Configurar um ESA para atualizações de encenação

Índice

Introdução

Este documento descreve o processo para beta clientes, e os dispositivos preprovisioned usados testando, que precisa de ser configurado a fim usar e puxar atualizações da plataforma atualizam server para a ferramenta de segurança do email de Cisco (ESA) e o dispositivo do Gerenciamento de segurança (S A). Mantenha na mente, os server da plataforma não devem ser usada por clientes da produção padrão para a produção ESA ou S A.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Nota: Os clientes devem ser somente uso o server URL da atualização da plataforma se acederam a preprovisioning através de Cisco para o beta uso somente. Se você não tem uma licença válida aplicada para o beta uso, seu dispositivo não receberá atualizações dos server da atualização da plataforma. Estas instruções devem somente ser usadas para beta clientes ou pelos administradores que participam nos testes beta.

A fim receber atualizações da plataforma:

GUI

1. Escolha **atualizações do > serviços dos Serviços de segurança > editam ajustes da atualização…**
2. Confirme que todos os serviços estão configurados para usar server da atualização de Cisco IronPort.

CLI

1. Incorpore o **updateconfig do** comando.
2. Incorpore hidden o **dynamichost do** subcommand.
3. Incorpore um destes comandos: Para o hardware ESA/SMA: **stage-update-manifests.ironport.com:443**Para ESA/SMA virtual: **stage-stg-updates.ironport.com:443**
4. A imprensa entra até que você esteja retornado ao alerta principal.
5. Entre **comprometem** a fim salvar todas as mudanças.

Verificar

A verificação pode ser considerada nos *updater_logs* com uma comunicação que sucede para a fase apropriada URL. Do CLI no dispositivo, incorpore **updater_logs da fase do 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"
```

Se há algum erro de comunicação inesperado, entre no **<stage URL> da escavação** a fim verificar o 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
```

A fim verificar o dispositivo pode ao telnet sobre a porta 80, incorpora o comando do **<stage URL> 80 do 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 '^]'.
```

Reverta

A fim reverter de volta à produção padrão atualize server, terminam estas etapas:

1. Incorpore o **updateconfig do** comando.
2. Incorpore hidden o **dynamichost do** subcommand.
3. Incorpore um destes comandos: Para o hardware ESA/SMA: **update-manifests.ironport.com:443**Para ESA/SMA virtual: **update-manifests.sco.cisco.com:443**
4. A imprensa entra até que você esteja retornado ao alerta principal.
5. Seja executado **comprometem** a fim salvar todas as mudanças.

   Nota: As ferramentas de hardware (C1x0, C3x0, C6x0, e X10x0) devem SOMENTE usar o host dinâmico URL de *stage-update-manifests.ironport.com:443* ou de *update-manifests.ironport.com:443*. Se há uma configuração de grânulos com o ESA e o vESA, o **updateconfig** deve ser configurado a nível da máquina e confirmar que o **dynamichost** está ajustado então em conformidade.

Filtragem URL

Se a Filtragem URL está configurada e no uso no dispositivo, uma vez que um dispositivo esteve reorientado para usar a fase URL para atualizações, o dispositivo igualmente deverá ser configurado para usar o server da plataforma para a Filtragem URL:

1. Alcance o dispositivo através do CLI
2. Incorpore o **websecurityadvancedconfig do** comando.
   A etapa com a configuração e muda o valor para a opção *entra no hostname do serviço de segurança da Web* a: **v2.beta.sds.cisco.com**
3. Mude o valor para a opção incorporam o valor de limiar para requisições consideráveis a: **5.** (o padrão é 50 pés.)
4. Aceite padrões para todas as outras opções.
5. A imprensa entra até que você esteja retornado ao alerta principal.
6. Entre **comprometem** a fim salvar todas as mudanças.

Seguimento da interação da Web

Se o seguimento da interação da Web está configurado e no uso no dispositivo, uma vez que um dispositivo esteve reorientado para usar a fase URL para atualizações, o dispositivo igualmente deverá ser configurado para usar o server do agregador da plataforma:

1. Alcance o dispositivo através do CLI
2. Incorpore o **aggregatorconfig do** comando.
3. Use o comando EDIT e incorpore este valor: **stage.aggregator.sco.cisco.com**
4. A imprensa entra até que você esteja retornado ao alerta principal.
5. Seja executado **comprometem** a fim salvar todas as mudanças.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- o vESA não pode transferir e aplicar atualizações para Antispam ou Antivirus
- Suporte Técnico e Documentação - Cisco Systems