DIATEAM
31 rue Yves Collet
29200 BREST CEDEX2
Tél: +33 (0) 298 050 050
contact@diateam.net - http://www.diateam.net

diateam®
military & civil cybersecurity solutions

HNS PRO HARDWARE & SOFTWARE PLATFORMS

ADMINISTRATION AND MAINTENANCE GUIDE

Ref: HNS-HYNESIM-PRO-3.0-AdministrationGuide-2.0-EN
Version: 2.0

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

1. Starting & shutting down the platform

If the platform includes a UPS, it is to start first.

1.1 Starting the platform

1.1.1 NAS (optionnal)

If your platform has a NAS, start it so that NFS exports are available for the other servers.

1.1.2 Master

Start the master. The rest of the startup procedure is automatic and starts the different services as well as the nodes.

1.2 Shutting down down the platform

To shut down the platform, connect to the master and run the **cleanHalt** command as root user;

```
cleanHalt
```

To have the procedure description for your platform, see Annex B.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

2. Administrating the platform

2.1 Connecting to the master operating system

2.1.1 Local access

The administrator can connect to the Master server by logging into the desktop environment specified in the technical description of the platform using the **hns** user.

2.1.2 Remote access

The administrator can use SSH to connect to the Master server. Username is **hns** or **root** and IP is stated in the implementation plan.

2.2 User management in hynesim

Hynesim has the ability to have multiple users at the same time. Users usually have a default group, but they may belong to several additional groups. Only **admin** user is able to manage users and groups. However, any user can modify its default group. An user can be created, cloned, edited or deleted. All management takes place in the hyneview user manager part.

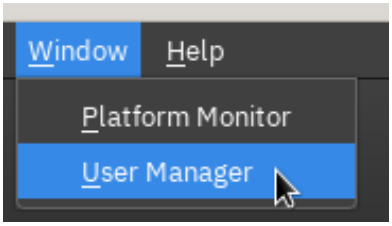

Figure 2.1: Access to user manager

2.2.1 Creating an user

In the user section, click the **Add** user button.

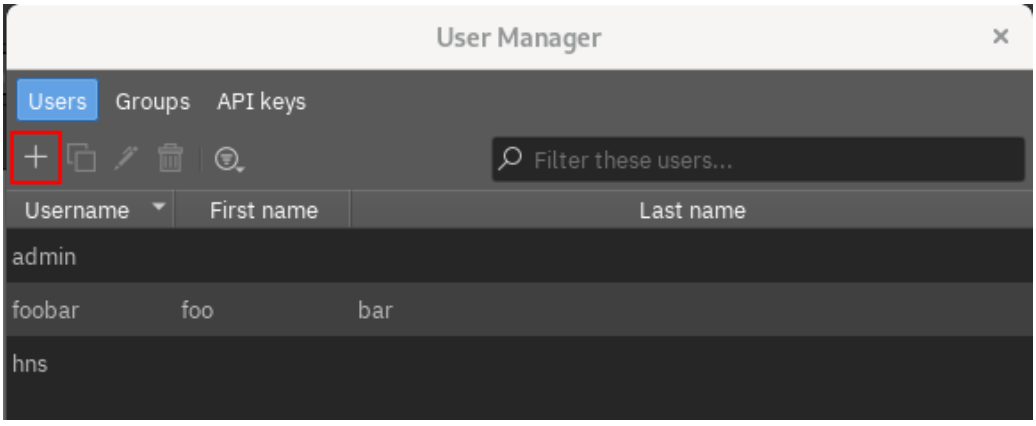

Figure 2.2: Creating an user

A new popup appears. You have to fill in the information and click the **OK** button.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

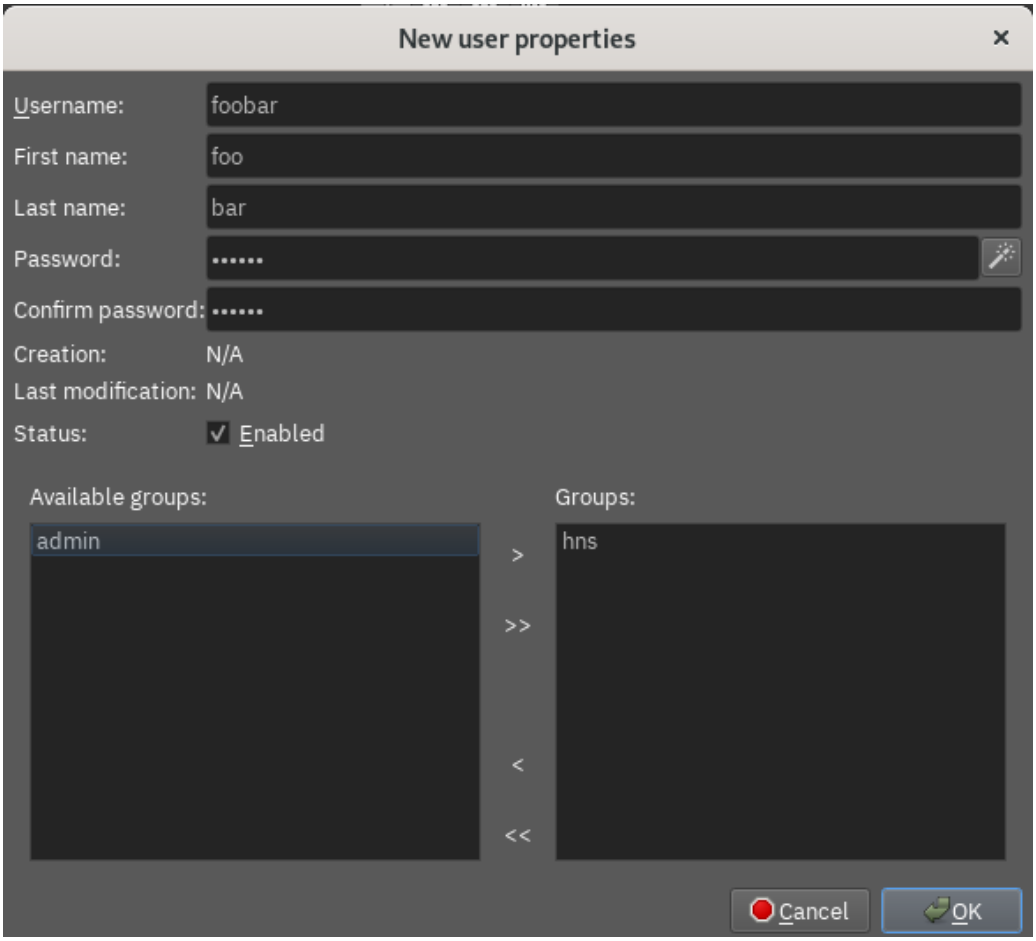

Figure 2.3: New user properties

When the user is created, a new group with the user name is also created. The created user belongs to this group. An user account can be enabled by checking the Enabled checkbox and disabled by unchecking it. The advanced checkbox only enables an advanced version of the user properties dialog; this may change in the future.

