

# Problem Detection and Notifications

---

Dynatrace Training Module



# Agenda

---

- Overview of Dynatrace Problems
- How Problems are detected
  - Events
  - Baselines
  - Thresholds
- Frequent Issues
- Problems Severity Types
- Problems Overview Page
- Alert Profiles
- Problem Notifications
- Maintenance windows

# Problems Overview

---

## Problem Overview

---

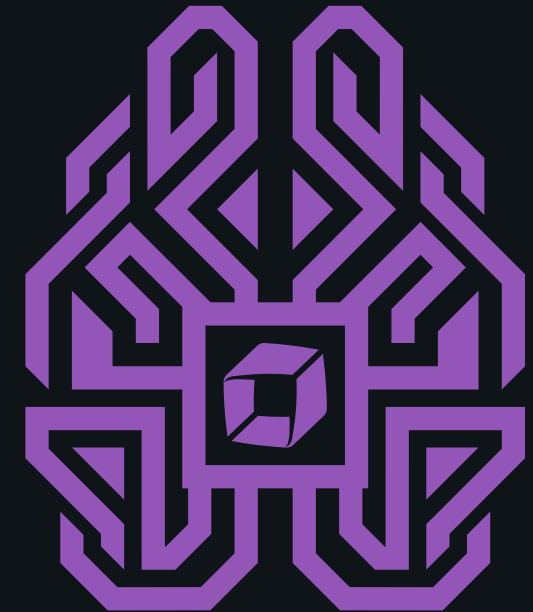
- Dynatrace uses a sophisticated AI causation engine, called Davis<sup>®</sup>, to automatically detect performance anomalies.
- Dynatrace applications, services, processes, hosts and externally supplied metrics are analyzed.
- Dynatrace-detected problems are used to report and alert on abnormal situations, such as performance degradations, failure rate increases, high resource consumption or lack of availability.
- Problems have defined lifespans and are updated in real time with all incoming events and findings.

<https://www.dynatrace.com/support/help/shortlink/problems-hub>

## Problem Overview

---

- *A Problem is a logical grouping of all related events, context, and root-cause analysis details for a given incident in your monitoring environment*
- Problems are what you work with when being notified of and responding to issues in your monitored applications
- Davis® powers the problem creation and root cause analysis.



# What is a problem?

---

## How Problems are detected

---

- Dynatrace continuously monitors certain metrics against auto-created baselines or fixed thresholds.
- Events can represent different types of individual incidents
- Events can be metric-threshold breaches, baseline deviations or availability issues
- Not all events warrant a problem. Events can also be point-in-time events, VMotions, software deployments or configuration file changes.
- Events can be detected within Dynatrace data or pushed from external sources (e.g. Azure Events or Deployment Tools).
- “Severe” Events will result in a Problem being created. Some Examples:
  - Unexpected high or low traffic
  - Slower response times
  - Increased failure rates
  - High CPU or memory utilization
  - Network Issues

# Understanding Event Thresholds

---

- Dynatrace utilizes two types of thresholds to create events
- Automated baselines
  - Multidimensional baselining automatically detects individual reference values that adapt over time.
  - Automated baseline reference values are used to cope with dynamic changes within your applications or service response times, error rates, and load.
  - Multidimensional baselining works out of the box and automatically adapts to changes in patterns.
- Static thresholds
  - Dynatrace uses built-in static thresholds for all infrastructure events (for example, detecting high CPU, low disk space, or low memory).
  - Thresholds are set out-of-the-box but can be customized.

<https://www.dynatrace.com/support/help/shortlink/problems-intro#understanding-thresholds>



## Automatic baselining summarized

---

- Baselines are evaluated over 5-min (for fast changing values) and 15-min (for slow changing values) sliding time intervals
- Median and 90th percentiles are evaluated
- Values for response times, error rates and load are automatically detected for each individual application and service.
  - Each Application baseline is split by user action, geolocation, browser type and hardware type (such as Windows or Linux)
  - Services are baselined by each service request
- Applications and services must run for at least 20% of a week (~1.5 days) before slowdown and error rate Problems are raised
- Applications and Services must run for at least a full week before traffic spike and drop Problems are created

<https://www.dynatrace.com/support/help/shortlink/automated-baselining>

## Adjusting Threshold Sensitivity

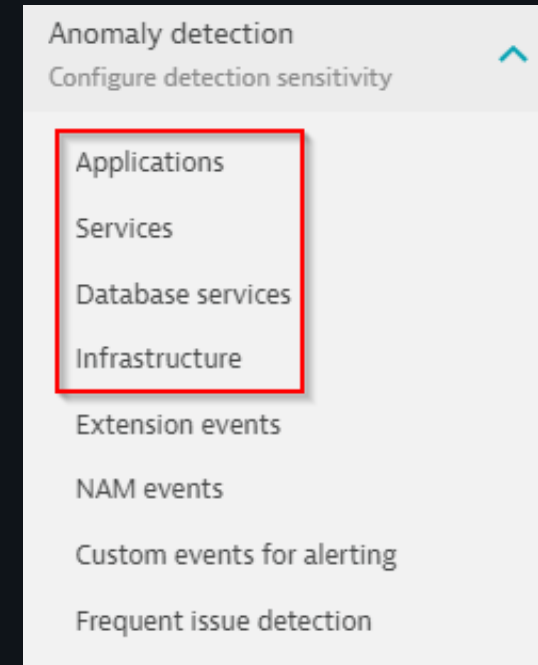
---

- Typical application and service-level anomalies reported by Dynatrace include
  - Failure rate increases
  - Response time degradation
  - Spikes or Drops in application traffic.
- Dynatrace allows you to define specific thresholds that specify at what amounts above baseline performance are severe enough to generate problem alerts.
- Keep in mind that these threshold settings only adjust the levels at which Dynatrace alerts you to detected anomalies.
- These settings don't affect automated performance baselining.

<https://www.dynatrace.com/support/help/shortlink/problem-detection-sensitivity>

## Adjusting Threshold Sensitivity – Global Settings

- Typically, the global settings are set at a good starting point when starting to monitor the environment.
- Change the Global settings if there are extensive false-positive problems being created; such as while monitoring a development-only environment.
- If specific applications, databases, services or hosts are over-alerting, modify the anomaly detection settings on the specific entity.
- Modify global settings by navigating to Settings->Anomaly detection and selecting the entity type: Applications, Services, Database services or Infrastructure.



# Adjusting Threshold Sensitivity – examples

- Applications, Services and Database services have similar configurations for:
  - Performance
  - Error Rates
  - Traffic Drops
  - Traffic Spikes
- Applications detect increased JavaScript error rates.
- Services detect failure rates (HTTP 400-500 status)
- Database Services also detect failed database connects.
- Services and Database Services have traffic drop and spike detection off by default.

Web applications

Mobile apps

Custom applications

Detect key performance metric degradations

automatically

Alert if the key performance metric degrades beyond

100

ms and by 

50

%.

Alert if the key performance metric of the slowest 10% degrades beyond

1000

ms and by 

100

%.

To avoid over-alerting do not alert for low traffic applications with less than 

10

 actions/min.

Alert if the application stays in abnormal state for at least 

0

 minutes.

Detect traffic drops

Dynatrace learns your typical application traffic over an observation period of one week. Depending on this expected value Dynatrace detects abnormal traffic drops within your application.

Alert if the observed traffic is less than 

50

 % of the expected value.

Detect traffic spikes

Dynatrace learns your typical application traffic over an observation period of one week. Depending on this expected value Dynatrace detects abnormal traffic spikes within your application.

Alert if the observed traffic is more than 

200

 % of the expected value.

Detect increases in failure rate

automatically

Alert if the percentage of user actions affected by JavaScript errors increases by 

5

 % absolute and by 

50

 % relative.

Example: If the expected error percentage is 1.5% we calculate  
the absolute threshold as  $1.5\% + 5\% = 6.5\%$   
and the relative threshold as  $1.5\% + 1.5\% * 50\% = 2.3\%$   
Dynatrace alerts if both thresholds are exceeded.

To avoid over-alerting do not alert for low traffic applications with less than 

0

 actions/min.

Alert if the application stays in abnormal state for at least 

0

 minutes.

# Adjusting Threshold Sensitivity – examples

- Davis automatically detects infrastructure-related performance anomalies such as high CPU saturation, memory outages, and low disk-space conditions across both physical and virtual infrastructure components.
- Infrastructure monitoring typically uses static thresholds.

<https://www.dynatrace.com/support/help/shortlink/problem-evaluation>

## Anomaly detection for infrastructure

Dynatrace automatically detects infrastructure-related performance anomalies such as high CPU saturation, memory outages, and low disk-space conditions. Use these settings to configure detection sensitivity, set alert thresholds, or disable alerting for infrastructure components.

- ☒ Detect host or monitoring connection lost problems
- ☐ Alert on graceful host shutdowns

☒ Detect CPU saturation on host

☒ Detect high memory usage on host

☒ Detect high GC activity

You may also configure high GC activity alerting for .NET processes on [extension events page](#).

