Installation instructions for the Impex family

SYSCTL AB

Table of Contents

1 Installation basics

Installation media can be downloaded from ***https://portal.sysctl.se as*** an ISO-file for every installation type or an Azure image for the ICC server. The installation supports only installation from ISO and not any kind of images with the exception for Azure image. Only the ICC server can be installed on Azure cloud infrastructures Azure.

1.1 Getting the installation media

All Impex products can be installed from ISO, the example below is for the ICC ISO but the procedure is the same for all products.

Download the ICC ISO from https://portal.sysctl.se and verify the SHA256 checksum

```
sha256sum sysctl-icc-5.0.0.iso

or on Windows system using powershell:

Get-FileHASH sysctl-icc-5.0.0.iso
```

Most common is to install the servers in a virtualization environment, but it is also possible to install the software on physical hardware. The USB Protect is always installed on physical hardware.

Use the Linux command dd to add the iso to a USB-device, this is most common for the USB Protect installation

```
dd if=sysctl-usbprotect-5.0.0.iso of=/dev/sdX bs=4096
```

Note: replace `sdX` above with the actual device. Probably it is `sda` but please verify since using the incorrect device here could lead to irreparable harm to your computer.

It may also be possible to burn it with tools like rufus, but ensure the tool uses *dd-mode*.

1.2 Installation from the installation media

All installations are unattended and require only the root password to be configured with exception for USB Protect which does not have any static root password.

1.2.1 Installation in virtual environments

The software and installation media requires EFI enabled virtual hardware to boot. This must be configured before the installation starts.

1.2.2 USB Protect installation instructions

Before you begin, contact SYSCTL to obtain the UEFI password for your USB Protect hardware.

1. Press “F12” to access the boot menu and select the option to boot from the USB.
2. Enter the UEFI password when prompted.
3. The installation will proceed automatically without further input.

If a USB Protect upgrade is necessary, follow the same procedure outlined above. The installation will preserve the current configuration and apply it after the new installation. If you need to erase the old configuration as well, interrupt the installation process and restart it. This works because, after collecting the old settings from the hard drive, the system clears the disk. When the installation is restarted, it proceeds with a fresh configuration.

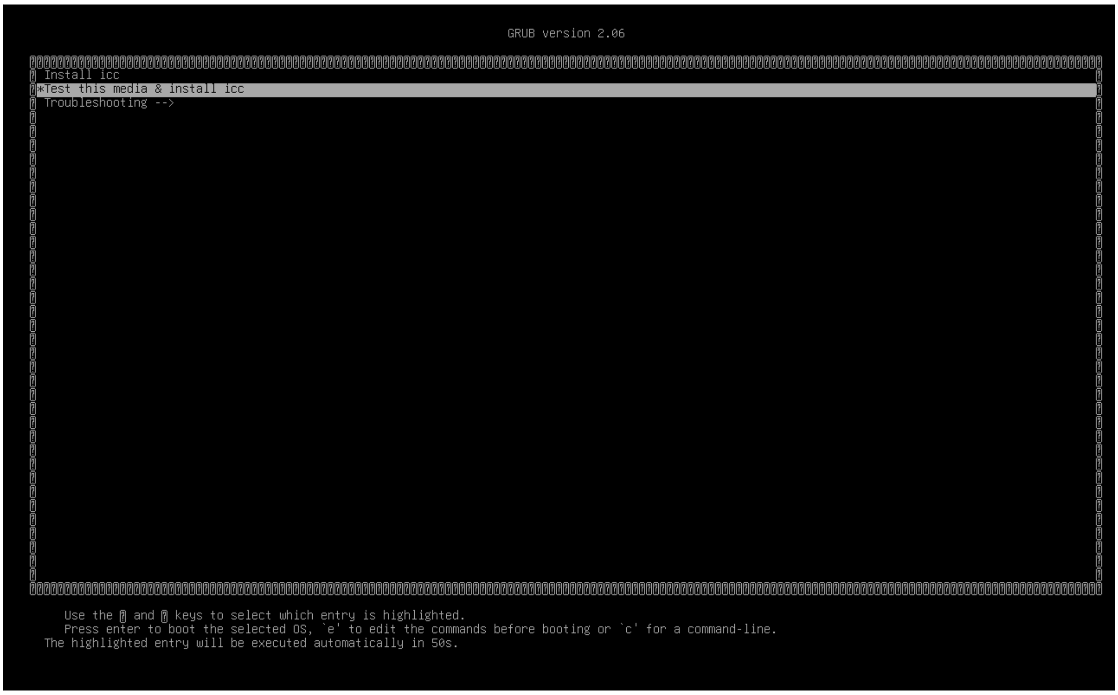
To connect the station to an ICC server, refer to the USB Protect user manual for detailed instructions.

To set the station in offline mode, refer to the USB Protect user manual for detailed instructions.

1.2.3 Installation steps for ICC, Repo and DataLock

Choose the correct ISO for your installation and if needed, create a bootable USB. Boot the system from the installation media.

The installation will start to install after 60 seconds if no option is selected.

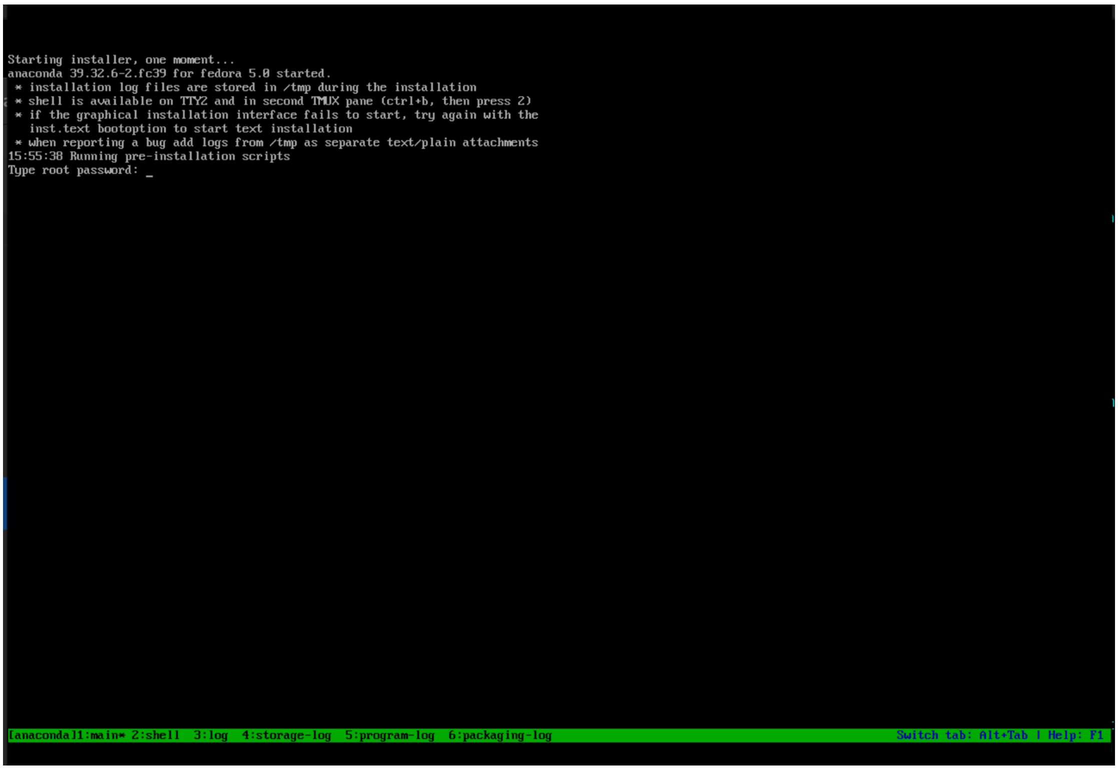


```
                              GRUB version 2.06

 Install icc
*Test this media & install icc
 Troubleshooting -->

    Use the ▯ and ▯ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands before booting or `c' for a command-line.
 The highlighted entry will be executed automatically in 50s.
```

Boot menu for an ICC installation

After one of the options has been selected the installation will begin and the harddrive will be wiped. If the ICC or Repo has been selected it will be possible to set the root password during the installation. If it is a USB Protect installation will the system automatically look for a previous installation and copy the configurations from the old installation. If this is not the desired action one can abort the installation after it created a new filesystem and then boot again on the installation USB drive. This time the system disk will have been wiped and no previous configuration files will be found, making this a new clean installation.

