Log Analytics

Dynatrace Training Module

dynatrace

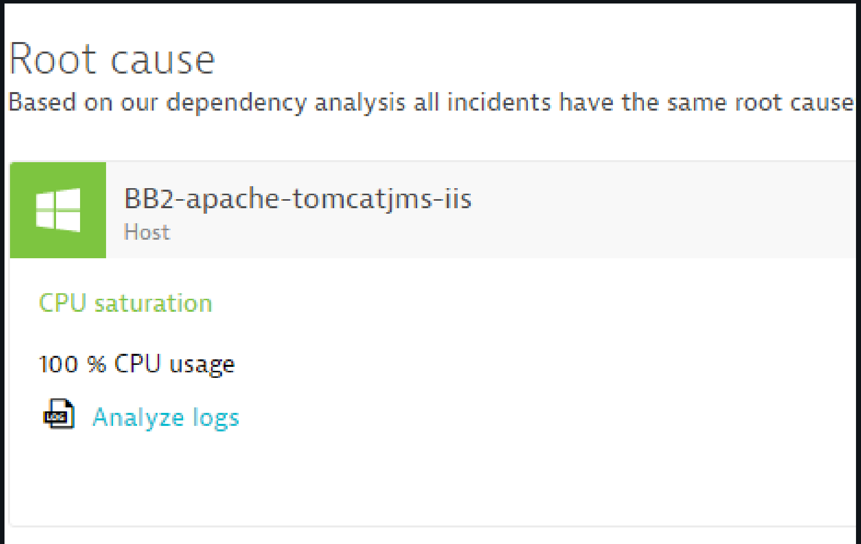
Agenda

- Value
- Architecture
- Permissions
- Analysis
- Custom Log Events
- Log Analytics Free Tier
- Log Analytics Paid Tier

Value

Why create a log analytics software?

- Use log content as monitoring data source
  - Search inside of log messages using query strings
  - Generate problem notifications based on patterns
- Enhance troubleshooting
  - Use log information within root cause drill down
  - Add more context with event logs
- Lots of applications rely on logging for diagnostics
  - Provide DevOps with information they are used to having
  - Easy insights into unsupported technologies



Root cause

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

BB2-apache-tomcatjms-iis

Host

CPU saturation

100 % CPU usage

Use Cases

- Reactive log search
  - Similar to classic enterprise log management tools
  - Realized via Log Viewer interface
  - Select scope, query, timeframe
- Proactive pattern-based notification
  - User defines scope and pattern
  - Pattern presence generates event
  - Event is integrated with AI on process/host level
- Contextual drilldown to log data
  - Biggest competitive advantage
  - Allows quick access to log content in context of problem analysis
  - Can be executed from problem, host, PGI and PG reports

Competitive differentiators

- No additional agent required
- Automatic log discovery
  - Manual also available
- Easy to learn, intuitive pattern language
- Log information and monitoring information available in same place in context
- Support for OS and docker log files
- Automatic support for rotated logs
- Basic approach requires no additional license cost

