Setup and use of Virtual Machines for risk-bearing data

Approved by the IG Committee 2021-02-18

Background

Virtual machines (VMs) provide a remote virtualised environment on which to store and process data. The use of virtual machines can allow users to process data entirely within the University of Sheffield's infrastructure with only a "screen view" of data flowing outside of the University network (e.g. over users' residential broadband connection). Following the process outlined below will enable users to process risk-bearing data within the scope of ScHARR's NHS DSPT assurance and within the scope of the Cyber Essentials Plus information security assurance.

Scope

IT Services provides many possible setups of Virtual Machines. However, this process will cover only the use of **Windows Server Research Virtual Machines** that - by following this process - may be used for risk-bearing data within the "business as usual" scope of the ScHARR IG Policy. Other VM setups for risk-bearing data, as per any other deviations to ScHARR IG Policy, would need to be approved by the ScHARR IG Committee.

VM setup and management

Definitions

- **User(s)** - All users of the VM (including the Lead User). All Users must have permission to access the data being stored on the VM.
- **Lead User** - The User to act as the contact on behalf of the relevant project team in all communications with ScHARR-DS in relation to the VM. The User making the initial request for a VM **MUST** be the Lead User.

Requesting a VM

1. The Lead User will use the VM Request form to make a VM request.
2. ScHARR-DS will request the IT Services' Storage & Server Group to create a new VM.
   ScHARR-DS will have server admins roles and Users will have server user roles.
3. ScHARR-DS will install and configure software on the VM, as per the Lead User's request.

4. ScHARR-DS will inform the Lead User that the VM has been set up.
5. ScHARR-DS will maintain an audit log (based on the VM Request form) for the provisioning of VMs.

Managing a Virtual Machine

Change of Lead User

The Lead User MUST inform ScHARR-DS if they cease to be a Lead User (e.g. if they cease to be a member of the relevant project team). A new Lead User MUST be nominated at this time or the VM deleted.

Modification to the VM's configuration

The Lead User MUST make requests for modification to the configuration of a VM (e.g. adding/removing Users; changes to system resources [vCPUs/RAM/storage]) by emailing ScHARR-DS.
Changes to software MUST be requested by the Lead User by emailing ScHARR-DS.

Deleting a Virtual Machine

Research VMs that require a data destruction certificate

The VM Lead User should follow the guidance in ScHARR Certified Data Deletion Process Sept 20.pdf.

VMs that do not require a data destruction certificate

The VM Lead User should email ScHARR-DS requesting deletion of a VM with:

- name of the VM to be deleted; and,
- confirmation that no data deletion certificate is required.

Using a Virtual Machine

See Appendix 1: Virtual machine checklist and Appendix 2: Working on Windows VMs.

All Users of VMs with restricted access from specific IP addresses MUST ensure their local (IP whitelisted) computer is NOT accessible to any other machine.

Appendix 1: Virtual machine checklist

Background

This document sets out the minimum user training requirements, permissible devices and connections by which authorised users may access ScHARR Virtual Machines for risk-bearing data.

The guidance below is based on that contained in the ScHARR Information Governance Policy and the University of Sheffield IT Services's policies. For any queries regarding this policy document, please email: scharr-ig@sheffield.ac.uk.

User Training Requirements

All users accessing ScHARR-managed data assets are required to comply with the ScHARR Information Governance Policy, regardless of their employer or department.

Minimum Standard

Users MUST have satisfactorily completed within the past year ALL of the training modules specified by the ScHARR IG Policy and additionally the module:

- Training for Cyber Essentials Assured Computing

Passwords

As a Research VM user/admin you will be required to set a new password for the additional username(s) provided by IT Services.

Minimum Standard

As per your contract of employment with the University of Sheffield, you MUST ensure all passwords you use for University of Sheffield systems comply with the University's password policy.

NB:
You MUST NOT share your passwords with anyone.
You MUST NOT reuse the same password (with different usernames or across different systems).

Device and Software

You will require a local device/computer from which to access VMs.

Minimum standard

Devices MUST require username and password authentication.
Devices MUST NOT be accessed by- or accessible to- unauthorised users. If using a shared device, user files MUST NOT be accessible to other device users.
Devices' operating system MUST be up-to-date and currently supported by the operating system vendor with ALL security patches and recommended updates applied.
Anti-virus software MUST be active.
ALL attached device storage MUST be encrypted.
ALL software installed on devices MUST be from a reputable source and kept up-to-date.
Devices MUST require re-authentication after no more than 5 minutes of inactivity.

NB: VPN clients, RDP clients are software so MUST be from reputable sources and kept up-to-date.

Example

For a Microsoft Windows devices, this currently means using a Windows 10 operating system with:

- BitLocker/Device Encryption enabled;
- Automatic Updates enabled and up-to-date;
- Windows Defender enabled;
- All software up-to-date.

The built-in Windows 10 VPN client and RDP client are from a "reputable source and kept up-to-date" provided Automatic Updates are enabled and up-to-date.

Preferred standard

Devices SHOULD be University of Sheffield managed devices running the latest "Managed Desktop" or "YoYo" environments (currently Windows 10).

Connection to University of Sheffield core IT infrastructure

Minimum standard

Connection to virtual machine MUST ONLY be made via one of the following:

- University of Sheffield (wired) Local Area Network (LAN) connection;
- Wireless (WiFi) connection AND University of Sheffield Direct Access or VPN;
- Other (not University of Sheffield LAN) reputable wired connection AND University of Sheffield Direct Access or VPN.

When using VPN you MUST ensure you connect using a VPN client from a reputable source and which is kept up-to-date.

