Red Hat Infrastructure Migration Solution 1.2

Infrastructure Migration Solution Guide

Migrating from VMware to Red Hat Virtualization or Red Hat OpenStack Platform

Last Updated: 2020-03-11
Migrating from VMware to Red Hat Virtualization or Red Hat OpenStack Platform

Red Hat Migration Documentation Team
migration-docs@redhat.com
Abstract

This guide describes how to migrate VMware virtual machines to Red Hat Virtualization 4.3 or Red Hat OpenStack Platform 13 (or later), using Red Hat CloudForms 4.7.
Table of Contents

PREFACE ............................................................................................................. 5

PART I. MIGRATING FROM VMWARE TO RED HAT VIRTUALIZATION ............................. 6

CHAPTER 1. UNDERSTANDING THE MIGRATION .......................................................... 7
  1.1. UNDERSTANDING THE MIGRATION PROCESS .............................................. 7
  1.2. MIGRATION NETWORK REQUIREMENTS .................................................... 8

CHAPTER 2. PLANNING THE MIGRATION .................................................................. 9
  2.1. QUESTIONS TO ASK BEFORE MIGRATION .................................................. 9
    2.1.1. How long will the migration take? .......................................................... 9
    2.1.2. What operating systems can I migrate? ................................................. 10
    2.1.3. How many conversion hosts do I need? .............................................. 10
    2.1.4. Should I migrate my virtual machines with VDDK or SSH? ................. 10
  2.2. OPTIMIZING YOUR MIGRATION .................................................................... 10
    2.2.1. Preparing the migration environment .................................................. 11
    2.2.2. Deploying the conversion hosts ......................................................... 11
    2.2.3. Scheduling the migration .................................................................... 12
    2.2.4. Grouping virtual machines for migration ........................................... 12

CHAPTER 3. PREPARING THE MIGRATION ENVIRONMENT .......................................... 14
  3.1. PREPARING THE VMWARE ENVIRONMENT .................................................... 14
    3.1.1. Preparing the VMware network ............................................................ 14
    3.1.2. Preparing the VMware virtual machines ............................................. 14
    3.1.3. Configuring a VMware hypervisor for more than ten concurrent migrations 14
  3.2. PREPARING THE RED HAT VIRTUALIZATION ENVIRONMENT ..................... 15
    3.2.1. Prerequisites ........................................................................................ 15
    3.2.2. Installing and configuring Red Hat Virtualization ............................... 15
    3.2.3. Installing and configuring CloudForms .............................................. 16
  3.3. DEPLOYING THE RED HAT VIRTUALIZATION CONVERSION HOSTS ............ 17
    3.3.1. Downloading the VMware Virtual Disk Development Kit .................... 17
    3.3.2. Configuring the conversion hosts for VDDK transformation ............... 17
    3.3.3. Verifying the conversion hosts in a browser ....................................... 18

CHAPTER 4. MIGRATING THE VIRTUAL MACHINES .................................................... 20
  4.1. MIGRATION PREREQUISITES ....................................................................... 20
    4.1.1. Creating a CSV file to add virtual machines to the migration plan ....... 20
    4.1.2. Adding Ansible playbooks to CloudForms for premigration and postmigration tasks 21
    4.1.3. Creating a RHEL premigration playbook for RHEL/Linux virtual machines 21
  4.2. CREATING AN INFRASTRUCTURE MAPPING ............................................... 22
  4.3. CREATING AND RUNNING A MIGRATION PLAN ......................................... 24
    4.3.1. Scheduling a saved migration plan ..................................................... 26
    4.3.2. Viewing a migration plan in progress ................................................. 26
    4.3.3. Canceling a migration plan in progress .............................................. 27
    4.3.4. Retrying a failed migration plan ....................................................... 27
  4.4. CHANGING THE MAXIMUM NUMBER OF CONCURRENT MIGRATIONS ............ 27

CHAPTER 5. TROUBLESHOOTING ............................................................................. 29
  5.1. MIGRATION LOGS ....................................................................................... 29
    5.1.1. Downloading the conversion host and playbook logs ......................... 29
    5.1.2. Accessing the CloudForms migration log ......................................... 29
  5.2. COMMON ISSUES AND MISTAKES .............................................................. 30
    5.2.1. Infrastructure mapping errors ............................................................ 30
5.2.2. Migration plan errors
5.2.3. IP address errors
5.2.4. Environment configuration errors
5.3. KNOWN ISSUES

APPENDIX A. CONFIGURING THE RED HAT VIRTUALIZATION ENVIRONMENT FOR SSH TRANSFORMATION

A.1. CONFIGURING THE VMWARE HYPERVISORS FOR SSH TRANSFORMATION
A.2. REINSTALLING IPA-CLIENT
A.3. CONFIGURING THE CONVERSION HOSTS FOR SSH TRANSFORMATION
A.4. COPYING THE VMWARE SSH KEYS TO THE CONVERSION HOSTS
   A.4.1. Copying keys collected during VMware hypervisor configuration
   A.4.2. Copying keys collected with ssh-keyscan
A.5. CONFIGURING SECURE REMOTE LOGIN TO THE VMWARE HYPERVISORS

PART II. MIGRATING FROM VMWARE TO RED HAT OPENSTACK PLATFORM

CHAPTER 6. UNDERSTANDING THE MIGRATION
6.1. UNDERSTANDING THE MIGRATION PROCESS
6.2. MIGRATION NETWORK REQUIREMENTS

CHAPTER 7. PLANNING THE MIGRATION
7.1. QUESTIONS TO ASK BEFORE MIGRATION
   7.1.1. How long will the migration take?
   7.1.2. What operating systems can I migrate?
   7.1.3. How many conversion hosts do I need?
   7.1.4. Should I migrate my virtual machines with VDDK or SSH?
7.2. OPTIMIZING YOUR MIGRATION
   7.2.1. Preparing the migration environment
   7.2.2. Deploying the conversion hosts
   7.2.3. Scheduling the migration
   7.2.4. Grouping virtual machines for migration

CHAPTER 8. PREPARING THE MIGRATION ENVIRONMENT
8.1. PREPARING THE VMWARE ENVIRONMENT
   8.1.1. Preparing the VMware network
   8.1.2. Preparing the VMware virtual machines
   8.1.3. Configuring a VMware hypervisor for more than ten concurrent migrations
8.2. PREPARING THE RED HAT OPENSTACK PLATFORM ENVIRONMENT
   8.2.1. Prerequisites
   8.2.2. Installing and configuring Red Hat OpenStack Platform 13 or later
   8.2.3. Installing and configuring CloudForms
8.3. DEPLOYING THE RED HAT OPENSTACK PLATFORM CONVERSION HOSTS
   8.3.1. Creating the Red Hat OpenStack Platform conversion hosts
   8.3.2. Downloading the VMware Virtual Disk Development Kit
   8.3.3. Configuring the conversion hosts for VDDK transformation
   8.3.4. Verifying the conversion hosts in a browser

CHAPTER 9. MIGRATING THE VIRTUAL MACHINES
9.1. MIGRATION PREREQUISITES
   9.1.1. Creating a CSV file to add virtual machines to the migration plan
   9.1.2. Adding Ansible playbooks to CloudForms for premigration and postmigration tasks
   9.1.3. Creating a RHEL premigration playbook for RHEL/Linux virtual machines
9.2. CREATING AN INFRASTRUCTURE MAPPING
9.3. CREATING AND RUNNING A MIGRATION PLAN
9.3.1. Scheduling a saved migration plan
9.3.2. Viewing a migration plan in progress
9.3.3. Canceling a migration plan in progress
9.3.4. Retrying a failed migration plan
9.4. CHANGING THE MAXIMUM NUMBER OF CONCURRENT MIGRATIONS

CHAPTER 10. TROUBLESHOOTING

10.1. MIGRATION LOGS
   10.1.1. Downloading the conversion host and playbook logs
   10.1.2. Accessing the CloudForms migration log
10.2. COMMON ISSUES AND MISTAKES
   10.2.1. Infrastructure mapping errors
   10.2.2. Migration plan errors
   10.2.3. IP address errors
   10.2.4. Environment configuration errors
10.3. KNOWN ISSUES

APPENDIX B. CONFIGURING THE RED HAT OPENSTACK PLATFORM ENVIRONMENT FOR SSH TRANSFORMATION

B.1. CONFIGURING THE VMWARE HYPERVISORS FOR SSH TRANSFORMATION
B.2. CONFIGURING THE CONVERSION HOSTS FOR SSH TRANSFORMATION
B.3. COPYING THE VMWARE SSH KEYS TO THE CONVERSION HOSTS
   B.3.1. Copying keys collected during VMware hypervisor configuration
   B.3.2. Copying keys collected with ssh-keyscan
Red Hat Infrastructure Migration Solution (IMS) 1.2 enables you to migrate virtual machines from VMware 6.0 (or later) to Red Hat Virtualization or Red Hat OpenStack Platform, using Red Hat CloudForms:

**Red Hat Virtualization 4.3**

Red Hat Virtualization provides a virtualization platform built on Red Hat Enterprise Linux. You can manage your virtual infrastructure, including hosts, virtual machines, networks, storage, and users, from a centralized graphical user interface or with a REST API. See Red Hat Virtualization 4.3 documentation for more information.

See Part I, “Migrating from VMware to Red Hat Virtualization”.

**Red Hat OpenStack Platform 13 (or later)**

Red Hat OpenStack Platform provides a scaleable, fault-tolerant, private or public cloud based on Red Hat Enterprise Linux. See Red Hat OpenStack Platform documentation for more information.

See Part II, “Migrating from VMware to Red Hat OpenStack Platform”.

**Red Hat CloudForms 4.7.6 or later**

Red Hat CloudForms is the environment in which you perform the migration. Red Hat CloudForms is a unified set of management tools for use across virtualized, private cloud, and public cloud platforms. See Red Hat CloudForms 4.7 documentation for more information.
PART I. MIGRATING FROM VMWARE TO RED HAT VIRTUALIZATION

This guide describes how to plan your migration, to prepare the VMware source and Red Hat target environments, and to migrate the virtual machines.
1.1. UNDERSTANDING THE MIGRATION PROCESS

This workflow describes the process of migrating VMware virtual machines to Red Hat Virtualization.

**Figure 1.1. VMware to Red Hat Virtualization migration workflow**

1. You create and run a migration plan in CloudForms.
2. CloudForms uses the migration plan to locate the source virtual machines.
3. CloudForms captures the ESXi host fingerprint for authentication during the virtual machine conversion process.
4. Using the attributes defined for the Red Hat Virtualization environment, CloudForms initiates communication with the conversion hosts (Red Hat Virtualization hosts with `virt-v2v` and `virt-v2v-wrapper` installed).
5. `virt-v2v-wrapper` connects to the source datastore through the ESXi host. `virt-v2v` streams the source disks to the target data domain and converts the source disks.
**virt-v2v-wrapper** creates a target Red Hat Virtualization virtual machine, using the source virtual machine’s metadata in order to maintain its attributes (tags, power state, MAC address, CPU count, memory, disks, and virtual machine name) after migration.

**virt-v2v** attaches the converted disks to the Red Hat Virtualization virtual machine. (The virtual machine’s power state is the same as the source virtual machine’s power state.)

The migration process is complete and the migration plan’s status is displayed in CloudForms.

### 1.2. MIGRATION NETWORK REQUIREMENTS

The network communication between the VMware source environment, the Red Hat target environment, the conversion hosts, and CloudForms must be uninterrupted and reliable.

The firewall rules must enable the following ports for migration.

**Table 1.1. Firewall rules for migration**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>CloudForms</td>
<td>Conversion hosts</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>CloudForms</td>
<td>RHV Manager</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>CloudForms</td>
<td>VMware ESXi hosts</td>
</tr>
<tr>
<td>902</td>
<td>TCP</td>
<td>CloudForms</td>
<td>VMware ESXi hosts</td>
</tr>
<tr>
<td>902</td>
<td>TCP</td>
<td>Conversion hosts</td>
<td>VMware ESXi hosts</td>
</tr>
<tr>
<td>5480</td>
<td>TCP</td>
<td>Conversion hosts</td>
<td>VMware vCenter</td>
</tr>
</tbody>
</table>
CHAPTER 2. PLANNING THE MIGRATION

During the planning phase, you will formulate a specific migration goal, for example, "I want to migrate 2000 virtual machines, with 200 TB of data, in less than 6 months".

