

Xesar

Installationsanleitung Server mit Ubuntu 22.04

Impressum

Produktcode: I.X.3-2-UBUN.AN.INST.SDE.LN | 24R1

Version: Xesar 3.2 | 3.2.x

Ausgabe: 04/2024 DE

Originalbetriebsanleitung

Herausgeber

EVVA Sicherheitstechnologie GmbH

Für den Inhalt verantwortlich

EVVA Sicherheitstechnologie GmbH

Mit dem Erscheinen eines neuen Handbuchs verliert diese Ausgabe seine Gültigkeit.

Die aktuelle Ausgabe erhalten Sie im Downloadbereich von EVVA:



<https://www.evva.com/at-de/service/downloads/>

Alle Rechte vorbehalten. Ohne schriftliche Zustimmung des Herausgebers darf dieses Handbuch, auch nicht auszugsweise, in irgendeiner Form reproduziert oder unter Verwendung elektronischer, mechanischer oder chemischer Verfahren vervielfältigt oder verarbeitet werden.

Dieses Handbuch orientiert sich am Stand der Technik zum Zeitpunkt der Erstellung. Der Inhalt des Handbuchs wurde auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden. Für Fehler technischer oder drucktechnischer Art und ihre Folgen übernehmen wir keine Haftung. Die Angaben in diesem Handbuch werden jedoch regelmäßig überprüft und Korrekturen vorgenommen.

Alle Warenzeichen und Schutzrechte werden anerkannt, Änderungen im Sinne des technischen Fortschritts können ohne Vorankündigungen vorgenommen werden.

Inhaltsverzeichnis

1	EINLEITUNG.....	4
1.1	Allgemeine rechtliche Hinweise	4
1.2	EVVA-Support.....	5
1.3	Zeichenerklärung	6
2	INSTALLATIONSANLEITUNG SERVER MIT UBUNTU 22.04	7
2.1	Voraussetzungen.....	7
2.2	Ubuntu installieren	7
2.3	Docker Maschine erstellen	11
2.4	Xesar 3.1 Installation	13
2.5	Daten-Sicherung	14

1 Einleitung

Dieses Dokument ist ein Auszug des Systemhandbuchs Xesar 3.2.

Die im Xesar-Systemhandbuch beschriebenen Produkte/Systeme dürfen nur von Personen betrieben werden, die für die jeweiligen Aufgabenstellungen qualifiziert sind. Qualifiziertes Personal ist aufgrund seines Know-hows befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

1.1 Allgemeine rechtliche Hinweise

EVVA schließt den Vertrag zur Nutzung von Xesar auf Basis der EVVA-AGB (Allgemeine Geschäftsbedingungen) sowie EVVA-ALB (Allgemeine Lizenzbedingungen) für die Software zum Produkt ab.

Die EVVA-AGB und EVVA-ALB können Sie abrufen:



<https://www.evva.com/at-de/impressum>



Beachten Sie, dass der Einsatz von Xesar gesetzliche, insbesondere datenschutzrechtliche Genehmigungs-, Melde- und Registrierungspflichten (zum Beispiel, wenn ein Informationsverbundsystem entsteht) sowie, bei Einsatz in Unternehmen, Mitbestimmungsrechte der Belegschaft auslösen kann. Die Verantwortung für den rechtskonformen Einsatz des Produktes liegt beim Betreiber.



Die vorstehenden Informationen sind gemäß der im Produkthaftungsgesetz definierten Haftung des Herstellers für seine Produkte zu beachten und müssen an die Betreiber und Nutzer weitergegeben werden. Die Nichtbeachtung entbindet EVVA von der Haftpflicht.

Die nicht verwendungsgemäße Benutzung sowie von EVVA nicht zugelassene Reparaturarbeiten bzw. Modifikationen und nicht fachgerechter Service können zu Funktionsstörungen führen und sind daher zu unterlassen. Änderungen, die nicht von EVVA ausdrücklich zugelassen sind, führen zum Verlust von Haftungs-, Gewährleistungs- und gesondert vereinbarten Garantieansprüchen.



Halten Sie die Systemkomponenten von Kleinkindern und Haustieren fern. Erstickungsgefahr durch verschluckbare Kleinteile.



Für **Architekten und beratende Institutionen** stellt EVVA alle erforderlichen Produktinformationen zur Verfügung, damit sie ihren Informations- und Instruktionspflichten gemäß Produkthaftungsgesetz nachkommen können.

Fachhändler und Verarbeiter müssen alle Hinweise in den EVVA-Dokumentationen beachten und diese bei Bedarf an ihre Kunden übermitteln.

