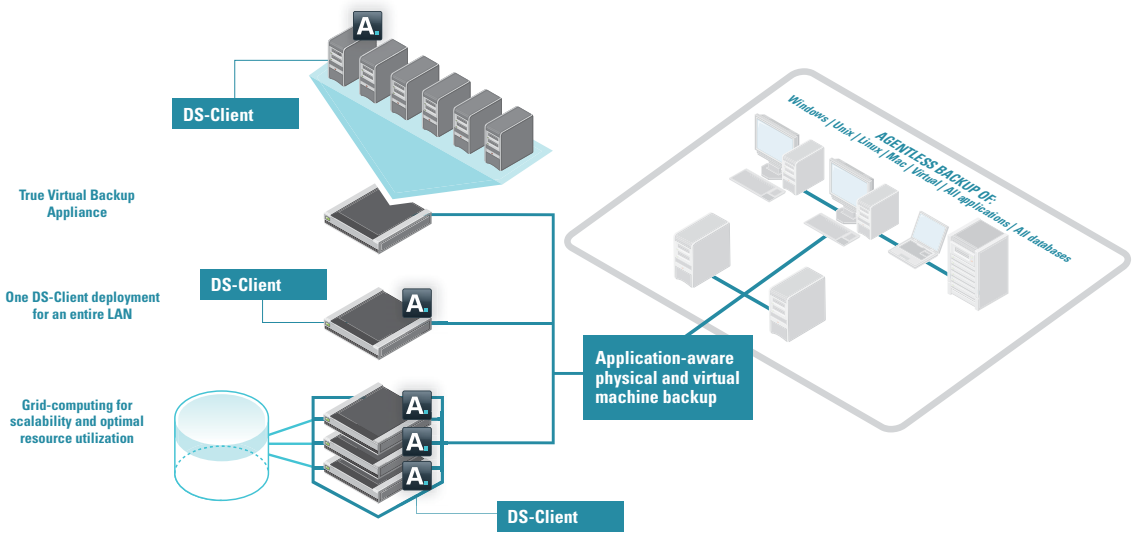
# Asigra v9 Virtual Environment Protection

## Server consolidation is driving deployment of virtualization across enterprises of all sizes. However, to fully realize the benefits of virtualization, organizations must consider their information recovery management strategy. Traditional backup and recovery strategies are not adequate to deliver the granular recovery demanded by the business. More important, the cost associated with traditional or agent based technologies essentially negates many of the cost advantages of virtualization.

Traditional agent-based backup and recovery force the enterprise into a series of unattractive choices. Agent based technologies pollute the virtual environment. Agents, by their nature, lack cohesion. The need to physically install and manage agents on each application within the virtual server and each machine on the LAN is time and labor intensive. A single agent adds as much as 16% server overhead to each application. Add to that the security risk and cost of each agent and it becomes quite clear, agent-based backup and recovery dramatically impacts the TCO and performance of the virtual environment.

Asigra v9 is the next generation software aligned with Cloud Computing and designed to offer backup efficiencies unavailable with traditional backup architecture by allowing you to capture less, ingest less, and store less data thus reducing the amount of backup assets you buy, manage and maintain.

- Recover your Data and Systems.
- Recover your IT resources spent on mundane backup jobs.
- Recover your strategic focus by transforming your backup architecture.




RecoverYourCool.com

Asigra.

## Asigra v9 provides a robust feature set ideal for virtual environments.

Asigra v9 delivers an efficient, cost-effective and transformational solution that enables the enterprise to maximize their virtualization strategy while achieving superior information protection and recovery management without performance degradation.

Asigra v9 DS-Client agentless backup/restore, as well as running the DS-Client as a virtual appliance, has been tested and certified on a very wide range of virtualization platforms:

- VMware ESX 3.0, ESX 3.5, ESXi, Workstation and Server
- XenSource
- Microsoft Hyper-V
- Parallels and Virtuozzo Containers
- Virtual Iron

## VMs and their Data Protection challenges.

A specific challenge emerges when protecting the data of guest VMs. Each physical ESX server may host ten or more guest VMs that individually host different operating systems and applications. Data protection software now needs to account for the following variables when protecting guest VMs on the same physical ESX server:

**Discovering when new VMs are created:** The ease in creating guest VMs can result in lapses in data protection since companies can forget to configure data protection software to protect new guest VMs as they are created.

**Agent installation:** Each guest VM acts and functions like a normal server. To protect each guest VM, companies may need to install and configure an agent on each guest VM just like when they were protecting individual servers.

**Scheduling backup jobs:** As servers are consolidated and virtualized on the same physical ESX server,scheduling backup jobs across the different guest VMs becomes more challenging. Schedule too many backup jobs at the same time and the jobs compete for the server's limited resources. Schedule backup jobs too far apart and they may not complete before the next day's production activities begin.

**Different backup products:** Guest VMs on the same physical machine may use different backup software due to different operating systems and/or applications on each one. This adds to the complexity of managing and scheduling backup jobs across guest VMs on the same physical server.

