Plixer Replicator Documentation

Release 19.1.1

Plixer

Jan 13, 2026

VERSION 19.1.1

CHAPTER

ONE

PLIXER REPLICATOR - OVERVIEW

1.1 What is Plixer Replicator?

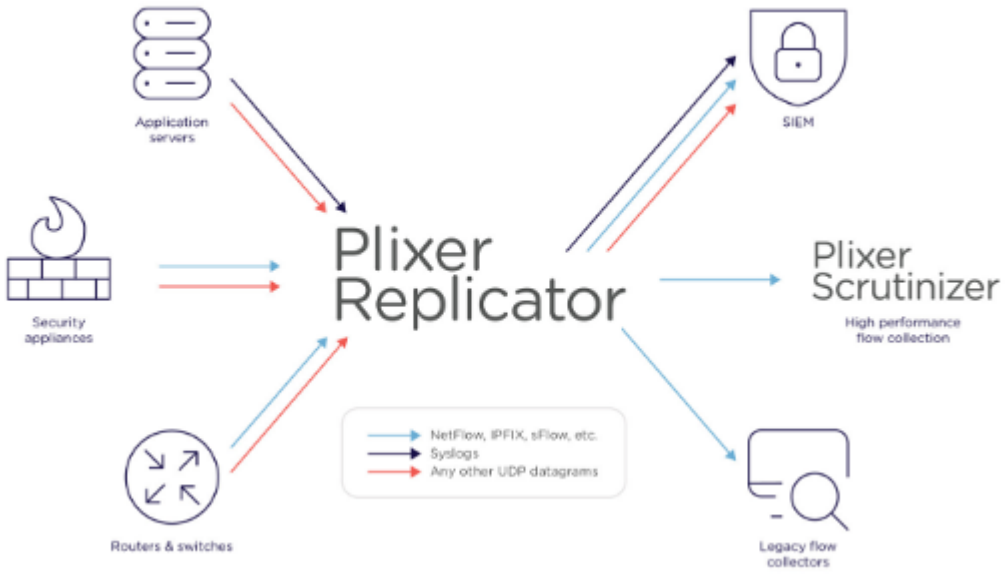
Plixer Replicator is a networking appliance that can collect, replicate, and load-balance streams from UDP metadata-exporting devices before forwarding them to any number of collector systems.

1.2 How does Plixer Replicator work?

When network devices like switches, routers, and firewalls are configured to send flow data to Plixer Replicator, it automatically replicates and forwards packets to destination collectors following parameters in user-defined profiles.

Plixer Replicator eliminates the need for 1:1 correspondence between flow-exporting devices and network intelligence collectors, allowing teams to maximize the value of their existing infrastructure.

Plixer Replicator is available as either a rack-mountable hardware appliance or a virtualized ESX, Hyper-V, or KVM solution.



1.3 Main features

Fully configurable replication
Create profiles to manage exporter-to-collector assignments and use inclusion/exclusion policies to keep profiles updated as your environment expands

Insightful, real-time alarms
Gain additional visibility into all devices sending flows to Plixer Replicator and get alerted to drops in traffic and other irregularities

Full-featured web interface
View and manage the Plixer Replicator environment in an intuitive web interface

Robust command line interface (CLI)
Use interactive commands to configure Plixer Replicator's functions and leverage advanced features

CHAPTER

TWO

DEPLOYMENT GUIDES

This section contains guides for the installation/deployment and initial setup of the different types of Plixer Replicator appliances.

Note:

- An active Plixer Replicator license is required to complete the setup process. To learn more about licensing options, contact *Plixer Technical Support*.
- After the hardware or virtual appliance is deployed, the initial setup script walks the user through the process of applying a license, as described *here*.

2.1 Hardware appliance

The Plixer Replicator hardware appliance is designed for a 1U server rack and should be securely mounted before the deployment process is started.

To deploy the Plixer Replicator hardware appliance, follow these steps:

1. Use the provided power cable to plug the appliance into an appropriate power source.
2. Connect the Plixer Replicator to the network. When facing the rear of the appliance, the network cable should be plugged into the left hand side NIC.
3. Connect a monitor and keyboard directly to the Plixer Replicator appliance and power it on.
4. Log in with the username `replicator` and the password `replicator`, and then follow the prompts to configure the appliance.
5. After the appliance reboots, *log in to the web interface* and follow the setup wizard to prepare Plixer Replicator for use.

2.2 Virtual appliances

Plixer Replicator is available in all-in-one virtual appliance packages for VMware ESX, Microsoft Hyper-V, and KVM environments.

All types of Plixer Replicator virtual appliances are available through Plixer or a local reseller, who will assist you with acquiring the evaluation or subscription license key required to activate the product.

To deploy the virtual appliance of your choice, follow the corresponding guide below:

2.2.1 ESX

To deploy the Plixer Replicator virtual appliance for ESX environments, note the following system requirements and proceed with the instructions that follow:

Note: The Plixer Replicator virtual appliance for ESX is provided as an all-in-one OVF template to streamline the deployment process.

System requirements for ESX deployments:

- RAM: 4 GB
- Storage: 100 GB
- Processor: 2 CPU, 2 cores, 2 GHz+
- OS: ESX/ESXi5+
- VMware Tools (to shut down the machine via the VMware vSphere client)

Deploying the OVF template

1. Contact *Plixer Technical Support* and use the link (e.g., https://files.plixer.com/PACKAGE_PATH/PACKAGE_FILENAME.tar.gz) they provide to download the latest ESX virtual appliance package.
2. Extract the contents of the package to a location on the ESX server.
3. After connecting to the ESX host via VMware vSphere or vCenter, select **File > Deploy OVF Template**.
4. Select **Deploy from File**, navigate to the OVF Template, and then click **Next**.
5. Review the OVF template details, and then click **Next**.
6. Provide a name for the virtual appliance and follow the deployment wizard that follows.
7. Review the virtual settings provided, and then click **Finish** to complete importing the OVF Template.
8. Right-click on the Plixer Replicator virtual machine to boot it up.
9. Navigate to the **Console** tab and log in with the username `replicator` and password `replicator`.
10. After the machine performs a quick setup, follow the prompts to configure the appliance.
11. After the appliance reboots, *log in to the web interface*, and then follow the setup wizard to prepare Plixer Replicator for use.

Note: VMware Tools is installed as part of the the Plixer Replicator package by default. For more information, refer to the VMware Tools documentation.

Upgrading the virtual machine hardware version

The Plixer Replicator virtual appliance for ESX is built on virtual machine hardware version 7 to maintain backwards compatibility with ESXi 5 hypervisors.

To upgrade the hardware version:

1. Shut down the virtual machine.
2. Right-click on the virtual machine in vSphere (or vCenter), and then select **Upgrade Virtual Hardware**.

2.2.2 Hyper-V

To deploy the Plixer Replicator virtual appliance for Hyper-V environments, note the following system requirements and proceed with the instructions that follow:

System requirements for Hyper-V deployments:

- RAM: 4 GB
- Storage: 100 GB
- Processor: 2 CPU, 2 cores, 2 GHz+

Importing the virtual machine

1. Contact *Plixer Technical Support* and use the link (e.g., https://files.plixer.com/PACKAGE_PATH/PACKAGE_FILENAME.tar.gz) they provide to download the latest Hyper-V virtual appliance package.
2. Extract the contents of the package to a location on the Hyper-V server.
3. In *Hyper-V Manager*, select **Import Virtual Machine**, and then browse to the Plixer Replicator system folder.
4. Select the virtual machine and import type.
5. Go to **Settings**, select the network adapter, and assign it to the appropriate virtual switch.
6. In the network adapter's *Advanced Features* section, set the MAC address to **Static**, enter a unique MAC address, and then press **OK**.
7. Start the virtual machine, right-click on it, and then select **Connect**.
8. Log in with the username `replicator` and the password `replicator`, and then follow the prompts to configure the appliance.
9. After the appliance reboots, *log in to the web interface*, and then follow the setup wizard to prepare Plixer Replicator for use.

2.2.3 KVM

To deploy the Plixer Replicator virtual appliance for KVM environments, note the following system requirements and proceed with the instructions that follow:

System requirements for KVM deployments:

- RAM: 4 GB
- Storage: 100 GB
- Processor: 2 CPU, 2 cores, 2 GHz+

Importing the virtual machine

1. Contact *Plixer Technical Support* and use the link they provide to download the latest KVM virtual appliance package:

```
curl -k -o PACKAGE_FILENAME.tar.gz https://files.plixer.com/PACKAGE_PATH/PACKAGE_
↪FILENAME.tar.gz
```

2. Create a directory for the install:

```
mkdir /kvm/replicator
```

3. Extract the contents of the package to the new directory:

```
sudo tar xvzf PACKAGE_FILENAME.tar.gz -C /kvm/replicator/
```

4. Run the installation script in the new directory:

```
cd /kvm/replicator/PACKAGE_FILENAME
sudo ./install.sh
```

5. Access the console to log in to the appliance:

```
virsh console Replicator
```

6. Follow the initial appliance setup prompts.
7. After the appliance reboots, *log in to the web interface*, and then follow the setup wizard to prepare Plixer Replicator for use.

2.3 Initial configuration

After the Plixer Replicator appliance has been deployed and configured, the web interface can be accessed by pointing a supported browser to the IP address or hostname assigned to the appliance.

Note: The default username for the web interface is `admin` and the default password is `admin`. To change the default login credentials, use the Interactive Mode command `password webui`.

Logging into the web interface for the first time will start a setup wizard that walks the user through finalizing the Plixer Replicator setup process.

2.3.1 First login

The final steps of the Plixer Replicator setup process must be completed in the web interface, after logging in as the default `admin` user.

Note: The default username for the web interface is `admin` and the default password is `admin`. To change the default login credentials, use the *interactive command* `password webui`.

A setup wizard will walk the user through the following steps:

Applying a license key
: When the user first logs in, Plixer Replicator automatically checks for a valid license key before proceeding. If no license key has been applied, the user will be prompted to enter one.

  Once a valid subscription or evaluation key has been entered, the wizard will continue to the next step.

  Note: License keys are available from Plixer or local resellers. Users can view and manage their license details by going to **Settings > Licensing** in the web interface.

Creating a profile
: If there are currently no profiles configured, the wizard will walk the user through creating one.

Important: Before attempting to add a profile, configure a device to start sending packets to the Plixer Replicator and take note of the port it uses to send data.

To create a profile, the user will need to provide the following:

1. A unique name for the profile
2. The port for inbound packets (*In Port*)
3. The port for outbound packets (*Out Port*)

For more information on creating and configuring profiles, see the section on *profile management*.

After a profile has successfully been created, the wizard will continue to the next step.

Confirming that packets are inbound

The **Dashboard** and **Streams** tabs of the Plixer Replicator web interface provide real-time oversight of the appliance's packet activity.

As the last step of the setup wizard, the user will be directed to the **Streams** tab to verify the Plixer Replicator is receiving packets from devices that have been configured to send flows to it.

See the section on the Plixer Replicator *web interface* to learn more about other UI functions.

2.3.2 Setting up SSL

SSL can be enabled for the Plixer Replicator appliance during the initial appliance setup. It can also be *enabled or re-configured at a later time*.

Note: An Internet connection is required to download the latest OpenSSl package and other required resources.

The following information will be required for the creation of the self-signed certificate:

Name Field	Description
Country name	The two-letter ISO abbreviation for a country example: US = United States
State / province	The state/province where the organization is located (no abbreviations) example: Maine
City / locality	The city where the organization is located (no abbreviations) example: Kennebunk
Organization	The full legal name of the organization example: Plixer
Email address	The email address for the CA (whom to contact) example: someone@your.domain
Common name	URL to attach to the certificate example: 10.1.1.19 or replicator.company.com
Extra attributes	A challenge password and an optional company name can be added to the certificate request

Reconfiguring SSL

If SSH was not enabled during appliance setup, the `enable_ssh.sh` script (located in `/home/replicator/util/`) can be used to enable SSH and create a self-signed certificate.

The script can also be used to create a new certificate using different details. However, the existing certificate must be deleted before the script is run.

2.3.3 Creating a CA-signed certificate

To create an SSL certificate signed by a trusted certificate authority or CA, follow these steps:

1. After enabling SSL, send the `/etc/pki/tls/private/ca.csr` file to the CA to be signed and ask them to return it as **Base64** encoded.

Important: When exporting a certificate, do **not** select **DER encoded** as the export file format.

