



SUMMIT  
ONLINE / 2020

# “USER ROLES FOR THE ENTERPRISE”

**Arturs Lontons**

Technical Support Engineer

ZABBIX, LATVIA



# 01

## PERMISSION GRANULARITY

GRANULAR PERMISSION REQUIREMENTS IN  
CORPORATE ENVIRONMENTS



# PERMISSIONS GRANULARITY

## NOC Team role

- ✓ Access to Dashboards and maps
- ✓ Restrict unnecessary UI elements
- ✓ Restrict API access
- ✓ Restrict configuration
- ✓ Restrict closing problems

## Network Administrator role

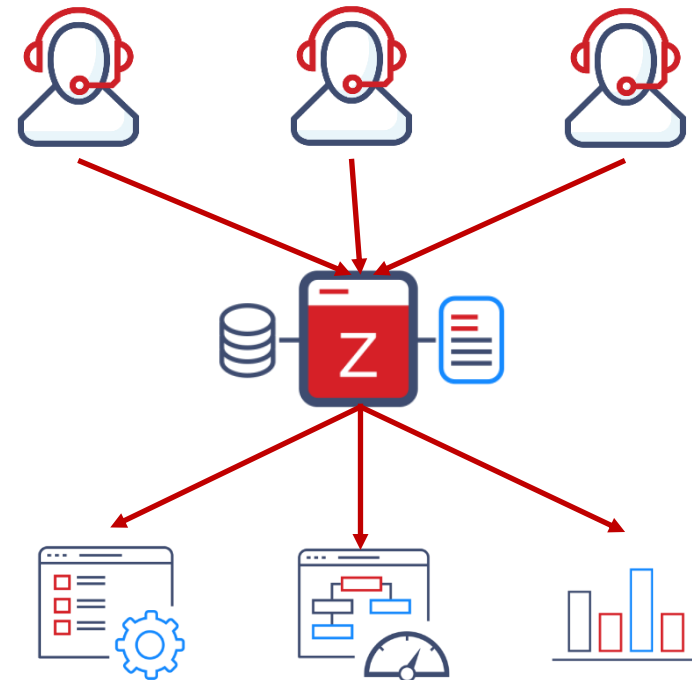
- ✓ Access to Dashboards and Maps
- ✓ Access to Configuration
- ✓ Restrict API access
- ✓ Restrict unnecessary UI elements



# ROLES AND MULTI-TENANCY

In multi-tenant environments granular permission play a very important role

- ✓ The UI should be as intuitive as possible for different roles and tenants
- ✓ Each tenant can have different monitoring requirements
- ✓ Restricted access to elements per tenant
- ✓ Isolation between tenants





# 02

## USER ROLES IN 5.2

IMPLEMENTING A MORE GRANULAR PERMISSION  
LOGIC WITH USER ROLES



# USER ROLE

Starting from 5.2 users will have a User role assigned to them. Depending on the role, a corresponding User type will also be assigned:

## Users

UserMediaPermissions

\* RoleUser role xSelect

User typeUser

Permissions

Host groupAll groups

PermissionsNone

Permissions can be assigned for user groups only.

Access to UI elements

MonitoringDashboardProblemsHostsOverviewLatest dataScreensMapsServices

InventoryOverviewHosts

ReportsAvailability reportTriggers top 100

Access to modules

No enabled modules found.

Access to API

Enabled

Access to actions

Create and edit dashboards and screensCreate and edit mapsAcknowledge problemsClose problems