☒ Detect Java out of memory problem

☒ Detect Java out of threads problem

### Network

☒ Detect high number of dropped packets

☒ Detect high number of network errors

☒ Detect high network utilization

☒ Detect TCP connectivity problems for process

☒ Detect high retransmission rate

### Disk

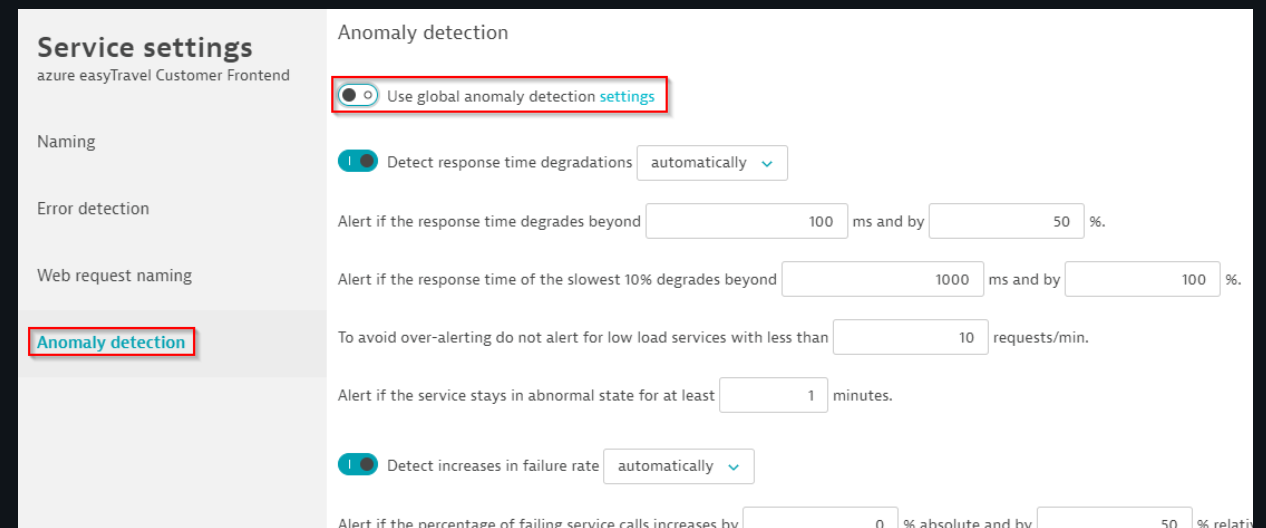
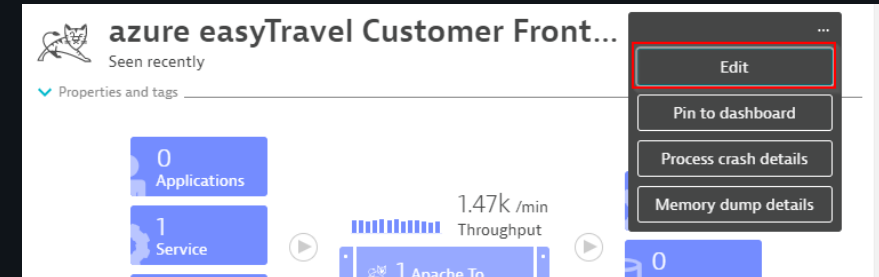
☒ Detect low disk space

☒ Detect slow-running disks

☒ Detect low inodes number available

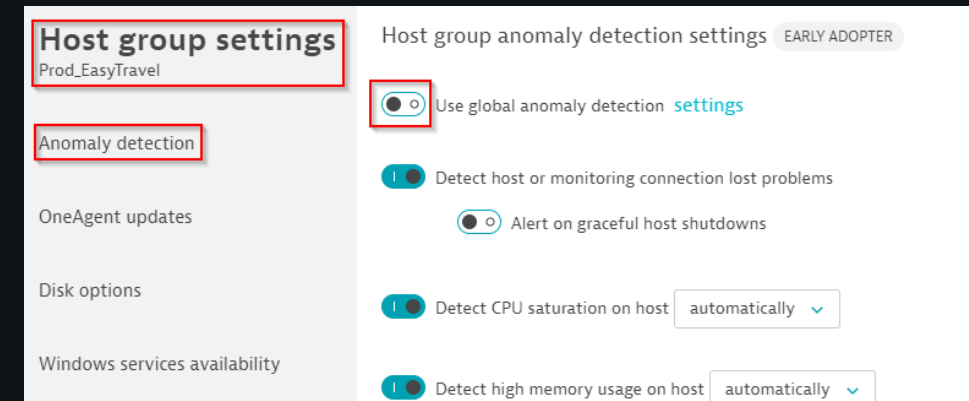
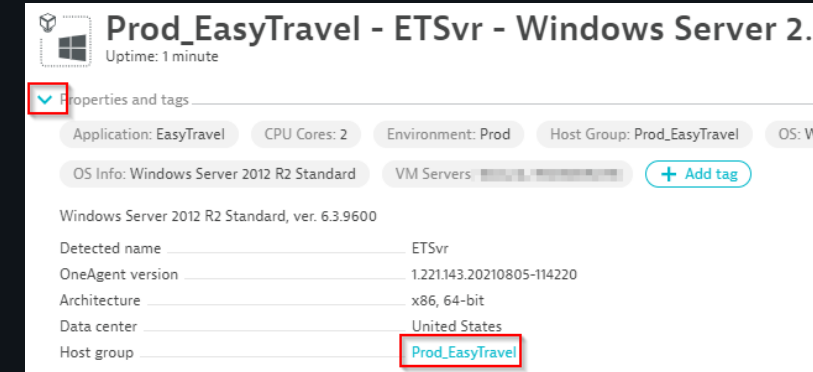
## Adjusting Threshold Sensitivity – Host group or entity Settings

- Global thresholds can be overridden at a Host Group or on an individual entity.
- If a specific Application, Service or Database Service is over alerting, or under alerting:
  - Navigate to the entity
  - Edit the settings on the entity
  - Open the Anomaly detection settings to disable the global setting inheritance
  - Set custom thresholds on the object itself.



## Adjusting Threshold Sensitivity – Host group or entity Settings

- Typically hosts performing the same function will be in the same Host Group
- Those hosts may also need to have the same detection settings.
- Navigate to the Host Group for the host
  - Open one host in the group
  - Open the properties
  - Select the Host Group in the properties list
- Disable global setting inheritance
- Modify the settings on the Host Group to change the settings for all hosts in the group.
- Individual hosts can still have unique settings if needed.



## Custom Events

---

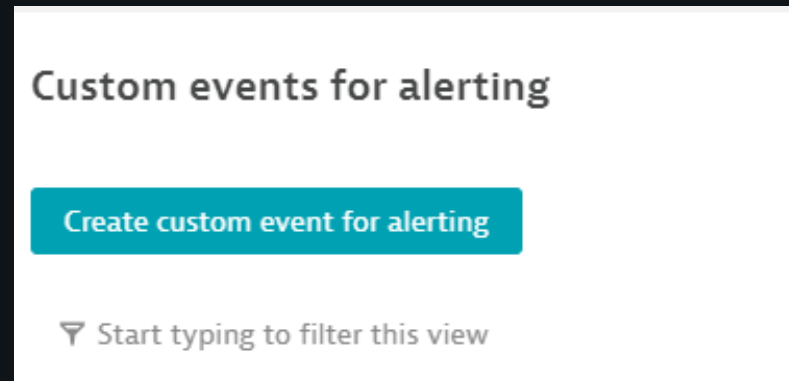
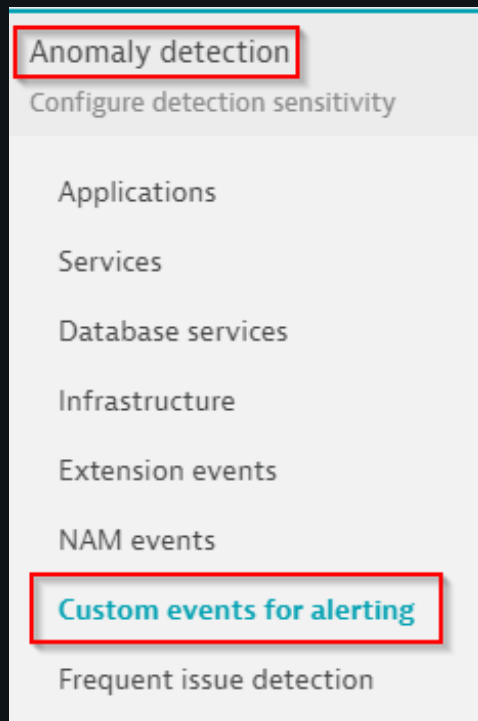
- Custom events can be configured in addition to the wide range of events automatically detected.
- Multiple events can be configured with different thresholds to indicate warning or severe events.
- Any Metric captured or imported into Dynatrace can be used.
- Custom Metrics created in Dynatrace can be used. Such as:
  - Calculated Metrics from Multi-Dimensional Analysis views
  - Log metrics, etc
- Static thresholds or auto-adaptive baselines can be utilized to create the event.

