



ZABBIX
PREMIUM PARTNER

ZABBIX
CERTIFIED TRAINER

Webinar

Zabbix organization of permissions

all your microphones are muted

ask your questions in Q&A, not in the Chat

use Chat for discussion, networking or applause

There is no one way how to do it right



Purpose of the system



Newly installed system vs. 10 year upgraded Zabbix



Unknowns... in the beginning

Purpose of the system



Human oriented



Alert oriented

New system – takes time but you'll thank yourself later



Talk, talk, talk ...find out as much as possible about the processes



Who, how, what for will it be used, onboarding of new technologies



Prepare naming convention, stick to it.....change it 😊

Old systems – can't change it completely, simplify



Talk, talk, talk ...find out as much as possible about the processes



Who, how, what for will it be used, onboarding of new technologies



Prepare naming convention, stick to it.....change it 😊

Unknown in the beginnings



Exceptions will always occur ! It's not just the one guy ...



If you do a good job, you "will be rewarded"



Teams that didn't want to be part of it in the beginning will join....later



1

Host groups

Host groups - basics

- ▶ Every host needs at least one host group
- ▶ Only Super admin users can create host groups
- ▶ Deleting host groups doesn't delete hosts in them
- ▶ You can't delete host group if it's the only one for the host

- ▶ Nesting applies: **grandparent group/parent group/child group/Cisco**
- ▶ Parent host groups will **not** be created automatically

- ▶ Using leading or trailing slashes, or several slashes in a row is not allowed
- ▶ Escaping of '/' is not supported.



Host groups – think about it in front

- ▶ Nesting
- ▶ Structure
- ▶ “Reversed tags” ?
- ▶ Don’t go ballistic (3 – 4 level in nesting might cover it all)
- ▶ Read all approach ? Can be useful in some environments



Host groups – the big mystery

- ▶ New subgroup to an existing parent host group inherits user group permissions from parent
- ▶ If you create a parent to existing subgroup no permissions are set
- ▶ If possible don't create parents
- ▶ Hint: Doesn't work in real life too 😊



Zabbix organization of permissions

Host groups – the big mystery

- ▶ “Apply permissions and tag filters to all subgroups” button
- ▶ Who reads documentation upfront ?

Host groups

Name ▲
 all
 all/customer
 all/customer/linux
 all/customer1
 all/customer1/linux

0 selected

Host group

* Group name

Apply permissions and tag filters to all subgroups



Host groups – the big mystery

- ▶ Marking this checkbox and clicking on *Update* will apply the same level of permissions and tag filters to all current and future subgroups of the host group being edited.
- ▶ Note that this option is not saved in the database and will override existing permissions. Any changes made through this option can be reverted only manually.
- ▶ Be careful with host groups



Host groups – what's the best way ?

- ▶ Consider following scenarios
- ▶ Customer1/OS/Linux, Customer2/App/MyApp
- ▶ All/Customer1/OS/Linux, All/Customer2/OS/Linux,
- ▶ All/Linux/Customer1/OS, All/Linux/Customer2/OS



Zabbix organization of permissions

Host groups – best of both worlds?

- ▶ Run two trees if it makes sense to your environment
- ▶ Tree 1 (Technology): Linux/RHEL, Linux/Ubuntu, Windows/Servers...
- ▶ Tree 2 (Location): CZ/Prague/DC1, CZ/Brno, SK/Bratislava...

