ZStack Cloud

ZMigrate Support Matrix

Document Version: V20250930

Shanghai Yunzhou Technology Co.,Ltd.

ZStack Cloud

Copyright Statement

Trademark

Shanghai Yunzhou Technology Co., Ltd. reserves all rights to its trademarks, including, but not limited to ZStack and other trademarks in connection with Shanghai Yunzhou Technology Co., Ltd.

Other trademarks or registered trademarks presented in this document are owned or controlled solely by its proprietaries.

Notice

The products, services, or features that you purchased are all subject to the commercial contract and terms of Shanghai Yunzhou Technology Co., Ltd., but any part or all of the foregoing displayed in this document may not be in the scope of your purchase or use. Unless there are additional conventions, Shanghai Yunzhou Technology Co., Ltd. will disclaim any statement or warranty, whether implicit or explicit, on the contents of this document.

In an event of product version upgrades or other reasons, the contents of this document will be irregularly updated and released. Unless there are additional conventions, this document, considered solely as a reference guide, will not make any warranty, whether implicit or explicit, on all the statements, information, or suggestions.

Table of Contents

1 ZMigrate Support Matrix

1.1 Overview

This article aims to explain the compatibility of ZStack ZMigrate migration software, including compatibility support for clients as well as support instructions for VMware agentless mode.

Regarding the support for Linux client software, currently, only the corresponding kernels for which installation packages and drivers have been compiled and adapted are listed. If the system to be migrated in a project is not on the compatibility list, please contact the support team and provide the corresponding Linux distribution and kernel number. The backend will evaluate the compatibility for the corresponding kernel version.

1.2 Management console deployment

The Treker single installation package includes both Treker and management services. It is compatible with physical machines, virtual machines, or cloud instances running the following operating systems:

Operating system	Management + treker	Treker
Windows Server 2012R2	√	√
Windows Server 2016	√	√
Windows Server 2019	√	√
Windows 2022	√	√
Linux Image	√	√
Linux ARM[1]	√	√

[1] Please contact the technical support team if customer has requirement.

1.3 TrekerLite

TrekerLite is a pre-installed version of Treker designed for WinPE based systems. It is available in ISO, VHD, QCOW2, and OVA (VMware) file formats. Once booted from the host system, TrekerLite enables the Treker service on both physical and virtual machines. It can also be utilized to create target cloud instances on any private or public cloud by applying images generated through the VHD, QCOW2, or OVA files associated with TrekerLite.

TrekerLite operates in two modes:

	ISO mode	Image mode
Usage	Movement	Movement and DR
Supported platform	Physical or virtual machines which support booting from DVD/ISO	Private and public cloud, virtual machines (VMware, Hyper-V, Xen)
Footprint system	Run on memory	Run on disk
Keep settings	No, after reboot	Yes, after reboot
Keep jobs	No, after reboot	Yes, after reboot
System Disk Size	Same as source system disk	Source disk plus 5GB
Data Disk Size	Same as source system disk	Same as source system disk
Min. requirement	1 core/2GB memory	1 core/1GB memory

Service roles:

	ISO mode	Image mode
Management	No	No
Source Server – receives synchronized data from source machine	No[1]	Yes
Target Server – writes protection data into target disk	Yes	Yes

[1] In ISO mode, TrekerLite supports only the writing of data into the target disk. In this mode, users are required to set up another Treker to receive protection from the source machine.

1.4 Source Agent

1.4.1 Source Agent Types and Usage

Source Agent supports four major source machine types:

1. Source Agent for Windows: Source machine agent installed on the Windows server/source machine platform to record IO changes and provide online protection to the source server.
2. Source Agent for LinuxSource machine agent installed on the Linux platform to record IO changes and provide online protection to the source server.
3. Source Agent Offline Kit： Pre-installed Source Agent service on WinPE platform to perform protection for shutdown server and attach offline system and data disks to source Treker. Delivered in ISO, VHD, QCOW2, OVA (VMDK) formats

4. Offline Source machine: Source agent installed on the Windows platform, then switched to offline mode. Used to perform protection and attach offline system and data disks to the source server.

Source Agent Types and Usage:

	Windows	**Linux**	**OfflineKit**	**Offline Source machine**
Windows platform	Yes	Yes	Yes	Yes
Linux platform	Yes	Yes	Yes	Yes
For source machine that cannot install agent	No	No	Yes	No
For cloud/SAN disk offline protection	No	No	Yes	Yes
For raw device offline protection	No	No	Yes	Yes
On-line schedule protection	Yes	Yes	No	No
Continuous protection	Yes[1]	Yes[2]	No	No
Incremental protection by snapshot	Yes	Yes	No	No
Incremental protection by checksum	Yes	Yes	Yes	Yes
Protection disk blocks only used by file system (excluded deleted files)	Yes	Yes	Yes	Yes
Exclude selected folders/files	Yes	Yes	No	No
Snapshot Pre/Post-Script	Yes	Yes	No	No

[1] Source Agent for Windows v644 and later support Continuous Data Protection CDP.

[2] Source Agent for Linux v811 and later support Continuous Data Protection CDP.

1.4.2 Source Agent for Windows Support Matrix

Source Agent for Windows can be installed on the following platforms to support any-to-any disk protection and system conversion:

	Installation	Offline Kit	Offline Source machine
Windows 7	√	√	√
Windows 8	√	√	√
Windows 10 32/64bit	√	√	√
Windows Server 2003(SP2) 32bit[1]	√	√	√
Windows Server 2003(SP2) 64bit[1]	√	√	√
Windows Server 2008 32bit	√	√	√
Windows Server 2008 64bit	√	√	√
Windows Server 2008R2	√	√	√
Windows Server 2012	√	√	√
Windows Server 2012R2	√	√	√
Windows Server 2016	√	√	√
Windows Server 2019	√	√	√
Windows Server 2022	√	√	√

[1] It is recommended to update Windows Server 2003 to SP2 and apply latest patches before

[2] The Source Agent for Windows installation package includes Microsoft WHQL certificated IO journal driver. Users do not need to reboot Windows server or source machine after installation. A system reboot is only required for continuous protection.

1.4.3 Source Agent for Linux Support Matrix

Source Agent for Linux can be installed on the following platformsto support any-to-any disk protection and system conversion.

An independent installation package is provided for each Linux kernel. If your Linux kernel version is not listed below, please contact the Lightrek support team. The team will assist in compiling the snapshot driver for your specific kernel.

