

BASTION DOCUMENTATION



WALLIX Bastion 10.0

hotfix 6

QUICK START GUIDE

Reference: <https://doc.wallix.com/en/Bastion/10.0/Bastion-quickstart-en.pdf>

Copyright © 2024 WALLIX

Table of Contents

1. Introduction	3
1.1. Preamble	3
1.2. Copyright & Licenses	3
1.3. Legend	3
1.4. About this document	3
2. Connection to a physical WALLIX Bastion appliance	5
2.1. Powering on	5
2.2. Physical connection	5
2.3. Sizing of the physical appliance	5
3. Connection to a virtual WALLIX Bastion appliance	6
3.1. Deploying on-premises images	6
3.1.1. Retrieving the ISO and the on-premises images	6
3.1.2. Installing the on-premises images	7
3.2. Deploying Cloud tenant images	8
3.2.1. Retrieving the Cloud tenant images	8
3.2.2. Installing the Cloud tenant images	8
3.3. Configuring the virtual machine	9
3.3.1. Setting the CPUs and the memory	10
3.3.2. Setting the number of concurrent sessions	11
3.3.3. Extending the disk space capacity	12
3.4. Deploying High-Availability in a virtual environment	13
4. Logical connection	17
5. System and network configuration	18
5.1. Factory settings	18
5.2. Pre-configuration of TCP/UDP network ports	18
5.2.1. Communication from WALLIX Bastion	18
5.2.2. Communication to WALLIX Bastion	19
5.3. Configuring the appliance from the Web interface	19
5.3.1. Accessing the Web interface	19
5.3.2. Encryption configuration	20
5.3.3. Network configuration	21
5.3.4. Time service configuration	22
5.3.5. SMTP server configuration	23
5.4. Changing self-signed certificates of services	23
5.4.1. Changing the Web interface certificate	23
5.4.2. Changing the RDP proxy certificate	24
5.4.3. Changing the SSH proxy host key	24
6. License key activation	26
7. First steps	28
8. Contact WALLIX Bastion Support	29

Chapter 1. Introduction

1.1. Preamble

Thank you for choosing WALLIX Bastion.

The WALLIX Bastion solution is marketed in the form of a dedicated, ready-to-use server or as a virtual device for the following virtual environments:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Kernel-based Virtual Machine (KVM)
- Microsoft Azure
- Microsoft Hyper-V
- Nutanix AHV
- OpenStack
- VMware vSphere

This product has been engineered with the greatest care by our teams at WALLIX and we trust that it will deliver complete satisfaction.

1.2. Copyright & Licenses

This document is the property of WALLIX and may not be reproduced without its prior consent.

All the product or company names mentioned herein are the registered trademarks of their respective owners.

WALLIX Bastion is subject to the WALLIX software license contract.

WALLIX Bastion is based on free software. The list and source code of GPL and LGPL licensed software used by WALLIX Bastion are available from WALLIX. Please send your request on Internet by creating a new case at <https://support.wallix.com/> or in writing to:

WALLIX
Service Support
250 bis, Rue du Faubourg Saint-Honoré
75008 PARIS
FRANCE

1.3. Legend

```
prompt $ command to input <parameter to replace>  
command output  
on one or more lines  
prompt $
```

1.4. About this document

This document is the Quick Start Guide for WALLIX Bastion 10.0.6. Use it to guide you through the initial start-up of your device for configuration.


If your device is a physical appliance, refer to Chapter 2, “*Connection to a physical WALLIX Bastion appliance*”, page 5.

If your device is a virtual appliance, refer to Chapter 3, “*Connection to a virtual WALLIX Bastion appliance*”, page 6.

Chapter 2. Connection to a physical WALLIX Bastion appliance

2.1. Powering on

Remove the appliance from its packaging and connect the two redundant power supplies at the back of the device to two 220-volt electrical power sockets using the power cords provided.

Press the start button  on the front to power on the unit.

2.2. Physical connection

Caution:

When adding a network card, the four Ethernet ports eth4 to eth7 at the back of the device are set from right to left.

You can connect to the appliance:

- in console mode, by connecting a screen to the VGA output and a keyboard to a USB slot on either the front or back of the unit
- in network mode, from a workstation running Linux, Windows or Mac OS X that is directly connected to the device with an RJ45 crossed cable (not provided), or through your network if the 192.168.10.5 address is available on it. You must use the Ethernet port labelled "1" at the back of the unit.

2.3. Sizing of the physical appliance

Refer to the sizing information provided in the Table 3.1, "Resource specifications", page 10.

Chapter 3. Connection to a virtual WALLIX Bastion appliance

WALLIX Bastion can be deployed in the following virtual environments:

- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)
- Kernel-based Virtual Machine (KVM)
- Microsoft Azure
- Microsoft Hyper-V
- Nutanix AHV
- OpenStack
- VMware vSphere

WALLIX provides a generic ISO and specific images for the above-mentioned environments.

Whenever a platform-specific image is provided by WALLIX, we recommend installing this image rather than the generic ISO image.

3.1. Deploying on-premises images

On-premises images are available for the following virtual environments:

- the ISO
- AHV
- KVM
- Hyper-V
- OpenStack
- VMware

3.1.1. Retrieving the ISO and the on-premises images

The ISO and the on-premises images available for the deployments on the above-mentioned environments can be downloaded from WALLIX Support portal (<https://support.wallix.com>).

The procedure is as follows:

1. Connect from you Web browser to <https://support.wallix.com> from you Web browser and enter your WALLIX Support credentials.
2. Click on the “Downloads” tab and download the desired image and the corresponding integrity check files for WALLIX Bastion 10.0.6. The available images are as follows:
 - the generic image (.iso)
 - the AHV image (.qcow2 and .ova)
 - the Hyper-V image (.vhdx)

- the KVM image (.qcow2)
 - the OpenStack image (.qcow2)
 - the VMware image (.ova)
3. Check the integrity of the downloaded image using a platform-dependent tool, such as HashCheck on a Windows environment (<https://github.com/gurnec/HashCheck>) or by running the following command for Linux-based systems:

```
$ sha256sum -c bastion-$VERSION-PLATFORM.PLATFORM_EXTENSION.sha256sum
```

where the values for “PLATFORM” and “PLATFORM_EXTENSION” must both match respectively the image type and the image file extension, such as described in the table below:

PLATFORM	PLATFORM_EXTENSION
AHV	qcow2 and ova
Hyper-V	vhdx
KVM	qcow2
OpenStack	qcow2
VMware	ova

3.1.2. Installing the on-premises images

3.1.2.1. AHV

For instructions on how to import the downloaded WALLIX Bastion .qcow2 or .ova disk image into AHV, please refer to the official documentations at <https://portal.nutanix.com/page/documents/list?type=software> and https://portal.nutanix.com/page/documents/details?targetId=Prism-Central-Guide-Prism-v6_0:mul-vm-create-acropolis-pc-t.html.

