA ASYCNos 14.0.1-033

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنن سمل اذه يف ةدراولا تامولعمل عاشن اتم تناك اذى. (يضا رتفا) حوسمم نيوكتب دنن سمل اذه يف ةمدختسمل ةزهجال عيمج تادب رما اىل لمحتمل ريثا تلل كمهف نم دكأتف، ليغشتلا دي قكتك بش

0365 ماطنل ةطلتخملا رشنلا تايلمع يف ديربل او شحبال لكاشم لج معدم تي: **ةظحالم** Exchange 2013 PreM ليغشتلا ماطن اىل Exchange رشنلا تايلمعو 2019 و Exchange 2016 و طقف.

## نيوكتلا

1. [ESA يف باسحلا تاداعا نيوكت](#)
2. [فيرعت فلم اىل \(تالاجملا\) لاجملا نيغيتو لسل ستملا فيرعتلا فلم نيوكت باسحلا](#)
3. [SMA و ESA عم CTR جمدم](#)

## ققحتلا

مادختساب حالصالل ةلاسرلا ديحتو CTR ةبابو يف تاظالملا يف قيقحتلا كنكمي ةيلال تاوطلخال:

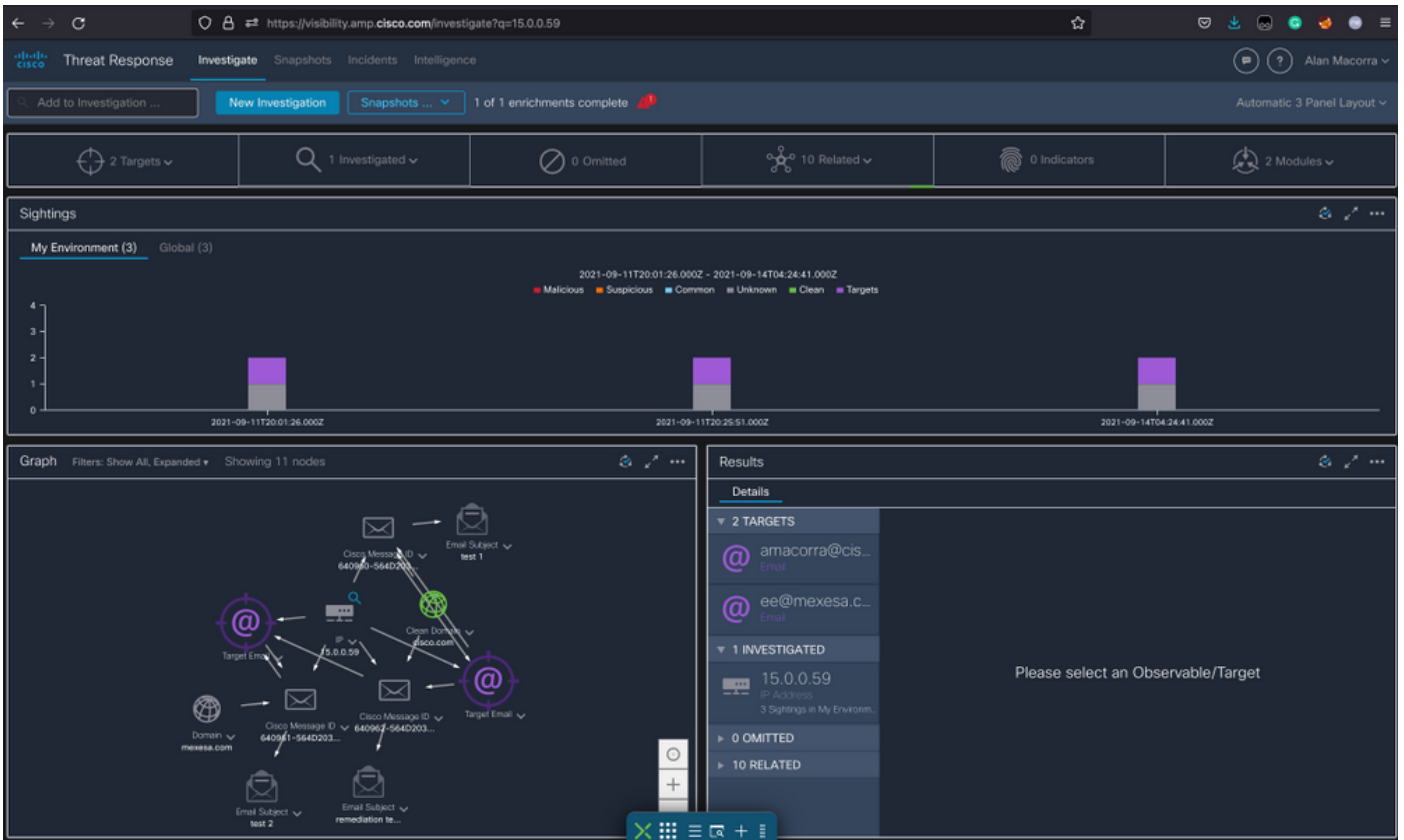
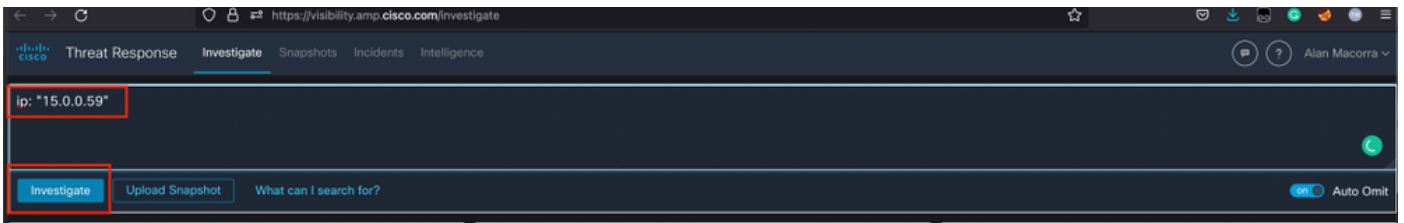
## ةرفوتملا مداوخل اىل لوصول اىل ادانتسا CTR ةبابو اىل لوصول 1. ةوطخلال قيقحتلا