Zusätzliche Informationen erhalten Sie im Produktkatalog von EVVA:



<https://www.evva.com/at-de/xesar>

1.2 EVVA-Support

Mit Xesar steht Ihnen ein ausgereiftes und geprüftes Schließsystem zur Verfügung. Wenn Sie zusätzlich Unterstützung benötigen, wenden Sie sich bitte direkt an Ihren EVVA-Partner.

Die Liste zertifizierter EVVA-Partner können Sie hier abrufen:



<https://www.evva.com/at-de/haendlersuche/>

Aktivieren Sie die Filter-Option „Elektronik-Partner“, um gezielt nach EVVA-Partnern, die elektronische EVVA-Schließsysteme vertreiben und über ein qualifiziertes Fachwissen verfügen, zu suchen.



<https://www.evva.com/de/xesar/support/>








Allgemeine Informationen zu Xesar können Sie hier abrufen:



<https://www.evva.com/at-de/xesar>

1.3 Zeichenerklärung

Folgende Zeichen werden im Systemhandbuch zur besseren Darstellung verwendet:

Symbol	Bedeutung
	Achtung, Gefahr eines Sachschadens, wenn die entsprechenden Vor- sichtsmaßnahmen nicht eingehalten werden
	Hinweise und zusätzliche Informationen
	Tipps und Empfehlungen
	Vermeiden bzw. Fehlermeldungen
	Optionen
	Links
	Schritt bei Handlungsanweisungen

2 Installationsanleitung Server mit Ubuntu 22.04

Nachfolgend erhalten Sie Informationen zur Vorbereitung der Xesar 3.2-Installation auf einem Server mit dem Betriebssystem Ubuntu 22.04 Server.



Die Herstellung der notwendigen IT und Serverumgebung ist nicht Teil dieser Installationsanleitung. Diese muss kundenseitig zur Verfügung gestellt werden und liegt nicht in der Verantwortung von EVVA.

- » Prüfen Sie die Systemvoraussetzungen für Xesar 3.2. **Vor der Installation müssen Sie bestätigen, dass die Systemvoraussetzungen für Xesar 3.2 laut Projektcheckliste und Systemhandbuch erfüllt sind.**

Beachten Sie die aktuelle Projektcheckliste von EVVA:



<https://www.evva.com/at-de/xesar/>



Wir empfehlen dringend, die Xesar 3.2-Installation nur in enger Zusammenarbeit mit dem zuständigen IT-Administrator des Betreibers durchzuführen.

2.1 Voraussetzungen

Für eine erfolgreiche Installation von Xesar 3.2 auf einem Server mit dem Betriebssystem Ubuntu 22.04 LTS Server müssen folgende Voraussetzungen erfüllt sein:

- Xesar Admin PC fortan genannt „Windows Admin Client“ WIN 10/11 PRO mit Installation Manager
- Server mit Ubuntu 22.04
- Xesar 3.2 Systemanforderungen sind erfüllt
- Unterstützte Hypervisor für Virtualisierung: VMWare und Windows Server ab 2016. Nested Virtualization wird hierbei nicht unterstützt.

2.2 Ubuntu installieren

Die nachfolgenden Anweisungen gelten für 22.04

- » Ubuntu 22.04 downloaden



<http://releases.ubuntu.com/>



Tutorial zu Ubuntu Installation



<https://tutorials.ubuntu.com/tutorial/tutorial-install-ubuntu-server#0>

Bootable USB-Stick



<https://tutorials.ubuntu.com/tutorial/tutorial-create-a-usb-stick-on-windows#0>

- » Folgen Sie den Anweisungen bei der Installation
- » Während der Installation von Ubuntu wählen Sie im letzten Schritt des Installiers als Option **open ssh server**.



Wenn diese Option nicht zur Auswahl steht, kann sie mit dem Befehl **sudo apt install openssh-server** in der Linux Konsole im Nachhinein installiert werden. Wenn „sudo ohne Passwort“ (siehe unten) noch nicht konfiguriert ist, wird das user-Passwort abgefragt.

- » Um sudo ohne Passwort einzurichten, geben Sie folgende Befehle in der Linux Konsole ein:
 - » Befehl **sudo visudo** zur Passwortabfrage für sudo eingeben (Passwort wird abgefragt und das file /sudoers.d wird geöffnet)
 - » Scrollen Sie bis zum Ende der geöffneten Datei und tippen Sie den Befehl **username ALL=(ALL) NOPASSWD: ALL** unter die letzte Zeile:

```
@includedir /etc/sudoers.d
shqadmin ALL=(ALL) NOPASSWD: ALL
```

- » Datei speichern (Strg+O und anschließend ENTER)
- » Datei schließen (Strg+X)
- » Prüfen Sie, ob das comand **sudo visudo** jetzt ohne Passwortabfrage funktioniert.

