User Management

Dynatrace Training Module

dynatrace

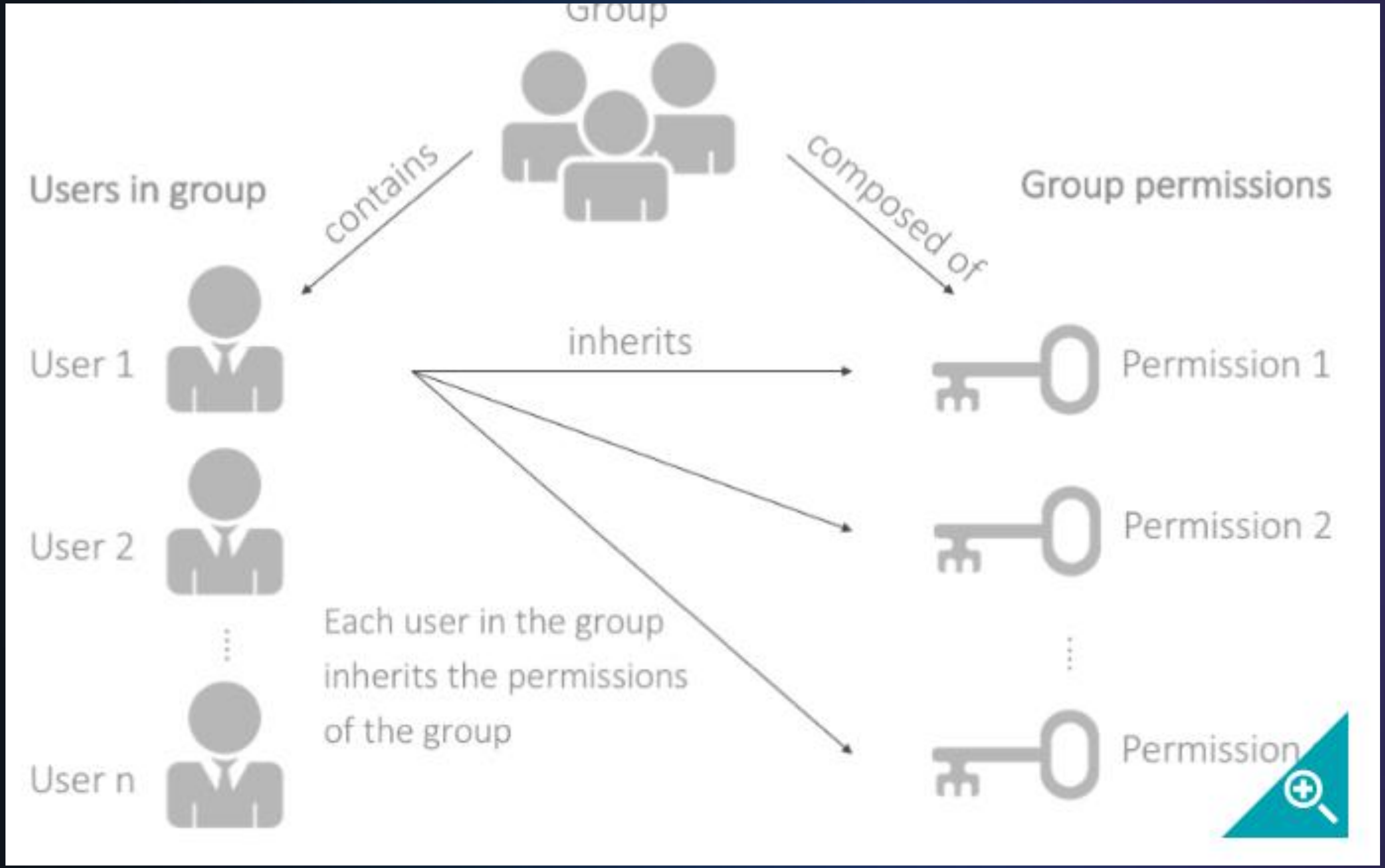
Agenda

- Overview
- Permissions
  - Environment Permissions
  - Management Zone Permissions
- Managing Groups and Users

Overview

Overview

- The permission management system is based on groups
  - Reflecting Unix- and Windows-based permissions
- It enables you to create groups that have pre-defined (fully customizable) permissions sets
  - Users added to a group inherit the permissions of that group



Permissions

Permissions

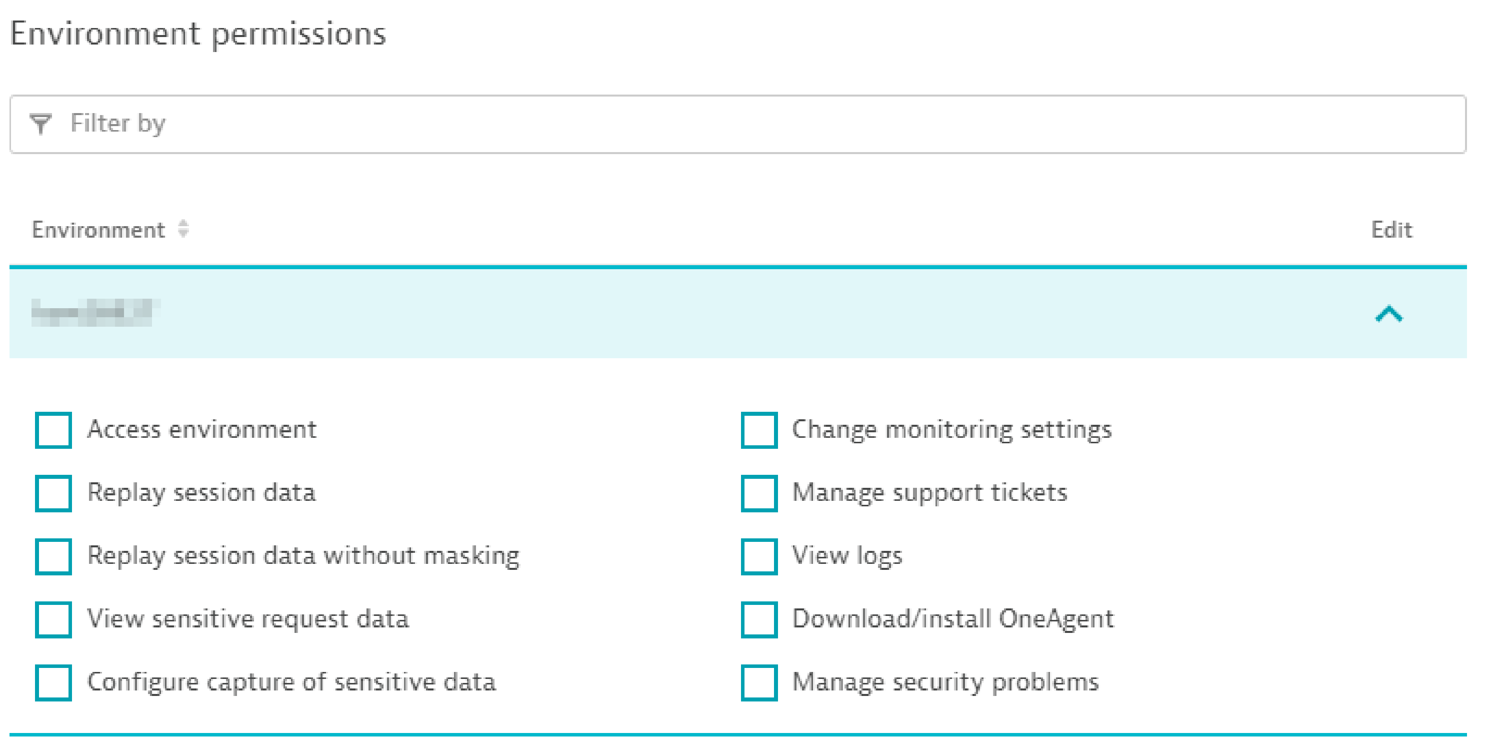
- Each user group is assigned a set of permissions.
- Each user account is assigned to one or more user groups.
- Each user assigned to a group inherits the permissions of that group.
- When you change the permissions of a group, the permissions of each user in that group change accordingly.
- When you assign a user to multiple groups, the user inherits the combined permissions of all those groups. Groups are fully customizable and can be modified to contain any permission you require for a specific group
- Even the default groups can be modified to meet your needs

https://www.dynatrace.com/support/help/shortlink/users-sso-hub

Environment Permissions

Environment Permissions

- Managed and SaaS Environment Permissions
  - https://www.dynatrace.com/support/help/shortlink/user-groups-setup#environment-permissions-



