Syslog Support APIs

Table 1: Syslog Support APIs

Action	Method	Payload Required	API
To configure syslog server	POST	Yes	/api/config/system/settings/logging
To update the syslog server information	PUT	Yes	/api/config/system/settings/logging/host/<host-address>
To remove the syslog server information	DELETE	No	/api/config/system/settings/logging/host/<host-address>
To configure syslog severity	PUT	Yes	/api/config/system/settings/logging/severity
To configure syslog facility	PUT	Yes	/api/config/system/settings/logging/facility
To view syslog configuration	GET	No	/api/operational/system/settings/logging

- Example: POST Syslog Server, on page 1
- Example: PUT Remote Logging Host Configuration, on page 2
- Example: DELETE Remote Logging Host Configuration, on page 3
- Example: PUT Syslog Severity, on page 4
- Example: PUT Syslog Facility, on page 5
- Example: GET Remote Logging Host, on page 6

Example: POST Syslog Server

```
curl -k -v -u admin:Cisco123# -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml-X POST
https://172.19.162.209/api/config/system/settings/logging -d
'<host><host>172.19.162.143</host><transport><udp/></transport><port>525</port></host>'

Note: Unnecessary use of -X or --request, POST is already inferred.
* Trying 172.19.162.209...
* Connected to 172.19.162.209 (172.19.162.209) port 443 (#0)
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
```

```
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
 CApath: none
* TLSv1.0 (OUT), TLS handshake, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Client hello (1):
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS change cipher, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.0 / DHE-RSA-AES256-SHA
* Server certificate:
* subject: CN=nfvis
* start date: Jun 2 18:39:33 2017 GMT
* expire date: May 31 18:39:33 2027 GMT
* issuer: CN=nfvis
* SSL certificate verify result: self signed certificate (18), continuing anyway.
* Server auth using Basic with user 'admin'
> POST /api/config/system/settings/logging HTTP/1.1
> Host: 172.19.162.209
> Authorization: Basic YWRtaW46Q2lzY28xMjMj
> User-Agent: curl/7.49.1
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 85
>
* upload completely sent off: 85 out of 85 bytes
< HTTP/1.1 201 Created
< Server: nginx/1.10.1
< Date: Thu, 08 Jun 2017 09:01:40 GMT
< Content-Type: text/html
< Content-Length: 0
< Location: https://172.19.162.209/api/config/system/settings/logging/host/172.19.162.143
< Connection: keep-alive
< Last-Modified: Thu, 08 Jun 2017 09:01:40 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1496-912500-289655
< Pragma: no-cache
<
```

Example: PUT Remote Logging Host Configuration

```
curl -k -v -u admin:Cisco123# -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml-X PUT
https://172.19.162.209/api/config/system/settings/logging/host/172.19.162.143 -d
'<host><host>172.19.162.143</host><transport><tcp/></transport><port>1525</port></host>'

* Trying 172.19.162.209...
* Connected to 172.19.162.209 (172.19.162.209) port 443 (#0)
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
 CApath: none
* TLSv1.0 (OUT), TLS handshake, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Client hello (1):
```

```
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS change cipher, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.0 / DHE-RSA-AES256-SHA
* Server certificate:
* subject: CN=nfvis
* start date: Jun 2 18:39:33 2017 GMT
* expire date: May 31 18:39:33 2027 GMT
* issuer: CN=nfvis
* SSL certificate verify result: self signed certificate (18), continuing anyway.
* Server auth using Basic with user 'admin'
> PUT /api/config/system/settings/logging/host/172.19.162.143 HTTP/1.1
> Host: 172.19.162.209
> Authorization: Basic YWRtaW46Q2lzY28xMjMj
> User-Agent: curl/7.49.1
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 86
>
* upload completely sent off: 86 out of 86 bytes
< HTTP/1.1 204 No Content
< Server: nginx/1.10.1
< Date: Thu, 08 Jun 2017 09:11:58 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Last-Modified: Thu, 08 Jun 2017 09:11:58 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1496-913118-15836
< Pragma: no-cache
<
```

Example: DELETE Remote Logging Host Configuration

```
curl -k -v -u admin:Cisco123# -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml-X DELETE
https://172.19.162.209/api/config/system/settings/logging/host/172.19.162.143

* Trying 172.19.162.209...
* Connected to 172.19.162.209 (172.19.162.209) port 443 (#0)
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
 CApath: none
* TLSv1.0 (OUT), TLS handshake, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Client hello (1):
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS change cipher, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.0 / DHE-RSA-AES256-SHA
* Server certificate:
* subject: CN=nfvis
* start date: Jun 2 18:39:33 2017 GMT
* expire date: May 31 18:39:33 2027 GMT
* issuer: CN=nfvis
* SSL certificate verify result: self signed certificate (18), continuing anyway.
```

```
* Server auth using Basic with user 'admin'
> DELETE /api/config/system/settings/logging/host/172.19.162.143 HTTP/1.1
> Host: 172.19.162.209
> Authorization: Basic YWRtaW46Q2lzY28xMjMj
> User-Agent: curl/7.49.1
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
>
< HTTP/1.1 204 No Content
< Server: nginx/1.10.1
< Date: Thu, 08 Jun 2017 09:18:10 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Last-Modified: Thu, 08 Jun 2017 09:18:10 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1496-913490-383818
< Pragma: no-cache
<
```

