Landslide Advanced Security Feature

Advanced Security is supported on Landslide Ubuntu20.04. An option to configure Advanced Security was added to the ipcfg script for virtual machines and in release 21.6 it was also added for physical TAS and test servers.

Enabling this option in ipcfg will do the following:

- Removes Telnet from the server completely. Disabling Advanced Security at a later time will not re-install Telnet.
- Removes FTP from the server completely. Disabling Advanced Security at a later time will not re-install FTP.
- Allows user to configure the port used for ssh.
- TAS http access will be disabled, user should use https. If the user needs to use http to access the TAS homepage, it can be enabled by running “enable-tas-http” command from the TAS CLI (run tas-help from CLI will get more commands and information).
- Disables ssh for all users except for the cfguser, spirent and spcoast users.
    - The cfguser password for the TAS must be changed to a more secure password. Password Requirements: Password Length must be between 8 - 16 Characters, include at least one upper case letter, one lower case letter, one digit and one special character (" ' " (single quote), ' " ' (double quote), or " \ " (backslash) are not supported).
    - The cfguser password set on a TAS with Advanced Security will be automatically propagated to any test servers connected to that TAS that are also using Advanced Security. This password is needed for logging in via ssh, console or performing activities like test server administration from the TAS Client.
    - The spirent user can only ssh to systems via private / public key pair. The public key is required to be entered on the Landslide system via ipcfg prompt.
    - The spcoast user will appear in the TAS Manager | Manager Radius Users window.
- Advanced Security should be disabled prior to downgrading to a version prior to 19.6 on virtual machine or 21.6 on physical servers.
- If Advanced Security is disabled, the cfguser password will be reset to cfguser and the ssh port will be reset to port 22. Telnet and FTP will not be re-installed / enabled. The Settings in “Manage Radius Users” will be reset as well.

Enabling advanced security is done by invoking `**ipcfg**`.

IPCFG Prompt Sequence to Enable Advanced Security –

```
Modify security settings {Basic} (yes/no)? [no]: yes
```
- Enter yes to modify security settings

```
Enable Advanced Security (yes/no)? [no]: yes
```
- Enter yes to enable advanced security

```
WARNING: Setting the SSH port number incorrectly may block network access!
Enter SSH port number: [22]: 22
  Final SSH port number:  22
```

- Enter a valid number for the port, **22** is the default

```
WARNING:  Setting the OpenSSH public key incorrectly will block the spirent user login!
REQUIRED:  The contents of an OpenSSH public key file (.pub) generated by ssh-keygen,
        single line format, consisting of 3 parts (Algorithm Key Comment).
Enter the entire contents of your initial OpenSSH public key file {spirent}: []: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/q0nXXwkmr9eWMo7nyWW4dW+yig8bMybnRMD86XU8r6w/8LCIRdqMrco0iOz8cbooLlV8cPqOIV9lXScNKDFHP3
WSMYun5oU/MO1cfiv1uJm6cMWgyVNRbN2sfkCGiM8bMt5qzfLxEnPlyTxzzQyFaSW0tZeqWPUX7VZyB8jJjjw0bfZD67dUsRgVND0bMGfhv1pUppBLvCWF30cvYApyrVXC7/PKsWmHPcghxznVgzjez1s8+zMY9OuD6WEnKPpmSWXxLl9FDh5F+3wNXroc2F8mzTyvJ53mZ5eXm
pS+O4cMBImfWeNzEvh8UoJH2AtHH0VVv4fvh1WJm6YnfWfv root@DonvTS1
Verify final OpenSSH public key file << information >> {spirent}:
  Total text length:  << 393 >>
  Algorithm:  << ssh-rsa >>  Comment:  << root@DonvTS1 >>
  Final key file md5 - future verification {spirent}:
    << ae7ac936cfbfe24569436e8efb8c8729 >>
  Final key file sha1 - future verification {spirent}:
    << 8be9d196a782dcae6deb921fb1afbe3772a97b2e >>
  Final key file sha256 - future verification {spirent}:
    << 29e808aa2a6c48ec900f87d6014f363b6c31fa293d025116383c723a357d6fe1 >>
```

- Enter a valid ssh **public key,** a valid ssh key contains **three segments**
    - Algorithm which is used to generate the key
        - eg: ssh-rsa
    - Body of the key
    - Comment
        - eg: root@DonvTS1
- Different checksums provided can be used to verify the entered content
- The ssh public key will be used when a user tries to **ssh in as spirent** with the **private key** they possess

TAS Only

```
Enter the contents of the new cfguser password []: cfgUser1!
```

The cfguser password for the TAS must be changed to a more secure password. Password Requirements: Password Length must be between 8 - 16 Characters, include at least one upper case letter, one lower case letter, one digit and one special character (" ' " (single quote), ' " ' (double quote), or " \ " (backslash) are not supported).

