為暫存更新配置思科郵件安全和安全管理

目錄

簡介

本文檔介紹需要升級AsyncOS版本以及獲取運行Beta和預發行測試的ESA和SMA的更新的測試版客戶和預調配裝置的測試流程。 本檔案直接適用於思科電子郵件安全裝置(ESA)和思科安全管理裝置(SMA)。 請記住，標準生產客戶不會將登台伺服器用於生產ESA或SMA。 暫存作業系統版本、服務規則和服務引擎因生產環境而異。

在升級之前，請記住，生產許可證將無法升級到階段版本，因為它們無法通過許可證的驗證和身份驗證。生產VLAN在生成許可證時寫入了簽名值，它將與生產許可證服務匹配。暫存許可證只為暫存許可證服務編寫單獨的簽名。

必要條件

需求

1. 管理員先前已收到有關beta（預發行版作業系統）安裝或升級的通訊。
2. 參與Beta和預發行測試的客戶已完成了Beta應用程式，在開始測試Beta之前，他們已閱讀並同意了保密協定。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

為暫存更新配置思科郵件安全和安全管理

> **附註**：如果客戶僅能通過思科獲取預調配的Beta（預發行版作業系統）使用許可權，則只能使用登台更新伺服器URL。如果您沒有為試用版應用有效的許可證，裝置將不會從暫存更新伺服器接收更新。這些說明只能用於Beta客戶或參與Beta測試的管理員。

為了接收臨時更新和升級：

登入到GUI

1. 選擇**Security Services > Services Updates > Edit Update Settings...**
2. 確認所有服務均配置為使用Cisco IronPort更新伺服器

登入到CLI

1. 運行命令**updateconfig**
2. 運行隱藏子命令**dynamichost**
3. 輸入以下命令之一： 對於硬體ESA/SMA:**stage-update-manifests.ironport.com:443**對於虛擬ESA/SMA:**stage-stg-updates.ironport.com:443**
4. 按Enter鍵，直到返回到主提示符
5. 輸入**Commit**以儲存所有更改

驗證

可以在*updater_logs*中看到驗證，並且成功與適當的階段URL通訊。從裝置上的CLI輸入**grep stage updater_logs**:

```
esa.local> updatenow force

Success - Force update for all components requested
esa.local > grep stage updater_logs

Wed Mar 16 18:16:17 2016 Info: internal_cert beginning download of remote file "http://stage-
updates.ironport.com/internal_cert/1.0.0/internal_ca.pem/default/100101"
Wed Mar 16 18:16:17 2016 Info: content_scanner beginning download of remote file "http://stage-
updates.ironport.com/content_scanner/1.1/content_scanner/default/1132001"
Wed Mar 16 18:16:17 2016 Info: enrollment_client beginning download of remote file
"http://stage-updates.ironport.com/enrollment_client/1.0/enrollment_client/default/102057"
Wed Mar 16 18:16:18 2016 Info: support_request beginning download of remote file "http://stage-
updates.ironport.com/support_request/1.0/support_request/default/100002"
Wed Mar 16 18:16:18 2016 Info: timezones beginning download of remote file "http://stage-
updates.ironport.com/timezones/2.0/zoneinfo/default/2015100"
Wed Mar 16 18:26:19 2016 Info: repeng beginning download of remote file "http://stage-
updates.ironport.com/repeng/1.2/repeng_tools/default/1392120079"
```

如果存在任何意外的通訊錯誤，請輸入**dig <stage URL>**以驗證域名伺服器(DNS)。

範例：

```
esa.local > dig stage-updates.ironport.com


; <<>> DiG 9.8.4-P2 <<>> stage-updates.ironport.com A
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52577
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;stage-updates.ironport.com. IN A

;; ANSWER SECTION:
stage-updates.ironport.com. 275 IN A 208.90.58.21

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Tue Mar 22 14:31:10 2016
;; MSG SIZE rcvd: 60
```

驗證裝置是否能夠通過埠80 telnet，運行命令**telnet <stage URL> 80**。

範例：

```
esa.local > telnet stage-updates.ironport.com 80

Trying 208.90.58.21...
Connected to origin-stage-updates.ironport.com.
Escape character is '^]'.
```

恢復

要恢復為標準生產更新伺服器，請完成以下步驟：

1. 輸入命令**updateconfig**
2. 輸入隱藏子命令**dynamichost**
3. 輸入以下命令之一： 對於硬體ESA/SMA:**update-manifests.ironport.com:443**對於虛擬ESA/SMA:**update-manifests.sco.cisco.com:443**
4. 按Enter鍵，直到返回到主提示符
5. 運行命令**Commit**以儲存所有更改

附註：硬體裝置（C1x0、C3x0、C6x0和X10x0）應僅使用*stage-update-manifests.ironport.com:443*或*update-manifests.ironport.com:443*的動態主機URL。如果同時使用ESA和vESA的群集配置，則必須在電腦級別配置**updateconfig**，並確認已相應地設定*dynamichost*。