---

2. Once the CA-signed certificate is received, stop the Apache service by entering `service httpd stop`.
3. Replace the active SSL certificate with the new one and rename the file to `*//etc/pki/tls/certs/ca.crt`.
4. Restart the Apache service by entering `service httpd start`.

CHAPTER

THREE

FEATURES AND FUNCTIONALITY

This section contains detailed guides and further information on Plixer Replicator's main functions and added features.

3.1 Plixer Replicator web interface

The Plixer Replicator web interface provides access to management and administrative functions for the appliance, allowing users to set up replication profiles, monitor environment resources, and configure system preferences/settings.

The web interface can be accessed from any supported browser, using the IP address or hostname assigned to the appliance during the initial setup script. The default credentials for the Plixer Replicator administrator account are `admin:admin`.

3.1.1 Dashboard

The **Dashboard** tab/page allows the user to toggle between three different dashboards summarizing statistics related to Plixer Replicator's functions.

Note:

- The web interface header also includes a virtual notification LED that will alert the user to any issues related to system services. Clicking the LED opens a more detailed view that shows all services and includes resolution recommendations for those with issues.
- The default update/refresh interval for live data is 60 seconds. This can be changed by modifying the *Update Interval* value in the *Settings tab/page*.

Real-Time Statistics

The **Real-time Statistics** dashboard contains visualizations for the following statistics:

- Current CPU utilization
- Average packet rate (in and out)
- Average bit rate (in and out)
- Packet rates over time (in and out)
- Bit rates over time (in and out)
- Total number of exporters in profiles
- Total number of collectors in profiles

- Total number of unique collector-exporter pairs across all profiles
- Current number of profiles configured
- Total bits received and sent
- Total number of packets received and sent

Hover over the packet rate or bit rate timeline to view details for a specific point in time.

Replication Tree

The **Replication Tree** dashboard shows all resources associated with the Plixer Replicator appliance through its configured profiles.

Topology

The **Topology** dashboard shows the flow of packets from exporters to their destination collectors.

To view the topology for a single profile instead of all profiles (default), select the profile in the dropdown.

3.1.2 Streams

The **Streams** tab/page displays information for all inbound streams and can be used to verify that the Plixer Replicator appliance is successfully receiving streams from exporters.

The list/table shows the following details for each stream:

- IP address of the source exporter
- DNS name of the source exporter
- Timestamp when packets associated with the stream were last received
- Current status of the stream
- Total number of packets received as part of the stream (with average rate)
- Total volume of data received as part of the stream (with average rate)
- Total number of packets sent with the stream as their source (with average rate)
- Total volume of data sent with the stream as its source (with average rate)

Any streams that have triggered alarms will be highlighted in red, with the reason indicated in the **Status** column of the table.

Note:

- Click the icon in the **DNS Name** column to force a manual resolution of an exporter's DNS name from its IP address.
- Use the **Alarms Only** toggle to view only streams that have triggered alarms.
- The *Search* field can also be used to find exporters whose IP address matches the entered string.

3.1.3 Exporters

The **Exporters** tab/page of the web interface can be used to view all exporters currently sending packets/flows to the Plixer Replicator appliance.

The list/table includes the following details for each exporter:

- IP address
- DNS name
- Timestamp when packets were last received from the exporter
- Current status of the exporter
- Total number of packets packets received from the exporter (with average rate)
- Total volume of data received from the exporter (average rate)
- Profiles that include the exporter

Any exporters that have triggered alarms will be highlighted in red, with the details of the alarm dispalyed in the **Status** column of the table.

Exporter management

The exporter summary table also provides access to the following functions:

- Deleting exporters from all profiles
- Adding/editing notes attached to exporters
- Manually forcing a DNS name resolution for exporter IP addresses
- Adding exporters to specified profiles
- Removing exporters from specified profiles
- Inspecting profiles containing a specific exporter

Note:

- The list can be set to show only exporters currently included in at least one profile or only exporters that are not in any profile. A filter to display only exporters with alarms can also be applied.
- The search field can also be used to find exporters whose IP address or DNS name matches the entered string.
- When viewing only exporters not currently included in any profiles, alarms will only be indicated for devices that were previously included in at least one profile.

3.1.4 Collectors

The **Collectors** tab/page of the web interface can be used to view all collectors that are currently assigned to at least one *profile*.

The list/table includes the following details for each collector:

- IP address
- DNS name
- Timestamp when the collector was last confirmed as available
- Current status of the collector

- Total number of packets sent to the collector (with average rate)
- Total volume of data sent to the collector (average rate)
- All profiles associated with the collector

Any collectors that have triggered alarms will be highlighted in red, with the details of the alarm displayed in the **Status** column of the table.

Collector management

The collector overview table also provides access to the following functions:

- Deleting collectors from all profiles
- Adding/editing notes attached to collectors
- Manually forcing DNS name resolution for collector IP addresses
- Adding packet thresholds/caps to limit the packet sending rates to collectors
- Assigning collectors to specified profiles
- Removing collectors from specified profiles
- Inspecting profiles associated with a specific collector

Note:

- The list can be filtered to show only collectors with alarms.
- The search field can also be used to find collectors whose IP address or DNS name matches the entered string.
- If a collector is deleted from all profiles, it will be removed from the list until it is manually added to at least one profile.

3.1.5 Profiles

The **Profiles** tab/page of the web interface can be used to create, edit, and manage replication profile configurations.

The list/table shows the following details for all profiles currently saved on the Plixer Replicator appliance:

- Profile name
- Number of *policies* added to the profile
- Number of exporters included in the profile
- Number of collectors assigned to the profile
- In/receiving port used by the profile
- Out/sending port used by the profile
- Total number of packets sent to collectors assigned to the profile (with average rate)
- Total volume of data sent to collectors assigned to the profile (average rate)
- Total number of packets packets received from exporters in the profile (with average rate)
- Total volume of data received from exporters in the profile (average rate)

Any profiles that have triggered alarms or include exporters or collectors with alarms will be highlighted in red. To view information about the alarm(s), drill into the profile details page by clicking the edit (pencil) icon.

Profile management

The main **Profiles** page also provides access to the following functions:

- Creating new profiles
- Deleting profiles
- Editing existing profiles

To learn more about creating and editing profiles, see the section on *profile management*.

Additional profile settings

The following additional settings can be configured via the profile details view:

- Enable/disable the profile
- Enable/disable showing a packet's origin as the source exporter's IP address (if disabled, collectors will interpret packets as having come from the Plixer Replicator appliance)

3.1.6 Settings

The **Settings** tab/page can be used to configure global settings for the following:

Setting	Description
Alarm Tolerance	The duration in minutes that an incoming stream must be stopped or a collector must be unreachable for the system to consider it down.
Auto Acknowledge	The number of hours before an incoming stream is automatically acknowledged as being down. Default is 24 hours.
CPU Threshold	Send alerts about the CPU when it exceeds this percentage. Default is 90%.
Check Collectors	If enabled, Plixer Replicator will routinely check the configured collectors for availability.
DNS Retention	When enabled, exporters and collectors will be resolved and cached for the number of hours specified.
DNS Retention Time	Number of hours to cache DNS information for exporters and collectors.
LDAP Administrator DN	The Distinguished Name (DN string) to use when connecting to LDAP.
LDAP Administrator Password	Password used in combination with the Administrator DN to bind to LDAP.
LDAP Certificate File	OPTIONAL: Path to the server's certificate (must be in PEM format)
LDAP Certificate Verification	If you specify a server certificate, you can configure whether Plixer Replicator will require that it is valid for that server.
LDAP ID Attribute	Determines what attribute to check provided usernames against on the directory server. The default is `sAMAccountName` for Active Directory. OpenLDAP generally uses `uid`.
LDAP SSL Protocol	If LDAP is configured, you may optionally specify a version of the SSL/TLS protocol that must be used.
LDAP Searchbase	Defines the group where Plixer Replicator will look for authorized users. Multiple OU's can be added by entering a semicolon separated list. Authentication can be narrowed further by specifying security groups.
LDAP Security Groups Allowed	OPTIONAL: Specify the DN of one or more security groups (semicolon delimited). Specifying at least one security group is strongly recommended, to limit the total number of users that will have full access to Plixer Replicator.
LDAP Port	The TCP port the LDAP Server is configured to use.
LDAP Server	The hostname or IP address of the LDAP server. Multiple, redundant servers can be included by using a comma separated list.
Licensing	Manages the Plixer Replicator's license key and displays license details.
Notifications	Sends Plixer Replicator alert and notification syslogs to the server IP and port number specified using the following format: <destination ip>:<destination port>.
Replication Buffer	The number of bytes to set aside for a buffer on each listening socket. Default is 32000000. Do not change this setting unless instructed by *Plixer Technical Support*.
Stop Replication	If ping is enabled and a collector is unreachable, this stops replicating data to that device. Replication will continue when the collector begins to respond to pings.
System Metrics	When enabled, statistics on CPU and memory per process are exported to the IPFIX collector specified in the *metricsSent* setting.
System Metrics Destination	Export Plixer Replicator statistics and metrics to an IPFIX collector on the specified collector IP and port number using the following format: <destination ip>:<destination port>.
Update Interval	The number of seconds to update live data. Valid range is 30 - 60 seconds.

After making changes, click the **Save** button to save the updated settings. An error message will be displayed if there are any invalid values entered.

Note: Settings can also be modified via the *interactive CLI*. See the list of supported commands to learn more.

3.2 Profile management

Plixer Replicator's replication functions are controlled by user-configured profiles, which define the destination collector(s) for the packets/flows it receives.

This section discusses how profiles work and includes instructions for their configuration and management.

3.2.1 How profiles work

As a Plixer Replicator appliance receives packets/flows, it compares a packet stream's source exporter and the UDP port it was received on against those defined in all configured profiles. If a matching profile (or profiles) exists, the stream is replicated and forwarded to the collector(s) assigned to that profile.

A profile must be configured with the following details to be considered valid:

- *Exporters*: Source network devices, such as routers, switches, or servers, whose packets/flows should be managed by the profile
- *Collectors*: Flow collectors, such as NPM, SIEM, or NDR systems, where packets associated with the profile should be sent
- *Policies*: Exporter inclusion/exclusion rules based on subnet/CIDR (can be used in place of or to complement adding individual exporters to the profile)
- *In port*: The in/listening port a packet must be received on (i.e., packets received from the same exporter but on a different port will not be managed by the profile)
- *Out Port*: The out/sending port to use to send packets to the collector(s) assigned to the profile

As part of the web interface's first login wizard, the user is walked through the process of *creating a new profile*. This profile can later be *edited* to add *exporters*, assign *collectors*, and define *policies*. Additional profiles can also be created/configured at any time.

Note:

- To send the same stream(s) to more than one collector, assign the destination collectors to a profile with the corresponding exporters.
- When a Plixer Replicator appliance is deployed as part of a Plixer Scrutinizer environment, a special *seed profile* with no collector defined must be created to allow Plixer Scrutinizer to automatically manage load balancing across its collectors. To learn more about the *Auto Replicate* feature, see this section of the Plixer Scrutinizer documentation.

3.2.2 Creating a new profile

To create a new profile, navigate to the **Profiles** tab/page of the web interface, and then proceed with the following steps:

1. Click the add (**+**) icon.
2. Fill in the fields of the **New Profile** form with the following details:
    - A name for the profile
    - The in/listening port packets must be received *from exporters* on
    - The out/sending port to use for forwarding packets *to collectors*
3. Click the **Save** button to save the profile configuration.

Once created, new profiles will be added to the main **Profiles** list/table and can be further configured at a later time.

Note: The option to automatically add exporters to the profile's *in port* can be used to automatically include new exporters to the profile after they start sending packets/flows to the Plixer Replicator appliance. To use multiple profiles to manage streams from different exporters, leave this option unchecked/disabled.

Creating new profiles via CLI

New profiles can also be created from the Plixer Replicator *interactive prompt* as follows:

1. SSH to the Plixer Replicator appliance as the `replicator` user and launch the interactive CLI.
2. Enter the following command at the `REPLICATOR>` prompt:

```
profile add [PROFILE_NAME] [IN_PORT] [OUT_PORT]
```

This will create a new profile called PROFILE_NAME with the specified *in* and *out ports*.

Deleting profiles

Profiles can be permanently deleted from either the main **Profiles** tab/page of the web interface or the profile's edit/details page.

To delete a profile via the interactive `REPLICATOR>` prompt instead, use the following command:

```
REPLICATOR> profile remove [PROFILE_NAME]
```

Note: Profiles can also be temporarily disabled and later re-enabled from the profile's edit/details page.

