

# **DOCUMENT D'EXPLOITATION TECHNIQUE (DEX) PRJ3\_LYON2**

## **DESCRIPTION**

Ce document décrit comment le système doit être géré et maintenu. Il contient des informations sur les procédures d'exploitation standard, la surveillance du système et d'autres tâches d'administration système. Il peut également contenir des informations sur les problèmes courants et comment les résoudre.

## **GROUPE PRÉSENTANT**

**RODET** Nathan  
**RIVALLAND** Gregory  
**CHELIAN** David  
**HARMEL** Enguerrand

## Enregistrement des changements

Date d'édition	NOM / Prénom	Version du document	Description
30/11/2023	RIVALLAND Gregory	1.1	Création du document
03/12/2023	HARMEL Enguerrand	1.2	Ajout de contenu
10/12/2023	HARMEL Enguerrand	1.3	Complétion et réajustement des parties à traiter
10/01/2024	HARMEL Enguerrand	1.4	Refonte du document
13/01/2024	RIVALLAND Gregory	1.5	Correction & Mise en page

## SOMMAIRE

<b>DOCUMENT D'EXPLOITATION TECHNIQUE (DEX) PRJ3_LYON2.....</b>	<b>1</b>
Enregistrement des changements.....	2
<b>SOMMAIRE.....</b>	<b>3</b>
<b>1. L'environnement Azure et ses fonctionnalités.....</b>	<b>4</b>
a. Les environnements de déploiement.....	4
b. Le workflow.....	4
c. Gestions des artefacts.....	4
d. La pipeline CI/CD.....	4
<b>2. Mode opératoire.....</b>	<b>5</b>
a. Lancement du projet manuellement.....	5
b. Lancement du projet avec le workflow.....	6
c. Accéder au site web.....	7
<b>3. Suivre l'état de la solution à travers les logs.....</b>	<b>8</b>
a. Azure Monitor.....	8
b. Insights & Log Analytics.....	10
c. Azure Alert & Budget alert.....	12

# 1. L'environnement Azure et ses fonctionnalités

## a. Les environnements de déploiement

Le projet est séparé en deux environnements distincts : développement et production.

Pour implémenter de nouvelles fonctionnalités il convient d'utiliser l'environnement de développement dédié aux tests réservé aux développeurs.

L'environnement de production est réservé aux fonctionnalités testées, de qualité et stable, on ne l'utilise que pour ajouter les nouveautés qui ont été revues et validées au préalable dans l'environnement de développement car il s'agit de l'environnement déployé pour les clients/utilisateurs.

## b. Le workflow

Chaque ajout de fonctionnalités ou correctifs est développé dans une branche features, qui est un clone de la branche développement. Une fois les nouveautés incluses dans la branche développement, si elles sont avérées stable après les avoir testées, on peut procéder à la fusion de la branche de développement vers la branche principale main, via une merge request, qui doit être analysée et approuvée.

## c. Gestions des artefacts

Les artefacts générés pendant le processus CI sont stockés dans Azure Artifacts pour une gestion centralisée.

Utilisez la fonctionnalité de versionnement des artefacts pour garantir la traçabilité des versions déployées dans chaque environnement.

Les artefacts sont déployés sélectivement dans l'environnement de développement ou de production en fonction des besoins.

## d. La pipeline CI/CD

La pipeline vient construire l'ensemble des services du projet lorsqu'elle est lancée. Elle vient activer le provisioning des ressources via les scripts Terraform. Elle s'actionne manuellement ou lors d'un push ou d'un pull request dans le dépôt git.

## 2. Mode opératoire

### a. Lancement du projet manuellement

Déployer le projet avec Azure DevOps :

- Manuellement
- Avec le Workflow

Pour déployer manuellement le projet, il convient de lancer la pipeline PJR3\_LYON2 qui se chargera de construire le projet à travers l'exécution des différents jobs.

La marche à suivre est de se rendre dans l'onglet Pipelines depuis la plateforme Azure Devops, sélectionner la pipeline PJR3\_LYON2 et cliquer sur "Run pipeline" puis choisir la branche qui convient : main pour la prod, develop ou features pour les nouvelles fonctionnalités dans un environnement de test.