## Asigra v9 and VM Data Protection.

Asigra v9 removes many of the traditional hassles associated with the protection and recovery of VMs. It meets new data protection requirements that VMware ESX creates by:

- Discovering new guest VMs.
- Centralizing backup configuration and management.
- Controlling software licensing costs.
- Minimizing initial backup job configuration and ongoing management.
- Providing multiple backup options.
- Providing backup options specific to VMware.
- Broad application and operating system support.

## VM Auto-Discovery and Management.

Asigra v9 addresses the new corporate challenges around the discovery, configuration and ongoing management of new guest VMs on VMware ESX servers. To ease in the discovery of new guest VMs, Asigra v9 directly communicates with either an individual ESX server or a VMware VirtualCenter Management Server in order to obtain the list of guest VMs that each ESX server hosts. To build the list of guest VMs from an individual VMware ESX server, Asigra v9 communicates directly with the ESX's hypervisor and queries it for the list of VMs that it hosts. In companies that have deployed VMware's VirtualCenter Management software, Asigra v9 can query it alternatively. Since VirtualCenter manages all of the ESX servers, it maintains a list of the guest VMs hosted on each ESX host which Asigra v9 requests.

Once Asigra v9 has this information, it can now display the individual ESX servers on its management console GUI and the guest VMs on each physical ESX server. This serves three important functions.

- Asigra v9 can automatically discover new guest VMs on individual VMware ESX servers as guest VMs are created. This minimizes the possibility that as new guest VMs are created they are not configured for data protection.
- Automatically obtaining information about guest VMs on each ESX server enables Asigra v9 to track the movement of guest VMs from one ESX server to another. Using VMware's VMotion, administrators can dynamically move a VM from one physical ESX server to another for purposes such as failover or to granting it access to another ESX with more (or less) resources. This feature ensures that guest VMs ontinue to receive uninterrupted data protection regardless of on which ESX server they reside.
- Asigra v9 supports a wide range of operating systems and applications. Supported operating systems include Linux, Windows and all major forms of Unix while supported applications include DB2, MS-Exchange, MS-Sharepoint, MS-SQL and Oracle among others. Supporting this range of operating systems and applications provides companies a single platform to use for the protection of all guest VMs regardless of what operating system or application it hosts.

## Simplified VM Backup Configuration.

By automatically discovering and tracking what guest VMs are on each ESX server, Asigra v9 addresses some of the specific, hidden problems associated with protecting guest VMs. An initial problem that Asigra v9 solves is the need to install an agent on a newly created guest VM. By using the agentless technology in conjunction with its automated discovery of the guest VMs, a company can immediately configure each guest VM for backup without waiting for the install of an agent on each guest VM.

Since Asigra v9 knows what guest VMs are on each physical ESX server, it facilitates the scheduling of multiple backup jobs of guest VMs on the same ESX server. As backup jobs complete on one guest VM,

Asigra v9 can detect that and then initiate a subsequent backup job on another guest VM on that ESX server. Having visibility into what guest VMs are on an individual ESX server thereby minimizes the possibility of multiple backup jobs kicking off at the same time on the same ESX server. Using the information companies can also prioritize in what order backups jobs run on the guest VMs to ensure that backup service level agreements (SLAs) are met for specific application.

## Reigning in VMware Costs and Complexity.

The often forgotten part of the equation in implementing VMware server environments is reigning in the ensuing costs and complexity that VMware introduces. Nowhere do these management costs and complexity become more evident than when a company goes to protect its guest VMs on its VMware ESX servers.

Asigra v9 gives you the opportunity to change that equation. By delivering the means to auto-discover guest VMs on individual VMware ESX servers and coupling that with the agentless backup of guest VMs using CDP, incremental or VMDK-based forms of backups, Asigra v9 fundamentally changes how companies can protect their VMware environment going forward.

Asigra's capacity-based model plays particularly well in VMware environments since the amount of redundant data is typically high so de-duplication ratios are equally high. Couple this model with the simplicity of deploying Asigra v9 into VMware environments because of its agentless architectures and it becomes evident that many of the hidden costs and complexity associated with the protection of VMwareVMs are simplified by the introduction and use of Asigra v9.

To get more details on Asigra v9, click on www.RecoverYourCool.com/v9query to enter in your question and a product representative will get back to you.

## About Asigra.

Leading organizations reduce costs by applying cloud computing to backup and recovery with efficient, cost-effective and transformational solutions from Asigra. Customers consistently redirect savings derived from our approach to projects of higher strategic and personal value, many of which have been on-hold for a year or more. The positive business outcomes made possible from a low-touch agentless architecture are revealed through Asigra's Day One ROI™ - an exercise that delivers enormous value with little up-front investment.

Tel: 416.736.8111 Fax: 416.736.7120 Email: info@asigra.com

RecoverYourCool.com

Asigra.