- » Erstellen Sie in der Linux Konsole ein **SSH Keypair** mit dem Befehl **ssh-keygen -t ed25519**.

```
shqadmin@test:~$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/shqadmin/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shqadmin/.ssh/id_ed25519
Your public key has been saved in /home/shqadmin/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:/gxqd3yA/mdFKVLce154ADDkzQ07+FcIVT6ZA2BkYxk shqadmin@test
The key's randomart image is:
+--[ED25519 256]--+
  |                |
  |  .=EB=...      |
  |  .+*+=+00     |
  |   0.= 0X0     |
  |   ...=. *     |
  |   S. ..0.+    |
  |   .. . . .    |
  |   .0. . .     |
  |   ..0+0 +     |
  |   ... 0++     |
  +-----[SHA256]-----+
```

Der SSH Key wird standardmäßig unter `/home/user/.ssh` auf dem Linuxserver abgelegt. In unserem Beispiel ist der User **shqadmin**, den wir beim Erstellen der Linuxinstallation angelegt haben.

Als nächsten Schritt müssen Sie in der Linux Konsole den erstellten public key (.pub) des keypairs zu den autorisierten Keys auf dem Linux Server hinzufügen.

- » Wechseln Sie mit der ersten Kommandozeile ins zuvor erstellte Verzeichnis
- » Fügen Sie mit der zweiten Zeile den Key hinzu:

- » **cd /home/user/.ssh**
- » **cat id_ed25519.pub > authorized_keys**

```
shqadmin@test:~$ cd /home/shqadmin/.ssh
shqadmin@test:~/.ssh$ cat id_ed25519.pub > authorized_keys
```

- » Installieren Sie Docker:
 - » **sudo apt install docker.io**
- » Installieren Sie ein Programm am Windows Admin Client (z.B. putty oder WINSXP), um Daten sicher vom Windows Admin Client) zum Server und entgegengesetzt zu übertragen). In unserem Beispiel wird WINSXP verwendet.



Freeware-Programm



<https://winscp.net/eng/download.php>

» Mittels WINSCP am Server einloggen

Übertragungsprotokoll **1** ist SFTP

Rechnername **2** ist die IP-Adresse des Servers (kann in der Linux Konsole mit dem Befehl **ifconfig** ermittelt werden)

Port **3** ist 22 (Standard)

Benutzer und Kennwort **4** entsprechen dem User und seinem Kennwort am Linux Server

```

shqadmin@test:~$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:13:b6:29:de txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.8.145 netmask 255.255.255.0 broadcast 192.168.8.255
    inet6 fe80::215:5dff:fe14:ca15 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:14:ca:15 txqueuelen 1000 (Ethernet)
    RX packets 1234 bytes 612765 (612.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 140 bytes 12653 (12.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                
```

2 → eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

Sitzung

Übertragungsprotokoll: **1** SFTP

Serveradresse: **2** 192.168.8.216 Portnummer: **3** 22

Benutzername: **4** shqadmin Kennwort:

Speichern Erweitert...

» Den Private Key **id_ed25519** mittels WINSCP auf den Windows Admin Client kopieren.

(In unserem Beispiel von `/home/shqadmin/.ssh` **5** am Server nach `C:/Program Files\EVVA\Xesar3 Installation Manager 2.0\runtime\bin` **6** auf den Windows Admin Client

- » Windows Konsole öffnen
(Mit **cmd** in Suche, Rechtsklick als Admin ausführen)
- » Mit dem Befehl **cd C:/Program Files\EVVA\Xesar3 Installation Manager 2.0\runtime\bin** in der Windows Konsole in das Verzeichnis, in dem der Private Key id_ed25519 abgelegt wurde, wechseln

2.3 Docker Maschine erstellen

- » Geben Sie den Befehl zur Erstellung der Docker-Maschine in die Windows Konsole ein (ebenfalls aus dem Verzeichnis, in dem der Private Key liegt)

```
C:\Users\Administrator>cd C:\Program Files\EVVA\Xesar3 Installation Manager 2.0\runtime\bin
C:\Program Files\EVVA\Xesar3 Installation Manager 2.0\runtime\bin>docker-machine --debug create --driver generic
--generic-ip-address 192.168.8.10 --generic-ssh-key id_ed25519 --generic-ssh-user shqadmin hostname
```

Der Befehl lautet generell:

docker-machine create --driver generic --generic-ip-address (IP Adresse des Servers) --generic-ssh-key (Name des Private keys) --generic-ssh-user (Name des users der für Ubuntu Server erstellt wurde) (Name der docker machine)

Befehlsteil	Erklärung
docker-machine create	ist der generelle Befehl zum Erstellen einer Docker Maschine
--driver generic	ist der generische Treiber zum Installieren von Docker auf dem Server
--generic-ip-address	ist die IP Adresse des Servers
--generic-ssh-key	ist die Angabe des verwendeten Private Keys. (Wenn aus dem Verzeichnis, in dem er abgelegt ist, ausgeführt wird. Bei einem anderen Verzeichnis muss der ganze Pfad angegeben werden.)
--generic-ssh-user	ist Angabe des ssh users (in unserem Beispiel „shqadmin“). Mit einem Abstand folgt der Name der Docker Maschine (in unserem Beispiel xs3ubuntu1804).



