Práctica 4: Migración de máquinas virtuales.

El objetivo de esta actividad es realizar operaciones de migración de máquinas virtuales.

1 Introducción

El objetivo fundamental de esta actividad es realizar migraciones de máquinas virtuales entre diferentes anfitriones. La migración de máquinas virtuales requiere un almacenamiento compartido del disco, por lo que será necesario disponer de algún servicio de almacenamiento compartido (NFS, iSCSI, SAMBA, etc…). En nuestro caso emplearemos el contendor **`CONT_VOL_COMP`** creado en la práctica 3. Este contendor proporciona un espacio de almacenamiento compartido soportado mediante NFS.

Tanto el almacenamiento compartido como la propia migración requieren comunicación entre los anfitriones, por lo que será necesario configurar el cortafuegos para permitir dichas comunicaciones.

Las principales fuentes de información de consulta para el desarrollo de la práctica son las siguientes:

- *"Virtualization Deployment and Administration Guide" [1]*. El capítulo 15 de esta guía está dedicado a explicar la operación de migración de MVs con KVM y es muy recommendable su lectura.
- *"Red Hat Enterprise Linux 7 Networking Guide" [2]*. En el capítulo 6 de esta guía se explica la forma adecuada de asignar un nombre de dominio completamente cualificado al host.
- "*Red Hat Enterprise Linux 7 Security Guide*" [3]. La operación de migración de máquinas virtuales va a requerir de modificar la configuración del cortafuegos del host anfitrión. En el capítulo 5 de esta guía se explica el funcionamiento del cortafuegos *Firewalld*, que es el servicio de cortafuegos que viene por defecto en *Fedora 39*.

2 Requisitos previos

Para abordar esta práctica se debe haber completado la práctica 3 (Recursos de almacenamiento virtual).

3 Plan de actividades y orientaciones

Cada estudiante deberá preparar su equipo de trabajo de forma que pueda realizar la migración de una máquina virtual al anfitrión de otro compañero o compañera. Para poder realizar esta práctica será necesario llevar a cabo las siguientes tareas:

Tarea 1: configurar de forma adecuada los nombres de los anfitriones: nombre de dominio completamente cualificado (*FQDM*)

Esta tarea debe haberse realizado en la práctica 1. En cualquier caso, deberá asegurarse de que efectivamente la ha completado de forma correcta. El *FQDN* es obtenido de forma automática a través del servidor de DNS, siempre que las máquinas están declaradas en dicho servidor. Sin embargo, esto no ocurre así en el laboratorio de la asignatura, por lo que cada estudiante deberá asignarle el nombre al anfitrión manualmente (para ello debe hacer uso de la orden `hostnamectl`). En el capítulo 6 de [2] encontrarán una explicación detallada sobre el uso de esta orden.

Para la asignación de nombres a cada anfitrión, se deberá seguir el siguiente patrón:

Etiqueta_de_equipo.vpd.com

Por ejemplo, ***pc1087.vpd.com.*** Para evitar confusiones, ponga el IdentificadorPC en minúsculas.

Tarea 2: Uso de un contendor de almacenamiento compartido

Tal y como ya se ha indicado, el espacio compartido de almacenamiento requerido para realizar esta práctica lo proporciona el contenedor **CONT_VOL_COMP** creado en la práctica 3.

Deberá crear una nueva máquina virtual llamada **mvp4_etiqueta_de_equipo, por ejemplo, mvp4_lqd19**. Esta nueva máquina virtual deberá ser el resultado de clonar la máquina virtual **mvp1** creada en la práctica 1 pero con una diferencia importante: la imagen de disco de la nueva máquina **mvp4_etiqueta_de_equipo** debe almacenarse en el espacio de almacenamiento compartido proporcionado por el contenedor **CONT_VOL_COMP**. Por último, e importante, para evitar conflictos entre los nombres de las imágenes de disco de las máquinas huésped de cada estudiante en el espacio de almacenamiento compartido, el nombre de las imágenes de disco deberá respetar el siguiente patrón:

pcHOST_LQX_ANFITRIONY_p4.qcow2

Por ejemplo, un estudiante que trabaje en el host pc1087 en el laboratorio LQ-1 en la partición ANFITRION1, deberá crear el volumen de disco que se indica en este apartado con el siguiente nombre: **pc1087_LQ1_ANFITRION1_p4.qcow2.** Los laboratorios empleados en la asignatura son LQ-1 (D07), LQ-2 (D08), LQ-C (E06) y LQ-D (E05). Por tanto, LQX deberá coincidir con alguno de los siguientes patrones: LQ1, LQ2, LQC o LQD.

Una vez que ha conseguido clonar la máquina con éxito, compruebe que la máquina está totalmente operativa. Tenga en cuenta que es normal que el arranque de la máquina se demore al tener su disco en un espacio de almacenamiento externo, a diferencia de cuando la máquina huésped tiene el disco en el host anfitrión.

