Configuring SL1 PowerFlow for Military Unique Deployment (MUD)

SL1 PowerFlow Version 3.0.0

Configuring SL1 PowerFlow for Military Unique Deployment (MUD)

This manual describes how to configure PowerFlow for Military Unique Deployment (MUD).

This manual covers the following topics:

Installing from the ISO File

You can access the 3.0.0 ISO file from the **PowerFlow** page at the ScienceLogic Support site: https://support.sciencelogic.com/s/powerflow.

Configuring the New Node After ISO

To configure the new node after installing the ISO:

1. Change the password for the Linux system so that the Linux and the "isadmin" PowerFlow administrator user passwords are different.

> **NOTE:** When you SSH into the PowerFlow system as "isadmin" you will be forced to change the password.

2. If needed, run the following commands to update the default application password:

```
sudo rm -rf /etc/iservices/is_pass && sudo pfctl password set
```

```
sudo pfctl password encrypt
```

3. For MUD deployments, run the following command to encrypt the password before starting:

```
pfctl password encrypt
```

> **TIP:** You can run the following command to view the decrypted password on standard output (this command does not alter the contents of **/etc/iservices/is_pass** in place, but just decrypts to **stdout**): `pfctl password decrypt`

4. Find the interface network name by running `ifconfig` or `ls /etc/sysconfig/network-scripts`. In the following example, we use `ens192`.

5. Update the firewall rule to place the interface in the zone for allowing comms (these settings are only needed to enable clustered comms). Use the interface network name used by the host, such as `ens192`.

```
sudo firewall-cmd --zone=public --remove-interface=ens192

sudo firewall-cmd --zone=drop --add-interface=ens192

sudo firewall-cmd --zone=public --remove-interface=ens192 --permanent

sudo firewall-cmd --zone=drop --add-interface=ens192 --permanent

sudo firewall-cmd --reload

sudo systemctl restart docker
```

6. Install your choice of Docker. MUD deployments of PowerFlow are certified on the Docker Enterprise Edition (docker-ee) container platform, but these packages are not shipped with PowerFlow. MUD deployment works with the default docker-ce. After Docker is installed, enable and start it.

```
/bin/systemctl enable docker

/bin/systemctl start docker
```

> **NOTE:** Docker-ee is not provided by ScienceLogic; it is a subscription licensed product from Docker. To use Docker-ee you need to obtain a license from Docker. You can still deploy PowerFlow in MUD with docker-ce; the only difference is that you will be running a version of Docker that is not certified by the DoD. For more information, see https://docker-docs.netlify.app/ee/supported-platforms/#docker-ee-tiers.

Configuring PowerFlow as a Single-node MUD Deployment

To continue configuring PowerFlow as a single-node MUD deployment, run the following command on the node using sudo:

```
sudo /opt/iservices/scripts/pull_start_iservices.sh
```

Configuring PowerFlow for Any Cluster Deployment

To continue configuring PowerFlow for any cluster deployment:

1. Run the **autocluster** action with the the **powerflowcontrol** (pfctl) command-line utility to begin clustering the initial three-core node; the latest **autocluster** will automatically detect and apply MUD settings for the installation:

   ```
   pfctl --host <PowerFlow_host1> '<username>:<password>' --host
   <PowerFlow_host2> '<username>:<password>' --host <PowerFlow_host3>
   '<username>:<password>' autocluster
   ```

   For example:

   ```
   pfctl --host 10.64.166.201 'isadmin:dH&2R9el36RO5$X' --host
   10.64.166.202 'isadmin:dH&2R9el36RO5$X' --host 10.64.166.203
   'isadmin:dH&2R9el36RO5$X' autocluster
   ```

2. Apply the load balancer to the cluster. First, generate the proxy config with pfctl:

   ```
   pfctl --host 10.64.166.201 'isadmin:dH&2R9el36RO5$X' --host
   10.64.166.202 'isadmin:dH&2R9el36RO5$X' --host 10.64.166.203
   'isadmin:dH&2R9el36RO5$X' cluster-action --action generate_haproxy_
   config
   ```

3. Install haproxy on an ISO system running Oracle Linux 8:

   ```
   wget https://yum.oracle.com/repo/OracleLinux/OL8/appstream/x86_
   64/getPackage/haproxy-1.8.27-5.el8.x86_64.rpm
   ```

