



## Containers

### 18.1 Overview

Fidelia's Container technology allows you to correlate your IT infrastructure to your business service. The technology helps you answer questions such as:

- why is my eCommerce service down? Is it because of a server, router, database or application server?
- a server is down, but does it impact any critical service, and if so, which services?
- what was the cause of service downtime for the past month?
- why are users complaining about slow performance (which component of the distributed service is causing the slow performance).

You can model your end-to-end services easily using NetVigil Containers using some of the flexible features such as:

- creating containers using rules
- nesting containers
- creating “virtual devices” with selected tests from different devices
- having the same device in multiple containers
- setting the severity of containers based on rules

Note that ‘containers’ are distinct from “user departments”. You should use containers for modelling your “services”, while the departments in NetVigil allow you to create a “virtual” Network Management platform for different departments in your organization.

## 18.2 Managing Service Containers

**Service containers** allow you to group tests and devices to create logical, business-oriented views of your network in addition to your hardware-oriented views. An Administrator can create a service container that includes tests and/or devices from multiple Departments (e.g., any Departments associated with a User-Class that the Administrator controls).

You can generate reports on service containers, get uptime, and get real-time status if any of the underlying components fail or cross any threshold.

**NOTE Service Container** is a generic term, and can refer to either a Test Container (Virtual Device) or a Device Container (see below).

**NOTE** Updating or deleting a Service Container has no impact on devices or tests. If you delete a Test Container, for example, the tests included in the Test Container still exist in NetVigil.

There are two types of service containers:

**Test Containers (or Virtual Devices)** contain tests only. A real NetVigil device has a collection of tests associated with it. A Virtual Device is a collection of tests that are logically related, but not associated with the same physical device. For example, you can create a Virtual Device that includes ping tests for all devices on your network. This allows you to see at a glance which devices are unreachable without looking at test results for individual devices.

**Device Containers** can include both real devices and Virtual Devices (described above). They can also include other Device Containers, creating a nested hierarchy. For example, you can create a Device Container called Payroll that comprises the web server, router, and back end database used by the Payroll division. This allows you to quickly spot and troubleshoot problems that affect the Payroll group's ability to provide service.

Figure 18.1 illustrates a Device Container that encompasses real devices, a Service Container, and a nested Device Container.

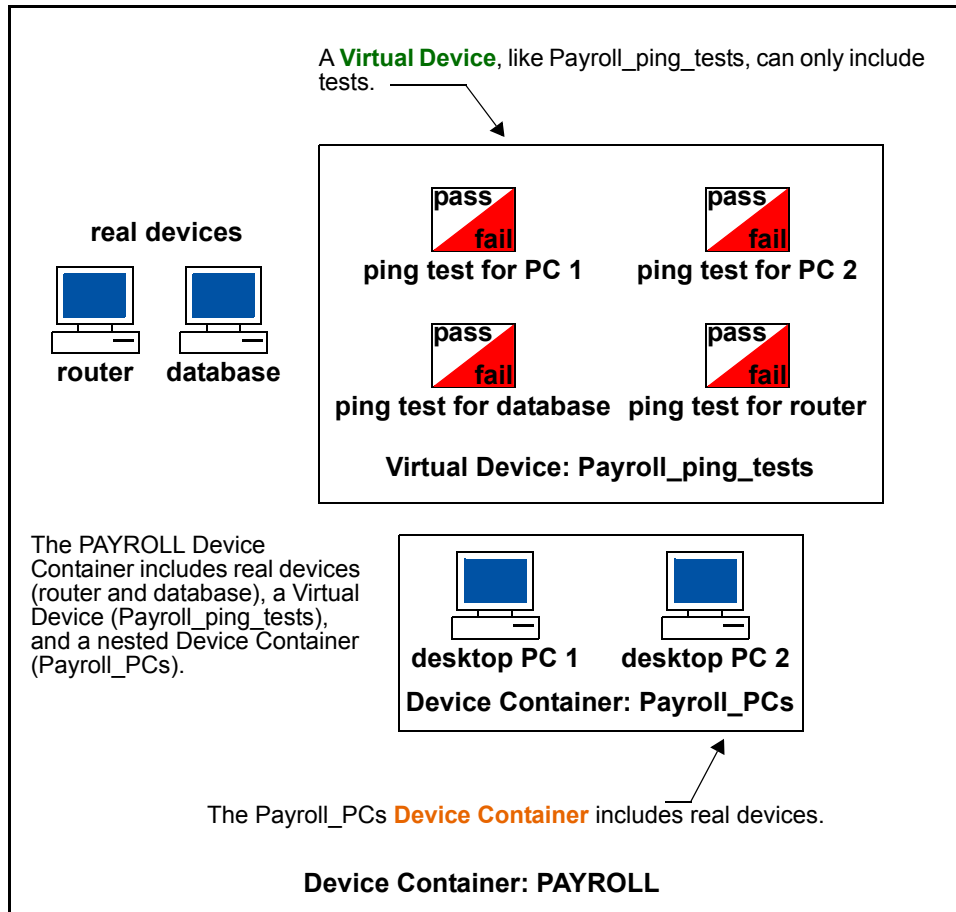


Figure 18.1 Example: Device Containers and Virtual Devices

## Device Tags

In addition to standard device properties (device name, model, etc.) NetVigil provides five customizable tags, which you can define to meet your needs. You can use these tags to create rules for populating Device Containers, as described in “Rule-Based Device Containers” on page 244.