Environment permissions

Filter by

Environment — Edit

[redacted]

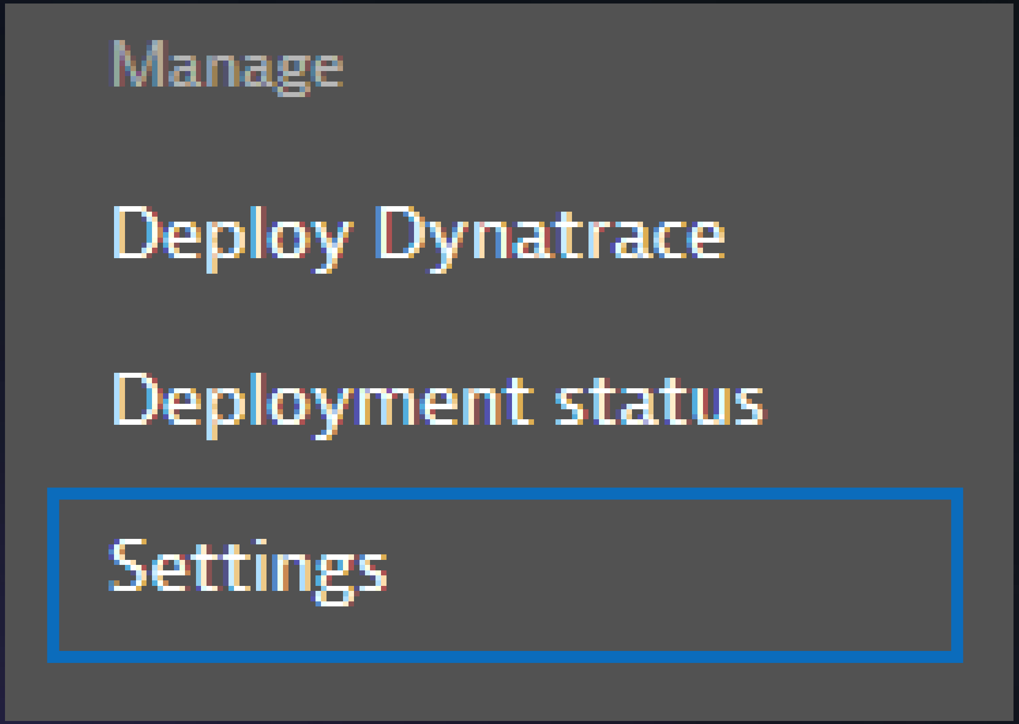
□ Access environment
□ Replay session data
□ Replay session data without masking
□ View sensitive request data
□ Configure capture of sensitive data
□ Change monitoring settings
□ Manage support tickets
□ View logs
□ Download/install OneAgent
□ Manage security problems

Environment Permissions

- Access Environment
  - Allows read-only access to the environment. Can’t change settings. Can’t install OneAgent
  - The Access Environment Permissions allow the users to do the following:
    - View the monitored data
    - View Dynatrace reports
    - Build, clone, & share dashboards
    - Create custom charts
    - Add/Remove key user actions

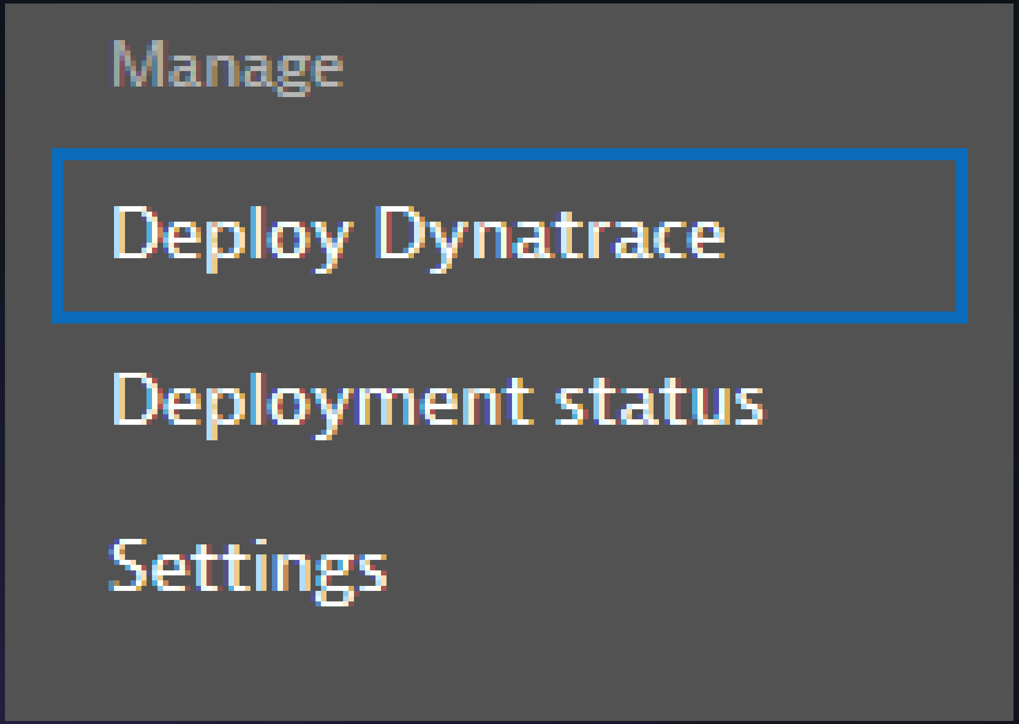
Environment Permissions

- Change monitoring settings
    - Can change all Dynatrace monitoring settings. Can't install OneAgent



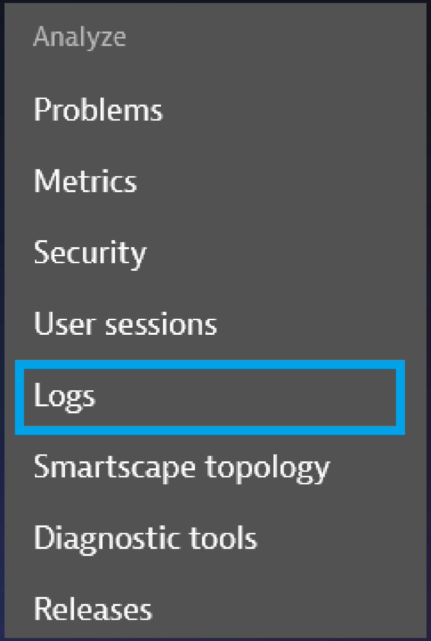
Environment Permissions

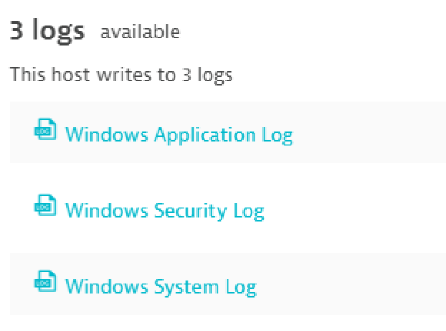
- Download & install OneAgent
  - Allows download and installation of OneAgent on hosts. Can't change Dynatrace monitoring settings



Environment Permissions

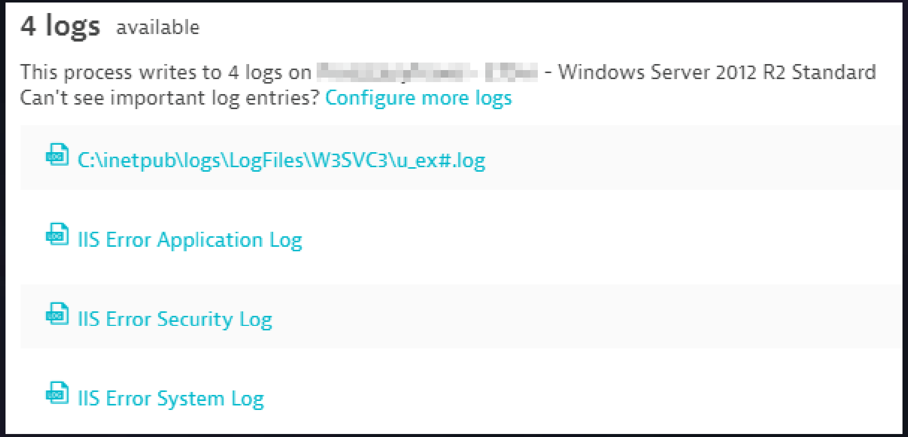
- View logs
  - Allows access to log file content, which may contain sensitive information
- Log file data can be masked by the OneAgent prior to being seen in the UI or stored on the Dynatrace Server
  - https://www.dynatrace.com/support/help/shortlink/log-analytics-mask-info#mask-personal-data