Example

Details of how to set up a University of Sheffield VPN connection on a range of operating systems are published by the University of Sheffield's IT Services team. University of Sheffield managed (YoYo) laptop devices are required by IT Services to have a University of Sheffield Direct Access connection enabled.

Remote Desktop

Minimum standard

On compatible devices and operating systems, you SHOULD use a Microsoft Remote Desktop (RDP) client for connecting to Windows VMs.
You MUST share only the minimum local resources possible with the virtual machine.
You MUST NOT operate as a user with elevated (admin) rights unless solely for the purpose of making changes which require elevated rights (e.g. installing appropriately risk-assessed, software).

Example

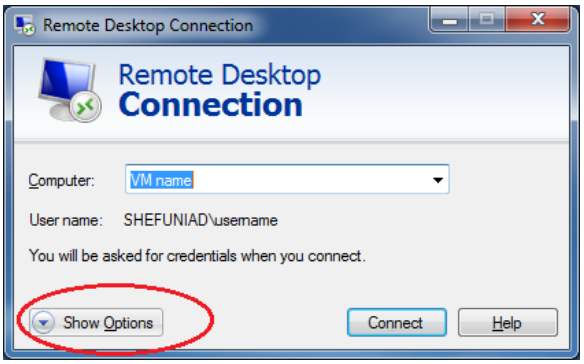
Microsoft Windows 10 has a built-in Remote Desktop client.

Appendix 2: Working on Windows VMs

Connecting to a VM

1. Click the Start menu on your local (desktop) computer and begin typing "remote desktop connection" until "Remote Desktop Connection" appears.
   Click on it.
   [To add a (quick access) link to a program to the taskbar (the bit next to the Start button), do as above but, instead of (left) clicking, right click on the "Remote Desktop Connection" and select "Pin to taskbar".]

2. The following small window may appear:



   If so, click "Show Options".

3. In the "General" tab, enter the name of the virtual machine.

4. In the username box enter "SHEFUNIAD*[VM username]*". Your VM username usually takes the form: "su_" followed by your normal university username.

5. In the "Advanced" tab, under "If server authentication fails:" select "Do not connect" from the drop-down box.

6. In the "Display" tab, tick "Use all my monitors for the remote session" if you wish to work on the VM using all your monitors (assuming you have more than one).

7. Go back to the "General" tab. To save these connection settings for quicker access in the future (recommended) click "Save As...". Otherwise, click "Connect".

8. Enter your VM password and click OK.
   If MFA is enforced for this VM you will receive an MFA prompt (sometimes more than one) - this is directed to the MFA device connected to your standard university username. Complete the MFA prompt(s) and response(s) as per usual.

Disconnecting from the VM

Having completed processing

1. Open the (VM's) Start menu
2. Click on your user profile
3. Click "Sign out" and wait for the window to close (connection to be terminated).
   NOTE: DO NOT simply exit the window as you will be unnecessarily using IT resources.

Whilst processing is continuing

1. Open the (VM's) Start menu
2. Click on your user profile
3. Click "Lock"
4. Close the Remote Desktop Connection window.

Working on the VM

You SHOULD disconnect your Remote Desktop Connection to the VM when no longer actively working on the VM by following one of the sets of instructions under Disconnecting from the VM

Appendix 3: Access restricted to specific IP addresses only

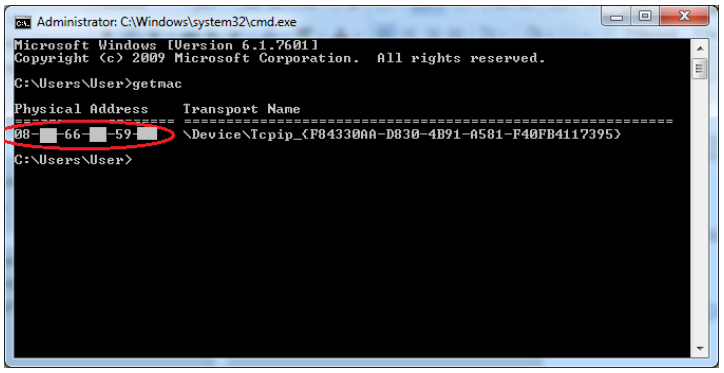
Lead Users requiring a VM with access restricted to specific on-campus IP addresses only must:

1. Ask all proposed Users for the static IP address for their local (work desktop) computer. If Users do not already have a static IP, they must make a Static IP request to IT Services (this form can be accessed from the IT Services Forms page), see below.
2. The Lead User must collate the static IP addresses assigned by IT Services to the proposed Users and supply these to ScHARR-DS, together with the corresponding usernames.

Static IP Request form

The IT Services Static IP Request "Computer Registration System" form asks for a variety of information, most are obvious, the less obvious ones are:

1. **Username**: Your standard university username; not the separate username you will receive for the virtual machine.
2. **MAC address**: For Windows 10 users you can find this for the computer you are using by following these steps:
    a. Click the Start menu then type "cmd.exe", press enter.
    b. In the window that appears type "getmac" and press enter.
    c. The MAC address of the local machine is the sequence of (hexadecimal) digits under "Physical Address".



3. **What DNS name (if any) do you want to use?**: Ignore this.
4. **Reason for request**: Try "Data security measure required by data provider."

IT Services will email each User providing them with the static IP address that has been assigned to their computer (Users will need to restart their computers to apply the static IP address). Users can also find their IP address by following these steps (only after the static IP has been applied):

A. In the search box in the Start menu, type "cmd.exe" and press enter.

B. In the window that appears type "ipconfig" and press enter.
C. The IP address is the sequence of digits specified for "IPv4 Address" under the "Ethernet adapter Ethernet:" heading.