Set a password for the root user if this is an ICC, REPO or Datalock installation.

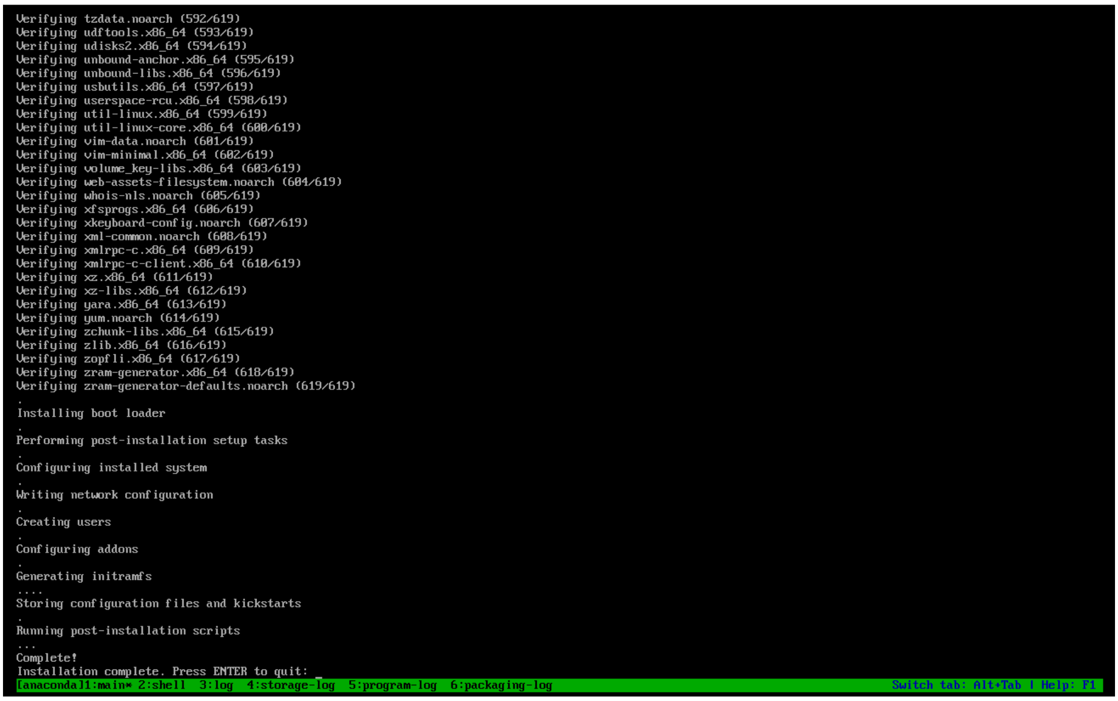


```
Starting installer, one moment...
anaconda 39.32.6-2.fc39 for fedora 5.0 started.
 * installation log files are stored in /tmp during the installation
 * shell is available on TTY2 and in second TMUX pane (ctrl+b, then press 2)
 * if the graphical installation interface fails to start, try again with the
   inst.text bootoption to start text installation
 * when reporting a bug add logs from /tmp as separate text/plain attachments
15:55:38 Running pre-installation scripts
Type root password: _
```

```
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log  6:packaging-log                    Switch tab: Alt+Tab | Help: F1
```

Set root password

After the installation is completed, press *enter* to reboot.



```
Verifying tzdata.noarch (592/619)
Verifying udftools.x86_64 (593/619)
Verifying udisks2.x86_64 (594/619)
Verifying unbound-anchor.x86_64 (595/619)
Verifying unbound-libs.x86_64 (596/619)
Verifying usbutils.x86_64 (597/619)
Verifying userspace-rcu.x86_64 (598/619)
Verifying util-linux.x86_64 (599/619)
Verifying util-linux-core.x86_64 (600/619)
Verifying vim-data.noarch (601/619)
Verifying vim-minimal.x86_64 (602/619)
Verifying volume_key-libs.x86_64 (603/619)
Verifying web-assets-filesystem.noarch (604/619)
Verifying whois-nls.noarch (605/619)
Verifying xfsprogs.x86_64 (606/619)
Verifying xkeyboard-config.noarch (607/619)
Verifying xml-common.noarch (608/619)
Verifying xmlrpc-c.x86_64 (609/619)
Verifying xmlrpc-c-client.x86_64 (610/619)
Verifying xz.x86_64 (611/619)
Verifying xz-libs.x86_64 (612/619)
Verifying yara.x86_64 (613/619)
Verifying yum.noarch (614/619)
Verifying zchunk-libs.x86_64 (615/619)
Verifying zlib.x86_64 (616/619)
Verifying zopfli.x86_64 (617/619)
Verifying zram-generator.x86_64 (618/619)
Verifying zram-generator-defaults.noarch (619/619)
.
Installing boot loader
.
Performing post-installation setup tasks
.
Configuring installed system
.
Writing network configuration
.
Creating users
.
Configuring addons
.
Generating initramfs
....
Storing configuration files and kickstarts
.
Running post-installation scripts
...
Complete!
Installation complete. Press ENTER to quit: _
[anaconda]1:main* 2:shell  3:log  4:storage-log  5:program-log  6:packaging-log                          Switch tab: Alt+Tab | Help: F1
```

