INFINIBOX SECURITY GUIDE

Lat updated: 10/31/2018

Table of Contents

1 Best Practice for contacting INFINIDAT Support

- How to contact INFINIDAT support
- How to open a ticket on the Support site
- Set up Call Home
- Set Up Remote Support Session (RSS)
- InfiniTunnel
    - Precedence of the Remote Support Appliance
    - How to run InfiniTunnel
- Considerations for INFINIDAT Support Professional onsite

Our customers may engage INFINIDAT support when inquiring for a microcode upgrade, reporting on a bug, etc. Here are some best practice guidelines for contacting INFINIDAT support.

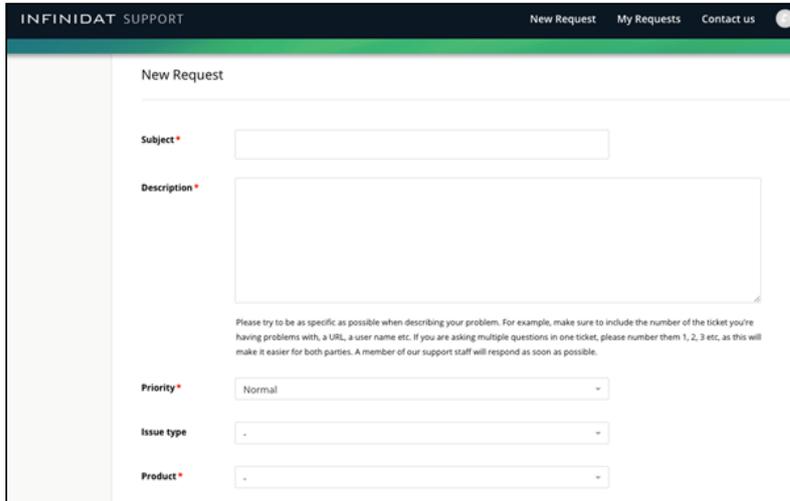## 1.1 How to contact INFINIDAT support

Contact methods:

- Contact your INFINIDAT Technical Advisor
    - For any issue, your first contact point is your TA.
    - The INFINIDAT Technical Advisor (TA) is a professional service person who is provided by INFINIDAT and assigned as the customer's first contact point.
    - Each customer has a dedicated TA for consulting and support activity arrangement.
    - If you do not have a TA or you don't know your TA contact info, please consult your INFINIDAT sale representative.
- Self-service on the Support website
    - https://support.infinidat.com
    - INFINIDAT provides self-service support website. In the website, the customer may check out:
        - InfiniBox documentation
            - Getting Started
            - Latest Release Notes
            - And many more help topics
        - Knowledge Base
        - Downloadable utilities to work with InfiniBox, get best practices and new release notes, etc.
    - On the Support website, the customer can also open a support ticket and INFINIDAT support will address it in a timely fashion.
- Email support@infinidat.com
- Call Center
    - A list of phone numbers is available on the support site

1.2 How to open a ticket on the Support site

1. Log into the Support site at: https://support.infinidat.com.

2. Click on the **New Request** button on the top bar of the screen.

A request form opens on the screen.

Fill in the following fields:

    a. Subject

    b. Description

    c. Priority - the default value is **Normal**. Set it to your needs.

    d. Issue type

    e. Product - the product that the request relates to. This is a mandatory field.

    f. System serial - the ID of your InfiniBox system.

3. Click **Submit**.

The request is submitted.

An automatic email is sent to you, acknowledging receiving the email.

4. The request is visible on the **My Requests** screen.

5. Upon INFINIDAT Support's reply, all email communication is logged into the request. There is no need to log into the support site in order to reply to a comment.

1.3 Set up Call Home

Using Call Home, the customer can set up InfiniBox to automatically send pre-failure or failure notifications to INFINIDAT event store. Based on pre-defined rules, these notifications will generate alerts in INFINIDAT issue tracking system. INFINIDAT support will analyze the alerts promptly and take appropriate actions. If the alert requires service, the customer will be informed and action will be taken with customer's approval (recovering the service in the system, sending replacement parts etc.).

Call Home notifications are sent through emails via an SMTP server. This is a one-way method of communication, which means Call Home cannot be used for INFINIDAT to access the InfiniBox.

1.4 Set Up Remote Support Session (RSS)

- INFINIDAT Remote Support is an optional software running on the Support Appliance (SA).
  - The INFINIDAT Remote Support provides a means of creating a secure point-to-point connection for supporting InfiniBox, accelerating the resolution of support cases.
    - On-demand secured connection to the InfiniBox on the customer site.
    - End-to-end encrypted channel.
    - Full customer control of the connection.
    - Full visibility and auditing of the session logs.
  - The Remote Support provides the INFINIDAT Support personnel with an access only to the Management interfaces of the InfiniBox system. This is equivalent to attaching a keyboard and a screen to the InfiniBox with the added benefit of exposing a full audit trail of the support session.
- Remote Support Release Notes are available here: INFINIDAT Remote Support Release Notes

1.5 InfiniTunnel

InfiniTunnel is a self-sustained support tool, designed to ease the process of opening an SSH tunnel for support purposes.

InfiniTunnel is designed to be run from a customer desktop/laptop system (Windows, Linux, Mac), and opens an SSH tunnel from InfiniBox storage system to INFINIDAT Support Server.