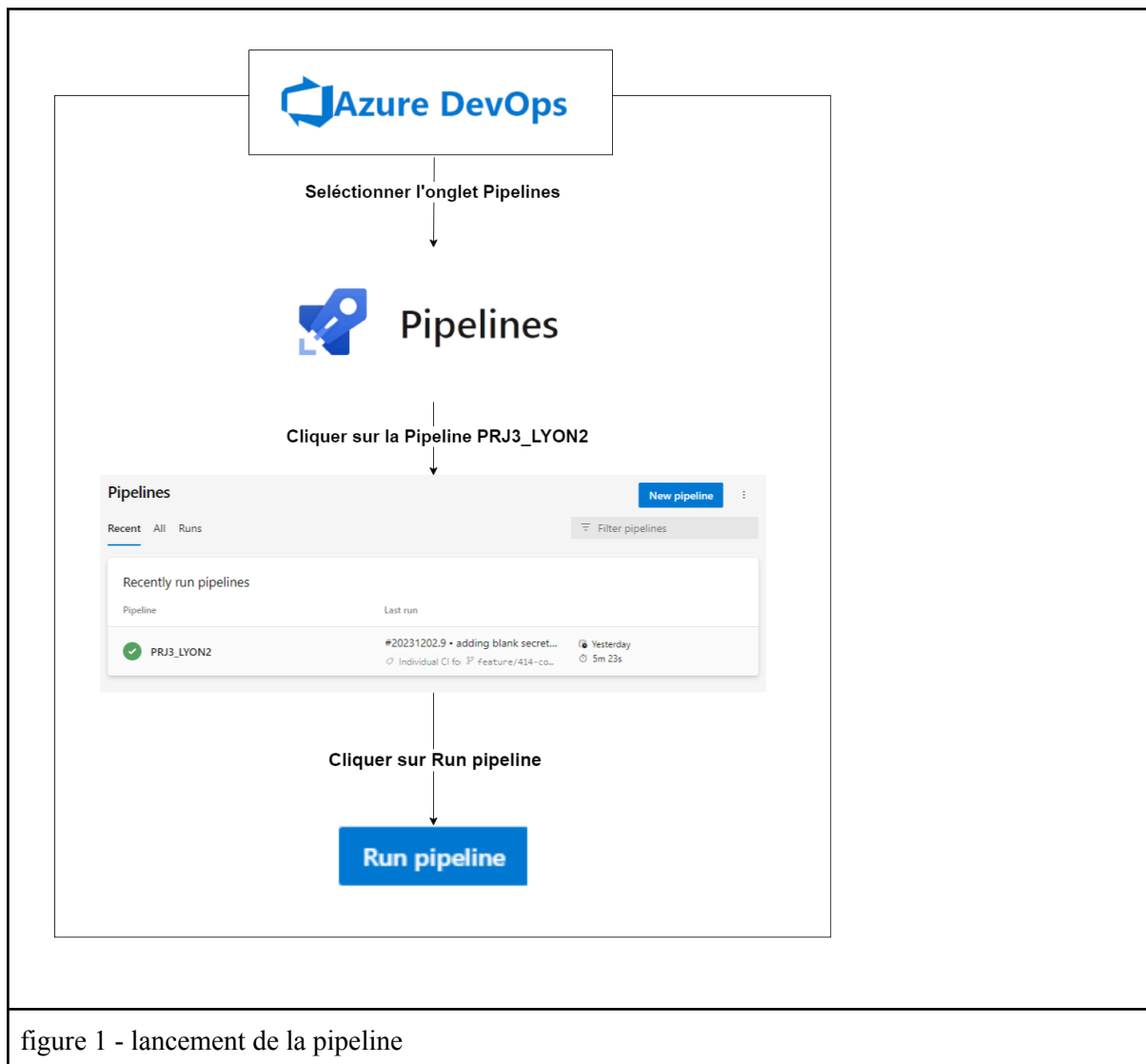
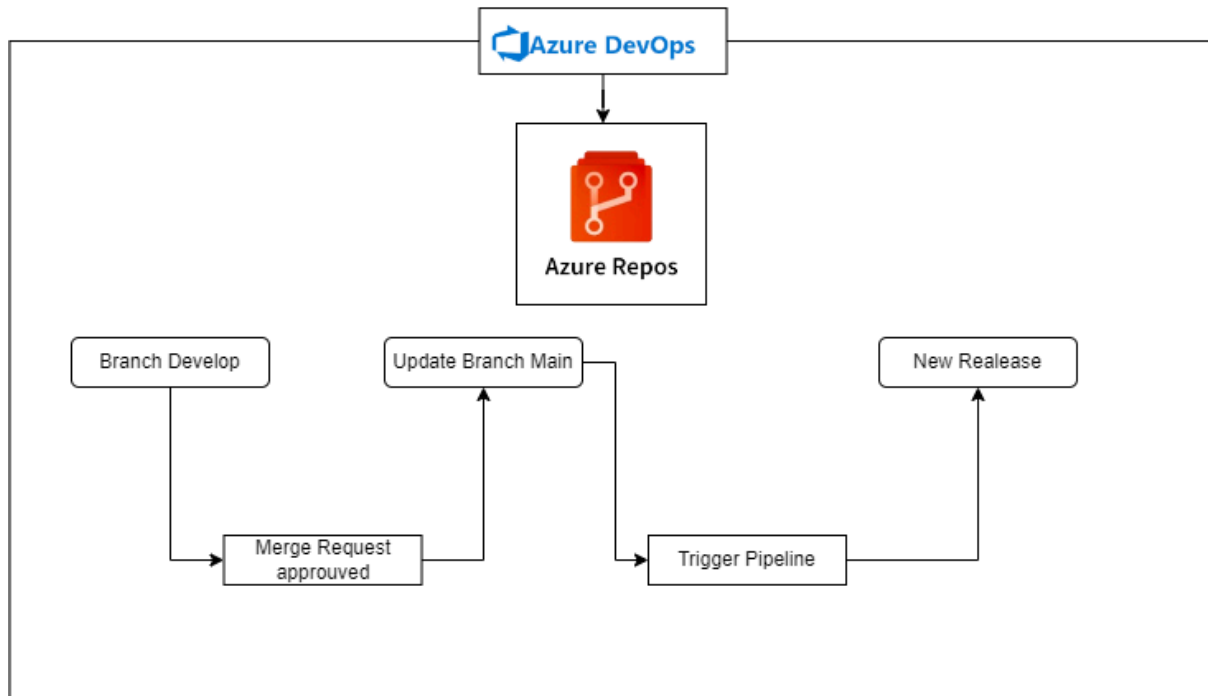


figure 1 - lancement de la pipeline

## b. Lancement du projet avec le workflow

Le projet se met à jour automatiquement avec le workflow lorsque l'on merge la branche développement avec la branche main, ce qui trigger la pipeline qui viendra build la nouvelle version du projet.



