I

BDHP Software Installation Guide 4.4

Single Node

Release Status:Issued and Effective

Contents

BDHP Software Installation Guide 4.4 1

Single Node 1

Purpose 4

Prerequisites 4

Installation Checklist 5

Digital Signature 7

Hypervisor setup 7

Hypervisor support 7
Hypervisor setup of Virtual Machines 8

LVA Setup (Baxter Engineer Begins Here) 11

Change the IP Address to a Statically Assigned Value ..... **Error! Bookmark not defined.**
Change the Hostname 17
Offline installation: Mount image 17
NTP Synchronization 18

Install Microk8s and basic Kubernetes infrastructure 20

Set up storage for microk8s 20
Install Etcd 20
Install Microk8s 21
Installing Load balancer - MetalLB 21
Install OpenEBS 22
Install Ingress 22
Install Loki 23

Database Backups 23

Postgres Full Recovery Mode (WAL) 23

MinIO 23

Database setup 23

Database Storage Setup 24
Node labelling 24
Install the Database(s) 24
Postgres 24
MySQL 25
Mongo 26
Neo4j 26

Antivirus protection 26

Installing BDHP platform 27

Check Databases 27
Install the Platform 29
Add additional features to Platform 32

Certificates 33

List Installed Applications 33

Release Status:Issued and Effective

Log on to the BDHP UI **34**

BDHP Instance Connection Guide **36**

Summary **36**

Appendix **37**

A. Checking LVA digital signature 37
B. Setting UEFI Secure boot on a hypervisor 38
C. Offline installation 41
D. LVA Interactive setup 45
E. Hypervisor installation of a Linux Virtual Application image 55
E. License information for MySQL 69
F. BDHP installation variables 69
G. Example YAML files 81
H. Certificates in BDHP 84
I. Additional Virtual IP for VerneMQ 91
J. Configuration of SecureLink for remote access 93
K. Installing, upgrading and configuring guest applications 103
L. Using the Keycloak admin console 105
Appendix M ..... **Error! Bookmark not defined.**

Reference **107**

A- Configuring troubleshooting user 107
B- Language & Manuals Library - importing assets 111

Validation **114**

1 Procedure 114
1.1.1 JAMA Test Cases for Qualification 114
1.1.2 Qualification acceptance criteria 114

Release Status:Issued and Effective

Purpose

This document is a guide to the installation of version **>=4.4.x** of the BDHP (Baxter Digital Health Platform).

For this version of the platform, the virtual machine (node) should be built using version **>=7.107.x** of the LVA image.

The image will need to be provided to the customer.

BDHP can be installed in both High Availability (HA) and non-HA configurations. **Only non-HA – single node** – installation is described in this document.

The installation is expected to be run by two separate users:

1. **Customer**- This person is expected to provide the virtual machine(s) environment, using the hypervisor of their choice.
2. **Baxter engineer**- This person is responsible for installing BDHP into the provided environment.

The BDHP platform can be installed in either online or offline.

Offline installations does not require the customer to have internet access. Extra steps are required for offline installation.

Prerequisites

The users involved must understand the linux operating system and must be familiar with the Kubernetes container orchestration software and the databases that can be installed.

A **linux virtual appliance (LVA)** is a packaged pre-configured, virtualization-ready solution in a single software package that is secure, easy to distribute, and easy to manage.

To begin an installation, the customer must have been provided with:

- the latest version of the BDHP LVA (Linux Virtual Appliance)
- a Baxter public key (ppk file) to allow for user access to the LVA.
- an LVA signature file, which can be used to check integrity of the LVA.
- the Pre-Installation Workbook (*BXU587774*). The customer must complete this workbook.
    - This is needed by the installer of the BDHP platform.

Release Status:Issued and Effective

Installation Checklist

Below are the steps in a BDHP installation:

Installation name: _____	Date Click or tap to enter a date.	Installer name: _____

☐	1. VM created within Hypervisor
☐	2. Node accessible remotely by SSH, console, etc
☐	3. IP address changed to static value
☐	4. Hostname changed to
☐	5. Node date is correct and chronyd is running *Take snapshot called '**IP, Hostname and time provisioned**'*
☐	6. Microk8s storage setup
☐	7. Etcd installed
☐	8. Microk8s installed and all pods running *Take snapshot called '**Etcd and Microk8s installed**'*
☐	9. Metallb installed
☐	10. OpenEbs installed
☐	11. Ingress installed
☐	12. Loki installed
☐	13. Database backup store setup and external storage configured, if required
☐	14. Storage for all databases setup. List databases:
☐	15. MinIO installed (if required) and Node labelling is correct for database installation
☐	16. Databases installed and all pods running and complete *Take snapshot called '**DBs installed**'*
☐	17. Installation variables set
☐	18. Platform deployed and running correctly. Version installed:

Release Status:Issued and Effective

	*Take snapshot called '**Platform installed**'*
☐	19. Ingress and device certificates setup. Verne pods re-started.
☐	20. BDHP Login screen accessible (without warnings)
☐	21. Required guest apps installed and their version: *Take snapshot called '**Fully Deployed**'*

Release Status:Issued and Effective

Digital Signature

Digital signatures allow the recipient to verify both authenticity and integrity of the received LVA

These files are digitally signed with a Baxter managed private key. The package (lva, key and signature file) can be checked for integrity. See *Appendix A* for more information.

Hypervisor setup

A hypervisor, also known as a virtual machine monitor, is software that runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.

The BDHP Linux Virtual Appliance is designed to be installed onto a supported Hypervisor.

Hypervisor support

The following Hypervisors are supported:

- VMWare ESX 7 or greater
- Microsoft Hyper V on Windows Server 2016 or greater
- Redhat Enterprise Virtualization (RHEV) version 4.4 or greater
- Nutanix V6.5 or greater

The BDHP Linux Virtual Application is distributed in three formats (VHD, QCOW2 and OVA) which are targeted at different hypervisors as detailed below. It is expected that the customer is experienced in installation of their chosen hypervisor

Hypervisor	Distribution Format
VMWare ESX	OVA
Microsoft Hyper-V	VHDX
Redhat Enterprise Virtualization	QCOW2
Nutanix	QCOW2

Server Requirements Specification

The infrastructure requirements for the BDHP platform will vary according to the size of the deployment and the levels of availability required. Additional compatible Baxter products installed on the platform may require further infrastructure requirements.

Release Status:Issued and Effective

Release Status:Issued and Effective

NOTE: Consult with Baxter Global Technical Services to finalize the infrastructure requirements before installation.

Server	Minimum Requirements
Standard - Single Node	• 8 Core CPU • 32 GB Memory • 3 TB Hard drive • Up to 5 Disk drives • 1 Gbps Network

Hypervisor setup of Virtual Machines

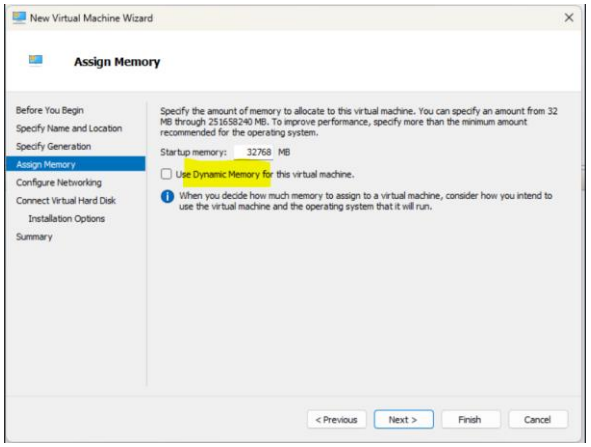
The customer must create the virtual machine, or node using the LVA file supplied.

UEFI secure boot is required to make the solution secure. See Appendix *B* for how to set this for different hypervisors.

See *Appendix D* for a guide to creation of the VM using the VMWare hypervisor.

IMPORTANT: For each platform node - on all hypervisors - The system should be set to reserve/lock or turn off 'dynamic memory' to the size that it's been allocated.

Below, as an example, is the relevant box to leave unticked for the Hyper-v hypervisor.



WARNING: It is recommended to import an LVA each time and provision drives and networking manually when creating cluster nodes versus **cloning** virtual machines.

If cloning is the method, make sure that the original virtual machine has not been turned on and did not complete the initial power up/boot up sequence. Drive provisioning should be completed, and network provisioning should be set for unique MAC generation.

Cloning can produce unwanted artefacts in multi-nodal/HA deployments.

Make sure that unique machine-id values are set by checking */etc/machine-id*

Drive setup

- The node requires a hard drive into which Microk8s can be installed.
- A hard drive is required for each database that is to be needed.
- A separate database backup hard drive is required.
- All drives should be a minimum size of 110Gb.

As an example, a single node solution requiring both PostgreSQL and Mongo databases should have 4 added drives:

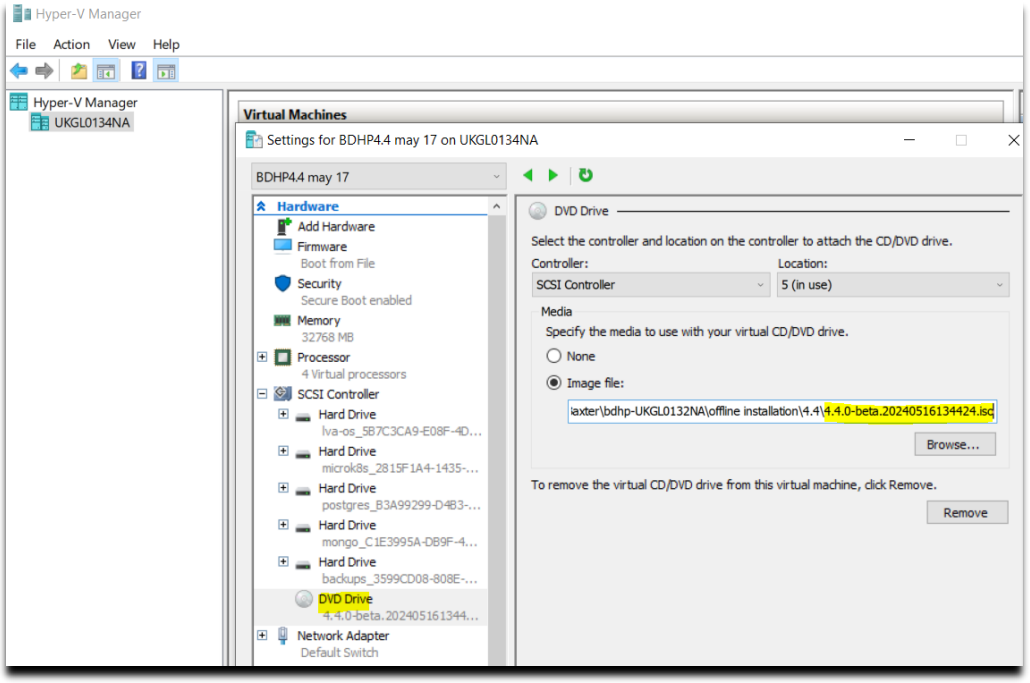
- The microk8s drive
- The PostgreSQL drive
- A Mongo drive
- The database backups drive

Offline installation: Upload iso image

An offline installation a package containing the helm charts and container images must be uploaded to the LVA. The first step is to upload an iso image to the SCSI Controller.

Below is an example using the Hyper-v hypervisor.

Release Status:Issued and Effective



The OS will automatically recognize this as a device with reference /dev/**sr0**

Summary of hypervisor setup

The environment should be complete, and the rest of the installation sits with the Baxter Engineer.

NOTE: Take a snapshot/checkpoint of the VM at this point.

Release Status:Issued and Effective

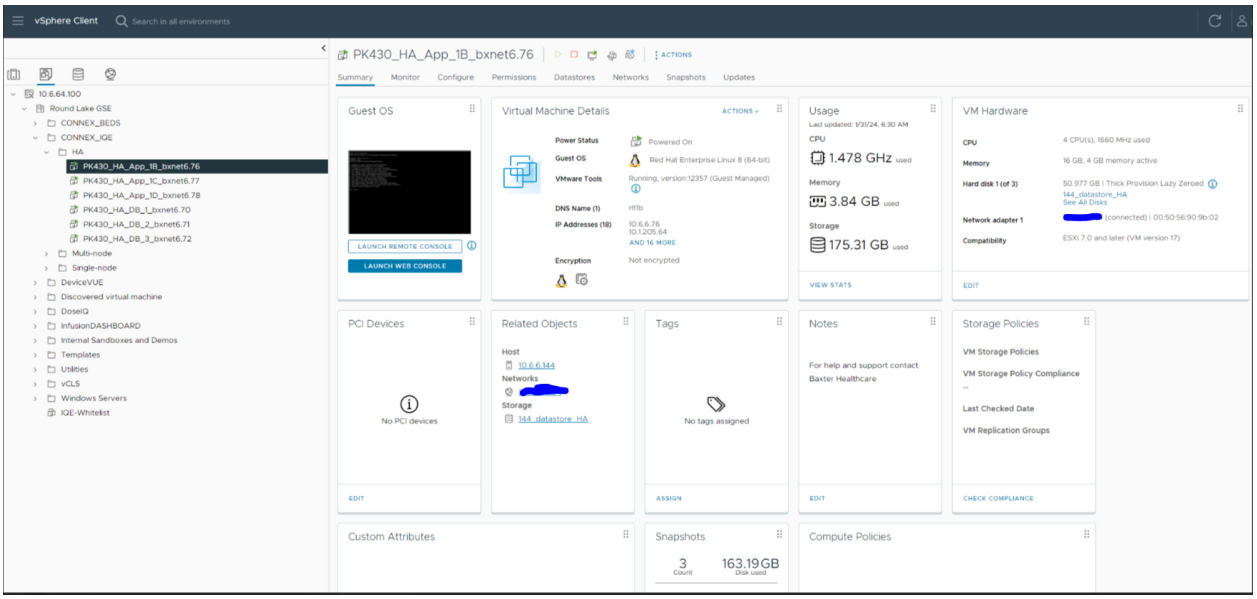
Release Status:Issued and Effective

Use of sudo

Often administrative users open a root console session (**sudo -i**) and run all commands as root.

However, we have adopted the principle that being root for prolonged period is a bad idea. Therefore, in the shell, you should aim to stay as the *baa* user and specifically prefix commands with **sudo** as and when you need elevated privileges.

Log on to the Virtual Appliance (in this case from the VMWARE hypervisor)



1. From the Virtual machine list, click the new VM.

   The VM's details appear underneath the list.

2. Click the console image next to the VM's details.

   A full-size console window opens.

```
Baxter Virtual Appliance
Authorized uses only. All activity may be monitored and reported.

IP Address eth0: 10.6.6.76
IP Address eth1:
Machine ID: 2681f921c45e44c79c4bbd3616c95832

cs: Požádejte o pomoc společnost Baxter Healthcare
da: Kontakt Baxter Healthcare for at få hjælp
el: Για βοήθεια, επικοινωνήστε με την Baxter Healthcare
de: Für Unterstützung wenden Sie sich bitte an Baxter Healthcare
en: For support, please contact Baxter Healthcare
es: Para obtener ayuda, comuníquese con Baxter Healthcare
fi: Jos tarvitset apua, ota yhteyttä Baxter Healthcareen
fr: Pour obtenir de l'aide, veuillez contacter Baxter Healthcare
it: Per assistenza, contattare Baxter Healthcare
nb: For hjelp, vennligst kontakt Baxter Healthcare
nl: Neem voor hulp contact op met Baxter Healthcare
pl: Aby uzyskać pomoc, skontaktuj się z firmą Baxter Healthcare
pt: Para obter assistência, entre em contato com a Baxter Healthcare
sv: Kontakta Baxter Healthcare för hjälp

rlt1b login: _
```

Configuring network settings on a node

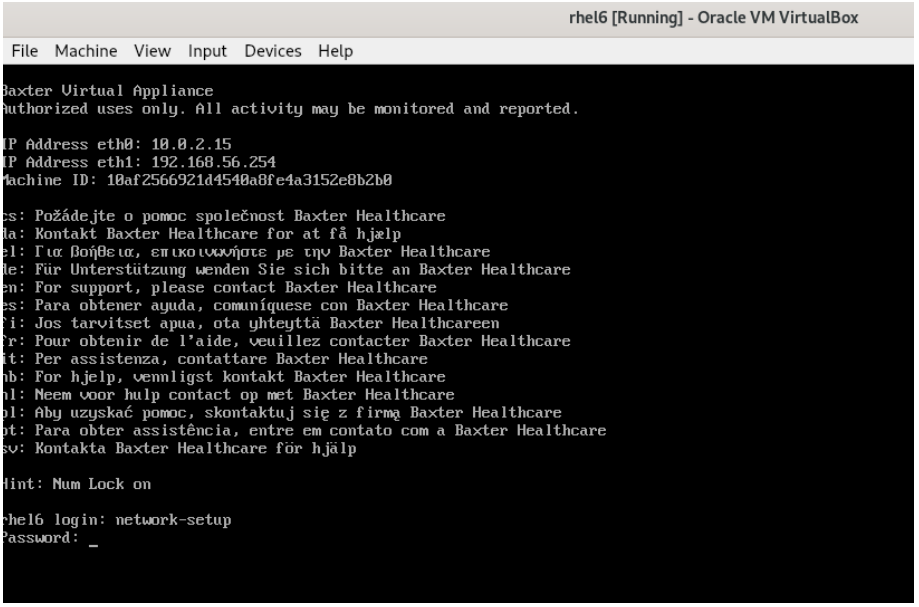
This functionality is intended for customer IT people. They have just downloaded our LVA and booted it up in a hypervisor. They have access to it via their hypervisor console.

By default, the LVA is set to configure its network using DHCP. This functionality is for customers who want to assign a static IP to each node as per their network requirements..

Logging in

The user must login using the designated account **network-setup**

Release Status:Issued and Effective



The password is **Network@123** - the user will be forced to choose a new password on first login. It must meet strong password standards - e.g. mixed case, combination of letters, numbers and symbols and not based on a dictionary word.

NOTE: US keyboard users may need to press *shift* and *apostrophe* to obtain an ampersand character needed for the above password.

Network setup program

Upon successful login, the network setup program is launched.

An entry will appear for each network interface attached to the machine.

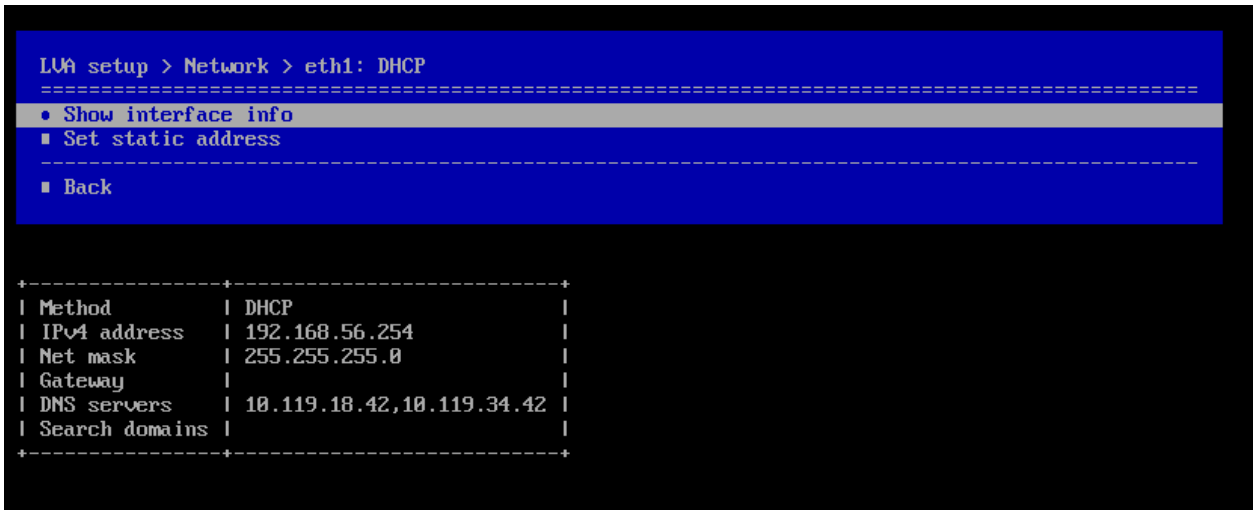
Choosing Exit will leave the program and log the user out of the console session.

Changing the network interface settings

For each interface there are 2 options:

Release Status:Issued and Effective

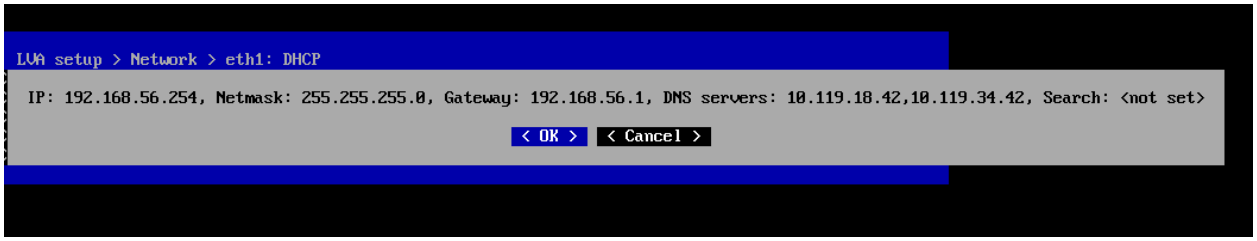
Show interface info will output a summary of the current configuration of the interface - e.g.



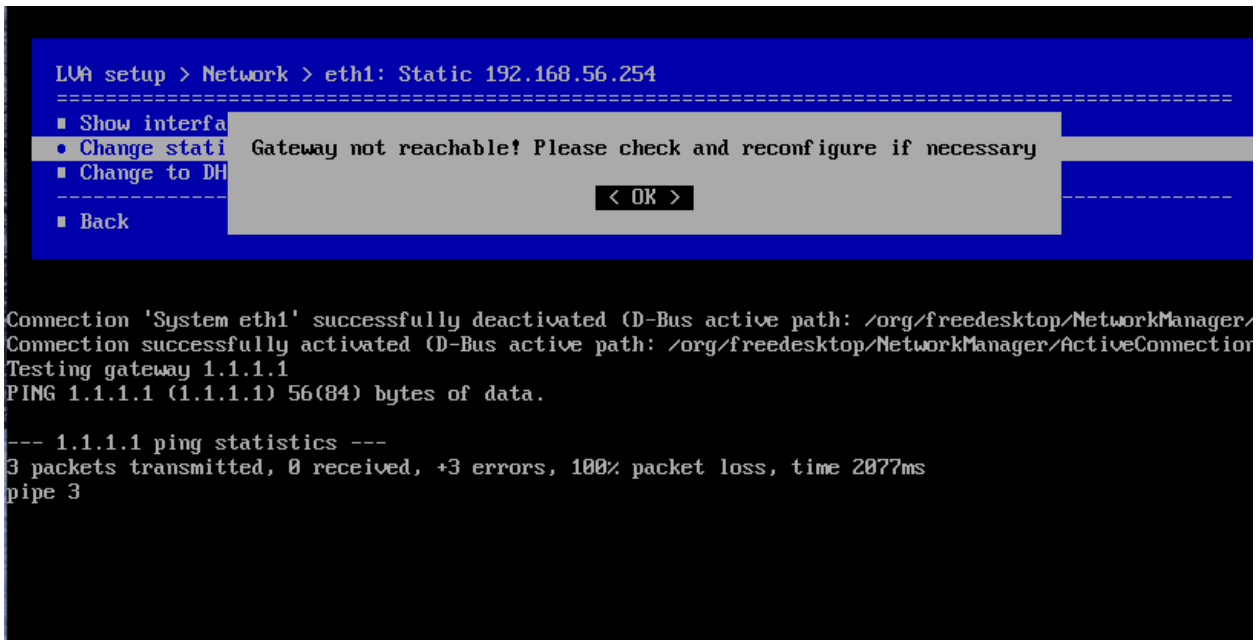
Set static address allows the user to set a static address for this interface. It will prompt for

- Static IP address
- Net mask
- Gateway IP address
- DNS servers
- Search domains (may be left blank)

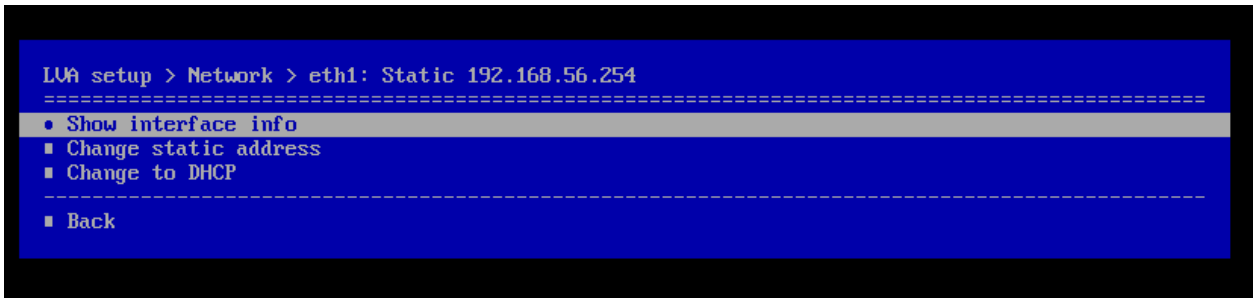
Once all information has been entered, a confirmation will appear allowing the user to proceed or cancel.



Once the static network details have been set, the program will attempt to ping the configured Gateway. If it cannot be reached, a warning will be shown.



The user may continue to change the settings (until they are correct) using the *Change static address* option.



Alternatively, Change to DHCP may be chosen to revert the settings back to DHCP.

Post setup

This user and program are designed to only be used during the initial set up of the LVA. The user account is automatically disabled during the subsequent installation of the container orchestration software by Baxter. Should it be required again - for example if the internal network settings are due to change - the customer

will need to contact Baxter support and arrange for the account to be re-enabled.

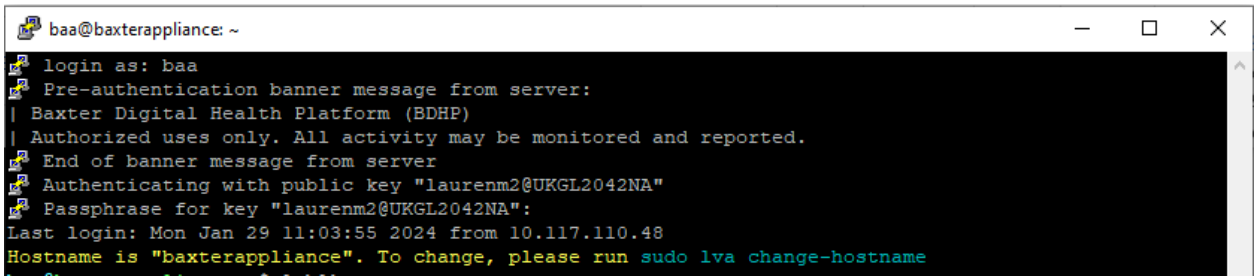
Enable SSH

To enable SSH on the network segment, run the following command to open port 22 on the firewall

sudo ufw allow openssh

Only do this if not using Securelink for access

Login via SSH



Now the firewall has been changed to accept OpenSSH connections.

Log on to the virtual appliance as **baa** (Baxter Appliance Administrator).

The previously provided baa public key will be required for authentication.

NOTE The password should have been provided.

Release Status:Issued and Effective

Release Status:Issued and Effective

Change the Hostname

Change the hostname to a suitable name (from the default of baxterappliance). Run the following command:

sudo lva change-hostname

It is not possible to rename the hostname after kubernetes installation.

NOTE: The changed hostname will only be viewable after a new ssh session is initiated.

NOTE: Per RFC-1123, hostnames must be 1-63 characters in length and consist of lower-case ASCII letters a-z, 0-9, and hyphens. Hostnames may not begin with a hyphen. Using the first part of the FQDN for the VM as hostname is recommended. For example, if the FQDN is iqe31.baxter.com**,** use **iqe31** as the hostname.

Offline installation: Mount image

NOTE: *For an online installation, skip this section*

Mount the ISO image at a single mount point - */opt/baxter/offline* –

Use the following command (check that sr0 is the correct reference):

sudo mount -o ro /dev/sr0 /opt/baxter/offline

Use **tree** to verify that the charts and images now exist in the offline directory.

```
baa@baxterappliance:~$ sudo mount -o ro /dev/sr0 /opt/baxter/offline
baa@baxterappliance:~$ tree /opt/baxter/offline
/opt/baxter/offline
├── charts
│   ├── bdhp-k8sdashboard-oauth2-proxy-1.16.0.tgz
│   ├── bdhp-minio-migration-1.4.1.tgz
│   ├── bdhp-minio-operator-1.1.0.tgz
│   ├── bdhp-minio-tenant-1.3.2.tgz
│   ├── bdhp-mongodb-cluster-1.10.1.tgz
│   ├── bdhp-mongodb-operators-1.1.2.tgz
│   ├── bdhp-mysql-cluster-1.5.1.tgz
│   ├── bdhp-mysql-operators-1.2.2.tgz
│   ├── bdhp-neo4j-cluster-1.4.6.tgz
│   ├── bdhp-openebs-4.4.2.tgz
│   ├── bdhp-postgres-cluster-1.10.1.tgz
│   ├── bdhp-postgres-operators-1.2.1.tgz
│   ├── bdhp-vernemq-bed-oauth2-proxy-1.5.0.tgz
│   ├── bdhp-vernemq-pump-oauth2-proxy-1.5.1.tgz
│   ├── loki-stack-2.14.8.tgz
│   └── mdap-4.4.0-beta.20240516134424.tgz
├── images
│   ├── bdhpcr.azurecr.io
│   │   └── images
│   │       ├── bdhp-account:4.12.3.tar
│   │       ├── bdhp-adt:4.48.0.tar
```

List the block devices to see that the sr0 reference is now mounted to */opt/baxter/offline*

```
baa@baxterappliance:~$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda             8:0    0   51G  0 disk
├─sda1          8:1    0   50M  0 part /boot/efi
├─sda2          8:2    0  974M  0 part /boot
└─sda3          8:3    0   50G  0 part
  ├─vg0-lv--0 253:0    0  9.8G  0 lvm  /
  ├─vg0-lv--6 253:1    0  1.5G  0 lvm  /tmp
  ├─vg0-lv--5 253:2    0  1.5G  0 lvm  /var/tmp
  ├─vg0-lv--4 253:3    0  4.9G  0 lvm  /var/log/audit
  ├─vg0-lv--3 253:4    0  3.9G  0 lvm  /var/log
  ├─vg0-lv--2 253:5    0 27.4G  0 lvm  /var
  └─vg0-lv--1 253:6    0  468M  0 lvm  /home
sdb             8:16   0  120G  0 disk
sdc             8:32   0  110G  0 disk
sdd             8:48   0  105G  0 disk
sde             8:64   0  100G  0 disk
sr0            11:0    1    9G  0 rom  /opt/baxter/offline
```

NTP Synchronization

The date and time of the LVA must be correct and kept in sync with a network time server.

Verify NTP source

BDHP will connect with the default NTP server pools at ntp.org.

Check BDHP is connecting run the following command:

chronyc sources

```
baa@lva-434-offline-may-16-24:/opt/baxter$ chronyc sources
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^- cheddar.halon.org.uk          2   8   377    43    -11ms[  -11ms] +/-   33ms
^- kvm-1.shar.coreservers.uk     2   8   377    48    -11ms[  -20ms] +/-   36ms
^- research.knoq.nl              2   8   377   307  +7546us[-1445us] +/-   27ms
^* 85.199.214.98                 1   8   377    48    -11ms[  -20ms] +/- 7010us
baa@lva-434-offline-may-16-24:/opt/baxter$ date
Thu 16 May 09:34:13 UTC 2024
```

The presence of sources indicates that BDHP is reaching the pre-configured sources and so will keep its clock synchronised.

Use the following command to check the correct datetime is returned by the VM:

date

If no sources are returned, the NTP server pools must be changed.

Change the NTP Server Pools

To change the server pools edit the **/etc/chrony.conf** file and change the set pool addresses as shown.

```
sudo vim /etc/chrony.conf

# Use the NTP servers on hospital network
pool 0.pool.hospital.com minpoll 8
pool 1.pool.hospital.com minpoll 8
```

Release Status:Issued and Effective

```
pool 2.pool.hospital.com minpoll 8
pool 3.pool.hospital.com minpoll 8
```

If this file is changed restart the chronyd service

sudo systemctl restart chronyd.service

Verify the Chronyd Server Is Running

To verify that the Chronyd server is running, run the following command:

systemctl status chronyd.service

The green text next to the **Active** heading confirms that the NTP server is running. Type **CTRL + C** to exit the status message.

```
baa@rhel1:~$ systemctl status chronyd.service
● chronyd.service - NTP client/server
   Loaded: loaded (/usr/lib/systemd/system/chronyd.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2024-01-26 09:18:04 UTC; 3h 45min ago
     Docs: man:chronyd(8)
           man:chrony.conf(5)
 Main PID: 881 (chronyd)
    Tasks: 1 (limit: 80588)
   Memory: 1.4M
   CGroup: /system.slice/chronyd.service
           └─881 /usr/sbin/chronyd -u chrony

Jan 26 09:18:04 baxterappliance chronyd[881]: chronyd version 4.2 starting (+CMDMON +NTP +REFCLOCK +RTC +PRIVDROP +SCFILTER +SIGND +ASYNCDNS +NTS +SECHASH +IPV6 +DEBUG)
Jan 26 09:18:04 baxterappliance chronyd[881]: commandkey directive is no longer supported
Jan 26 09:18:04 baxterappliance chronyd[881]: Could not open keyfile /etc/chrony/chrony.keys
Jan 26 09:18:04 baxterappliance chronyd[881]: Frequency 0.000 +/- 1000000.000 ppm read from /var/lib/chrony/chrony.drift
Jan 26 09:18:04 baxterappliance systemd[1]: Started NTP client/server.
Jan 26 09:26:44 rhel1 chronyd[881]: Selected source 99.119.214.210 (3.pool.ntp.org)
Jan 26 09:26:44 rhel1 chronyd[881]: System clock wrong by 0.997517 seconds
Jan 26 09:31:04 rhel1 chronyd[881]: Source 129.146.193.200 replaced with 108.61.73.243 (1.pool.ntp.org)
Jan 26 09:35:21 rhel1 chronyd[881]: Selected source 157.245.125.229 (2.pool.ntp.org)
Jan 26 09:52:39 rhel1 chronyd[881]: Selected source 99.119.214.210 (3.pool.ntp.org)
```

NOTE Do not proceed if chronyd.service is not running.

