Acronis

Acronis Monitoring Service

USER GUIDE

Table of contents

Copyright © Acronis International GmbH, 2003-2019

Copyright © Acronis International GmbH, 2003-2019

1 About Monitoring Service

This service helps monitor the uptime and performance of web services and operating systems in your infrastructure.

This service is available through a web interface.

2 Software Requirements

Supported web browsers

The Acronis monitoring service web interface supports the following web browsers:

- Google Chrome 29 or later
- Mozilla Firefox 23 or later
- Opera 16 or later
- Windows Internet Explorer 10 or later
- Latest Safari version running in the OS X and iOS operating systems

In other web browsers (including Safari browsers running on other operating systems), the user interface might be displayed incorrectly or some functions may be unavailable.

Supported operating systems and environments

Agent for Windows

- Windows Vista – all editions
- Windows Server 2008 – all editions
- Windows 7 – all editions
- Windows Server 2008 R2 – all editions
- Windows 8/8.1 – all editions except for the Windows RT editions (x86, x64)
- Windows Server 2012/2012 R2 – all editions
- Windows 10 – all editions

Agent for Linux

- Linux with kernel from 2.4.20 to 4.1 and glibc 2.3.2 or later

Various x86 and x86_64 Linux distributions, including:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, and 7.x
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, and 16.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, and 22
- Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, and 8.1
- CentOS 5.x, 6.x, and 7.0
- CloudLinux 6.x

Copyright © Acronis International GmbH, 2003-2019

3 Understanding basic concepts

Private agents

The Acronis Private Agent is a server application that allows you to monitor internal network resources (including 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.

Public agents

The Acronis Public Agent is an external poller that is located in different locations (see the "Public agents (p. 15)" locations and IP addresses topic) and is accessible as an out-of-the-box feature. The agent allows you to determine the uptime of your web services when accessed from those spots.

Component

A Component it 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 is called component dependencies. By using logical dependencies, you can avoid false alert notifications and obtain a hierarchical view of your IT assets.

Status

Status represents the health state 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: lost connection or something goes down.
- WARNING (orange color) —brings attention to a potential, but not critical issue; such as, hard drive is almost full or web services are responding slowly.
- NO DATA (grey color) —used in some cases to show that Acronis Monitoring has no information yet about a monitored object and cannot be sure that an ERROR happened.

The statuses of monitors are 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.

Event type (problem and incident)

There are two event types in Acronis Monitoring Service: 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 useful in that one incident aggregates more than one problem and you are only alerted about those, instead of 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.

Copyright © Acronis International GmbH, 2003-2019

Infrastructure

An infrastructure is a collection of IT resources grouped by their location, type, or another user-defined concept. The Acronis monitoring service allows for multiple infrastructures to be created for a single account.

An infrastructure consists of different components, which can represent categories.

Hierarchy

The Acronis monitoring service uses a hierarchy model that consists of four levels: Account, Infrastructure, Component, and Monitor.

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 an infrastructure resource, there may be many monitor types. For instance, server CPU load, website HTTP latency, log file, or MySQL.

Monitor period

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

Notifications

The Acronis monitoring service enables you to send notifications to different people within your organization, so that the right person is notified when an issue occurs. Thus, notification events are divided into alert notification and recovery notification. An alert notification is used when an incident occurs, as opposed to a recovery notification, which is sent when a problem was solved or it disappeared.

Person

A person represents a contact who can be notified in case of an emergency with at least one component. Each person can be made responsible for many components, so this person will receive notifications for all the components that are assigned to them.

Group of persons

Several persons can be gathered into a group. The group helps to inherit notification settings to many persons as you need, where each of them will receive an alert and/or recovery notification.

Severity

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 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 severity level. For example:

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

Copyright © Acronis International GmbH, 2003-2019

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

Once a 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. Let's 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

4 Getting started

4.1 Setting up website monitoring

How do I set up a website monitor via a public agent?

In order to create a new website monitor via a public agent, choose the **Infrastructure** tab on the main menu and select **Add Component**. Then, follow the New Component Wizard to create a website component:

1. Choose **Website Component**, and then click **Next**.
2. Select **HTTP(s) Monitor** and **Ping 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 Acronis 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.

How do I configure parameters for created website component?

On the **Infrastructure** page, double click on the website component that you created or click on the component and click **View** to go to the **Component** page.

How do I configure HTTP(s) monitor parameters?

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

1. [Optional] On the **General Settings** tab, change the public agent.
2. Select the **Monitoring Settings** tab.

Copyright © Acronis International GmbH, 2003-2019

3. In the HTTP properties, 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 if your website exceeds this 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 of**. By default, the **Matched** method is selected.
9. [Optional] Enter a value for **Status pattern**.
10. [Optional] Enter an amount for **Redirection attempts**.
11. If your web site uses basic authentication, you need to provide the user name and password in order to enable monitor access to your web site. 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**.

How do I configure ping monitor parameters?

To configure created ping monitor parameters, click **Edit** for **Ping Monitor** and follow the steps below.

1. [Optional] On the **General Settings** tab, change the public agent.
2. Select the **Monitoring Settings** tab.
3. [Optional] In **General** properties, change the default value (min:sec) for the **Monitor period**.
4. [Optional] In the **Options** properties, select IPv6.
5. [Optional] In the **Timeouts** properties, enter the **Warning threshold (ms)** and/or **Error threshold (ms)**.
6. Click **Finish**.

4.2 Setting up Windows monitoring

In order to create a new Windows 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 component:

1. Choose **Windows 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.

While adding a monitor for the first time for your component, if you haven't yet downloaded the Acronis private agent, click the help icon and click **About Acronis software package and how to install it**. Alternatively, you can go to the **Agents** page and select **Add agent**.

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

Copyright © Acronis International GmbH, 2003-2019

1. Ensure that the machine is connected to the Internet.
2. Log on as an administrator.
3. Click on the installation file **Windows Vista or newer, Windows Server 2008 or newer** link to download the private agent for the Windows operating system (see “Software requirements (p. 4)”).
4. The .msi file download will start.
5. Run the acronis-agent.msi file.
6. The Acronis Monitoring Setup Wizard window will open.
7. Read the instruction 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 Acronis Agent Manager** and click **Finish** when finished.
11. Enter your Acronis Monitoring **Account Name** and **Account Password**.
12. Enter an **Agent Name**.
13. [Optional] Set-up proxy server settings.
14. Click **Connect**.

When the installation is complete, go to the second step of the wizard and click **Update agent connection**. In the agents list, select your server, and then click **Next** to continue. Complete the rest of the steps in the wizard.

How do I configure Monitors for a new Windows Server Component?

When a server Component is created, you will see the Component manager page where you can choose monitors.

Choose the monitors that you want to monitor. You may keep the default values for the parameters.

How do I configure disk monitor parameters?

Select the **Free Space** and/or **Disk Usage** slider(s) if you need to monitor the available free space and/or disk usage on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. [Optional] In the **Disk space** and **Disk usage** thresholds, enter the **Error threshold (Gb/%)** to receive an error if your server exceeds this amount of space or percentage of time while a drive is busy with operations, and/or enter the threshold value under **Warning threshold**.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
5. Click **OK**.

Select the S.M.A.R.T. attributes slider if you need to monitor the S.M.A.R.T. status of your hard drives. In the **Monitor Parameters** window, set the following values:

Note: The S.M.A.R.T. drive Monitor is unavailable for virtual machines.

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).

Copyright © Acronis International GmbH, 2003-2019

3. Select monitoring metrics.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
5. Click **OK**.

How do I configure CPU monitor parameters?

Select the **CPU Usage** and/or **CPU Load** slider(s) if you need to monitor the CPU usage and/or CPU load on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. [Optional] In the **CPU usage** and **CPU load** thresholds, enter the **Error threshold (%)** to receive an error if your server exceeds this amount of usage (loads) and enter the threshold value under **Warning threshold**.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.

How do I configure network monitor parameters?

Select the **Network** slider if you need to monitor the network channel on your server. In the *Monitor Parameters* window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. Enter the **Error threshold** and/or **Discards** values (packages per min), to create a notification for when a threshold exceeded.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.

How do I configure Windows event log Monitor parameters?

Select the **Application event log** slider if you need to monitor the Windows event logs on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. [Optional] Change the log name.
4. You can enter the threshold values if any of the user-defined events are logged and/or the number of error events is reached (events with "Error" or "Critical" severity levels) and equals or exceeds the specified value.
5. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
6. Click **OK**.

How do I configure Windows Services monitor parameters?

Select the **Windows service monitoring** slider if you need to monitor the Windows services on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. Select the services that you want to monitor.

 Copyright © Acronis International GmbH, 2003-2019

How do I add a custom monitor for the server?

If you want to add other monitors, click **Add custom monitor** and choose another monitor.

4.3 Setting up Linux monitoring

In order to create a new Linux server Monitor, choose the **Infrastructure** page on the main menu and select **Add Component**. Then, follow the New Component Wizard to add a Linux Server Component:

1. Choose **Linux Server Component** and click **Next**.
2. Under Servers with installed agents, select the agent from the list.

   Note: Only currently connected agents are shown in the list.

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

The first time you add a monitor for your component, download Acronis Private Agent if you haven't already done so. To do this, click the help icon and click **About Acronis software package and how to install it**. Alternatively, you can go to the **Agents** page and select **Add new agent**.

Downloading Acronis Private Agent for Linux

1. Ensure that the machine is connected to the Internet.
2. Click on the installation file **Linux i686** (https://monitoring.acronis.com/download/acronis-agent-i686.tar.gz) or **Linux x64** (https://monitoring.acronis.com/download/acronis-agent-x86_64.tar.gz) to download the private agent for Linux (the supported Linux versions are shown).
3. The .tar.gz file will start downloading.

   Wait for the download to complete, and then follow the steps below to install the private agent.
4. Log on as the root user.
5. Place the file onto your Linux server. Once the private agent is on the server, extract the .tar file.

```
Example:  sudo tar -xvwzf acronis-agent-i686.tar.gz
```

6. Navigate to the extracted private agent directory and run the following command:

```
install-acronis-agent.sh
```

Downloading Acronis Private Agent for Linux through the command line

1. First, obtain the download link for the private agent from the agent installation window.
2. Go to the **Agents** page and select **Add new agen**t or click the help icon and click **About Acronis software package and how to install it**.
3. Copy the installation command from the pop up window.
4. Log on as the root user.
5. Ensure that the machine is connected to the Internet.
6. In Linux, run the copied command. The agent will be downloaded and installed.

If everything goes well, you will see the following:

```
Starting Acronis Agent
Setting settings...
Success
Connecting to server...
```


Copyright © Acronis International GmbH, 2003-2019

```
Success
Sending command to server...
Provision finished successfully.
```

When the installation is complete, go to the second step of the wizard and click **Update agent connection status**. In the servers list, select your agent. Then click **Next**. Complete the rest of the steps in the wizard.