   ```
   yum install haproxy-1.8.27-5.el8.x86_64.rpm
   ```

4. For haproxy on SE Linux, run the following command:

   ```
   setsebool -P haproxy_connect_any=1
   ```

5. Run the following firewall commands:

   ```
   firewall-cmd --add-service=https --zone=drop --permanent
   ```

   ```
   firewall-cmd --add-port=3141 --zone=drop --permanent
   ```

   ```
   firewall-cmd --add-port=5556 --zone=drop --permanent
   ```

   ```
   firewall-cmd --reload
   ```

6. Copy the generated haproxy config to **/etc/haproxy/haproxy.conf** and run the following commands:

   ```
   systemctl enable haproxy
   ```

   ```
   systemctl start haproxy
   ```

7. Update **/etc/iservices/isconfig.yml** with the following:
    - add this line: `LOAD_BALANCED: true`
    - update `HOST_ADDRESS` to point to the load balancer.
8. Remove and re-deploy the stack.

Enabling Session Management

To enable session management, update **/etc/isevices/isconfig.yml** with the following line:

```
ENABLE_SESSION_STORAGE: true
```

Applying CAC Authorization

To enable Common Access Card (CAC) authorization on the PowerFlow system:

1. Link to a valid server CA certificate:
    - ScienceLogic Certificate: http://ca.pivkey.com/server-ca.crt
    - DODIN Certificate for sample CAC cards: http://repository.auto.sciencelogic.local/artifactory/misc-artifacts/DoD_CAs.crt
2. Set up Public-Key Cryptography Standards (PKCS) #11 in Firefox for your CAC card according to the following instructions: https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/API/pkcs11.

> **NOTE:** Use the certificates in step 1 for loading authorities.

3. Add the corresponding `server-ca` secret into the **gui** container in the **docker-compose** file:

```
gui:
  secrets
   - source: server-ca.crt
secrets:
 server-ca.crt:
   file: /etc/iservices/server-ca.crt
```

4. Add the following line to **/etc/iservices/isconfig.yml**:

```
CAC_AUTH: 'true'
```

Adding CRL to CAC Authentication

To add a certificate revocation list (CRL) to CAC authentication:

1. Download an example CRL from this site: http://ca.pivkey.com/server-ca.crt.
2. Install the following SyncPack that contains a PowerFlow application that you can run to continually update CRL: http://repository.auto.sciencelogic.local/artifactory/pypi-local/is_syncpack_mud/1.0.0/is_syncpack_mud-1.0.0-py3-none-any.whl.
3. Add the corresponding `volume` information to `gui` and `syncpacks_steprunner` in the **docker-compose** file:

```
syncpacks_steprunner:
volumes:
...
- source: ca_crl
      target: /var/crl
      type: volume
gui:
...
volumes:
    - read_only: true
      source: ca_crl
      target: /var/crl
      type: volume
volumes:
...
  ca_crl: {}
```

4. Restart the PowerFlow services.
5. Install the MUD SyncPack from step 2 and run the PowerFlow application to Fetch CRL.

> **NOTE:** Alternatively, you can manually mount a PEM-formatted CRL file to **/var/server-ca.crl**.

6. After the CRL is applied to the volume, update the configuration of **/etc/iservices/isconfig.yml** with the following line and then re-deploy:

```
CAC_CRL: 'true'
```

Specifying CAC SAN

If a Subject Alternative Name (SAN) is found in the x509 certificate, the SAN will take priority and be used in group membership searches over Common Name (CN).

Add LDAP to CAC Query

CAC authentication with LDAP requires **ldapCA.pem**, which is a file with the internal LDAP server CA chain. This will get concatenated to **tls-ca-bundle.pem**, the ca-trust bundle of the **is_gui** container.

To copy an LDAP CA certificate for verification:

1. Create **tls-ca-bundle.pem** by running the following commands:

```
docker cp $(docker ps -q --filter name=iservices_gui):/etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem /etc/iservices/tls-ca-bundle.pem
```

```
cat ldapCA.pemt >> /etc/iservices/tls-ca-bundle.pem
```