2.2.2 Cloning an user

In the user section, select an user. There are 2 different ways to clone an user:

- Right click and select **Clone user**;
- Click the **Edit user** button.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

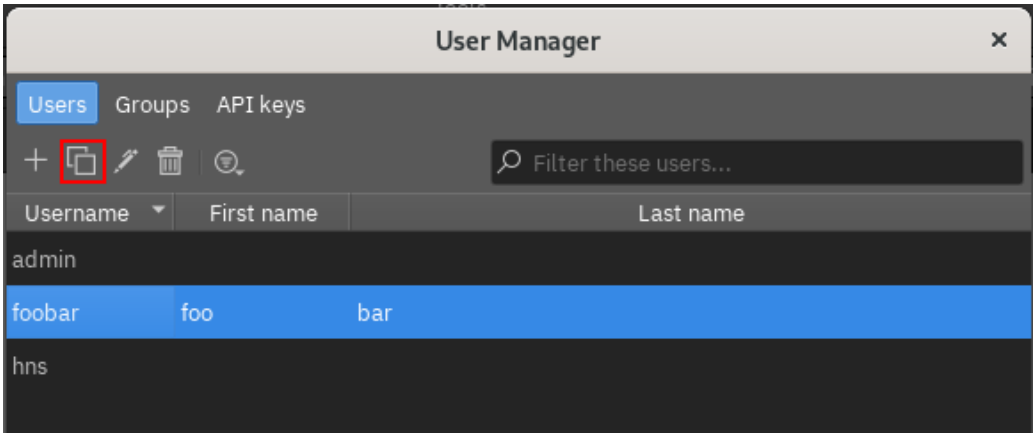

Figure 2.4: Cloning an user

A new popup appears. There you can define the desired number of clones. You also have to enter a new password. Validate by clicking the **OK** button.

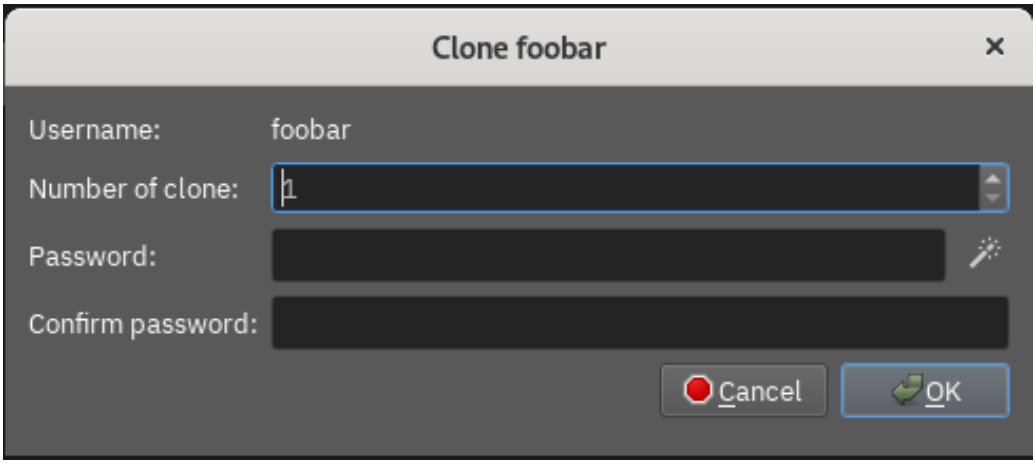

Figure 2.5: Cloning an user dialog

2.2.3 Editing an user

In the user section, select an user. There are 3 different ways to edit an user:

- Double click the user;
- Right click and select **Edit user**;
- Click the **Edit user** button.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

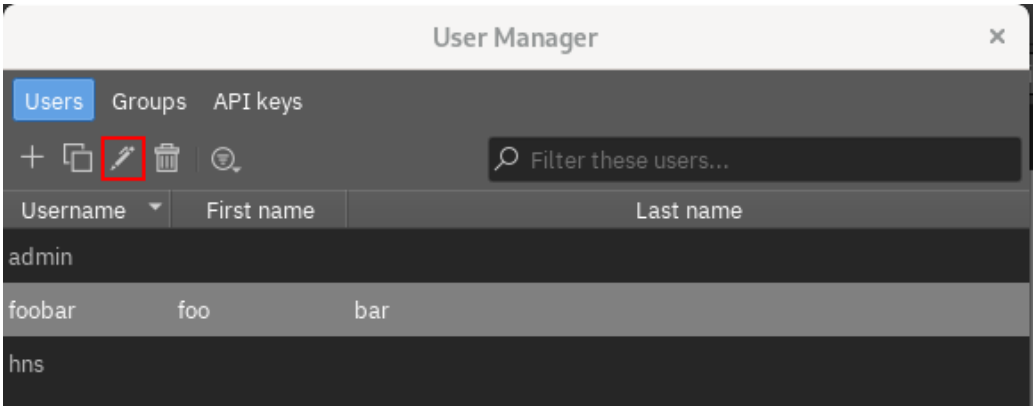

Figure 2.6: Editing an user

You access a popup where you can edit user properties, and confirm by clicking the **OK** button.