Log Analytics

Architecture ◀

Permissions

Problem Logs

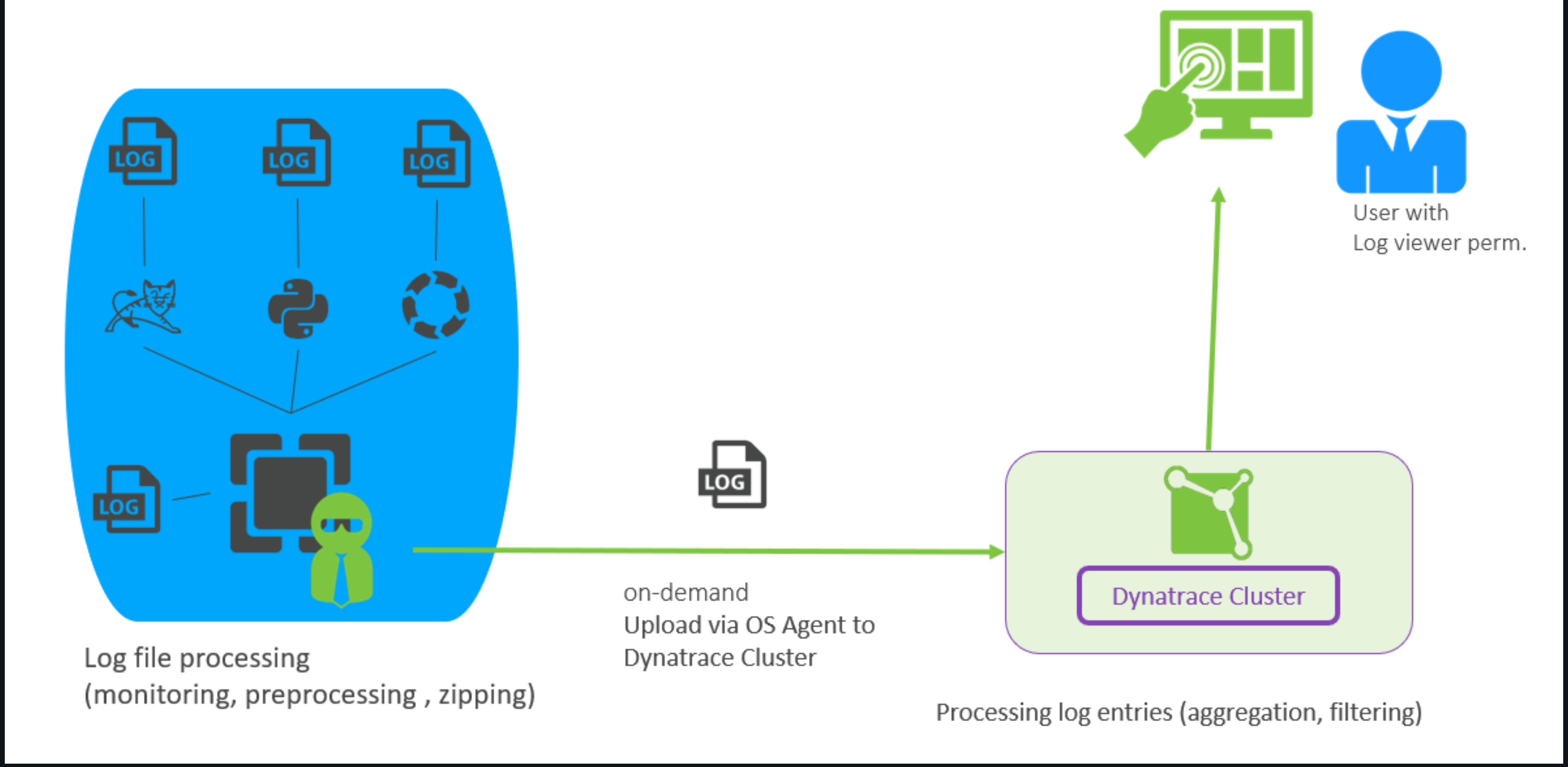
Host Logs

Process Logs

Troubleshooting

Log Monitoring

Architecture



Log Analytics

Architecture

Permissions ◀

Problem Logs

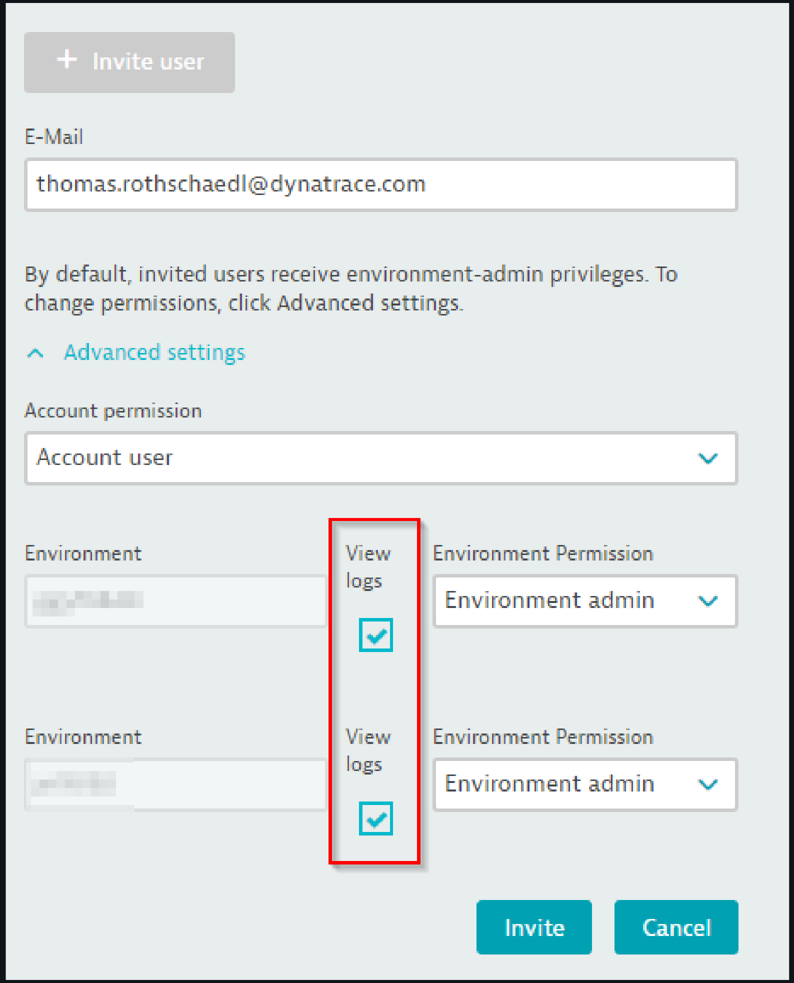
Host Logs

Process Logs

Troubleshooting

Log Monitoring

Permissions



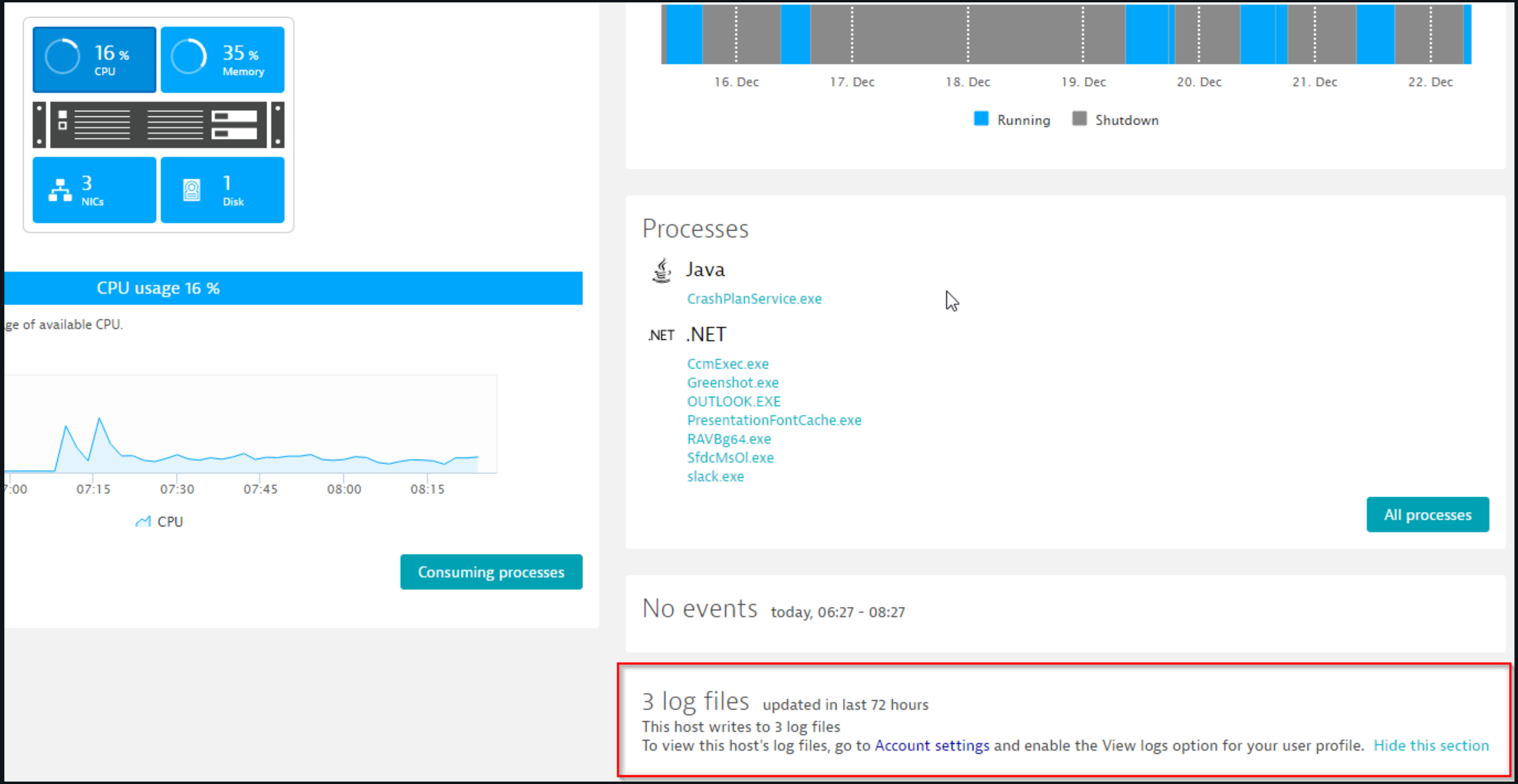
E-Mail: thomas.rothschaedl@dynatrace.com