2. Use an SCP tool to move **tls-ca-bundle.pem** to **/etc/iservices/**.

Update the Docker configuration:

```
configs:
  isconfig:
    file: /etc/iservices/isconfig.yml
  tlsbundle:
    file: /etc/iservices/tls-ca-bundle.pem
```

```
  dexserver:
    configs:
    - source: isconfig
      target: /etc/iservices/isconfig.yml
    - source: tlsbundle
      target: /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
    deploy:
      replicas: 3
      restart_policy:
        condition: on-failure
    environment:
      db_host: couchbase.isnet,couchbase-worker.isnet,couchbase-worker2.isnet
    networks:
      isnet:
        aliases:
        - dexserver
        - dexserver.isnet
    secrets:
    - source: is_pass
```

```
gui:
    read_only: true
    configs:
    - source: isconfig
```

```
      target: /etc/iservices/isconfig.yml
    - source: tlsbundle
      target: /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
...
```

Update the **isconfig.yml** configuration:

```
CAC_AUTH: 'true'
CAC_LDAP_VERIFY: 'true'
DEX_CONNECTORS:
- type: ldap
  name: ldap
  id: ldap

  config:
    host: rstcsdc01.sciencelogic.local
    rootCA: /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem

    bindDN: CN=svc-ldap-commander,OU=_Service,OU=Domain User Account-
s,DC=sciencelogic,DC=local
    bindPW: <pass removed>
    usernamePrompt: silo credentials
    userSearch:
      baseDN: OU=Domain User Accounts,DC=ScienceLogic,DC=local
      filter: "(objectClass=user)"
      username: userPrincipalName
      idAttr: DN
      emailAttr: userPrincipalName
      baseDN: OU=Domain User Accounts,DC=ScienceLogic,DC=local
      filter: "(objectClass=user)"
      username: userPrincipalName
      idAttr: DN
      emailAttr: userPrincipalName
      nameAttr: cn

    groupSearch:
      baseDN: OU=Domain Groups,DC=ScienceLogic,DC=local
      filter: "(objectClass=group)"
      userAttr: DN
      groupAttr: member
      nameAttr: cn
```

To make sure that user sessions are terminated upon account deletion from the Active Directory server, the following configuration can be set in the **isconfig.yml** file. This setting ensures that the user account validation is executed during every user request:

```
FORCE_CAC_LDAP_REVALIDATION: 'true'
```

This configuration is disabled by default, as it can cause overhead in the Active Directory server. For more information, see *Configuring Authentication Settings in PowerFlow*.

Updating the docker_compose File

```
configs:
  isconfig:
    file: /etc/iservices/isconfig.yml
  tlsbundle:
    file: /etc/iservices/tls-ca-bundle.pem
```

```
dexserver:
    configs:
    - source: isconfig
      target: /etc/iservices/isconfig.yml
    - source: tlsbundle
      target: /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
    deploy:
      replicas: 3
      restart_policy:
        condition: on-failure
    environment:
      db_host: couchbase.isnet,couchbase-worker.isnet,couchbase-work-
er2.isnet
    networks:
      isnet:
        aliases:
        - dexserver
        - dexserver.isnet
    secrets:
    - source: is_pass
```

```
gui:
    read_only: true
    configs:
    - source: isconfig
```

```
      target: /etc/iservices/isconfig.yml
    - source: tlsbundle
      target: /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem
...
```

Updating the isconfig.yml File

```
CAC_AUTH: 'true'
CAC_LDAP_VERIFY: 'true'
DEX_CONNECTORS:
- type: ldap
  name: ldap
  id: ldap

  config:
    host: rstcsdc01.sciencelogic.local
    rootCA: /etc/pki/ca-trust/extracted/pem/tls-ca-bundle.pem

    bindDN: CN=svc-ldap-commander,OU=_Service,OU=Domain User Account-
s,DC=sciencelogic,DC=local
    bindPW: <pass removed>
    usernamePrompt: silo credentials
    userSearch:
      baseDN: OU=Domain User Accounts,DC=ScienceLogic,DC=local
      filter: "(objectClass=user)"
      username: userPrincipalName
      idAttr: DN
      emailAttr: userPrincipalName
      baseDN: OU=Domain User Accounts,DC=ScienceLogic,DC=local
      filter: "(objectClass=user)"
      username: userPrincipalName
      idAttr: DN
      emailAttr: userPrincipalName
      nameAttr: cn

    groupSearch:
      baseDN: OU=Domain Groups,DC=ScienceLogic,DC=local
      filter: "(objectClass=group)"
      userAttr: DN
```

```
    groupAttr: member
    nameAttr: cn
```

Locking Down Ports for Security

To secure port access:

1. Disable Couchbase and RabbitMQ port access.
2. Update `gui` in the **docker-compose** file to remove all ports 8091, 15672 from being exposed.
3. Remove additional ports from other Couchbase nodes and Rabbit nodes.