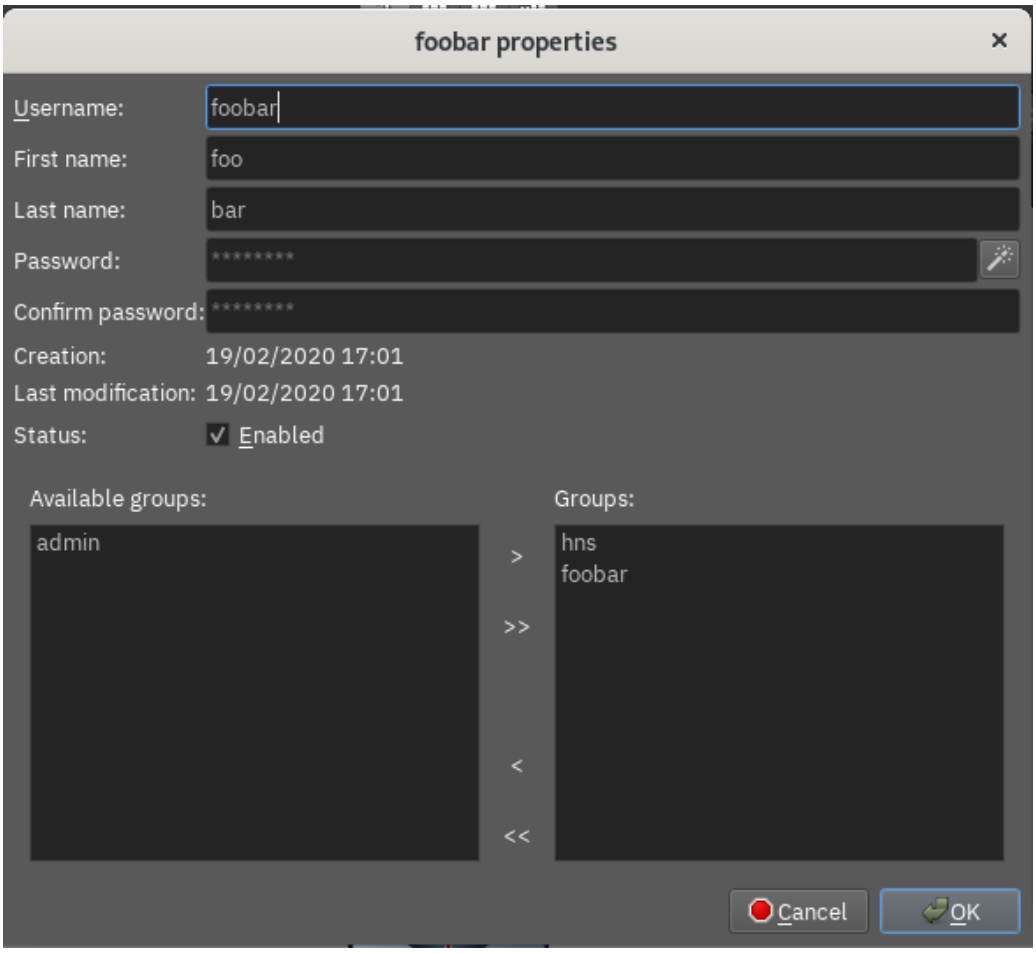

Figure 2.7: User properties dialog

2.2.4 Deleting an user

In the user section, select an user. There are 3 different ways to delete an user:

- Press **Del** key;

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

- Right click and select **Delete user**;
- Click the **Delete user** button.

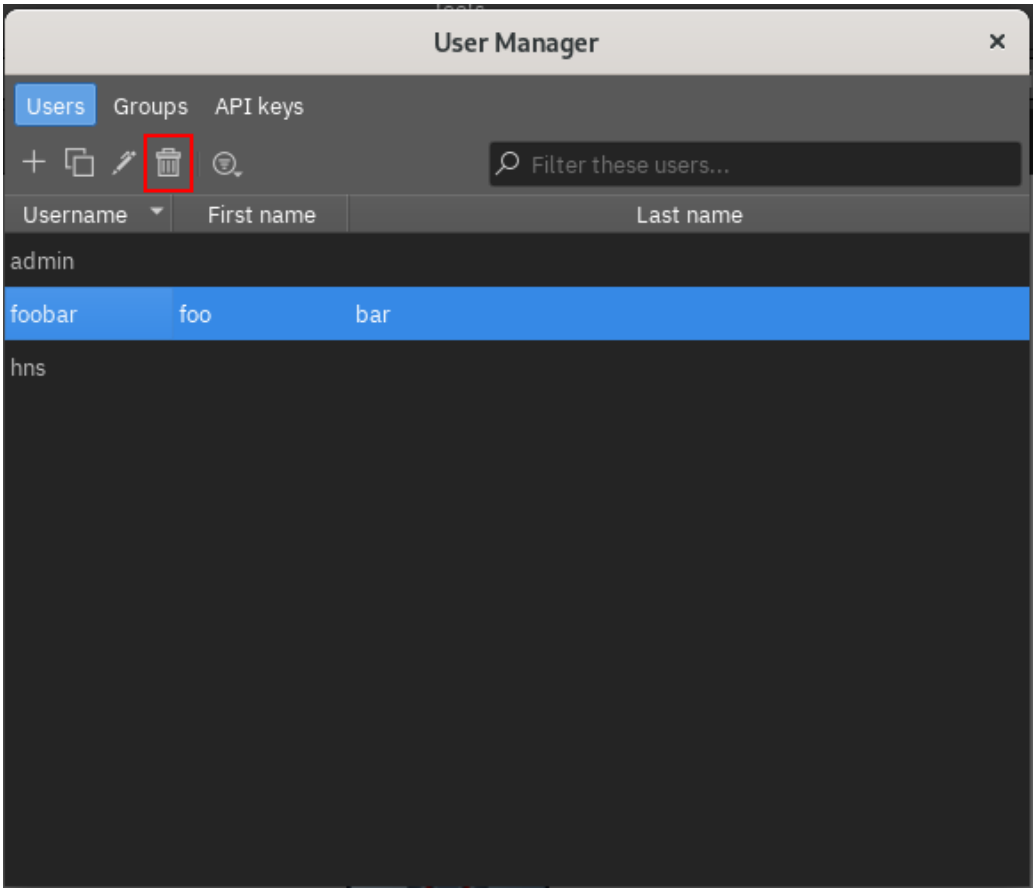

Figure 2.8: Deleting an user

2.2.5 Creating a group

In the group section, click the **New group** button

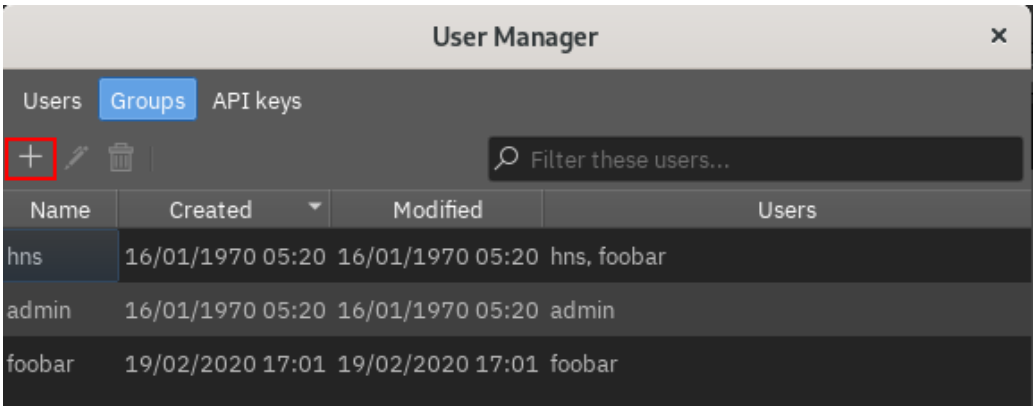

Figure 2.9: Creating a group

A new group popup appears. You have to fill in the information and click the **OK** button.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

