Anturis

Getting started with the product
Contents

INTRODUCTION .......................................................................................................................... 2

INSTALLING ANTURIS AGENTS .......................................................................................... 3

ANTURIS HIERARCHY .......................................................................................................... 3
INFRASTRUCTURE .................................................................................................................. 3
COMPONENT .......................................................................................................................... 3
MONITOR ................................................................................................................................ 4
INSTALLING ANTURIS PRIVATE AGENT FOR WINDOWS .................................................. 5
INSTALLING ANTURIS PRIVATE AGENT FOR LINUX THROUGH THE COMMAND LINE ...... 6
INSTALLING ANTURIS PRIVATE AGENT FOR LINUX MANUALLY ...................................... 6

SETTING UP SERVER PERFORMANCE MONITORING ...................................................... 7

MONITOR PERIOD (REFRESH INTERVAL) ........................................................................... 8
STATUS ................................................................................................................................. 8
CONFIGURING A MONITOR STATUS CHANGE RULE ....................................................... 8

SETTING UP EXTERNAL MONITORING ............................................................................. 10

SETTING UP WEBSITE MONITORING ............................................................................. 10
CONFIGURING HTTP(S) MONITOR PARAMETERS ............................................................... 11

SETTING UP ADDITIONAL MONITORS ............................................................................. 12

ADDING A NEW MONITOR ............................................................................................... 13

SETTING UP COMPONENT DEPENDENCIES ................................................................... 15

CONFIGURING NOTIFICATIONS ......................................................................................... 16

ADD NEW PERSONS ........................................................................................................... 16
CHOOSE NOTIFICATION TYPES FOR THE PERSONS ....................................................... 17
ABOUT SEVERITY LEVELS ................................................................................................. 17
CHOOSE THE RESPONSIBLE PERSONS FOR EACH COMPONENT .................................. 18
CONFIGURE STATUS MAPPING FOR EACH COMPONENT ................................................ 19

SUBSCRIBING TO SLA REPORTS ...................................................................................... 20
Introduction

Hello, and welcome to Anturis!

This document will guide you through the steps required to start effectively monitoring the IT systems’ availability and performance and get a single-pane-of-glass view of the health of your on-premise, cloud-based or hybrid infrastructures.

A few words about how Anturis works. The service operates via two types of checks:

1. External monitoring is performed remotely using the global monitoring network of Anturis’ public agents. With no software to install, you are able to ensure your websites, web services and internet-facing devices are up and running smoothly.

2. Internal monitoring uses small-footprint native agents installed on the on-premise or cloud-based servers, thus enabling monitoring of the full IT infrastructure (system, network and application metrics) behind a firewall.

To get the most out of the service, we suggest you complete the following steps:

1. Install Anturis Agents on the hosts (operating systems) you want to monitor.
2. Set up server performance monitoring.
3. Set up external monitoring (e.g., web services and websites).
4. Set up additional monitors.
5. Set up component dependencies.
6. Configure notifications.
7. Subscribe to SLA reports.

In the following sections, we will cover each of the above steps to help you get the most value from the product in the quickest amount of time. We hope you enjoy using Anturis.
Installing Anturis Agents

Before you install your first agent, let’s walk through a few important product concepts.

Anturis hierarchy

The Anturis uses a hierarchical model that consists of four levels: Account, Infrastructure, Component, and Monitor.

Infrastructure

An infrastructure is a collection of IT resources grouped by their location, type, or another user-defined concept. Anturis supports the creation of multiple infrastructures for a single account.

Component

A Component is an entity that represents a group of monitors or a specific device or application. A Component has a set of properties, and each Component consists of a number of monitors. Components can be linked in what are called component dependencies. By using logical dependencies, you can avoid false alert notifications and obtain a hierarchical view of your IT assets.
Monitor

A Monitor represents a single IT infrastructure resource that needs to be checked. For each Component, you can add a number of Monitors. A Monitor is not considered a device, because depending on the type of infrastructure resource, there may be many kinds of monitors, such as a server CPU load, website HTTP latency, log file, or MySQL.
Now that you’re familiar with the hierarchy concept, it’s time to install the agent.