How do I configure monitors for a Linux Server Component?

When the server component is created, you will see the **Component Manager** page, where you can choose monitors.

Choose the monitors that you want to monitor. You may keep the default values for the parameters.

How do I configure disk monitor parameters?

Select the **Free Space** and/or **Disk Usage** slider(s) if you need to monitor the available free space and/or disk usage on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. [Optional] In the **Disk space** / **Disk usage** thresholds, enter an **Error threshold (Gb/%)** to receive an error message if your server exceeds this amount of space or amount of usage and/or enter the threshold value under **Warning threshold**.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.

Select the S.M.A.R.T. Attributes slider if you need to monitor the S.M.A.R.T. status of your hard drives. In the **Monitor Parameters** window, set the following values:

Note: The S.M.A.R.T. drive Monitor is unavailable for virtual machines.

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. Select a monitoring metric.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
5. Click **OK**.

How do I configure CPU Monitor parameters?

Select the **CPU Usage** and/or **CPU Load** slider(s) if you need to monitor the CPU usage and/or CPU load on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. [Optional] In the **CPU usage** and **CPU load** thresholds, enter the **Error threshold (%)** to receive an error if your server exceeds this amount of usage (loads) and enter the threshold value under the **Warning threshold**.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.

Copyright © Acronis International GmbH, 2003-2019

How do I configure Network Monitor parameters?

Select the **Network** slider if you need to monitor the network channel on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. Enter the **Error threshold** and/or **Discards** values (packages per min), to create a notification for when a threshold exceeded.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.

How do I configure Linux services Monitor parameters?

Select the **Services** slider if you need to monitor the Linux services on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. Select the services that you want to monitor.

How do I add a custom Monitor for the server?

If you want to add other monitors, open the wizard and click **Add custom monitor**, and then choose another monitor.

5 About Acronis agents

5.1 Private agents

Installing agents

In Linux

Downloading Acronis Private Agent for Linux

1. Ensure that the machine is connected to the Internet.
2. Go to the **Agents** page and select **Add agent** or click help icon and then click **About Acronis software package and how to install it**.
3. Click on the installation file **Linux i686** (https://monitoring.acronis.com/download/acronis-agent-i686.tar.gz) or **Linux x64** (https://monitoring.acronis.com/download/acronis-agent-x86_64.tar.gz) to download the Private Agent for Linux operating system (the supported Linux versions are shown).
4. The .tar.gz file will start downloading.

   Wait for the download to complete, and then follow the steps below to install 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

```
Example:  sudo tar -xvwzf acronis-agent-i686.tar.gz
```

7. Navigate to the extracted private agent directory and run the following command:

```
install-acronis-agent.sh
```


Copyright © Acronis International GmbH, 2003-2019

Downloading the Acronis Private Agent for Linux through the command line

1. Go to the **Agents tab** and select **Add agent** or click **About Acronis software package and how to install it.** in the Component wizard.
2. Copy the command from the pop up window.
3. Log on as the root user on Linux Server.
4. Ensure that the machine is connected to the Internet.
5. In Linux, run the copied command.

The agent will be downloaded and installed. If everything goes well you will see the following:

```
Starting Acronis Agent

  Setting settings...

  Success

  Connecting to server...

  Success

  Sending command to server...

  Provision finished successfully.
```

In Windows

1. Ensure that the machine is connected to the Internet.
2. Log on as an administrator.
3. Go to the **Agents** tab and select **Add agent** or click **About Acronis software package and how to install it** in the Component wizard.
4. Click on the **Windows Vista or newer, Windows Server 2008 or newer** link to download the Private Agent for Windows operating system (see “Software requirements (p. 4)”).
5. The .msi file will start to download.
6. Run the acronis-agent.msi file and start the setup program.
7. The Acronis Monitoring Setup Wizard window will open.
8. Read the instruction and click **Next**.
9. Read the terms and conditions and select **I accept the terms in the License Agreement**.
10. Click **Install**.
11. When the Agent has been installed, select **Start Acronis Agent Manager** and click **Finish** when finished.
12. Enter your Acronis Monitoring **Account Name** and **Account Password** (See "Credentials for your Private Agents").
13. Enter an **Agent Name**. The name you provide here for the agent will be used in Acronis Monitoring.
14. [Optional] Set-up the proxy server settings.
15. Click **Connect**.

Uninstalling agents

In Linux

Follow the steps below to uninstall Acronis private agents by using a command line:

1. Log on as the root user.

 Copyright © Acronis International GmbH, 2003-2019

2. Run /opt/acronis/uninstall-acronis-agent.sh
3. Confirm your decision.

In Windows

Follow the steps below to uninstall Acronis Private Agents:

1. Log on as an administrator.
2. Go to the **Control Panel**, and then select **Programs and Features > Acronis Monitoring > Uninstall**.
3. Confirm your decision.

Updating agents

To update an agent by using the web interface:

1. Go to the **Agents** page.
2. Select the agents that you want to update.
3. Click **Update**.

Credentials for your Private Agents

After product registration you should receive the email with your credentials. The email contains Account Name and Account Password, which you should use during configuration of your Private Agent.

> *If you do not receive the email, please check your spam folder to be sure that our emails are not being detected as spam. Otherwise, please contact support team to resend the email.*

5.2 Public agents

Public agents overview

The Acronis Public Agent (locations) is an external poller that is located in different locations and is accessible as an out- of- the- box feature. The agent allows you to determine the uptime of your web services when accessed from those spots.

Public agents' locations and IP addresses

The Acronis monitoring service has a range of public agent locations:

- Sydney, Australia
- Strasbourg, France
- Frankfurt am Main, Germany
- Nagano, Japan
- Moscow, Russia
- Singapore
- London, UK
- Ashburn, Virginia, US
- Dallas, Texas, US

The following is a list of public IP addresses for these locations.

- Ashburn - 199.193.156.166
- Dallas - 199.193.158.206

Copyright © Acronis International GmbH, 2003-2019

- Frankfurt - 185.151.161.254/32
- London - 185.151.162.253/32
- Moscow - 193.32.199.134
- Nagano- 45.254.38.63
- Singapore - 209.58.170.8
- Strasbourg - 85.25.240.143
- Sydney - 103.101.129.40

Note: You can always deploy an Acronis private agent to any server of your choice and use it for your Web service Monitors.

5.3 How do I filter traffic from a public agent (Google Analytics)?

In order to exclude public agent traffic from your Google Analytics statistics, follow the steps below.

1. Sign in to your Google Analytics account.
2. Go to the **Admin tab** and navigate to the account that you want to create the filter for.
3. In the **VIEW** column, click **All Filters**.
4. Click **+ New Filter**.
5. Select **Create New Filter**.
6. Enter a name for the filter.
7. Set the filter type to **Predefined filters**.
8. Choose **Select filter type** from the drop-down menu and select **Exclude**.
9. Set the **Filter** field to traffic from the IP addresses.
10. Enter the public agent IP address and click **Save** when finished.

6 Infrastructure management

6.1 Adding and managing a new infrastructure

Adding and managing a new infrastructure

In order to create a new infrastructure, follow the steps below:

1. Open the drop-down menu in the top left corner.
2. Click **Add new Infrastructure**.
3. Enter an **Infrastructure name** and click **Add**.

To make changes for your infrastructure, open the top left drop-down menu. Then, click the gear icon for your infrastructure and choose the **Delete** or **Rename** option in the dialog box.

Note: The first infrastructure is created automatically and cannot be deleted.

Infrastructure page

The **Infrastructure** page has three views: a schema view, a problems view, and a dashboard view. To switch between the views, click the corresponding name in the top center of the screen.

All views provide access to the different features and operations that are described below.

Copyright © Acronis International GmbH, 2003-2019

Schema view

The **Schema Overview** page allows you to see all components that are in your infrastructure. The schema overview is selected by default.

Each schema component shows health statuses as small circles in the top left corner. If any component fails, the circle is marked red. If all are okay, the circle is marked green. If no data is gathered, the circle is marked grey. If there is a warning, the circle is marked orange.

Above the main area is a toolbar with three tools: **Select**, **Link**, and **Unlink**. To select a tool, just click on it.

- The **Select** tool allows users to manage components. Clicking on any component opens a pop-up box menu, which has a list of monitors included in that particular component and their latest statuses. Alternatively, point at a component and a pop-up box will appear.
- The **Link** tool allows users create component dependencies between different components.
- The **Unlink** tool allows users to remove component dependencies.

Problems view

The **Problem Overview** page represents all current and recent problems with your components.

To navigate through the problem overview, you can switch between the **Current Problem** tab and the **Recent Problem** tab. By default, the **Current Problem** tab is selected.

If there is a current problem with an existing component in your chosen infrastructure, the details of the problem will be shown. To see detailed information, follow the steps below.

1. Click on the left arrow.
2. Click **Detail**.
3. Read more about the error and click **OK** when finished.

To configure the **Problems Overview** table, click the gear icon, and then customize the table columns. The table will simultaneously update.

Dashboards view

The **Dashboard Overview** page allows you to see a graphical representation of data points on a monitor over a period of time.

To create a new dashboard, follow the steps below.

1. Click **+**.
2. Create a **Dashboard name.**
3. Click **+** and select the monitors that you want to see on the dashboard.

   Note: You cannot add more than seven monitors for each dashboard.
4. Click Create.

Now, you can see the graphical representation of data points on the selected monitors over a period of time.

To view your collected data from the **Dashboard Overview** page, you can select the date segment you wish to view. This includes day, hour, month, and year. You can also select a single date in time through the popup window calendar, by clicking on that day.

If you want to view just one or two measured lines, unselect the checkboxes under the graph. The legend will be replaced with only the selected lines.

Copyright © Acronis International GmbH, 2003-2019

To view all data again, select the checkboxes.

In order to modify the current dashboard, follow the steps below.

1. Click the gear icon, select **Edit**, and then select **Manage Monitors**.
2. Click **Save Dashboard** to make changes.

To delete a dashboard, click the gear icon, select **Delete**, and then agree with the warning message.

6.2 Component

In order to create a new component, follow the steps below.

1. From the **Infrastructure** page, click **Add Component**.
2. Select the component category and click **Next**.
3. Complete the wizard steps, and then click **Finish**.

To modify an existing component, follow the steps below.

1. Single click on the component that you want to edit or point at the component and a dialog box will appear. Alternatively, select the component on the left component panel and click on the gear icon.
2. Click **Edit**.
3. Switch between the tabs for the components and make changes, if needed.
4. Click **Save**.