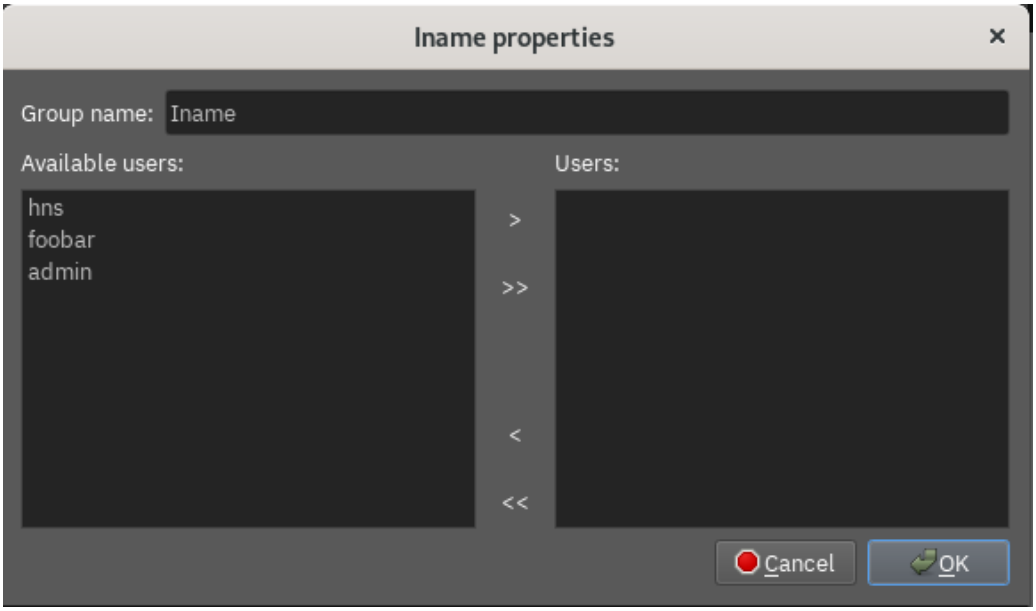

Figure 2.10: New group properties

To add users to and remove users from the group, select a user and use the arrows in the center of the popup. Confirm by clicking the **OK** button.

2.2.6 Editing a group

In the group section, select a group. There are 3 different ways to edit a group:

- Double click the group;
- Right click and select **Edit group**;
- Click the **Edit group button**.

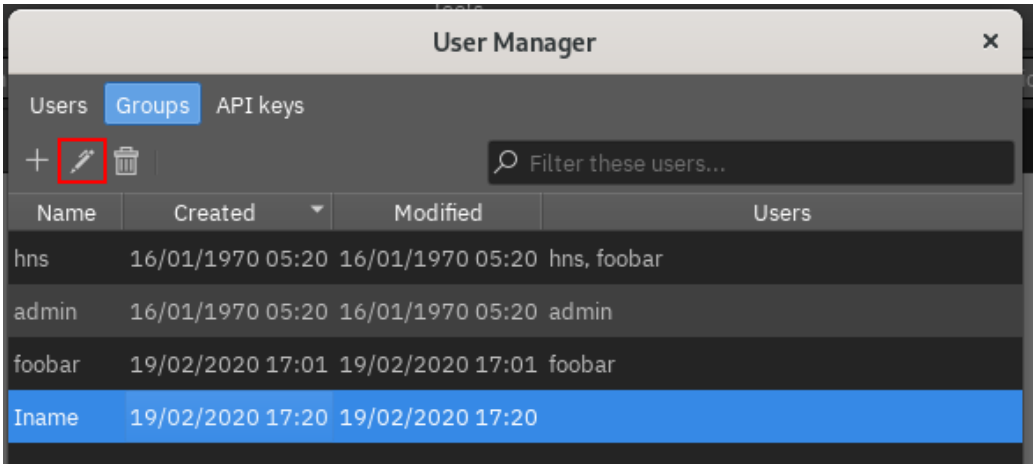

Figure 2.11: Editing a group

The same popup used to create a group appears. Confirm by clicking the **OK** button.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

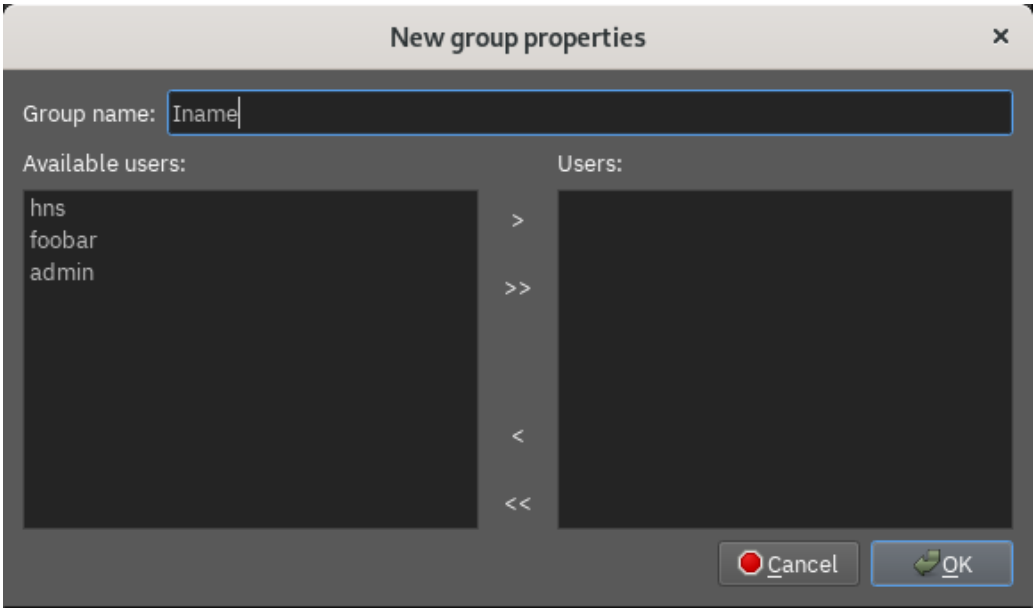

Figure 2.12: Group properties dialog

2.2.7 Deleting a group

In the group section, select a group. There 3 different ways to delete a group:

- Press **Del** key;
- Right click and select **Delete group**;
- Click the Delete group button.

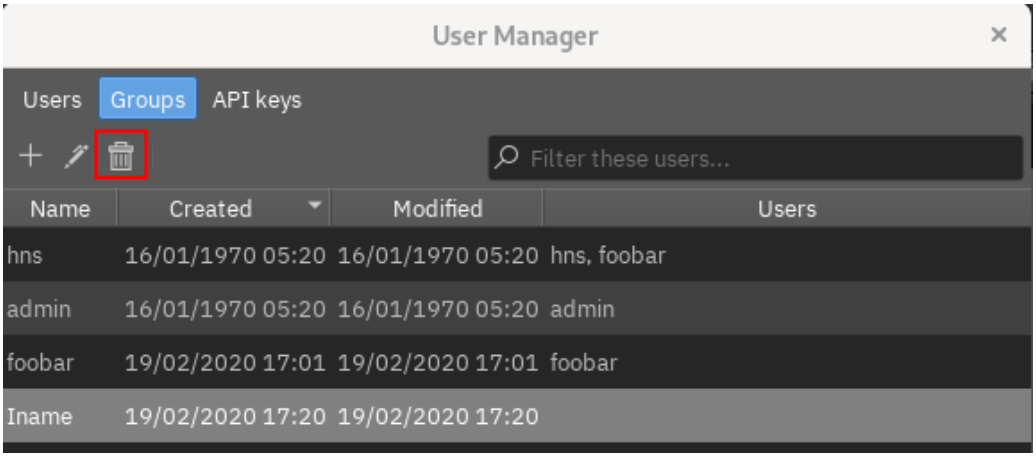

Figure 2.13: Deleting a group

Note that the group must be empty to be deleted.