3 logs available

This host writes to 3 logs

- Windows Application Log
- Windows Security Log
- Windows System Log

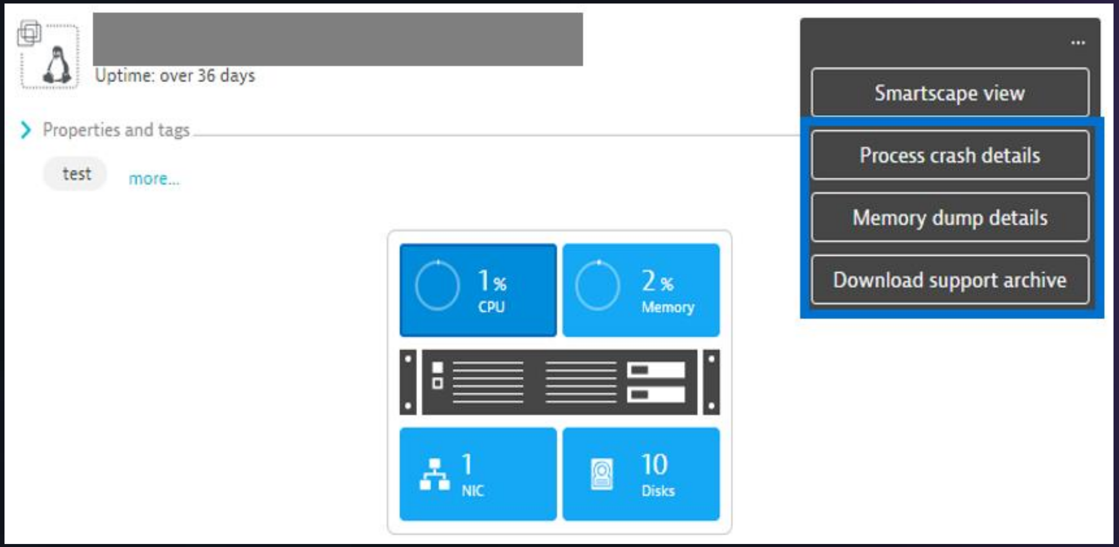

4 logs available

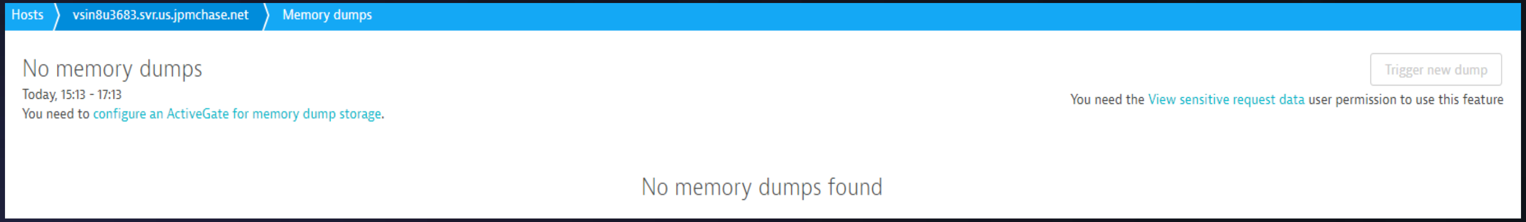
This process writes to 4 logs on [redacted] - Windows Server 2012 R2 Standard
Can't see important log entries? Configure more logs

- C:\inetpub\logs\LogFiles\W3SVC3\u_ex#.log
- IIS Error Application Log
- IIS Error Security Log
- IIS Error System Log

Environment Permissions

- View sensitive request data
  - Allows viewing of potentially sensitive data
  - Users who do not have this permission see that the data point exists, but the personal data is masked by asterisks (*****)
  - See details of what is considered sensitive on next slide





Hosts 〉 vsin8u3683.svr.us.jpmchase.net 〉 Memory dumps

No memory dumps

Today, 15:13 - 17:13

You need to configure an ActiveGate for memory dump storage.

Trigger new dump

You need the View sensitive request data user permission to use this feature

No memory dumps found

Sensitive Data

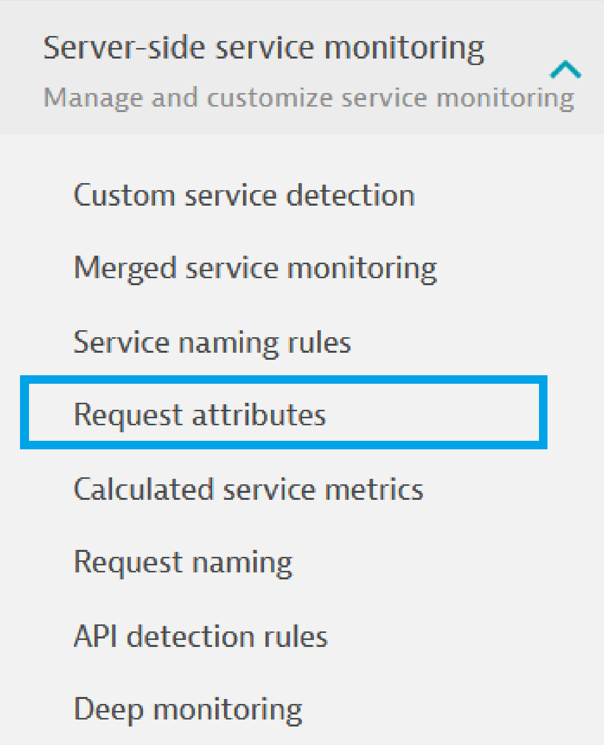
- Dynatrace will automatically classify certain data items as sensitive
- This includes things like client IP addresses, Exception messages, URL query parameters, HTTP Headers/post parameters and extends to certain patterns in exception messages like GUIDs
- Support archives and memory dumps are considered sensitive data
- Users can configure the capture of additional data, which will require the user to have the permission to do so (Configure capture of sensitive data)
  - The User will be able to explicitly designate these newly captured data points as sensitive or non sensitive
- OneAgent diagnostics and memory dumps are also considered sensitive data

  https://www.dynatrace.com/support/help/shortlink/sensitive-data

  https://www.dynatrace.com/support/help/shortlink/section-data-privacy-and-security

Environment Permissions

- Configure capture of sensitive data
  - Allows configuration of request-attribute capture rules. These can be used to capture elements such as HTTP headers or Post parameters for storage, filtering, and search.
  - Also allows manually triggering memory dumps. Captured request data can be stored, filtered, and searched

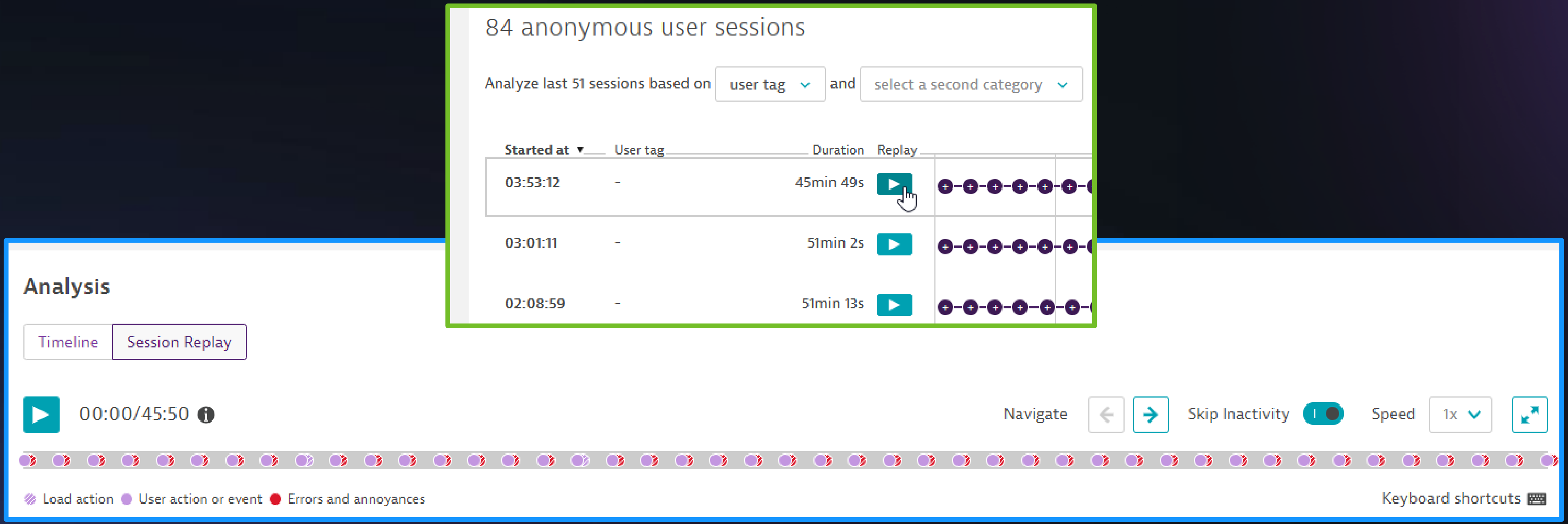


Server-side service monitoring

Manage and customize service monitoring

Environment Permissions

- Replay session data
  - Allows replaying recorded user sessions with playback masking rules applied at the time of *playback*.
    - Note: Any data masked at time of *recording* is never captured, therefore, always masked during play.



