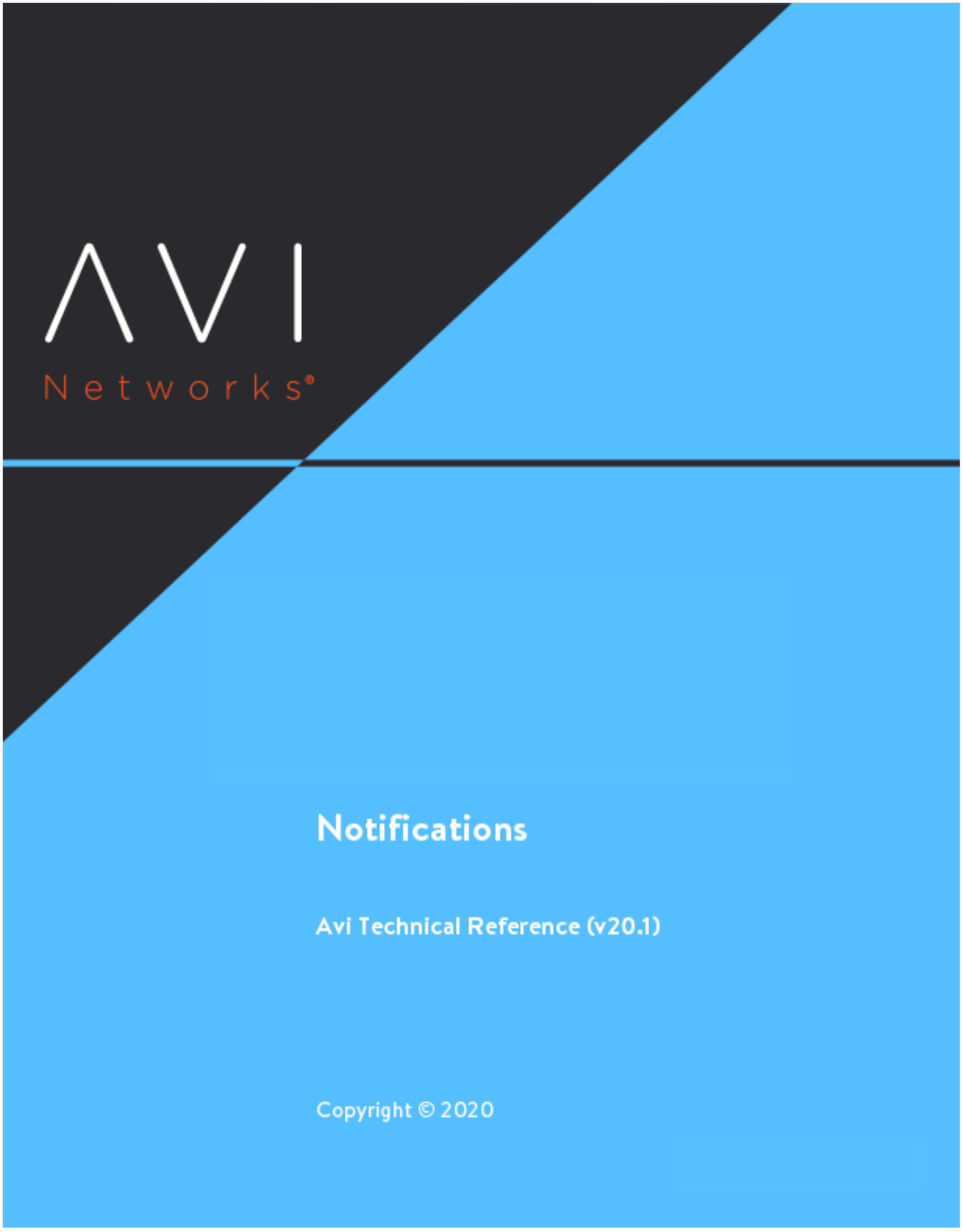


Notifications

Avi Technical Reference (v20.1)

Notifications

view online

Alert actions are configured to proactively send notifications to an administrator using the Notifications option available on the Avi user interface. The options to send notifications are available under Operations > Notifications and alerts are sent using email, syslog, and SNMP options.

