On Prem VM User Addition and Deletion

Standard Operating Procedure

Redback Operations

Document Owner:	Cybersecurity	Last Modified By:	Joel Daniel
Next Review Date:	27th July 2024	Last Modified on:	27th April 2024

Version	Modified By	Approver	Date	Changes made
0.1	Joel Daniel	NA	27th April 2024	First Draft
0.2	Joel Daniel	NA	7th May 2024	Added sudo permission addition and removal
1.0	Joel Daniel	Ben Stephens	13th May 2024	Approved for Publishing.

Document Owner: Cybersecurity   Last Modified By: Joel Daniel
Next Review Date: 27th July 2024   Last Modified on: 27th April 2024

2

Table of Contents

Document Owner: Cybersecurity   Last Modified By: Joel Daniel
Next Review Date: 27th July 2024   Last Modified on: 27th April 2024

3

1 Purpose and Scope of the SOP

This SOP will detail the steps to be taken in granting and revoking user access to the on-premise virtual machine (and any other) being used by Redback Operations.

This SOP is scoped only to any on-premise virtual machines.

2 Pre-requisites

- Ensure that you have administrative access (sudo permissions) to the virtual machine.
- Ensure that all relevant authorities are informed of the new user.
- Ensure that you are either on the Deakin VPN or on-campus directly accessing Deakin's eduroam network.

3 User Naming and Assignment Convention

1. When creating users, each user will be assigned to a user group on the virtual machine that is created for the relevant project/department the user is in. Note that all names should be in lowercase and not contain any spaces.

2. Create the user group based on the project they are in.
    a. The naming convention will have the word *redops_* at the beginning, followed by a shortened form wording of the project/department (eg:- *proj1, proj4, dataware, cysec*). Note that the naming convention when applied for one project should not change or have any alternatives created.

        eg:- redops_cyssec, redops_proj1, redops_dataware

    b. Should a sub-department designation be required, a shortened word of the subteam after an _ (eg:- seccod, dataanly) should be appended to the relevant group name assigned to the project (after the new group is created for this department)

        eg:- redops_cyssec_secod, redops_proj2_dataanly

3. The user naming must follow the below steps.

Document Owner: Cybersecurity   Last Modified By: Joel Daniel
Next Review Date: 27th July 2024   Last Modified on: 27th April 2024

4

a. The user's first (or preferred) name can be used as their username

   eg:- joel, mehak, kaylin, prajwal

b. In the same project, if two or more members having the same first name or same preferred name or same first/preferred name combo, then the first letter of their surname must be appended to their name to create the username.

   eg:- joeld, joell, joels

c. In the same project, if two or more members share the same first/preferred name combo as well as the same starting letter for their surname, their entire surname (or a shortened form if surname too long) must be appended to their name to create the username.

   eg:- joeldaniel, joeldavis, joeldavi, joeldinel

d. In the same project, if two or more members share the same first/preferred name combo as well as the same surname, then a number must be appended to their name to create the username.

   eg:- joeldaniel1, joeldaniel2

4 User Addition

1. Log into the virtual machine using SSH and provide your password when prompted.

   ssh *<username>*@redback.it.deakin.edu.au

2. Run the below command to confirm if the user's relevant project group is on the VM.

   getent group

Document Owner: Cybersecurity   Last Modified By: Joel Daniel
Next Review Date: 27th July 2024   Last Modified on: 27th April 2024

5

Note :- This command will also showcase usernames since users by default are their own groups

    a. If the relevant group has not been created, run the below command with the expected group name to create it.

        sudo addgroup *<groupname>*

3. Create the user in accordance to the naming convention with this command.

        sudo adduser *<username>*

    a. Fill the password for user requested (note the password as it will be temporary), but do not fill any of the other details requested (press Enter to continue when each option is asked). Type **Y** when asked if the information is correct. This would result in the user being created.

Note :- By default, users are not created with sudo rights

4. Add the created user to the user group with this command.

        sudo usermod -aG *<groupname> <username>*

5. Finally run this command so that the user is prompted to create a new password after they login to their account with the temporary password created in Step 3 for the first time.

        sudo chage -d 0 *<username>*

5 Sudo Permission granting and revoking

1. When giving a user sudo permissions, note down whether it is to be a permanent role or a temporary privilege access.
    a. If temporary, note down until when sudo permissions are required, and promptly follow step three to remove the user's sudo access.

Document Owner: Cybersecurity   Last Modified By: Joel Daniel
Next Review Date: 27ᵗʰ July 2024   Last Modified on: 27ᵗʰ April 2024

6

2. In order to grant sudo access, add the user to the sudo group with the following command.

   sudo usermod -aG sudo *<username>*

3. When revoking sudo access, remove the user from the group with the below command.

   sudo deluser *<username>* sudo

6 User Deletion

1. When deleting a user, run the below command.

   sudo deluser *<username>*

2. Do a review of the existing user groups and delete any empty/old/irrelevant groups with the below command.

   sudo delgroup *<groupname>*

Document Owner: Cybersecurity   Last Modified By: Joel Daniel
Next Review Date: 27th July 2024   Last Modified on: 27th April 2024

7