See Appendix M for further information on configuring BDHP-NTPD service.

Release Status:Issued and Effective

Install Microk8s and basic Kubernetes infrastructure

Verify the required drives have been provisioned, using the command lsblk.

The shot below shows that six drives – sdb, sdc, sdd, sde, sdf and sdg – are available.

```
baa@baxterappliance:~$ lsblk
NAME           MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda              8:0    0   51G  0 disk
├─sda1           8:1    0   50M  0 part /boot/efi
├─sda2           8:2    0  974M  0 part /boot
└─sda3           8:3    0   50G  0 part
  ├─vg0-lv--0 253:0    0  9.8G  0 lvm  /
  ├─vg0-lv--6 253:1    0  1.5G  0 lvm  /tmp
  ├─vg0-lv--5 253:2    0  1.5G  0 lvm  /var/tmp
  ├─vg0-lv--4 253:3    0  4.9G  0 lvm  /var/log/audit
  ├─vg0-lv--3 253:4    0  3.9G  0 lvm  /var/log
  ├─vg0-lv--2 253:5    0 27.4G  0 lvm  /var
  └─vg0-lv--1 253:6    0  468M  0 lvm  /home
sdb              8:16   0  120G  0 disk
sdc              8:32   0  120G  0 disk
sdd              8:48   0  120G  0 disk
sde              8:64   0  120G  0 disk
sdf              8:80   0  120G  0 disk
sdg              8:96   0  120G  0 disk
baa@baxterappliance:~$
```

Interactive guide

New in version 4.4. is the option to use an interactive guide for the following steps:

- Installing Microk8s
- Configuring Database Backup Storage
- Installing Databases

For the interactive guide, see Appendix D - LVA Interactive setup. Otherwise, follow the the non-interactive steps below.

Set up storage for microk8s

A single command will automatically partition and mount a newly attached storage volume for use for microk8s.

In the example below it is assumed that the dedicated storage volume is present as */dev/sdb*. If this is not the case, adjust the parameter as required.

sudo lva setup-m8s-storage /dev/sdb

Install Etcd

etcd (pronounced et-see-dee) is a distributed, consistent key-value store for shared configuration, service discovery, and scheduler coordination of distributed systems or clusters of machines. etcd is the backend database for kubernetes itself.

Release Status:Issued and Effective

On a single node installation, install etcd on localhost using the following command.

sudo lva install-etcd

Install Microk8s

The Linux Virtual Appliance uses the Microk8s version of Kubernetes. Microk8s is a small lightweight, and fully conformant Kubernetes distribution from Canonical. It's a minimalistic distribution focused on simplicity and performance. Given its footprint, Microk8s can be easily deployed in IoT and edge devices.

The terms Kubernetes, K8S and Microk8s are used interchangeably.

Install microk8s using the following command:

sudo lva install-microk8s

or, for an *offline installation*, pass the offline flag:

sudo lva install-microk8s ofoffline

The offline flag will indicate to the installer to import all container images from the mount iso:

```
baa@baxterappliance:~$ sudo lva install-microk8s --offline
/var/snap/microk8s
** OFFLINE installation - no internet **
You are about to install a first node of microk8s cluster.
This will remain a single-node configuration, unless you convert it to a High Availability cluster by adding additional nodes on separate LVAs.
 > Encryption secret: {randomly generated}
Continue? [y,n]y
2024-05-17T11:39:01Z INFO Waiting for automatic snapd restart...
2024-05-17T11:39:04Z INFO Waiting for automatic snapd restart...
snapd 2.62 from Canonical✓ installed
core20 20240416 from Canonical✓ installed
microk8s v1.30.0 from Canonical✓ installed
"microk8s" switched to the "1.30/stable" channel

General refreshes of "microk8s" held indefinitely
Stopped.
/opt/baxter/appliance/bin/../lib/install_microk8s.sh: line 458: 13951 Terminated              microk8s start 2> /dev/null
/opt/baxter/images Pre-loading containerd images from /opt/baxter/offline/images
bdhp-account:4.12.3.tar
Pushing OCI images to 172.28.87.176:25000
bdhp-adt:4.48.0.tar
Pushing OCI images to 172.28.87.176:25000
bdhp-alarm-reporter:4.18.3.tar
Pushing OCI images to 172.28.87.176:25000
bdhp-catalog-configuration:4.43.0.tar
Pushing OCI images to 172.28.87.176:25000
bdhp-catalog-service-jobs:4.2.0.tar
Pushing OCI images to 172.28.87.176:25000
bdhp-catalog:4.127.0.tar
Pushing OCI images to 172.28.87.176:25000
bdhp-clamav:4.14.2.tar
Pushing OCI images to 172.28.87.176:25000
bdhp-communication:4.16.0.tar
Pushing OCI images to 172.28.87.176:25000
bdhp-device-gateway-engine:4.15.0.tar
```

NOTE This may take up to 10 minutes to complete. A message of 'Microk8s setup complete' is returned. An option of **–-debug** can be used to view and confirm each step of the installation. Validate that all containers are in a running state and showing 1 of 1 before proceeding.

Installing Load balancer - MetalLB

Users normally interact with applications running the Kubernetes cluster via a DNS record. For example, suppose a customer wants to use **https://baxterapps.myhospital.com**.

A DNS record is created that maps that address to the *virtual IP address*. The virtual IP address must be kept unused so that it is not inadvertently assigned to another machine via DHCP or some other mechanism.

BDHP uses **MetalLB** as its load balancer. A load balancer requires a **Virtual IP address (VIP)** be assigned to it

In a single node solution, a load balancer is typically configured with the IP address of the node - as all traffic will be directed to that node - as the VIP.

Occasionally, such as an installation requiring beds as well as pumps, there may be two virtual IPs available. The load balancer should use the VIP considered the primary address

- only use the additional VIP for the supplementary device, such as beds.

To set the Virtual IP address used by MetalLB, run the following command to use the node's IP address:

lva install-metallb "$(ip addr | grep eth0 | grep inet | cut -d" " -f6 | cut -d"/" -f1)"

Or set manually to the desired IP address.

metalVIP=<Enter static VIP here>

lva install-metallb $metalVIP

Install OpenEBS

In previous versions of the LVA, OpenEBS was installed at the same time as Microk8s. Changes to OpenEBS backend modules have meant that OpenEBS can only be installed once all nodes of the Microk8s cluster have been installed and joined. This necessitates an additional command.

Furthermore, OpenEBS must be installed before any of the following installation steps, including.

- Installing Loki/Grafana
- Installing databases
- Installing the BDHP platform software

OpenEBS is used for provisioning local storage. On a single-node installation this constitutes *all* storage requirements. On a multi-node installation, the databases use local storage as each replica will only write data to the node on which it is running (and therefore needs OpenEBS).

To install OpenEBS please run

lva install-openebs

Install Ingress

Since BDHP 4.4+, the ingress-nginx controller which comes bundled with Microk8s is no longer used. This now requires an additional command.

To install the ingress controller, please run the following command:

lva install-ingress

Release Status:Issued and Effective

Release Status:Issued and Effective

Install Loki

Loki/Grafana provides a cluster-wide logging system.

To install Loki/Grafana please run the following command:

lva install-loki

Database Backups

For databases to be installed, a database backups storage area **must** be configured (change sdg to match the available drive in the environment).

sudo lva setup-backups-storage /dev/sdg

Postgres Full Recovery Mode (WAL)

Installations involving the Postgres database can, *optionally*, be configured to save incremental, *physical*, backups - called **full recovery mode.**

The incremental files are called Write-Ahead Logs (WAL). This means the database can be restored to a point in time.

NOTE that full recovery mode has storage requirement implications and adds complexity to activities such as guest app upgrades. so careful thought is required before its implementation. It is recommended that HA implementations do use full recovery mode

MinIO

To use full recovery mode: Postgres requires AWS S3 compatible storage. MinIO provides this storage to on-premise deployments, and so **must** be installed.

The previous **setup-backups-storage** command will have labelled the node as minio.

To check the minio-node label exists on the appropriate node, *before* installing MinIO, use the command:

lva label-node

If the minio label is not present use the following command on the appropriate node:

lva label-node $HOSTNAME minio

then install minio using the command:

sudo lva install-minio

Database setup

Before installing databases to the cluster, storage must be provisioned (except Redis which is a cache)

Containerized Databases

The following databases are installed as containerized services:

- PostgreSQL – Normally used for platform storage and pump related applications such as IQE Gateway.
- MongoDB – Only required for bed-related installations that require CDR
- Redis - Only required for bed-related installations
- MySQL – **Only** required for **ICNET** installations.
- Neo4j – **Only** required for **ICNET** installations.

Database Storage Setup

Before the installation of databases plan and provision storage. The size of attached storage must consider the size of the installation and needs of the organization.

A single command is available to partition and mount our standard database filesystems on an attached storage volume.

In the example below, it is assumed that the dedicated storage volume is present as /dev/sdc. If this is not the case, adjust the parameter as required.

sudo lva setup-db-storage /dev/sdc postgres

For Mongo

sudo lva setup-db-storage /dev/sdd mongodb

For MySQL

sudo lva setup-db-storage /dev/sde mysql

For Neo4j

sudo lva setup-db-storage /dev/sdf neo4j

Node labelling

The above **lva setup-db-storage** commands will also put appropriate labels on the node which will be used when the database is installed to detect where to run the containers and connect to the database storage.

Examine the existing labels of nodes in the cluster with the following command:

lva label-node

Install the Database(s)

Postgres

Postgres can be installed as either community or enterprise editions.

- Community - CloudNativePG
- Enterprise - EDB Postgres for Kubernetes

It is recommended that enterprise is *only* used in multi-node, High Availability, configurations due to it being designed for such a solution. There are costs and licensing requirements to using the enterprise edition, but this comes with premium support.

Full Recovery Mode

Full recovery mode is recommended for HA configurations, principally due to the benefit of self-healing it provides. Self-healing means that the database node is re-synced with the master, upon reconnection after a period of downtime.

Full recovery mode can be enabled for the community edition. While it doesn't gain the benefits of self-healing, it does allow for point-in-time restorations.

Community Installation

To install PostgreSQL CloudNativePG (community) database without full recovery mode, run the following command:

lva install-postgres

Postgres Enterprise installation with Full Recovery Mode

To install PostgreSQL enterprise database, with full recovery mode, run the following command:

lva install-postgres --enterprise --full-recovery-mode

NOTE: MinIO must have previously been installed if Full Recovery Mode is selected.

Extra install options

The following options can be provided to the installation command:

1. available-memory
2. max-connections

If not specified, then values of **2Gb** (2048Mb) and **100** connections are used.

For installations with greater resources available to PostgreSQL there may be a need to increase the allocation in the following manner:

lva install-postgres --available-memory=6144 --max-connections=250

MySQL

There are 2 options of operators Community or Enterprise editions. There are costs to using the Enterprise edition, but this comes with premium support

Installation for *Community* edition use the following commands:

lva install-mysql

Release Status:Issued and Effective

or for the *Enterprise* edition:

lva install-mysql --enterprise

See *Appendix E* for MySQL License information (enterprise only).

Mongo

MongoDB is a document-oriented database. Installations of the platform which implement the Clinical Data Repository (CDR) use Mongo. Mongo must be installed for any Bed or Vitals installation.

Install onto the LVA using the following command:

lva install-mongodb

Neo4j

The ICNET guest application uses the neo4j graph database. If additional database is needed install with the following comand:

lva install-neo4j

Redis

The **Bed Device Gateway** (BDG) component uses the Redis cache - which requires persistent storage. A node **must** be labeled for Redis. Redis will then be installed during the platform installation.

lva label-node $HOSTNAME redis-bdg

Antivirus protection

BDHP has two parts to its Antivirus protection.

LVA ClamAV

LVA ClamAV is always installed as part of the LVA and is responsible for scanning the LVA filesystem for threats.

- AV definition updates are configured in **/etc/freshclam.conf .**
  - If the configured ClamAV mirror is blocked, then the LVA ClamAV service will continue to run every night but will effectively do nothing if it can't update its mirrors.
- Customer could uninstall clamav and replace with their own AV software, at their own risk.

Service ClamAV

The Service ClamAV is disabled by default on platform. It can be enabled using the following tag as part of the installation command:

--set 'clamav.enabled=true'

Freshclam is the Antivirus updates service which runs regularly to check that the software is

Release Status:Issued and Effective

updated with the latest threat definitions. By default, it connects to the following mirror:

kube-prod-eus.connex.baxter.com/clamavmirror

But definition mirrors can be changed using

--set clamav.freshclam.mirror1=

For example, a pre-production mirror can be used. It is hosted at **kube-prod-eus.connex.baxter.com/clamavmirror**. Only use for testing.

Freshclam can be run manually at any time using the comand:

sudo freshclam

```
baa@bdhp-iain-75550:~$ kubectl get po -A | grep clam
ns              clamav-7cb78468ff-wswvx                          1/1     Running
baa@bdhp-iain-75550:~$ sudo freshclam
[sudo] password for baa:
ClamAV update process started at Wed May 22 09:04:00 2024
WARNING: DNS Update Info disabled. Falling back to HTTP mode.
Trying to retrieve CVD header from http://kube-prod-eus.connex.baxter.com/clamavmirror/daily.cld
WARNING: remote_cvdhead: file not found: http://kube-prod-eus.connex.baxter.com/clamavmirror/daily.cld
Trying to retrieve CVD header from http://kube-prod-eus.connex.baxter.com/clamavmirror/daily.cvd
Time:    0.4s, ETA:    0.0s [========================>]       512B/512B
OK
daily.cvd database is up-to-date (version: 27282, sigs: 2061432, f-level: 90, builder: raynman)
Trying to retrieve CVD header from http://kube-prod-eus.connex.baxter.com/clamavmirror/main.cld
WARNING: remote_cvdhead: file not found: http://kube-prod-eus.connex.baxter.com/clamavmirror/main.cld
Trying to retrieve CVD header from http://kube-prod-eus.connex.baxter.com/clamavmirror/main.cvd
Time:    0.4s, ETA:    0.0s [========================>]       512B/512B
OK
main.cvd database is up-to-date (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Trying to retrieve CVD header from http://kube-prod-eus.connex.baxter.com/clamavmirror/bytecode.cld
WARNING: remote_cvdhead: file not found: http://kube-prod-eus.connex.baxter.com/clamavmirror/bytecode.cld
Trying to retrieve CVD header from http://kube-prod-eus.connex.baxter.com/clamavmirror/bytecode.cvd
Time:    0.5s, ETA:    0.0s [========================>]       512B/512B
OK
bytecode.cvd database is up-to-date (version: 335, sigs: 86, f-level: 90, builder: raynman)
```

If ClamAV is enabled, there is configuration which tells guest applications that it can be used. If it IS enabled and can't get its AV updates, guest applications will find that their file uploads get marked as viruses.

If ClamAV is NOT enabled, guest applications switch off ClamAV validation in their file uploads

General

Unless a customer can *guarantee* that inbound HTTPS traffic from **kube-prod-eus.connex.baxter.com/clamavmirror** will not be blocked.

Do not not enable the ClamAV service.

Customers could only implement independent LVA AV software. They cannot change the service that runs in the microk8s cluster.

Installing BDHP platform

Check Databases

First, check that the installed databases are running by inspecting the postgres, mysql, mongodb and neo4j namespaces and confirm the correct number of pods are running. Run the following commands:

kubectl get po -n postgres && kubectl get po -n mysql &&

kubectl get po -n mongodb && kubectl get po -n neo4j

For a single node installation with just mongo and postgres installed a output similar to that below should be seen.

```
baa@bdhp-iain-75550:/var/log$ kubectl get po -n postgres && kubectl get po -n mysql &&
> kubectl get po -n mongodb && kubectl get po -n neo4j
NAME                      READY   STATUS    RESTARTS      AGE
bdhp-postgres-cluster-1   1/1     Running   1 (39d ago)   78d
No resources found in mysql namespace.
NAME                                        READY   STATUS    RESTARTS      AGE
mongodb-0                                   2/2     Running   2 (39d ago)   78d
mongodb-kubernetes-operator-d9c7f9998-6856f 1/1     Running   1 (39d ago)   78d
No resources found in neo4j namespace.
baa@bdhp-iain-75550:/var/log$
```

No pods will be returned for databases that have not been installed. A multi-node installation with all databases installed might return:

```
baa@glos-ha-n01:~$ kubectl get po -n postgres && kubectl get po -n mysql &&
> kubectl get po -n mongodb && kubectl get po -n neo4j
NAME                      READY   STATUS    RESTARTS   AGE
bdhp-postgres-cluster-1   1/1     Running   0          60m
bdhp-postgres-cluster-2   1/1     Running   0          59m
bdhp-postgres-cluster-3   1/1     Running   0          58m
NAME                            READY   STATUS    RESTARTS   AGE
mysql-0                         2/2     Running   0          62m
mysql-1                         2/2     Running   0          62m
mysql-2                         2/2     Running   0          62m
mysql-router-684f7884d7-zhlxv   1/1     Running   0          59m
NAME                                        READY   STATUS    RESTARTS   AGE
mongodb-0                                   2/2     Running   0          64m
mongodb-1                                   2/2     Running   0          63m
mongodb-2                                   2/2     Running   0          62m
mongodb-kubernetes-operator-86d87c87fb-xtlwx 1/1    Running   0          65m
NAME                      READY   STATUS    RESTARTS   AGE
bdhp-neo4j-cluster-0      1/1     Running   0          63m
```

Expected number of database pods:

	Single node	**Multi-node**
Postgres	1	1 per database node
Mysql	1 plus a router pod	1 per database node plus a router pod
Mongo	1 plus an operator	1 per database node plus a operator
Neo4J	1	1

Do not proceed if any pods are NOT in running state.

Next, set the variables that will be used during the installation.

Setting the Variables

Run the commands listed in the Set Variable column.

Variable	Description	Set Variable

FQDN (Fully Qualified Domain Name)	What is typed into the browser (*e. g.,* **https://<fqdn>**) to reach the web UI.	**bdhpFqdn=[**replace with the FQDN from the Intake Form**]**
Version of BDHP to install	Sets the version of BDHP to install.	**bdhpVersion=[**release version from the intake form -eg 4.3.8]
Namespace	A name that is short and easy to copy and paste where needed (*e. g.* **ns**). The namespace cannot be any of the following reserved namespaces*:* **backups**, **default**, **ingress**, **kube-system**, **kube-public**, **kube-node-lease**, **linkerd**, **monitoring**, **openebs**	**namespace=[**your namespace name**]**

NOTE: These Global variables are for the current SSH session. The next SSH session will have to set them again.

Install the Platform

Install the BDHP platform

To simply install the BDHP platform – and nothing else – use the following lva command:

lva platform:install -n $namespace $bdhpVersion

The above command – without any command-line flags - will interactively prompt for important information such as the FQDN.

Install BDHP with flags

Typically, the installer will want to install, for example, Bed or Pump functionality that will send data to the CDR; or have Clam Antivirus installed.

--set flags

The platform has a wide variety of different installation configurations. Please see the section titled '**BDHP installation variables**' in *Appendix F* for more information.

An install command for functionality such as beds and pumps, with monitoring of metrics, might be:

```
# Install the platform
## Variable: bdhpFqdn is the Fully Qualified Domain Name and must be set
 ## This is what you'll type into your browser (https://<fqdn>) to use the web UI.
```


Release Status:Issued and Effective

```
## Variable: bdhpVersion is the Version of BDHP to install and must be set
lva platform:install -n $namespace $bdhpVersion \
--domain=$bdhpFqdn \
--database=postgres \
--set 'tags.beds=true' \
--set 'tags.pumps=true' \
--set 'tags.manual-adt=true' \
--set 'tags.monitoring=true' \
--set 'clamav.enabled=true' \
--set 'bdhp-ntpd.enabled=true' \
--set 'smtp.host=relays.customer.com,smtp.port=25,smtp.from=no-reply@customer.com,smtp.ssl=false'
```

NOTE Replace the smtp.host and from values with customer-supplied values

NOTE The above example has both beds and pumps functionality enabled.

This requires two separate verne instances. An alternative IP address must be used. See the A*ppendix I* titled '*Additional Virtual IP for VerneMQ*' for more information.

Install BDHP using YAML file

Alternatively, the above flags can be placed into a yaml file. It is recommended if the same features are needed for multiple installations.

yamlFile = install-values.yaml

lva platform:install -n $namespace $bdhpVersion --domain=$bdhpFqdn -f $yamlFile

An example yaml file is available in *appendix G*.

Wait for completion

Once the installation scripts have finished running wait for the installation to complete. This may take several minutes.

Release Status:Issued and Effective

```
>> STEP 5 - Install platform
secret "platform-onprem-install-values-mdap" deleted
secret/platform-onprem-install-values-mdap created
Running: helm upgrade --install mdap /home/baa/mdap-4.3.1-beta.20240130124622.tgz
Release "mdap" does not exist. Installing it now.
NAME: mdap
LAST DEPLOYED: Tue Jan 30 16:34:45 2024
NAMESPACE: moose
STATUS: deployed
REVISION: 1
NOTES:
---------------------------------------------------------------------------------------------------------------
 Fully Qualified Domain Name: moose.org.uk
 ◉ INFO: ClamAV service is disabled. It can be enabled by setting "clamav.enabled=true".
 ◉ INFO: This is NOT a production site. For test/evaluation only. Change to production by setting "global.customer.live=true".
---------------------------------------------------------------------------------------------------------------
secret "platform-onprem-install-values-mdap" deleted
secret/platform-onprem-install-values-mdap created
configmap/platform-chart-uris created

 > MDAP is now installed! Please wait while pods are brought up according to their dependencies
 > It has been installed as mdap
Run 'helm list -n "moose"' to see it!

 > To upgrade this chart run 'mdap upgrade mdap ...'
 > Run 'mdap upgrade --help' for information

 > Install any MDAP-compliant application with 'mdap install'
 > Run 'mdap install --help' for information

Backup encryption key not found and will be created now...
namespace/backups created
secret/mdap-db-backups-tls-secret created
EC Cert saved to mdap-db-backups-tls-secret
-----BEGIN EC PRIVATE KEY-----
MIGkAgEBBDAFdbajelIZFvnOV9LfPo+PlV7o2vrewrKcCQQgB4fcm1f8JeHh71hS
JrNSYmQ/l22gBwYFK4EEACKhZANiAAS2726jWtSGPNewBuwnsyuMcbIUXzGGSuDL
/vOs8gcs1LShiChHTWAXThQ4FVL1cqmFJku8W5ku30avLtp9NcFLKQsDCjZ9UIDu
e1gFG8DOU6sCFdakK1zq5hBB9YTxFiQ=
-----END EC PRIVATE KEY-----

*** IMPORTANT - Please ensure a copy of the EC Private Key is safely stored for recovery purposes. ***
Alternatively, to import a customer supplied X.509 certificate run lva change-backup-certs
Keycloak console admin credentials:
    baxter / QceLnMLTZKcjxWMx59LlQ9tlOLZqHQ
```

The BDHP platform is now installed successfully, as evidenced by the '*MDAP is now installed*' message in green.

Exporting Private key

The yellow warning in the above screenshot refers to the private key used to encrypt database backups.

Ensure the private key is safely copied and stored off the LVA – copy from the start of the '-----BEGIN EC PRIVATE KEY' line to the end of the 'END EC PRIVATE KEY-----' line.

The key can be output at any time using the following command:

sudo lva decrypt-backup --export-private-key

Verify platform is running

Run the following command to show the status of the pods after installation:

watch kubectl get po -n $namespace

Wait until all the pods are "1/1" in the "READY" column - the 'watch' command refreshes the status every 2 seconds.

This means that the container is running and has passed its readiness checks. The installation is completed.

```
Every 2.0s: kubectl get po -n ns

NAME                                          READY   STATUS    RESTARTS       AGE
clamav-6c87b49dcf-xgw5h                       1/1     Running   0              20m
bdhp-mirth-connect-0                          2/2     Running   0              20m
keycloak-0                                    1/1     Running   0              20m
bdhp-rabbitmq-0                               1/1     Running   0              20m
bdhp-vernemq-0                                1/1     Running   0              20m
bdhp-ecp-ui-7cb65d7858-gbh9q                  1/1     Running   0              20m
bdhp-emr-vitals-78bb5776c-f48pc               1/1     Running   0              20m
bdhp-device-gateway-6cc646699-v4pfk           1/1     Running   0              20m
bdhp-iqecs-799785f5dd-ghrc6                   1/1     Running   0              20m
bdhp-location-7d98678945-f5rpq                1/1     Running   0              20m
bdhp-adt-6bc94465b9-h5n8b                     1/1     Running   0              20m
bdhp-patient-754dbc8658-289r5                 1/1     Running   0              20m
bdhp-device-7c474f7cf5-6t4x6                  1/1     Running   0              20m
bdhp-encounter-5dddd76667-szfms               1/1     Running   0              20m
bdhp-observation-6bddcf7d5-h78pn              1/1     Running   0              20m
bdhp-communication-79948b8678-b2fdf           1/1     Running   0              20m
bdhp-practitioner-7f44b84884-xbsmr            1/1     Running   0              20m
bdhp-terminology-7b47d454cb-spz45             1/1     Running   0              20m
bdhp-publisher-7d75795765-fh2ts               1/1     Running   0              20m
mdap-redis-shared-master-0                    1/1     Running   0              20m
mdap-redis-mirth-master-0                     1/1     Running   0              20m
mdap-redis-bdg-master-0                       1/1     Running   0              20m
bdhp-wacp-58c4c6dbd8-4q5bj                    2/2     Running   0              20m
bdhp-vitals-outbound-cd8479b98-pd8kj          1/1     Running   1 (11m ago)    20m
bdhp-alarm-reporter-77c5648ddd-kpp44          1/1     Running   3 (12m ago)    20m
bdhp-hl7outbound-687cfb6c8f-gswqp             1/1     Running   3 (11m ago)    20m
bdhp-device-gateway-engine-5fc555465d-vjkmc   1/1     Running   2 (12m ago)    20m
bdhp-catalog-865d54fbcc-59k7n                 1/1     Running   4 (11m ago)    20m
```

Add additional features to Platform

This installation guide is **not** intended to guide on how to upgrade the platform from one version to another. It is possible to install a new feature via an upgrade command – even if the upgrade version is identical to the current version of the BDHP platform.

The platform can be upgraded with extra 'set' options; alternatively a yaml file of options can be specified.

```
# Can upgrade platform to use new feature from the BDHP installation variables
lva upgrade mdap:$bdhpVersion -n "$namespace" --set my.new.option=true
# or use yaml
lva upgrade mdap:$bdhpVersion -n "$namespace" -f install-values.yaml
```

For example, if a customer requires bed functionality – and it wasn't specified at installation time -then add the following tag to the command:

--set tags.beds=true

Please see the section titled ' **BDHP installation variables**' in the *appendix F* for more information

Release Status:Issued and Effective

Certificates

Digital Certificates are needed for secure connections when messages/requests pass across the load balancer of BDHP. Two sets of certificates are required at a BDHP installation:

1. Ingress web certificates. These are requests from web browsers on the customer's network
2. Device certificates. These are interactions between Baxter devices and BDHP

A full explanation of Certification theory, in relation to BDHP, is given in *Appendix H*.

Once the ingress and device certificates have been moved to the BDHP server, ensure that they are installed in the following manner:

Ingress:

For ingress 2 files are needed:

a. Certificate generated to match the FQDN of the installation ($cert)
b. Private key ($key)

Use the command

lva ingress:change-ui $cert $key -n $namespace

Device:

For devices 3 files are required, the certificate and private key. Certificate Authority permissions are required - which is the issuer of the certificate – certificate named $*cacert* below.

Run the **lva ingress:change-device** command to load these files into secrets

lva ingress:change-device $cert $key $cacert -n $namespace

Restart the VerneMQ pods:

kubectl delete pod bdhp-vernemq-0 bdhp-vernemq-pumps-0 -n $namespace --force

NOTE: Make sure the private keys are safely stored off the server, prior to deletion!

Following the installation, web browsers will display the login screen without warning messages; and devices will be able to connect.

List Installed Applications

To list installed applications, run the following command:

helm list -n **$namespace**

```
root$ bdhp4lecp1:~# helm list -n ns
NAME    NAMESPACE       REVISION        UPDATED                                   STATUS          CHART           APP VERSION
mdap    ns              1               2024-01-24 18:48:10.122324703 +0000 UTC deployed        mdap-4.3.0      4.3.0
root$ bdhp4lecp1:~#
```

This command will also list guest applications, when they are installed.

Verify that mdap *(mdap is the internal product name for BDHP)* has been installed, and the APP VERSION is as expected.

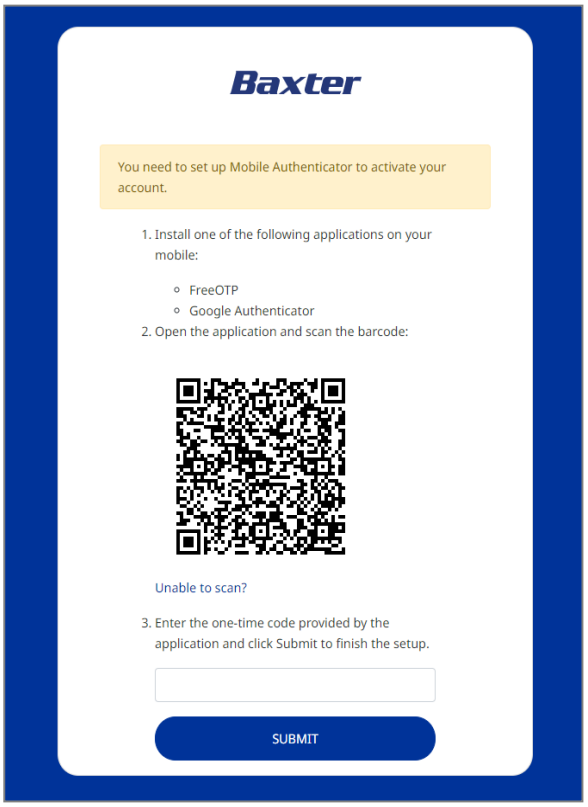
Log on to the BDHP UI

Go to **https://[FQDN]**, replacing **FQDN** with the bdhpFqdn environment variable. (See ***Error! Reference source not found.***)

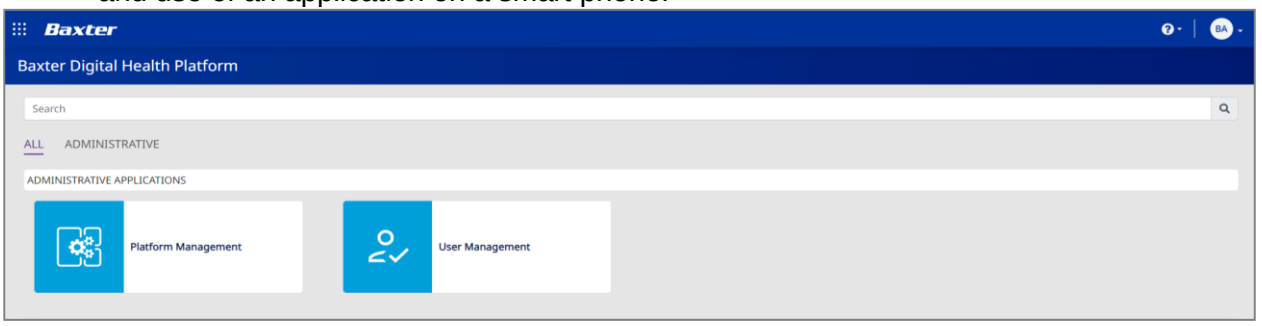
Log on with the default user account and password below.

Account	Roles	Password
baxter_admin	User Management/Platform Management	Baxter@1

Release Status:Issued and Effective



NOTE: This account is set up with two-factor authentication, which requires download and use of an application on a smart phone.



Verify the **Platform Management** and **User Management** roles are available for the *baxter_admin* user. Success verifies platform installation.

BDHP Instance Connection Guide

Securelink is BDHP's chosen method of secure remote connectivity.

After a customer deploys a BDHP image into the virtual environment and turns the server on, a service called slink runs a script that makes API calls to the SecureLink gateway and creates and registers a new Gatekeeper with the Machine ID shown on the console.

Please see *Appendix J* titled '*J – Configuration of SecureLink for remote access*' for more information on how to configure Securelink for support users.