3.2.3 Adding exporters to a profile

To add an exporter to a profile, navigate to the **Profiles** tab/page of the web interface, and then proceed with the following steps:

1. Click the edit (pencil) icon in the **Actions** column to open the edit/details page for the profile.
2. On the edit/details page, click the add (**+**) icon for the **Exporters** list.
3. Enter the IP address of the exporter in the **Add Exporter** dialog.
4. Click the **Save** button to save the exporter to the profile.

Once saved, new exporters will be added to the **Exporters** list of the edit/details page.

Adding exporters via CLI

New exporters can also be added to profiles from the Plixer Replicator *interactive prompt* as follows:

1. SSH to the Plixer Replicator appliance as the `replicator` user and launch the interactive CLI.
2. Enter the following command at the `REPLICATOR>` prompt:

```
exporter add [EXPORTER_IP] [PROFILE_NAME]
```

This will add the exporter with the `EXPORTER_IP` IP address to the `PROFILE_NAME` profile.

Deleting exporters from a profile

To delete an exporter from a profile, click on the corresponding **-** icon in the profile's **Exporters** list.

To delete an exporter via the interactive `REPLICATOR>` prompt instead, use the following command:

```
exporter remove [EXPORTER_IP] [PROFILE_NAME]
```

This will delete the exporter with the `EXPORTER_IP` IP address from the `PROFILE_NAME` profile.

Note: The `exporter allremove [EXPORTER_IP]` command can be used to delete an exporter from all existing profiles.

3.2.4 Assigning collectors to a profile

To assign a collector to a profile, navigate to the **Profiles** tab/page of the web interface, and then proceed with the following steps:

1. Click the edit (pencil) icon in the **Actions** column to open the edit/details page for the profile.
2. On the edit/details page, click the add (**+**) icon for the **Collectors** list.
3. Enter the IP address of the collector in the **Add Collector** dialog.
4. Click the **Save** button to save the collector to the profile.

Once saved, new collectors will be added to the **Collectors** list of the edit/details page.

Assigning collectors via CLI

New collectors can also be assigned to profiles from the Plixer Replicator *interactive prompt* as follows:

1. SSH to the Plixer Replicator appliance as the `replicator` user and launch the interactive CLI.
2. Enter the following command at the `REPLICATOR>` prompt:

```
collector add [COLLECTOR_IP] [PROFILE_NAME]
```

This will assign the collector with the COLLECTOR_IP IP address to the PROFILE_NAME profile.

Deleting collectors from a profile

To delete a collector from a profile, click on the corresponding **-** icon in the profile's **Collectors** list.

To delete a collector via the interactive REPLICATOR> prompt instead, use the following command:

```
collector remove [COLLECTOR_IP] [PROFILE_NAME]
```

This will delete the collector with the COLLECTOR_IP IP address from the PROFILE_NAME profile.

Note: The `collector allremove [COLLECTOR_IP]` command can be used to delete a collector from all existing profiles.

3.2.5 Defining policies for a profile

To define an exporter inclusion or exclusion policy for a profile, navigate to the **Profiles** tab/page of the web interface, and then proceed with the following steps:

1. Click the edit (pencil) icon in the **Actions** column to open the edit/details page for the profile.
2. On the edit/details page, click the add (**+**) icon for the **Policies** list.
3. Enter the subnet/CIDR for the exporters to be defined by the policy.
4. Select whether to *include* or *exclude* the specified subnet/CIDR for the policy.
5. Click the **Save** button to save the policy to the profile.

Once saved, new policies will be added to the **Policies** list of the edit/details page.

Note:

- Policies can be only be defined using subnet/CIDR notation.
- When the Plixer Replicator receives a packet, inclusion policies are checked before exclusion policies.

Defining policies via CLI

New policies can also be defined from the Plixer Replicator *interactive prompt* as follows:

1. SSH to the Plixer Replicator appliance as the `replicator` user and launch the interactive CLI.
2. Enter the following command at the REPLICATOR> prompt:

```
policy add [SUBNET_CIDR] [PROFILE_NAME] <include|exclude>
```

This will define an `include` or `exclude` policy for the SUBNET_CIDR subnet for the PROFILE_NAME profile.

Deleting policies from a profile

To delete a policy from a profile, click on the corresponding **-** icon in the profile's **Policies** list.

To delete a policy via the interactive REPLICATOR> prompt instead, use the following command:

```
policy remove [SUBNET_CIDR] [PROFILE_NAME]
```

This will delete the policy for the SUBNET_CIDR subnet from the PROFILE_NAME profile.

3.3 Alarms

Plixer Replicator continuously monitors all collectors and exporters defined in its saved *profiles* and can alert users when a resource becomes unavailable. If an exporter stops sending packets/flows or a collector becomes unreachable, the alarm is reported via the Plixer Replicator UI and can also be sent as a syslog message to a specified server.

This section discusses how alarms work in Plixer Replicator and includes additional details related to their configuration.

3.3.1 How alarms are triggered

Once every minute, Plixer Replicator scans all interfaces in either direction (Rx and Tx).

If packet drops are observed, the system will continue to monitor the exporter or collector associated with the drops and flag it as down if it remains inactive. This will trigger an alarm for the resource and any profile it has been assigned to.

Alarms are also triggered by high CPU usage or abnormal process termination.

Note:

- Statistics reported in the *Plixer Replicator web interface* are a good reference for packet activity but not packet drops.
- The amount of time before an inactive exporter or collector is flagged is down is controlled by the *Alarm Tolerance* setting in the **Settings** tab of the UI.
- The CPU utilization percentage that will trigger an alarm is controlled by the *CPU Threshold* setting in the **Settings** tab of the UI.

3.3.2 Configuring alarm settings

The following settings in the **Settings** tab of the web interface control global behavior related to alarms in Plixer Replicator:

Alarm Tolerance	The number of minutes before an exporter or collector is flagged as down (default: 70)
Auto Acknowledge	The number of hours the alarm for a stream being down is automatically acknowledged (default: 24)
CPU Threshold	CPU utilization threshold for an alarm to be triggered (default: 90)
Check Collectors	Enable to have Plixer Replicator regularly ping collectors to confirm availability (default: enabled)
Notifications	Set a destination IP address and port to enable *syslog alarms*
Stop Replication	Enable to stop packet/flow replication and forwarding to collectors that are down (default: enabled)

Configuring alarm settings via the interactive CLI

The above settings can also be set/modified via the *interactive CLI*, by using the `setting` command with the following flags:

- **Alarm Tolerance**: `flowStopAlert`
- **Auto Acknowledge**: `downDisplayHour`
- **CPU Threshold**: `highCPUThreshold`
- **Check Collectors**: `pingCollectors`
- **Notifications**: `notificationSent`
- **Stop Replication**: `noRepWhenDown`

To learn more about issuing commands via the Plixer Replicator interactive CLI, see the command list.

3.3.3 Alarm reporting

All collectors and exporters, as well as any associated streams and profiles, that have triggered alarms are highlighted in red in their respective tabs in the Plixer Replicator web interface. Drilling into the details page for a profile will show additional information about any alarms associated with it.

Alarms via syslog

Plixer Replicator can also send alarm details in a syslog message to an external server.

To enable syslog alarms, follow these steps:

1. Log in to the web interface and navigate to the **Settings** tab.
2. In the *Notifications* setting field, enter the destination IP address and port for syslog alarms in the following format:

   ```
   SERVER_IP:PORT
   ```

3. Click the **Save** button to save any changes made.

As long as a destination server is defined for the *Notifications* setting, Plixer Replicator will automatically send alarm details in a syslog message every time an alarm is triggered.

Hint: Plixer Scrutinizer includes corresponding alarm policies for all Plixer Replicator alarms and can be used to monitor an environment for collectors and exporters that go down. View the Plixer Scrutinizer online documentation or contact *Plixer Technical Support* to learn more.

Viewing alarms via CLI

To view all active alarms in the Plixer Replicator CLI, launch the interactive prompt and enter the following command:

```
REPLICATOR> show alarms
```

The interactive commands `show` and `setting` can also be used to display additional information or generate reports based on live data. For more details on these commands and their arguments/directives, see the section on Plixer Replicator's *Interactive Mode*.

CHAPTER

FOUR

ADVANCED SERVICES

This section covers the use of Plixer Replicator's advanced functions and services.

4.1 Interactive CLI

The Plixer Replicator interactive command line interface can be used as an alternative to the web interface and supports additional administrative functions for the appliance.

The interactive prompt (REPLICATOR>) is accessed by establishing an SSH session with the Plixer Replicator server as the `replicator` user.

The `REPLICATOR>` prompt confirms that the Plixer Replicator is ready to accept commands.

Note:

- The password for the `replicator` user is configured as part of the appliance's initial setup script.
- If the SSH session is started as the `root` user, run the following to get to the `REPLICATOR>` prompt:

```
su replicator
```

Select a command below to view details about its function and usage.

4.1.1 acknowledge

The `acknowledge` command is used to set the status of an unavailable exporter or collector as *acknowledged* and stops the Plixer Replicator from sending additional notifications about the resource being down.

Syntax

```
acknowledge <exporter|collector> [ip_address:port]
```

Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.1.2 backup

The `backup` command is used to create a backup of the Plixer Replicator appliance's database in `/home/replicator/backups/`. Backup filenames cannot contain spaces.

Syntax

```
backup [filename]
```

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.3 collect supportfiles

The `collect supportfiles` command is used to compile all relevant logs and configuration files and compress them into a tar.gz file in the `/home/replicator/supportfiles` directory. Use the *upload supportfiles* command to send collected support files to Plixer support for analysis.

Syntax

```
collect supportfiles
```

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.4 collector

The `collector` command is used to add or remove a collector to/from a profile or set a rate threshold for the collector.

Options and syntax

`collector add`	Adds a collector (IP) to the Plixer Replicator profile name specified.
`collector remove`	Removes a collector (IP) from the Plixer Replicator profile name specified.
`collector allremove`	Removes the collector (IP) from all the Plixer Replicator profiles.
`collector threshold`	Sets the maximum packet/s for the collector (IP).

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.5 exporter

The `exporter` command is used to manage exporters in a Plixer Replicator profile.

Options and syntax

`exporter add [exporter_ip] [profile_name]`	Adds an exporter (IP) to/from the Plixer Replicator profile name specified.
`exporter remove [exporter_ip] [profile_name]`	Removes a collector (IP) from the Plixer Replicator profile name specified.
`exporter allremove`	Removes the exporter (IP) from all the Plixer Replicator profiles.
`exporter noprofile`	Returns a list of exporters not currently assigned to any profile.

If an exporter does not need to be added to any profile, it should be configured to stop sending flows to the Plixer Replicator appliance. It is normal for exporters that send flows infrequently to be listed as having sent 0 packets.

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.6 ldapadminpass

The `ldapadminpass` command is used to set the LDAP admin password.

Syntax

```
ldapadminpass
```

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.7 license

The `license` command is used to set a new license key or display the details of the current license.

Options and syntax

`license <set|update>`	Opens a popup for the user to enter a new license key. To generate a license key, Plixer or the reseller will need the Plixer Replicator appliance's unique machine ID.
`license <check|status>`	Returns the details of the currently applied license key. The machine ID can be viewed with the `license check` command.

The *show status* command can also be used to verify that a license key has been properly applied. To learn more about licensing options or obtain a key, *contact Plixer Technical Support*.

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.8 notate

The `notate` command is used to add a description/note to a profile or IP address.

Options and syntax

`notate profile [profile_name]␣ ↪[description]`	Adds a description to the profile specified.
`notate ip [ip_address] [description]`	Adds a description to the IP address specified.

If a blank description is passed in for an IP address, then the entry is removed from the asset report.

To use quotes in a description they will need to be escaped as \. To use a backslash use, \\.

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.9 password

The `password` command is used to set the password for the `admin` user (web interface) or `replicator` user (interactive CLI). The new password will be applied for the next login.

Options and syntax

`password interactive`	Sets a password for the `replicator` user (interactive CLI). When setting a new `replicator` user password, you will be prompted to enter the current password.
`password webui`	Sets a password for the `admin` user (web interface).

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.10 policies

The `policies` command is used to add or remove a policy to/from a Plixer Replicator profile. Policies can only be defined using the subnet/CIDR notation.

Options and syntax

`policies add [subnet/cidr] [profile] <include|exclude>`	Adds a subnet/CIDR to the Plixer Replicator profile name specified.
`policies remove [subnet/cidr] [profile]`	Removes a subnet/CIDR from the Plixer Replicator profile name specified.

`<include|exclude>` is only required if `add` is used.

