

Conditions of Use for JASMIN Virtual Machine Administrators

Version 1.0.4 – 31/01/2018

Introduction

The JASMIN platform managed by the Centre for Environmental Data Archival (CEDA) and the STFC Scientific Computing Department provides virtual machines (VMs) for scientific usage. Some users may be granted the role of VM Administrator, which will give them “root” or “sudo” access to specific servers on JASMIN. The condition of use presented here must be agreed to in order for VM Administrator access to be granted.

Virtual Machine Roles

The following roles have been defined for users of the JASMIN system:

1. JASMIN Service Manager – is the overall manager of the JASMIN service who needs to be consulted for any change requests to services.
2. JASMIN Infrastructure Manager – is in charge of setting up JASMIN VMs and ensuring that any major security and operating system updates are applied. The JASMIN Infrastructure Manager does not have responsibility for individual software packages outside of general operating system management.
3. VM Administrator – is a JASMIN user who has been granted with either “root” or “sudo” access on a JASMIN VM. The VM Administrator is in charge of managing software installations on the VM.
4. VM User – is a JASMIN user who has a login account (via SSH – see below) on a JASMIN VM but no access to “root” or “sudo” privileges.
5. JASMIN User – is anyone who holds a JASMIN user account (administered via the JASMIN accounts portal¹).

Conditions of Use for VM Administrators

A VM Administrator may be employed by an organisation external to CEDA. All VM Administrators must agree to abide by the following conditions in order to gain access to “root” or “sudo” privileges on a JASMIN VM.

1. I will not undertake any illegal activity or copy any offensive material onto the VM.
2. I will make my home institution aware that I have this responsibility and that I have signed up to these conditions of use.
3. I will not add or modify any disk mount points on the VM.
4. I will not create any user accounts on the system to enable others to connect to the VM.
5. I will not modify the login credentials (such as the “.ssh/” directory) of any users on the system.
6. I will not grant any other user “root” or “sudo” privileges on the VM.
7. I will not open any ports on the VM.
8. I will not access, or facilitate access to, any datasets visible on the VM that I do not have permission to access (via the CEDA catalogue).
9. I will only login to the server via SSH using a Public/Private key pair as set up by the JASMIN Infrastructure Manager.
10. I will not run the “yum update” command (without specifying a particular package), or equivalent command, to update all packages on the system at once without first discussing it with the JASMIN Infrastructure Manager.
11. I will not modify iptables rules on the VM.

Failure to comply will result in the suspension of the VM and may result in complete removal of access to the JASMIN platform. VM Administrators should note that all root commands are logged.

If you have any concerns about any activity that might breach the above conditions please contact the JASMIN Service Manager.

¹ The JASMIN Accounts Portal is available at: <https://accounts.jasmin.ac.uk>

Agreement to Conditions of Use for JASMIN Virtual Machine Administrators

I agree to abide by the Conditions of Use for VM Administrators on the JASMIN Platform as specified above.

Name: _____

E-mail: _____

Telephone: _____

Head of Group: _____

Head of Group E-mail: _____

Institution: _____

Signature: _____ Date: ____/____/____