New host

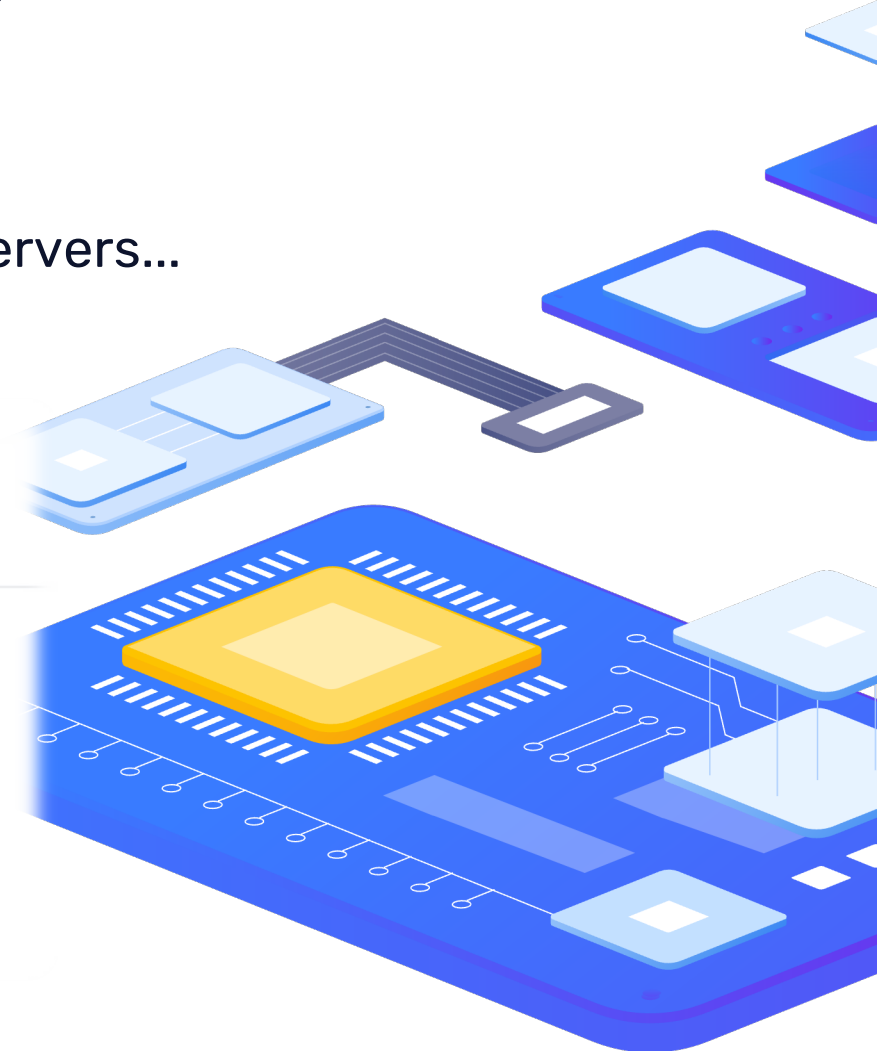
Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name

Visible name

Templates

* Host groups



Zabbix organization of permissions

Host groups – the pain?

