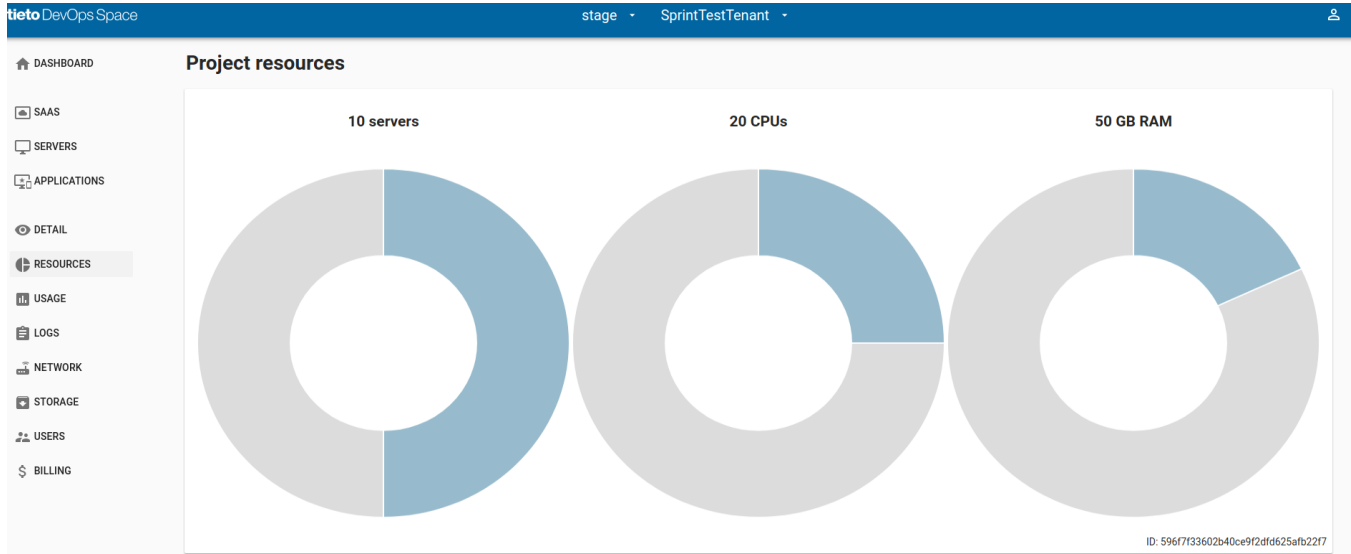


Cloud Resources

- [Resources Page](#)
- [Resource Request](#)
- [Project Resources Usage](#)
- [Project Network](#)
 - [Default Security Group](#)
 - [Server Security Group](#)
 - [Add Security Rule](#)

Resources Page

Resources page shows users how many cloud resources is allocated and currently used by Project.



The user gets information about the following cloud resources:

- Servers
 - Number of all allocated Servers to the Project
 - Number of currently used Servers
 - Number of free available Servers in Project
- CPUs
 - Number of all allocated CPU Cores to the Project
 - Number of currently used CPU Cores
 - Number of free available CPU Cores in Project
- RAM
 - Number of all allocated RAM to the Project
 - Number of currently used RAM
 - Number of free available RAM in Project

Resource Request

When Project was created without Cloud Resources, user can use  button to request adding of Cloud Resources to the project.

tieto DevOps Space golddluktest123 LukTest002

Project resources

No virtual resources are available. If you want to use virtual resources to deploy your own virtual servers and application use please contact [support](#).

Create resources

Request for virtual resources does not imply any costs, resources are only charged when any applications and servers are deployed. Below pricing is valid for such deployments and resulting monthly costs will be shown in application order dialogue.

Pricing (€ per hour)

Servers (pcs)	CPU (pcs)	RAM (GB)	HDD (GB)	SSD (GB)	Network (GB)
0.001	0.001	0.001	0.001	0.001	0.001

By clicking on the create button you **confirm validity** of entered cost center or project number. If entered value is not valid then the cost center linked to your account will be billed.

CANCEL CREATE

Project Resources Usage

Usage page shows cloud resources usage in the current project during the current month.