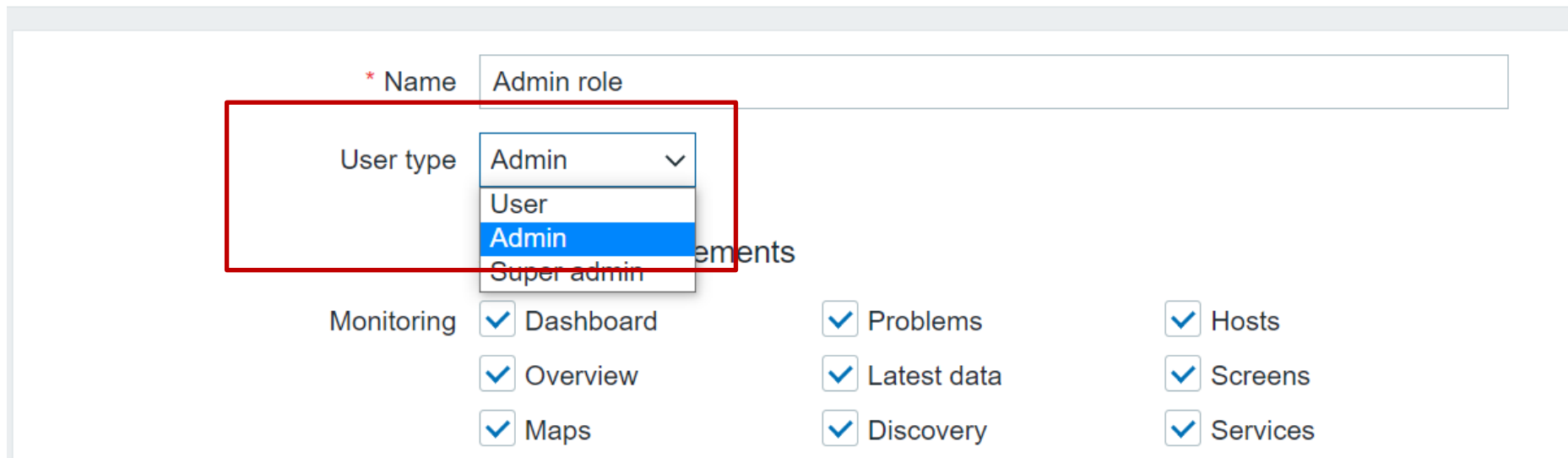
Change severityAdd problem commentsExecute scripts

AddCancel

# USER TYPES

- ❑ User types are not being removed
- ❑ A role is linked to one of the 3 user types

## User roles



\* Name Admin role

User type Admin ▾

User

Admin

Super admin

Monitoring ☒ Dashboard ☒ Problems ☒ Hosts

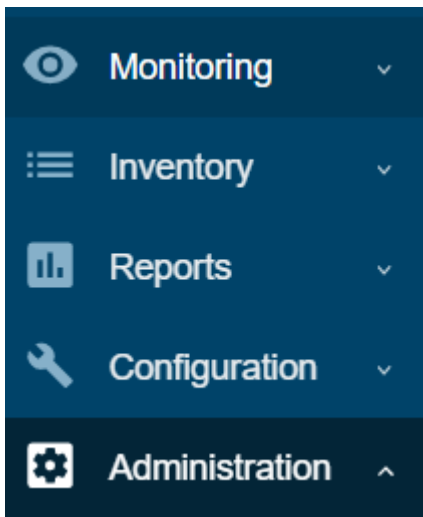
☒ Overview ☒ Latest data ☒ Screens

☒ Maps ☒ Discovery ☒ Services

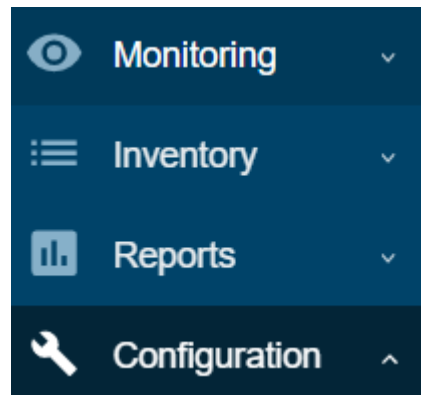
# USER TYPES

Frontend sections restricted by user type

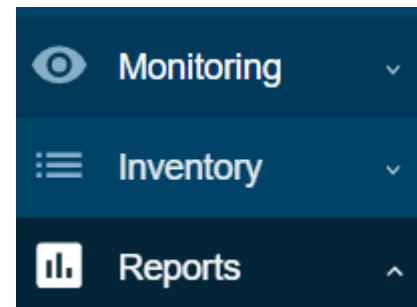
Superadmin:



Admin:



User:





# DEFAULT USER ROLES

Available in Administration – User roles

By default this section contains 4 preconfigured user roles

- ✓ Super admin role
- ✓ Admin role
- ✓ User role
- ✓ Guest role



# SUPER ADMIN ROLE

- ✓ Default Super admin role is static – users cannot modify this role

<input type="checkbox"/> Name ▲	#	Users
<input type="checkbox"/> Admin role	Users 1	<a href="#">Tenant Admin</a>
<input type="checkbox"/> Guest role	Users	
<input checked="" type="checkbox"/> Super admin role	Users 1	<a href="#">Admin (Zabbix Administrator)</a>
<input type="checkbox"/> User role	Users 4	<a href="#">API</a> , <a href="#">Arturs</a> , <a href="#">guest</a> , <a href="#">Tenant User</a>