This section provides guidelines for planning your migration.

2.1. QUESTIONS TO ASK BEFORE MIGRATION

The following questions can help you to estimate the resources and time required for migration.

What am I migrating?

- Identify the VMware virtual machines that you will be migrating.

What am I missing?

- Identify resource gaps, such as bandwidth, storage, licenses, or a suitable maintenance window, before you begin the migration.

What is the maximum number of disks or virtual machines that I can migrate?

- There is no maximum number of disks or virtual machines that you can migrate. However, you may not want to migrate all your virtual machines at the same time, in order to minimize the impact on your users.

IMPORTANT

If you exceed the capabilities of your environment, the migration will fail. This situation could affect existing applications running on virtual machines attached to the network and storage.

What impact will the migration have on my users?

- Assess the effects the migration may have on a production environment. It may be possible to migrate your applications in phases, without downtime at the application layer, if the applications are distributed in a high-availability architecture.

- Check whether users will lose access to critical applications.

2.1.1. How long will the migration take?

There is no formula to estimate how long the actual migration will take. Migration speed is determined by your hardware, network speed, and other factors.

The following example is provided as a guide:

Example 2.1. Migration to Red Hat Virtualization 4.3, with Smart Zero Write

Duration: 55 minutes
Speed: 603 MBps
Environment:
- 20 virtual machines with 100 GB disks (66 GB usage)
- Two conversion hosts (24 CPUs each), with a maximum of ten concurrent migrations each
- SSD storage
- iSCSI interface between VMware hosts and storage
- Fiber Channel interface with multipath access between Red Hat hosts and storage
- 10 GbE NICs

2.1.2. What operating systems can I migrate?
You can migrate any guest operating system that is certified and supported.
See Certified Guest Operating Systems in Red Hat OpenStack Platform and Red Hat Virtualization.

2.1.3. How many conversion hosts do I need?
The number of conversion hosts you create depends on the size of your migration. All the virtual machines in a migration plan are migrated at the same time, in parallel. The number of virtual machines that you can migrate simultaneously depends on your infrastructure capabilities. Each migration requires a certain amount of network bandwidth, I/O throughput, and processing power for the conversion process.

Multiple conversion hosts provide load-balancing and better performance, even for small migrations.

Conversion hosts are limited to a maximum of ten concurrent migrations, unless you change the default values.

You should test your environment thoroughly before the migration to determine how many migrations it can support without negative effects, for example, five conversion hosts, each running ten concurrent migrations.

2.1.4. Should I migrate my virtual machines with VDDK or SSH?
You can migrate your virtual machines with either the VMware Virtual Disk Development Kit (VDDK) or SSH. VDDK is the default because it is much faster than SSH and easier to configure.

VDDK is limited to 20 concurrent migrations per conversion host, because of network limitations, and 10 concurrent migrations per VMware hypervisor, unless you increase the hypervisor’s NFC service memory.

If you cannot use VDDK, SSH is a fallback option.

2.2. OPTIMIZING YOUR MIGRATION
You can minimize the impact of the migration on your environment and improve performance.

For details on performance-related configurations, see Performance recommendations for migrating from VMware to Red Hat Virtualization or Red Hat OpenStack Platform with IMS.
2.2.1. Preparing the migration environment

You can configure the VMware and Red Hat environments to optimize your migration.

**VMware environment**

You can improve performance with the following configurations:

- Extend the VMware VM network to the Red Hat environment.
- Ensure that the VMware network provides high throughput. VMware and Red Hat hosts often have multiple network interfaces. By default, the conversion hosts use the VMware hosts’ admin interface to import VMs. Configure your routing for the fastest possible connection between the Red Hat and VMware environment. You can use host routes or IP table filtering to control the traffic flow.
- Ensure that the VMware network does not affect production machines, for example, by using a backup network to avoid overload.
- Divide the VMware virtual machines equally between two VMware hosts, if possible.
- Remove unnecessary data from the VMware disks.

**Red Hat environment**

You can improve performance with the following configurations:

- Update your Red Hat environment to the latest z-stream release and install required patches.
- Use fast, full SSD storage.
- Ensure that the network connection between the bare metal hosts and storage is at least 10 GbE.
- Use Fibre Channel interfaces between the hosts and storage.
- Configure multipath access between the hosts and storage.

2.2.2. Deploying the conversion hosts

You can improve performance with the following conversion host configurations:

- Configure midrange or high-end machines, with at least 10 GB of available RAM and 4 CPUs, as conversion hosts. If you increase the maximum number of concurrent migrations beyond 10 (up to 20 concurrent migrations), add 1 GB RAM for each additional migration.

**NOTE**

If you increase the maximum number of concurrent migrations, you must perform test migrations to assess the capabilities of your environment’s infrastructure and to ensure that the actual migration does not fail.

- Enable high performance and disable power-saving in the BIOS settings of the bare metal hosts.
- Ensure that the conversion host is not hosting virtual machines with heavy read/write workloads during the migration.

- Ensure that virtual machines on the conversion host are idle during the migration process. Their presence will not affect migration performance.

- Deploy multiple conversion hosts (up to five) for load-balancing and improved performance. The virtual machines in a migration plan are automatically distributed among the conversion hosts. This decreases the load on the conversion hosts and allows you to increase the concurrent migrations beyond the limits of a single conversion host.

### 2.2.3. Scheduling the migration

You can improve performance and minimize the impact on your users by scheduling the migration carefully:

- Prepare your users for downtime. Currently, IMS supports only cold migration. Virtual machines are powered off gracefully as part of the migration process.

- Stagger the migration schedules.

- Move critical applications during maintenance windows.

- Schedule the migration when storage input/output usage is low.

- Create multiple migration plans for finer control.

### 2.2.4. Grouping virtual machines for migration

You can improve performance and minimize the impact on your users by creating migration groups of virtual machines:

- Create migration groups for your virtual machines, so that you are not migrating all of them at the same time.

- Migrate virtual machines as a group, rather than individually. You can deploy up to 5 conversion hosts, with each host migrating up to 20 virtual machines concurrently. **These limits should not be exceeded.**

- Consider the following questions when creating migration groups:
  - How are the virtual machines grouped now?
  - Which virtual machines should be migrated together?
  - Which workloads or linked applications should be migrated together?
  - What applications must remain available?

- Consider which parts of the workload to migrate first:
  - Databases
  - Applications
  - Web servers
- Load balancers
CHAPTER 3. PREPARING THE MIGRATION ENVIRONMENT

You must prepare the VMware source and Red Hat Virtualization target environments for migration.

The virtual disks are converted with the VMware Virtual Disk Development Kit (VDDK). If you cannot use VDDK, SSH transformation is a fallback option.

3.1. PREPARING THE VMWARE ENVIRONMENT

You must prepare the VMware network and virtual machines for migration.

If you are performing more than ten concurrent migrations from a single VMware hypervisor, you must configure the hypervisor.

3.1.1. Preparing the VMware network

Extend the VMware network to your Red Hat environment.

**IMPORTANT**
- The network configuration must not be changed in any way during the migration.
- IP addresses, VLANs, and other network configuration must not be changed before or after migration because the conversion process preserves the source virtual machine MAC addresses.

3.1.2. Preparing the VMware virtual machines

Perform the following steps on each VMware virtual machine that you are migrating:

1. Install VMware Tools to capture IP addresses.
   To download and install VMware Tools, see [VMware Workstation 5.0: Installing VMware Tools](#).

2. Unmount mounted ISO/CDROM disks.

3. Ensure that each NIC has no more than one IPv4 and/or one IPv6 address.

4. Ensure that the virtual machine names contain only upper- or lower-case letters, numbers, underscores (_), hyphens (-), or periods (.)

   **NOTE**
   International characters and spaces are not permitted.

5. Ensure that the virtual machine names do not duplicate names of virtual machines in the Red Hat Virtualization environment.

3.1.3. Configuring a VMware hypervisor for more than ten concurrent migrations

If you are performing more than ten concurrent migrations from a VMware hypervisor using VDDK transformation, the migration will fail because the hypervisor’s NFC service memory buffer is limited to ten parallel connections. See [VMware Virtual Disk Programming Guide NFC session connection limits](#) and [Virt-v2v. VDDK: ESXi NFC service memory limits](#) for details.
You can increase the hypervisor’s NFC service memory to enable additional connections for migrations.

**Procedure**

1. Log in to a VMware hypervisor.
2. Change the value of `maxMemory` to 1000000000 in `/etc/vmware/hostd/config.xml`:
   ```xml
   <nfcsvc>
     <path>libnfcsvc.so</path>
     <enabled>true</enabled>
     <maxMemory>1000000000</maxMemory>
     <maxStreamMemory>10485760</maxStreamMemory>
   </nfcsvc>
   ```
3. Restart `hostd`:
   ```
   # /etc/init.d/hostd restart
   
   You do not need to reboot the VMware hypervisor.
   ```

### 3.2. PREPARING THE RED HAT VIRTUALIZATION ENVIRONMENT

You must install and configure Red Hat Virtualization and CloudForms and deploy the conversion hosts.

#### 3.2.1. Prerequisites

Ensure that the following prerequisites are met in your Red Hat environment:

1. Set the BIOS settings of the physical hosts for optimal performance, rather than power-saving, according to the vendor’s recommendations.
2. Disable CPU enhanced halt (CIE) in the BIOS settings, if applicable.
3. Check your software versions for compatibility.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>Red Hat Virtualization</td>
<td>4.3.4 (or later)</td>
</tr>
<tr>
<td>Red Hat CloudForms</td>
<td>4.7.6 (or later), with the CFME 5.10.5 (or later) virtual appliance</td>
</tr>
</tbody>
</table>

#### 3.2.2. Installing and configuring Red Hat Virtualization

You must install and configure Red Hat Virtualization.

**Procedure**

1. Install Red Hat Virtualization Manager 4.3.4.
2. Install Red Hat Virtualization Host 4.3.4 or Red Hat Enterprise Linux 7.6 on physical hosts.

**NOTE**

Some of these hosts will be deployed as conversion hosts. The number of conversion hosts depends on your migration size and infrastructure capabilities.

3. Create and attach data and ISO storage domains to the data center.

**NOTE**

IMS only supports shared storage, such as NFS, iSCSI, or FCP. Local storage is not supported. Although the ISO storage domain has been deprecated, it is required for migration.

4. Upload the VirtIO and RHV Guest Tools image files to the ISO storage domain. The VirtIO file name must include the version number (virtio-win-version.iso). The guest tools are required for migrating Windows virtual machines.

5. Optionally, you can create a MAC address pool that includes the MAC addresses of the VMware virtual machines to be migrated.

**IMPORTANT**

If the Red Hat Virtualization MAC address pool range overlaps the VMware MAC address range, you must ensure that the MAC addresses of the migrating virtual machines do not duplicate those of existing virtual machines. Otherwise, the migration will fail.

If you do not create a MAC address pool, the migrated virtual machines will not have MAC addresses in the same range as virtual machines created in Red Hat Virtualization.

### 3.2.3. Installing and configuring CloudForms

You must install and configure CloudForms.

Removing or changing a provider in CloudForms, after creating infrastructure mappings or migration plans, will cause migration errors.

**IMPORTANT**

CFME 5.10.4 does not support migration.

**Procedure**

1. Install Red Hat CloudForms 4.7.6 (or later) on the Manager machine.

2. Add VMware to CloudForms as an infrastructure provider.

3. Add Red Hat Virtualization to CloudForms as an infrastructure provider.
3.3. DEPLOYING THE RED HAT VIRTUALIZATION CONVERSION HOSTS

Deploying the conversion hosts involves the following tasks:

1. Downloading the VMware Virtual Disk Development Kit (VDDK)
2. Configuring the conversion hosts in CloudForms
3. Verifying the conversion hosts in a browser

3.3.1. Downloading the VMware Virtual Disk Development Kit

You must download the VMware Virtual Disk Development Kit (VDDK).