### c. Accéder au site web

Une fois le site déployé, il est accessible à l'adresse via le service AKS dans “Ingress” comme ci-dessous.

Microsoft Azure

Home > rg-prj3-prd-northeurope-001 > aks-prj3-prd-northeurope-001

aks-prj3-prd-northeurope-001 | Services and ingresses

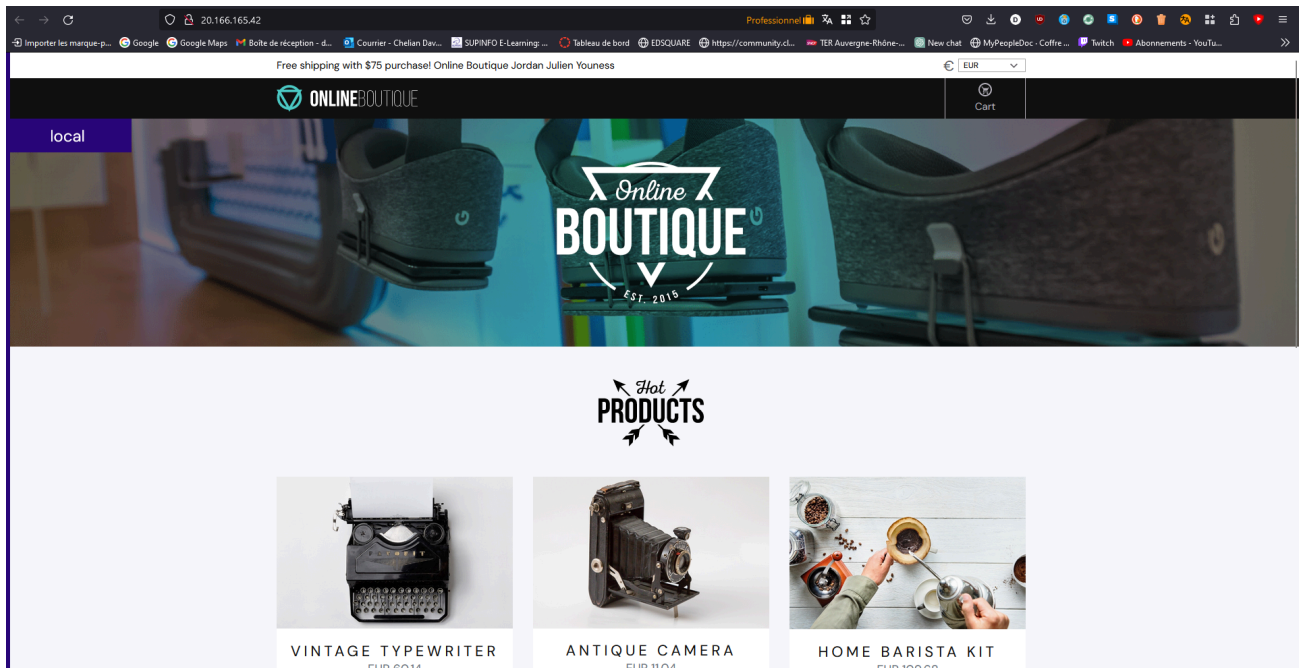
Search

Services **Ingresses**

Filter by ingress name:  Filter by namespace:  [Add label filter](#)

<input type="checkbox"/>	Name	Namespace	Class	Hosts	Address	Ports	Age	
<input type="checkbox"/>	frontend-ingress	ns-app	nginx	*	20.166.165.42	80	10 minutes	...

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Microsoft Defender for Cloud  
Kubernetes resources  
Namespaces  
Workloads  
**Services and ingresses**  
Storage  
Configuration  
Custom resources  
Events  
Run command  
Settings  
Node pools  
Cluster configuration  
Networking  
Extensions + applications  
Backup  
Open Service Mesh  
GitOps