Finish installation

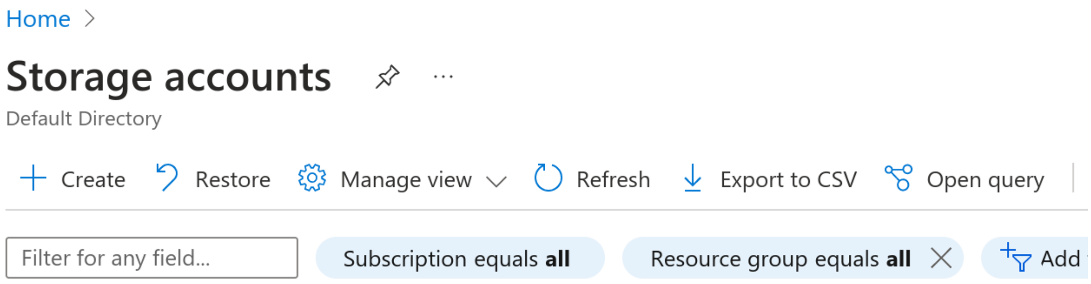
1.3 Azure

1.3.1 Get the installation image

Download the Azure image from https://portal.sysctl.se

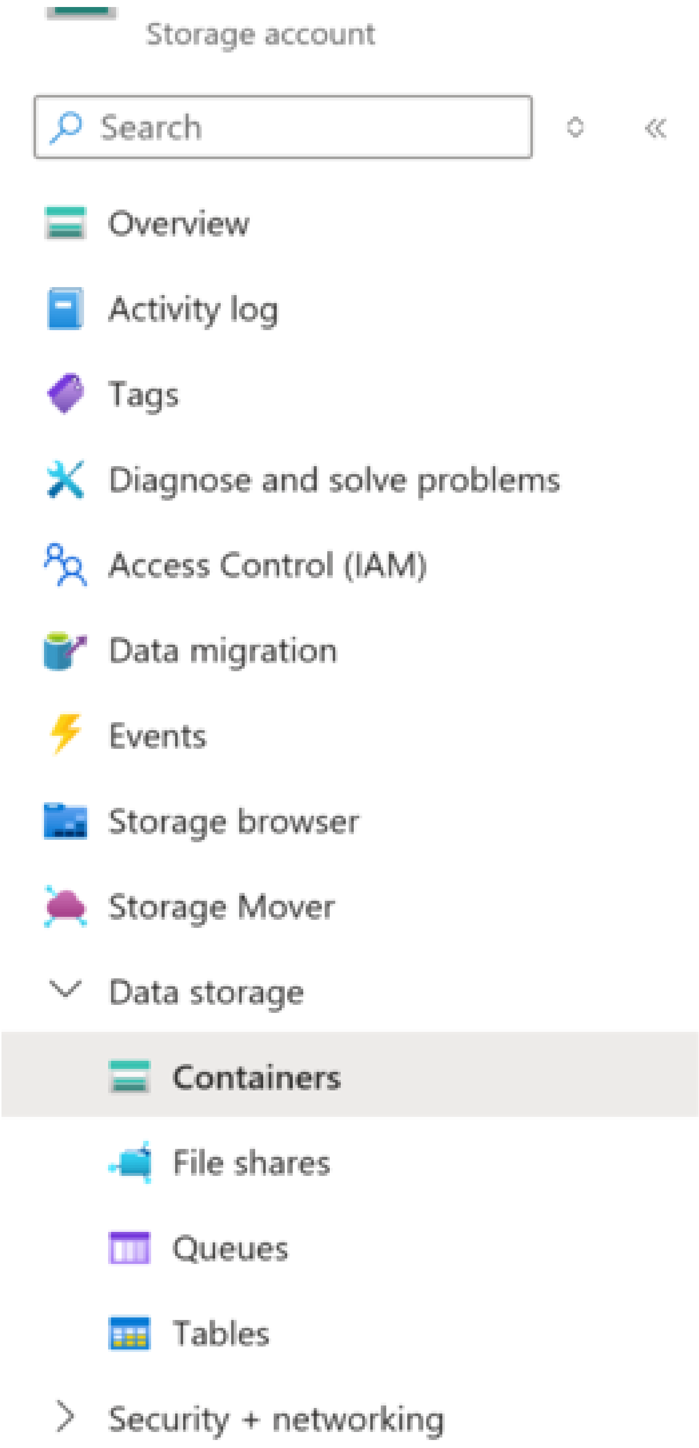
1.3.2 Azure configuration

Create a storage account



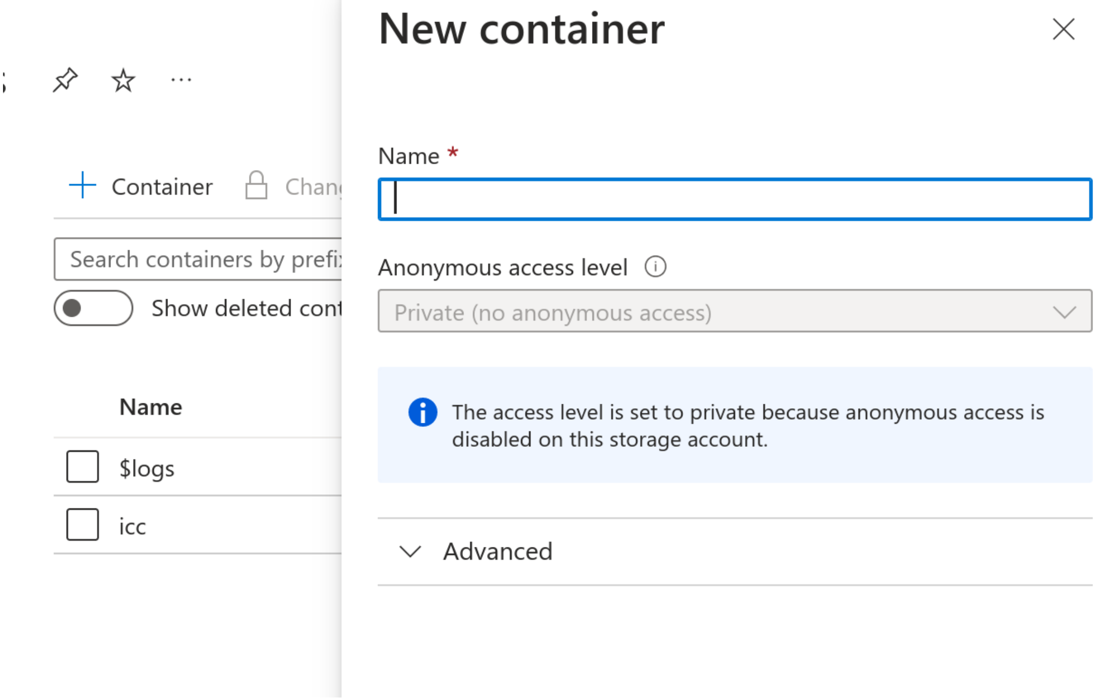
Create Storage Account

In the storage account, go to **Containers**



Storage Account Container

Create a new container



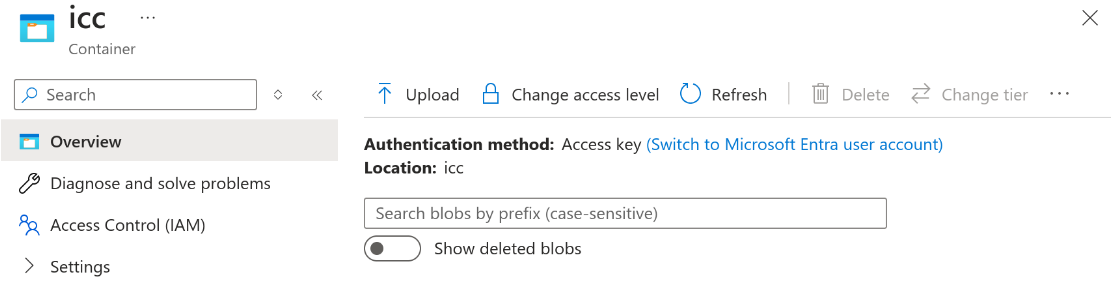
Name *

Anonymous access level: Private (no anonymous access)

The access level is set to private because anonymous access is disabled on this storage account.

Storage Account Create Container

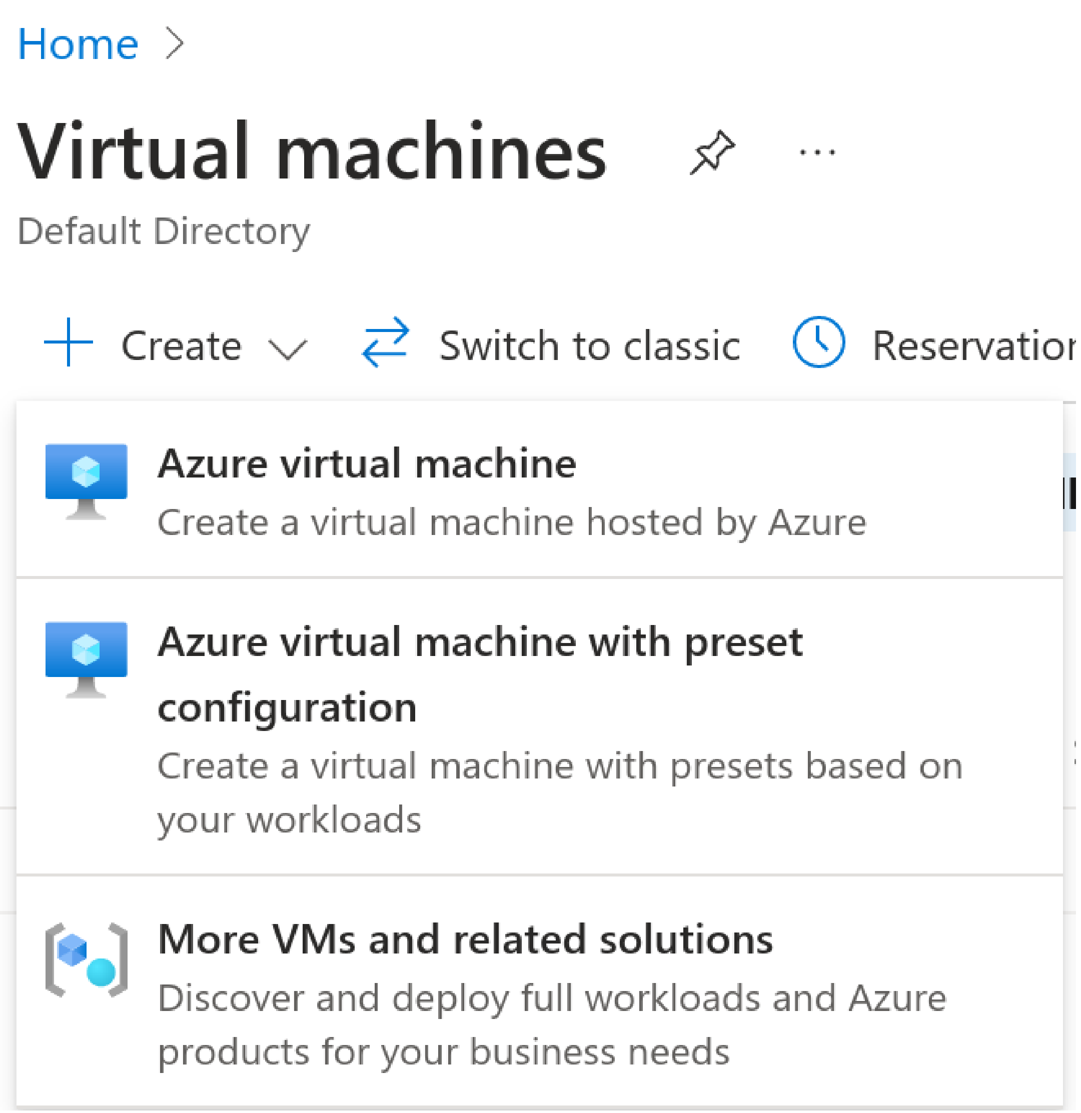
Upload the VHD-file to a **Storage account** under **Data storage - Containers**