InfiniTunnel might be helpful when the Remote Support Appliance:

- Is not available
- Has no internet connection (for example, due to a firewall policy)

1.5.1 Precedence of the Remote Support Appliance

If the Remote Support Appliance is available, customers are advised to prefer using it over InfiniTunnel.

> ⚠️ InfiniTunnel temporarily enables an encrypted SSH tunnel from InfiniBox to a secured server over the internet.

1.5.2 How to run InfiniTunnel

1. Download InfiniTunnel
   a. A list of download locations is vailable here: InfiniTunnel.
2. To use InfiniTunnel, the following requirements have to be fulfilled:
   a. Run InfiniTunnel from a desktop / laptop system with Windows, Linux, or OS X operating systems.
   b. The system you are using must have internet access (port 22).

c. The system has to be connected to InfiniBox (using either a direct Ethernet cable or connecting to InfiniBox LAN).

1.6 Considerations for INFINIDAT Support Professional onsite

INFINIDAT Support Professional needs to be onsite, to support:

- Parts (Drive, Node, DIMM, etc.) replacement
- Remote session establishment if RSS and InfiniTunnel are not available from customer

The customer needs to provide INFINIDAT Support Professional with:

- Data Center Entrance Permit
- Internet Access (WIFI) if cellphone/hotspot is not allowed in Data Center

2 Accessing InfiniBox via HTTPS only

2.1 About this task

InfiniBox can be set to allow access via HTTPS only.

Upon setting the InfiniBox to allow access via HTTPS only, all access requests are redirected to SSL. The setting takes place during runtime and is persistent across reboot and hot upgrade.

2.2 GUI Instructions

1. Click the **Settings** icon on the navigation tree. On the **General** tab, slide the **Always redirect to HTTPS** slider.
2. Click **Update**.

2.3 InfiniShell Instructions

1. To set InfiniBox to be accessed via SSL only, run the following infinishell command: `config.system.set_ssl_redirection`.

2.4 Returned HTTP code

The redirection returns HTTP code 307.

3 Communicating with InfiniBox using an SSL certificate

3.1 About this task

This task allows the customer to secure the communication between the management tools and InfiniBox using an SSL certificate. The certificate can be either imported from a certificate authority, or created by InfiniBox. Using a self-signed certificate, eliminates the need to expose the private keys to INFINIDAT support.

InfiniBox validates:

- That the certificate is in PEM format
- The digital signature fits the certificate content

InfiniBox **does not** validate:

- The certificate trust-chain

3.1.1 Terminology

- Certificate - A file allowing a client to validate the identity of the server it is communicating with using information from a 3_{rd} party CA
  Each certificate is signed by another certificate, creating a chain up to a parent that both sides can trust.
- CA - Certificate Authority, a trusted 3rd party the client and server use to verify the identity of the server to the client.
- SSL-Certificate - a certificate used to verify HTTPS servers.
- Root certificate (a.k.a. trust chain) - the set of certificates leading up to the trusted 3rd party both client and server know.

3.2 Checking the validity of the current certificate

Click the **Settings** icon on the navigation tree. On the **General** tab, click **Modify HTTPS Certificate**. The **HTTPS Configuration** screen opens.
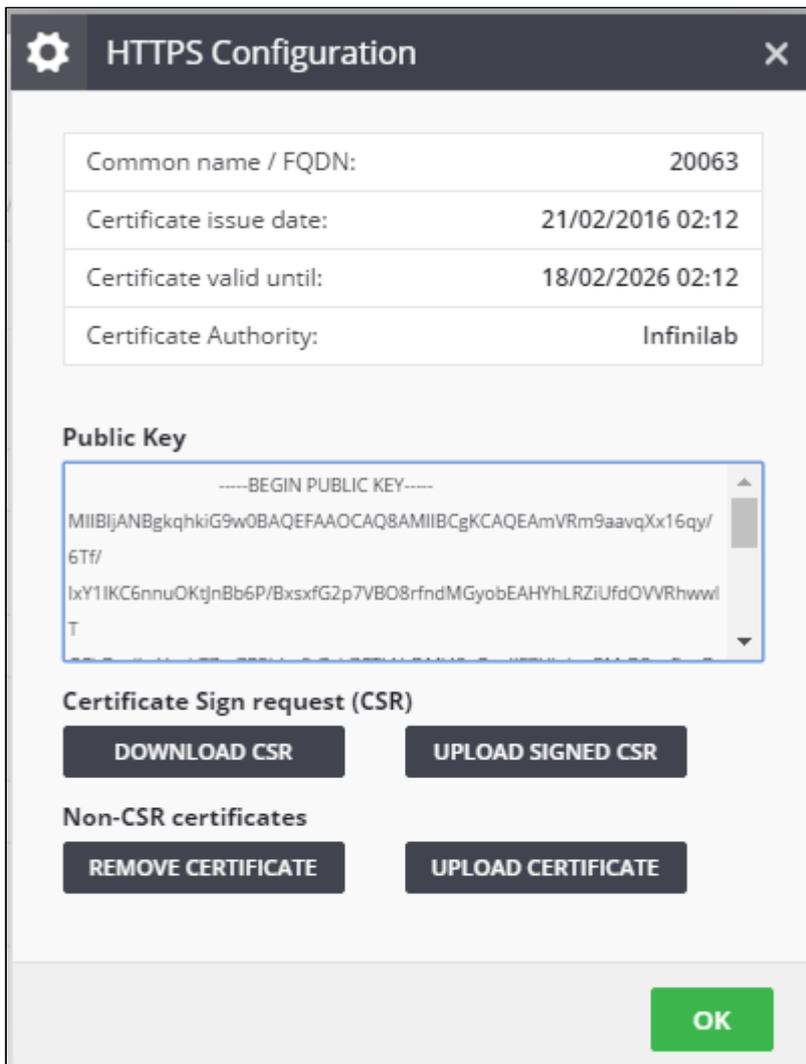
The screen color scheme indicates the certificate validity:

- Black text - the certificate is valid for at least 30 days
- Orange color - the certificate is valid for less than 30 days
- Red color - the certificate is no longer valid

3.3 Importing a certificate to InfiniBox

You can upload either a self-signed certificate or a certificate that was approved by an external certificate authority.