Displaying 4 of 4 found

- ✓ This is because at least a single Super admin role MUST exist in your environment
- ✓ Newly created roles of type Super admin can be modified

# USER ROLES SECTION

Each of the default roles contains the maximum allowed permissions per user type:

**ZABBIX** << User roles

\* Name: Admin role

User type: Admin

Access to UI elements

Monitoring	<input checked="" type="checkbox"/> Dashboard	<input checked="" type="checkbox"/> Problems	<input checked="" type="checkbox"/> Hosts
	<input checked="" type="checkbox"/> Overview	<input checked="" type="checkbox"/> Latest data	<input checked="" type="checkbox"/> Screens
	<input checked="" type="checkbox"/> Maps	<input checked="" type="checkbox"/> Discovery	<input checked="" type="checkbox"/> Services
Inventory	<input checked="" type="checkbox"/> Overview	<input checked="" type="checkbox"/> Hosts	
Reports	<input type="checkbox"/> System information	<input checked="" type="checkbox"/> Availability report	<input checked="" type="checkbox"/> Triggers top 100
	<input type="checkbox"/> Audit	<input type="checkbox"/> Action log	<input checked="" type="checkbox"/> Notifications
Configuration	<input checked="" type="checkbox"/> Host groups	<input checked="" type="checkbox"/> Templates	<input checked="" type="checkbox"/> Hosts
	<input checked="" type="checkbox"/> Maintenance	<input checked="" type="checkbox"/> Actions	<input type="checkbox"/> Event correlation
	<input checked="" type="checkbox"/> Discovery	<input checked="" type="checkbox"/> Services	
Administration	<input type="checkbox"/> General	<input type="checkbox"/> Proxies	<input type="checkbox"/> Authentication
	<input type="checkbox"/> User groups	<input type="checkbox"/> User roles	<input type="checkbox"/> Users
	<input type="checkbox"/> Media types	<input type="checkbox"/> Scripts	<input type="checkbox"/> Queue

# UI ELEMENT RESTRICTION

Access to UI elements for each role can be restricted

- ✓ NOC user role that has access only to Dashboards and maps

## User roles

\* Name

User type

Access to UI elements

Monitoring	<input checked="" type="checkbox"/> Dashboard	<input type="checkbox"/> Problems	<input type="checkbox"/> Hosts
	<input type="checkbox"/> Overview	<input type="checkbox"/> Latest data	<input type="checkbox"/> Screens
	<input checked="" type="checkbox"/> Maps	<input type="checkbox"/> Discovery	<input type="checkbox"/> Services
Inventory	<input type="checkbox"/> Overview	<input type="checkbox"/> Hosts	
Reports	<input type="checkbox"/> System information	<input type="checkbox"/> Availability report	<input type="checkbox"/> Triggers top 100
	<input type="checkbox"/> Audit	<input type="checkbox"/> Action log	<input type="checkbox"/> Notifications
Configuration	<input type="checkbox"/> Host groups	<input type="checkbox"/> Templates	<input type="checkbox"/> Hosts
	<input type="checkbox"/> Maintenance	<input type="checkbox"/> Actions	<input type="checkbox"/> Event correlation
	<input type="checkbox"/> Discovery	<input type="checkbox"/> Services	
Administration	<input type="checkbox"/> General	<input type="checkbox"/> Proxies	<input type="checkbox"/> Authentication
	<input type="checkbox"/> User groups	<input type="checkbox"/> User roles	<input type="checkbox"/> Users
	<input type="checkbox"/> Media types	<input type="checkbox"/> Scripts	<input type="checkbox"/> Queue

## Users

User Media Permissions

\* Role

User type

Permissions

Host group	Permissions
All groups	Read-write

Permissions can be assigned for user groups only.

Access to UI elements

Monitoring ☒ Dashboard ☐ Problems ☐ Hosts ☐ Overview ☐ Latest data ☐ Screens ☒ Maps ☐ Services

