OpenVMS / MISER Password Policy Notes

Password Policy

The VMS password policy places password length and formatting requirements on user accounts of the MISER SCADA system. The password formatting requirements are:

- Passwords MUST be at least sixteen and no more than thirty-two characters in length.
- Passwords must be mixed case and contain at least two uppercase and two lowercase characters.
- Passwords must contain at least two numeric characters.
- Passwords must contain two special characters. Special characters are $ (dollar sign) and _ (underscore) ***ONLY***.

All passwords are checked against these rules and if they do not meet the criteria, they are rejected.

In addition to the password formatting requirements, passwords will expire after ninety days. Users are notified when their password has expired at login time. At login, the current username and password are accepted. After they are accepted, a message is displayed in a dialog box that the password has expired.

The dialog will prompt for a new password and a confirmation of the new password to ensure the user remembers what password has been entered. When entering the password, nothing is displayed in the new and confirmed password text entry area.

When the new password and confirmation are entered, click **[OK]**. This will start the process that does the following:

- Compares the new password and confirmation password fields. If they do not match, then the password change is rejected. If they match, then the password goes to the next verification step.
- The password is checked to see that it matches the password formatting policy (explained above). If the password conforms to the policy then the process continues, otherwise the password change is rejected.
- The password is checked against the contents of the password history dictionary. Each newly accepted password change is added to the password history dictionary. If the password has already been used (it is in the history), then the password is rejected. If the password is not rejected, then the operation proceeds.
- Passwords that contain words/phrases that are easy to guess are already in the password history dictionary. Additionally, VMS has an algorithm that grades a password's complexity or how easy it is to guess. If the new password meets any of the two checks, then it is rejected. For example, using the username as part of the password.

- If the password passes all of the tests listed above, it is applied to the user's VMS and MISER login account on all nodes in the MISER system that are up.
- When the password passes all of the tests, a MISER journal record is generated for the password change on each MISER node that is up.
- If the new password fails any of the above tests, the change is rejected and the user is placed back into the password change dialog. After five tries and failures, the user is logged out of the terminal. The next time the user tries to login they will be prompted again to change the password. The user will not be logged in completely until the password change is properly completed.

NOTE: The password change typically takes three to five minutes. While the update is occurring, the terminal where the password change is happening is locked. When the password change is complete on all MISER nodes, the password change dialog box closes and the user is logged on using the new password. This new password will now work on all MISER nodes.

Password Formatting Suggestions

Security officials often have a strict rule that passwords should be remembered and not written down. If they have to be written down, then it is required that the paperwork be stored in a safe. With all of the above requirements and the password history it can be hard to create a new password that is easy to remember.

While testing the VMS password policy it was necessary to create a large number of workable passwords and it was difficult to remember them all. It was discovered that it was best to use short sentences or phrases using the following rules:

- Select a sentence/phrase (e.g., `This is a test`).
- Each word in the sentence/phrase should have the first character be uppercase with all of the remaining characters be lowercase (e.g., `This Is A Test`).
- The spaces in the sentence/phrase should be replaced by either of the two special characters ($ or _) (e.g., `This$Is$A$Test` or `This_Is_A_Test`).
- Add a "$" and four numbers on the end of the sentence/phrase (e.g., `This$Is$A$Test$1234`).

This method typically works well. In ninety days the password will expire and can no longer be used. Try to alter the password so that it is different enough to pass the complexity test (e.g., `Test$Is$A$This$4321`).

Changes in UAL for Adding/Modifying User Accounts

Only one thing has changed when adding/modifying user accounts using **UAL**. When entering a password, it must be enclosed in double quotes ("). For example, when adding a user:

```
                    Processing MJJERABEK's account

Password [MJJERABEK]: "This$Is$A$Test$1234"
Enter the Access Level: 7

  Enter the area(s) for which this user will be responsible.
  There are thirty-two areas, numbered from 0 through 31.
  Separate each area specified by commas, ie:
  Area(s): 0,1,2,5,8,12
  This would give the user access to these six areas.  If you wish to give
  access to all areas, type "ALL", and all areas will be allowed.

Area(s): ALL
```

Login/Logout Report

NOTE: Throughout this document **DEMVSA** is used as a generic node/Host name. Please substitute your actual Host name where appropriate.