To catch all exporters, add an include policy of 0.0.0.0/0. Although you can create policies for a single IP address (e.g., 192.168.2.4/32), it is recommended to manually create policies that include groups of addresses (e.g., 192.168.2.0/24).

Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.1.11 profile

The `profile` command is used to add a new Plixer Replicator profile or update an existing profile's settings.

Options and syntax

`profile <add|update> [profile_name] [listen_port] [send_port]`	Adds a new profile or updates an existing profile's settings. All parameters are required when add or update is used.
`profile <remove|disable|enable> [profile_name]`	Removes, disables, or enables the profile specified.
`profile rename [old_name] [new_name]`	Renames the profile.
`profile singularity [profile_name] <enable|disable>`	Enables or disables sending the Plixer Replicator appliance's IP address as a packet's source (default: disabled).

You can manipulate a profile with spaces in its name by enclosing the name in quotes. Furthermore, if you must manipulate a profile with quotes in its name, you can do so by using `\"` to escape the quote, as well `\\` to escape a backslash.

Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.1.12 rebuild

The `rebuild` command is used to rewrite the internal configuration of the appliance when replication services are down and issues cannot be resolved by other means.

Note: This command can alter Plixer Replicator functionality and should be used with caution.

Syntax

```
rebuild
```

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.13 restore

The `restore` command is used to restore a database from a file in `/home/replicator/backups`. The backup must share the same version as the current version of Plixer Replicator.

Important: Restore also reverts the database to the same version of PostgreSQL that was in use when the backup file was created.

Syntax

```
restore [filename]
```

The Plixer Replicator database can be also backed up with the *backup* command. Available backups can be viewed with the *show backup* command.

Hint: For assistance, enter <command> `help`, `help` <command>, <command> `?`, or `?` at any time.

4.1.14 role

The `role` command is used to assign roles to individual appliances in *high availability configurations*.

Note: These commands can alter Plixer Replicator functionality and should be used with caution.

Options and syntax

`role set ha master [ip_address]`	Sets the IP address of the primary replicator.
`role set ha off`	Reverts the primary and secondary Plixer Replicator appliances to their previous state.
`role set ha on [priority] [virtual_ip] [ifname] <master|backup>`	Enables single-network high availability on the primary replicator.
`role set primary`	Assigns the replicator the primary role. If the replicator is set as a secondary and you wish to make it a primary, make sure to set the current primary replicator offline first, else, duplicate packets will be replicated to the configured collectors.
`role set secondary [primary_replicator_ip:listener_port] [timeout]`	Assigns the appliance the secondary role. `[timeout]` represents number of sample cycles (10 seconds) before the secondary appliance deems the primary appliance unavailable and then springing into action as the primary. The default timeout is 2 sample cycles (or 20 seconds).
`role test <ha|secondary>`	Tests the secondary appliance's connectivity to the primary appliance.

Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.1.15 setting

The `setting` command is used to configure the Plixer Replicator appliance's global settings, allowing features to be enabled, disabled, or modified.

Note: These commands can alter Plixer Replicator functionality and should be used with caution.

Options and syntax

`setting set <flag> [value]`	Sets a replicator setting based on the variable and value provided.
`setting <enable|disable> <flag>`	Enables/disables a replicator setting based on the variable and value provided.

Settings can also be managed via the *Settings* tab/page of the Plixer Replicator web interface.

Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.1.16 show

The `show` command is used to generate various reports on the Plixer Replicator appliance's configuration and operational data.

Options and syntax

`show alarm [filter]`	Lists exporters that have stopped sending packets and collectors that can no longer be reached.
`show asset [filter]`	Lists IP addresses associated with the appliance, along with their roles (exporter or collector), DNS names, and descriptions/notes.
`show backups [filter]`	Lists files in the `home/replicator/backups` directory along with the date they were last accessed.
`show collector [filter]`	Lists collectors, with their IP addresses, DNS names, descriptions/notes, and profiles they're currently assigned to.
`show config`	Lists all commands necessary to rebuild profile settings.
`show exporter [filter]`	Lists exporters, along with their IP addresses, DNS names, descriptions/notes, and profiles they're currently assigned to.
`show profile [filter]`	Lists profiles, along with their policies, exporters, and collectors.
`show realtime [filter]`	Displays real-time data on exporters, such as their inbound and outbound traffic and CPU usage (press CTRL+C to exit the report).
`show setting [filter]`	Displays all global settings along with their statuses (enabled or disabled) and/or current values.
`show status`	Lists all of the Plixer Replicator's services and licenses along with their statuses.

Most `show` commands can also be entered with a filter argument to display only details that match the provided string. When no filter is entered, the full report will be returned.

Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.1.17 system

The `system` command is used to manage the state and certain settings of the Plixer Replicator appliance.

Note: These commands can alter Plixer Replicator functionality and should be used with caution.

Options and syntax

`system change`	Changes the host name or the IP address of the replicator.
`system restart`	Reboots the entire appliance.
`system shutdown`	Powers off the appliance completely.
`system virtualip <enable|disable> ↪<interface_name> [virtual_ip]`	Adds or removes a virtual IP address for High Availability (HA) configurations.

Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.1.18 upload supportfiles

The `upload supportfiles` command is used to send collected support files to Plixer support for analysis after using the *collect supportfiles* command.

Syntax

```
upload supportfiles
```

Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.1.19 version

The `version` command is used to show the current version of the Plixer Replicator appliance.

Syntax

```
version
```

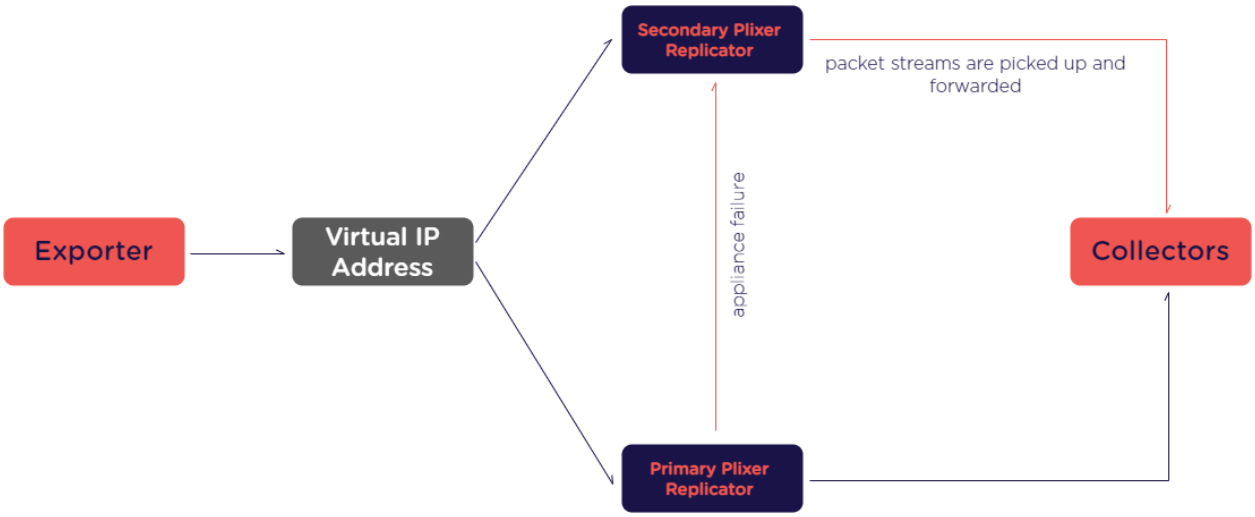
Hint: For assistance, enter `<command> help`, `help <command>`, `<command> ?`, or `?` at any time.

4.2 High availability configurations

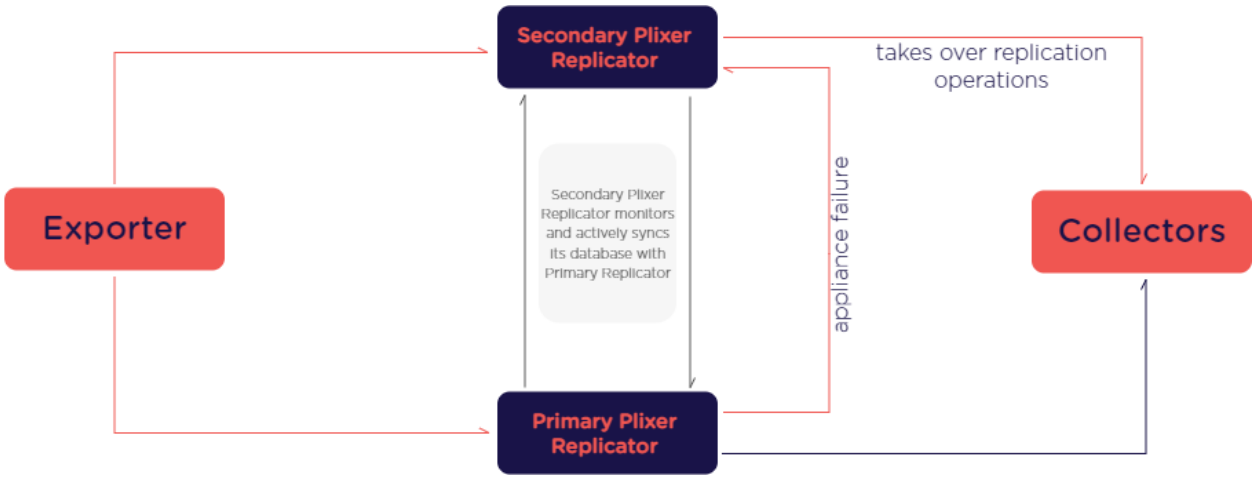
A second Plixer Replicator appliance can be deployed for fault tolerance in environments where high availability is critical. Both hardware and virtual appliances (in any combination) can be used for these configurations.

Plixer Replicator appliances have two high-availability configurations that can be used:

Single Network High Availability configuration:



Multi-Network High Availability configuration:



4.2.1 Single-network high availability

The single-network high availability configuration is meant for environments where two Plixer Replicator appliances can be deployed on the same subnet. In this configuration, packets are sent to a virtual IP address that the primary (master) and secondary (backup) appliances are both configured to listen to for traffic. Because each appliance in high availability mode is assigned a priority, they are aware of their role in the configuration.

When the primary appliance goes offline, the packet streams are immediately picked up by the secondary instance and forwarded to the same collectors. Once the primary appliance is active again, it will resume its previous functions.

The single-network high availability configuration can also be extended to create additional redundancy beyond a basic primary + secondary setup.

Requirements

Setting up a single-network high availability configuration has the following requirements:

- A primary Plixer Replicator
- A secondary Plixer Replicator
- Exporters must be configured to send flows to a single virtual IP address.
- The primary and secondary appliances must have the same password set for the web interface `admin` user.

Important: The secondary Plixer Replicator appliance must be licensed specifically for use as a secondary/backup appliance in a single-network high availability configuration. After a valid failover license is obtained, it should be applied to the appliance intended for use as the secondary/backup instance. Contact *Plixer Technical Support* to learn more.

Configuration steps

To set up the primary and secondary Plixer Replicator appliances for single-network high availability, follow these steps:

1. Deploy the primary and secondary appliances as normal following the instructions in the *deployment guides*.
2. SSH to the primary appliance as the `replicator` user and launch the interactive prompt (`REPLICATOR>`).
3. Add the virtual IP address to the primary Plixer Replicator appliance:

   ```
   system virtualip enable eth0 [VIRTUAL_IP]
   ```

4. Set the IP address of the primary appliance:

   ```
   role set ha master [PRIMARY_IP]
   ```

5. Enable single-network high availability on the primary appliance:

   ```
   role set ha on 101 [VIRTUAL_IP] eth0 master
   ```

   When prompted, enter the web interface `admin` user's password.

6. SSH to the secondary appliance as the `replicator` user and launch the interactive prompt (`REPLICATOR>`).
7. Add the virtual IP address to the secondary Plixer Replicator appliance:

   ```
   system virtualip enable eth0 [VIRTUAL_IP]
   ```

8. Add the IP address of the primary appliance to the secondary appliance:

   ```
   role set ha master [PRIMARY_IP]
   ```

9. Enable single-network high availability on the secondary appliance:

   ```
   role set ha on 100 [VIRTUAL_IP] eth0 backup
   ```

   When prompted, enter the web interface `admin` user's password.

10. Test whether single-network high availability has been enabled successfully:

a. Run the following command from the REPLICATOR> prompt on both appliances:

```
role test ha
```

b. Shut down the primary appliance and ping the virtual IP address.