3.1.2.2. Hyper-V

Important:

The WALLIX Bastion .vhdx disk image must be imported to create a generation 1 virtual machine.

The WALLIX Bastion .iso disk image must be imported to create a generation 2 virtual machine.

For instructions on how to import the downloaded WALLIX Bastion .vhdx or .iso disk image into a Hyper-V hypervisor, please refer to the official documentation at <https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/hyper-v-on-windows-server>.

3.1.2.3. KVM

The virtual machine can be instantiated and the downloaded WALLIX Bastion .qcow2 disk image can be attached using the “libvirt” utility. For further information, please refer to <https://wiki.libvirt.org>.

3.1.2.4. OpenStack

For instructions on how to import the downloaded WALLIX Bastion .qcow2 disk image into OpenStack, please refer to the official documentation at <https://docs.openstack.org>.

Note:

When a raw image is needed for this platform, it is possible to convert the downloaded WALLIX Bastion .qcow2 disk image using the “qemu-img” utility.

As an example, the downloaded .qcow2 disk image for WALLIX Bastion 8.0.0 (i.e. “bastion-8.0.0-openstack.qcow2”) can be converted to a raw format (i.e. “bastion-8.0.0-openstack.img”) by running the following command:

```
qemu-img convert -O raw bastion-8.0.0-openstack.qcow2
bastion-8.0.0-openstack.img
```

3.1.2.5. VMware

For instructions on how to import the downloaded WALLIX Bastion .ova image into a VMware hypervisor, please refer to the official documentation at <https://docs.vmware.com>.

Note:

Only VMware vSphere versions from ESXi 5.5 inclusive are supported.

3.2. Deploying Cloud tenant images

The images are available for the following Cloud environments:

- AWS
- GCP
- Microsoft Azure

3.2.1. Retrieving the Cloud tenant images

The AWS and GCP images are available for WALLIX Bastion 10.0.6 upon request from WALLIX Support (<https://support.wallix.com>).

The image for Microsoft Azure Cloud environment is available for download from the Azure Marketplace.

3.2.2. Installing the Cloud tenant images

Important:

Please contact the WALLIX Support Team for the up-to-date documentation regarding the deployment of WALLIX Bastion in a Cloud environment.

3.2.2.1. Amazon Web Services

Once the WALLIX Support Team has shared the AMI image, WALLIX Bastion can be deployed in an AWS infrastructure.

For instructions on how to deploy the virtual machine from the shared AMI image, please refer to the official documentation at <https://docs.aws.amazon.com>.

Note:

When deploying WALLIX Bastion in an AWS infrastructure, the default password for the factory-set administrator account corresponds to “admin-{instanceID}” where “instanceID” is the EC2 instance ID.

As an example, if this ID corresponds to “i-04a4e1764e07bd88e” then the default password will be “admin-i-04a4e1764e07bd88e”.

3.2.2.2. Google Cloud Platform

Once the WALLIX Support Team has shared the GCP image, WALLIX Bastion can be deployed in a GCP infrastructure.

For instructions on how to deploy the virtual machine on a Google Cloud environment from the shared image, please refer to the official documentation at <https://cloud.google.com/compute/docs>.

3.2.2.3. Microsoft Azure

In order to access the WALLIX Bastion image from the Azure Marketplace, it is required to:

1. Connect from your Web browser to the Microsoft Azure portal at <https://portal.azure.com>.
2. On the home page, click on “Create a resource”.
3. On the “New” page, enter “WALLIX” in the search field then select “WALLIX Bastion”.
4. On the page dedicated to the image for WALLIX Bastion, it is then possible either to create and configure the virtual machine or start with a pre-set configuration.

For instructions on how to create a virtual machine on Microsoft Azure Cloud environment, please refer to the official documentation at <https://docs.microsoft.com/en-us/azure>.

Note:

The virtual machine creation wizard on the Microsoft Azure portal and the programmatic approaches via Azure CLI or Powershell request the creation of a user and password for the virtual machine.

Please note that these credentials will be requested to log on to WALLIX Bastion from the SSH admin channel (port 2242) and will replace the connection with the predefined “wabadmin” user.

3.3. Configuring the virtual machine

Note:

The configuration provided in this section applies to all virtual platforms.

The screenshots describe configuration from vSphere 7.0 hypervisor and are intended for example purposes only.

The parameters of the virtual machine (CPU, RAM) require to be adjusted to fit the needs of your environment.

It is advised, for performance reason, to keep the resources above the following values: 2 CPUs, 4GB of RAM and 50GB HDD.

Number of concurrent sessions (RDP / SSH)	SFTP / SCP network traffic	Number of CPUs	Memory (GB) to reserve
25 / 110	1.6 Gbit/s	4	8
25 / 240	1.6 Gbit/s	4	16
40 / 240	3.2 Gbit/s	8	16
50 / 480	3.2 Gbit/s	8	32
75 / 480	5.0 Gbit/s	16	32

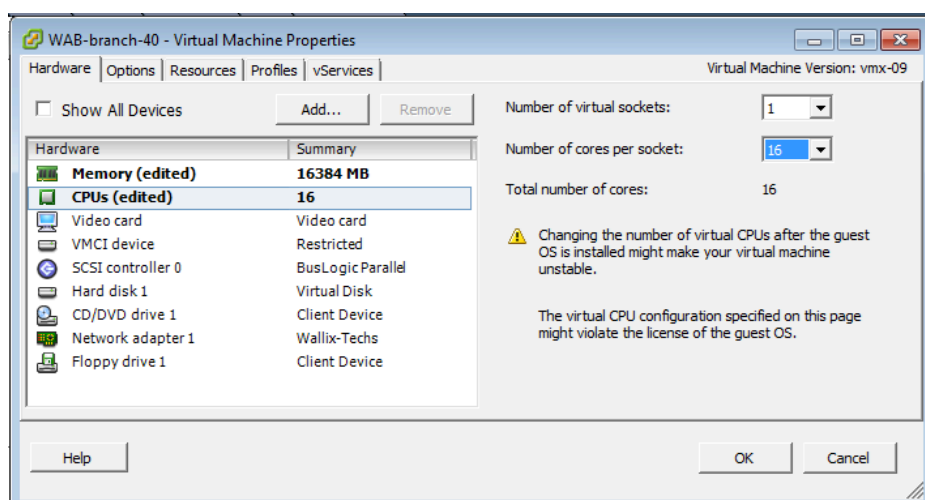
Table 3.1. Resource specifications

The display resolution is 1920x1080 pixels and recording files are not encrypted.

