# Don’t Lose Your (Virtual) Desktop!

Protecting Persistent Virtual Desktop Infrastructure (VDI) with Zerto

The surge in virtual desktop infrastructure (VDI) adoption can be attributed to several key factors, chief among them being the rapid evolution of remote and hybrid work models. Organizations are increasingly relying on VDI to provide seamless access to desktop environments from anywhere, ensuring productivity while maintaining stringent security standards. This shift underscores the critical role VDI plays in modern IT strategies, as businesses strive to meet the demands of an ever-changing digital landscape.

Traditionally, many VDI deployments leveraged non-persistent VDI. Non-persistent VDI provides users with a generic desktop image that is reset to a clean state after each session. Any changes made by the user, such as installed applications or saved files, are discarded once the user logs out. While this is nice for users—like task workers who don’t require a customized desktop with applications installed—this isn’t great for the growing number of remote workers who have grown attached to their virtual desktops (generally knowledge and power workers), leading IT teams to make the change to persistent VDI.

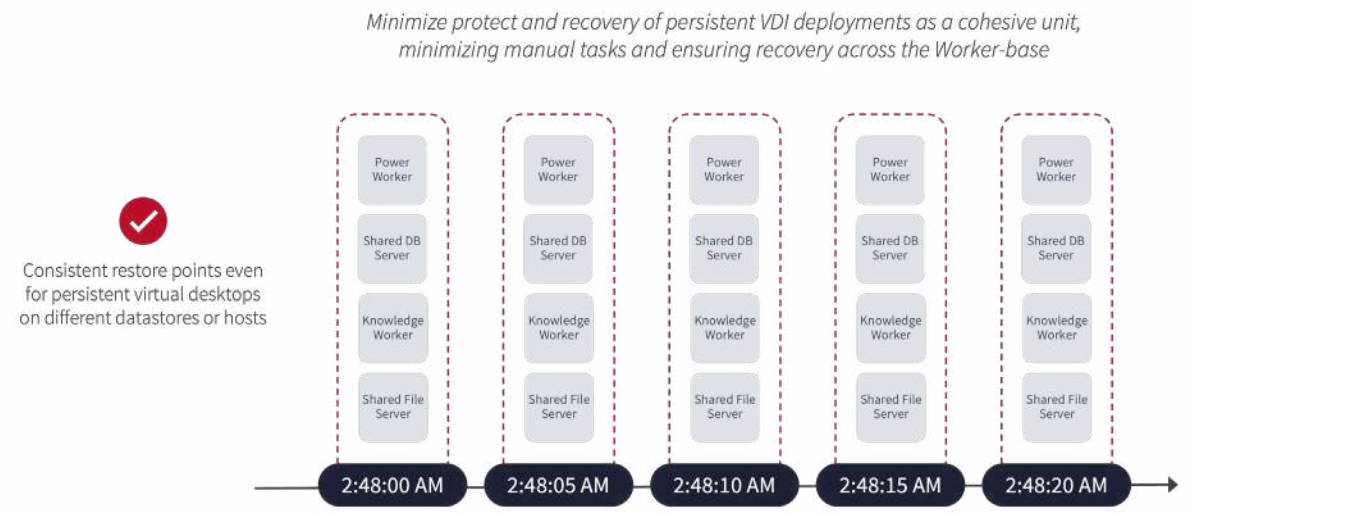
In a persistent VDI setup, each user is assigned a dedicated virtual desktop (almost a 1:1 mapping of user to VM) that retains all their customizations, settings, and data between sessions. This means that each time a user logs in, they get the same desktop environment with their personalized configurations, applications, and files.

## How Zerto Keeps Your Virtual Desktops Running

### *Protecting Power & Knowledge Workers with Continuous Data Protection (CDP)*

Knowledge and power workers—particularly graphic artists, financial analysts, designers, or scientists who take advantage of working remote—typically use applications such as computer-aided design (CAD) or financial modeling, which generates data stored on and unique to that virtual desktop.

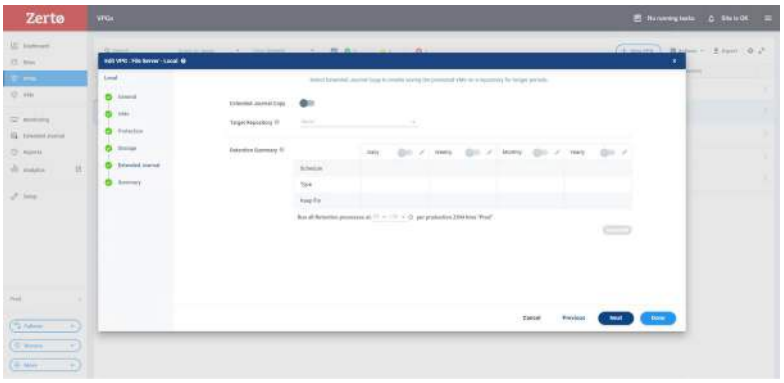
Zerto, a Hewlett Packard Enterprise company, uses CDP that enables granular replication and journal-based recovery by logically grouping persistent virtual desktops and shared virtual assets among those workers into groups, ensuring replication and recoverability in that group at scale.



## *Layers of Recoverability for Shared Virtual Resources*

Part of the flexibility of a VDI infrastructure is its ability for persistent virtual desktops to have access to shared resources critical to their roles, such as virtual file and database servers.

Zerto's extended journal copies enable longer-term retention of critical virtual servers alongside Zerto's CDP. An extended journal copy sends a scheduled incremental copy of protected virtual servers to an immutable S3-compatible repository, adding in another layer of recoverability for the worst-case scenarios.

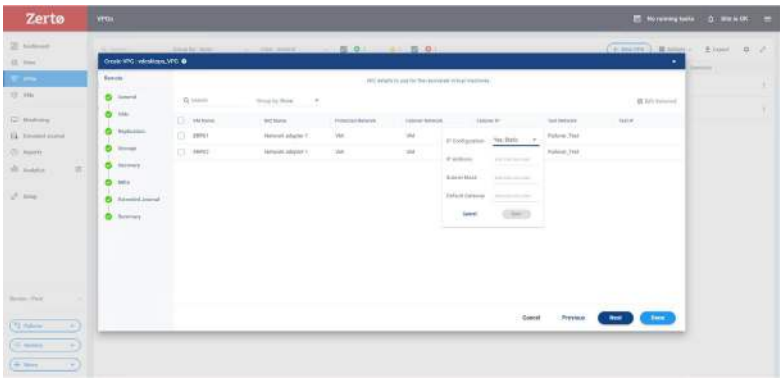


## *Keep Protected Virtual Desktop IP Addresses Persistent During Recovery*

IP addresses can get gobbled up in VDI deployments as each virtual desktop takes up an address. Particularly for customized persistent VDI deployments, IT departments must ensure that the same IP address is there so the user can log in even during a disaster failover scenario.

When protecting persistent virtual desktops with Zerto, users can preserve the IP address of the instance in the event of live or test failover.

During setup, users protecting their persistent VDI infrastructures with Zerto can also take advantage of other deep feature sets, including boot ordering, pre- and post-recovery scripts, and auto-protect back to the source site.



## Do you want to try Zerto for yourself? Sign up for our free Hands-on Labs!

**Free Hands-on Labs**



RITM0108857