DELTA LOGIC Connectivity Service

Network Monitoring

Frequently Asked Questions

Version: Februar 2024

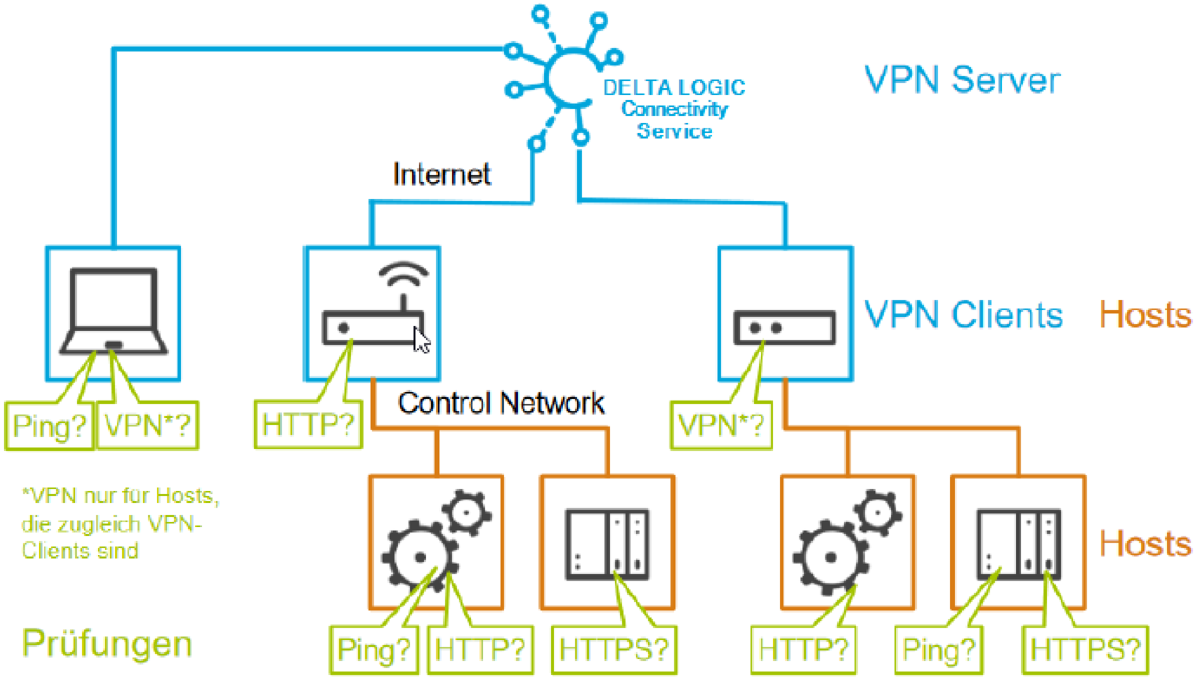
Frequently Asked Questions about Network Monitoring (DLCS)

What is Network Monitoring?

Remote plants deliver data continuously, report in case of an alarm or need to be available for remote maintenance. These services that are essential for your business processes must be available if they are required. Network Monitoring serves for checking this continuously.
The integrated monitoring of the DELTA LOGIC Connectivity Service monitors the availability of individual clients integrated in the VPN (e.g. routers or PC clients) and devices and applications behind that support IP communication.
You will receive an e-mail notification even before you have to realise that the connectivity is already lost.

The applications include the following examples:

- Is the SCADA control center computer connected via VPN?
- Responds the PLC or HMI on the plant upon a ping?
- Reacts the web server for configuration of the remote maintenance router?
- Does the Condition Monitoring or EDGE Computing device in the plant work?



The two terms “Host” and “Check” are relevant for the “Monitoring” function of the DELTA LOGIC Connectivity Service and are explained in the following.

Hosts

What is a host?

In the concept of integrated monitoring, a host is a network device that can be addressed using an IP-address via VPN: these are typically the VPN clients (router, PCs, smartphones) itself and the controls, panel PCs, HMIs, data loggers, measurement devices, Condition Monitoring or Edge Computing devices in the network (control network , OT) of the plant.

- In order to monitor a network device, it must be defined as host in the DELTA LOGIC Connectivity Service

How to define a host?

There are three options for this:

1. You can add a new host or copy an existing one in the Monitoring > Hosts view with its name an IP-address.
2. When adding a new check, the necessary host can be inserted under "+add new host…" if it not already exists.
3. When adding a new device (on the Devices tab), it can be added together with a check (default monitoring, ping, 60 minutes). In this case, the system will add a host for this device automatically. This host will be named by default as "VPN client" followed by the device name, but can also be renamed later.

Checks

What is a check?

A check is a concrete monitoring rule to verify the availability of a host via the network.

How to define a check?