The certificate file is validated for:

- Format - the certificate has to be in PEM format only
- Integrity - the certificate digital signature has to match the certificate file content (this validation assures that the certificate file was not hampered anywhere down the trust chain)

1. Click the **Settings** icon on the navigation tree. On the **General** tab, click **Configure HTTPS**.

   The **HTTPS Configuration** screen opens.

2. Click either:
   - **Upload certificate**
   - **Upload signed CSR** - for a self-signed certificate

3. Browse to the certificate file and click **Select**.

4. Click **Modify**.

   a. The certificate file is uploaded

   b. The certificate file is validated

3.4 Removing a certificate

When the certificate is removed from InfiniBox, the connection between the GUI and InfiniBox is no longer secured.

1. Click the **Settings** icon on the navigation tree. On the **General** tab, click **Configure HTTPS**.

   The **HTTPS Configuration** screen opens.

2. Click either:

   a. **Download CSR**

   b. **Remove certificate**

3. Click **Modify**.

3.5 InfiniShell instructions

- `config.system.ssl_certificate.upload` - sets the SSL certificate for the system
- `config.system.ssl_certificate.create_csr` - creates a Certificate Sign Request (CSR) file. This file includes only the public key and is a more secure method of generating a certificate.
- `config.system.ssl_certificate.upload_signed_csr` - sets the certificate using a signed CSR file
- `config.system.ssl_certificate.clear` - clears the existing SSL certificate and replaces it with a self-signed certificate
- `config.system.certificate.query` - displays a list of the certificate that are currently in use. The screen color scheme indicates the certificate validity (see above)

3.6 Returned HTTP code

The redirection returns HTTP code 307.

4 Overview of user management

4.1 InfiniBox user management

The InfiniBox management interface is exposed in the form of a comprehensive REST API,GUI and CLI. To prevent unauthorized access to the system configuration and monitoring capabilities, access to the API requires a succesful authentication in the form of providing user and password credentials of a user with a valid role in InfiniBox.

InfiniBox supports multiple types of user repositories which can be used for user authentication and access rights resolution. InfiniBox supports using multiple user repositories concurrently with the ability to define the credentials resolution across the repositories.

Administrative user repository types

- Local users - User repository defined and managed within the InfiniBox system itself
- Active Directory (AD) - Microsoft Active Directory of a specific domain (representing multiple AD servers)
- OpenLDAP - Open LDAP repository stored on an OpenLDAP server

4.1.1 Limits

- Max number of local users in the system: 50
- Max number of external user repositories: 10
- Max number of servers within an OpenLDAP repository: 3

4.2 Role Based Access Control (RBAC)

InfiniBox role-based access-control (RBAC) assigns authenticated users into predefined access permission roles. The access rights of each of the roles are pre-configured, thus the extent of the user actions is predictable. InfiniBox supports 4 role types, where each user must have a single role assigned to it.

4.2.1 Available user roles

Read-only

A read-only user can query for information only. The query permissions are sufficient for carrying out monitoring tasks, viewing the system health, events, capacity utilization, etc. The read-only user cannot, however, make any changes to the system.

Admin

The admin (system administrator) has permission for all InfiniBox software functionality, including network administration, provisioning pools and entities, and creating other users. For creating other users, see below.

Create user(s) with this user role for Host products and Snap Rotator.

Pool admin

The pool admin has admin rights for a specific pool (or multiple pools). Within this pool (or pools), the pool admin can provision datasets, map them to hosts and take snapshots, but cannot create new pools or change the definitions of existing pools.

The pool admin has read-only permissions outside its pool (or pools).

Technician

The technician is a role that is typically assigned to INFINIDAT technicians that take care of InfiniBox hardware on the customer premise.

The technician role has permissions that are identical to the read-only user, with additional access to FRU API, CLI and GUI commands.

The status of the InfiniBox system physical components is visible to all user roles (admin, pool admin, read-only). However, only the technician has access to commands that are required for hardware maintenance (for example, the deactivation of a faulty drive and the activation of the new drive that replaces the faulty drive).

4.2.2 InfiniBox functionality for user roles

InfiniBox functionality	Admin	Pool Admin	Read Only	Technician
Pool administration	👍	❌	❌	❌
Provisioning volumes, filesystems, consistency groups and their snapshots	👍	👍	❌	❌
Exporting a filesystem	👍	👍	❌	❌
Assigning pools and volumes to a QoS policy	👍	❌	❌	❌
Host and cluster management	👍	👍	❌	❌
Event rules administration	👍	❌	❌	❌
Provisioning a replica	👍	👍	❌	❌
Network management	👍	❌	❌	❌
Hardware operations	❌	❌	❌	👍
User management	👍	❌	❌	❌

4.3 User repositories

4.3.1 Local users

InfiniBox provides you with a set of out-of-the-box local users. On top of these out-of-the-box users, you can define more local users. All of the local users have to have one of the available user roles.