- ▶ Join the dark side: API magic and automation is required

New host

Host IPMI Tags Macros Inventory Encryption Value mapping

* Host name

Visible name

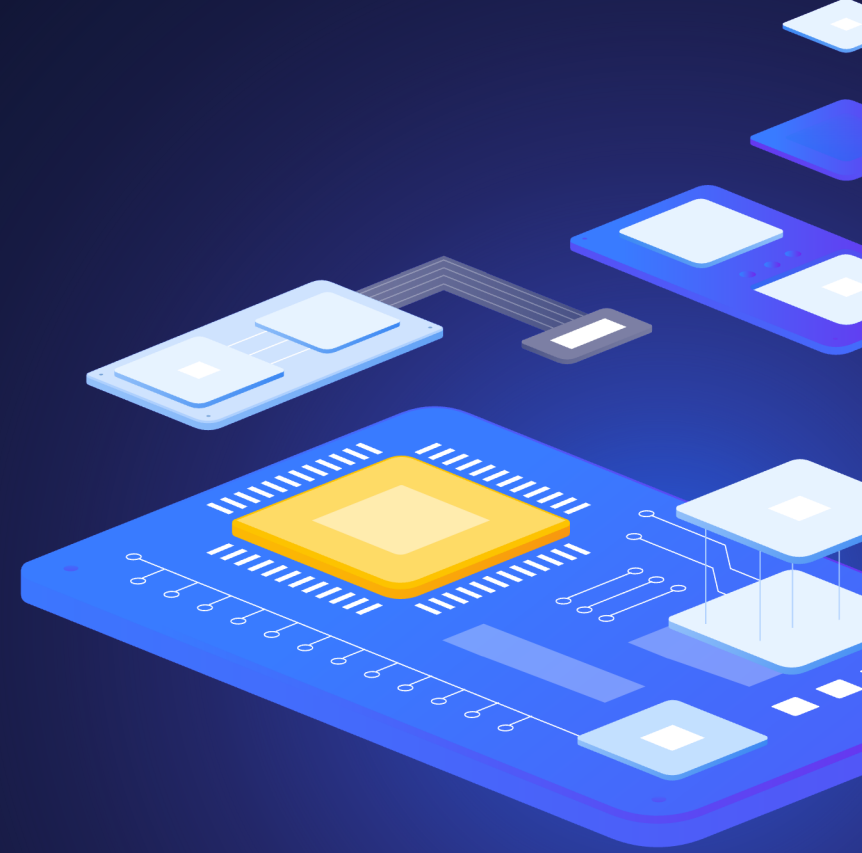
Templates

* Host groups



2

Template groups



Template groups - basics

- ▶ Every template needs at least one template group
- ▶ Only Super admin users can create template groups
- ▶ Deleting template groups doesn't delete templates in them
- ▶ You can't delete template group if it's the only one for a template

- ▶ Nesting applies: **grandparent group/parent group/child group/templates**
- ▶ Parent host groups will **not** be created automatically

- ▶ Using leading or trailing slashes, or several slashes in a row is not allowed
- ▶ Escaping of '/' is not supported.



Template groups – think about it in front

- ▶ Nesting
- ▶ Structure
- ▶ Don't go ballistic (3 – 4 level in nesting might cover it all)
- ▶ Read all approach ? Can be useful in some environments



Template groups – the big mystery

- ▶ New subgroup to an existing template group inherits user group permissions from parent
- ▶ If you create a parent to existing subgroup no permissions are set
- ▶ “Apply permissions and tag filters to all subgroups” button
- ▶ Same as in host groups scenario



Template groups – the big mystery

- ▶ Marking this checkbox and clicking on *Update* will apply the same level of permissions and tag filters to all current and future subgroups of the host group being edited.
- ▶ Note that this option is not saved in the database and will override existing permissions. Any changes made through this option can be reverted only manually.
- ▶ Be careful with template groups as well 😊



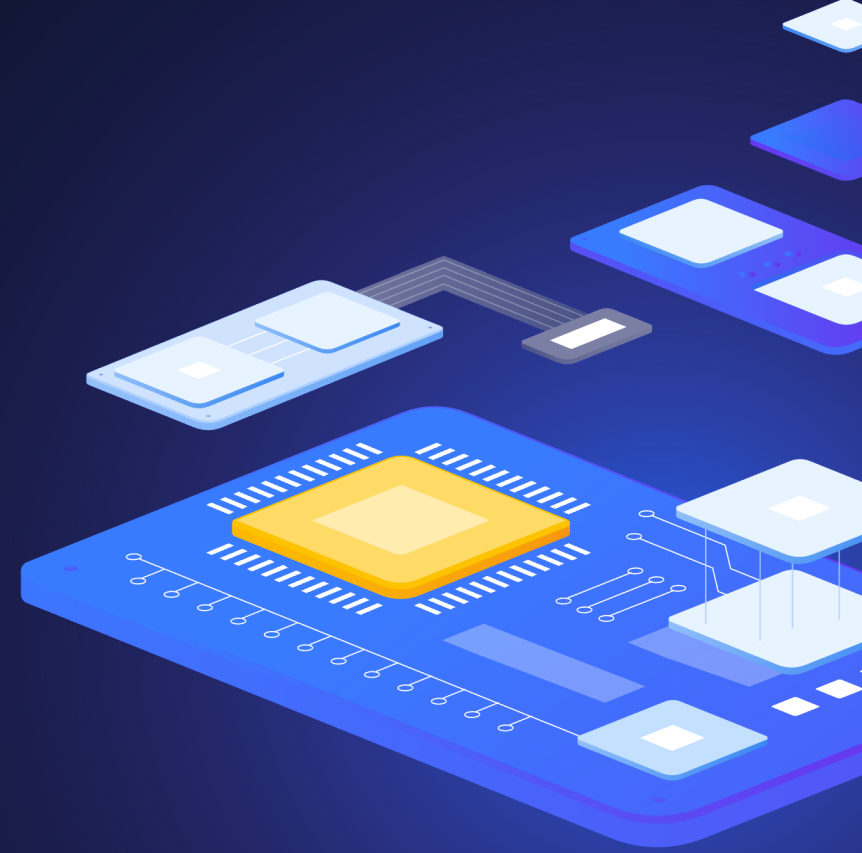
Host groups – what's the best way ?