84 anonymous user sessions

Analyze last 51 sessions based on user tag and select a second category

Started at ▼	User tag	Duration	Replay
03:53:12	-	45min 49s	▶
03:01:11	-	51min 2s	▶
02:08:59	-	51min 13s	▶

Analysis

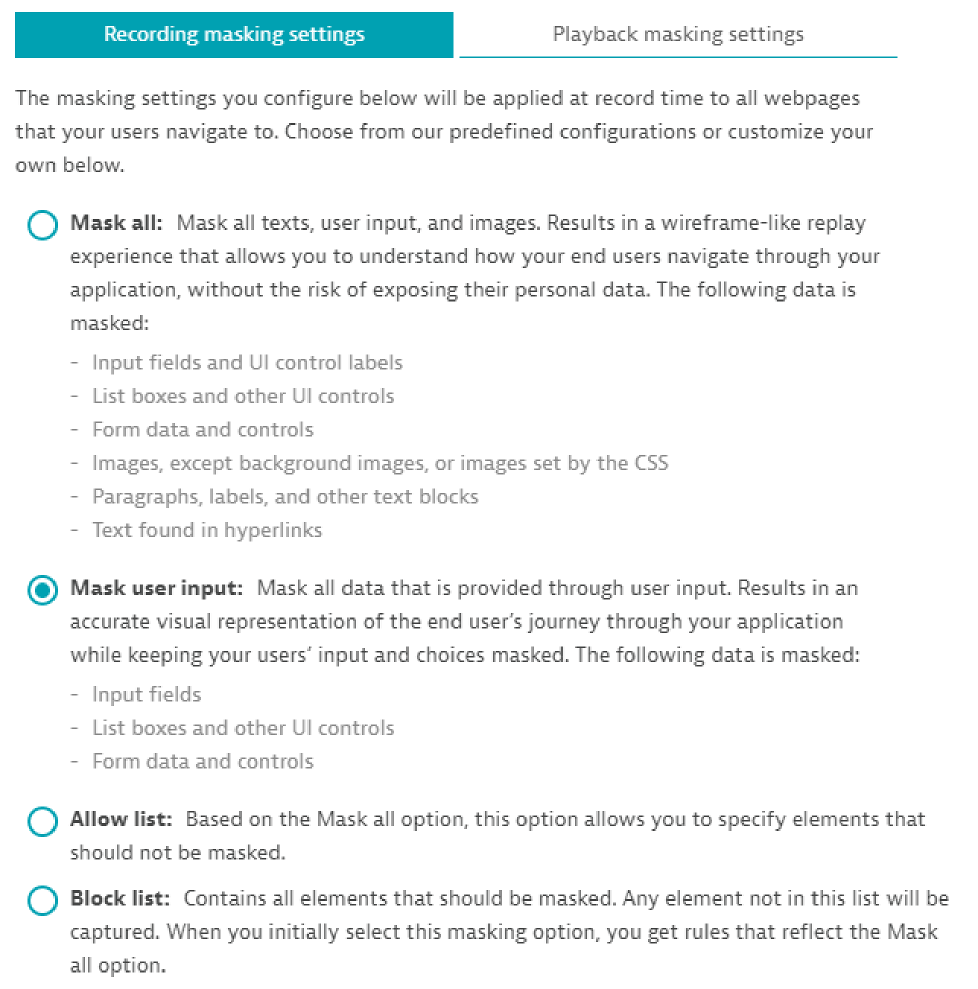
Timeline | Session Replay

▶ 00:00/45:50

▨ Load action ● User action or event ● Errors and annoyances

Environment Permissions

- Replay session data without masking
  - Allows replaying recorded user sessions without playback masking rules applied.
    - Note: Any data masked at time of *recording* is never captured, therefore, always masked during play.
  - Recording and Playback masking rules are set within each application



The masking settings you configure below will be applied at record time to all webpages that your users navigate to. Choose from our predefined configurations or customize your own below.

○ **Mask all:** Mask all texts, user input, and images. Results in a wireframe-like replay experience that allows you to understand how your end users navigate through your application, without the risk of exposing their personal data. The following data is masked:

- Input fields and UI control labels
- List boxes and other UI controls
- Form data and controls
- Images, except background images, or images set by the CSS
- Paragraphs, labels, and other text blocks
- Text found in hyperlinks

● **Mask user input:** Mask all data that is provided through user input. Results in an accurate visual representation of the end user's journey through your application while keeping your users' input and choices masked. The following data is masked:

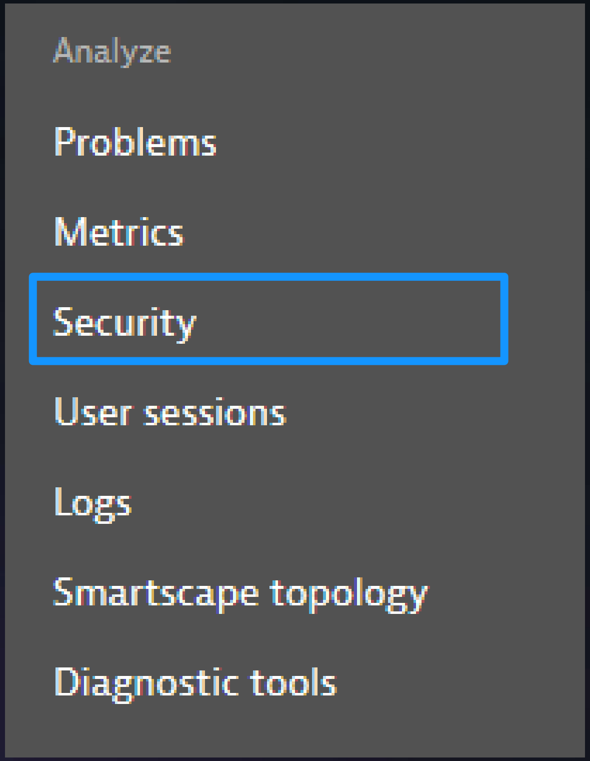
- Input fields
- List boxes and other UI controls
- Form data and controls

○ **Allow list:** Based on the Mask all option, this option allows you to specify elements that should not be masked.

○ **Block list:** Contains all elements that should be masked. Any element not in this list will be captured. When you initially select this masking option, you get rules that reflect the Mask all option.

