Documentación de Ansible
The Hive y Cortex

Instalación de The Hive

La instalación comienza con la ejecución del comando ***ansible-playbook -i hosts -l thehive setup.yml --extra-var "target=thehiveuser --ask-become-pass*** dentro de la carpeta *thehive-ansible*. Esta instrucción ejecuta la instalación de los roles dentro del archivo *setup*: *java_install*, *elastic_install* y *thehive_install.*

Roles

java_install: En la carpeta de este role, encontramos la subcarpeta task y dentro de ella el archivo *main.yml*, que ejecuta la instalación de Java en su versión 11: *default-jre* y *openjdk-11-jre-headless*

elastic_install: En la carpeta de este role, encontramos la subcarpeta task y dentro de ella el archivo *main.yml*, que ejecuta las siguientes tareas: agrega una clave desde un keyserver (controlando que no exista previamente), luego configura el repositorio de elastic (ubicado en */etc/apt/sources.list.d/elastic-5.x.list*) agregando la línea *deb https://artifacts.elastic.co/packages/5.x/apt stable main* al archivo anteriomente mencionado. A continuación, se procede a instalar el soporte para *apt con https*, la instalación de *elasticsearch* desde el repositorio general del sistema; una vez instalado elasticsearch, agregamos las siguientes líneas de configuración al archivo */etc/elasticsearch/elasticsearch.yml*:

network.host: 127.0.0.1
script.inline: true
cluster.name: hive
thread_pool.index.queue_size: 100000
thread_pool.search.queue_size: 100000
thread_pool.bulk.queue_size: 100000

Finalmente, reiniciamos los *daemon* para ejecutar el servicio de elasticsearch, habilitamos e iniciamos el servicio y concluimos con la revisión del estado de este.

thehive_install: En la carpeta de este role, encontramos la subcarpeta task y dentro de ella el archivo *main.yml*, que ejecuta las siguientes tareas: agrega el repo de TheHive: para esto necesitaremos crear un archivo en la lista de sources y luego agregar el repositorio propiamente dicho. Para la primera parte de esta tarea, creamos el archivo */etc/apt/sources.list.d/thehive-project.list* y luego escribimos en él la linea del repositorio de TheHive: *deb https://dl.bintray.com/thehive-project/debian-stable any main.*

Luego instalamos curl, agregamos una clave desde un keyserver (controlando que no exista previamente https://raw.githubusercontent.com/TheHive-Project/TheHive/master/PGP-PUBLIC-KEY), actualizamos el repositorio e instalamos TheHive.

A continuación, se crea la carpeta */etc/thehive* (en el caso de que no existiera previamente). creamos la clave *play.http.secret.key* y la insertamos en el archivo *application.conf* que se encuentra en la carpeta que habíamos creado previamente: */etc/thehive/application.conf*.

Posteriormente, reiniciamos los *daemon* para ejecutar el servicio de thehive, habilitamos e iniciamos el servicio y concluimos con la revisión de su estado. Para finalizar, el siguiente software es instalado: *python-pip*, *python3-pip* y *thehive4py*.

En la carpeta principal, *thehive-ansible*, encontramos también a la carpeta *host_var* y el archivo *hosts* que contiene el grupo [thehive] y la variable *thehiveuser*, que luego será usada para llamar al archivo *thehiveuser.yml* de la carpeta *host_vars*. Este archivo contiene las variables *ansible_host* y *ansible_user* que contienen la IP del host y el usuario del sistema, respectivamente.

Instalación de Cortex

La instalación comienza con la ejecución del comando ***ansible-playbook -i hosts -l cortex setup.yml --extra-var "target=thehiveuser --ask-become-pass*** dentro de la carpeta *cortex-ansible*. Esta instrucción ejecuta la instalación de los roles dentro del archivo *setup*: *java_install*, *elastic_install*, cortex_*install*, *download_default_analyzers_responders, cortex_analyzers* y *cortex_responders*.

Roles

j*ava_install*: En la carpeta de este role, encontramos la subcarpeta task y dentro de ella el archivo *main.yml*, que ejecuta la instalación de Java en su versión 11: *default-jre* y *openjdk-11-jre-headless*

elastic_install: En la carpeta de este role, encontramos la subcarpeta task y dentro de ella el archivo *main.yml*, que ejecuta las siguientes tareas: agrega una clave desde un keyserver (controlando que no exista previamente), luego configura el repositorio de elastic (ubicado en */etc/apt/sources.list.d/elastic-5.x.list*) agregando la línea *deb https://artifacts.elastic.co/packages/5.x/apt stable main* al archivo anteriomente mencionado. A continuación, se procede a instalar el soporte para *apt con https*, la instalación de *elasticsearch* desde el repositorio general del sistema; una vez instalado elasticsearch, agregamos las siguientes líneas de configuración al archivo */etc/elasticsearch/elasticsearch.yml*:

network.host: 127.0.0.1
script.inline: true
cluster.name: hive

thread_pool.index.queue_size: 100000
thread_pool.search.queue_size: 100000
thread_pool.bulk.queue_size: 100000

Finalmente, reiniciamos los *daemon* para ejecutar el servicio de elasticsearch, habilitamos e iniciamos el servicio y concluimos con la revisión del estado de este.

cortex_install: En la carpeta de este role, encontramos la subcarpeta task y dentro de ella el archivo *main.yml*, que ejecuta las siguientes tareas: agrega el repo de Cortex: para esto necesitaremos crear un archivo en la lista de sources y luego agregar el repositorio propiamente dicho. Para la primera parte de esta tarea, creamos el archivo */etc/apt/sources.list.d/thehive-project.list* y luego escribimos en él la linea del repositorio de TheHive: *deb https://dl.bintray.com/thehive-project/debian-stable any main.*

Los pasos anteriores no serán ejecutados si previamente se instaló TheHive en el sistema. Luego, se agrega una clave desde un servidor (*https://raw.githubusercontent.com/TheHive-Project/Cortex/master/PGP-PUBLIC-KEY*), se instala Cortex desde el repositorio, se crea la carpeta */etc/thehive* (esto sera ejecutado si previamente se ejecuto el ansible de TheHive en el sistema o si la carpeta ya existia) se crea una clave *play.http.secret.key* y se la agrega en el archivo */etc/cortex/application.conf*.

Finalmente, se reinician los *daemon* para ejecutar el servicio de cortex, se habilita e inicia el servicio y se comprueba su estado.

download_default_analyzers_responders: En la carpeta de este role, encontramos la subcarpeta task y dentro de ella el archivo *main.yml*, que ejecuta las siguientes tareas: Actualiza los repositorios e instala un conjunto de dependencias necesarias para los analyzers y los responders (*python-pip, python2.7-dev, python3-pip, python3-dev, ssdeep, libfuzzy-dev, libfuzzy2, libimage-exiftool-perl, libmagic1, build-essential, git y libssl-dev*), con pip y pip3 se instala *setuptools,* luego se clona el repositorio de Analyzers y Responders de Cortex (*https://github.com/TheHive-Project/Cortex-Analyzers*) en el directorio "{{path_default_analyzers_and_responders }}".

Posteriormente, se buscan los requerimientos necesarios para instalar en el archivo *requirements.txt* en el directorio mencionado anteriormente. Una vez localizados, estos requerimientos se instalan con pip y pip3.

cortex_analyzers: En la carpeta de este role, encontramos la subcarpeta task y dentro de ella el archivo *main.yml*, que ejecuta las siguientes tareas: