The Service Availability feature of Server Visibility enables you to monitor internal or external HTTP and HTTPS services. You configure service monitoring from the controller UI. After you configure monitoring for a service, Service Availability evaluates the service as follows:

- The agent evaluates each response, based on your specified violation rules, and flags each response as failed (rule violation) or successful (no violation).
- The service monitor maintains a rolling buffer of evaluated responses. This buffer has a configurable window size (number of evaluated responses), success threshold (number of successful responses), and failure ratio (number of failed responses).
- The monitor collects evaluated responses until the response buffer is full. Then it evaluates the service as:
  - NORMAL - Successful responses are greater than or equal to the success threshold.
  - CRITICAL - Failed responses is greater than or equal to the failure threshold.
- When the buffer is full, the monitor re-evaluates the service every time it evaluates a new response.

For example, with the following values:

- Success threshold = 3
- Failure threshold = 1
- Results window size = 5
The agent waits until five check results are received and from these five results if there is one failure then the target state is CRITICAL. If there are at least three successful results, then the target state is NORMAL.

Licensing and System Requirements

Service Availability Monitoring requires a separate license and a Server Visibility license. Server Visibility is currently available for Linux, Windows, and Solaris. See License Management and Server Visibility Requirements and Supported Environments.

Viewing the Monitored Services

The monitored services can be viewed in the Monitored Services list. The state is determined as described above by evaluating the Response Validators during the results window. Response Validators are rules you configure that are used to evaluate against the responses received from the service.

The possible states are:

- NORMAL - The number of successful responses in the result window is greater than or equal to the configured success threshold.
- CRITICAL - The number of failed responses in the result window is greater than or equal to the configured failed threshold.
- UNKNOWN - If the machine agent does not provide any data.

Monitored Services List

From the top navigation bar, click Servers > Service Availability to see a list of monitored services. Use the action toolbar to manage your monitored services by adding new ones, viewing details and so on.

<table>
<thead>
<tr>
<th>Monitored Service</th>
<th>Server</th>
<th>State</th>
<th>Success Rate (%)</th>
<th>Response Time (ms)</th>
<th>Response (b)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECommerce Homepage</td>
<td>ECommerce_MA</td>
<td>✔</td>
<td>100.0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>ECommerce Marketing Landing Page</td>
<td>ECommerce_MA</td>
<td>☀</td>
<td>0.0</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

Monitored Service Details

Select a monitored service and double-click to see the associated details.
Configure Service Availability

By default, configuration changes take effect within at least two minutes of the change, so you do not need to restart the Machine Agent after changing the configuration. If the protocol, target, or method of a service are changed once a service is created, the state of the service is set to UNKOWN, and is re-evaluated with the new configuration.

To configure this feature, users need the Configure Server Visibility permission. See Server Visibility Permissions for more details.

To access the configuration window do the following:

1. From the Controller top navigation bar, select Servers > Service Availability. You see a list of monitored services if any are configured.
2. To add a service, click Add. You see the Add Service Monitoring Configuration window with three tabs.

3. On the Main tab, specify the required fields and save the configuration. Each field has an associated tooltip that provides help. For details, see Main Configuration Window.

4. On the Request Configuration tab, specify your request headers. For details, see Request Configuration.

5. On the Response Validators tab, configure your validation rules. For details, see Response Validators.

### Main Configuration Window

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Default</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of your choice for this target configuration. This name appears in the Service Availability list.</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Target</td>
<td>The resource to be monitored, for example, <a href="http://myThirdPartyService.com/data">http://myThirdPartyService.com/data</a>. Specify which HTTP method to use to send the request (GET, POST, HEAD)</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Server</td>
<td>Name of the machine agent performing the monitoring. Only servers that are enabled for Server Visibility show in the drop-down list.</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Socket Timeout</td>
<td>How long to wait, in milliseconds, after a successful connection for a complete HTTP response.</td>
<td>30000</td>
<td>Yes</td>
</tr>
<tr>
<td>Success threshold</td>
<td>Number of required successes within the results window for a NORMAL state.</td>
<td>3</td>
<td>Yes</td>
</tr>
<tr>
<td>Check Interval</td>
<td>Interval time in between checks in seconds. Note - Setting this interval to more than 60 seconds will result in visible gaps in the metric graphs for monitored services.</td>
<td>10</td>
<td>Yes</td>
</tr>
<tr>
<td>Results Window Size</td>
<td>Number of most recent results to use in determining the state of the service.</td>
<td>5</td>
<td>Yes</td>
</tr>
<tr>
<td>Connect Timeout</td>
<td>How long to wait (in ms) for the service to respond to a connection request.</td>
<td>30000</td>
<td>Yes</td>
</tr>
<tr>
<td>Failure threshold</td>
<td>Number of required failures within the result window for a CRITICAL state.</td>
<td>1</td>
<td>Yes</td>
</tr>
<tr>
<td>Max response size</td>
<td>Maximum response size to collect in bytes.</td>
<td>5000</td>
<td>Yes</td>
</tr>
<tr>
<td>Follow redirects</td>
<td>Follow redirect to determine the state of service.</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

### Request Configuration
You can define a list of customized headers to send with requests. For example, the list can mimic desktop or mobile browsers. You can also define a request body for POST requests. An "Authorization" header can be specified if credentials are required.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Field</th>
<th>Value Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>header name and value pair</td>
<td>String</td>
<td>empty</td>
<td>Customized header to send with requests.</td>
</tr>
<tr>
<td></td>
<td>body</td>
<td>String</td>
<td>empty</td>
<td>Any data to send with the request. Usually used for POST.</td>
</tr>
</tbody>
</table>

**Response Validators**

You can provide a list of rules for the machine agent to use to validate whether the monitored service is healthy. If any rule is violated, the response is considered failed.

For each rule you can specify the following:

- HTTP property
- operator
- a value

The list of operators varies depending on the property selected in the first drop-down.

**Monitoring the Service Health**

An event is sent to the controller for every state change and periodically (by default every 5 minutes). The update interval can be changed by setting the System property:

appdynamics.machine.agent.sam.event.updateIntervalMillis. For more detail, see "Service Availability Update Interval" in the Configuration Property Reference.

The events are visible from the Monitored Service details window and from the Server Visibility Events list.
You can see details by double-clicking the event.

The event properties are as follows:

- Category: CUSTOM
- Event Type: Service Availability
- Property: severity - values can be ERROR (failure) or INFO (passing).

Configuring Alerts

Use these steps to create alerts for your monitored services:

1. From the Servers window, click Alert & Respond.
2. Select Policies.
3. Select Create Policy Manually.
   If policies already exist, you may not see this option. Just click + to add a policy manually.
4. Under Custom Events, click + to Add Custom Event.
5. In the Actions section of the Policy window, add the action you want to execute if the policy violates and save the policy.