Note: If predefined components such as Windows Server or Active Directory are added with additional features (parameters) in future releases or you add a new hard drive, follow the steps below.

*On the **Component** page, click **Manage Monitors**.*

*Click **Rebuild component**.*

Select new parameters, if needed.

*Click **Finish**.*

To remove an existing component, follow the steps below.

1. Single click on the component that you want to edit or point at the component and a pop-up box will appear. Alternatively, select the component on the left component panel and click the gear icon.
2. Click **Delete**.
3. Verify your decision to delete the component.

6.3 Monitor

There are two primary types of monitors: an external or web-site monitor, and an internal or infrastructure local resource monitor.

A web-site monitor allows you to check web services by using web protocols such as HTTP.

A Local Resource Monitor allows you to create a network, server, or application monitor to check local intranet resources, such as a server CPU or memory or SNMP-enabled devices.

To create a new monitor, follow the steps below.

Copyright © Acronis International GmbH, 2003-2019

1. Double click on the component that you want to customize or point at the component and the monitor page will appear.
2. Click **Manage Monitors > Add Custom Monitor**.
3. Choose Monitor.
4. Click **Next**.
5. Click **Finish**.

To modify an existing monitor, follow the steps below.

1. Click **Edit** for monitor.
2. [Optional] On the **General Settings** tab, change the public agent.
3. [Optional] Select the **Monitoring Settings** tab, and make changes.
4. [Optional] Select **Status rules** and change measurements.
5. Click **Save**.

To remove a monitor, follow the steps below.

1. Double click on the component that you want to edit or point at the component and the monitor page will appear.
2. Click **Manage Monitors**.
3. Click the **"X"** icon.
4. Confirm deletion.

6.4 Global overview page (problem overview)

The **Global Overview** page displays a table with all discovered (current and recent) problems.

To navigate through the problem overview, you can switch between the **Current Problem** tab and the **Recent Problem** tab. By default, the **Current Problem** tab is selected.

If there are current problems with the existing components in the infrastructure, those details will appear.

To access detailed information about the problem, follow the steps below.

1. Click on the left arrow of the existed problem to open the second sub-view.
2. Click **Detail**.
3. Click **OK** when finished.

To configure the **Problems Overview** table, click the gear icon, and then customize the columns. The table will simultaneously update.

6.5 Setting up component dependencies

The hierarchical arrangement Infrastructure > Components > Monitors helps avoid notification "spam" in the event that several components fail simultaneously.

For this purpose, the dependencies should be set on your infrastructure components:

1. Connect components using the **Link** and **Unlink** tools on the **Infrastructure** page.
2. Create meaningful and logical dependencies between components with the top-level component (e.g., router), the middle one being next (e.g., server), and the bottom one being the lowest-level component (e.g., Apache Server).

Copyright © Acronis International GmbH, 2003-2019

In real life, if a server goes down, the database goes down as well. If router stops working, too, then all network resources are unavailable. Hence, the above arrangement reflects a real-life situation.

When components are linked and an incident happens, the Acronis monitoring service sends out only one notification stating “Incident involving Router … STARTED” (see “Notifications (p. 23)”).

Such impact dependencies make sense only if hardware and software components are logically connected in real life. If not, don’t force-link the components. Just leave them as unlinked.

With an unlinked infrastructure, if several independent components fail simultaneously, the corresponding number of problems are generated and a corresponding number of notifications are sent.

6.6 Configuring a monitor status change rule

Depending on the monitor thresholds, the monitor status change rule, and the actual measurement or check results, each monitor can have the following statuses: OK (green), Warning (orange), Error (red), or No data (grey).

The statuses of monitors are 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 should 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.

To set status rules, go to the **New monitor** dialog or the **Edit Monitor** dialog, and then select the **Status Rule** tab.

For example, for the Ping Monitor, you can set two out of two consecutive measurements. This means that if two out of 2 two measurements exceed the threshold, the status will change. If only one out of two measurements exceed the threshold, the status does not change.

6.7 Mapping a component status to a problem severity level

When a component fails with the monitor metric exceeding the threshold, there are two possible statuses: Warning or Error. Each of them can have one of the four severity levels: info, minor, major, critical. Such variability in severity levels allows for a flexible and comprehensive notification system (see “Notifications (p. 23)”).

To set a severity level, click the gear icon for the component and select the **Status Mapping** tab.

The default values for severity level are: Warning status — Major severity, Error status — Critical severity. You can change these values, if needed.

Copyright © Acronis International GmbH, 2003-2019

7 Maintenance mode

The maintenance mode feature allows you to designate a period of time when you want to automatically suspend all problem reporting and notifications. Your monitoring will not be stopped during the scheduled maintenance period — you will just stop receiving alert notifications.

To set a maintenance mode, click **Start maintenance**.

The maintenance mode window will open.

Under maintenance mode, select the option you want by clicking its radio button:

- Select **Start now** to start maintenance mode immediately. You have to stop it manually.
- Select **Start later** to schedule your maintenance period for a specific date and time, by using the **Start time** and **End time** options. The maintenance mode stops automatically, based on the specified end time.

Note: You can change the time zone via your account settings.

8 People and groups

8.1 Person

You can manage people (a person) in your account from **People and Groups** page.

Add Person

Add a new person by clicking **Add > People** from the **People and Groups** page.

The following settings are available in the **General** *tab for every person.*

Name

Enter a name to identify the person.

Email address

Enter a primary email address for the person. This contact method will be used for all email alerts and recovery messages.

Use HTML

Check if you want to send the notification in HTML format.

Phone number

[Optional] If entered, it is available as a contact method for voice alerts and SMS alerts.

Notify about all incidents

Select if you want the person to be notified only about incidents.

The following settings are available in the **Groups** *tab.*

Checkbox for group(s) to assign a current person to that group.

Copyright © Acronis International GmbH, 2003-2019

The following settings are available in the **Notification** *tab.*

Select the severity level for alerts when they must be sent to responsible person.

If needed, you can change recovery notification options by using the drop-down menu.

The following options are available: Same as alert (default value), none, email, SMS, call.

The following settings are available in the **Subscription** *tab.*

You can schedule any report to be auto-delivered via email. Select how often the report should be emailed. Choose from: weekly, daily, or monthly.

Edit a person

Select a person, click the gear icon, and then select **Edit** to modify user details.

View existing people

The left side panel displays all the people in your account.

To delete a person, select the person, click the gear icon, and then select **Delete**.

8.2 Group

Several persons can be united into a group. You can manage the group in your account from the **People and Groups** page.

Add group

Go to the **People and Groups** page and click **Add > Group**.

The following settings are available in the General tab of every person.

Name

Enter a name to identify the group.

The following settings are available in the **People** *tab.*

Select people from the list and assign them to the current group.

The following settings are available in the **Subscription** *tab.*

You can schedule any report to be auto-delivered via email. Select how often the report should be emailed. Choose from: weekly, daily, or monthly.

Adding a person into the group

To add a person into the group, follow the steps below.

1. Select a Group, click the gear icon, and then select **Edit**.
2. Open the **People** tab and select the person that you want to add.
3. Click **Save**.

Alternatively, follow the steps below.

1. Select the person, click the gear icon, and then select **Edit**.
2. Open the **Groups** tab and select a group for the person.

Copyright © Acronis International GmbH, 2003-2019

3. Click **Save**.

Editing groups

Select a group, click the gear icon, and then select **Edit** to modify the group details.

To delete a group, select the group, click the gear icon, and then select **Delete**.

View existing groups

The left side panel displays all groups in your account.

9 Notifications

How notifications work?

The Acronis monitoring service enables you to send alert and recovery notifications to different people within your organization, so that the right person is notified when an issue occurs. Notifications can be delivered via email, text message, or over a voice call. If one recipient is unable to deal with or respond to the alert, the alert is automatically sent to the all people on the notifications list.

Configuring notifications

Problem and incident severity helps define which person is notified about an event.

To configure notifications, follow the steps below.

1. Go to the **People and Groups** page.
2. Select a person to receive notifications.
3. Click the gear icon and select **Edit**.
4. Open the **Notifications** tab.

There are two different ways to set up notifications.

1. You can make a person responsible for more than one component. This person will receive notifications about all problems with the component(s) they are responsible for.

   Where to set: Go to the **Infrastructure** page, select the Component, click **Edit**, and then click the **Responsible** tab.
2. If you want a person to be notified only about incidents, check **Notify about all incidents**.

Where to set: Go to **People and Groups**, select the person, click the gear icon, select **Edit**, and click the **General** tab.

If the **Notify about all incidents** is checked, notifications work differently depending on the organization of the infrastructure. The two ways of working with notifications are described below.

1. When a problem starts in an infrastructure with linked components, one notification is sent – even if several components fail simultaneously. For example, “Incident ... involving … -STARTED”. Additional email-only notifications are sent if a new problem occurs on a higher infrastructure level. Such notifications look like this: “Incident ... involving … -New problem with COMPONENT_NAME”.
2. When an infrastructure with unlinked components fails, the notification about each failed component is sent to recipients. If several components fail simultaneously, an individual notification is sent for each failed component.

Copyright © Acronis International GmbH, 2003-2019

There are four combinations for the settings described above:

1. Both options are enabled (a person is made responsible for one or several components, and Notify about all incidents is checked for the person).
2. The responsible person is assigned and **Notify about all incidents** is not checked.
3. The responsible person is not assigned and **Notify about all incidents** is checked.
4. None of the two options are enabled (no persons are assigned and **Notify about all incidents** is unchecked).

Outcomes for each of the four combinations:

1. The person will receive notifications for every problem on the component(s) they are responsible for. Additionally, they will receive notifications about all incidents. In the case of unlinked components, the total number of notifications is doubled and half of them are redundant.
2. The person will receive notifications for every problem on the component(s) they are responsible for.
3. The person will receive notifications about all incidents, the number of notifications depends on whether the components are linked or not.
4. No notifications are sent.

Thus, to optimize notifications flow and receive only important alerts, follow the steps below:

- Make logical component dependencies.
- Select the person who needs to be notified about incidents.
- Select the **Notify about all incidents** checkbox.
- DO NOT assign any personal responsibility for individual components.

It is possible to further fine-tune notifications about problem and incident severity, and how a person is notified.

10 Reports

Acronis Monitoring service generates reports on the status of servers in your environment, based on the criteria (threshold) specified in **Monitor Properties**.

Reports are useful when you need to pinpoint the source of a problem within your infrastructure. With a report, you can visually analyze how individual critical resources — such as memory, CPU, and disk resources — are consumed. You can schedule and email reports to the responsible people in your organization via daily, weekly, or monthly subscriptions.

How do I use the Reports page?