Authentication method: Access key (Switch to Microsoft Entra user account)
Location: icc

Storage Account Upload Container

Go to Virtual machines and click on **Create** and select **Azure virtual machine**



Home >

Virtual machines

Default Directory

+ Create ∨ ⇄ Switch to classic Reservatior

Azure virtual machine

Create a virtual machine hosted by Azure

Azure virtual machine with preset configuration

Create a virtual machine with presets based on your workloads

More VMs and related solutions

Discover and deploy full workloads and Azure products for your business needs

Virtual machines Create New

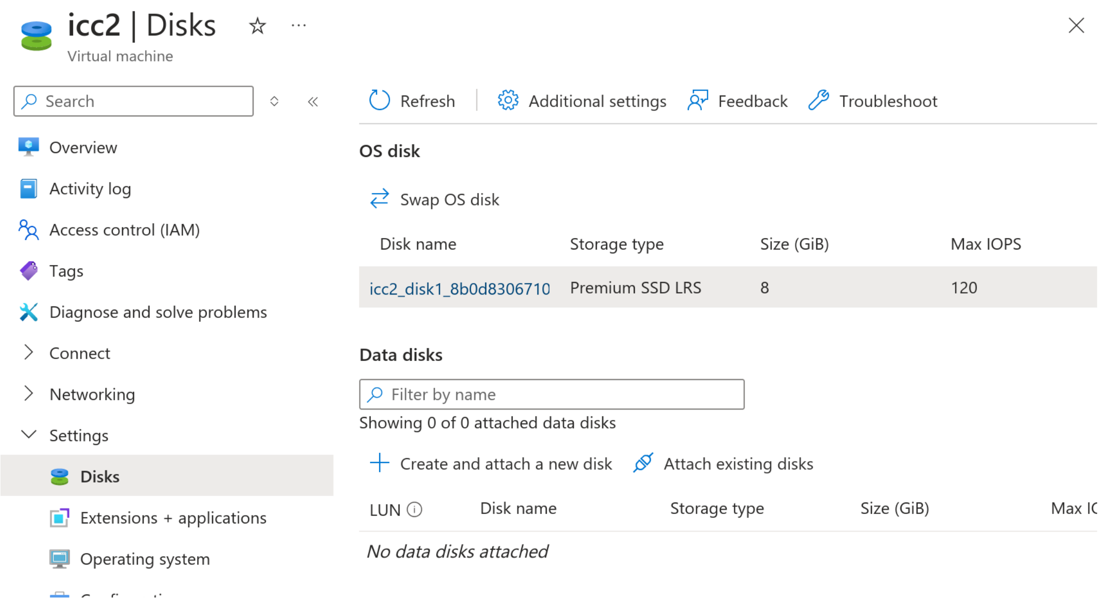
The following configuration works with the image

- Subscription: Your subscription
- Subscription - Resource group: The resource for the image
- Virtual machine name: ICC or similar
- Image: The container image that was uploaded
- VM architecture: x64
- Size: 2vcpu 16GiB memory
- Authentication type: SSH public key or Password
- Public inbound ports: Depends on the installation architecture

- OS type: Linux
- VM generation: Gen 2
- Storage blob: the uploaded VHD-file
- Host caching: Read/write
- License type: Other

1.3.3 Expand the disk

Go to the Virtual machine and select **Settings -> Disks** and the click on the **Disk name**



OS disk

Disk name	Storage type	Size (GiB)	Max IOPS
icc2_disk1_8b0d8306710	Premium SSD LRS	8	120