If a response is received from the virtual IP address, single-network high availability has been correctly configured. The primary Plixer Replicator appliance can then be restarted as normal.

Disabling single-network high availability

To revert the primary and secondary Plixer Replicator appliances to their previous state, run the following commands from the REPLICATOR> prompt on both appliances:

```
role set ha off
system virtualip disable eth0 [VIRTUAL_IP]
```

4.2.2 Multi-network high availability

The multi-network/traditional high availability configuration is meant for environments where two Plixer Replicator appliances are on different subnets. In this configuration, the secondary appliance actively monitors the state of the primary appliance and regularly syncs its database with the primary's settings.

When the secondary appliance detects that the primary is offline, it attempts to reach all known collectors. If it can reach the collectors, the secondary appliance takes over replication using the profiles that were last synced from the primary appliance. If the collectors are not reachable, it retains its secondary role until a collector or the primary Plixer Replicator becomes reachable again.

The secondary appliance continues to monitor the state of the primary appliance, even after it has taken over replication. When the primary appliance becomes available again, any updates will be synced to the database before the secondary appliance reverts to the monitor-and-sync role.

Important: When a Plixer Replicator appliance is assigned the secondary role, its current configuration will be replaced by the database synced from the primary appliance and changes to its settings will no longer be allowed. The `role` and `show` commands may still be issued from the interactive prompt, but any modification to its profiles or global settings must be applied through the primary appliance.

Requirements

Setting up a multi-network high availability configuration has the following requirements:

- A primary Plixer Replicator
- A secondary Plixer Replicator
- Exporters must be configured to send flows to both the primary and secondary appliances.

Configuration steps

To set up the secondary Plixer Replicator appliance in a multi-network high availability configuration, follow these steps:

1. Deploy the appliance as normal following the instructions in the *deployment guides*.
2. SSH to the appliance as the `replicator` user and launch the interactive prompt (`REPLICATOR>`).
3. Assign the appliance the secondary role:

   ```
   role set secondary [PRIMARY_IP:LISTENER_PORT] [TIMEOUT]
   ```

   `LISTENER_PORT` must be the port being used by the primary appliance to actively listen for packets, and the `TIMEOUT` argument defines the number of missed polls allowed before the secondary appliance attempts to take over replication (default: 2).
4. Test the the secondary appliance's connectivity to the primary appliance by running the following command:

   ```
   REPLICATOR> role test secondary
   ```

If the test is successful, the appliance has successfully been assigned the secondary role for multi-network high availability.

Disabling multi-network high availability

A secondary appliance in a multi-network high availability configuration can be reverted to its standalone state at any time by running the following from the `REPLICATOR>` prompt:

```
REPLICATOR> role set primary
```

Note:

- To set up either type of HA configuration, a failover license must first be obtained and applied to the Plixer Replicator appliance intended for use as the secondary/backup. Contact *Plixer Technical Support* to learn more.
- Both hardware and virtual appliances (in any combination) can be used in these configurations.

4.3 Plixer Replicator APIs

Plixer Replicator provides a comprehensive set of RESTful APIs that enable programmatic management and monitoring of its functionalities.

Select an API below to view details about its function and usage.

4.3.1 Acknowledge

Used to acknowledge collectors and exporters that have triggered alarms

Resource URL:

`https://[replicator]/api/1/acknowledge/[entity]/[ip:port]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[entity]	`exporter` or `collector`
[ip:port]	IP address and port of the [entity] to be acknowledged

Example request:

`https://10.30.17.131/api/1/acknowledge/collector/10.1.10.4:2055`

Example response:

```
{
   "description": "Success: collector '10.1.10.4:2055' acknowledged.",
   "result": "success"
}
```

4.3.2 Authentication

Used to authenticate the user and start/stop API sessions

Login

Starts a new API session

GET request:

Note: Legacy API – Deprecated- recommend using POST

Resource URL:

`https://[replicator]/api/1/login/[sha3]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[sha3]	Web interface *admin* password converted to SHA3 512-bit hex

Example request:

`https://10.30.17.131/api/1/login/098f6bcd4621d373ca098f6bcd4621d563cade4e832629b4f6d098f4bcd4621d37`

POST request:

Starts a new API session

Resource URL:

`https://[replicator]/api/1/login/`

```
{
 “user” : “[user]”
 “passwd”: “[passwd]”
}
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[user]	*admin* or (if configured) LDAP username
[passwd]	Plaintext password for the specified user

Example response:

```
{
 "path": "login successful.",
 "result": "success"
}
```

Log out

Manually terminates an API session (API sessions are automatically terminated after 30 minutes)

Resource URL:

`https://[replicator]/api/1/logout`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator

Example request:

`https://10.30.17.131/api/1/logout`

Example response:

```
{
 "path": "logout successful.",
 "result": "success"
}
```

4.3.3 Collector

Used for collector management operations for profiles

Resource URL:

Manages a collector for an individual profile

`https://[replicator]/api/1/collector/[action]/[ip]/[profile]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[action]	`add` or `remove`
[ip]	IP address of the collector
[profile]	Target profile for the operation

Example request:

`https://10.30.17.131/api/1/collector/add/10.1.10.60/myprofile`

Example response:

```
{
  "description": "Success: Collector [10.1.10.60] -> Profile [myprofile]",
  "result": "success"
}
```

Resource URL:

Removes a collector from all profiles

`https://[replicator]/api/1/collector/allremove/[ip]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[ip]	IP address of the collector to be removed

Example request:

`https://10.30.17.131/api/1/collector/allremove/10.1.10.4`

Example response:

```
{
  "description": "Success: Collector [10.1.10.4] <- All Profiles",
  "result": "success"
}
```

4.3.4 DNSCheck

Used to perform a DNS check on an IP address

Resource URL:

Forces a DNS name resolution for an IP address

`https://[replicator]/api/1/dnscheck/[ip]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[ip]	IP address to resolve

Example request:

`https://10.30.17.131/api/1/dnscheck/10.1.1.3`

Example response:

```
{
  "dnscheck": {
  "addr": "10.1.1.3",
  "expiry": {
  "epoch": 1462801036,
  "time": "Mon May 9 09:37:16 2016"
  },
  "name": "newexp.plxr.local",
  "resolveTime": 0.04485,
  "status": "success"
  }
}
```

4.3.5 Exporter

Used for exporter management operations for profiles

Resource URL:

Manages an exporter for an individual profile

```
https://[replicator]/api/1/exporter/[action]/[ip]/[profile]
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[action]	`add` or `remove`
[ip]	IP address of the exporter
[profile]	Target profile for the operation

Example request:

```
https://10.30.17.131/api/1/exporter/add/10.1.1.1/myprofile
```

Example response:

```
{
  "description": "Success: Exporter [10.1.1.1] -> Profile [myprofile]",
  "result": "success"
}
```

Resource URL:

Removes an exporter from all profiles

```
https://[replicator]/api/1/exporter/allremove/[ip]
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[ip]	IP address of the exporter to be removed

Example request:

```
https://10.30.17.131/api/1/exporter/allremove/10.1.1.4
```

Example response:

```
{
   "description": "Success: Exporter [10.1.1.4] <- All Profiles",
   "result": "success"
}
```

Resource URL:

Identifies exporters that are sending data to the Plixer Replicator but not assigned to any profiles

```
https://[replicator]/api/1/exporter/noprofile/[filter]
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[filter]	Optional filter to apply to the displayed list of exporters not assigned to any profiles; returns the full list if not provided

Example request:

```
https://10.30.17.131/api/1/exporter/noprofile/0
```

Example response:


```
{
  "noprofile": {
    "10.30.17.131": {
      "in_o_delta": 0,
      "in_o_rate": "0.0",
      "in_p_delta": 0,
      "in_p_rate": "0.0",
      "lastseen": "Tue Apr 19 09:55:18 2016",
      "out_o_delta": 1493,
      "out_o_rate": "49.8",
      "out_p_delta": 6,
      "out_p_rate": "0.2",
      "unixtime": 1461074118
    },
    "total": 1
  }
}
```


4.3.6 License

Used to check the license status/details for the Plixer Replicator appliance

Resource URL:

Returns the details of the current license

```
https://[replicator]/api/1/license/check
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator

Example request:

```
https://10.30.17.131/api/1/license/check
```

Example response:


```
{
    "daysLeft" : "365 day(s)",
    "expiration" : "Thu May 18 2017",
    "licensedType" : "eval",
    "licensedVersion" : "16.6",
    "machineID" : "6YZ6XEPTA66JA6VHFPXG749B",
    "role" : "failover"
}
```

4.3.7 Notate

Used to add a description to an exporter, collector, or profile

Resource URL:

`https://[replicator]/api/1/notate/[entity]/[identity]/[description]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[entity]	`profile` or `ip`
[identity]	`[profile_name]` or `[ip_address]` of entity specified
[description]	Description or note to add to the entity in standard ASCII URI-compatible characters

Example request:

`https://10.30.17.131/api/1/notate/profile/myprofile/My_Fantastic_Description`

Example response:

```
{
    "description": "Success: Profile 'myprofile' has a new description",
    "result": "success"
}
```

4.3.8 Policies

Used to manage policies for profiles

Resource URL:

`https://[replicator]/api/1/policies/[action]/[network]/[cidr]/[profile]/[incexc]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[action]	`add` or `remove`
[network]	address of the network (e.g. 172.17.0.0)
[cidr]	CIDR of the network specified (e.g. 16)
[profile]	Target profile for the operation
[incexc]	`include` or `exclude`

Example request:

`https://10.30.17.131/api/1/policies/add/10.1.20.0/16/myprofile/include`

Example response:

```
{
    "description": "Success: Policy [10.1.20.0/16] -> Profile [myprofile]",
    "result": "success"
}
```

4.3.9 Profile

Used to manage profile settings and behavior

Resource URL:

Renames an existing profile

`https://[replicator]/api/1/profile/rename/[current]/[new]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[current]	Name of the profile to be renamed
[new]	New name for the profile

Example request:

`https://10.30.17.131/api/1/profile/rename/oldprofile/myprofile`

Example response:

```
{
    "description": "Success: Profile 'oldprofile' is now 'myprofile'",
    "result": "success"
}
```

Resource URL:

Toggles the singularity setting for a profile

`https://[replicator]/api/1/profile/singularity/[name]/[action]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[name]	Name of the profile to be updated
[action]	`enable` or `disable`

Example request:

`https://10.30.17.131/api/1/profile/singularity/myprofile/enable`

Example response:

```
{
    "description": "Success: Profile 'myprofile' singularity enabled",
    "result": "success"
}
```

Resource URL:

Removes, disables, or enables a profile

`https://[replicator]/api/1/profile/[action]/[name]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[action]	`remove`, `disable`, or `enable`
[name]	Target profile for the operation

Example request:

`https://10.30.17.131/api/1/profile/disable/myprofile`

Example response:

```
{
    "description": "Success: Profile myprofile has been set to 'disable'",
    "result": "success"
}
```

Resource URL:

Creates a new profile or updates an existing profile

`https://[replicator]/api/1/profile/[action]/[name]/[listeningport]/[sendingport]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[action]	`add` or `update`
[name]	Name of the profile to create or update
[listeningport]	UDP port to listen to for incoming packets (In Port)
[sendingport]	The UDP port to send packets from (Out Port)

Example request:

`https://10.30.17.131/api/1/profile/add/myprofile/2055/4739`

Example response:

```
{
    "description": "Success: Profile 'myprofile' has been added and enabled.",
    "result": "success"
}
```

4.3.10 Rebuild

Used to force the Plixer Replicator appliance to immediately rebuild its internal configuration

Resource URL:

`https://[replicator]/api/1/rebuild`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator

Example request:

`https://10.30.17.131/api/1/rebuild`

Example response:

```
{
    "description": "rebuild request submitted",
    "result": "success"
}
```

4.3.11 Role

Used to test whether a secondary appliance in a high availability configuration has been configured correctly

Resource URL:

`https://[replicator]/api/1/role/test/secondary`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator

Example request:

`https://10.30.17.131/api/1/role/test/secondary`

Example response:

```
{
    "description": "!!! This replicator is the primary !!!",
    "result": "error"
}
```

4.3.12 Setting

Used to manage the Plixer Replicator appliance's global settings

Resource URL:

Sets the value for the specified setting

`https://[replicator]/api/1/setting/set/[name]/[value]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[name]	Exact name of the setting to modify
[value]	New value for the setting specified

Example request:

`https://10.30.17.131/api/1/setting/set/metricssent/10.1.2.3:2055`

Example response:

