Session Alarms

For supported software information, click here.

Versa Operating System™ (VOS™) devices send session utilization alarms to alert users about issues related to active sessions. These alarms report issues about connectivity issues and stopped applications.

org-session-utilization

VOS devices implement a multitenant design that allows configuration of several organizations (or tenants), and each organization has a maximum number of sessions for such things as stateful and next-generation firewall and CGNAT. This design enforces equal resource sharing among multiple organizations across the device. By default, a VOS device limits the number of sessions per organization to 1 million, and you can modify this number, up to a maximum of 5 million. An alarm is raised if this limit is exceeded, which generally occurs when a compromised host on that tenant's network is invalidly generating numerous sessions whose traffic that appears to be legitimate (that is, it is not DoS traffic).

Description	Consider a tenant entitled to 10,000 sessions, and with a session timing out after the default time of 300 seconds with no activity. If the session table reaches the capacity of 10,000 entries, no new sessions are created until older sessions age out or until the administrator increases the maximum session count. An alarm is generated to indicate that the tenant has exceeded the maximum configured session count and that additional traffic that requires a new session is attempting to traverse the VOS device. The device-session-threshold alarm is similar to the org-session-threshold alarm, at a device level. This is a critical alarm because it indicates a halt in new session creation for an organization and leads to connectivity issues and application stoppages. It also indicates that the VOS device is not running optimally.

Cause	• Many users are accessing the system simultaneously • DoS attack in which users are trying to scan IP address of different destinations.
Action	• Configure additional session capacity. • Allocate a higher-bandwidth connection. • Verify that the traffic flows generated at the time of the alarm are legitimate. To do this, verify the source and destination IP addresses in the IPFIX records in the Versa Analytics database. • If this traffic is legitimate, increase the organization limits for total amount of sessions.

Related Commands

- Run the **show orgs org** *customer-name* **sessions brief** CLI command to view the system resource alarm related details.

```
admin@v(PE101-cli> show orgs org Provider sessions brief

VSN VSN  SESS              DESTINATION  SOURCE  DESTINATION
ID  VID  ID   SOURCE IP     IP          PORT    PORT      PROTOCOL NATTED SDWAN APPLICATION
0   2    4    192.168.5.101  192.168.5.1  1025    1025      1      No     No    -
0   2    18   10.0.192.101   192.168.1.6  1034    1234      6      No     No    -
0   2    3    192.168.4.101  192.168.4.1  1025    1025      1      No     No    -
```

- Run the **show device clients** CLI command to view the device resource alarms details.

```
admin@CPE101-cli> show device clients

CLIENT  VSN  CPU   MEM   MAX      ACTIVE    FAILED
ID      ID   LOAD  LOAD  SESSIONS  SESSIONS  SESSIONS
8       0    2     18    1000000   2         0
```

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Configure VOS Device Alarms