Major Version	Kernel	Antenna	Offline Kit	Conversion
CentOS				
CentOS 5.3	2.6.18-128.el5	√	√	√
	2.6.18-128.1.1.el5.x86_64	√	√	√
	2.6.18-128.1.6.el5.x86_64	√	√	√
	2.6.18-128.1.10.el5.x86_64	√	√	√
	2.6.18-128.1.14.el5.x86_64	√	√	√
	2.6.18-128.1.16.el5.x86_64	√	√	√
	2.6.18-128.2.1.el5.x86_64	√	√	√
	2.6.18-128.4.1.el5.x86_64	√	√	√
	2.6.18-128.7.1.el5.x86_64	√	√	√
CentOS 5.4	2.6.18-164.el5.x86_64	√	√	√
	2.6.18-164.2.1.el5.x86_64	√	√	√
	2.6.18-164.6.1.el5.x86_64	√	√	√
CentOS 5.5	2.6.18-194.el5	√	√	√
CentOS 5.6	2.6.18-238.el5	√	√	√
CentOS 5.7	2.6.18-274.el5	√	√	√
CentOS 5.8	2.6.18-308.el5	√	√	√
CentOS 5.9	2.6.18-348.el5	√	√	√
CentOS 5.10	2.6.18-371.el5	√	√	√
CentOS 5.11	2.6.18-398.el5	√	√	√
CentOS 6.0	2.6.32-71.el6.x86_64	√	√	√
	2.6.32-71.7.1.el6.x86_64	√	√	√
	2.6.32-71.14.1.el6.x86_64	√	√	√
	2.6.32-71.18.1.el6.x86_64	√	√	√

	2.6.32-71.18.2.el6.x86_64	√	√	√
	2.6.32-71.24.1.el6.x86_64	√	√	√
	2.6.32-71.29.1.el6.x86_64	√	√	√
CentOS 6.1	2.6.32-131.0.15.el6.x86_64	√	√	√
	2.6.32-131.2.1.el6.x86_64	√	√	√
	2.6.32-131.4.1.el6.x86_64	√	√	√
	2.6.32-131.6.1.el6.x86_64	√	√	√
	2.6.32-131.12.1.el6.x86_64	√	√	√
	2.6.32-131.17.1.el6.x86_64	√	√	√
	2.6.32-131.21.1.el6.x86_64	√	√	√
CentOS 6.2	2.6.32-220.el6.x86_64	√	√	√
	2.6.32-220.2.1.el6.x86_64	√	√	√
	2.6.32-220.4.1.el6.x86_64	√	√	√
	2.6.32-220.4.2.el6.x86_64	√	√	√
	2.6.32-220.7.1.el6.x86_64	√	√	√
	2.6.32-220.13.1.el6.x86_64	√	√	√
	2.6.32-220.17.1.el6.x86_64	√	√	√
	2.6.32-220.23.1.el6.x86_64	√	√	√
CentOS 6.3	2.6.32-279.el6.x86_64	√	√	√
	2.6.32-279.1.1.el6.x86_64	√	√	√
	2.6.32-279.2.1.el6.x86_64	√	√	√
	2.6.32-279.5.1.el6.x86_64	√	√	√
	2.6.32-279.5.2.el6.x86_64	√	√	√
	2.6.32-279.9.1.el6.x86_64	√	√	√
	2.6.32-279.11.1.el6.x86_64	√	√	√
	2.6.32-279.14.1.el6.x86_64	√	√	√
	2.6.32-279.19.1.el6.x86_64	√	√	√
	2.6.32-279.22.1.el6.x86_64	√	√	√
CentOS 6.4	2.6.32-358.el6.x86_64	√	√	√
	2.6.32-358.0.1.el6.x86_64	√	√	√
	2.6.32-358.2.1.el6.x86_64	√	√	√

	2.6.32-358.6.1.el6.x86_64	√	√	√
	2.6.32-358.6.2.el6.x86_64	√	√	√
	2.6.32-358.11.1.el6.x86_64	√	√	√
	2.6.32-358.14.1.el6.x86_64	√	√	√
	2.6.32-358.18.1.el6.x86_64	√	√	√
	2.6.32-358.23.2.el6.x86_64	√	√	√
CentOS 6.5	2.6.32-431.el6.x86_64	√	√	√
	2.6.32-431.1.2.0.1.el6.x86_64	√	√	√
	2.6.32-431.3.1.el6.x86_64	√	√	√
	2.6.32-431.5.1.el6.x86_64	√	√	√
	2.6.32-431.11.2.el6.x86_64	√	√	√
	2.6.32-431.17.1.el6.x86_64	√	√	√
	2.6.32-431.20.3.el6.x86_64	√	√	√
	2.6.32-431.20.5.el6.x86_64	√	√	√
	2.6.32-431.23.3.el6.x86_64	√	√	√
	2.6.32-431.29.2.el6.x86_64	√	√	√
CentOS 6.6	2.6.32-504.el6.x86_64	√	√	√
	2.6.32-504.1.3.el6.x86_64	√	√	√
	2.6.32-504.3.3.el6.x86_64	√	√	√
	2.6.32-504.8.1.el6.x86_64	√	√	√
	2.6.32-504.12.2.el6.x86_64	√	√	√
	2.6.32-504.16.2.el6.x86_64	√	√	√
	2.6.32-504.23.4.el6.x86_64	√	√	√
	2.6.32-504.30.3.el6.x86_64	√	√	√
CentOS 6.7	2.6.32-573.el6.x86_64	√	√	√
	2.6.32-573.1.1.el6.x86_64	√	√	√
	2.6.32-573.3.1.el6.x86_64	√	√	√
	2.6.32-573.7.1.el6.x86_64	√	√	√
	2.6.32-573.8.1.el6.x86_64	√	√	√
	2.6.32-573.12.1.el6.x86_64	√	√	√
	2.6.32-573.18.1.el6.x86_64	√	√	√

	2.6.32-573.22.1.el6.x86_64	√	√	√
	2.6.32-573.26.1.el6.x86_64	√	√	√
CentOS 6.8	2.6.32-642.el6.x86_64	√	√	√
	2.6.32-642.1.1.el6.x86_64	√	√	√
	2.6.32-642.3.1.el6.x86_64	√	√	√
	2.6.32-642.4.2.el6.x86_64	√	√	√
	2.6.32-642.6.1.el6.x86_64	√	√	√
	2.6.32-642.6.2.el6.x86_64	√	√	√
	2.6.32-642.11.1.el6.x86_64	√	√	√
	2.6.32-642.13.1.el6.x86_64	√	√	√
	2.6.32-642.13.2.el6.x86_64	√	√	√
	2.6.32-642.15.1.el6.x86_64	√	√	√
CentOS 6.9	2.6.32-696.el6.x86_64	√	√	√
	2.6.32-696.1.1.el6.x86_64	√	√	√
	2.6.32-696.3.1.el6.x86_64	√	√	√
	2.6.32-696.3.2.el6.x86_64	√	√	√
	2.6.32-696.6.3.el6.x86_64	√	√	√
	2.6.32-696.10.1.el6.x86_64	√	√	√
	2.6.32-696.10.2.el6.x86_64	√	√	√
	2.6.32-696.10.3.el6.x86_64	√	√	√
	2.6.32-696.13.2.el6.x86_64	√	√	√
	2.6.32-696.16.1.el6.x86_64	√	√	√
	2.6.32-696.18.7.el6.x86_64	√	√	√
	2.6.32-696.20.1.el6.x86_64	√	√	√
	2.6.32-696.23.1.el6.x86_64	√	√	√
	2.6.32-696.28.1.el6.x86_64	√	√	√
	2.6.32-696.30.1.el6.x86_64	√	√	√
CentOS 6.10	2.6.32-754.el6.x86_64	√	√	√
	2.6.32-754.2.1.el6.x86_64	√	√	√
	2.6.32-754.3.5.el6.x86_64	√	√	√
	2.6.32-754.6.3.el6.x86_64	√	√	√

