10th International Scientific Conference
Technics, Informatics, and Education – TIE 2024
20-22 September 2024

Session: *Computer Sciences and Information Technology*
Professional paper
DOI: 10.46793/TIE24.144M

Issues During Data Migration

Mirko Marković[1] [0009-0006-5779-1490], Nikola Davidović[2] [0009-0004-6976-5535], Milan Vesković[3] [0000-0002-7668-4387], Srđan Nogo[2] [0009-0009-8423-5520] and Jelena Govedarica[2] [0009-0003-2625-3081]

[1] LANACO, Banja Luka, Republic of Srpska, Bosnia and Herzegovina
[2] University of East Sarajevo, Faculty of Electrical Engineering, East Sarajevo, Bosnia and Herzegovina
[3] Faculty of Technical Sciences Čačak/Department of Computer and Software Engineering, Čačak, Serbia
*mirko.markovic@lanaco.com

Abstract: *Virtualization represents one of the key technologies in modern computing, offering numerous advantages such as running multiple operating systems on a single computer, efficient resource utilization, process execution independence from specific hardware, and enhanced data security. This paper presents the process of virtual machine migration, including migration from one physical server to another without interrupting application operations. Additionally, it discusses some of the key benefits of virtual machines in various contexts, such as resource isolation, resource allocation flexibility, software testing, migration and backup, resource efficiency, and support for different operating systems. Through the analysis presented in this paper, the importance of virtualization as a fundamental technology in modern computing is highlighted, as well as the necessity of understanding the migration process and optimal use of virtual environments.*

Keywords: *virtualization, operating systems, resources, independence, security, virtual machine migration, efficiency, software testing, hardware resources.*

1. INTRODUCTION

Running multiple different operating systems on the same computer, more efficient resource utilization, independence of process execution from hardware, better protection and increased security, and the reduction of physical limitations are just some of the reasons why virtualization is becoming increasingly popular and indispensable in today's computing. Virtualization involves the abstract representation of computing resources (servers, memory, networks, applications, etc.) so that they can be used by different physical systems. Virtual machines are systems that contain their own operating system and applications, and they can run on different hosts, i.e., physical servers [1].

Virtual machine migration involves transferring it from one physical server to another without impacting its operation and the services it provides [2]. During the attempt to carry out this process, various issues and errors may occur, which can result in unsuccessful migration. Some of the most common ones are listed and briefly described below.

The research described in the paper examined how likely each error and problem was to happen when moving a machine from VMWare to Microsoft HyperV, two popular and widely used virtualization platforms nowadays. In addition to pinpoint the situations where errors could arise, the aim was to find solutions for them.

1.1. Cluster of two or more servers

Putting two or more servers into a cluster is the process of creating a highly available and redundant system. A cluster is a group of connected computers that work together as a single unit to ensure stability, increased availability, and fault tolerance [6].

Procedure for Creating a Cluster with Two Servers [6]:

- *Selection of Cluster Technology:* Choosing the appropriate cluster technology that is compatible with the needs and environment. For example, Windows Server offers clustering options, as do Linux systems with tools such as Pacemaker or Corosync.
- *Hardware and Software Preparation:* Provisioning appropriate hardware and network infrastructure. Servers in the cluster need to be connected via high-quality networking to facilitate fast communication between cluster members. Installing operating systems on each server and the required clustering software,

along with any additional tools specific to the clustering technology being used.

- *Network Configuration:* Setting up network settings so that servers in the cluster can communicate efficiently. This includes configuring static IP addresses, DNS settings, and, if necessary, additional network resources.
- *Configuration of Shared Resources:* Setting up shared resources that the cluster will use, such as shared storage that all cluster members can access.
- *Cluster Service Configuration:* Configure specific cluster services that are desired to be provided. This may include application services, web servers, databases, or other resources.
- *Testing and Optimization:* Testing the cluster to ensure it functions correctly. Conducting fault tolerance tests and simulating scenarios where one server becomes unavailable. Optimizing the cluster according to performance and availability requirements.
- *Maintenance and Management:* Regularly maintaining the cluster, upgrading software, and monitoring performance. Managing the cluster using available administration tools.