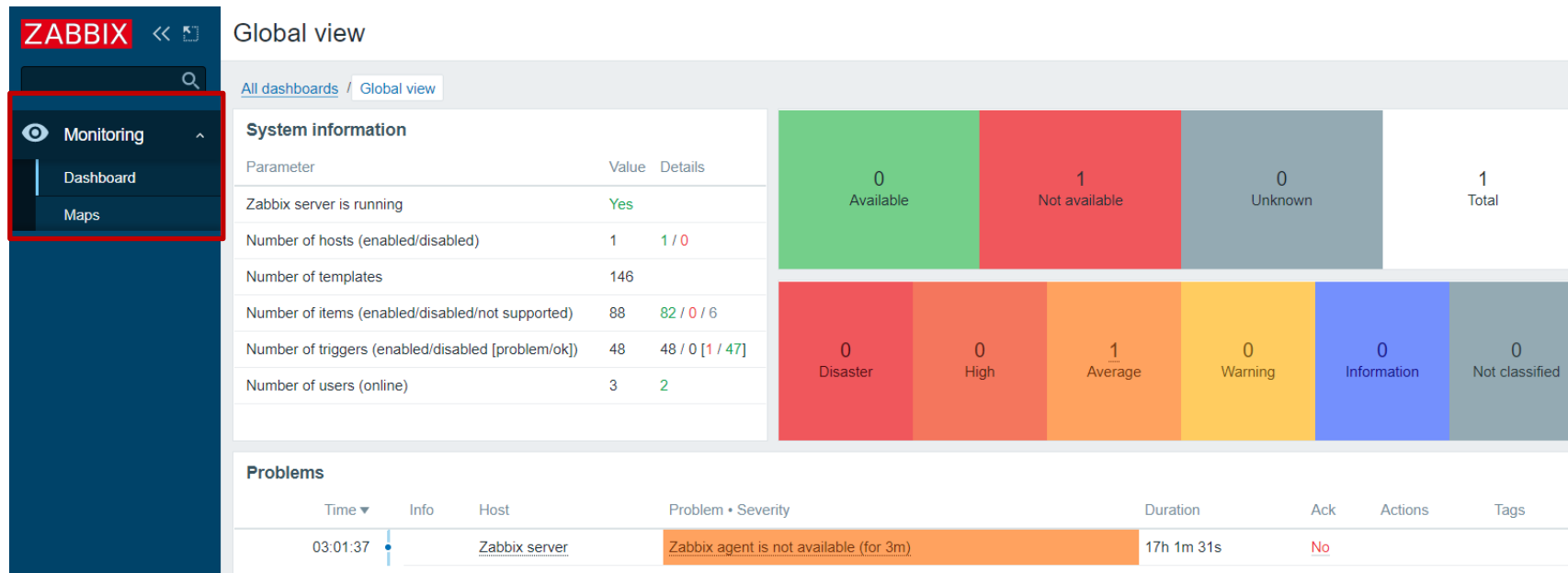
Inventory ☐ Overview ☐ Hosts

Reports ☐ Availability report ☐ Triggers top 100

# UI ELEMENT RESTRICTION

Access to UI elements for each role can be restricted

- ✓ NOC user role that has access only to Dashboards and maps



The screenshot displays the Zabbix web interface. On the left, a sidebar menu is visible with the 'Monitoring' section highlighted by a red box. The main content area shows the 'Global view' dashboard. The 'System information' section includes a table of system parameters and a corresponding bar chart. The 'Problems' section at the bottom shows a list of issues, with one problem highlighted in orange.

**System information**

Parameter	Value	Details
Zabbix server is running	Yes	
Number of hosts (enabled/disabled)	1	1 / 0
Number of templates	146	
Number of items (enabled/disabled/not supported)	88	82 / 0 / 6
Number of triggers (enabled/disabled [problem/ok])	48	48 / 0 [1 / 47]
Number of users (online)	3	2

**Problems**

Time	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
03:01:37		Zabbix server	Zabbix agent is not available (for 3m)	17h 1m 31s	No		



# HOST GROUP PERMISSIONS

Note, that User Group access to Host Group still have to be properly assigned!

[User group](#) [Permissions](#) [Tag filter](#)

Permissions

Host group

*All groups*

Application Servers

Linux servers

Network devices

Riga Servers

Permissions

None

Read-write

Read

Deny

None

Read-write

Read

Deny

None

Read-write

Read

Deny

None

Read-write

Read

Deny

None

Select

Read-write

Read

Deny

None

☐ Include subgroups

[Add](#)

Add

Cancel

# ACCESS TO API

API Access can also be restricted for each role

- ✓ Used when creating API specific user roles

Access to API

Enabled ☒

API methods

Allow list

Deny list

type here to search

Select

# API METHOD RESTRICTION

Ability to implement API method Allow or Deny lists

- ✓ Useful in environments with many administrative roles
- ✓ For example - create a user that can only use get methods

## Access to API

Enabled ☒

API methods

Allow list

Deny list

event.get ✕

history.get ✕

host.get ✕

item.get ✕

template.get ✕

trend.get ✕

trigger.get ✕

type here to search

Select

# API METHOD RESTRICTION EXAMPLE

If the method execution is not permitted, «no permission to call method» error will be displayed:

```
{
  "jsonrpc": "2.0",
  "error": {
    "code": -32602,
    "message": "Invalid params.",
    "data": "No permissions to call \"host.create\"."
  },
  "id": 1
}
```



# ACCESS TO ACTIONS

Each role can have a specific list of actions that it can perform with respect to the role User type.