Summary

A BDHP platform has been installed and is accessible.

The platform itself does not 'do' anything, until other applications are installed onto it and configured. For information on how to install guest applications please visit *Appendix K - Installing, upgrading and configuring guest applications*.

BDHP uses the Keycloak application to control user and group roles and permissions. Information on how to access the keycloak administration section can be found here in *Appendix L. Using the Keycloak admin console*

Server maintenance routines such as database backups must be configured.

Release Status:Issued and Effective

Appendix

Articles have been placed within this appendix to provide extra information relevant to the install process

A. Checking LVA digital signature

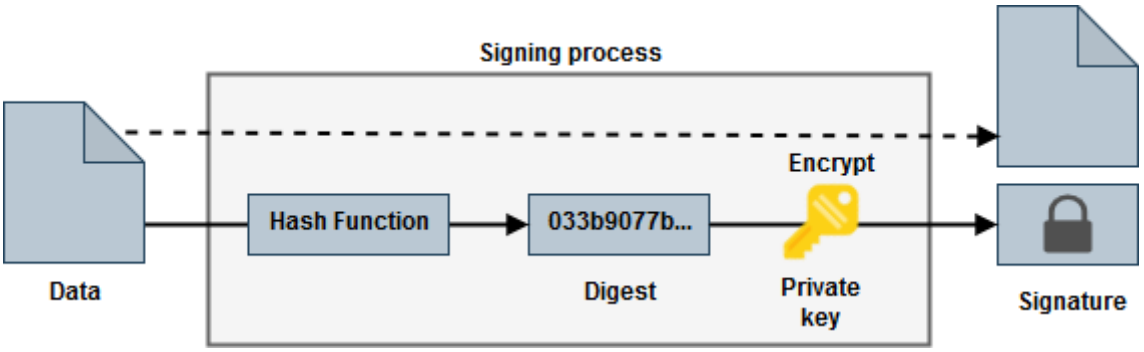
Digital signatures allow the recipient to verify both authenticity and integrity of the received LVA

The LVA is distributed in the following formats

- ova
- qcow2
- vhdx

These files are now digitally signed with a Baxter self signed certificate. The digital signature file accompanies the lva file and has the extension .sha512

The lva files are digitally signed using certificates, using the following method.

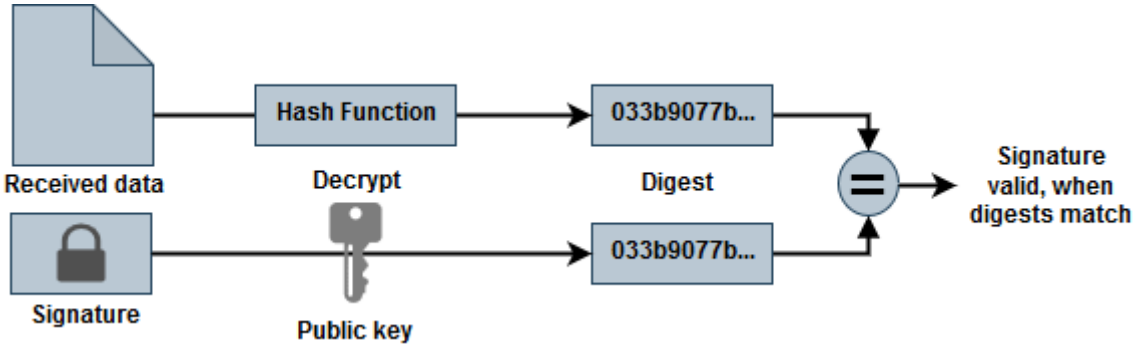


To check the file pre-requirements must be present:

- LVA file (ova, qcow2, vhdx)
- LVA signature file (*.sha512)
- Baxter public key (*.pub)

To verify the files it requires a public key (*.pub) to decrypt and check the signature. The public key would need to be provided to the customer

Release Status:Issued and Effective



Using an ova file as an example here are the possible names.

- BDHP-LVA-v7.96.50.ova
- BDHP-LVA-v7. 96.50.ova.sha512
- BSIGN.CA.key.pub

Using openssl test the verification of the files together.

```
# openssl command
openssl dgst -sha512 -verify <ca-public-key> -signature <lva signature file>.sha512 <lva file name>

# This is the command using the example files
openssl dgst -sha512 -verify BSIGN.CA.key.pub -signature BDHP-LVA-v7.96.50.ova.sha512 BDHP-LVA-v7.96.50.ova

# You get this response if the LVA file or digital signature have changed in anyway and are not to be trusted
Verification failure
# You get this if the digital signature is correct and verified
Verified OK
```

The public key file required can be produced from the CA kept in the keystore using the following

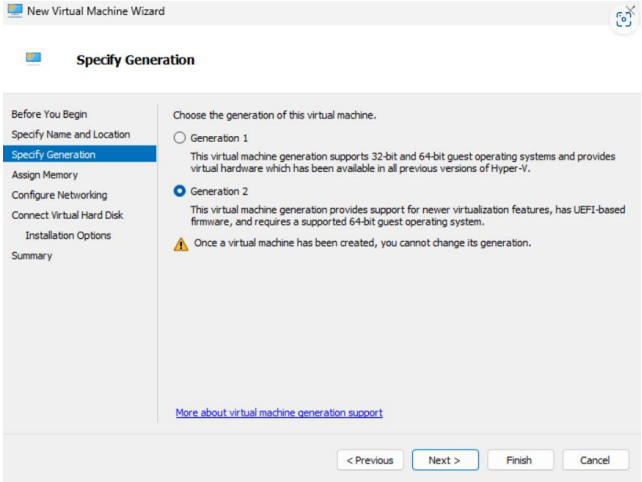
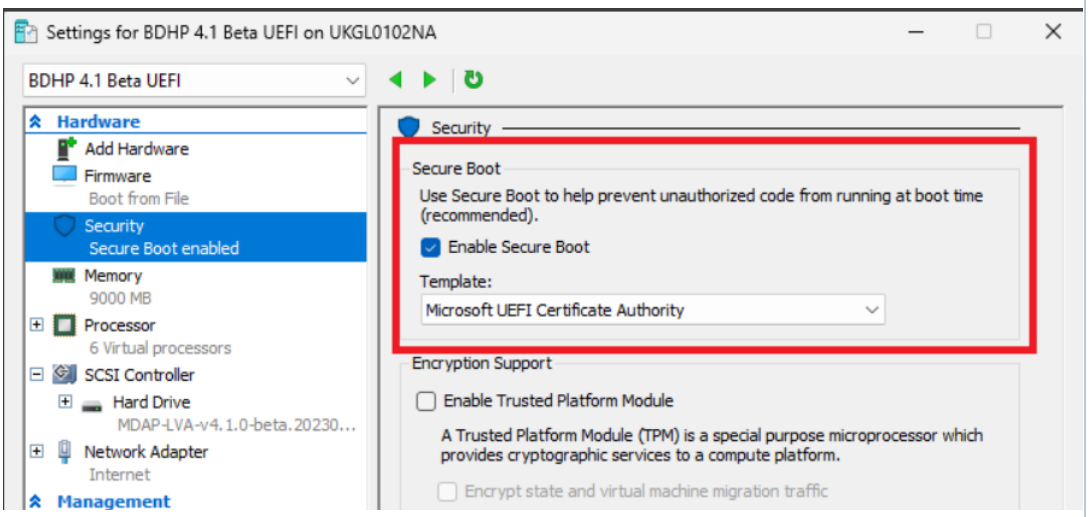
```
# Export the public key from the CA, this is to be used to verify the signed LVA files
openssl x509 -in <ca-cert> -pubkey -noout > <public-key-name>
```

B. Setting UEFI Secure boot on a hypervisor

UEFI secure boot must be setup. The table below describes how this much be done.

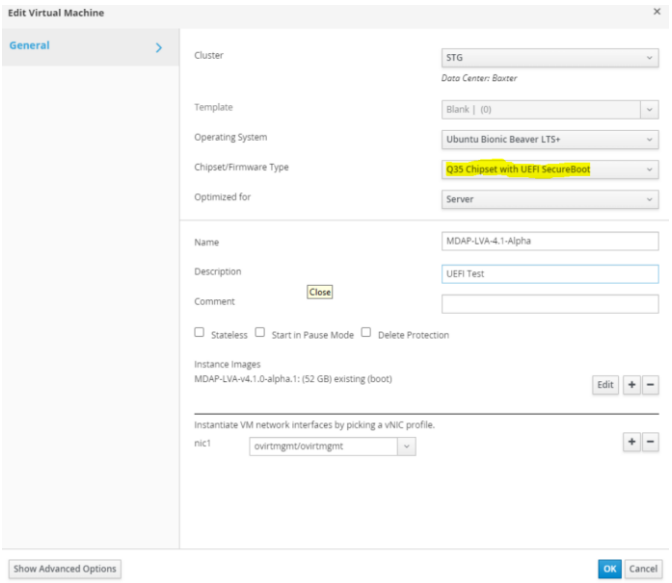
Hypervisor	UEFI selection
VMWare ESX	UEFI Secure boot requires the compatibility version of VMWare to be a minimum of 6.5.

Release Status:Issued and Effective

	The default network adapter has been changed from E1000 to VmxNet3
Microsoft Hyper-V	Select Generation 2  And ensure secure boot is selected and set to UEFI Certificate Authority 
Redhat Enterprise Virtualization	Select UEFI Securehost as the Chipset/Firmware type

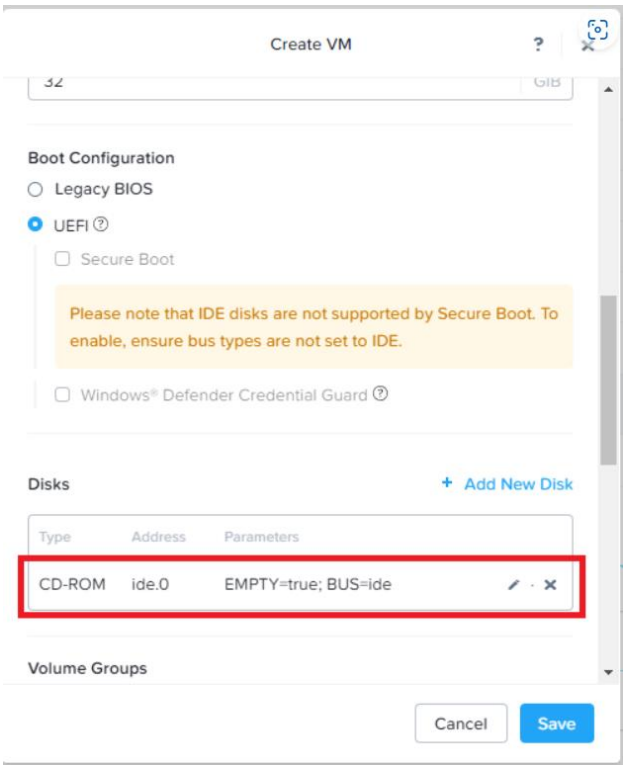
Release Status:Issued and Effective

Release Status:Issued and Effective

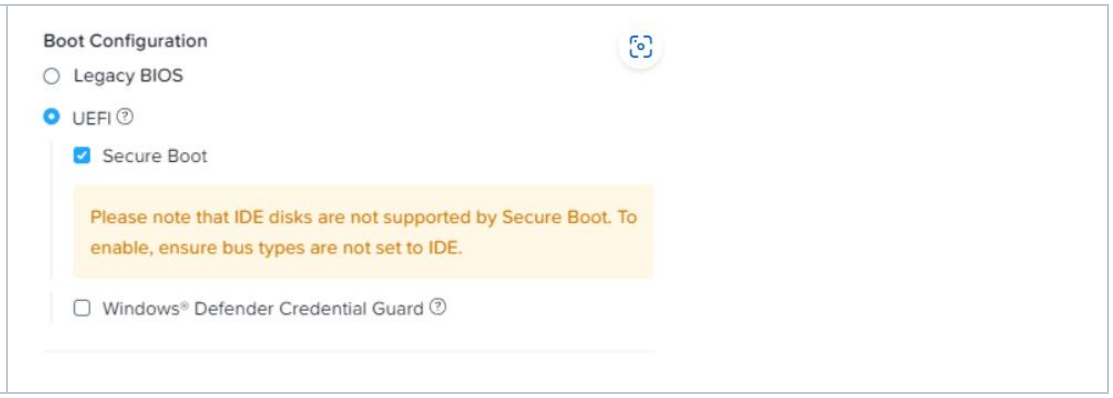


Nutanix

When selecting the **UEFI** setting delete the default attached CD-ROM, in order to be able to select **Secure Boot**



Once CD_ROM is removed select **Secure Boot**



Release Status:Issued and Effective

C. Offline installation

Background

A typical on-line installation reaches out to the internet for multiple software packages. Some customer installations are shielded/firewalled off from the outside internet.

Because of this, BDHP Platform supports the ability to enact an **'offline'** installation.

Offline packages

It is possible to manually load containers into containerd (the container runtime supported by Kubernetes) and the offline deployment processes leverages this capability. So long as a helm chart isn't configured with an image pull policy of 'Always', then containerd will prefer to use a locally cached image rather than downloading from the internet.

For each release of BDHP, a separate media file is distributed which contains all the container images needed by kubernetes and BDHP. This package will need to be manually uploaded into the LVA before installation. These resources hold

- helm charts
- container images

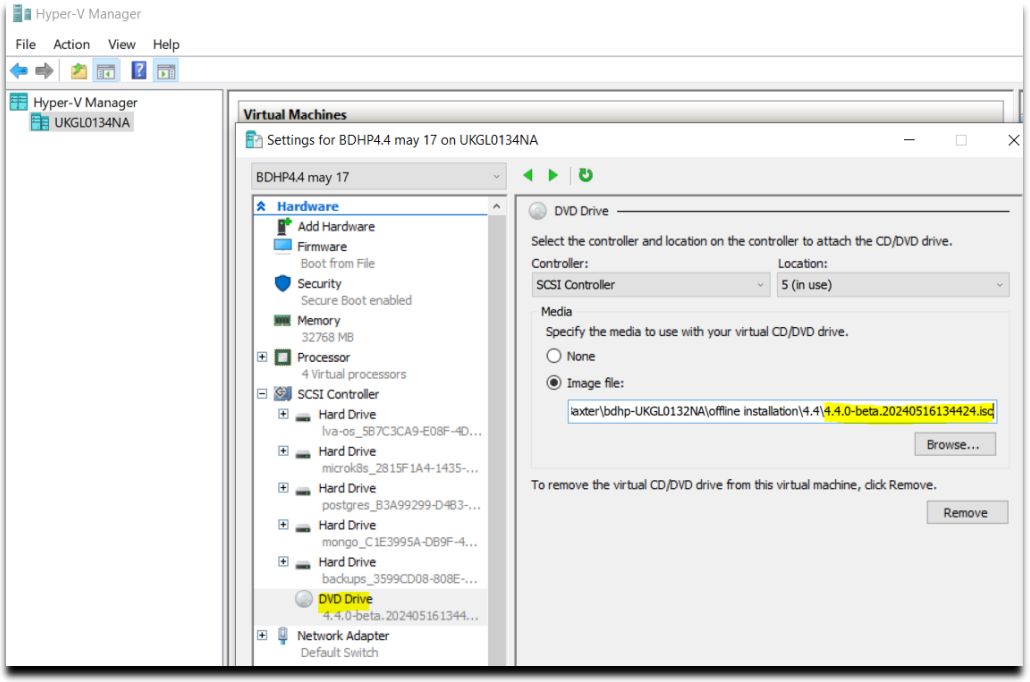
Manually uploading media file

In VirtualBox, the following commands can be used:

set COMBINED_ISO=D:\VBOX\4.3.8.iso

"C:\Program Files\Oracle\VirtualBox\VBoxmanage" storageattach "%VMNAME%" --storagectl LsiLogic --port 5 --type dvddrive --medium "%COMBINED_ISO%"

Using Hyper-V the same can be achieved using the GUI:



Mount the Image

Remote access to the VM will now show the media file with a reference of /dev/sr0. For example:

```
baa@bdhp-4-4-offline:~$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda             8:0    0   51G  0 disk
├─sda1          8:1    0   50M  0 part /boot/efi
├─sda2          8:2    0  974M  0 part /boot
└─sda3          8:3    0   50G  0 part
  ├─vg0-lv--0 253:0    0  9.8G  0 lvm  /
  ├─vg0-lv--6 253:1    0  1.5G  0 lvm  /tmp
  ├─vg0-lv--5 253:2    0  1.5G  0 lvm  /var/tmp
  ├─vg0-lv--4 253:3    0  4.9G  0 lvm  /var/log/audit
  ├─vg0-lv--3 253:4    0  3.9G  0 lvm  /var/log
  ├─vg0-lv--2 253:5    0 27.4G  0 lvm  /var
  └─vg0-lv--1 253:6    0  468M  0 lvm  /home
sdb             8:16   0  120G  0 disk
sdc             8:32   0  110G  0 disk
sdd             8:48   0  105G  0 disk
sde             8:64   0  100G  0 disk
sr0            11:0    1    9G  0 rom
```

Mount the ISO image at a single mount point - */opt/baxter/offline* – using the following command (check that sr0 is the correct reference):

sudo mount -o ro /dev/sr0 /opt/baxter/offline

Use **tree** to verify that the charts and images now exist in the offline directory

```
baa@baxterappliance:~$ sudo mount -o ro /dev/sr0 /opt/baxter/offline
baa@baxterappliance:~$ tree /opt/baxter/offline
/opt/baxter/offline
├── charts
│   ├── bdhp-k8sdashboard-oauth2-proxy-1.16.0.tgz
│   ├── bdhp-minio-migration-1.4.1.tgz
│   ├── bdhp-minio-operator-1.1.0.tgz
│   ├── bdhp-minio-tenant-1.3.2.tgz
│   ├── bdhp-mongodb-cluster-1.10.1.tgz
│   ├── bdhp-mongodb-operators-1.1.2.tgz
│   ├── bdhp-mysql-cluster-1.5.1.tgz
│   ├── bdhp-mysql-operators-1.2.2.tgz
│   ├── bdhp-neo4j-cluster-1.4.6.tgz
│   ├── bdhp-openebs-4.4.2.tgz
│   ├── bdhp-postgres-cluster-1.10.1.tgz
│   ├── bdhp-postgres-operators-1.2.1.tgz
│   ├── bdhp-vernemq-bed-oauth2-proxy-1.5.0.tgz
│   ├── bdhp-vernemq-pump-oauth2-proxy-1.5.1.tgz
│   ├── loki-stack-2.14.8.tgz
│   └── mdap-4.4.0-beta.20240516134424.tgz
├── images
│   ├── bdhpcr.azurecr.io
│   │   └── images
│   │       ├── bdhp-account:4.12.3.tar
│   │       ├── bdhp-adt:4.48.0.tar
```

List the block devices to see that the sr0 reference is now mounted to */opt/baxter/offline*

```
baa@baxterappliance:~$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda             8:0    0   51G  0 disk
├─sda1          8:1    0   50M  0 part /boot/efi
├─sda2          8:2    0  974M  0 part /boot
└─sda3          8:3    0   50G  0 part
  ├─vg0-lv--0 253:0    0  9.8G  0 lvm  /
  ├─vg0-lv--6 253:1    0  1.5G  0 lvm  /tmp
  ├─vg0-lv--5 253:2    0  1.5G  0 lvm  /var/tmp
  ├─vg0-lv--4 253:3    0  4.9G  0 lvm  /var/log/audit
  ├─vg0-lv--3 253:4    0  3.9G  0 lvm  /var/log
  ├─vg0-lv--2 253:5    0 27.4G  0 lvm  /var
  └─vg0-lv--1 253:6    0  468M  0 lvm  /home
sdb             8:16   0  120G  0 disk
sdc             8:32   0  110G  0 disk
sdd             8:48   0  105G  0 disk
sde             8:64   0  100G  0 disk
sr0            11:0    1    9G  0 rom  /opt/baxter/offline
```

BDHP Installation

NOTE: Multi-node offline is fully supported but requires a kubernetes cluster as normal; but all the nodes must have all the container images pre-installed

The typical BDHP installation steps are the same as an on-line installation with just two differences:

1. Microk8s installation
2. BDHP Platform installation

NOTE: Database packages (Postgres and MySQL) are included with the LVA and so there is no need to connect to the internet to retrieve them. The standard install-database commands can be used.

Microk8s installation:

Use:

sudo lva install-microk8s

Installation of microk8s will take some time to complete as each image is loaded into containerd.

NOTE: The text confirming the images are pulled from the offline location.

```
baa@bdhp-4-4-offline:~$ sudo lva install-microk8s --offline
/var/snap/microk8s
** OFFLINE installation - no internet **
You are about to install a first node of microk8s cluster.
This will remain a single-node configuration, unless you convert it to a High Availability cluster by adding additional nodes on separate LVAs.
 > Encryption secret: {randomly generated}
Continue? [y,n]y
2024-05-20T13:35:19Z INFO Waiting for automatic snapd restart...
2024-05-20T13:35:21Z INFO Waiting for automatic snapd restart...
snapd 2.62 from Canonical✓ installed
core20 20240416 from Canonical✓ installed
microk8s v1.30.0 from Canonical✓ installed
"microk8s" switched to the "1.30/stable" channel

General refreshes of "microk8s" held indefinitely
Stopped.
/opt/baxter/appliance/bin/../lib/install_microk8s.sh: line 458: 13369 Terminated              microk8s start 2> /dev/null
/opt/baxter/images Pre-loading containerd images from /opt/baxter/offline/images
bdhp-account:4.12.3.tar
Pushing OCI images to 172.28.80.68:25000
bdhp-adt:4.48.0.tar
Pushing OCI images to 172.28.80.68:25000
bdhp-alarm-reporter:4.18.3.tar
Pushing OCI images to 172.28.80.68:25000
bdhp-catalog-configuration:4.43.0.tar
```

At any time after installing microk8s, load more container images into containerd using the command:

lva import-images

Install platform

Set a variable to the chart we mounted earlier tin the **/opt/baxter/offline/charts/** directory:

mdap_chart=/opt/baxter/offline/charts/mdap-4.3.8.tgz

Since this is an offline installation, assume that ClamAV will not be able to connect to the internet.

Disable the service using the flag using the command: **--set clamav.enabled=false**

We will also disable ntpd and the metrics service, which sends data to cumulocity.

These flags are entered into a yaml file and referenced by the installation command:

lva platform:install -n ns $mdap_chart -f offline.yaml

Alternatively set the flag in the installation command.

```
# Install the platform, disabling services that use the internet.
lva platform:install -n ns $mdap_chart \
--database=postgres \
--domain=bdhp-offline.local \
--set 'global.customer.name=bdhp-offline.local' \
```

```
--set 'clamav.enabled=false' \
--set 'mdap-ntpd.enabled=false' \
--set 'tags.monitoring=false' \
--set 'metrics.enabled=false' \
--set 'tags.beds=true'
```

Here is an example of the yaml used:

```
## The core platform components are defined as 'tags'
tags:
  beds: true
  pumps: false
  manual-adt: false
  monitoring: false
smtp:
  host: relays.baxter.com
  port: 25
  from: no-reply@baxter.com
  username: ""
  password: ""
  ssl: false
## Customer set up
global:
  customer:
    name: iain-offline-may20
    live: false
    country: US
  domain: imc3.org.uk
  database:
    vendor: postgresql
## VerneMQ pumps configuration
bdhp-vernemq-pumps:
  service:
    mqtts:
## Platform Anti-virus service
clamav:
  # If the installation is offline (isolated from the internet) the system
  # cannot reach out for AV updates. If this is the case, please set this to false.
  enabled: false
## Platform NTP service
bdhp-ntpd:
  enabled: false
```

D. LVA Interactive setup

The **lva setup** command is introduced in 4.4+ and provides an interactive command interface for the

Release Status:Issued and Effective

following tasks

- Installing Microk8s
- Configuring Database Backup Storage
- Installing Databases

It is an *alternative* to the Non-interactive commands. Offline installation is available with the interactive setup.

NOTE: Ensure that if the hostname requires changing, that this is carried out prior to running the interactive setup.

NOTE: the interactive setup does not include the following areas:

- Minio installation
- Redis labelling
- Platform installation

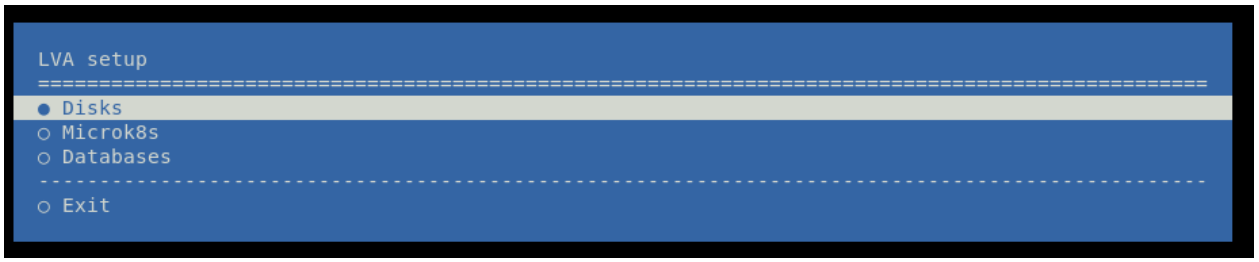
These installation steps need to be run outside of the interactive setup

Launching the interactive set

Type **lva setup** into the command prompt.

On initial opening, you get a screen offering you 3 main areas

- Disks
- Microk8s
- Databases

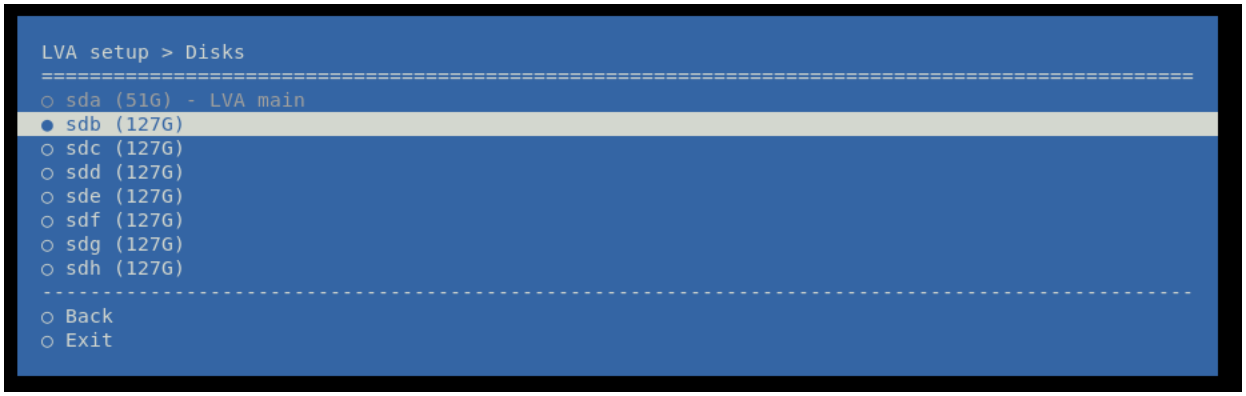


Navigate these using the arrow keys and ENTER.

Disks

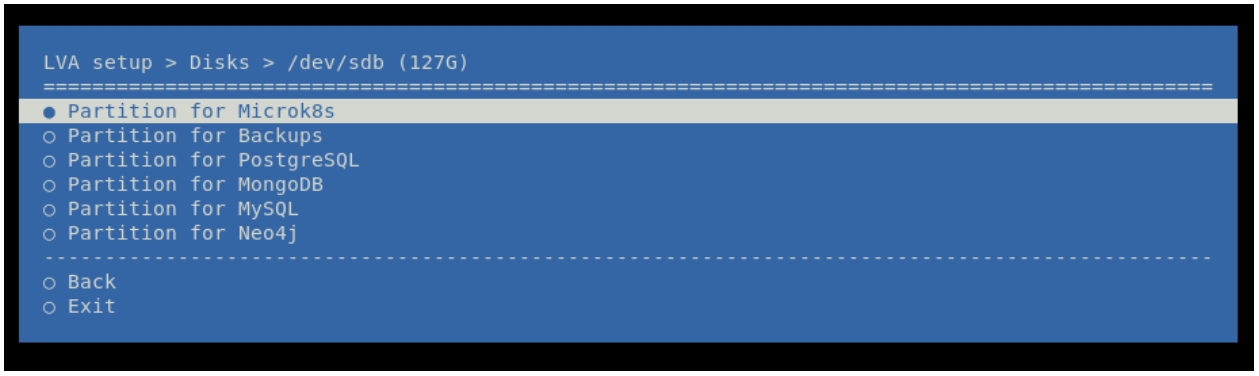
You are initially presented with a menu of all the attached block storage devices detected on the LVA. It shows their names and how big they are.

Release Status:Issued and Effective



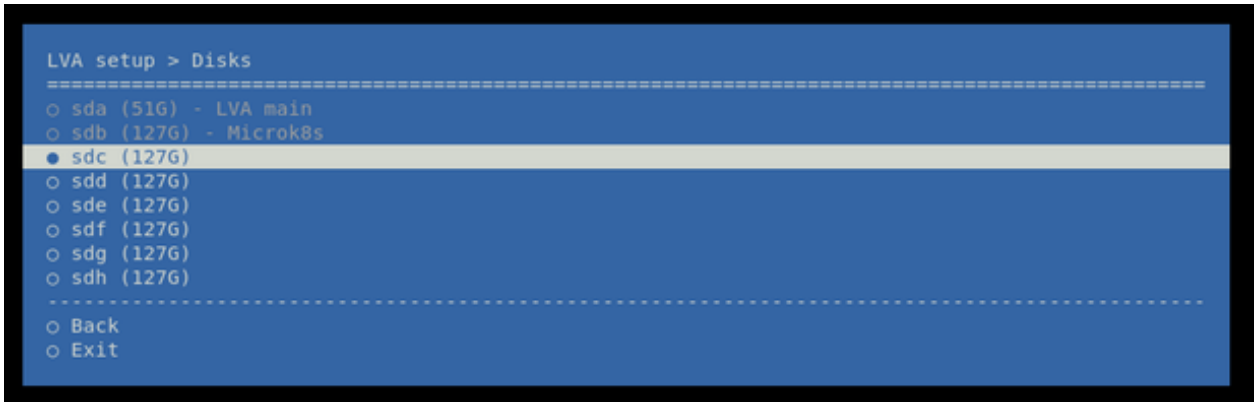
The top sda entry will be there already as this is where the base LVA partitions are located.

If you choose a disk, it will take you to another menu which allows you to select a partition type

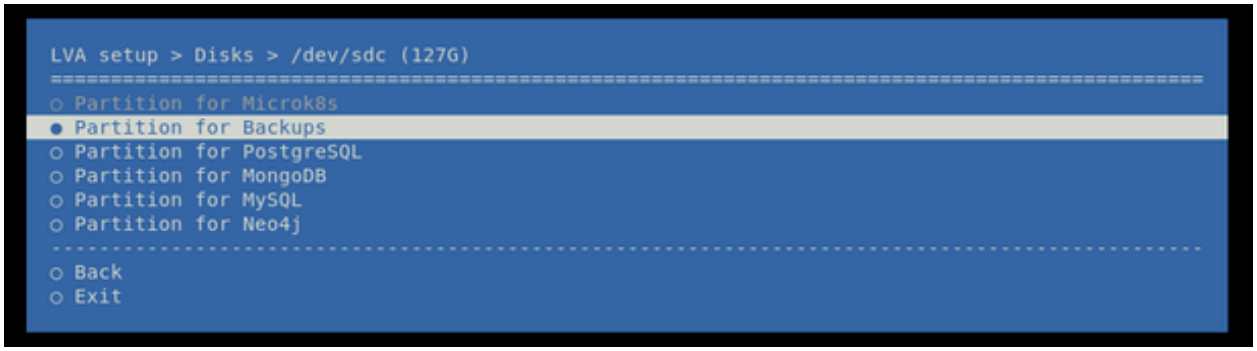


For every choice you will be prompted to proceed or cancel.

When the partitioning has finished you are returned to the previous menu. You will see now that sdb is marked as Microk8s, is greyed out and is unselectable from now on.



If you choose another disk, for example **sdc**, then you can choose to partition it for one of the other purposes, like backups or storage for a particular database.



Notice that as **Microk8s** has already been used, you cannot partition another disk for this purpose. The same will happen for each type. You can only have one Microk8s, Backups, PostgreSQL, MongoDB, MySQL or Neo4j partition per node.

Continue to partition all disks as per the requirements of your chosen install.

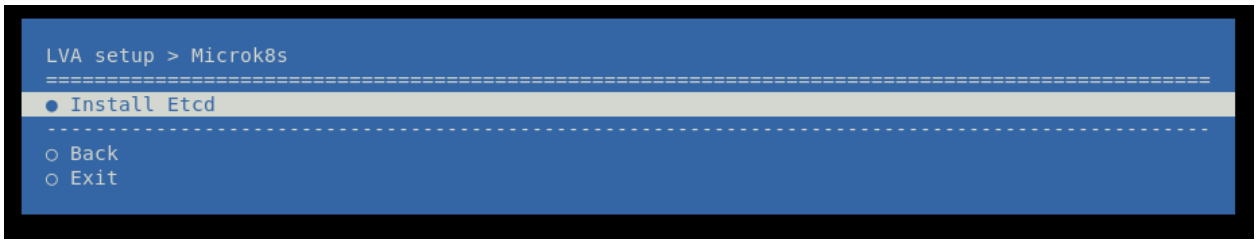
Offline assets ISO

If you are installing in an air-gapped 'offline' environment, our *offline assets ISO* should have been attached in the hypervisor. You should get an additional entry in the Disks menu for mounting this into the filesystem.