- ةدحتملا تاىالول <https://visibility.amp.cisco.com/investigate>
- زكرملا <https://visibility.apjc.amp.cisco.com/investigate> راوجلل [يقيرفأل](#) زكرملا
- بيوروال داخالا <https://visibility.eu.amp.cisco.com/investigate>

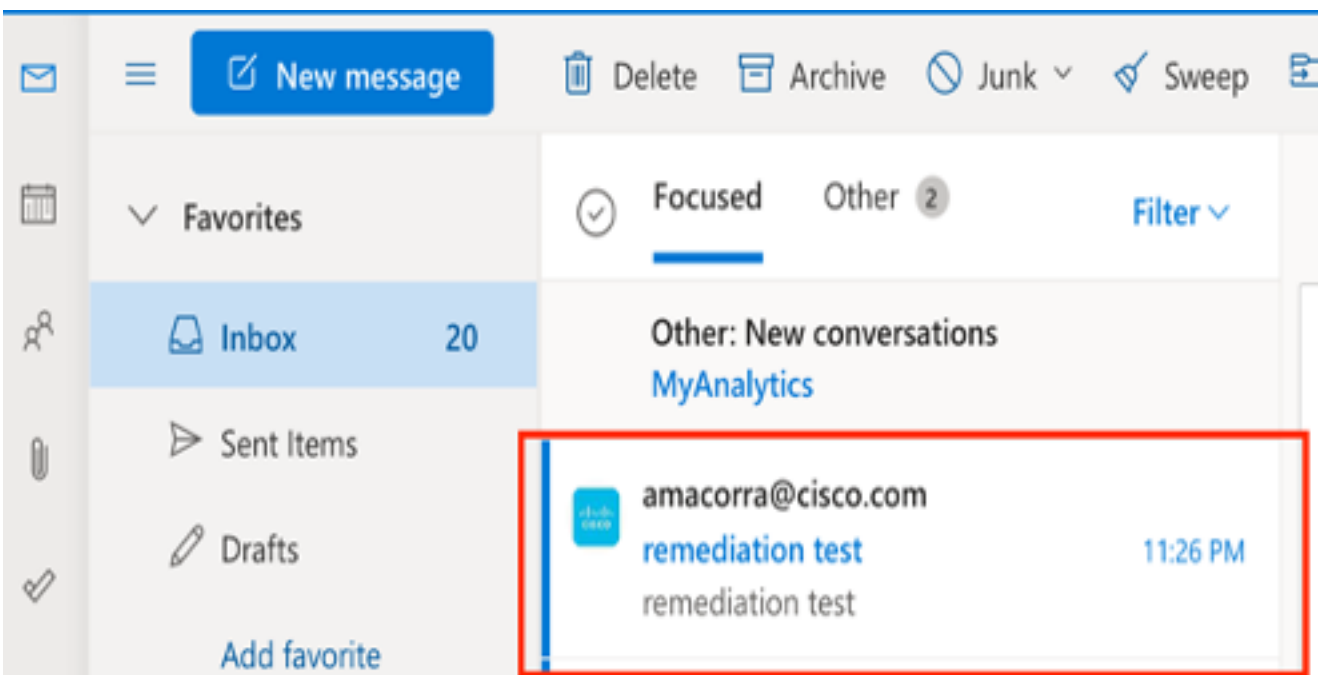
أو ةراض اهانأ وديي يتلا واهم ليست مت يتلا لئاسرلا نم ققحت 2. ةوطخلال تاوطلخال نع شحبال كنكمي. ةمومدملا تاوطلخال مادختساب اديدهت لكشت ةروصلال يف حضورم وه امك ةيلال ريعمباب