Before creating an alert action, the notification destinations must be configured. These can be syslog servers, email servers and addresses, and SNMP trap servers.

To verify notification in advance, refer to verify notification settings in advance. In addition to notifications, an alert action also can include running a ControlScript. Notifications need to be configured only if they are going to be used for an alert action.

Syslog Notifications

Syslog messages may be sent to one or more syslog servers. Communication is non-encrypted via UDP, using a customizable port. According to RFC 5426, syslog receivers must support accepting syslog datagrams on the well-known port 514 (Avi Vantage?s default), but may be configurable to listen on a different port. The alert action determines which log levels (high, medium, low) should be sent. Avi Vantage uses this process internally for receiving logs. This appears on the Syslog tab as System-Syslog.

Configuring syslog notifications pushes alerts to syslog servers. It does not export Avi Vantage?s virtual service logs. These may be pulled from an external logging system via the API, or may be scripted to push from the Avi Controller to a remote log system.

Syslog over TLS

Note: Avi Vantage supports only TLS 1.2 for syslog over TLS.

Starting with Avi Vantage release 18.2.5, an encrypted channel has been introduced. The Controller acts as a syslog client and sends encrypted syslogs to a remote server. This ensures that the syslog events are secured as they traverse through the network.

To configure syslog over TLS, 1. Configure `alertsyslogconfig` and enter the `syslog_servers` submode. 2. Change the flags as follows: * udp ? False * enable_tls ? True 3. Use the `show alertsyslogconfig` command to confirm the settings.

```
[admin:10-10-24-65]: > show alertsyslogconfig Syslog-tls
    +--------------------------------------------------------------------------+
```

```
      | Field               | Value                                                 |
      +---------------------+-------------------------------------------------------ex+
      | uuid                | alertsyslogconfig-d4b2a910-7750-4d20-b5c7-0009816c7300 |
      | name                | Syslog-tls                                            |
      | syslog_servers[1]   |                                                       |
      |   syslog_server     | 10.1.1.1                                              |
      |   syslog_server_port| 516                                                   |
      |   udp               | False                                                 |
      |   format            | SYSLOG_LEGACY                                         |
      |   tls_enable        | True                                                  |
      | tenant_ref          | admin                                                 |
      +-------------------------------------------------------------------------+
```

Note: In case of multiple syslog servers, repeat this configuration for all TLS syslog servers.

A sample `AlertSyslogConfig` object appears as shown below:


```
"AlertSyslogConfig": [
        {
            "url": "/api/alertsyslogconfig/alertsyslogconfig-9147e015-5540-4580-8eb5-304cab8da9b1",
            "tenant_ref": "/api/tenant/?name=admin",
            "syslog_servers": [
                {
                    "tls_enable": true,
                    "udp": false,
                    "pkiprofile_ref": "/api/pkiprofile/?tenant=admin&name=syslog_ca",
                    "format": "SYSLOG_LEGACY",
                    "ssl_key_and_certificate_ref": "/api/sslkeyandcertificate/?tenant=admin&name=ctlr syslog client",
                    "anon_auth": false,
                    "syslog_server_port": 6514,
                    "syslog_server": "10.140.7.251"
                }
            ],
            "name": "rsyslog_tcp",
            "uuid": "alertsyslogconfig-9147e015-5540-4580-8eb5-304cab8da9b1"
        }
]
```


In the sample object, note the following: * `tls_enable` is set to *true*. * `udp` is set to *false*. * `anon_auth` is set to *false*. This flag is enabled only to get anonymous authorization. If `anon_auth` is set to *true*, then PKI profile and `SSLKeyAndCertificate` are not required. * Enter the CA certificate reference as the `pkiprofile_ref`. * Enter the certificate and key reference in the field `ssl_key_and_certificate_ref`.