By default, invited users receive environment-admin privileges. To change permissions, click Advanced settings.

Account permission: Account user

Environment	View logs	Environment Permission
[redacted]	☑	Environment admin
[redacted]	☑	Environment admin

Permissions per User



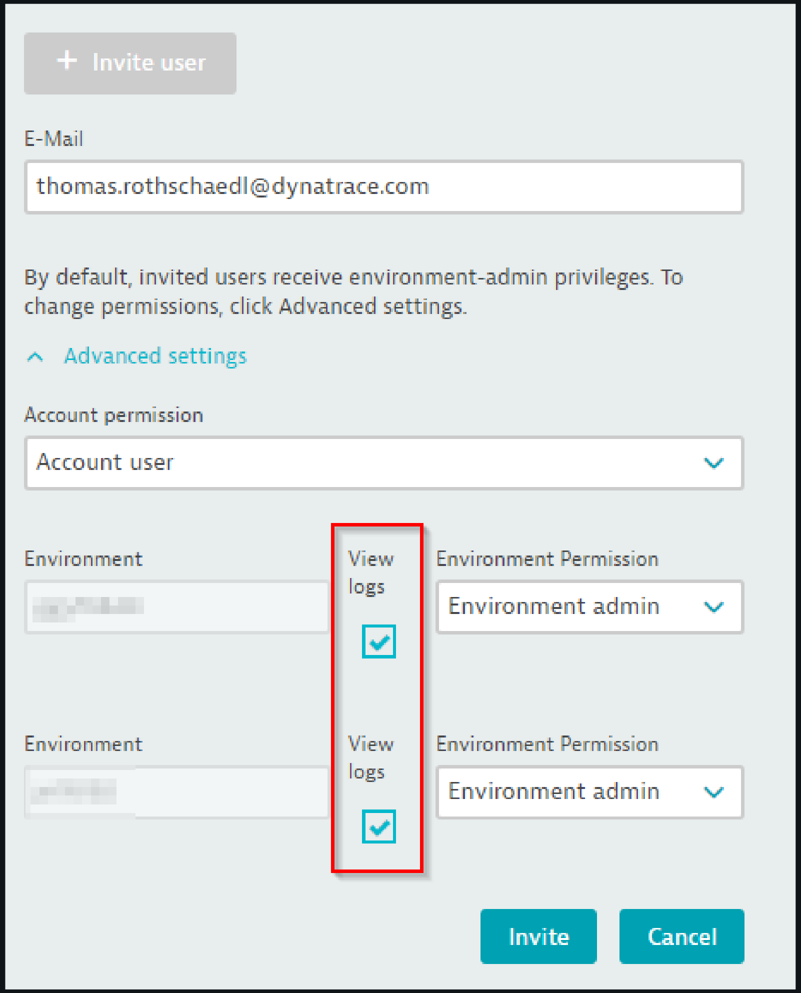
No events today, 06:27 - 08:27

3 log files updated in last 72 hours

This host writes to 3 log files

To view this host's log files, go to Account settings and enable the View logs option for your user profile. Hide this section

Permissions per User



E-Mail

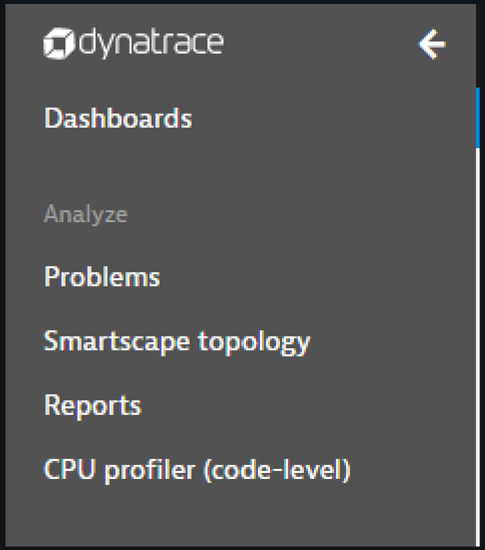
thomas.rothschaedl@dynatrace.com

By default, invited users receive environment-admin privileges. To change permissions, click Advanced settings.

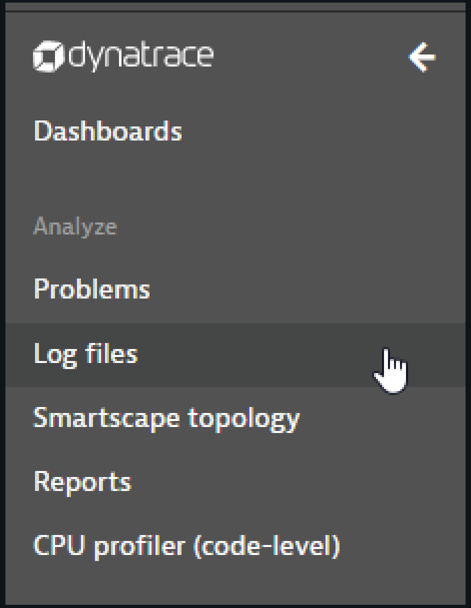
Account permission: Account user

Environment	View logs	Environment Permission
[redacted]	☑	Environment admin
[redacted]	☑	Environment admin