User type: User

## Access to actions

- ☒ Create and edit dashboards and screens
- ☒ Create and edit maps
- ☐ Create and edit maintenance
- ☒ Acknowledge problems
- ☒ Close problems
- ☒ Change severity
- ☒ Add problem comments
- ☒ Execute scripts

User type: Admin

## Access to actions

- ☒ Create and edit dashboards and screens
- ☒ Create and edit maps
- ☒ Create and edit maintenance
- ☒ Acknowledge problems
- ☒ Close problems
- ☒ Change severity
- ☒ Add problem comments
- ☒ Execute scripts





# RESTRICTING ACTIONS EXAMPLE (1)

## Restricting the role

### Access to actions

- ☒ Create and edit dashboards and screens
- ☒ Create and edit maps
- ☐ Create and edit maintenance
- ☐ Acknowledge problems
- ☐ Close problems
- ☒ Change severity
- ☒ Add problem comments
- ☒ Execute scripts

## Result in the frontend

### Update problem

Problem Zabbix agent is not available (for 3m)

Message

History

Time	User	User action	Message
------	------	-------------	---------

Scope

- ☒ Only selected problem
- ☐ Selected and all other problems of related triggers 1 event

Change severity

☐ Not classified Information Warning Average High Disaster

Acknowledge

☐

Close problem

☐

# RESTRICTING ACTIONS EXAMPLE (2)

## Unrestricted role

### Access to actions

- ☒ Create and edit dashboards and screens
- ☒ Create and edit maps
- ☐ Create and edit maintenance
- ☒ Acknowledge problems
- ☒ Close problems
- ☒ Change severity
- ☒ Add problem comments
- ☒ Execute scripts

## Result in the frontend

### Update problem

Problem Zabbix agent is not available (for 3m)

Message

History

Time	User	User action	Message
------	------	-------------	---------

Scope

- ☒ Only selected problem
- ☐ Selected and all other problems of related triggers 1 event

Change severity

☐ Not classified Information Warning Average High Disaster

Acknowledge ☒

Close problem ☒

# DEFAULT ACCESS

Default access for new elements of different types can be enabled or disabled for user roles:

Default access to new actions ☒

Default access to new modules ☒

Default access to new UI elements ☒

If enabled, whenever a new element is added, the user belonging to this role will automatically have access to it.



# ROLE ASSIGNMENT POST-UPGRADE

After migration to 5.2, the users will have the pre-created Admin/User/Super admin roles assigned to them:

UserMediaPermissions

\* RoleAdmin role xSelect

User typeAdmin

Permissions

Host group	Permissions
All groups	None
Linux servers	Read-write
Training/Servers	Read-write

UserMediaPermissions

\* RoleUser role xSelect

User typeUser

Permissions

Host group	Permissions
All groups	None
Linux servers	Read-write
Training/Servers	Read-write

# 03

## EXAMPLE USE CASES

HOW ROLES CAN BE USED IN DIFFERENT  
ENVIRONMENTS





# READ ONLY ROLE

A role that has no ability to create or modify any elements

- ✓ Read only access to dashboards
- ✓ Read only access to problems
- ✓ No access to API
- ✓ No permissions to execute frontend scripts



# READ ONLY ROLE

First off, let's decide on User type and sections, which this role should have access to