<https://www.dynatrace.com/support/help/shortlink/metric-events-for-alerting>



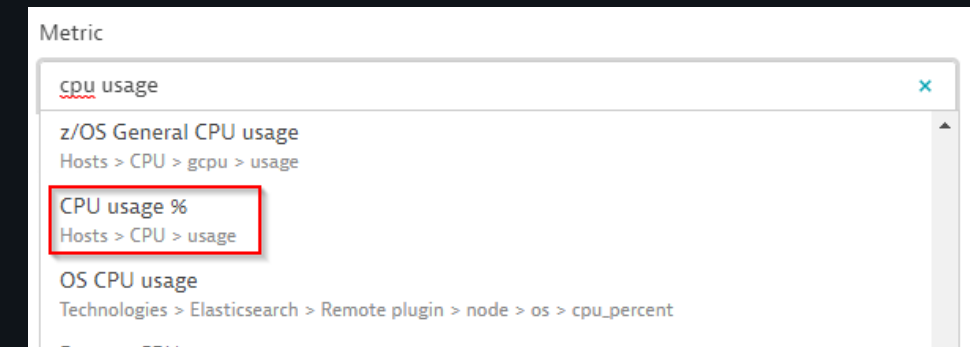
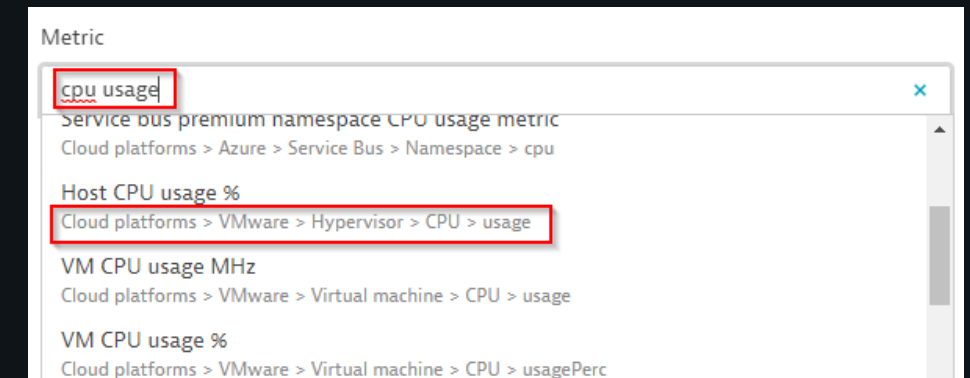
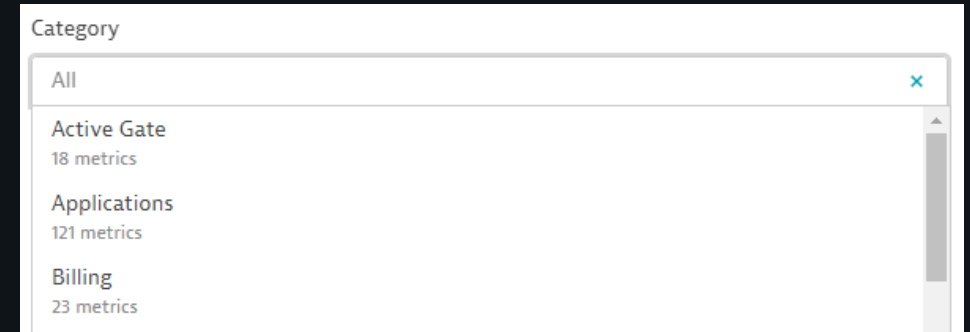
## Custom Events

- Navigate to Settings->Anomaly Detection->Custom events for alerting
- Select "Create custom Event for Alerting"



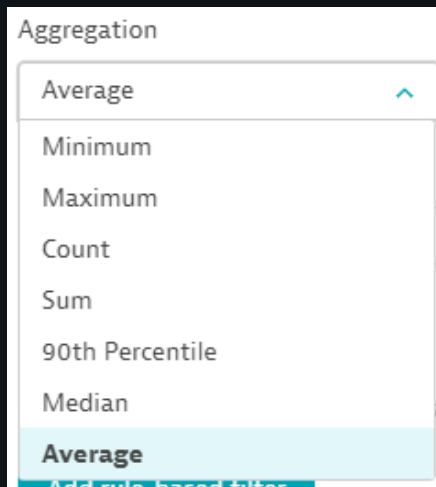
## Custom Events – Select the Metric

- Utilize the “Category” pull down to view the metric groupings
- Select the Metric to create the event.
  - Use the pull-down to view the list of available metrics.
  - Type in the name of the metrics to filter the list.
  - Be careful to review the second line in the metric to ensure the correct metric is being selected.
  - Typing text in the metric field will also search the second line in the metric. For example, try “mobile”.
  - Expert tip: type in “calc” in the dialog to get a list of all calculated metrics.

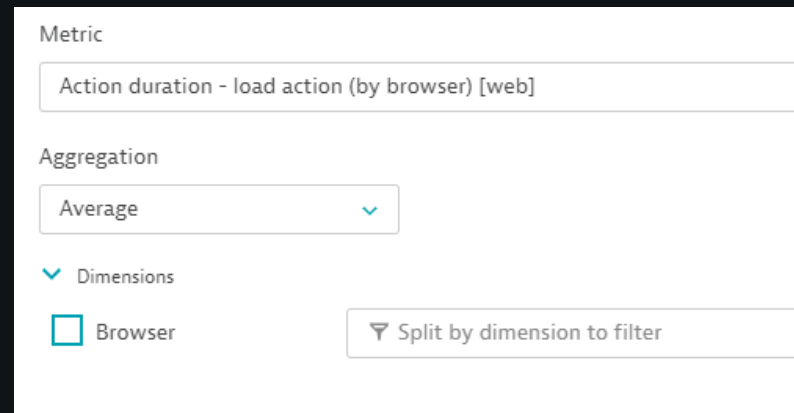


## Custom Events – Select Aggregation

- Select the Aggregation to be use.
  - Metrics may have different aggregations
  - Use the pull-down to see available values
- Some metrics are composed of multiple dimensions. You can select what dimensions and values should be considered for the event.



A screenshot of a dropdown menu titled "Aggregation". The menu is open, showing a list of aggregation options: Average, Minimum, Maximum, Count, Sum, 90th Percentile, Median, and Average. The "Average" option at the bottom is highlighted in light blue. A small upward arrow is visible next to the top "Average" option.



A screenshot of a configuration panel for a metric. The "Metric" field is set to "Action duration - load action (by browser) [web]". Below it, the "Aggregation" dropdown is set to "Average". Under the "Dimensions" section, the "Browser" checkbox is checked. A button labeled "Split by dimension to filter" is located to the right of the checkbox.

## Custom Events – Filter the Entities

- Add a rule-based filter to limit the scope, or entities, the event will apply to.
- Once the rule is saved the Alerting Scope Preview will update.

Entities

Use rule-based filters to define the scope this event monitors.

Add rule-based filter

Property

Name

Name

Entity

Tag

Management zone

Host group name

Cancel Create rule-based filter

Entities

Use rule-based filters to define the scope this event monitors.

Add rule-based filter

Property	Operator	Value	Delete	Edit
Name	contains (case insensitive)	Prod	X	^

Property

Name

Operator

contains (case insensitive)

Value

Prod

Update Cancel

---

Alerting scope preview (2 Host entities)

Prod\_DT-SaaS - ag-plugins - CentOS Linux 7

Prod\_EasyTravel - ETSvr - Windows Server 2012 R2 Standard

# Custom Events – Select a Monitoring Strategy

- Select a threshold
  - Static threshold—threshold that doesn't change through time. Dynatrace suggests a value based on the previous data.
  - Auto-adaptive baseline—Automatically calculated threshold that adapts dynamically to your metric's behavior. Select how many times the signal fluctuation is added to the baseline.
- Specify a sliding window for comparison
  - Defines how often the threshold must be violated within a sliding window of time to raise an event. Violates do not have to be consecutive.
- Choose the missing data alert behavior. If enabled, it is combined with the baseline/threshold condition by the OR logic.

## Monitoring strategy

The monitoring strategy defines what types of anomalies can be detected on a selected metric. While a static threshold is preferred for detecting breaches of hard set limits, auto-adaptive baselines are used to detect anomalies within metrics that show a regular change over time.

- ☒ Static threshold
- ☐ Auto-adaptive baseline

### Static threshold settings

A static threshold monitoring strategy is preferred for alerting on hard limits within a given metric. An example is the violation of a critical memory limit. Use this section to adapt the suggested static threshold to your own needs. [Documentation](#)



Few datapoints available for the selected metric. Threshold suggestion might be unreliable.

Alert anomalies with a static threshold of

Raise an alert if the metric is  the threshold for  minutes during any  minute period.

if data is missing within the above observation period. We recommend to not alert on missing data for sparse timeseries as this leads to alert spam.

- ☐ Static threshold
- ☒ Auto-adaptive baseline

### Auto-adaptive baseline settings

An auto-adaptive baseline is preferred for detecting anomalies within metrics that show a regular change over time, as the baseline is also updated automatically. An example is to detect an anomaly in the number of received network packets or within the number of user actions over time. Use this section to adapt the detection sensitivity to your own needs. [Documentation](#)

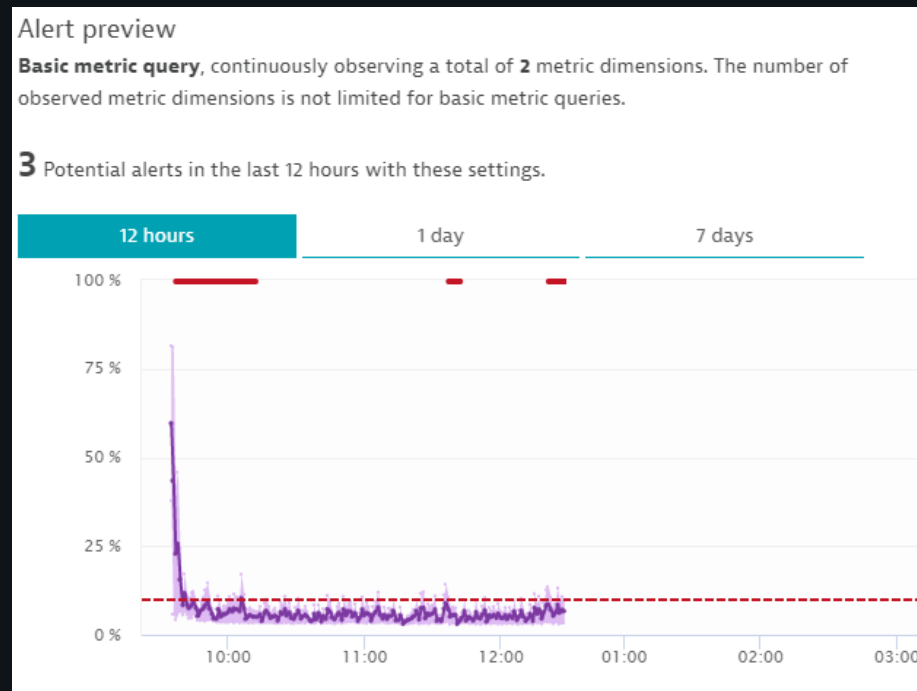
Alert anomalies of  times the normal signal fluctuation.

