Managing Physical and Virtual Machines in Paragon Protect & Restore

Best Practices

last updated: August 2013

Overview

Paragon Software's Protect & Restore (PPR) offers a unified system and data protection solution for virtual and physical machines. PPR delivers comprehensive agentless protection for virtual environments hosted by VMware vSphere or standalone ESX servers[1], and agent-based protection for physical and virtual Windows systems on any hypervisor. As its backbone, Paragon leverages a patent-pending distributed architecture allowing for efficient centralized and remote management of hundreds or even thousands of machines on the network.

Administration and control of all components within the PPR infrastructure (i.e. the PPR Server, PPR Console, Backup Server, Backup Agent, ESX Bridge) and all target machines can be carried out through either of two consoles: the Windows PowerShell-based console for users who are accustomed to scripting and command-line tools and who want to have the ultimate control and flexibility in configuring protection scenarios, or the GUI-based console for users who are more comfortable in a point-and-click or wizard-based environment. In this document we will only look at the GUI console, which is a very easy-to-use and efficient management tool for PPR. Here are a few key benefits of this console:

- Feature rich and tailored to the needs of the most demanding users
- Unified ribbon-style interface for management of physical and virtual environments
- Smart wizards and dialogs with a context-sensitive tool tips
- Allows powerful monitoring through popup and email notifications, along with event and activity views
- Collect and Save operation logs from all or specific components deployed within the infrastructure

Now, going back to the headline of this document, you may wonder why physical and virtual machines are managed in different ways in PPR. The reason is the different ways machines of these two types are accessed. Let's take a closer look at each technique.

[1] Agentless Hyper-V support is scheduled for December 2013.

Managing Virtual Machines

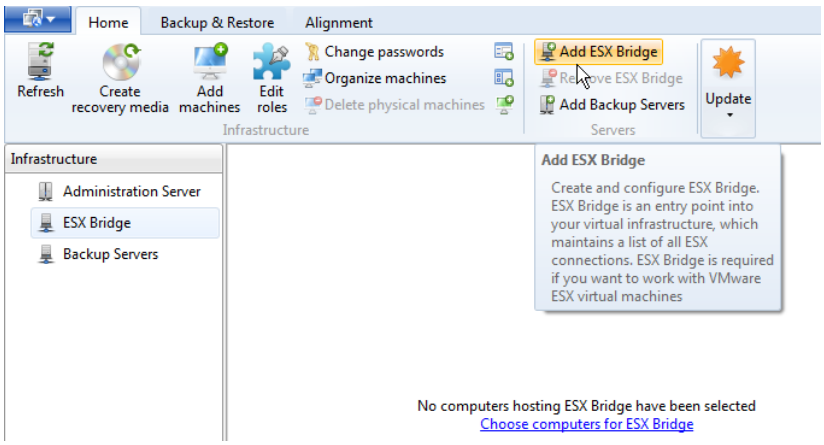
In the context of this document, when we say “virtual machines”, we are specifically referring to guest machines hosted by VMware ESX.

Access to virtual machines is done directly through the VMware API. This approach offers a number of important benefits:

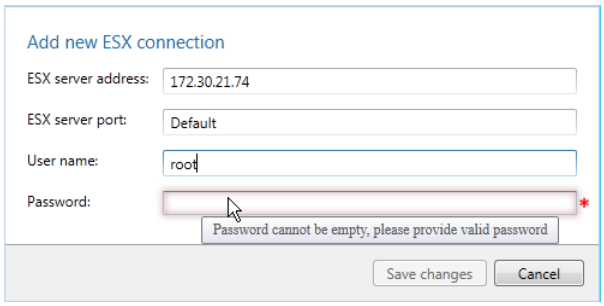
- There is no need for embedding an agent in each target machine to manage the system and perform backups or restores (agentless protection).
- It significantly improves backup/restore performance, while minimizing the load on target machines and the hypervisor during the process.
- It allows VM replication for high-availability systems that run first tier applications, to achieve the best RTO (Recovery Time Objective), as replicas can be booted and take over tasks in minutes.
- There is no need to provide credentials for each guest.