URL篩選

AsyncOS 13.0及更高版本

如果裝置上配置了URL過濾並正在使用，則一旦裝置重定向到使用階段URL進行更新，則裝置也需要配置為使用階段伺服器進行URL過濾：

1. 通過CLI訪問裝置

2. 輸入命令 **websecurityadvancedconfig** 逐步執行配置，將*Enter the Web security service hostname* 選項的值更改為**v2.beta.sds.cisco.com**
3. 將選項的值從默*認值更改為5輸入未處*理請求的**閾值**
4. 接受所有其他選項的預設值
5. 按Enter鍵，直到返回到主提示符
6. 運行命令**Commit**以儲存所有更改

恢復

要恢復為生產Web安全服務，請完成以下步驟：

1. 通過CLI訪問裝置
2. 輸入命令**websecurityadvancedconfig** 逐步執行配置，將*Enter the Web security service hostname* 選項的值更改為**v2.sds.cisco.com**
3. 接受所有其他選項的預設值
4. 按Enter鍵，直到返回到主提示符
5. 運行命令**Commit**以儲存所有更改

AsyncOS 13.5及更高版本（利用Cisco Talos服務）

從AsyncOS 13.5 for Email Security開始，引入了雲URL分析(CUA)，並更改了**websecurityadvancedconfig**選項。 由於現在在Talos雲中執行URL分析，因此不再需要網路安全服務主機名。 這已由**talosconfig**命令替換。 這僅在ESA的命令列中可用。

```
esa.local> talosconfig


Choose the operation you want to perform:
- SETUP - Configure beaker streamline configuration settings
[]> setup

Configured server is: stage_server

Choose the server for streamline service configuration:
1. Stage Server
2. Production Server
[]> 1
```

如果您正在運行階段許可證，您應該指向用於Talos服務的階段伺服器。

您可以運行**talosupdate**和**talosstatus**，以請求所有Talos驅動服務的更新和當前狀態。

範例：

```
esa.local> talosstatus

Component                          Version            Last Updated
Sender IP Reputation Client        1.0                Never updated
URL Reputation Client              1.0                Never updated
Service Log Client                 1.0                Never updated
Talos Engine                       1.95.0.269         Never updated
Talos Intelligence Services Module 1.95.0.808         Never updated
Talos-HTTP2 Component              0.9.330            Never updated
Libraries                          1.0                Never updated
Protofiles                         1.0                Never updated
```

有關詳細資訊，請參閱《思科郵件安全裝置AsyncOS 13.5使用手冊》。

訪問Cisco Talos服務的防火牆設定

您需要為下列主機名或IP地址（請參閱下表）在防火牆上開啟HTTPS（外寄）443埠，將您的電子郵件網關連線到Cisco Talos服務。

主機名	IPv4	IPv6
grpc.talos.cisco.com	146.112.62.0/24	2a04:e4c7:ffff::/48
email-sender-ip-rep-grpc.talos.cisco.com	146.112.63.0/24	2a04:e4c7:fffe::/48
serviceconfig.talos.cisco.com	146.112.255.0/24	-
	146.112.59.0/24	-

Web互動追蹤

Web互動跟蹤功能提供有關點選已重寫的URL的終端使用者以及與每個使用者點選相關聯的操作（允許、阻止或未知）的資訊。

根據您的要求，可以在以下全域性設定頁面之一啟用Web互動跟蹤：

1. 爆發過濾器。跟蹤點選由爆發過濾器重寫的URL的終端使用者
2. URL篩選。跟蹤點選策略重寫的URL的終端使用者（使用內容和郵件過濾器）

如果配置了Web互動跟蹤並在使用中，則在裝置重定向到使用階段URL進行更新之後，還需要將裝置配置為使用暫存聚合器服務器：

1. 通過CLI訪問裝置
2. 輸入命令**aggregatorconfig**
3. 使用EDIT命令並輸入以下值：**stage.aggregator.sco.cisco.com**
4. 按Enter鍵，直到返回到主提示符
5. 運行**Commit**以儲存所有更改

如果聚合器未配置為暫存，您將通過管理員電子郵件警報每30分鐘看到類似的警報：

```
Unable to retrieve Web Interaction Tracking information from the Cisco Aggregator Server.
Details: Internal Server Error.
```

或者，通過在CLI上運行**displayalerts**命令：

```
20 Apr 2020 08:52:52 -0600 Unable to connect to the Cisco Aggregator Server.
Details: No valid SSL certificate was sent.
```

恢復

要恢復為標準生產聚合器伺服器，請完成以下步驟：

1. 通過CLI訪問裝置
2. 輸入命令**aggregatorconfig**
3. 使用**EDIT**命令並輸入以下值：**aggregator.cisco.com**
4. 按Enter鍵，直到返回到主提示符
5. 運行命令**Commit**以儲存所有更改

疑難排解

本檔案「驗證」部分中列出了故障排除命令。

如果在執行**upgrade**命令時看到以下內容：

```
Failure downloading upgrade list.
```

請驗證是否已更改動態主機。 如果這種情況繼續存在，請詢問並驗證您的ESA或SMA是否已正確調配用於Beta測試或發行前測試。

相關資訊

- [vESA無法下載和應用反垃圾郵件或防病毒更新]
- [技術支援與文件 - Cisco Systems]