2.3 Rights management in hynesim

Hynesim makes it possible to share entities and topologies with other users or groups. By default, only the **admin** user and the owner of the topology or entity can view, use and modify the item. To share an item, right click the entry in the catalog and select **Rights**.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

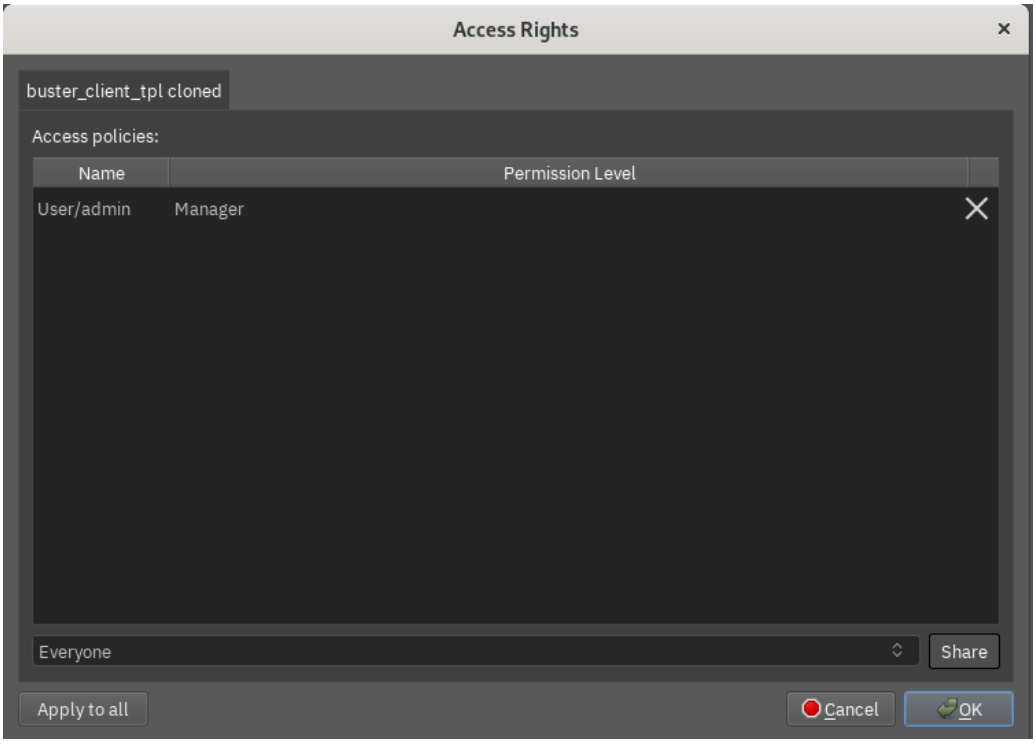

Figure 2.14: Rights properties

Use the combo box to select the group/user you want to share the item with and click the **Share** button. To share the item with everyone, select **Everyone**. Click the **OK** button to confirm.

2.4 API keys

2.4.1 Add an API key

In the API key section, click on **Add**

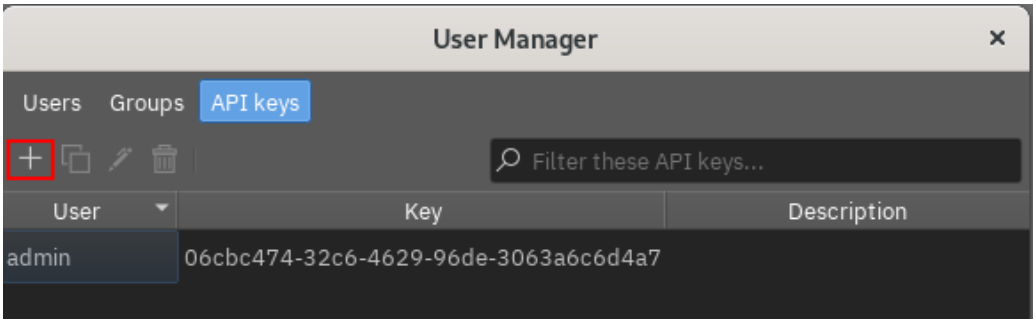

Figure 2.15: Adding an API key

A new window opens in which you can choose the user for whom to generate a key as well as entering a description. Once the information is entered, click OK which will generate a new API key.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

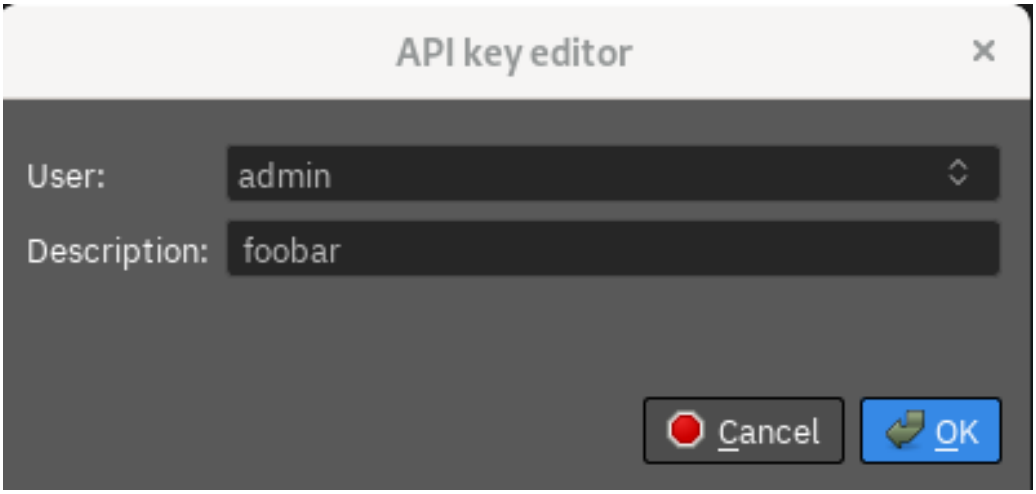

Figure 2.16: new API key window

2.4.2 Delete an API key

In the API key section, select a key to delete. There are two ways to proceed:

- Press the **DEL** key;
- Click on the **Delete** button.