For effective agentless management of virtual machines, the PPR administrator should:

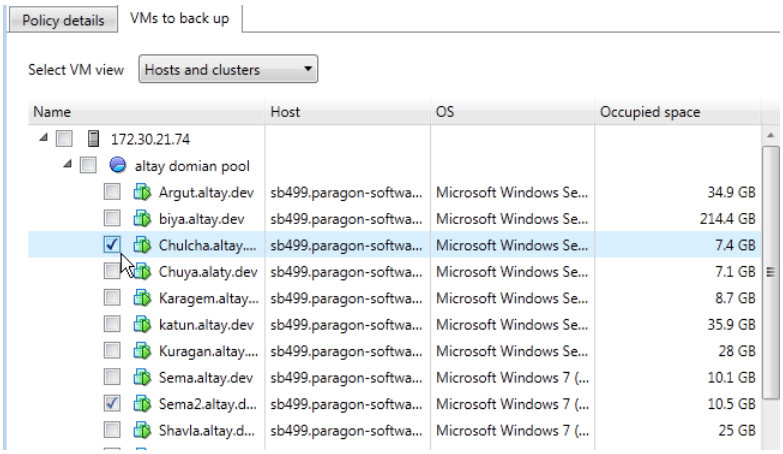
- Install PPR’s ESX Bridge, a special service that interacts with the VMware infrastructure, on a Windows-based guest machine that resides within the ESX environment. The ESX Bridge will subsequently provide access to all the hosted virtual machines. There are several configuration options available, but this one will yield the best performance.



- Establish a connection to vSphere or the standalone ESX host by providing its DNS name or IP address, a communication port (if necessary), and administrator credentials with sufficient privileges (a datacenter admin account with the ‘Global.Licenses’ privilege, for instance).



When done, the PPR administrator can create and submit backup, replication, or other policies for one or a group of virtual machines that run on the specified ESX environment.



Managing Physical Machines

By “physical machines” we refer to Windows-based machines that are accessed through the network. They can be domain or workgroup machines, either physical or virtual. The latter assumes that we are treating a virtual machine as if it were a physical machine. In this context, these virtual machines can reside on any hypervisor, not only VMware ESX (whereas in the previous section on agentless management of VMs, only ESX hosted virtual machines are supported).

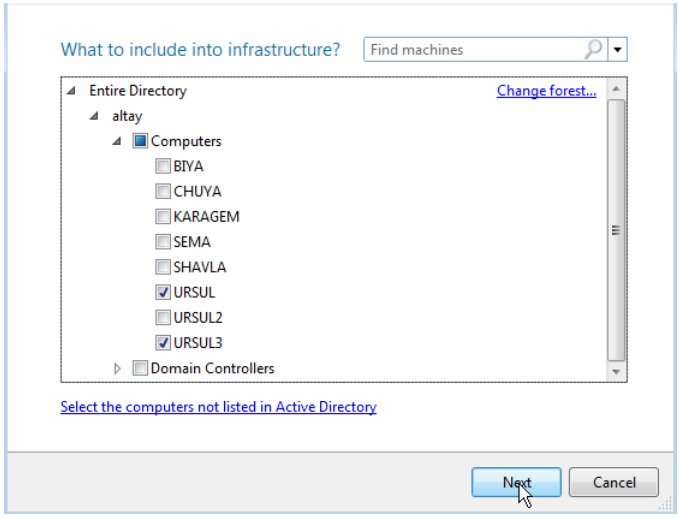
Key benefits of this type of approach are:

- Agent-based protection and management through a centralized console for any Windows-based machine, physical or virtual (supports any hypervisor).
- Backup and restore entire systems, specific volumes, or individual files and folders.
- Protection of VMware fault-tolerant configurations, as well as guests hosted by non-commercial versions of VMware ESX, i.e. machines that do not allow for agentless protection through the VMware snapshot mechanism.
- Supports Windows virtual machines residing on any hypervisor.
- MS Exchange protection for email databases, at the application level (coming soon).

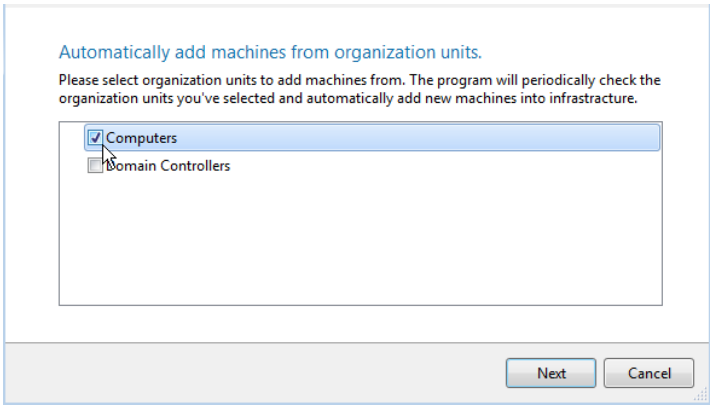
For best results, when managing machines through physical agents, the PPR administrator should:

- Add the target machines to PPR’s infrastructure. This can be done either by manually specifying all required machines individually, or through an automated discovery policy. While the first option is pretty straight forward, the second one might require some explanation. In a corresponding wizard the administrator would specify one or several organizational units (OUs) to be monitored in Active Directory for new systems, and then, when new machines are found, they will be added to the infrastructure automatically.

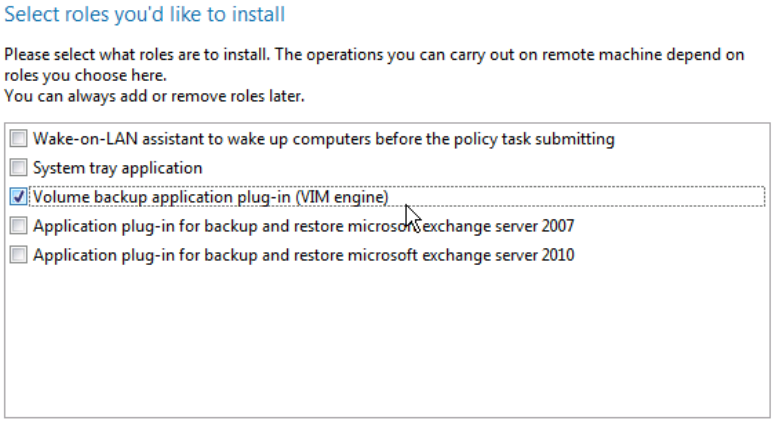
Adding machines



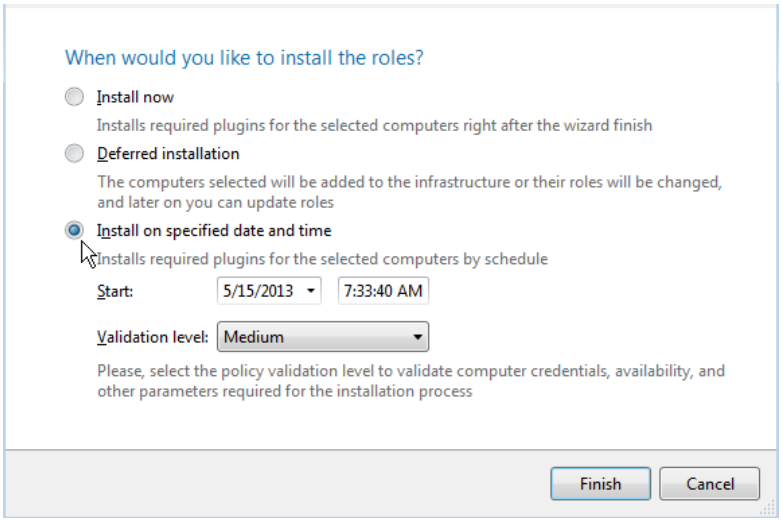
Configuring a discovery policy



- First, you need to specify the role of the machine. By default, machines are added with the general role of Agent. To allow for sector-level protection (image-based snapshots) for instance, the administrator should extend the functionality of this agent by selecting the 'Volume backup application plug-in (VIM engine)'. The number of available plug-ins depends on the PPR product license that's been purchased.



Next, you specify how and when the selected roles should be installed.



Now, the PPR administrator can create and submit backup, restore, or other policies for one or a group of target machines. If necessary, roles can always be changed through a corresponding interface. If a machine is no longer needed, it can be removed from the infrastructure.

Conclusion

Paragon Protect & Restore allows you to manage all of your Windows systems – physical or virtual, server or workstation – as well as VMware ESX-based virtual machines of any supported operating system conveniently from one centralized console. ESX-based machines are typically being managed agentlessly, through vSphere (via Paragon's ESX Bridge), while virtual machines on other hypervisors, as well as all physical machines, require a PPR agent reside on them.

For additional information, please contact us at: **www.paragon-software.com**, **www.protect-restore.com** or **+1 (888) 347-5462**.