1.2. Advantages of virtual machines

Virtual machines offer a range of advantages in various contexts, including software development, testing, system maintenance, and efficient hardware resource utilization. [5]

Main advantages of virtual machines [5]:

- *Resource Isolation:* Virtual machines enable resource isolation, meaning each VM has its own separate workspace. This helps prevent conflicts between different applications and operating systems running on the same physical computer.
- *Resource Flexibility:* Virtual machines facilitate dynamic adjustment of resources for each VM according to needs. It's possible to increase or decrease allocated resources (CPU, RAM, storage) to a virtual machine without the need for physical hardware changes.
- *Software Testing and Development:* Development teams can use virtual machines to test software on different operating systems and configurations, facilitating issue identification and ensuring that the software functions correctly in diverse environments.
- *Migrations and Backups:* Virtual machines enable easy relocation and migration between different physical servers or data centers. Additionally, creating backups of virtual machines becomes easier and more efficient.
- *Resource Efficiency:* Through resource sharing, virtual machines enable more efficient utilization of physical hardware. Multiple virtual machines can operate on the same physical server, reducing the need to purchase additional physical machines.
- *Faster implementation:* Creating virtual machines is often faster than configuring physical computers. This means that new instances of operating systems can be deployed and put into use more quickly.
- *Security:* Virtual machines can provide an additional level of security through isolation. If one virtual machine experiences an issue or attack, other virtual machines on the same system can remain unaffected.
- Broad Support for Different Operating Systems: Virtual machines enable running various operating systems on the same physical hardware, which is useful in situations where supporting different platforms is necessary.

2. RESEARCH METHODOLOGY

2.1. Live migration of virtual machines

Live migration is the process of moving a virtual machine from one physical server to another without interrupting the operation of the virtual machine. This technique allows IT administrators to maintain the functionality of applications and services during the transfer process, ensuring that users do not notice the migration and that operations continue uninterrupted. Data transfer occurs over an Ethernet network using the TCP/IP protocol, connecting servers within a cluster. The live migration process involves copying the state of the virtual machine, including memory, CPU state, and network connections, from one physical server to another. This process requires careful management to ensure data consistency and minimize downtime. Various virtualization platforms such as VMware, Microsoft Hyper-V, or KVM/QEMU provide live migration as part of their functionality [5].

Benefits of live migration include [5]:

- *Minimal downtime:* End users do not notice the transfer, as applications and services on the virtual machine remain accessible throughout the entire process.
- *Resource Optimization:* Enables optimal use of resources by allowing virtual machines to dynamically adjust to changes in workload and resource demands.
- *Increased Availability:* Provides the ability to maintain physical servers or perform other administrative tasks without interrupting system and service operation.
- *Management Efficiency:* In addition to resource optimization, live migration facilitates the

administration and management of virtualized environments.

- *Load Balancing:* Enables dynamic load balancing between physical servers, improving overall system performance.

System load balancing, energy savings, resource allocation flexibility, and fault tolerance depend on live migration. From a process perspective, live migration has three different types (Figure 1) [7]:

1. Pre-copy,
2. Post-copy,
3. Hybridcopy.

Pre-copy live migration is a data migration strategy that involves preemptively copying data from the old to the new system before the final transfer. This strategy enables continuous synchronization of data between the old and new systems over a specified period, ensuring that data on the new system is up-to-date and ready for use. Once the data has been successfully pre-copied, the final transfer is executed quickly and without prolonged delays or interruptions in system operation. This method is often used to reduce downtime and minimize potential risks during system migration.

Post-copy live migration is a data migration strategy that involves copying data from the old system to the new system after the migration has already begun and when the new system is already live and operational. This strategy differs from pre-copy migration strategy, where data is copied to the new system before the migration begins. In post-copy live migration, the migration starts without fully completing the data copy. Instead, data copying continues after the migration has started, and data is transferred in real-time or in small batches to reduce system downtime. This strategy can be useful when reducing the time needed to complete migration or when it's impractical to stop the system for an extended period for full data copying before migration. However, there is a risk of data loss or data inconsistencies if the data copying process is not carefully managed.