Example: PUT Syslog Severity

```
curl -k -v -u admin:Cisco123# -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml-X PUT
https://172.19.162.209/api/config/system/settings/logging/severity -d
'<severity>error</severity>'

* Trying 172.19.162.209...
* Connected to 172.19.162.209 (172.19.162.209) port 443 (#0)
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
 CApath: none
* TLSv1.0 (OUT), TLS handshake, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Client hello (1):
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS change cipher, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.0 / DHE-RSA-AES256-SHA
* Server certificate:
* subject: CN=nfvis
* start date: Jun 2 18:39:33 2017 GMT
* expire date: May 31 18:39:33 2027 GMT
* issuer: CN=nfvis
* SSL certificate verify result: self signed certificate (18), continuing anyway.
* Server auth using Basic with user 'admin'
> PUT /api/config/system/settings/logging/severity HTTP/1.1
> Host: 172.19.162.209
> Authorization: Basic YWRtaW46Q2lzY28xMjMj
> User-Agent: curl/7.49.1
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 26
>
* upload completely sent off: 26 out of 26 bytes
< HTTP/1.1 204 No Content
```

```
< Server: nginx/1.10.1
< Date: Thu, 08 Jun 2017 09:33:01 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Last-Modified: Thu, 08 Jun 2017 09:33:01 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1496-914381-204591
< Pragma: no-cache
<
```

Example: PUT Syslog Facility

```
curl -k -v -u admin:Cisco123# -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml-X PUT
https://172.19.162.209/api/config/system/settings/logging/facility -d
'<facility>local5</facility>'
* Trying 172.19.162.209...
* Connected to 172.19.162.209 (172.19.162.209) port 443 (#0)
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
 CApath: none
* TLSv1.0 (OUT), TLS handshake, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Client hello (1):
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS change cipher, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.0 / DHE-RSA-AES256-SHA
* Server certificate:
* subject: CN=nfvis
* start date: Jun 2 18:39:33 2017 GMT
* expire date: May 31 18:39:33 2027 GMT
* issuer: CN=nfvis
* SSL certificate verify result: self signed certificate (18), continuing anyway.
* Server auth using Basic with user 'admin'
> PUT /api/config/system/settings/logging/facility HTTP/1.1
> Host: 172.19.162.209
> Authorization: Basic YWRtaW46Q2lzY28xMjMj
> User-Agent: curl/7.49.1
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
> Content-Length: 27
>
* upload completely sent off: 27 out of 27 bytes
< HTTP/1.1 204 No Content
< Server: nginx/1.10.1
< Date: Thu, 08 Jun 2017 09:20:21 GMT
< Content-Type: text/html
< Content-Length: 0
< Connection: keep-alive
< Last-Modified: Thu, 08 Jun 2017 09:20:21 GMT
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Etag: 1496-913621-135440
< Pragma: no-cache
<
```

Example: GET Remote Logging Host

```
curl -k -v -u admin:Cisco123# -H Accept:application/vnd.yang.data+xml -H
Content-Type:application/vnd.yang.data+xml-X GET
'https://172.19.162.209/api/operational/system/settings/logging?deep'

Note: Unnecessary use of -X or --request, GET is already inferred.
* Trying 172.19.162.209...
* Connected to 172.19.162.209 (172.19.162.209) port 443 (#0)
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: /etc/pki/tls/certs/ca-bundle.crt
 CApath: none
* TLSv1.0 (OUT), TLS handshake, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Server hello (2):
* TLSv1.0 (IN), TLS handshake, Certificate (11):
* TLSv1.0 (IN), TLS handshake, Server key exchange (12):
* TLSv1.0 (IN), TLS handshake, Server finished (14):
* TLSv1.0 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.0 (OUT), TLS change cipher, Client hello (1):
* TLSv1.0 (OUT), TLS handshake, Finished (20):
* TLSv1.0 (IN), TLS change cipher, Client hello (1):
* TLSv1.0 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.0 / DHE-RSA-AES256-SHA
* Server certificate:
* subject: CN=nfvis
* start date: Jun 2 18:39:33 2017 GMT
* expire date: May 31 18:39:33 2027 GMT
* issuer: CN=nfvis
* SSL certificate verify result: self signed certificate (18), continuing anyway.
* Server auth using Basic with user 'admin'
> GET /api/operational/system/settings/logging?deep HTTP/1.1
> Host: 172.19.162.209
> Authorization: Basic YWRtaW46Q2lzY28xMjMj
> User-Agent: curl/7.49.1
> Accept:application/vnd.yang.data+xml
> Content-Type:application/vnd.yang.data+xml
>
< HTTP/1.1 200 OK
< Server: nginx/1.10.1
< Date: Thu, 08 Jun 2017 09:03:37 GMT
< Content-Type: application/vnd.yang.data+xml
< Transfer-Encoding: chunked
< Connection: keep-alive
< Cache-Control: private, no-cache, must-revalidate, proxy-revalidate
< Pragma: no-cache
<

<logging xmlns="http://www.cisco.com/nfv" xmlns:y="http://tail-f.com/ns/rest"
xmlns:system="http://www.cisco.com/nfv">
 <host>
   <host>172.19.162.117</host>
   <transport>
    <tcp/>
   </transport>
   <port>1635</port>
 </host>
 <host>
   <host>172.19.162.111</host>
   <transport>
     <udp/>
```

```
    </transport>
    <port>163</port>
  </host>
  <host>
    <host>172.19.162.112</host>
      <port>1523</port>
    </host>
  <host>
    <host>172.19.162.143</host>
    <transport>
      <udp/>
    </transport>
    <port>525</port>
  </host>
</logging>
```