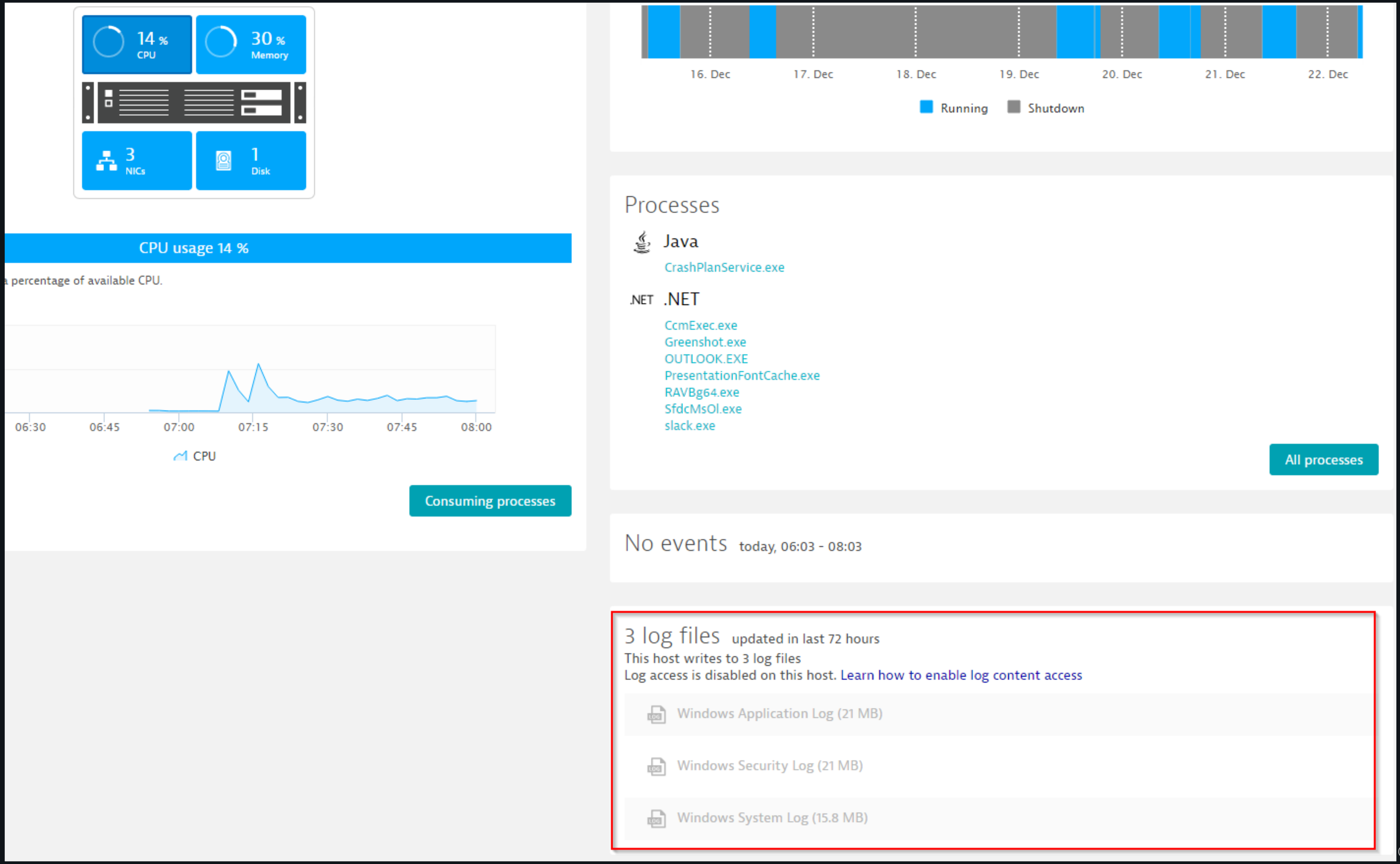
Without Log viewer permission



With Log viewer permission



Permissions per Host



a percentage of available CPU.

Processes

Java

CrashPlanService.exe

.NET

CcmExec.exe
Greenshot.exe
OUTLOOK.EXE
PresentationFontCache.exe
RAVBg64.exe
SfdcMsOl.exe
slack.exe