The **Reports** page displays a percentage for the OK status, error status, warning status, and the number of occurred problems for one or more components and monitors. This information is displayed in a tabular data format. Hence, you may find this report useful for quickly reviewing status availability metrics across all infrastructure resources.

Date range

Choose the time range for which you would like to see data. To do so, use the calendar on the left side panel.

Copyright © Acronis International GmbH, 2003-2019

Subscribing to reports

You can send up-to-date data about your infrastructure by creating a subscription for the responsible person. There are three types of the subscriptions: daily, weekly, or monthly. To subscribe, click Subscribe, choose the recipient, and choose the report delivery frequency.

11 Setting up monitors

11.1 Network protocols

11.1.1 Ping

The Ping Monitor allows you to test the accessibility of your web server over a IP/URL/domain name, via public and private agents.

Once you added a ping monitor for your component, the Acronis agent will start pinging your web server at your customized monitor periods to check if your URL, IP address, and domain name are accessible.

If the server fails to respond, or if it responds with an error or warning status indicating that the web service is not available, the Acronis monitoring service considers the test to have failed. Most often, a failure status is returned by your ping monitor if there is no response from the server within the set timeout.

Adding a Ping Monitor

There are two options for adding a Ping Monitor.

The first option is available if a component is created.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Go to the **Web-Servers Monitors** tab and **Web protocols** sub-tab view.
3. Select **Ping** and click **Next**.
4. Select the agents (servers) from the list.
5. Enter the **IP/domain name/URL** of the target web site, under **Host**.
6. Choose a period of time from the **Monitor Period** drop-down menu.
7. Click **Next**.
8. [Optional] Enable IPv6.
9. [Optional] Under **Timeout**, set the value for an **Error threshold** and **Warning threshold**.
10. Enter a **Monitor Name** and set consecutive measurements.
11. Click **Next**.
12. On the **Monitor test result** step, click **Next** when the test is passed.
13. Click **Finish**.

To manage your monitor, click **Edit**.

To add a Ping Monitor via the second option, follow the steps below:

1. From the **Infrastructure view** page, click **Add Component**.
2. Select **Server Component** and click **Next**.
3. Enter the **URL/domain name/IP address** of your target web site.

Copyright © Acronis International GmbH, 2003-2019

4. Select **Ping Monitor** and click **Next**.
5. [Optional] Enter a **Monitor Name**.
6. Click **Finish**.

11.1.2 HTTP

The HTTP Monitor allows you to test the availability and response time of your website, via public and private agents.

Once you add an HTTP monitor for your website, Acronis Agent will start sending out HTTP requests to your website to check if your website is accessible, according to the time intervals you specified.

Usually, a failure status is returned by your HTTP monitor if there is no response from the server within the specified time.

Adding an HTTP monitor

There are two options for adding an HTTP monitor.

The first option is available if the component is already created.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Web-Servers Monitors** tab and **Web protocols** sub tab view.
3. Select **HTTP** and click **Next**.
4. Select the agents (servers) from the list.
5. Enter the **IP** or **domain name** of the target web site, under **Host**.
6. Select a period of time from the **Monitor Period** drop-down menu.
7. [Optional] Select the type of **Security**.
8. Click **Next**.
9. Enter the **path URL**.
10. In **HTTP properties**, select the **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.
11. [Optional] Enter the **Port Number**.
12. [Optional] Change the default value under for **Monitor period**.
13. [Optional] Under **Timeout**, set the value for an **Error threshold** and W**arning threshold**.
14. Enter a **Monitor Name** and set consecutive measurements.
15. In **HTTP Status properties**, select **Matched** or **Not matched** under **Valid of**. By default, **Matched** is selected.
16. [Optional] Enter the pattern value under **Status pattern**.
17. [Optional] Enter an amount of redirection attempts, under **Redirection attempts**.
18. If your website uses basic authentication mechanism, you need to provide the user name and password for it, in order to enable monitor access to your web site. By default, this parameter is not selected.
19. In the **Content Matching properties**, select **Found in** or **Not found in** under **Body content**. By default, this parameter is not selected.
20. Click **Next**.
21. On the **Monitor test result** step, click **Next** when the test is passed.
22. Click **Finish**.

Copyright © Acronis International GmbH, 2003-2019

To manage your monitor, click **Edit**.

Adding an HTTPS Monitor

There are two options for adding an HTTPS Monitor.

The first option is available if a component is already created.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Web-Servers Monitors** tab and **Web protocols** sub tab view.
3. Select **HTTP/HTTPs** and click **Next**.
4. Select the agents (servers) from the list.
5. Enter the **IP** or **domain name** of the target web site, under **Host**.
6. Select a period of time from the **Monitor Period** drop-down menu.
7. Enable SSL/TLS security.
8. Click **Next**.
9. Enter the **path URL** (do not forget to use https).
10. In **HTTP Properties**, 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.
11. [Optional] Enter the **Port Number**.
12. [Optional] Select a specific protocol.
13. [Optional] Change the default value for **Monitor period**.
14. [Optional] Under **Timeout**, set the value for an **Error threshold** and **Warning threshold**.
15. Enter a **Monitor Name** and set consecutive measurements.
16. In **HTTP Status properties**, select **Matched** or **Not matched** under **Valid of**. By default, **Matched** is selected.
17. [Optional] Check the Certificate expiration box and set the value.
18. [Optional] Enter the pattern value under **Status pattern**.
19. [Optional] Enter an amount of redirection attempts, under **Redirection attempts**.
20. If your web site uses basic authentication mechanism, you need to provide the user name and password for it, in order to enable monitor access to your web site. By default, this parameter is not selected.
21. In the **Content Matching properties**, select **Found in** or **Not found in** under **Body content**. By default, this parameter is not selected.
22. Click **Next**.
23. On the **Monitor test result** step, click **Next** when the test is passed.
24. Click **Finish**.

To manage your monitor, click **Edit**.

To add an HTTP/HTTPs Monitor via the second option, follow the steps below:

1. From the **Infrastructure view** page, click **Add Component**.
2. Select the **Server Component** and click **Next**.
3. Enter the **URL/domain name/IP address** of your target web site.
4. Select **HTTP/HTTPs Monitor** and click **Next**.
5. [Optional] Enter a name under **Monitor Name**.

Copyright © Acronis International GmbH, 2003-2019

6. Click **Finish**.

Note: For an HTTPs monitor, use secure URLs (https://). If you want to use a complex URL, please use the first option listed (adding through the custom monitor).

11.1.3 TCP

A TCP Monitor allows you to test the availability and response time of your TCP server, via public and private agents.

Once you add a TCP monitor for your TCP server, Acronis Agent will start trying to connect to your web server according to the time intervals you specified, to check if your TCP server is accessible.

Adding a TCP monitor

Before proceeding, please ensure that you have created the component.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Web-Servers Monitors** tab and **Web protocols** sub tab view.
3. Select **TCP** and click **Next**.
4. Select the agents (servers) from the list.
5. Under **Host**, enter the **IP** or **domain name** of the target web site.
6. Select a period of time from the **Monitor Period** drop-down menu.
7. Click **Next**.
8. [Optional] Change the **Port Number**.
9. [Optional] Select SSL/TLS.
10. [Optional] Under **Timeout**, set the value for an **Error threshold** and **Warning threshold**.
11. Enter a **Monitor Name** and set consecutive measurements.
12. Click **Next**.
13. On the **Monitor test result** step, click **Next** when the test is passed.
14. Click **Finish**.

To manage your monitor, click **Edit**.

11.1.4 SSH

An SSH Monitor allows you to test the availability and response time of your designated SSH server, via public and private agents.

Once you add an SSH monitor for your SSH server, the Acronis agent will start trying to connect to your web server according to the time intervals you specified, to check if your SSH server is accessible.

Adding an SSH monitor

Before proceeding, please ensure that you have created the component.

1. On the **Component page**, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Web-Servers Monitors** tab and **Web protocols** sub tab view.
3. Select **SSH** and click **Next**.
4. Select the agents (servers) from the list.
5. Under **Host**, enter the **IP/domain name** of the target server.

Copyright © Acronis International GmbH, 2003-2019

6. Select a period of time from the **Monitor Period** drop-down menu.
7. Click **Next**.
8. [Optional] Change the **Port Number**.
9. [Optional] Under **Timeout**, set the value for an **Error threshold** and **Warning threshold**.
10. Enter a **Monitor Name** and set consecutive measurements.
11. Click **Next**.
12. On the **Monitor test result** step, click **Next** when the test is passed.
13. Click **Finish**.

To manage your monitor, click **Edit**.

11.1.5 FTP

An FTP Monitor allows you to test the availability and response time of your FTP server, via public and private agents.

Once you add an FTP monitor for your FTP server, Acronis Agent will start trying to connect to your FTP server according to the time intervals you specified, to check if your FTP server is accessible.

An FTP Monitor connects to the specified FTP port and waits for the server to respond with a standard "Service Ready for a new user" Code 220 message.

Adding an FTP monitor

Before proceeding, please ensure that you have created the component.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Web-Servers Monitors** tab and **Web protocols** sub tab view.
3. Select **FTP/FTPs** and click **Next**.
4. Select the agents (servers) from the list.
5. Under **Host**, enter an **IP/domain name** of the target FTP server.
6. Select a period of time from the **Monitor Period** drop-down menu.
7. If needed, select **security properties**.
8. Click **Next**.
9. [Optional] Change the **Port Number**.
10. [Optional] Select SSL/TLS.
11. [Optional] Under **Timeout**, set the value for an **Error threshold** and **Warning threshold**.
12. Enter a **Monitor Name** and set consecutive measurements.
13. Click **Next**.
14. On the **Monitor test result** step, click **Next** when the test is passed.
15. Click **Finish**.

To manage your monitor, click **Edit**.

11.1.6 SMTP

An SMTP Monitor allows you to test the availability and response time of your SMTP server by connecting to a designated SMTP port (optional: through the secure SSL/TLS connection), via public and private agents.

Copyright © Acronis International GmbH, 2003-2019

Once you add an SMTP monitor for your SMTP server, Acronis Agent will start trying to connect to your server according to the time intervals you specified, to check if your SMTP server is accessible.

Adding an SMTP monitor

Before proceeding, please ensure that you have created the component.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Web-Servers Monitors** tab and **Mail protocols** sub tab view.
3. Select **SMTP/SMTPs** and click **Next**.
4. Select the agents (servers) from the list.
5. Under **Host**, enter the **IP/domain name** of the target Mail/SMTP server.
6. Select a period of time from the **Monitor Period** drop-down menu.
7. If needed, select **security properties**.
8. Click **Next**.
9. [Optional] Change the **Port Number**.
10. [Optional] Select SSL/TLS.
11. [Optional] Under **Timeout**, set the value for an **Error threshold** and **Warning threshold**.
12. Enter a **Monitor Name** and set consecutive measurements.
13. Click **Next**.
14. On the **Monitor test result** step, click **Next** when the test is passed.
15. Click **Finish**.