Raise an alert if the metric is  the baseline for  minutes during any  minute period.

if data is missing within the above observation period. We recommend to not alert on missing data for sparse timeseries as this leads to alert spam.

## Custom Events – Preview

- Utilize the preview to see when the event would be created given the configuration.
- Different timeframes can be selected.
- Red bars appear at the top of the chart if an event would have been generated.



## Custom Events – Preview and description

- Select a title for your event. The title should be a short, easy-to-read string describing the situation
- In the Event description section, create a more detailed message. The following placeholders can be used: {metricname}, {severity}, {alert\_condition}, {missing\_data\_samples}, and {baseline} or {threshold}.
- Severity level is important to configure properly. It determines whether a Problem is also created with the event and if Davis includes it in any analysis.

[https://www.dynatrace.com/support/help/shortlink/metric-events-for-alerting#anchor\\_severity](https://www.dynatrace.com/support/help/shortlink/metric-events-for-alerting#anchor_severity)

Event description

Title

CPU Utilization Warning

Severity

Custom alert

Availability

Error

Slowdown

Resource

Info

Custom alert

Every receiver of this event.

{metricname} was {alert\_condition} your custom threshold of {threshold}

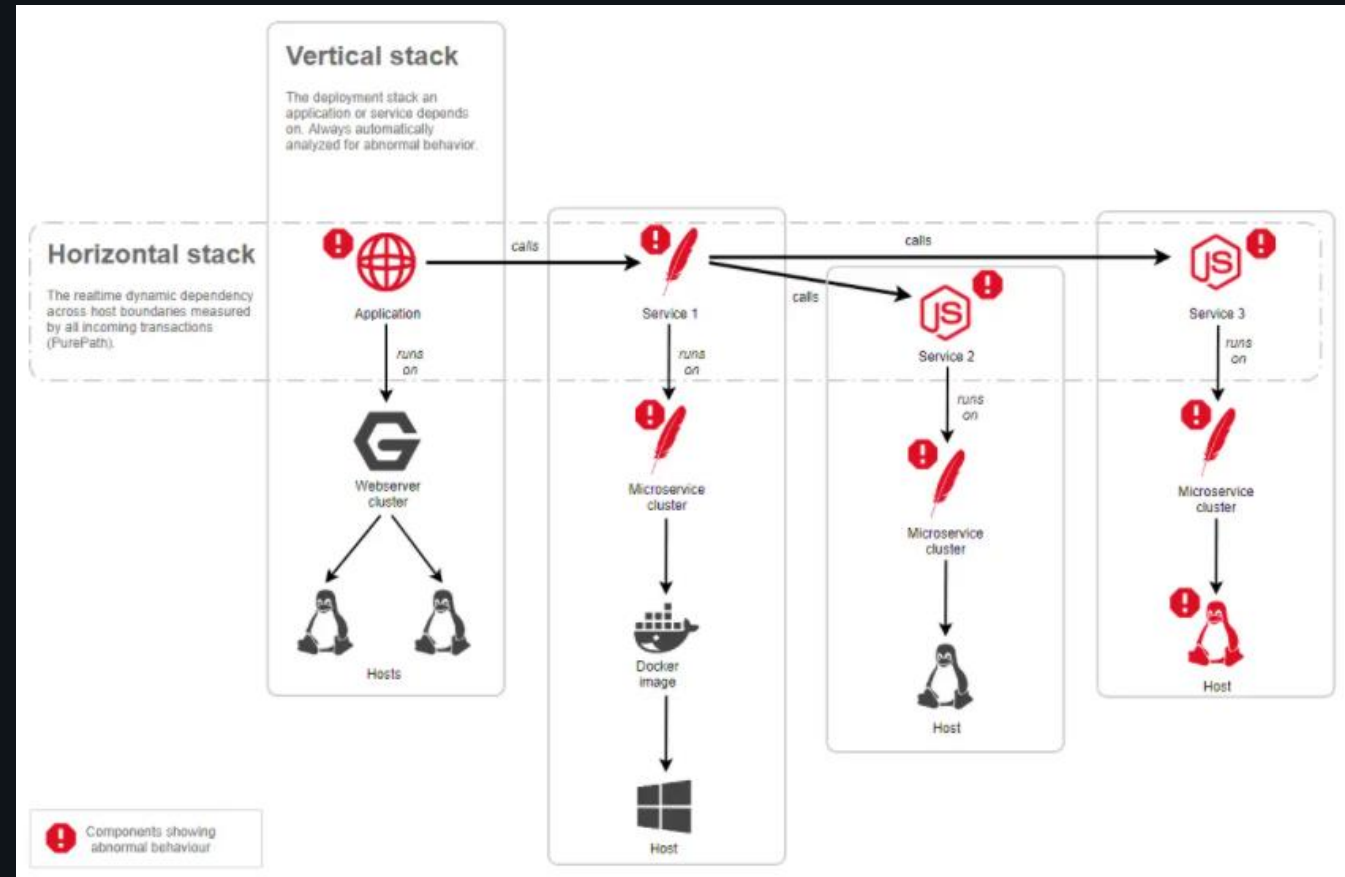
### Types of severities

The following types of severities are available.

Severity	Problem raised	Davis analysis	Semantic
Availability	Yes	Yes	Reports any kind of severe component outage
Error	Yes	Yes	Reports any kind of degradation of operational health due to errors
Slowdown	Yes	Yes	Reports a slowdown of an IT component
Resource	Yes	Yes	Reports a lack of resources or a resource-conflict situation
Info	No	Yes	Reports any kind of interesting situation on a component, such as a deployment change
Custom alert	Yes	No	Triggers an alert without causation and Davis AI involved

# Problems and Root Cause Analysis

- For each detected Problem, Dynatrace investigates the problem's impact and root cause.
- Dynatrace correlates the sequence of detected events that led up to a problem.
- Dynatrace follows a context-aware approach that detects interdependent events across time, processes, hosts, services and applications.
- Both vertical and horizontal topological monitoring perspectives are analyzed.
- Only through such a context-aware approach is it possible to pinpoint the true root causes of problems.



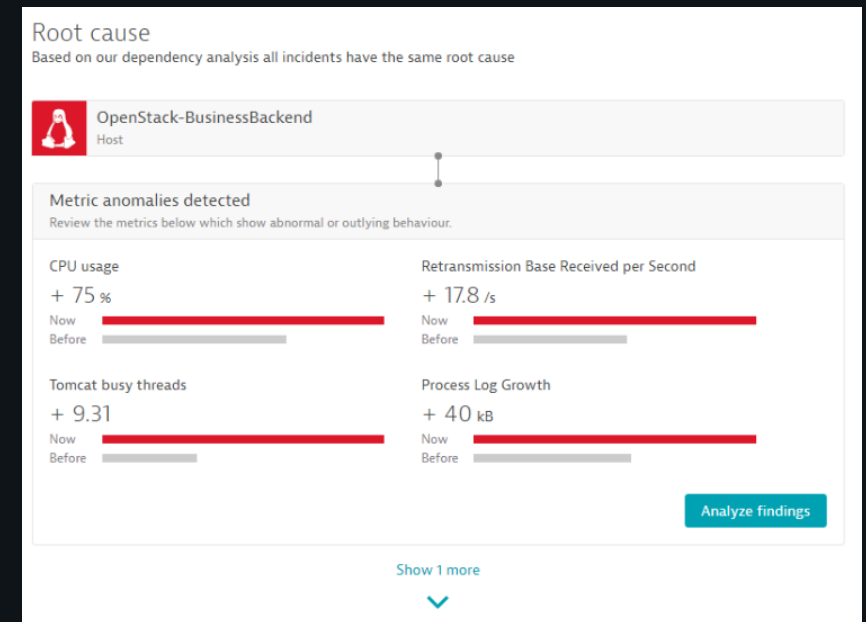
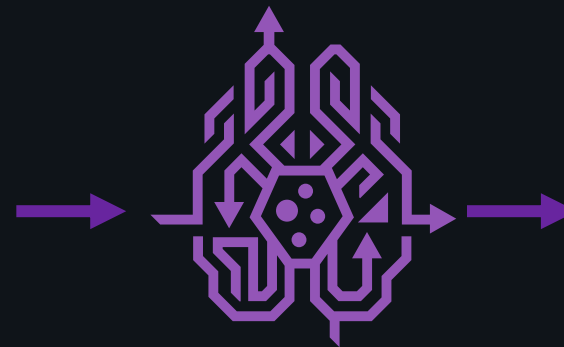
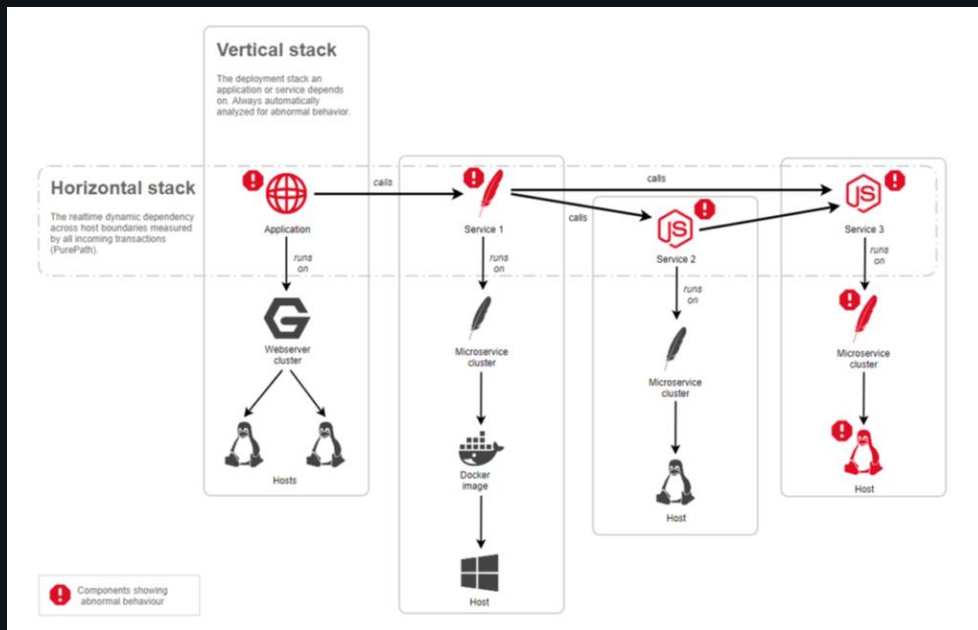