There are two options for this:

1. You can add a new check for a host or copy an existing one in the Monitoring > Checks view.
2. When adding a new device (on the Devices tab), it can be added together with a check (default monitoring, ping, 60 minutes). In this case, the system will add a host for this device automatically. This host will be named by default as "VPN client" followed by the device name, but can also be renamed later.

- A host always requires at least one monitoring rule, i.e. the first check of a host cannot be deleted. This monitoring rule will only be deleted with the deletion of the host.

What is network monitoring and how does it check?

The integrated network monitoring supports checks of the assigned host of 3 different types:

- **PING**: Dispatch of a ping (ICMP echo request) to the destination address of the host to be checked
  - The host not ignore a ping since this will be considered as a failed check otherwise.
  - Firewalls between the server of the DELTA LOGIC Connectivity Service and the host must be configured accordingly.
- **HTTP/HTTPS**: Attempt to log in to the web server of the host via basic authentication (username/password)
  - The host must provide an appropriately configured web server.
  - The validity of the server certificate will not be checked (HTTPS).
  - Firewalls between the server of the DELTA LOGIC Connectivity Service and the host must be configured accordingly.
- **VPN**: Internal check of the server of the DELTA LOGIC Connectivity Service, whether the host to be checked is still connected as VPN client.

When is a check passed / failed?

For a check of the **VPN type**, this is considered as “passed”, if the VPN client is connected to the VPN server of the DELTA LOGIC Connectivity Service.
In all other cases, the check is considered as “failed”.

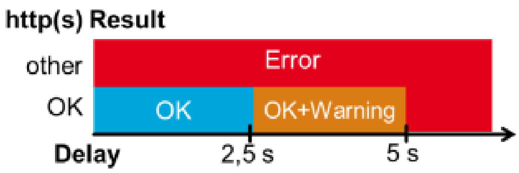
In case of a “passed” check of the **PING type**, the host must

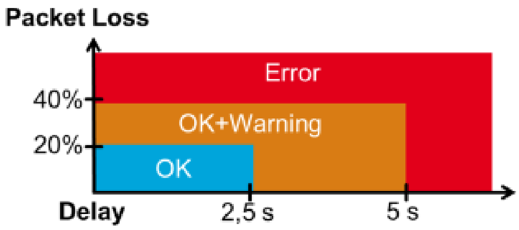
- Respond to the request within 5 s and
- Respond to 3 of 5 pings issued.

If a check oft he **PING type** is only hardly passed with

- more than 2.5 s delay or if
- more than 1 of 5 pings remain unresponded,

the result will be interpreted as “Warning” in the status-display.
In all other cases, the check is considered as “failed”.





In case of a “passed” check of the **HTTP/HTTPS type**, the host must

- respond to the request within 5 s and
- respond to the request with “OK” (http status code 200).

If a check of the **HTTP/HTTPS type** is only hardly passed with

- more than 2.5 s delay,

the result will be interpreted as “Warning”in the status display.
In all other cases, the check is considered as “failed”.

Can a host be checked in different types?

Yes, several checks can be added for a host simultaneously. Several checks of the same type are also permitted, e.g. to trigger an escalation for failures that last longer.

How often will the checks be performed?

The interval for checking the state will usually be defined for each check.
As soon as a check fails for the first time ("failed"), it will be continued with the "Retry interval".
As soon as a check is completed as "passed", the regular "Check interval" will be used again.
If the number of failed attempts exceeds the "Max. check attempts", it will be started again with the regular "Check interval".

What happens if a check fails?

As soon as a check fails for the first time, the state will be marked as error with a red symbol in the web interface of the monitoring function.
As soon as all retry attempts (parameter "Max. check attempts") have been completed as "failed", an alarm e-mail will be triggered.

E-Mails

Will I be notified about a failure?

If the check fails for the maximum number of retries, the system will send an email with the subject "ERROR:" and the name of the check to the specified e-mail address.

How to find out if a problem has been solved?

If a check fails it will be repeated. As soon as the check is considered as "passed", the e-mail recipients will receive a notification with the subject "RECOVERY:" and the name of the check.

- If you do not want to receive a notification upon recovery, you can check the checkbox "Send ERROR messages only".

Which information does the e-mail contain?

The DELTA LOGIC Connectivity Service integrates detailed information into the e-mails automatically.
In addition to the state of the check, the state of the underlying host and the corresponding VPN client will also be specified.

- All times in the email text are given in universal time (GMT, UTC); local time in middle Europe is 1 hour later in winter (CEZ) and 2 hours in summer (CEST).

How to integrate own information into the e-mails?

The field “description” in the check configuration is at your disposition – e.g. for service contact data or further details of the installed plant.

- If you only want to send your own description and do without the automatically generated detail information, you can check the checkbox “Send only description as messages”.

How to send an e-mail to several recipients?