Setting user names and passwords

- Both user names and passwords are case-sensitive
- User names have to conform to the following guidelines:
- Maximum of 65 Latin characters, numbers, spaces, and the following symbols: "^&'@()[]$=!-#{}%.+~_" (excluding quotation marks).
    - Leading and trailing whitespace characters are stripped.

4.3.2 Role management in external user repositories

Unlike the local users repository, external repositories role assignment is done at the group level - i.e. a group from AD or OpenLDAP repository can be assigned one of the access roles. Users belonging to this group will be granted the role of the group.

4.3.3 Definining an Active Directory domain as user repository

Defining an Active Directory domain repository as a user repository in InfiniBox requires the following information:

- AD Domain name
- Repository Name
- Bind username and password
- Whether to use LDAPS
- Users (optional) - in order to limit InfiniBox access only to some of the repository users, specify these users according to these attributes:
    - User Class, Username Attribute, Users Base DN
- Groups (optional) - in order to limit InfiniBox access only to some of the repository user groups, specify these users according to these attributes:
    - Group Class, Group Name Attribute, memberof Attribute, Group Base DN

InfiniBox dynamically discovers all AD domain controllers by issuing a DNS query to the provided AD domain, InfiniBox will then try to use the fastest responding domain controller for its AD queries.

4.3.4 Defining OpenLDAP server as user repository

Defining an Active Directory or LDAP server to work with InfiniBox requires the following information:

- Repository Name
- OpenLDAP Server(s) ip/hostname
- Use SSL - select whether to use LDAPS
- Port
- Bind username and password
- Users (optional) - in order to limit InfiniBox access only to some of the repository users, specify these users according to these attributes:
    - User Class, Username Attribute, Users Base DN
- Groups (optional) - in order to limit InfiniBox access only to some of the repository user groups, specify these users according to these attributes:
    - Group Class, Group Name Attribute, memberof Attribute, Group Base DN

For resiliency, it is highly recommended to define multiple OpenLDAP servers managing the same user repository, so that in case of a unavaliability of one of the OpenLDAP servers, InfiniBox can transparently failover to use others.

4.4 Authentication methods

InfiniBox authenticates local users by comparing the username and password that the user provides during the login to InfiniBox to the credentials that are stored on the InfiniBox.

An LDAP / Active Directory user does not authenticate directly to InfiniBox. The user authenticates to LDAP / Active Directory, and the LDAP / Active Directory is defined as an InfiniBox user group. User management is done in the user repository.
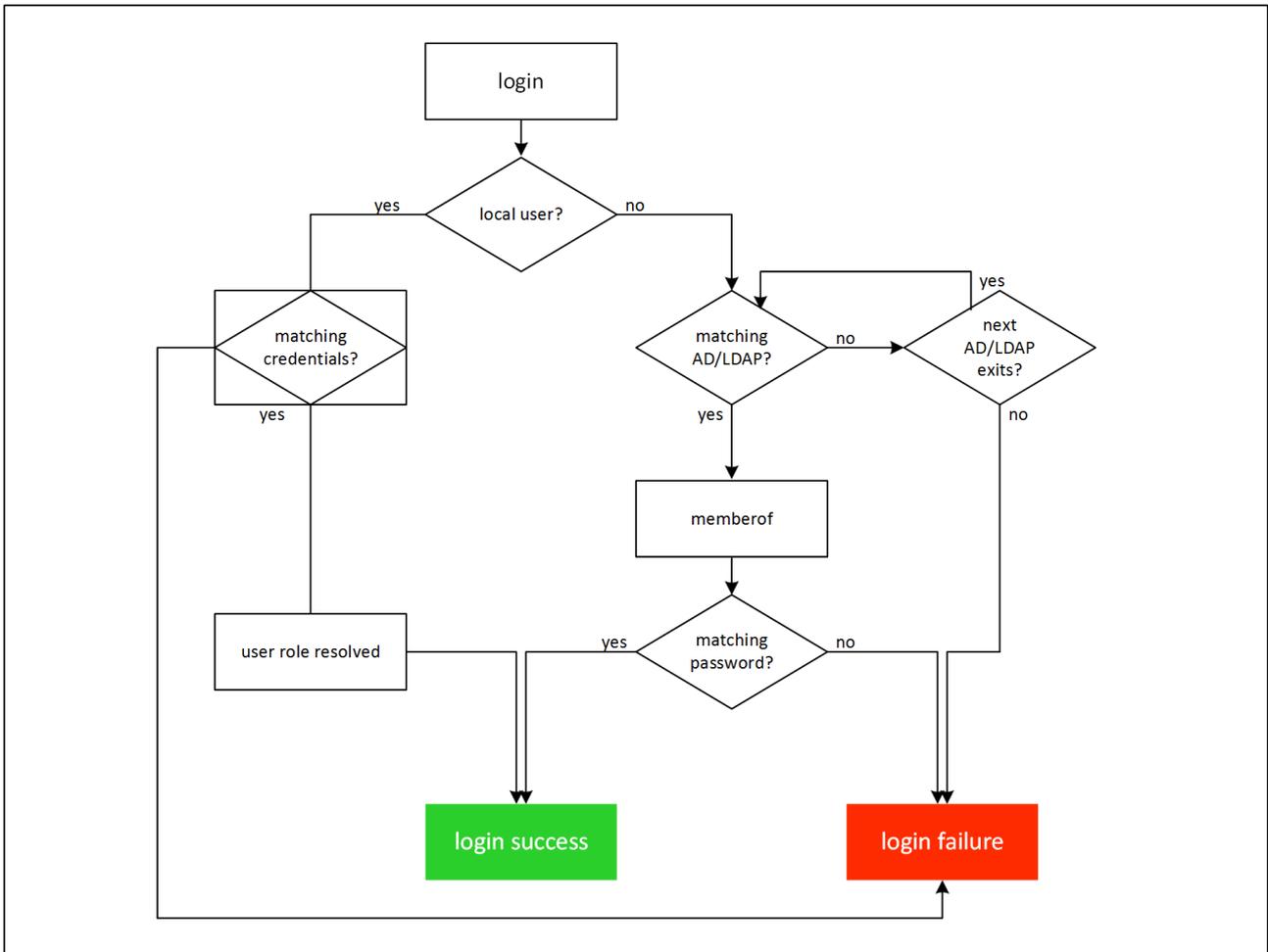
For a broader discussion, see: InfiniBox Security Guide.

