為ESA刷新配置發件人域信譽2024年4月

目錄

簡介

必要條件

- 需求
- 採用元件

概觀

設定

- 啟用域信譽服務WebUI
- 域異常清單
  - 建立地址清單
  - 將地址清單應用於SDR全域性域例外清單
  - 將地址清單應用於內容/郵件過濾器
  - 郵件過濾器
- 建立內容過濾器以對SDR判定執行操作
- 通過使用消息過濾器配置SDR

驗證

疑難排解

- AsyncOS版本高於14的重要更新

相關資訊

簡介

本檔案介紹電子郵件安全裝置(ESA)的發件人網域信譽(SDR)配置。

必要條件

需求

思科建議您瞭解以下主題：

- ESA概念
- ESA配置

- 對SEG功能/功能的一般知識包括：郵件流策略、郵件過濾器、內容過濾器、全域性域信譽。

採用元件

本文檔中的資訊基於AsyncOS for ESA 14.2及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

1. SDR已被開發為一項附加服務，用於改進垃圾郵件釣魚檢測。

2. SDR捕獲多個報頭值，並將它們上傳到Talos威脅情報伺服器，在該伺服器上，龐大的Talos資源以分級方式確定每條消息的判定結果。

3.決定中包括的標題值包括：

- 信封發件人
- 自
- 回覆
- DMAR、DKIM和SPF驗證（如果已配置）。
- 電子郵件地址的（使用者名稱）值可以選擇從「發件人」(From)、「信封發件人」(Envelope-From)和「回覆收件人」(Reply-To)標題提交
- 發件人IP
- 在From和Reply-To標頭中顯示名稱。

5.對所有入站郵件執行SDR掃描。

6. SDR掃描僅在簡單郵件傳輸協定(SMTP)接受郵件之後才執行。

7.可以在初始郵件流策略階段以及郵件過濾器或內容過濾器選項處執行SDR操作。

8.配置的元件包括：

- 啟用域信譽服務
- 域例外清單（可選）
    - 域例外清單（全域性）
    - 使用特定消息/內容過濾器的域異常清單。
    - 使用郵件流策略進行域修復的全域性操作。
    - 域信譽全域性操作在SMTP會話級別執行操作。

- 郵件篩選器或內容篩選器

設定

啟用域信譽服務WebUI

可以從WebUI或CLI介面啟用SDR。

WebUI:

1.導航到Mail Security Services > Domain Reputation > Enable。

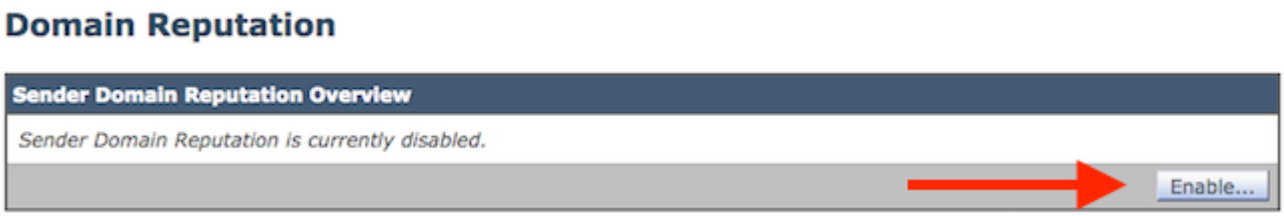
2.按一下Enable Sender Domain Reputation Filtering旁邊的框。

