**Technical Operations (TechOps)**

OS Admin

Linux Narrative Exercises

© FDM Group Ltd 2011. All Rights Reserved.

Any unauthorised reproduction or distribution in part  
or in whole will constitute an infringement of copyright.

|  |
| --- |
| Page left intentionally blank |

# User Management Exercises

|  |
| --- |
| **L**ogging into the Linux Env |
| Your instructor will explain how to connect to the linux machine you are to use for the practical exercises. Use the ssh command from the windows powershell. You will first need to know your *connection string* which you past into the poweshell window and run as a poweshell command. This you can obtain by following the link in the email sent to you from Azure.    This gives you:    The connection string lives here. (Click)    Click to copy the connection string into the buffer.  If you are accessing the Azure environment, you will be given a connection string that will look something like:  ssh -p 49196 instructor@ml-lab-80add82f-5463-4584-b9cd-cdc3616ee4b5.ukwest.cloudapp.azure.com  The part of the string that comes after the ‘@’ symbol is the hostname. In this case the hostname is ml-lab-80add82f-5463-4584-b9cd-cdc3616ee4b5.ukwest.cloudapp.azure.com  The name in front of the ‘@’ symbol is the user name. In the example you are logging is as the user instructor. If you wanted to login as ‘jill’ the connaction string would be like:  ssh -p 49196 **jill**@ml-lab-80add82f-5463-4584-b9cd-cdc3616ee4b5.ukwest.cloudapp.azure.com  The connection string should be pasted directly into a powershell window. To launch the powershell app, type ‘power’ in the search bar. (Do not launch the version with (x86) in the name.). Select the App as per below.    Once you have launched powershell you can use the right mouse click to paste the connection string into the powershell window.    If you want to log in as another user, simply use the arrow keys to move your cursor to the left of the ‘@’ symbol, delete the name instructor and replace it with the user name of your choice.  The ssh command is now built into powershell (Windows 10) and is the same as the command you might type from a Linux terminal. In case you are wondering, the -p option defines a network port number. Azure use this number to direct you to the ssh login of the correct virtual machine.  On Apple Mac machines, just bring up the terminal App. Paste the connectiob string into the terminal window.  If you login as ‘instructor’, as you will do 98% of the time, you can run the command  “sudo -i” in order to become ‘root’. For these exercises you will need to be root, unless you are directed otherwise. |
| 1. Log in as root. 2. Create two or more user accounts, alison and robert   Leave all user attributes to default except for the comment, which should be:- “user for test purposes”   * + - 1. useradd –c “user for test purposes” alison       2. useradd –c “user for test purposes” robert   chech with: cat /etc/shadow  [root@ml-refvm-422293 ~]# cat /etc/shadow  root:\*LOCK\*:14600::::::  bin:\*:18353:0:99999:7:::  daemon:\*:18353:0:99999:7:::  adm:\*:18353:0:99999:7:::  lp:\*:18353:0:99999:7:::  sync:\*:18353:0:99999:7:::  shutdown:\*:18353:0:99999:7:::  halt:\*:18353:0:99999:7:::  mail:\*:18353:0:99999:7:::  operator:\*:18353:0:99999:7:::  games:\*:18353:0:99999:7:::  ftp:\*:18353:0:99999:7:::  nobody:\*:18353:0:99999:7:::  systemd-network:!!:18437::::::  dbus:!!:18437::::::  polkitd:!!:18437::::::  libstoragemgmt:!!:18437::::::  sshd:!!:18437::::::  