IP address	ip:"4.2.2.2"	Email subject	email_subject:"Invoice Due"
Domain	domain:"cisco.com"	Cisco Message ID (MID)	cisco_mid:"12345"
Sender email address	email:"noreply@cisco.com"	SHA256 filehash	sha256:"sha256filehash"
Email message header	email_messageid:"123-abc-456@cisco.com"	Email attachment file name	file_name:"invoice.pdf"

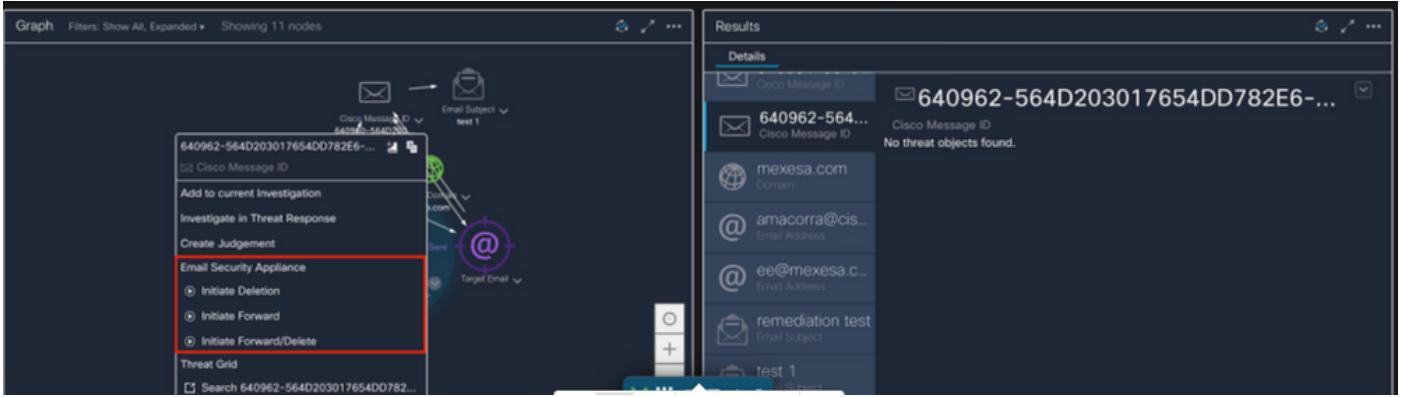
روصلال يف ني بم وه امك، يلي امي قيقحتلا وةلودلا ةطرشلا قيقحت اىل لاثم 2-1:



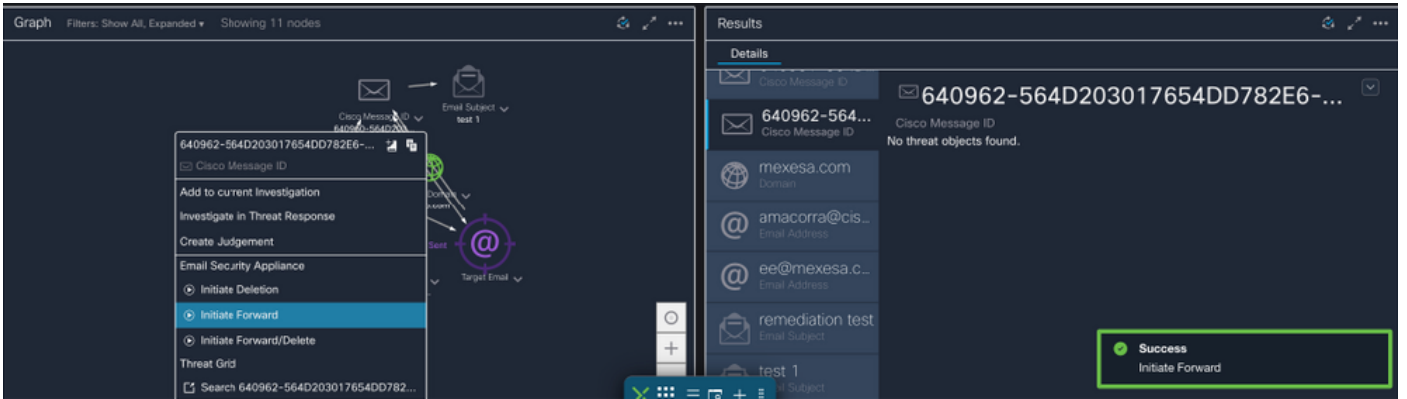
ةروصللا يف حضوم وه امك ،ةلاسرلا حالصا لبق دراولا ةبلع يف هيلع لصحت ام اذه 2.2:



تاءارجال" نم يا ةمئاقلا تاراخي نم ددح ، Cisco ةلاس ر فرعم" قوف رقنلا دنع 2.3  
 ةروصللا يف حضوم وه امك ، ةمومدملا ةيجالعال



نكرلا يف ةحجان ةقثب نم ةذفان رهظتو "ةردابم مي دقت" دي دحت متي ، لاثملا اذه يف 2.4  
 ةروصللا يف حضوم وه امك ، نم يال يلفسلا

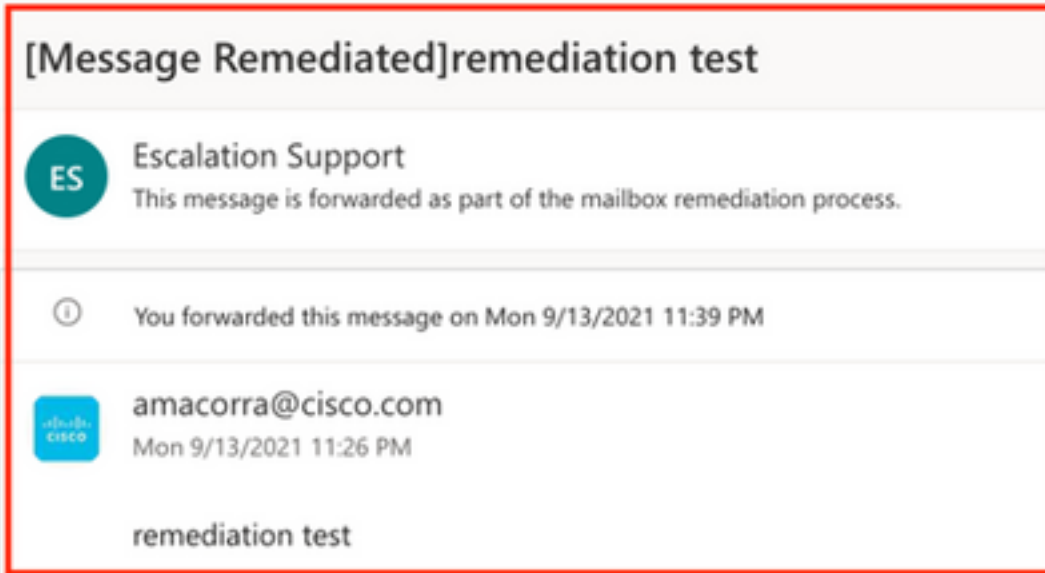


نأ رهظت يتلا "mail\_log" تحت ةيلا تالجالسلا لىع عالطالا كنكمي ، ESA يف 2.5  
 ةيئاهنلا ةلجالاو ، ددحمال اءارجال او ، أدبي "CTR" حالصلا

Mon Sep 13 23:38:03 2021 Info: Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcac-9b3d-404c-9327-f114fd5d89c7'.

Mon Sep 13 23:38:06 2021 Info: Message 640962 was processed with 'Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcac-9b3d-404c-9327-f114fd5d89c7'. Remediation status: Remediated.