Prerequisites

- VMware account credentials for downloading the VDDK SDK

Procedure

1. In a browser, navigate to VMware Documentation.
2. Click VMware SDK & API Product Documentation → VMware Virtual Disk Development Kit (VDDK).
3. Select the latest VDDK release.
4. Click Download SDKs to download the .tar.gz VDDK archive file.
5. Save the VDDK archive file in an HTTP-accessible location and record its path.

3.3.2. Configuring the conversion hosts for VDDK transformation

Prerequisites

- If the Red Hat Virtualization provider has been active for a while, verify that each host has valid subscriptions and repositories by logging in using SSH and running the following commands:

  ```bash
  # subscription-manager list --consumed
  # yum repolist
  ```

- If a host has an SSH private key in /var/lib/vdsm/.ssh/id_rsa, delete the key manually before configuring the host. Conversion host configuration does not overwrite existing keys.

Procedure

1. In CloudForms, click Compute → Migration → Migration Settings.
2. In the Conversion Hosts tab, click Configure Conversion Host. The Configure Conversion Host wizard is displayed.
3. In the **Location** screen, add the provider details:

   a. Select a **Provider Type**.
   
   b. Select a **Provider**.
   
   c. Select a **Cluster** and click **Next**.

4. In the **Host(s)** screen, select one or more hosts from the dropdown list and click **Next**.

5. In the **Authentication** screen, add the conversion hosts' SSH key and the transformation method:

   a. Click **Browse** to browse to the SSH private key or paste it in the **Conversion host SSH private key** field.

      The Manager deploys a private SSH key on the conversion hosts in order to send commands and run playbooks. The default key file is `/etc/pki/ovirt-engine/keys/engine_id_rsa` on the Manager machine.

   b. Select **VDDK** as the **Transformation method**.

   c. Enter the path of the VDDK package in the **VDDK library path** field.

   d. Click **Configure**.

6. In the **Results** screen, wait for the conversion host configuration to finish and click **Close**.

   The configured conversion hosts and status information, including error messages, appear in the **Configured Conversion Hosts** list.
If an error occurs, you can download a host’s log by clicking the More Actions icon (…) and selecting Download Log.

You can click Retry if the conversion host configuration failed for reasons unconnected with your environment.

You can click Remove to remove the configuration from a configured conversion host.

3.3.3. Verifying the conversion hosts in a browser

You can verify your conversion hosts in a browser:

1. In the address bar of a browser, enter the following:

   https://<CloudForms_FQDN>/api/conversion_hosts

   Specify the FQDN of the CloudForms machine.

   A log-in screen is displayed.

2. Enter your CloudForms Username and Password and click Sign in.

   The conversion hosts and their IDs are displayed in JSON format in the output:

   ```json
   {
   "name":"conversion_hosts","count":3,"subcount":3,"pages":1,"resources":
   [{"href":"https://cloudforms.example.com/api/conversion_hosts/10000000000001"},
   {"href":"https://cloudforms.example.com/api/conversion_hosts/10000000000002"},
   {"href":"https://cloudforms.example.com/api/conversion_hosts/10000000000003"}],"actions":
   [{"name":"create","method":"post","href":"https://cloudforms.example.com/api/conversion_hosts"},
   {"name":"edit","method":"post","href":"https://cloudforms.example.com/api/conversion_hosts"},
   {"name":"delete","method":"post","href":"https://cloudforms.example.com/api/conversion_hosts"}],"links":{
   ```
CHAPTER 4. MIGRATING THE VIRTUAL MACHINES

Migrating the virtual machines involves the following steps:

1. Checking for migration conditions that have prerequisites
2. Creating an infrastructure mapping to map the resources of your source and target environments
3. Creating and running a migration plan in CloudForms

Optionally, you can change the maximum number of concurrent migrations for conversion hosts or providers to control the migration process.

4.1. MIGRATION PREREQUISITES

Check your migration for the following conditions, which have prerequisites:

- If you are migrating previously migrated virtual machines, you must add previously migrated machines to the migration plan with a CSV file. A CSV file is also recommended for large migrations.
- If you are using Ansible playbooks for premigration/postmigration tasks, you must create an Ansible repository and add credentials and playbooks to CloudForms.
- If you are migrating virtual machines running RHEL or other Linux operating system, you must create a RHEL premigration playbook to preserve IP addresses. You will select this playbook when you create a migration plan.

4.1.1. Creating a CSV file to add virtual machines to the migration plan

If you are migrating virtual machines that were migrated in the past, you should create a CSV file to add the virtual machines to the migration plan, because the migration plan cannot discover them automatically.

NOTE

A CSV file is recommended for large migrations because it is faster than manually selecting individual virtual machines.

Table 4.1. CSV file fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Virtual machine name. Required</td>
</tr>
<tr>
<td>Host</td>
<td>Optional. Only required if virtual machines have identical Name fields.</td>
</tr>
<tr>
<td>Provider</td>
<td>Optional. Only required if virtual machines have identical Name and Host fields.</td>
</tr>
</tbody>
</table>

CSV file example
4.1.2. Adding Ansible playbooks to CloudForms for premigration and postmigration tasks

You can add Ansible playbooks to CloudForms to perform automated premigration and postmigration tasks on specific virtual machines, for example:

- Removing webservers from a load-balancing pool before migration and returning them to the pool after migration
- Preserving the IP addresses of VMware virtual machines running RHEL or other Linux operating systems

Procedure

1. Log in to the CloudForms user interface.
2. Enable the Embedded Ansible server role.
3. Add an Ansible playbook repository.
4. Add the credentials of each virtual machine that you are migrating.
5. Add your playbook as an Ansible service catalog item.

You will select the playbooks and the virtual machines on which they run in the Advanced Options screen when you create the migration plan.

4.1.3. Creating a RHEL premigration playbook for RHEL/Linux virtual machines

If you are migrating virtual machines running RHEL or other Linux operating systems, you must create and run a RHEL premigration playbook to call the Ansible ims.rhel_premigration role.

The ims.rhel_premigration role ensures that the virtual machine IP addresses are accessible after migration.

Prerequisites

- The rhel-<version>-server-rpms repository must be enabled for the source virtual machines. If you have disabled it, you can re-enable it in the RHEL premigration playbook.

Procedure

1. Install the ims.rhel_premigration role with Ansible Galaxy.
2. Create a RHEL premigration playbook according to the following example:

```yaml
---
- hosts: to_migrate
  vars:
```
Specify the configuration parameters for your environment.

Passwords and other sensitive information should be encrypted with Ansible vault.

You will add this playbook when you create your migration plan.

4.2. CREATING AN INFRASTRUCTURE MAPPING

The infrastructure mapping maps the resources of your VMware source and Red Hat target environments.

**IMPORTANT**

If you add or remove providers or provider objects from an infrastructure mapping, the mapping will have missing resource errors. You must delete the infrastructure mapping and create a new one.

**Procedure**

1. Click **Compute → Migration → Infrastructure Mappings**.

2. Click **Create Infrastructure Mapping**. The **Create Infrastructure Mapping** wizard is displayed.
3. In the **General** screen, add the infrastructure mapping details:
   a. Enter the infrastructure mapping **Name** and (optional) **Description**.
   b. Select the **Target Provider**.
   c. Click **Next**.

4. In the **Map Compute** screen, map the source and target clusters:
   a. Select a **Source Provider \ Datacenter \ Cluster** and a **Target Provider \ Datacenter \ Cluster**.
      If the target cluster does not contain a conversion host, a warning icon (⚠️) appears. You can create and save an infrastructure mapping, but you must configure the conversion hosts before running a migration plan.
   b. Click **Add Mapping**. You can map additional clusters.
   c. Click **Next**.

5. In the **Map Storage** screen, map the source and target storage:
   a. Select a **Source Provider \ Datacenter \ Datastore** and **Target Datastores**.
   b. Click **Add Mapping**. You can map additional datastores.
   c. Click **Next**.
6. In the Map Networks screen, map the source and target networks:
   a. Select a source cluster from the drop-down list.
   b. Select one or more networks from Source Provider \ Datacenter \ Network and Target Project \ Network.
   c. Click Add Mapping. You can map the networks of additional source clusters.
   d. Click Create.

7. In the Results screen, click Close. The infrastructure mapping is saved in Compute → Migration → Infrastructure Mappings.

You can click an infrastructure mapping element to view its details:

Infrastructure Mappings list

4.3. CREATING AND RUNNING A MIGRATION PLAN

Before attempting a large migration, you should perform several test migrations with different maximum numbers of concurrent migrations for your conversion hosts or providers. This will enable you to assess the capabilities of your environment’s infrastructure.

NOTE

A CSV file is optional, but recommended, for large migrations because it is faster than manually selecting each virtual machine.

Procedure

1. Click Compute → Migration → Migration Plans.

2. Click Create Migration Plan. The Create Migration Plan wizard is displayed.
3. In the General screen, add the details of the migration plan:
   a. Select an infrastructure mapping from the drop-down list.
   b. Enter the migration plan Name and (optional) Description.
   c. Select a virtual machine discovery method:
      - Choose from a list of VMs discovered in the selected infrastructure mapping
        If the virtual machines cannot be discovered, check that the source datastores and
        networks in the infrastructure mapping are correct.
      - Import a CSV file with a list of VMs to be migrated
        A CSV file is required for previously migrated source virtual machines and
        recommended for large migrations.
   d. Click Next.

4. In the VMs screen, select the virtual machines for migration:
   - If you selected Choose from a list of VMs discovered in the selected infrastructure
     mapping, select the virtual machines for migration.
     You can search for virtual machines by VM Name, Data Center, Cluster, and Folder.
   - If you selected Import a CSV file with a list of VMs to be migrated
     a. Click Import.
b. Browse to the CSV file and click **Open**. If the virtual machines cannot be added to the migration plan, check the CSV file format and fields for errors.

**NOTE**

If the **Create Migration Plan** wizard freezes, refresh the web page, check the CSV file for errors (for example, virtual machines with duplicate **Name** fields and no other fields to distinguish them), and create a new migration plan.

c. Click **Next**.

5. In the **Advanced Options** screen, select the playbook service options:

   a. Select a premigration and/or postmigration playbook service from the dropdown lists.

   b. Select the virtual machines on which to run the playbook services.

   c. Click **Next**.

6. In the **Schedule** screen, select a schedule option and click **Create**:

   - **Save migration plan to run later**
     The migration plan is saved in **Migration Plans Not Started** and will not run unless you **schedule** it or click **Migrate** to run the scheduled migration plan immediately.

   - **Start migration immediately**
     The migration plan may take some time to complete. Progress bars indicate the amount of transferred data, the number of migrated virtual machines, and the elapsed time. You can **view a migration plan’s progress** or **cancel a migration plan in progress**.

7. In the **Results** screen, click **Close**. When the migration plan has finished, click **Migration Plans Complete** to view the status of the migration plan. The completed migration plan shows the status of the migrated virtual machines.

In the migration plans list, you can click the **More Actions** icon ( ) to archive, edit, or delete a migration plan.

If a migration fails because of external circumstances (for example, power outage), you can **retry the migration plan**.

### 4.3.1. Scheduling a saved migration plan

To schedule a saved migration plan to run in the future:

1. Click **Migration Plans Not Started**

2. Click the **Schedule** button of a migration plan.

3. In the **Schedule Migration Plan** window, select a date and time and click **Schedule**. The plan’s status is **Migration Scheduled** with the date and time.

### 4.3.2. Viewing a migration plan in progress
To view the progress of a migration plan:

1. Click **Migration Plans in Progress**
2. Click a migration plan name to view its details, including the status of the migrating virtual machines.

**NOTE**

The counter in **Compute → Migration → Migration Plans** may be a few seconds ahead of the counter in the migration plan details view. This is because the **Migration Plans** counter displays the total time for running the migration plan, while the details counter displays the time for migrating the virtual machines.

