Revertir ESA y SMA a la configuración original

Contenido

Introducción

En este documento se describe el procedimiento para revertir y volver a implementar un dispositivo de seguridad de correo electrónico (ESA) o un dispositivo de administración de seguridad (SMA).

Solución

Dispositivos de hardware (ESA/SMA)

Pasos para limpiar y revertir un dispositivo físico.

1. SSH al dispositivo y ejecute la versión y tome nota de la versión activa que se ejecuta en el dispositivo.

2. Ejecute Revert, seleccione una versión de código anterior a From # 1 y escriba Y.

```
sma.example.com> revert

This command will revert the appliance to a previous version of AsyncOS.

WARNING: Reverting the appliance is extremely destructive.
The following data will be destroyed in the process:
- all configuration settings (including listeners)
- all log files
- all databases (including messages in Virus Outbreak and Policy quarantines)
- all reporting data (including saved scheduled reports)
- all message tracking data
```

```
- all Cisco IronPort Spam Quarantine messages
  and end-user safelist/blocklist data

Only the network settings (except the 'allow_arp_multicast' configuration variable)
will be retained. If you need to establish connectivity to a Microsoft Network Load Balancer,
you must configure the 'allow_arp_multicast' configuration variable after the revert process
is complete.

Before running this command, be sure you have:
- saved the configuration file of this appliance (with passwords unmasked)
- exported the Cisco IronPort Spam Quarantine safelist/blocklist database
  to another machine (if applicable)
- waited for the mail queue to empty

Reverting the device causes an immediate reboot to take place.
After rebooting, the appliance reinitializes itself and reboots
again to the desired version.

    Available versions
    ==================
 1. 16.0.1-010
 2. 16.0.2-088
 3. 16.0.3-016
Please select an AsyncOS version [2]: 1
Do you want to continue? [N]> y
Are you sure you want to continue? [N]> y
```

Advertencia: Este procedimiento borrará la configuración, los datos y el historial de actualizaciones del dispositivo

---

4. Deje que la máquina complete la reversión y se espera que tome aproximadamente 30 minutos para completar.

3. Una vez que la reversión esté completa y el dispositivo esté activo, acceda a la línea de comandos nuevamente y ejecute Recargar vía Diagnóstico.

```
esa.example.com> diagnostic

Choose the operation you want to perform:
- RAID - Disk Verify Utility.
- NETWORK - Network Utilities.
- REPORTING - Reporting Utilities.
- TRACKING - Tracking Utilities.
- RELOAD - Reset configuration to the initial manufacturer values.
- RELOAD_STATUS - Display status of last reload run
- SERVICES - Service Utilities.
[]> reload

This command will remove all user settings and reset the entire device.

If this is a Virtual Appliance, all feature keys will be removed, and the license must be reapplied. Th
Are you sure you want to continue? [N]> y
Are you *really* sure you want to continue? [N]> y
```

```
Do you want to wipe also? Warning: This action is recommended if the device is being sanitized before s
Sometimes, it may take several minutes to complete the process because it follows the NIST Purge standa
Reverting to "virtualimage" preconfigure install mode.
```

Dispositivos virtuales (ESA/SMA)

Para obtener información sobre los requisitos de hardware y la plataforma de hipervisor compatible, consulte https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/Cisco_Content_S

VMware ESXi

1. Descargue la imagen del dispositivo virtual y el hash MD5 de Cisco.
2. Descomprima el archivo .zip del dispositivo virtual en su propio directorio; Por ejemplo, C:\vESA\C100V.
3. Abra VMware vSphere Client en su equipo local.
4. Seleccione el host o clúster de ESXi en el que desea implementar el dispositivo virtual.
5. Elija File > Deploy OVF template.
6. Introduzca la ruta del archivo OVF en el directorio que ha creado y haga clic en Next. Complete el asistente.
7. Si DHCP está desactivado, configure el dispositivo en la red. Instale el archivo de licencia.
8. Inicie sesión en la interfaz de usuario web de su dispositivo y configure el software del dispositivo.

Microsoft Hyper-V

1. Descargue la imagen del dispositivo virtual y el hash MD5 de Cisco.

2. Abra el Administrador de Hyper-V, utilice el "Asistente para nueva máquina virtual" para crear una nueva máquina virtual.