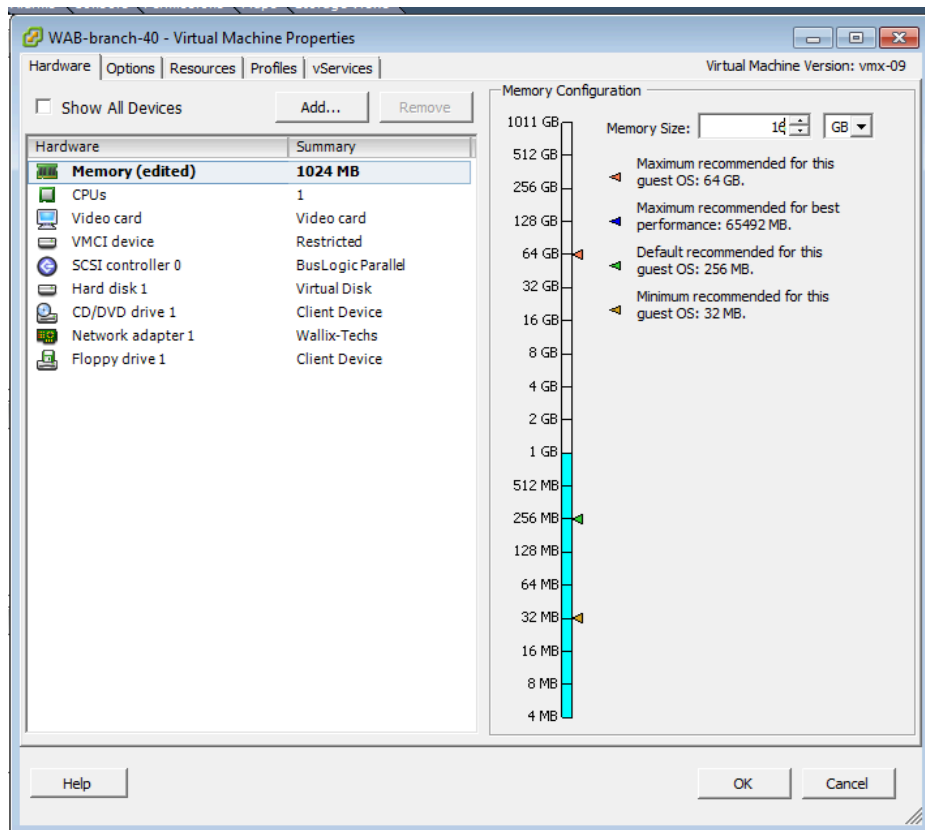
3.3.1. Setting the CPUs and the memory

In order to set the number of CPUs and the memory size:

1. Open the VM properties.
2. On the "Hardware" tab, select "CPUs".
3. In the "Number of virtual sockets" field displayed on the right, set the number of sockets to **1**.
4. In the "Number of cores per socket" field, set the number of cores per socket according to the number of CPUs in the above table (see Table 3.1, "Resource specifications", page 10):



5. On the same tab, select "Memory" and set the size according to the number of GB in the above table (see Table 3.1, "Resource specifications", page 10):



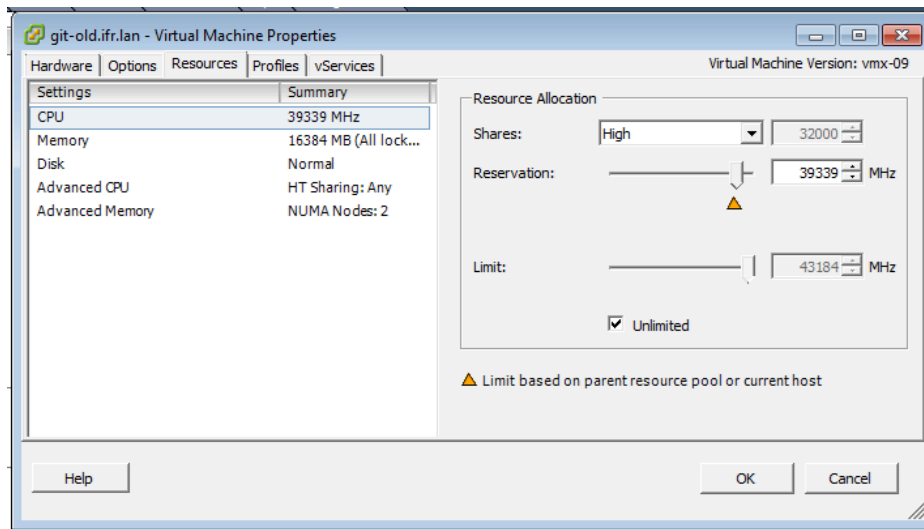
3.3.2. Setting the number of concurrent sessions

The number of concurrent sessions can only be guaranteed if the appropriate numbers of CPU Mhz and the appropriate memory size are reserved.

The reservation operation is necessary to ensure that the resources are available when needed.

To perform these operations:

1. Open the VM properties.
2. On the "Resources" tab, select "CPU".
3. In the "Resource Allocation" area on the right part of the tab, set the value in the "Shares" field to "High" and set the value in the "Reservation" field according to the number displayed in the above table (see Table 3.1, "Resource specifications", page 10).
4. On the same tab, select "Memory" and set the size according to the number of GB in the above table (see Table 3.1, "Resource specifications", page 10):



3.3.3. Extending the disk space capacity

If the session recording files have to be kept for a long time, the default disk space may be too small.

To extend the disk space capacity:

1. Add a new hard drive in the VM hardware properties.
2. Boot up the VM.
3. Log on to the system using the wabadmin account (locally or remotely through SSH).
4. Use the "super" command then the "sudo -i" command to be assigned "root" privileges.
5. Check if the new drive is recognized by WALLIX Bastion: it should be named "**sdb**":

```
# cat /proc/partitions
 8          0      8388608 sda
 8          1      487424 sda1
 8          2           1 sda2
 8          5      7898112 sda5
8          16      8388608 sdb
11          0      1048575 sr0
254         0      1683456 dm-0
254         1      974848 dm-1
254         2      520192 dm-2
254         3      1974272 dm-3
254         4      2744320 dm-4
254         5      520192 dm-5
```

6. Create a new physical volume (PV):

```
# pvcreate /dev/sdb
```

7. Extend the logical volume **vg00**:

```
# vgextend vg00 /dev/sdb
```

8. Stop the services of WALLIX Bastion:

```
# for i in wabwatchdog wabrestapi wabgui wabengine redemption sashimi
wabsystemconfiguration syslog-ng acpid cron wallix-backupdaemon mariadb; do
systemctl stop $i; done
```

9. Resize the **lvwab** volume:

```
# lvresize /dev/vg00/lvwab -l +100%FREE
```

10. Run a check disk:

```
# e2fsck -f /dev/vg00/lvwab
```

11. Resize the filesystem on the new volume:

```
# resize2fs /dev/vg00/lvwab
```

3.4. Deploying High-Availability in a virtual environment

Warning:

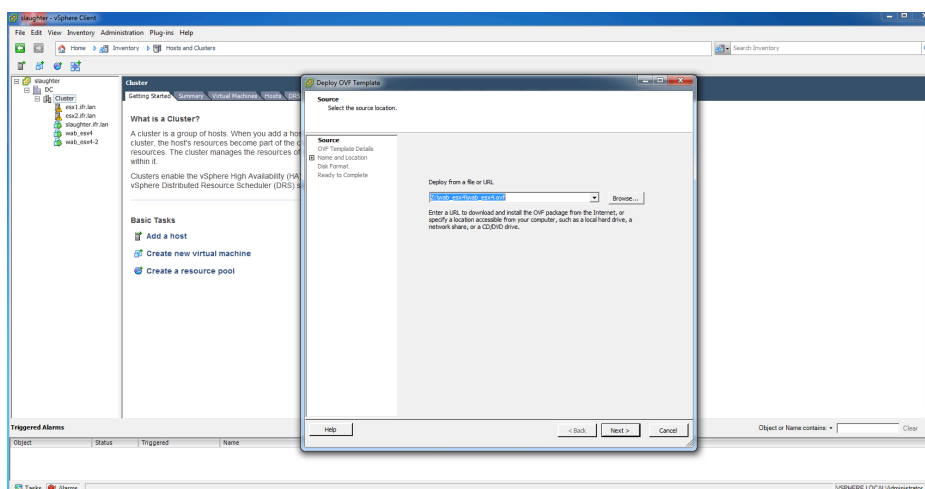
The HA (High-Availability) feature of WALLIX Bastion delivers continuous WALLIX Bastion service through a failover (or active/passive) bi-device cluster (access to target devices and the Web interface, session recordings) in the event that the "Master" device becomes unavailable.

The WALLIX Bastion HA feature is designed to answer hardware issues related to disk, motherboard, network card, etc and is not supported through virtual appliances.

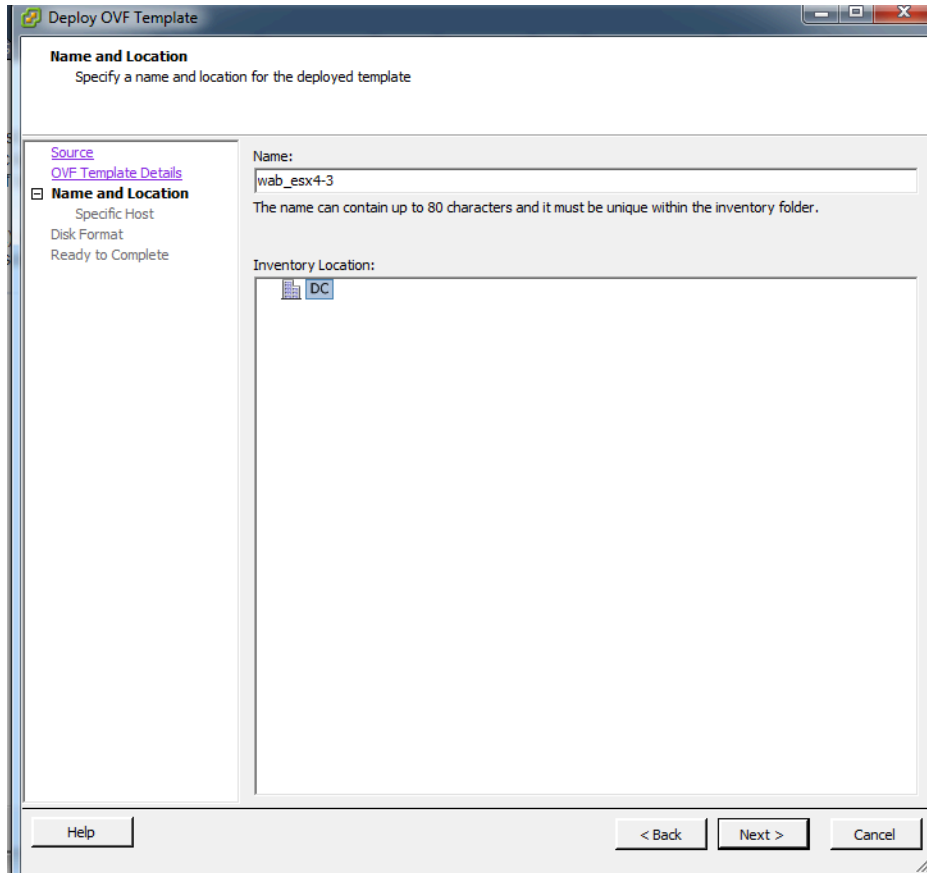
In a virtual environment, the setup is different as there is no "hardware" part. We thus recommend using the High-Availability feature provided by VMware. The High-Availability provided by VMware is available from the entry level VMware license (VMware vSphere Standard) and requires at least two hypervisors. For further information, see <https://www.vmware.com/uk/products/vsphere/high-availability.html>

To deploy the High-Availability feature:

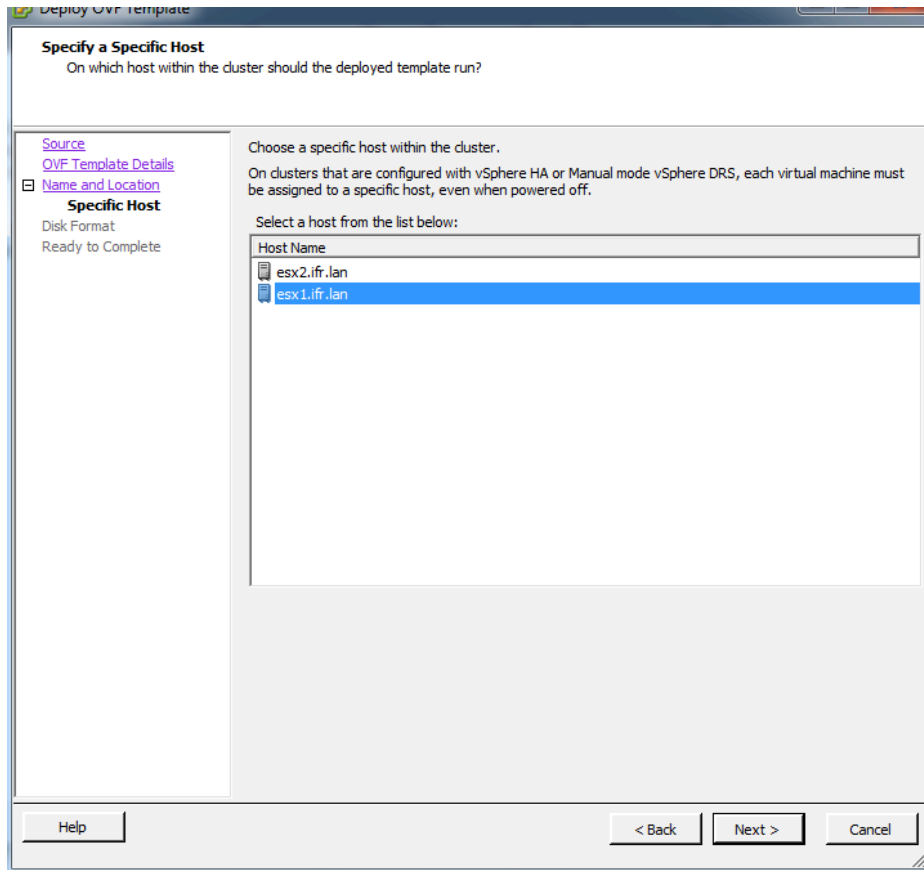
1. Proceed with the deployment of the OVF template the same way as the StandAlone mode.
2. Select the cluster and click on the "File" menu then select "Deploy OVF Template".
3. On the "Deploy OVF Template" window, click on "Browse" and select the file "wab_esx4.ovf" in the "wab_esx4" directory:



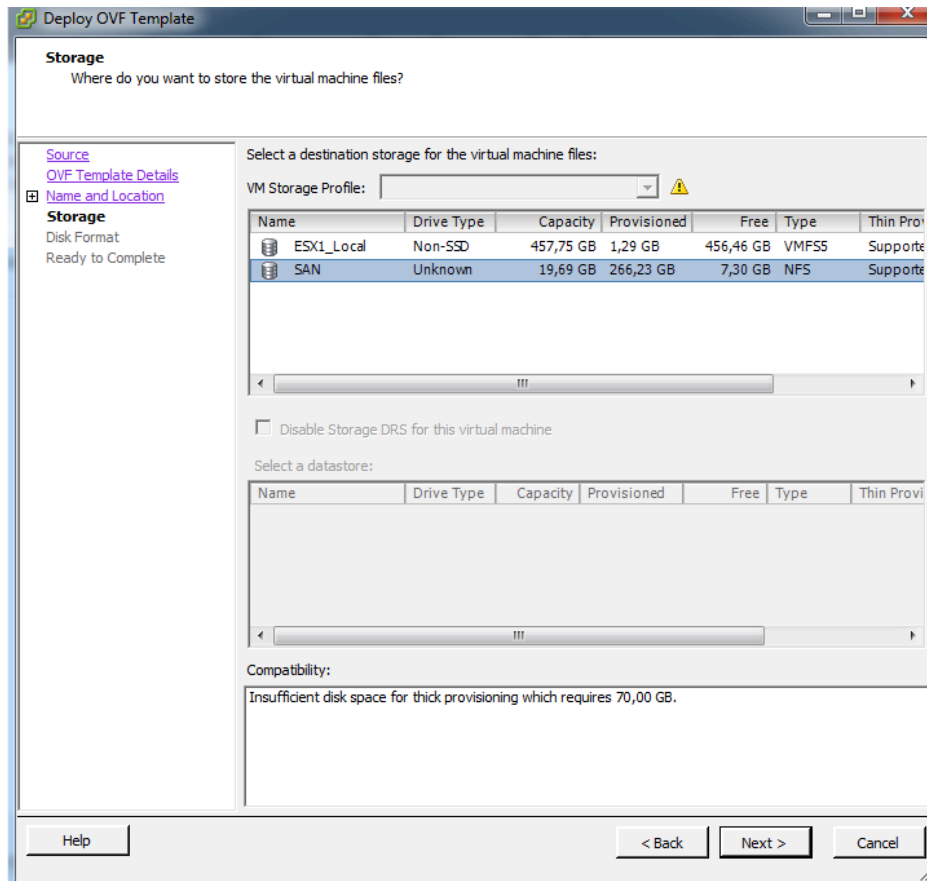
- Click on "Next" until you reach the "Name and Location" section on the left part of window, then specify a datacenter:



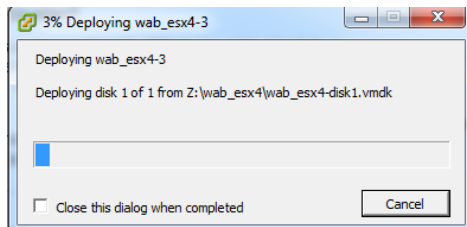
- Click on "Next" and select the desired ESX host on which you want to import the VM:



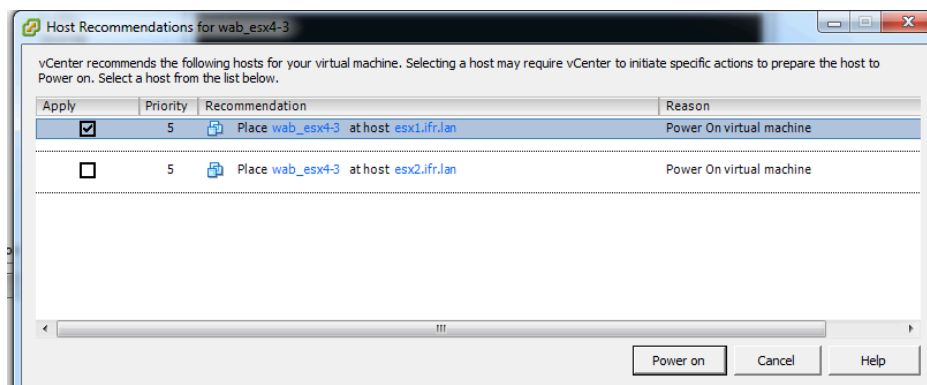
6. Click on "Next" and select the cluster's shared data store:



- Wait until the end of the deployment:



- When you start the VM, a recommendation window is displayed if the settings of the DRS are set to manual: just click on "Power on" at the bottom of the window:



- You now have a hardware resilient WALLIX Bastion using the VMware HA feature.

Chapter 4. Logical connection

You can now connect to the appliance and log on using the following credentials:

- Login: wabadmin
- Password: **SecureWabAdmin**

In console mode:

- using the keyboard and screen connected to the device

In network mode:

- via an SSH connection to WALLIX Bastion:

On your workstation, add a temporary IP address in sub-net 192.168.10.0/24 (other than 192.168.10.5), then use a mater version of an SSH client, for example the "ssh" command (under Linux or Mac OS X) or the PuTTY software (under Windows or Linux), to connect to the address 192.168.10.5 port 2242.

Important:

For security reasons, all system passwords must be immediately changed on first connection. By default, the "wabadmin" user is configured with minimum privileges. The "wabsuper" password can be passed to the "super" command to access higher privileges, including the ability to get access to "root" privileges using the "sudo" command, which uses the same password.