	2.6.32-754.9.1.el6.x86_64	√	√	√
	2.6.32-754.10.1.el6.x86_64	√	√	√
	2.6.32-754.11.1.el6.x86_64	√	√	√
	2.6.32-754.12.1.el6.x86_64	√	√	√
	2.6.32-754.14.2.el6.x86_64	√	√	√
	2.6.32-754.15.3.el6.x86_64	√	√	√
	2.6.32-754.17.1.el6.x86_64	√	√	√
	2.6.32-754.18.2.el6.x86_64	√	√	√
	2.6.32-754.22.1.el6.x86_64	√	√	√
	2.6.32-754.23.1.el6.x86_64	√	√	√
	2.6.32-754.24.2.el6.x86_64	√	√	√
	2.6.32-754.24.3.el6.x86_64	√	√	√
	2.6.32-754.25.1.el6.x86_64	√	√	√
	2.6.32-754.27.1.el6.x86_64	√	√	√
	2.6.32-754.28.1.el6.x86_64	√	√	√
	2.6.32-754.29.1.el6.x86_64	√	√	√
	2.6.32-754.29.2.el6.x86_64	√	√	√
	2.6.32-754.30.2.el6.x86_64	√	√	√
	2.6.32-754.31.1.el6.x86_64	√	√	√
	2.6.32-754.33.1.el6.x86_64	√	√	√
	2.6.32-754.35.1.el6.x86_64	√	√	√
CentOS 7.0	3.10.0-123.el7.x86_64	√	√	√
	3.10.0-123.1.2.el7.x86_64	√	√	√
	3.10.0-123.4.2.el7.x86_64	√	√	√
	3.10.0-123.4.4.el7.x86_64	√	√	√
	3.10.0-123.6.3.el7.x86_64	√	√	√
	3.10.0-123.8.1.el7.x86_64	√	√	√
	3.10.0-123.9.2.el7.x86_64	√	√	√
	3.10.0-123.9.3.el7.x86_64	√	√	√
	3.10.0-123.13.1.el7.x86_64	√	√	√
	3.10.0-123.13.2.el7.x86_64	√	√	√

	3.10.0-123.20.1.el7.x86_64	√	√	√
CentOS 7.1	3.10.0-229.el7.x86_64	√	√	√
	3.10.0-229.1.2.el7.x86_64	√	√	√
	3.10.0-229.4.2.el7.x86_64	√	√	√
	3.10.0-229.7.2.el7.x86_64	√	√	√
	3.10.0-229.11.1.el7.x86_64	√	√	√
	3.10.0-229.14.1.el7.x86_64	√	√	√
	3.10.0-229.20.1.el7.x86_64	√	√	√
CentOS 7.2	3.10.0-327.el7.x86_64	√	√	√
	3.10.0-327.3.1.el7.x86_64	√	√	√
	3.10.0-327.4.4.el7.x86_64	√	√	√
	3.10.0-327.4.5.el7.x86_64	√	√	√
	3.10.0-327.10.1.el7.x86_64	√	√	√
	3.10.0-327.13.1.el7.x86_64	√	√	√
	3.10.0-327.18.2.el7.x86_64	√	√	√
	3.10.0-327.22.2.el7.x86_64	√	√	√
	3.10.0-327.28.2.el7.x86_64	√	√	√
	3.10.0-327.28.3.el7.x86_64	√	√	√
	3.10.0-327.36.1.el7.x86_64	√	√	√
	3.10.0-327.36.2.el7.x86_64	√	√	√
	3.10.0-327.36.3.el7.x86_64	√	√	√
CentOS 7.3	3.10.0-514.el7.x86_64	√	√	√
	3.10.0-514.2.2.el7.x86_64	√	√	√
	3.10.0-514.6.1.el7.x86_64	√	√	√
	3.10.0-514.6.2.el7.x86_64	√	√	√
	3.10.0-514.10.2.el7.x86_64	√	√	√
	3.10.0-514.16.1.el7.x86_64	√	√	√
	3.10.0-514.21.1.el7.x86_64	√	√	√
	3.10.0-514.21.2.el7.x86_64	√	√	√
	3.10.0-514.26.1.el7.x86_64	√	√	√
	3.10.0-514.26.2.el7.x86_64	√	√	√

CentOS 7.4	3.10.0-693.el7.x86_64	√	√	√
	3.10.0-693.1.1.el7.x86_64	√	√	√
	3.10.0-693.2.1.el7.x86_64	√	√	√
	3.10.0-693.2.2.el7.x86_64	√	√	√
	3.10.0-693.5.2.el7.x86_64	√	√	√
	3.10.0-693.11.1.el7.x86_64	√	√	√
	3.10.0-693.11.6.el7.x86_64	√	√	√
	3.10.0-693.17.1.el7.x86_64	√	√	√
	3.10.0-693.21.1.el7.x86_64	√	√	√
	5.7.11-1.el7.elrepo.x86_64	√	√	√
	5.18.10-1.el7.elrepo.x86_64	√	√	√
CentOS 7.5	3.10.0-862.el7.x86_64	√	√	√
	3.10.0-862.2.3.el7.x86_64	√	√	√
	3.10.0-862.3.2.el7.x86_64	√	√	√
	3.10.0-862.3.3.el7.x86_64	√	√	√
	3.10.0-862.6.3.el7.x86_64	√	√	√
	3.10.0-862.9.1.el7.x86_64	√	√	√
	3.10.0-862.11.6.el7.x86_64	√	√	√
	3.10.0-862.14.4.el7.x86_64	√	√	√
	6.2.11-1.el7.elrepo.x86_64	√	√	√
	6.6.1-1.el7.elrepo.x86_64	√	√	√
CentOS 7.6	3.10.0-957.el7.x86_64	√	√	√
	3.10.0-957.1.3.el7.x86_64	√	√	√
	3.10.0-957.5.1.el7.x86_64	√	√	√
	3.10.0-957.10.1.el7.x86_64	√	√	√
	3.10.0-957.12.1.el7.x86_64	√	√	√
	3.10.0-957.12.2.el7.x86_64	√	√	√
	3.10.0-957.21.2.el7.x86_64	√	√	√
	3.10.0-957.21.3.el7.x86_64	√	√	√
	3.10.0-957.27.2.el7.x86_64	√	√	√
	5.4.145-1.el7.elrepo.x86_64	√	√	√