- ▶ Consider following scenarios
- ▶ Customer1/Templates, Customer2/Templates
- ▶ All/Linux/Customer1, All/Linux/Customer2
- ▶ Keep your naming as close as possible to host groups



3

User groups



Zabbix organization of permissions

User groups - basics

- ▶ Permissions start here (they're propagated to users)
- ▶ User needs at least one user group

- ▶ Template permissions (read-write, read, deny)
- ▶ Host permissions (read-write, read, deny)
- ▶ Problem tag filter (All tags, tags list)

- ▶ It will get a bit more complicated from now



Zabbix organization of permissions

User groups - basics

- ▶ Name it and configure it

User groups

User group [Template permissions](#) [Host permissions](#) [Problem tag filter](#)

* Group name

Users

Frontend access ▼

LDAP Server ▼

Multi-factor authentication ▼

Enabled

Debug mode



Zabbix organization of permissions

User groups - basics

► Template permissions

User groups

User group **Template permissions** Host permissions Problem tag filter

Permissions

Template groups

type here to search

[Add](#)



Zabbix organization of permissions

User groups - basics

► Host permissions

User groups

User group Template permissions **Host permissions** Problem tag filter

Permissions Host groups Permissions

type here to search Select Read-write Read Deny Remove

Add

Add Cancel



User groups - nasty details part 1

- ▶ If the same template/host group is added in several rows with different permissions set, the strictest permission will be applied.
- ▶ If a user group has **Read-write** permissions to a host and **Deny** or no permissions to a template linked to this host, the users of such group will not be able to edit templated items on the host, and template name will be displayed as *Inaccessible template*.
- ▶ “Read-write” permissions have precedence over “Read” permissions.
- ▶ But....
- ▶ If the host is in a host group that user has access denied....
- ▶ Regardless of other host group permissions the host will be **unavailable**



Zabbix organization of permissions

User groups - basics

► Problem tag filter

User groups

User group Template permissions Host permissions **Problem tag filter**

Permissions

Host groups

Add

Add Cancel

New tag filter ✕

* Host groups

Filter



Zabbix organization of permissions

User groups - basics

► Problem tag filter

User group A			User group B			Visible result for a user (member) of both groups
<i>Tag filter</i>						
<i>Host group</i>	<i>Tag name</i>	<i>Tag value</i>	<i>Host group</i>	<i>Tag name</i>	<i>Tag value</i>	
Databases	target	mysql	Databases	target	oracle	target:mysql or target:oracle problems visible
Databases	set to: <i>All tags</i>		Databases	target	oracle	All problems visible
Not configured in the Problem tag filter			Databases	target	oracle	target:oracle problems visible



Zabbix organization of permissions

User groups - nasty details part 2

- ▶ Problem tag filter
- ▶ Tag names without values can be added, but values without names cannot.
- ▶ Adding a filter results in not being able to see the problems of other host groups.