To manage your monitor, click **Edit**.

To add an SMTP/SMTPs Monitor via the second option, follow the steps below:

1. From the **Infrastructure view** page, click **Add Component**.
2. Select the **Email Service component** and click **Next**.
3. Enter the **domain name** or **IP address** of your target web site.
4. Select **SMTP Monitor** and click **Next**.
5. [Optional] Enter a **Monitor Name**.
6. Click **Finish**.

11.1.7 IMAP

An IMAP Monitor allows you to test the availability and response time of your IMAP server by connecting to elected IMAP port (optional: through the secure SSL/TLS connection), via public and private agents.

Once you add an IMAP Monitor for your IMAP server, Acronis agent will start trying to connect to your server according to the time intervals you specified, to check if your IMAP server is accessible.

An IMAP Monitor connects to the specified IMAP port and waits for the server to respond. If the IMAP server fails to respond, or responds with an error code indicating that the service is not available, Acronis Agent considers the test to have failed.

Adding an IMAP Monitor

Before proceeding, please ensure that you have created the component.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.

Copyright © Acronis International GmbH, 2003-2019

2. Select the **Web-Servers Monitors** tab and **Mail protocols** sub tab view.
3. Select **IMAP/IMAPs** and click **Next**.
4. Select the agents (servers) from the list.
5. Under **Host**, enter the **IP** or **domain name** of the target web site.
6. Select a period of time from the **Monitor Period** drop-down menu.
7. If needed, select **security properties**.
8. Click **Next**.
9. [Optional] Change the **Port Number**.
10. [Optional] Select SSL/TLS.
11. [Optional] Under **Timeout**, set the value for an **Error threshold** and **Warning threshold**.
12. Enter a **Monitor Name** and set consecutive measurements.
13. Click **Next**.
14. On the **Monitor test result** step, click **Next** when the test is passed.
15. Click **Finish**.

To manage your monitor, click **Edit**.

To add an IMAP/IMAPs Monitor via the second option, follow the steps below:

1. From the **Infrastructure view** page, click **Add Component**.
2. Select the E**mail Service component** and click **Next**.
3. Enter the **domain name** or **IP address** of your target web site.
4. Select **IMAP Monitor** and click **Next**.
5. [Optional] Enter a **Monitor Name**.
6. Click **Finish**.

11.1.8 POP3

A POP3 Monitor allows you to test the availability and response time of your POP3 server by connecting to the elected POP3 port (optional: through the secure SSL/TLS connection), via public and private agents.

Once you add the POP3 monitor for your POP3 server, Acronis Agent will start trying to connect to your server according to the time intervals you specified, to check if your POP3 server is accessible.

Adding a POP3 Monitor

Before proceeding, please ensure that you have created the component.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Web-Servers Monitors** tab and **Mail protocols** sub tab view.
3. Select **POP3/POP3s** and click **Next**.
4. Select the agents (servers) from the list.
5. Under **Host**, enter the **IP** or **domain name** of the target web site.
6. Select a period of time from the **Monitor Period** drop-down menu.
7. If needed, select **security properties**.
8. Click **Next**.
9. [Optional] Change the **Port Numbe**r.
10. [Optional] Select SSL/TLS.

Copyright © Acronis International GmbH, 2003-2019

11. [Optional] Under **Timeout**, set the value for an **Error threshold** and **Warning threshold**.
12. Enter a **Monitor Name** and set consecutive measurements.
13. Click **Next**.
14. On the **Monitor test result** step, click **Next** when the test is passed.
15. Click **Finish**.

To manage your monitor, click **Edit**.

To add a POP3/POP3s Monitor via the second option, follow the steps below:

1. From the **Infrastructure view** page, click **Add Component**.
2. Select the **Email Service component** and click **Next**.
3. Enter the **domain name** or **IP address** for your target web site.
4. Select **POP3 Monitor** and click **Next**.
5. [Optional] Enter a **Monitor Name**.
6. Click **Finish**.

11.2 OS Performance

11.2.1 CPU usage

The CPU usage Monitor allows you to analyze the average and peak values to decide if you need to increase the number or speed of the CPUs on the server. Depending on your conditions, configuration, and requirements, the critical value of CPU usage, and if the period over which CPU usage is high, your values can vary. You have to exercise good judgement regarding these parameters, based on the monitored data, in order to ensure a high level of performance.

CPU usage is calculated over a sample period. For example, if a CPU usage of 70 percent is measured over two seconds, this can really mean that the CPU was 100 percent busy for one second, and then 30 percent busy for another second. Such short bursts of activity with a 100 percent usage are not critical, because the queue is freed up quickly, but longer periods of high CPU usage can indicate a possible problem. To understand if peaks of CPU activity are causing issues, you can use the CPU load monitor that shows how many processes are waiting in the queue for execution.

Note: For all types of local resource monitors, you must have the Acronis private agent downloaded, installed, and running on your machine to configure the monitoring.

Adding a CPU usage Monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”).

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources Monitors** tab and **Hardware** sub tab view.
3. Select **CPU usage** and click **Next**.
4. Select a period of time from the **Monitor Period** drop-down menu.
5. Select the agents (servers) from the list.
6. Click **Next**.
7. Set the appropriate error value for the CPU usage threshold.
8. Enter a **Monitor Name** and set consecutive measurements.
9. Click **Next**.

 Copyright © Acronis International GmbH, 2003-2019

10. On the **Monitor test result** step, click **Next** when the test is passed.
11. Click **Finish**.

To manage your monitor, click **Edit**.

To add a CPU usage Monitor via the second option, follow the steps below:

1. From the **Infrastructure** page, click **Add Component**.
2. Select the server component and click **Next**.
3. Select the agent (server) from the list and click **Next**.
4. Click **Finish**.
5. On the **Manage Component Monitors** page, select the **CPU usage** slider.
6. [Optional] Change the **monitor Name**.
7. [Optional] Change the default value for **refreshing intervals** (min.).
8. Enter the appropriate threshold values, under **Warning** and **Error**.
9. Go to **Monitor Status Change Rule** and specify the number of consecutive measurement
10. Click **OK**.

To manage your monitor, go to the **Monitor Manager** and click on the slider to deactivate the monitor.

11.2.2 CPU load

The CPU load Monitor allows you to analyze the workloads performed by your server and understand what can be done. As a general rule, you want the CPU usage to be as high as possible (for maximum efficiency), but keep the CPU load below one (for minimum delays). This requires analysis of the average and peak values for CPU usage and the CPU load. You have to arrive at a sound judgement of these measurements based on the monitoring data, in order to ensure a high level of performance.

In most cases, while CPU usage is below 100 percent for a certain period, the CPU load will remain less than one for that period, because idle time means that there are no processes waiting in the queue. However, on Linux, processes waiting for disk activity are also included in the system load measurement. In this case, when the processor is not calculating anything, processes can still remain queued while write or read operations are performed. This can be misleading and you have to be aware that on Linux, there can be a long queue of processes, even if CPU usage remains below 100 percent most of the time.

If a client requests your server to be placed in the queue, this will lead to increased response times, which may be critical to your business. As previously noted, in case of a Linux server, if it performs a large number of I/O operations in a distant part of the world with high latency, this can create a queue for other operations that do not require a long time to be executed by the CPU, but are forced to wait, thus leading to severe performance issues. This can be a sign that you need to divide the different types of workloads between different servers.

Note: For all types of local resources monitors, you need to have the Acronis private agent downloaded, installed, and running on your machine, in order to configure monitoring.

Adding a CPU load Monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”).

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.

 Copyright © Acronis International GmbH, 2003-2019

2. Select the **Local Resources Monitors** tab and **Hardware** sub tab view.
3. Select **CPU load** and click **Next**.
4. Select a period of time from the **Monitor Period** drop-down menu.
5. Select the agents (servers) from the list.
6. Click **Next**.
7. Under **CPU load threshold**, set the appropriate values for an **Error threshold** and **Warning threshold**.
8. Enter a **Monitor Name** and set consecutive measurements.
9. Click **Next**.
10. On the **Monitor test result** step, click **Next** when the test is passed.
11. Click **Finish**.

To manage your monitor, click **Edit**.

To add a CPU load monitor via the second option, follow the steps below:

1. From the **Infrastructure view** page, click **Add Component**.
2. Select the Server component and click **Next**.
3. Select the agent (server) from the list and click **Next**.
4. Click **Finish**.
5. On the **Manage Component Monitors** page, select the **CPU load** slider.
6. [Optional] Change the **monitor Name**.
7. [Optional] Change the default value for refreshing intervals (min).
8. Enter the appropriate threshold values, under **Warning** and **Error**.
9. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
10. Click **OK**.

To manage your monitor, go to the **Monitor Manager** and click on the slider to deactivate the monitor.

11.2.3 Free physical memory

The free physical memory Monitor allows you to identify a memory leak early by establishing a threshold and properly reacting to any problems before a crash occurs.

Running out of free physical memory is a reason for server performance degradation. Some systems use secondary storage as virtual memory, moving the least-used data from the physical memory and retrieving it back when it is required. Besides the fact that secondary storage is much slower, such swapping leads to file system fragmentation, which contributes to an even greater decrease in server performance.

When there is little RAM left, you may want to consider optimizing the way physical memory is used by the OS and other software. If you are not able to reduce the amount of used physical memory, then you should add more RAM to the server.

A memory leak is a common problem for server software. It usually happens due to poor design, when an application does not properly discard unused objects from the main memory. The amount of memory constantly increases until there is no memory left for new objects, and then the application crashes.

Copyright © Acronis International GmbH, 2003-2019

Note: For all types of local resources monitors, you need to have Acronis Private Agent downloaded, installed, and running on your machine, in order to configure the monitoring.

Adding a free physical memory monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows or Linux is running.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources monitors** tab and **Hardware** sub tab view.
3. Select **Free physical memory Monitor** and click **Next**.
4. Select a period of time from the **Monitor Period** drop-down menu.
5. Select the agents (servers) from the list.
6. Click **Next**.
7. Under **Free host memory threshold**, set the appropriate values for an **Error threshold** and **Warning threshold**.
8. Enter a **Monitor Name** and set consecutive measurements.
9. Click **Next**.
10. On the **Monitor test result** step, click **Next** when the test is passed.
11. Click **Finish**.

To manage your monitor, click **Edit**.

11.2.4 Free disk space

The free disk space Monitor allows you to set disk space thresholds so that you are alerted if your machine's disk space utilization reaches the warning or error level that you specified. The free disk space monitor uses local communication to test the amount of space available.