abrt:!!:18437::::::  rpc:!!:18437:0:99999:7:::  tss:!!:18437::::::  postfix:!!:18437::::::  chrony:!!:18437::::::  ntp:!!:18437::::::  tcpdump:!!:18437::::::  instructor:$6$D4m3yCqp$Y8eCu.KDgaABy9vsnD35f/EHE80ThDxTLF3ifXAVYtgG9irKRUSCbsoduxcQGBnVlK5Enjtbj5Ib2aKrCtNJJ/:19192:0:99999:7:::  student:$6$zCAhcHwa$ofiMwHhLcaPxN.N4rMygqSQdeidFoXt9jPKaoxA4st3..DKCsCqhWWQtKRBnw.JEJUA0p9A42hGS.HDhRkQRM1:18469:0:99999:7:::  apache:!!:18469::::::  archie:$6$vEX5.kzF$oiJbnOPl0UjyraJ7HebrBF6JsJwRhoguzb0uo2UmaD8cz6Q2Twq7Gokavim544yUWi95ZUT5s/7Qlb22ebOry/:18664:0:99999:7:::  omi:!!:19016::::::  omsagent:!!:19016::::::  nxautomation:!!:19016::::::  alison:!!:19194:0:99999:7:::  robert:!!:19194:0:99999:7:::   1. Check /etc/passwd for the new user accounts. In which field is the comment?    * 1. grep ‘robert’ /etc/passwd   [root@ml-refvm-422293 ~]# grep 'robert' /etc/passwd  **robert**:x:1004:1004:user for test purposes:/home/**robert**:/bin/bash   * + 1. grep ‘alison’ /etc/passwd   [root@ml-refvm-422293 ~]# grep 'alison' /etc/passwd  **alison**:x:1003:1003:user for test purposes:/home/**alison**:/bin/bash   * + 1. field 5  1. Check /etc/group. Are there two new groups present? What is their group IDs?    * 1. tail -2 /etc/group   [root@ml-refvm-422293 ~]# tail -2 /etc/group  alison:x:1003:  robert:x:1004:   * + 1. Two new groups, alison and robert, 1003 & 1004 resp   (your values may vary slightly)   1. In which field are the respective groups ids present in alison and robert’s **passwd** file entries?   alison:x:1003: (NB: 1003 is the group ID)   * + 1. field 4 (– looks like it might not have a group yet? )  1. What does this field specify for the user account in question?    * 1. It specifies which group is the user’s primary group. |
| 1. Add a new group called “cluster” (Use defaults)    * 1. groupadd cluster 2. Check /etc/group for the new entry. What is the new group ID?    * 1. grep cluster /etc/group      2. 1005 3. Leaving the private primary groups alone for Alison and Robert, modify ‘cluster’ to include robert & alison as group members.    1. either       1. gpasswd –M alison,robert cluster 4. Check /etc/group for changes.    * 1. grep cluster /etc/group   **cluster**:x:1005:alison,Robert (NB: alison and Robert are shown in the 4th field showing that they are they are in the group cluster) |
| 1. Check the entries for ‘alison’ & ‘robert’ in /etc/shadow. The second field contains the user’s encrypted password. At present no passwords are set for the new users.    * 1. grep ‘robert’ /etc/shadow   **robert**:!!:19194:0:99999:7:::   * + 1. grep ‘alison’ /etc/shadow   **alison**:!!:19194:0:99999:7:::   * + 1. :!!: in field 2  1. Set passwords for ‘robert’ & ‘alison’. You will need to think of a suitable password.    * 1. passwd robert … [interaction]   Try: passwd robert  When prompted to type in: FDM@2020!   * + 1. passwd alison … [interaction]   Try: passwd alison  When prompted to type in: FDM@2020!  suggest FDM@2020! For the password   1. Check /etc/shadow. What is the length of the password encryption?    * 1. grep ‘robert’ /etc/shadow | cut –d: -f2 | wc –c   [root@ml-refvm-422293 ~]# grep 'robert' /etc/shadow | cut -d: -f2 | wc -c  99   * + 1. 98 characters (wc –c counts the linefeed character and reports 99 characters)  1. Check /etc/login.defs for the password hashing algorithm. Which is it?    1. grep –i ‘encrypt\_method’ /etc/login.defs   [root@ml-refvm-422293 ~]# grep -i 'encrypt\_method' /etc/login.defs  **ENCRYPT\_METHOD** SHA512   * 1. sha512 |