```
{
    "description": "Success: setting 'metricssent' has been set to '10.1.2.3:2055'",
    "result": "success"
}
```

Resource URL:

Enables or disables the specified feature

`https://[replicator]/api/1/setting/[action]/[name]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[action]	`enable` or `disable`
[name]	Exact name of the feature to enable/disable

Example request:

```
https://10.30.17.131/api/1/setting/disable/metricssent
```

Example response:

```
{
    "description": "Success: setting 'metricssent' has been set to 'disable'",
    "result": "success"
}
```

4.3.13 Show

Displays configuration details and real-time information from the Plixer Replicator appliance

Resource URL:

Displays the current configuration of the Plixer Replicator

```
https://[replicator]/api/1/show/config
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator

Example request:

```
https://10.30.17.131/api/1/show/config
```

Example response:

```
{
 "api": {
  "collector": [
   "/api/1/collector/add/10.30.1.20/benchmark-20",
   ...
  ],
  "notate": [
   "/api/1/notate/ip/10.1.4.101/ej-win2012 install test machine (fresh)",
   ...
  ],
  "policy": [
   "/api/1/policies/add/10.1.1.252/32/buildqa/include",
   ...
  ],
  "profile": [
   "/api/1/profile/add/frandev/2002/2055",
   ...
  ]
 },
 "cli": {
  "collector": [
   "collector add 10.30.1.20 benchmark-20",
   ...
  ],
  "notate": [
   "notate ip 10.1.4.101 ej-win2012 install test machine (fresh)",
   ...
```

(continues on next page)

(continued from previous page)

```
  ],
  "policy": [
   "policy add 10.1.1.252/32 buildqa include",
   ...
  ],
  "profile": [
   "profile add frandev 2002 2055",
   ...
  ]
 }
}
```

Resource URL:

Displays the current status of the appliance

```
https://[replicator]/api/1/show/status
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator

Example request:

```
https://10.30.17.131/api/1/show/status
```

Example response:

```
{
   "converting syslog" : "active",
   "ipfixify system metrics" : "active",
   "replicating port 2002" : "active",
   "replicating port 2003" : "active",
   "replicating port 2055" : "active",
   "replicator api" : "active",
   "replicator license" : "259 day(s)",
   "replicator monitor" : "active",
   "replicator vitalizer" : "active",
   "result" : "success",
   "version" : "v17.12.19.2255"
}
```

Resource URL:

Displays real-time data from the appliance

```
https://[replicator]/api/1/show/realtime/[filter]
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[filter]	Currently not supported; defaults to full report if not provided

Example request:

```
https://10.30.17.131/api/1/show/realtime/0
```

Example response:

```
{
 "collector": {
  "10.1.4.19": {
   "in": {
    "octets": {
     "delta": 0,
     "rate": 0
    },
     "packets": {
     "delta": 0,
     "rate": 0
    }
   }
  },
  "10.1.4.20": {
   ...
  },
},
"exporter": {
 "10.30.17.131": {
  "awareness": {
   "last_epoch": 1461175921,
   "last_timestamp": "2016-04-20 14:12:01"
  },
  "in": {
   "octets": {
    "delta": 0,
    "rate": "0.0"
   },
   "packets": {
    "delta": 0,
    "rate": "0.0"
   }
  },
  "out": {
   "octets": {
    "delta": 0,
    "rate": "0.0"
   },
   "packets": {
    "delta": 0,
    "rate": "0.0"
   }
  },
  "profiles": [
   "benp"
  ]
 }
},
"pair": {
 "10.30.17.131 -> 10.1.4.19": {
  "octets": {
   "delta": 0,
```


(continues on next page)

(continued from previous page)


```
   "rate": 0
  },
  "packets": {
   "delta": 0,
   "rate": 0
  }
 },
 "10.30.17.131 -> 10.1.4.20": {
  ...
 },
 "profile": {
  "benp": {
   "in": {
    "octets": {
     "delta": 0,
     "rate": 0
    },
    "packets": {
     "delta": 0,
     "rate": 0
    }
   },
   "out": {
    "octets": {
     "delta": 0,
     "rate": 0
    },
   "packets": {
    "delta": 0,
    "rate": 0
   }
  }
 }
},
"stats": {
 "totals": {
  "collectors": 2,
  "exporters": 1,
  "pairs": 2,
  "profiles": {
   "disabled": 3,
   "enabled": 67,
   "total": 70
  }
 }
},
"system": {
 "cpu": "0"
}
```


Resource URL:

Displays various configuration details for the appliance

`https://[replicator]/api/1/show/[entity]/[filter]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[entity]	`alarms`, `assets`, `collectors`, `config`, `exporters`, `profile`, `realtime`, `settings`, or `status`
[filter]	Optional filter to apply to the output; defaults to the full report if not provided

Example request:

`https://10.30.17.131/api/1/show/collectors/10.1.10.1`

Example response:


```
{
 "collectors": {
  "10.1.10.1": {
   "acknowledged": [
    9996
   ],
   "description": "erpdev",
   "in_profiles": [
    "steady-replays"
   ],
   "ip": "10.1.10.1",
   "name": null,
   "status": {
    "unreachable_port": [
     "9996"
    ],
   }
   "threshold": 10000
  }
 }
}
```


4.3.14 Threshold

Used to set packet per second thresholds that will trigger warnings for collectors

Resource URL:

`https://[replicator]/api/1/collector/threshold/[collector]/[threshold]`

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator
[collector]	IP address of the collector
[threshold]	Threshold value in packets per second; disabled if set to 0

Example request:

`https://10.30.17.131/api/1/collector/threshold/10.1.5.2/10000`

Example response:

```
{
  "description": "Success: Collector [10.1.5.2] threshold set to 10000",
  "result": "success"
}
```

4.3.15 Version

Used to display the Plixer Replicator appliance's version information

Resource URL:

```
https://[replicator]/api/1/version
```

Parameter	Description
[replicator]	Hostname or IP address of the Plixer Replicator

Example request:

```
https://10.30.17.131/api/1/version
```

Example response:

```
{
      "apiversion" : "1",
      "bestipfixcollector" : "Need an IPFIX Collector? Download Scrutinizer at␣
↪https://www.plixer.com",
      "build" : "2019-12-03 13:07:44 -0500 (Tue, 03 Dec 2019)",
      "copyright" : "Copyright (C) 2012 - 2019 Plixer, All rights reserved.",
      "name" : "Plixer Replicator (TM) v19.0.0.101236",
      "result" : "success",
      "yeswecan" : "Replicate Anything!"
}
```

4.4 Version upgrades

Version upgrades may include additional functionality, performance enhancements, and/or other improvements over previous versions. Fixes for certain types of issues will also be included in these updates.

Select a version below for upgrade instructions:

4.4.1 Upgrading to v19.1.1

Because Plixer Replicator v19.1.1 includes an OS update, v19.0.1 is **required** for the upgrade. If you are running an older version, follow *this guide to upgrade your appliance to v19.0.1*.

For assistance or clarifications, contact *Plixer Technical Support*.

Important notes

- The upgrade will take **at least** one hour to complete.
- If the Plixer Replicator appliance is able to access files.plixer.com, the `REPO_HOST` variable should be set to *files.plixer.com* for the steps outlined below. For *offline upgrades*, the IP address of the offline repo should be used instead.
- Due to an increase in minimum specs, older VMs with 2 GB of RAM should be provisioned with 4 GB RAM before the upgrade.
- The upgrade requires a minimum of 16 GB free space on root (`/`). There may be older logs (`sudo rm /var/log/messages-*`) that can be deleted to free up space.

Upgrade process

The process of upgrading a v19.0.1 Plixer Replicator appliance to v19.1.1 involves the following steps:

- Backing up the v19.0.1 database and server-specific files using the `backup` *interactive mode command*
- Downloading the operating system upgrade script, `olmigrate.run`, and running it a total of four times (with a reboot between runs)
- Downloading and running the Plixer Replicator v19.1.1 installation script (`replicator-install.run`)
- Verifying that the v19.0.1 data has been successfully migrated after v19.1.1 is installed

Pre-upgrade preparation

- [Hardware appliances] Create a backup of the current Plixer Replicator appliance using the `backup` *interactive mode command* (under `/home/replicator/backups`) and store it on an external system/drive.
- [Virtual appliances] Backup the current Plixer Replicator install by taking a VM snapshot.
- Confirm the current password for the `replicator` SSH user (run `passwd replicator`)
- Verify that root login is disabled by running:

```
sudo sed -i 's/^#PermitRootLogin.*/PermitRootLogin no/g' /etc/ssh/sshd_config
```

- [Offline upgrades] If the Plixer Replicator appliance does not have access to `files.plixer.com`, *set up an offline repository for this upgrade*.

Upgrading the server

Once all preparation steps have been completed, follow these steps to upgrade the appliance:

Important:

- For offline upgrades, `REPO_HOST` should point to the IP address of the *offline repo* instead of `files.plixer.com`.
- In *high-availability configurations*, complete the upgrade for the secondary appliance before the primary.
- To verify the current progress of the OS upgrade at any time:

```
cat /etc/motd
```

or check versions between runs (NAME= and VERSION= lines):

```
cat /etc/os-release
```

---

1. SSH to the v19.0.1 appliance to be upgraded as the `replicator` user.
2. Verify that the current working directory is correct (`replicator`):

```
cd /home/replicator/
```

3. Download the OS upgrade script and its checksum file:

```
REPO_HOST=files.plixer.com
curl -k -o olmigrate.run https://$REPO_HOST/plixer-repo/replicator/19.1.1/olmigrate.
↪run
curl -k -o olmigrate.run.sha256 https://$REPO_HOST/plixer-repo/replicator/19.1.1/
↪olmigrate.run.sha256
```

4. Validate the integrity of `olmigrate.run`:

```
cat olmigrate.run.sha256
sha256sum olmigrate.run
```

5. Set the correct permissions for the OS upgrade script:

```
chmod a+x olmigrate.run
```

6. Run the `olmigrate.run` script a total of four times:

```
REPO_HOST=files.plixer.com ./olmigrate.run -- -k
```

Important: Reboots between runs of the OS upgrade script (`olmigrate.run`) can take a long time. Before trying to reconnect to the appliance, start a `PING` to the Plixer Replicator IP address and wait for it to become available again. **Do NOT manually reboot the server**.

---

7. After the fourth `olmigrate.run` run (there will be no reboot), change directories to `/tmp` for the installation of Plixer Replicator v19.1.1:

```
cd /tmp/
```

8. Download the Plixer Replicator v19.1.1 installation script and its checksum file:

```
REPO_HOST=files.plixer.com
curl -k -o replicator-install.run https://$REPO_HOST/plixer-repo/replicator/19.1.1/
↪replicator-install.run
curl -k -o replicator-install.run.sha256 https://$REPO_HOST/plixer-repo/replicator/
↪19.1.1/replicator-install.run.sha256
```

9. Validate the integrity of `replicator-install.run`:

```
cat replicator-install.run.sha256
sha256sum replicator-install.run
```

10. Update permissions for the `replicator-install.run` script:

```
chmod a+x replicator-install.run
```

11. Run `replicator-install.run` to install Plixer Replicator v19.1.1:

```
REPO_HOST=files.plixer.com ./replicator-install.run -- -k
```

12. After the installation script finishes running, reboot the appliance:

```
sudo shutdown -r now
```

13. After the reboot, SSH to the appliance again to reset the password for the `admin` UI user:

```
manage --cli
password webui
```

After completing the above steps, the Plixer Replicator appliance will be on v19.1.1.

Offline upgrades to v19.1.1

The following instructions for setting up an offline repo are intended for upgrading to Plixer Replicator v19.1.1 only.

1. Deploy a new Plixer Scrutinizer v19.5.0 VM and assign an IP address to it.
2. SSH to the VM as the `plixer` user:

```
ssh plixer@SCRUTINIZER_VM_IP
```

3. Create the offline repo directory and assign it the correct permissions:

```
sudo mkdir /var/db/big/offline
sudo chown plixer:plixer /var/db/big/offline
```

4. Download the offline tar file for Plixer Replicator 19.1.1 and its checksum file:

```
curl -o /var/db/big/offline/19.1.1_offline.tgz https://files.plixer.com/plixer-repo/
↪replicator/19.1.1_offline.tgz
curl -o /var/db/big/offline/19.1.1_offline.tgz.sha256 https://files.plixer.com/
↪plixer-repo/replicator/19.1.1_offline.tgz.sha256
```

5. Validate the integrity of `19.1.1_offline.tgz`:

```
cat /var/db/big/offline/19.1.1_offline.tgz.sha256
sha256sum /var/db/big/offline/19.1.1_offline.tgz
```

6. Extract the offline tar file:

```
cd /var/db/big/offline
tar xvf 19.1.1_offline.tgz
```

7. Create a symlink in the html directory to the offline repo:

```
ln -s /var/db/big/offline/plixer-repo /home/plixer/scrutinizer/html/plixer-repo
```

After the offline repo has been set up, the VM's IP address should be used in place of `files.plixer.com` for `REPO_HOST` in the *upgrade instructions*.