4.4.1 User authentication and role resolution process

When the user logs into InfiniBox and types the username and password, the username is resolved in the following order:

1. InfiniBox checks whether the username belongs to a local user. If it is, InfiniBox checks whether the password matches and the login succeeds

2. If the username does not belong to a local user, InfiniBox looks for it in the AD and LDAP that are configured to work with InfiniBox.

    a. If the username belongs to any of the AD or LDAP and belongs to a user group that is allowed to log into InfiniBox, the login succeeds.

    b. The username is assigned with a user role that is determined by the user group that the repository is mapped to.

    c. In case that the username sppears in more than one repository, the username is resolved according to the repository that ranks first in the order of resolution list. The order of resolution is configurable.

3. The login fails in the following cases:

    a. The username does not belong to any local user, nor any AD or LDAP

    b. The username belongs to an AD or LDAP that is configured to work with InfiniBox, but is not a member of a group that is allowed to work with InfiniBox

    c. The usename is listed as a local user, or belongs to the right group, but the provided password is incorrect

Authentication and Role resolution diagram

```
                    ┌─────────────┐
                    │    login    │
                    └─────────────┘
                           │
                           ▼
        yes          ◇ local user? ◇          no
    ┌──────────────                 ──────────────┐
    │                                             │
    ▼                                             ▼
◇ matching        ◇ matching ◇    no    ◇ next        ◇   yes
  credentials?      AD/LDAP?   ──────►    AD/LDAP
                                          exits?
    yes                │                      │
    │                 yes                     no
    ▼                  ▼
┌──────────────┐   ┌──────────┐
│ user role    │   │ memberof │
│ resolved     │   └──────────┘
└──────────────┘        │
                        ▼
              yes  ◇ matching ◇  no
                     password?
```

┌─────────────────┐   ┌─────────────────┐
│ login success │   │ login failure │
└─────────────────┘   └─────────────────┘

5 Locking a local user

- About this task
  - A note on predefined user
- Disabling a user
- Enabling a user

5.1 About this task

This security feature allows the system admin to better control local accounts, refraining them from accessing InfiniBox on demand. The system admin can lock any of the local users. The locked user is still listed on the users list, but cannot log into the InfiniBox system until unlocked by the system admin.

- NFINIDAT recommends to disable all **local** all users and only use Active Directory users.
- This operation is applicable only to local users.
- For more information on managing LDAP users, see here: Overview of user management