Microk8s

Etcd

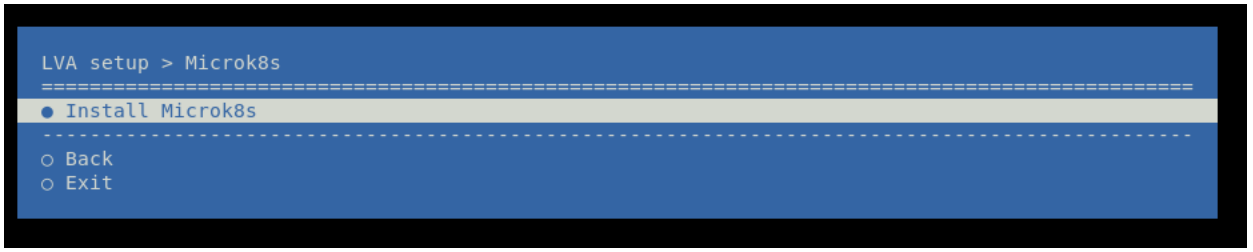
Before installing Microk8s, you need to set up Etcd as the data store for Microk8s.



When you choose **Install Etcd**, you will be prompted to enter the addresses of the nodes where you want Etcd installed. For a single node, you should use "localhost".

Microk8s

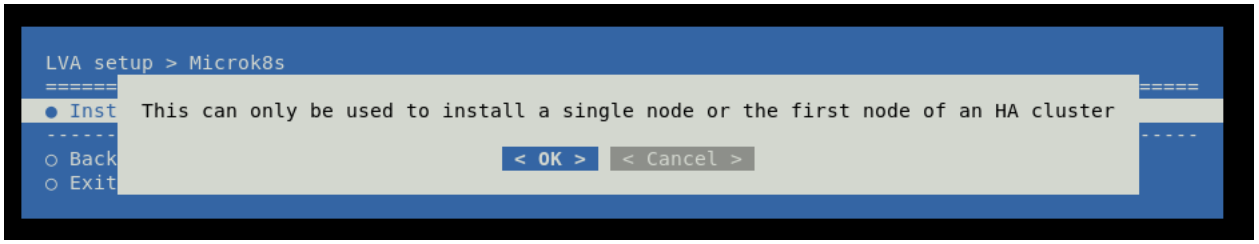
Once Etcd is installed, the **Microk8s** menu will allow you to: **Install Microk8s**.

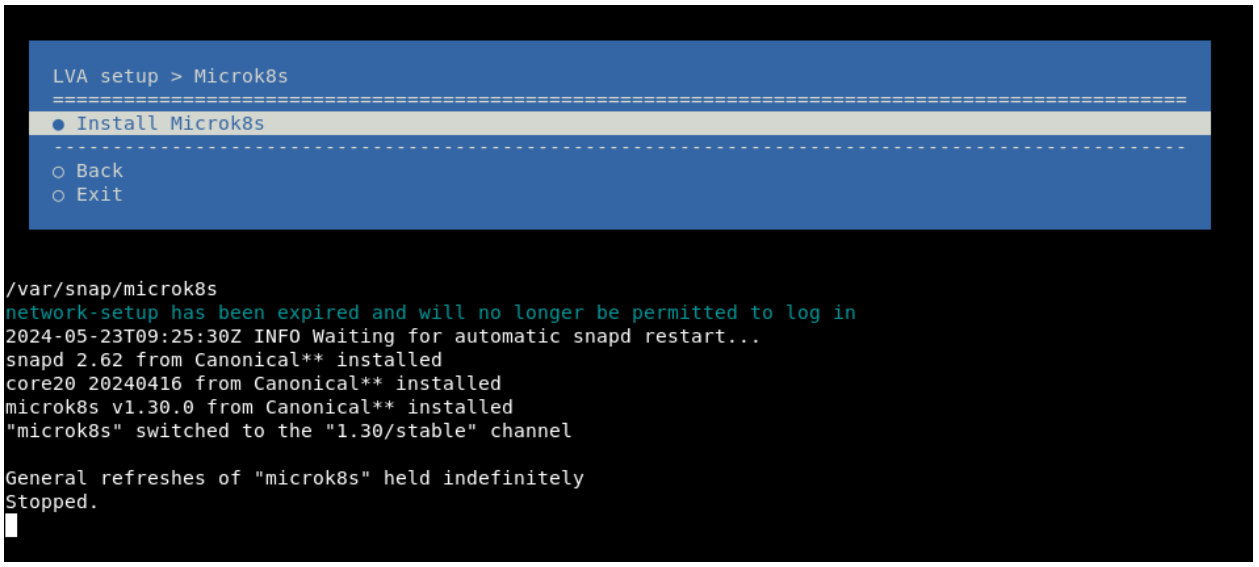


NOTE: If you are installing in an air-gapped environment, you will need to make sure that you have mounted the offline assets ISO before you install microk8s

If you have not set up partitioning for **Microk8s** in the Disks section (see above), you will get the following message when you try to install it.

Assuming that you have partitioned correctly, you will get a prompt to confirm continuation of the installation.



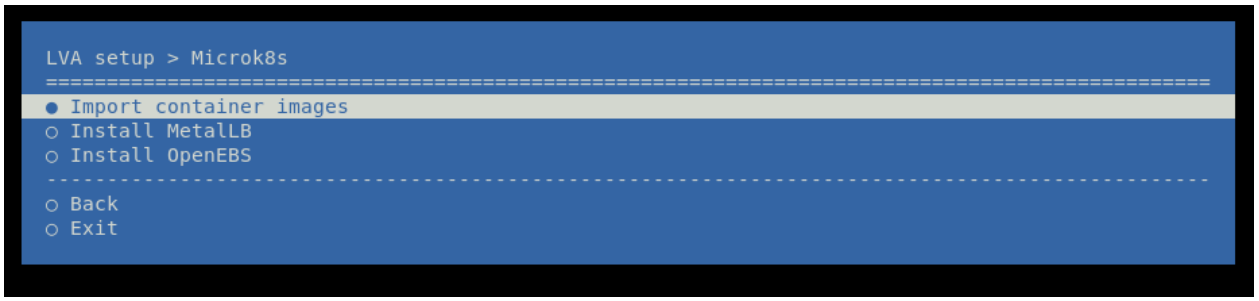


As the installation takes place you will see the command line output showing its progress. Once the install has completed you will be returned to the previous Microk8s menu. Now Microk8s is installed, you will now be able to install additional components.

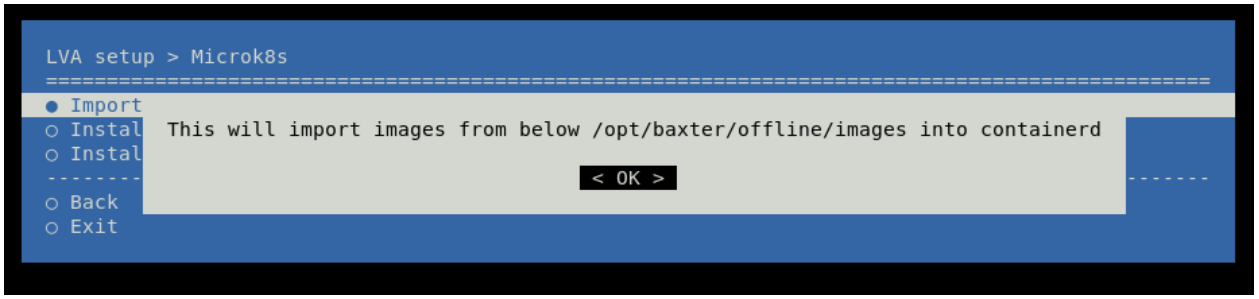
Import offline images

NOTE: If you are installing in an air-gapped environment and you have already mounted the ISO assets in the Disk menu (see above), you will get an additional menu option to import container images into containerd.

You will need to run Import container images before you continue with the other steps in this guide, as the system will be unable to reach out to the internet to download the container images.



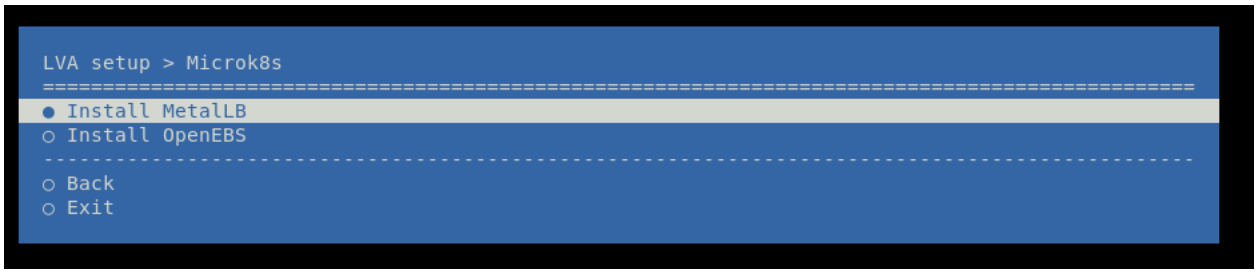
You will be prompted to confirm before the command continues.



The command will proceed to import every image into containerd. This may take some time to complete

MetalLB

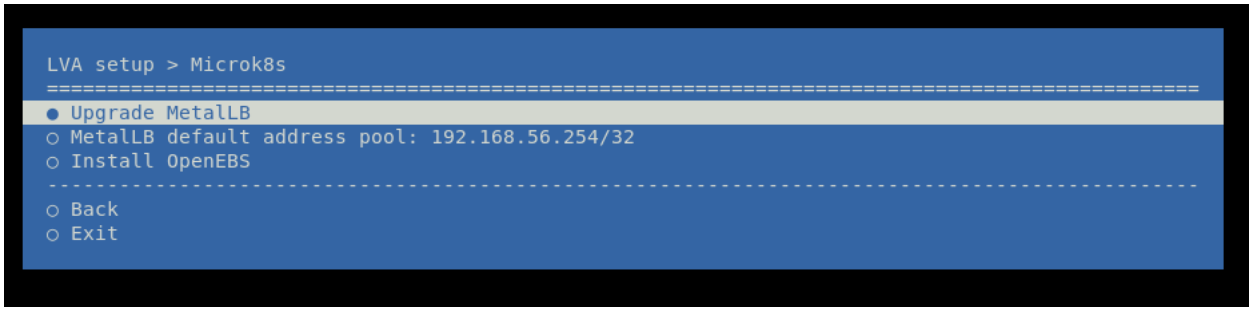
To install the MetalLB load balancer please choose the **Install MetalLB** option



For initial installation, it will scan the physical network interfaces on the machine and suggest the IP for the Load Balancer default address pool. For a single node installation where the load balancer is the same as the main network interface address, this is a sensible option. For an HA setup, you would want to change this to an appropriate virtual IP address on the network.

NOTE: a valid IP/CIDR must be entered.

Once it has completed, you are returned to the Microk8s menu where you can see the CIDR value of the default address pool which you just set in a new menu item.

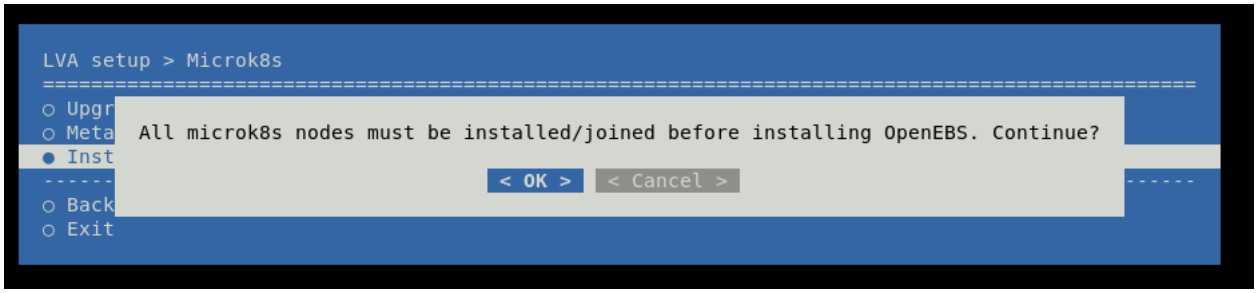


You can return to this menu entry to change the MetalLB address pool if you need to.

OpenEBS

Before you proceed to install anything else, you need to install OpenEBS.

NOTE: If you are installing a multi-node cluster it is important that you have installed and joined all Microk8s nodes *before* installing OpenEBS



Ingress

After you have installed OpenEBS, a menu option will appear which allows you to install the main cluster ingress.

```
LVA setup > Microk8s
==========================================================================================
○ Upgrade MetalLB
○ MetalLB default address pool: 192.168.56.254/32
○ Upgrade OpenEBS
● Install ingress
○ Install Loki/Grafana
------------------------------------------------------------------------------------------
○ Back
○ Exit

Installing Ingress
```

Loki/Grafana

A menu option will also appear which allows you to install the Loki/Grafana logging system.

```
LVA setup > Microk8s
==========================================================================================
○ Upgrade MetalLB
○ MetalLB default address pool: 192.168.56.254/32
○ Upgrade OpenEBS
○ Upgrade ingress
● Install Loki/Grafana
------------------------------------------------------------------------------------------
○ Back
○ Exit

Installing Loki
Pulled: bdhpcr.azurecr.io/charts/loki-stack:2.14.12
Digest: sha256:a414f5b81d8d39d7c3f85d28fae562aec0e6959921456f9c5bfacfa37e272658
secret/platform-onprem-install-values-loki created
Running: helm upgrade --install loki oci://bdhpcr.azurecr.io/charts/loki-stack:2.14.12
Release "loki" does not exist. Installing it now.
```

Databases

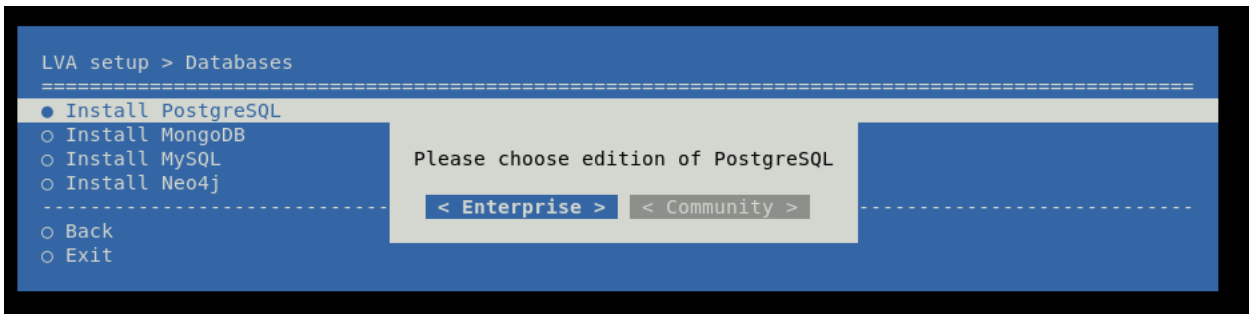
This menu item allows you to install and upgrade databases. You have an option for each supported database type.

Release Status:Issued and Effective

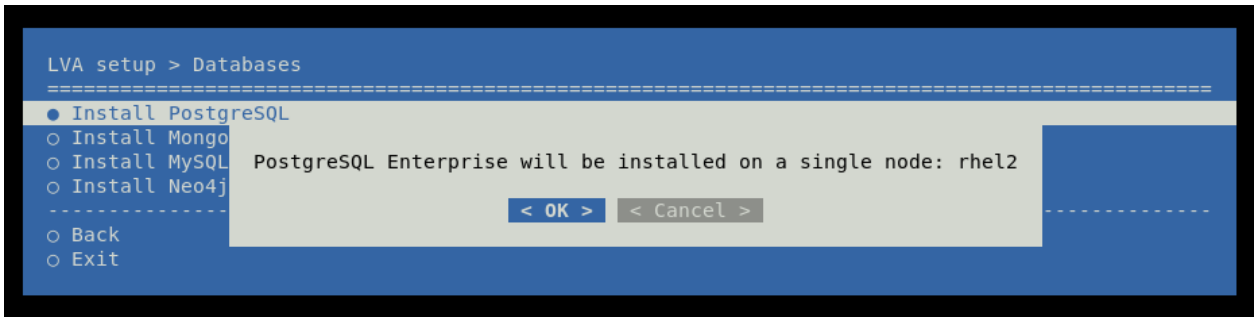
Once the necessary partitioning has been done, you can proceed.

Installing

For a single node, if there is a choice of Enterprise or Community editions (PostgreSQL and MySQL) you will be asked to choose at this point.



There will follow a confirmation of your choice of edition and upon which nodes it will be installed.



Once installation has completed, you will be returned to the Databases menu.

By default, Postgres is configured based on an assumption that 2 GB of memory will be available (a quarter of this is reserved for shared buffers) and 100 connections. This configuration is designed for use where the majority of data processing is being done on MongoDB. It is not an optimal configuration where Postgres is being used for heavy data processing / reporting so the installation will output a warning if it detects that the memory limits should be reviewed. This will happen in the following situations:

- The node does not have MongoDB storage provisioned. In this case it is likely that 8 GB of memory is available for use by Postgres.
- Multi-node cluster. In this case it is likely that at least 16 GB of memory can be used by Postgres

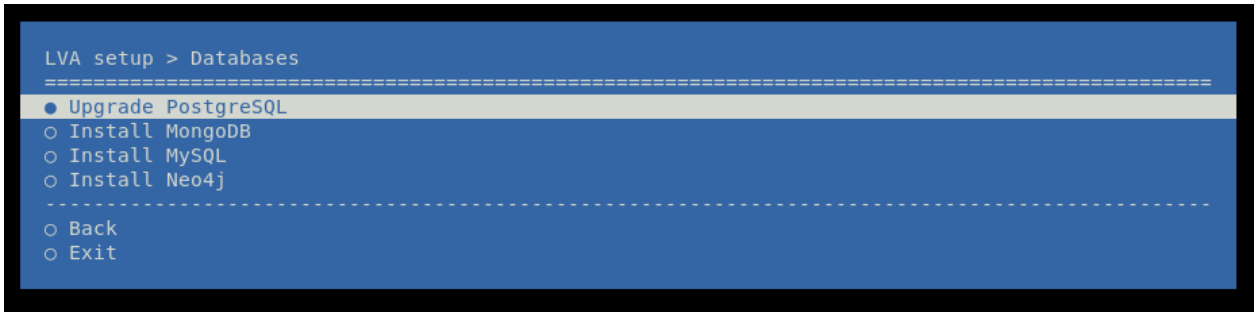
Release Status:Issued and Effective

(although it is only recommended to provision this much memory if Postgres will be hosting large databases).

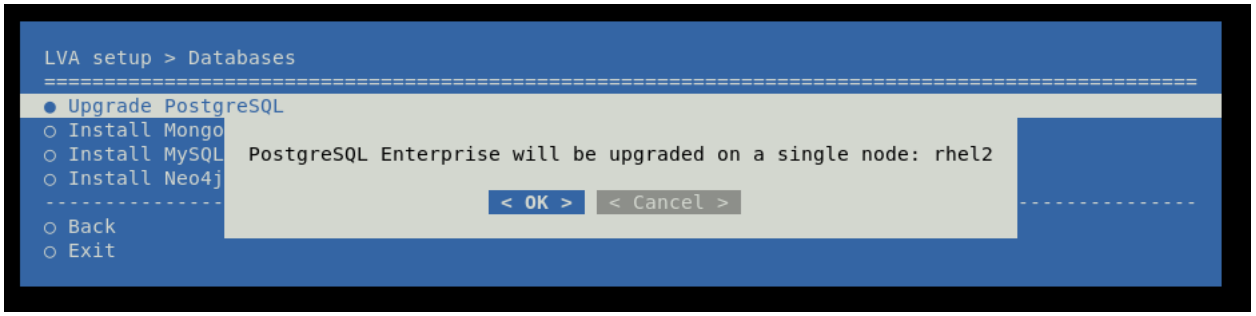
It is not currently possible to boost the memory or the connections via the interactive setup. This can be done subsequently by running **lva install-database --available-memory=<available-memory> --max-connections=<max-connections>**

Upgrading

For databases which are already installed, the menu item changes from **Install <Database>** to **Upgrade <Database>**



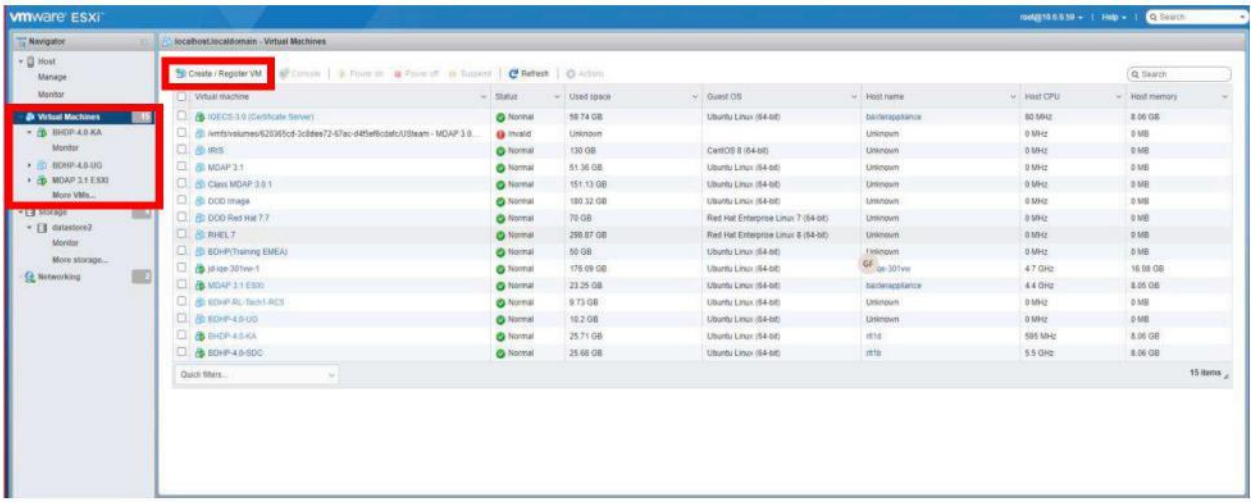
You can select this option to upgrade your chosen database. By default it will upgrade the helm chart to the same version, but with subsequent upgrades of the LVA, the version will change over time when upgradeable versions are available.



E. Hypervisor installation of a Linux Virtual Application image

The guide below details how to import an OVA image on the VMware ESXI server. For information on other hypervisor imports please visit [Hypervisor Installation - BDHP LVA Handbook (v7) - Confluence (atlassian.net)]

Release Status:Issued and Effective

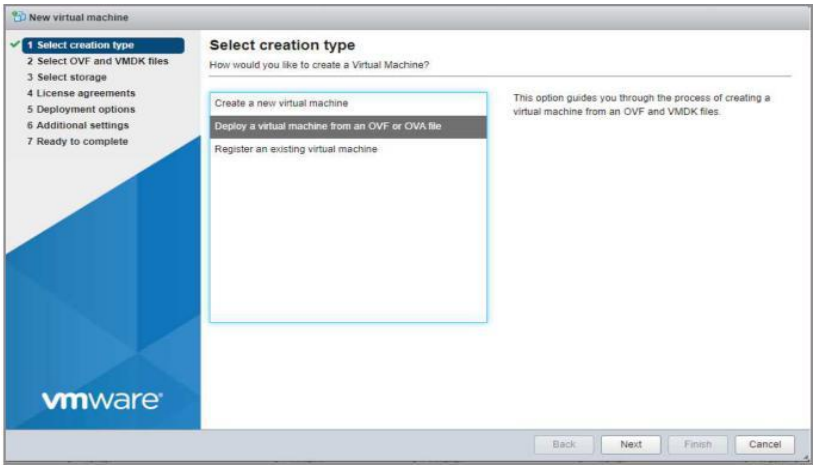


Log on to the virtual machine environment.

In the Navigator pane on the left side, click **Virtual Machines**.

In the Virtual Machines pane on the right side, click **Create / Register VM**.

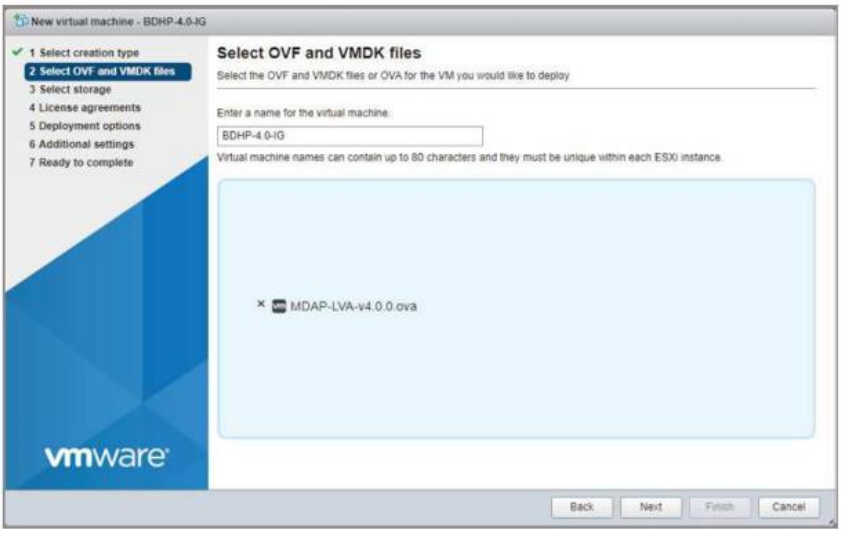
The New virtual machine dialog opens.



On the Select creation type page:

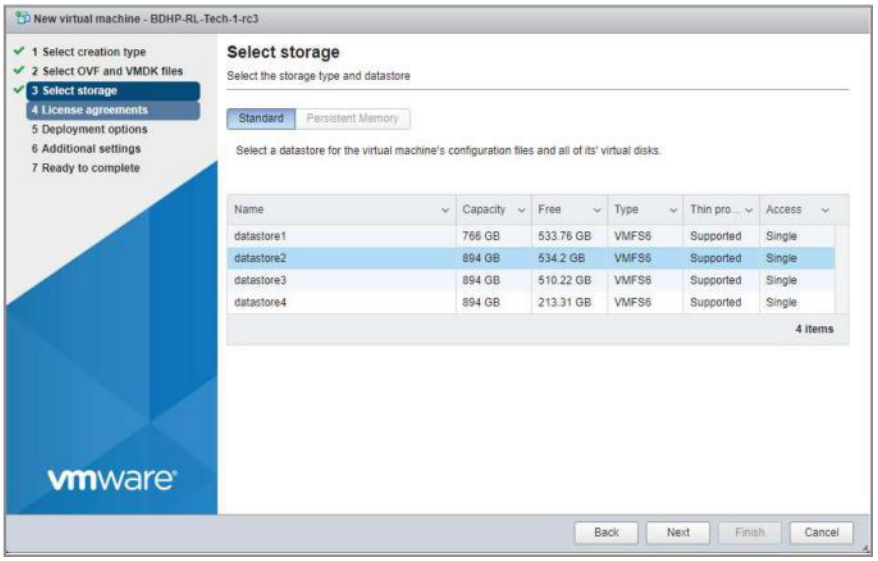
a. Select **Deploy a virtual machine from an OVF or OVA file**.

b. Click **Next**.



On the Select OVF and VMDK files page:

a. Enter a name for the virtual machine.
b. Click the center of the screen and select the desired OVA image. **OR** drag and drop the desired OVA image onto the center of the screen.
c. Click **Next**.

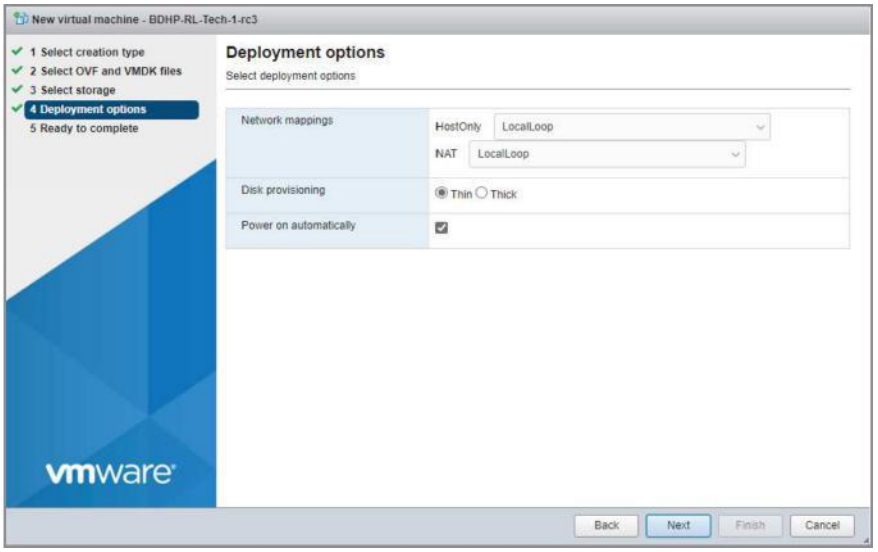


On the Select storage page:

a. Click a datastore with sufficient space for the install. Refer to the server requirement for installation needs.

NOTE Some servers may only have one datastore.

b. Click **Next**.



On the Deployment options page:

a. For Network mappings, select the desired **HostOnly** and **NAT** options.

> **NOTE:** For installation in our lab, use the **VM Network** setting. For customer installations, these options will have different names.

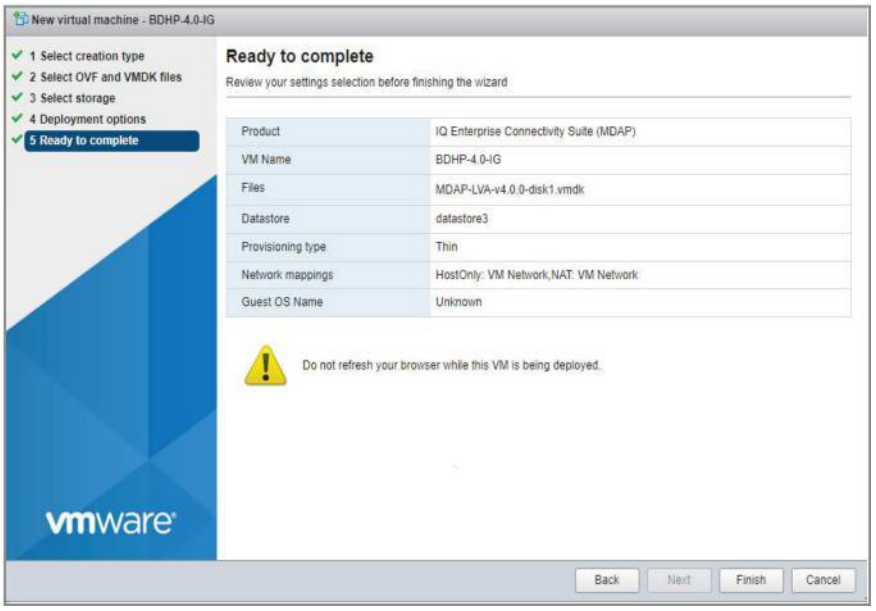
b. For Disk provisioning, select **Thin** or **Thick**.

> **NOTE:** For production installs at customer sites, **Thick** is strongly recommended. **Thin** is acceptable for non-production installs and for conserving drive space.

c. Ensure the **Power on automatically** checkbox is selected.

d. Click **Next**.

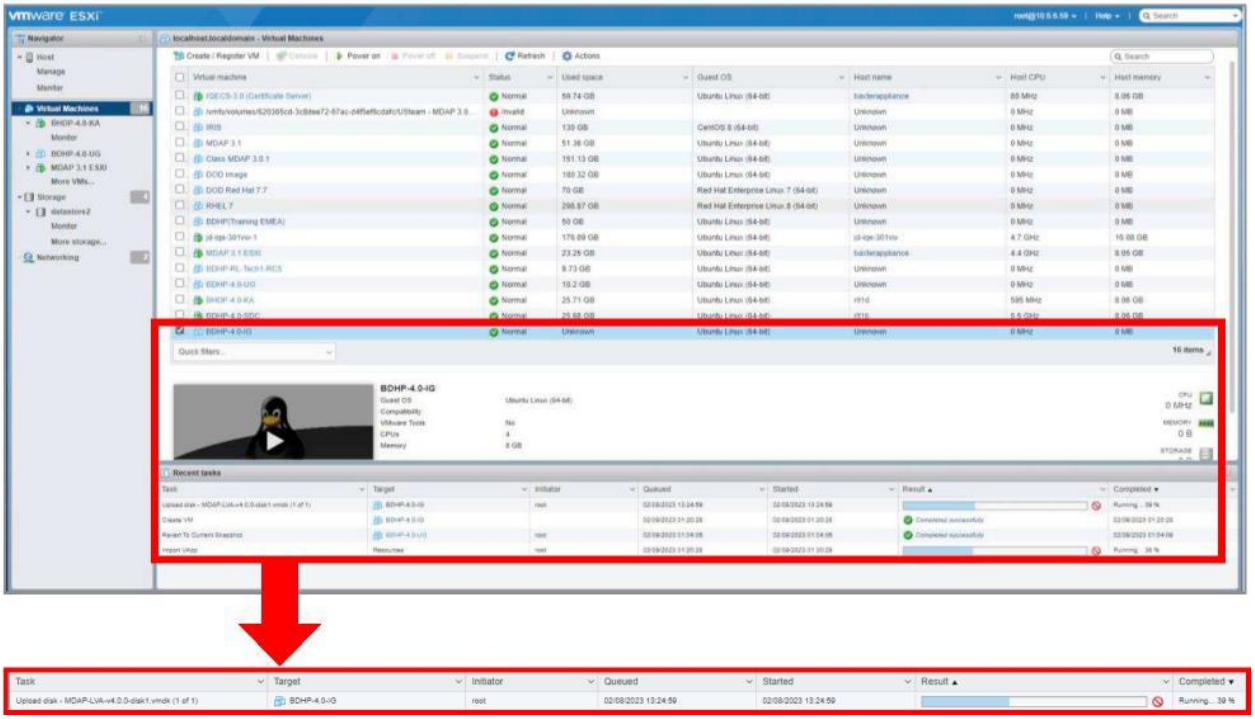
Release Status:Issued and Effective



On the Ready to complete page:

a. Verify the selections.

b. Click **Finish**.