3.如果要將可選的題頭值包括在已選資料中，以提高功效，請選擇包括附加屬性：（可選）。按一下?學習。

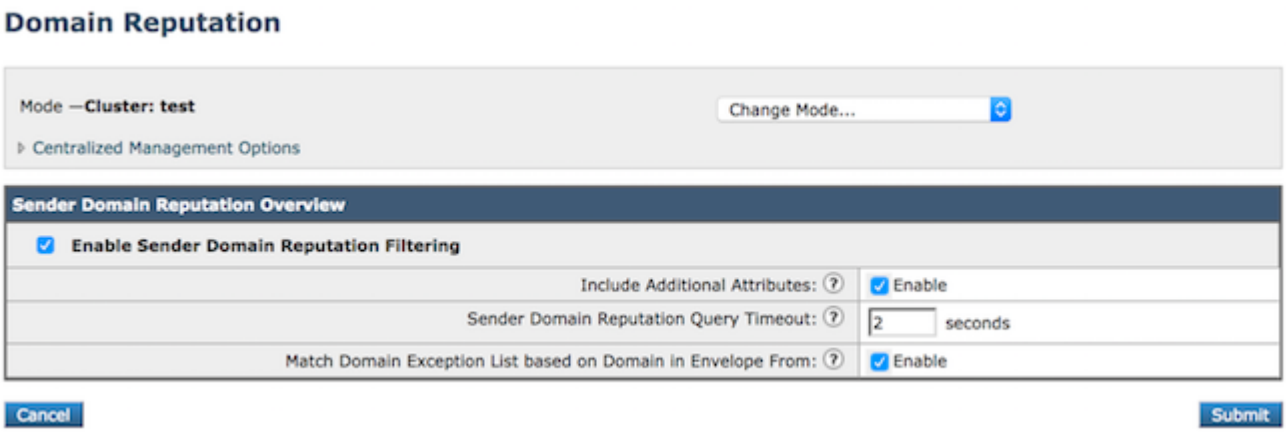
4.選擇此框「發件者域信譽查詢超時」。按一下?學習。

5.選擇Match Domain Exception List based on Domain in Envelope From - Enabled。

6.按一下「Submit > Commit」，如下圖所示。



發件人（域信譽）服務



安全服務>域信譽

域異常清單

1. 「域例外清單」可以繞過入站郵件流的發件人域信譽掃描。

2.域例外清單可在不同位置應用，以便影響郵件流。

3. 「全域性」應用程式可應用於所有已掃描的郵件。

4.內容/郵件過濾器中的更詳細應用程式只能影響已配置的過濾器。

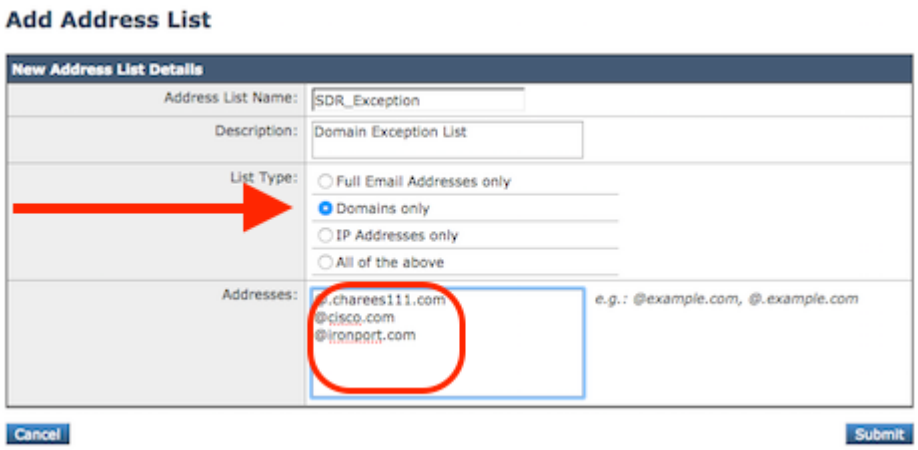
5.域例外清單提供2個選項，既提供簡單選項，又提供更加安全的選項。

6.本文檔介紹了為成功繞過使用域例外清單的報文的SDR而提供的選項。

7.解釋了域例外清單要求

建立地址清單

1. 導航到郵件策略>地址清單>新增地址清單>名稱>說明>清單型別：僅限域。
2. 使用逗號分隔來新增每個域名。
3. 按一下「Submit」和「Commit Changes」，如下圖所示。