Chapter 5. System and network configuration

Before running any configuration tasks, enter the following command to log on as a super-user:

```
wabadmin$super
[sudo] password for wabsuper:
wabsuper$sudo -i
[sudo] password for wabsuper:
#
```

5.1. Factory settings

The WALLIX Bastion appliance is delivered with the following factory configuration:

- eth0 IP address: 192.168.10.5
- Default gateway: 192.168.10.1
- Login and password of system account: "wabadmin"/"**SecureWabAdmin**"
- SSH TCP port: 2242
- Web interface (also called GUI) port: 443 (HTTPS)
- Login and password of WALLIX Bastion administrator account: "admin"/"admin"
- Web interface and RDP proxy services configured with SSL unique self-signed certificates
- Administration and SSH proxy are configured with unique encryption keys

If you wish to change temporarily your WALLIX Bastion IP address from the console before configuring the Web interface, enter the command below with the desired IP address:

```
# ifconfig eth0 <ip_address>
```

5.2. Pre-configuration of TCP/UDP network ports

5.2.1. Communication from WALLIX Bastion

The following ports should be opened to allow communication from WALLIX Bastion:

- SSH: 22
- RDP: 3389
- HTTP/HTTPS: 80/443
- SMTP: 25
- SMTPS: 465
- SMTP+STARTTLS: 587
- NTP: 123

- DNS: 53
- Kerberos external authentication: 88
- LDAP external authentication: 389
- LDAP over SSL external authentication: 636
- RADIUS external authentication: 1812
- TACACS+ external authentication: 49
- NFS network storage: 2049
- CIFS network storage: 445
- SMB for password management: 139 | 445
- Syslog: 514
- SNMP: 162 for trap notifications

5.2.2. Communication to WALLIX Bastion

The following ports should be opened to allow communication to WALLIX Bastion:

- SSH/SFTP/TELNET/RLOGIN proxy: 22
- RDP/VNC proxy: 3389
- SNMP: 161 for read/write access to OIDs
- WALLIX Bastion administration command line interface (SSHADMIN console): 2242
- WALLIX Bastion administration Web interface (GUI): 443

5.3. Configuring the appliance from the Web interface

The system and network configuration must be configured via the WALLIX Bastion Web interface.

5.3.1. Accessing the Web interface

To access the Web interface, enter the following URL in your browser's address bar:

`https://bastion_ip_address/ui` or `https://<bastion_name>/ui`

Note:

Please refer to the *Release Notes* to check the list of browsers supported by WALLIX Bastion 10.0.6.

When using old web browsers, it may be necessary to lower the security settings of the WALLIX Bastion web server in order to allow connections. To do so, please refer to Section 15.29, “Cryptographic configuration of services” in the *Administration Guide*. However we recommend rather using a modern web browser, such as Firefox or Chrome, to maintain a satisfactory security level.

You can access the legacy interface by clicking on the “Legacy interface” icon at the top of the page.

Then log on as an administrator using the following default credentials:

- User name: admin
- Password: admin

Warning:

For security reasons, it is required to change the administrator account password on first login (from the **My Preferences** page accessible by hovering your mouse over your user name at the top right of the screen).

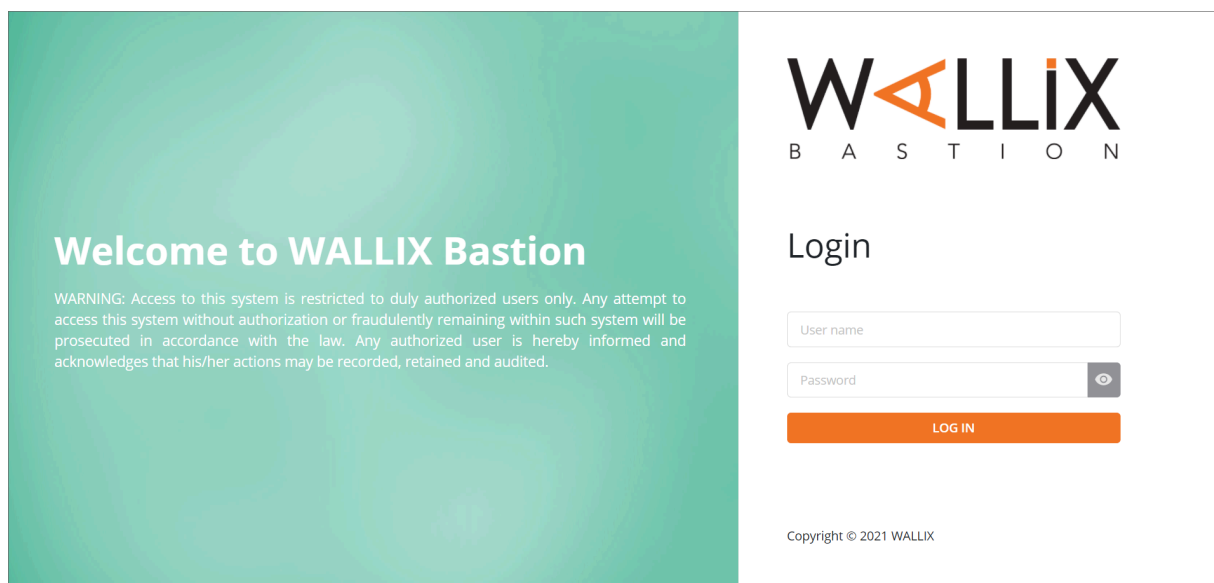


Figure 5.1. Login screen

5.3.2. Encryption configuration

The encryption of WALLIX Bastion secures sensitive data (such as target accounts' credentials, local users' passwords, Web interface connections, SSH and RDP proxy connections, etc.) by using a strong cryptographic algorithm. This algorithm uses an encryption key which is secret and unique to your WALLIX Bastion.

When you first log on to WALLIX Bastion, it is recommended to secure this encryption key by defining a passphrase with a minimum length of 12 characters. This creates an additional protection to prevent a malicious user from decrypting your data. Make sure you remember the passphrase as it must be entered at each reboot of WALLIX Bastion and when changing the passphrase.

Note that once a passphrase has been set, it cannot be deleted.

The screenshot displays the WALLIX Bastion web interface. The top navigation bar includes the WALLIX logo, a home icon, and links for 'Legacy interface', 'Help', and 'admin Bastion Super Administrator'. The left sidebar shows 'Configuration' and 'Bastion' options. The main content area is titled 'Encryption' and features a light blue warning box with the following text:

The encryption feature of Bastion secures sensitive data (target account passwords, etc.) by using a strong cryptographic algorithm. The algorithm uses a confidential encryption key unique to your Bastion.

The definition of a passphrase involves a more complex access to Bastion and raises the protection of your data as no malicious user who does not know the passphrase can access your product. Moreover, at each system reboot, connections using Bastion proxies will not be usable as long as the passphrase is not entered by an administrator in the Web administration interface.

After the encryption initialization phase, we highly recommend you to back up Bastion at least once to keep a copy of the encryption key in a safe place. If you do not perform this action and the passphrase is lost, you will no longer be able to access your data on remote storage.