No events today, 06:03 - 08:03

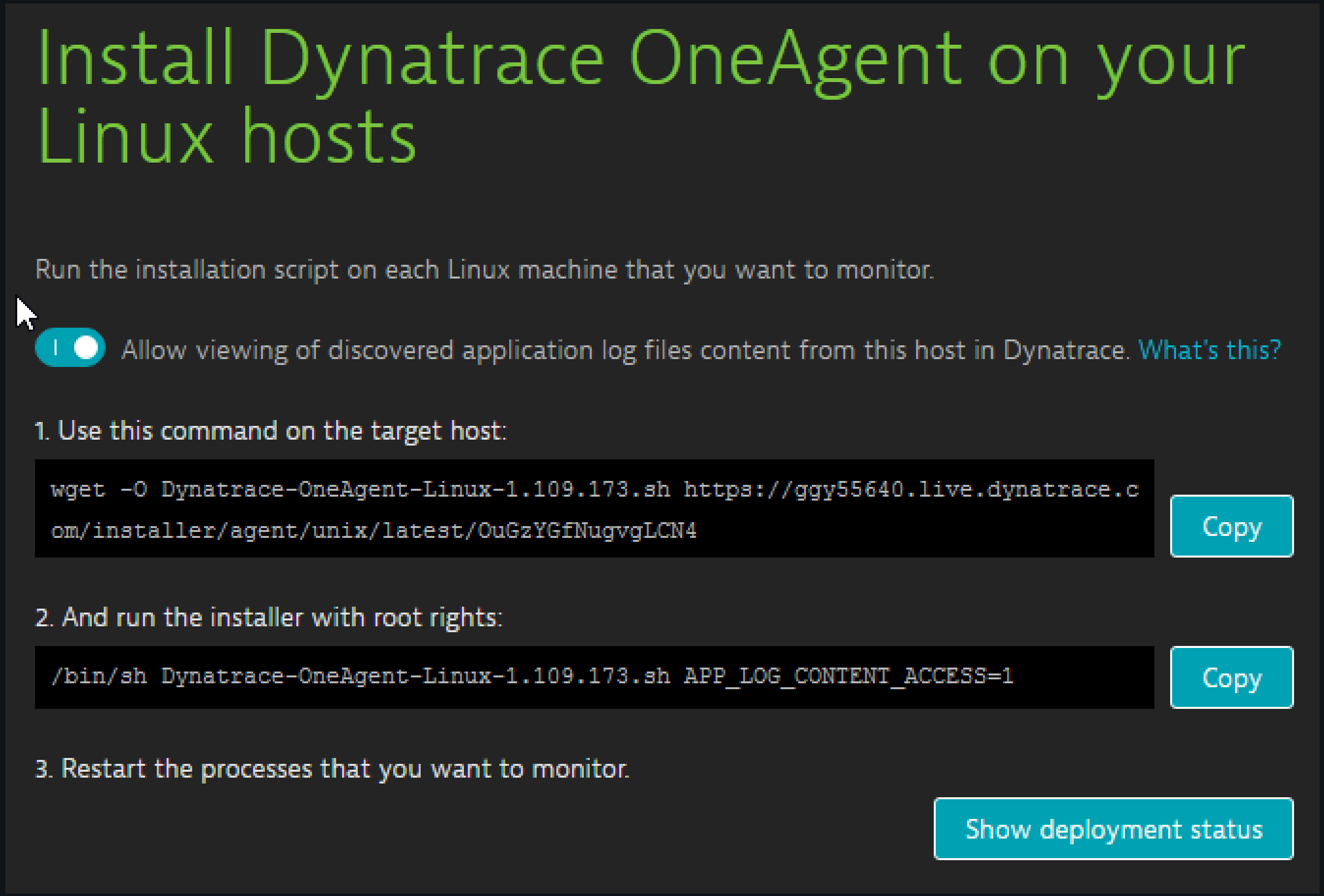
3 log files updated in last 72 hours

This host writes to 3 log files

Log access is disabled on this host. Learn how to enable log content access

- Windows Application Log (21 MB)
- Windows Security Log (21 MB)
- Windows System Log (15.8 MB)

Permissions per Host – during Installation



Install Dynatrace OneAgent on your Linux hosts

Run the installation script on each Linux machine that you want to monitor.

● Allow viewing of discovered application log files content from this host in Dynatrace. What's this?

1. Use this command on the target host:

```
wget -O Dynatrace-OneAgent-Linux-1.109.173.sh https://ggy55640.live.dynatrace.c
om/installer/agent/unix/latest/OuGzYGfNugvgLCN4
```

2. And run the installer with root rights:

```
/bin/sh Dynatrace-OneAgent-Linux-1.109.173.sh APP_LOG_CONTENT_ACCESS=1
```

3. Restart the processes that you want to monitor.

Log Analytics

Architecture

Permissions

Problem Logs ◀

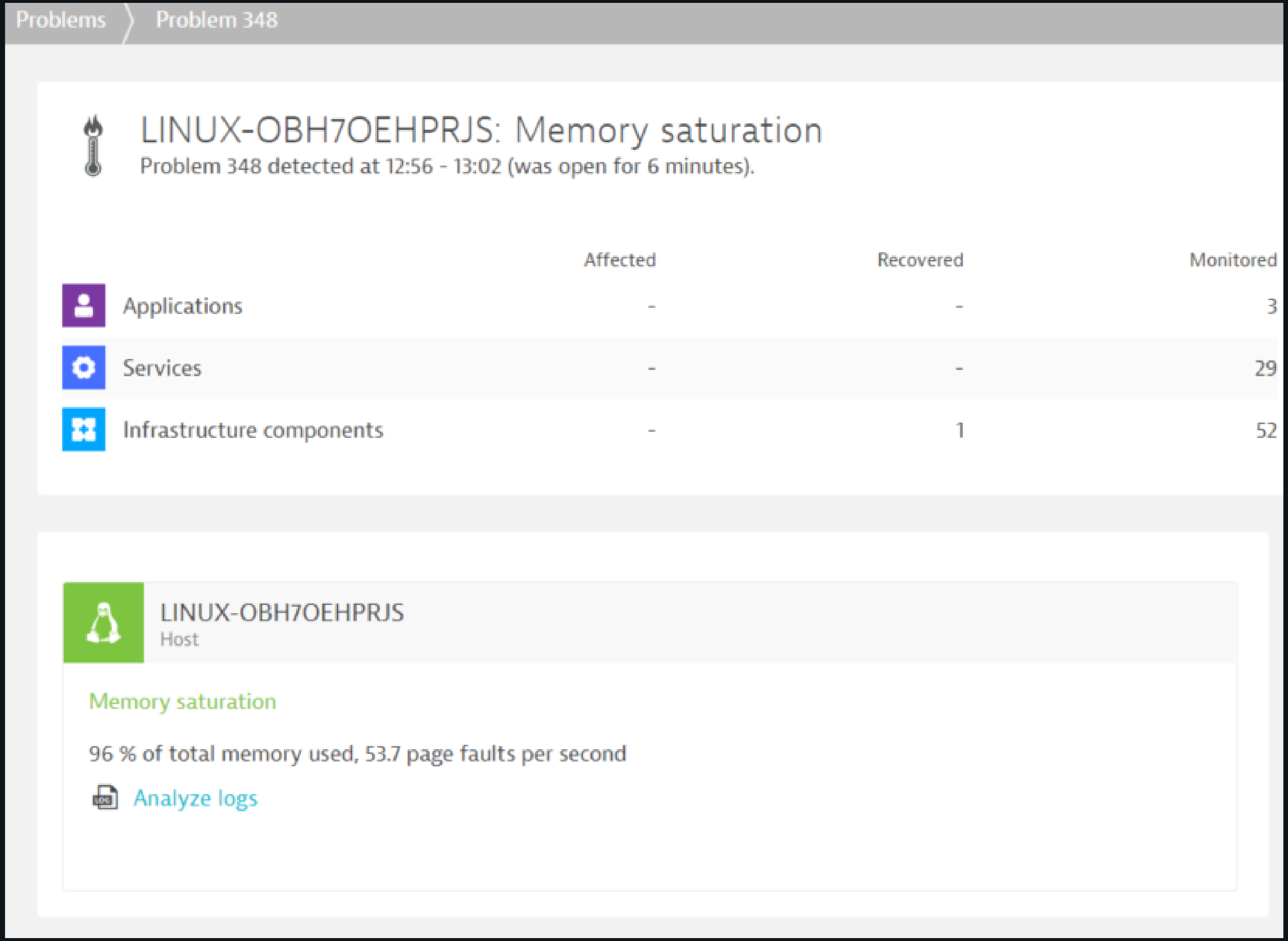
Host Logs

Process Logs

Troubleshooting

Log Monitoring

Problem Logs



LINUX-OBH7OEHPRJS: Memory saturation

Problem 348 detected at 12:56 - 13:02 (was open for 6 minutes).