The page is visible only for a project with cloud resources added to the project.

tieto DevOps Space tdsoper

Project resources usage

Usage Volumes

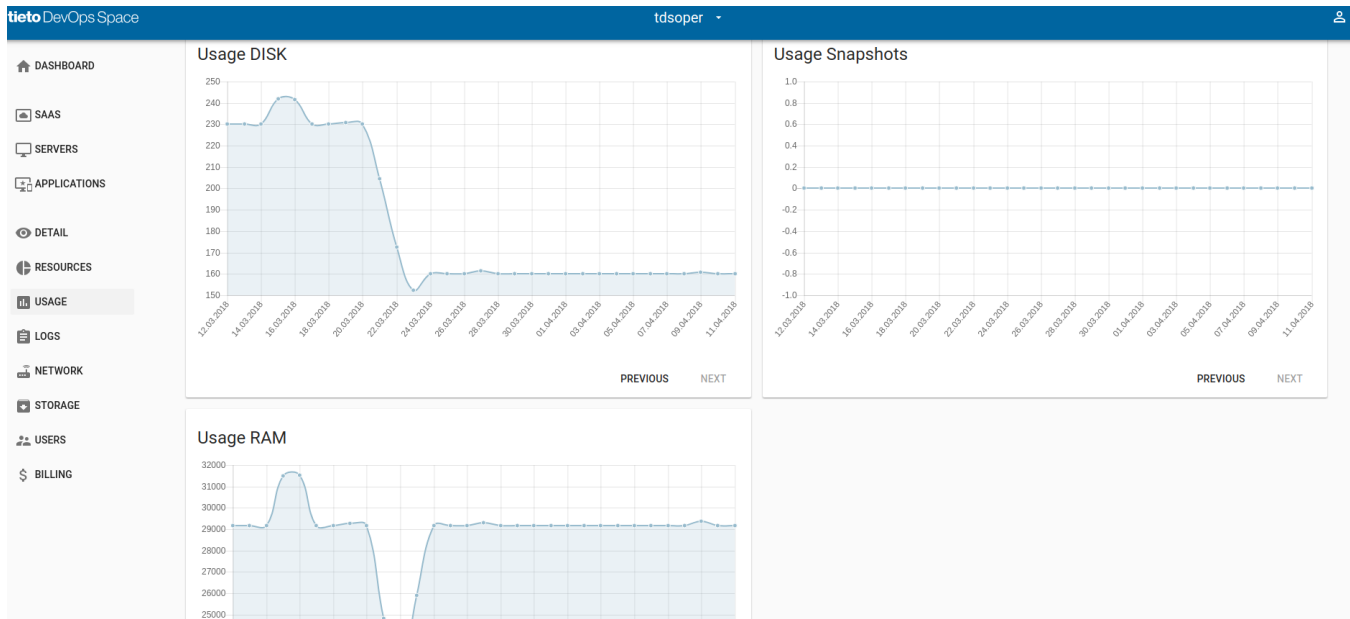
PREVIOUS NEXT

Usage Images

PREVIOUS NEXT

Usage CPU

Usage INSTANCES



It's possible to move to the previous or next month using the PREVIOUS or NEXT button.

The following cloud resources are visible in the usage page:

- Volumes (GB)
 - the second disk volume used in server attached to server or unattached
 - It's not possible currently to add volume to the server in TDS. Volumes can be requested using tickets only
- Images (GB)
 - Private user images
 - Backups of servers
- CPU (core numbers)
 - number of used CPU cores
- Instances (server number)
 - number of created servers
- Disk (GB)
 - root disks used in servers
- Snapshots (GB)
 - server snapshots stored and kept in the project
- RAM (MB)
 - RAM memory used by servers in the project

Project Network

TDS Project Networks includes TDS Security Groups where user can create/delete/modify Security Rules related to TDS Servers access.

There is one Security Group named "default" which includes a few default security rules.


For every TDS Server, there is created a separate Security Group called "<server hostname>_default".

User can maintain the server's access using that sever Server Security Group.


tiesto DevOps Space stage SprintTestTenant

Project Networks

- c7ldap_default**
Default security group for c7ldap
c7ldap.sprinttesttenant.stage.tdsdev.tieto.com
- ub16ldaptest_default**
Default security group for ub16ldaptest
ub16ldaptest.sprinttesttenant.stage.tdsdev.tieto.com
- default**
Default security group
c7sshnew.sprinttesttenant.stage.tdsdev.tieto.com,ub16ldaptest.sprinttesttenant.stage.tdsdev.tieto.com,costestssh.sprinttesttenant.stage.tdsdev.tieto.com,c7ldap.sprinttesttenant.stage.tdsdev.tieto.com
- costestldap1_default**
Default instance's security group
costestldap1.sprinttesttenant.stage.tdsdev.tieto.com,costestssh.sprinttesttenant.stage.tdsdev.tieto.com
- costestssh_default**
Default instance's security group
costestssh.sprinttesttenant.stage.tdsdev.tieto.com,costestldap1.sprinttesttenant.stage.tdsdev.tieto.com
- jenkinsmaster8_default**
Default security group for jenkinsmaster8
jenkinsmaster8.sprinttesttenant.stage.tdsdev.tieto.com
- c7sshnew_default**
Default security group for c7sshnew
c7sshnew.sprinttesttenant.stage.tdsdev.tieto.com



Security Group List view includes all Server Security Groups and Project Default Security Group.