Data disks

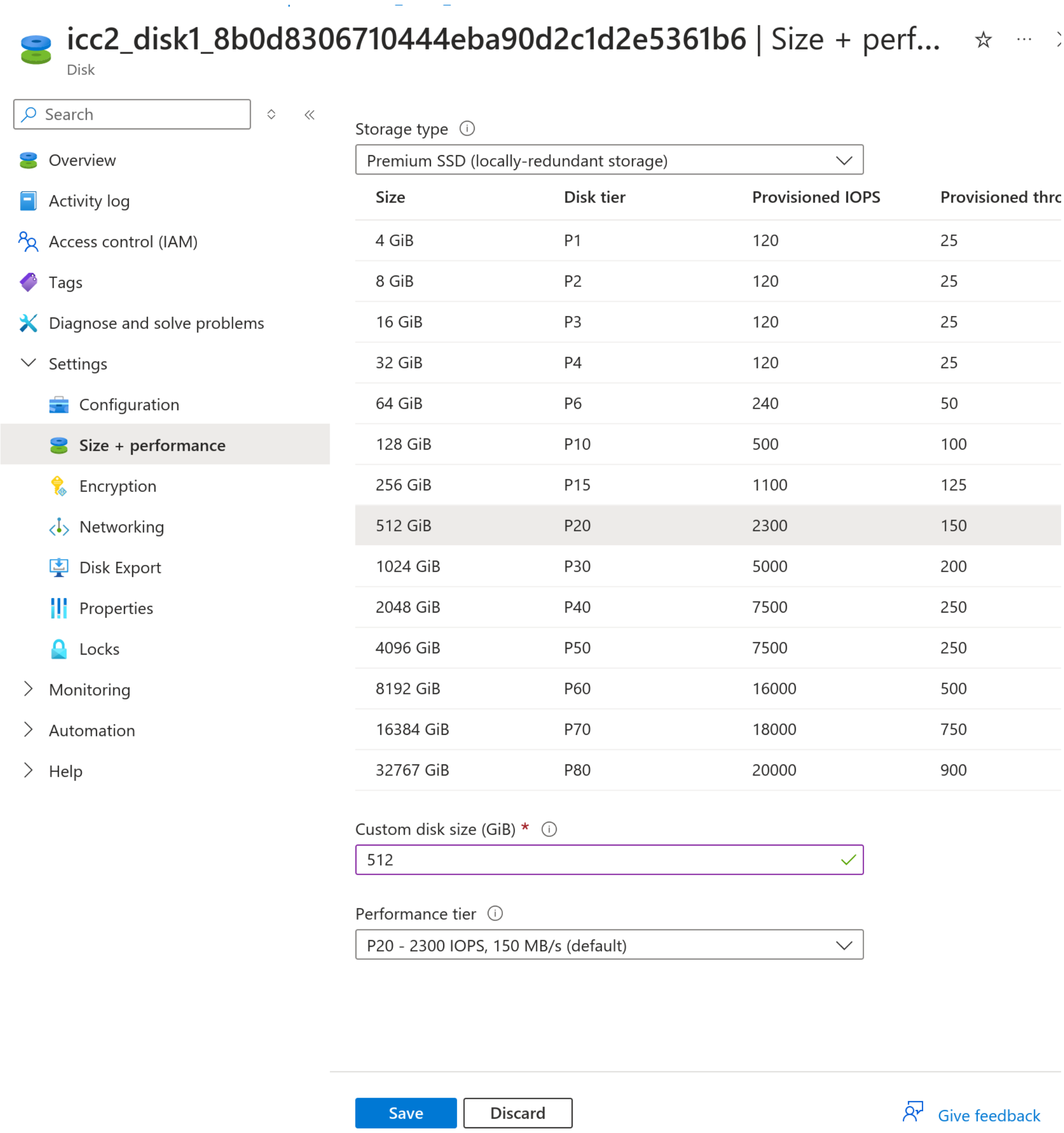
Showing 0 of 0 attached data disks

LUN ⓘ	Disk name	Storage type	Size (GiB)	Max IC

No data disks attached

Virtual machines Select Disk

Select **Settings -> Size + performance** and select a larger disk and save



icc2_disk1_8b0d8306710444eba90d2c1d2e5361b6 | Size + perf...

Disk

Storage type: Premium SSD (locally-redundant storage)

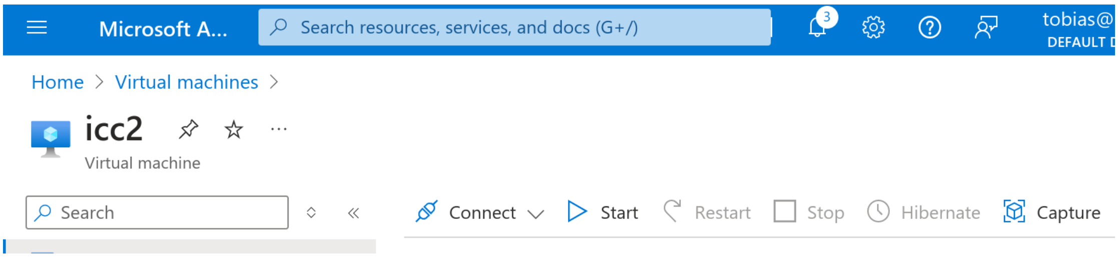
Size	Disk tier	Provisioned IOPS	Provisioned thrc
4 GiB	P1	120	25
8 GiB	P2	120	25
16 GiB	P3	120	25
32 GiB	P4	120	25
64 GiB	P6	240	50
128 GiB	P10	500	100
256 GiB	P15	1100	125
512 GiB	P20	2300	150
1024 GiB	P30	5000	200
2048 GiB	P40	7500	250
4096 GiB	P50	7500	250
8192 GiB	P60	16000	500
16384 GiB	P70	18000	750
32767 GiB	P80	20000	900

Custom disk size (GiB) *: 512

Performance tier: P20 - 2300 IOPS, 150 MB/s (default)

Virtual machines Select Large Disk

Start the Virtual machine



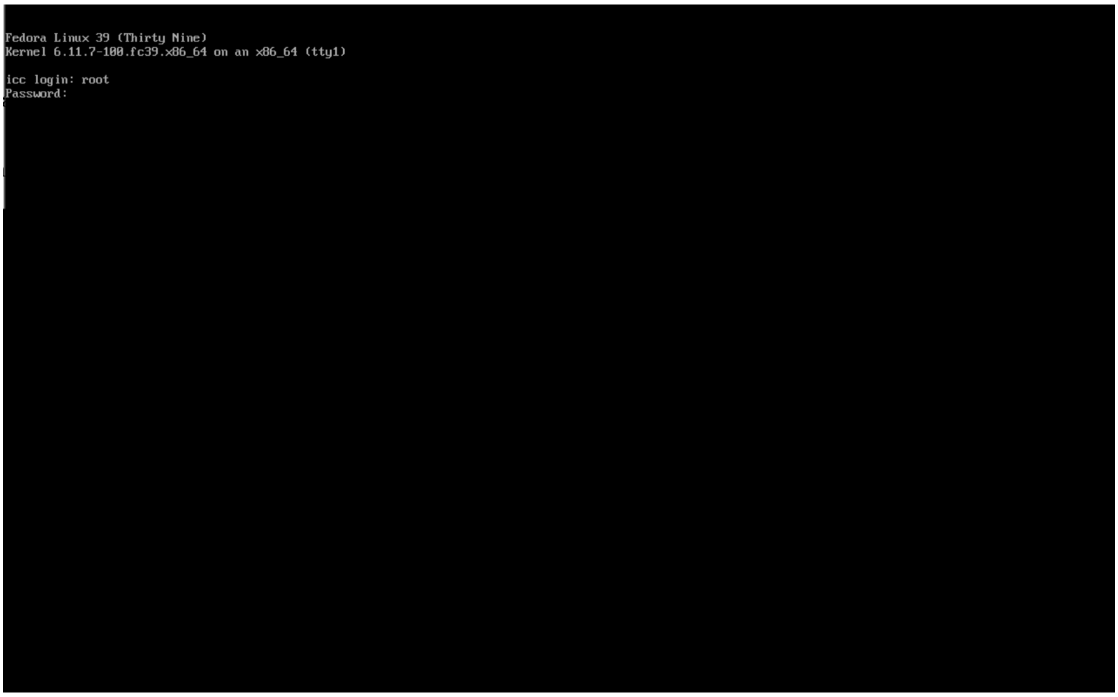
Virtual machines start

1.4 Initial configuration

These steps are only needed for the ICC, Repo and Datalock installations. One needs to configure IP addresses to allow SSH connection for the configuration of the Impex solution.

Login to the console with the root user is enabled and the root password is configured during the installation.

Once logged in, the follows steps need to be done: * Configure IP address * Expand the disk * Set the hostname * Install a certificate



```
Fedora Linux 39 (Thirty Nine)
Kernel 6.11.7-100.fc39.x86_64 on an x86_64 (tty1)

icc login: root
Password:
```