In both cases, the action must be confirmed

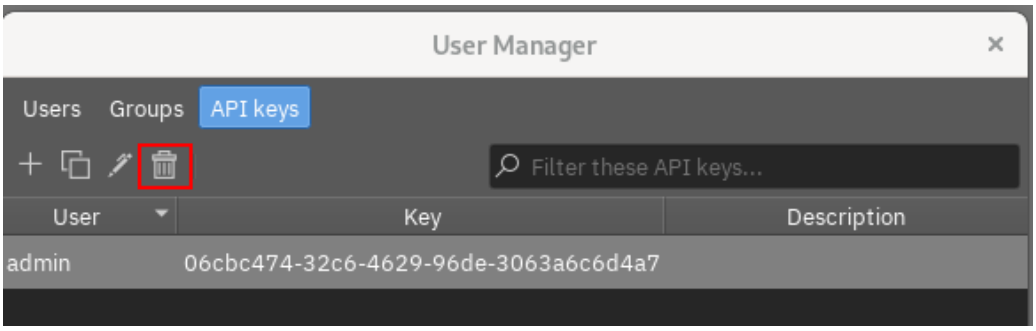

Figure 2.17: Delete an API key

2.4.3 Modify an API key

In the API key section, select a key to modify. There are two ways to proceed:

- Double click on the key;
- Click the **Modify** button.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

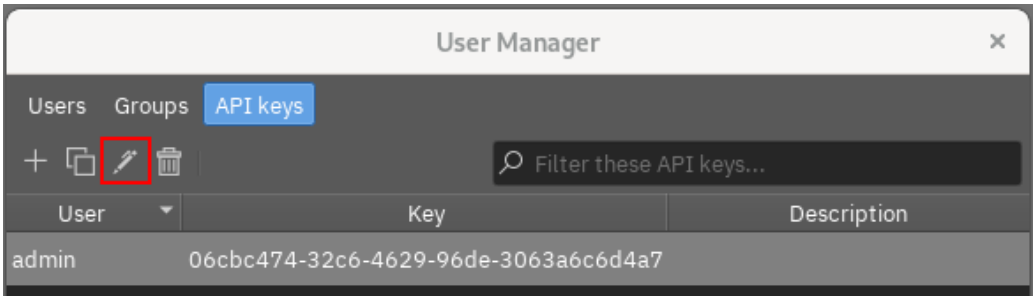

Figure 2.18: Editing an API key window

In both cases, the next window in which you can edit the description of the key and copy its value opens.

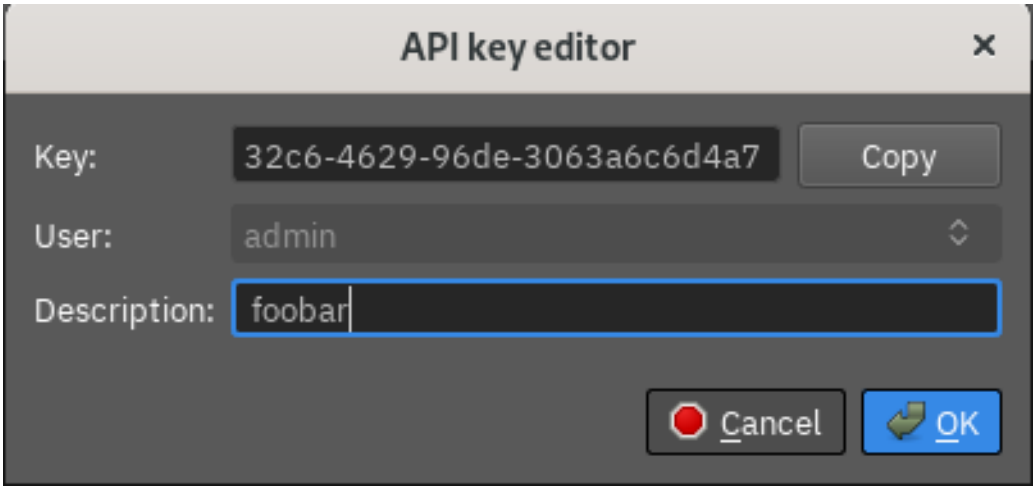

Figure 2.19: Edit API key window

2.5 Hynesim configuration

2.5.1 hynesim-glacier

hynesim-glacier is used to relay connections between hyneview and hynesim-master. The configuration file is located in **/etc/hynesim/hynesim-glacier.conf**.

```
Glacier2.Client.Endpoints=tcp -p 4063
Glacier2.Server.Endpoints=tcp
Glacier2.PermissionsVerifier=PermissionsVerifier:tcp -p 5656
Glacier2.SessionManager=SessionManager:tcp -p 5656
Glacier2.Client.ForwardContext=1
Glacier2.Server.ForwardContext=1
Glacier2.AddConnectionContext=1
Ice.Default.Host = 127.0.0.1
Ice.UseSyslog=1
Ice.ThreadPool.Server.Size = 1
Ice.ThreadPool.Server.SizeMax = 32
Ice.ThreadPool.Server.SizeWarn = 0
Ice.ProgramName=hynesim-glacier
```

The **Ice.Default.Host** entry is the IP address used to allow connection of clients. It can be changed to another IP. The **Ice.ThreadPool.Server.SizeMax** entry is used to define the number of incoming requests to dispatch to hynesim-master.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

We recommend you to set this value to the server CPU thread count. The log file is available at **/var/log/hynesim-glacier.log**.

2.5.2 Hynesim-master

The hynesim-master configuration file is located in **/etc/hynesim/hynesim-master.ini**.

Diamesh section

```
[Diamesh]
masterName = "My Master"
shortName = "Master"
description = "This is the master"

LogFilter = "*=true"
; Log method
; System  : Syslog
; File    : File specified with LogFile=
; Default : Standard output
LogMethod = System
LogFile = /var/log/hynesim-master.log

defaultDb = /etc/hynesim/diamesh.db

authorizedNodes/1/key = node-0
authorizedNodes/2/key = node-1
authorizedNodes/3/key = node-2
authorizedNodes/4/key = node-3
authorizedNodes/5/key = node-4
authorizedNodes/size = 5
```

The **masterName**, **shortName** and **description** entries are used to describe and identify hynesim-master. Several log levels are available, spanning from debug to fatal. The smaller the log level, the more verbose it is. To modify the log level, update the **LogLevel** entry. There are several log methods:

- log to syslog;
- log to a specified file;
- log to the standard output.

The System log method is strongly recommended. By default, the log file is available at **/var/log/hynesim-master.log**. hynesim-master manages user and authentication data in database files. These database files are configured by the **authDBName** and **defaultDb** entries. For the nodes to be able to connect to the master, the **authorizedNodes** array entry is used. For this you have to specify the node key described below. Each key must be unique for each node.