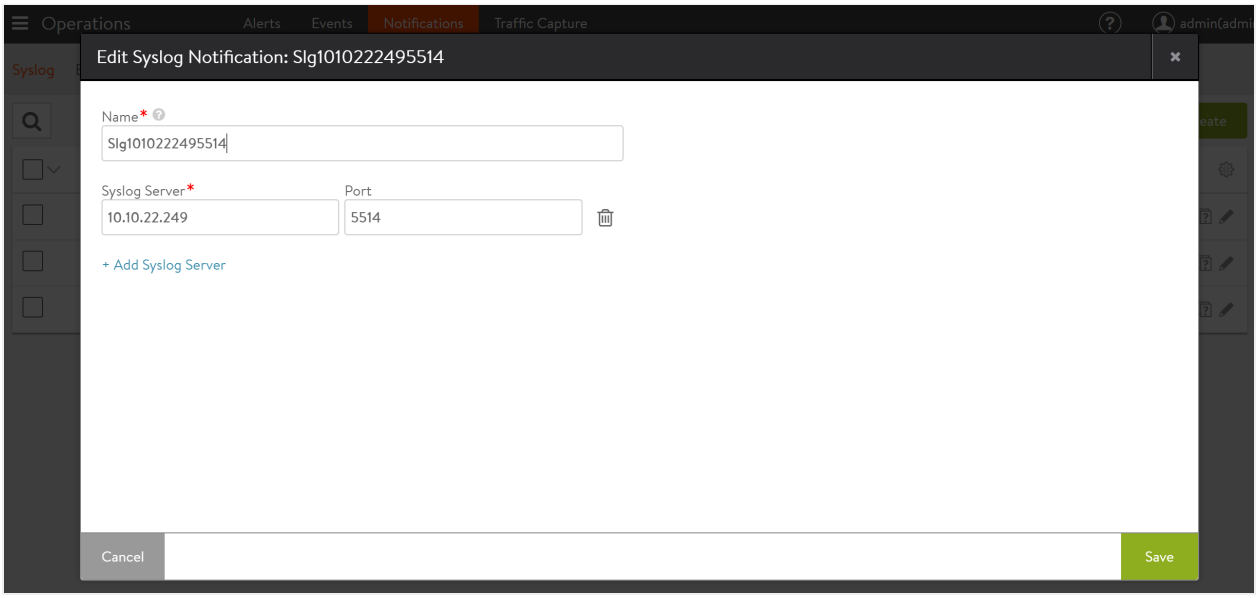
Syslog Notifications Settings

Select Operations > Notifications > Syslog to open the syslog notifications tab. This tab includes the following functions:

- Search: Search through the configure list of syslog entries.
- Create: Opens the Create syslog Notification popup.
- Edit: Opens the Edit syslog Notification popup.

- Delete: Remove the selected syslog notifications. The default System-Syslog notification may be modified, but not deleted.

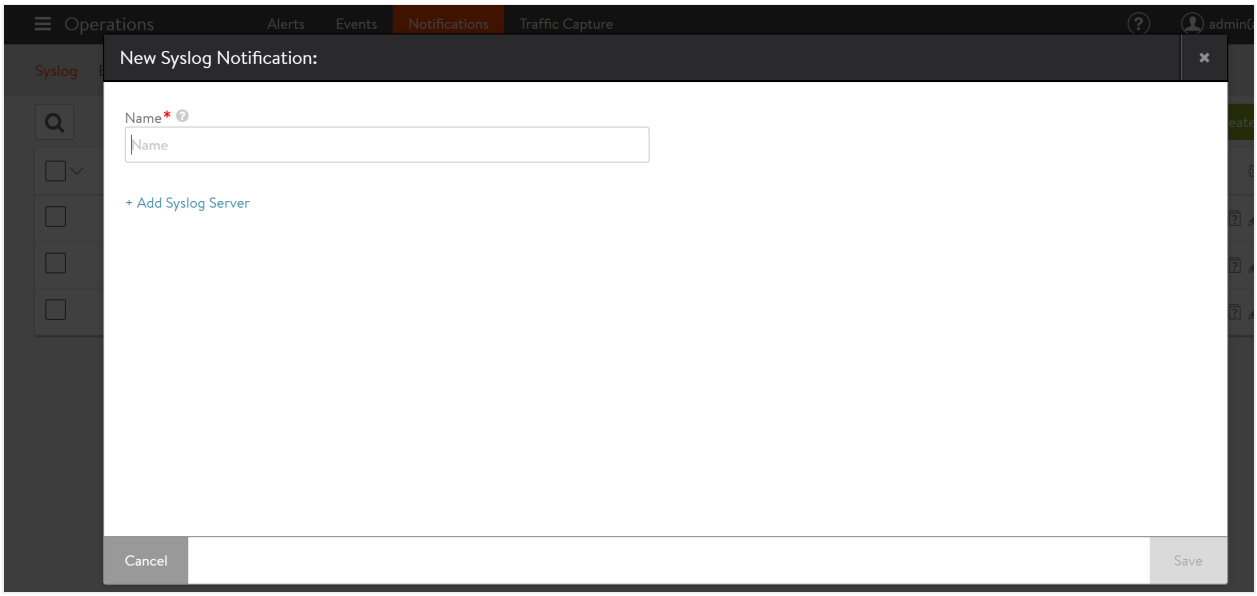
The table on this tab contains the following information for each syslog notification:



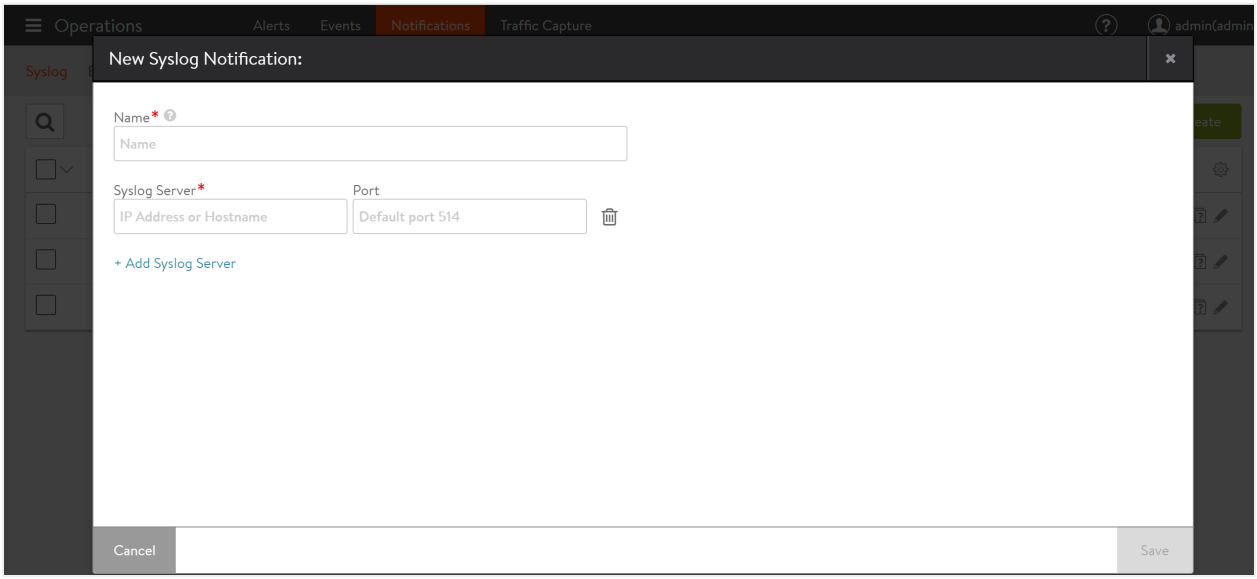
- Name: Name of the syslog notification.
- Syslog Server: IP address or hostname of the destination syslog server for the log entries. The server must be listening for UDP.
- Port: The service port number of the destination syslog server.

Create Syslog Notification

The New Syslog Notification and Edit Syslog Notification popups share the same interface. To create a new syslog server, navigate to Operations > Notifications > Syslog, click on the Create option and provide the desired name for the syslog server.



Click on Add Syslog Server, and provide the required details for Syslog Server and Port as shown below.



The following are the descriptions for each attributes:

- Name: Enter a unique name for the Syslog destination.
- Syslog Server: Enter either the IP address or hostname of the remote syslog server.
- Port: Enter the service port of the destination Syslog server. Avi Vantage uses UDP as the protocol for sending logs.