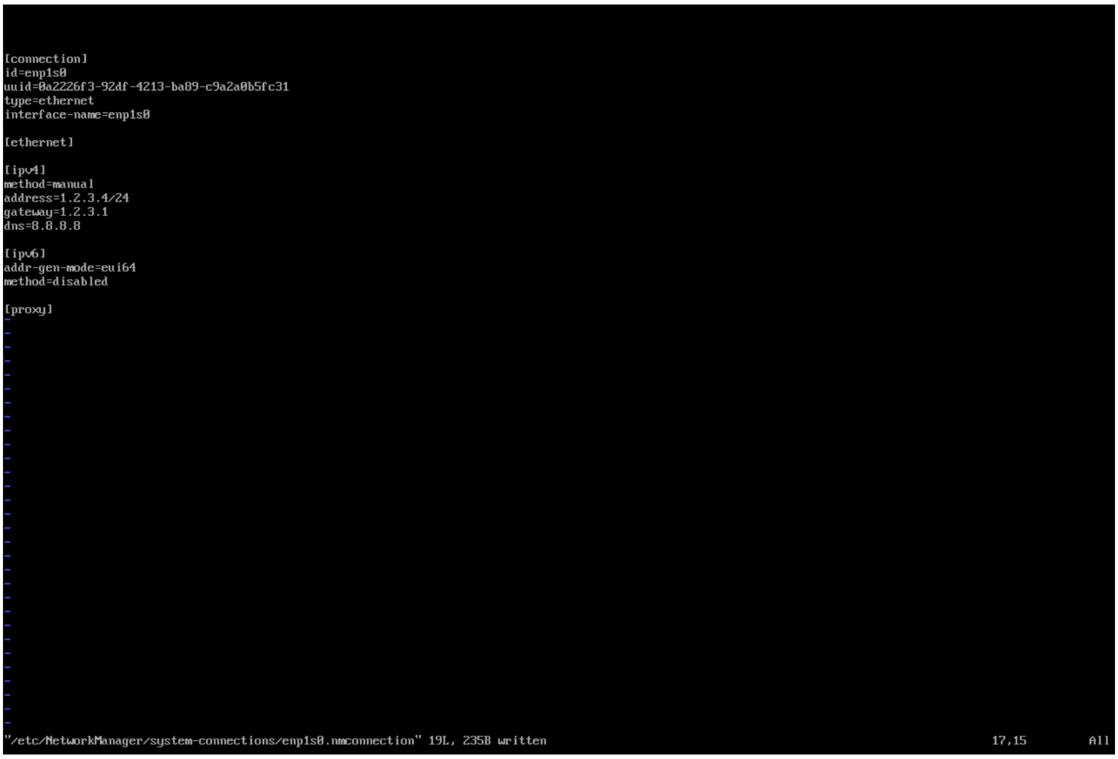
Console logins

1.4.1 Configure IP address

Configure the IP address in the file “*/etc/NetworkManager/system-connections/enp1s0.nmconnection*” with the VI text editor. The interface name “enp1s0” can be another name depending on the hardware.

Edit the ipv4 and ipv6 sections:

```
[ipv4]

method=manual

address=1.2.3.4/24

gateway=1.2.3.1

dns=8.8.8.8;8.8.4.4;

[ipv6]

method=disabled
```



```
[connection]
id=enp1s0
uuid=0a2226f3-92df-4213-ba89-c9a2a0b5fc31
type=ethernet
interface-name=enp1s0

[ethernet]

[ipv4]
method=manual
address=1.2.3.4/24
gateway=1.2.3.1
dns=8.8.8.8

[ipv6]
addr-gen-mode=eui64
method=disabled

[proxy]

"/etc/NetworkManager/system-connections/enp1s0.nmconnection" 19L, 235B written          17,15         All
```

IP configuration

After the configuration the network service needs to be restarted with the following command.

```
systemctl restart NetworkManager
```

Verify that the server is reachable with SSH.

1.4.2 Expand the disk

The default partition may be changed depending on the installation

To see the current partition table use the command *df -h*

Depending on the usage, expand the root partition and the var partition. The following example will expand the partitions with 100Gb

```
/usr/sbin/lvextend -r -L+100G /dev/mapper/root_vg-lv_root
```

```
/usr/sbin/lvextend -r -L+100G /dev/mapper/root_vg-lv_var
```

1.4.3 Set the hostname

The server needs to have a fully qualified domain name (FQDN) configured. The FQDN should reflect the subject alt name (SAN) in the certificate for the ICC and Repo server installation.

To configure hostname use the following command

```
/usr/bin/hostnamectl set-hostname servername.domain.tld
```

When the hostname has been configured, the ICC service *impex-icc* must be restarted by executing the following command

```
systemctl restart impex-icc
```

1.4.4 Install a Certificate

A trusted certificate is only needed for the ICC and Repo server. To create a certificate signing request, run the script

```
/opt/sysctl/impex-server/tools/cert.sh
```

In the examples below EPOCH and FQDN are variables that will differ in your setup. EPOCH is the number of unix seconds since 1970 and FQDN should be replaced with the full hostname and domain of your server. For example icc.internal.example.com.

The script will create a private key and a certificate signing request (CSR) file located in /root/pki/EPOCH/fqdn.{key,crt}

Copy the CSR and let the issuing CA sign the request.

Copy the /root/pki/EPOCH/FQDN.key to /opt/sysctl/impex-server/etc/apache/certs/FQDN.key

Add the signed certificate to /opt/sysctl/impex-server/etc/apache/certs/FQDN.crt. This file must also include intermediate CA certificates, sorted from leaf to root. This starts with the leaf and then the issuing CA certificate of the server certificate and must range up to the root CA certificate. The file must include the concatenation of the various PEM-encoded CA Certificate files, in certificate chain order.

The file must have the certificates in the following order:

1. Leaf certificate (server certificate).
2. Issuing certificates
3. Root certificate

Ensure the /opt/sysctl/impex-server/etc/apache/conf.d/cert.d/cert.conf match the correct path to the certificates and private key.

```
SSLCertificateFile /opt/sysctl/impex-server/etc/apache/certs/FQDN.crt
SSLCertificateKeyFile /opt/sysctl/impex-server/etc/apache/certs/FQDN.key
```

Once the new certificate is installed, restart the web service with the following command

```
systemctl restart impex-server
```

1.4.5 Add Certificate Trust in ICC

The ICC server needs to trust the certificate authority used in the Repo server. To trust the certificate copy the root CA certificate to

```
/etc/pki/ca-trust/source/anchors/repo_ca.crt
```

then update the trust store with the command

```
update-ca-trust
```

Verify with curl that the Repo server is trusted by executing the command *curl https://servername.domain.tld*

1.4.6 Configure the appliance

All other configurations must be done from the graphical web interface (https://fqdn). To login to the interface use the default user name *admin* and the pregenerated passsword which is saved in the file */root/icc_admin*. Once loged in, the password can be changed and configuration can be made according to the ICC manual.

1.5 Connect a Datalock to the ICC

The DataLock server must be connected to a ICC server. By editing the file

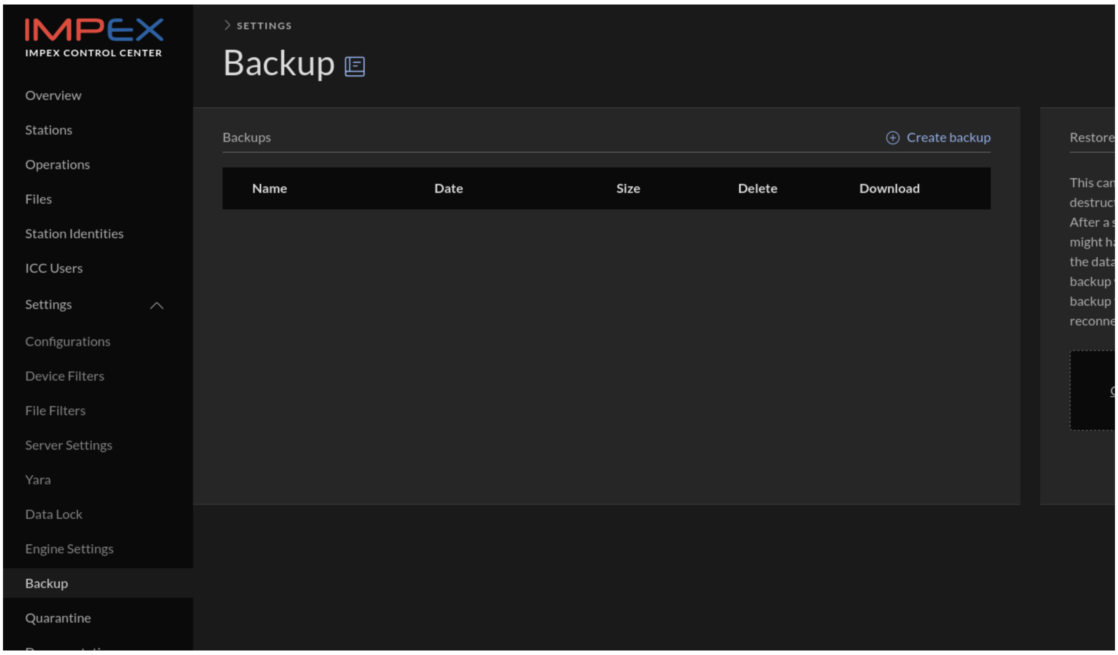
```
/etc/dnf/dnf.conf
```

and adding the setting *icc_server=https://hostname.domain.tld*, according to the Subhect Alt Name in the certificate. The DataLock will connect to the ICC with TOFU (Trust On First Use) and store the root-certificate in the trust store. The DataLock will only do TOFU during the first initial connection to the ICC.

