Linux Pulse Client Setup

Linux Pulse Client Pre-requisites:

- PCS running 8.1R7+ or 8.2R1+.
- PCS Host Name or IP Address. (Example: https://wormhole.brandeis.edu)
- PCS Username and Password used to authenticate.
  NOTE: SAML authentication is supported in versions 5.3+.
- PCS Sign-In URL (Example: https://wormhole.brandeis.edu)
- Pulse Secure Linux Client installer package in RPM or DEB format.
  NOTE: The packages can be downloaded from the Pulse software section version 8.1R7 in https://software.brandeis.edu/Pulse

Known Issues / Limitations:

- KB40111 - [Pulse Secure Linux] Pulse Secure for Linux client does not support multiple authentication servers
- KB40109 - [Host Checker] - Pulse Secure Linux client fails to launch when enabled on a realm/role
- KB40110 - [Pulse Secure Linux] - "Status is not available. Please check if pulse client is running" when checking status

Installing the Pulse client:

Installing Pulse Secure Client for Linux
The Pulse Secure client for Linux currently is designed only for CLI-based installation.

Unbuntu Note
Note: On Ubuntu distributions, installing through Ubuntu Software Center is supported.

Installation Command:
Debian – based installation: dpkg -i <package name>
RPM – based installation: rpm -ivh <package name>

The Dependencies Installation Command:
64 bit machines: /usr/local/pulse/PulseClient_x86_64.sh install_dependency_packages
32 bit machines: /usr/local/pulse/PulseClient.sh install_dependency_packages

Upgrade Command:
Debian – based installation: dpkg -i <package name>
RPM – based installation: rpm -Uvh <package name>

The Uninstallation Command:
Debian – based installation: dpkg -r <package name>
RPM – based installation: rpm -e <package name>

Launching the Pulse client Cli
To launch UI from the Desktop Pulse Linux Client UI can be launched by searching for Pulse Secure Icon under Applications List.

Use the following command to launch the VPN client from the command line:

For PCS 8.1R8 and above:

```
/usr/local/pulse/PulseClient.sh -h <PCS appliance IP/hostname> -u <vpn username> -p <vpn password
-U <PCS SIGNINURL> -r <Realm>
```

Example: /usr/local/pulse/.PulseClient.sh -h secure.company.com -u user01 -p password01
-U https://secure.company.com/linux -r Realm

NOTE: The -f option is deprecated in 8.1R8+. The Certificate Authority (CA) certificate store is used to verify that the PCS certificate is signed by a valid CA. NOTE: In RHEL/CentOS/Fedora, "/etc/pki/tls/certs/ca-bundle.crt" is used as CA certificate store. NOTE: In Ubuntu, "/etc/ssl/certs/ca-certificates.crt" is used as CA certificate store.

NOTE: If -r <Realm_Name> is not stated, by default, it will attempt to connect to the "Users" realm. If the realm name has a white space, refer to KB40158.

NOTE: In the event that a user does not want the password to be revealed in the terminal history, the argument <vpn password> can be omitted and the user will instead be prompted for the password at run time.

NOTE: After the VPN tunnel is creates successfully, the terminal window will remain blank and must remain open. If the terminal window is closed, this will close the VPN connection.

Related articles

- Gmail
- Google Team Drives
- Setting up DUO
- DUO - Two-Factor Authentication
- Voicemail