3. Asigne los recursos de hardware recomendados. (consulte la guía de instalación virtual)

4. Adjunte la imagen del dispositivo virtual descargada como el disco duro virtual. Complete el asistente e inicie la máquina virtual.

5. Si DHCP está desactivado, configure el dispositivo en la red. Instale el archivo de licencia.

6. Inicie sesión en la interfaz de usuario web de su dispositivo y configure el software del dispositivo.

KVM

Implemente la máquina virtual mediante Virtual Machine Manager. Descargue la imagen del dispositivo virtual y el hash MD5 de Cisco,

1. Inicie la aplicación virt-manager. Seleccione Nuevo.

2. Introduzca un nombre único para el dispositivo virtual. Seleccione Importar imagen existente.

3. Seleccione Reenviar, introduzca las opciones Tipo de SO: UNIX, versión: FreeBSD 13.

4. Busque y seleccione la imagen del dispositivo virtual que se descargó y seleccione Forward.

5. Introduzca los valores de RAM y CPU para el modelo de dispositivo virtual que debe desplegarse. (consulte la guía de instalación virtual)

6. Seleccione Reenviar, seleccione la casilla de control Personalizar y seleccione Finalizar.

7. Configure la unidad de disco. En el panel izquierdo, seleccione la unidad y en Opciones avanzadas, Bus de disco: Virtio, Formato de almacenamiento: qcow2 y seleccione Aplicar.

8. Configure el dispositivo de red para la interfaz de gestión. En el panel izquierdo, seleccione una NIC y las opciones de selección Dispositivo de origen: Su Vlan de gestión, modelo de dispositivo: virtIO, modo de origen: VEPA, seleccione Apply.

9. Configure los dispositivos de red para las interfaces adicionales. Repita el paso 8 para cada interfaz agregada a la máquina virtual.

10. Seleccione Comenzar instalación.

Nutanix

1. Descargue la imagen del dispositivo virtual y el hash MD5 de Cisco.

2. Acceda a Nutanix Prism, descomprima la imagen del dispositivo virtual qcow2 y cárguela en su grupo de almacenamiento.

3. Haga clic en el icono Hamburguesa en la esquina superior izquierda del panel de control Prisma de Nutanix, seleccione Compute and Storage > VM en el panel de navegación izquierdo.

4. Haga clic en el botón Crear VM, introduzca los detalles para configurar la VM y haga clic en Siguiente.

5. Configure los recursos de hardware según el modelo (consulte la guía de instalación virtual)

6. Haga clic en el botón Adjuntar disco en Discos y seleccione Clonar desde imagen de la lista desplegable Operación y cargar la imagen qcow2 de la lista desplegable Imagen.

7. Haga clic en el botón Attach to Subnet en Networks y configure los parámetros de la interfaz de red.

8. Complete el asistente para implementar el dispositivo virtual en Nutanix Prism.

Implementación de nube pública

Para obtener información y conocer los procedimientos para implementar ESA y SMA en la nube

pública, consulte
https://www.cisco.com/c/dam/en/us/td/docs/security/content_security/virtual_appliances/ESA_SMA_Virtua

Azure

1. Cree los componentes necesarios.

2. Obtenga la imagen de VM.

3. Configuración del control de acceso: gestión de identidades y accesos (IAM)

4. Inicie sesión y cree la máquina virtual.

Consulte las páginas 4 a 18 de la guía de implementación de nubes públicas para obtener información detallada sobre el procedimiento para implementar la máquina virtual en Azure.

AWS

1. Póngase en contacto con el TAC de Cisco para obtener la ID de AMI.

2. Abra la consola Amazon EC2.

3. Seleccione AMI en el panel de navegación.

4. Elija Public Images en el primer filtro.

5. En la barra de búsqueda, introduzca el "número de build" y el "modelo" según el modelo de dispositivo virtual requerido.

Consulte las páginas 19 a 29 de la guía de implementación de nubes públicas para obtener información detallada sobre el procedimiento para implementar la máquina virtual en AWS.

GCP

1. Prepare el entorno y configure la máquina virtual.

2. Seleccione SO y Almacenamiento.

3. Configure la red, el firewall y la interfaz de red.

4. Configure la máquina virtual.

Consulte las páginas 30 a 34 de la guía de implementación de nubes públicas para obtener información detallada sobre el procedimiento para implementar la máquina virtual en GCP.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).