Lab Validation Report

Asigra Public Cloud Backup v11

Cloud-based Backup, Powered by Asigra

By Brian Garrett with Jason Buffington

October 2011

Contents

ESG Lab Reports

The goal of ESG Lab reports is to educate IT professionals about emerging technologies and products in the storage, data management and information security industries. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments. This ESG Lab report was sponsored by Asigra.

Introduction

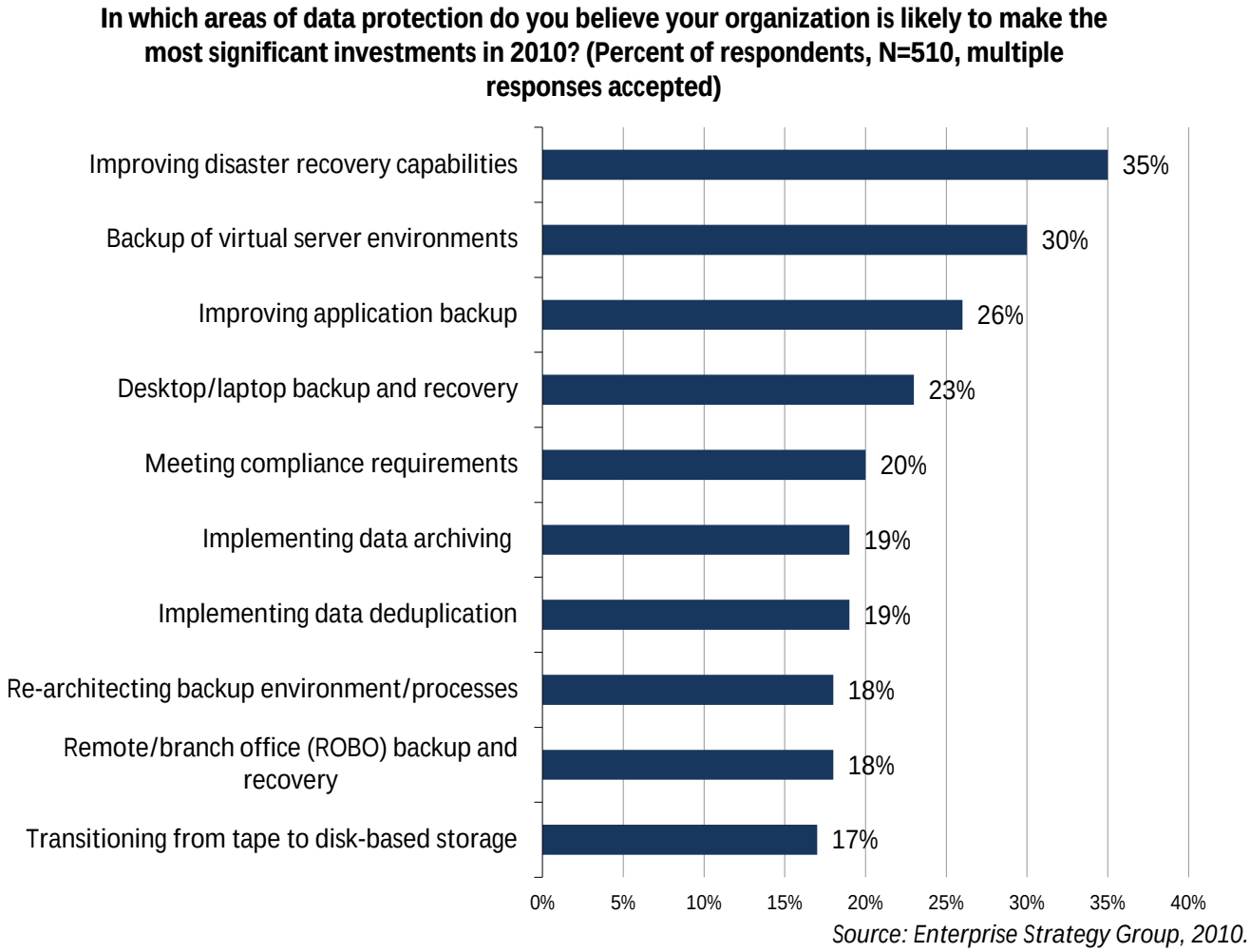
With more than 25 years of remote data protection experience, Asigra has created a field-proven software platform that provides cloud-based protection of data center, remote office, and mobile endpoint devices from a single platform. This ESG Lab Validation report documents the results of hands-on testing of Asigra Cloud Backup version 11, focusing on security, performance, efficiency, scalability, and breadth of coverage.

Background

Data protection processes and technologies are vital to ensuring an organization's operational, regulatory, legal, and financial health; as a result, they are included in every IT budget and are top of mind for data center staff. However, due to the complexity and expense of backup, restore, and disaster recovery, many organizations are willing to invest in methods that can save time, reduce costs, and simplify management.

Respondents to a recent ESG survey indicated that their most significant data protection investments would be in the areas of improving disaster recovery (35%), backing up virtual server environments (30%), improving application backup (26%), and desktop/laptop backup and recovery (23%) (see Figure 1). Also among the top ten were re-architecting backup environment/processes and ROBO backup and recovery.[1]

Figure 1. Top Ten Areas of Data Protection Investment



Source: Enterprise Strategy Group, 2010.