	5.4.170-1.el7.elrepo.x86_64	√	√	√
	5.18.2-1.el7.elrepo.x86_64	√	√	√
CentOS 7.7	3.10.0-1062.el7.x86_64	√	√	√
	3.10.0-1062.1.1.el7.x86_64	√	√	√
	3.10.0-1062.1.2.el7.x86_64	√	√	√
	3.10.0-1062.4.1.el7.x86_64	√	√	√
	3.10.0-1062.4.2.el7.x86_64	√	√	√
	3.10.0-1062.4.3.el7.x86_64	√	√	√
	3.10.0-1062.7.1.el7.x86_64	√	√	√
	3.10.0-1062.9.1.el7.x86_64	√	√	√
	3.10.0-1062.12.1.el7.x86_64	√	√	√
	3.10.0-1062.18.1.el7.x86_64	√	√	√
CentOS 7.8	3.10.0-1127.el7.x86_64	√	√	√
	3.10.0-1127.8.2.el7.x86_64	√	√	√
	3.10.0-1127.10.1.el7.x86_64	√	√	√
	3.10.0-1127.13.1.el7.x86_64	√	√	√
	3.10.0-1127.18.2.el7.x86_64	√	√	√
	3.10.0-1127.19.1.el7.x86_64	√	√	√
	4.17.11-1.el7.elrepo.x86_64	√	√	√
CentOS 7.9	3.10.0-1160.el7.x86_64	√	√	√
	3.10.0-1160.2.1.el7.x86_64	√	√	√
	3.10.0-1160.2.2.el7.x86_64	√	√	√
	3.10.0-1160.6.1.el7.x86_64	√	√	√
	3.10.0-1160.11.1.el7.x86_64	√	√	√
	3.10.0-1160.15.2.el7.x86_64	√	√	√
	3.10.0-1160.21.1.el7.x86_64	√	√	√
	3.10.0-1160.24.1.el7.x86_64	√	√	√
	3.10.0-1160.25.1.el7.x86_64	√	√	√
	3.10.0-1160.31.1.el7.x86_64	√	√	√
	3.10.0-1160.36.2.el7.x86_64	√	√	√
	3.10.0-1160.41.1.el7.x86_64	√	√	√

	3.10.0-1160.42.2.el7.x86_64	√	√	√
	3.10.0-1160.45.1.el7.x86_64	√	√	√
	3.10.0-1160.49.1.el7.x86_64	√	√	√
	3.10.0-1160.53.1.el7.x86_64	√	√	√
	3.10.0-1160.59.1.el7.x86_64	√	√	√
	3.10.0-1160.62.1.el7.x86_64	√	√	√
	3.10.0-1160.66.1.el7.x86_64	√	√	√
	3.10.0-1160.71.1.el7.x86_64	√	√	√
	3.10.0-1160.76.1.el7.x86_64	√	√	√
	3.10.0-1160.80.1.el7.x86_64	√	√	√
	3.10.0-1160.81.1.el7.x86_64	√	√	√
	3.10.0-1160.83.1.el7.x86_64	√	√	√
	3.10.0-1160.88.1.el7.x86_64	√	√	√
	3.10.0-1160.90.1.el7.x86_64	√	√	√
	3.10.0-1160.92.1.el7.x86_64	√	√	√
	3.10.0-1160.95.1.el7.x86_64	√	√	√
	3.10.0-1160.99.1.el7.x86_64	√	√	√
	3.10.0-1160.102.1.el7.x86_64	√	√	√
	3.10.0-1160.105.1.el7.x86_64	√	√	√
	3.10.0-1160.108.1.el7.x86_64	√	√	√
	3.10.0-1160.114.2.el7.x86_64	√	√	√
	3.10.0-1160.118.1.el7.x86_64	√	√	√
	3.10.0-1160.119.1.el7.x86_64	√	√	√
	5.4.92-1.el7.elrepo.x86_64	√	√	√
	5.4.109-1.el7.elrepo.x86_64	√	√	√
	5.4.119-1.el7.elrepo.x86_64	√	√	√
	5.4.134-1.el7.elrepo.x86_64	√	√	√
	5.4.182-1.el7.elrepo.x86_64	√	√	√
	5.4.206-1.el7.elrepo.x86_64	√	√	√
	5.4.210-1.el7.elrepo.x86_64	√	√	√
	5.4.217-1.el7.elrepo.x86_64	√	√	√

	5.4.265-1.el7.elrepo.x86_64	√	√	√
	5.8.14-1.el7.elrepo.x86_64	√	√	√
	5.16.0-1.el7.elrepo.x86_64	√	√	√
	5.18.3-1.el7.elrepo.x86_64	√	√	√
CentOS 8.0	4.18.0-80.el8.x86_64	√	√	√
	4.18.0-80.11.2.el8_0.x86_64	√	√	√
CentOS 8.1	4.18.0-147.el8.x86_64	√	√	√
CentOS 8.2	4.18.0-193.el8.x86_64	√	√	√
	4.18.0-193.14.2.el8_2.x86_64	√	√	√
	4.18.0-193.28.1.el8_2.x86_64	√	√	√
CentOS 8.3	4.18.0-240.el8.x86_64	√	√	√
	4.18.0-240.1.1.el8_3.x86_64	√	√	√
	4.18.0-240.10.1.el8_3.x86_64	√	√	√
CentOS 8.4	4.18.0-305.el8.x86_64	√	√	√
	4.18.0-305.3.1.el8.x86_64	√	√	√
	4.18.0-305.12.1.el8_4.x86_64	√	√	√
	4.18.0-305.19.1.el8_4.x86_64	√	√	√
CentOS 8.5	4.18.0-348.el8.x86_64	√	√	√
	4.18.0-348.7.1el8.x86_64	√	√	√
	4.18.0-383.el8.x86_64	√	√	√
Redhat				
Redhat 5.5	2.6.18-194.el5	√	√	√
Redhat 5.7	2.6.18-274.el5	√	√	√
Redhat 5.8	2.6.18-308.el5	√	√	√
Redhat 6.2	2.6.32-220.el6.x86_64	√	√	√
Redhat 6.3	2.6.32-279.el6.x86_64	√	√	√
Redhat 6.4	2.6.32-358.el6	√	√	√
Redhat 6.5	2.6.32-431.el6.x86_64	√	√	√
Redhat 6.6	2.6.32-504.el6.x86_64	√	√	√
Redhat 6.8	2.6.32-642.el6.x86_64	√	√	√
	2.6.32-642.11.1.el6.x86_64	√	√	√
	2.6.39-400.278.2.el6uek.i686	√	√	√