The new VM appears at the bottom of the Virtual machine list on the right side, and a new task for uploading the disk appears in the Recent tasks list.

Wait until the new Task shows Completed successfully in the Result column before proceeding to the next section.

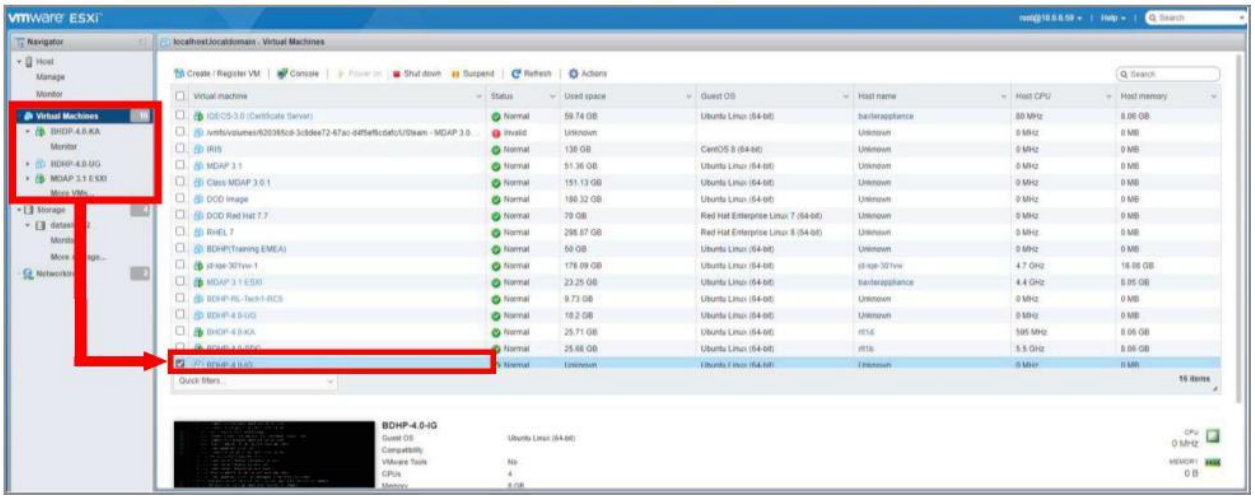
Add an Additional Hard Drive to a VMWare ESXI Server

Prerequisite

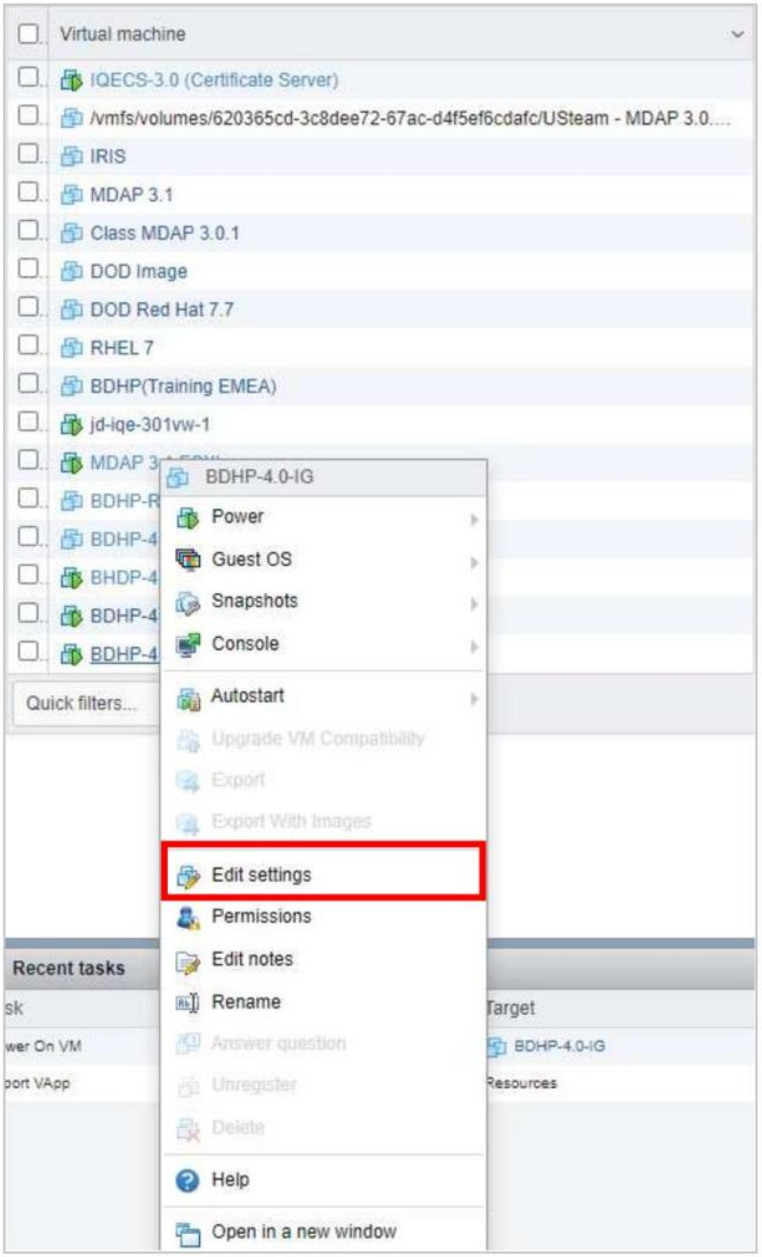
This version of BDHP requires adding four additional hard drives, which are not included in the OVA or VHD images. These drives will be used for the following:

- Microk8s
- Postgres Database Storage
- Backup Database Storage
- Mongo Database Storage

NOTE: Customer IT staff should perform this task. Reach out to Customer if any of these four drives are not there.



1. Under Virtual Machines on the left side, click the VM's name.
   If the VM isn't listed under Virtual Machines:
   a. Click **More VMs...**
   b. In the Virtual Machines pane on the right side, right-click the VM's name.

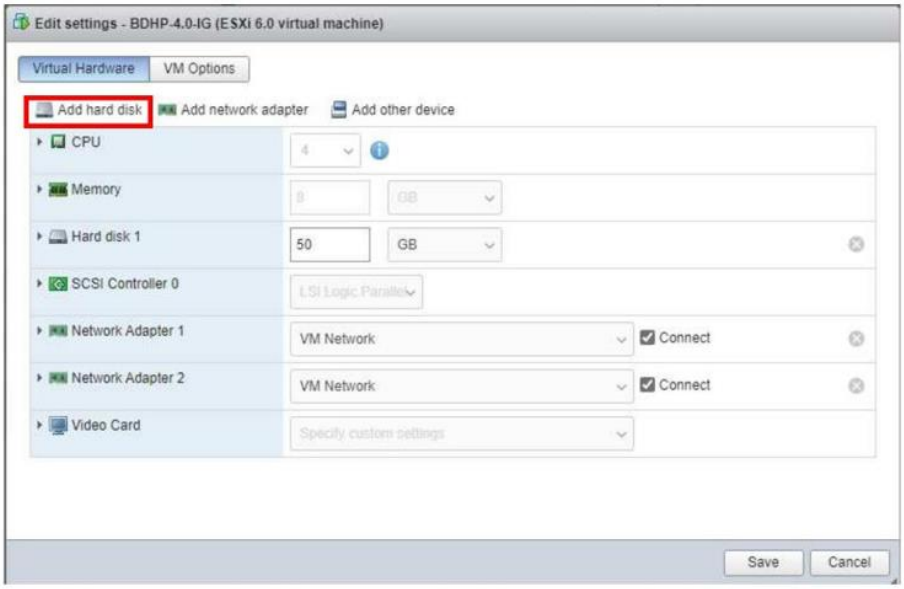


Click **Edit Settings**.

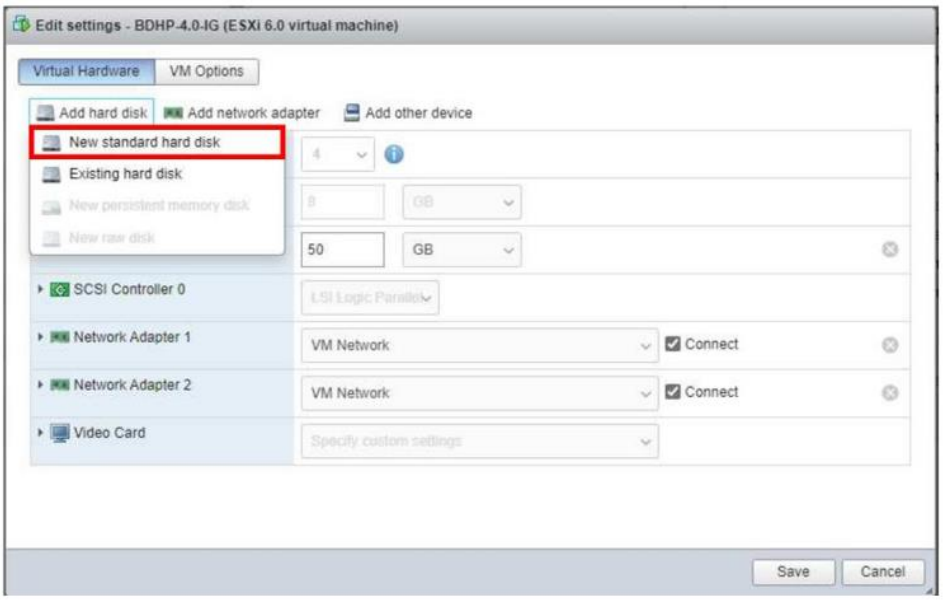
Add the Microk8s Drive

NOTE: This task requires an extra attached drive for application images.

Release Status: Issued and Effective

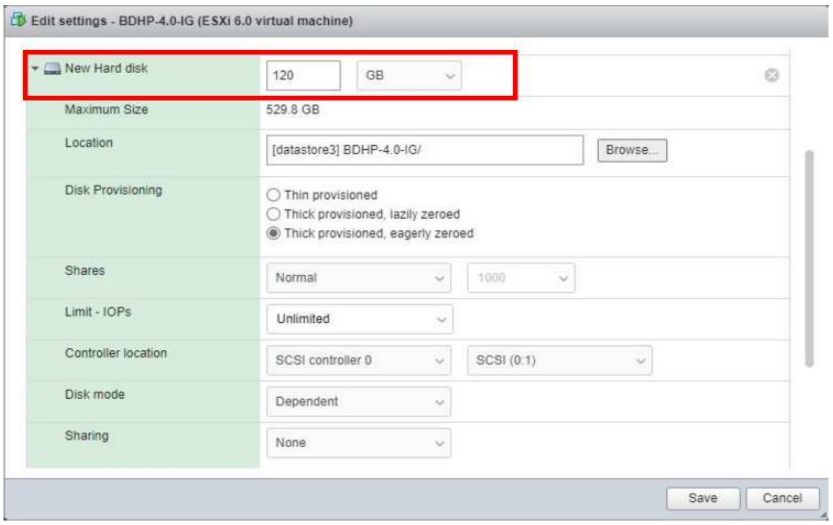


1. On the Edit settings dialog, click **Add hard**



2. On the pop-up menu, click **New standard hard disk.**

Release Status:Issued and Effective



3. Set the New Hard disk size to **120 GB**.

4. Click the arrow to expand the **New Hard disk** menu.

5. Select the desired Disk Provisioning option.

NOTE: Encourage the customer to select **Thick provisioned eagerly zeroed**. See *Disk Provisioning* for more information and supported productionsettings.

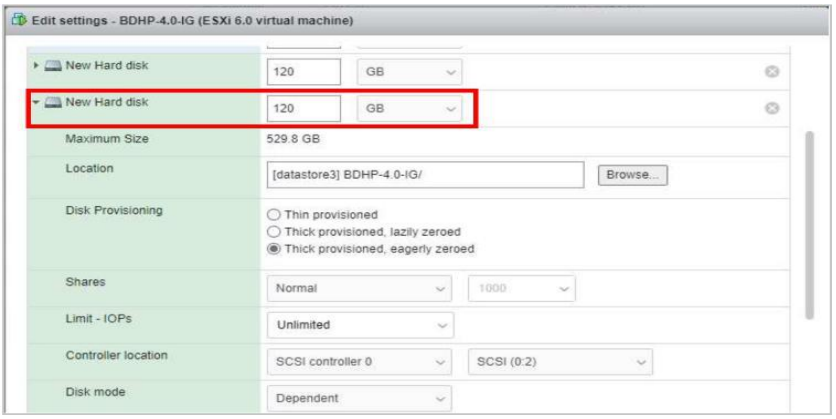
Keep the default values for **Shares**, **Limit – IOPs**, **Controller location**, and **Disk mode**.

Add the Postgres Drive

NOTE This task requires an extra attached drive for application images

1. At the top of the Edit settings dialog, click **Add hard disk**.

2. On the pop-up menu, click **New standard hard disk**.



3. For this New Hard disk size, consult the server requirements for the guest application being installed. Minimum value must exceed **100 GB**.
4. Click the arrow to expand the **New Hard disk** menu.
5. Select the desired Disk Provisioning option.

NOTE: Encourage the customer to select **Thick provisioned eagerly zeroed**.

See *Disk Provisioning* for more information and supported production settings.

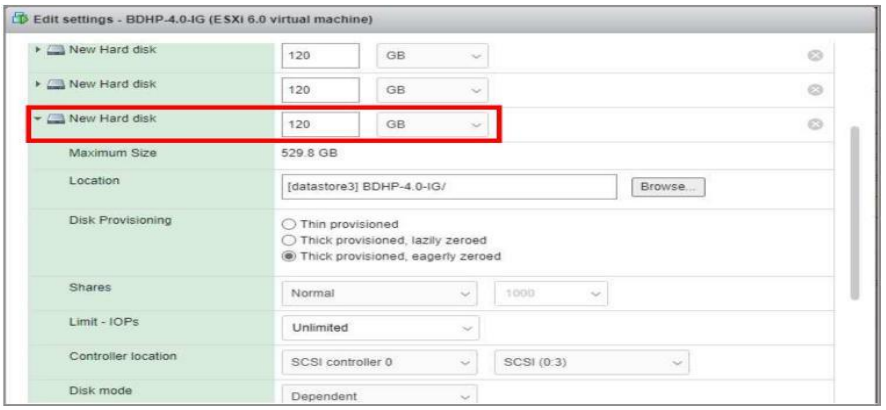
Keep the default values for **Shares**, **Limit – IOPs**, **Controller location**, and **Disk mode**.

Add the Database Backup Storage Drive

NOTE This task requires an extra attached drive for application images

1. At the top of the Edit settings dialog, click **Add hard disk**.

2. On the pop-up menu, click **New standard hard disk**.

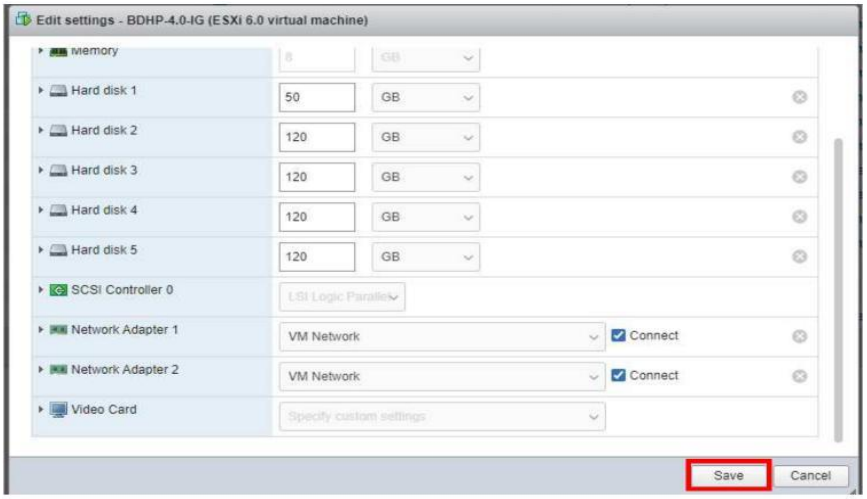


3. For this New Hard disk size, consult the server requirements for the guest application being installed. Minimum value must beat least 60% of all database drive sizes and exceed **100 GB**.
4. Click the arrow to expand the **New Hard disk** menu.
5. Select the desired Disk Provisioning option.

NOTE: Encourage the customer to select **Thick provisioned eagerly zeroed**. See *Disk Provisioning* for more information and supported productionsettings.

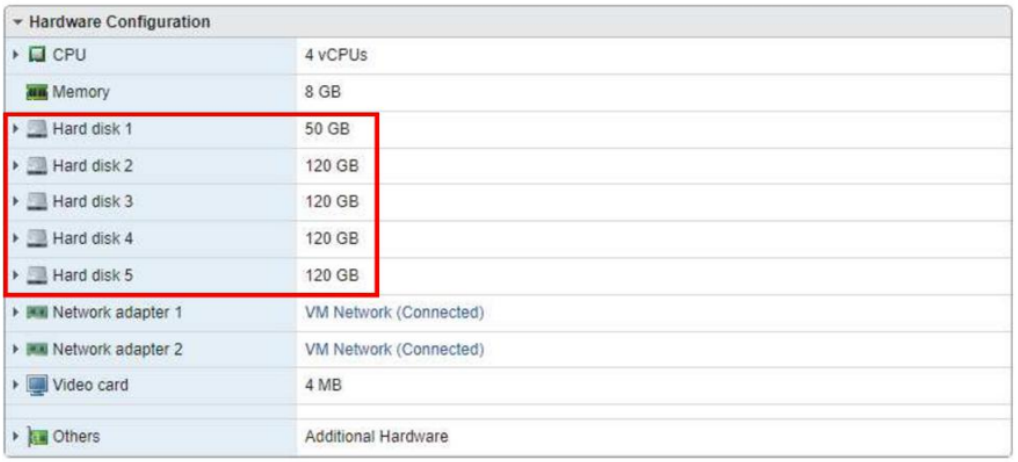
Keep the default values for **Shares, Limit – IOPs, Controller location, Disk mode**, and **Sharing**.

Verify Addition of Four Drives to the VMWare EXSI Server



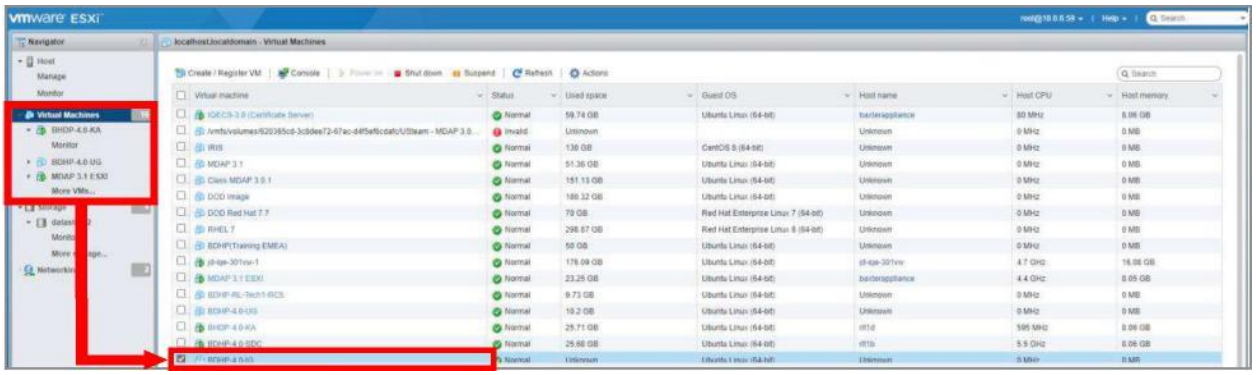
To complete the addition of all four drives to the VMWare ESXI server, click **Save**

Release Status:Issued and Effective



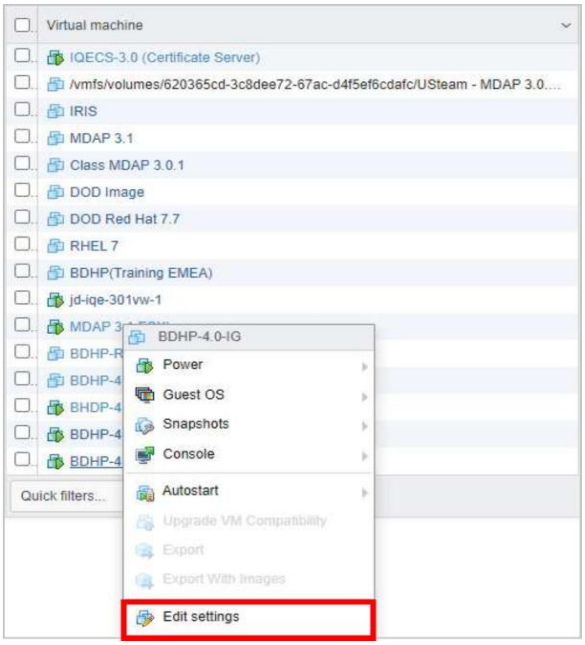
Hard disks 1-5 now appear under **Hardware Configuration**.

Remove the Second Network Adapter



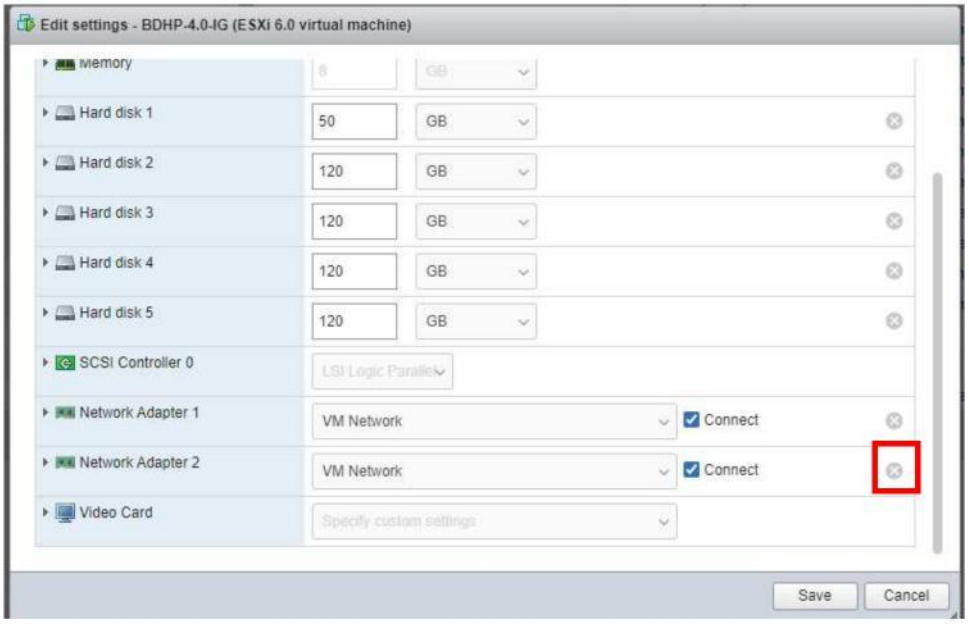
1. Under Virtual Machines on the left side, click the VM's name.
   If the VM isn't listed under Virtual Machines:
   a. Click **More VMs...**
   b. In the Virtual Machines pane on the right side, right-click the VM's name.

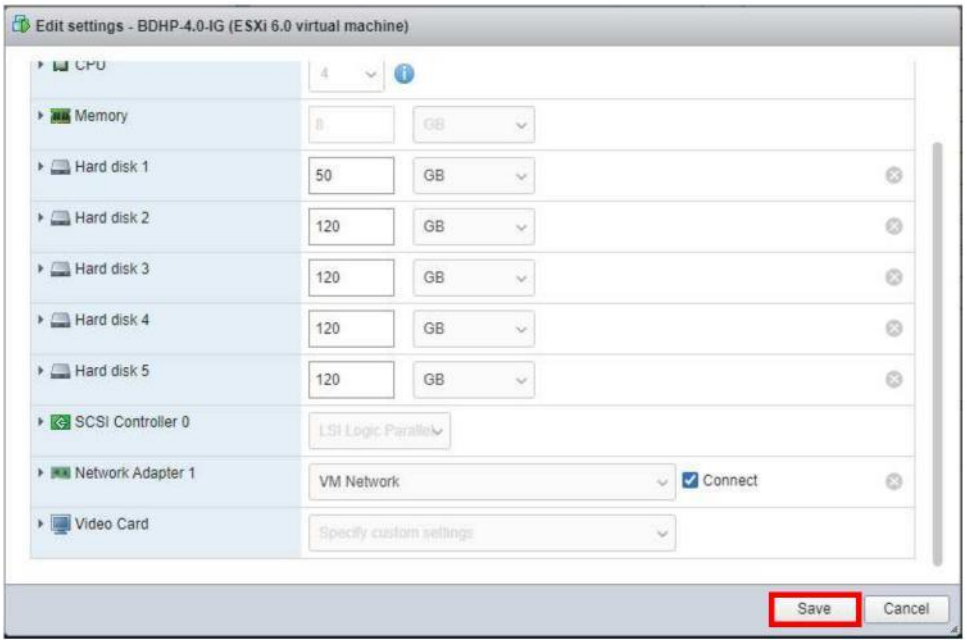
Release Status: Issued and Effective



2. Click **Edit Settings**.

Release Status:Issued and Effective





3. Click **Save.**

NOTE: The customer should take a snapshot (backup) of the VM at this

Release Status:Issued and Effective

Release Status:Issued and Effective

F. License information for MySQL

Both Postgres and MySQL Enterprise require licensing to ensure compliance and access to support services.

Activation and Usage

MySQL Enterprise does not require an activation key for use. Instead, customers are required to report their need for MySQL Enterprise to Oracle. A License must be obtained, and a unique Customer Support Identifier (CSI) number is generated for each customer. This CSI number serves as a reference during any support-related interactions.

Licensing Structure

The licensing structure for MySQL Enterprise is based on the configuration of the nodes, whether they are running in VMs or on physical servers. The following guidelines outline the licensing requirements:

Nodes Running in VMs:

VMs with 16 vCPUs or fewer require 1 license per VM.

VMs with more than 16 vCPUs require 2 licenses per VM.

Physical Servers:

Servers with 4 or fewer sockets require 1 license per physical server.

Servers with more than 4 sockets require 2 licenses per physical server.

Reference Use Cases:

MySQL EnterPrise License Options						License Count
1	Use Case1	VM	Single Node Cluster	Less than or Equal to 16 vCPU	1 License Per VM	1
				Greater than 16 vCPU	2 License Per VM	2
2	Use Case 2	VM	6 Node HA Cluster	Less than or Equal to 16 vCPU	1 License Per VM	6
				Greater than 16 vCPU	2 License Per VM	12
3	Use Case 3	Physical Server	3 Node Hypervisior Cluster	Less than or Equal to 4 Sockets	1 License Per Machine	3
				Greater than 4 Sockets	2 License Per Machine	6

G. BDHP installation variables

Background

This page records the variables that may be set on installation/upgrade of the MDAP platform chart (**mdap**).

Any of these keys may be passed as **--set** arguments on commands which install or upgrade the platform:

- **lva platform:install**
- **lva upgrade** on the "mdap" chart

Settings can be placed into a YAML file and pass these in using the -f or --values argument.

This is the recommended way - especially if there is a large number of --set options.

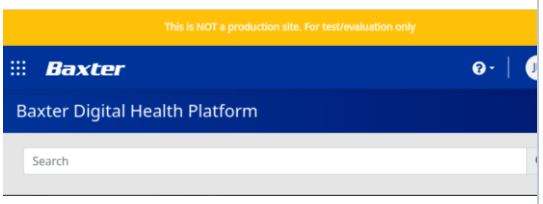
```
--set=stringarray
  Helm install values. You can specify multiple or separate values with commas:
section1.key1=val1,section1.key2=val2
  If you are specifying a string value which includes commas, these should be escaped by a
backslash.
  e.g. --set "ip.ranges=10.0.0.0/8\,172.16.0.0/12\,192.168.0.0/16"
  Arrays can be specified using their indices.
  e.g. --set "mdap-ntpd.deny[0]=10.0.0.1/32,mdap-ntpd.deny[1]=10.2.0.0/2"
  To set a value to an empty string, you should use 2 single quotes.
  e.g. --set "my.string=''"
-f|--values=path
  YAML file containing helm install values
```

Global

These variables are set at a global level and are inherited by all dependencies of the master helm chart.

Key	Description	Notes
global.database.vendor	Relational database type used for the core platform installation	Possible values: "postgresql", "mysql" or "sql-server" This is set automatically by the **--database** argument passed to the l**va** platform:install script
global.domain	Fully Qualified Domain Name of the installation	This is set automatically by the **--domain** argument passed to the l**va** platform:install script
global.customer.name	Human readable name of customer	This can be passed into the **platform:install** s

Release Status:Issued and Effective

Key	Description	Notes
		cript using the **--customer** argument
global.customer.live	Indicates whether the platform installation can be can considered the customer's live site. The context is that for most on-premise installations there will be, at a minimum, 2 installations of the software. One with User Acceptance Testing/Live Staging data and another which is the true *live* site with *real* patient data. The requirements state that we need to make it very clear that when a customer is looking at a site with test data they do not, under any circumstances, use it to influence the decision making on real patients. If this *isn't* set to **true** the UI of the software will display a prominent banner at the top of every page like below. 	**true/false** - default **false**
global.customer.country	Constrains the list of available platform locales to only be in the country of deployment. Must be a valid 2-letter country code representing a country supported by the platform (invalid codes will be ignored). AE - United Arab Emirates AT - Austria AU - Australia	

Release Status:Issued and Effective

Key	Description	Notes
	BE - Belgium BR - Brazil CA - Canada CH - Switzerland CN - China CO - Columbia CZ - Czechia DE - Germany DK - Denmark DO - Dominican Republic EG - Egypt ES - Spain FI - Finland FR - France GB - United Kingdom GR - Greece HK - Hong Kong IE - Ireland IL - Israel IT - Italy MA - Morocco MX - Mexico NL - Netherlands NO - Norway NZ - New Zealand OM - Oman PL - Poland PR - Puerto Rico PT - Portugal QA - Qatar SA - Saudi Arabia SE - Sweden SG - Singapore TH - Thailand US - United States of America ZA - South Africa	

SMTP

NOTE: It is **essential** that the platform is connected to a suitable SMTP relay so that it can send email to users as part of the Single Sign-On system

Configuration details are stored in the **platform-shared-smtp-secret** which is available to guest applications.

It is also used as the SMTP configuration for Keycloak. This is important as Keycloak needs

to send email to users about things like forgotten passwords and new registrations.

Key	Description	Notes
smtp.host	SMTP host name	**Required**
smtp.port	SMTP port	**Required**
smtp.from	SMTP from email address	**Required**
smtp.from_display_name	SMTP from display name	Default: "DeviceBridge"
smtp.reply_to	SMTP reply to email address	Optional - if a different address is needed in the reply to field from the **from** address
smtp.reply_to_display_name	SMTP reply to display name	Optional - if a different address is needed in the reply to field from the **from** address
smtp.envelope_from	SMTP envelope from email address	Optional – If there is a need for a designate a different mailbox to receive email bounces
smtp.ssl	SSL enabled	**true/false -** this must always be enabled in a production context
smtp.starttls	StartTLS enabled	**true/false**
smtp.username	SMTP username	For SMTP authentication
smtp.password	SMTP password	For SMTP authentication

For testing inside the *Baxter* network, use the following relay

```
--set 'smtp.host=relays.baxter.com,smtp.port=25,smtp.from=no-reply@baxter.com,smtp.ssl=false'
```

These values **MUST NOT** be used in production

Tags

By default, the platform installs with a minimal "core" set of services for single sign-on and a relational database.

- Keycloak
- IQECS (the platform UI dashboard, the "MDAP API" and the Language and Manuals Library service)

Release Status:Issued and Effective

Depending on which guest applications you wish to install, you will need to add support for common services they need. These common services have been put into sets which are identified by tags.

Any of the tagged sets of applications are activated by appending **--set tags.<tagname>=true** to an install or upgrade command - e.g.

```
# Install the platform with all required services for bed devices
lva platform:install <version> --set tags.beds=true -n <namespace>
```

Note: red ticks ✓ denote changes since 4.3

EMR integration and Mirth have been added under the "cdr" tag. Also the wa-vitals tag has been removed as the WACP listener used by Baxter monitoring devices has become a separate installable guest application.