Backup is the first line of defense against downtime. Using the cloud can improve the backup/recovery process by enabling secure, reliable data protection for data centers and remote offices while reducing costs. But IT

[1] ESG Research Report, 2010 Data Protection Trends, April 2010

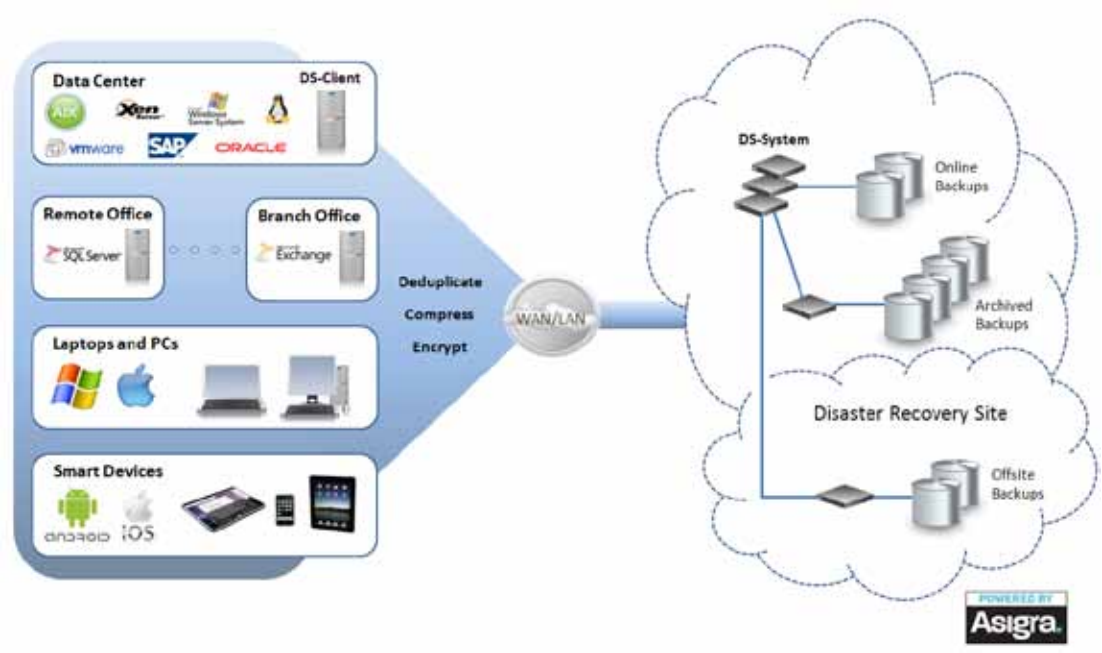
organizations still face an uphill battle: employees increasingly depend on mobile devices that are hard to keep track of and manage. In addition, as data volumes continue to skyrocket, backup windows shrink and SLAs become harder to meet. Budget constraints also drive organizations to seek solutions that are highly optimized while requiring little administration.

Powered by Asigra

Asigra is a leading provider of cloud-based backup and recovery solutions for IT organizations and managed service providers. Supporting private, public, and hybrid cloud environments, Asigra provides backup and continuous data protection (CDP) with global deduplication, compression, and WAN optimization to minimize costs. Intelligent and simple to deploy and use, Asigra offers rollback to any point across all devices, ensuring the ability to meet a range of recovery time and recovery point objectives. Asigra Cloud Backup is easy to manage and scale, and is plug-compatible with existing backup software, enabling simple deployment in data centers and remote offices. Its security features are second to none and combining it with Asigra's Recovery and Restore Assurance (R2A) creates a trusted environment whether backup is on-premises or provided as a service.

In June 2011, Asigra introduced version 11, the first offering to provide end-to-end cloud-based data protection for an organization's entire digital footprint. As shown in Figure 2, Asigra collects data from data centers, remote offices, and user laptops and desktops as well as smart phone and tablet computers. This data is then deduplicated, compressed, and encrypted before being transmitted across the network to a cloud-based target site to be stored. Target systems can be located onsite, in a remote data center, or with a service provider.

Figure 2. Cloud Backup, Powered by Asigra



Components

Asigra's offering consists of two primary components: the DS-Client installed in the data center (or wherever the production data resides) and the DS-System located where the backups will reside. This architecture enables Asigra to support a wide range of physical and virtual operating systems, servers, databases, applications, and storage environments. Enterprise and SME organizations benefit from a pay-as-you-grow licensing model based on the amount of compressed and deduplicated data stored. A central GUI is used for management and task automation. For management efficiency, Asigra can be mass deployed to physical and virtual LAN devices as well as remote devices; configuration, scheduling, backup set creation, and retention rules can all be set simultaneously.

At the production site, a single DS-Client runs on a dedicated Windows, Linux, or Macintosh server to collect data from all agent-less production sources. After data is gathered, it is deduplicated, compressed, encrypted, and sent over the WAN to the target site.

The DS-System is installed in the cloud core or data center at the target site. This Windows or Linux server accepts the data set and maintains, manages, and validates the online storage repository residing on direct, network, or storage area network attached storage (DAS, SAN, or NAS). DS-Systems are available in standalone or highly available N+1 configurations. For long term retention, the optional Backup Lifecycle Management (BLM) Archiver enables archiving of DS-System data. Additional Replication DS-Systems can be located in a disaster recovery site for redundancy and high availability; DS-Client data is redirected there if the primary DS-System is unavailable. Additional components are available, including:

- **LAN Discovery**, which analyzes and reports on storage inefficiencies, enabling IT to optimize storage and backup processes to reduce costs and improve performance.
- **Autonomic Healing**, which scans to detect problems and sends alerts so IT can intervene.
- **Local Storage**, which provides hybrid cloud support as it stores copies locally for fast recovery.
- **A Network Operation Console (DS-NOC)**, which provides centralized management of backup and recovery services.
- **A license management server**, which provides a single point of management for Asigra licenses, regardless of where Asigra services are deployed: within the organization or around the globe.

The balance of this report explores how Asigra Hybrid Cloud backup version 11 can be used to address the key challenges associated with deploying a cloud-based backup solution:

Breadth

Asigra's 25-year heritage of providing cloud-based backup services has resulted in a single solution that can be used to protect a broad and comprehensive set of data sources from mission-critical applications residing in the data center; to business-critical applications running in remote and branch offices; to mobile laptops, PCs, smartphones, and tablets located anywhere on the globe.