Redhat6.9	2.6.32-696.el6.x86_64	√	√	√
Redhat 7.2	3.10.0-327.el7.x86_64	√	√	√
Redhat 7.3	3.10.0-514.el7.x86_64	√	√	√
Redhat 7.4	3.10.0-693.e17.x86 64	√	√	√
	3.10.0-693.17.1.el7.x86_64	√	√	√
	3.10.0-693.21.1.el7.x86_64	√	√	√
Redhat 7.6	3.10.0-957.el7.x86_64	√	√	√
Redhat 7.7	3.10.0-1062.4.3.el7.x86_64	√	√	√
	3.10.0-1062.21.1.el7.x86 64	√	√	√
Redhat 7.8	3.10.0-1127.el7.x86_64	√	√	√
Redhat 7.9	3.10.0-1160.e17.x86_64	√	√	√
	3.10.0-1160.6.1.e17.x86_64	√	√	√
	3.10.0-1160.105.1.el7.x86_64	√	√	√
	3.10.0-1160.119.1.el7.x86_64	√	√	√
RedHat 8.1	4.18.0-147.el8.x86_64	√	√	√
RedHat 8.4	4.18.0-305.17.1.el8_4.x86_64	√	√	√
RedHat 8.5	4.18.0-348.2.1.el8_5.x86_64	√	√	√
RedHat 8.6	4.18.0-372.9.1.el8.x86_64	√	√	√
RedHat 8.9	4.18.0-513.24.1.el8_9.x86_64	√	√	√
RedHat 8.10	4.18.0-553.el8_10.x86_64	√	√	√
RedHat 9.2	5.14.0-284.25.1.el9_2.x86_64	√	√	√
Asianux				
Asianux 3 SP2	2.6.18-128.7AXS3	√	√	√
Asianux 3 SP3	2.6.18-194.1.AXS3	√	√	√
Asianux 3 SP4	2.6.18-238.2.AXS3	√	√	√
Asianux 4.5	2.6.32-754.3.5.AXS4.x86_64	√	√	√
	2.6.32-279.2.1.el6.x86_64	√	√	√
SUSE				
SUSE 10 SP4	2.6.16.60-0.85.1-smp	√	√	√

SUSE 11 SP1	2.6.32.59-0.19.1.11768.0.PTF-default	√	√	√
SUSE 11 SP3	3.0.76-0.11-default	√	√	√
SUSE 11 SP4	3.0.101-63-default	√	√	√
SUSE 12 SP2	4.4.21-69-default	√	√	√
SUSE 12 SP4	4.12.14-94.41-default	√	√	√
	4.12.14-95.77-default	√	√	√
	4.12.14-95.80-default	√	√	√
SUSE 12 SP5	4.12.14-122.147-default	√	√	√
SUSE 15 SP1	4.12.14-195-default	√	√	√
	4.12.14-197.29-default	√	√	√
	4.12.14-197.64-default	√	√	√
SUSE 15 SP4	5.14.21-150400.22.1-default	√	√	√
Ubuntu				
Ubuntu 12.04 LTS	3.2.0-23-generic	√	√	√
Ubuntu14.04 LTS	3.13.0-24-generic	√	√	√
	4.4.40-31-generic	√	√	√
Ubuntu 15.04 LTS	3.19.0-15-generic	√	√	√
Ubuntu 16.04 LTS	4.4.0-21-generic	√	√	√
	4.4.0-87-generic	√	√	√
	4.4.0-97-generic	√	√	√
	4.4.0-116-generic	√	√	√
	4.4.0-131-generic	√	√	√
	4.4.0-210-generic	√	√	√
	4.4.0-229-generic	√	√	√
	4.15.0-36-generic	√	√	√
Ubuntu 18.04 LTS	4.15.0-20-generic	√	√	√
	4.15.0-22-generic	√	√	√
	4.15.0-23-generic	√	√	√
	4.15.0-24-generic	√	√	√

	4.15.0-29-generic	√	√	√
	4.15.0-30-generic	√	√	√
	4.15.0-32-generic	√	√	√
	4.15.0-33-generic	√	√	√
	4.15.0-34-generic	√	√	√
	4.15.0-36-generic	√	√	√
	4.15.0-38-generic	√	√	√
	4.15.0-39-generic	√	√	√
	4.15.0-42-generic	√	√	√
	4.15.0-43-generic	√	√	√
	4.15.0-44-generic	√	√	√
	4.15.0-45-generic	√	√	√
	4.15.0-46-generic	√	√	√
	4.15.0-47-generic	√	√	√
	4.15.0-48-generic	√	√	√
	4.15.0-50-generic	√	√	√
	4.15.0-51-generic	√	√	√
	4.15.0-52-generic	√	√	√
	4.15.0-54-generic	√	√	√
	4.15.0-55-generic	√	√	√
	4.15.0-58-generic	√	√	√
	4.15.0-60-generic	√	√	√
	4.15.0-62-generic	√	√	√
	4.15.0-64-generic	√	√	√
	4.15.0-65-generic	√	√	√
	4.15.0-66-generic	√	√	√
	4.15.0-69-generic	√	√	√
	4.15.0-70-generic	√	√	√
	4.15.0-72-generic	√	√	√
	4.15.0-74-generic	√	√	√
	4.15.0-76-generic	√	√	√

	4.15.0-88-generic	√	√	√
	4.15.0-91-generic	√	√	√
	4.15.0-96-generic	√	√	√
	4.15.0-99-generic	√	√	√
	4.15.0-101-generic	√	√	√
	4.15.0-106-generic	√	√	√
	4.15.0-108-generic	√	√	√
	4.15.0-109-generic	√	√	√
	4.15.0-111-generic	√	√	√
	4.15.0-112-generic	√	√	√
	4.15.0-115-generic	√	√	√
	4.15.0-117-generic	√	√	√
	4.15.0-118-generic	√	√	√
	4.15.0-121-generic	√	√	√
	4.15.0-122-generic	√	√	√
	4.15.0-123-generic	√	√	√
	4.15.0-124-generic	√	√	√
	4.15.0-128-generic	√	√	√
	4.15.0-129-generic	√	√	√
	4.15.0-130-generic	√	√	√
	4.15.0-132-generic	√	√	√
	4.15.0-134-generic	√	√	√
	4.15.0-135-generic	√	√	√
	4.15.0-136-generic	√	√	√
	4.15.0-137-generic	√	√	√
	4.15.0-139-generic	√	√	√
	4.15.0-140-generic	√	√	√
	4.15.0-141-generic	√	√	√
	4.15.0-142-generic	√	√	√
	4.15.0-143-generic	√	√	√
	4.15.0-144-generic	√	√	√

	4.15.0-147-generic	√	√	√
	4.15.0-151-generic	√	√	√
	4.15.0-153-generic	√	√	√
	4.15.0-154-generic	√	√	√
	4.15.0-156-generic	√	√	√
	4.15.0-158-generic	√	√	√
	4.15.0-159-generic	√	√	√
	4.15.0-161-generic	√	√	√
	4.15.0-162-generic	√	√	√
	4.15.0-163-generic	√	√	√
	4.15.0-166-generic	√	√	√
	4.15.0-167-generic	√	√	√
	4.15.0-169-generic	√	√	√
	4.15.0-171-generic	√	√	√
	4.15.0-173-generic	√	√	√
	4.15.0-175-generic	√	√	√
	4.15.0-176-generic	√	√	√
	4.15.0-177-generic	√	√	√
	4.15.0-180-generic	√	√	√
	4.15.0-184-generic	√	√	√
	4.15.0-187-generic	√	√	√
	4.15.0-188-generic	√	√	√
	4.15.0-189-generic	√	√	√
	4.15.0-191-generic	√	√	√
	4.15.0-192-generic	√	√	√
	4.15.0-197-generic	√	√	√
	4.15.0-210-generic	√	√	√
	4.15.0-213-generic	√	√	√
	5.4.0-84-generic	√	√	√
	5.4.0-92-generic	√	√	√
	5.4.0-120-generic	√	√	√

