Lo que hay que saber sobre las políticas de seguridad

Aprenda a proteger su ordenador personal, su servidor y sus sistemas en la nube con SELinux, la seguridad de Kubernetes y los cortafuegos.

Escrito por Chris Collins y Seth Kenlon, publicado por Open Source Com bajo licencia Creative Commons 4.0; traducción al castellano de Venezuela (es_VE) hecha por Jimmy Olano.

Seguridad, llave y candado. Crédito de imagen: JanBaby, via Pixabay CC0.

Una **política de seguridad** es un conjunto de permisos que regulan el acceso a un sistema, ya sea una organización, un ordenador, una red, una aplicación, un archivo o cualquier otro recurso. Las políticas de seguridad suelen empezar de arriba abajo: Asumir que nadie puede hacer nada, y luego permitir excepciones.

En una computadora de escritorio, la política por defecto es que ningún usuario puede interactuar con el ordenador hasta después de iniciar la sesión. Una vez que ha iniciado la sesión con éxito, hereda un conjunto de permisos digitales (en forma de metadatos asociados a su cuenta de inicio de sesión) para realizar algún conjunto de acciones. Lo mismo ocurre con un teléfono, un servidor o una red en Internet, o cualquier nodo en una red privada virtual.

Hay políticas de seguridad diseñadas para:

- Sistemas de archivos.
- Cortafuegos.
- Servicios.
- *Demonios.*
- Archivos individuales.

Asegurar la infraestructura digital es un trabajo que realmente nunca termina y eso puede parecer frustrante e intimidante. Sin embargo, las políticas de seguridad existen para que no tenga usted que pensar en quién o qué puede acceder a los datos. El estar cómodamente familiarizado con los posibles problemas de seguridad es importante, y la lectura de los problemas de seguridad conocidos (como la gran fuente RSS del NIST para las entradas de CVE) cuando tome su desayuno energético puede ser más reveladora que una buena taza de café, pero igualmente importante es estar familiarizado con las herramientas a su disposición para ofrecerle valores predeterminados sensatos.

«To me this is party time. Everything I need.» Justin Matthew (Flickr)

Éstas varían dependiendo de lo que esté asegurando, así que este artículo se centra en tres áreas: ordenadores personales, el servidor y las redes privadas virtuales.

SELinux

SELinux es un sistema de etiquetado para ordenadores personales, servidores y los nodos GNU/Linux de la red privada virtual. En un sistema GNU/Linux moderno que ejecuta SELinux, cada proceso tiene una etiqueta, al igual que cada archivo y directorio. De hecho, cualquier objeto

del sistema tiene una etiqueta. Afortunadamente, no es el usuario quien tiene que hacer el etiquetado. Estas etiquetas son creadas automáticamente por SELinux.

Las reglas de la política gobiernan el acceso que se concede entre los procesos etiquetados y los objetos etiquetados. El **kernel** hace cumplir estas reglas. En otras palabras, SELinux puede asegurar que una acción es segura tanto si un usuario parece merecer el derecho a realizar esa acción como si no. Lo hace entendiendo qué procesos están permitidos. Esto protege a un sistema de un mal actor que obtiene elevación de permisos -*ya sea a través del aprovechamiento de una falla de seguridad o sentándose en la silla del usuario después de haberse levantado para rellenar la taza de café*- al entender las interacciones esperadas de todos los componentes de la computadora.

Para conocer más acerca de SELinux (en idioma inglés):

- "Illustrated guide to SELinux" por Dan Walsh.
- "A sysadmin's guide to SELinux" por Alex Callejas.
- "SELinux cheat sheet".

Seguridad en los *Kubernetes pod*

En el mundo de Kubernetes, existen **Políticas de Seguridad** y **Contextos de Seguridad** aplicado a los nodos (vainas o *pods*, como son mejor conocidos).

Las políticas de seguridad de los *pods* son una implementación de los recursos de seguridad de Kubernetes. Son recursos integrados que describen condiciones específicas que los *pods* deben cumplir para ser aceptados y programados. Por ejemplo, las políticas de seguridad de los *pods* pueden aprovechar las restricciones sobre los tipos de volúmenes que un *pod* puede montar o los ID de usuario o grupo que el *pod* no puede utilizar. A diferencia de los **Contextos de Seguridad**, estas son restricciones controladas por el **Plano de Control** del racimo o *cluster* que deciden si un *pod* determinado está permitido dentro del sistema Kubernetes, incluso antes de ser creado. Si la especificación del *pod* no cumple con los requisitos de la Política de Seguridad del *pod*, este es rechazado.

Los **Contextos de Seguridad** son similares a las Políticas de Seguridad de los *pods*, en el sentido de que describen lo que un *pod* o contenedor puede y no puede hacer, *pero en el contexto del tiempo de ejecución del contenedor*. Recuerde que las políticas de seguridad de los *pods* se aplican en el plano de control. Los Contextos de Seguridad se proporcionan en la especificación del *pod* y describen al tiempo de ejecución del contenedor (por ejemplo, Docker, CRI-O, etcétera) específicamente cómo debe ejecutarse el *pod*. Hay un gran solapamiento en los tipos de restricciones que se encuentran en las políticas de seguridad de los *pods* y en los contextos de

seguridad. Las primeras pueden ser consideradas como "estas son las cosas que un *pod* en esta política puede hacer", mientras que las segundas son "este *pod* debe ser ejecutado con estas reglas específicas".

El estado de las políticas de seguridad de los *pods*

Las políticas de seguridad de los *pods* están obsoletas y se eliminarán en Kubernetes 1.25. En abril de 2021, Tabitha Sable, de Kubernetes SIG Security, escribió sobre la eliminación y la sustitución de las políticas de seguridad de los *pods*. Hay una solicitud de extracción abierta que describe las mejoras propuestas de Kubernetes con un nuevo controlador de admisión para hacer cumplir las normas de seguridad de los *pods*, que se sugiere como el reemplazo de las políticas de seguridad de los *pods* obsoletos. La arquitectura reconoce, sin embargo, que existe un amplio ecosistema de complementos y servicios complementarios que pueden mezclarse y combinarse para proporcionar una cobertura que satisfaga las necesidades de una organización.

Por el momento, Kubernetes ha publicado los Estándares de Seguridad de los *Pods*, que describen el concepto general de los tipos de políticas en capas, desde los *pods* con Privilegios Totales y sin restricciones hasta las políticas de Línea de Base mínimamente restringidas y luego fuertemente restringidas, y publican estas políticas de ejemplo como Políticas de Seguridad de los Pods. La documentación describe qué restricciones componen estos diferentes perfiles y proporcionan un excelente punto de partida para familiarizarse con los diferentes tipos de restricciones que podrían aplicarse a un pod para aumentar la seguridad.