Trust

Trusted cloud-based backup and restore services are provided via FIPS-140 certified military-grade encryption of data in transit and at rest. No Asigra system has been breached or compromised in 20 years—a testament to Asigra's commitment to trust and security.

Efficiency

Asigra reduces the resource impact of cloud-based backup and recovery services using an advanced and field-proven agent-less architecture design to reduce application server overhead. Utilization of LAN, WAN, and disk-based backup capacity are reduced through a combination of global deduplication and compression.

Performance

Version 11 includes several new features designed to improve performance, including support for 10 Gbps LAN interface and continuously-improving IO processing and delta algorithms. Asigra has also added API-level integration with NetApp FAS devices, which enables Asigra to leverage NetApp snapshots.

Scalability

The field-proven power and durability of the N+1 DS-System design can be used to meet the backup and recovery performance needs of any organization regardless of size.

Partners, Powered by Asigra

Asigra's multi-tenant cloud backup and recovery solution enables providers to deliver cloud-based backup services to customers of all sizes. Everything a provider needs to deploy, provision, and sell cloud-based backup is included. Asigra Cloud Backup includes a multi-dimensional, multi-tiered billing system for rapid service deployment and centralized manageability. SLA monitoring and management tools simplify administration, while extensive reporting, notification, and audit trail capabilities ensure providers can track problems, identify unprotected devices, and remain apprised of backup status. In addition to the data security features, the multi-tenant provider environment has role-based vault access which enables different information to be viewed by backup administrators and business executives, and restricts access for account changes. Tiered recovery lets providers offer service tiers at various price points so customers can match data value to protection cost.

Several new features in version 11 are designed to improve management and help service providers differentiate their offerings:

- *DS-NOC* is the new network operations center designed to improve visibility and control of all DS-Systems, DS-Clients, BLM Archivers, and DS-Billing Centers. License status, capacity usage, and backup completion can be viewed at a glance. Providers can manage across all systems and drill down to view details and manage DS-Clients.
- The *single cloud License Server* manages all licenses of all components across the Asigra environment. This enables providers to allocate storage capacity where and when needed, while allowing components to draw capacity from the unallocated pool.
- *Central configuration of DS-Clients* enables service providers to differentiate their offerings based on levels of customer control and flexibility. Providers can offer a range of service levels at different price points.
- *Multi-tenant DS-Client* enables providers to save the costs of managing individual DS-Clients with the new secure tenant layer that allows a single DS-Client to house multiple customers.

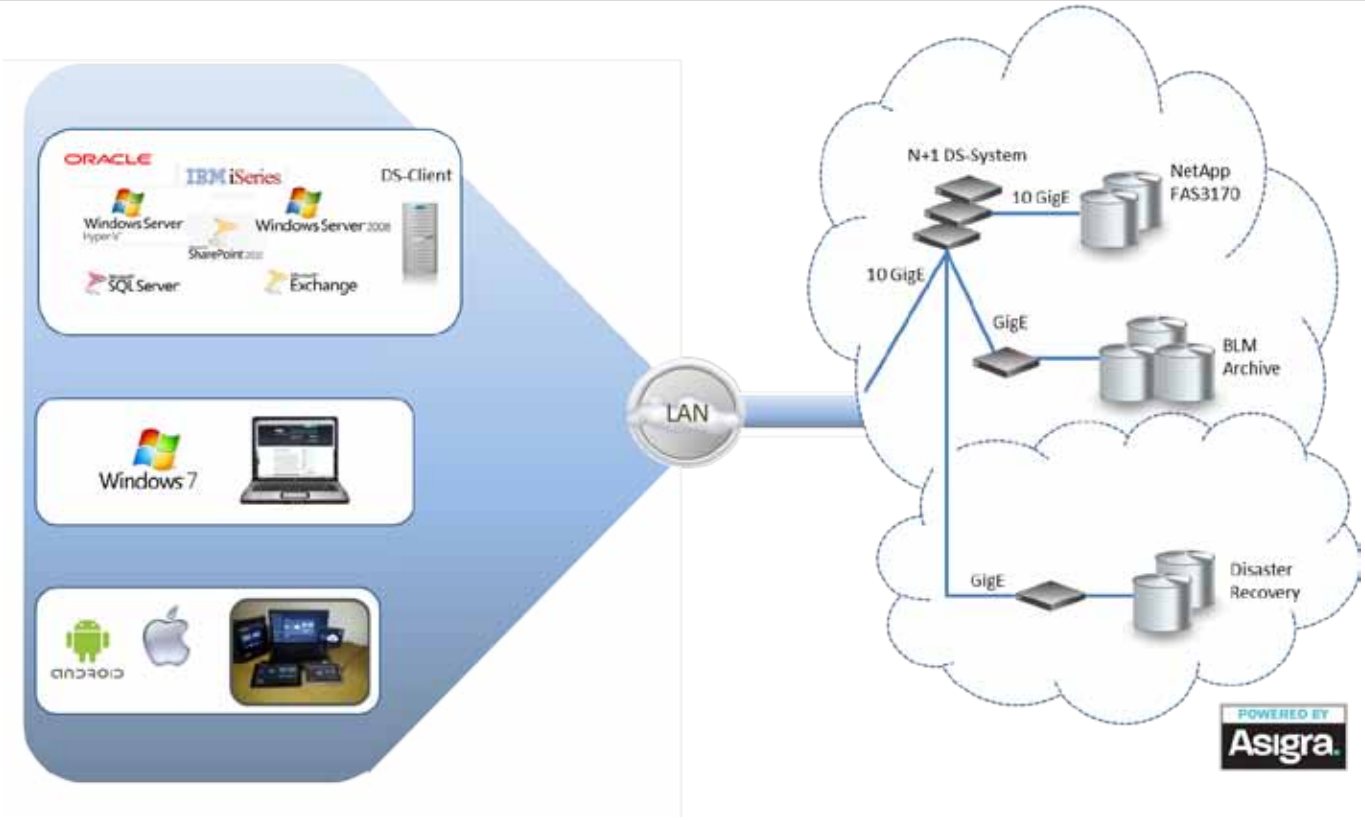
ESG Lab Validation

ESG Lab performed hands-on evaluation and technical auditing of several aspects of the Asigra v11 technologies and solution offerings at the Asigra headquarters in Toronto, Canada.