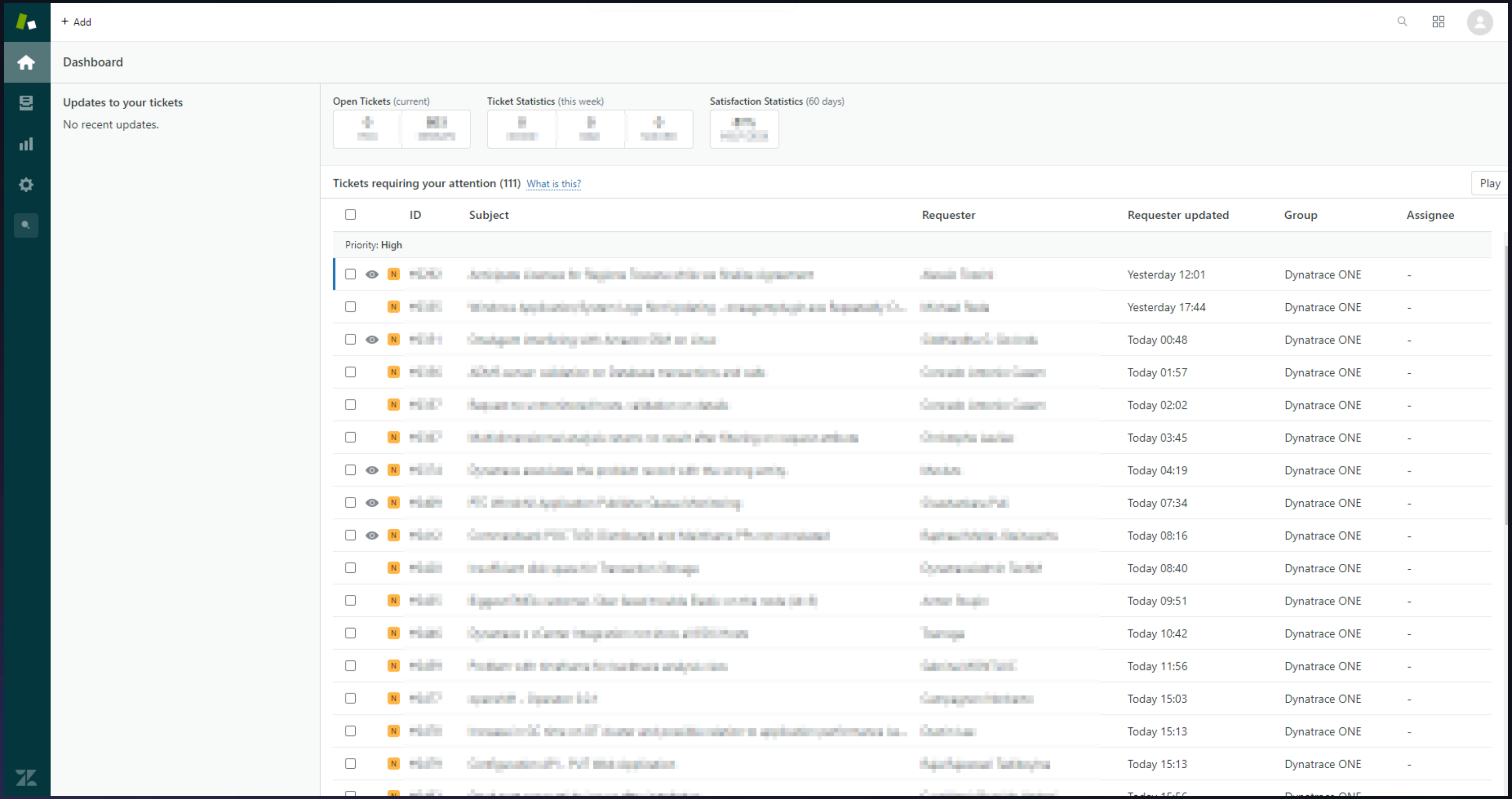
Environment Permissions

- Manage security problems
  - Allows management of problems reported by Dynatrace Application Security



Environment Permissions

- Manage Support Tickets
  - Allows access to all support tickets that have been created for this environment.



Updates to your tickets

No recent updates.

Open Tickets (current) [redacted]

Ticket Statistics (this week) [redacted]

Satisfaction Statistics (60 days) [redacted]

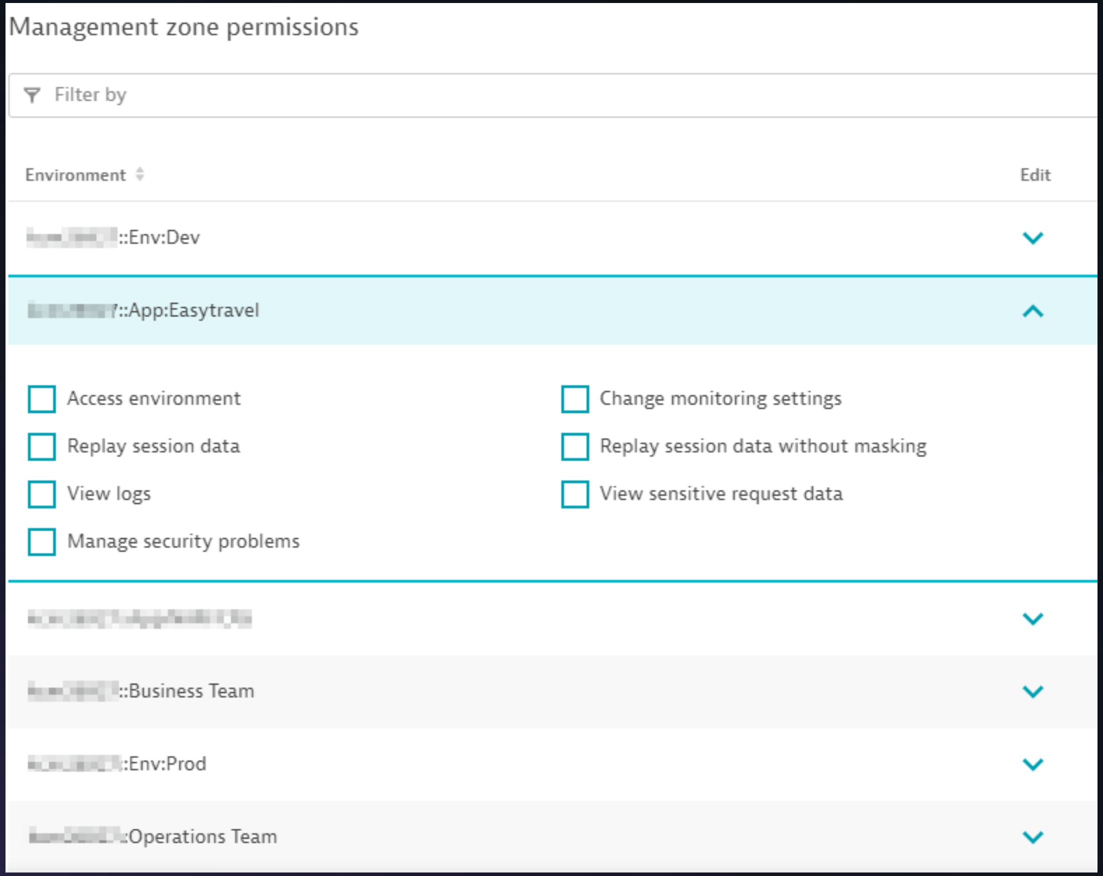
Tickets requiring your attention (111) What is this?

☐	ID	Subject	Requester	Requester updated	Group	Assignee
Priority: High						
☐ 👁 N	[redacted]	[redacted]	[redacted]	Yesterday 12:01	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Yesterday 17:44	Dynatrace ONE	-
☐ 👁 N	[redacted]	[redacted]	[redacted]	Today 00:48	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 01:57	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 02:02	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 03:45	Dynatrace ONE	-
☐ 👁 N	[redacted]	[redacted]	[redacted]	Today 04:19	Dynatrace ONE	-
☐ 👁 N	[redacted]	[redacted]	[redacted]	Today 07:34	Dynatrace ONE	-
☐ 👁 N	[redacted]	[redacted]	[redacted]	Today 08:16	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 08:40	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 09:51	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 10:42	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 11:56	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 15:03	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 15:13	Dynatrace ONE	-
☐ N	[redacted]	[redacted]	[redacted]	Today 15:13	Dynatrace ONE	-

Management Zone Permissions

Management Zone Permissions

- Management Zone Permissions
  - https://www.dynatrace.com/support/help/shortlink/user-groups-setup#management-zone-permissions-



Management zone permissions

Filter by

Environment ⇕ Edit

[redacted]::Env:Dev ⌄

[redacted]::App:Easytravel ⌃

□ Access environment
□ Replay session data
□ View logs
□ Manage security problems
□ Change monitoring settings
□ Replay session data without masking
□ View sensitive request data

[redacted] ⌄

[redacted]::Business Team ⌄

[redacted]:Env:Prod ⌄

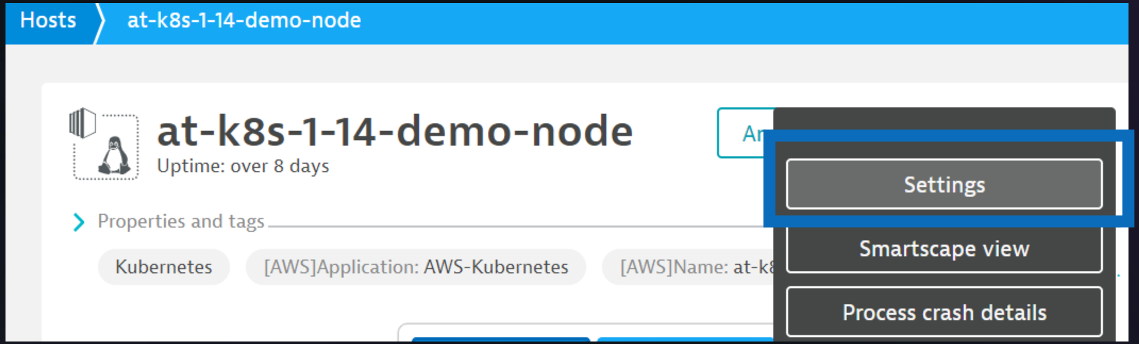
[redacted]:Operations Team ⌄

Management Zone Permissions

- Access Environment
  - Allows read-only access to the entities within the Management Zone. Can’t change settings. Can’t install OneAgent.
  - The Access Environment Permission on the Management Zone allow the users to do the following:
    - View the monitored data
    - View Dynatrace reports
    - Build, clone, & share dashboards
    - Create custom charts
    - Add/Remove key requests
  - “Access Environment” is automatically selected for the management zone when you select any other management zone permission.