Disk space is the amount of secondary storage (also known as auxiliary memory), which is not directly accessible by the CPU. It uses I/O channels to transfer necessary data to primary storage (physical memory) that the CPU can then access directly. Accessing data on a secondary storage device is slower, but it is also less expensive and provides more storage space than physical memory. Secondary storage is also non-volatile, meaning that data is stored even without power. The most commonly used secondary storage devices are hard disk drives and flash memory devices.

Faulty applications may consume all free disk space when they hang or crash. Certain viruses, Trojans, and network attacks are based on draining the storage space. Running out of free disk space can disrupt processes that write data to secondary storage. These processes may include logging, maintaining a database, and installing updates. Some of these processes may be critical to the operation of your business.

Low free disk space can also lead to file system fragmentation. This causes performance issues when pieces of data need to be read from different parts of the disk.

Some systems use secondary storage as virtual memory, moving the least-used data from the physical memory and retrieving it back when it is required. On such systems, running out of free disk space can lead to performance degradation similar to running out of free physical memory.

Adding a free disk space monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see "About Acronis agents (p. 13)").

 Copyright © Acronis International GmbH, 2003-2019

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources Monitors** tab and the **Hardware** sub tab view.
3. Select **Free disk space** Monitor and click **Next**.
4. Select a period of time from the **Monitor Period** drop-down menu.
5. Select the agents (servers) from the list.
6. Click **Next**.
7. Choose the **Drive / Mount** point from the list.
8. Under **free disk space threshold**, set the appropriate values for an **Error threshold** and **Warning threshold**.
9. Enter a **Monitor Name** and set consecutive measurements.
10. Click **Next**.
11. On the **Monitor test result step**, click **Next** when the test is passed.
12. Click **Finish**.

To manage your monitor, click **Edit**.

To add a free disk space monitor via the second option, follow the steps below:

1. From the **Infrastructure view** page, click **Add Component**.
2. Select the Server component and click **Next**.
3. Select the agent (server) from the list and click **Next**.
4. Click **Finish**.
5. On the **Manage Component Monitors** page, select the **free disk space** slider.
6. [Optional] Change the monitor **Name**.
7. [Optional] Change the default value for refreshing intervals (min).
8. Enter the appropriate threshold values, under **Warning** and **Error**.
9. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
10. Click **OK**.

To manage your monitor, go to the **Monitor Manager** and click on the slider to deactivate the monitor.

11.2.5 Disk usage

The disk usage Monitor allows you to identify when the workload of the server becomes too intensive for the current disk I/O capabilities. This is a critical issue for database management systems, that use MySQL. Response times of a MySQL server can decrease greatly if disk I/O becomes a bottleneck. You must ensure that data is distributed over multiple disks in such a way that their usage is low and can handle sudden bursts of activity. You can also configure disk striping, which divides data into blocks and automatically spreads those blocks over multiple disks.

Adding a disk usage monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”).

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources Monitors** tab and **Hardware** sub tab view.
3. Select **Disk Usage** Monitor and click **Next**.

 Copyright © Acronis International GmbH, 2003-2019

4. Select a period of time from the **Monitor Period** drop-down menu.
5. Select the agents (servers) from the list.
6. Click **Next**.
7. Choose the **Drive / Mount** point from the list.
8. Under the **host disk usage threshold**, set the appropriate values for an **Error threshold** and **Warning threshold**.
9. Enter a **Monitor Name** and set consecutive measurements.
10. Click **Next**.
11. On the **Monitor test result** step, click **Next** when the test is passed.
12. Click **Finish**.

To manage your monitor, click **Edit**.

To add a disk usage monitor via the second option, follow the steps below:

1. From the **Infrastructure view** page, click **Add Componen**t.
2. Select the Server component and click **Next**.
3. Select the agent (server) from the list and click **Next**.
4. Click **Finish**.
5. On **Manage Component Monitors** page select **Disk usage** slider.
6. [Optional] Change the monitor **Name**.
7. [Optional] Change the default value for refreshing intervals (min).
8. Enter the appropriate threshold values, under **Warning** and **Error**.
9. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
10. Click **OK**.

To manage your monitor, go to the **Monitor Manager** and click on the slider to deactivate the monitor.

11.2.6 S.M.A.R.T. drive

A S.M.A.R.T. drive Monitor allows you to be alerted if your machine's S.M.A.R.T. status reaches the warning or error level preset by the manufacturer of your hard drive.

Note: For all types of local resource monitors, you must have the Acronis Private Agent downloaded, installed, and running on your machine to configure the monitoring. The S.M.A.R.T. drive Monitor is unavailable for virtual machines.

Adding a S.M.A.R.T. drive Monitor

Before proceeding, please ensure that you have created the component, Acronis Private Agent for Windows/Linux is running and installed on physical machine (server) (see "About Acronis agents (p. 13)").

1. On the **Windows/Linux Server** component page, activate the **S.M.A.R.T. drive** slider.
2. In the **Monitor Wizard**, enter a name and set consecutive measurements under **Name**.
3. Select the notifications that you would like to receive.
4. Click **OK**.

To manage your monitor, click **Edit**.

 Copyright © Acronis International GmbH, 2003-2019

11.2.7 Full page load

The full page load Monitor allows you to see how long does it take to load a full HTML page in the browser. By tracking the performance of individual web page components such as CSS and JavaScript, the monitor measures your web visitor's user experience and satisfaction level.

Adding a full page load monitor

Before proceeding, please ensure that you have created the component.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Web-server monitors** tab and **Web protocols** sub tab view.
3. Select **Full page** and click **Next**.
4. Select the agents from the list.
5. Under **Host**, enter the **IP address/domain name** of the target web site.
6. Click **Next**.
7. [Optional] Enter the **Port Number**.
8. Select the protocol from the drop-down menu.
9. Enter the **Path** for the web page.
10. [Optional] In the **Timeouts properties**, enter **Error threshold** (ms).
11. In **HTTP Status properties**, select **Matched** or **Not matched** under **Valid of**. By default, **Matched** is selected.
12. [Optional] Enter the pattern value under **Status pattern**.
13. In the **Content Matching properties**, select **Found in** or **Not found in** under **Body content**. By default, this parameter is not selected.
14. Click **Finish**.

To manage your monitor, click **Edit**.

Note: The Path attribute is not case-sensitive. For example, for the URL:

http://www.rbc.ru/politics/18/03/2016/

the path is:

politics/18/03/2016/.

11.2.8 Custom shell command

A custom shell command allows you to execute a command to implement any custom checks and receive verified output.

It is configured with an arbitrary Linux or Windows shell commands, which is then executed by private agent, deployed on a selected server. Command output is collected and uploaded to Acronis backend for interpretation. Instead of a shell command there may be a script, a PowerShell command or script, or an executable being used. You are able to specify criteria for "success" and "failure", and as the command is being repeatedly launched you will be promptly alerted if something goes wrong.

There are two ways to check the output of the command execution. First, treat it as a number ("a measurement"). In this case the Acronis monitoring service will graph this value and check if it stays inside user-defined bounds. Another option is to treat the output as a text and check if there is a certain word, such as "OK" or "Error" present (or missing).

Copyright © Acronis International GmbH, 2003-2019

Custom diagnostics

In case a failure is detected, each monitor gathers additional information to provide problem context for faster troubleshooting. With Custom Shell Command Monitor a user possesses flexibility to set custom diagnostic actions to be executed.

This is achieved simply by collecting all the information sent by the command to the standard error stream (stderr) and attaching it to failed checks. So while standard output (stdout) is used to define success or failure (treating it either as a text or a number), stderr is used as a container for extra diagnostically data. Several examples are given below.

Examples

Let's use well-known Linux commands to build some examples of how Custom Shell Command Monitor can be used.

Are you renting a virtual machine? Then you probably wonder if you get the processing power you pay for and if your VM is not occasionally migrated to a weaker machine. So, for example you may measure the time it takes to calculate pi with high precision using the following command:

```
/usr/bin/time -f "%U" 2>&1 bash -c 'echo "scale=2000; a(1)*4" | bc -l >
/dev/null'
```

To count the number of processes under the "user" account, and also collect and store the list of those processes for you run the following command:

```
ps -U user -u user uf | tee /dev/stderr | wc -l
```

To spot and troubleshoot IO problems you may want to watch the time processes that are blocked on IO, using iostat tool:

```
(iostat -c 10 2 | tail -2 | head -n 1 | gawk '{print $4}' ; ps auxf |  grep
"D[^[]" >/dev/stderr; exit 0)
```

Custom monitoring configured with this command will report the percentage of time presented by iowait utility. Where the time goes above the threshold, the list of processes in uninterruptible sleep state ("D" state in ps output) will be collected and stored.

You may also plug in your favorite Nagios plugin, like in the following example, which will trigger alerts if there are less than 10 days left until domain expiration:

```
./check_domain –d somedomainname –c 10
```

For this command you will need to configure the monitor to treat the command output as a string and to look for an "OK" word.

Adding a custom shell command monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see "About Acronis agents (p. 13)").

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the L**ocal Resources monitors** tab and **Software** sub tab view.
3. Select **Shell Command** and click **Next**.
4. Select the agents from the list.
5. Type command under **Command** and click **Execute**.
6. Select **Check type**.

 Copyright © Acronis International GmbH, 2003-2019

7. Specify the interval type.
8. Enter the range checks.
9. Click **Next**.
10. Click **Finish**.

To manage your monitor, click **Edit**.

11.3 Networks

11.3.1 SNMP device

A Simple Network Monitoring Protocol (SNMP) is the protocol that allows you to check network-attached devices, such as routers and switches, for reachability and the returned value.

Adding an SNMP device Monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”).

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources Monitors** tab and **Hardware** sub tab view.
3. Select SNMP device and click **Next**.
4. Select a period of time from the **Monitor Period** drop-down menu.
5. Select the agents (servers) from the list.
6. Click **Next**.
7. Under **SNMP get properties**, select the SNMP version.
8. Set the response timeout.
9. Set the number of retries for connecting to the server.
10. Under **SNMP device details**, enter the **host IP** under **Hostname**.
11. Enter the **Community name**.
12. Enter the object identifier under **Object ID**.
13. [Optional] Set the minimum and maximum values for the monitored SNMP object under **Valid values intervals**.
14. Enter a **Monitor Name** and set consecutive measurements.
15. Click **Next**.
16. On the **Monitor test result** step, click **Next** when the test is passed.
17. Click **Finish**.

To manage your monitor, click **Edit**.

11.3.2 Printers

A Printers Monitor allows you to set supply thresholds so that you are alerted when your printer device reaches the warning or error level you designated and to check the reachability of the printers.

Adding a Printer Monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents” (p. 13)).