Getting Started

The test bed during the ESG Lab Validation is shown in Figure 3. A subset of the operating systems, server virtualization platforms, applications, laptops, and smart devices that can be protected with Asigra Cloud backup version 11 is shown to the left. Testing was performed using a combination of 10 Gbps and 1 Gbps Ethernet network connections in a simulated data center. Online backup data was stored on a NetApp FAS 3170 Filer. A BLM archive and a disaster recovery solution at a simulated remote site were also used to test the "Powered by Asigra" solution.

Figure 3. ESG Test Bed



Breadth

ESG Lab testing began with an examination of the breadth and depth of the data types that can be protected with an Asigra solution. A server virtualization platform powered by Microsoft Hyper-V was tested (VMware ESX and Citrix Xen Server are also supported). An Oracle 11g database was backed up and restored with the "classic" Asigra agent-less method and the more recently added SBT method. Microsoft Windows Server file system data was tested with and without the use of Microsoft volume shadow copy (VSS) services. Microsoft SQL Server was also tested with and without the use of VSS. Microsoft Exchange was tested with the classic agent-less method and with DS-Recovery Tools, which provided mailbox-level recovery. Data residing in a folder on an IBM iSeries server was backed up and restored as well.

A laptop running the Windows 7 operating system was tested along with an assortment of smart devices including an Apple iPhone, an Apple iPad, and a tablet running the Android operating system. A summary of the data types

that can be protected with Asigra Cloud Backup version 11 is depicted in Table 1. The protectable types tested by ESG are indicated with a check mark.

Table 1. Protectable Data Types with Asigra Cloud Backup

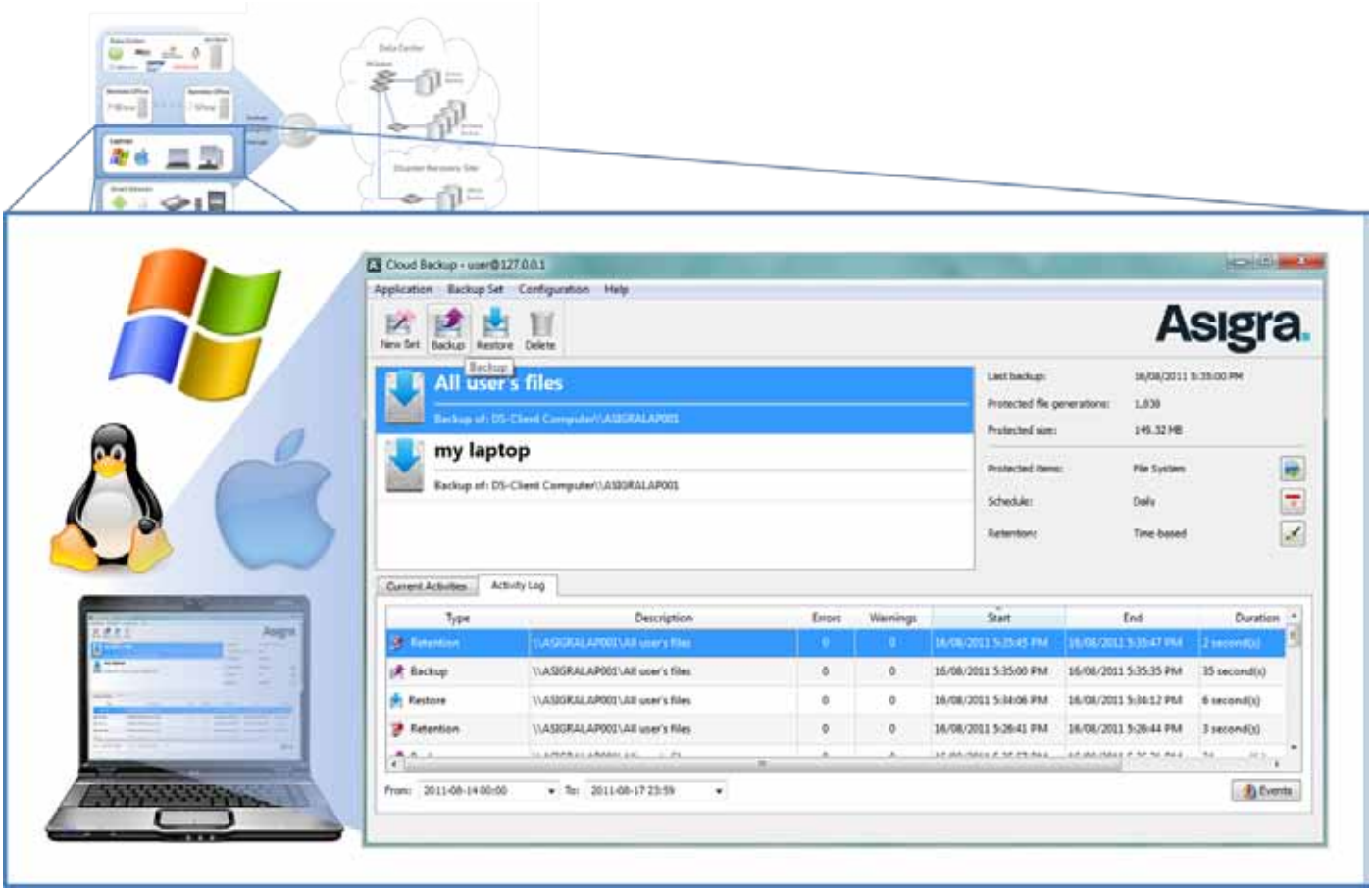
Servers		Mobile Laptops and PCs	
DB2		Windows XP	
File System	ü	Windows Vista	
GroupWise		Windows 7	ü
Hyper-V	ü	Windows Server 2000	
Lotus Domino		Windows Server 2003 and 2003 R2	
Lotus Notes		Windows Server 2008 and 2008 R2	ü
Microsoft Exchange Server	ü	Mac OS/X – up to Snow Leopard	
Microsoft Outlook		SUSE Linux	
Microsoft SharePoint		Red Hat Linux	ü
Microsoft SQL Server	ü		
MySQL			
Oracle	ü		
PostgreSQL			
SAP			
Sybase		**Consumer Devices**	
System i/Power 6		iOS for iPad & iPod	ü
VMware		Android Smartphone 2.2+	ü
XenServer		Android Tablets 3.0+	ü