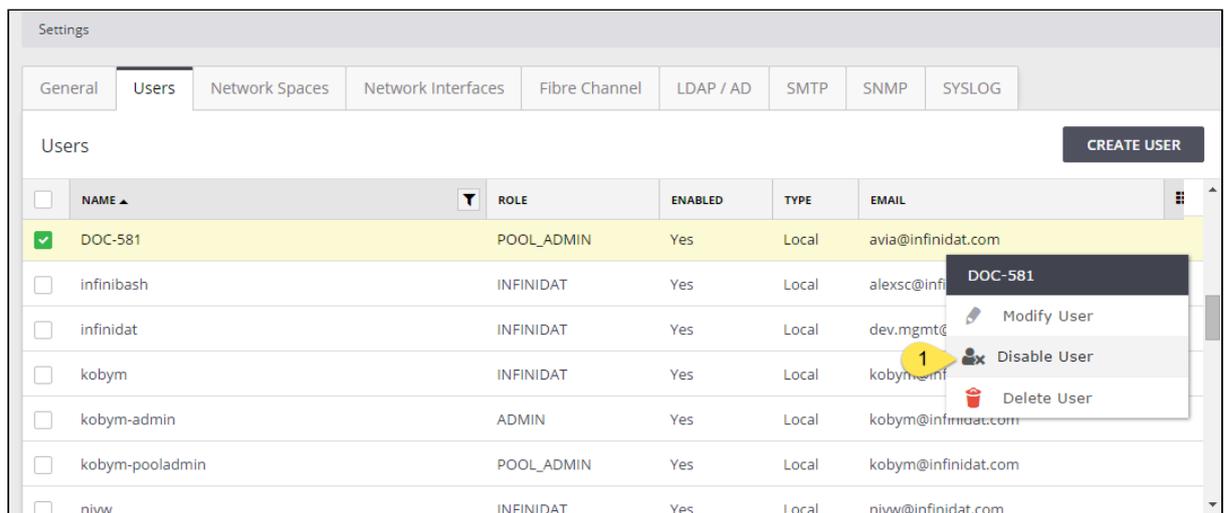### 5.1.1 A note on predefined user

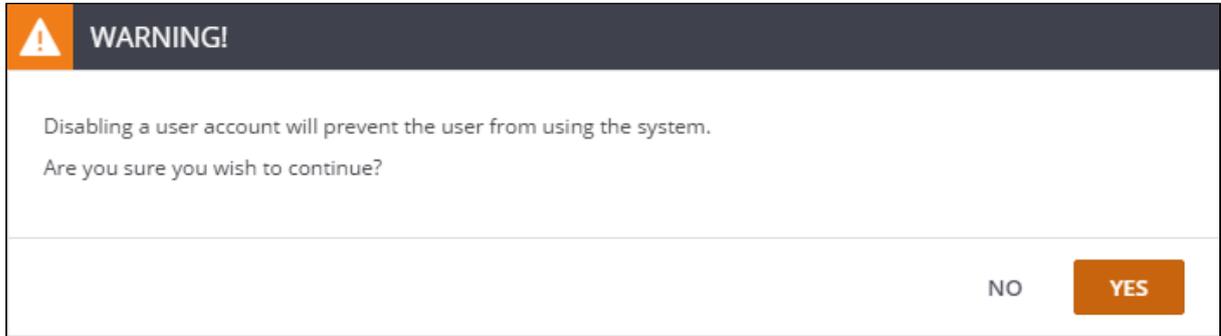This task allows to lock all predefined local users, including:

- INFINIDAT
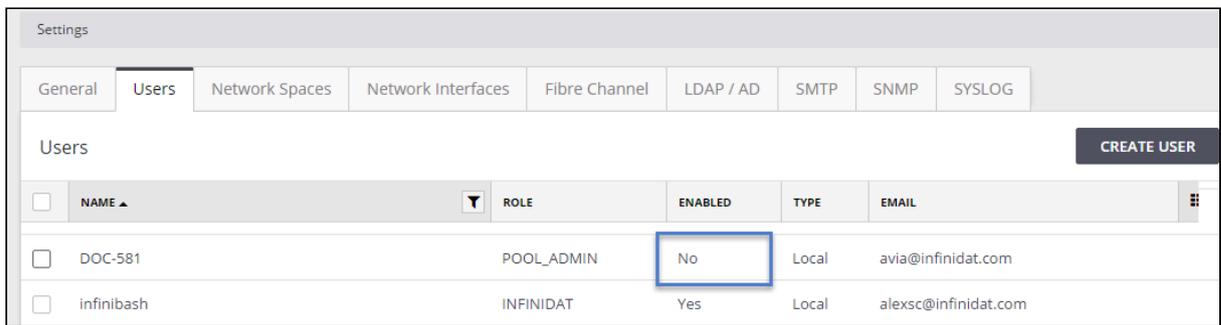- Technician

5.2 Disabling a user

1. Click the GUI **Settings** icon and then the **Users** tab.
2. Check a user and select **Disable user** from the actions menu.

3. Approve the operation:

The user is marked as disabled.

5.3 Enabling a user

1. Click the GUI **Settings** icon and then the **Users** tab.

2. Check a user and select **Enable user** from the actions menu.

   The user is enabled.

6 Setting the session timeout

6.1 About this task

InfiniBox session timeout values are configurable from the GUI and CLI. These values apply to all of the clients (GUI, CLI, API).

- Idle session timeout - sets the session to expire in case of user inactivity
  - The user's credentials are kept for the timeout period. Within this period, when opening the GUI in the browser, there is no need to type the user and password.
  - By default, the session terminates after 1 hour of inactivity
- Active session timeout - sets the session to disconnect the user
  - By default, the session expires after 24 hours

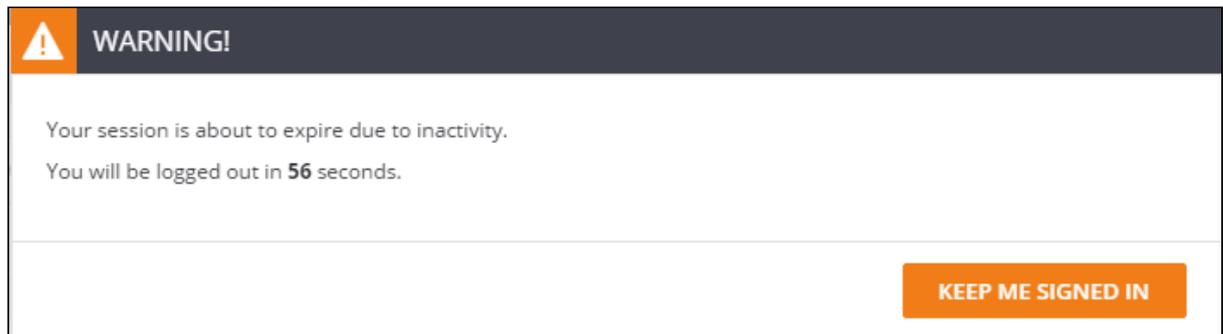These values are configurable, as described below.

6.2 Handling session expiry

6.2.1 Idle session timeout

When the session is about to expire due to inactivity, a message pops-up on screen.

1. To keep the session, click on **Keep me signed in**.
    The Idle Timeout counter is reset, allowing another hour of inactivity (1 hour by default, or the
    amount of time configured by the user).