	Affected	Recovered	Monitored
Applications	-	-	3
Services	-	-	29
Infrastructure components	-	1	52

LINUX-OBH7OEHPRJS

Host

Memory saturation

96 % of total memory used, 53.7 page faults per second

Log Analytics

Architecture

Permissions

Problem Logs

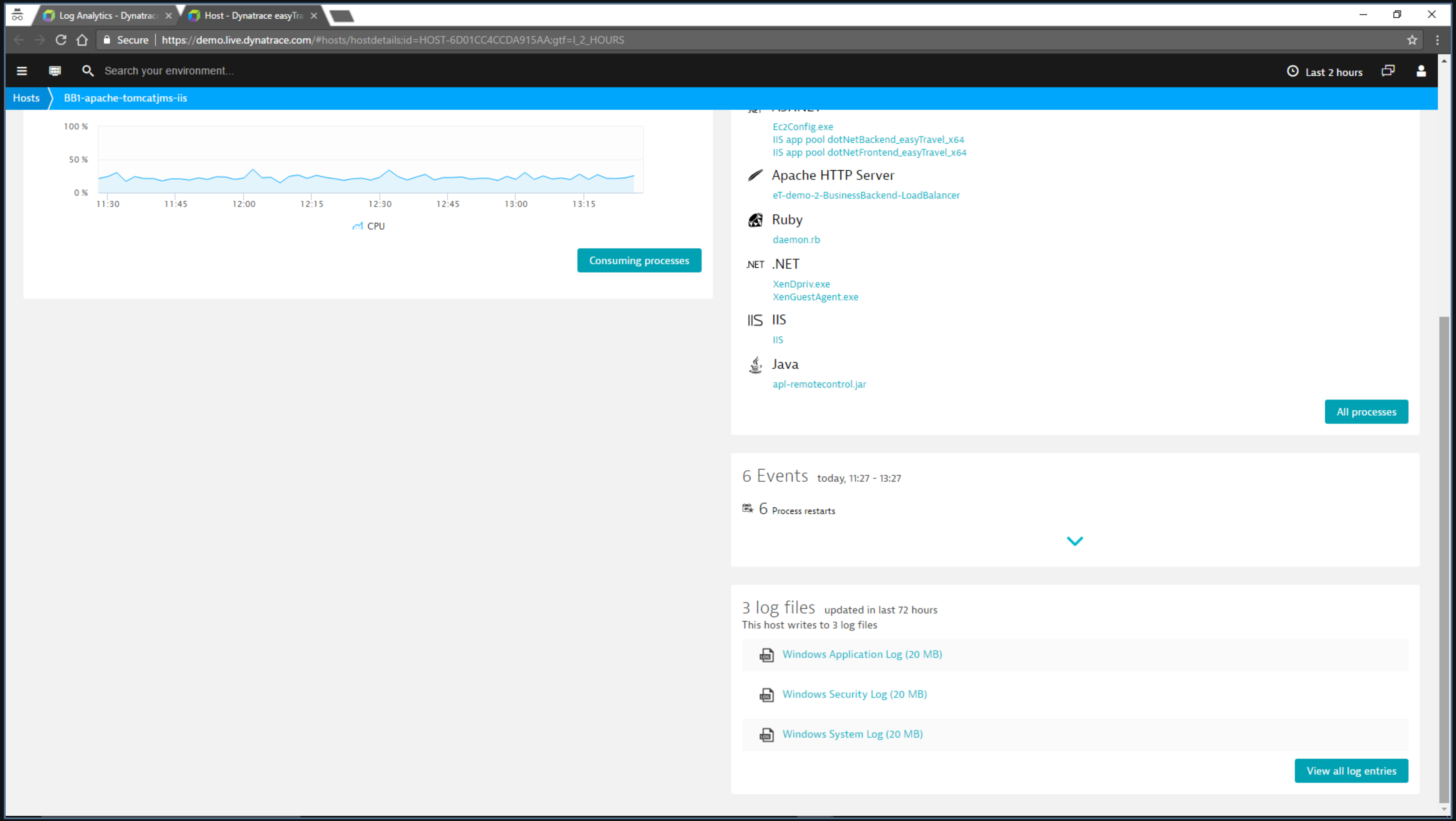
Host Logs

Process Logs

Troubleshooting

Log Monitoring

Host Logs



Ec2Config.exe
IIS app pool dotNetBackend_easyTravel_x64
IIS app pool dotNetFrontend_easyTravel_x64

Apache HTTP Server
eT-demo-2-BusinessBackend-LoadBalancer

Ruby
daemon.rb

.NET
XenDpriv.exe
XenGuestAgent.exe

IIS
IIS

Java
apl-remotecontrol.jar

All processes

6 Events today, 11:27 - 13:27

6 Process restarts

3 log files updated in last 72 hours
This host writes to 3 log files

Windows Application Log (20 MB)

Windows Security Log (20 MB)

Windows System Log (20 MB)