**IMPORTANT:** By default, tags are labeled on the Create Device page as **Custom Attribute 1**, **Custom Attribute 2**, etc. If you use tags to create rule-based containers, we strongly recommend that you (or your NetVigil Administrator) replace the defaults with meaningful labels (e.g., **State**, **City**, etc.) as described in Section 3.4.13, “Customizing Device Tag Labels” on page 38. Otherwise, users may confuse the different tags, which can cause devices to be incorrectly added to or omitted from Device Containers.

## Rule-Based Device Containers

When you create a Device Container, you can populate it in one of the following ways:

- Manually select the real devices, Device Containers, and/or Virtual Devices that belong to the new Device Container.
- Create one or more rules. All *real devices* that match the rule(s) will automatically be added to the Device Container. Rule-based containers cannot contain Virtual Devices or Device Containers.

Rules work through Perl 5 regular expression matching and have the following form:

*device\_property* is like *regular\_expression*

Where *device\_property* can be device name, device type, device model, vendor name, or a tag (see “Device Tags” on page 243 for additional information).

When a rule-based container is created, existing devices whose properties match the rule(s) are automatically added to the container. When a new device is added to NetVigil, its properties are checked and it is assigned to all rule-based containers whose rules it matches.

## Using regular expressions in rules

You can use simple regular expressions in the rules.

So `*rtr*` would match anything with the word `*rtr*` in it. You can use `*` or `^` or `$` in the regular expressions. Note that `p.*x.*q` would not match `apxqb` but `. *p.*x.*q.*` or `*p*x*q*` would match `apxqb`.

**Example: Tags and rule-based containers**



A NetVigil administrator wants to create Device Containers for devices in specific locations. She also wants to create Device Containers for devices belonging to specific corporate groups. She defines tags as follows:

- Custom Attribute 1: State
- Custom Attribute 2: City
- Custom Attribute 3: Branch Office
- Custom Attribute 4: Corporate Dept.

Then, the administrator creates the following containers:

Container Name	Rules
NJ_branch_01_device_cont	State is like: NJ City is like: Princeton Branch Office is like: Pr*
NJ_branch_02_device_cont	State is like: NJ City is like: Trenton Branch Office is like: Tr*
Payroll_device_cont	Corporate Dept. is like: PAYROLL
Manuf_device_cont	Corporate Dept. is like: MANUFACTURING

When a user creates a device, they fill in the state, city, branch office, and corporate department properties. NetVigil then assigns the newly-created device to all of the containers whose rules it matches.



**□ To create a Test Container (Virtual Device):**

1. Select `MANAGE | containers`.
2. On the Manage Service Containers page click **Create a Service Container**.
3. On the Create a Service Container page, enter the **Service Container Name**.
4. For the **Container Will Include** option, select **Tests (Virtual Device)**.

5. Populate the container by selecting devices in the **Available** column and clicking the right arrow to transfer them to the **Currently Used** column. DO NOT select containers (those names that are prefaced with a # sign). If you select containers when creating a Virtual Device, the selection is silently ignored by NetVigil.
6. When you have selected all of the devices whose tests you want to include in this Virtual Device, click **Create Container**.
7. On the Create a Virtual Device (Test Container) page, select those tests that you want to include in the Virtual Device. For each real device that you selected, you can include **all current and future tests**, or you can specify **only the selected tests**. If you specify **only the selected tests**, select the desired tests from the scroll list provided.
8. Click **Submit** to create the Virtual Device.

#### To delete a Test Container

1. Select `MANAGE | containers`
2. Click on the `Delete` link for the container
3. Note that the component tests are not deleted since they still belong to real-devices, but the 'test container' is deleted.

#### To create a Device Container:

1. Select `MANAGE | containers`.
2. On the Manage Service Containers page click **Create a Service Container**.
3. On the Create a Service Container page, enter the **Service Container Name**.
4. For the **Container Will Include** option, select **Devices and Containers**.
5. Choose the method by which you want to assign devices to the container. In the **For Device Containers, Assign Devices:** field, select one of the following:

##### ► **Manually By Selecting Items From List Below**

If you choose this option, you can manually add real devices, Virtual Devices, and nested Device Containers. Continue with Step 6.

► **Automatically Based on Specified Rule**

If you choose this option, NetVigil automatically assigns all real devices that match the rules to this Device Container. Continue with Step 7.