### 4.3.3. Canceling a migration plan in progress

To cancel a migration plan in progress:

1. Click **Migration Plans in Progress**
2. Select a migration plan and click **Cancel Migration**.
3. Click **Cancel Migrations** to confirm the cancellation. The canceled migration appears in **Migration Plans Complete** with a red x indicating that the plan did not complete successfully.

### 4.3.4. Retrying a failed migration plan

To retry a migration plan that failed because of external circumstances (for example, power outage):

1. Delete all objects created by the failed migration plan:
   - Delete newly created virtual machines to avoid name conflicts with migrating VMware virtual machines.
   - Delete converted disks to free up space.
2. Click **Compute → Migration → Migration Plans**.
3. Click **Migration Plans Complete**.
4. Click the **Retry** button beside the failed migration plan.

### 4.4. Changing the Maximum Number of Concurrent Migrations

You can change the maximum number of concurrent migrations for conversion hosts or providers to control the impact of the migration process on your infrastructure.

The provider setting has priority over the conversion host setting. For example, if the maximum number of concurrent migrations is 20 for a provider and 3 for five conversion hosts, the maximum number of concurrent migrations is 20, not 15 (5 conversion hosts x 3 concurrent migrations per host).

An increase in the maximum number of concurrent migrations affects all migration plans immediately. Virtual machines that are queued to migrate will migrate in greater numbers.
A decrease maximum number of concurrent migrations affects only future migration plans. Migration plans that are in progress will use the limit that was set when the plan was created.

**CAUTION**

For VDDK transformation, the number of concurrent migrations must not exceed 20. Otherwise, network overload will cause the migration to fail.

**Changing the maximum number of concurrent migrations for all conversion hosts**

1. Log in to the CloudForms user interface.

2. Click **Compute → Migration → Migration Settings**.

3. In the **Migration Throttling** tab, select a value for **Maximum concurrent migrations per conversion host** or **Maximum concurrent migrations per provider** and click **Apply**. The value of **Maximum concurrent migrations per conversion host** is constrained so that it cannot be greater than **Maximum concurrent migrations per provider**.

**Changing the maximum number of concurrent migrations for a specific conversion host**

1. Log in to the conversion host using SSH.

2. Obtain the **conversion_host_id**:

```
# curl -sk -u <username>:<password> https://<CloudForms_FQDN>/api/conversion_hosts/
```

Specify the CloudForms FQDN.

3. Enter the following command:

```
# curl -sk -u <username>:<password> https://<CloudForms_FQDN>/api/conversion_hosts/<conversion_host_id> -X POST -d '{"action": "edit", "resource": {"max_concurrent_tasks": _15_}}'
```

Specify the CloudForms admin username and password. Specify the FQDN of the CloudForms machine. Specify the **conversion_host_id**. Specify the maximum number of concurrent migrations. The default is 10.
CHAPTER 5. TROUBLESHOOTING

You can review the migration logs, check common issues and mistakes, and known issues to troubleshoot a migration error.

5.1. MIGRATION LOGS

You can check the conversion host logs, playbook logs, and the CloudForms migration log to identify the cause of a migration error.

**IMPORTANT**

If you need to open a Red Hat Support call, you must submit both the migration (virt-v2v) log and virt-v2v-wrapper log for analysis.

5.1.1. Downloading the conversion host and playbook logs

You can download the conversion host and playbooks logs in CloudForms.

When disk migration starts, two logs are created in the conversion host:

- **virt-v2v**: Debug output from virt-v2v itself. This log tracks the core of the virtual machine migration process, including libguestfs traces and disk migration details.

- **virt-v2v-wrapper**: Log of the daemonizing wrapper for virt-v2v. This log traces the orchestration of the virtual machine conversion on the conversion host, including disk migration percentages and virt-v2v error reporting.

**Procedure**

1. Log in to the CloudForms user interface.
2. Click Compute → Migration → Migration Plans.
3. Click a completed migration plan to view its details.
4. Click Download Log of a virtual machine and select a log from the dropdown list:
   - **Premigration log** This option only appears if a premigration playbook is used.
   - **Migration log** The Migration log is the virt-v2v log.
   - **Virt-v2v-wrapper log**
   - **Postmigration log** This option only appears if a postmigration playbook is used.

5.1.2. Accessing the CloudForms migration log

This log traces the orchestration of the virtual machine migration in CloudForms.

**Procedure**

1. Log in to the CloudForms machine using SSH.
2. The migration log is /var/www/miq/vmdb/log/automation.log.
5.2. COMMON ISSUES AND MISTAKES

5.2.1. Infrastructure mapping errors

- **Networks missing, Datastores missing, and Clusters missing** error messages
  If you create an infrastructure mapping and then change a provider or refresh the Red Hat Virtualization hosts, the provider’s object IDs change. Delete the infrastructure mapping and create a new one.

5.2.2. Migration plan errors

- Virtual machines are being migrated for the first time and are not discovered by the migration plan
  Check that the source datastores and networks appear in the infrastructure mapping.

- Previously migrated virtual machines cannot be discovered by the migration plan
  Use a CSV file to add the virtual machines to the migration plan.

- Virtual machines cannot be added to the migration plan with a CSV file
  Check the CSV file format and fields. Create a new migration plan with the updated CSV file.

- **Create Migration Plan** wizard hangs while importing a CSV file
  Invalid CSV file (for example, virtual machines with a duplicate Name field and no Host/Provider field to distinguish them, or with a duplicate Name field and duplicate Host/Provider fields). Correct the CSV file, refresh the web page, and create a new migration plan.

- **Unable to migrate VMs because no conversion host was configured at the time of the attempted migration. See the product documentation for information on configuring conversion hosts.**
  You can create and save a migration plan whose infrastructure mapping does not contain conversion hosts, but you cannot run the migration plan without conversion hosts. Cancel the migration plan, create the conversion hosts, and run the migration plan again.

5.2.3. IP address errors

- IP address of a migrated RHEL (or other Linux-based operating system) virtual machine is not accessible
  You must create a RHEL premigration playbook and add it to the migration plan.

- Migrated virtual machine does not have an IP address
  You must install VMware Tools on the VMware virtual machine before migration.

5.2.4. Environment configuration errors

**VMware**

- A VMware virtual machine cannot be migrated if it has any of the following conditions:
  - Mounted ISO/CDROM disk
  - Invalid name, containing spaces or special characters
If you are performing more than ten concurrent migrations from a single VMware hypervisor, you must increase the hypervisor’s NFC service memory.

Red Hat Virtualization

- Name conflict
  VMware virtual machine has the same name as a Red Hat Virtualization virtual machine.

- MAC address conflict
  VMware virtual machine has the same MAC address as a Red Hat Virtualization virtual machine in a MAC address pool.

- Check that the conversion host does not have an existing private SSH key in /var/lib/vdsm/.ssh/id_rsa. Conversion host configuration does not overwrite old SSH keys. They must be deleted manually.

- SSH transformation only:
  - If you are using SSSD with single sign-on, you must reinstall `ipa-client` without OpenSSH.
  - Check that you enabled SSH access on the VMware hypervisors and correctly configured your conversion hosts for SSH transformation.

5.3. KNOWN ISSUES

The following are known issues:

- BZ#1726939: Run the preflight check of migration task before waiting for a conversion host.
  Currently, the preflight check that monitors the migration is performed after a conversion host is assigned to the task. As a result, the total volume of the Datastores reported in Migration Plans In Progress reflects the total volume of the virtual machines that are currently migrating, not the total volume of the migration plan. When all the virtual machines have started to migrate, the correct value of the total volume is displayed.
APPENDIX A. CONFIGURING THE RED HAT VIRTUALIZATION ENVIRONMENT FOR SSH TRANSFORMATION

You can configure your environment for SSH transformation if you cannot use VDDK.

NOTE

The default transformation method, VDDK, is much faster than SSH.

This configuration involves adding the following steps to Chapter 3, *Preparing the migration environment*:

Table A.1. Additional configuration for SSH transformation

<table>
<thead>
<tr>
<th>Section</th>
<th>Additional configuration for SSH transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>After Preparing the VMware environment</td>
<td>Go to Configuring the VMware hypervisors for SSH transformation</td>
</tr>
<tr>
<td></td>
<td>You can collect the SSH keys from the hypervisors at this time, if your security policies allow.</td>
</tr>
<tr>
<td></td>
<td>The private key of the SSH key pair that is generated in this step will be used in Configuring the conversion hosts for SSH transformation.</td>
</tr>
<tr>
<td>After Installing and configuring Red Hat Virtualization</td>
<td>If the conversion hosts are using SSSD with single sign-on, go to Reinstalling <em>ipa-client</em></td>
</tr>
<tr>
<td>Instead of Configuring the conversion hosts for VDDK transformation</td>
<td>Go to:</td>
</tr>
<tr>
<td></td>
<td>● Configuring the conversion hosts for SSH transformation</td>
</tr>
<tr>
<td></td>
<td>● Copying the VMware SSH keys to the conversion hosts</td>
</tr>
</tbody>
</table>

A.1. CONFIGURING THE VMWARE HYPERVERSORS FOR SSH TRANSFORMATION

For SSH transformation, you must enable SSH access and copy a public SSH key to each VMware hypervisor. The corresponding private key will be used to configure the conversion hosts.

IMPORTANT

A single SSH key pair is recommended because this key pair is used only for virtual machine conversion and it simplifies conversion host management.

If you wish to use a dedicated SSH key pair for each conversion host, you can copy the public key of each conversion host to all the VMware hypervisors.
**Procedure**

1. Enable SSH access on each VMware hypervisor. For instructions, navigate to VMware vSphere Documentation and enter **Enable ESXi Shell and SSH Access with the Direct Console User Interface** in the Search field. You can collect the SSH public keys of the VMware hypervisors at this stage, to copy to the conversion hosts.

2. Generate an SSH key pair without a passphrase:
   ```
   # ssh-keygen -N ''
   ```

3. Copy the public SSH key to `/etc/ssh/keys-root/authorized_keys` on each VMware hypervisor. You will use the private SSH key to configure the conversion hosts.

**A.2. REINSTALLING IPA-CLIENT**

If you are using SSH transformation and configuring your conversion hosts for SSSD with single sign-on, you must reinstall `ipa-client` without the OpenSSH client. Otherwise, SSH will fail for the `vdsm` user. See BZ#1544379: `ipa-client-install` changes system-wide SSH configuration for more information. This issue cannot be resolved by modifying the configuration file because the file is restored during upgrades.

**Procedure**

1. Log in to the Manager machine using SSH.

2. Uninstall `ipa-client`:
   ```
   # ipa-client-install --uninstall
   ```

3. Reinstall `ipa-client` without OpenSSH:
   ```
   # ipa-client-install --no-ssh
   ```

**A.3. CONFIGURING THE CONVERSION HOSTS FOR SSH TRANSFORMATION**

**Prerequisites**

- If the Red Hat Virtualization provider has been active for a while, verify that each host has valid subscriptions and repositories by logging in using SSH and running the following commands:
  ```
  # subscription-manager list --consumed
  # yum repolist
  ```

- If a host has an SSH private key in `/var/lib/vdsm/.ssh/id_rsa`, delete the key manually before configuring the host. Conversion host configuration does not overwrite existing keys.

**Procedure**

1. In CloudForms, click **Compute → Migration → Migration Settings**.
2. In the **Conversion Hosts** tab, click **Configure Conversion Host**. The **Configure Conversion Host** wizard is displayed.

3. In the **Location** screen, add the provider details:
   a. Select a **Provider Type**.
   b. Select a **Provider**.
   c. Select a **Cluster** and click **Next**.

4. In the **Host(s)** screen, select one or more hosts from the dropdown list and click **Next**.

5. In the **Authentication** screen, add the conversion hosts’ SSH key and the transformation method:
   a. Click **Browse** to browse to the SSH private key or paste it in the **Conversion host SSH private key** field.
      The Manager deploys a private SSH key on the conversion hosts in order to send commands and run playbooks. The default key file is `/etc/pki/ovirt-engine/keys/engine_id_rsa` on the Manager machine.
   b. Select **SSH** as the **Transformation method**.
   c. Click **Browse** to browse to the SSH private key you created for enabling SSH access on the VMware hypervisors or paste it in the **VMware hypervisors SSH private key** field.
   d. Click **Configure**.