An easy way to determine login/logout times is to use the VMS search command. Search the AP0 log file for "WATCH-DOG" login and logout messages. You must first login to the online system. On the command line type the following:

```
DEMVSA$ set default SITE$DATA:
DEMVSA$ search 111004.AP0 "login","logout"
```

A listing of login and logout messages will be displayed as shown below:

```
DEMVSA$ set def site$data:
DEMVSA$ search 111004.ap0 "login","logout"
  5:47:30.060  4-OCT-11 DEMVS3::W_DOG-SYSTEM
FIMPLE LOGOUT
  5:48:29.688  4-OCT-11 DEMVS3::W_DOG-SYSTEM
SMITH LOGIN
  5:48:29.942  4-OCT-11 DEMVS3::W_DOG-SYSTEM
SMITH LOGIN
  5:48:35.582  4-OCT-11 DEMVS3::W_DOG-SYSTEM
SMITH LOGIN
 ...
 18:01:41.620  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TSI LOGOUT
 18:01:47.983  4-OCT-11 DEMVS5::W_DOG-SYSTEM
```

```
SYSTEM LOGIN
18:01:48.262  4-OCT-11 DEMVS5::W_DOG-SYSTEM
SYSTEM LOGIN
 18:02:00.353  4-OCT-11 DEMVS5::W_DOG-SYSTEM
SYSTEM LOGIN
 18:02:02.563  4-OCT-11 DEMVS5::W_DOG-SYSTEM
SYSTEM LOGIN
 18:03:11.460  4-OCT-11 DEMVS5::W_DOG-SYSTEM
SYSTEM LOGOUT
 18:03:14.570  4-OCT-11 DEMVS5::W_DOG-SYSTEM
SYSTEM LOGOUT
 18:11:24.588  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TESTTSI LOGIN
 18:11:24.872  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TESTTSI LOGIN
 18:12:27.940  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TESTTSI LOGOUT
 18:14:02.287  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TSI LOGIN
 18:14:02.660  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TSI LOGIN
 18:14:02.686  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TSI LOGIN
 18:14:05.430  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TSI LOGIN
 18:14:05.488  4-OCT-11 DEMVS5::W_DOG-SYSTEM
TSI LOGIN
DEMVSA$
```

A LOGIN message is shown below:

```
  5:48:29.688  4-OCT-11 DEMVS3::W_DOG-SYSTEM
SMITH LOGIN
```

The LOGIN message contains a timestamp representing the login time for the user. It also contains the node/Host name, in this case DEMVS3. Finally the message contains the username (SMITH) and the word LOGIN.

A LOGOUT message is shown below:

```
18:01:47.983  4-OCT-11 DEMVS5::W_DOG-SYSTEM
SYSTEM LOGIN
```

The LOGOUT message contains a timestamp representing the logout time for the user. It also contains the node/Host name, in this case DEMVS5. Finally the message contains the username (SYSTEM) and the word LOGOUT.

To determine when a user logs in and out, match LOGIN and LOGOUT messages in pairs based on the username that represents a specific user's session.

The AP0 log file names are encoded as YYMMDD.APO (where YY is the year, MM is the month, and DD is the day).

Some other sample search commands are:

```
DEMVSA$ search /match=and 111004.AP0 "login","rider"
```

This command searches for LOGIN records for user RIDER.

FORCING a Workstation LOGOUT – Brute Force Method

The safest way to force a logout of a user on a workstation is to go to the keyboard of the workstation and end the user's session. If doors, locks, distance, etc. make this impractical, you can login to a workstation and restart DECWindows. When DECWindows is restarted, any logged on users are forcefully logged out.

To restart DECWindows on a workstation you must login to that workstation via the "SET HOST" command as shown below:

```
DEMVSB$ set host demvs2
        DEMVS2 running VAX/VMS V8.3
Username: hsq
Password:
   Welcome to OpenVMS (TM) Alpha Operating System, Version V8.3 on node DEMVS2
    Last interactive login on Wednesday,  5-OCT-2011 16:19:15.55
    Last non-interactive login on Wednesday,  5-OCT-2011 16:19:25.31
DEMVS2$ sh sys
DEMVS2$ @sys$startup:decw$startup restart
Shared linkage sections are in use on this system and images will not
be reinstalled.  If you are restarting DECwindows to reinstall images
then you must reboot the system.

Restarting the DECwindows Software stops everything displaying on your
workstation.  Do you really want to restart the DECwindows Software? Y
Restarting DECwindows Software, server 0.  Please wait.
%RUN-S-PROC_ID, identification of created process is 000002BA
DEMVS2$
```

To determine whether someone is still left logged on to DECWindows you can use the "SHOW SYSTEM" command as shown below:

```
DEMVS2$ sh system/proc=DECW*
OpenVMS V8.3  on node DEMVS2   5-OCT-2011 17:03:08.09  Uptime  1 05:31:20
  Pid    Process Name    State  Pri      I/O       CPU       Page flts  Pages
000002BB DECW$SERVER_0   HIB      8      567   0 00:00:00.26       610    871
000002BC DECW$LOGINOUT   LEF      4      535   0 00:00:00.28       455    512
```

If you see a process named "DECW$LOGINOUT" in the listing, then no one is logged onto the terminal.