2 ICC backup and restore

2.1 Creating a backup

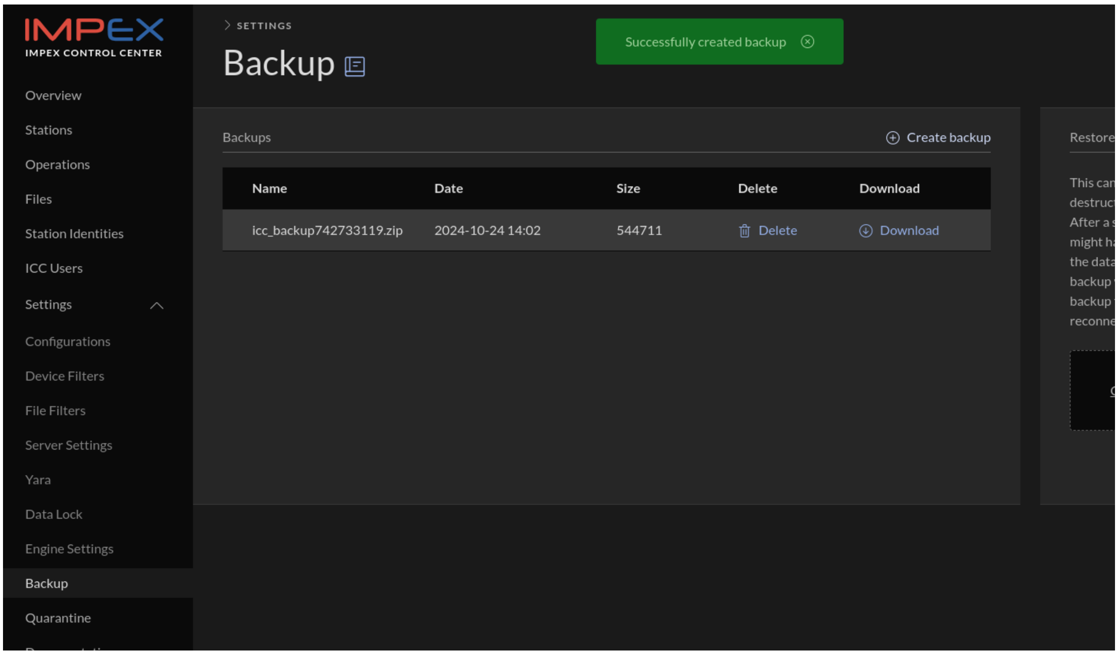
Select the “Backup” view on the left pane in the ICC.



Name	Date	Size	Delete	Download

Backup view

Click “Create backup” and then after a while, depending on how much data needs to be archived, the following view should appear.



Successfully created backup

Backups

Name	Date	Size	Delete	Download
icc_backup742733119.zip	2024-10-24 14:02	544711	Delete	Download

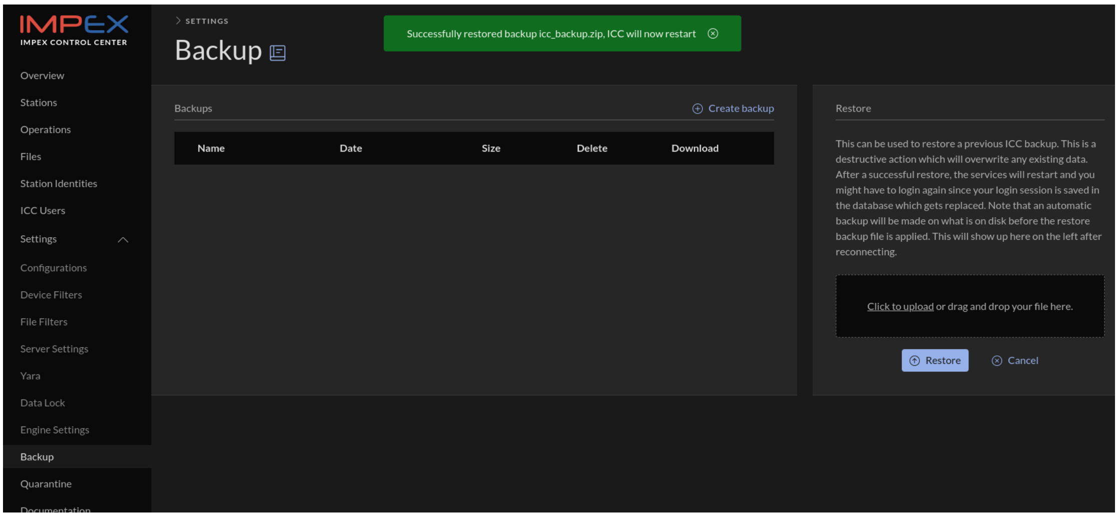
Successful backup

Download the file, which will be called `icc_backup.zip` on disk when downloaded. This file contains ICC secrets so make sure that no one not authorized can access it.

2.2 Restoring a backup

Go to the “Backup” view, select the previously downloaded file in the “Restore” card and click “Restore”.

The file will then be uploaded and unpacked and verified by the ICC. If all is ok it will then continue to restart the ICC services. Since the database was replaced your login session will be cleared and you will need to login again with the password the account had during the time of the backup.



Successfully restored backup icc_backup.zip, ICC will now restart

This can be used to restore a previous ICC backup. This is a destructive action which will overwrite any existing data. After a successful restore, the services will restart and you might have to login again since your login session is saved in the database which gets replaced. Note that an automatic backup will be made on what is on disk before the restore backup file is applied. This will show up here on the left after reconnecting.

Successful restore

2.3 Migrating ICC to new server

A new machine needs to be installed from the ICC ISO and then a backup from the old ICC can be restored on the new ICC installation.

The steps are:

1. Create a backup on the old ICC server
2. Download the backup from the old ICC server. The archive contains secrets and must be well protected.
3. Shutdown the old ICC
4. Install the new ICC server, according to the installation guide.
5. Update the IP configuration and hostname on the new ICC so it is identical to the old ICC
6. Reboot the new ICC
7. Login to the admin GUI on the new ICC server and go to backup view
8. Select the previously backed up file in the Restore card and click “Restore”
9. Verify that all the stations are still connected by checking the “Last seen” field on the station card. If not, contact SYSCTL support

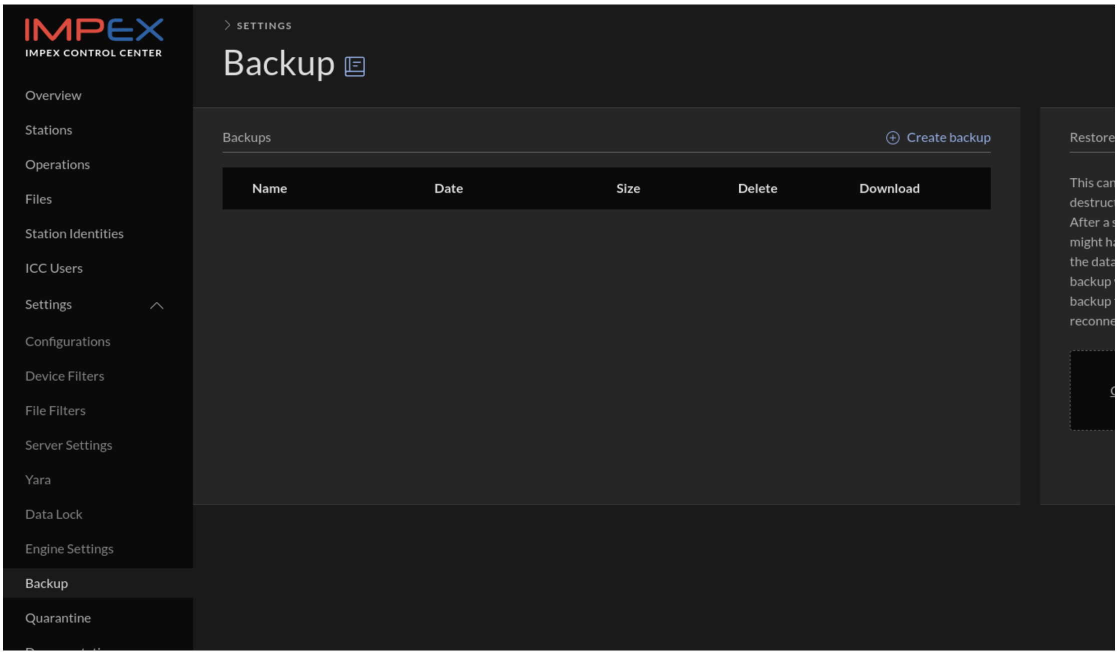
The backup includes the database, ICC signify keys, logs, quarantined files, ssh keys, yara rules and TLS certificates.

If the migration is from a 4.x.x installation to a 5.x.x installation the repository configuration must be reconfigured, ensure to get the old username and password and potential proxy configuration stored in /etc/yum.conf

Note: The ICC server uses HSTS, this will deny users from accessing the web application on the newly installed ICC server until it has a trusted certificate. The trusted certificate will be restored from the backup which requires access to the web application. To circumvent this issue it is possible to use the browser’s privacy mode (called incognito, inPrivate or private mode depending on the browser of your choice).

2.4 Doing a backup and downloading it

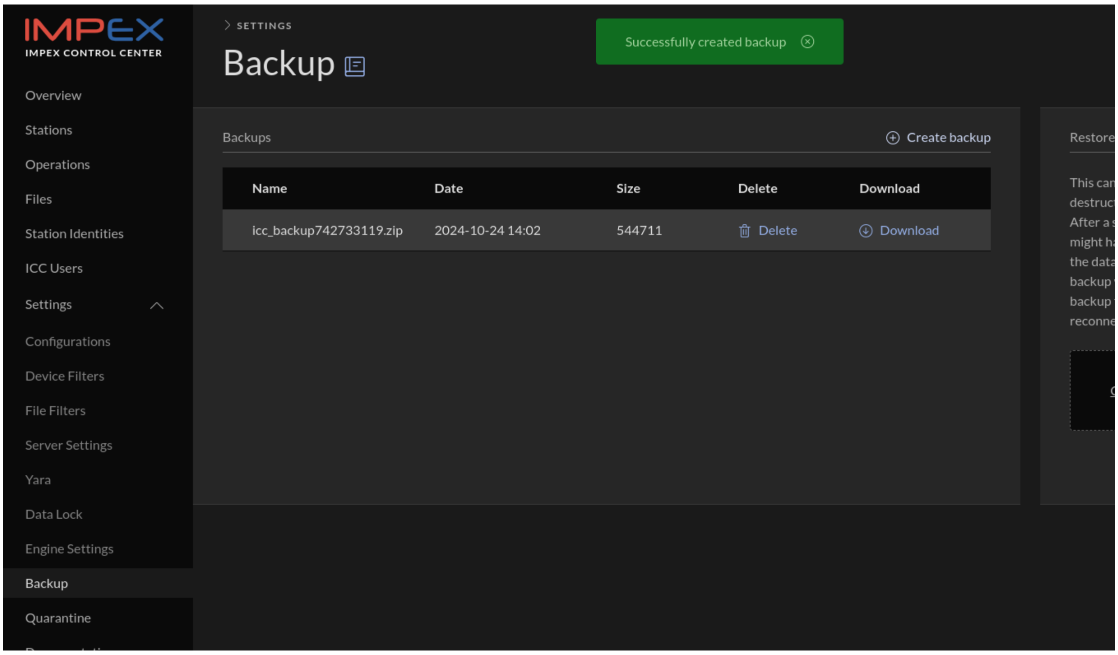
Select the “Backup” view on the left pane in the ICC.



Name	Date	Size	Delete	Download

Backup view

Click “Create backup” and then after a while, depending on how much data needs to be archived, the following view should appear.



Successfully created backup

Name	Date	Size	Delete	Download
icc_backup742733119.zip	2024-10-24 14:02	544711	Delete	Download

Successful backup

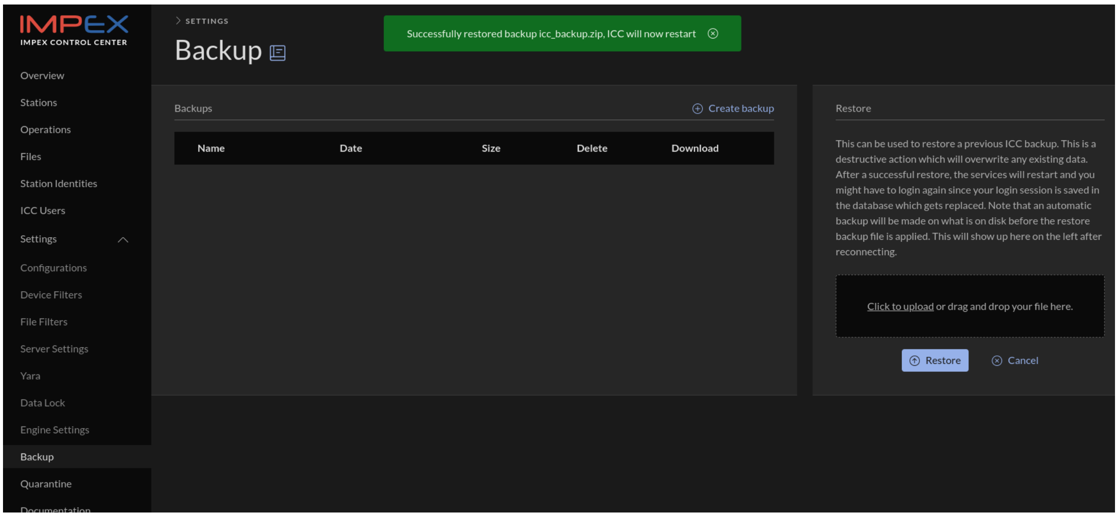
Download the file, which will be called `icc_backup.zip` on disk when downloaded. This file contains ICC secrets so make sure that no one not authorized can access it.

2.5 Install a new ICC and restore the backup archive on it

Download the ICC iso from https://portal.sysctl.se, boot on it and install a new ICC. Ensure that the disk is large enough.

After the ICC is installed, go to the “Backup” view, select the downloaded file in the “Restore” card and click “Restore”.

The file will then be uploaded and unpacked and verified by the ICC. If all is ok it will then continue to restart the ICC services. Since the database was replaced your login session will be cleared and you will need to login again.



Successfully restored backup icc_backup.zip, ICC will now restart

Name	Date	Size	Delete	Download

This can be used to restore a previous ICC backup. This is a destructive action which will overwrite any existing data. After a successful restore, the services will restart and you might have to login again since your login session is saved in the database which gets replaced. Note that an automatic backup will be made on what is on disk before the restore backup file is applied. This will show up here on the left after reconnecting.

Click to upload or drag and drop your file here.

Successful restore

To verify all went well you can for example check that the Station cards have appeared in the Stations view.

2.6 Do the swap

If any error messages showed up in the backup or restore logs on the Backup view, contact SYSCTL support, do not proceed with the swap until you have cleared it with SYSCTL support.

Now that the data from the old ICC has been migrated to the new it is time to shut down the old ICC. After it has been shut down, change the IP address and hostname on the new ICC to finish the takeover. Reboot the new ICC and verify that the stations are able to communicate with the new ICC by checking the “Last seen” field on the station cards.

2.7 Troubleshooting

If you see “To access ICC you need to use a hostname, FQDN or ip configured in ALLOWED_HOSTS” message in your web browser when surfing to the new ICC you have not configured the IP or/and the hostname correctly. Doublecheck hosts files, IP configuration and hostname. To set a new hostname:

```
# hostnamectl set-hostname somename.example.org
# systemctl restart impex-icc
```