User groups

User group Template permissions Host permissions **Problem tag filter** ●

Permissions	Host groups	Tags	Actions
	all/customer	target	Edit Remove
	Add		



User groups - nasty details part 3 - other details

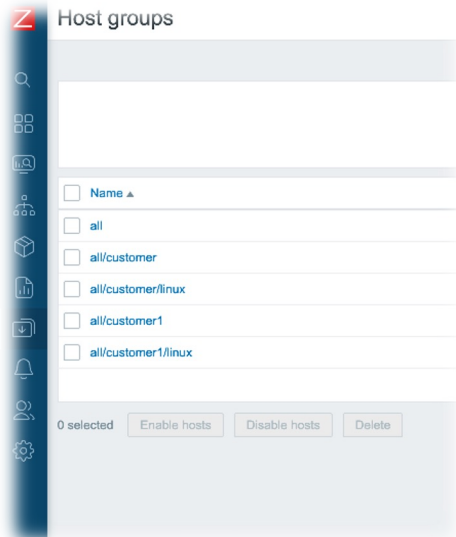
- ▶ An Admin level user with *Read-write* access to a host will not be able to link/unlink templates, if he has no access to the template group they belong to. With *Read* access to the template group he will be able to link/unlink templates to the host, however, will not see any templates in the template list and will not be able to operate with templates in other places.
- ▶ An Admin level user with *Read* access to a host will not see the host in the configuration section host list; however, the host triggers will be accessible in IT service configuration.
- ▶ Any non-Super Admin user (including 'guest') can see network maps as long as the map is empty or has only images. When hosts, host groups or triggers are added to the map, permissions are respected.
- ▶ Zabbix server will not send notifications to users defined as action operation recipients if access to the concerned host is explicitly "denied".

User groups - recommendations

- ▶ Don't go into too much detail unless you have to 😊
- ▶ Automate
- ▶ Simulate nesting in naming - relate them to host groups (easier trouble shooting)
- ▶ Read release notes
- ▶ Read documentation if unsure (previous version were simpler)