Hybridcopy live migration refers to a data migration strategy that combines elements of multiple different migration approaches, including pre-copy and post-copy strategies, to optimize the migration process. This strategy may involve applying various data copying and synchronization techniques between the source and target systems, tailored to specific migration requirements and characteristics. For example, certain data or applications may be pre-copied to the target system before migration, while other data may be transferred live during or after migration. The goal of hybridcopy live migration is to minimize system downtime and reduce the risk of data loss, while providing flexibility and adaptability to the migration process according to specific organizational requirements and constraints. This strategy can be useful in situations where achieving a balance between migration speed, data integrity, and minimal disruptions to system operation is necessary.

2.2. Imaging

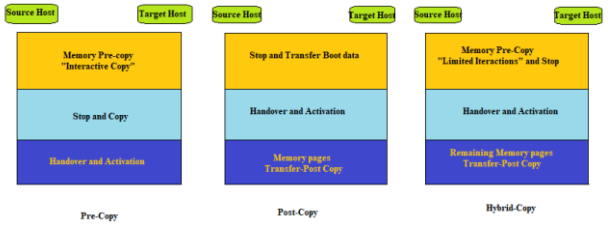

Figure 1. *Types of live migration*

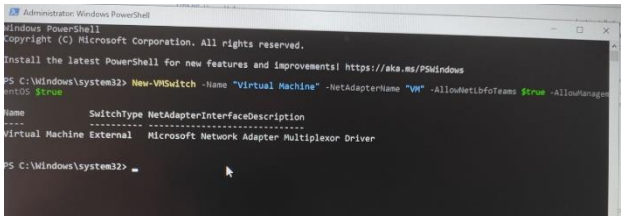

Figure 2. *Adding an External Virtual Switch through PowerShell*

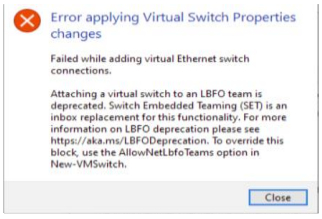

Figure 3. *Error when adding External Virtual Switch*

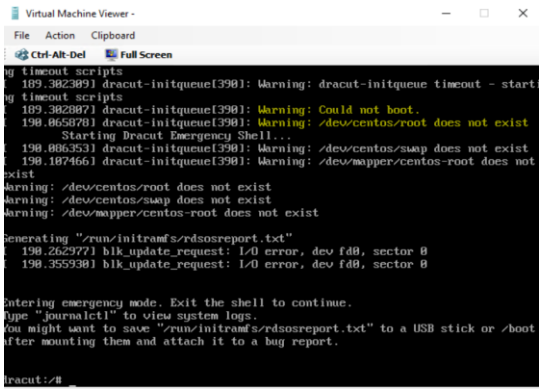

Figure 4. *Errors during the startup of the migrated virtual machine [9]*

3. RESULTS AND DISCUSSION

In the paper, a brief overview is provided on the concept of virtual machines, their migration, and the errors that may occur during this process. Additionally, measures are outlined that should be implemented before starting the migration to minimize the possibility of errors. The second part of the paper discusses the most common errors encountered in a specific example of migrating a

virtual machine from VMWare to the HyperV virtualization system, along with possible solutions.

3.1. Lack of isolation of virtual machine from physical components

The inability to migrate a production virtual machine (VM) from one server to another may occur as an error, not because the VM is designated for a specific server, but due to the presence of an attached CD/DVD within the VM itself.

3.2. Incorrect configuration of the virtual switch

For proper communication of a virtual machine with other machines, it is necessary to configure different types of virtual switches. During this process, errors can also occur. One of them, which may occur when trying to add an External Virtual Switch through PowerShell on Windows Server 2022 Datacenter (Figure 2), is shown in Figure 3.

