Operational guidelines: public IP address usage in research computing

Version: 1

Effective Date: May 2023

Review Date: May 2024

Approval Authority: Cybersecurity and Research Computing Services

1. Objective

1.1 The objectives of these operational guidelines are to:

a) govern the acceptable use of public IP addresses for virtual machines (VMs) provisioned to researchers and their collaborators by Research Computing Services (RCS);
b) protect individual research projects and the University community more broadly against cyber attacks and data breaches; and
c) set clear roles and responsibilities for RCS resource users and providers.

2. Scope

2.1 These guidelines apply to the use of public IP addresses:

a) by RCS resource users;
b) for VMs provisioned by RCS.

They sit within the broader RCS Terms of Service that govern all use of RSC resources.

3. Guidelines

3.1 Public IPs are more vulnerable to cyberattack than private IPs, therefore RCS and the Cybersecurity team enforce measures to ensure the security of VMs using them.

Justification and assignment of public IPs

3.2 Public IP addresses will only be granted via a request and approval process (VMs will be issued by default with private IP addresses).

3.3 Users must provide a clear justification for requesting a public IP address.

3.4 Public IPs will be assigned to VMs for specific purposes only, with example cases potentially including:

a) running web servers; or
b) hosting public-facing applications.

3.5 The Cybersecurity team will evaluate each request to determine if a public IP will be assigned.

Standard network ports

3.6 Users must only use standard network ports like 443 (https) on VMs assigned with public IP addresses, limiting the potential attack surface and reducing the risk of unauthorised access.

Security measures

3.7 Users must install the prescribed Antivirus and Vulnerability Scanning Agent on VMs assigned with public IP addresses, to protect against known vulnerabilities and continuously monitor for security threats. (Noting that installation is not required for managed instances such as Researcher Desktop or Research Server, which come with these applications pre-installed).

3.8 Users must not deactivate any security applications that come pre-installed on managed instances, unless given explicit approval by the Cybersecurity team to do so.

3.9 The Cybersecurity team will regularly monitor VMs assigned with public IP addresses, including:

a) vulnerability assessments;
b) intrusion detection; and

c) log analysis.

3.10 The Cybersecurity team will immediately investigate any suspicious activity, and take appropriate action, potentially taking the instance offline.

Confirmation of public IP usage

3.11 Users with public IPs must reconfirm their public IP requirement with Cybersecurity every year if they wish to continue using them.

3.12 Users with public IPs who no longer require them and/or meet assignment criteria for them must notify the Cybersecurity team so that the IP address can be relinquished.

Network connectivity

3.13 Users must not use their central University username and password to connect to public IPs VMs, but instead must use a unique username and password, or security keys, specifically created for accessing the VM, ensuring that their central credentials are not compromised in the case of the machine being compromised.

3.14 Users must ensure the security and confidentiality of their VM access credentials or security keys and must not share them with anyone.

3.15 Remote access to public IP VMs is not allowed:

a) users must only connect to their public IP VMs by remote desktop and/or SSH clients via the internal network; and
b) users must be connected to the University network, either through an on-campus connection or the University provided VPN, to access their public IP VMs.

3.16 Users must ensure that their remote desktop and/or SSH clients are up to date and have the necessary security measures in place to protect against potential threats.

Compromised VMs

3.17 VMs with public IPs that are compromised will immediately be taken offline and will not be allowed to return to the network until such time as the problem is resolved.

3.18 Users must work with the Cybersecurity team and RCS to address the issue, and implement measures to prevent similar incidents from happening in the future.

Compliance

3.19 By requesting a public IP address, users agree to comply with these operational guidelines.

3.20 Failure to comply with any of these operational guidelines may result in revocation of access to the VM and/or the VM being shut down. Non-compliance may also breach University policy on acceptable use of IT resources.