Project Admin can add another Security Group using  button.

Default Security Group

Network ✕

Security Group name *
default

Security Group description
Default security group

Select related servers

- costestssh.sprinttesttenant.stage.tdsdev.tieto.com
- costestldap1.sprinttesttenant.stage.tdsdev.tieto.com
- c7sshnew.sprinttesttenant.stage.tdsdev.tieto.com
- c7ldap.sprinttesttenant.stage.tdsdev.tieto.com
- ub16ldaptest.sprinttesttenant.stage.tdsdev.tieto.com
- jenkinsmaster8.sprinttesttenant.stage.tdsdev.tieto.com

Direction	Protocol	Remote IP	Port from	Port to	Action
Ingress	TCP	0.0.0.0/0	22	22	REMOVE
Ingress	TCP	89.46.83.22/24	61614	61614	REMOVE
Egress	Any	0.0.0.0/0	0	0	REMOVE

ADD RULE

DELETE SAVE

Default Security Group is enabled by default to all project servers and includes a few Security Rules which enables access from Servers to external networks and opens ssh connection to Servers.

User can disable Default Security Group to any project server changing Server switch button to the off state.

User can't create any new Security Rule in Default Security Group.

Server Security Group

Security Group name *
jenkinsmaster8_default

Security Group description
Default security group for jenkinsmaster8

Select related servers

- costestssh.sprinttesttenant.stage.tdsdev.tieto.com
- costestldap1.sprinttesttenant.stage.tdsdev.tieto.com
- c7sshnew.sprinttesttenant.stage.tdsdev.tieto.com
- c7ldap.sprinttesttenant.stage.tdsdev.tieto.com
- ub16ldaptest.sprinttesttenant.stage.tdsdev.tieto.com
- jenkinsmaster8.sprinttesttenant.stage.tdsdev.tieto.com

Direction	Protocol	Remote IP	Port from	Port to	Action
Ingress	TCP	0.0.0.0/0	80	80	REMOVE
Ingress	TCP	0.0.0.0/0	59288	59288	REMOVE
Egress	Any	0.0.0.0/0	0	0	REMOVE
Ingress	TCP	0.0.0.0/0	443	443	REMOVE

ADD RULE

DELETE SAVE

Server Security Group includes Security Rules for a selected server.

The server name is included in Security Group called "<server hostname>_default".

When Server with optional Application is created, TDS Server Security Group is created including all necessary Security Rules for installed Application.

User can enable Server Security Group for another Server - not recommended.

There is a Project quota limit for Security Rules in public TDS - a maximum number of Project Security Rules is the same as the maximum number of Servers allowed in the Project.

User can save changes or delete Server Security Group using button **SAVE** respective **DELETE**.

User can cancel his actions in Security Server Group view pressing button Escape.

User can add a new Security Rule into Server Security Group using button **ADD**.

Add Security Rule

Network

Security Group name *

Security Group description

Select related servers



Direction	Protocol	Remote IP	Port from	Port to	Action
Ingress	▼ TCP	▼ 0.0.0.0/0	443	443	REMOVE
Egress	▼ Any	▼ 0.0.0.0/0	0	0	REMOVE
Select direction *	▼ Any	▼ xxx.xxx.xxx.xxx *			REMOVE

ADD RULE

DELETE

SAVE

User can add a new Security Rule in that view or modify existing Security Rules.

Security Rule includes the following fields:

- Direction
 - Egress direction means a direction from TDS Server to other hosts or networks. By default, egress is allowed to all networks and for all protocols and ports.
 - Ingress direction means a direction from external hosts or servers to TDS Server. By default, ingress is not allowed except to Application protocols and ports installed by TDS.
- Protocol
 - Possible values:
 - Any
 - TCP
 - UDP
 - ICMP
- Remote IP
 - Source of the traffic to be allowed via this rule. Expected values should be entered in the form of an IP address block. For all IPs 0.0.0.0 /0 can be used.
- Port from
 - The field means a single port or beginning of the range of ports which will be used for the rule
 - Valid only for TCP and UDP protocols
 - Integer value between 1 and 65535 can be used only
- Port to
 - The field means a single port or end of the range of ports which will be used for the rule
 - Valid only for TCP and UDP protocols
 - Integer value between 1 and 65535 can be used only
- Action
 - Action which will be performed for the rule
 - The only action which can be used for the rule is to REMOVE
 - After removing the rule from the view, it's necessary to press SAVE to write REMOVE action to Server Security Group.

User can modify existing Security Rules and save all changes pressing SAVE to write REMOVE action to Server Security Group.