Management Zone Permissions

- Change monitoring settings
  - Can change entity monitoring settings for the entities within the Management Zone.
  - Create Synthetic Monitors in the Management Zone.
  - No Access to Environment Settings



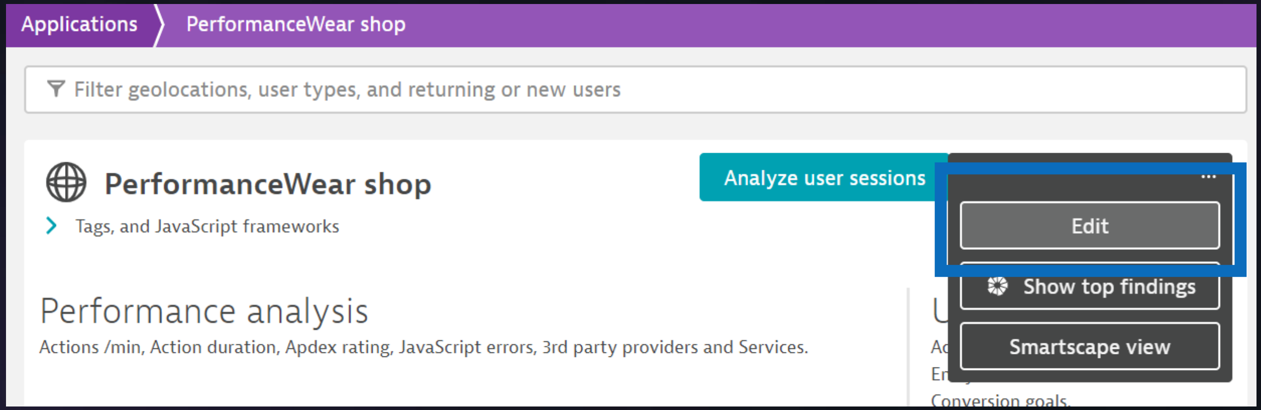
Hosts 〉 at-k8s-1-14-demo-node

at-k8s-1-14-demo-node

Uptime: over 8 days

Properties and tags

Kubernetes [AWS]Application: AWS-Kubernetes [AWS]Name: at-k8



Applications 〉 PerformanceWear shop

Filter geolocations, user types, and returning or new users

PerformanceWear shop

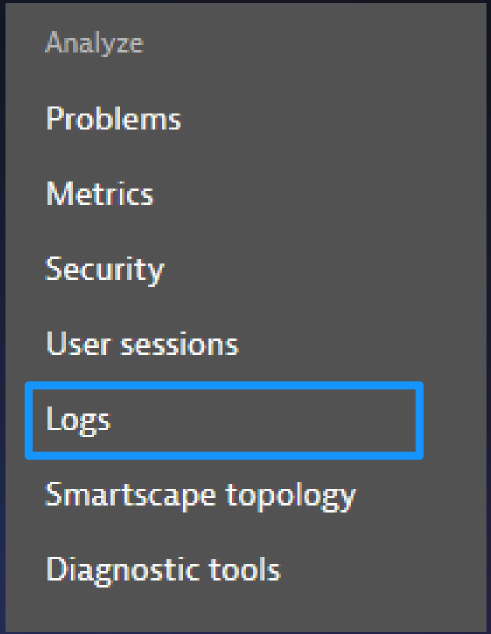
Tags, and JavaScript frameworks

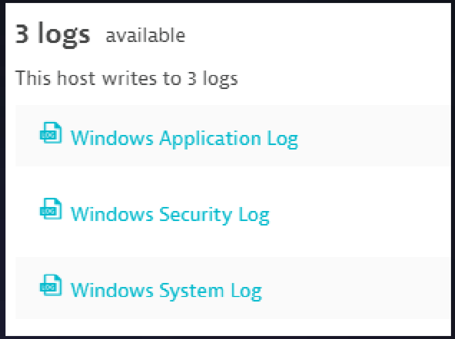
Performance analysis

Actions /min, Action duration, Apdex rating, JavaScript errors, 3rd party providers and Services.

Management Zone Permissions

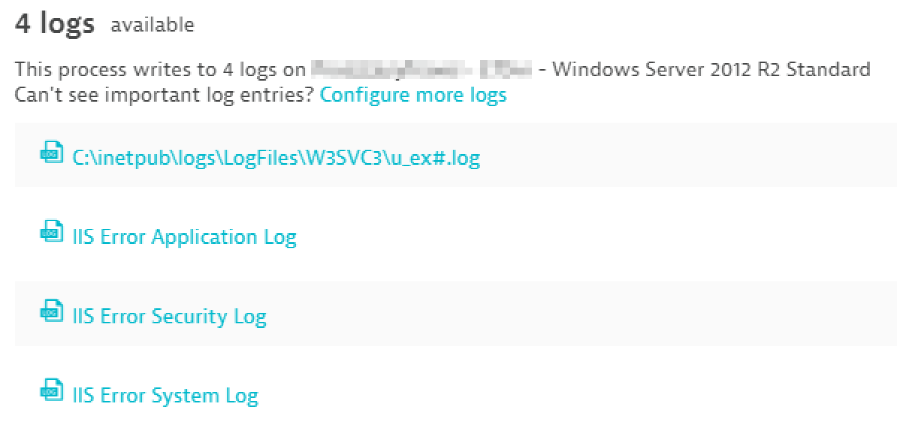
- View logs
  - Allows access to log file content for entities within the Management Zone, which may contain sensitive information
- Log file data can be masked by the OneAgent prior to being seen in the UI or stored on the Dynatrace Server
  - https://www.dynatrace.com/support/help/shortlink/log-analytics-mask-info#mask-personal-data




3 logs available

This host writes to 3 logs

- Windows Application Log
- Windows Security Log
- Windows System Log

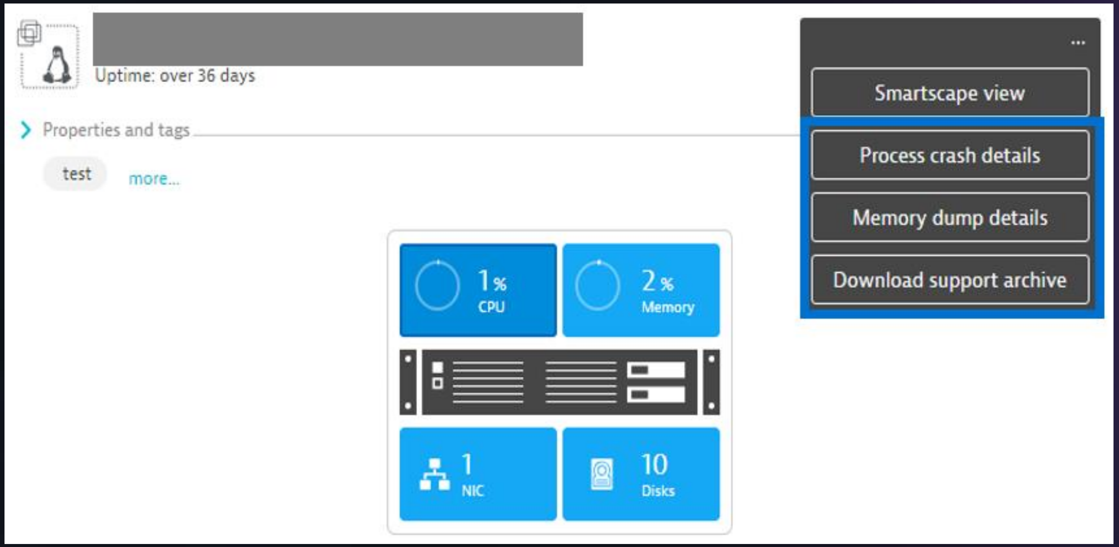

4 logs available

This process writes to 4 logs on [redacted] - Windows Server 2012 R2 Standard
Can't see important log entries? Configure more logs

