Setting Unix profiles

As a Splunk engineer, you may work with various Unix-based operating systems and correspondingly different standards and practices. In these environments, the Splunk installation may not be in the same location, which can make it difficult to use the Splunk command-line features needed for your job function. Since you cannot ask all operating systems to conform to one set of standards, a non-intrusive alternative is to use environment variables to mask such differences, which creates a consistent and effective environment to work in.

Guidelines for implementing Splunk Unix profiles

The code examples here are unsupported and can vary depending on the Unix shell you use. Refer to the documentation for your Unix shell to ensure these guidelines are valid for your environment.

Use the following variables and commands to provide a consistent shell experience regardless of differences in the underlying operating system.

Set SPLUNK_HOME

Splunk can be installed in many locations. To normalize the variation of installation directories across instances, you can use a script to define and map them to SPLUNK_HOME.

The first line in the following example is pre-populated with some common installation locations. Modify this to match your needs.

```bash
for SPLUNK_HOME in "/Applications/Splunk" "/Applications/SplunkForwarder" "/opt/splunk" "/opt/splunkforwarder" "/Applications/SplunkBeta" "/Applications/SplunkForwarderBeta" ";" 
  do
    if [ -d "$SPLUNK_HOME" ]; then
      break
    fi
  done
if [ "${SPLUNK_HOME}" == "" ]; then
  echo "WARNING: SPLUNK_HOME env variable undefined"
fi
export SPLUNK_HOME
```
Set history control

Unix keeps command line history. This can be troublesome from a security standpoint when Splunk commands require that you enter a username and password at the command line. The Unix variable HISTCONTROL controls how the shell terminal stores command history. Set the HISTCONTROL variable in your environment and use the flag ignorespace to ignore commands that have a leading space. Execute the Splunk commands that use a username and password with a leading space so they won't persist to the history.

- HISTCONTROL=ignore space

Add Splunk to PATH

You do not have to navigate to ${SPLUNK_HOME}/bin every time to run ./splunk! You can add items to your PATH to reference wherever your command line navigation takes you.

- export PATH=$PATH:/usr/bin:$SPLUNK_HOME/bin

Add btool to PATH

The troubleshooting utility btool is powerful, but you might avoid using it because you have to remember how to navigate to it. By adding btool to your PATH, you can call upon it wherever and whenever you need it. For more about btool and how to use it, see Use btool to troubleshoot configurations in the Splunk Enterprise Troubleshooting manual.

```
KERNEL=`uname -s`
case "x$KERNEL" in
  "xLinux")
    if [ -f /etc/lsb-release -o -d /etc/lsb-release.d ]; then
      export DISTRO=$(lsb_release -i | cut -d: -f2 | sed s/^\t//)
    else
      export DISTRO=$(ls -d /etc/[A-Za-z][_\-][rv]e[lr]* | grep -v "lsb" | cut -d'/' -f3 | cut -d'-' -f1 | cut -d'_' -f1)
    fi
    if [ "x$DISTRO" != "xUbuntu" ];then
      export LD_LIBRARY_PATH=$SPLUNK_HOME/lib
    fi
    ;;
  "xDarwin")
    export DYLD_LIBRARY_PATH=$SPLUNK_HOME/lib
    ;;
  *)
    echo "ERROR: Unable to set LIBRARY_PATH"
    exit 1
    ;;
esac
```
Prompt string 1 (PS1)

PS1 is the primary prompt that is displayed before each command. If you have Splunk instances distributed on systems with OS variations, having consistent PS1 prompt information from system to system can save time and reduce mistakes. Here are some suggestions about what variables to set and why so you have the same prompt information for each OS variation you work with.

PS1="[\`date\`] [\u@h \w]\n> "

- Use brackets and special characters as needed to format the prompt string, for example, '[ ]', '@', and '>'
- Use '>' as the prompt character, since it resembles the Splunk logo
- Use [\`date\`] to automatically execute a timestamp on every command prompt so you can have an approximate timeframe of the commands you issue on that system
- \u includes the username of the current user
- \h includes the host name the user is working from up to to the first period '.'
- \w includes the fully qualified path of the current working directory
- \n establishes a new line to make the results easy to read

Template for Splunk Unix profiles

The following template contains all the variables and commands listed in these guidelines. Edit it for your needs.

```
#History Control
HISTCONTROL=ignorecase

#Set SPLUNK_HOME
for SPLUNK_HOME in "/Applications/Splunk" "/Applications/SplunkForwarder" "/opt/splunk" "/opt/splunkforwarder" "/Applications/SplunkBeta" "/Applications/SplunkForwarderBeta" "/${HOME}/splunkforwarder";do
    if [ -d ${SPLUNK_HOME} ]; then
        break
    fi
done
if [ "${SPLUNK_HOME}" == "" ];then
    echo "WARNING: SPLUNK_HOME env variable undefined"
fi

export SPLUNK_HOME

#Add splunk to PATH
export PATH=$PATH:/usr/bin:${SPLUNK_HOME}/bin

#Add btool to PATH
```
Simplify distribution of the shell profile using the deployment server

You can leverage these shell commands on all your deployment clients using the deployment server. You can push out the shell profile with an app that contains the shell script in a `bin` directory. To leverage the shell profile on each deployment client, add a line to the Unix account's existing shell profile to "source" (or load) your creation from its deployment target.

Append the following to the unix user's default profile:

```
#Load Splunk-specific profile
./path/to/splunk/etc/apps/my_unix_profile/bin/splunk_profile
```

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.