ICE section

```
[Ice]
Ice.Default.Host=127.0.0.1
Master.Endpoints=tcp -p 5656

Ice.ThreadPool.Server.Size=1
Ice.ThreadPool.Server.SizeMax=3
Ice.ThreadPool.Server.SizeWarn=0
Ice.Warn.Connections=1
```

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

You can update the **Ice.Default.Host** entry to match the desired listening master IP address. The **Ice.ThreadPool.Server.SizeMax** entry is used by the hynesim-master to manage parallel incoming requests. We recommend you to set this value to the server CPU thread count. Other entries must not be modified.

hynesim section

```
[Hynesim]
catalog/dbName=/etc/hynesim/catalog.db
;catalog/maxCloneJobs = 1

FileStorages/1/path = /data/hynesim/catalog/entities
FileStorages/1/name = "Entities Catalog"
FileStorages/1/type = entity

FileStorages/2/path = /data/hynesim/catalog/topologies
FileStorages/2/name = "Topologies Catalog"
FileStorages/2/type = topology

FileStorages/3/path = /data/hynesim/catalog/isos
FileStorages/3/name = "Isos Catalog"
FileStorages/3/type = ISO

FileStorages/size = 3

dataDirectory = /usr/share/hynesim
scriptsDirectory = /usr/share/hynesim/scripts
entityCatalogImport/path = /data/hynesim/import
exportCatalog/path = /data/hynesim/export
CustomResourcePath = /data/hynesim/resources

;VMWare/dummy = 1
;VMware/hostname = "10.0.0.2"
;VMware/username = "root"
;VMware/password = "toor"
;VMware/datastore = "nfs"

;monitoringEnabled = false
;diskCapacityParsingEnabled = true
;SpicePortPoolLow = 6901
;SpicePortPoolHigh = 9999
```

hynesim-master maintains a database to manage its catalog. This database is stored in a file described by the **catalog/dbName** entry. By default, hynesim-master can only clone one entity at a time. If you wish to increase the number of parallel clones, you can modify the **catalog/maxCloneJobs** entry. However, note that a virtual machine clone uses a lot of I/O, so we recommend you to avoid having too many clones at the same time. hynesim-master has two file storages: one for entities and another one for topologies. Those folders can be configured by the **FileStorages** array entry :

- The **dataDirectory** entry configures the folder where hynesim resources are.
- The **scriptDirectory** entry configures the folder where hynesim scripts are.
- The **entityCatalogImport/path** entry configures the import folder.
- The **exportCatalog/path** entry configures the export folder.
- The **CustomResourcePath** entry configures the folder where entity customized icons are.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

- The **VMware** entries allow VMware entities import via hyneview.
- The **VMware/dummy** entry allows the feature.
- The **VMware/hostname** entry configures the ESXi IP address.
- The **VMware/username** entry configures the username to connect.
- The **VMware/password** entry configures the password to connect.
- The **VMware/datastore** entry configures the datastore in which to store the VMs to import. It is important to note that this one must point to the root of a hynesim catalog.

2.5.3 hynesim-node

hynesim-node configuration file is located in **/etc/hynesim/hynesim-node.ini**.

diamesh section

```
[Diamesh]
Key = node-0
ShortName = "Node 0"
Description = "This is Node 0"

LogFilter = "*=true"

; Log method
; System  : Syslog
; File    : File specified with LogFile=
; Default : Standard output
LogMethod = System
LogFile = /var/log/hynesim-node.log
```

The **key** entry is used to connect to hynesim-master. The **shortName** and **description** entries are used to describe the node. Several log levels are available, spanning from debug to fatal. The smaller the log level, the more verbose it is. To modify the log level, update the **LogLevel** entry. There are several log methods:

- log to syslog;
- log to a specified file;
- log to the standard output.

The System log method is strongly recommended. To modify the log method, update the LogMethod entry. If you choose to have a file log method, the LogFile entry can be updated as well.

ICE section

```
[Ice]
Ice.Default.Host=127.0.0.1
MasterProxy = master:tcp -p 5656
Node.Endpoints = tcp
Ice.Warn.Connections=1
Ice.RetryIntervals=-1
Ice.ThreadPool.Server.Size = 1
Ice.ThreadPool.Server.SizeMax = 32
Ice.ThreadPool.Server.SizeWarn = 0
```

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

The **Ice.Default.Host** entry configures the hynesim-node listening IP address. This IP is also used to access remote displays. The **MasterProxy** entry configures hynesim-master connection information. The **Ice.ThreadPool.Server.SizeMax** entry configures parallel incoming requests. We recommended you to set this value to the server CPU thread count. Other entries found here are used and should not be modified.

Platforms section

```
[Platforms]
HybridNetcard/cards/1/device = hybrid0
HybridNetcard/cards/1/plug = "Plug 1"
;HybridNetcard/cards/2/device = eth2
;HybridNetcard/cards/2/plug = "Plug 2"
HybridNetcard/cards/size = 1

;WifiAP/wifiDevice/1/device = wlan0
;WifiAP/wifiDevice/1/maxSsid = 4
;WifiAP/wifiDevice/size = 1

TopologyGate/gates/1/name = topogate1
TopologyGate/gates/1/isHub = 0
TopologyGate/gates/2/name = topogate2
TopologyGate/gates/2/isHub = 0
TopologyGate/gates/size = 2

LXC/dummy = 1
KvmQemu/dummy = 1
KvmQemu/tmpDir = /data/hynesim/tmpDir
;UEFIFirmwarePath = /usr/share/OVMF/OVMF_CODE.fd
;HandleStateLink = false

;VMware/dummy = 1
;VMware/hostname = 10.100.1.20
;VMware/username = root
;VMware/password = toor
;VMware/trunkInterface = eth2
```

The **Platforms** section makes it possible to support different domain types in the node. If you do not want to use a domain type, disable the entry by prefixing the row(s) with the character ";".

- The **LXC/dummy** entry enables LXC support.
- The **KVMQemu/dummy** entry enables KVM/Qemu support.
- When an immutable KVM/Qemu domain is defined, a temporary directory is used. By default, this directory is **/var/tmp** but it can be modified by updating the **KvmQemu/tmpDir** entry.
- The **HandleStateLink** entry allows to notify KVM/Qemu domains when a cable is plugged or unplugged.
- The **VMware/dummy** entry allows the feature.
- The **VMware/hostname** entry configures the ESXi IP address.
- The **VMware/username** entry configures the username to connect.
- The **VMware/password** entry configures the password to connect.
- The **VMware/trunkInterface** entry configures the network interface plugged between the node and the ESXi server.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

- The **HybridNetcard** array entry configures hybrid net cards. The **device** entry has to be associated with the desired interface, and a name must be given in the **plug** entry. NB: network interfaces used as hybrid net cards must be configured as manual interfaces in the **/etc/network/interfaces** file.
- The **WifiAP** array entry configures Wi-Fi access points. A Wi-Fi device is associated with the **device** entry. In some cases, hardware Wi-Fi AP support multiple access points. To take advantage of this feature, you can modify the **maxSsid** entry.
- The **TopologyGate** array entry configures topology gates. They are described by a name in the **name** entry. A topology gate may be used as a HUB by changing the **isHub** entry to 1.

hynesim section

```
[Hynesim]
FileStorages/1/path = /data/hynesim/catalog/entities
FileStorages/1/name = "Entities Catalog"
FileStorages/1/type = entity

FileStorages/2/path = /data/hynesim/catalog/topologies
FileStorages/2/name = "Topologies Catalog"
FileStorages/2/type = topology

FileStorages/3/path = /data/hynesim/catalog/isos
FileStorages/3/name = "Isos Catalog"
FileStorages/3/type = ISO

FileStorages/size = 3
```

Hynesim section configures topology and entity catalogs, as referred in **Section 2.4.2.3**.