6. In the **Results** screen, wait for the conversion host configuration to finish and click **Close**.
The configured conversion hosts and status information, including error messages, appear in the Configured Conversion Hosts list.

If an error occurs, you can download a host’s log by clicking the More Actions icon ( ) and selecting Download Log.

You can click Retry if the conversion host configuration failed for reasons unconnected with your environment.

You can click Remove to remove the configuration from a configured conversion host.

**A.4. COPYING THE VMWARE SSH KEYS TO THE CONVERSION HOSTS**

Copy the SSH public keys of the VMware hypervisors to the conversion hosts.

You can collect the VMware keys either when you configure the VMware hypervisors for SSH transformation or by using `ssh-keyscan`.

**A.4.1. Copying keys collected during VMware hypervisor configuration**

1. Copy the VMware keys to `/var/lib/vdsm/.ssh/known_hosts` on each conversion host.

2. Verify the SSH connection by connecting to each VMware hypervisor as `vdsm`:

   ```
   $ sudo -u vdsm ssh root@<Vmware_host_name>
   ```

   Specify the host name of your VMware hypervisor.

   If the SSH connection fails, check that the VMware hypervisor has SSH access enabled and that you copied the correct keys. Otherwise, all migrations from that hypervisor using SSH transformation will fail.

**A.4.2. Copying keys collected with ssh-keyscan**

You must run `ssh-keyscan` for each VMware hypervisor. Otherwise your conversion hosts will not have all the VMware hypervisor keys and the migration will fail.

Perform the following procedure on each conversion host:

1. Run `ssh-keyscan` for each VMware hypervisor and copy its public key to `known_hosts`, as in the following example:

   ```
   $ ssh-keyscan <Vmware_host_1_ip> > /var/lib/vdsm/.ssh/known_hosts
   $ ssh-keyscan <Vmware_host_2_ip> >> /var/lib/vdsm/.ssh/known_hosts
   $ ssh-keyscan <Vmware_host_3_ip> >> /var/lib/vdsm/.ssh/known_hosts
   ```

   Specify the IP address, not the host name, of each VMware hypervisor.

2. Change the ownership of the `known_hosts` file to `vdsm` user and `kvm` group:

   ```
   $ chown 36:36 /var/lib/vdsm/.ssh/known_hosts
   ```
3. Verify the SSH connection by connecting to each VMware hypervisor as `vdsm`:

```
$ sudo -u vdsm ssh root@<Vmware_host_name>
```

1. Specify the host name of the VMware hypervisor.

If the SSH connection fails, check that the VMware hypervisor has SSH access enabled and that you copied the correct keys. Otherwise, all migrations from that hypervisor using SSH transformation will fail.

### A.5. CONFIGURING SECURE REMOTE LOGIN TO THE VMWARE HYPERVISORS

You can configure secure remote login to the VMware hypervisors by using `ssh-agent` and `ssh-add`.

Secure remote login must be verified for each VMware hypervisor. If secure remote login fails, all migrations from that hypervisor will fail.

**Procedure**

1. On the Manager machine, create an `ssh-agent` session for the `vdsm` user:

```
$ sudo -u vdsm ssh-agent
SSH_AUTH_SOCK=<ssh_auth_sock>; export SSH_AUTH_SOCK;
SSH_AGENT_PID=139150; export SSH_AGENT_PID;
echo Agent pid 139150;
```

2. Copy the `<ssh_auth_sock>` value from the output.

3. Run `ssh-add` to authorize the `vdsm` user’s private key for the `ssh-agent` session:

```
$ sudo -u vdsm SSH_AUTH_SOCK=<ssh_auth_sock> ssh-add
```

1. Specify the `<ssh_auth_sock>` value.

4. Connect to a VMware hypervisor to verify the secure remote login:

```
$ sudo -u vdsm
    SSH_AUTH_SOCK=<ssh_auth_sock> ssh root@<Vmware_host_name>
```

1. Specify the `<ssh_auth_sock>` value.

2. Specify the host name of the VMware hypervisor.
PART II. MIGRATING FROM VMWARE TO RED HAT OPENSTACK PLATFORM

This guide describes how to plan your migration, to prepare the VMware source and Red Hat target environments, and to migrate the virtual machines.
CHAPTER 6. UNDERSTANDING THE MIGRATION

6.1. UNDERSTANDING THE MIGRATION PROCESS

This workflow describes the process of migrating VMware virtual machines to Red Hat OpenStack Platform.

Figure 6.1. VMware to Red Hat OpenStack Platform migration workflow

1. You create and run a migration plan in CloudForms.
2. CloudForms uses the migration plan to locate the source virtual machines.
3. CloudForms captures the ESXi host fingerprint for authentication during the virtual machine conversion process.
4. Using the attributes defined for the Red Hat OpenStack Platform environment, CloudForms initiates communication with the conversion hosts (Red Hat OpenStack Platform instances created from a conversion host appliance, with `virt-v2v` and `virt-v2v-wrapper` installed).
5. **virt-v2v-wrapper** connects to the source datastore through the ESXi host. **virt-v2v** streams the source disks to the target data domain and converts the source disks.

6. After the source disks are converted, **virt-v2v** detaches the volumes from the conversion host, migrates the volumes to the destination project, and creates the network ports defined in the infrastructure mapping.

7. **virt-v2v-wrapper** creates the target Red Hat OpenStack Platform instance with the flavor and security group defined in the migration plan. **virt-v2v** attaches the newly created network ports and the disks mapped in the block storage to the instance and the instance is powered on.

The migration process is complete and the migration plan’s status is displayed in CloudForms.

### 6.2. MIGRATION NETWORK REQUIREMENTS

The network communication between the VMware source environment, the Red Hat target environment, the conversion hosts, and CloudForms must be uninterrupted and reliable.

The firewall rules must enable the following ports for migration.

**Table 6.1. Firewall rules for migration**

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>TCP</td>
<td>CloudForms</td>
<td>Conversion hosts</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>CloudForms</td>
<td>VMware ESXi hosts</td>
</tr>
<tr>
<td>902</td>
<td>TCP</td>
<td>CloudForms</td>
<td>VMware ESXi hosts</td>
</tr>
<tr>
<td>902</td>
<td>TCP</td>
<td>Conversion hosts</td>
<td>VMware ESXi hosts</td>
</tr>
<tr>
<td>5480</td>
<td>TCP</td>
<td>Conversion hosts</td>
<td>VMware vCenter</td>
</tr>
</tbody>
</table>

**NOTE**

All outbound traffic is enabled by default. If you have changed this setting, check that ports 902 and 5480 are enabled in the security groups.
CHAPTER 7. PLANNING THE MIGRATION

During the planning phase, you will formulate a specific migration goal, for example, “I want to migrate 2000 virtual machines, with 200 TB of data, in less than 6 months”.

This section provides guidelines for planning your migration.

7.1. QUESTIONS TO ASK BEFORE MIGRATION

The following questions can help you to estimate the resources and time required for migration.

**What am I migrating?**

- Identify the VMware virtual machines that you will be migrating.

**What am I missing?**

- Identify resource gaps, such as bandwidth, storage, licenses, or a suitable maintenance window, before you begin the migration.

**What is the maximum number of disks or virtual machines that I can migrate?**

- There is no maximum number of disks or virtual machines that you can migrate. However, you may not want to migrate all your virtual machines at the same time, in order to minimize the impact on your users.

---

**IMPORTANT**

If you exceed the capabilities of your environment, the migration will fail. This situation could affect existing applications running on virtual machines attached to the network and storage.

**What impact will the migration have on my users?**

- Assess the effects the migration may have on a production environment. It may be possible to migrate your applications in phases, without downtime at the application layer, if the applications are distributed in a high-availability architecture.

- Check whether users will lose access to critical applications.

7.1.1. How long will the migration take?

There is no formula to estimate how long the actual migration will take. Migration speed is determined by your hardware, network speed, and other factors.

The following example is provided as a guide:

---

**Example 7.1. Migration to Red Hat OpenStack Platform**

Duration: 133 minutes

Environment:
- 20 virtual machines, with 1000 GB total data
- Two conversion hosts, with a maximum of ten concurrent migrations each
- Bare metal host with 40 cores and 500 GB RAM
- SSD storage
- iSCSI interface between VMware hosts and storage
- Fiber Channel interface with multipath access between Red Hat hosts and storage
- 10 GbE NICs

### 7.1.2. What operating systems can I migrate?

You can migrate any guest operating system that is certified and supported.

See [Certified Guest Operating Systems in Red Hat OpenStack Platform and Red Hat Virtualization](#).

### 7.1.3. How many conversion hosts do I need?

The number of conversion hosts you create depends on the size of your migration. All the virtual machines in a migration plan are migrated at the same time, in parallel. The number of virtual machines that you can migrate simultaneously depends on your infrastructure capabilities. Each migration requires a certain amount of network bandwidth, I/O throughput, and processing power for the conversion process.

Multiple conversion hosts provide load-balancing and better performance, even for small migrations.

Conversion hosts are limited to a maximum of ten concurrent migrations, unless you change the default values.

You should test your environment thoroughly before the migration to determine how many migrations it can support without negative effects, for example, five conversion hosts, each running ten concurrent migrations.

### 7.1.4. Should I migrate my virtual machines with VDDK or SSH?

You can migrate your virtual machines with either the VMware Virtual Disk Development Kit (VDDK) or SSH. VDDK is the default because it is much faster than SSH and easier to configure.

VDDK is limited to 20 concurrent migrations per conversion host, because of network limitations, and 10 concurrent migrations per VMware hypervisor, unless you increase the hypervisor’s NFC service memory.

If you cannot use VDDK, SSH is a fallback option.

### 7.2. OPTIMIZING YOUR MIGRATION

You can minimize the impact of the migration on your environment and improve performance.

For details on performance-related configurations, see [Performance recommendations for migrating from VMware to Red Hat Virtualization or Red Hat OpenStack Platform with IMS](#).
7.2.1. Preparing the migration environment

You can configure the VMware and Red Hat environments to optimize your migration.

**VMware environment**

You can improve performance with the following configurations:

- Extend the VMware VM network to the Red Hat environment.
- Ensure that the VMware network provides high throughput. VMware and Red Hat hosts often have multiple network interfaces. By default, the conversion hosts use the VMware hosts’ admin interface to import VMs. Configure your routing for the fastest possible connection between the Red Hat and VMware environment. You can use host routes or IP table filtering to control the traffic flow.
- Ensure that the VMware network does not affect production machines, for example, by using a backup network to avoid overload.
- Divide the VMware virtual machines equally between two VMware hosts, if possible.
- Remove unnecessary data from the VMware disks.

**Red Hat environment**

You can improve performance with the following configurations:

- Update your Red Hat environment to the latest z-stream release and install required patches.
- Use fast, full SSD storage.
- Ensure that the network connection between the bare metal hosts and storage is at least 10 GbE.
- Use Fibre Channel interfaces between the hosts and storage.
- Configure multipath access between the hosts and storage.

7.2.2. Deploying the conversion hosts

You can improve performance with the following conversion host configurations:

- Deploy the conversion host instances with at least 10 GB of available RAM and 4 CPUs. If you increase the maximum number of concurrent migrations beyond 10 (up to 20 concurrent migrations), add 1 GB RAM for each additional migration.

  **NOTE**

  If you increase the maximum number of concurrent migrations, you must perform test migrations to assess the capabilities of your environment’s infrastructure and to ensure that the actual migration does not fail.

- Deploy the conversion hosts on dedicated bare metal hosts.
- Ensure that the virtual machines on those hosts have low storage input/output usage.
- Deploy multiple conversion hosts (up to five) for load-balancing and improved performance.
The virtual machines in a migration plan are automatically distributed among the conversion hosts. This decreases the load on the conversion hosts and allows you to increase the concurrent migrations beyond the limits of a single conversion host.

7.2.3. Scheduling the migration

You can improve performance and minimize the impact on your users by scheduling the migration carefully:

- Prepare your users for downtime. Currently, IMS supports only cold migration. Virtual machines are powered off gracefully as part of the migration process.

