¿Cómo ruedo detrás de mi versión actual de AsyncOS en un dispositivo de seguridad del correo electrónico de Cisco?

Pregunta:

Entorno: Dispositivo de seguridad del correo electrónico de Cisco (ESA), todas las versiones de AsyncOS

Resumen

En AsyncOS, “invierta” la característica tiene en cuenta rodar apoyan el dispositivo a una versión anterior.

No todas las versiones anteriores estarán disponibles:

Las actualizaciones causan la transformación unidireccional de los subsistemas dominantes que complican el proceso de la reversión. Cisco certifica las versiones específicas del CASO, de Sophos, de VOF y del McAfee a las versiones de AsyncOS, para asegurar una reversión inconsútil, las estructuras de la versión de destino tiene que ser calificado por Cisco. No todas las estructuras anteriores estarán disponibles; las solamente posibilidades limitadas, predeterminadas de la reversión existirán.

La reversión tomará mientras la actualización:

Para salvar los recursos de sistema de archivos, los medios de instalación no se guardan en los dispositivos. El proceso de la reversión requiere fluir, hacer-él-mientras que-transferencia, instalación.

La reversión es destructiva:

Cualquier mensaje en la cola de trabajo o la cola de la salida se borra. Se borran todos los datos y archivos del registro de la información. Solamente, se preservan se pierden los datos de las teclas de función, el resto de las configuraciones. Todas las bases de datos y Seguimiento de mensajes los datos serán perdidas. Todos mandan spam el mensaje de la cuarentena y los datos del usuario final safelist/blocklist. Solamente las configuraciones de red serán preservadas. Usted debe hacer que el acceso a la consola al poste del cuadro invierta pues el IP invertirá al valor por defecto de 192.168.42.42. La inversión del dispositivo hace una reinicialización inmediata ocurrir. Después de reiniciar, el dispositivo se reinicializa y reinicia otra vez a la versión deseada.

Prepárese para una reversión posible antes de actualizar:

Como mejor práctica, Cisco recomienda el prepararse para una actualización tomando las medidas siguientes:

1. Salve el archivo de configuración XML del cuadro (con las contraseñas desenmascaradas)
2. Si usted está utilizando la característica Safelist/Blocklist, exporte la lista del cuadro

3. Suspenda a los módulos de escucha
4. Drene la cola del correo y la cola de la salida
5. Exporte la base de datos de la cuarentena safelist/blocklist del Spam a otra máquina (si procede)

No olvide vuelven a permitir la actualización del poste de los módulos de escucha.

Cómo:

1. Login al CLI
2. El tipo “invierte”
3. El ESA presentará un menú de las versiones previamente instaladas, calificadas
4. La selección invierte la versión
5. Reinicialización
6. Primera reinicialización - el sistema sube, los discos de claros, desempaqueta los media de instalar
7. El sistema de la reinicialización (automática) - viene en segundo lugar usando la versión seleccionada, inicializa los datos frescos, comienzo del dispositivo
8. Cargue el archivo de configuración XML que usted guardó mientras que actualizaba
9. Si procede, importe el archivo Safelist/Blocklist