要應用於域例外清單的地址清單

將地址清單應用於SDR全域性域例外清單

1. 導航到安全服務(Security Services)>域信譽(Domain Reputation)>域異常清單(Domain Exception List)>編輯設定(Edit Settings)>域異常清單(Domain Exception List)（選擇您的清單）。
2. 按一下「Submit」和「Commit Changes」，如下圖所示。

從下拉選單中選擇一個地址清單

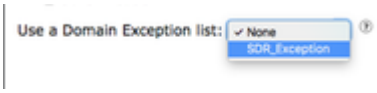
將地址清單應用於內容/郵件過濾器

傳入內容過濾器：

1.定位至「條件」>「URL信譽」>「威脅源選項」。

2.條件域信譽。

3.按一下此處：



域異常清單允許每個策略操作。

郵件過濾器

消息過濾器中的域例外清單應用程式將作為條件中的一個選項包括在內。

附註：這些示例包括domain_exception_list作為整個條件的一部分。

1. sdr-reputation(['bad', 'poor', 'intained', 'weak', 'unknown', 'neutral', 'good'], domain_exception_list)
2. sdr-age(「天」， <, 5, domain_exception_list)
3. sdr-unscannable(domain_exception_list)

有關郵件過濾器應用程式的更全面說明和示例，請參閱ESA使用者指南，標題如下：

- ETF的域信譽規則
- 根據使用郵件過濾器的發件人域信譽過濾郵件

建立內容過濾器以對SDR判定執行操作

1. SDR僅對傳入郵件流啟用。
2. SDR條件名稱：域信譽。
3. 可以建立多個條件來組合不同的結果。
4. 域信譽條件包含2個不同的檢查，每個檢查包含多個選項：

- 發件人域信譽
  - 發件人域信譽裁決
  - 發件人域期限
  - 無法掃描發件人域信譽
- 外部威脅源
  - 允許使用威脅源下載的內容清單對為SDR收集的相同域標題進行掃描。

附註：域信譽條件中的這些選項可以根據每個選擇的不同選項進行可視更改。

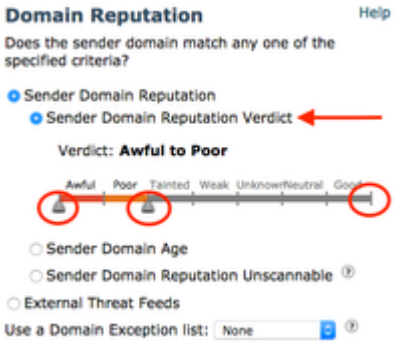
5.域信譽條件中的最後一個選項是域例外清單。

6.與「地址清單」關聯的「域例外清單」功能通過將該清單應用於更詳細的郵件策略級別郵件處理，為操作的應用新增了更多的控制。

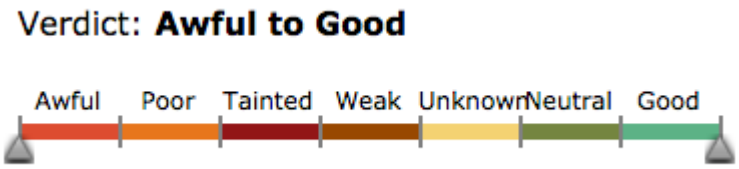
7.導航到Mail Policy > Incoming Content Filters > Add Filter > Add Condition > Domain Reputation。

8.條件1:發件人域信譽裁決。

- 糟糕，貧窮，受汙染，虛弱，未知，中性，好
- 包含滑動三角標籤以選擇要匹配的範圍。
- 「糟糕」和「貧窮」是採取行動時的建議值。
- 匹配「可惡」和「差」的郵件可以有額外的類別，例如「郵件跟蹤」中的「垃圾郵件」或「惡意的可檢視郵件」值。