Smartphone and tablet support is one of the most noticeable enhancements in version 11. The deceptively simple single-click user interface for an Apple iPhone is shown in Figure 4. With a single operation, this interface was used to back up iPhone contacts using an application that's freely available at the Apple App Store.

Figure 4. Smart Device Support for Android and iOS

While Figure 4 shows the simplicity that is expected with smart devices, Figure 5 shows how user-centric laptops and desktops offer a wider variety of options and customization. This simple and easy to use GUI was used to backup and restore files in a "my documents" folder on a laptop running the Windows 7 operating system.

Figure 5. Mobile Device Support for Laptops and PCs

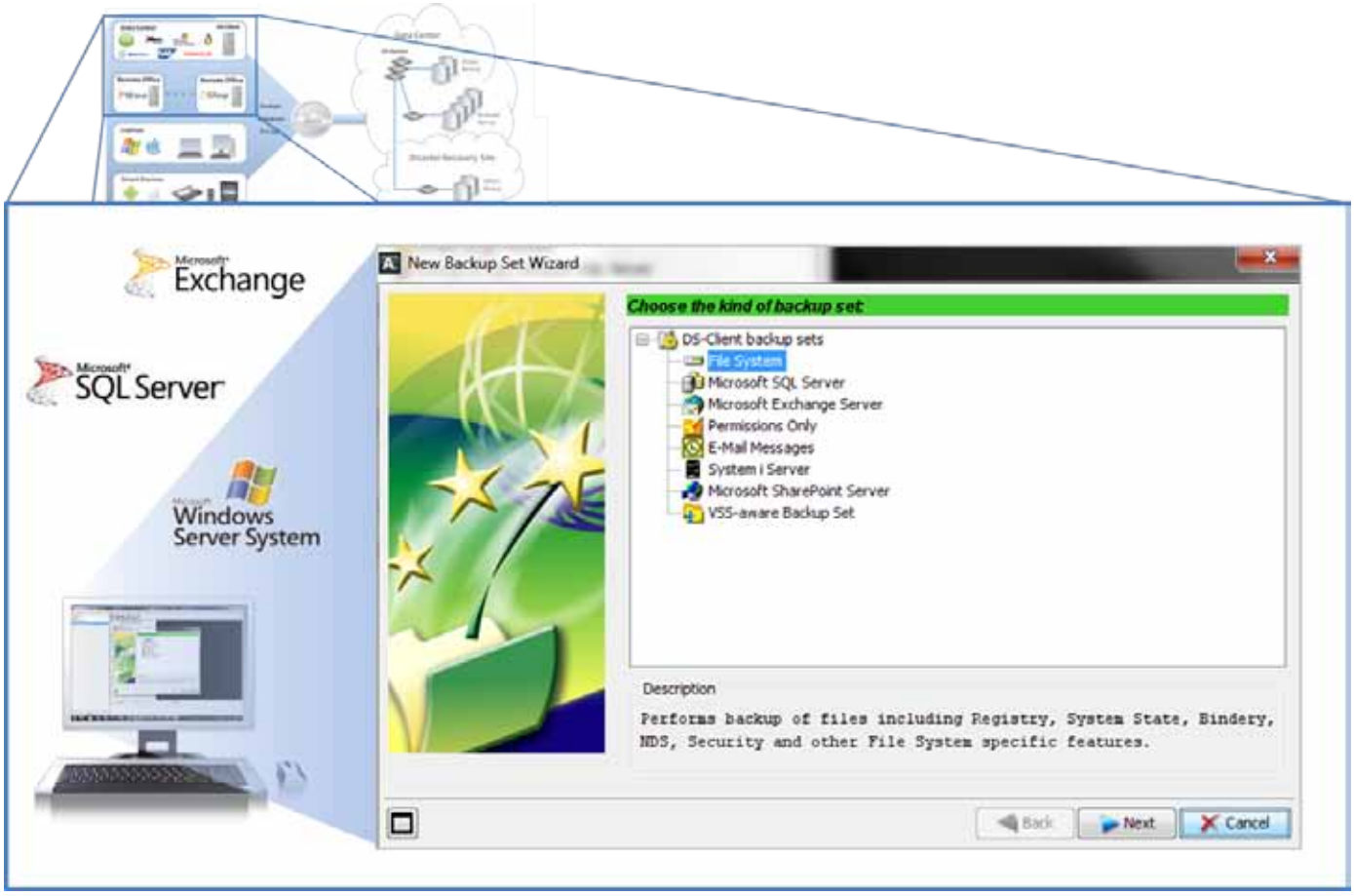


ESG Lab examined the mass deployment option which can be used to automatically deploy the Asigra Mobile application to hundreds or thousands of users within an organization. This option can be used to automatically "push" the installation of the Asigra Mobile application to users when they log into a Microsoft active directory domain. Mass deployment can not only be used to automatically install and start the Asigra Mobile application the next time a user logs in, it can also be used to deploy custom backup policies. Restores from the DS-System can be performed by an administrator or by end-users.