 Copyright © Acronis International GmbH, 2003-2019

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor.**
2. Select the **Local Resources Monitor**s tab and **Hardware** sub tab view.
3. Select **Printers** and click **Next**.
4. Enter the **IP address** of your network printer under **IP address**.
5. Enter the **SNMP Community name**.
6. Select **SNMP version**.
7. Select an agent (server) from the list.
8. Click **Next**.
9. Set **Monitor period**.
10. Enter the **Monitor Name** and set the consecutive measurements.
11. Select the supply level, to be alerted if your printer reaches a warning or error level.
12. [Optional] Select the check box **Get printer status warnings**.
13. [Optional] Select the check box **Get printer status errors**.
14. Click **Next**.
15. On the **Monitor test result** step, click **Next** when the test is passed.
16. Click **Finish**.

To manage your monitor, click **Edit**.

11.3.3 Network channel quality

A network channel quality Monitor allows you to check the network performance between two machines.

Note: For all types of local resources monitors, you must have the Acronis private agent downloaded, installed, and running on your machine (both sender and receiver) to configure the monitor.

Adding a network channel quality monitor

In Windows:

1. Install Acronis Agent (see “About Acronis agents (p. 13)”).
2. Install WinPcap.
3. http://www.winpcap.org/install/default.htm
4. Open port 8099.
5. Run the following script:

```
<installation_path>\Acronis Monitoring>agent-config.exe -p --enable_ipsla=true
```

   Here, <installation_path> is the agent installation path. By default, it is %ProgramFiles%\Acronis in 32-bit Windows and %ProgramFiles(x86)%\Acronis in 64-bit Windows.

6. Restart Acronis Monitoring Agent service.

Note: If an Acronis agent is already installed, you still need to restart the Acronis Agent service after installing WinPcap.

In Linux:

1. Install Acronis Agent (see “About Acronis agents (p. 13)”).
2. Open port 8099.
3. Run the following script:

Copyright © Acronis International GmbH, 2003-2019

```
/opt/acronis/bin/agent-config -p --enable_ipsla=true
```

4. Restart acronis-monitoring-agent service .

When both agents (on the sender and receiver machines) are installed, follow the steps below.

1. On the **Component** page, click **Add Component**.
2. In the **Component wizard**, select **Network channel quality**.
3. Select the sender and receiver.
4. Enter a **Name**.
5. If more than one monitor is needed, click **+**.
6. Click **Next**.
7. [Optional] Change the default value for refreshing intervals (min).
8. Set the thresholds for receiving an error or warning if these values are exceeded.
9. Set the packet count per test.
10. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
11. Click **Add**.

To manage your monitor, click **Edit**.

Note: For best network channel quality, you must sync the NTP server on both machines. It is needed to decrease false delays between machines.

11.3.4 Network interface

A network interface allows you to monitor the network channel on your server so that you are alerted if your machine's network channel reaches the warning or error level that you specified.

Adding a network interface monitor

Before proceeding, please ensure that your Acronis Private Agent for Windows/Linux is running (see "About Acronis agents (p. 13)").

Select the Network slider if you need to monitor the network channel on your server. In the Parameters window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. Enter the **Error threshold** and/or **Discards** values (packages per min), to create a notification for when a threshold exceeded.
4. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
5. To manage your monitor, go to the **Monitor Manager** and click on the slider to deactivate the monitor.

Copyright © Acronis International GmbH, 2003-2019

11.4 Software and applications

11.4.1 MySQL database

The MySQL database Monitor allows you to not miss abnormal and hazardous conditions in your MySQL server. Moreover, it will help you troubleshoot many application problems rooted in the any misconfigurations of the database.

We pre-selected the most important metrics out of several hundred available in MySQL database. Our goal was to retrieve vital actionable information, avoiding any overwhelming complexity of MySQL tuning.

Adding a MySQL database monitor

Before proceeding, please ensure that your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”).

There are two options of adding MySQL database monitor.

The first option available if you already created a component.

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor.**
2. Select the **Local Resources Monitors** tab and **Software** sub tab view.
3. Select **MySQL Database** and click **Next**.
4. Select agents (servers) from the list and click **Next**.
5. Enter authorization details to **MySQL DB**, and then click **Next**.
6. Select **MySQL Metrics** and set thresholds.
7. Enter a **Monitor Name** and set consecutive measurements.
8. Click **Next**.
9. On the **Monitor test result** step, click **Next** when the test is passed.
10. Click **Finish**.

To manage your monitor, click **Edit**.

To add a MySQL database monitor via the second option, follow the steps below.

1. From the **Infrastructure view** page, click **Add Component**.
2. Select the Server component and click **Next**.
3. Enter the **MySQL DB** authorization details and click **Next**.
4. Select **MySQL Metrics** and set the thresholds.
5. Click **Next**.
6. [Optional] Enter a **Monitor Name**.
7. Click **Finish**.

Metrics

Metric name	Description
Slow queries rate (%)	Ratio of queries exceeding configurable long_query_time limit
Slow threads rate (%)	Ratio of current slow running thread connection
Heavy join rate (%)	Ratio of heavy join

Copyright © Acronis International GmbH, 2003-2019

Metric name	Description
Table lock contention (%)	Ratio of table locked contention
On-disk temporary table rate (%)	Ratio of writing on disk temporary table
On-disk binary log rate (%)	Ratio of writing on disk binary log
Key cache miss rate (%)	Ratio of missing key cache
Query cache miss rate (%)	Ratio of missed cache
QUery cache prunes rate (%)	Ratio of cut cache
Innodb buffer pool miss rate (%)	Ratio of missed to total pages in the buffer pool
Innodb buffer pool wait rate (%)	Ratio of waiting pages in the buffer pool
Innodb log cache wait rate (%)	Ratio of waiting log cache
Thread cache miss rate (%)	Ratio of missed connection cache
Innodb buffer pool usage (%)	Ratio of used to total pages in the buffer pool
Connections usage (%)	Ratio of used connections

11.4.2 Apache web server

An Apache web server Monitor allows you to monitor key Apache performance metrics such as processes, workers who are busy or idle, and traffic. By setting metrics thresholds, you will receive alerts if any Apache web server monitor metrics (parameters) reaches a warning or error level that you specified.

Adding an Apache web server monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”).

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources Monitors** tab and **Software** sub tab view.
3. Select **Apache Web Server** and click **Next**.
4. Select a server from the list and click **Next**.
5. Under **Apache Statistics web page URL** enter **URL address** to server with configured mod_status (see Apache module (mod_status)).
6. Select **Apache Server Metrics** and set the threshold for selected metrics.
7. Enter a **Monitor Name** and set consecutive measurements.
8. Click **Next**.
9. On the **Monitor test result** step, click **Next** when the test is passed.
10. Click **Finish**.

To manage your monitor, click **Edit**.

To add an Apache web server monitor via the second option, follow the steps below:

 Copyright © Acronis International GmbH, 2003-2019

1. From the **Infrastructure view** page, click **Add Component**.
2. Select the **Apache** component and click **Next**.
3. Select the agent (server) from the list and click **Next**.
4. [Optional] Select **Apache statistics** monitor.
5. Click **Next**.
6. [Optional] Enter a **Monitor Name**.
7. Click **Finish**.

Apache module (mod_status)

There is an Apache module (mod_status) responsible for presenting the current view of Apache key parameters. To configure the mod_status parameter, follow the steps below.

For Apache version 2.3 or earlier:

1. Open the httpd.conf file.
2. Uncomment the following lines:

```
<Location /server-status>
   SetHandler server-status
   Order deny,allow
   Deny from all
   Allow from 127.0.0.1
</Location>
```

3. Save httpd.conf.

For Apache version 2.4 version or later, follow the steps below.

1. Open the httpd.conf file.
2. Add the following lines of code:

```
<Location /server-status>
    SetHandler server-status
    Require ip 127.0.0.1
</Location>
```

3. Save httpd.conf.

Metrics

Metric name	Description
Number of Busy Workers (workers)	The number of workers that are currently busy serving requests
Number of idle Workers (workers)	The number of workers that are currently idle serving requests
Average number of requests per second (requests)	The Average number of requests
Average number of Kbytes served per second (Kb/request)	The Average number of Kbytes served

Copyright © Acronis International GmbH, 2003-2019

Metric name	Description
CPU usage by all Apache workers (%)	Ratio of used CPU by all workers
Average number of Kbytes per request (Kb/request)	The Average number of Kbytes

11.4.3 Log file

The log file Monitor allows you to monitor any type of log files (.txt) generated by your machine's operating system. By configuring the log file monitor, you can receive the following outputs:

- Number of lines processed
- Number of regular expression matches found in the processed lines

Adding a log file monitor

Before proceeding, please ensure that you have created the component and that your Acronis private agent for Windows/Linux is running (see "About Acronis agents (p. 13)").

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources Monitors** tab and **Software** sub tab view.
3. Select **Log File** and click **Next**.
4. Select a server from the list and click **Next**.
5. Enter the **Log file path**.
6. Under **Count Expression** enter the string or regular expression to look it up.
7. Enter the **Expression Syntax**, if needed.
8. Select **Rolling file** if you want to read the file from the last marked string.
9. Select **Read Whole file** if you want to read the log file from the beginning.
10. [Optional] Select the **Valid amount of found expression attribute**; choose the interval type and set the values for the chosen interval.
11. [Optional] Select the **Look for marker attribute** and enter the expression under **Expression**; select **Found in** or **Not found in** under **Expected** and choose the expression syntax from the drop-down menu.
12. Enter a **Monitor Name** and set consecutive measurements.
13. Click **Next**.
14. On the **Monitor test result** step, click **Next** when the test is passed.
15. Click **Finish**.

To manage your monitor, click **Edit**.

11.4.4 Swap usage

The swap usage Monitor allows you setting to set swap usage thresholds so that you are alerted if your machine's swap (OS) utilization reaches the warning or error level that you specified. The swap usage monitor uses local communication to test the amount of processor capacity.

Note: For all types of local resources monitors, you must have the Acronis private agent downloaded, installed, and running on your machine to configure the monitor.

Adding a swap usage monitor

Copyright © Acronis International GmbH, 2003-2019

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”).

1. On the **Component** page, click **Manage Monitors**.
2. Click **Add Custom Monitor** (“**+**”).
3. Select the **Local Resources Monitors** tab and **Software** sub tab view.
4. Select **Swap usage** and click **Next**.
5. Select the server from the list and click **Next**.
6. Select a **Value for chart** type.
7. **Check swap usage** is selected by default.
8. [Optional] Enter **Error threshold (%)** to receive an error if your swap capacity will exceed this amount of usage and enter the threshold value under the **Warning threshold**.
9. **Check swap-out rate** is selected by default.
10. [Optional] Enter **Error threshold (%)** to receive an error if your swap-out rate exceeds this usage and/or enter the threshold value under the **Warning threshold**.
11. Enter a **Monitor Name** and set consecutive measurements.
12. Click **Next**.
13. On the **Monitor test result** step, click **Next** when the test is passed.
14. Click **Finish**.