Converting from Standard 3-node MUD cluster to 6+ Node with Drain Managers and Dedicated Workers

To convert from a standard three-node MUD cluster to a six or more node cluster:

1. Add drained managers. For more information, see https://docs.sciencelogic.com/latest/Content/Web_Content_Dev_and_Integration/IS_Platform/app_multitenant.htm#Using_Drained_Managers.
2. Change leaders to drain managers. Copy files from the current manager to drained managers:

   ```
   pfctl --host ..... cluster-action --action update_cluster_configs
   ```

3. Add and label a dedicated step runner. For more information, see https://docs.sciencelogic.com/latest/Content/Web_Content_Dev_and_Integration/IS_Platform/app_multitenant.htm#Creating_a_Node_Label.

Additional Configurations

You can use the following configurations to meet the requirements called out in the OL8 STIG.

Grub and PowerFlow Users

OL08-00-010149

PowerFlow sets a default name for the grub super users account, which can be updated as needed.

Edit the **/etc/grub.d/01_users** file and add or modify the following lines:

```
set superusers="[someuniqueUserNamehere]"

export superusers

password_pbkdf2 [someuniqueUserNamehere] ${GRUB2_PASSWORD}
```

Generate a new **grub.cfg** file with the following command:

```
sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

or

```
sudo grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

OL08-00-010660

Some files that are part of the PowerFlow Docker GUI image are still flagged when validating this rule. This is because the base images used by the PowerFlow UI image set world-writable directories, which are only available in the LowerDir, so they are not available in the merged layers anymore. The only lowerdir directories displayed when executing `sudo find /var -xdev -type f -perm -0002 -print` are:

- **/dsop-fix/scripts**
- **/etc/issu**
- **/etc/yum.repos.d/**

For more details about overlay2 layers, see the Docker documentation: https://docs.docker.com/storage/storagedriver/overlayfs-driver/#image-and-container-layers-on-disk.

USBGuard

OL08-00-010600

If you need to use removable media, be sure to configure the **/etc/fstab** to use the "nodev" option on file systems that are associated with removable media.

AIDE

OL08-00-010360

Aide is configured by default to use the mail **root@localhost**, which should be changed for a valid mail in the file **/etc/crontab** . The default configuration is set to run at 5:00 AM every day, but that can be also changed as needed.

Networking

OL08-00-040110

Configure the system to disable all wireless network interfaces with the following command:

```
sudo nmcli radio all off
```

OL08-00-040259

IPv4 forwarding needs to be enabled for a PowerFlow system to work properly.

SysLog

OL08-00-030690

Configure OL8 to offload audit records onto a different system or media from the system being audited by specifying the remote logging server in **/etc/rsyslog.conf** or **/etc/rsyslog.d/[customfile].conf** with the name or IP address of the log aggregation server.

For example: Replace the default value `**.** @@logcollector` by a valid remote server name and port `**.** @@[remoteloggingserver]:[port]`.

Informational Points

Partition mount flags or options

The following mount options (or flags) are required:

Filesystem	Mount options/flags
/	
/boot	nosuid,nodev
/home	nodev,nosuid,nodev,noexec
/var	nodev,nosuid,nodev,noexec
/var/log	nodev,nosuid,nodev,noexec
/var/log/audit	nodev,nosuid,nodev,noexec
/tmp	nodev,nosuid,nodev,noexec
/var/tmp	nodev,nosuid,nodev,noexec
/dev/shm	nodev,nosuid,noexec
/var/data	nodev

Cryptography Ciphers and FIPS

The PowerFlow UI image uses FIPS 140-2 compliant ciphers. The ciphers used by the UI service can be verified by checking the Nginx configuration file using the following command:

```
docker exec -i -t $(docker ps --filter name=iservices_gui -q) grep ssl_
/data/nginx/conf.d/default.conf
```

The PowerFlow UI image was also validated following NGINX Plus FIPS Compliance documentation: https://docs.nginx.com/nginx/fips-compliance-nginx-plus/#step-2-verify-the-operating-system-and-openssl-are-in-fips-mode.

Sessions IDs are created by the lua-resty-session package using FIPS 140-2 compliant ciphers, and IDs are not sequential and are randomly created.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com. For more information, see https://sciencelogic.com/company/legal.

800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010