The **Anturis Private Agent** is a server application that allows you to monitor internal network resources (including those behind a firewall) and capture performance metrics of your operating system. The agent can be installed on various supported machines (including cloud- and IaaS-based) to gather all required data.

### Installing Anturis Private Agent for Windows

To download and install **Anturis Private Agent for Windows**, follow the steps below.

1. Ensure that the Windows machine is connected to the Internet.
2. Log on as an administrator.
3. Click on the “Agents & Locations” tab > “Add new agent” (”+” icon) > “Windows” and click on the required Windows version.
4. The .msi file download will start.
5. Run the Anturis-agent.msi file.
6. The Anturis Monitoring Setup Wizard window will open.
7. Read the instructions and click Next.
8. Read the terms and conditions and select “I accept the terms” in the License Agreement to proceed further.
9. Click Install.
10. Wait until the agent is being installed, select Start Anturis Agent Manager, and click Finish when finished.
11. Enter your Anturis Monitoring Account Name and Account Password.
12. Enter an Agent Name.
14. Click Connect.
There are two ways to install Anturis Private Agent for Linux: through the command line or by downloading the installation package.

**Installing Anturis Private Agent for Linux through the command line**

1. Click on the “Agents” tab > “Add new agent” (“+” icon).

2. Log on as the root user.
3. Ensure that the machine is connected to the Internet.
4. Run the specified command in the Linux command line. The agent will be downloaded and installed.

**Installing Anturis Private Agent for Linux manually**

1. Ensure that the machine is connected to the Internet.
2. Click on the installation file Linux or Linux x64 to download the private agent for Linux (the supported Linux versions are shown).
3. The .tar.gz file will start downloading.
4. Wait for the download to complete, and then follow the steps below to install the private agent.
5. Log on as the root user.
6. Place the file onto your Linux server. Once the private agent is on the server, extract the .tar file.
7. Example: tar -xzf anturis-agent-i686.tar.gz
8. Navigate to the extracted private agent directory and run the following command:
   Under root:  
   `install-anturis-agent.sh`
   Or:  
   `sudo ./install-anturis-agent.sh`
Setting Up Server Performance Monitoring

Now that your agents are installed, it's time to set up server performance monitoring.

To create a new Server Monitor, go to the Infrastructure page on the main menu and select Add Component. Then, follow the New Component Wizard to add a Windows Server or a Linux Server component:

1. Choose either the Windows Server or Linux Server Component, and then click Next.

2. Select an agent under Servers with Installed Agents.
   
   *Note: Only currently connected agents are shown in the list.*

3. [Optional] Change the default name of the component.

4. Turn the required monitors on and configure monitoring settings.
After a few minutes you’ll be able to see the gathered data by accessing the needed monitor inside the component.

Please review the following concepts to better configure the monitoring parameters:

**Monitor period (Refresh interval)**

The monitor period is the period of time between two subsequent checks of a monitored object.

**Status**

Status represents the state of health of monitors, components, and infrastructures. A monitored object can have one of the following statuses:

- **OK** (green color) — normal state
- **ERROR** (red color) — designates a severe problem, such as a lost connection or something gone down
- **WARNING** (orange color) — brings attention to a potential but not critical issue, such as if the hard drive is almost full or web services are responding slowly
- **NO DATA** (grey color) — used in some cases to show that Anturis Monitoring has no information yet about a monitored object and cannot be sure that an ERROR has occurred

The status of monitors is used to calculate the component status, with the worst status among all monitors being the one escalated to Component level.

Accordingly, the worst status among all components defines the infrastructure status.

**Configuring a monitor status change rule**

Each monitor can have one of the following statuses, depending on the monitor thresholds, the monitor status change rule, and the actual measurement or check results: OK (green), Warning (orange), Error (red), or No data (grey).
The status of monitors is used to calculate component status, with the worst status among all monitors being the one escalated to the component level.