Email

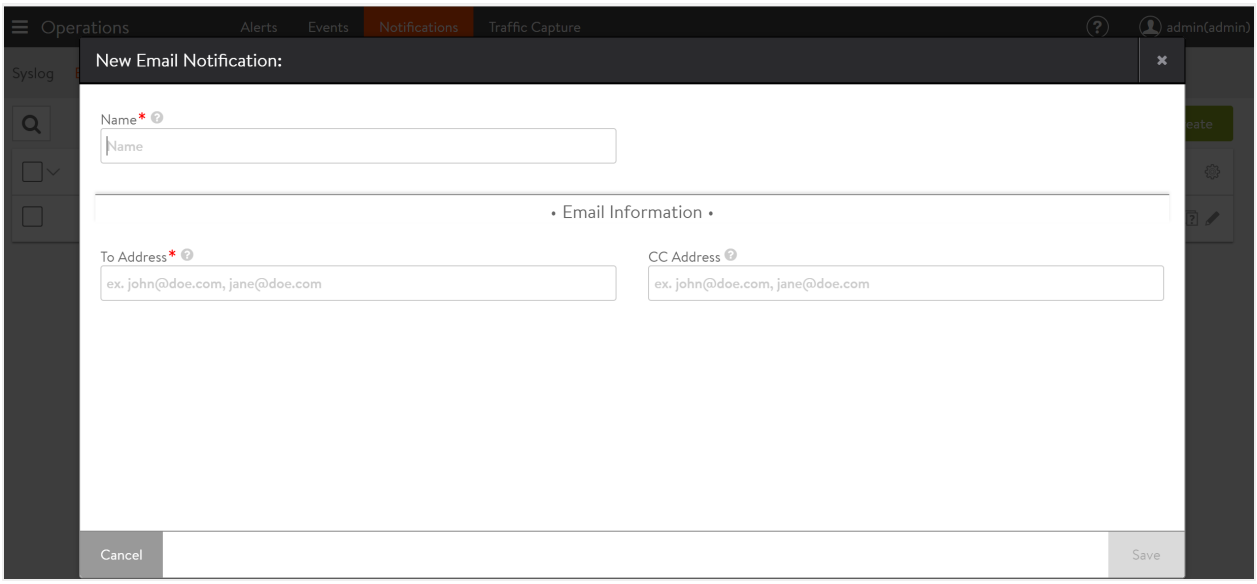
Alert Actions may be configured to send alerts to administrators via email. These emails could be sent directly to administrators or to reporting systems that accept email. Either option requires the Vantage Controller to have a valid DNS and default gateway configured so it can resolve the destination and properly forward the messages.

Information regarding the SMTP server and the sender must be configured in the Administration > Settings > Email/SMTP page.

Select Operations > Notifications > Email to open the email tab. This tab includes the following functions:

- Search: Search through this list of email notification names.
- Create: Opens the Create/Edit Email Notification popup.
- Edit: Opens the Create/Edit Email Notification popup.
- Delete: Remove the selected email notifications.

The table on this tab contains the following information for each email notification:



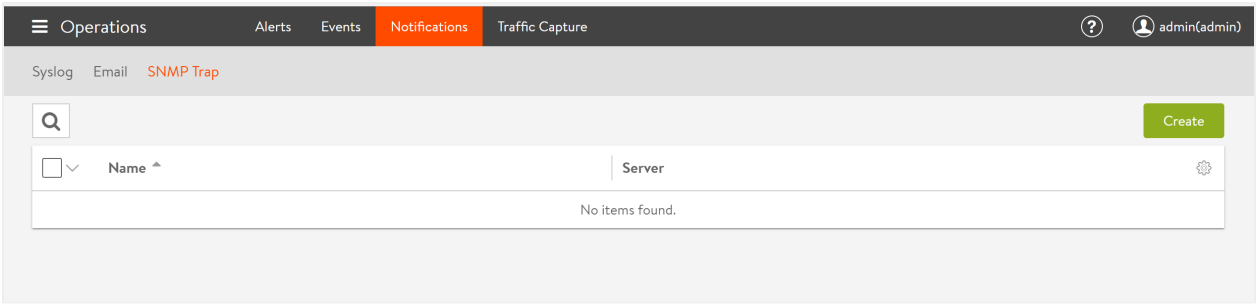
- Name: Name of the email notification.
- To Address: The email address used as the primary destination for the Alert Action. Use comma separation for multiple email addresses.
- CC Address: The email address used as the secondary, or CC'd email destination for the Alert Action. Use comma separation for multiple email addresses.