Agent-less server backups were tested with the DS-Client user interface. Asigra agent-less backups leverage industry standard operating systems and APIs to retrieve backup data over the network, ensuring that backups do not drain processing power from servers, and they simplify Asigra deployments and upgrades. The agent-less design simplifies scaling to easily accommodate additional capacity, applications, backup sources, and target sites. In addition, it eliminates security risks that agents can present.

Wizards provided within the DS-Client user interface were used to configure, execute, and monitor backups and restores for physical and virtual servers running a variety of operating systems and applications. A DS-Client screen shot showing a subset of the servers that were backed up during ESG Lab testing is shown in Figure 6.

Figure 6. Physical and Virtual Servers in Data Centers and Remote Offices



Why This Matters

More and more organizations are struggling with the cost and complexity of maintaining multiple backup solutions. Whether through acquisition or out of necessity, different solutions are often used to protect different types of data. Some organizations are forced into a new solution for virtual servers due to overhead or performance concerns. Others adopt new methods for protecting remote and branch offices. And a growing number are concerned about the risk of losing vital information assets residing on mobile laptops and smart devices.

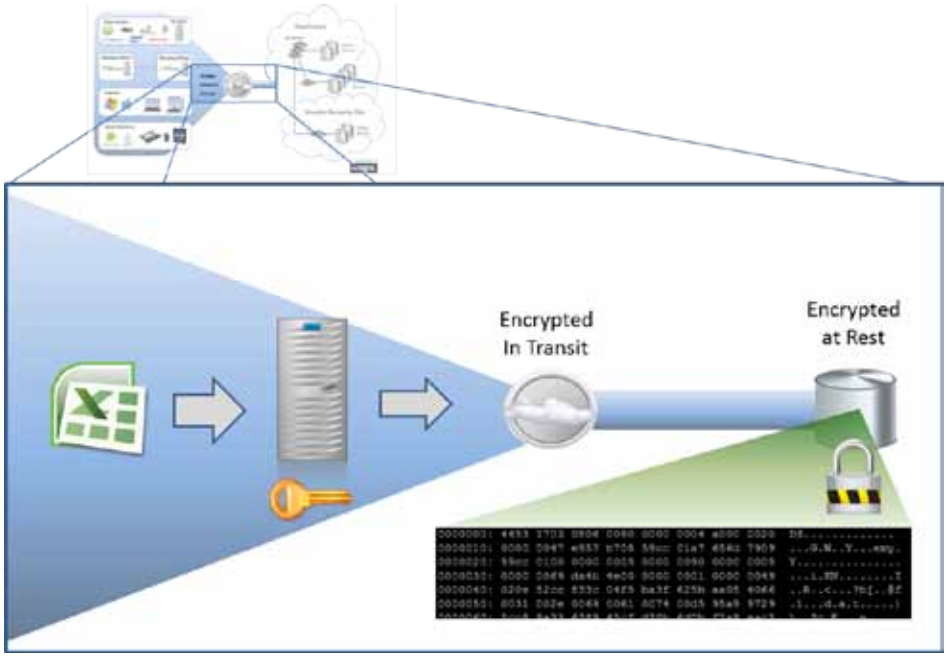
Most of the early cloud backup solutions (Asigra excluded) were created with consumers or small businesses in mind. These solutions haven't grown to support the breadth and depth of operating systems, applications, and data types supported by Asigra and backed by 25 years of experience in enterprise deployments.

ESG Lab has confirmed a single solution from Asigra can be used to protect an amazingly broad set of data types from mission-critical Oracle servers, to business-critical Microsoft applications, to laptops and iPhones.

Trust

One of the most common concerns when evaluating a cloud-based backup solution is security. More specifically, users must know that they can trust their backup provider, whether that is a third-party cloud provider or even their own IT team. The key to the Asigra security model is in the security keys themselves, which are DES-128 by default with up to 256-bit encryption supported. As shown in Figure 7, backup data is encrypted at the source site and remains so both in flight as well as at rest on Asigra DS-System storage. The encryption key is typically held by the customer or a third-party escrow agent, which eliminates the risk of unauthorized decryption by Asigra or a cloud backup provider. The screenshot of an encrypted data block at rest that's shown toward the right of Figure 7 was obtained during ESG Lab testing.

Figure 7. FIPS 140-2 Certified End-to-End Encryption



The Federal Information Processing Standard (FIPS) 140-2 certification is the most stringent security accreditation defined for cryptographic modules by the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce. Asigra participated in a multi-year effort to become "FIPS Certified" with a goal of obtaining independent verification of the security of its encryption methods.[2] As of this writing, Asigra is the only remote backup solution to have achieved this level of certification.[3]

Why This Matters

When the offer is "remote backup," a primary objection is almost always trust. In fact, a recent ESG research survey on cloud computing adoption trends showed that data security/privacy was the number one concern limiting broader adoption of public cloud computing.[4]