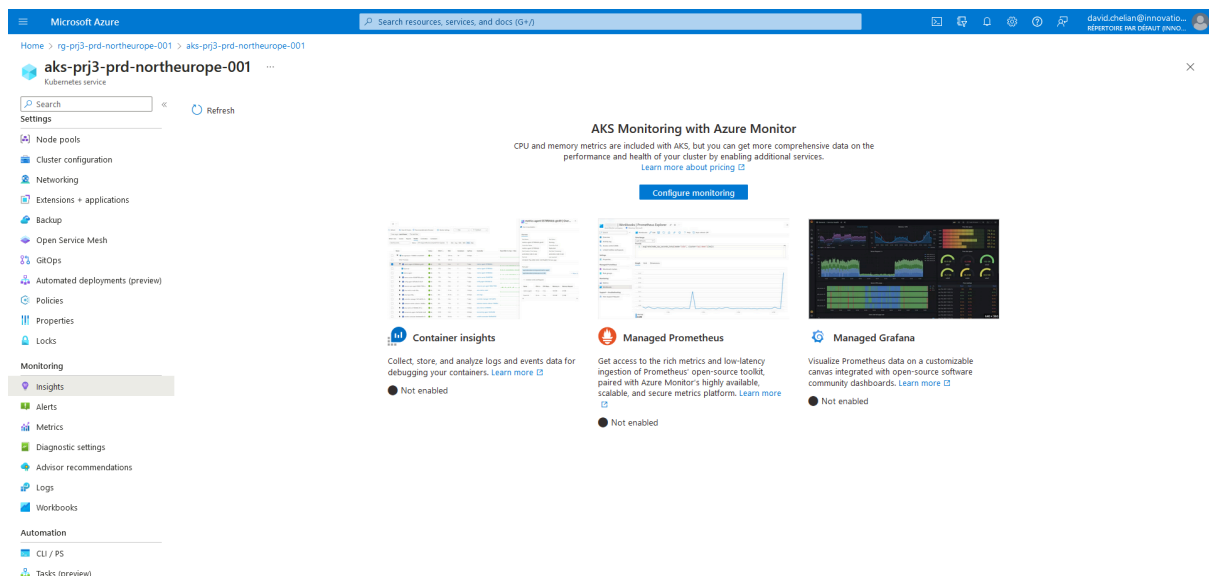
### 3. Suivre l'état de la solution à travers les logs

L'utilisation efficace des logs issus d'Azure Monitor et Application Insights est essentielle pour la surveillance et la résolution des problèmes de fonctionnement du projet.

#### a. Azure Monitor

Azure Monitor collecte une variété de métriques pour surveiller l'utilisation des ressources, les performances du cluster AKS et la disponibilité des services. Pour exploiter ces informations :

- Accédez au portail Azure et naviguez vers le service Azure Monitor.
- Dans la section "Métriques", choisissez la ressource spécifique (par exemple, le cluster AKS) pour laquelle vous souhaitez consulter les métriques.
- Utilisez les filtres disponibles pour affiner la plage de temps et sélectionner des métriques spécifiques telles que l'utilisation CPU, la mémoire, etc.
- Utilisez les graphiques pour visualiser les tendances et les variations. Cela peut aider à identifier les points chauds de l'utilisation des ressources ou les moments de faible disponibilité.



The screenshot shows the Azure portal interface for a Kubernetes service named 'aks-prj3-prd-northeurope-001'. The left sidebar contains navigation links for Settings, Node pools, Cluster configuration, Networking, Extensions + applications, Backup, Open Service Mesh, GitOps, Automated deployments (preview), Policies, Properties, Locks, Monitoring, Insights, Alerts, Metrics, Diagnostic settings, Advisor recommendations, Logs, Workbooks, Automation, CLI / PS, and Tasks (preview). The main content area is titled 'AKS Monitoring with Azure Monitor' and includes a 'Configure monitoring' button. Below this, three monitoring options are listed: 'Container insights' (Not enabled), 'Managed Prometheus' (Not enabled), and 'Managed Grafana' (Not enabled). Each option has a brief description and a 'Learn more' link.

## Configure Container insights



### Container Insights

Container insights collects container logs, Kubernetes events, and cluster inventory data with the Azure Monitor agent to enable debugging your applications. [Learn more](#)

Enable container logs



A Log Analytics workspace (defaultworkspace-426eed83-4d2c-4b8f-a934-4ec10895c140-neu) will be created automatically.

### Managed Prometheus

Managed Prometheus provides a highly available, scalable and secure metrics platform to monitor your containerized workloads. [Learn more](#)

Enable Prometheus metrics



An Azure Monitor workspace (defaultazuremonitorworkspace-neu) will be created automatically.

### Managed Grafana

Selecting a fully managed instance of Grafana to visualize your managed Prometheus data stored in your Azure Monitor workspace. [Learn more about pricing](#)

