Configure un ESA para las actualizaciones que efectúan

Contenido

Introducción

Este documento describe el proceso para los clientes beta, y los dispositivos preprovisioned usados para probar, que necesita ser configurada para utilizar y tirar de las actualizaciones de los servidores de actualización del estacionamiento para Cisco envían por correo electrónico el dispositivo de seguridad (ESA) y el dispositivo de la Administración de seguridad (S A). Tenga presente, los servidores temporales no deben ser utilizados por los clientes de la producción estándar para la producción ESA o S A.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

> Nota: Los clientes deben ser solamente uso el servidor de actualización URL del estacionamiento si han accedido a preprovisioning con Cisco para el uso beta solamente. Si usted no tiene una licencia válida solicitada el uso beta, su dispositivo no recibirá las actualizaciones de los servidores de actualización del estacionamiento. Estas instrucciones se deben utilizar solamente para los clientes beta o por los administradores que participan en las pruebas Beta.

Para recibir las actualizaciones del estacionamiento:

GUI

1. Elija las **actualizaciones del > Services (Servicios) de los Servicios de seguridad > editan las configuraciones de la actualización…**
2. Confirme que configuran a todos los servicios para utilizar los servidores de actualización de Cisco IronPort.

CLI

1. Ingrese el **updateconfig del** comando.
2. Ingrese el **dynamichost** ocultado del submandato.
3. Ingrese uno de estos comandos: Para el hardware ESA/SMA: **stage-update-manifests.ironport.com:443**Para ESA/SMA virtual: **stage-stg-updates.ironport.com:443**
4. Presione ENTER hasta que le vuelvan al prompt principal.
5. Ingrese el **cometer** para salvar todos los cambios.

Verificación

La verificación se puede considerar en los *updater_logs* con la comunicación que tiene éxito para la etapa apropiada URL. Del CLI en la aplicación, ingrese los **updater_logs de la etapa del grep**:

```
9.9.5-033.local (SERVICE)>  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"
```

Si hay algunos errores de comunicación inesperados, ingrese el **<stage URL> del empuje** para verificar el Domain Name Server (DNS).

```
9.9.5-033.local (SERVICE)>  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
```

Para verificar la aplicación puede al telnet sobre el puerto 80, ingresa el comando del **<stage URL> 80 telnet**.

```
9.9.5-033.local (SERVICE)>  telnet stage-updates.ironport.com 80

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

Invierta

Para invertir de nuevo a los servidores de actualización de la producción estándar, complete estos pasos:

1. Ingrese el **updateconfig del** comando.
2. Ingrese el **dynamichost** ocultado del submandato.
3. Ingrese uno de estos comandos: Para el hardware ESA/SMA: **update-manifests.ironport.com:443**Para ESA/SMA virtual: **update-manifests.sco.cisco.com:443**
4. Presione ENTER hasta que le vuelvan al prompt principal.
5. Ejecute el **cometer** para salvar todos los cambios.

   Nota: Los dispositivos de hardware (C1x0, C3x0, C6x0, y X10x0) deben utilizar SOLAMENTE el host dinámico URL de *stage-update-manifests.ironport.com:443* o de *update-manifests.ironport.com:443*. Si hay una configuración de clúster con el ESA y el vESA, el **updateconfig** debe ser configurado en el nivel de equipo y confirmar que el **dynamichost** entonces está fijado por consiguiente.

Filtrado de URL

Si el Filtrado de URL es configurado y funcionando en el dispositivo, una vez que un dispositivo se ha reorientado para utilizar la etapa URL para las actualizaciones, el dispositivo también necesitará ser configurado para utilizar el servidor temporal para el Filtrado de URL:

1. Acceda el dispositivo vía el CLI
2. Ingrese el **websecurityadvancedconfig del** comando.
   El paso con la configuración y cambia el valor para la opción *ingresa el nombre de host del servicio de seguridad de la red* a: **v2.beta.sds.cisco.com**

3. Cambie el valor para la opción ingresan el valor de umbral para las peticiones extraordinarias a: **5.** (el valor por defecto es 50.)
4. Valide los valores por defecto para todas las otras opciones.
5. Presione ENTER hasta que le vuelvan al prompt principal.
6. Ingrese el **cometer** para salvar todos los cambios.

Seguimiento de la interacción de la red

Si el seguimiento de la interacción de la red es configurado y funcionando en el dispositivo, una vez que un dispositivo se ha reorientado para utilizar la etapa URL para las actualizaciones, el dispositivo también necesitará ser configurado para utilizar el servidor del aggregator del estacionamiento:

1. Acceda el dispositivo vía el CLI
2. Ingrese el **aggregatorconfig del** comando.
3. Utilice el comando del EDITAR y ingrese este valor: **stage.aggregator.sco.cisco.com**
4. Presione ENTER hasta que le vuelvan al prompt principal.
5. Ejecute el **cometer** para salvar todos los cambios.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- el vESA no puede descargar y aplicar las actualizaciones para Antispam o el antivirus
- Soporte Técnico y Documentación - Cisco Systems