Accordingly, the worst status among all components defines the infrastructure status.

The monitor status change rule allows you to fine-tune conditions for monitor status change. The rule defines how many consecutive measurements X out of consecutive measurements Y can go beyond the threshold or return within its limits in order for the monitor status to change.

Note: For monitors with two or more public agents, this rule applies only if at least two agents exceed the threshold or return within its limits within the same period of time.
Setting Up External Monitoring

As mentioned above, there are two types of checks: external and internal. In the previous section we set up server performance monitoring via the internal checks. Now, as an example of external monitoring, let’s configure website monitoring (in this case an HTTP(s) monitor).

Setting up website monitoring

In order to create a new website monitor via a Public Agent, choose the Infrastructure tab on the main menu and select Add Component (“+” icon). Then follow the New Component Wizard to create a website component:

1. Choose Website Component, and then click Next.

2. Select HTTP(s) Monitor. Enter the URL, domain name or IP of the target website.  
   *Note: When entering an IP address, be sure to use a public IP address and not an internal IP address. To monitor an internal IP address, please use an Anturis private agent.*

3. Click Next.

4. [Optional] Change the name of the monitor.

5. Click Finish.

Once a new monitor is created, you can see it on the Component page on the Monitors tab. You need to wait one or two monitor periods before there is enough data collected for the monitor status to be updated.
Configuring HTTP(s) monitor parameters

To configure HTTP(s) monitor parameters, click Edit and follow the steps below.

2. Select the Monitoring Settings tab.
3. In the HTTP Properties box, select POST or GET under Method. By default, the GET method is selected. If you select POST, the POST BODY box will appear, where you can input the data that you want to post.
4. [Optional] Enter the Port Number.
5. [Optional] Change the default value (min:sec) under Monitor Period.
6. [Optional] For the Timeouts option, enter the Error Threshold (ms) to receive an error warning if your website exceeds that amount of time, and/or enter the threshold value under the Warning Threshold.
7. The HTTP Status is selected by default.
8. For the HTTP Status option, select Matched or Not Matched under Valid If. By default, the Matched method is selected.
11. If your website uses basic authentication, you need to provide the user name and password in order to enable monitor access to your website. By default, this parameter is not selected.
12. Select Found In or Not Found In under Body Content under Content Matching. By default, this option is not selected.
13. Click Finish.
Setting Up Additional Monitors

In Anturis there are two ways of setting up the monitors: (1) by using the component creation wizard or (2) by adding new monitors to an existing component. In the previous section we followed the first approach, which offers a simplified way of setting up the monitors. However, adding a single monitor to an existing component allows you to choose from a wider range of monitor types. Here is an overview of all monitors available at this time:

Server (OS) performance
- CPU usage & load
- RAM
- Disk space
- Disk usage
- SMART drive
- Swap usage

Custom shell scripts

Services
- ICMP
- HTTP
- TCP
- SSH
- FTP
- SMTP
- IMAP
- POP3

Networks
- SNMP devices
- Ping
- Printers
- Network channel quality
- Network interfaces

Software
- MySQL database
- Apache server
- Log files
- Custom scripts
- OS processes
- Windows services
- Windows Event Logs
- Active Directory
- Java Virtual Machine

Websites
- Full page load
- Uptime & response time
- SSL Certificate expiration
- Body and header
- Content
- Web transactions
Adding a new monitor

As described earlier, a Component is an entity that represents a group of monitors or a specific device or application. A Component has a set of properties and each Component consists of a number of monitors. It’s important to mention that there can’t be a monitor without a component.

To add a monitor using a new component, please follow the steps below. (To add a monitor to an existing component, go directly to step 4.)

1. From the Infrastructure page, click Add Component (“+” icon).
2. Select the component category and click Next.
   Note: if you need to create an “empty” component, please choose the “Custom” option.

3. Complete the wizard steps, and then click Finish.
4. Double-click on the component that you want to customize, or point at the component and the monitor page will appear. Click “Add / Remove monitors”.