Enable Grafana



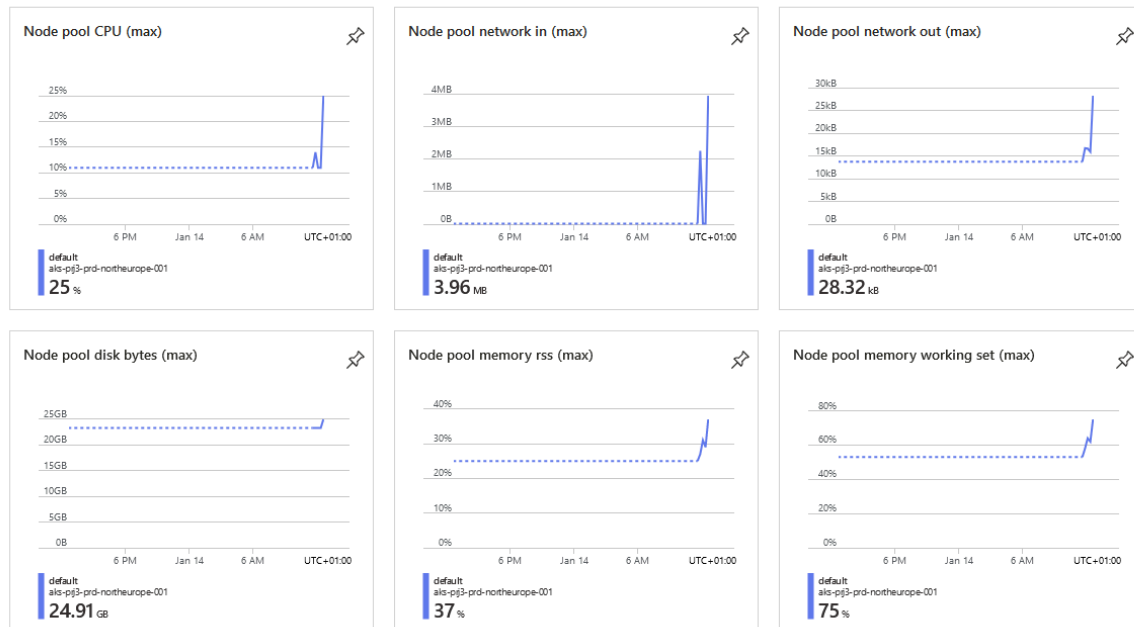
> Advanced settings

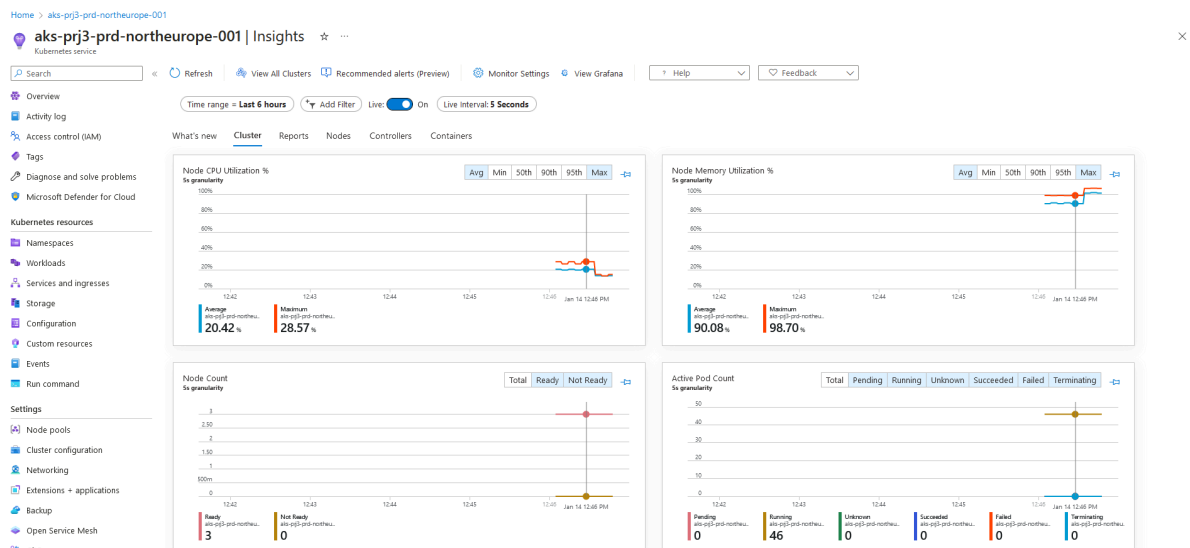
Configure

Cancel

Platform metrics [See all Metrics](#)

[View Grafana workspaces](#)





## b. Insights & Log Analytics

Application Insights offre une visibilité approfondie sur les performances des applications, les dépendances entre composants et la détection d'erreurs. Pour tirer parti de ces fonctionnalités :

- Accédez au portail Azure et sélectionnez le service Application Insights associé à votre application.
- Dans la section "Performances", explorez les métriques relatives aux temps de réponse, aux dépendances, et aux erreurs.
- Utilisez la fonction "Explorer" pour rechercher des détails spécifiques sur les erreurs, notamment les messages d'erreur, les traces et les exceptions.
- Exploitez les cartes de dépendances pour comprendre les interactions entre différents composants de l'application, ce qui peut être crucial pour la détection des goulots d'étranglement.
- Analyse des logs et stockage des logs

Home > rg-prj3-prd-northeurope-001

**rg-prj3-prd-northeurope-001** | Diagnostic settings

Subscription: PRJ3\_IYON2 | Resource group: rg-prj3-prd-northeurope-001 | Resource type: RG selected | Resource: 80 selected

Select any of the resources to view diagnostic settings.