		Tags			
Category	**Service**	**cdr**	**beds**	**manual-adt**	**pumps**
Device connectivity	Bed Device Gateway (BDG) and Engine + Redis BDG cache		✓		
	VerneMQ for beds		✓		
	VerneMQ for infusion pumps				✓
Messaging	RabbitMQ	✓	✓	✓	✓
Mirth	Mirth Connect + Redis Mirth cache	✓	✓		✓
Configuration	Enterprise Configuration Portal (ECP) + Catalog service (backend)	✓	✓	✓	
CDR	CDR FHIR services • Communication • Device • Encounter • Location • Observation • Patient • Practitioner + Publisher (sends data to RabbitMQ)	✓	✓	✓	

	+ Redis shared cache				
EMR integration	From Mirth to CDR • ADT service • EMR service From RabbitMQ to Mirth • Alarm reporter service • HL7 outbound service • Vitals outbound service + Mirth channels for EMR (Enterprise Gateway) + Terminology service (translates codes for EMR)	✓	✓		
Non-EMR integration	Manual ADT service			✓	

Pumps

```
--set tags.pumps=true
```

To install infusion pump related applications set the *pumps* tag. This will install RabbitMQ and VerneMQ with pump connectivity. Also (new in BDHP 4.3), it will install Mirth.

If configuring both tags.pumps and tags.bed as true, Configure the service to use a different port (the alternative is to create another IP address - see reference 'Additional Virtual IP for VerneMQ') The recommended alternative port for pumps is 8884.

```
--set 'vernemq.service.mqtts.port=8884'
```

Beds

```
--set tags.beds=true
```

If the beds need device gateway set the *beds* tag. This will install RabbitMQ and VerneMQ with beds connectivity. It will also install the CDR services.

CDR (Clinical Data Repository)

```
--set tags.cdr=true
```

Release Status:Issued and Effective

This tag is for customers who require the CDR (Clinical Data Repository) and EMR integration but do not need device connectivity such as beds.

Manual ADT

```
--set tags.manual-adt=true
```

For installations where there is no EMR integration, install the platform with Manual ADT support. This also installs CDR services (without *Mirth)* and RabbitMQ.

Additional configuration

In addition to the tags above, the following configuration options are available to fine tune the installation.

Keycloak

Key	Description	Notes
keycloak.okta.client_id	OKTA client ID	For connecting the system up to the Baxter Single Sign-On system Baxter users connecting via OKTA will get user, platform and application management permissions in IQECS and administrative rights in the Keycloak admin console
keycloak.okta.client_secret	OKTA client secret	
keycloak.okta.base_url	Base URL of the OKTA installation	e.g. **https://iam.baxter.com**
keycloak.okta.hide_on_login_page	Hides the Baxter SSO link on the login page for the MDAP realm	This is set to **true** by default. Baxter employees can get to the SSO by navigating to https://fqdn.of.system**/mdap/mdap/baxter/login**
keycloak.okta.disable_master_login	If OKTA is configured this disables the standard browser login screen for the Keycloak admin console - thus making the OKTA identity provider the only route by which it is	This is set to **true** by default

Release Status:Issued and Effective

Key	Description	Notes
	possible to log in to the admin console. Instead it will always redirect to OKTA making this the only available authentication route.	

VerneMQ (for Beds)

Key	Description	Notes
bdhp-vernemq.metallb.addresspool.cidr	Sets the CIDR IP address of a separate virtual IP address on the Load Balancer	**New functionality in 4.4** This creates a new IpAddressPool in metallb-system namespace which is distinct from the default address pool. Needs to be a full CIDR address - e.g. 10.100.67.100/32 See Additional Virtual IP for VerneMQ

VerneMQ (for Pumps)

Key	Description	Notes
bdhp-vernemq-pumps.metallb.addresspool.cidr	Sets the CIDR IP address of a separate virtual IP address on the Load Balancer	**New functionality in 4.4** This creates a new IpAddressPool in metallb-system namespace which is distinct from the default address pool. Needs to be a full CIDR address - e.g. 10.100.67.100/32 See Additional Virtual IP for VerneMQ
bdhp-vernemq-pumps.service.mqtts.port	Sets the port on which Verne MQ listens for incoming connections	*This is an alternative to allocating a different address pool on the LB for VerneMQ* integer default = **8883**

Release Status:Issued and Effective

Key	Description	Notes
		When the platform is configured with both bed and pump support, the verne for pumps service may be configured to use a different port.

Release Status:Issued and Effective

ClamAV

Key	Description	Notes
clamav.enabled	Disables ClamAV service	default = **false** Some on-premise customers may disable outside internet which means that ClamAV cannot get updated anti-virus definitions. In this scenario we would need to disable the service.
clamav.freshclam.mirror1	First mirror ClamAV will try for AV definitions updates	Default: "**us.platform.baxter.com/clamavmirror**"
clamav.freshclam.mirror2	Second mirror ClamAV will try	Default "**database.clamav.net**"
clamav.freshclam.mirror3	Third mirror ClamAV will try	Default ""

NTPD

Key	Description	Notes	Examples
bdhp-ntpd.enabled	Turns the ntpd for pumps on/off	**true**/**false** - default **false**	
bdhp-ntpd.nts.enabled	Enabled the use of NTS using certificates for devices (This	true/false - default false	

Key	Description	Notes	Examples
	requires the bdhp-ntpd.enabled to be set to true) Certificates need to be installed into the secret ntp-nts-certificates as tls.key and tls.crt in x509 format		
bdhp-ntpd.servers	IP or FQDN of a single NTP source server, multiple servers can be assigned. The values are entered using the environment as an array [0] **bdhp-ntpd.servers[0]=ntp.ubuntu.com**	default **ntp.ubuntu.com**	This is how to set an array of two by incrementing the array value for each server required and then comma separated **bdhp-ntpd.servers[0]=ntp.ubuntu.com,mdap-ntpd.servers[1]=ntp.debian.com**
bdhp-ntpd.pools	The pool name is expected to resolve to multiple addresses, multiple pools can be assigned. The values are entered using the environment as an array [0] The pool **ubuntu.pool.ntp.org** will use **1.ubuntu.pool.ntp.org** and **2.ubuntu.pool.ntp.org**	default **NA**	This is how to set an array of two by incrementing the array value for each server required and then comma separated **bdhp-ntpd.pools[0]=ubuntu.pool.ntp.org, bdhp-ntpd.pools[1]=ntp.debian.pools.com**
bdhp-ntpd.allow	CIDR Addresses of allowed network devices, multiple CIDR ranges can be assigned. The values are entered using the environment as an array [0] **bdhp-ntpd.allow[0]=0.0.0.0/0**	default **0.0.0.0/0**	This is how to set an array of two by incrementing the array value for each server required and then comma separated **bdhp-ntpd.allow[0]=0.0.0.0/0, bdhp-ntpd.allow[1]=10.0.0.0/24**
bdhp-ntpd.deny	CIDR Addresses of denied network devices, multiple CIDR ranges can be assigned. The values are entered using the environment as an array [0]	default **NA**	This is how to set an array of two by incrementing the array value for each server required and then comma separated **bdhp-ntpd.deny[0]=10.0.0.1/32, bdhp-ntpd.deny[1]=10.2.0.0/24**

Release Status:Issued and Effective

Linkerd

Linkerd is a service mesh for kubernetes

Key	Description	Notes
linkerd.enabled	Turns the linkerd service mesh on/on	**true/false** - default **false**
linkerd.identity.issuer.tls.keyPEM	Issuer certificate (ECDSA). It must be provided during install	You do not need to set this as the **lva platform:install** command will automatically generate this when *linkerd.enabled=true*
linkerd.identity.issuer.tls.crtPEM	Key for the issuer certificate (ECDSA). It must be provided during install	You do not need to set this as the **lva platform:install** command will automatically generate this when *linkerd.enabled=true*
linkerd.identityTrustAnchorsPEM	Trust root certificate (ECDSA). It must be provided during install	You do not need to set this as the **lva platform:install** command will automatically generate this when *linkerd.enabled=true*

Monitoring

```
--set tags.monitoring=true
```

This installs a suite of diagnostic tools which accompany the installation, including *Prometheus.* The Metrics agent sends data to *Cumulocity* which is our cloud-based system for collecting data from customer installations. Setting the tag *monitoring* installs

- Metrics agent (sends data to *Cumulocity*)
- Prometheus
- Prometheus Blackbox exporter
- Prometheus PostgreSQL exporter

Additional configuration in this section is as follows:

Key	Description	Default	Notes
kube-prometheus-stack.prometheus-node-exporter.hostRootFsMount.enabled	Controls whether to disable host root file system mounting.	**true**	**true/false**
prometheus.enabled	Enables/disables *Prometheus*	**true**	**true/false**

Key	Description	Default	Notes
prometheus-blackbox-exporter.enabled	Enables/disables *Prometheus Blackbox Exporter*	**false**	**true/false**
prometheus-mysql-exporter.enabled	Enables/disables *Prometheus MySQL Exporter*	**true**	**true/false**
prometheus-postgres-exporter.enabled	Enables/disables *Prometheus PostgreSQL Exporter*	**true**	**true/false**
metrics.enabled	Enables/disables the metrics agent that sends data to Cumulocity	**true**	**true/false**

H. Example YAML files

Below is a yaml file that could be used during a platform installation or upgrade. This particular yaml file is considered a 'Comprehensive deployment' and would install all BDHP functionality.

Other example yaml files (such as a bed-only or pump-only installation) can be found in the handbook: Sample YAML install/upgrade files - BDHP LVA Handbook (v7) - Confluence (atlassian.net)

Release Status:Issued and Effective

Install-values.yaml

```
# Prepared for version 4.4 BDHP
#
# Version 1.0
#
# Includes FQDN and database
#
# This YAML represents a 'Comprehensive deployment' and so includes:
# Keycloak, IQECS, ClamAV, Bed Verne, pump verne, rabbit, SDC services, manual ADT (beds, pumps, vitals, manual ADT tags enabled)
#


## Main configuration section
## The core platform components are defined as 'tags'
tags:
  # For bed connectivity, set this to true
  beds: true

  # For pumps connectivity, set this to true
  pumps: true

  # For the CDR (Clinical Data Respository) set this to true
  cdr: true

  # For confirmed outbound services (e.g. vitals outbound service)
  confirmed-outbound: false

  # If Manual ADT (no connected EMR system, set this to true)
  manual-adt: false

  # Prometheus monitoring and Cumulocity
  monitoring: true

## Connect the platform to an appropriate SMTP server on the CUSTOMER network
## This is essential for Keycloak to email users with registration/forgotten passwords etc.
smtp:
  # SMTP details would  need to change to the CUSTOMER's SMTP setup,
  # SMTP host name - eg within Baxter the value would be relays.baxter.com
  # below is just a placeholder value that NEEDS CHANGING
  host: relays.customer.com
  # SMTP port
  port: 25
  # SMTP default from address. eg no-reply@baxter.com
  # below is just a placeholder value that NEEDS CHANGING
  from: no-reply@customer.com
  ## SMTP authentication
  # SMTP username
  username: ""
  # SMTP password
  password: ""
  # SSL enabled - this should ALWAYS be set to true on a customer network!
  ssl: false

## Customer set up
global:
  customer:
    # Human-readable name of customer. Setting this value saves users selecting their LOCALE.
    # below is just a placeholder value that NEEDS CHANGING
    name: customerName

    # Setting this to true removes the banner at the top of the UI which says "This is NOT a production site. For test/evaluation only"
    # This should be done on the production system, once the customer has 'gone live'
    live: false
```

Install-values.yaml

```
    # Country code constrains the list of available platform locales to those available in the country of deployment
    # Must be a valid 2-letter country code representing a country supported by the platform (invalid codes will be ignored).
    # AE - United Arab Emirates
    # AT - Austria
    # AU - Australia
    # BE - Belgium
    # BR - Brazil
    # CA - Canada
    # CH - Switzerland
    # CN - China
    # CO - Columbia
    # CZ - Czechia
    # DE - Germany
    # DK - Denmark
    # DO - Dominican Republic
    # EG - Egypt
    # ES - Spain
    # FI - Finland
    # FR - France
    # GB - United Kingdom
    # GR - Greece
    # HK - Hong Kong
    # IE - Ireland
    # IL - Israel
    # IT - Italy
    # MA - Morocco
    # MX - Mexico
    # NL - Netherlands
    # NO - Norway
    # NZ - New Zealand
    # OM - Oman
    # PL - Poland
    # PR - Puerto Rico
    # PT - Portugal
    # QA - Qatar
    # SA - Saudi Arabia
    # SE - Sweden
    # SG - Singapore
    # TH - Thailand
    # US - United States of America
    # ZA - South Africa
    # below is just a placeholder value that NEEDS CHANGING. Use a value from list above
    country: US

  # Fully Qualified Domain Name of the installation eg bdhp4-abc-01.stg.baxter.com
  # below is just a placeholder value that NEEDS CHANGING
  domain: bdhp.customer.com

  # Relational database type used for the core platform installation
  database:
    #By default, Keycloak uses a postgres backend. it is possible to change it to use mysql below. Only options are mysql and
postgresql
    vendor: postgresql
## VerneMQ pumps configuration
bdhp-vernemq-pumps:
  service:
    mqtts:
      # If installing both beds and pumps they connect via
      # 2 different VerneMQ services and so must use different ports.
      # If this is the case, change this to 8884 so it doesn't conflict
      # with the beds. NOTE another way to circumvent this issue is to create an additional IP address for pumps or beds to use.
      # port: 8883

## Platform Anti-virus service
clamav:
```


Release Status:Issued and Effective

Install-values.yaml

```
  # If the installation is offline (isolated from the internet) the system
  # cannot reach out for AV updates. If this is the case, please set this to false.
  enabled: true

## Platform NTP service
bdhp-ntpd:
  # Enable the NTP service
  enabled: true
```

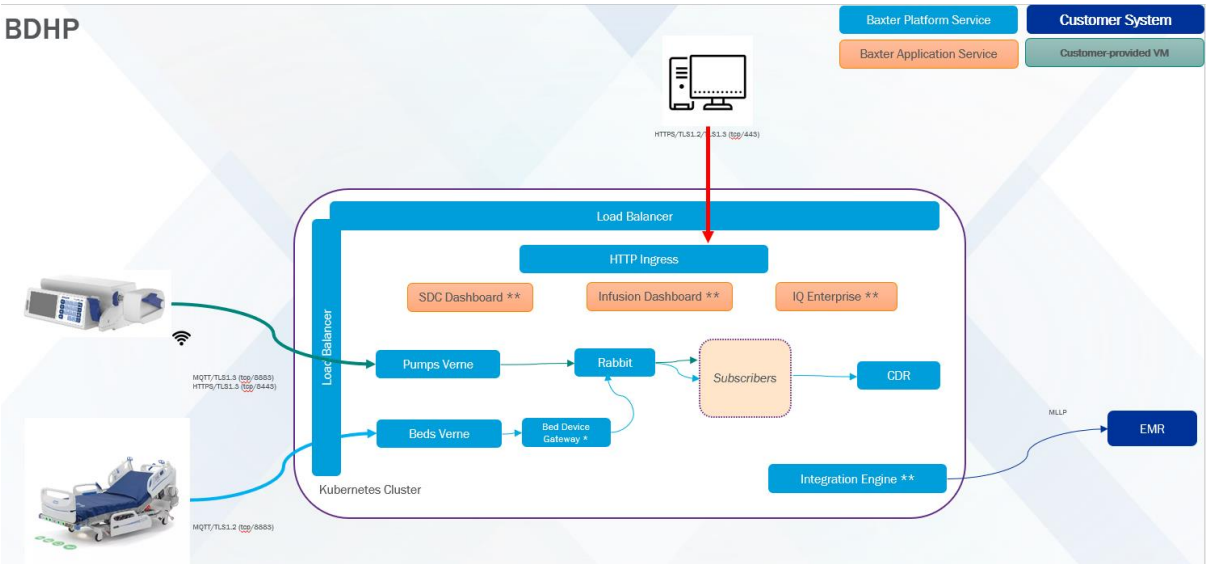
I. Certificates in BDHP

Termininology

- A Certificate authority (CA) is a trusted organization that signs and issues digital certificates for websites and other entities. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate

Digital Certificates are needed for secure connections when messages/requests pass across the load balancer of BDHP. Two sets of certificates are required at a BDHP installation:

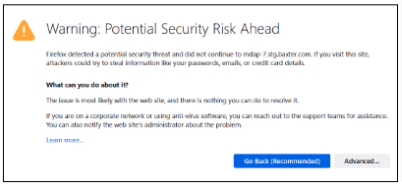
1. Ingress web certificates (red arrow below). These are requests from web browsers on the customer's network
2. Device certificates (green and blue arrows below). These are interactions between Baxter devices and BDHP

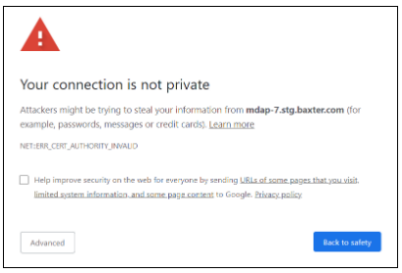


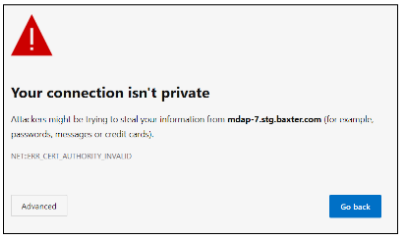
A key point to understand is that the client (either browser or device) only needs to trust the CA that has signed a certificate, rather than the certificate per se.

Ingress Web Certificates

Ingress certificates are needed for safely connecting inbound end-user web traffic to BDHP. By default, after BDHP installation, the ingress certificate is signed by the internal kubernetes Certificate Authority (CA). This certificate is untrusted outside of the Kubernetes cluster. As a result, end users will get undesirable browser warnings on connection, such as







Best practice is to replace the default ingress certificate with one signed by a CA trusted by the end-users' browser.
The customer's browser will already hold a CA certificate that will trust a valid certificate that has been signed by that *customer's* Certificate Authority.
Therefore, we need the *customer* to sign the ingress certificate; if it were signed by *Baxter CA*, the browser would not trust it.
For the ingress certificate to be considered valid by the browser, it must

1. Be valid in terms of its stated validity dates
2. The certificate's Common Name (CN) must match the FQDN (Fully Qualified Domain Name) of the BDHP. At a customer installation this would need to match the URL that end-users type into their browsers (without the https:// prefix).

Obtaining Ingress Certificates

There are two ways for *ingress* certificates to be obtained.

1. Method 1: The customer generates and provides both the private key and the certificate.
2. Method 2: We/Baxter, as administrators of the Platform, generate a private key and a Certificate Signing Request ("CSR"). The CSR is then distributed to the customer where it is signed by their preferred CA and returned to us.

Method 1: Customer provided private key and certificate

The customer's ingress certificate must

1. Be an EC key of size 384 bits or an RSA key of key size 4096 bits
2. The certificate must be signed by an appropriate Certificate Authority of their choosing.
3. The Common Name of the certificate must match the FQDN of the BDHP server. In other words, it must match the URL that end-users type into their browsers (without the https:// prefix).

Once the customer has supplied Ingress certificates, they should be moved onto the BDHP server.

Method 2: Certificate Signing Request

In this method, we create an EC key of size 384 bits. We will then create a Certificate Signing Request ("CSR"). This is achieved with a single lva command. This command should ideally be run on the BDHP server so that the private key never leaves the server.
This is considered the most secure method of certificate management.
Use the **lva create-web-ingress-csr** commands which will interactively prompt the required fields. This will create the private key and CSR. Copy off the CSR and send it to the customer for signing with their own authority.

Release Status:Issued and Effective

```
baa@jonh:~$ lva create-web-ingress-csr
Please enter 2 letter ISO-3166-1 country code: gb
Please enter the state: gl
Please enter the city: Gloucester
Please enter the organization: [Jon Hospital]Baxter
Please enter the organizational unit: BaxterUK
Please enter the FQDN: [jonh.stg.baxter.com]facility.customer.com
Generating a RSA private key
.....................................++++
.++++
writing new private key to '/home/baa/certs/web-ingress/2024-05-07-1010/facility.customer.com.key'
-----
CSR and private key written to /home/baa/certs/web-ingress/2024-05-07-1010

CSR contents outputted below. This will need to be sent to the customer for signing by their preferred certifying authority

-----BEGIN CERTIFICATE REQUEST-----
MIIE6zCCAtMCAQAwczELMAkGA1UEBhMCZ2IxCzAJBgNVBAgMAmdsMRMwEQYDVQQH
DApHbG91Y2VzdGVyMQ8wDQYDVQQKDAZCYXh0ZXIxETAPBgNVBAsMCEJheHRlclVL
MR4wHAYDVQQDDBVmYWNpbGl0eS5jdXN0b21lci5jb20wggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDPNUxGMPlW2OqIjecKm+viMXjIGSoeYu+bPy1eV/qS
CTJIPgfsd+5mMxTMoU54adsxHzv5nf99CHKluoDDj4dsrMOEjQaD1DgHGmS0//Zk
5YEZQqOYBE3AaE2ShT1Ru3X4OdtiFZeJAvdUq5BywmYZZi/L35LHHws3KkV6g9i4
eZ1rInWTqJmhTqr3z9wxTiw711Yb4YImhjjq5s7UrGPSH1V9RPjxYr5KCBD2aX6B
+Edw64yxbixcoOGnqBmlYAfTfmmnmVaiqYPMJ3m2I9fxwmO9yHwqrG9krqi8D+y4
tTOZmkztZb+Y3Jks1OBEoaHclxoY9Sr0A9PFxIZ9EYe/j+mo9W4Exy7sTD3+UVLR
VMk9Ey0uE8N+K/akDL7HI2GYeTA5qV5dDX17Ngx/xCFwJKn0FmWO6RHp8NQifnMo
EDw0xHcNKEvakRu9571yA1iwADUqKthlSj2KErzPIm7sDogrdYnaBz7D0uCK0+WR
KsbkiFt1s6EhLQAQA6wz7tjK52IY9gN2TYTq6u00CrtaeMApBsyrR4cfpAlT62Q9
QQ6+zPUxWY2GFQFblPsLJ8o/5dWAz+33ZQY1X+yywHYhPXvQHB2hK1dL9HIDM33c
EsHllmcxnPqXP/MSj/I1/JOPSjYvBsxMIfLGRb2+wgM5U8enc2GEZigmQ5egabHg
GwIDAQABoDMwMQYJKoZIhvcNAQkOMSQwIjAgBgNVHREEGTAXghVmYWNpbGl0eS5j
dXN0b21lci5jb20wDQYJKoZIhvcNAQELBQADggIBAHNui/W/iQhJACbgZ5H4jA0X
Z68cFi/D+73n2pesKRxtK/Iqnk0mwLFxsVAnM8ih0WY3t2x3QFZOTtnMzpaj4Rik
6i9ts0rD+ufhXX/Ai2FotvogmvGEqBYPuY1p5CiRLeMHmiPcJLaJfmEkM6a1Yzbe
BYO7jsPyyN84mZN5NL+Y+Yf+G7oOm9yqVaBl7L9vusJTRwf0yCW5YwsTLCef54Op
ro5+1SVyJJJf9q/1k+lZO/WRJ7HH3bEZ6DUd5W80sMFMeyLXdqxxlNRsEIysqrbN
v7AGH7q1+PrA7k0p92/ajkdEKiIaNo2eYFrQr8VK1DmqvkFnRGgp9mbeqSxmfQRG
KPv+L4bxScho/tKM6bGVNUMY+OVCrriV/D3ecLuWFblCDAKPW4Z25Qb1KrKzTXk2
kRjvp7sQZkeO2h20iuZv+6qXgnQNzIWvHljlLQ51PVZGNF88toD9Bb5aAersLkrL
KsGfEs6rkYGiasMNqxa96YBTnp+/Awq5Mvpd63Fcrb/mDDXvSdZn9hEIezIQGCSb
WUV/V6LALJcyCtmFtGZNYzP/YAyg0vPHnwPYW1jwiS/gZ95bax9r8Gy5LLhvnu1F
NRLunafYkUq8F4X25JKrtaYcJNabjPo0Pr9U1CAYOacmAvBZV52P4mtURa6dAq5h
/nlvItiU/pFT6QswOINi
-----END CERTIFICATE REQUEST-----
baa@jonh:~$ ls /home/baa/certs/web-ingress/2024-05-07-1010
facility.customer.com.csr  facility.customer.com.key
```

WARNING: The private key should stay on the server and not be shared with anyone. It will be imported later as per the steps in the documentation below.

Once the customer has supplied Ingress certificates, they should be moved onto the BDHP server.

Device Certificates

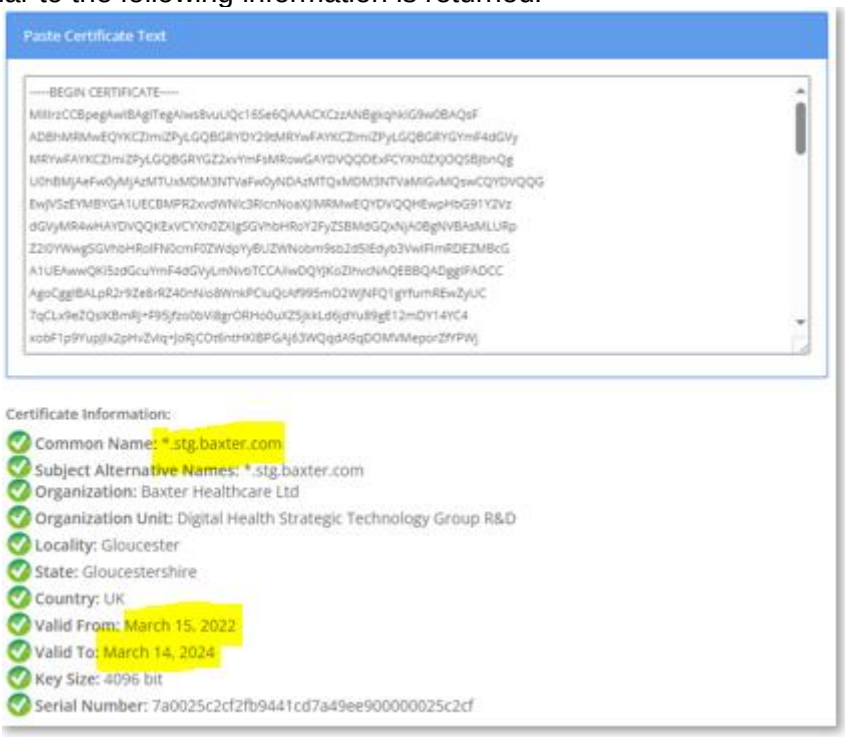
A Baxter device (eg a bed or pump) needs to trust a BDHP server. To this end, a certificate and private key can be loaded into Verne (the MQTT broker on a BDHP server). When the device connects to Verne, this certificate will be presented. The device will check that the certificate is signed by a certificate authority that it trusts.

NOTE that:

- Novum IQ Infusion pumps are bundled with the Baxter CA Certificate in the device firmware. The certificate is valid for a long time; 20+ years.
- Beds do not have this CA certificate. It is planned that this will be added to their firmware soon. This means the Baxter IOT root certificate has to be installed onto the beds for them to trust a Baxter certificate.

So, because Baxter devices hold (or will hold) Baxter Certificate Authority certificates, we need Verne to be installed with device certificates that have been signed by the Baxter CA. i.e **not** signed by the customer.

If the text of the certificate presented by Verne/BDHP is entered into a <u>certificate decoder,</u> then something similar to the following information is returned:



For successful validation of the Verne certificate by the device, the device must

1. View the certificate as valid in terms of its stated validity dates. This also means that the date and time set on the device must be correct!
2. The certificate's <u>Common Name (CN)</u> must match the FQDN (Fully Qualified Domain Name) of the BDHP. In the above example the common name shows a wildcarded value for *stg.baxter.com*. At a customer installation this would need to match the URL that end-users type into their browsers (without the https:// prefix). Otherwise, the bed will not agree to connect to BDHP.
3. The accompanying certificate authority that signs the certificate must be trusted by the device – eg the Baxter Certificate authority

Installing the Ingress and Device Certificates

Once both sets of certificates have been provided and are on the BDHP server, they need to be installed:

Ingress certificate installation

The **lva ingress:change-ui** command should be used as below to load these files into secrets

```
namespace="<your namespace>"
cert="<path-to-certificate-file>"
key="<path-to-key-file>"
# ensure the private key has the most restrictive file permissions
chmod 0400 $key
# Change the ingress certificate
lva ingress:change-ui $cert $key -n $namespace
# for best security, delete the PRIVATE KEY from the filesystem.
```

```
# MAKE SURE YOU HAVE A BACKUP! THIS IS IRREVERSIBLE
rm -f $key
```

Device certificate installation

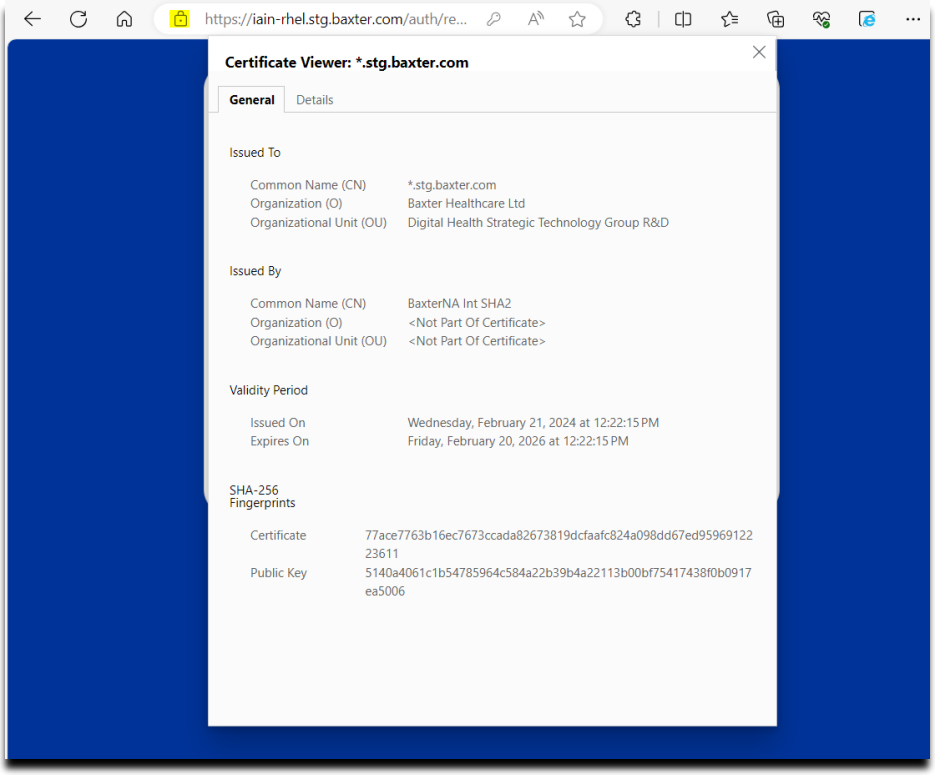
The **lva ingress:change-device** command should be used as below to load these files into secrets and restart VerneMQ services.

```
namespace="<your namespace>"
cert="<path-to-certificate-file>"
key="<path-to-key-file>"
cacert="<path-to-ca-file>"
# Create the new secret
lva ingress:change-device $cert $key $cacert -n $namespace
# Restart VerneMQ pods
kubectl delete pod bdhp-vernemq-0 bdhp-vernemq-pumps-0 -n $namespace --force
```

Testing Certificate Validation

Ingress certificate testing

The first obvious change to notice is that the web browser, when connecting to BDHP, no longer displays the warning '*your connection is not private'* (assuming the browser has the customer's CA certificate installed).
Secondly, clicking on the padlock icon will reveal the correct certificate information



These two tests demonstrate the successful installation of ingress certificates.

Release Status:Issued and Effective

Device certificate testing

Check which port is used by Verne.

```
baa@bdhp-iain-75550:~$ kubectl get svc -n ns | grep Load
bdhp-vernemq                        LoadBalancer   10.152.183.250   10.117.111.147   8883:30394/TCP
                24d
bdhp-ntpd                           LoadBalancer   10.152.183.219   10.117.111.147   123:31782/UDP
                24d
bdhp-mirth-svc-tcp-lb               LoadBalancer   10.152.183.234   10.117.111.147   10000:31369/TCP,10003:32210/TCP
                24d
```

If we connect to a server on the verne port (8883 in this case) using *openssl* with the *s_client* command we can view the certificate that is presented.