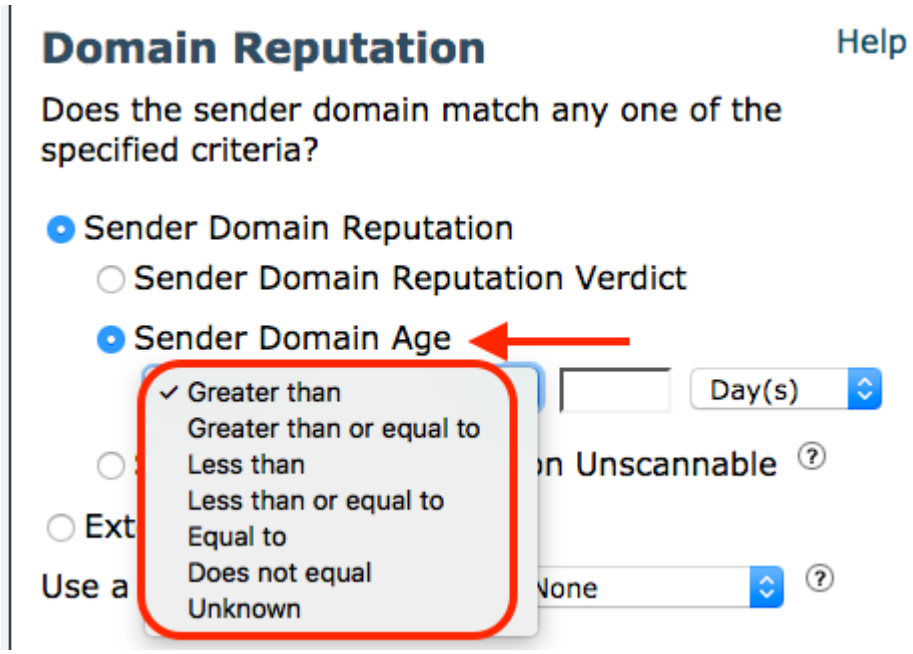
SDR判定可調整範圍滑動條。



SDR判定滑動條的完整檢視。

9.條件2:發件人域期限。

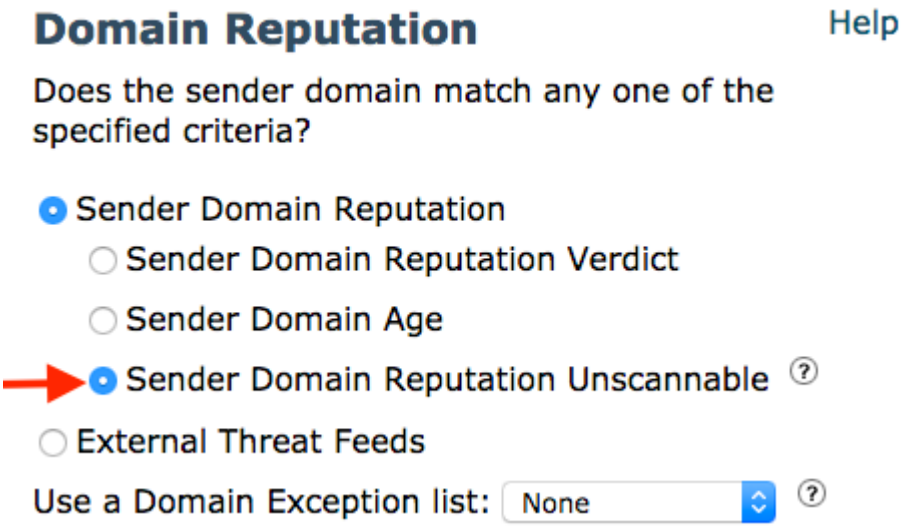
- 域的使用年限可能與更多的風險或長期的可靠性有關。
- 年齡小於10天的域的可能性會更高。