6.2.2 Active session timeout

When the session expires, the user returns to the login screen.

6.3 Setting the session timeout parameters

6.3.1 Using the GUI

1. Log into InfiniBox GUI and click the **Settings** icon. The Setting screen opens,
    displaying the **General** tab.
2. Set the session timeout parameters:
    a. Idle session timeout
    b. Active session timeout

3. Click **Update.**
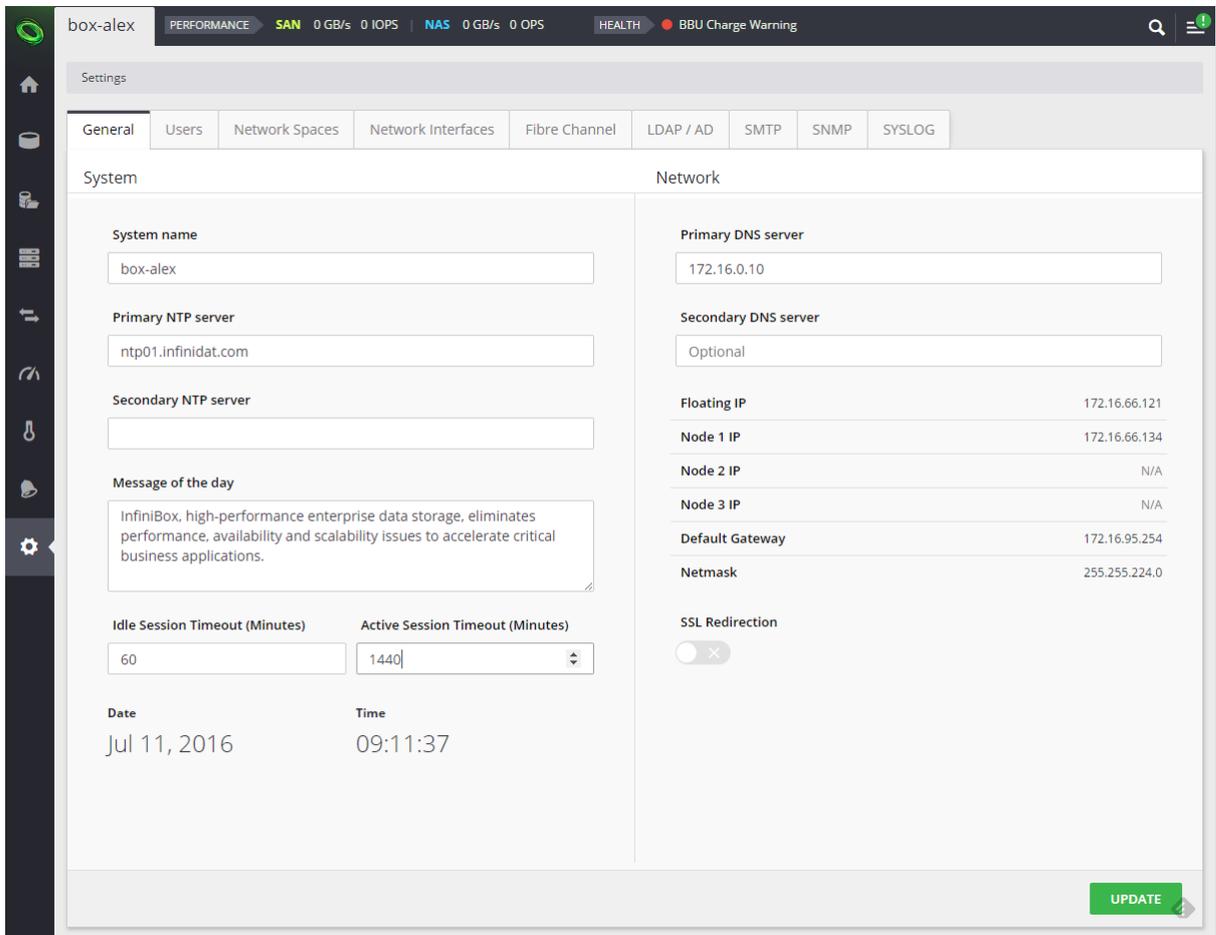
6.3.2 Using InfiniShell

Set both active and idle system timeout

```
config.system.set_session_timeout active_session=1440 idle_session=60
```

Query for the active and idle system timeout

```
config.system.query
```

6.3.3 Using the API

Setting the active session timeout

Required URL parameters

None

Required JSON data

The time in minutes.

```
"2880"
```

API endpoint

```
PUT api/rest/config/mgmt/mgmt.session_expiry
```

Returned code

```
{
    "metadata": {
        "ready": true
    },
    "result": 2880,
    "error": null
}
```

Setting the idle session timeout

Required URL parameters

None

Required JSON data

The time in minutes.

```
"60"
```

API endpoint

```
PUT api/rest/config/mgmt/mgmt.session_idle_timeout
```

Returned code

```
{
    "metadata": {
        "ready": true
    },
    "result": 120,
    "error": null
}
```

Getting the active session timeout

Required URL parameters

None

Required JSON data

None

API endpoint

```
GET api/rest/config/mgmt/mgmt.session_expiry
```

Returned code

```
{ "metadata": { "ready": true }, "result": 1440, "error": null }
```

Getting the session idle timeout

Required URL parameters

None

Required JSON data

None

API endpoint

```
GET api/rest/config/mgmt/mgmt.session_idle_timeout
```

Returned code

```
{ "metadata": { "ready": true }, "result": 60, "error": null }
```

7 Setting the host security properties

- About this task
- Before you begin
- Prerequisites
- GUI instructions

7.1 About this task

This task sets the security properties of an iSCSI host.