- Stagger the migration schedules.

- Move critical applications during maintenance windows.

- Schedule the migration when storage input/output usage is low.

- Create multiple migration plans for finer control.

7.2.4. Grouping virtual machines for migration

You can improve performance and minimize the impact on your users by creating migration groups of virtual machines:

- Create migration groups for your virtual machines, so that you are not migrating all of them at the same time.

- Migrate virtual machines as a group, rather than individually. You can deploy up to 5 conversion hosts, with each host migrating up to 20 virtual machines concurrently. These limits should not be exceeded.

- Consider the following questions when creating migration groups:
  - How are the virtual machines grouped now?
  - Which virtual machines should be migrated together?
  - Which workloads or linked applications should be migrated together?
  - What applications must remain available?

- Consider which parts of the workload to migrate first:
  - Databases
  - Applications
  - Web servers
  - Load balancers
CHAPTER 8. PREPARING THE MIGRATION ENVIRONMENT

You must prepare the VMware source and Red Hat Virtualization target environments for migration.

The virtual disks are converted with the VMware Virtual Disk Development Kit (VDDK). If you cannot use VDDK, **SSH transformation** is a fallback option.

8.1. PREPARING THE VMWARE ENVIRONMENT

You must prepare the VMware network and virtual machines for migration.

If you are performing more than ten concurrent migrations from a single VMware hypervisor, you must configure the hypervisor.

8.1.1. Preparing the VMware network

Extend the VMware network to your Red Hat environment.

**IMPORTANT**

- The network configuration must not be changed in any way during the migration.
- IP addresses, VLANs, and other network configuration must not be changed before or after migration because the conversion process preserves the source virtual machine MAC addresses.

8.1.2. Preparing the VMware virtual machines

Perform the following steps on each VMware virtual machine that you are migrating:

1. Install VMware Tools to capture IP addresses.
   To download and install VMware Tools, see *VMware Workstation 5.0: Installing VMware Tools*.

2. Unmount mounted ISO/CDROM disks.

3. Ensure that each NIC has no more than one IPv4 and/or one IPv6 address.

4. Ensure that the virtual machine names contain only upper- or lower-case letters, numbers, underscores (_), hyphens (-), or periods (.)
   **NOTE**
   International characters and spaces are not permitted.

5. Ensure that the virtual machine names do not duplicate names of virtual machines in the Red Hat OpenStack Platform tenant.

8.1.3. Configuring a VMware hypervisor for more than ten concurrent migrations

If you are performing more than ten concurrent migrations from a VMware hypervisor using VDDK transformation, the migration will fail because the hypervisor’s NFC service memory buffer is limited to ten parallel connections. See *VMware Virtual Disk Programming Guide NFC session connection limits* and *Virt-v2v. VDDK: ESXi NFC service memory limits* for details.
You can increase the hypervisor’s NFC service memory to enable additional connections for migrations.

**Procedure**

1. Log in to a VMware hypervisor.

2. Change the value of `maxMemory` to `1000000000` in `/etc/vmware/hostd/config.xml`:

   ```xml
   <nfcsvc>
     <path>libnfcsvc.so</path>
     <enabled>true</enabled>
     <maxMemory>1000000000</maxMemory>
     <maxStreamMemory>10485760</maxStreamMemory>
   </nfcsvc>
   ```

3. Restart `hostd`:

   ```bash
   # /etc/init.d/hostd restart
   ```

   You do not need to reboot the VMware hypervisor.

**8.2. PREPARING THE RED HAT OPENSTACK PLATFORM ENVIRONMENT**

You must install and configure Red Hat OpenStack Platform and CloudForms and deploy the conversion hosts.

**8.2.1. Prerequisites**

Ensure that the following prerequisites are met in your Red Hat environment:

1. Set the BIOS settings of the physical hosts for optimal performance, rather than power-saving, according to the vendor’s recommendations.

2. Disable CPU enhanced halt (C1E) in the BIOS settings, if applicable.

3. Check the firewall and security group rules to ensure that the ports required for migration are open.

4. Check your software versions for compatibility.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>6.0 or later</td>
</tr>
<tr>
<td>Red Hat CloudForms</td>
<td>4.7.6 (or later), with the CFME 5.10.5 (or later) virtual appliance</td>
</tr>
<tr>
<td>Red Hat OpenStack Platform</td>
<td>13 (or later)</td>
</tr>
<tr>
<td>RHOSP V2V Image for Red Hat OpenStack Director</td>
<td>14.0.4</td>
</tr>
</tbody>
</table>
8.2.2. Installing and configuring Red Hat OpenStack Platform 13 or later

1. Install Red Hat OpenStack Platform.

2. Create provider networks for the target instances to preserve the IP addresses of the source virtual machines.

3. Create a project for the conversion hosts and any target projects you require for the target instances.

4. Ensure that the admin user has member and admin roles in the conversion host and target projects.

5. Create a volume and set at least one volume type for the target block storage. Otherwise, CloudForms will not detect the storage when you create the infrastructure mapping.

6. Ensure that the storage backends have sufficient space for the migrated virtual machines.

**IMPORTANT**

If you are using Red Hat Ceph Storage, you will require three times the space of the source virtual machines for the migrated virtual machines. A Ceph storage cluster, by default, creates two copies of an object in a replicated storage pool, for a total of three copies.

The migrated disks use all of the space because it is preallocated. For example, a source virtual machine with a 100 GB disk requires 300 GB of storage, regardless of how much data the disk actually contains. To save storage space, you can use the fstrim command on the migrated virtual machines as a postmigration task or playbook.

7. Create flavors for the source virtual machines. If you do not create custom flavors, CloudForms will try to map each source virtual machine to an existing flavor.

8.2.3. Installing and configuring CloudForms

You must install and configure CloudForms.

Removing or changing a provider in CloudForms, after creating infrastructure mappings or migration plans, will cause migration errors.

**IMPORTANT**

CFME 5.10.4 does not support migration.

**Procedure**

1. Install Red Hat CloudForms 4.7.6 (or later) on Red Hat OpenStack Platform.

2. Add VMware to CloudForms as an infrastructure provider.

3. Add Red Hat OpenStack Platform to CloudForms as an infrastructure provider. Do not complete the fields in the RSA key pair tab. You will add the SSH private key when you configure the conversion hosts.
If the Red Hat OpenStack Platform provider has been active for a while, you must wait for CloudForms to update its event history before attempting to use the provider. You can check the cloud provider timeline to verify that all events have been processed.

8.3. DEPLOYING THE RED HAT OPENSTACK PLATFORM CONVERSION HOSTS

Deploying the conversion hosts involves the following tasks:

1. Creating the conversion hosts from the conversion appliance
2. Downloading the VMware Virtual Disk Development Kit (VDDK)
3. Configuring the conversion hosts in CloudForms
4. Verifying the conversion hosts in a browser

8.3.1. Creating the Red Hat OpenStack Platform conversion hosts

You can create the Red Hat OpenStack Platform conversion hosts with the conversion appliance. The number of conversion hosts you deploy depends on your migration size and infrastructure capabilities.

**NOTE**

For optimal performance, deploy conversion hosts on compute nodes with nested virtualization enabled. Nested virtualization is a technology preview.

**Procedure**

1. Navigate to Red Hat Product Downloads.
2. In the A-Z tab, click Red Hat OpenStack Platform.
3. Click Download Latest.
4. Select 14.0 from the Version list.
5. In the Product Software tab, locate the RHOSP V2V Image for Red Hat OpenStack Director 14.0.3 (x86_64) (or later), click Download Now, and save the image.
6. Upload the image to Red Hat OpenStack Platform.
7. Launch the image as a conversion host instance, with the following resources:
   - 4 vCPUs
   - 10 GB RAM, if you use the default maximum number of concurrent migrations per conversion host, which is 10. If you increase the number of concurrent migrations, you must add 1 GB RAM for each additional concurrent migration. If you reduce the number, you can reduce the RAM but the conversion host cannot have less than 8 GB RAM.
   - `/tmp` (10 GB, or 1 GB for each concurrent migration)
   - `/var/tmp` (10 GB, or 1 GB for each concurrent migration)
   - `/var/logs` (5 GB)
8. **Resize the instance** to accommodate its file system. The instance is created from an image, but the disk space defined in the image will not be sufficient. You can either extend the partition (and subsequently, extend the physical volume in the volume group) to the required size, or you can create a new partition and add it as a physical volume to the volume group.

**NOTE**

You must resize `lv_root` to use all available disk space because the image will not use it by default.

### 8.3.2. Downloading the VMware Virtual Disk Development Kit

You must download the VMware Virtual Disk Development Kit (VDDK).

**Prerequisites**

- VMware account credentials for downloading the VDDK SDK

**Procedure**

1. In a browser, navigate to [VMware Documentation](#).

2. Click [VMware SDK & API Product Documentation → VMware Virtual Disk Development Kit (VDDK)](#).

3. Select the latest VDDK release.

4. Click [Download SDKs](#) to download the `tar.gz` VDDK archive file.

5. Save the VDDK archive file in an HTTP-accessible location and record its path.

### 8.3.3. Configuring the conversion hosts for VDDK transformation

**Procedure**

1. In CloudForms, click [Compute → Migration → Migration Settings](#).

2. In the [Conversion Hosts](#) tab, click [Configure Conversion Host](#). The Configure Conversion Host wizard is displayed.
3. In the **Location** screen, add the provider details:
   a. Select a **Provider Type**.
   b. Select a **Provider**.
   c. Select a **Project** and click **Next**.

4. In the **Host(s)** screen, select one or more hosts from the dropdown list and click **Next**.

5. In the **Authentication** screen, add the conversion hosts' SSH key and the transformation method:
   a. Click **Browse** to browse to the SSH private key or paste it in the **Conversion host SSH private key** field.
      The Red Hat OpenStack Platform user uses a private SSH key to connect to the conversion hosts.
   b. Select **VDDK** as the **Transformation method**.
   c. Enter the path of the VDDK package in the **VDDK library path** field.
   d. Click **Configure**.

6. In the **Results** screen, wait for the conversion host configuration to finish and click **Close**.
   The configured conversion hosts and status information, including error messages, appear in the **Configured Conversion Hosts** list.
If an error occurs, you can download a host’s log by clicking the **More Actions** icon ( ) and selecting **Download Log**.

You can click **Retry** if the conversion host configuration failed for reasons unconnected with your environment.

You can click **Remove** to remove the configuration from a configured conversion host.

### 8.3.4. Verifying the conversion hosts in a browser

You can verify your conversion hosts in a browser:

1. In the address bar of a browser, enter the following:

   ```
   https://<CloudForms_FQDN>/api/conversion_hosts
   ```

   Specify the FQDN of the CloudForms machine.

   A log-in screen is displayed.

2. Enter your CloudForms **Username** and **Password** and click **Sign in**.

   The conversion hosts and their IDs are displayed in JSON format in the output:

   ```
   {
   "name": "conversion_hosts",
   "count": 3,
   "subcount": 3,
   "pages": 1,
   "resources": [
   {
   "href": "https://cloudforms.example.com/api/conversion_hosts/10000000000001",
   
   "href": "https://cloudforms.example.com/api/conversion_hosts/10000000000002",
   
   "href": "https://cloudforms.example.com/api/conversion_hosts/10000000000003"}],
   "actions": [
   {
   "name": "create",
   "method": "post",
   "href": "https://cloudforms.example.com/api/conversion_hosts"},
   {
   "name": "edit",
   "method": "post",
   "href": "https://cloudforms.example.com/api/conversion_hosts"},
   {
   "name": "delete",
   "method": "post",
   "href": "https://cloudforms.example.com/api/conversion_hosts"
   },
   "links": {
   "self": "https://cloudforms.example.com/api/conversion_hosts?offset=0",
   "first": "https://cloudforms.example.com/api/conversion_hosts?offset=0",
   "last": "https://cloudforms.example.com/api/conversion_hosts?offset=0"
   }
   }
   ```
CHAPTER 9. MIGRATING THE VIRTUAL MACHINES

Migrating the virtual machines involves the following tasks:

1. Checking for migration conditions that have prerequisites
2. Creating an infrastructure mapping to map the resources of your source and target environments
3. Creating and running a migration plan in CloudForms

Optionally, you can change the maximum number of concurrent migrations for conversion hosts or providers to control the migration process.