Tarea 3: migración

Para poder realizar la migración de máquinas virtuales entre diferentes anfitriones es necesario realizar una conexión *ssh* entre ellos. Esta conexión se realiza empleando el *virt-manager*. Sin embargo, si intentamos realizar una conexión *ssh* con otro sistema anfitrión con el usuario *root*, se nos pedirá la contraseña para poder establecer la conexión. Obviamente y como ustedes saben, la contraseña de *root* debe conocerla exclusivamente el administrador del sistema anfitrión, y por tanto en ningún caso les vamos a pedir que compartan esa clave. Sin embargo, *ssh* permite otros mecanismos de autenticación alternativos al esquema básico de usuario/contraseña. Uno de ellos consiste en la autenticación mediante clave pública/privada. Para ello es necesario:

1. Que cada usuario genere un par de claves pública/privada de forma que el servidor SSH conozca la clave pública del usuario al que va a permitir el acceso y sólo dicho usuario conozca su clave privada (orden `ssh-keygen`).
2. Compartir el fichero que contiene la clave pública con el compañero o compañera con el que queremos establecer la conexión (orden `ssh-copy-id`). Una vez realizado estos pasos, la conexión *ssh* se establecerá de forma automática sin pedir usuario y contraseña, puesto que la autenticación se llevará a cabo mediante el par de claves pública/privada generadas. Es muy importante que tomen en cuenta que, una vez realizadas las pruebas, deberán impedir que los usuarios con accesos autorizados de forma temporal puedan acceder nuevamente al host anfitrión como *root*.

Por otro lado, la operación de migración utiliza el rango de puertos 49152 a 49216, por lo que será necesario habilitarlos en el receptor de la migración.

Una vez establecida la conexión con el anfitrión de destino, bastará con realizar la migración a partir del *virt-manager*. Se deja como trabajo optativo la realización de la operación de migración mediante línea de ordenes (orden *virsh migrate*).

4 Checklist

Cuando finalice las tareas, los profesores de la asignatura realizarán las siguientes comprobaciones:

- ☐ Verificación de la migración de la máquina virtual **mvp4_etiqueta_de_equipo** empleando como espacio de almacenamiento compartido el proporcionado por el contenedor **`CONT_VOL_COMP.`**

5 Entrega

Se debe entregar un informe que contenga todos los pasos y órdenes que ha necesitado para realizar las tareas indicadas en esta práctica.

6 Rúbrica de evaluación

Los/as estudiantes deberán validar el trabajo realizado en esta práctica ante su profesor/a de prácticas, preferiblemente durante el horario de prácticas de

laboratorio. Será responsabilidad de los/as estudiantes concertar una cita con el/la profesor/a correspondiente si desean realizar la defensa en otro momento:

- Un estudiante obtendrá una calificación de 7 en esta práctica si realiza las tareas propuestas con el *virt-manager*, supera la validación de la misma y además entrega el informe que contiene las evidencias del trabajo realizado dentro del plazo estipulado.
- Un estudiante obtendrá una calificación de 8 en esta práctica si realiza las tareas propuestas con el *virt-manager* y con órdenes, supera la validación de la misma y además entrega el informe que contiene las evidencias del trabajo realizado dentro del plazo estipulado.
- Un estudiante obtendrá una calificación de 10 en esta práctica si realiza las tareas propuestas con el *virt-manager* y con órdenes (*virsh migrate*), supera la validación de la misma, entrega el informe que contiene las evidencias del trabajo realizado dentro del plazo estipulado y además, en dicho informe se explican los parámetros y el sentido de cada una de las órdenes que se emplean para desarrollar cada una de las tareas.

Por otro lado, si un estudiante concluye las tareas de esta práctica obligatoria de forma satisfactoria en las sesiones oficialmente programadas para su desarrollo por el equipo docente (3 sesiones en el caso de esta práctica), el estudiante obtendrá una calificación acumulable en el ítem de "Participación activa" que se explica en el proyecto docente de 0,143. La correcta culminación de las tareas será verificada por el profesor responsable en la última sesión de la práctica, no incluyéndose la realización del informe de la práctica.

Bibliografía

[1] Herrmann J, Zimmerman Y, Novich L, Parker D, Radvan S, Richardson T. *Red Hat Enterprise Linux 7. Virtualization Deployment and Administration Guide. Installing, configuring, and managing virtual machines on a RHEL physical machine*, Red Hat; 2019. Disponible en: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/virtualization_deployment_and_administration_guide/index

[accedido el 24/02/2025]

[2] Muehlfeld M, Gkioka I, Jahoda M, Heves J, Wadeley S, Huffman C. *Red Hat Enterprise Linux 7 Networking Guide. Configuring and managing networks, network interfaces, and network services in RHEL 7*, Red Hat; 2019. Disponible en: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/networking_guide/index

[accedido el 24/02/2025]

[3] Jahoda M, Fiala J, Wadeley S, Krátky R, Prpic M, Gkiova I, Capek T, Ruseva Y, Svoboda M. *Red Hat Enterprise Linux 7. Red Hat Enterprise Linux 7 Security Guide. Concepts and techniques to secure RHEL servers and workstations*, Red Hat; 2019. Disponible en:

https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/7/html/security_guide/index
[accedido el 24/02/2025]