# Root cause analysis (RCA)

First event is raised, Davis automatically follows all related components

Davis follows transactions and collects evidence, such as events, abnormal states and outlying metrics

Davis presents all findings within root-cause section



# Frequent Issues

---

## Frequent Issues

- Problems may come from components or machines that are not critical, thereby are not corrected.
- The Dynatrace AI engine automatically detects regularly occurring Problems that originate from sub-optimal conditions.
- Dynatrace reviews the problem patterns of monitored entities within periods of one day and one week.
- When the same problem for an entity is detected multiple times Dynatrace evaluates the problem based on the breach severity and the duration of the problem.
- If the severity or duration increases, compared to past breaches, a new Problem is created. Otherwise, the Problem is considered a Frequent Issue.
- Recuring Problems that are not handled, even on important components, may also be considered Frequent Issues.

<https://www.dynatrace.com/support/help/shortlink/frequent-issues>



Problem 756  
Since 2015 Jul 9 20:34:00  
You are viewing this service in time context of this problem. [Remove this context](#)

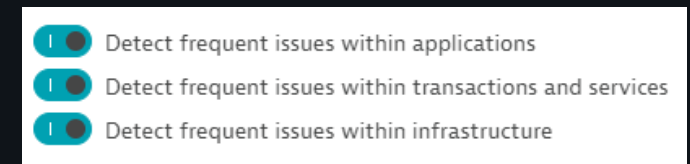
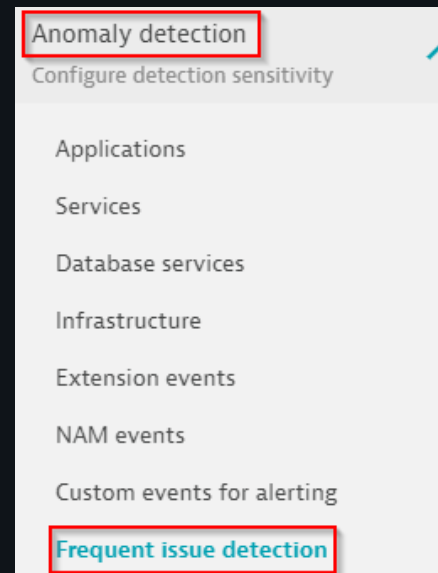
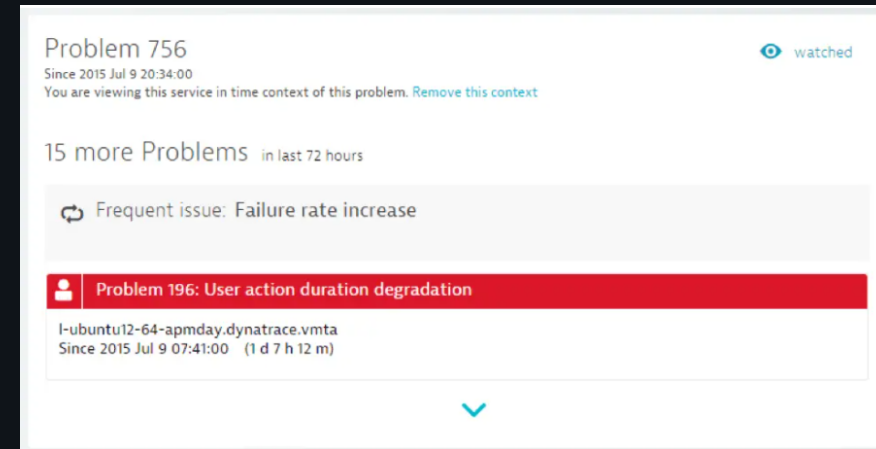
15 more Problems in last 72 hours

↻ Frequent issue: Failure rate increase

**Problem 196: User action duration degradation**  
l-ubuntu12-64-apmday.dynatrace.vmta  
Since 2015 Jul 9 07:41:00 (1 d 7 h 12 m)

# Frequent Issues

- This approach to the detection and handling of frequent issues only alerts for problems that increase in severity over time while avoiding alert spamming.
- Entity overview pages display the frequent issues messages
- Frequent issue detection is configured in Setting->Anomaly Detection->Frequent Issue Detection.
- Frequent issue detection can be configured for Applications, Transactions and Services or Infrastructure



# Problem Severity

---

## Problems Severity Types

---

- Problems aggregate all included events and are evaluated with the highest severity level of the constituent events.
- During its lifespan, a problem might raise its severity level.
  - For example, a problem might begin in slowdown level (3) and then be raised automatically to availability level (1) when an outage is detected.
- Severity types can be used to filter the problem screen
- Severity types are used as filters in alert profiles

<https://www.dynatrace.com/support/help/shortlink/event-types>

# Problems Severity Types

---



- Availability (Severity 1)
  - Indicates if a resource may be unavailable by detecting low traffic, host monitoring or process availability, synthetic outages, or custom metrics configured with an availability severity.



- Error (Severity 2)
  - Informs of increased error rates or error-related incidents such as javascript or service failures, mobile app crashes, network interface errors or custom metrics configured with an error severity.



- Slowdown (Severity 3)
  - Indicates an increase of response time for applications, services, databases, synthetics or custom metrics configured with a slowdown severity.



- Resource (Severity 4)
  - Indicate resource contention such as CPU or memory saturation, unexpected high traffic, low disk space, increased GC time or custom metrics configured with a resource severity.



- Custom (Severity 5)
  - Used for user-defined thresholds on metrics. Custom severity events are not correlated by Davis.

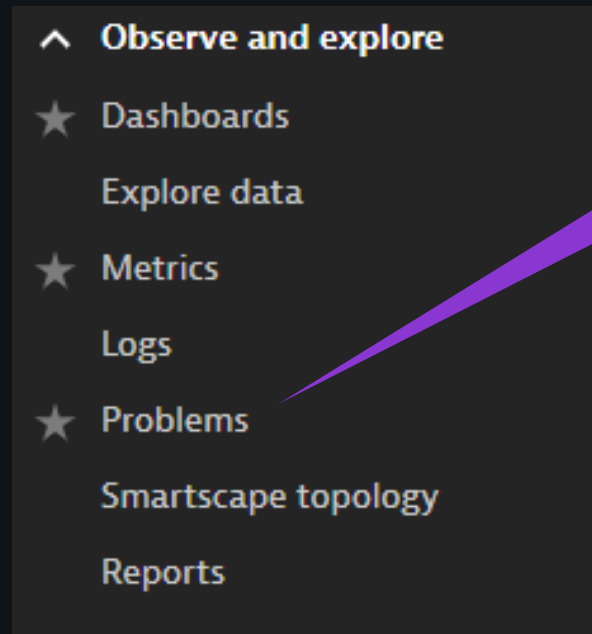
- Info (Severity 6)
  - Indicate events that don't result in the creation of a new problem, Java Framework changes, deployments or VMotions.