9.1. MIGRATION PREREQUISITES

Check your migration for the following conditions, which have prerequisites:

- If you are migrating previously migrated virtual machines, you must add previously migrated machines to the migration plan with a CSV file. A CSV file is also recommended for large migrations.
- If you are using Ansible playbooks for premigration/postmigration tasks, you must create an Ansible repository and add credentials and playbooks to CloudForms.
- If you are migrating virtual machines running RHEL or other Linux operating system, you must create a RHEL premigration playbook to preserve IP addresses and select this playbook when you create a migration plan.

9.1.1. Creating a CSV file to add virtual machines to the migration plan

If you are migrating virtual machines that were migrated in the past, you should create a CSV file to add the virtual machines to the migration plan, because the migration plan cannot discover them automatically.

NOTE

A CSV file is recommended for large migrations because it is faster than manually selecting the security group and flavor of each virtual machine.

Table 9.1. CSV file fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Virtual machine name. <strong>Required</strong></td>
</tr>
<tr>
<td>Host</td>
<td><strong>Optional.</strong> Only required if virtual machines have identical <strong>Name</strong> fields.</td>
</tr>
<tr>
<td>Provider</td>
<td><strong>Optional.</strong> Only required if virtual machines have identical <strong>Name</strong> and <strong>Host</strong> fields.</td>
</tr>
<tr>
<td>Security Group</td>
<td><strong>Optional.</strong> The default is <strong>Default</strong>.</td>
</tr>
</tbody>
</table>
### Field | Comments
--- | ---
**Flavor** | Optional If you do not create flavors for the migration or if you leave this field blank, CloudForms tries to map the source virtual machines to existing flavors.

CSV file example

<table>
<thead>
<tr>
<th>Name, Host, Provider, Security Group, Flavor</th>
</tr>
</thead>
<tbody>
<tr>
<td>vm01, host1, vSphere3, webservers, x1.medium</td>
</tr>
<tr>
<td>vm02, host1, vSphere3, webservers, x1.medium</td>
</tr>
<tr>
<td>vm03, host1, vSphere3, webservers, x1.medium</td>
</tr>
</tbody>
</table>

9.1.2. Adding Ansible playbooks to CloudForms for premigration and postmigration tasks

You can add Ansible playbooks to CloudForms to perform automated premigration and postmigration tasks on specific virtual machines, for example:

- Removing webservers from a load-balancing pool before migration and returning them to the pool after migration
- Preserving the IP addresses of VMware virtual machines running RHEL or other Linux operating systems
- Running `fstrim` after migration to reduce the space required by virtual machines migrating to Red Hat OpenStack Platform with Ceph storage

**Procedure**

1. Log in to the CloudForms user interface.

2. Enable the **Embedded Ansible** server role.

3. Add an Ansible playbook repository.

4. Add the credentials of each virtual machine that you are migrating.

5. Add your playbook as an Ansible service catalog item.

You will select the playbooks and the virtual machines on which they run in the **Advanced Options** screen when you create the migration plan.

9.1.3. Creating a RHEL premigration playbook for RHEL/Linux virtual machines

If you are migrating virtual machines running RHEL or other Linux operating systems, you must create and run a **RHEL premigration** playbook to call the Ansible `ims.rhel_premigration` role.

The `ims.rhel_premigration` role ensures that the virtual machine IP addresses are accessible after migration.

**Prerequisites**
- The **rhel-<version>-server-rpms** repository must be enabled for the source virtual machines. If you have disabled it, you can re-enable it in the RHEL premigration playbook.

**Procedure**

1. Install the **ims.rhel_premigration** role with Ansible Galaxy.

2. Create a **RHEL premigration** playbook according to the following example:

   ```yaml
   ---
   - hosts: to_be_migrated
     vars:
       rhsm_config: ①
         server_hostname: "server.example.com"
         server_username: "admin"
         server_password: "secret" ②
       org_id: "my_organization"
       rhsm_repositories:
         - "rhel-<version>-server-rpms"
     roles:
       - role: ims.rhel_pre_migration
   ``

   ① Specify the configuration parameters for your environment.

   ② Passwords and other sensitive information should be encrypted with Ansible vault.

You will add this playbook when you create your migration plan.

### 9.2. CREATING AN INFRASTRUCTURE MAPPING

The infrastructure mapping maps the resources of your VMware source and Red Hat target environments.

**IMPORTANT**

If you add or remove providers or provider objects from an infrastructure mapping, the mapping will have missing resource errors. You must delete the infrastructure mapping and create a new one.

**Procedure**

1. Click **Compute → Migration → Infrastructure Mappings**.

2. Click **Create Infrastructure Mapping**. The **Create Infrastructure Mapping** wizard is displayed.
3. In the **General** screen, add the infrastructure mapping details:
   a. Enter the infrastructure mapping **Name** and (optional) **Description**.
   b. Select the **Target Provider**.
   c. Click **Next**.

4. In the **Map Compute** screen, map the source and target clusters:
   a. Select a **Source Provider \ Datacenter \ Cluster** source cluster and a **Target Provider \ Project**.
      If the target project does not contain a conversion host, a warning icon (⚠️) appears. You can create and save an infrastructure mapping, but you must configure the conversion hosts before running a migration plan.
   b. Click **Add Mapping**. You can map additional projects.
   c. Click **Next**.

5. In the **Map Storage** screen, map the source and target storage:
   a. Select a **Source Provider \ Datacenter \ Datastore** and **Target Provider \ Volume Type**.
      If the volume type is missing, check that the volume type has been set. Block storage requires at least one volume type. See **Create a Volume** and **Changing a Volume’s Type (Volume ReTyping)** in the **Red Hat OpenStack Platform Storage Guide**.
b. Click **Add Mapping**. You can map additional datastores.

c. Click **Next**.

6. In the **Map Networks** screen, map the source and target networks:

a. Select a source cluster from the drop-down list.

b. Select one or more networks from **Source Provider \ Datacenter \ Network** and **Target Project \ Network**.
   IMS supports both provider and tenant networks.

c. Click **Add Mapping**. You can map the networks of additional source clusters.

d. Click **Create**.

7. In the **Results** screen, click **Close**. The infrastructure mapping is saved in **Compute → Migration → Infrastructure Mappings**.

You can click an infrastructure mapping element to view its details:

**Infrastructure Mappings list**

![Infrastructure Mappings list](image)

---

**9.3. CREATING AND RUNNING A MIGRATION PLAN**

Before attempting a large migration, you should perform several test migrations with different maximum numbers of concurrent migrations for your conversion hosts or providers. This will enable you to assess the capabilities of your environment’s infrastructure.

**NOTE**

A CSV file is optional, but recommended, for large migrations because it is faster than manually selecting the security group and flavor of each virtual machine.

**Procedure**

1. Click **Compute → Migration → Migration Plans**.

2. Click **Create Migration Plan**. The **Create Migration Plan** wizard is displayed.
3. In the **General** screen, add the details of the migration plan:
   a. Select an infrastructure mapping from the drop-down list.
   b. Enter the migration plan **Name** and (optional) **Description**.
   c. Select a virtual machine discovery method:
      - **Choose from a list of VMs discovered in the selected infrastructure mapping**
        If the virtual machines cannot be discovered, check that the source datastores and networks in the infrastructure mapping are correct.
      - **Import a CSV file with a list of VMs to be migrated**
        A CSV file is required for previously migrated source virtual machines and recommended for large migrations.
   d. Click **Next**.

4. In the **VMs** screen, select the virtual machines for migration:
   - If you selected **Choose from a list of VMs discovered in the selected infrastructure mapping**, select the virtual machines for migration.
     You can search for virtual machines by **VM Name**, **Data Center**, **Cluster**, and **Folder**.
   - If you selected **Import a CSV file with a list of VMs to be migrated**
     a. Click **Import**.
b. Browse to the CSV file and click Open. If the virtual machines cannot be added to the migration plan, check the CSV file format and fields for errors.

**NOTE**
If the Create Migration Plan wizard freezes, refresh the web page, check the CSV file for errors (for example, virtual machines with duplicate Name fields and no other fields to distinguish them), and create a new migration plan.

c. Click Next.

5. In the **Instance Properties** screen, select the networks and/or flavors:
   a. Click the pencil icon to edit the network or flavor of each selected virtual machine. Flavors that are too small for the virtual machine are marked with an asterisk (*). If you have not created flavors for the migration, CloudForms tries to map the source virtual machines to existing flavors.
   b. Click Next.

6. In the **Advanced Options** screen, select the playbook service options:
   a. Select a premigration and/or postmigration playbook service from the dropdown lists.
   b. Select the virtual machines on which to run the playbook services.
   c. Click Next.

7. In the **Schedule** screen, select a schedule option and click Create:
   - **Save migration plan to run later**
     The migration plan is saved in **Migration Plans Not Started** and will not run unless you schedule it or click **Migrate** to run the scheduled migration plan immediately.
   - **Start migration immediately**
     The migration plan may take some time to complete. Progress bars indicate the amount of transferred data, the number of migrated virtual machines, and the elapsed time. You can view a migration plan’s progress or cancel a migration plan in progress.

8. In the **Results** screen, click Close. When the migration plan has finished, click **Migration Plans Complete** to view the status of the migration plan. The completed migration plan shows the status of the migrated virtual machines.

In the migration plans list, you can click the More Actions icon ( ) to archive, edit, or delete a migration plan.

If a migration fails because of external circumstances (for example, power outage), you can retry the migration plan.

**9.3.1. Scheduling a saved migration plan**
To schedule a saved migration plan to run in the future:
1. Click **Migration Plans Not Started**

2. Click the **Schedule** button of a migration plan.

3. In the **Schedule Migration Plan** window, select a date and time and click **Schedule**.
   The plan’s status is **Migration Scheduled** with the date and time.

### 9.3.2. Viewing a migration plan in progress

To view the progress of a migration plan:

1. Click **Migration Plans in Progress**

2. Click a migration plan name to view its details, including the status of the migrating virtual machines.

   **NOTE**

   The counter in **Compute → Migration → Migration Plans** may be a few seconds ahead of the counter in the migration plan details view. This is because the **Migration Plans** counter displays the total time for running the migration plan, while the details counter displays the time for migrating the virtual machines.

### 9.3.3. Canceling a migration plan in progress

To cancel a migration plan in progress:

1. Click **Migration Plans in Progress**

2. Select a migration plan and click **Cancel Migration**.

3. Click **Cancel Migrations** to confirm the cancellation.
   The canceled migration appears in **Migration Plans Complete** with a red x indicating that the plan did not complete successfully.

### 9.3.4. Retrying a failed migration plan

To retry a migration plan that failed because of external circumstances (for example, power outage):

1. Delete all objects created by the failed migration plan:
   - Delete newly created instances to avoid name conflicts with migrating VMware virtual machines.
   - Delete network ports of failed instances.

2. Click **Compute → Migration → Migration Plans**.

3. Click **Migration Plans Complete**.

4. Click the **Retry** button beside the failed migration plan.

### 9.4. changing the maximum number of concurrent migrations
You can change the maximum number of concurrent migrations for conversion hosts or providers to control the impact of the migration process on your infrastructure.

The provider setting has priority over the conversion host setting. For example, if the maximum number of concurrent migrations is 20 for a provider and 3 for five conversion hosts, the maximum number of concurrent migrations is 20, not 15 (5 conversion hosts \( \times 3 \) concurrent migrations per host).

An increase in the maximum number of concurrent migrations affects all migration plans immediately. Virtual machines that are queued to migrate will migrate in greater numbers.

A decrease maximum number of concurrent migrations affects only future migration plans. Migration plans that are in progress will use the limit that was set when the plan was created.

**CAUTION**

Red Hat OpenStack Platform conversion hosts require an additional 1 GB RAM for each additional concurrent migration above 10.

For VDDK transformation, the number of concurrent migrations must not exceed 20. Otherwise, network overload will cause the migration to fail.

### Changing the maximum number of concurrent migrations for all conversion hosts

1. Log in to the CloudForms user interface.

2. Click **Compute → Migration → Migration Settings**.

3. In the **Migration Throttling** tab, select a value for **Maximum concurrent migrations per conversion host** or **Maximum concurrent migrations per provider** and click **Apply**.

   The value of **Maximum concurrent migrations per conversion host** is constrained so that it cannot be greater than **Maximum concurrent migrations per provider**.

### Changing the maximum number of concurrent migrations for a specific conversion host

1. Log in to the conversion host using SSH.

2. Obtain the **conversion_host_id**:

   ```
   # curl -sk -u <username>:<password> https://<CloudForms_FQDN>/api/conversion_hosts/
   ```

   Specify the CloudForms FQDN.

3. Enter the following command:

   ```
   # curl -sk -u <username>:<password> https://<CloudForms_FQDN>/api/conversion_hosts/<conversion_host_id> -X POST -d 
   '{"action": "edit", "resource": {"max_concurrent_tasks": _15_}}'
   ```

   Specify the CloudForms admin username and password.

   Specify the FQDN of the CloudForms machine.

   Specify the **conversion_host_id**.
Specify the maximum number of concurrent migrations. The default is 10.
CHAPTER 10. TROUBLESHOOTING

You can review the migration logs, check common issues and mistakes, and known issues.

10.1. MIGRATION LOGS

You can check the conversion host logs, playbook logs, and the CloudForms migration log to identify the cause of a migration error.

**IMPORTANT**

If you need to open a Red Hat Support call, you must submit both the migration (*virt-v2v*) log and *virt-v2v-wrapper* log for analysis.

10.1.1. Downloading the conversion host and playbook logs

You can download the conversion host and playbooks logs in CloudForms.

When disk migration starts, two logs are created in the conversion host:

- **virt-v2v**: Debug output from *virt-v2v* itself. This log tracks the core of the virtual machine migration process, including *libguestfs* traces and disk migration details.

- **virt-v2v-wrapper**: Log of the daemonizing wrapper for *virt-v2v*. This log traces the orchestration of the virtual machine conversion on the conversion host, including disk migration percentages and *virt-v2v* error reporting.

**Procedure**

1. Log in to the CloudForms user interface.
2. Click **Compute → Migration → Migration Plans**.
3. Click a completed migration plan to view its details.
4. Click **Download Log** of a virtual machine and select a log from the dropdown list:
   - **Premigration log** This option only appears if a premigration playbook is used.
   - **Migration log** The **Migration log** is the *virt-v2v* log.
   - **Virt-v2v-wrapper log**
   - **Postmigration log** This option only appears if a postmigration playbook is used.

10.1.2. Accessing the CloudForms migration log

This log traces the orchestration of the virtual machine migration in CloudForms.

**Procedure**

1. Log in to the CloudForms machine using SSH.
2. The migration log is */var/www/miq/vmdb/log/automation.log*. 
10.2. COMMON ISSUES AND MISTAKES

10.2.1. Infrastructure mapping errors

- **Networks missing, Datastores missing, and Clusters missing** error messages
  If you create an infrastructure mapping and then change a provider, the provider’s object IDs change. Delete the infrastructure mapping and create a new one.

- Storage volume type not detected
  Check that you have set at least one volume type.

10.2.2. Migration plan errors

- Virtual machines are being migrated for the first time and are not discovered by the migration plan
  Check that the source datastores and networks appear in the infrastructure mapping.

- Previously migrated virtual machines cannot be discovered by the migration plan
  Use a CSV file to add the virtual machines to the migration plan.

- Virtual machines cannot be added to the migration plan with a CSV file
  Check the CSV file format and fields. Create a new migration plan with the updated CSV file.

- **Create Migration Plan** wizard hangs while importing a CSV file
  Invalid CSV file (for example, virtual machines with a duplicate Name field and no Host/Provider field to distinguish them, or with a duplicate Name field and duplicate Host/Provider fields). Correct the CSV file, refresh the web page, and create a new migration plan.

- **Unable to migrate VMs because no conversion host was configured at the time of the attempted migration. See the product documentation for information on configuring conversion hosts.**
  You can create and save a migration plan whose infrastructure mapping does not contain conversion hosts, but you cannot run the migration plan without conversion hosts. Cancel the migration plan, create the conversion hosts, and run the migration plan again.

10.2.3. IP address errors

- IP address of a migrated RHEL (or other Linux-based operating system) virtual machine is not accessible
  You must create a RHEL premigration playbook and add it to the migration plan.

- Migrated virtual machine does not have an IP address
  - You must install VMware Tools on the VMware virtual machine before migration.
  - Check the VMware virtual machine for an interface configuration file mapped to a non-existent interface (for example, /etc/sysconfig/network-scripts/ifcfg-eth1 exists, but eth1 interface does not). Log example:

