

Hitachi Data Instance Director (HDID) Support Matrix: File Systems

Introduction: Agent-based and Agentless protection

HDID can provide consistent protection either with or without the use of a host agent.

- Agent based protection performs the application interaction required to provide application aware consistency.
- Agentless protection protects the application data on disk and therefore provides crash consistency. It can also call pre-execution scripts and post-execution scripts as part of a policy to enable the use of user scripts to ensure application aware consistency.

This support matrix describes the environments supported by either method of protection.

Agent Based Protection

Agent based protection provides application consistent protection support with the following operating systems and configurations.







Operating System		File System/ASM	Supported Protection Types		
			Host Based	Storage Based	
			Repository	Hitachi Block	Hitachi NAS
Microsoft® Windows	Windows Server 2008 (32-bit) Windows Server 2008 (64-bit) Windows Server 2008 R2 (64-bit) Windows Server 2012 (64-bit) Windows Server 2012 R2 (64-bit) Windows 10 Windows Server 2016 (64-bit) (8)		✓	✓	✗
Microsoft® Windows (Desktop)	Windows 7 SP1 Windows 8 / 8.1 Windows 10		✓	✗	✗
Linux (1)	RHEL 6 x64 (6.3 and newer) RHEL 7 x64 (7.0 and newer) OEL 6 x64 (6.3 and newer) OEL 7 x64 (7.0 and newer) SUSE 11 x64 (11.3 and newer) SUSE 12 x64 (12.0 and newer)	EXT3 EXT4 LVM CIFS NFS (HNAS) ASM	✓	✓	✓
IBM® AIX®	AIX v6.x (6.1 TL9 and newer) AIX v7.x (7.1 TL3 and newer)	JFS2 CIFS NFS (HNAS) ASM	✓	✓	✗
Oracle Solaris (Intel)	Solaris 11 (11.0 and newer)	ZFS CIFS NFS (HNAS) ASM	✓	✓	✗

Oracle Solaris (SPARC)	Solaris 11 (11.0 and newer)	ZFS CIFS NFS (HNAS) ASM			
------------------------	-----------------------------	----------------------------------	--	--	--

Operating Systems	Host Based Backup			Hitachi Block Hardware (2)			Hitachi NAS	
	Backup	Real-Time Replication	Batch Replication	Snapshot (TI)	Live Replicate (SI /TC / UR ⁽³⁾ / GAD)	Batch Replicate (TI / SI)	Directory Clone	File Replication
Microsoft Windows								
Linux								
IBM® AIX® ⁽⁴⁾								
Oracle Solaris (Intel) ⁽⁴⁾⁽⁵⁾								
Oracle Solaris (SPARC) ⁽⁴⁾⁽⁵⁾								

Agentless Protection

Agentless protection provides crash consistent protection for any operating system version and configuration as follows (subject to operating system and application vendor support):

Application Configurations	Host Based Backup		Hitachi Block Hardware ⁽²⁾		Hitachi NAS	
	Batch	Real Time/CDP	Snapshot (TI)	Replicate (SI /TC / UR ⁽³⁾ / GAD)	Directory Clone	File Replication
"LDEV Based"						
VMware	Not Applicable					

-
- (1) It is recommended that Linux source nodes have a logical volume manager (LVM) on each volume group that is to be backed up. A minimum of 10GB of free space is required in the "unused" portion of the LVM, which is in addition to the required space for the allocated storage area. For example, if 100GB of usable storage is required, then the total disk size will be 110GB (100GB of usable storage and 10GB of unused storage).
 - (2) In virtual environments, the volumes must be VMWare physical Raw Device Mapping (pRDM) or Hyper-V pass-through disks.
 - (3) Operating System consistent remote SI / TI are not supported in conjunction with UR
 - (4) ACLs or Extended Attributes are not protected, if they are present on data that is backed up then they will not be restored.
 - (5) For a system which has zones on it, HDID should be installed on the 'global' system and then back up the data from the zones, instead of installing HDID on all of the zones individually. HDID does not support the backup and restore of whole zones
 - (6) A VMware proxy node must be configured on the master to support mounting to VMware Virtual machines
 - (8) Windows 2016 is supported only with features compatible with Windows 2012