Run:

```
openssl s_client -connect iain-ha.stg.baxter.com:8883
```

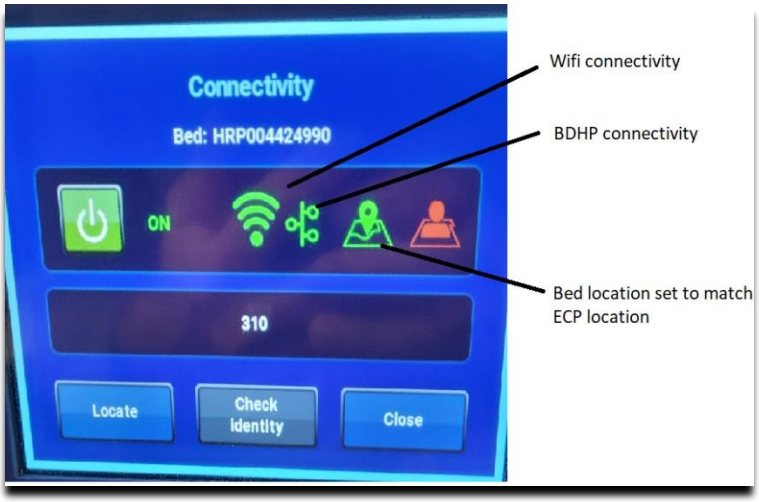
Returns:

```
baa@bdhp-ha4-07: ~
openssl s_client -connect iain-ha.stg.baxter.com:8883
CONNECTED(00000003)
depth=2 C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = Baxter
 Medical Device IoT TS Root CA G1
verify error:num=19:self signed certificate in certificate chain
verify return:1
depth=2 C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = Baxter
 Medical Device IoT TS Root CA G1
verify return:1
depth=1 C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = Baxter
 Medical Device IoT TS Issuing CA G1
verify return:1
depth=0 C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = *.stg.
baxter.com
verify return:1
---
Certificate chain
 0 s:C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = *.stg.bax
ter.com
   i:C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = Baxter Me
dical Device IoT TS Issuing CA G1
 1 s:C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = Baxter Me
dical Device IoT TS Issuing CA G1
   i:C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = Baxter Me
dical Device IoT TS Root CA G1
 2 s:C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = Baxter Me
dical Device IoT TS Root CA G1
   i:C = US, ST = Illinois, L = Deerfield, O = Baxter Healthcare, CN = Baxter Me
dical Device IoT TS Root CA G1
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICpTCCAiugAwIBAgIUekqWOttIThrXKKBro8K1MFzka2owCgYIKoZIzj0EAwMw
gYUxCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhJbGxpbm9pczESMBAGA1UEBwwJRGV1
cmZpZWxkMRowGAYDVQQKDBFCYXh0ZXIgSGVhbHRoY2FyZTEzMDEGA1UEAwwqQmF4
dGVyIE1lZGljYWwgRGV2aWN1IE1vVCBUUyBJc3N1aW5nIENBIEcxMB4XDTIyMDMw
MjEwMTY1MloXDTQyMDIyNTEwMTY1MlowazELMAkGA1UEBhMCVVMxETAPBgNVBAgM
CElsbGlub2lzMRIwEAYDVQQHDAlEZWVyZmllbGQxGjAYBgNVBAoMEUJheHRlciBI
ZWFsdGhjYXJlMRkwFwYDVQQDDBAqLnN0Zy5iYXh0ZXIuY29tMHYwEAYHKoZIzj0C
AQYFK4EEACIDYgAE58vI3DDvel/zwTFG4lySpILk7BuljYjqZNZl/J88Y8nW2IKg
```

Certificate chain shows
0 – the certificate specific to this Verne. This is wildcarded to '*.stg.baxter.com'
1 – the intermediate certificate with value '*Baxter Medical Device IoT TS* ***Issuing*** *CA G1*'
2 – the root certificate with value '*Baxter Medical Device IoT TS* ***Root*** *CA G1*'

This output demonstrates that the certificate is installed and is being presented to requests on the specified Verne port

The other, obvious, test for device certificates is that the device successfully connects with BDHP. For example, a bed may display



Release Status:Issued and Effective

J. Additional Virtual IP for VerneMQ

Introduction

Both beds and pumps communicate with VerneMQ on port 8883, by default. This is fine if a BDHP installation *only* has either beds or pumps configured.

But, if an installation of BDHP needs **both** beds and pumps, then the standard approach has been to change pumps to use port 8884 instead; as beds cannot use a different port.

There are some installation scenarios where it is undesirable to change pumps to use port 8884. The obvious example is a BDHP installation with many hundreds of pumps already configured on port 8883 that then decides to install beds - this would create a large amount of work as pump configuration is a manual process using a USB-A stick.

So the solution is to configure an additional virtual IP in BDHP. This means, in the example above, that pumps continue to use the same IP address and port number (8883) as before; and the beds also use port 8883 but use this new virtual IP address.

Method

The load balancer can advertise more than one virtual IP address. So, the way of allowing both device types to use the same port number is by creating a new IP Address Pool inside the MetalLB namespace (within Kubernetes). MetalLB will then have two virtual IP addresses associated with it.

NOTE- The new Virtual IP address needs to be allocated by the customer

Then either the **bdhp-vernemq-pumps** or the **bdhp-vernemq** (beds) service can be patched to use this new IP address from the address pool.

A single LVA command has been developed to achieve this.

```
baa@bdhp-ha4-07:~$ lva vernemq:set-ip -h
Sets a new Virtual IP address for VerneMQ connections
Usage: lva vernemq::set-ip {type} {ip-address} [options]
If invoked with no arguments, the script will interactively prompt for input
Positional arguments:
  {type}
  The VerneMQ whose IP address we are changing
  Allowable values: "pumps" or "beds"
  {ip-address}
  The Virtual IP address to set
```

It's called **vernemq:set-ip** and can be used to set <u>either</u> the pumps or the beds to use the new IP address that is prompted to provide.

```
baa@bdhp-ha4-07:~$ lva vernemq:set-ip
Checking for running VerneMQs
✓ Beds
✓ Pumps
Please choose which VerneMQ whose virtual IP you wish to change: [pumps/beds] pumps
Enter the required Virtual IP address: 10.117.110.253
ipaddresspool.metallb.io/pumps-addresspool created
service/bdhp-vernemq-pumps patched
```

It is important to check that the pumps and beds services are now using the correct IP addresses.

```
baa@bdhp-ha4-07:~$ kubectl get svc -n ns | grep verne
bdhp-vernemq-pumps-headless   ClusterIP      None            <none>          4369/TCP,8888/TCP
bdhp-vernemq-headless         ClusterIP      None            <none>          4369/TCP,8888/TCP
bdhp-vernemq                  LoadBalancer   10.152.183.43   <pending>       8883:30581/TCP
bdhp-vernemq-pumps            LoadBalancer   10.152.183.155  10.117.110.253  8883:31043/TCP
```

In this case, the pumps are using the new IP address (10.117.110.253), but the beds (named bdhp-vernemq) are in a pending state.

The rationale is that the pumps were using the original VIP of 10.117.110.252 blocking the beds service and MetalLB has not yet re-assigned beds to the now available original VIP.

To fix this, restart the MetalLB system using the command:

kubectl rollout restart deployment.apps/controller -n metallb-system

Release Status:Issued and Effective

```
baa@bdhp-ha4-07:~$ kubectl rollout restart deployment.apps/controller -n metallb-system
deployment.apps/controller restarted
baa@bdhp-ha4-07:~$ kubectl get po -n metallb-system
NAME                          READY   STATUS              RESTARTS   AGE
controller-8467d88d69-4pfcv   1/1     Running             0          2d21h
speaker-w4mtk                 1/1     Running             0          2d21h
speaker-kpkr8                 1/1     Running             0          2d21h
speaker-7m6zm                 1/1     Running             0          2d21h
controller-697c4f94d4-749sd   0/1     ContainerCreating   0          4s
baa@bdhp-ha4-07:~$ kubectl get po -n metallb-system
NAME                          READY   STATUS    RESTARTS   AGE
speaker-w4mtk                 1/1     Running   0          2d21h
speaker-kpkr8                 1/1     Running   0          2d21h
speaker-7m6zm                 1/1     Running   0          2d21h
controller-697c4f94d4-749sd   1/1     Running   0          67s
baa@bdhp-ha4-07:~$ kubectl get svc -n ns | grep verne
bdhp-vernemq-pumps-headless         ClusterIP      None             <none>           4369/TCP,8888/TCP
bdhp-vernemq-headless               ClusterIP      None             <none>           4369/TCP,8888/TCP
bdhp-vernemq-pumps                  LoadBalancer   10.152.183.155   10.117.110.253   8883:31043/TCP
bdhp-vernemq                        LoadBalancer   10.152.183.43    10.117.110.252   8883:30581/TCP
```

NOTE: that pumps and beds are now using different IP address but the same port number of 8883.

DNS setup

Now that two (or more) virtual IP addresses exist for this BDHP platform, it is possible to set one DNS for each VIP

DNS Entries

Name.....Information

beds.stg.baxter.com..... 10.100.27.100

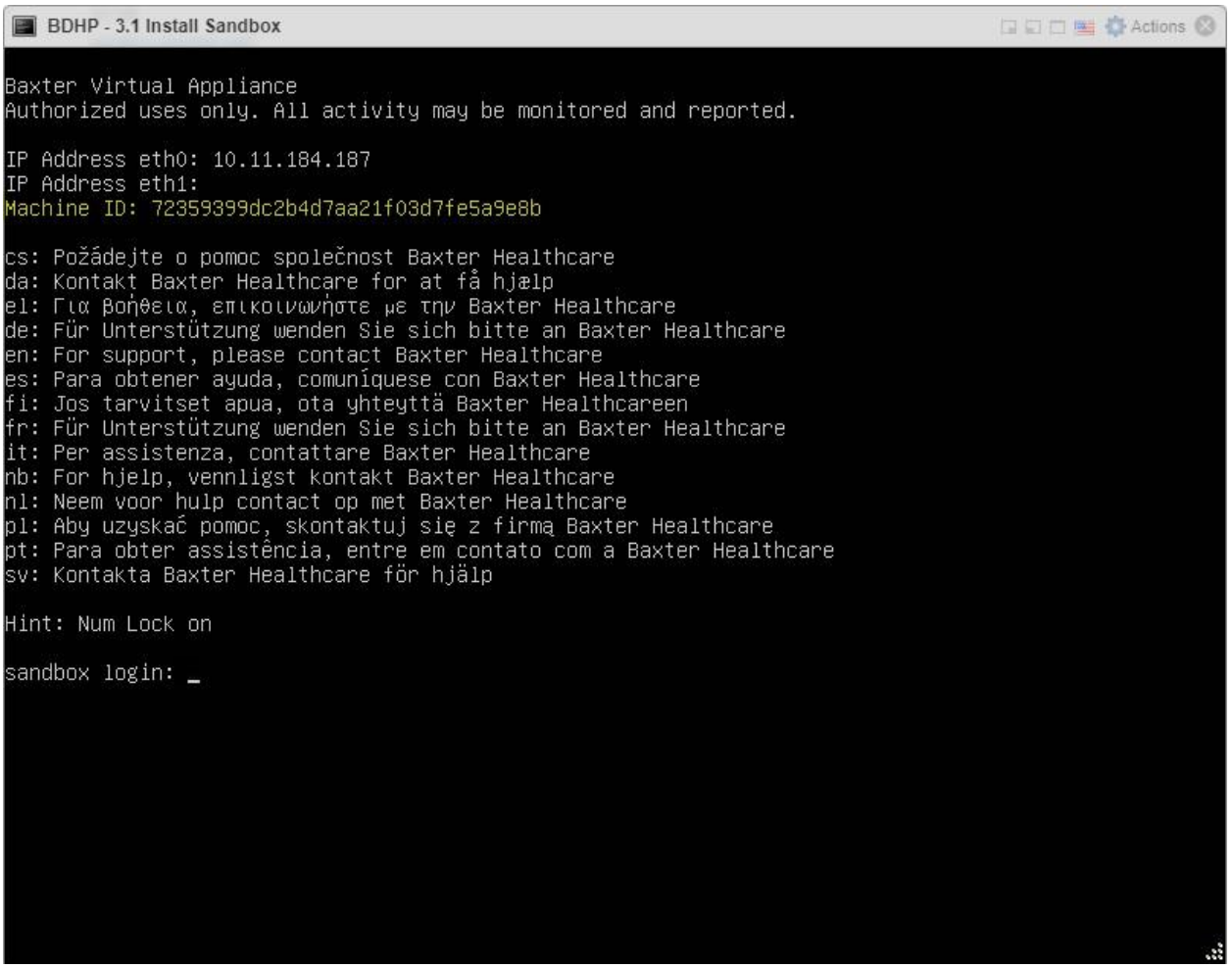
pumps.stg.baxter.com..... 10.100.27.101

In this way it is possible to demarcate the usage of the Virtual IPs on the load balancer.

K. Configuration of SecureLink for remote access

After a customer deploys a BDHP image into the virtual environment and turns the server on, the slink service runs a script named ***create-gatekeeper.py***. This script makes API calls to the SecureLink gateway and creates and registers a new Gatekeeper with the Machine ID shown on the console.

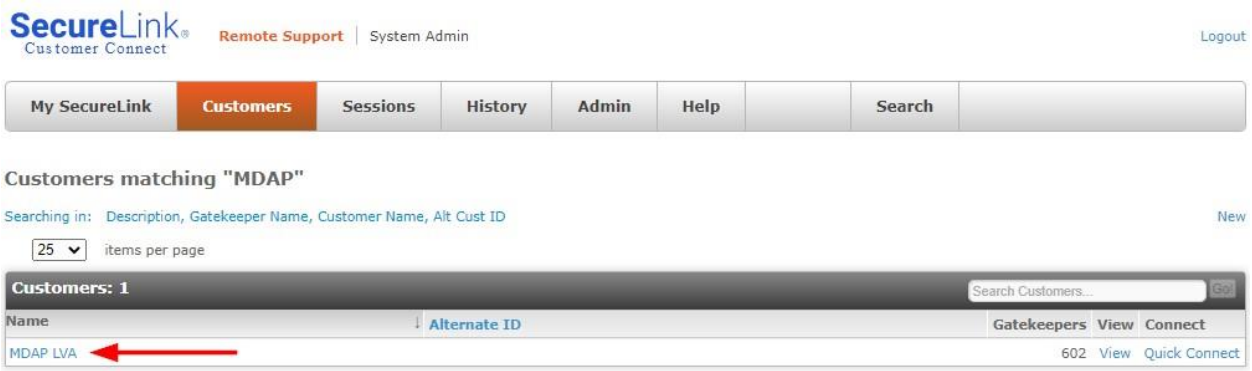
Release Status:Issued and Effective



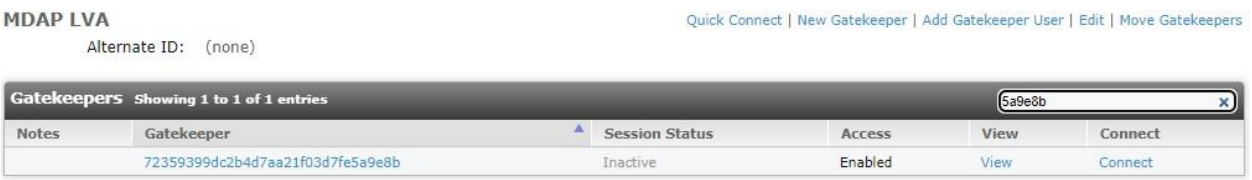
- If unable to locate the Machine ID:
  - Log into the Baxter Virtual Appliance.
  - Navigate to the etc directory (**cd /etc**).
  - Run the following command (**cat machine-id**).

```
 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

58 updates can be applied immediately.
14 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable


1 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log

*** System restart required ***
Last login: Wed Mar  1 18:17:07 2023 from 10.134.3.32
baa@baxterappliance:~$ cd /etc
baa@baxterappliance:/etc$ ls
adduser.conf            ca-certificates.conf          dconf           group           issue           login.defs
aide                    ca-certificates.conf.dpkg-old debconf.conf    group-          issue.net       logrotate.conf
alternatives            calendar                      debian_version  grub.d          java-8-openjdk  logrotate.d
apparmor                clamav                        default         gshadow         kernel          lsb-release
apparmor.d              cloud                         deluser.conf    gshadow-        landscape       ltrace.conf
apport                  console-setup                 depmod.d        gss             ldap            lvm
apt                     cracklib                      dhcp            hdparm.conf     ld.so.cache     machine-id
at.allow                cron.allow                    dpkg            host.conf       ld.so.conf      magic
audisp                  cron.d                        e2scrub.conf    hostname        ld.so.conf.d    magic.mime
audit                   cron.daily                    environment     hosts           legal           mailcap
bash.bashrc             cron.hourly                   ethertypes      hosts.allow     libaudit.conf   mailcap.order
bash_completion         cron.monthly                  fonts           hosts.deny      libblockdev     mailname
bash_completion.d       crontab                       fstab           init.d          libnl-3         mail.rc
bindresvport.blacklist  cron.weekly                   fuse.conf       initramfs-tools locale.alias    manpath.config
binfmt.d                cryptsetup-initramfs          fwupd           inputrc         locale.gen      mdadm
byobu                   crypttab                      gai.conf        iproute2        localtime       mime.types
ca-certificates         dbus-1                        groff           iscsi           logcheck        mke2fs.conf
baa@baxterappliance:/etc$ cat machine-id
d1776747b7934d1baeb40733e4fd1de7
baa@baxterappliance:/etc$
```

1. Log into SecureLink Customer Connect: (https://baxter.securelink.com/rss-servlet/)
   a. Find a customer named MDAP LVA.



   b. Search for the Machine ID that matches the value displayed on the VM console.

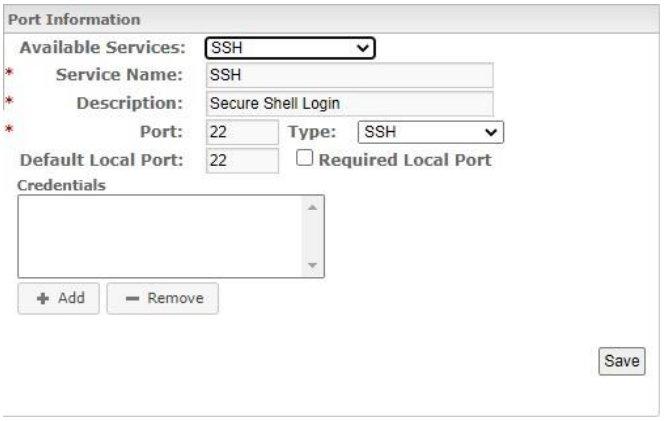


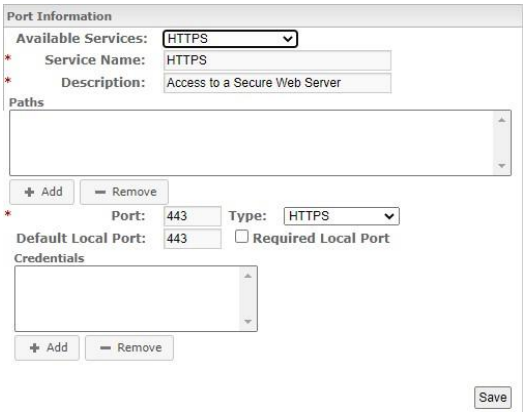
   c. Click on the Gatekeeper name.
   d. Click **Edit Services**.

By default, only the following two services will be configured.

1. Select **Add New Port**.

2. Select Add SSH and HTTPS.



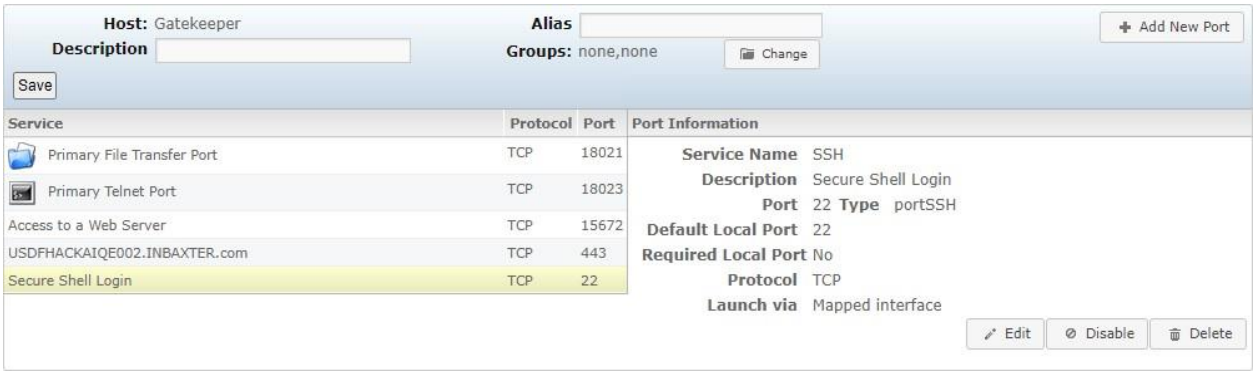


Other notable ports to want to forward:

15672	RabbitMQ
4680	SecureLink Gatekeeper Webpage

When a connection is made to a remote server Gatekeeper through SecureLink Customer Connect, SecureLink establishes a tunnel from the customer's server to a randomized 127.x.x.x IP address on the workstation from where the connection was made.
External applications can use the established IP address as a means of navigating the tunnel. To gain access to specific ports over the tunnel, define SecureLink services to port forward from the connected server to the local workstation.

Release Status:Issued and Effective



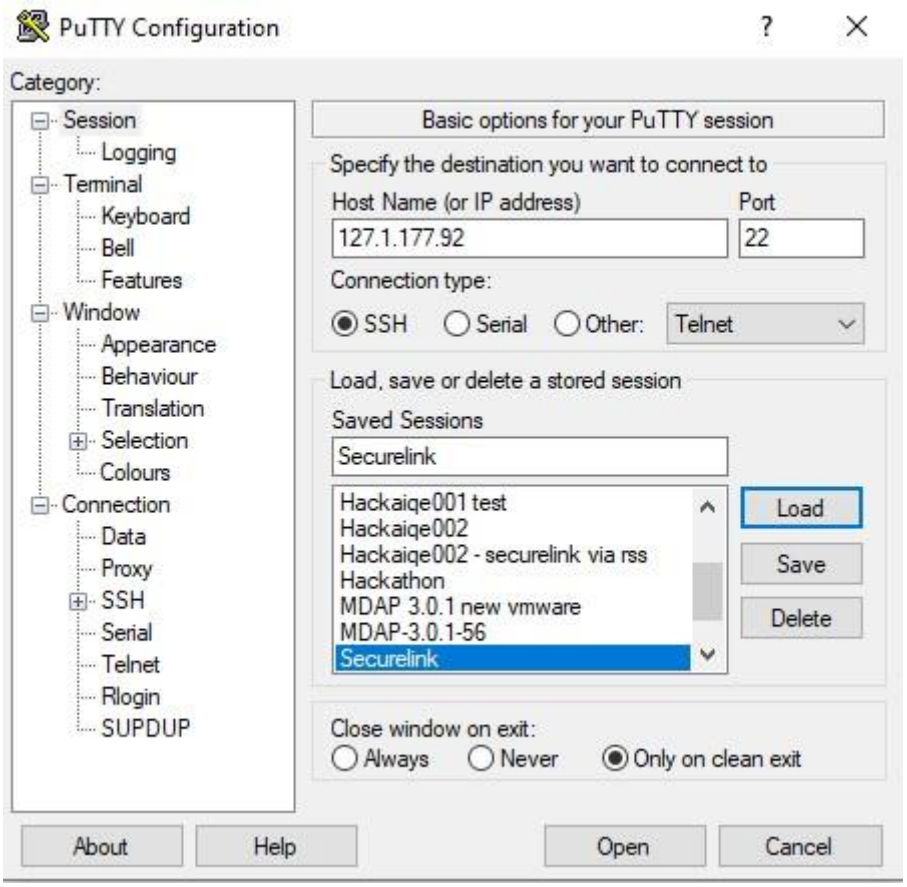
After the services are built and a connection is established, gain access to the customer servers. it is not possible to connect to the server over SSH by clicking on the Secure Shell Login. Attempting to make a connection will result in an error.
Use the following workaround to successfully connect to the customer servers.

1. Connect to Gatekeeper.
2. After the tunnel is established, copy the Interface IP address.

Connect to the Remote Tunnel via the SSH Client

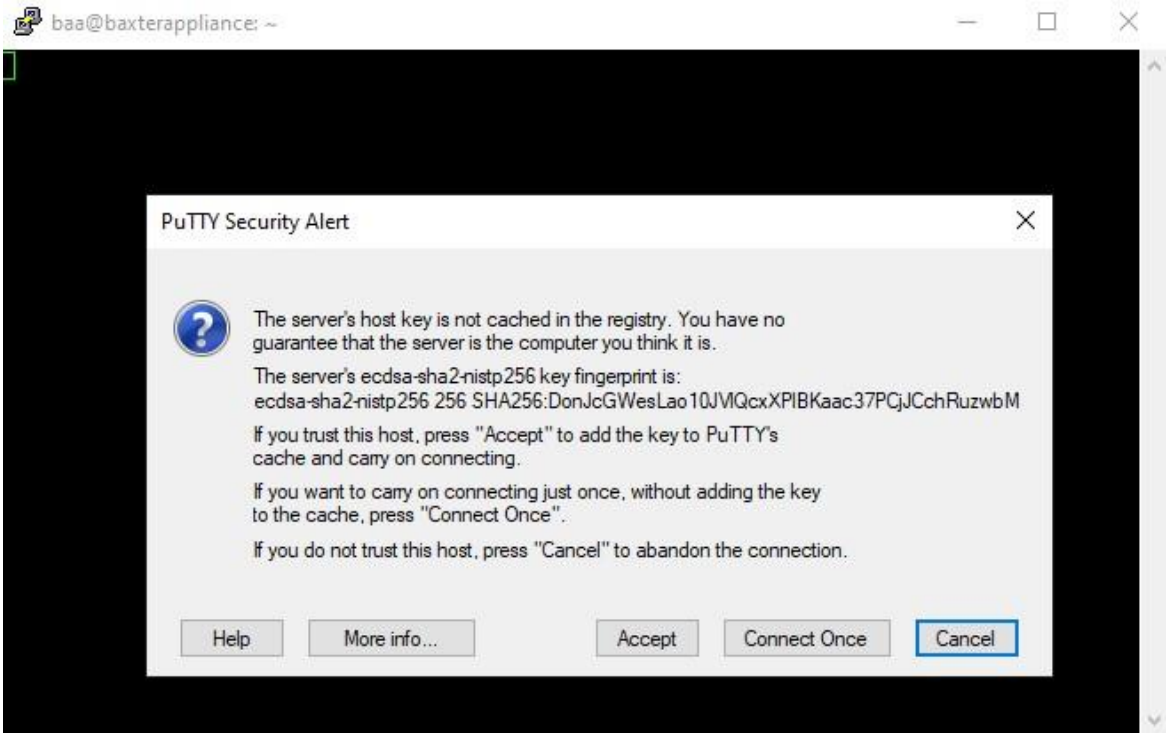
3. Open an external SSH application, such as PuTTY and configure an SSH connection using that IP address.

Release Status:Issued and Effective

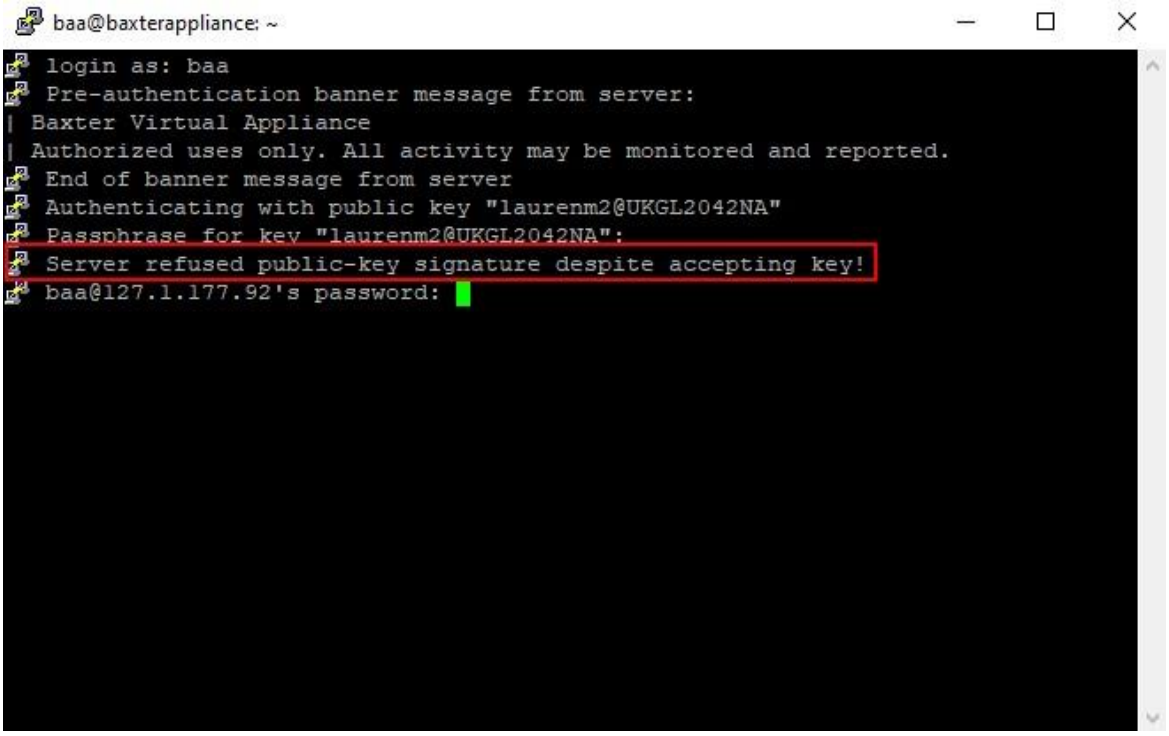


4. When prompted, accept the server fingerprint.

Release Status:Issued and Effective



5. The following error message may be displayed:

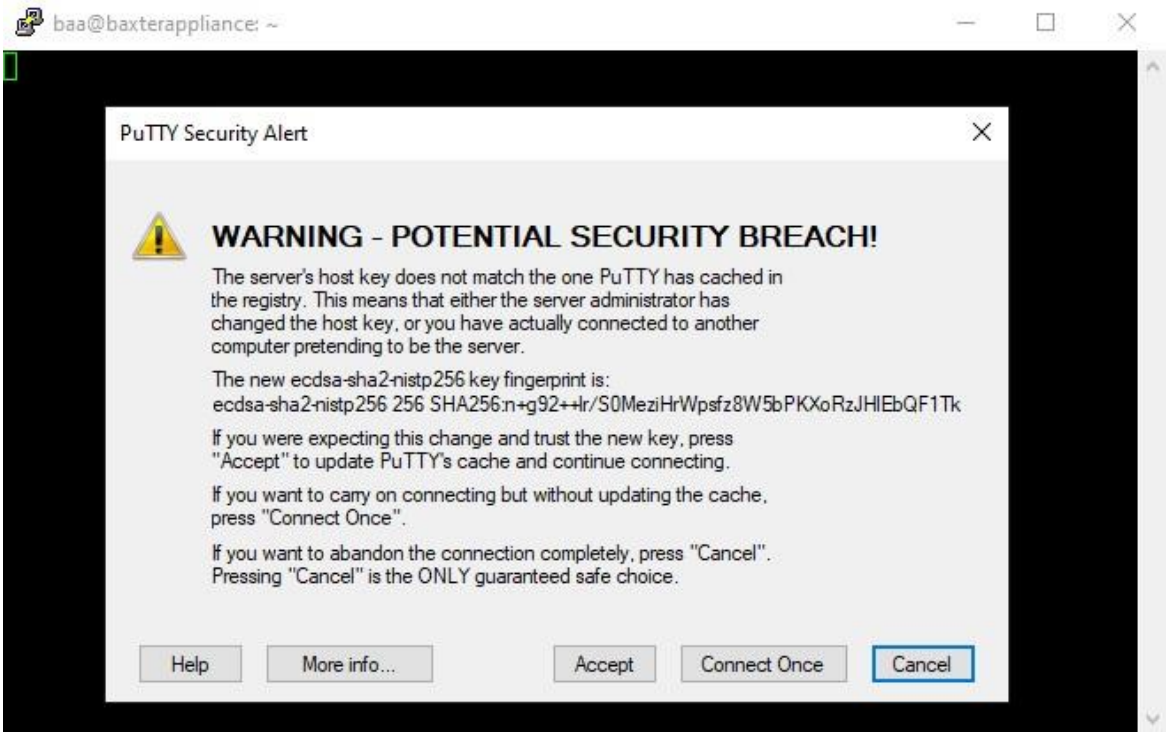


Release Status:Issued and Effective

6. Close the window and reconnect again.

   When you connect the second time, it will show that the server fingerprint has changed. This change occurs because SecureLink cycles the fingerprint, and it must be accepted again. In some cases, your

   might need to delete the fingerprint out of the **known_hosts** file before connecting again, or you will continue to see the previous error message. The **known_hosts** file is located at **C:\Users\<username>\.ssh**.



7. Accept this key and it should allow you to log in.
8. Navigate to the hosts file on your local workstation and edit it at C:\Windows\System32\drivers\etc\hosts. Add an entry for the established service IP address and the fully qualified domain name (FQDN) of the server.