```
```

Red Hat Infrastructure Migration Solution 1.2 Infrastructure Migration Solution Guide
u'00:50:56:01:23:45', 'u'--enable', 'u'port_0', 'u'--fixed-ip', 'ip-address=None'"} returned non-zero exit status 1

```bash
date time:ERROR: Command output:
BadRequestException: Unknown errors
```

## 10.2.4. Environment configuration errors

### VMware

- A VMware virtual machine cannot be migrated if it has any of the following conditions:
  - Mounted ISO/CDROM disk
  - Invalid name, containing spaces or special characters
  - Powered off during migration
- If you are performing more than ten concurrent migrations from a single VMware hypervisor, you must increase the hypervisor’s NFC service memory.

### Red Hat OpenStack Platform

- **disallowed by policy** error
  
  The Red Hat OpenStack Platform admin user in CloudForms does not have admin role privileges in the target project. Add the admin user as member and admin to your target project.

```bash
ERROR: Command exited with non-zero return code 1, output: HttpException: 403: Client Error for url: https://example.com:13696/v2.0/ports, {"NeutronError": {"message": "((rule:create_port and rule:create_port:mac_address) and rule:create_port:fixed_ips) is disallowed by policy", "type": "PolicyNotAuthorized", "detail": ""}}
```

## 10.3. KNOWN ISSUES

The following are known issues:

- **BZ#1726939**: Run the preflight check of migration task before waiting for a conversion host. Currently, the preflight check that monitors the migration is performed after a conversion host is assigned to the task. As a result, the total volume of the Datastores reported in Migration Plans In Progress reflects the total volume of the virtual machines that are currently migrating, not the total volume of the migration plan. When all the virtual machines have started to migrate, the correct value of the total volume is displayed.
APPENDIX B. CONFIGURING THE RED HAT OPENSTACK PLATFORM ENVIRONMENT FOR SSH TRANSFORMATION

You can configure your environment for SSH transformation if you cannot use VDDK.

NOTE
The default transformation method, VDDK, is much faster than SSH.

This configuration involves adding the following steps to Chapter 8, Preparing the migration environment:

Table B.1. Additional configuration for SSH transformation

<table>
<thead>
<tr>
<th>Section</th>
<th>Additional configuration for SSH transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>After Preparing the VMware environment</td>
<td>Go to Configuring the VMware hypervisors for SSH transformation. You can collect the SSH keys from the hypervisors at this time, if your security policies allow. The private key of the SSH key pair that is generated in this step will be used in Configuring the conversion hosts for SSH transformation.</td>
</tr>
</tbody>
</table>
| Instead of Configuring the conversion hosts for VDDK transformation | Go to:  
  - Configuring the conversion hosts for SSH transformation  
  - Copying the VMware SSH keys to the conversion hosts |

B.1. CONFIGURING THE VMWARE HYPERVISORS FOR SSH TRANSFORMATION

For SSH transformation, you must enable SSH access and copy a public SSH key to each VMware hypervisor. The corresponding private key will be used to configure the conversion hosts.

IMPORTANT
A single SSH key pair is recommended because this key pair is used only for virtual machine conversion and it simplifies conversion host management.

If you wish to use a dedicated SSH key pair for each conversion host, you can copy the public key of each conversion host to all the VMware hypervisors.

Procedure
1. Enable SSH access on each VMware hypervisor. For instructions, navigate to VMware vSphere Documentation and enter Enable ESXi Shell and SSH Access with the Direct Console User Interface in the Search field. You can collect the SSH public keys of the VMware hypervisors at this stage, to copy to the conversion hosts.

2. Generate an SSH key pair without a passphrase:

```bash
# ssh-keygen -N ''
```

3. Copy the public SSH key to /etc/ssh/keys-root/authorized_keys on each VMware hypervisor. You will use the private SSH key to configure the conversion hosts.

**B.2. CONFIGURING THE CONVERSION HOSTS FOR SSH TRANSFORMATION**

**Procedure**

1. In CloudForms, click Compute → Migration → Migration Settings.

2. In the Conversion Hosts tab, click Configure Conversion Host. The Configure Conversion Host wizard is displayed.

3. In the Location screen, add the provider details:
   a. Select a Provider Type.
   b. Select a Provider.
c. Select a **Project** and click **Next**.

4. In the **Host(s)** screen, select one or more hosts from the dropdown list and click **Next**.

5. In the **Authentication** screen, add the conversion hosts’ SSH key and the transformation method:
   
   a. Click **Browse** to browse to the SSH private key or paste it in the **Conversion host SSH private key** field.
      
      The Red Hat OpenStack Platform user uses a private SSH key to connect to the conversion hosts.
   
   b. Select **SSH** as the **Transformation method**.
   
   c. Click **Browse** to browse to the SSH private key you created for enabling SSH access on the VMware hypervisors or paste it in the **VMware hypervisors SSH private key** field.
   
   d. Click **Configure**.

6. In the **Results** screen, wait for the conversion host configuration to finish and click **Close**.
   
   The configured conversion hosts and status information, including error messages, appear in the **Configured Conversion Hosts** list.

If an error occurs, you can download a host’s log by clicking the **More Actions** icon ( ) and selecting **Download Log**.

You can click **Retry** if the conversion host configuration failed for reasons unconnected with your environment.

You can click **Remove** to remove the configuration from a configured conversion host.

### B.3. Copying the VMware SSH keys to the conversion hosts

Copy the SSH public keys of the VMware hypervisors to the conversion hosts.

You can collect the VMware keys either when you configure the VMware hypervisors for SSH transformation or by using **ssh-keyscan**.

#### B.3.1. Copying keys collected during VMware hypervisor configuration

1. Copy the VMware keys to `/root/.ssh/known_hosts` on each conversion host.

2. On each conversion host, verify the SSH connection by connecting to each VMware hypervisor as **cloud-user**:

   ```
   $ sudo -u cloud-user ssh root@<Vmware_host_name>  
   ```

   Specify the host name of the VMware hypervisor.

   If the SSH connection fails, check that the VMware hypervisor has SSH access enabled and that you copied the correct keys. Otherwise, all migrations from that hypervisor using SSH transformation will fail.

#### B.3.2. Copying keys collected with ssh-keyscan
You must run `ssh-keyscan` for each VMware hypervisor. Otherwise your conversion hosts will not have all the VMware hypervisor keys and the migration will fail.

Perform the following procedure on each conversion host:

1. Run `ssh-keyscan` for each VMware hypervisor and copy its public key to `known_hosts`, as in the following example:

```
$ ssh-keyscan <Vmware_host_1_ip> > /root/.ssh/known_hosts
$ ssh-keyscan <Vmware_host_2_ip> >> /root/.ssh/known_hosts
$ ssh-keyscan <Vmware_host_3_ip> >> /root/.ssh/known_hosts
```

Specify the IP address, not the host name, of each VMware hypervisor.

2. Verify the SSH connection by connecting to each VMware hypervisor as `cloud-user`:

```
$ sudo -u cloud-user ssh root@<Vmware_host_name>
```

Specify the host name of the VMware hypervisor.

If the SSH connection fails, check that the VMware hypervisor has SSH access enabled and that you copied the correct keys. Otherwise, all migrations from that hypervisor using SSH transformation will fail.