Node section

```
[Node]
scriptsDirectory = /usr/share/hynesim/scripts
sharedFolder = /data/hynesim/shared

ActionManagerBridgeName = br0

resources/maxCpu = 32
resources/maxMemory = 28672

VxlanInterface = eth0
VxlanHost = 127.0.0.1

enableSpiceCompression = true

enableSpiceTLS = false
;spiceTLSCaCertPath = /etc/pki/libvirt-spice/ca-cert.pem
;spiceTLSServerCertPath = /etc/pki/libvirt-spice/server-cert.pem

ActionManagerSerialProxyHost = 127.0.0.1
ActionManagerSerialProxyPort = 4555

ActionManagerLXCConsoleNumber = 2
```

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

The **scriptsDirectory** entry configures the directory where the hynesim scripts used by hynesim-node are. The **sharedFolder** entry configures the path of the shared folder for virtual machines. The **resources/MaxCPU** and **resources/maxMemory** entries are used by the load balancer to perform the best load balancing when defining entities. Network communication between 2 domains defined on different node is done with the VXLAN (Virtual Extensible LAN). The **VxlanInterface** entry configures the VXLAN interface used by hynesim-node. NB: the network interface must support JumboFrame technology and must be configured by a MTU (Maximum Transmission Unit) of 1600. Virtual machines remote displays are made using the SPICE communication protocol (http://www.spice-space.org). SPICE connections are compressed to support multiple remote displays at the same time. Update the entry **enableSpiceCompression** to false if you wish to disable this feature.

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

3. Precautions

3.1 Immutable domains

When a domain is immutable, all disk modifications are written in a temporary file. The longer the domain is running, the larger this file becomes. It is important to check that you have sufficient disk space. By default, the temporary folder is located in **/var/tmp**. This path can be changed using the **KvmQemu/tmpDir** entry in the hynesim-node configuration file.

3.2 LXC containers manual copy

If you wish to export a topology with LXC domains, we recommended you to compress the topology. If you do not compress the topology and want to move it afterwards, please use the rsync tool with the options described below instead of cp binary. This is important to avoid any domain corruption.

```
rsync -avPH -numeric-ids sourcefolder dest_folder
```

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

4. Troubleshooting

4.1 Unable to open a topology

A topology will not open for several reasons. Entities used in the topology may already be used in another topology, and are consequently locked in the catalog and unavailable for use. Unload the other topologies to open the desired topology. Entities used in the topology may have been deleted. In this case, use hyneview to access the topology catalog, and right click the broken topology and select **Fix Topology**. This action will remove deleted entities from the topology.

4.2 hynesim-node is running in degraded mode

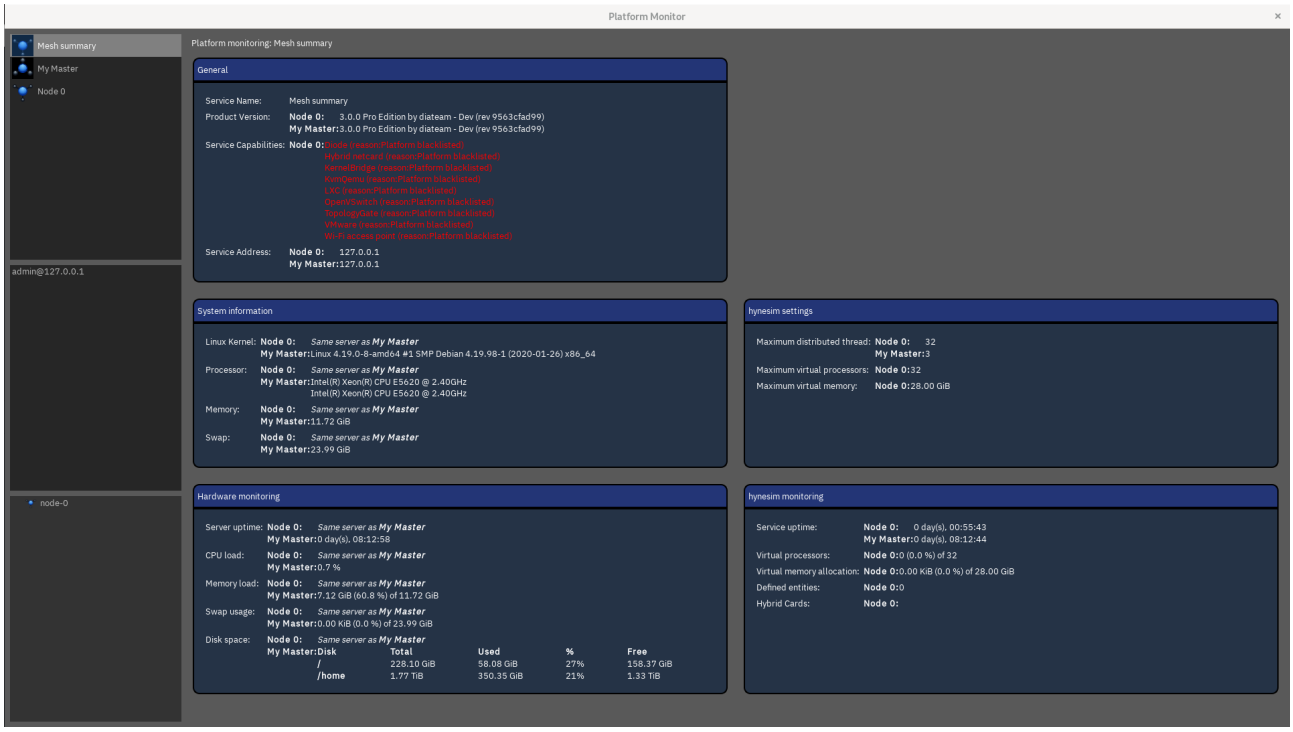

Figure 4.1: hynesim-node running in degraded mode

Sometimes, hynesim-node may run in degraded mode and blacklist all platforms. There may be several causes to this:

- a dependency is missing or the version mismatches;
- hynesim-node is not correctly configured;
- hynesim-node has been stopped while entities were running.

To fix the problem:

- Check hynesim-node logs in /var/log/hynesim-node.log;
- Install the missing dependency;
- Update hynesim-node configuration;

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN

- Stop, clean and start hynesim-node:

From the master, as user root:

```
dispatchAction node_name resetNode
```

From the node as root:

```
resetNode
```

4.3 A service has crashed or is frozen

When a service is frozen, generate debugging information from the master:

```
packageDebugInfo
```

Debugging information is generated in the **/data/hynesim/debug** folder. When a service has crashed, a core dump is generated in the **/home/core** folder. In any case you have to restart all services form the master:

```
resetPlatform
```

This document is the sole and exclusive property of DIATEAM and may not be duplicated or distributed without its consent.
STRICTLY CONFIDENTIAL - DISCLOSURE FORBIDDEN