![Component Selection](image_url)

![Component Selection](image_url)
5. Click Add Custom Monitor.

6. Choose the required monitor type and follow the steps in the wizard.
Setting Up Component Dependencies

Using impact dependencies, you’re able to track down infrastructure components that may be causing a problem and also assess the problem’s impact on other infrastructure components. This provides the most complete picture of a problem’s cause and effect and, by helping to correctly gauge the severity of the problem, it allows for more accurate alerting of the appropriate responsible party.

For example, a website depends on web server software, which in turn depends on a server machine, where it is running. If the machine goes down, the web server software appears to be down as well, and the website becomes unreachable. In other words, the server impacts the application and the application impacts the website.

There are two main benefits of setting up the dependencies:

1. **You have a visual and intuitive representation** of an infrastructure.
2. **You get prevention of an alert spam** when one failed component affects all the dependent components and you get alerted (“spammed”) for each problem. With component dependencies enabled, you get only one notification about the root cause of the problem.

To create a logical infrastructure schema with existing components, go to the Infrastructure page and select Schema in the middle of the screen. Above the main area is a toolbar with three tools: Select, Link, and Unlink. To select a tool, just click on it.
Configuring Notifications

In order to properly configure the notifications system, please follow the steps below:

1. Add New Persons.
2. Choose the notification types for the Persons.
3. Choose the responsible Persons for each Component.
4. Configure Status Mapping for each Component.

Add New Persons

Go to the “People and Groups” page > click “New Person”.

Note: The “Notify about all incidents” option means that the Person will be alerted about any incident even if he/she is not responsible for it (responsibility setup will be shown below).

About the event types (Problem and Incident)

There are two event types in Anturis: Problem and Incident. A Problem happens on the Component level when a Component’s status becomes non-OK. An Incident happens on the Infrastructure level when at least one Component within an Infrastructure is given a non-OK status.

For linked components, Incidents are very helpful, in that several problems are aggregated into one Incident; therefore, you only receive one Incident alert rather than receiving notifications about all problems, which can cause an “alert spam.”

For independent components, an Incident equals a Problem as each component generates its own incident.
Choose notification types for the Persons

In the Notifications tab in the New Person window, choose the notification method that fits the corresponding severity level.

About Severity Levels

Severity indicates the importance or urgency of the problem.

The following severity levels are possible:

- Critical—most severe
- Major
- Minor
- Info—least severe

To ensure correct notifications, it is possible to map a component status to a problem's severity. Thus, once a problem occurs with a component, it is assigned a severity level. Each component contains the mapping between its status and the new problem's severity level. For example:

If the new Status is ERROR, then the new problem is assigned a severity of Critical.

If the new Status is WARNING, then the new problem is assigned a severity of Major.

Once problem severity is defined, alert notifications are sent to the persons responsible for the component.

It is possible to adjust the status-severity mapping of a component, in order to set up the relative priority of different components. Consider the following example:

The "very important" component has the following mapping:

- ERROR → Critical
- WARNING → Major

The "not that important" component has the following mapping:

- ERROR → Major
- WARNING → Minor
Choose the responsible Persons for each Component

1. Go to the Infrastructure page.
2. Click on the component and click Edit.
3. Select the Responsible tab to get to the selectable list of Users.
4. Select the checkbox for each person you wish to make responsible.
Configure Status Mapping for each Component

In the Edit Component window, choose the Status Mapping tab and set problem severity for the component statuses (i.e., “Warning – Major” and “Error – Critical”) and click Save.
Subscribing to SLA Reports

You can send up-to-date data about your infrastructure by having the responsible person subscribe to Reports. There are three types of subscriptions: daily, weekly, or monthly. To subscribe, follow the steps below:

1. Go to the Reports page.
2. Click Subscribe to Uptime Report.
3. Choose the recipient and then choose the report delivery frequency.
4. Click Save.

![Image of Subscribe to reports dialog box]

1. Go to the Reports page.
2. Click Subscribe to Uptime Report.
3. Choose the recipient and then choose the report delivery frequency.
4. Click Save.