3.3. Unsupported hardware

Unsupported hardware during virtual machine migration can lead to various issues and challenges. Possible problems during virtual machine migration related to unsupported hardware include:

- *Incompatibility with virtualization:* If the hardware on the desired (target) host or server is not compatible with the virtualization used on the source host, the migration may fail. This can involve different versions or types of virtualization technologies.
- *Lack of appropriate drivers:* If the desired hardware lacks suitable drivers for virtual machines, the operating system within the virtual environment will not function correctly. This can lead to performance issues or even the inability to boot the virtual machine. This manifests when the Hypervisor has its own drivers for the operating system running on the virtual machine. However, during the migration of the virtual machine, since the Hypervisor encounters different hardware, it needs to add drivers that correspond to this new hardware, essentially requiring an upgrade.
- *Different hardware configurations:* If the source and target hardware have different configurations, issues with resources such as CPU, RAM, or storage space may arise. This can affect the performance of the virtual machine and may require specific adjustments during migration.
- *Network issues:* The network configuration of the source and target systems may differ, leading to connectivity problems for the virtual machine after migration.
- *Unsupported hardware features:* If a virtual machine relies on specific hardware features that are not available on the target hardware, it can lead to issues. For example, if a certain type of graphics card is used that is not present on the desired hardware, visualization within the virtual machine may be compromised.

To avoid the previously described issues, careful planning of virtual machine migration is recommended, including checking compatibility between the source and target hardware, updating drivers, adjusting configurations, and testing migration before going into production. Using migration management tools like VMware vMotion or Microsoft Hyper-V Live Migration can also facilitate the process and reduce the risk of hardware-related issues during migration.

3.4. Lack of resources

Lack of resources during virtual machine migration can lead to various issues, including reduced performance, loss of availability, or even failed migration. Insufficiency in different types of resources can pose different challenges that need to be overcome for the virtual machine migration to be successful. Some of these challenges include:

- *Insufficient CPU Resources:* If the desired or target host lacks sufficient processor cores or processor speed to support demanding tasks of a virtual machine, this can result in significant performance degradation or system failure.
- *Insufficient RAM:* It's possible that the host to which the migration is being performed does not have enough RAM to support the operation of the virtual machine being migrated, leading to similar issues as in the previous case, potentially causing application freezes as well. Virtual machines with high memory demands may also likely fail to start altogether on the desired host or server.
- *Insufficient Storage Space:* If the desired host lacks sufficient free storage space to accommodate virtual disks, migration will be prevented. This can lead to operational interruptions or data loss.
- *Insufficient Network Bandwidth:* The lack of sufficient bandwidth between the source and destination hosts can slow down or prevent efficient virtual machine migration. This is particularly critical for live migration scenarios where data is continuously transferred during the migration process.
- *Resource Conflicts:* The host to which a virtual machine is being migrated may already host other virtual machines that are using its resources. Additionally, the host may be running various tasks that also consume resources, leading to competition for resources that can affect the performance of the new virtual machine.

To reduce the risk of resource shortages during virtual machine migration, it is recommended to:

- Careful resource planning, which involves analyzing the requirements of each virtual machine and ensuring sufficient resources are allocated on the desired host.
- Continuous monitoring of resources, i.e., tracking resource usage on the desired host over time to ensure there will be enough resources available for new virtual machines.
- Resource management automation, i.e., using tools for automating resource management to dynamically adjust resources according to the needs of virtual machines.
- Testing before migration, i.e., conducting test migrations to identify and resolve resource issues before moving to production.

3.5. VM (Linux OS) – from VMWare to HyperV

Two of today's most popular virtualization programs, VMWare and HyperV, are compatible, allowing virtual machines created with one to be migrated and run on the other. Certain conditions need to be met for this to work. One of them is that the virtual machine must have appropriate drivers for the program it is running on.

When migrating a Linux virtual machine from VMware to Hyper-V, various issues may arise, including [8]:

- *Virtual drivers:* Linux distributions often come with drivers optimized for VMware environments. When migrating to Hyper-V, different drivers may be required to ensure proper functionality of the virtual machine.
- *Network configuration:* Network configuration on Hyper-V may require adjustment, especially if different types of virtual network adapters are used or if specific settings from the VMware environment are incompatible with Hyper-V.
- *Virtual hardware conflicts:* Virtual hardware conflicts can arise if a Linux VM is configured to use specific features of the VMware platform that are not supported or implemented differently in the Hyper-V environment.
- *Performance loss:* While both Hyper-V and VMware are powerful virtualization platforms, performance can vary between them. Certain optimized procedures that work well in one environment may not deliver the same performance in the other.
- *Setting up tool integration:* Integration tools for Linux (such as Integration Services for Hyper-V) may be necessary to ensure proper functionality and improved performance of the virtual machine on the Hyper-V platform.