Name	Resource type	Resource group	Diagnostics status
aks-prj3-prd-northeurope-001	Kubernetes service	rg-prj3-prd-northeurope-001	<input type="radio"/> Disabled
sqlserver-prj3-prd-northeurope	Azure Database for MySQL sin...	rg-prj3-prd-northeurope-001	<input type="radio"/> Disabled
vfstateprj3prd	Storage account	rg-prj3-prd-northeurope-001	<input type="radio"/> Disabled
blob	Storage account	rg-prj3-prd-northeurope-001	<input type="radio"/> Disabled
queue	Storage account	rg-prj3-prd-northeurope-001	<input type="radio"/> Disabled
table	Storage account	rg-prj3-prd-northeurope-001	<input type="radio"/> Disabled
file	Storage account	rg-prj3-prd-northeurope-001	<input type="radio"/> Disabled

## Diagnostic setting ...

[Save](#) [Discard](#) [Delete](#) [Feedback](#)

Diagnostic setting name \*

all-metrics-to-log-aks ✓

## Logs

## Categories

☐ Kubernetes API Server☐ Kubernetes Audit☐ Kubernetes Audit Admin Logs☐ Kubernetes Controller Manager☐ Kubernetes Scheduler☐ Kubernetes Cluster Autoscaler☐ Kubernetes Cloud Controller Manager☐ guard☐ csi-azuredisk-controller☐ csi-azurefile-controller☐ csi-snapshot-controller

## Destination details

☒ Send to Log Analytics workspace

## Subscription

PRJ3\_LYON2

## Log Analytics workspace

defaultworkspace-426eed83-4d2c-4b8f-a934-4ec10895c140-neu ( northe... ✓

## Destination table ⓘ

Azure diagnostics

Resource specific

☐ Archive to a storage account☐ Stream to an event hub☐ Send to partner solution

## Metrics

☒ AllMetrics

defaultworkspace-426eed83-4d2c-4b8f-a934-4ec10895c140-neu ✨ ☆ ...

Log Analytics workspace

[Search](#) [Delete](#)

## Overview

[Activity log](#)[Access control \(IAM\)](#)[Tags](#)[Diagnose and solve problems](#)[Logs](#)[Settings](#)[Tables](#)[Agents](#)[Usage and estimated costs](#)[Data export](#)[Network isolation](#)[Linked storage accounts](#)[Properties](#)[Locks](#)

## Classic

[Legacy agents management](#)[Legacy activity log connector](#)[Legacy storage account logs](#)[Legacy computer groups](#)[Legacy solutions](#)[System center](#)

The Log Analytics agents (MMA,OMS) used to collect logs from virtual machines and servers will no longer be supported from August 31, 2024. Plan to migrate to Azure Monitor Agent before this date. [Learn more about migrating to Azure Monitor Agent](#)

## Essentials

Resource group [\(move\)](#) : defaultresourcegroup-neu

Status : Active

Location : North Copy to clipboard

Subscription [\(move\)](#) : PRJ3\_LYON2

Subscription ID : 426eed83-4d2c-4b8f-a934-4ec10895c140

Tags [\(edit\)](#) : Add tags

Workspace Name : defaultworkspace-426eed83-4d2c-4b8f-a934-4ec10895c140-neu

Workspace ID : 14634127-c607-4dc-bc46-2d669393ef17

Pricing tier : Pay-as-you-go

Access control mode : Use resource or workspace permissions

Operational issues : [OK](#)

JSON View

## Get started with Log Analytics

Log Analytics collects data from a variety of sources and uses a powerful query language to give you insights into the operation of your applications and resources. Use Azure Monitor to access the complete set of tools for monitoring all of your Azure resources.

## 1 Connect a data source

Select one or more data sources to connect to the workspace

[Azure virtual machines \(VMs\)](#)[Windows and Linux Agents management](#)[Storage account log](#)[System Center Operations Manager](#)

## 2 Configure monitoring solutions

Add monitoring solutions that provide insights for applications and services in your environment

[View solutions](#)

## 3 Monitor workspace health

Create alerts to proactively detect any issue that arise in your workspace

[Learn more about monitor workspace health](#)

## Useful links

[Documentation site](#)[Community](#)

## Maximize your Log Analytics experience

## 1 Search and analyze logs

Use Log Analytics rich query language to analyze logs

[View logs](#)

## 2 Manage alert rules

Notify or take action in response to important information in your data

## 3 Manage usage and costs

Understand your usage of Log Analytics and estimate your costs for each month

## 4 Create and Share Workbooks

Use Workbooks to create rich interactive reports with your data

[Create Workbooks](#)

Home > aks-prj3-prd-northeurope-001 | Logs ☆ ...

aks-prj3-prd-northeurope-001  
Kubernetes service

Search

Extensions + applications

Backup

Open Service Mesh

GitOps

Automated deployments (preview)

Policies

Properties

Locks

Monitoring

Coll

Alerts

Metrics

Diagnostic settings

Advisor recommendations

Logs

Workbooks

Automation

CLI / PS

Tasks (preview)

Export template

Help

Support + Troubleshooting

New Query 1\*

Queries

Query packs: Select query packs

Topic

Resource type: Kubernetes Services

Add filter

Always show Queries

Feedback

Queries

Documentation

Alerts

Container CPU

View all the container CPU usage averaged over 30mins.

Run

Example query

Container memory

View container CPU averaged over 30 mins intervals.

Run

Load to editor

Example query

Maximum node disk

Max node disk usage averaged over 30 mins intervals.