Below the warning box, the 'Need first initialization' section prompts the user to enter a passphrase to protect the system. It includes two input fields: 'Passphrase' and 'Passphrase confirmation', each with a toggle icon. An 'OR' separator is provided, followed by a checkbox labeled 'No, I do not need a passphrase protection'. An 'Apply' button is located at the bottom of the section.

Figure 5.2. Encryption initialization screen

You can go back at any time to the “Encryption” page on the “Configuration” menu either to check that your WALLIX Bastion is ready and secured or to change the passphrase.

5.3.3. Network configuration

From **System/Network** on the left menu, you access the "Network" page to enter all the parameters required for correct WALLIX Bastion operation.

WALLIX

System > Network

Network configuration

Name

Hostname

URL / Notifications

FQDN

The fully qualified domain name used in URL to access GUI and in email notifications (shared with the other node when HA is enabled).

Interfaces

Interface name	Bonding interface	Enable IP	DHCP	IP address	Netmask
eth0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No		
eth1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No		
eth2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	No		
eth3	<input type="checkbox"/>	<input type="checkbox"/>	No		

VLAN interfaces

Physical interface: eth0

VLAN tag: +

Interface bonding

Interface name: bond0

Mode: +

Virtual interfaces

Physical interface	Name	Address	Netmask
eth0			+

Routes

☐ Enable IP source routing

Default egress interface: eth0

Gateway: +

Interface name: +

Network: +

Netmask: +

Gateway: +

☐ Enable ICMP redirect

/etc/hosts

Hostname: +

IP: +

localhost: +

bastion? : -

DNS

Domain name: +

Search: +

Server list: +

Apply

Figure 5.3. Network configuration via the Web interface

5.3.4. Time service configuration

From **System/Time Service** on the left menu, you access the "Time Service" page to configure the time zone in which WALLIX Bastion is located, declare external NTP servers and enable or disable the NTP service provided by WALLIX Bastion.

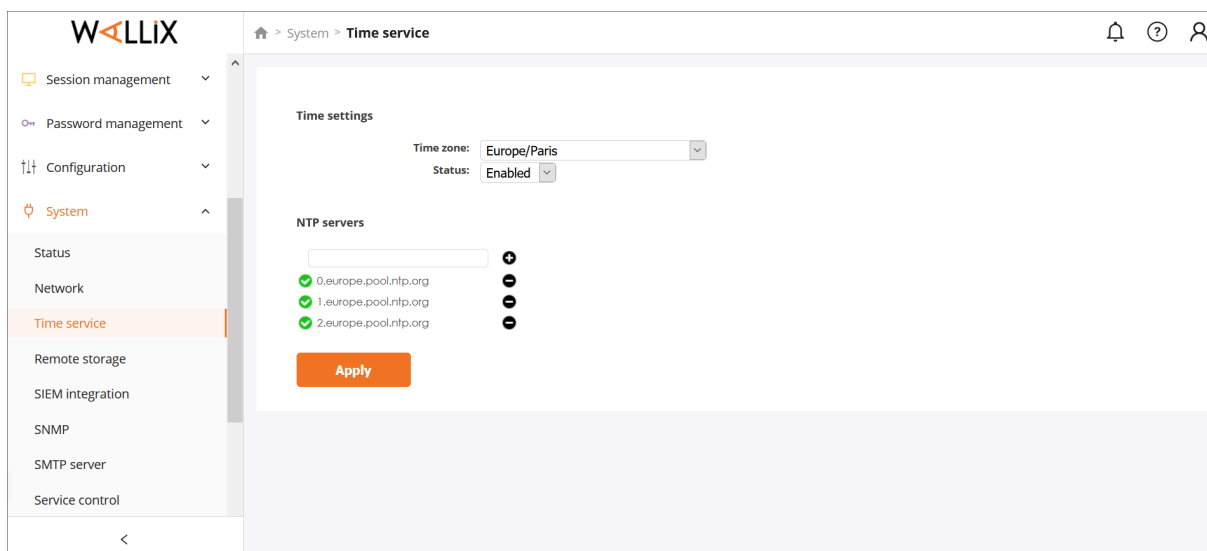


Figure 5.4. NTP configuration via the Web interface

5.3.5. SMTP server configuration

From **System/SMTP Server** on the left menu, you access the "SMTP Server" page to configure your SMTP server. The page includes a "Test" button to test the SMTP server settings.

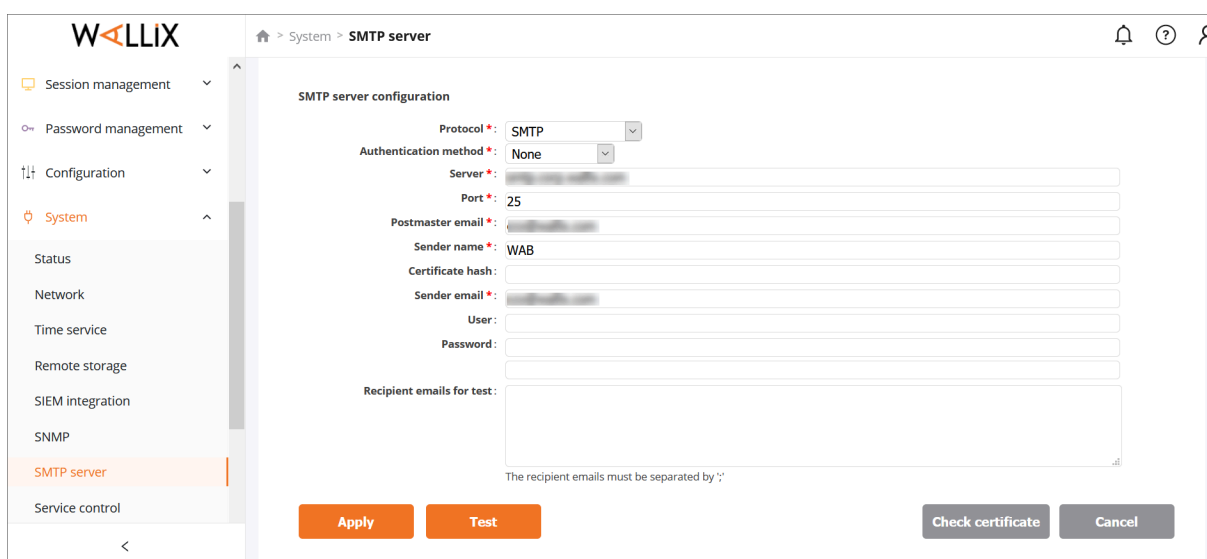


Figure 5.5. SMTP configuration via the Web interface

5.4. Changing self-signed certificates of services

5.4.1. Changing the Web interface certificate

Replace the following certificate files in the directory `/var/wab/apache2/ssl.crt`:

- `ca.crt` (root authority certificate)

Note:

The new certificate generated as a .pem file must be converted into a .crt file prior to be replaced in the directory.