Upon applying changes becomes the cfguser password for

- TAS itself
- TSs **with advanced security** registered with the TAS

TS Only

```
Enter the contents of root key of the TAS at 10.71.16.91 []: 8bb4e19e5698758b99d9c916cae95ba900001
Verify new root key:
Total text length:  <37>
Final root key md5: 5719dbe8e6a14e809e47d22ea1f1001c
Final root key sha1: 1cd79556f88b198f247acf0cb819aed18cced4ed
Final root key sha256: b6e680123f317e36b19692d18acc54662ed226c47261045671233e74715da054
```

- Root key is obtained from the TAS with which the TS is going to register
- **Only the TSs possessing the root key** of a TAS can have user accounts authenticated by the TAS
- To obtain the root key of a TAS
    - Run `display-original-rootkey` on the TAS

```
##>display-original-rootkey
656443878ee55f8d65f9f927df4c127e91010
##>
```

    - Copy the root key (8bb4e19e5698758b99d9c916cae95ba900001)
    - Enter the copied content at the prompt on the TS
    - Different checksums provided can be used to verify the entered content

```
Save Advanced Security modifications (save/discard)? [save]: save
Saved new Advanced Security settings.
```

- Enter `save` to save the changes
- Saving changes **will not apply** them

```
System must be rebooted for these changes to take effect.  If cancel is selected,
user must rerun ipcfg to make and apply changes. (reboot/cancel) [reboot]:
```

    - Enter `reboot` or return to have the box rebooted to apply the changes

Note: TAS TCL API provides SshPort attribute on the ApiOptions:

Example:

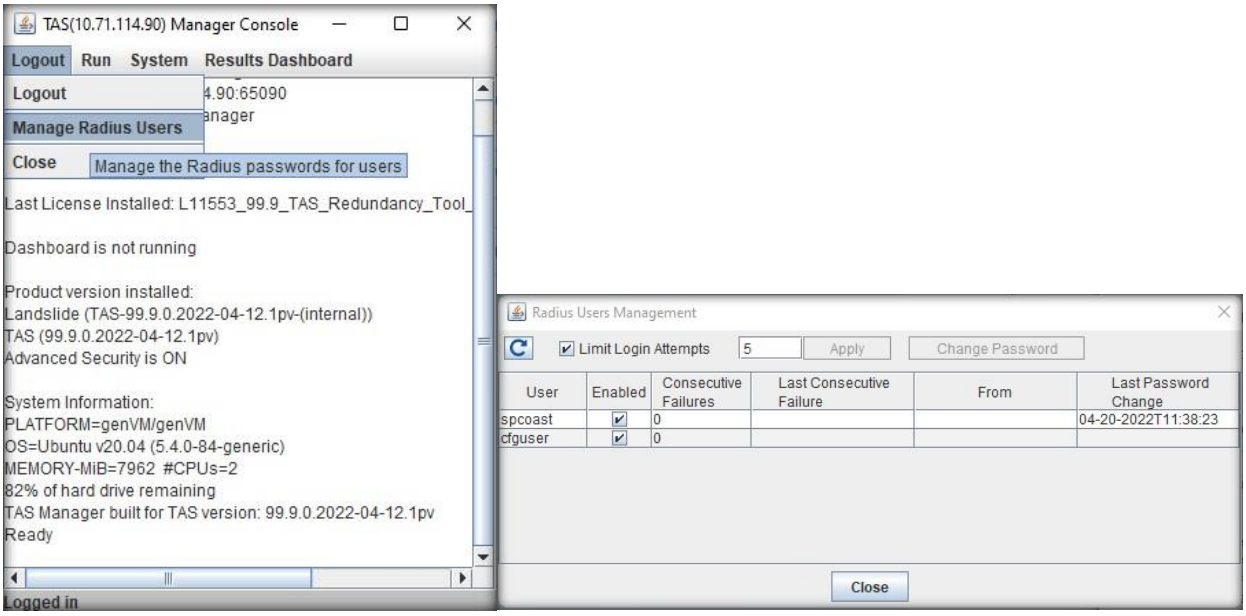
ls::config ApiOptions -SshPort 8765 -SecureClient true

ls::get ApiOptions
{FileLogging {}} {JREMemoryUsage {Memory: 257771816 remaining, 16252928 of 259522560 allocated, 14502184 free, }} {LogLevel 6} {NoReturnSuccessResponseString {}} {SecureClient true} {SshPort 8765} {StdOutLogging false} {SuppressTclErrors false}

After reboot, the TAS will come up with Advanced Security enabled. You can login into the TAS manager GUI by the cfguser password you just set during ipcfg setup, then access the radius user management window by clicking menu “Manager Radius Users” under “logout”.

Below is an example of the “Radius Users Manager” window, which allows the user to set the max login attempts (default value is disabled), if a value is set for it. Any user with failed login attempts bigger than or equal to the set limit will be blocked. However, the user can unblock an account in the same window by clicking on the checkbox next to the username.

Change password option is also provided in the same window.



Limitations:

- Advanced security does not work if the test server is configured to use IPv6 TAS address.
- All test servers registered to an advanced security TAS need to use advanced security.
- Combo TAS does not support advanced security.