4.4.2 Upgrading to v19.0.1

To upgrade to Plixer Replicator v19.0.1, *v18.14 or higher* is required.

Hint: For clarifications or assistance with upgrading, contact *Plixer Technical Support*.

Upgrade requirements

- v18.14 or higher installed
- CentOS 7 (OS)
- An active Internet connection

Upgrade instructions

Before performing an upgrade (or any other system change), it is highly recommended to use the `backup` *interactive mode command* to back up the Plixer Replicator database.

Hint: Backups are stored in `/home/replicator/backups`. To restore from a backup file, use the restore command.

Important: When upgrading Plixer Replicator appliances in *HA configurations*, the fail-over appliance should be upgraded before the primary to minimize downtime.

The following instructions cover the upgrade process for both primary and fail-over appliances in HA configurations:

1. SSH to the appliance as the `replicator` user and start a new tmux session:

```
tmux new -s upgrade
```

2. Download the installer/upgrade script:

```
cd /tmp
curl -o replicator-install.run https://files.plixer.com/plixer-repo/replicator/19.0.
↪1/replicator-install.run
```

3. Download the checksum file and validate the integrity of the `replicator_install.run` file:

```
curl -o replicator-checksums.txt https://files.plixer.com/plixer-repo/replicator/19.
↪0.1/replicator-checksums.txt
cat replicator-checksums.txt
sha256sum replicator-install.run
```

4. Set the correct permissions for the installer:

```
chmod 755 replicator-install.run
```

5. Run `replicator-install.run`:

```
./replicator-install.run
```

After the upgrade is complete, the appliance will automatically reboot. To verify that the upgrade was successful, launch interactive mode and check the version number when the tool loads.

Hint: After upgrading a fail-over appliance in an HA deployment, use the `role test secondary` interactive mode command to verify the current HA configuration before proceeding to upgrade the primary appliance.

4.4.3 Upgrading to v18.14

To upgrade to Plixer Replicator v18.14 from v18.5 or higher, follow the steps described below.

Hint: For clarifications or assistance with upgrading, contact *Plixer Technical Support*.

Upgrade requirements

- v18.5 or higher installed
- An active Internet connection

Upgrade instructions

Before performing an upgrade (or any other system change), it is highly recommended to use the `backup` *interactive mode command* to back up the Plixer Replicator database.

1. SSH to the appliance as the `replicator` user and start a new tmux session:

```
tmux new -s upgrade
```

2. Download the upgrade script:

```
cd /home/replicator/files
curl -k -o upgrade_18.14.sh https://files.plixer.com/downloads/replicator/18/
↪upgrade_18.14.sh
```

3. Set the correct permissions for the upgrade script:

```
chmod 755 upgrade_18.14.sh
```

4. Run `upgrade_18.14.sh`:

```
./upgrade_18.14.sh
```

After the upgrade is complete, the appliance will automatically reboot. To verify that the upgrade was successful, launch interactive mode and check the version number when the tool loads.

CHAPTER

FIVE

ADDITIONAL RESOURCES

This section contains additional resources and materials related to Plixer Replicator and this user manual.

5.1 Changelog

For additional details on any of the new features below, refer to the Plixer Replicator documentation on the Plixer website.

KEY: Description (Ticket Number)

Ex. Added thresholds based on outbound traffic (1640)

5.1.1 Version 19.1.1 - October 2024

Note: This release addresses CentOS going EOL. To migrate the OS to Oracle Linux 9, Plixer Replicator must be on version 19.0.1. Please contact *Plixer Technical Support* with any questions.

New Features

- KVM virtual appliance image

Fixes

- Addressed various security issues
- System metrics errors (167)
- HA configuration errors (170)
- Set license command error (174)
- net-snmp package not in repo (178)
- sethostname.sh script missing (187)
- Set password from CLI (189)
- Web certificate file name (193)

5.1.2 Version 19.1.0 - June 2024

Note: This release addresses CentOS going EOL. To migrate the OS to Oracle Linux 9, Plixer Replicator must be on version 19.0.1. Please contact *Plixer Technical Support* with any questions.

New Features

- Oracle Linux v9.4

Fixes

- Addressed various security issues
- Added back missing enable_ssl.sh script (161)

5.1.3 Version 19.0.1 - January 2024

Fixes

Addressed various security issues
Fixed authentication issue (150)

5.1.4 Version 19.0.0 - November 2023

Updates

Improved UI responsiveness
Updated EULA
Updated branding

Fixes

Addressed various security issues
API may hang on invalid input (23)
Exporter id out of range (25)
Remote root access disabled by default (34)
Improved process management (60)

5.1.5 Version 18.14.1 - 1/28/2020

New Features

Updated the EULA
New Plixer Replicator UI skin

Fixes

Fixed a potential issue when setting up High Availability pairs (931)
Plixer Replicator's vitals processes can no longer enter a bad state, which may cause it to lock up indefinitely (1739)
Plixer Replicator excludes Collectors from being Exporters in Profiles with the same destination port the Collector is already receiving on (1771)
Exporters will now be added to Profiles correctly regardless of the time of the matching Policy's creation (1891)
Very high volume Plixer Replicators will no longer crash due to a database integer overflow (2007)

5.1.6 Version 18.12.14 - 1/25/2019

Updates

Future Plixer Replicator releases will no longer support CentOS 6

Fixes

Replication no longer starts and restarts spontaneously (410)
Plixer Replicator will no longer attempt to sync with its own database (428)
`system change` now works on all configurations (436)
Plixer Replicator stats are now more reliable (611)

5.1.7 Version 18.5 - 5/31/2018

Updates

Updated the EULA (5633)

Fixes

`show config` output now has Profile names enclosed in quotation marks ("") (25257)
Fixed an issue where Apache fails to start if SSL is enabled/setup via install script or enable_SSL.sh (25292)
Updated licensing checks (25653)
Fixed an issue where an install script was pointing to a previous version (25770)
Added the new online manual from docs.plixer.com (25828)
Fixed an issue where `policy remove profile include/exclude` results in an internal error (500) but still removes profile (25832)
Fixed an issue where the refresh countdown timer would default to one (1) day (26000)

5.1.8 Version 18.1 - 1/30/2018

New Features

LDAP authentication support
Profiles displayed in alphabetical order
Replicator install and upgrade logs
Backup process from the CLI
Ability to make API calls via HTTPS
Support for upper case letters and spaces in profile names
Ability to restrict snoop command by port
Current Plixer Replicator version displayed under the Status LED
Postgres replicator database support

Fixes

Improved performance and responsiveness of the web interface (22918)
Replicator now replicates SNMP traps on low port numbers (23820)
Exporters no longer enter a false Alarm state at start up (23824)
Exporters not in Profiles and not sending packets are no longer displayed under 'Exporters Not in Profiles' indefinitely (23828)
Search filters are no longer lost on page refresh (23904)
Fixed an issue that could result in phantom Collector alarms (23977)
Upgrades no longer reset the web interface password (24299)

5.1.9 Version 17.6 - 7/14/2017

New Features

Web interface updates
Fully supported and documented API
Ability to receive packets from multiple interfaces
Profile singularity

Fixes

Licensing says expired one day before expiration date (19835)
ICMP drops have been added to iptables (19396)
Semicolon at end of command yields unexpected results (19285)
Removing a Policy doesn't remove the associated Exporters (20848)
Plixer Replicator falsely reporting more packets inbound than out (21086)

5.1.10 Version 16.9 - 10/3/2016

New Features

New web interface
Fully supported and documented API
Ability to receive packets from multiple interfaces
Profile singularity

Fixes

Licensing says expired one day before expiration date (19835)
ICMP drops have been added to iptables (19396)
Semicolon at end of command yields unexpected results (19285)
Removing a policy doesn't remove the associated Exporters (20848)
Plixer Replicator falsely reporting more packets inbound than out (21086)

5.2 FAQ

Important: For additional questions or concerns, contact *Plixer Technical Support*.

Q) Can we use additional Plixer Replicators as failsafes against downtime and other issues?

A) Yes. For instructions on how to configure a secondary or backup Plixer Replicator appliance see the section on *high availability configurations*.

Q) Why is our Plixer Replicator still not receiving packets from our router even though I've configured it to send data to the correct IP address?

A) A firewall or access control list may be blocking traffic to the Plixer Replicator appliance. To verify that it can see traffic from a device, run `snoop [NETWORK_DEVICE_IP]` from the *REPLICATOR> prompt*.

Q) Can I create additional admin and/or user accounts for other users in our organization?

A) Each Plixer Replicator appliance currently only supports a single adminstrator account for the web interface. However, future updates to the product may add support for multiple local user accounts and roles.

Q) How long should it take for collectors to start receiving packets after I've configured an exporter to send flows to the Plixer Replicator appliance?

A) When a new exporter starts sending UDP packets to the Plixer Replicator appliance, it may take up to two minutes for the packets to be received by collectors.

Q) How do I find out if there are exporters not assigned to any profiles sending packets to the Plixer Replicator?

A) To view all currently unassigned exporters, select *Exporters Not in a Profile* in the **View** dropdown menu in the **Exporters** tab of the web interface or run `exporters noprofile` from the *REPLICATOR> prompt*.

Q) We have a closed network with no gateway. Why is our Plixer Replicator appliance dropping packets instead of replicating them?

A) The default behavior for the Plixer Replicator appliance is to drop all packets that come into an interface that the host has no route to. To change this, find the `net.ipv4.all.rp_filter` setting in the `/etc/sysctl.conf` file and change its value to `0`.

Q) How do I configure a profile to allocate exporter flows across a distributed Plixer Scrutinizer cluster?

A) If you are using Plixer Scrutinizer's distributed architecture to handle an extremely large number of flows and/or exporters, you can enable the *Auto Replicate* feature to have it manage Plixer Replicator profiles for its collectors and automatically assign exporter streams to them as they're added. Additional information and instructions on how to set up Plixer Replicator integration can be found in the Plixer Scrutinizer documentation here.

Q) Do Plixer Replicator appliances support IPFIX?

A) Yes, IPFIX is supported.

Q) Can I convert syslog messages to IPFIX?

A) By default, the Plixer Replicator appliance replicates syslog messsages received from exporters and forwards them to their assigned collectors in the same format. To have syslogs automatically converted to IPFIX before being forwarded, run `setting enable convertSyslog` from the *REPLICATOR> prompt*.

Q) How do I send the syslog notifications and/or IPFIX metrics generated by the Plixer Replicator appliance to more than one collector?

A) To send the appliance's syslog notifications and/or IPFIX metrics to multiple collectors, first configure the Plixer Replicator appliance to send the packets back to itself. After that, create a profile with the same appliance as an exporter and assign collectors as needed.

Note: Since there are separate settings for syslog notifications and IPFIX metrics, they will require separate profiles.

Q) Why am I receiving an error about a loop being created when I try to add a new exporter or collector?

A) A loop is created when a profile is configured in a way that incoming packets will be sent back to the source. This can happen when a collector is added to a profile with an inclusion policy that defines the same IP address as an exporter.

Q) Can a Profile have the same *in*/listening and *out*/sending port?

A) Yes. The Plixer Replicator will automatically verify updates to a profile's settings to ensure that no loops are created when new exporters and/or collectors are added.

Q) How do I change the ``root`` user password on the Plixer Replicator appliance?

A) To change the root password, SSH to the appliance as the `root` user and issue the `passwd` command.

Q) How do I change the web interface ``admin`` user password on the Plixer Replicator appliance?

A) To change the password for the web interface `admin` user, SSH to the appliance as the `replicator` user and run `password webui` from the *REPLICATOR> prompt*.

Q) How do I change the hostname and IP address of the Plixer Replicator appliance?

A) To change the hostname and IP address of the appliance, log in as the root user, and then run `/home/replicator/conf/sethostname.sh`. Alternatively, `system change` can be run from the *REPLICATOR> prompt*.

Q) In a multi-network/traditional high availability configuration, how often does the secondary appliance poll the primary to check if it's available?

A) The polling interval is controlled by the *Update Interval* setting on the **Settings** tab/page of the web interface and can be set anywhere between 30 to 60 seconds.