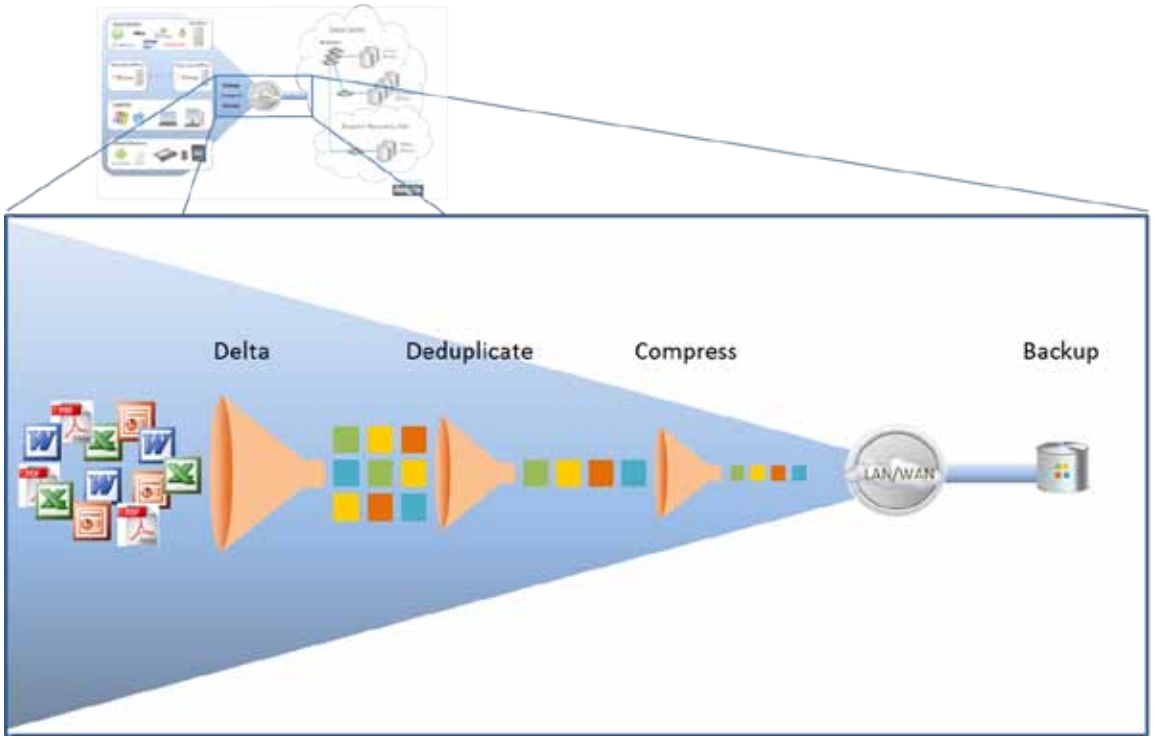
Asigra has gone to great lengths to not only deliver a solution that securely addresses the concerns of data confidentiality, but also to pursue the significant achievement of gaining military-grade FIPS 140-2 certification.

[2] http://www.asigra.com/fips-140-2-certification-backup
[3] http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm#1240
[4] Source: ESG Research Report, *Cloud Computing Adoption Trends*, May 2011.

Efficiency

Asigra was designed from the ground up with a goal of optimizing the use of expensive WAN bandwidth and disk capacity. By removing redundant data (globally across sites and servers) and compressing unique data at the client before transferring backup data across the network, Asigra reduces the amount of disk storage and bandwidth needed for backups. The result is efficient use of network bandwidth and disk capacity, faster backup and recovery times, and lower costs. The efficiency of the Asigra architecture is summarized in Figure 8. Delta differences in data to be backed up are digitally hashed and compared with data that has already been stored. Only unique data is compressed before it is sent over the network and stored on disk at the DS-System.

Figure 8. Optimizing Network Bandwidth, Performance, and Disk Capacity



ESG Lab Testing

- A 500 MB Oracle database was backed up[5]
- After deduplication and compression, only 83 MB of data was stored on the DS-System (6:1 reduction)
- Three rows were deleted and two rows were added
- The second backup moved only 2.8 MB of delta data was stored (180:1 reduction)

Why This Matters

Data protection and disaster recovery are key areas of concern and investment for most organizations. Constantly growing data volumes put pressure on data protection systems, processes, and budgets. A backup-as-a-service solution that reduces the cost of network bandwidth and disk capacity is a compelling alternative to traditional backup and recovery software.

ESG Lab has confirmed that Asigra Cloud Backup uses a combination of delta, deduplication, and compression technologies to dramatically reduce the cost of network bandwidth and disk capacity.

[5] The 500 GB demonstration database included in the Oracle distribution kit was used during testing.

Performance

Performance is a key concern when implementing a cloud-based backup solution. First and foremost, the solutions must be designed to optimize the use of WAN or LAN bandwidth. As described previously in the efficiency section of this report, Asigra uses a combination of global source-side deduplication and compression to minimize the amount of data sent over a WAN or LAN. Restore performance is optimized with hybrid cloud support that leverages an optional copy of the most recently backed up data on a DS-Client. With an Asigra hybrid cloud, the vast majority of restore requests for accidentally deleted, overwritten, or corrupted files are provided by a LAN attached DS-Client, which eliminates the need for sending data over a WAN.

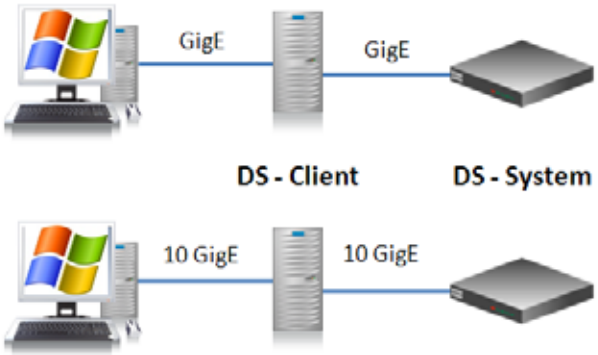
Asigra version 11 includes several new features designed to improve performance. These include support for 10 Gbps LAN interfaces, upgrades to Asigra internal process that speed reads/writes, multi-threaded deduplication, and improved IO processes and delta algorithms. Asigra has also added API-level integration with NetApp FAS devices, which enables Asigra to leverage NetApp snapshots.