# Problems Overview Page

---

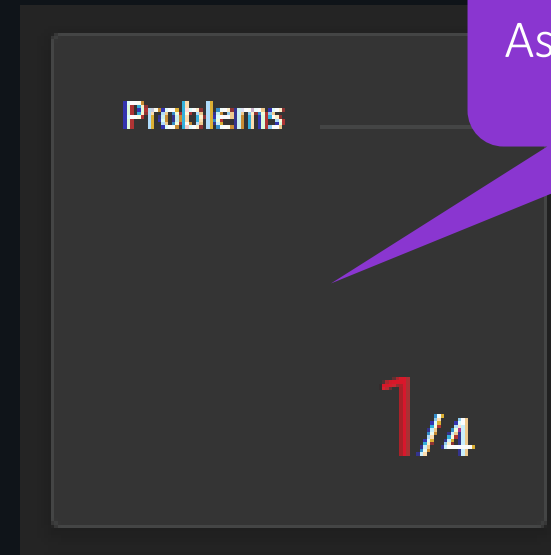


## How do I access Problems?

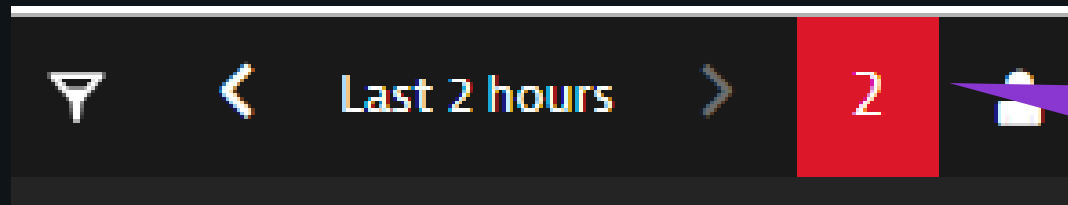


Main menu

OR



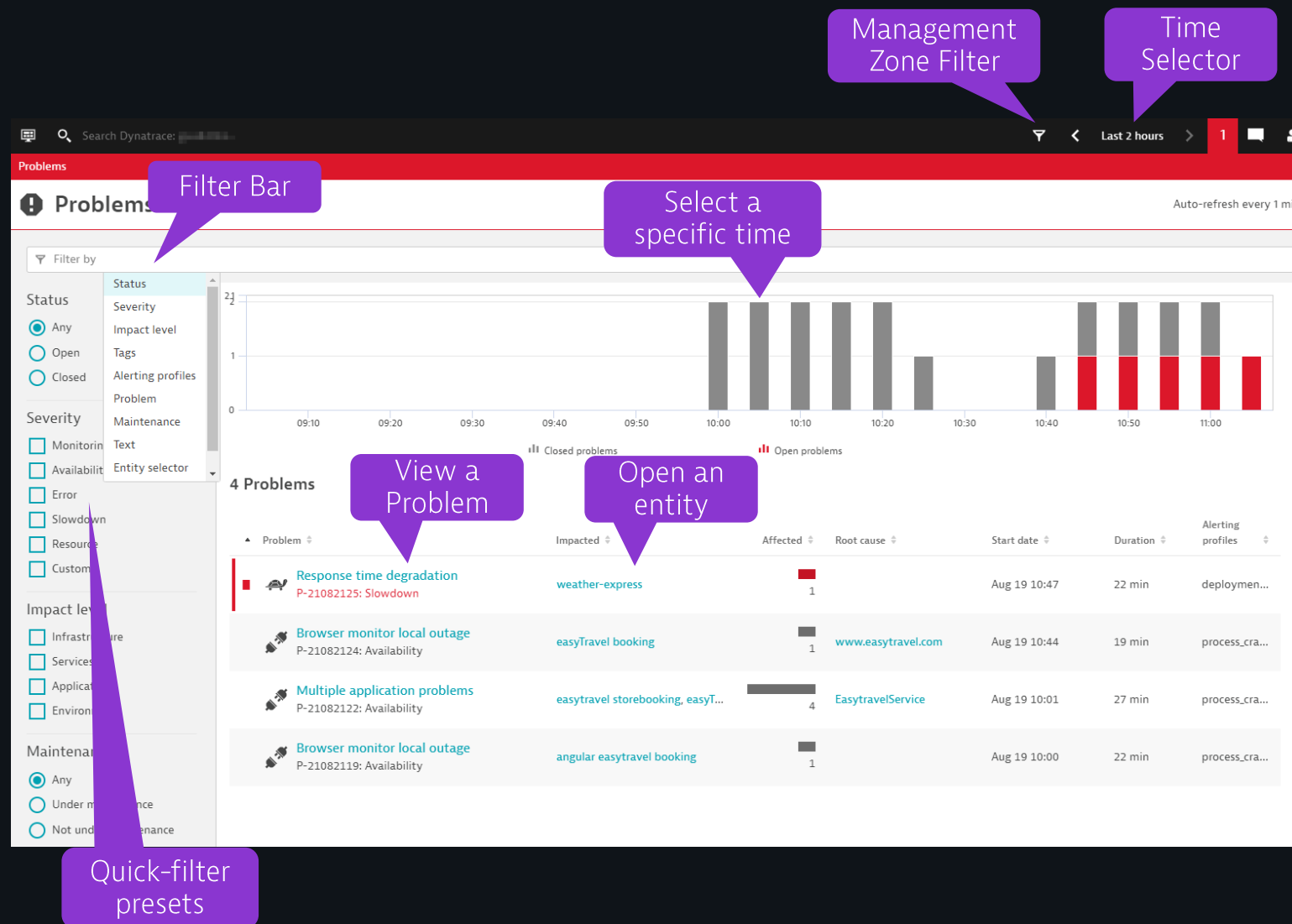
As a dashboard tile



On the top menu

# Problems Overview Page

- Once the Problems feed is open several options are available to refine the view or navigate.
- Use the time selector to view problems over a given timeframe.
- Click on a specific column in the graph to filter on that time
- Filter the view
  - Using the quick-filter presets
  - Select Filtering options in the top filter bar
  - Select a Management Zone
- Open a problem by clicking on the problem description
- Go right to an entity by clicking on the "impacted" entity column
- The view updates every minute



# Aspects of a Problem

- Several sections will display information about the selected problem.
- Start with Root Cause or the Impacted entity
  - Look for drill-downs to analyze failures or performance degradations.
- Open the entity in the "Impacted section"
  - Navigating to an impacted entity will set the Time Control to the time from the problem card.
- Visual resolution path will play through the events of the problem
- Open problems may evolve and change as Davis relates additional events to the problem

**Overview**

www.easytravel.com: User action duration degradation  
Problem 970 detected on Jun 13 23:27 - 00:16 (was open for 49 minutes). This problem affects real users.

	Affected	Recovered	Monitored
Applications	-	1	28
Services	-	10	105
Infrastructure components	-	-	667

58,829,400 Dependencies analyzed

**Business impact analysis**  
Snapshot of problem-affected service calls and impacted real users at start of problem

434 Impacted users    6.5k Affected service calls

**1 impacted application**  
48.4 User actions per minute impacted

www.easytravel.com Application

User action duration degradation  
The current response time (3.28 s) exceeds the auto-detected baseline (1.87 s) by 75 %

Affected user actions	User action
48.4/min	Loading of page /orange.jsf

Browser: All    Geolocation: Multiple    OS: All

**Comments**

No comments posted

**Root cause analysis**  
Based on our dependency analysis all incidents have the same root cause:

easyTravel-Business Database service

Response time degradation  
The current response time (251 ms) exceeds your custom threshold (200 ms) by 26 %

Affected requests: 2.24k /min    Service method: 5 Service methods

**Visual resolution path**  
Click to see how we figured this out.

Visual resolution path diagram showing the flow of events and dependencies.

# Alert Profiles

---

## Alert Profiles

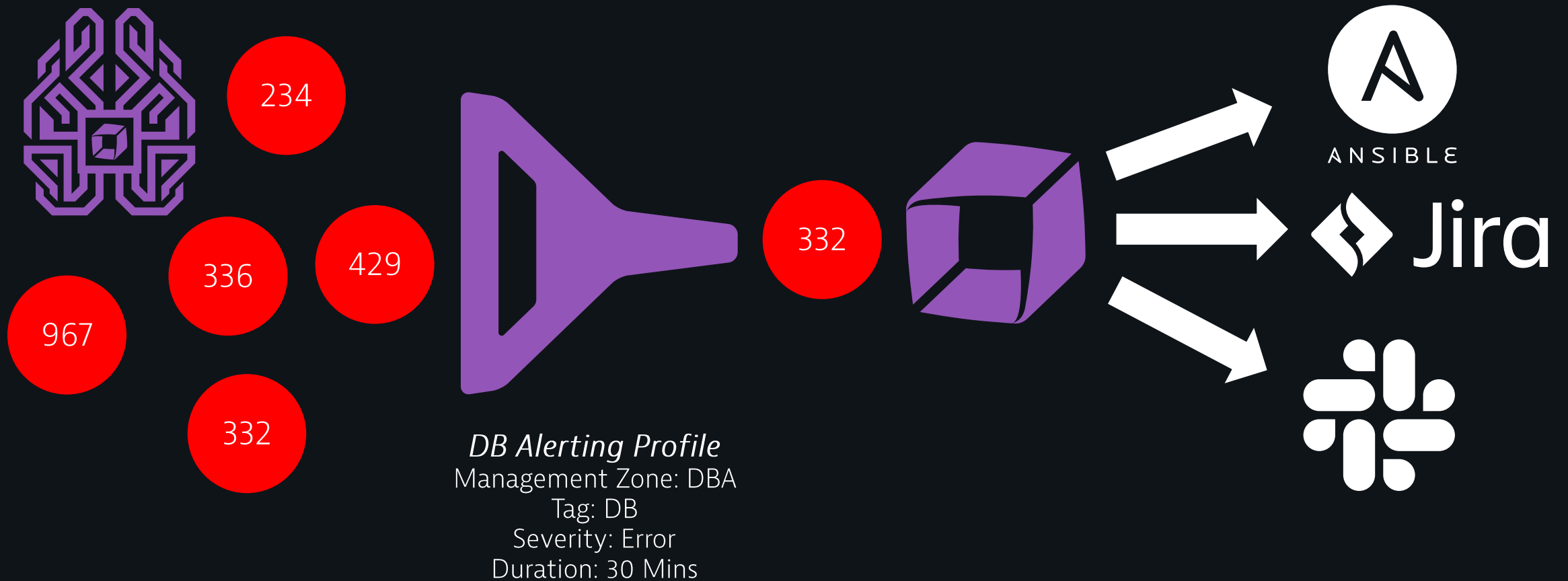
---

- Alert Profiles simply filter the full list of Problems.
- Alert Profiles are also the filtering mechanism for Problem Notifications
- By combining filter criteria, you can create custom profiles that filter Problems based on:
  - Management Zones
  - Severity
  - Tags
  - How long a problem has been open
  - Problems Titles or Descriptions
  - Specific event types

<https://www.dynatrace.com/support/help/shortlink/alerting-profiles>

## Alert Profiles

- Alerting profiles serve as a filter when deciding to send out a problem notification



# Alert Profiles

- To create an Alert Profile go to Settings->Alerting->Alerting Profiles and click "Add Alerting Profile"
- Provide a descriptive name for the profile
- Select a Management Zone, which perhaps the easiest way to create a profile and is highly recommended.