Zabbix organization of permissions

User groups - recommendations

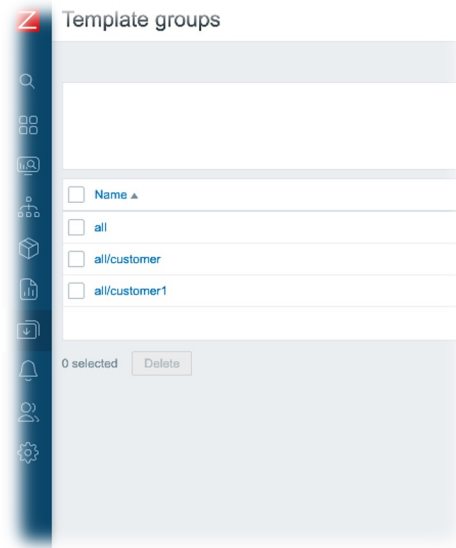


Host groups

Name ▲

- all
- all/customer
- all/customer/linux
- all/customer1
- all/customer1/linux

0 selected

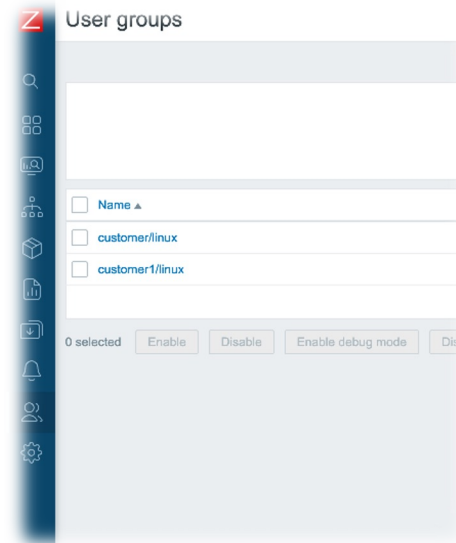


Template groups

Name ▲

- all
- all/customer
- all/customer1

0 selected



User groups

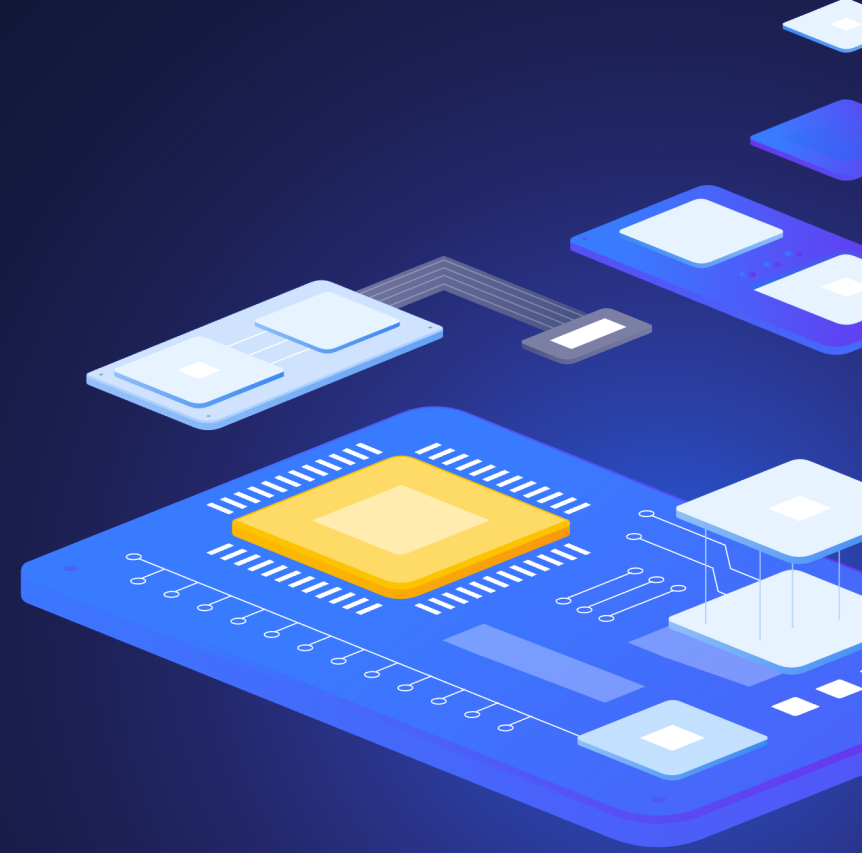
Name ▲

- customer/linux
- customer1/linux

0 selected

4

User roles



User roles - basics

- ▶ Configured by Super Admins
- ▶ Restricted access to some UI elements only prevents opening that page—it does not remove the ability to access underlying data on other parts of the interface.
- ▶ 4 types by default: Guest, User, Admin, Super Admin
- ▶ Not only menu access:
 - ▶ Services
 - ▶ Modules
 - ▶ API methods (`get.*`)
 - ▶ various actions in the frontend.



User roles - basics

- ▶ Default *Super admin role* cannot be modified or deleted, because at least one Super admin user with unlimited privileges must exist in Zabbix.
- ▶ Each user may have only one role assigned.
- ▶ If an element is restricted, users will not be able to access it even by entering a direct URL to this element into the browser.
- ▶ Users of type *User* or *Admin* cannot change their own role settings.
- ▶ Users of type *Super admin* can modify settings of their own role (not available for the default *Super admin role*), but not the user type.
- ▶ Users of all levels cannot change their own user type.