SNMP Trap

Alerts may be sent via SNMP Traps using SNMP v2c.

SNMP Trap Settings

Select Operations > Notifications > SNMP Trap to open the SNMP tab as shown in the below screenshot.



This tab includes the following functions:

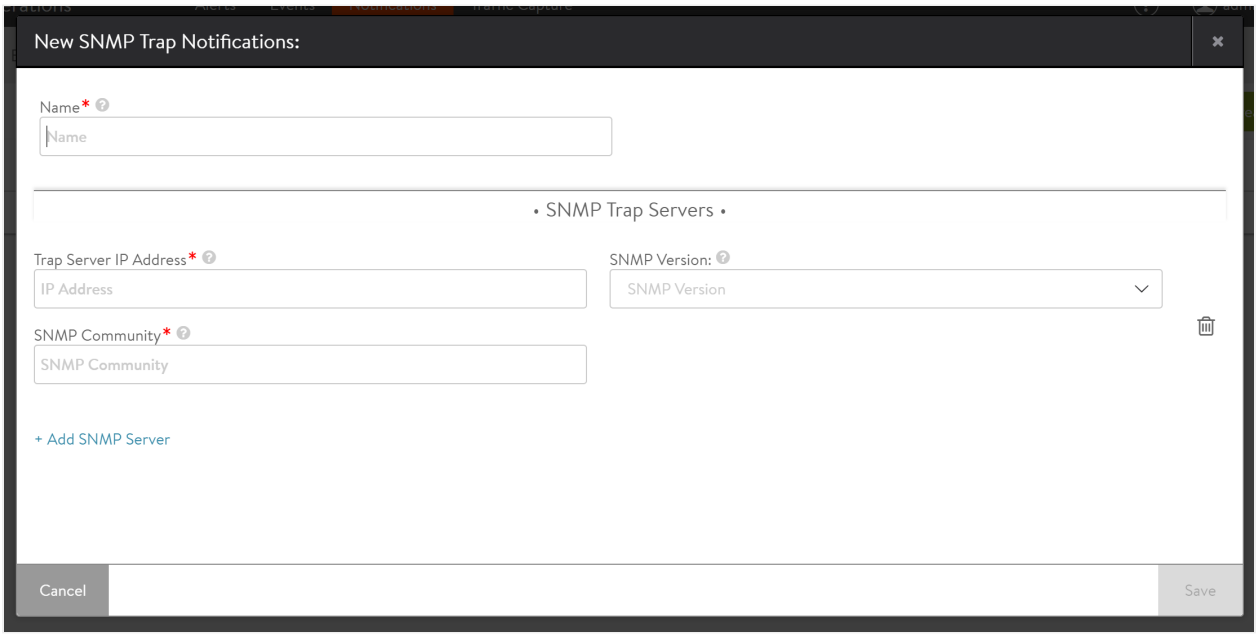
- Search: Search through this list of SNMP Trap server names.
- Create: Opens the Create/Edit SNMP Trap popup.
- Edit: Opens the Create/Edit SNMP Trap popup.
- Delete: Remove the selected SNMP Trap server.

Creating an SNMP trap server presents the following options:

- Name: Name of the SNMP server.
- Trap Server IP Address: The IP address or hostname of the server.
- SNMP Community: Trap servers may require a community string, which provides a basic form of security for access to the server.
- SNMP Version: SNMP version to be used. Avi Vantage supports SNMP v2c, and as of 17.2.3, the administrator can choose to use SNMP v3 instead.

For more information on SNMP support in Avi Vantage, refer to SNMP Support in Avi Vantage.

To add a new SNMP trap server, navigate to Operations > Notifications > SNMP Trap and click on Create.



Notes:

1. In a cluster, only the leader node sends the syslog notifications.
2. The IP address of the syslog traffic would be the interface IP of the leader node.
3. The notifications are sent in clear text format.