¿Cómo puedo deshacer mi versión actual de AsyncOS en un dispositivo de seguridad Cisco Email Security Appliance?

Pregunta:

Entorno: Dispositivo de seguridad Cisco Email Security Appliance (ESA), todas las versiones de AsyncOS

Resumen

En AsyncOS, la función "revert" permite retroceder el dispositivo a una versión anterior.

No todas las versiones anteriores estarán disponibles:

Las actualizaciones provocan una transformación unidireccional de los subsistemas clave que complica el proceso de reversión. Cisco certifica versiones específicas de las versiones CASE, Sophos, VOF y McAfee a AsyncOS, para garantizar una reversión sin fisuras, las versiones objetivo deben ser calificadas por Cisco. No todas las generaciones anteriores estarán disponibles; sólo existirán posibilidades de reversión limitadas y predeterminadas.

La reversión tardará tanto como la actualización:

Para guardar los recursos del sistema de archivos, los medios de instalación no se conservan en los dispositivos. El proceso de reversión requiere streaming, realizar la descarga mientras se realiza la instalación.

La reversión es destructiva:

Se eliminan todos los mensajes de la cola de trabajo o de la cola de entrega. Se eliminan todos los datos de informes y los archivos de registro. Sólo se conservan los datos de las claves de característica y se pierden todas las demás configuraciones. Se perderán todas las bases de datos y los datos de seguimiento de mensajes. Todos los mensajes de Spam Quarantine y los datos de lista de seguridad/lista de bloqueo del usuario final. Sólo se conservarán los parámetros de red. Debe tener acceso de consola al mensaje posterior de la caja ya que la IP volverá al valor predeterminado de 192.168.42.42. Revertir el dispositivo hace que se produzca un reinicio inmediato. Después del reinicio, el dispositivo se reinicializa y se reinicia nuevamente a la versión deseada.

Prepárese para una posible reversión antes de actualizar:

Como práctica recomendada, Cisco recomienda prepararse para una actualización mediante los siguientes pasos:

1. Guarde el cuadro Archivo XML de configuración (con contraseñas desenmascaradas)
2. Si utiliza la función Lista de seguridad/Lista de bloqueo, exporte el cuadro de lista de seguridad
3. Suspender los receptores

4. Dibujar la cola de correo y la cola de entrega
5. Exportar la base de datos de lista de seguridad/lista de bloqueo de Spam Quarantine a otra máquina (si procede)

No olvide volver a habilitar los receptores después de la actualización.

CÓMO:

1. Inicie sesión en la CLI
2. Escriba "revert"
3. ESA presentará un menú de versiones cualificadas previamente instaladas
4. Seleccionar versión revertida
5. Reiniciar
6. Primer reinicio: aparece el sistema, borra discos, desempaqueta los medios de instalación
7. Segundo reinicio (automático): el sistema utiliza la versión seleccionada, inicializa los datos nuevos y el dispositivo se inicia
8. Cargar el archivo de configuración XML que guardó al actualizar
9. Si es necesario, importe el archivo de lista de seguridad/bloqueo