\* Name

User type

Access to UI elements

Monitoring	<input checked="" type="checkbox"/> Dashboard	<input checked="" type="checkbox"/> Problems	<input checked="" type="checkbox"/> Hosts
	<input type="checkbox"/> Overview	<input checked="" type="checkbox"/> Latest data	<input checked="" type="checkbox"/> Screens
	<input checked="" type="checkbox"/> Maps	<input type="checkbox"/> Discovery	<input type="checkbox"/> Services
Inventory	<input type="checkbox"/> Overview	<input type="checkbox"/> Hosts	
Reports	<input type="checkbox"/> System information	<input type="checkbox"/> Availability report	<input type="checkbox"/> Triggers top 100
	<input type="checkbox"/> Audit	<input type="checkbox"/> Action log	<input type="checkbox"/> Notifications
Configuration	<input type="checkbox"/> Host groups	<input type="checkbox"/> Templates	<input type="checkbox"/> Hosts
	<input type="checkbox"/> Maintenance	<input type="checkbox"/> Actions	<input type="checkbox"/> Event correlation
	<input type="checkbox"/> Discovery	<input type="checkbox"/> Services	
Administration	<input type="checkbox"/> General	<input type="checkbox"/> Proxies	<input type="checkbox"/> Authentication
	<input type="checkbox"/> User groups	<input type="checkbox"/> User roles	<input type="checkbox"/> Users
	<input type="checkbox"/> Media types	<input type="checkbox"/> Scripts	<input type="checkbox"/> Queue

\* At least one UI element must be checked.

# READ ONLY ROLE

We also need to restrict access to actions, API and decide on the new UI element and module permission logic

Default access to new UI elements ☒

Access to modules

No enabled modules found.

Default access to new modules ☐

Access to API

Enabled ☐

API methods Allow list Deny list

Select

Access to actions

- ☐ Create and edit dashboards and screens
- ☐ Create and edit maps
- ☒ Create and edit maintenance
- ☐ Acknowledge problems
- ☐ Close problems
- ☐ Change severity
- ☐ Add problem comments
- ☐ Execute scripts

Default access to new actions ☐

# READ ONLY ROLE

- ❑ No option to create or edit a dashboard
- ❑ Access to dashboards is granted and evaluated based on Dashboard sharing options and User group – Host group relationship.

## Dashboards

Create dashboard

Filter

Name

Show

All

Created by me

Apply

Reset

☐ Name ▲

☐ Global view

☐ Network Dashboard

☐ Riga Dashboard

☐ Zabbix server health

Displaying 4 of 4 found

# READ ONLY ROLE

- ✓ Restricted UI elements hidden
- ✓ Acknowledge button is not clickable for this Role

The screenshot shows the Zabbix web interface for the 'Problems' page. The left sidebar menu is highlighted with a red box, showing the following items: Monitoring, Dashboard, Problems, Hosts, Latest data, Screens, and Maps. The main content area displays various filters and a table of problems. The 'Ack' button in the table is highlighted with a red box.

**Problems Page Filters:**

- Show: Recent problems, Problems, History
- Host groups: type here to search, Select
- Hosts: type here to search, Select
- Application: , Select
- Triggers: type here to search, Select
- Problem:
- Severity: ☐ Not classified, ☐ Warning, ☐ High, ☐ Information, ☐ Average, ☐ Disaster
- Age less than: ☐ 14 days
- Host inventory: Type, Remove
- Tags: And/Or, Or, tag, Contains, Equals, value, Remove
- Show tags: None, 1, 2, 3, Tag name: Full, Shortened, None
- Tag display priority: comma-separated list
- Show operational data: None, Separately, With problem name
- Show suppressed problems: ☐ Show unacknowledged only: ☐
- Compact view: ☐ Show timeline: ☒
- Show details: ☐ Highlight whole row: ☐

**Problem List:**

Time	Severity	Info	Host	Problem	Duration	Ack	Actions	Tags
10:22:01	Average		Linux Host B	/boot: Disk space is critically low (used > 90 %)	1m 26s	No		
10:22:01	Average		Linux Host B	/: Disk space is critically low (used > 90 %)	1m 26s	No		

Displaying 2 of 2 found



# RESTRICT ACCESS TO ADMINISTRATION SECTIONS

A Superadmin type role that has no access to User configuration and General Zabbix settings

- ✓ Ability to Create and manage proxies
- ✓ Ability to define media types and frontend scripts
- ✓ Access to queue section to see the Zabbix server and proxy health status