Summary

Production Alerts

Name

Production Alerts

Management zone

Optional

Define management zone filter for profile

Severity rules

Define severity rules for profile. A maximum of 20 severity rules is allowed.

Add severity rule

Event filters

Define event filters for profile. A maximum of 20 event filters is allowed.

Add event filter

Matches problems where

No filters, matches everything

# Alert Profiles

- Add one or more severity rules to the profile
- Specify how long the problem must be open before it is included in the profile.
- Further refine the rule by tag if necessary.
- Add event filters to filter for a specific event type. If the event types is not present in the problem, it will not be included in the profile.

Add severity rule

Filter items...

Summary

Availability alert (After 0 mins; Include all entities )

Problem severity level

Availability

Problem send delay in minutes

0

Send a notification if a problem remains open longer than X minutes.

Filter problems by tag

Include all entities

Availability

Custom

Error

Monitoring unavailable

Resource

Slowdown

Add event filter

Filter items...

Summary

Predefined: Contains events of type 'CPU saturation'

Filter problems by any event of source

Predefined

Filter problems by a Dynatrace event type

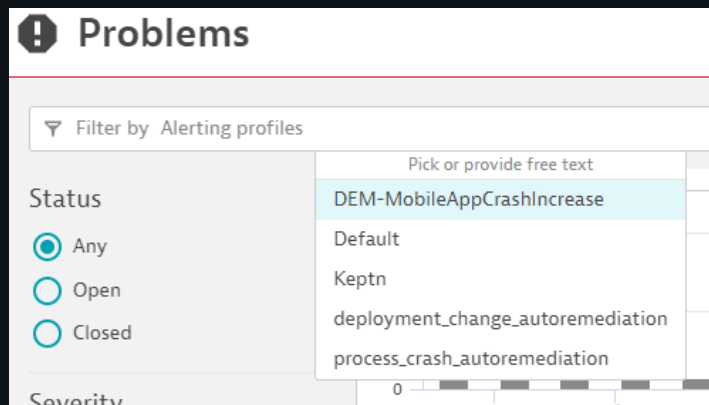
CPU saturation

Negate



# Alert Profiles

- Use the preview logic at the bottom of the alert definition to review what problems would be included in the profile.
- Save the changes when complete.
- Alert Profiles can also be used to filter the Problem Feed



## Matches problems where

Slowdown alert (After 10 mins; Include all entities )

OR

Resource alert (After 20 mins; Include all entities )

OR

Monitoring unavailable alert (After 15 mins; Include all entities )

OR

Error alert (After 15 mins; Include all entities )

OR

Availability alert (After 10 mins; Include all entities )

AND

Predefined: Contains events of type 'CPU saturation'

You have unsaved changes

Save changes

Discard changes

# Notifications

---

## Problem Notifications

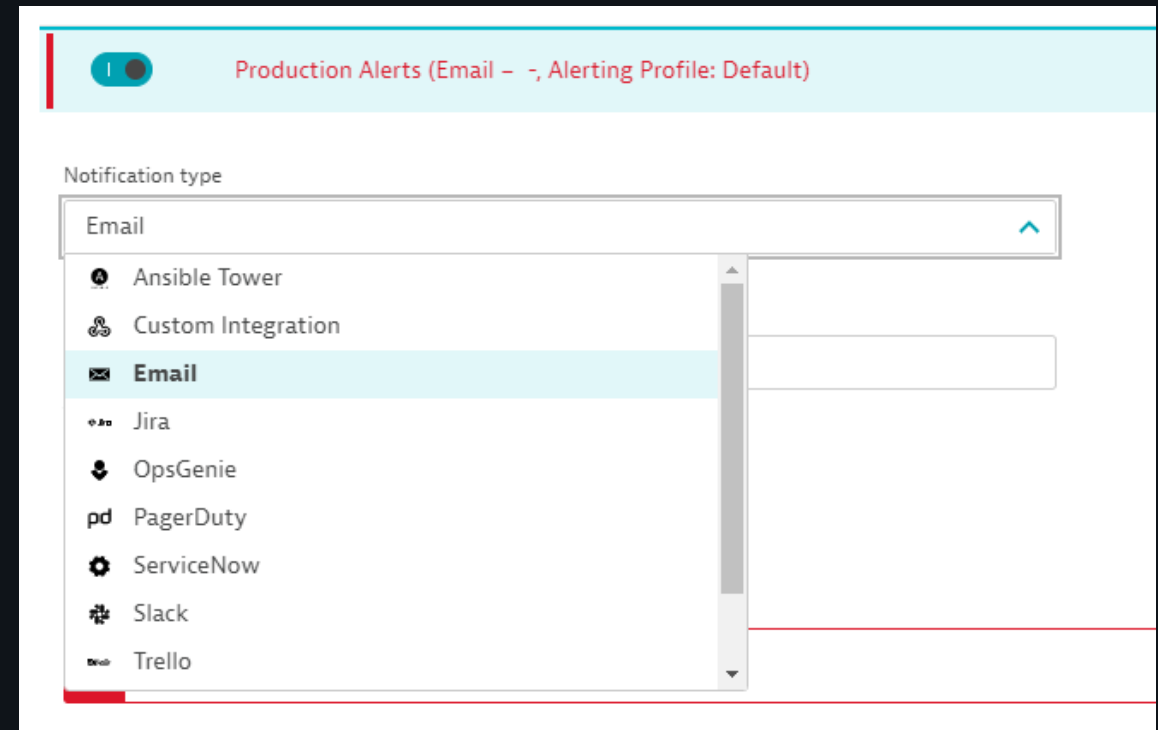
---

- Dynatrace enables the automatic push of problem notifications to third-party incident management or ChatOps services.
- Notifications are configured to use an Alert Profile to filter Problems.
- Open Problems are continuously updated based on correlated events.
- To avoid notification spam, problem notifications are only pushed to third-party systems when problems are initially detected and when they are resolved.
- Additional configuration may be necessary depending on the type of notification integration.
- An email integration or webhook integration might be used if Dynatrace doesn't yet offer an out-of-the-box integration for a specific system

<https://www.dynatrace.com/support/help/shortlink/third-party-integrations-hub#problem-notification>

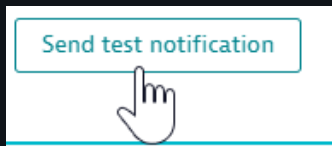
# Notifications

- To create a Notification Integration open Settings->Integration->Problem Notifications and click "Add Notification"
- Select the Notification Type
- Provide a descriptive name for the profile
- Fill in the details for the integration
- Follow the instructions for any additional setup that may be needed:  
<https://www.dynatrace.com/support/help/shortlink/third-party-integrations-hub>



# Notifications

- Customize the information sent to the notification.
  - Placeholders and typed text can be used to customize the message.
- Select the Alerting Profile to use for the notification.
- Be sure to “Send a Test Notification” to ensure the configuration is correct.



Subject

{State} Problem {ProblemID}: {ImpactedEntity}

The subject of the email notifications.

Body

{ProblemDetailsHTML}

The template of the email notifications.

**Available placeholders**

{ImpactedEntity}: Entity impacted by the problem (or x impacted entities when there are multiple).

{PID}: Unique system identifier of the reported problem.

{ProblemID}: Display number of the reported problem.

{ProblemImpact}: Impact level of the problem. Possible values are APPLICATION, SERVICE, or INFRASTRUCTURE.

{ProblemSeverity}: Severity level of the problem. Possible values are AVAILABILITY, ERROR, PERFORMANCE, RESOURCE\_CONTENTION, or CUSTOM\_ALERT.

{ProblemTitle}: Short description of the problem.

{ProblemURL}: URL of the problem within Dynatrace.

{State}: Problem state. Possible values are OPEN or RESOLVED.

{Tags}: Comma separated list of tags that are defined for all impacted entities.

Alerting profile

Default

**Default**

Easy Travel

Prod Alerts

# Maintenance Windows

---

## Maintenance windows


---


- Maintenance Windows can be defined in advance or retroactively
  - In Advanced for regularly scheduled maintenance periods
  - Retroactively for ongoing outages or emergency releases
- Metrics collected during a maintenance window do not become part of the baselines
- Problem handling can be defined
  - If problems are created, the problem card will have a wrench and bolt
- Maintenance windows can be used to stop synthetics
- Maintenance windows can be created for OneAgent updates




<https://www.dynatrace.com/support/help/shortlink/maintenance-window>


# Maintenance Windows

- If you open a problem that occurred during a maintenance window, Dynatrace shows a header on the Problem page

 Maintenance: [SaRe test \(Tuesdays 1400-1430 in August\)](#) (1 more)

 **easytravel dynatrace-dev: User action duration degradation**  
Problem 103 detected at 07:05 (open for 7 hours 35 minutes).  
This problem affects real users.