To overcome these issues, it is recommended [8]:

- Using migration tools that support virtual machine migration between VMware and Hyper-V platforms.
- Updating drivers and configuring the virtual machine to adapt to the Hyper-V environment.
- Testing the virtual machine post-migration to identify and resolve any issues that arise.
- Following guides and resources provided by Microsoft and Linux distributions for migrating virtual machines between different virtualization platforms.

3.6. Disabled Hyper-V network driver

If a virtual machine is created using VMWare and is being attempted to run on HyperV, it must have appropriate drivers for HyperV in addition to VMWare drivers [3].

Some of the most common driver issues that lead to the inability to start a virtual machine after migration include disabled drivers, changed or incorrect NIC MAC addresses, etc [4]. Figure 4 shows the appearance of errors on the console that are received if there is one of the previously listed problems.

The following describes possible ways to solve the above problems using the example of migrating a VMWare Linux virtual machine to HyperV.

The most common cause of issues when connecting a migrated virtual machine to the network is faulty operation of the network driver. To determine if there is indeed an issue with the network driver, access to the serial console on the virtual machine is necessary. For the serial console to function correctly, the operating system must be configured to read and write console messages to the serial port. Most Linux distributions have the serial console enabled and configured based on default settings. However, if this is not the case, the serial console needs to be enabled for the Linux VM in the /etc/inittab file to initiate the ttyS0 terminal.

During the mentioned procedure, sometimes it is necessary to instantiate a new getty (terminal management program) service on ttyS0, which can be done using the command systemctl start serial-getty@ttys0.service.

When it is determined that the network driver is disabled, it needs to be re-enabled using the serial console. Access the serial console of the virtual machine and log in with correct credentials, then switch to either the root or a user account with administrative privileges. The next step is to navigate to the /etc/modprobe.d directory and find the lines that disable the hv_netvsc driver. Use the command grep -nr "hv_netvsc" /etc/modprobe.d/ in the console to identify the file and their line numbers. Once found, modify the file by commenting out or deleting entries that disable the driver, typically in the form of install hv_netvsc /bin/true or blacklist hv_netvsc.

Finally, it is necessary to regenerate the initial RAM disk image for the currently loaded kernel and then restart the virtual machine [9].

The previously described solution can be implemented if serial console access is enabled. In case of network issues, serial console may not be available, necessitating an alternative method without network access, known as offline. In such cases, Azure serial console can be used for login. To access the OS disk content of the virtual machine (the disk with the installed operating system when the virtual machine was created) experiencing the issue, az vm repair commands are used. The filesystem part containing the necessary content is isolated using chroot instructions. Once successful access is achieved, locating the file containing the lines that disable the hv_netvsc driver and modifying it to re-enable the driver is done in the same manner as in the previous case. After making the changes, exit the chroot environment and regenerate the initial RAM disk image. The final step involves automatically replacing the OS disk with the virtual machine and restarting the system using the command az vm repair restore [9].

3.7. Incorrect NIC MAC address

Another possible reason for network service malfunction after migration is a changed or incorrect NIC (Network Interface Card) MAC address in the configuration, which can occur if the NIC was deleted, added by an administrator, or modified in the background. If the network driver is enabled and issues persist, checking the OS NIC configuration is necessary. Repairing the NIC MAC address can be done, similar to addressing a disabled driver, using either the serial console or offline methods [9].

The initial steps in troubleshooting using the serial console are the same as for a disabled driver. Therefore, access the console, log in with correct credentials, and switch to either the root or a user account with administrative privileges. Next, navigate to the /etc/cloud/cloud.cfg.d directory using the appropriate command, and open and modify the following files, depending on the Linux distribution [9]:

- 91-azure_datasource.cfg for RHEL.
- 90_dpkg.cfg for Debian and Ubuntu.