	5.4.0-122-generic	√	√	√
	5.4.0-148-generic	√	√	√
	5.4.0-150-generic	√	√	√
Ubuntu 20.04 LTS	4.15.0-213-generic	√	√	√
	5.4.0-26-generic	√	√	√
	5.4.0-28-generic	√	√	√
	5.4.0-29-generic	√	√	√
	5.4.0-31-generic	√	√	√
	5.4.0-33-generic	√	√	√
	5.4.0-37-generic	√	√	√
	5.4.0-39-generic	√	√	√
	5.4.0-40-generic	√	√	√
	5.4.0-42-generic	√	√	√
	5.4.0-45-generic	√	√	√
	5.4.0-47-generic	√	√	√
	5.4.0-48-generic	√	√	√
	5.4.0-51-generic	√	√	√
	5.4.0-52-generic	√	√	√
	5.4.0-53-generic	√	√	√
	5.4.0-54-generic	√	√	√
	5.4.0-58-generic	√	√	√
	5.4.0-59-generic	√	√	√
	5.4.0-60-generic	√	√	√
	5.4.0-62-generic	√	√	√
	5.4.0-64-generic	√	√	√
	5.4.0-65-generic	√	√	√
	5.4.0-66-generic	√	√	√
	5.4.0-67-generic	√	√	√
	5.4.0-70-generic	√	√	√
	5.4.0-71-generic	√	√	√
	5.4.0-72-generic	√	√	√

	5.4.0-73-generic	√	√	√
	5.4.0-74-generic	√	√	√
	5.4.0-77-generic	√	√	√
	5.4.0-80-generic	√	√	√
	5.4.0-81-generic	√	√	√
	5.4.0-84-generic	√	√	√
	5.4.0-86-generic	√	√	√
	5.4.0-88-generic	√	√	√
	5.4.0-89-generic	√	√	√
	5.4.0-90-generic	√	√	√
	5.4.0-91-generic	√	√	√
	5.4.0-92-generic	√	√	√
	5.4.0-94-generic	√	√	√
	5.4.0-96-generic	√	√	√
	5.4.0-97-generic	√	√	√
	5.4.0-99-generic	√	√	√
	5.4.0-100-generic	√	√	√
	5.4.0-104-generic	√	√	√
	5.4.0-105-generic	√	√	√
	5.4.0-107-generic	√	√	√
	5.4.0-109-generic	√	√	√
	5.4.0-110-generic	√	√	√
	5.4.0-113-generic	√	√	√
	5.4.0-117-generic	√	√	√
	5.4.0-120-generic	√	√	√
	5.4.0-121-generic	√	√	√
	5.4.0-122-generic	√	√	√
	5.4.0-124-generic	√	√	√
	5.4.0-125-generic	√	√	√
	5.4.0-126-generic	√	√	√
	5.4.0-128-generic	√	√	√

	5.4.0-131-generic	√	√	√
	5.4.0-132-generic	√	√	√
	5.4.0-135-generic	√	√	√
	5.4.0-136-generic	√	√	√
	5.4.0-137-generic	√	√	√
	5.4.0-139-generic	√	√	√
	5.4.0-144-generic	√	√	√
	5.4.0-146-generic	√	√	√
	5.4.0-155-generic	√	√	√
	5.4.0-156-generic	√	√	√
	5.4.0-169-generic	√	√	√
	5.4.0-174-generic	√	√	√
	5.4.0-176-generic	√	√	√
	5.4.0-182-generic	√	√	√
	5.4.0-189-generic	√	√	√
	5.4.0-190-generic	√	√	√
	5.4.0-216-generic	√	√	√
	5.15.0-139-generic	√	√	√
	5.13.0-39-generic	√	√	√
	5.15.0-86-generic	√	√	√
	5.15.0-91-generic	√	√	√
	5.15.0-117-generic	√	√	√
	5.15.0-125-generic	√	√	√
	5.15.0-130-generic	√	√	√
Ubuntu 22.04 LTS	5.15.0-25-generic	√	√	√
	5.15.0-43-generic	√	√	√
	5.15.0-56-generic	√	√	√
	5.15.0-58-generic	√	√	√
	5.15.0-60-generic	√	√	√
	5.15.0-86-generic	√	√	√
	5.15.0-94-generic	√	√	√

	5.15.0-107-generic	√	√	√
	5.15.0-112-generic	√	√	√
	5.15.0-113-generic	√	√	√
	5.15.0-117-generic	√	√	√
	5.15.0-118-generic	√	√	√
	5.15.0-119-generic	√	√	√
	5.15.0-125-generic	√	√	√
	5.15.0-133-generic	√	√	√
	5.15.0-134-generic	√	√	√
	5.15.0-139-generic	√	√	√
	5.15.0-140-generic	√	√	√
	5.15.0-141-generic	√	√	√
	5.15.0-142-generic	√	√	√
	6.8.0-40-generic	√	√	√
	6.8.0-47-generic	√	√	√
Ubuntu 24.04 LTS	6.8.0-41-generic	√	√	√
	6.8.0-59-generic	√	√	√
	6.8.0-51-generic	√	√	√
	6.8.0-57-generic	√	√	√
	6.11.0-8-generic	√	√	√
	6.8.0-52 -generic	√	√	√
	6.14.0-24-generic	√	√	√
AlmaLinux				
8.9	4.18.0-513.18.1.el8_9.x86_64	√	√	√
Kylin				
Kylin V10 x86_64	4.19.90-23.8.v2101.ky10.x86_64	√	√	√
	4.19.90-23.18.v2101.ky10.x86_64	√	√	√
	4.19.90-23.45.v2101.ky10.x86_64	√	√	√
	4.19.90-23.48.v2101.ky10.x86_64	√	√	√
	4.19.90-24.4.v2101.ky10.x86_64	√	√	√
	4.19.90-25.37.v2101.ky10.x86_64	√	√	√