To manage your monitor, click **Edit**.

11.4.5 Local processes

The local processes Monitor allows you to check local processes on the server.

Adding a local processes monitor

Before proceeding, please ensure that you have created the component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”).

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources monitors** tab and **Software** sub tab view.
3. Select **Local Processes** and click **Next**.
4. Select the agents from the list.
5. Set **Monitor period** and click **Next**.
6. Under **Process name**, type any process which runs and is listed in the table or use an asterisk (*) to monitor all running processes.
7. Under **Command name**, type any process command name which runs and is listed in the table or use an asterisk (*) to monitor all running processes.
8. Define the value for chart metrics.
9. [Optional] Select the check box **Check the number of matching processes** and enter a number.
10. [Optional] Select **Check the aggregate CPU usage for the selected processes** and enter **Error level (%)** to receive an error if your CPU usage will exceed this amount of usage and/or enter the threshold value under the **Warning level**.
11. [Optional] Select **Check the aggregate memory consumption for the selected processes** and enter **Error level (mb)** to receive an error if your memory usage exceeds this amount of usage and/or enter the threshold value under the **Warning level**.

Copyright © Acronis International GmbH, 2003-2019

12. Enter a **Monitor Name** and set consecutive measurements.
13. Click **Next**.
14. On the **Monitor test result** step, click **Next** when the test is passed.
15. Click **Finish**.

To manage your monitor, click **Edit**.

Note: The asterisk (*) is a wildcard character that can be used as a substitute for zero or more characters in a process name. For example, using "" matches all running processes.*

11.4.6 Linux services

The Linux services Monitor allows you to checks the status of Linux services running on your machine.

Adding a Linux service monitor

Before proceeding, please ensure that you have created the Linux server component and your Acronis Private Agent for Windows/Linux is running (see "About Acronis agents (p. 13)").

Select the **Services** slider if you need to monitor the Linux services on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. Select services that you want to monitor.
4. Click **OK**.

11.4.7 JVM

The JVM Monitor allows you to monitor total memory usage, heap, non-heap, and pool memory usages, threads and classes of JVMs, to ensure the best performance.

You can monitor all of your Java applications in one web-console, set up warning and error thresholds for each parameter and get actionable alerts in case of problems.

Adding a JVM monitor

Before proceeding, please ensure that you have created the Linux server component and your Acronis private agent for Windows/Linux is running (see "About Acronis agents (p. 13)").

1. On the **Component** page, click **Manage Monitors > Add Custom Monitor**.
2. Select the **Local Resources monitors** tab and **Software** sub tab view.
3. Select **JVM** and click **Next**.
4. Select the agents from the list.
5. Set the **Monitor Period** and click **Next**.
6. Set the **JVM connection**, enter the **Port Number**, and enter the **URL** under **Host**.
7. Select **Enable password authorization**, if needed, otherwise use the instructions to configure monitoring without authorization. Enter user details under **Password** and **Username**.
8. Click **Query** if you want to check the connection and look at the current JVM metrics.
9. Select the expression which will be represented in the **Monitor graph**.

Copyright © Acronis International GmbH, 2003-2019

10. Select metrics and enter for the **Error level (Mb)** to receive an error if your JVM usage exceeds this amount of usage and/or enter the threshold value under the **Warning level**.
11. Enter a **Monitor Name** and set consecutive measurements.
12. Click **Next**.
13. On the **Monitor test result** step, click **Next** when the test is passed.
14. Click **Finish**.

To enable monitoring without authorization, follow the instruction below.

Configure your Java service to start with the following VM parameters:

```
-Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=SELECTED_PORT
-Dcom.sun.management.jmxremote.local.only=false
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
```

The description of how to configure JVM monitor with authentication is given in JVM (with authentication) (p. 49) section.

Note: You should use your port number instead of 'SELECTED_PORT' (see the example below).

Example:

java -Dcom.sun.management.jmxremote \

-Dcom.sun.management.jmxremote.port=9010 \

-Dcom.sun.management.jmxremote.local.only=false \

-Dcom.sun.management.jmxremote.authenticate=false \

-Dcom.sun.management.jmxremote.ssl=false \

-jar tomcat.jar

Metrics

Metric name	Description
Total memory usage (MB)	Total number of used memory
Heap memory usage (MB)	Shows the amount of heap space used by the JVM
Non-Heap memory usage (MB)	Shows the amount of non-heap space used by the JVM
Total pool memory usage (MB)	Total number of pool used memory
Threads (threads)	The number of threads
Classes (classes)	The number of classes

11.4.8 JVM (with authentication)

In JVM Monitor (p. 48) section, we discussed what is JVM Monitor and how it could be added.

Copyright © Acronis International GmbH, 2003-2019

In this section, you will be able to configure JVM monitor with authentication. To do so, please follow the steps below.

Using Password and Access Files

The password and access files control security for monitoring. To be functional, a user must have an entry in both the password and the access files.

Password File

The password file defines different users and their passwords.

Create the password file (for example 'jmxremote.password') in a secure folder using the following template:

```
# The "monitorUser" user has password "QED".

monitorUser QED
```

The password file should be owned by the user who runs Java service and should have only reading permissions.

How to create the password file

On Linux systems:

start Terminal with the root rights

create a folder

create a file in an editor

change the file owner to the user which runs Java service by executing:

```
chown xxx jmxremote.password (where xxx is the user name)
```

set permissions for the password file by executing:

```
chmod 600 jmxremote.password
```

On Windows systems:

start windows session as administrator

create a folder in the root folder

create a file in an editor

set permissions for the password file by executing:

```
cacls jmxremote.password /G xxx:R (where xxx is the user name)
```

Access file

The access file defines users and their access levels. Note that it should be placed into the same folder where the password file is.

Create the access file (for example 'jmxremote.access') using the following template:

```
 # The "monitorUser" user has readonly access.

monitorUser readonly
```

The access file should be owned by the user who runs Java service and should have only reading permissions.

 Copyright © Acronis International GmbH, 2003-2019

How to create the access file

On Linux systems:

start Terminal with the root rights

create a folder

create a file in an editor using the template above

change the file owner to the user which runs Java service by executing:

```
chown xxx jmxremote.access (where xxx is the user name)
```

set permissions for the access file by executing:

```
chmod 600 jmxremote.access
```

On Windows systems:

start windows session as administrator

create a folder in the root folder

create a file in an editor using the template above

set permissions for the access file by executing:

```
cacls jmxremote.access /G xxx:R (where xxx is the user name)
```

Java service configuration

Configure your service to start with the following VM parameters:

```
-Dcom.sun.management.jmxremote.port=SELECTED_PORT
-Dcom.sun.management.jmxremote.local.only=false
-Dcom.sun.management.jmxremote.password.file=jmxremote.password
-Dcom.sun.management.jmxremote.access.file=jmxremote.access
-Dcom.sun.management.jmxremote.ssl=false
```

Note that you should use your port number instead of 'SELECTED_PORT' (see the example below).

Example:

```
java -Dcom.sun.management.jmxremote.port=9010 \
    -Dcom.sun.management.jmxremote.local.only=false \
    -Dcom.sun.management.jmxremote.password.file=jmxremote.password \
    -Dcom.sun.management.jmxremote.access.file=jmxremote.access \
    -Dcom.sun.management.jmxremote.ssl=false \
    -jar tomcat.jar
```

11.4.9 Active Directory

Before proceeding, please ensure that you have created the Active Directory component and your Acronis Private Agent for Windows is running (see "About Acronis agents (p. 13)").

 Copyright © Acronis International GmbH, 2003-2019

Select the AD monitor type slider, which you want to monitor. On the dialog box depending on chosen monitor set the following properties.

1. Enter a **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. [Optional] Enter an **Error threshold value (%)** under **Threshold**, if it exists, to receive an error if AD exceeds this amount of usage and/or enter the threshold value under the **Warning threshold**.
4. Enter the threshold value for receiving an error, under **Performance counter**.
5. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
6. Click **OK**.

To manage your monitor, go to the **Monitor Manager** and click on the slider to deactivate the monitor.

Metrics

Metric name	Description
Server sessions	The number of server sessions
LSASS CPU usage	The CPU usage by LSASS
LDAP Client Sessions	The number of sessions of connected LDAP clients
LDAP Searches	The number of search operations per second performed by LDAP clients
NTLM Authentications/sec	The number of NTLM authentications (per second) serviced by this domain controller
Kerberos Authentications/sec	The number of times per second that clients use a client ticket to this domain controller to authenticate to this domain controller
DS Threads in Use	The current number of threads in use by the directory service
Replication status	The current replication status
DRA Pending Replication Synchronizations	The number of directory synchronizations that are queued for this server that are not yet processed
DRA Pending Replication Operations	The number of directory operations that are queued for this server that are not yet processed

11.4.10 Windows Services

Windows Services Monitor allows you to checks the statuses of Windows services running on your machine.

Adding a Windows Services monitor

Copyright © Acronis International GmbH, 2003-2019

Before proceeding, please ensure that you have created the Windows Server component and your Acronis Private Agent for Windows/Linux is running (see “About Acronis agents (p. 13)”), and PowerShell 3.0 or later is installed.

Select the Windows service monitoring slider if you need to monitor the Windows services on your server. In the Parameters window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. Select the services that you want to monitor.
4. Click **OK**.

To manage your monitor, go to the **Monitor Manager** and click on the slider to deactivate the monitor.

11.4.11 Windows event logs

The Windows event logs Monitor allows you to monitor specific events logs.

Adding a Windows event logs monitor

Before proceeding, please ensure that you have created the Windows Server component and your Acronis Private Agent for Windows/Linux is running(see “About Acronis agents (p. 13)”), and PowerShell 3.0 or later is installed.

Select the **Application event log/Security event log/System event log** slider if you need to monitor the Windows event logs on your server. In the **Monitor Parameters** window, set the following values:

1. [Optional] Change the monitor **Name**.
2. [Optional] Change the default value for refreshing intervals (min).
3. [Optional] Change the **log name**.
4. You can enter the threshold values if any of user-defined events are logged and/or number of error events is reached (events with "Error" or "Critical" severity levels) and equals or exceeds set value.
5. Go to **Monitor Status Change Rule** and specify the number of consecutive measurements needed to change the monitor status.
6. Click **OK**.

To manage your monitor, go to the **Monitor Manage**r and click on the slider to deactivate the monitor.

Copyright © Acronis International GmbH, 2003-2019