The parameter apply_network_config should be set to true, ensuring that the new MAC address will be preserved in the network configuration after system restart. If no value is specified for this parameter, true is assumed. If the parameter is set to false, it should be changed to true before proceeding to the next step. If it is absolutely necessary for apply_network_config to remain false and the desired configuration cannot be achieved using cloud services, the solution involves deleting the /var/lib/cloud/instance/obj.pkl file with the command # rm /var/lib/cloud/instance/obj.pkl. After making changes to the NIC configuration, the system needs to be restarted to ensure proper functioning of the network services [9].

A similar scenario as with offline driver enabling repeats when troubleshooting issues with NIC MAC address, especially when serial console access is not possible. Azure serial console and az vm repair commands are again used to access the OS disk content. The procedure for making changes in the network configuration or deleting the obj.pkl file is the same as in the previous case. Finally, the az vm repair restore command is used to automatically replace the OS disk with the original virtual machine and restart the system [9].

3.8. Inappropriate drivers for Hyper-V

Besides the network driver, the culprit for issues that occur when starting a virtual machine migrated to Hyper-V can be an incorrect or disabled operation of another driver. In this case, serial console cannot be used, so the only solution is to use offline access to re-enable the driver. After accessing the content of the OS disk where the issue exists, similar to offline resolution of network issues, switch to a chroot environment, navigate to the /etc/modprobe.d directory, and identify all lines that disable hv_utils, hv_vmbus, hv_storvsc, and hv_netvsc drivers. To find the required file and the line numbers of problematic entries, use the command:

```
egrep -nr "hv_utils|hv_vmbus|hv_storvsc|hv_
netvsc" /etc/modprobe.d/
```

Within the identified file, comment out or delete entries related to these drivers, typically in the form of blacklist driver_name or install driver_name /bin/false. After successfully making these changes, regenerate the initial RAM disk image for the currently loaded kernel and replace the OS disk used in the repair process with the original virtual machine using the command az vm repair restore. The final step, after making any configuration changes, is to restart the system, which is necessary in this case as well [4].

4. CONCLUSION

This paper examines a number of virtual machine migration topics, with an emphasis on the main benefits of virtualization and potential difficulties that could occur. Virtualization is an essential technological advancement in modern computing due to its many advantages, including hardware independence, data security, and effective resource utilization. It is possible to move from one physical server to another through the process of virtual machine migration, particularly live migration, which guarantees continuous availability by not disrupting application services.

Analyzed are common migration errors, such as resource shortages, unsupported hardware, network switch configuration, and resource isolation problems. For each of these errors,

recommendations and potential fixes are given in order to reduce risks and guarantee a successful migration execution.

Lastly, it's critical to remember that the successful deployment of virtualization and virtual machine migration depends heavily on thorough planning, testing, and the use of the right migration management tools. Knowing these procedures improves the general security and dependability of information systems in addition to helping to use IT resources more effectively.

Based on the experiences gained during the research process, new opportunities for improving the work emerge, focusing on the analysis of the obtained results applied to other types of virtualization systems and determining migration methods that will minimize the occurrence of errors, regardless of the type of virtualization system.

REFERENCES

[1] https://www.vmware.com/solutions/virtualization.html
[2] Chaudhary, P., Kumar, V., Joshi, M., Vaqur, M., Joshi, K., Pathak, A.K. (2023). Live Virtual Machine Migration Techniques in Cloud Computing: A Review. 2023 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, pp. 446-451, doi: 10.1109/AIC57670.2023.10263955.
[3] https://blogs.vmware.com/workstation/2020/05/vmware-workstation-now-supports-hyper-v mode.html
[4] https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/linux-hyperv-issue
[5] Agarwal, A., Shangruff R. (2012). Live Migration of Virtual Machines in Cloud. International Journal of Scientific and Research Publications, Volume 2, Issue 6, June 2012 ISSN 2250-3153
[6] https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/jj863389(v=ws.11)
[7] Elsaid, E.M., Abbas, M.H., Meinel, C. (2020). Live Migration Timing Optimization for VMware Environments using Machine Learning Techniques. CLOSER 2020 - 10th International Conference on Cloud Computing and Services Science
[8] Thota, S. (2019). VMWARE Virtualization-Physical to Virtual Migration. ISSN: 2231-2803
[9] https://learn.microsoft.com/en-us/answers/questions/171320/linux-on-hyper-v