   This entry allows you to access the BDHP web server through the established SecureLink tunnel. You can navigate to the Fully Qualified Domain Name (FQDN) of the server in a local web browser.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
    127.0.0.1   app-prod.doseiq auth.doseiq vhsr-iqenterprise.tbay-hospitals.local hniqecs.gbin.local
#   10.11.184.72 USDFHACKAIQE001.INBAXTER.com mdap.local
    10.11.184.71 app-prod.doseiq auth.doseiq
#   10.11.184.71 doseiq.dryrundemo.inbaxter.com doseiq-security.dryrundemo.inbaxter.com
    10.11.184.163 security.doseiq myhospital.doseiq
    127.1.177.92 USDFHACKAIQE002.INBAXTER.com
```

9. Open a local web browser and navigate to the FQDN of the server.

10. After you verify the connectivity, rename the Gatekeeper and move it to the appropriate customer.

11. Click **Edit**.

12. Change the Gatekeeper name to something that is appropriate for the customer using standard naming conventions.

Release Status:Issued and Effective

13. Click **Save**.
14. Click **Edit** again and click **Move Gatekeeper**.

15. Select the appropriate customer or create a new customer, if applicable.

16. At the prompt, select confirm to move the Gatekeeper.

L. Installing, upgrading and configuring guest applications

A **Guest Application** is a product or tools implemented by a third-party development team that is designed to be compatible with BDHP.

Refer to Guest Application Documentation

NOTE: the examples on this page use guest applications maintained by the Baxter Hospital Platform team. Refer to the documentation of a specific guest application for information on how to install it and what specific configuration parameters may be needed.

Registries

BDHP maintain 2 registries from where all guest applications may be installed. An Azure ACR repository and an older AWS ECR repository (still in use but deprecated).

The commands below will allow you to

1. Install/upgrade directly from the ACR helm registry by giving the helm chart name and version you require
2. Install/upgrade directly from the ECR helm registry by giving the helm repository name and required version (note: in ECR the helm repository name does not necessarily match the helm chart name)
3. Install/upgrade directly from a downloaded helm chart on the LVA file system

Installing

To install any guest application, follow the examples below.

```
# The BHP "Test" Application installed 'direct' from the online registry (or /opt/baxter/charts
 for 'offline' installations - see note below)
lva install "mdap-test:2.3.0" -n "<namespace>"

# Installing from a downloaded helm chart (TGZ). Eg lva ecr-pull iqeg-gateway-helm:2.6.0 .
lva install /path/to/chart.tgz -n "<namespace>"

# Installing from a downloaded helm chart (uncompressed)
lva install /path/to/chart -n "<namespace>"
```

When installing 'direct', the software will firstly look under /opt/baxter/charts, then our ACR registry. If it can't find the requested helm chart it will fall back to searching in ECR.

Listing Installed Applications

Existing applications can be obtained with the 'helm' command.

```
helm list -n "<namespace>"
```

Which may output something similar to the following:

Command Output

```
baa@bhphimss:~$ helm list -n namespace
NAME                    NAMESPACE       REVISION        UPDATED                         STATUS          C
VERSION
```


Release Status:Issued and Effective

```
mdap                    namespace    1    2022-02-22 22:54:19.45351937 +0000 UTC  deployed
3.1.0                     3.1.0
mdap-test                 namespace    3    2022-02-23 11:15:40.326893526 +0000 UTC deployed
1.1.0                     1.1.0
```

Release Status:Issued and Effective

Upgrading

Existing applications can be upgraded from one version to another using the lva upgrade command. You can also upgrade an existing version to set new command line parameters

```
# Upgrade the BHP "Test" Application using the chart 'direct' from the online registry (or
/opt/baxter/charts for 'offline' installations - see note below)
lva upgrade "mdap-test:2.3.0" -n "<namespace>"

# Upgrade the BHP "Test" Application and using the --set option to turn on Linkerd service mesh
lva upgrade "mdap-test:2.3.0" --set "linkerd2.enabled=true"   -n "<namespace>"

# Upgrading from a downloaded helm chart (TGZ)
lva upgrade /path/to/chart.tgz  -n "<namespace>"

# Upgrading from a downloaded helm chart (uncompressed)
lva upgrade /path/to/chart  -n "<namespace>"
```

When upgrading 'direct', the software will firstly look under /opt/baxter/charts, then our ACR registry. If it can't find the requested helm chart it will fall back to searching in ECR.

NOTE: That you also use this command for upgrading the platform itself:

```
# Upgrade the platform 'mdap' chart
lva upgrade "mdap:<version>" -n "<namespace>"
```

Uninstalling

Existing applications may be uninstalled using the lva uninstall command. The name of the application to uninstall must be as per the output of 'helm list'.

```
# lva uninstall "<chart-name>" -n "<namespace>"
# e.g. Uninstall BHP "Test" application
lva uninstall "mdap-test" -n "<namespace>"
```

The 'lva uninstall' command will not remove any databases associated with your application. These must be deleted manually if you need to do so.

Pulling

Pull a helm chart from our software repositories to the LVA. Install/upgrade from the downloaded chart (see above).

```
# Pull down the chart of the mdap test application to the local filesystem
lva pull "mdap-test:2.3.0" /path/to/destination/folder
```

This command will not work in 'offline' installations.

Release Status:Issued and Effective

Search

Use the search command to look for available tags for the given guest application.

```
# Search for all production versions of ICNET PHOM (aka. NSOM)
lva search "icnet-phom-helm3"

# Search for all development versions of MDAP platform
lva search "mdap" --show-dev

# Search for the latest chart of the "test guest" application
lva search "mdap-test" --show-dev --latest
```

This command will not work in 'offline' installations

Configuring

After install/upgrade any --set values are remembered and recorded in a secret. These are automatically remembered and applied to subsequent upgrades, unless overwritten with more --set values.

To see the --set values used in the last install/upgrade of a given install, run the command:

lva install:values "<install-name-of-application>" -n "<namespace>"

M. Using the Keycloak admin console

Administrative user

Post-installation, administrators can log into the Keycloak admin console to view/configure the realm, clients, users and so on.

A default **baxter** user is created for each installation with full administrative rights. The password is randomly generated and stored in the **mdap-keycloak-console-secret**.

Access this secret by running the following command:

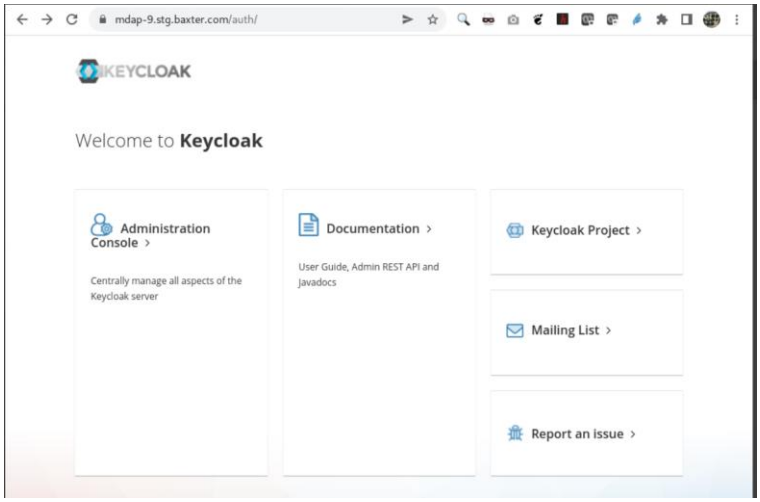
```
lva -n "<namespace>" password:reveal mdap-keycloak-console-secret
```

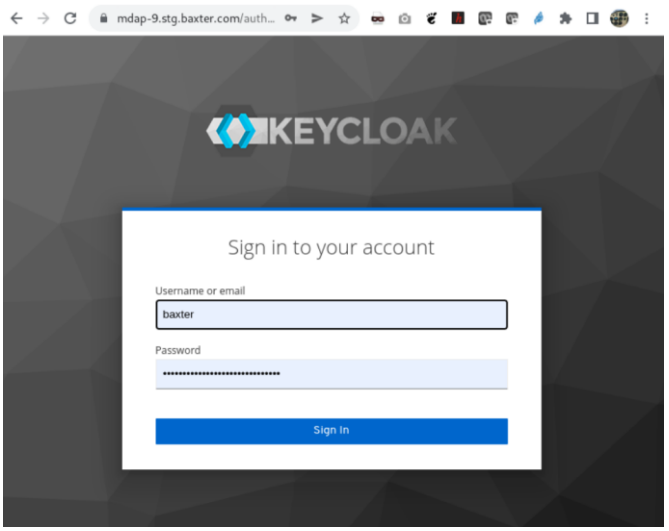
Copy the password to your clipboard.

Admin console

The Keycloak admin console is accessed via https://<**FQDN**>/auth with the **bdhpFqdn** environment variable.

Click on the link to *Administration Console* and sign in with your **baxter** username and password as above.





Release Status:Issued and Effective

Reference

Articles have been placed within this reference section as they do not pertain to the installation, but are useful articles on aspects of the BDHP platform

A- Configuring troubleshooting user

For support purposes it is useful to configure a troubleshooting user who has access to the following areas: Grafana & Verne dashboards. This reference article describes the configuration of this access.

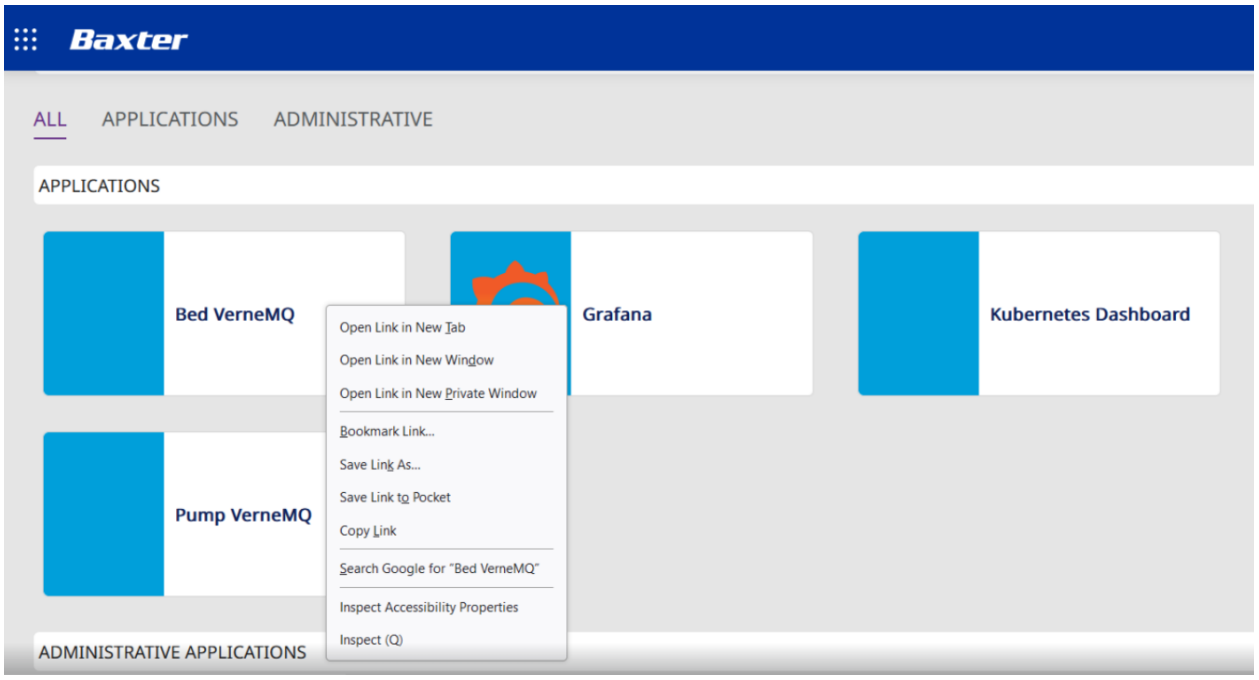
VerneMQ for Beds (experimental)

The VerneMQ dashboard can be configured within systems where VerneMQ is set up for beds. The VerneMQ for bed Pod will be named "**bdhp-verne**". To configure the dashboard in the cluster, use the below command. Ensure that the Installation namespace corresponds to the customer namespace in which the platform is installed.

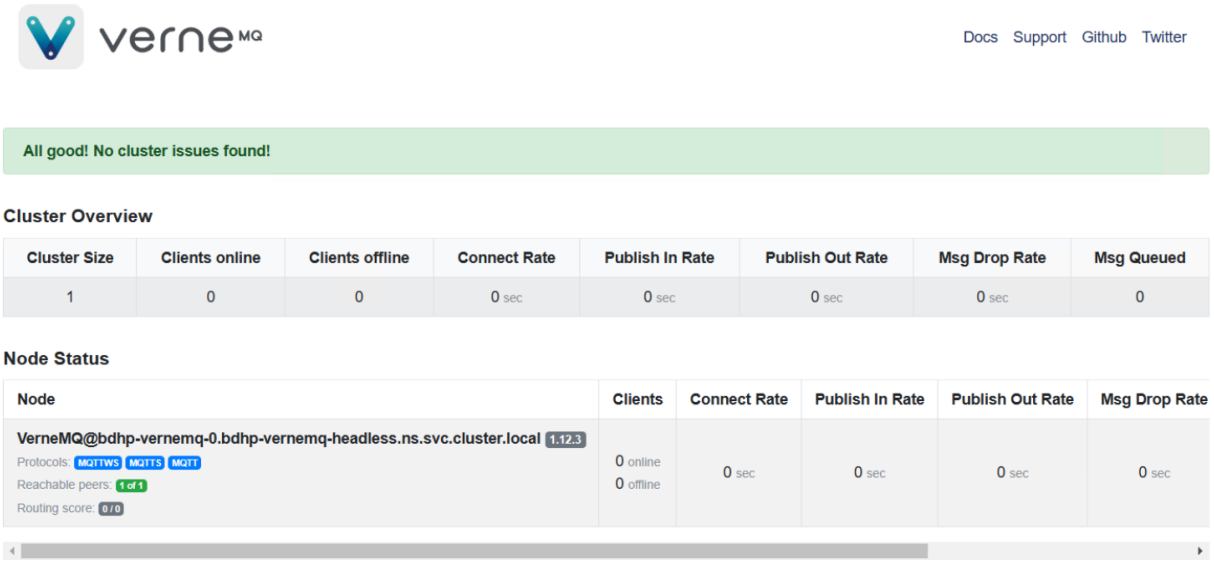
lva vmq-bed-dashboard:configure -n ns

Login to keycloak, in mdap realm, assign the user with “bed-vernemq vernemqbedstatus” role. The role assignment can also be created through the “User Management” area of the dashboard.

Once the user login to this portal, user will find the “**Bed VerneMQ**” tile. To open the VerneMQ dashboard for beds, right-click on the tile and select "Open in New Tab."



To see the Verne bed dashboard;



VerneMQ for Pumps (experimental)

The setup for pumps is identical to that for beds, with two exceptions:

1. Use the following command on the lva

   lva vmq-pump-dashboard:configure -n ns

2. Give the support user the following role: **pump-vernemq vernemqpumpstatus**. The role assignment can also be done through Connex (mdap) "User Management" Options.

Grafana

Access to Grafana provides the user with access to logs.

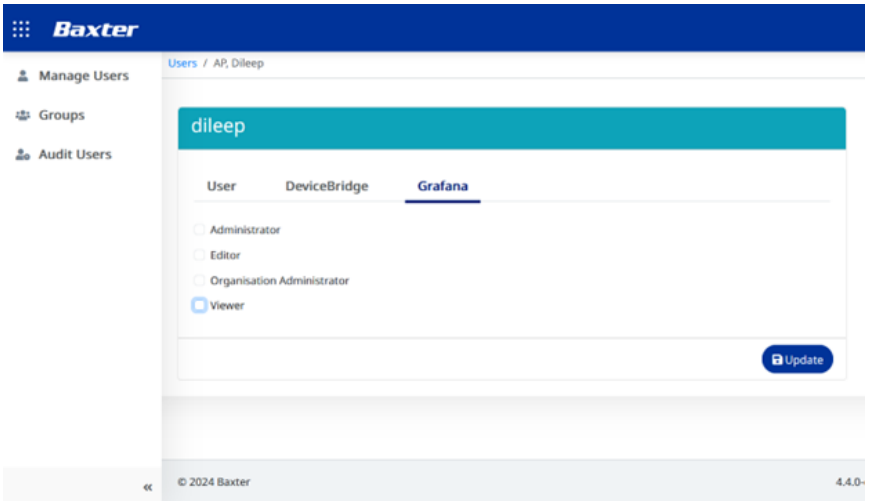
To grant a user access to the Grafana dashboard through IQECS, follow these steps:

Ensure the user has privilege for user management.

1. Navigate to User Management
2. Select the User
3. Select Grafana

Below are the available roles

Release Status:Issued and Effective

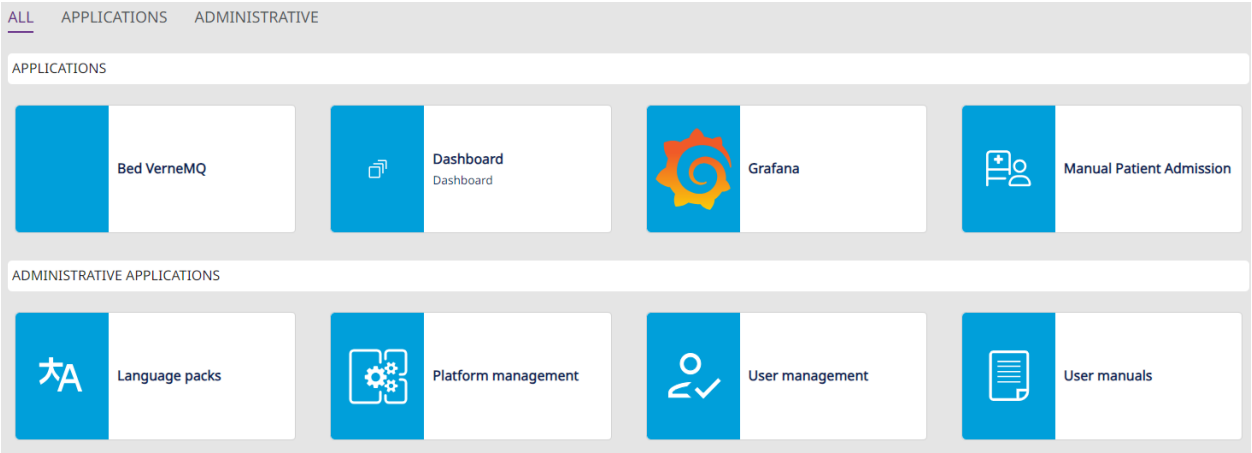


Here are the permissions for each role

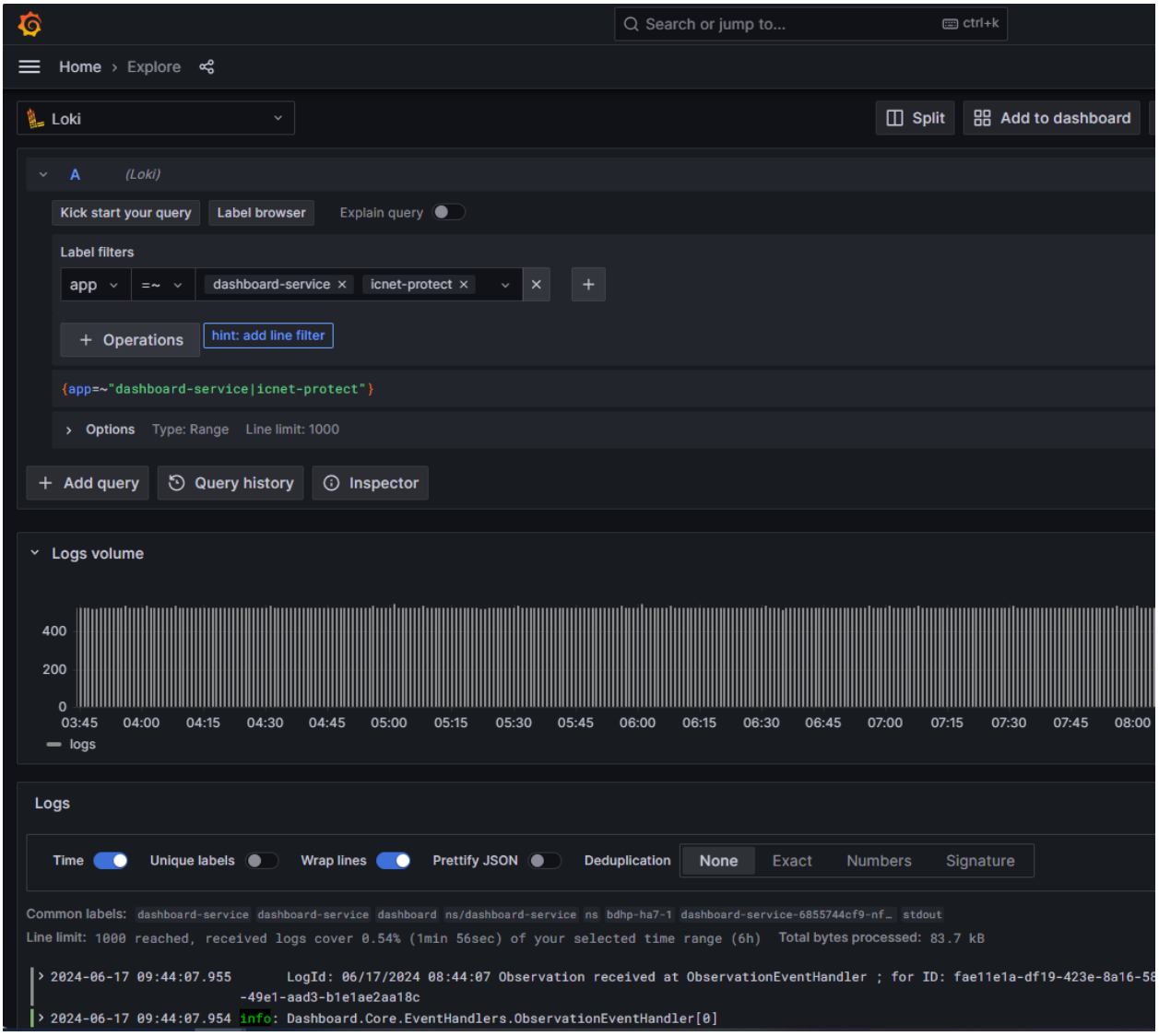
Permission	Organization administrator	Editor	Viewer
View dashboards	x	x	x
Add, edit, delete dashboards	x	x	
Add, edit, delete folders	x	x	
View playlists	x	x	x
Add, edit, delete playlists	x	x	
Create library panels	x	x	
View annotations	x	x	x
Add, edit, delete annotations	x	x	
Access Explore	x	x	
Add, edit, delete data sources	x		
Add and edit users	x		
Add and edit teams	x		
Change organizations settings	x		
Change team settings	x		
Configure application plugins	x		

The user will now see the Grafana tile upon the dashboard:

Release Status:Issued and Effective



Clicking the Grafana tile will provide access to the Grafana logs:



B- Language & Manuals Library - importing assets

Background

In version 3 of the platform, the Language and Manuals Library service connected over the internet to AWS S3 storage where the most recent versions of language packs and user manuals are maintained for guest applications.

From version 4.1.x, new functionality has been added to allow for on-premise installations where external internet may be restricted by a customer, therefore blocking this channel.

Version 4.1

From version 4.1 onwards, the Language and Manuals Library service no longer connects over the internet to AWS S3 storage. It is necessary to upload the necessary language packs and user manuals on a per installation basis. In addition, the functionality has been moved into the IQECS/BDHP UI container which provides the language-library-svc API endpoint to guest applications.

Obtaining latest assets

A download of the latest language packs and user manuals are available in zip format from https://lva-build.stg.baxter.com/language-library/packs/ and https://lva-build.stg.baxter.com/language-library/manuals/. These zip files contain the packs for all versions and languages of the respective applications. Individual packs may be downloaded via https://language-library-admin.stg.baxter.com/language-library/home and should be zipped if they are to be imported via the command line. The Administrative UI accepts either zipped packages or individually uncompressed files.

Import methods

There are 2 ways to import language packs and user manuals into the platform:

1. In a terminal session running **lva -n <namespace> language-library:import**
2. Administrative UI inside the BDHP UI. The maximum file size that may be uploaded in a single upload is limited to 100 MB.

lva language-library:import

When logged into the LVA server, use the lva language-library:import command to import the assets.tar.gz file.

```
# Assuming that assets.zip has been saved in the /tmp this command will upload
them into the language and manuals library service
# Please ensure there are no spaces in the full filename
lva -n <namespace> language-library:import /tmp/assets.zip
```

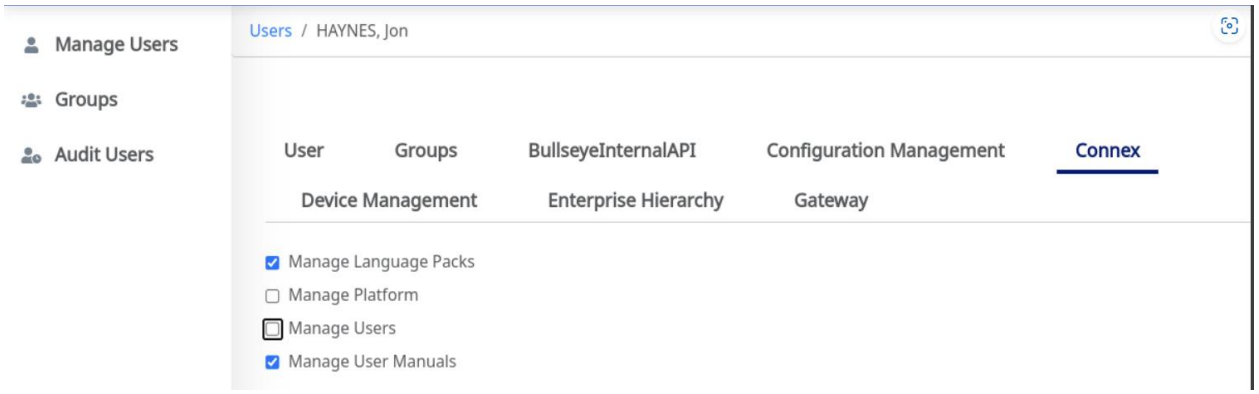
Once the language library assets have been uploaded some applications will automatically check and pick up translations. For example, IQECS will check every hour for translations and update on this schedule. Other guest applications *may* require their pods to be restarted to pick up translations.

Restart all guest application pods to be on the safe side

```
# Perform a graceful rolling restart of all deployed containers
# Make sure you replace <namespace> in BOTH places in the below statement
kubectl get deployments -n <namespace> -o custom-columns=NAME:.metadata.name|
grep -iv NAME|while read LINE; do kubectl rollout restart deployment $LINE -n <namespace> ;
done;
```

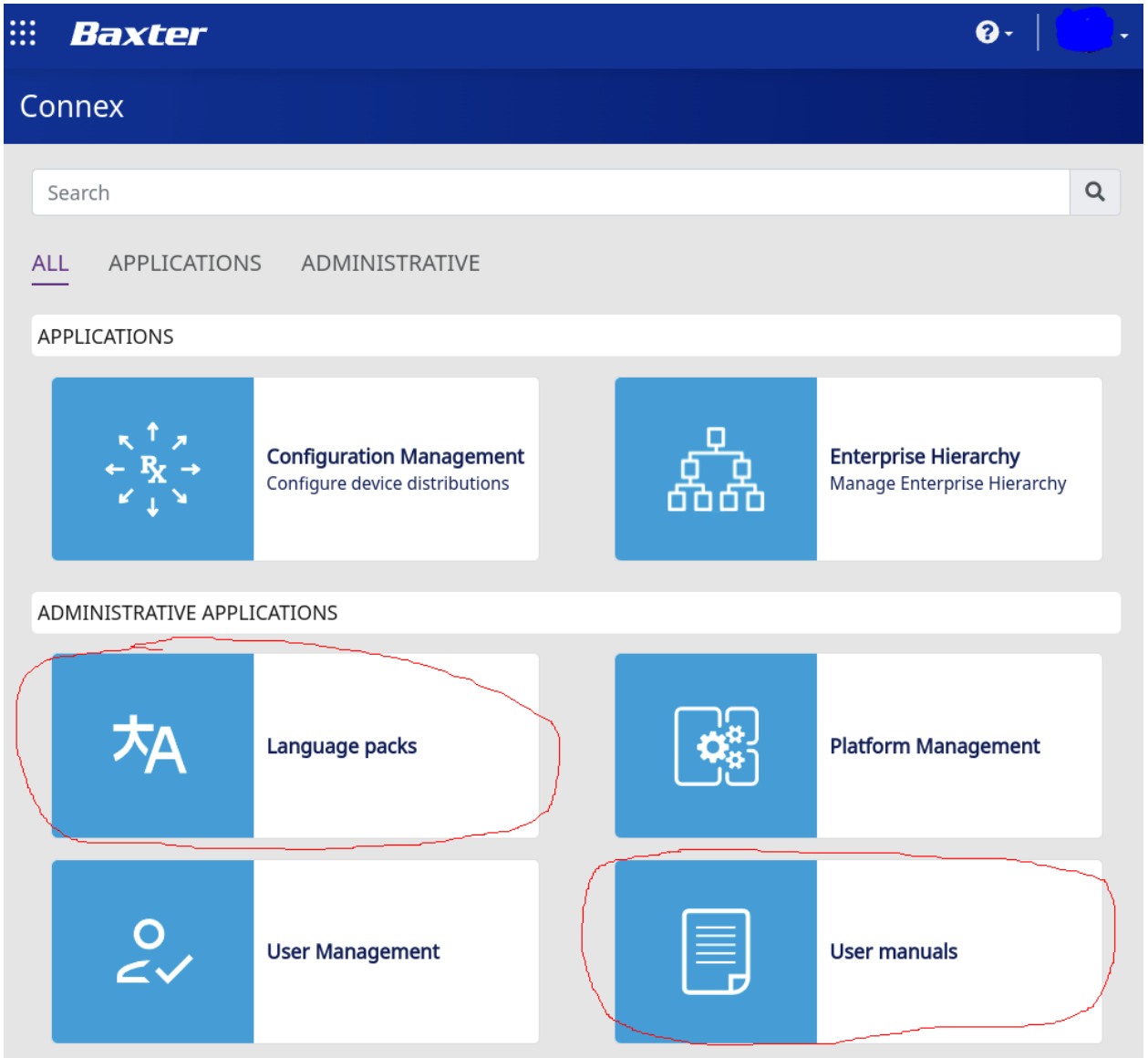
Administrative UI

From version 4.1 onwards, there is a new administrative UI in the BDHP UI. To use it, you need to ensure that your user has been granted the *Manage Language Packs* and/or *Manage User Manuals* permissions.



This will enable 2 new administrative tiles on the dashboard for **Language packs** and **User manuals** respectively.

Release Status:Issued and Effective



This allows you to upload specific language packs and user manuals required by the customer.

Release Status:Issued and Effective

Validation

Qualification of the “BDHP Software Installation Guide 4.4 Single Node” procedure.

1 Procedure

The steps to create the data scenarios and the test case for qualifying this procedure were captured in JAMA. The test case details are given below.

1.1.1 JAMA Test Cases for Qualification

The data pre-requisites and the test-case for qualifying the procedure is available in JAMA. The JAMA test case name is given below.

Test case ID	JAMA Test Case Name	Description
GID-2170980	On-Premise Deployment - LVA Installation with Internet Access - BHP.OP-201-405-410-413-424 CAR-505	To verify the system is able to be deployed into a customer provided virtual platform as an LVA with full internet access.
GID-2201234	On-Premise Deployment - LVA Installation without Internet Access - Postgres - BHP.OP-202	To verify the system is able to be deployed into a customer provided virtual platform as an LVA without internet access, on a Postgres database.
GID-2503142	On-Premise Deployment - LVA Installation without Internet Access - MySQL/Neo4j - BHP.OP-202	To verify the system is able to be deployed into a customer provided virtual platform as an LVA without internet access, onto a mySQL database.

1.1.2 Qualification acceptance criteria

The following conditions need to be met to consider this procedure as qualified:

1. Qualification test case is reviewed and approved.
2. Qualification test case is executed.
3. The Qualification test result is uploaded to JAMA and is reviewed and approved.
4. Any issues observed are documented, reviewed, and dispositioned.

Release Status:Issued and Effective

5. Upon successful completion of the installation the output of helm list -n $namespace | grep baxter-bullseye-gateway will be

i. Test case Test case GID-2170980 was executed, passed and approved à Referenced test run GID-2515763. Therefore this procedure is qualified
ii. Test case GID-2201234 was executed, passed and approved à Referenced test run GID-2515762. Therefore this procedure is qualified
iii. Test case GID-2503142 was executed, passed and approved à Referenced test run GID-2505564. Therefore this procedure is qualified.
iv. The above tests can be found in the BDHP Verification Report, BXU608109

See Attachment A BXU587777/I Install Guide for validation of the Installation Checklist in this document.

Release Status:Issued and Effective

Baxter

TcU ELECTRONIC SIGNATURE REPORT

REVISION INFORMATION	
Item ID: BXU587777	**Revision ID:** I
Item Name: BDHP Software Installation Guide Single Node	**Release Date:** 13-Sep-2024
Description:	
CHANGE INFORMATION	
CN/CR Number (if applicable):	
Description of Change (This field will be blank if required data is not available): PER PR 2856714	
Reason for Change (This field will be blank if required data is not available): PER PR 2856714	

APPROVALS & SIGNATURES for Document Release

Name	Role	Workflow Step	Date of Signature	Decision Taken
Bruning, Megan	Author	Initiate Review	12-Sep-2024	Approved
Johnson-Brand, Lori K	Quality	Document Review - SME & Quality	12-Sep-2024	Approved
Blasius, Christopher	SME	Document Review - SME & Quality	13-Sep-2024	Approved
Drowley, Devin D	Author	Document Review - SME & Quality	13-Sep-2024	Approved
Johnson, Thomas	Change Specialist 3	Release Document(s)	13-Sep-2024	Approved
Johnson, Thomas	Change Specialist 3	Set Effectivity	13-Sep-2024	Approved

Release Status:Issued and Effective