	4.19.90-52.15.v2207.ky10.x86_64	√	√	√
	4.19.90-52.19.v2207.ky10.x86_64	√	√	√
	4.19.90-52.22.v2207.ky10.x86_64	√	√	√
	4.19.90-52.23.v2207.ky10.x86_64	√	√	√
	4.19.90-52.33.v2207.ky10.x86_64	√	√	√
	4.19.90-52.42.v2207.ky10.x86_64	√	√	√
	4.19.90-52.44.v2207.ky10.x86_64	√	√	√
	4.19.90-52.48.v2207.ky10.x86_64	√	√	√
	4.19.90-89.11.v2401.ky10.x86_64	√	√	√
Kylin V10 SP1 x86_64	4.19.90-23.18.v2101.ky10.x86_64	√	√	√
Kylin Desktop V10 SP1	5.10.0-8-generic	√	√	√
Kylin V6	2.6.32-431.el6.x86_64	√	√	√
Kylin V7	3.10.0-327.el7.x86_64	√	√	√
	3.10.0-957.el7.x86_64	√	√	√
BCLinux for Euler				
BCLinux 21.10 LTS SP2	4.19.90-2107.6.0.0208.16.oe1.bclinux.x86_64	√	√	√
	4.19.90-2111.3.0.0121.oe1.x86_64	√	√	√
openEuler				
openEuler 20.03 LTS SP1	4.19.90-2012.5.0.0054.oe1.x86_64	√	√	√
openEuler 21.09	5.10.0-5.10.0.24.oe1.x86_64	√	√	√
openEuler 22.03 LTS	5.10.0-60.18.0.50.oe2203.x86_64	√	√	√
openEuler 22.03 LTS SP1	5.10.0-136.12.0.86.oe2203sp1.x86_64	√	√	√

openEuler 22.03 LTS SP2	5.10.0-153.12.0.92.oe2203sp2.x86_64	√	√	√
openEuler 22.03 LTS SP3	5.10.0-187.0.0.100.oe2203sp3.x86_64	√	√	√
openEuler 22.03 LTS SP4	5.10.0-216.0.0.115.oe2203sp4.x86_64	√	√	√
Euler				
Euler 2 SP2	3.10.0-327.62.59.83.h108.x86_64	√	√	√
Oracle Linux				
Oracle Linux 5.11	2.6.39-400.215.10.el5uek	√	√	√
Oracle Linux 6.6	3.8.13-44.1.1.el6uek.x86_64	√	√	√
Oracle Linux 6.7	3.8.13-68.3.4.el6uek.x86_64	√	√	√
Oracle Linux 6.9	4.1.12-61.1.28.el6uek.x86_64	√	√	√
Oracle Linux 6.10	4.1.12-124.16.4.el6uek.x86_64	√	√	√
Oracle Linux 7.3	4.1.12-61.1.18.el7uek.x86_64	√	√	√
	3.8.13-98.7.1.el7uek.x86_64	√	√	√
Oracle Linux 7.4	4.1.12-94.3.9.el7uek.x86_64	√	√	√
Oracle Linux 7.6	3.10.0-1160.42.2.el7.x86_64	√	√	√
Oracle Linux 7.9	5.4.17-2102.201.3.el7uek.x86_64	√	√	√
Oracle Linux 8.5	5.4.17-2136.300.7.el8uek.x86_64	√	√	√
Anolis				
Anolis 7.9	3.10.0-1160.an7.x86_64	√	√	√

	4.19.91-27.5.an7.x86_64	√	√	√
	4.19.91-27.8.an7.x86_64	√	√	√
Anolis 8.6	4.19.91-26.an8.x86_64	√	√	√
Anolis 8.8	5.10.134-13.an8.x86_64	√	√	√
Debian				
Debian 9.6	4.9.0-8-amd64	√	√	√
Debian 10.02	4.19.0-6-amd64	√	√	√
Debian 11.4	5.10.0-16-amd64	√	√	√
	5.10.0-19-amd64	√	√	√
	5.10.0-23-amd64	√	√	√
	5.10.0-25-amd64	√	√	√
Debian 12	6.1.0-10-amd64	√	√	√
Debian 12.2	6.1.0-15-amd64	√	√	√
	6.1.0-25-amd64	√	√	√
	6.1.0-28-amd64	√	√	√
Debian 12.5	6.1.0-18-amd64	√	√	√
UOS				
uos-server-20-1002a	4.19.0-91.77.97.uelc20.x86_64	√	√	√
uos-server-20-1050a	4.19.0-91.82.112.uelc20.x86_64	√	√	√
	4.19.0-91.82.141.6.uelc20.x86_64	√	√	√
uos-server-20-1050u2e	4.19.90-2210.5.0.0174.14.uel20.x86_64	√	√	√
	4.19.90-2211.5.0.0178.22.uel20.x86_64	√	√	√
uos-desktop-20-professional-1060	4.19.0-amd64-desktop	√	√	√
uos-server-20-1060a-amd64	4.19.0-91.82.152.uelc20.x86_64	√	√	√

uos-server-20-1060e-amd64	4.19.90-2305.1.0.0199.56.uel20.x86_64	√	√	√
UOS V20 1070a	5.10.0-74.3.uelc20.x86_64	√	√	√
Rocky				
8.8	4.18.0-477.10.1.el8_8.x86_64	√	√	√
	4.18.0-477.21.1.el8_8.x86_64	√	√	√
	4.18.0-477.27.1.el8_8.x86_64	√	√	√

[1] SUSE 10 SP4 is only supported via VADP reads and requires the target driver to be pre-loaded in advance.

Linux For ARM Compatibility					
Linux distributions	Major Version	Kernel	CPU model	Source Agent	Remarks
Ubuntu	18.04.3 LTS	4.15.0-70-generic	Hikunpeng 920	√	
	20.04.3 LTS	5.4.0-81-generic	Hikunpeng 920	√	
	22.04 LST	5.15.0-124-generic	Hikunpeng 920	√	
CentOS	7.6-1810	4.18.0-80.7.2.el7.aarch64	Hikunpeng 920	√	
UnionTechOS	V20-1020	4.19.0-arm64-server	Hikunpeng 920	√	
	V20-1020	4.19.0-arm64-server	Phytium	√	
	V20-1050d	4.19.0-arm64-server	Hikunpeng 920	√	
Kylin	V10	4.19.90-17.ky10.aarch64	Hikunpeng 920	√	
		4.19.90-11.ky10.aarch64	Hikunpeng 920	√	
		4.19.90-17.ky10.aarch64	phytium	√	
		4.19.90-17.5.ky10.aarch64	Hikunpeng 920	√	
		4.19.90-23.42.v2101.ky10.aarch64	Hikunpeng 920	√	
		4.19.90-24.4.v2101.ky10.aarch64	Hikunpeng 920	√	
		4.19.90-24.4.v2101.ky10.aarch64	Hikunpeng 920	√	
		4.19.90-25.21.v2101.ky10.aarch64	Hikunpeng 920	√	
		4.19.90-52.39.v2207.ky10.aarch64	Hikunpeng 920	√	
		4.19.90-89.11.v2401.ky10.aarch64	Hikunpeng 920	√	
	V10-GFB	4.19.90-52.23.v2207.gfb03e.ky10.aarch64	Hikunpeng 920	√	GFB
	KylinV10 Desktop arm	5.4.18-142-generic			

OpenEuler	20.03 LTS SP4	4.19.90-2312.1.0.0255.oe2003sp4.aarch64	Hikunpeng 920	√	
	22.03 LTS SP4	5.10.0-216.0.0.115.0e2203sp4.aarch64	Hikunpeng 920	√	
	24.04 LTS	6.6.0-28.0.0.34.oe2403.aarch64	Hikunpeng 920	√	

1.4.4 File System Compatibility

The task of client agent on the source machine is to ensure data consistency, so there are compatibility requirements for the file system. File systems not on the compatibility list do not support data replication and synchronization; special evaluation is required if customers has requirement.The specific compatibility list is as follows:

OS	File System	Snapshot	Not-Snapshot
Windows	FAT32	√	√
	NTFS	√	√
Linux	ext2	√	√
	ext3	√	√
	ext4	√	√
	xfs	√	√
	btrfs[1]	[2]	√

[1] For the btrfs file system, it is required to use client agent version 817 or above, together with TrekerLite version 672 or above;

[2] Due to the particularity of the file system, btrfs does not support consistency guarantees. A snapshot point is determined after the underlying synchronized data is in a "clean" state.

1.5 VMware Protection Support

Prerequisite

- Prepare a Windows Treker Server or a Linux CentOS Treker Server in the source VMware environment
- If using vCenter, the Treker server must have connectivity to both vCenter and ESXi.
- Ensure ports 902 and 443 are open for communication with vCenter and ESXi.
- Use an admin account or an account with vStorage permissions and administrative access to the source virtual machines.
- The VMware agentless feature is only applicable to VMware to Cloud and Any to VMware scenarios.
- For ZDR to perform disaster recovery by reading VMware data via VADP, it is recommended to use a Windows or Linux virtual machine with the server deployed, enabling agentless data read and write operations.

1.5.1 Protection from VMware

Server is integrated with the VMware API to perform agentless protection for the following VMware versions. For older VMware versions, it is recommended to install the source agent on each virtual machine's guest OS to avoid server performance issues. Note that most cloud platforms based on VMware vCloud Director do not publish an API. Installing the source agent on each virtual machine will enable the protection of servers from these vendors.

VMware version	VMware API (Agentless)	Antenna (Guest OS)
4.1		√
5.0		√
5.1	√	√
5.5	√	√
6.0	√	√
6.5	√	√
6.7	√	√
7.0	√	√
8.0	√	√
vCloud Director		√

[1] ESXi 5.1requires patch to downgrade VMware API related files.
[2] If data inconsistencies occur during migration due to CBT (Changed Block Tracking) issues on certain VMware virtual machines, the target VM may fail to start. It is recommended to use the CBT Reset feature and re-run replication and recovery to resolve the issue.
[*] To address VDDK version compatibility issues, the data gateway provides the ability to switch between different VDDK versions.

1.5.2 Protection into VMware

Server can write replicated data into the VM VMDK of the ESXi server datastore through the VMware API. It is not necessary to install Treker on each virtual machine within the ESXi server.
If VMware vCenter/ESXi Server/vCloud Director does not allow API connections, users can enable the virtual machine booting function on Server Lite (ISO) or create a virtual machine using Server Lite (OVA/VMDK) to receive replicated data, write it into the VMDK, and attach it to the target virtual machine.

VMware version	VMware API	TrekerLite (ISO)	TrekerLite (OVA/VMDK)
5.1	√	√	√
5.5	√	√	√
6.0	√	√	√
6.5	√	√	√
6.7	√	√	√
7.0	√	√	√
8.0	√	√	√
vCloud Director		√	√

1.6 Cloud Protection Modes

The software supports agentless mode, allowing virtual machines to be migrated from one ZStack Cloud to another. In this mode, a source server must be deployed within the source to enable data access and transmission.

ZStack Cloud	Agentless
ZStack Cloud 4.4	√
ZStack Cloud 4.7	√
ZStack Cloud 4.8	√
ZStack Cloud 5.1	√
ZStack Cloud 5.3 [2]	√
ZStack Cloud + ZCE V4[1]	√
ZStack Cloud + ZCE V5[1]	√

[*] The data gateway server must be deployed on the same primary storage as the source machine.

[*] It is necessary to ensure that the ZStack performance optimization tool has been installed on Windows if the windows gateway is used.

[1] Retrieving differential data blocks between snapshots via ZBS enables rapid incremental replication without the need for scanning and comparison. This requires version 671 or higher.

[2] ZStack 5.3.40 and later versions support agent-less data replication through ZStack CBT function, which requires pairing with ZMigrate version 681 or above.

1.7 ZStack Target Cloud Compatibility

ZMigrate automates the migration process by integrating ZStack Cloud APIs and leverages snapshots to retain historical recovery points. Target virtual machines in ZStack support both Ceph and non-Ceph storage types. Regardless of the target disk type, ZStack's backup feature can be used to retain historical copie with rolling retention. For Ceph storage, ZStack supports snapshot rotation—when the number of snapshots reaches the configured retention limit, the system will automatically delete the oldest snapshot to maintain a rolling snapshot chain. In contrast, non-Ceph storage cannot support snapshot rotation due to the snapshot tree mechanism.

For detailed information, refer to the official ZStack documentation:

- https://www.zstack.io/help/tutorials/volume_snapshot_tutorial/v4/2.html
- https://www.zstack.io/help/product_manuals/user_guide/v4/10.2.html#chapter-10-2-4-1-%E6%A6%82%E8%BF%B0

ZStack Cloud	TrekerLite Automation	Auto Mounting	Target Storage	Retention Type
ZStack Cloud 4.4	√	√	local storage and storage blocks	Snapshot
				Backup
			Ceph, ZStone	Snapshot
				Backup
ZStack Cloud 4.7	√	√	local storage and storage blocks	Snapshot
				Backup
			Ceph, ZStone	Snapshot
				Backup
ZStack Cloud 4.8	√	√	local storage and storage blocks	Snapshot
				Backup
			Ceph, ZStone	Snapshot
				Backup
	√	√	Ceph vhost (ZHPS)	Snapshot
				Backup
ZStack Cloud 5.1	√	√	local storage and storage blocks	Snapshot
				Backup
			Ceph, ZStone	Snapshot
				Backup
	√	√	Ceph vhost (ZHPS)	Snapshot
				Backup
	√	√		Snapshot

ZStack Cloud 5.3[1]			local storage and storage blocks	Backup
			Ceph, ZStone	Snapshot
				Backup
	√	√	Ceph vhost (ZHPS)	Snapshot
				Backup
ZStack ZSphere 4.2	√	√	local storage and storage blocks	Snapshot
				Backup
ZStack ZSphere 4.10	√	√	local storage and storage blocks	Snapshot
				Backup

[*] For non-Ceph storage, due to snapshot chain limitations, the migration platform retains one snapshot by default to ensure snapshot rotation.

[*] Using the ZStack Backup feature requires additional backup storage and a valid ZStack Cloud Backup license.

[*] Snapshot chain rotation is available from version 4.10.7 onwards, supporting multiple snapshot retention.

[1] ZStack Cloud 5.3.40 and later versions support snapshot chain rotation technology for local storage and storage blocks, allowing multiple snapshots to be retained, which requires pairing with ZMigrate version 682 or above.