- C:\inetpub\logs\LogFiles\W3SVC3\u_ex#.log
- IIS Error Application Log
- IIS Error Security Log
- IIS Error System Log

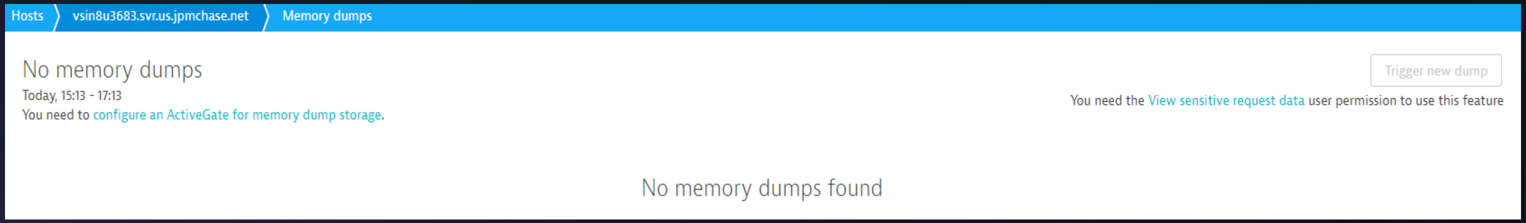
Management Zone Permissions

- View sensitive request data
  - Allows viewing of potentially sensitive data
  - Users who do not have this permission see that the data point exists, but the personal data is masked by asterisks (*****)
  - See details of what is considered sensitive on next slide



[redacted]

Uptime: over 36 days



No memory dumps

Today, 15:13 - 17:13

You need to configure an ActiveGate for memory dump storage.

You need the View sensitive request data user permission to use this feature

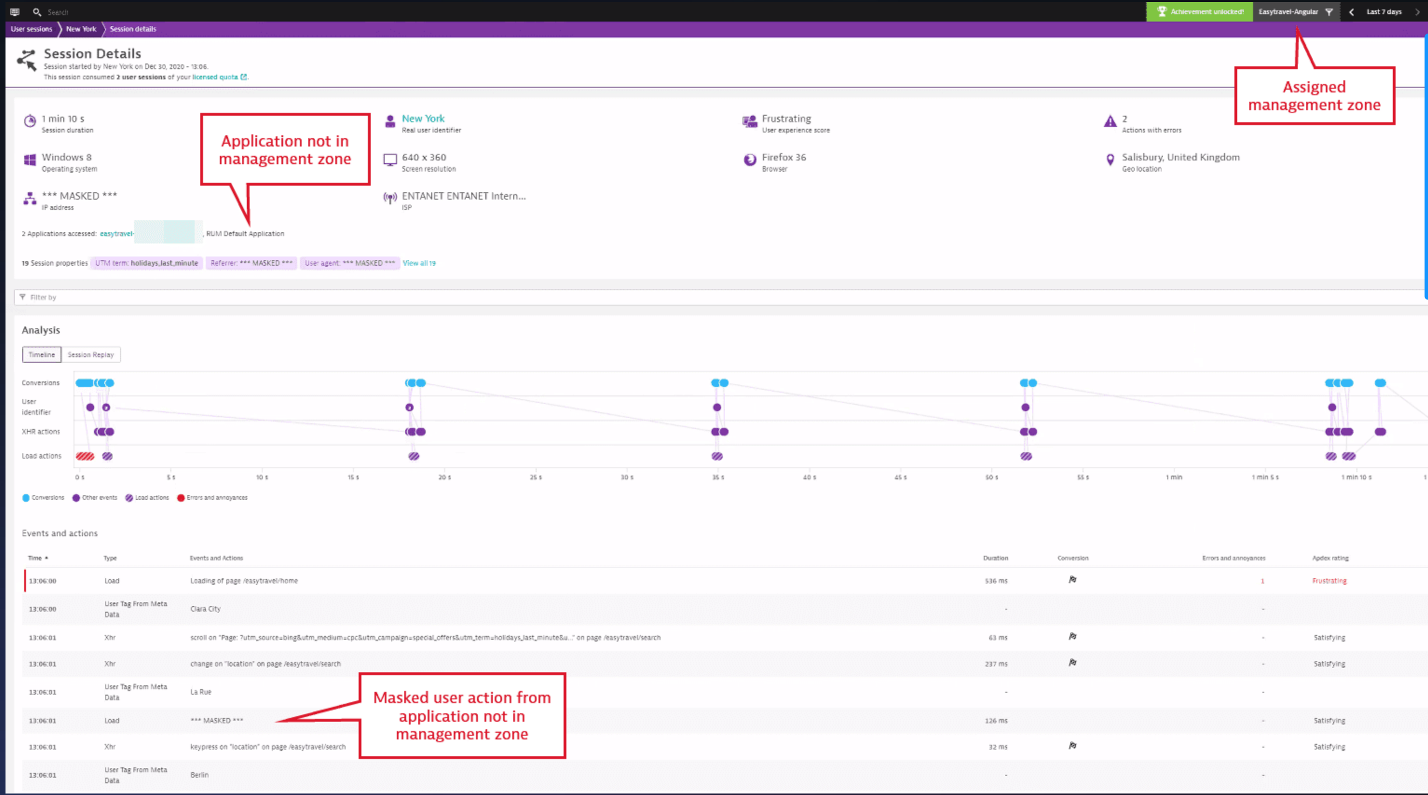
No memory dumps found

Sensitive Data

- Dynatrace will automatically classify certain data items as sensitive
- This includes things like client IP addresses, Exception messages, URL query parameters, HTTP Headers/post paramters and extends to certain patterns in exception messages like GUIDs
- Users are able to configure the capture of additional data, which will require the user to have the permission to do so (Configure capture of sensitive data)
    - The User will be able to explicitly designate these newly captured data points as sensitive or non sensitive
- OneAgent diagnostics and memory dumps are also considered sensitive data
- https://www.dynatrace.com/support/help/shortlink/sensitive-data
- https://www.dynatrace.com/support/help/shortlink/section-data-privacy-and-security

Management Zone Permissions

- Replay session data
  - Allows replaying recorded user sessions with playback masking rules applied at the time of *playback*.
    - Note: Any data masked at time of *recording* is never captured, therefore, always masked during play.
  - Applications outside of the user's assigned management zone will have user actions masked.



Assigned management zone

Session Details

Session started by New York on Dec 30, 2020 - 13:06.
This session consumed **2 user sessions** of your licensed quota.

1 min 10 s	Session duration
Windows 8	Operating system
*** MASKED ***	IP address
New York	Real user identifier
640 x 360	Screen resolution
ENTANET ENTANET Intern...	ISP
Frustrating	User experience score
Firefox 36	Browser
2	Actions with errors
Salisbury, United Kingdom	Geo location

Application not in management zone

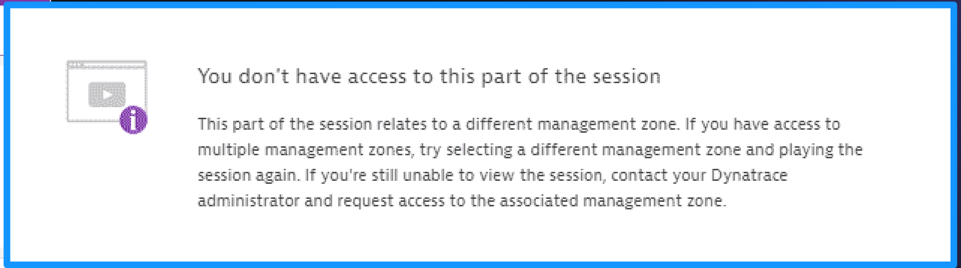
2 Applications accessed: easytravel-[redacted], RUM Default Application

19 Session properties: UTM term: holidays_last_minute | Referrer: *** MASKED *** | User agent: *** MASKED *** | View all 19