Zabbix organization of permissions

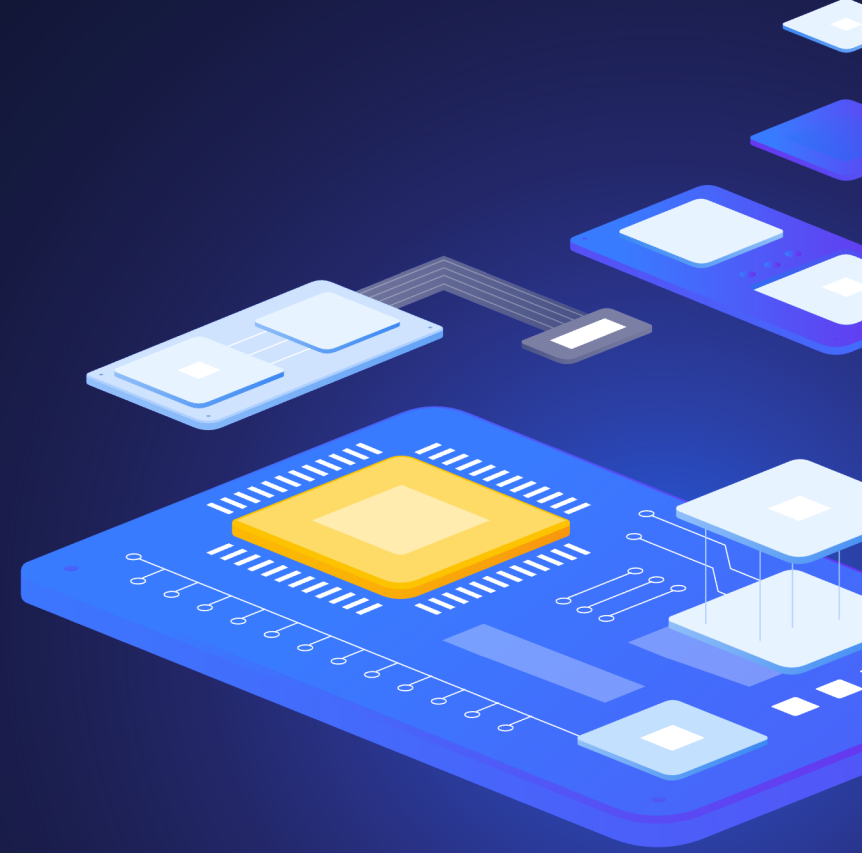
User roles - advanced

- ▶ Demo create Zabbix Super Admin with only read rights



5

Why it matters & where it breaks



Zabbix organization of permissions

User Media **Permissions**

* Role

User type

Permissions	Group	Type	Permissions
	All groups	Hosts	None
	Summit 2025 - Score	Hosts	Read-write
	Summit 2025 - Score hidden	Hosts	Read-write
	All groups	Templates	None
	Summit 2025 - Score	Templates	Read

Permissions can be assigned for user groups only.

Access to UI elements

Dashboards

Monitoring

Services

Inventory

Reports

Data collection

Alerts

Access to services

Read-write access to services

Read-only access to services

Access to modules



Zabbix organization of permissions

Access to services

Read-write access to services

Read-only access to services

Access to modules

Access to API

Enabled

Allowed methods

Access to actions



Zabbix organization of permissions

Identity provider integrations

- › Automatic provisioning of users through JIT
- › User group mapping
- › https://www.zabbix.com/documentation/current/en/manual/web_interface/frontend_sections/users/authentication
- › <https://www.initmax.com/wiki/zabbix-automation-of-user-management-jit/>



Zabbix organization of permissions

Your deed will show everywhere

- ▶ Troubleshooting
- ▶ Safety
- ▶ Customer isolation and multitenancy
- ▶ Notifications
- ▶ Dashboards
- ▶ Angry or happy users 😊 Network or NTWRK for host group name
- ▶ Further development & improvement
- ▶ Documentation and best practices
- ▶ Disabled users work remains (deprovisioned users group)



Zabbix organization of permissions

ZABBIX << < Host Group Permissions Matrix

fabian12

User groups

Host Group \ User Group	adroot users	cms2/Zabbix_Admins	cms2/Zabbix_ADO_Admins	cms2/Zabbix_ADO_Users	cms2/Zabbix_initMAX_Admins	cms2/Zabbix_initMAX_Users	Conti Admin	Disabled	Enabled debug mode	Guest
10.1.1.71: Kubernetes/Components: Kubelet	None	None	None	None	None	None	None	None	None	None
10.1.1.71: Kubernetes/Nodes/Role:	None	None	None	None	None	None	None	None	None	None
Applications	Read	None	Read	None	None	None	Read	None	None	None
Databases	Read	None	Read	None	None	None	Read	None	None	None
Discovered hosts	Read	None	Read	None	None	None	Read	None	None	None
DOMA	Read	None	None	None	None	None	Read	None	None	None
EMC Chassis	None	None	None	None	None	None	Read	None	None	None
Hypervisors	Read	None	Read-Write	None	None	None	Read	None	None	None
LAB	None	None	None	None	None	None	Read	None	None	None
LAB/AD	None	None	Read-Write	None	None	None	Read	None	None	None
LAB/Altepro	Read-Write	None	None	None	None	None	Read	None	None	None
LAB/Azure/DevTenant	None	None	Read-Write	None	None	None	Read	None	None	None
LAB/Discovery	None	None	None	None	None	None	Read	None	None	None
LAB/DNS	None	None	None	None	None	None	Read	None	None	None
LAB/IP	Read-Write	None	None	None	None	None	Read	None	None	None
LAB/Kubernetes	None	None	None	None	None	None	Read	None	None	None
LAB/NAKIT	None	None	None	None	None	None	Read	None	None	None
LAB/O2	None	None	None	None	None	None	Read	None	None	None