6. To manually populate the container, select real devices, Virtual Devices, and/or Device Containers in the **Available** column and click the right arrow to transfer them to the **Currently Used** column. (The names of Virtual Devices and Device Containers are preceded by a # sign.) Continue with Step 8.
7. To create rules, enter a regular expression for pattern matching in one or more of the **Property is like:** fields. For example, if all devices belonging to the Finance group have device names starting with "Fin\_", you can create a rule to match all devices where **Device Name is like: Fin\_\***.

Devices matching following rules should be added to container automatically (applicable only for device containers)

Device Name is like:	<input type="text"/>
Device Type is like:	<input type="text"/>
Device Model is like:	<input type="text"/>
Vendor Name is like:	<input type="text"/>
Custom Attribute #1 is like:	<input type="text"/>
Custom Attribute #2 is like:	<input type="text"/>
Custom Attribute #3 is like:	<input type="text"/>
Custom Attribute #4 is like:	<input type="text"/>
Custom Attribute #5 is like:	<input type="text"/>

- When you have either selected all of the devices and containers that you want to include, or created a rule for including real devices, click **Create Container** to create the Device Container.

5/10/05 5:32:44 PM EDT  
logged in as widget\_ny (user/rw)

STATUS REPORTS MANAGE HELP

devices ← containers ↓ actions ← messages ← other ← prefs+ logout ←

**Create a Service Container**  
Container: Manufacturing  
Select or complete the required fields below. Click 'Create Container' to confirm.  
\* - indicates a required field

\* Service Container Name: Manufacturing

Comment:

Display Comment In Summary Screen:

\* Container Will Include:  
 Devices & Containers  
 Tests (Virtual Device)

\* For Device Containers, Assign Devices:  
 Manually By Selecting Items From List Below  
 Automatically Based On Specified Rule

Available (# = Container)      Currently Used:

192.168.1.10  
 # App Group  
 # Application Discovery  
 BPA WebLogic Server  
 Cisco-gw  
 cisco-test  
 # Core VoIP Equip  
 demo  
 # Ecomm Cont.  
 # eCommerce Service

Cisco Core Rtr  
 Dell Switch  
 Foundry Switch

\* Severity Of Container Is Determined By:  
 Severity Of Devices/Tests  
 Rule Specified Below

Ratio	Device/Test Severity	Container Severity
<input type="text"/> %	Ok	= Ok
<input type="text"/> %	Warning	= Ok
<input type="text"/> %	Critical	= Ok

Figure 18.2 Creating Service Containers

Once the container is created, it is displayed in the Manage > Containers web page:

The screenshot shows the 'Manage Service Containers' page in the Fidelity NetVigil interface. At the top, there is a navigation bar with tabs for STATUS, REPORTS, MANAGE, and HELP. Below the navigation bar, there are links for devices, containers (selected), actions, messages, other, prefs, and logout. The main content area displays a table of service containers. The table has two columns: 'SERVICE CONTAINER' and 'MODIFY'. The containers listed are: Application Discovery, Ecomm Cont., eCommerce Service (with a sub-entry for Packaging Service), Finacial Risk Mgt, KDM container, KDM container 2, Network (with sub-entries for Routers and Switches). Each container row has 'Update' and 'Delete' links. A search bar and pagination controls are visible at the top right of the table area.

Figure 18.3 Sample Containers

#### ❑ To delete a Device Container

1. You cannot delete a device container until it is empty. So, in a nested container hierarchy such as  $X \rightarrow Y \rightarrow Z$ , you must delete or move  $Z$  before you can delete  $Y$ .
2. Go to **MANAGE** -> Containers
3. Click on the **Update** link for container  $Y$  (to remove the nested container  $Z$ )
4. Move  $Z$  out of the right side “include” box and hit **Submit**
5. Delete the now empty container  $Y$  by clicking on the **Delete** link for  $Y$

### 18.3 Controlling Severity of Containers

The severity of a container (warning, critical, ok) is set using one of the following methods:

1. the “worst” severity of any of the components in a container
2. by setting a rule such as 40% warning implies warning severity

The rule based approach is most useful for redundant or clustered devices such as behind a load balancer.

Ratio	Device/Test Severity	Container Severity
<input type="text"/> %	Ok	= Ok
<input type="text"/> %	Warning	= Ok
<input type="text"/> %	Critical	= Ok

Default Severity = Ok

Ignore Display Category When Calculating Severity

**NOTE:** You cannot change the severity type once you create a container.

#### Example

Assume an eCommerce service with a cluster of web servers in the front, connected via two redundant routers to a remote location housing a database.

Since the containers support nesting, you can model the above using multiple nested containers such as:

1. a container of all your web servers with a rule based severity
2. another container of the redundant networks paths between the front end web server farm and the back end database
3. a top level container (call it eCommerce) which has the above two containers as well as the backed database in it, with the default severity rule.

If any of the three components in the eCommerce container goes into a non-OK condition, the top level eCommerce container will also change its state in real time.