Several recipient addresses can be entered separated by commas or blanks.

How to use only the state display in the web interface instead of an e-mail?

If only the indication in the web interface is desired, do not specify any e-mail recipients.

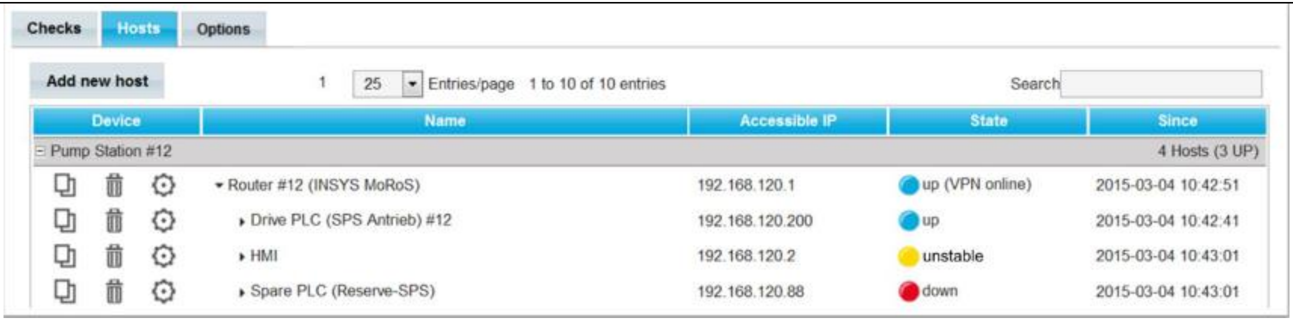
VPN-Clients

How to monitor a VPN without an accessible IP?

Each VPN client can be monitored, even if no routing information has been allocated for the respective device in the DELTA LOGIC Connectivity Service. This is usual for operating devices such as PCs.
The DELTA LOGIC Connectivity Service assigns a fix VPN IP address to each VPN client. This VPN IP-address is indicated on the “Devices” tab in the Info dialogue (Symbol “i”) and can be used as host IP.

Are there restrictions regarding group rules?

VPN hosts are also monitored by the server, if the group rules prohibit access to other VPN clients.



Device	Name	Accessible IP	State	Since
⊟ Pump Station #12				4 Hosts (3 UP)
⧉ 🗑 ⚙	▾ Router #12 (INSYS MoRoS)	192.168.120.1	● up (VPN online)	2015-03-04 10:42:51
⧉ 🗑 ⚙	▸ Drive PLC (SPS Antrieb) #12	192.168.120.200	● up	2015-03-04 10:42:41
⧉ 🗑 ⚙	▸ HMI	192.168.120.2	● unstable	2015-03-04 10:43:01
⧉ 🗑 ⚙	▸ Spare PLC (Reserve-SPS)	192.168.120.88	● down	2015-03-04 10:43:01

Views

What does the “Hosts” view display?

The hosts are grouped according to the name of the VPN client under “Monitoring > Hosts”. The group starts with the VPN host itself, followed by further hosts in the local network of the VPN client.
The network structure will be visualised by the indentation.
The hosts indicate whether the check have been performed successful.
The hots that are VPN client itself indicate additionally whether the VPN device is active.

What does the “Checks” view display?

The Checks are grouped according to the name of the underlying host under “Monitoring > Checks”.
If the last result of a check was “failed”, the “LED” in the State column is red; if a check has “passed”, it is blue.

How can these views be sorted?

Click on the column header to sort – a second click reverts the order.

Why are not all checks and all hosts displayed?

The checkbox “Collapse groups without disturbances” is active by default on the “Options” tab and only the groups with errors are displayed. The groups can always be expanded manually using the “+” symbol in front of the device name.

How do I prevent notifications upon every restart?

It is possible to specify how long monitoring will be suspended following a restart on the "Options" tab under "Downtime at instance restart".

How to detect unstable connections?

If the checkbox "Recognise unstable systems" is checked in the "Options" view, all events regarding connections will be monitored and a connection will then be classified as "unstable" if more than 4 state changes have occurred during the last 21 checks. The connection is classified as "stable" again if not more than one state change has occurred during the last 21 tests.
A state change is when the device connection changes from "connected" to "disconnected" or the connection quality becomes too poor (packet turnaround time ≥ 2500 ms) and vice versa.

Miscellaneous

How much hosts and checks can be added?

5 checks are permitted per valid VPN licence. The number of hosts is not restricted. Thus, you can add 50 checks altogether with 10 licences The checks may be distributed as desired across the VPN clients and hosts.

Do the checks generate additional data traffic?

The checks of the types PING, HTTP and HTTPS cause data traffic on the VPN connection. The checks of the type VPN do not cause additional data traffic since the continuous tunnel monitoring is evaluated on the VPN server.