6

Super admin with read-only



Zabbix organization of permissions

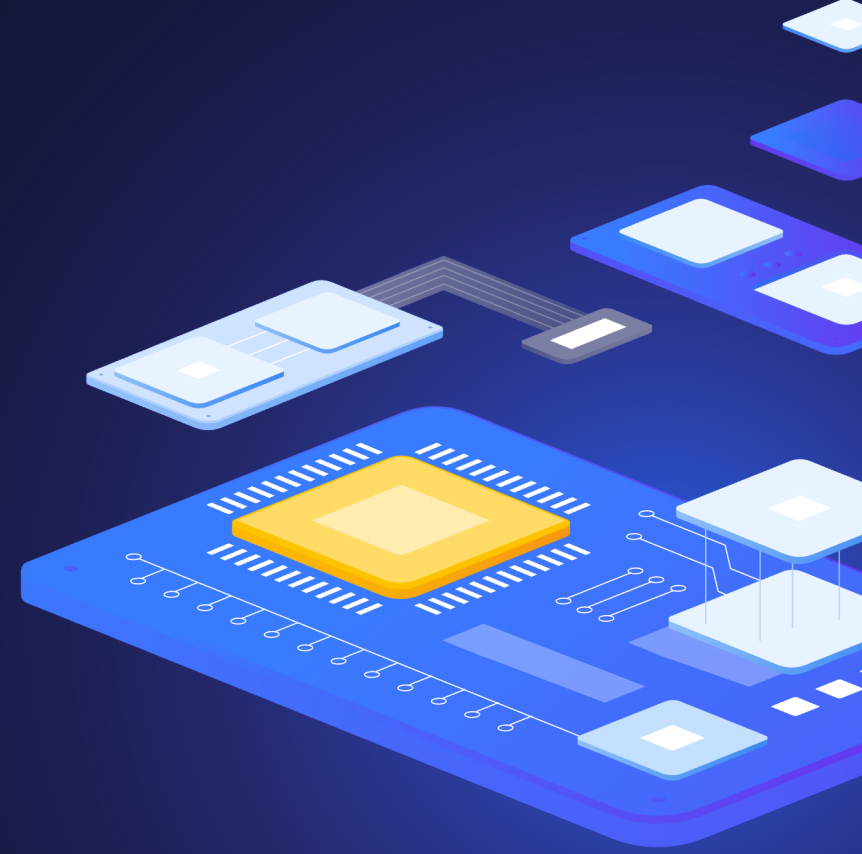
Super admin with read-only rights

▶ Demo



7

Tips for Grafana integration



Tips for Grafana integration

- ▶ Least privilege
- ▶ Good idea is to use the read-only Super admin
- ▶ Single datasource with read-write Super admin right can do a lot of harm



Tips and tricks

From time to time check our wiki, social networks or GitHub:



Wiki



LinkedIn



GitHub

Webinars

- ▶ CZ: <https://www.initmax.cz/webinare/>
- ▶ EN: <https://www.initmax.com/webinars/>

- ▶ **Advanced Windows Server Monitoring with Zabbix**
 - ▶ 2.4.2026

- ▶ **Nested LLD v praxi: praktické použití pro monitoring Proxmoxu v Zabbixu**
 - ▶ 16.4.2026

- ▶ **Korelace událostí v Zabbixu pomocí n8n: workflow a automatizace**
 - ▶ 23.4.2026



Questions?



Contact us:

Phone:



+420 800 244 442

Web:



<https://www.initmax.cz>

Email:



tomas.hermanek@initmax.cz

LinkedIn:



<https://www.linkedin.com/company/initmax>

Twitter:



<https://twitter.com/initmax>

Tomáš Heřmánek:



+420 732 447 184