Run

Example query

Prometheus disk read per second per n...

View Prometheus disk read metrics from the default kubernetes namespace as timechart.

Run

Example query

Avg node CPU usage percentage per m...

For your cluster view avg node CPU usage percentage per minute over the last hour.

Run

Example query

Avg node memory usage percentage p...

For your cluster view avg node memory usage percentage per minute over the last hour.

Run

Example query

Readiness status per node

For all your cluster view count of all the nodes by readiness.

Run

Example query

List all the pods count with phase

View pod phase counts based on all phases: Failed, Pending, Unknown, Running, or Succeeded.

Run

Example query

Instances Avg CPU usage growth from ...

Show Avg CPU growth by instance in the last week by descending order.

Run

Example query

Home > defaultazuremonitorworkspace-neu | Resources ☆ ...

defaultazuremonitorworkspace-neu  
Data collection rule

Search

+ Add

Save

Delete

Filter by name...

All resource groups

Name	Type	Location	Data collection endpoint	Resource group	Subscription
aks-default-82180059-vmss	Virtual machine scale set	North Europe	No endpoint required	mc_rg-prj3-prd-northeurope-001_aks-prj3...	PRJ3_LVON2

Overview

Activity log

Access control (IAM)

Tags

Settings

Locks

Configuration

Data sources

Resources

Security

Identity

Automation

Tasks (preview)

Export template

Help

Support + Troubleshooting

## c. Azure Alert & Budget alert

Azure Alert est un service qui permet de surveiller les données et de capturer des signaux indiquant qu'un événement se produit sur une ressource spécifiée. Une règle d'alerte capture le signal et vérifie s'il répond aux critères de la condition.

Quant à l'alerte budget, elle fait partie des alertes de coût dans Azure. Les alertes budgétaires vous avertissent lorsque les dépenses, basées sur l'utilisation ou le coût, atteignent ou dépassent la quantité définie dans la condition d'alerte du budget.

Home > aks-prj3-prd-northeurope-001

**aks-prj3-prd-northeurope-001 | Alerts** 🔍 ☆ ⋮

Kubernetes service

Search ⏪ 📅 View as timeline (preview) + Create ⌵ ☆ Set up recommendations 📄 Alert rules 🔵 Prometheus rule groups 📁 Action groups 🔍 Alert processing rules ✓ Change user response ⚙️ Actions ⌵ 🔄 Refresh

- Backup
- Open Service Mesh
- GitOps
- Automated deployments (preview)
- Policies
- Properties
- Locks
- Monitoring
- Insights
- Alerts**
- Metrics
- Diagnostic settings
- Advisor recommendations
- Logs
- Workbooks
- Automation
- CLI / PS
- Tasks (preview)
- Export template
- Help
- Resource health
- Support + Troubleshooting

## Set up recommended alert rules

Add commonly-used alert rules for resources like this to get notified on important events happening on this resource.

[View + set up](#) or [Create custom alert rule](#)



## Set up recommended alert rules


### Select alert rules

🔍 📊 node\_cpu\_usage\_percentage is greater than  ⌵ % 🔵

Alert rule name \*

Severity 🔴 2 - Warning ⌵

Threshold type 🔵 Static ⬜ Dynamic



📊 CPU Usage Percentage (Avg)  
aks-prj3-prd-northeurope-001  
**9.9832 %**

> 📊 node\_memory\_working\_set\_percentage is greater than  ⌵ % 🔵

### Notify me by

☒ Email 📧

☒ Email Azure Resource Manager Role 📧

[More alerting options](#)

Estimated monthly total: **0.20 USD**

[Save](#)

[Cancel](#)

Home &gt; aks-prj3-prd-northeurope-001

aks-prj3-prd-northeurope-001 | Alerts

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Microsoft Defender for Cloud

Kubernetes resources

Namespaces

Workloads

Services and ingresses

View as timeline (preview)

+ Create

Set up recommendations

Alert rules

Prometheus rule groups

Action groups

Alert processing rules

Change user response

Actions

Refresh

New: View alerts visualized on a timeline

Action group

Alert rule

Alert processing rule

Resource name: aks-prj3-prd-northeurope-001

Time range: Past 24 hours

Alert condition: Fired

Severity: all

Add filter

Total alerts

Critical

Error

Warning

Informational

Verbose

No grouping

Name

Severity

Affected resource

Alert condition

User response

Fire time

Home &gt; aks-prj3-prd-northeurope-001 | Alerts &gt;

## Create an alert rule

Scope **Condition** Actions Details Tags Review + create

Configure when the alert rule should trigger by selecting a signal and defining its logic.

Signal name \*  [See all signals](#)

## Alert logic

We have set the condition configuration automatically based on popular settings for this metric. Please review and make changes as needed.