# RESTRICT ACCESS TO ADMINISTRATION SECTIONS

User type – Super admin. General and User sections are restricted for this role

\* Name

User type

Access to UI elements

Monitoring	<input checked="" type="checkbox"/> Dashboard	<input checked="" type="checkbox"/> Problems	<input checked="" type="checkbox"/> Hosts
	<input checked="" type="checkbox"/> Overview	<input checked="" type="checkbox"/> Latest data	<input checked="" type="checkbox"/> Screens
	<input checked="" type="checkbox"/> Maps	<input checked="" type="checkbox"/> Discovery	<input checked="" type="checkbox"/> Services
Inventory	<input checked="" type="checkbox"/> Overview	<input checked="" type="checkbox"/> Hosts	
Reports	<input checked="" type="checkbox"/> System information	<input checked="" type="checkbox"/> Availability report	<input checked="" type="checkbox"/> Triggers top 100
	<input checked="" type="checkbox"/> Audit	<input checked="" type="checkbox"/> Action log	<input checked="" type="checkbox"/> Notifications
Configuration	<input checked="" type="checkbox"/> Host groups	<input checked="" type="checkbox"/> Templates	<input checked="" type="checkbox"/> Hosts
	<input checked="" type="checkbox"/> Maintenance	<input checked="" type="checkbox"/> Actions	<input checked="" type="checkbox"/> Event correlation
	<input checked="" type="checkbox"/> Discovery	<input checked="" type="checkbox"/> Services	
Administration	<input type="checkbox"/> General	<input checked="" type="checkbox"/> Proxies	<input type="checkbox"/> Authentication
	<input type="checkbox"/> User groups	<input type="checkbox"/> User roles	<input type="checkbox"/> Users
	<input checked="" type="checkbox"/> Media types	<input checked="" type="checkbox"/> Scripts	<input checked="" type="checkbox"/> Queue

# RESTRICT ACCESS TO ADMINISTRATION SECTIONS

- ✓ Restricted Administration elements are hidden
- ✓ The Monitoring Super admin user still has the ability to create new **Proxies**, **Media Types**, **Scripts** and has access to the **Queue** section

The screenshot displays the Zabbix web interface. On the left, the sidebar menu is visible, with the 'Administration' section expanded and highlighted by a red box. The main content area shows the 'Proxies' configuration page. At the top right, there is a 'Create proxy' button. Below it, there is a search bar and a filter icon. The main table lists proxies with columns: Name, Mode, Encryption, Compression, Last seen (age), Host count, Item count, Required performance (vps), and Hosts. The table contains one entry: 'Riga Proxy' with Mode 'Active', Encryption 'None', Compression 'On', Last seen 'Never', Host count '1', Item count '42', Required performance '0.5', and Hosts 'Linux Host C'. At the bottom, there are buttons for 'Enable hosts', 'Disable hosts', and 'Delete'.

Name	Mode	Encryption	Compression	Last seen (age)	Host count	Item count	Required performance (vps)	Hosts
Riga Proxy	Active	None	On	Never	1	42	0.5	Linux Host C

# ROLES FOR MULTI-TENANT ENVIRONMENTS

Zabbix Dashboards and maps are used by multiple tenants to provide monitoring data

- ✓ Read only access to dashboards
- ✓ Read only access to maps
- ✓ No access to API
- ✓ No access to configuration
- ✓ Isolation per tenant



# ROLES FOR MULTI-TENANT ENVIRONMENTS

We will be creating a user type role with very limited access to UI

\* Name

User type

Access to UI elements

Monitoring	<input checked="" type="checkbox"/> Dashboard	<input type="checkbox"/> Problems	<input type="checkbox"/> Hosts
	<input type="checkbox"/> Overview	<input type="checkbox"/> Latest data	<input type="checkbox"/> Screens
	<input checked="" type="checkbox"/> Maps	<input type="checkbox"/> Discovery	<input type="checkbox"/> Services
Inventory	<input type="checkbox"/> Overview	<input type="checkbox"/> Hosts	
Reports	<input type="checkbox"/> System information	<input type="checkbox"/> Availability report	<input type="checkbox"/> Triggers top 100
	<input type="checkbox"/> Audit	<input type="checkbox"/> Action log	<input type="checkbox"/> Notifications
Configuration	<input type="checkbox"/> Host groups	<input type="checkbox"/> Templates	<input type="checkbox"/> Hosts
	<input type="checkbox"/> Maintenance	<input type="checkbox"/> Actions	<input type="checkbox"/> Event correlation
	<input type="checkbox"/> Discovery	<input type="checkbox"/> Services	
Administration	<input type="checkbox"/> General	<input type="checkbox"/> Proxies	<input type="checkbox"/> Authentication
	<input type="checkbox"/> User groups	<input type="checkbox"/> User roles	<input type="checkbox"/> Users
	<input type="checkbox"/> Media types	<input type="checkbox"/> Scripts	<input type="checkbox"/> Queue



# ROLES FOR MULTI-TENANT ENVIRONMENTS

Let's use tag-based permissions to isolate our Hosts per tenant

User group Permissions ● Tag filter ●

Permissions	Host group	Permissions
	All groups	None
	Linux servers	<div>Read-write Read Deny None</div>