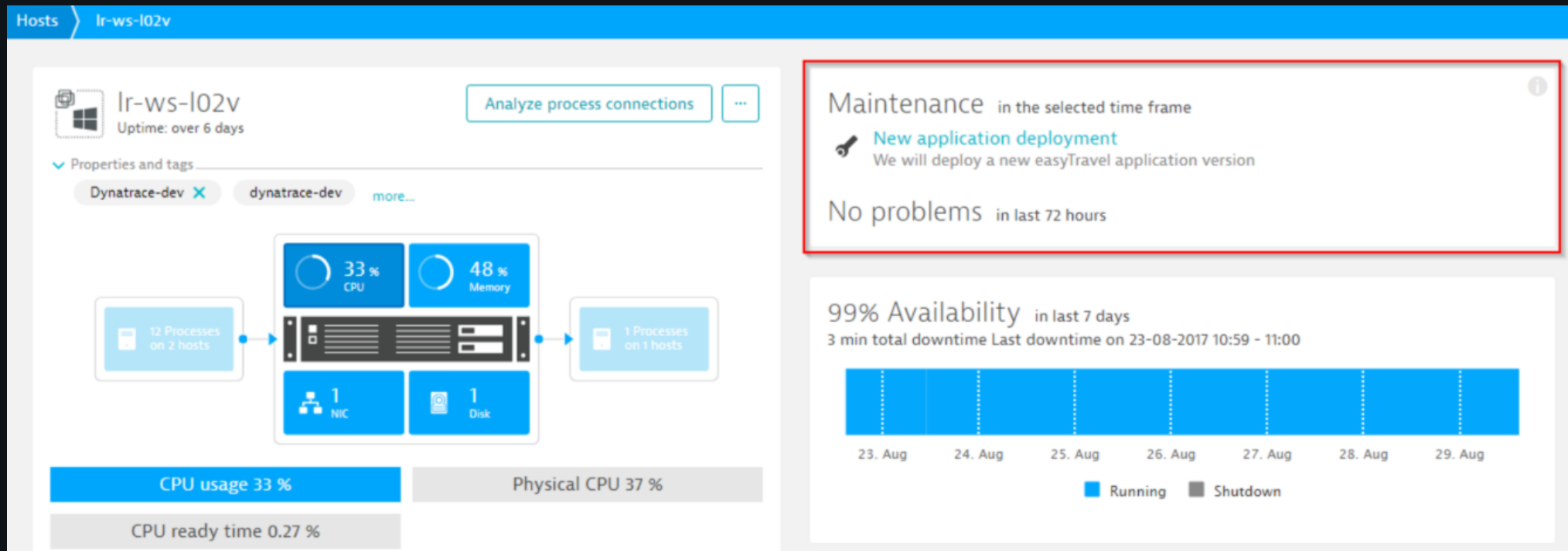
	Affected	Recovered	Monitored
 Applications	1	-	153
 Services	-	2	41
 Infrastructure components	-	1	3,282

  
3,582,309,564  
Dependencies analyzed



# Maintenance Windows

- Even if you aren't within a problem context and you select a timeframe in which a selected host was under maintenance, Dynatrace shows you the details on the Maintenance tile



# Maintenance windows

- To create a maintenance window open Settings -> Maintenance Windows -> "Monitoring, alerting and availability" and click "Create a Maintenance Window"
- Add a Name, Type and Description
- Select the schedule for the window
  - the actual time for the maintenance window
  - the dates it is in effect.

<https://www.dynatrace.com/support/help/shortlink/maintenance-window-define>

**Configured maintenance windows**

Name your maintenance window:

Maintenance type: **Planned** (dropdown menu open showing Planned and Unplanned)

Description:

Recurrence: **Day of week** (dropdown menu open showing Daily, Day of week, Day of month, and Once only)

Day of the week: **Sunday** (dropdown menu)

starting at:

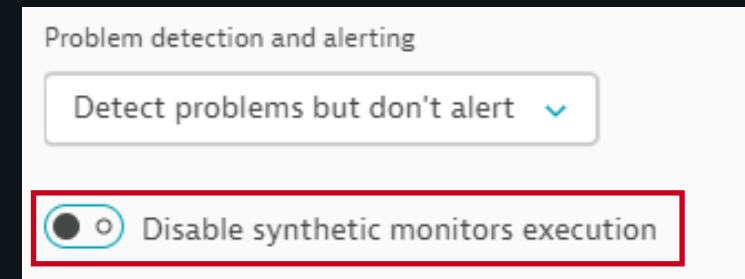
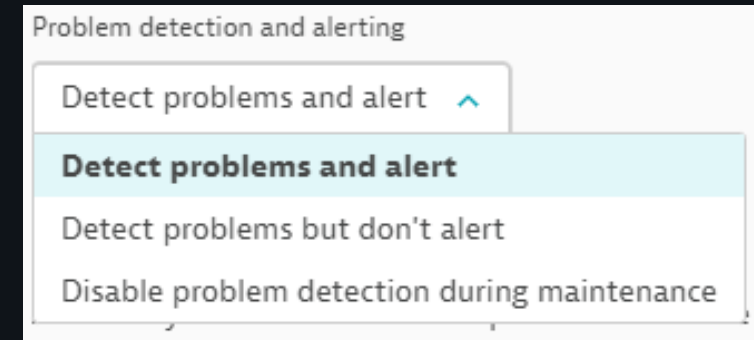
ending at:

Recurrence range start:

Recurrence range end:

# Maintenance windows

- Select how Problems will be handled.
  - Detect problems and alert: Problems are detected as usual. A maintenance window icon is displayed on the problem.
  - Detect problems but don't alert: Problems are detected but no notification is sent. A maintenance window icon is displayed on the problem.
  - Disable problem detection: Dynatrace will not detect problems or send out alerts for them.
- Select whether synthetics monitors (Browser or HTTP) should be executed during the maintenance window.
  - To only disabling Synthetic Monitors the scope must include the monitors in the entity and/or tag filters.
  - Execution will be disabled only for the matching synthetics.



# Maintenance windows

- By default, a maintenance window applies to the entire environment.
- Entities Filter – add if needed
  - Select the type of entity to be included in the Maintenance Window.
  - Narrow the list by selecting a specific entity names. These will be applied using and “OR” logic.
- Tags Filter – add if needed
  - Select an entity type if needed or use all entities.
  - Select the tag and/or value to filter against. Multiple tags on the same line are applied using “AND” logic.
- Use the Preview to see what would be included in the Maintenance Window.
- Save the changes when complete

**Add entity filters** to limit the scope of maintenance to only select entities, such as specific applications, services, or hosts. If no scope is defined, the maintenance window is valid for the whole environment. Each entity filter matches all of its properties (**OR**).

Hosts	Host: Prod_DT-SaaS - ag-plugi...	X
All entities	Host: Prod_EasyTravel - ETSvr ...	X
Hosts	Filter for entity names	X

[Add entity filter](#)

This maintenance window affects:

Hosts: Prod\_DT-SaaS - ag-plugins - CentOS Linux 7

**OR**

Hosts: Prod\_EasyTravel - ETSvr - Windows Server 2012 R2 Standard

**OR**

all hosts

**Add tag filters** to limit the scope of maintenance to only select entities with specific tags. If no scope is defined, the maintenance window is valid for the whole environment. Each tag filter matches all of its properties (**AND**) and multiple entity filters are evaluated separately (**OR**).

All entities	Environment: Prod	Application: EasyTravel	X
Hosts	Environment: Prod		X

[Add entity tag filter](#)

This maintenance window affects:

Tags:

All entities which match tags - "Environment:Prod" and "Application:EasyTravel"

**OR**

Hosts which match the tag - "Environment:Prod"

# Maintenance windows

- OneAgent Maintenance Windows are used in conjunction with the OneAgent update option.
- First – create a OneAgent Maintenance Window at Settings -> Maintenance Windows -> OneAgent Updates
- Specify the options and save the changes when complete.
- Select the Maintenance window in the update options at Settings -> Preferences -> OneAgent Updates.
- Save the changes when complete.

The screenshot shows the 'Weekly OA Update every 4 weeks - Weekly intervals' configuration page. The 'Name' field is highlighted with a red box and contains the text 'Weekly OA Update every 4 weeks'. The 'Recurrence' dropdown is set to 'Weekly intervals'. The 'Day of the week' section shows 'Saturday' selected. The 'Every X weeks' field is set to '4'. The 'Update time' section shows 'Start time (24-hour clock)' set to '21:00'. The 'Time zone' dropdown is set to 'GMT-05:00'. The 'Duration (minutes)' field is set to '360'. The 'Recurrence range' section shows 'Start' as '2021-08-20 00:00:00 GMT00:00' and 'End' as '2025-08-20 00:00:00 GMT00:00'.

The screenshot shows the 'OneAgent updates' configuration page. The 'Automatic updates during maintenance windows' option is selected and highlighted with a red box. The 'Maintenance window' dropdown is set to 'Weekly OA Update every 4 weeks' and is also highlighted with a red box. The 'Save changes' button is visible at the bottom right.

# Questions?

---



---

Simply smarter clouds