Events and actions

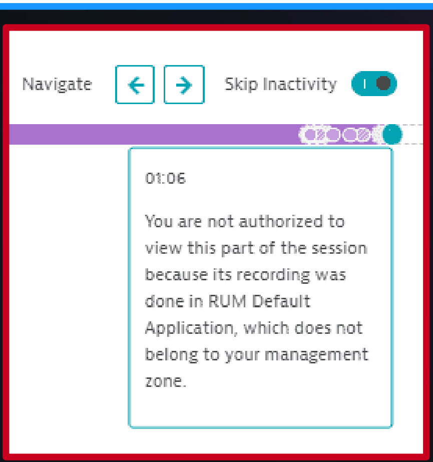
Time ▲	Type	Events and Actions	Duration	Conversion	Errors and annoyances	Apdex rating	Details
13:06:00	Load	Loading of page /easytravel/home	536 ms	🏁	1	Frustrating	⌄
13:06:00	User Tag From Meta Data	Clara City	-		-		⌄
13:06:01	Xhr	scroll on "Page: ?utm_source=bing&utm_medium=cpc&utm_campaign=special_offers&utm_term=holidays_last_minute&u..." on page /easytravel/search	63 ms	🏁	-	Satisfying	⌄
13:06:01	Xhr	change on "location" on page /easytravel/search	237 ms	🏁	-	Satisfying	⌄
13:06:01	User Tag From Meta Data	La Rue	-		-		⌄
13:06:01	Load	*** MASKED ***	126 ms		-	Satisfying	⌄
13:06:01	Xhr	keypress on "location" on page /easytravel/search	32 ms	🏁	-	Satisfying	⌄
13:06:01	User Tag From Meta Data	Berlin	-		-		⌄

Masked user action from application not in management zone



You don't have access to this part of the session

This part of the session relates to a different management zone. If you have access to multiple management zones, try selecting a different management zone and playing the session again. If you're still unable to view the session, contact your Dynatrace administrator and request access to the associated management zone.

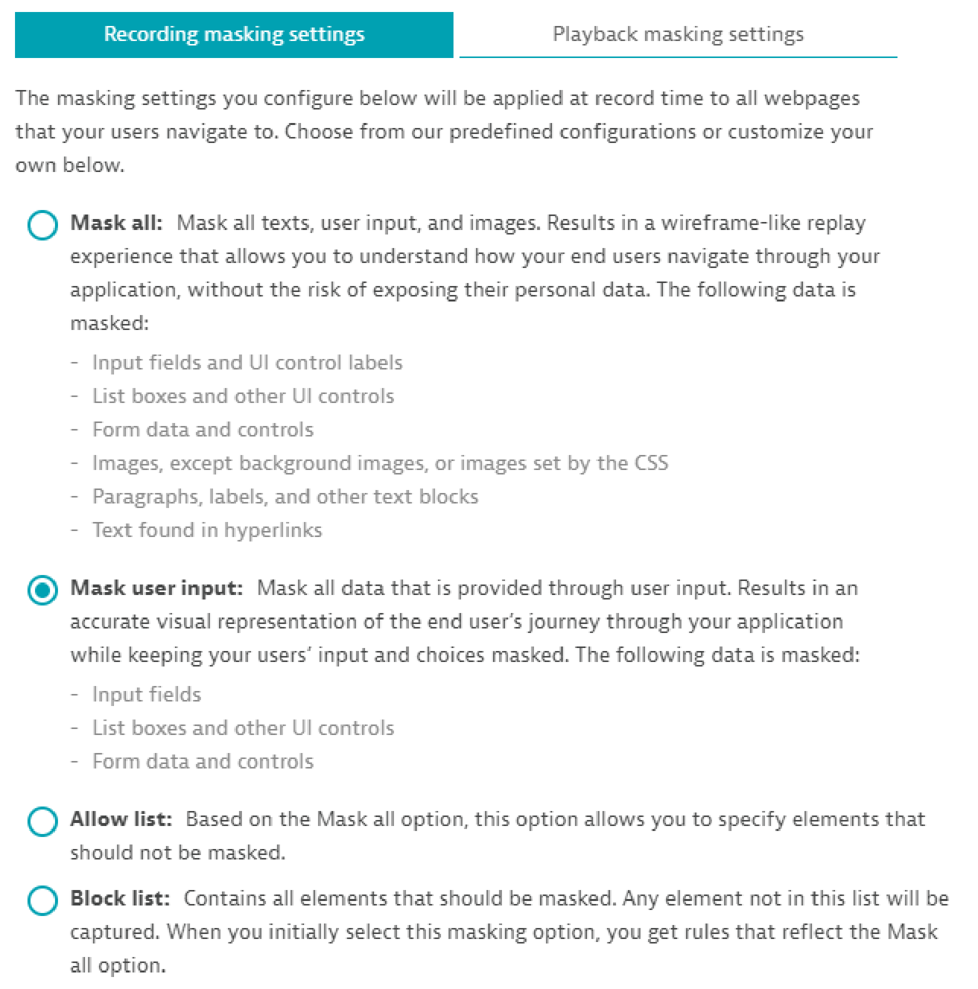


01:06

You are not authorized to view this part of the session because its recording was done in RUM Default Application, which does not belong to your management zone.

Management Zone Permissions

- Replay session data without masking
  - Allows replaying recorded user sessions without playback masking rules applied.
    - Note: Any data masked at time of *recording* is never captured, therefore, always masked during play.
  - Applications outside of the user's assigned management zone will have user actions masked.
  - Recording and Playback masking rules are set within each application



The masking settings you configure below will be applied at record time to all webpages that your users navigate to. Choose from our predefined configurations or customize your own below.

○ **Mask all:** Mask all texts, user input, and images. Results in a wireframe-like replay experience that allows you to understand how your end users navigate through your application, without the risk of exposing their personal data. The following data is masked:

- Input fields and UI control labels
- List boxes and other UI controls
- Form data and controls
- Images, except background images, or images set by the CSS
- Paragraphs, labels, and other text blocks
- Text found in hyperlinks

● **Mask user input:** Mask all data that is provided through user input. Results in an accurate visual representation of the end user's journey through your application while keeping your users' input and choices masked. The following data is masked:

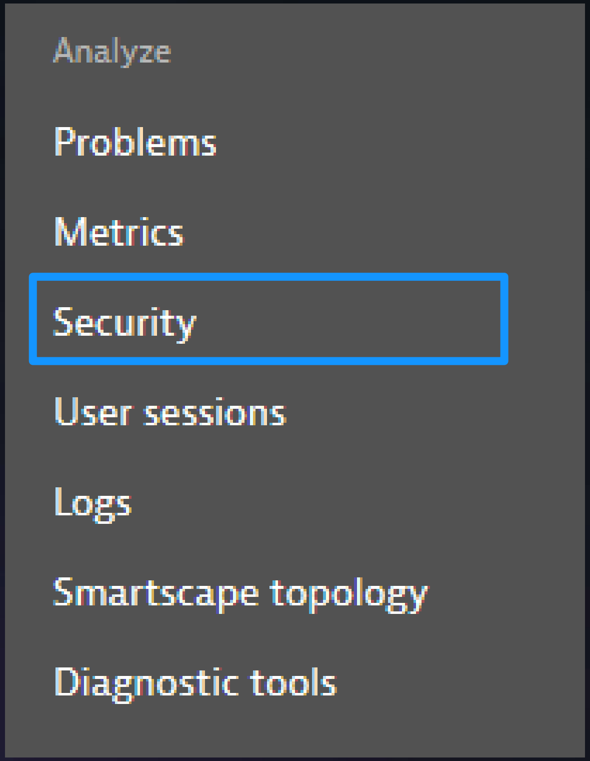
- Input fields
- List boxes and other UI controls
- Form data and controls

○ **Allow list:** Based on the Mask all option, this option allows you to specify elements that should not be masked.

○ **Block list:** Contains all elements that should be masked. Any element not in this list will be captured. When you initially select this masking option, you get rules that reflect the Mask all option.

Management Zone Permissions

- Manage security problems
  - Allows management of problems reported by Dynatrace Application Security



Manage Groups and Users

Managing Users and Groups

- Your AD Administrators are responsible for creating roles and assigning users to those roles. Allowing internal management of individual user access.
- If changes to AD Role (group) Permissions or New AD Roles are required, send a request to Dynatrace (team-devops-fedramp@dynatrace.com) with a list of exact Role Names and Permissions (including Management Zones, if applicable).

Questions?

dynatrace

Simply smarter clouds