Q) How often is the database of the primary appliance synced to the secondary, in a multi-network/traditional high availability configuration?

A) The secondary appliance checks the primary for changes every 5 minutes. If changes are detected, the secondary appliance's configuration is updated.

Q) Does the Plixer Replicator appliance support giant packets?

A) Jumbo frame sizes up to 65534 bytes are supported by the Plixer Replicator appliance. To take advantage of this, interfaces must be configured to support the maximum packet size expected for replication. Fragmented packets are **not** supported, and the appliance will not attempt to fragment packets, even if the *do not fragment* bit (`DF`) bit is not set.

5.3 Glossary

This glossary is a reference for terms and concepts used in the Plixer Replicator software environment or this product manual.

5.3.1 Plixer Replicator terms

Alarm Policy
Rule sets that define what types of network behavior or activity should be monitored as events and trigger alarms

Collectors
SIEMs, flow collectors, SNMP trap receivers, and other network management systems that capture, analyze, and report on flow data sent by exporters

EULA (End-User License Agreement)
A legal agreement between Plixer Replicator and the user, outlining the terms and conditions, including usage rights, restrictions, and liability limitations

Events
Changes in an endpoint's state or behavior that may result in profile reassignment and can be used to draw attention to endpoints of interest

Exporters
Network devices, such as routers, switches, or servers that can send traffic/activity logs as flows to external systems, such as Plixer Replicator and Plixer Scrutinizer

Policy
A subnet/CIDR-based rule that automatically includes or excludes matching exporters in a profile

Profile
A user-defined replication configuration that defines the packet streams (based on exporters and in/listening ports) that should be routed to one or more collectors

5.3.2 General networking terms

2LD (Second-level Domain)
Part of the naming convention for domain names. For example, in example.com, *example* is the second-level domain of the .com TLD (Top level domain)

3LD (Third-level Domain)
For example, in www.mydomain.com, *www* is the third-level domain

ACK (Acknowledgment Code)
A unique signal sent by a computer to show that it has successfully transmitted data

ACL (Access Control List)
A set of rules governing access to a particular object or system resource

Active Directory / AD
Proprietary directory service offered by Microsoft, which allows for centralized management of users, devices, and other IT assets

API (Application Programming Interface)
A software component that allows applications to share data and functionality

ARP (Address Resolution Protocol)
Protocol that maps a dynamic IP address to a physical machine's permanent MAC address in a local area network (LAN)

CA (Certification Authority)
A trusted entity that issues, signs, and stores digital certificates

CDP (Cisco Discovery Protocol)
Protocol used by Cisco devices to allow neighboring networking devices to learn about each other

CIDR (Classless Inter-Domain Routing)
An IP addressing method that improves the efficiency of allocating IP addresses

CLI (Command-line Interface)
A text-based interface for applications and operating systems that allows a user to enter commands

Collector
SIEMs, Flow Collectors, SNMPTrap Receivers, or other network management systems that analyze data forwarded from networked devices

DHCP (Dynamic Host Configuration Protocol)
Network management protocol used to automatically assign IP addresses and other communication parameters to devices on an Internet protocol network

DNS (Domain Name System)
A system by which computers and other devices on the Internet or Internet protocol networks are uniquely identified using names matched to their IP addresses

Egress
Traffic that exits a device or network

Endpoint
An entity (device, service, node, etc.) at the end of a network communication channel

Encapsulated Remote SPAN (ERSPAN)
Encapsulates mirrored traffic in GRE (Generic Routing Encapsulation) and sends it over Layer 3 networks

ESX (Elastic Sky X)
A pre-configured, ready-to-deploy virtual machine (VM) designed to run on VMware ESX or ESXi

Exporter
A networked device such as a router, switch, or server that generates data and sends it to the flow collector device

Fault tolerance
A system's ability to continue operating without interruptions in the event of hardware or software failure

FQDN (Fully Qualified Domain Name)
The complete address of a computer, host, or any other entity on the Internet

GRE (Generic Routing Encapsulation)
A tunneling protocol developed by Cisco Systems

Hyper-V
A pre-configured, ready-to-deploy virtual machine designed to run on Microsoft Hyper-V, typically packaged in VHD/VHDX format

ICMP (Internet Control Message Protocol)
A protocol used for devices within the network to determine possible network issues

Identity Provider (IdP)
A third-party entity and/or service that stores and manages identities and credentials for use by other websites, applications, or other digital resources

IP address
A unique numerical label assigned to a networked device

IPFIX (Internet Protocol Flow Information Export)
A protocol intended to collect and analyze the flow data from supported network devices

KVM (Kernel-based Virtual Machine)
A pre-configured virtual machine designed to run on KVM hypervisors, packaged in formats like QCOW2 or OVA for easy deployment in Linux-based virtualization environments

Latency
The latency of a network is the time it takes for a data packet to be transferred from its source to the destination

LDAP (Lightweight Directory Access Protocol)
An open, cross-platform protocol used to access and maintain directory services for assets in an Internet protocol network

LLDP (Link Layer Discovery Protocol)
A vendor-neutral protocol used by devices on IEEE 802 networks to advertise their identity, capabilities, and other information

MAC (Media Access Control) address
A unique hardware identifier typically assigned by manufacturers to network adapters and devices

MIB (Management Information Base)
A database that stores information used for managing a network

MTTR (Mean Time to Resolution)
The the average amount of time between the detection and remediation of a security threat or incident

NDR (Network Detection and Response)
A cybersecurity solution that use machine learning to detect cyber threats and aid remediation

Network interface
A (physical or software-based) point of connection between a network entity and the rest of the network

NIC (Network Interface Card)
Adapter that provides devices network connections, either wired or wireless

NID (Network Infrastructure Device)
Any device, such as an access point, router, or switch, that provide the means for entities to communicate with each other over a network

NTP (Network Time Protocol)
A networking protocol used to synchronize device clocks over the Internet

NXDOMAIN (No Existing Domain)
An error message that means that a domain mentioned in the Domain Name System (DNS) query does not exist

Open port
A TCP or UDP port that has been configured to accept packets

OUI (Organizationally Unique Identifier)
A unique 24-bit number in a MAC address that identifies the vendor or the manufacturer of the device

OVF (Open Virtualization Format)
An open source standard for packaging and distributing virtual machines and software applications

Packet
A block of data transmitted across a network

PDU (Protocol Data Unit)
An individual unit of information exchanged by entities on a network using the same protocol

PostgreSQL
An open-source relational database management system (RDBMS) that supports both SQL and JSON querying

PXE (Preboot Execution Environment)
A network booting protocol that allows computers to boot from a network rather than a local storage device like a hard drive or USB

RADIUS (Remote Authentication Dial-In User Service)
A client-server AAA (authentication, authorization, accounting) protocol used to manage remote user access to a network

Redundancy
The state of having duplicate or alternative services as backups to allow for continuous availability

REST API (Representational State Transfer Application Programming Interface)
A set of rules that allows systems to communicate over the web using standard HTTP methods

Router
A device that forwards or routes data packets to devices on a network

Server
A system or device that provides resources, data, services, or applications to other devices over a network

Single Sign-On (SSO)
Allows the integration of third-party authentication services for user access to the Plixer Endpoint Analytics web interface

SIP/RTP (Session Initiation Protocol/Real Time Protocol)
SIP is the control protocol, and RTP is the payload protocol used to send and receive Voice over IP (VoIP)

SNMP (Simple Network Management Protocol)
An IP network protocol used to collect data related to state and/or behavior from devices on a network

SNMP trap
An alert message that is initiated by an SNMP-enabled device to notify the management system of significant events or changes in status

Software agent
A persistent piece of software that performs certain actions and/or interacts with its environment on behalf of a user or another program

SPAN (Switched Port Analyzer)
A dedicated port on a switch that takes a mirrored copy of network traffic from within the switch to be sent to a destination

SSDP (Simple Service Discovery Protocol)
A network protocol used for advertising and discovering network services

SSH (Secure Shell Protocol)
A network communication protocol that allows network services to be used securely over an unsecured network

SSL (Secure Sockets Layer)
A protocol for establishing secure connections between networked devices

STIX (Structured Threat Information eXchange)
An industry-standard file format for the exchange of threat information between organizations and platforms

Suricata
A network threat detection engine used to analyze network traffic and identify potential security threats

Switch
A device that connects devices in a network and allows them to communicate with each other

SYN scan
A port scanning technique that allows for the discovery of the status of a communications port without establishing a full connection

Syslog
A cross-platform network logging protocol used to send and/or receive alerts between different devices on a network

TACACS+ (Terminal Access Controller Access-Control System)
A protocol where the remote access server and the authentication server provide validation for users attempting to access the network

TAXII (Trusted Automated eXchange of Indicator Information)
A protocol that allows the transmission of threat information, primarily in STIX format, between systems and organizations

TCP (Transmission Control Protocol)
A connection-oriented protocol that enables the bidirectional exchange of messages between devices on the same network

TLS handshake
The process that starts secure communication between a client and a server

TSIG (Transaction Signature)
A protocol that secures DNS packets and allows a Domain Name System to authenticate updates to the DNS database

TTL (Time To Live)
A field in the IP packet header that specifies the maximum number of hops (or router passes) a packet can take before being discarded

UDP (User Datagram Protocol)
A communication protocol for transmitting messages between applications and programs in a network

Virtual appliance
A pre-configured virtual machine image with pre-installed software that is meant to serve a specific function

VoIP (Voice over Internet Protocol)
A technology that allows voice calls using an internet connection

VPC (Virtual Private Cloud)
A secure and private cloud hosted in a public cloud

VRF (Virtual Routing and Forwarding)
A technology that separates routing tables to isolate management traffic to the management interface

Web server banner
A text-based greeting message, which includes information like open ports, services, and version numbers, returned by a web host

5.4 Third-Party attributions

The open source or other third-party software components listed below are integrated and/or redistributed with the Plixer Replicator software. The licenses are reproduced here in accordance with their licensing terms. These terms only apply to the libraries themselves and not the Plixer Replicator software.

Additional required license documentation can be found under `/home/Replicator/files/licenses`.

Backbone.js
https://github.com/jashkenas/backbone/blob/master/LICENSE Copyright (c) 2010-2017 Jeremy Ashkenas, DocumentCloud Licensed under the MIT License – see Licenses Directory

C3.js
https://github.com/c3js/c3/blob/master/LICENSE Copyright (c) 2013 Masayuki Tanaka Licensed under the MIT License – see Licenses Directory

D3.js
https://github.com/d3/d3/blob/master/LICENSE Copyright (c) 2010-2014 2010-2017 Mike Bostoc Licensed under the BSD 3-clause License – see Licenses Directory

Hogan.js
https://github.com/twitter/hogan.js/blob/master/LICENSE Copyright (c) 2011 Twitter, Inc. Licensed under the Apache License 2.0 – see Licenses Directory

JQuery
https://jquery.org/license/ Copyright jQuery Foundation and other contributors, https://jquery.org This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at https://github.com/jquery/jquery Licensed under the MIT License – see Licenses Directory

JQuery.floatThread.js
https://github.com/mkoryak/floatThead/blob/master/LICENSE Copyright (c) 2012-2017 Misha Koryak Licensed under the MIT License – see Licenses Directory

jsSHA
https://github.com/Caligatio/jsSHA/blob/master/LICENSE Copyright (c) 2008-2017 Brian Turek Licensed under the BSD 3-clause License – see Licenses Directory

JustGage
https://github.com/toorshia/justgage/blob/master/LICENSE Copyright (c) 2012-2015 Bojan Djuricic Licensed under the MIT License – see Licenses Directory

Raphaël
https://github.com/DmitryBaranovskiy/raphael/blob/master/license.txt Copyright © 2008-2013 Dmitry Baranovskiy, Sencha Labs Licensed under the MIT License – see Licenses Directory

UDP Samplicator
https://github.com/sleinen/samplicator/blob/master/COPYING Copyright (c) 2000-2015 Simon Leinen Licensed under the GNU GPL 2.0 – see Licenses Directory

Underscore.js
https://github.com/jashkenas/underscore/blob/master/LICENSE Copyright (c) 2009-2017 Jeremy Ashkenas, DocumentCloud and Investigative Reporters & Editors Licensed under the MIT License – see Licenses Directory

5.5 Plixer Technical Support

Plixer Technical Support is available with an active maintenance contract. Contact our support team at:

- +1 (207) 324-8805 ext 4
- https://www.plixer.com/support/

For further questions, check out the *FAQ page* or contact *Plixer Technical Support*.