4. Procedural principles

The request form

4.1 Users will fill out a request form to gain or maintain a public IP address for their RCS-issued VM.

4.2 The request form will collect:

a) user’s name;
b) contact information;
c) instance ID;
d) reason for needing a public IP address/justification for continued access to an existing public IP address;
e) required network ports; and
f) confirmation that the user will install the prescribed Antivirus and Vulnerability Scanning Agent on their instance

The review and approval process

4.3 The Cybersecurity team and/or RCS will assess submitted request forms, determining if the request is valid and if the user has provided sufficient justification for using a public IP address.

4.4 If approved, users will be notified by email of the successful outcome and must install prescribed Antivirus and Vulnerability Scanning Agent on their instance within seven days of the notification.

4.5 If not approved for a new public IP, users will be notified by email of the unsuccessful outcome and directed to default to a private IP.

4.6 If not approved for continued use of an existing public IP, users will be notified by email of the unsuccessful outcome and directed to either change to a private IP via the dashboard, or wait for RCS to make the change for them.

4.6 If users need assistance in changing to a private IP, they can submit a support request to Research Computing Services.

4.7 Users will be notified by email of any imminent change to their IP status and the outcome of that change.

5. Roles and responsibilities

SERVICE PROVIDERS **(RCS and the Cybersecurity team)**	**USERS** **(people who consume RCS resources)**
Are responsible for: • granting public IPs through a request and approval process • investigating suspicious activity, and taking appropriate action • taking compromised VMs offline • revoking access to non-compliant VMs	Are responsible for: • complying with RCS Terms of Service • justifying public IP usage • ensuring VMs are protected against known vulnerabilities and continuously monitored for any security threats • reconfirming their public IP requirement annually • notifying providers if they no longer require and/or meet assignment criteria for public IPs • ensuring the security and confidentiality of access credentials • ensuring remote desktop and/or SSH clients are up to date and have necessary security measures in place • working with providers when their VMs have been compromised, to diagnose issues and develop solutions • Must always: • use standard network ports only • install prescribed Antivirus and Vulnerability Scanning Agent • use unique access credentials or security keys (not central UoM credentials) • connect by remote desktop and/or SSH clients via the internal network only • be connected to the University network, either through an on-campus connection or the University provided VPN

6. Related information

For related and further advice, see:

- RCS Terms of Service
- Security Advice for the Melbourne Research Cloud
- Melbourne Policy Library, in particular:
    - Information Security Policy (MPF1270)
    - Provision and Acceptable Use of IT Policy (MPF1314)
    - Research Data Management Policy (MPF1242)
- Managing Sensitive Data

7. Definitions

public IP address and **public IPs** refer to IP addresses that are used on and reachable through the Internet (as opposed to private IP addresses that are used in local networks and are unreachable through the Internet).

RCS refers to Research Computing Services, a University of Melbourne service department.

VMs refer to virtual machines, computing resources that use software instead of a physical computer to run programs and deploy applications.

https (443) refers to hypertext transfer protocol secure, an extension of the hypertext transfer protocol (http), which uses encryption for secure communication over a computer network, and is widely used on the Internet.

Antivirus refers to the University Cybersecurity team's recommended Antivirus software which for suspicious processes running on your virtual machine and can stop them.

Vulnerability Scanning Agent refers to the University Cybersecurity team's recommended Vulnerability Scanning Agent which identifies and alerts support teams to installed packages that have known vulnerabilities.

remote desktop and/or SSH clients refers to a software or operating system feature that allows a personal computer's desktop environment to be run remotely off of one system (usually a PC, but the concept applies equally to a server or a smartphone), while being displayed on a separate client device.

University provided VPN refers to the Virtual Private Network that provides access to the University's systems and fileshares from off campus.

instance ID refers to the unique identifier assigned to a VM or an instance when it is created, which can be obtained from the MRC (Melbourne Research Cloud) dashboard's Instance view or the Research Computing Portal's Research Server options page.

the dashboard refers to the MRC (Melbourne Research Cloud) dashboard, which is the user interface for the MRC's Infrastructure-as-a-Service resources.