Read-write Read Deny None

☐ Include subgroups

[Add](#)

User group Permissions ● Tag filter ●

Permissions	Host group	Tags	Action
	Linux servers	Tenant: Zabbix SIA	<a href="#">Remove</a>

☐ Include subgroups

[Add](#)

# ROLES FOR MULTI-TENANT ENVIRONMENTS

Don't forget to tag your problems! This time I'm doing the tagging on the host level:

[Host](#) [Templates 1](#) [IPMI](#) [Tags 2](#) [Macros 2](#) [Inventory](#) [Encryption](#)

Name	Value	Action
<input type="text" value="Tenant"/>	<input type="text" value="Zabbix SIA"/>	<a href="#">Remove</a>
<input type="text" value="DC"/>	<input type="text" value="Riga"/>	<a href="#">Remove</a>

[Add](#)

Update

Clone

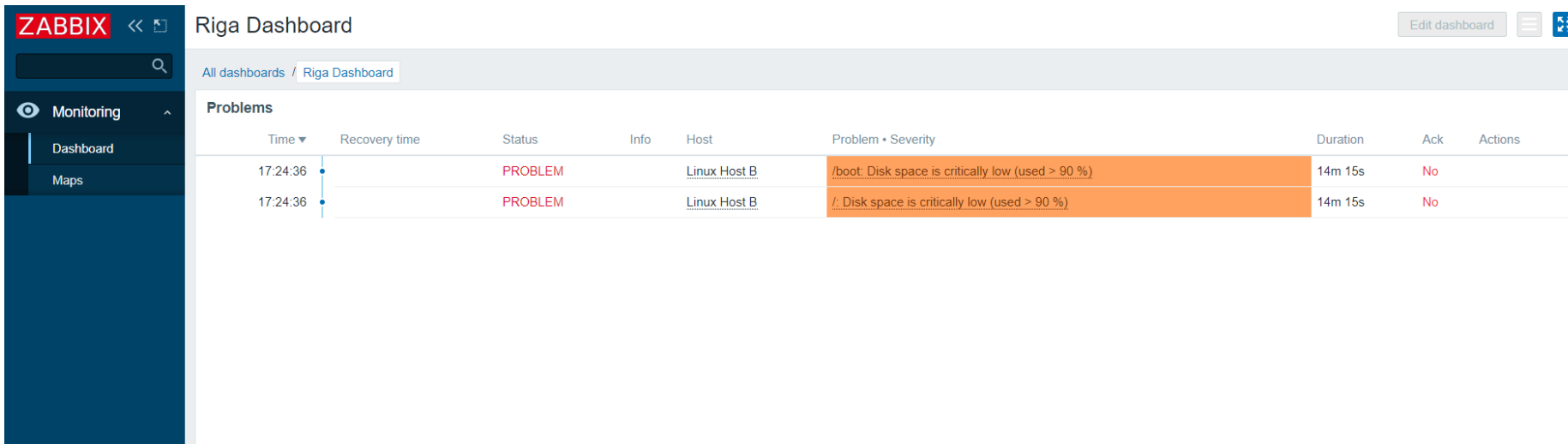
Full clone

Delete

Cancel

# ROLES FOR MULTI-TENANT ENVIRONMENTS

- ✓ The UI is restricted only to the required monitoring sections
- ✓ Tag-based permission ensure that we are seeing problems related to our tenant



The screenshot displays the Zabbix web interface. On the left is a dark blue sidebar with the ZABBIX logo and navigation links for Monitoring, Dashboard, and Maps. The main content area is titled 'Riga Dashboard' and shows a 'Problems' section. A table lists two active problems for 'Linux Host B', both indicating critically low disk space on the /boot and / partitions. The table columns include Time, Recovery time, Status, Info, Host, Problem • Severity, Duration, Ack, and Actions.

Time ▼	Recovery time	Status	Info	Host	Problem • Severity	Duration	Ack	Actions
17:24:36		PROBLEM		Linux Host B	/boot: Disk space is critically low (used > 90 %)	14m 15s	No	
17:24:36		PROBLEM		Linux Host B	/: Disk space is critically low (used > 90 %)	14m 15s	No	

# ROLES – WHAT'S NEXT?

Implementing user roles can help you manage your Zabbix environment!

- ✓ Improve auditing



- ✓ Restrict API access



- ✓ Restrict configuration



- ✓ Remove unwanted UI elements



Thank you!