View all log entries

Log Analytics

Architecture

Permissions

Problem Logs

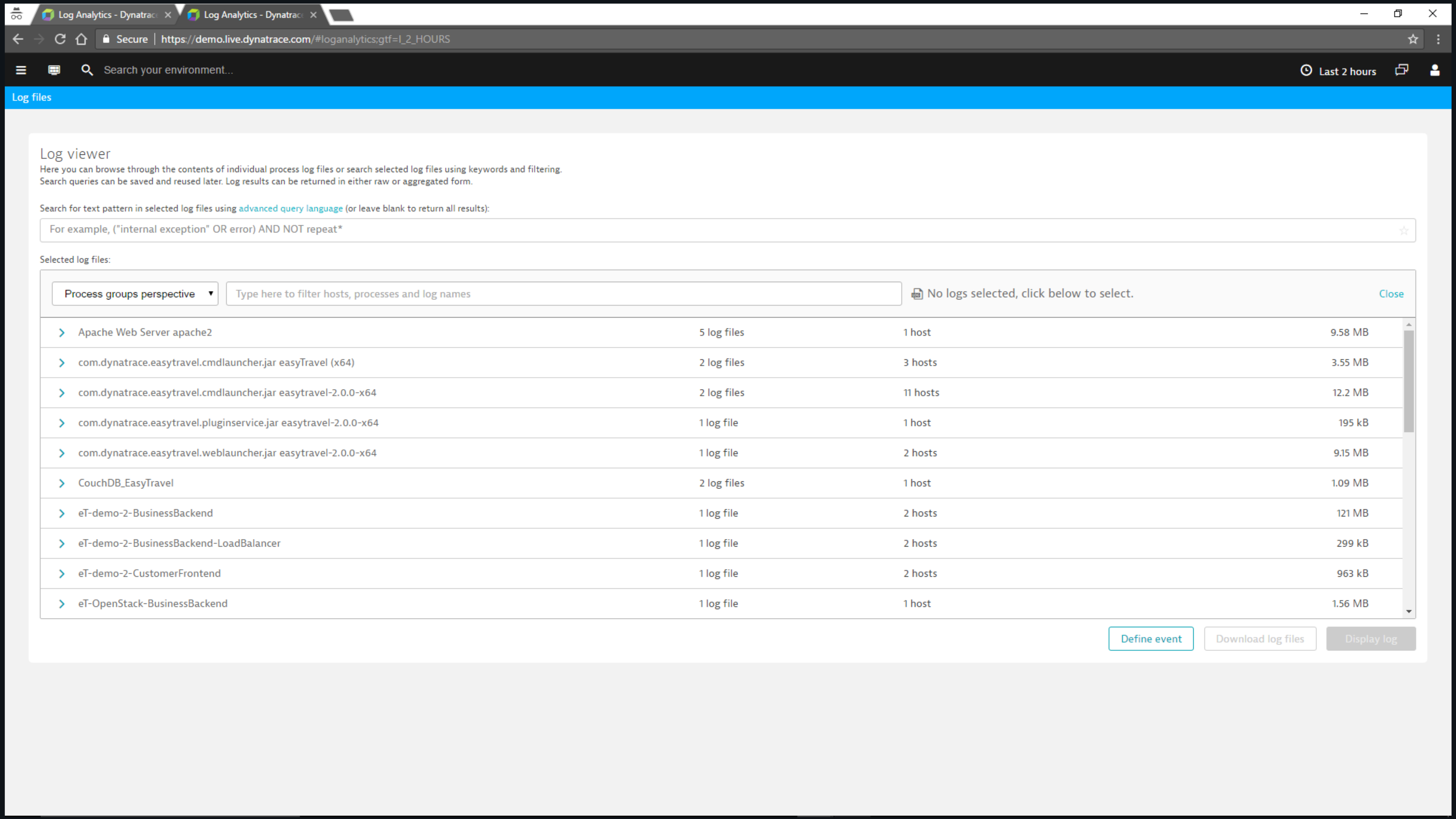
Host Logs

Process Logs ◀

Troubleshooting

Log Monitoring

Process Logs



Log Analytics - Dynatrace
Log Analytics - Dynatrace
Secure
https://demo.live.dynatrace.com/#loganalytics;gtf=l_2_HOURS
Search your environment...
Last 2 hours
Log files

Log viewer

Here you can browse through the contents of individual process log files or search selected log files using keywords and filtering. Search queries can be saved and reused later. Log results can be returned in either raw or aggregated form.

Search for text pattern in selected log files using advanced query language (or leave blank to return all results):

For example, ("internal exception" OR error) AND NOT repeat*

Selected log files:

Process groups perspective ▾ | Type here to filter hosts, processes and log names | No logs selected, click below to select. | Close

› Apache Web Server apache2	5 log files	1 host	9.58 MB
› com.dynatrace.easytravel.cmdlauncher.jar easyTravel (x64)	2 log files	3 hosts	3.55 MB
› com.dynatrace.easytravel.cmdlauncher.jar easytravel-2.0.0-x64	2 log files	11 hosts	12.2 MB
› com.dynatrace.easytravel.pluginservice.jar easytravel-2.0.0-x64	1 log file	1 host	195 kB
› com.dynatrace.easytravel.weblauncher.jar easytravel-2.0.0-x64	1 log file	2 hosts	9.15 MB
› CouchDB_EasyTravel	2 log files	1 host	1.09 MB
› eT-demo-2-BusinessBackend	1 log file	2 hosts	121 MB
› eT-demo-2-BusinessBackend-LoadBalancer	1 log file	2 hosts	299 kB
› eT-demo-2-CustomerFrontend	1 log file	2 hosts	963 kB
› eT-OpenStack-BusinessBackend	1 log file	1 host	1.56 MB

Log Analytics

Architecture

Permissions

Problem Logs

Host Logs

Process Logs

Troubleshooting ◀

Log Monitoring

Log Troubleshooting – On Demand

- On demand log file viewing for troubleshooting
- Logfiles must comply with specific row patterns (Timestamp, type,...)
- Log files are available for analysis only as long as they are stored on a host
- You can examine a maximum of **500MB** of log data.
- You can examine the log files for only the past **seven days**.
- You can examine log files one at a time in the context of your topology.