- server.pem (public key)
- server.key (private key)
- and possibly crl.pem (certificate revocation list). If there is no need to revoke a site, then do not replace the default crl.pem file.

Once the files have been replaced, it may be necessary to restart the Apache service by entering the following command:

```
# systemctl restart apache2
```

Note:

These files are also modified by applying the X509 authentication configuration procedure. For further information, refer to Section 9.7, “X509 certificate authentication configuration” in the *Administration Guide*.

If High-Availability is set, the directory into which the certificates are gathered is shared between both nodes. The procedure is to be applied on the active node only.

You could later generate back a self-signed certificate with the following command:

```
# WABGuiCertificate selfsign -f
```

5.4.2. Changing the RDP proxy certificate

To install your certificate, copy it on WALLIX Bastion in PEM format, with its associated private key. Then, on the SSH console (2242), execute the following command replacing the parameters by the full path of the corresponding files:

```
# rdpcert --key --inkey=./<2048_bit_rsa_private_key_file>.key --x509  
--inx509=./<X509_certificate_file>.pem --force
```

Once the files have been replaced, restart RDP proxy by entering the following command:

```
# systemctl restart redemption
```

Note:

You could later generate back a self-signed certificate with the following command:

```
# rdpcert --key --force
```

5.4.3. Changing the SSH proxy host key

To install your host key using RSA +PEM format, copy it on WALLIX Bastion in the directory /var/wab/etc/ssh/server_rsa.key location.

The host key must use RSA algorithm and a minimum 4,096-bit length is recommended.

To install your host key using ED25519 format, copy it on WALLIX Bastion in the directory /var/wab/etc/ssh/server_ed25519.key location.

Note:

You can generate an SSH proxy host key on WALLIX Bastion by deleting the current host keys and executing the generator script with the following command:

```
# rm /var/wab/etc/ssh/server_rsa.key  
# rm /var/wab/etc/ssh/server_ed25519.key  
# WABSSHServerGenRsaKey.sh
```

Chapter 6. License key activation

WALLIX Bastion 10.0.6 comes with a license mechanism that ensures you use the product in accordance with the terms of your sales contract. The terms of this contract are encoded into a license key provided by WALLIX.

From the “License” page on the “Configuration” menu, you can view the license properties and update the license key.

According to the terms of the sales contract, the license mechanism can check:

- the license type for a perpetual license agreement (“Legacy Bastion license”)
- the pack for a subscription license agreement (“WALLIX license”)
- the add-ons for a subscription license agreement (“WALLIX license”)
- the license expiration date
- the number of concurrent connections to the Bastion (i.e. primary connections)

Note:

Connections of the administrator account with the "product_administrator" profile are not counted.

- the number of concurrent connections to targets (i.e. secondary connections)
- the number of users which can be named, i.e. the number of unique users declared in WALLIX Bastion or who connected from an LDAP domain mapping
- the number of protected resources, i.e. the number of devices and applications declared in WALLIX Bastion
- when WALLIX Session Manager is associated with the license key, the number of targets included in groups which can be declared to initiate sessions

Note:

Each target is only counted once, regardless of the number of groups into which it is included.

Target accounts which can be used as scenario accounts are not counted.

- when WALLIX Password Manager is associated with the license key, the number of targets included in groups which can be declared to check out the accounts' credentials

Note:

Each target is only counted once, regardless of the number of groups into which it is included.

- when WALLIX Password Manager is associated with the license key, the number of clients using WALLIX Application-to-Application Password Manager (also called “WAAPM”). Documentation related to WAAPM can be downloaded from WALLIX Support portal (<https://support.wallix.com> [<https://support.wallix.com/>]).

To obtain a license, a context file must be created and sent to WALLIX Support (<https://support.wallix.com/>). To do so, click on the “Download context file” button to generate and

download a context file and send it to the WALLIX Support Team which will provide you with a license key update.

Once you have received the license update file, upload or drag-and-drop it in the “License update” section and click on the “Apply” button.

Once you have installed a license on WALLIX Bastion, it will be possible to revoke it by clicking on the “Revoke” button. The legacy licences (“Legacy Bastion license”) will be revoked immediately. The current licenses (“WALLIX license”) will become invalid 15 days after performing the revocation.

Chapter 7. First steps

Follow the steps below to start using WALLIX Bastion. For more advanced features, please refer to the *Administration Guide* or the *User Guide*.

1. Go to **Users/Accounts** on the left menu to create users.

Refer to Section 9.1, “User accounts” in the *Administration Guide*.

2. Create one or more user groups in **Users/Groups** on the left menu then add users into one or more groups.

Refer to Section 9.2, “User groups” in the *Administration Guide*.

3. Declare the target domains in **Targets/Domains** on the left menu, and link accounts.

Refer to Section 10.3, “Domains” in the *Administration Guide*.

4. Declare the target servers in **Targets/Devices** on the left menu, and add services.

Refer to Section 10.1, “Devices” in the *Administration Guide*.

5. Go to **Targets/Accounts** on the left menu to declare target accounts on each of your devices’ services.

Refer to Section 10.4, “Target accounts” in the *Administration Guide*.

6. Go to **Targets/Groups** on the left menu to create one more target groups and add the target accounts or resources using account mapping.

Refer to Section 10.5, “Target groups” in the *Administration Guide*.

7. Go to **Authorizations/Manage Authorizations** on the left menu to create authorizations for user groups on target groups for the different protocols.

Refer to Section 14.1, “Add an authorization” in the *Administration Guide*.

8. Go to **My Authorizations/Sessions** on the left menu to display the targets to which you can connect using your usual SSH, RDP or Web client and go to **My Authorizations/Passwords** to display the target accounts for which you can view/check out the password.

Refer to Section 12.1, “User authorizations on sessions” and Section 11.1, “User authorizations on passwords” in the *Administration Guide*.

Refer to Section 3.3, ““My authorizations” menu - Session authorizations” and Section 3.4, ““My authorizations” menu - Password authorizations” in the *User Guide*.

See also the various sub-headings of Chapter 4, “Connections to target devices” in the *User Guide*.

Chapter 8. Contact WALLIX Bastion Support

Our WALLIX Bastion Support Team is available to help you during hours defined in your support contract:

Web: <https://support.wallix.com/>

Telephone: **(+33) (0)1 70 36 37 50** for Europe, Middle East and Africa and **(+1) 438-814-0255** for the Americas

about WALLIX

A software company providing cybersecurity solutions, WALLIX Group is a European specialist in privileged account governance. In response to recent regulatory change (NIS/GDPR in Europe and OVIs in France) and the cybersecurity threats affecting all companies today, Bastion helps users protect their critical IT assets: data, servers, terminals and connected objects.

WWW.WALLIX.COM



WALLIX
CYBERSECURITY SIMPLIFIED