Der gesamte Vorgang docker-machine create dauert je nach Rechner ca. 2 bis 10 Minuten.



Sollte es zu einer unerwarteten Fehlermeldung kommen, können Sie den Prozess durch Beenden der Windows Konsole abbrechen. Öffnen Sie anschließend die Windows Konsole erneut und löschen Sie die nicht korrekt erstellte docker machine mit dem Befehl `docker-machine rm „name“` (name ist der vergebene Name).
Beispiel: `docker-machine rm xs3ubuntu1804`

- » Danach geben Sie den Befehl **docker-machine --debug create --driver generic --generic-ip-address (IP Adresse des Servers) --generic-ssh-key (Name des Private keys) --generic-ssh-user (Name des users der für Ubuntu Server erstellt wurde) (Name der docker machine)** ein. Verwenden Sie den Zusatz `--debug`, um eine genaue Fehlerausgabe zu erhalten.

Bei einer Fehlermeldung in Bezug auf die **ssh Verbindung**, prüfen sie nochmals den user mit **sudo** ohne Passwort bzw. die Ablage der **ssh-keys**.

Eine weitere Fehlerquelle in Bezug auf ssh stellt der Ordner `C:\Windows\System32\OpenSSH` dar. Benennen Sie diesen im Fehlerfall (ssh exit status) zu `...oldOpenSSH` um.

- » Nach erfolgreicher Erstellung der Docker-Maschine überprüfen Sie in der Windows Konsole mit dem Befehl **docker-machine ls**, ob die docker-machine auch läuft.

```
C:\Users\Test10>docker-machine ls
NAME      ACTIVE DRIVER  STATE  URL                SWARM  DOCKER  ERRORS
ks3r3     -      generic Running tcp://192.168.0.181:2376 v18.09.0
ks3photon2 -      generic Running tcp://192.168.0.136:2376 v18.06.2-ce
xs3ubnt18044 -      generic Timeout
```

2.4 Xesar 3.2 Installation

» Laden Sie die aktuelle Xesar 3.2-Software herunter

» <https://www.evva.com/at-de/produkte/elektronische-schliess-systeme-zutrittskontrolle/xesar/xesar-software-download/>

» Codierstation anstecken

» Öffnen Sie den Installation-Manager

» Wählen Sie Xesar-Anlagen auf Server → Anlagen verwalten

» Wählen Sie den Tab AdminCard

» Wählen Sie den benötigten Kartenleser 7

» Laden Sie die Admin-Karte 8

» Klicken Sie auf den Button 9, um die Nummer der Admin-Karte einzulesen

» Wählen Sie den Tab Konfiguration

» Wählen Sie die Docker Machine 10

» Wählen Sie den Tab **Installations**

» Fügen Sie mit „+“ eine neue Installation hinzu

» Wählen Sie den Namen 11, die Ports 12 sowie die Docker Machine 13 aus



Bei einem Update von Xesar 2.2 geben Sie den Datenbankpfad für den Import ein.

Nach Abschluss der Anlagen-Erstellung können Sie die Anlage starten und in Betrieb nehmen (siehe Systemhandbuch).

2.5 Daten-Sicherung

Folgende Daten müssen gesichert werden:

- Backup aus dem Installation Manager (Anlage → Stiftsymbol → Backup)
- **Windows Admin Client**
[XesarUser] ist dabei ein Platzhalter für den Windows User (z.B. admin), mit dem die Xesar 3.2-Installation durchgeführt wurde
 - C:\System\Users\[XesarUser]\.xesar
 - C:\System\Users\[XesarUser]\.xesar-cs
 - C:\System\Users\[XesarUser]\.docker
 - ssh key



Im Installation-Manager können manuelle und automatische Datensicherungen (Backup) durchgeführt werden.

- **VM Server**
 - Snapshot der VM nach jeder größeren oder wichtigen Änderung
 - Generell eine Spiegelung der ganzen Partition, besser der kompletten Festplatte, auf der die Xesar VM (z.B. Ubuntu) installiert ist – im Normalfall bei Servern üblich
 - ssh key
- **Server physisch**
 - komplette Festplatte

www.evva.com