يف ني بم وه امك ، ةلاس رلا عوضوم يف "[اهححصت مت يتلا ةلاس رلا]" ةرابعلا درت 2-6  
 ةروصللا



يذلل ناو ناعل وه ESA/SMA ةدحو ونوكت دن ع هبتكت يذلل ينورتكللال ديربل ناو ناع 2.7  
وأ "هيجوت ةداعا" رايل دل ددحت دن ع اهلصل م ت يلال ينورتكللال ديربل لئاسر لبقت س ي  
ةروصلال ي ف حضوم وه امك ، "فدح/هيجوت ةداعا":



ESA/SMA، ن ي ةد دجل ةهجالل لئاسرلل بقعت لي صافات ل ترظن اذا ، اريخ 2.8  
اهنأ ل ع "Last State" و "mail\_log" ي اه ل ل لوصحل م ت يلال تال جسلال سفن ىرت نأ كنكم ي  
ةروصلال ي ف حضوم وه امك ، "Remediated":

## Message Tracking

Message ID Header &lt;18fb395jhu2@mail.sergio.com&gt;

&lt; Previous Next &gt;

## Processing Details

## Summary

- 23:24:41 ● Start message 640962 on incoming connection (ICID 31).
- 23:24:41 ● Message 640962 enqueued on incoming connection (ICID 31) from amacorra@cisco.com.
- 23:24:41 ● Message 640962 direction: incoming
- 23:24:48 ● Message 640962 on incoming connection (ICID 31) added recipient (ee@mexesa.com).
- 23:25:07 ● Message 640962 original subject on injection: remediation test
- 23:25:07 ● Message 640962 not evaluated for Sender Domain Reputation. Reason: Disabled at Mail Flow Policy
- 23:25:07 ● Message 640962 (145 bytes) from amacorra@cisco.com ready.
- 23:25:07 ● Message 640962 has sender\_group: whitelist, sender\_ip: 15.0.0.59 and sbrs: None
- 23:25:07 ● Message 640962 matched per-recipient policy ee for inbound mail policies.
- 23:25:07 ● Message 640962 scanned by Advanced Malware Protection engine. Final verdict: SKIPPED(no attachment in message)
- 23:25:07 ● Message 640962 scanned by Outbreak Filters. Verdict: Negative
- 23:25:07 ● Message 640962 contains message ID header '<18fb395jhu2@mail.sergio.com>'
- 23:25:07 ● Message 640962 queued for delivery.
- 23:25:08 ● (DCID 6) Delivery started for message 640962 to ee@mexesa.com.
- 23:25:10 ● (DCID 6) Delivery details: Message 640962 sent to ee@mexesa.com
- 23:29:10 ● Message 640962 to ee@mexesa.com received remote SMTP response '2.6.0 <18fb395jhu2@mail.sergio.com> [internalid=27221502727676, Hostname=BY3PR19MB5169.namprd19.prod.outlook.com] 8351 bytes in 0.165, 49.369 KB/sec Queued mail for delivery'.
- 23:29:50 ● Incoming connection (ICID 31) lost.
- 23:38:03 ● Message 640962 was initiated for 'Forward' remedial action by 'admin' from source 'CTR' in batch '2b46dcdf-9b3d-404c-9327-f114fd5d89c7'.
- 23:38:06 ● Message 640962 was processed with 'Forward' remedial action for recipient 'ee@mexesa.com' in batch '2b46dcdf-9b3d-404c-9327-f114fd5d89c7'. Remediation status: Remediated.

## Envelope Header and Summary

## Last State

Remediated

## Message

Incoming

MID

640962

## Time

13 Sep 2021 23:24:41 (GMT -05:00)

## Sender

amacorra@cisco.com

## Recipient

ee@mexesa.com

## Subject

remediation test

## Sender Group

whitelist

## Cisco Hostname

(Name unresolved, SN:564D203017654DD782E6-AD81CB8ECD45)

## Incoming Policy Match

ee

## Message Size

145 (Bytes)

## Attachments

N/A

## Sending Host Summary

## Reverse DNS hostname

(unverified)

## IP address

15.0.0.59

## SIBRS Score

None

في ضيوعتالو و تحب الة زيم ةئيهت ب تم ق اذا ، حالص ا تاي لمع ةدع ءارج ا نكمي : ةظالم  
ESA/SMA نم كلذكو CTR نم ةلاس رلا س فن ةجال ام كنكمي ، ESA/SMA  
يذلا ناو نعل نع فل تخم ي نورتكل ا ل ديرب ناو نعل ا ل ةلاس رلا س فن هي جوت ةداع ا كلذ كل  
ة. طم نل ا لم اكل ا ةدحو ي ف هني وكت م

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل