BEST PRACTICE: RECOVERING PARAGON PROTECT & RESTORE INFRASTRUCTURE AFTER A DISASTER

Last updated in September 2018

Overview

Paragon Software’s Protect & Restore offers a unified system and data protection solution for virtual and physical machines. The software delivers comprehensive agentless protection for virtual environments hosted by VMware vSphere or standalone ESX servers, 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.

This paper explains how to correctly protect the Paragon Protect & Restore infrastructure deployed in a physical Windows domain environment to get it back on track in case of a disaster.

Protecting Paragon Protect & Restore Infrastructure

Members of the Paragon Protect & Restore infrastructure are distributed and any of these machines may fail at any time. It’s not a problem unless the machine that hosts Administration Server fails – that will certainly lead to complete infrastructure inoperability. Luckily, Paragon Protect & Restore can protect itself by backing up all the infrastructure members.

To do so, add ‘Volume backup application plug-in’ to the target physical machine through the Edit roles wizard.

![Edit roles wizard]

We already know that Administration Server needs priority protection.
To learn more let’s consider three possible emergency situations:

1 Administration Server fails, Backup Server with the backup images is running.

In fact this means the Paragon Protect & Restore infrastructure is completely down and no actions can be performed through the management consoles. The only option is to use the Bare Metal Restore Wizard from the WinPE recovery environment – it should be prepared beforehand on CD/DVD or flash. Administrator directly connects to the required Backup Server, selects the latest Administration Server backup image and initiates the restore.

Agentless Hyper-V support is scheduled for December 2013.
should additionally complete the P2P Adjust OS Wizard to make Windows OS bootable on the new hardware. Once Administration Server is online, it will initiate replication of all infrastructure databases to obtain the most up-to-date data. This way the Paragon Protect & Restore recovery is completed. Check user manual for more information on the subject.

② Administration Server is running, one of the Backup Servers fails, storages it takes care of are ok. There are two ways to address the issue: either restore failed Backup Server from a backup image (recommended), or import its storages to another Backup Server.

Both recovery scenarios can be initiated through one of the management consoles:

a) The first one involves restore by Recovery ID (a corresponding restore policy is preconfigured in the console, but initiated from the WinPE recovery media on-site by providing its ID).

b) The second one involves import of the target storages as network storages to another Backup Server (all actions are done in the console). Please note, this scenario implies that the administrator should properly modify all backup policies that use the target storages as backup destination. We do not recommend this option as it may require too many actions from user.
Both Administration and Backup Server are down. The only option here is to use Paragon Protect & Restore Express – it is aimed exclusively at agent-based protection of a single physical system. Based on the same architecture as Paragon Protect & Restore, it employs the same technologies and expertise. Thus being fully compatible it helps to recover the environment after a disaster.

In this scenario Paragon Protect & Restore Express helps with the Import Storage feature, also available on its WinPE based part. First, the administrator imports storage that contains backup images of Administration Server as network storage, selects the most recent backup image of Administration Server and initiates the restore, additionally completing the P2P Adjust OS Wizard if necessary. Then the administrator can either use Paragon Protect & Restore Express or usual to restore Backup Server. Check user manual for more information on the subject.

Summary

1. Administration Server should be regularly backed up by all means.
2. Paragon Protect & Restore administrator should have a WinPE recovery CD/DVD or USB-stick ready.
3. Backup Server with backup images of Administration Server is highly recommended to back up to one of the storages of another Backup Server. Otherwise, administrator may face a situation when the only way to recover the Paragon Protect & Restore infrastructure is to use Paragon Protect & Restore Express.

4. Backup Servers are recommended to back up to other Backup Servers storages to avoid time-consuming operations involving import of storages and reconfiguration of backup policies.

5. Additionally we recommend to update Administration Server and Backup Servers images once upgrade of the Paragon Protect & Restore infrastructure has been accomplished. Otherwise, the upgrade procedure should be re-initiated after restore to yield correct operation of all members of the infrastructure.

**Conclusion**

Paragon Protect & Restore can well be used to protect any of its members, including crucial for the entire infrastructure Administration Server. By following our recommendations the infrastructure can successfully be recovered after a disaster to continue protecting ESX guest machines and physical Windows-based systems.

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

Best Practices: Recovering Protect & Restore Infrastructure After a Disaster. Copyright© 1994-2018 Paragon Software Group. All rights reserved. Windows is a registered trademark of the Microsoft Corporation in the U.S. and other countries. Other company or product names may be trademarks or registered trademarks of their respective owners.