Log Monitoring – Centralized Storage

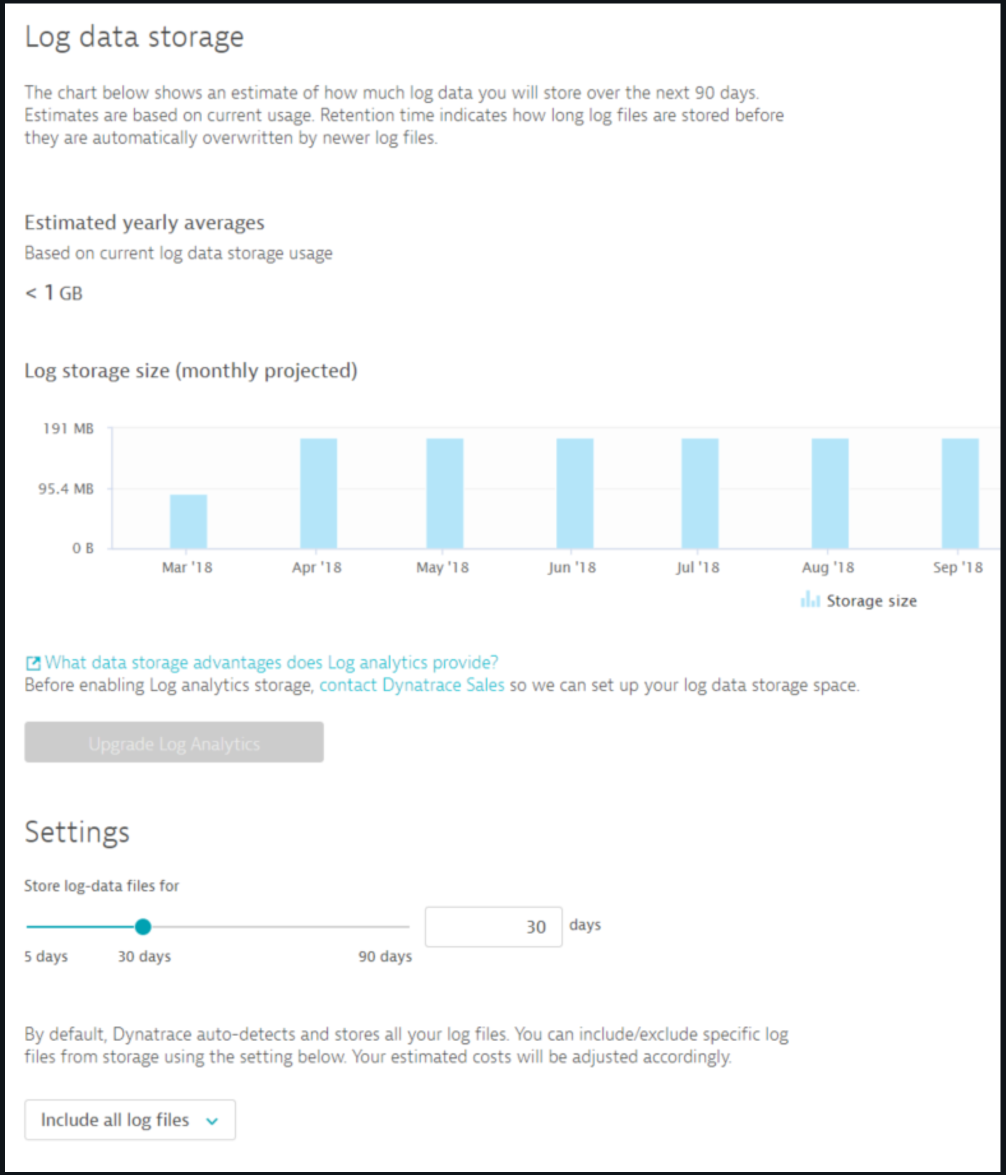
- You can analyze significant log events
  - across multiple logs
  - across parts of the environment (production)
  - potentially over a longer time frame.
- For immediate notification, consider setting alerts for monitored logs. You specify the log files to be stored on the Dynatrace server, enabling you to analyze longer time frames or to perform analysis across multiple log files.
- Important Characteristics
  - Transferred log data to the Dynatrace server is measured.
    - The initial quota is a total of 5GB of log data transfer.
  - You can retain data for as little as 5 days and up to 90 days.
  - You can create alerts based on text pattern occurrences across monitored logs.
  - You can bookmark search queries on multiple monitored logs.
  - You can parse columns and examine the top N occurrences.
  - You have access to the application programming interface (API) for these log files.

Log storage requirements

- Dynatrace SaaS
  - Log files are stored in Amazon Elastic File System in the zone where your Dynatrace environment resides
  - You don’t have to worry about storage performance, availability, or free space
  - Disk storage costs are included in your Log Analytics subscription and are based on the average volume of your cloud-based log storage
- Dynatrace Managed
  - To store log files centrally on your Dynatrace Managed cluster, you must provide a common Network File System (NFS) mount point (path) that is identical and available from all cluster nodes
  - With this approach, it's your responsibility to ensure appropriate levels of performance, availability, and free space on the mounted NFS volume
  - Costs for Premium (> 5GiB) are calculated based only on the amount of ingress log data, not total storage size, so retention time doesn't influence storage costs

Log Analytics Data Storage for Monitored Logs

- Set your desired retention period and alternatively decide what logs you want to store or not store on central log disk storage
- Then review your expected usage



Log data storage

The chart below shows an estimate of how much log data you will store over the next 90 days. Estimates are based on current usage. Retention time indicates how long log files are stored before they are automatically overwritten by newer log files.

Estimated yearly averages

Based on current log data storage usage

< 1 GB

Log storage size (monthly projected)

What data storage advantages does Log analytics provide?
Before enabling Log analytics storage, contact Dynatrace Sales so we can set up your log data storage space.

Settings

Store log-data files for: 30 days

By default, Dynatrace auto-detects and stores all your log files. You can include/exclude specific log files from storage using the setting below. Your estimated costs will be adjusted accordingly.

Include all log files

Licensing for Log Monitoring

- Managed - Ingress of logs
  - To store log files centrally on your Dynatrace Managed cluster, you must provide a common Network File System (NFS) mount point (path) that is identical throughout the cluster and available from all cluster nodes. With this approach, it's your responsibility to ensure appropriate levels of performance, availability, and free space on the mounted NFS volume. Costs are calculated based only on the amount of ingress log data (GB/day), not total storage size, so retention time doesn't influence storage costs.
- SaaS - Storage volume
  - Average daily ingress of log data over licensing period multiplied by retention period
    - For example, that your Log Monitoring agreement is configured for 90 days and you've arranged for 450 GiB of annual daily average storage. The anticipated average daily ingestion of log data in this case would be 5 GiB. 450 (GiB; base quota of annual average storage) / 90 (days) = 5 (GiB; anticipated average daily ingestion)

Questions?

dynatrace

Simply smarter clouds