Threshold ☒ Static ☐ Dynamic

Aggregation type

Operator

Threshold value \*  %

## Split by dimensions

Use dimensions to monitor specific time series and provide context to the fired alert. Dimensions can be either number or string columns. If you select more than one dimension value, each time series that results from the combination will trigger its own alert and will be charged separately. [About monitoring multiple time series](#)

Dimension name	Operator	Dimension values	Include all future values
<input type="text" value="Select dimension"/>	<input type="text" value="="/>	<input type="text" value="0 selected"/> <small>Add custom value</small>	<input type="checkbox"/>

## When to evaluate

[Review + create](#) [Previous](#) [Next: Actions >](#)

Home &gt; rg-prj3-prd-northeurope-001 | Cost alerts (preview) &gt; Cost Management: PRJ3\_LYON2 | Cost alerts &gt;

## Alert rules

Cost management

Scope: **PRJ3\_LYON2** (change)[+ Add](#) [Refresh](#) [Delete](#) [Help](#)

Name	Status	Condition	Action	Scope
<a href="#">Daily anomaly by resou...</a>	Active	Anomaly detected	Email 1 other	PRJ3_LYON2

## Create alert rule

PRJ3\_LYON2 (Subscription)

Subscribe to alerts and get notified about changes. [Learn more](#)

Condition

Alert type \*

View

Start on \*  
  
until 2025-01-14

Notifications

Subject \*

Recipients \*  

david.chelien@innovationneosoftfrout...

Message

Language \*

Information

Alert name \*

Create

Cancel

Home > aks-prj3-prd-northeurope-001 | Alerts

aks-prj3-prd-northeurope-001 | Alerts

Search

View as timeline (preview) | Create | Set up recommendations | Alert rules | Prometheus rule groups

New! View alerts visualized on a timeline for a clearer picture of your events. You can switch between views anytime. [View as timeline \(preview\)](#)

Search

Resource name: aks-prj3-prd-northeurope-001 Time range: Past 24 hours

Total alerts: 1 Critical: 0 Error: 0 Warning: 0 Informational: 1 Verbose: 0

Name Severity Affected resource

Memory Working Set Percentage - aks-prj3-prd-northeurope-001 3 - Informational aks-prj3-prd-northeurope-001

Showing 1 - 1 of 1 results.

Memory Working Set Percentage - aks-prj3-prd-northeurope-001

Metrics alert details

Copy link Go to alert rule

Summary History

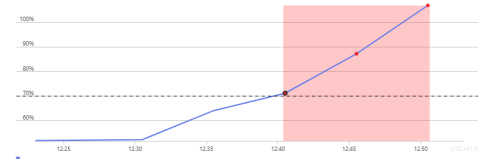
General details

Severity	Fired time	Affected resource	Monitor service	Alert condition	User response
3 - Informational	1/14/2024, 12:54 PM	aks-prj3-prd-northeurope...	Platform	Fired	New

Why did this alert fire?

The average node\_memory\_working\_set\_percentage crossed the threshold of 70% and reached 106.93%.

Value (when alert fired)	Threshold	Deviation
106.93%	70%	36.93%



Memory Working Set Percentage (Avg) 72.3222%

Additional details

Home > rg-prj3-prd-northeurope-001 | Budgets

## Create budget

Budget

Create a budget Set alerts

Configure alert conditions and send email notifications based on your spend.

### Alert conditions

Type	% of budget	Amount	Action group
Actual	90	135	Recommended...
Select type	Enter %	-	None

Manage action group

### Alert recipients (email)

Alert recipients (email)

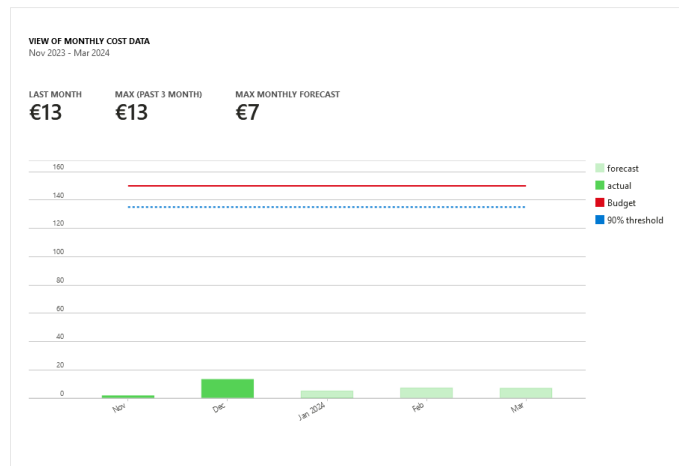
Example email address: david.chelani@supinfo.com

It is recommended to add azure-noreply@microsoft.com to your email allow list to ensure alert mails do not go to your spam folder.

### Language preference

Select your preferred language for receiving the alert email for all recipients provided above. Default is the language associated to your enrollment.

Previous Create



Home > rg-prj3-prd-northeurope-001 | Budgets

## rg-prj3-prd-northeurope-001 | Budgets

Resource group

Search Add Refresh Help

Security

Deployment stacks

Policies

Properties

Locks

Cost Management

...

How would you rate defining and enforcing spending limits? →

Scope: rg-prj3-prd-northeurope-001 Search by name All periods

Name	Scope	Reset period	Creation date	Expiration date	Budget	Forecasted	Evaluated spend	Progress	
budget-alert-threshold	rg-prj3-prd-northeurope...	BillingMonth	1/27/2024	1/26/2026	€150.00	0	€0.00	0.00%	...