發件人域期限。數值越低，風險越大。

十、條件3:無法掃描發件人域信譽。

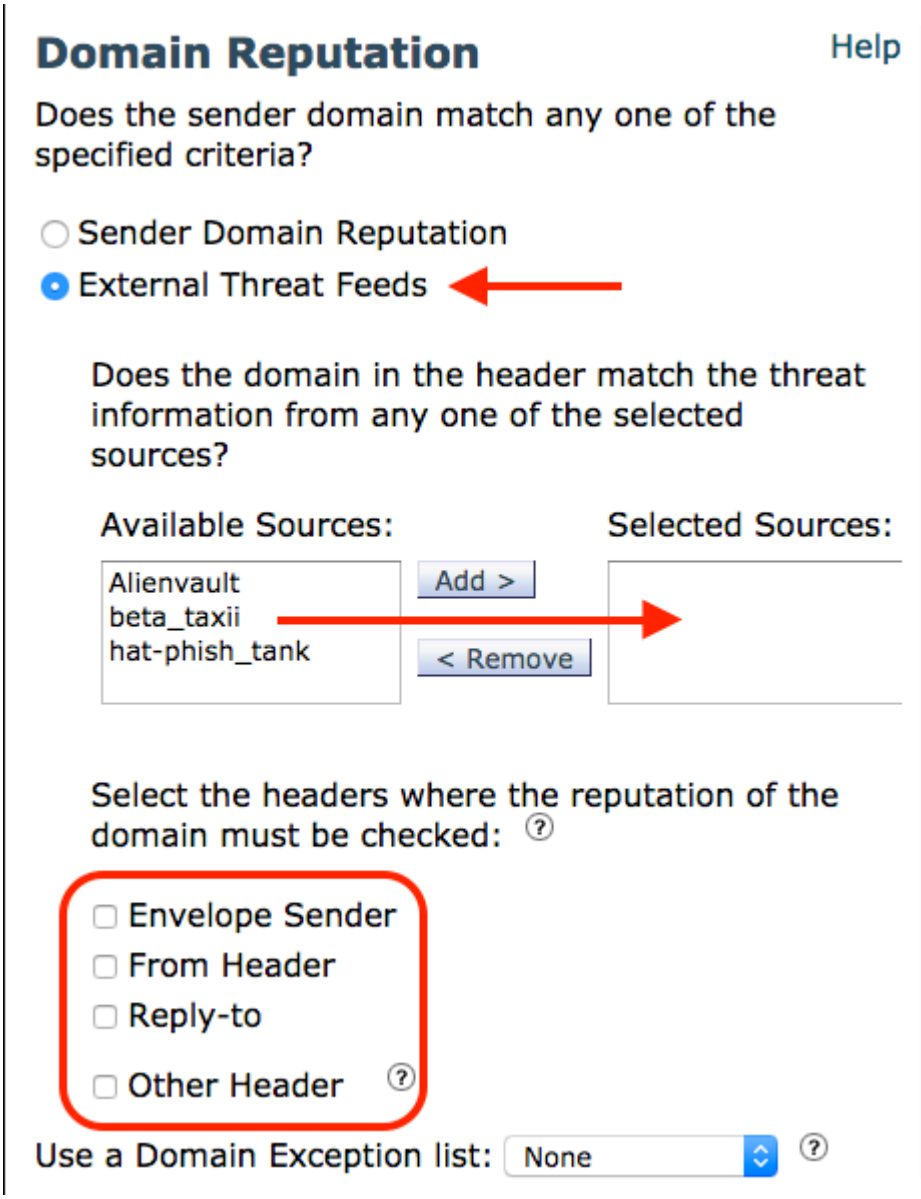
- 為管理員提供在無法獲取判定時採取操作的選項。



SDR不可掃描

十一、條件4:外部威脅源

- SDR掃描中包含的報頭也可以使用自定義下載的STIX/TAXII內容進行掃描。
- 此處將詳細介紹外部威脅源。外部威脅源。

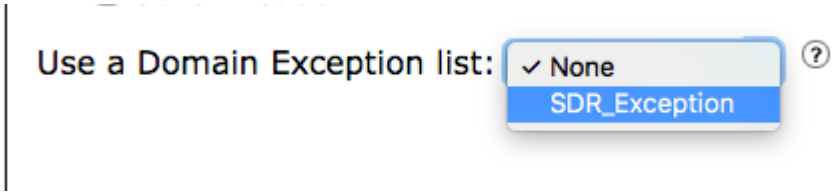


外部威脅源可用於掃描用於SDR的相同報頭。

- 電子郵件安全裝置使用手冊

十二、條件5:使用域例外清單。

- 使用內容過濾器內的域例外清單會增加比全域性清單更多的控制。



域異常清單允許每個策略操作。

13.結合這些條件的行動可能從最小到極大，這取決於管理員的預期結果。

14.列出了一些較受歡迎的行動：

- 隔離/複製到隔離
- drop
- 在郵件主題或正文中新增免責宣告或警告。
- 建立日誌條目以生成消息跟蹤日誌的特定單詞、短語或值。

通過使用消息過濾器配置SDR

1. ESA使用手冊是消息過濾器語法、定義和示例的絕佳來源。
2. 在《使用手冊》中搜尋此標題，以獲取郵件過濾器除此處提供的資訊以外的其他內容。

- 使用郵件過濾器根據發件人域信譽過濾郵件

3.以下條件與SDR消息過濾器相關聯：

- 如果sdr-reputation(['bad', 'poor'] >>>此值的所有值都包括：糟糕，貧窮，受汙染，虛弱，未知，中性，好
- if sdr-reputation(['bad', 'poor'], "<domain_exception_list>")>>這包括使用域例外清單
- 如果sdr-age(<'unit'>, <'operator'> <'actual value'>)>>，請參考《使用手冊》中的「operator」定義。
  - if(sdr-age("unknown", ""))>> unit = unknown。其餘值將替換為「」
  - 範例：if(sdr-age("months", <, 1, ""))。 >> unit = days， months， years。運算子= <（小於）。 實際值= 1
- 如果sdr-unscanable(<'domain_exception_list'>)>> As present（如圖所示），如果消息導致無法掃描。此示例還包括域異常清單條件。
- if(sdr-unscannable(""))>>>此示例不包括例外清單。值將替換為("")

驗證

使用本節內容，確認您的組態是否正常運作。

啟用SDR服務後，mail_logs和郵件跟蹤開始顯示SDR:日誌條目。

1.mail_logs包含收集的SDR資料的分數。

2.在確定郵件策略之前，先在郵件流中確定得分。

3.對裁決所採取的行動發生在郵件過濾和內容過濾器採取行動時。

<#root>

xxx.com>

mail_logs sample including SDR verdict

```
Tue Dec 3 15:22:44 2019 Info: New SMTP ICID 5539460 interface Data 1 (10.10.10.170) address 55.1.x.y re
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 ACCEPT SG Production_INBOUND match xxx1.xxx.com SBRS 2.5 cou
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES128-GCM-SHA
Tue Dec 3 15:22:44 2019 Info: Start MID 3291517 ICID 5539460
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 From: <customer@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 RID 0 To: <owner@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 IncomingRelay(PROD_TO_BETA): Header Received found, IP 172.20
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Message-ID '<mail>'
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Subject "You\\'ve Been Nominated for inclusion with Who\\'s W
```

Tue Dec 3 15:22:44 2019 Info: MID 3291517 SDR: Domains for which SDR is requested: reverse DNS host: Not

Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Consolidated Sender Reputation: Awful, Threat Category: M

Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Tracker Header : 5Zrl76622ZDGPsS6cByUUXq7LTXXS3/wonoZb5cG

```
Tue Dec 3 15:22:46 2019 Info: MID 3291517 ready 10011 bytes from <owner@xxx.com>
Tue Dec 3 15:22:46 2019 Info: MID 3291517 Custom Log Entry: MF_URL_Category_all HIT
Tue Dec 3 15:22:46 2019 Info: MID 3291517 matched all recipients for per-recipient policy DEFAULT in th
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim verdict using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim AV verdict using Sophos CLEAN
Tue Dec 3 15:22:47 2019 Info: MID 3291517 antivirus negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 AMP file reputation verdict : SKIPPED (no attachment in messa
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: GRAYMAIL negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 Custom Log Entry: SDR_Verdict_matched_Awful_Poor
Tue Dec 3 15:22:47 2019 Info: Start MID 3291519 ICID 0
```

4.簡單的grep命令，用於檢查特定判決的頻率或存在。

- **>>** grep "Sender Reputation:可怕" mail_logs
- **>>** grep "Sender Reputation:差" mail_logs

5.此外，可以使用CLI findevent命令連同MID值來獲取郵件日誌詳細資訊。

```
xxx.com> grep "SDR: Domain Reputation.*Poor" mail_logs
Tue Dec 3 11:07:01 2019 Info: MID 3265844 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
Tue Dec 3 12:57:28 2019 Info: MID 3277401 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
```

```
xxx.com> grep "SDR: Domain Reputation.*Awful" mail_logs
Tue Dec 3 10:24:08 2019 Info: MID 3261075 SDR: Consolidated Sender Reputation: Awful, Threat Category: N
Tue Dec 3 15:18:27 2019 Info: MID 3291182 SDR: Consolidated Sender Reputation: Awful, Threat Category: N
```

疑難排解

本節提供的資訊可供您用來疑難排解組態問題。

1. 無SDR:mail_logs或Message Tracking中存在的日誌。

- 對於通過ACCEPT Mail Flow Policy的郵件，始終可以顯示SDR日誌。
- 確保已按照本指南初始步驟中的說明啟用該服務。

2. SDR超時：

- 驗證SDR的思科雲伺服器是否已開啟且可供使用。
- v2.sds.cisco.com
- 可以使用CLI中的telnet執行非常一般的測試。
- 如果出現標語，則可以確認基本的可達性。
    - CLI > telnet v2.sds.cisco.com 443（這只能驗證時間點。）
- 檢查來自其他服務的日誌，以確定是否與基於Internet的服務存在潛在的通訊故障。
- CLI > displayalerts以檢查是否有其他通訊故障跡象。
- 在13.5版之前，SDR和URL過濾都使用v2.sds.cisco.com。
    - 如果網路路徑包含延遲，勾選URL Filtering CLI命令> websecuritydiagnostics可提供一些驗證。
- 檢查Sender Domain Reputation Timeout Setting，並確定值是否可以增加1-10秒。導航到Security Services > Domain Reputation > Edit > Sender Domain Reputation Query Timeout:2

預設值為2秒，最大設定為10秒。

AsyncOS版本高於14的重要更新

轉換後，主機名v2.sds.cisco.com仍然可用，但無法再針對URL過濾和SDR進行最佳化。

您需要在防火牆上允許這些主機名和IP地址用於出站TCP埠443流量。

主機名：

- serviceconfig.talos.cisco.com
- grpc.talos.cisco.com
- email-sender-ip-rep-grpc.talos.cisco.com

IP地址範圍：

- 146.112.62.0/24
- 146.112.63.0/24
- 146.112.255.0/24
- 146.112.59.0/24
- 2a04:e4c7:ffff::/48
- 2a04:e4c7:fffe::/48

這些是Cisco Talos智慧服務終端，用於獲取IP信譽、URL信譽和類別，並傳送服務日誌詳細資訊。

相關資訊

- ESA使用者指南
- ESA發行說明
- ESA CLI參考指南
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。