- The security settings cannot be used during the discovery of the iSCSI target

7.2 Before you begin

Read here on the available types of CHAP security: Overview of iSCSI connectivity.

7.3 Prerequisites

- iSCSI host

7.4 GUI instructions

1. Click the **Hosts & Clusters** icon on the toolbar at the left of the InfiniBox Management Console screen.
2. Select a **Host**.
3. Select **iSCSI Security** from the Actions menu.
4. Select between:
   a. **None** - the property that is set to the host upon creation
      i. Check whether to clear previously set users and passwords
   b. **CHAP** - an Inbound only security setting
      i. Set the **User**
      ii. Set the **Target Secret** - optional: click **Auto Generate** to generate a 16-digits secret
   c. **Mutual** - a both Inbound and Outbound security setting
      i. Set pairs of user and secret for the target and the initiator
5. Click **Modify**.

   The host security properties are set.

8 Assigning a PoolAdmin to a pool

8.1 About this task

The PoolAdmin user is the administrator of specific pools. This user has admin rights that are similar to the InfiniBox admin, but limited to the pool (or pools) that the PoolAdmin is assigned to.

8.2 Prerequisites

To assign a pool to a user you need:

- A user with PoolAdmin role
    - You can assign the user to a pool upon creation of the user, as well
- A pool

You may add more than one pool to the same PoolAdmin, and more than one PoolAdmin to a pool.

8.3 GUI instructions

1. Modify the pool (see instructions here: Deleting a pool)

2. On the **Modify Pool** screen, click **Advanced**

3. Click on the Pool Admin field to see a list of available users

4. Click **Modify**

   The PoolAdmin user is now associated to the pool.

8.4 PoolAdmin -related InfiniShell commands

- `user.create` - In the following example, we create a user with the type PoolAdmin.
    - ```
      user.create name=pool-01-admin password=123456 email=user@infinidat.com
       role=PoolAdmin
      ```
- `user.add_pool` - adding a pool to a user
    - ```
      user.add_pool name=pool-01-admin pool=pool-01
      ```
- `user.query` - query for the user and the pool
    - ```
      user.query user=pool-01-admin
      ```
- `pool.add_admin` - adds a PoolAdmin to a pool.
- `pool.remove_admin` - removes a PoolAdmin from a pool.
- `pool.user_query` - lists pool administrators per pool

9 Overview of event notification

InfiniBox monitors and issues events on its health, performance and capacity, as well as on the user activity. The events are displayed on a central event log that is accessible via the InfiniBox GUI, InfiniShell and API. The events can also be sent outside the InfiniBox for further troubleshooting.

- Events
    - Event severity
    - Event reporter
    - Event retention
    - Event behavior
    - Custom events
    - Heartbeat event
- Event notification
    - Event notification rule

9.1 Events

9.1.1 Event severity

InfiniBox assigns each of the events it generates with a severity level. The severity level is the quickest way to filter events that are displayed in the event log and when setting a notification rule. The severity level is preconfigured into the event definition and cannot be changed. The available severity levels are:

- Info - informational - the system reports on an operation that does not have a negative implication on the system operation. For example, a creation of an entity, user login.
- Warning - example, a change in the state of an hardware component, pool space low, etc.
- Error - a failure in a hardware component that requires user action, a user action that may limit the system operation. For example, pool space very low.
- Critical - a failure that requires an immediate user action

9.1.2 Event reporter

InfiniBox events are grouped by reporters, which are the InfiniBox component that generates them.

9.1.3 Event retention

- InfiniBox keeps 5M events
- Events are deleted in 100,000 increments

9.1.4 Event behavior

- The event is exposed to the event log 10 seconds after it is generated

9.1.5 Custom events

- Available templates
    - CUSTOME_INFO_EVENT
    - CUSTOM_WARNING_EVET
    - CUSTOM_ERROR_EVENT
    - CUSTOM_CRITICAL_EVENT
- Maximum event size: 100kb

9.1.6 Heartbeat event

- Sent to INFINIDAT via the preconfigured SMTP server once a day
- The content of the event informs INFINIDAT support on the state of the INfiniBox system
- The event does not contain user information

9.2 Event notification

InfiniBox sends event notification to the following destination types:

- SMTP
- SNMP
- SysLog

You can send the notifications to up to 10 destinations.

> Active polling for events (SNMPWALK, etc.) is not supported

9.2.1 Event notification rule

The event notification rule includes the following information:

- Rule name
- Destination
    - Target - a destination to where the notification is sent
    - Target parameters - for example, an email address for SMTP rule
- Filter
    - Event level - all of the events of this level will be sent
    - Additional events - events that belong to a level that is not marked by this rule, and will be sent
    - Excluded events - events that belong to a level that is marked by this rule, and will not be sent

10 Changes from previous releases

- The **Creating a Network Space for NAS** chapter is replaced with the **InfiniBox 4.0.x Best Practices Guide for Setting Up a NAS Service** document ([see here](#)).
- The content of the **Active directory integration chapter is integrated into Overview of InfiniBox user management.**

11 TCP and UDP ports required for INFINIDAT products

A list of TCP and UDP ports that are required for INFINIDAT products is available here.