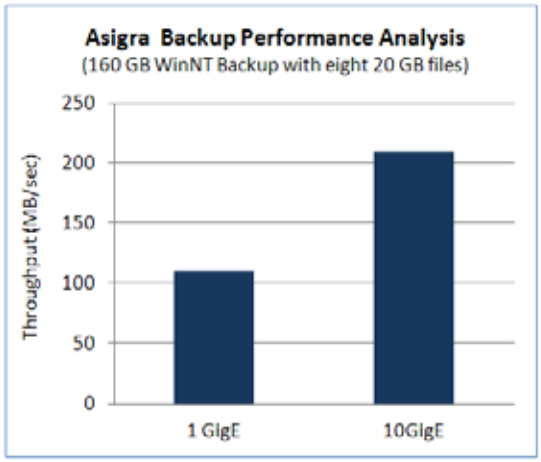
ESG Lab Testing

ESG Lab tested NetApp snapshot integration and 10 Gbps LAN support. NetApp Filer snapshot integration was easily configured from the DS-System management console. The use of snapshots to improve the performance and parallelism of restore and remote replication operations was confirmed via an audit of Asigra activity logs.

Support for a 10 Gbps LAN was tested with a variety of application servers and data types. An end-to-end 10 Gbps network was created with 10 Gbps Ethernet connections from application servers through DS-Clients to DS-Systems and NetApp storage. A server running the Windows Server 2008 R2 operating system was used to compare backup performance over 10 Gbps vs. 1 Gbps Ethernet. The elapsed time required to backup eight 20 GB files was used to calculate the overall throughput of backup jobs. The results are shown in Figure 9.

Figure 9. Optimizing Network Throughput





What the Numbers Mean

- The 1 GigE test bed delivered 111 MB/sec of backup throughput.
- 111 MB/sec over a single GigE interface is very impressive when compared with a theoretical maximum of 128 MB/sec for a single GigE interface. This extremely efficient use of available bandwidth is due to the continuously improving performance and parallelism developed by Asigra.
- The 10 GigE test bed yielded 205 MB/sec, which is nearly twice the capabilities of a 1 GigE network.
- ESG Lab testing was not able to saturate the available bandwidth of the 10 GigE network. This is likely due to the fact that the network was no longer the limiting factor in the overall throughput of the backup

solution. The bottleneck had more likely shifted to the capabilities of the storage in the server being backed up.

- An-end to-end backup throughput rate of 205 MB/sec can be used to back up data at a rate of 738 GB per hour—that's 5.9 TB during an eight-hour backup window.
- While these results provide a good indicator of the mature and well-tuned performance capabilities of the Asigra architecture, they cannot be used to predict the performance of Asigra technology deployed in a public or hybrid cloud backup with limited WAN bandwidth.

Why This Matters

Strict SLAs and business continuance requirements are pressing organizations to back up and restore data as rapidly as possible. However, massively growing data volumes and shrinking backup windows make this difficult.

Asigra has been continuously improving the performance of its growing family of backup-as-a-service offerings over the past 25 years. With recently added 10 Gigabit Ethernet support, Asigra has turbocharged its highly efficient and parallel architecture that uses source-side deduplication and compression to minimize WAN and LAN usage.

ESG Lab observed sustained private cloud backup speeds of 111 and 205 MB/sec over 1 and 10 Gbps Ethernet networks, respectively. The 111 MB/sec result proves that Asigra has a highly efficient and well-tuned architecture that maximizes available bandwidth. The 205 MB/sec result proves that Asigra not only improves backup speeds, but in fact removes the network as the bottleneck for backups running in a private cloud.

As a growing number of organizations deploy 10 Gbps Ethernet in the core of the data center, Asigra provides a future-ready solution with turbocharged backup and restore performance.

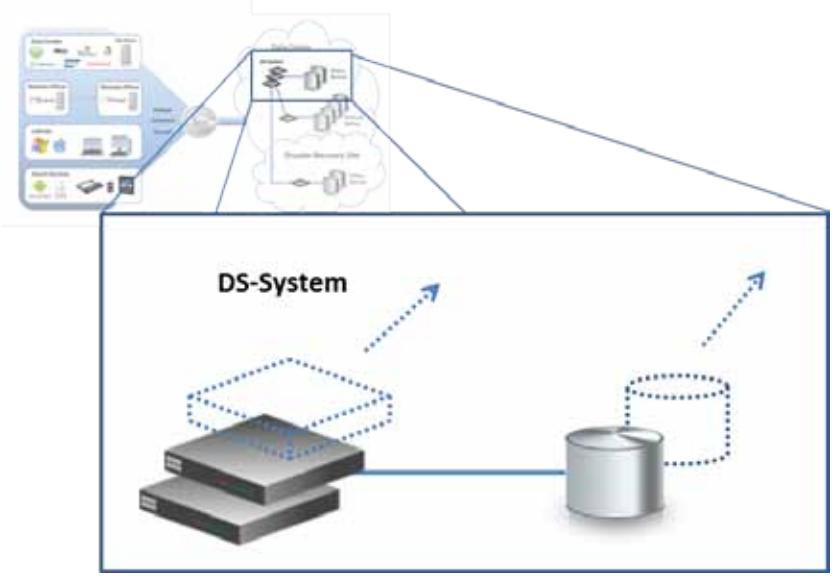
Scalable Manageability

The Asigra Cloud Backup solution was architected to provide online upgrades to transparently meet the changing needs of the business. The clustered N+1 design of the DS-System supports online addition of server and storage capacity.

ESG Lab Testing

ESG Lab performed an online upgrade of an existing DS-System. As shown in Figure 10, a server and additional NetApp disk capacity was added to a two-node DS-System. Backup jobs ran without interruption both upgrades.

Figure 10. Wizard-driven Online Cloud Backup Infrastructure Upgrades



The "add node" DS-System wizard was used to add the new server to the cluster. The simple single panel wizard was used to specify the IP address and network port of the new server. Four mouse clicks and three minutes later, the new node had been successfully added to the cluster.

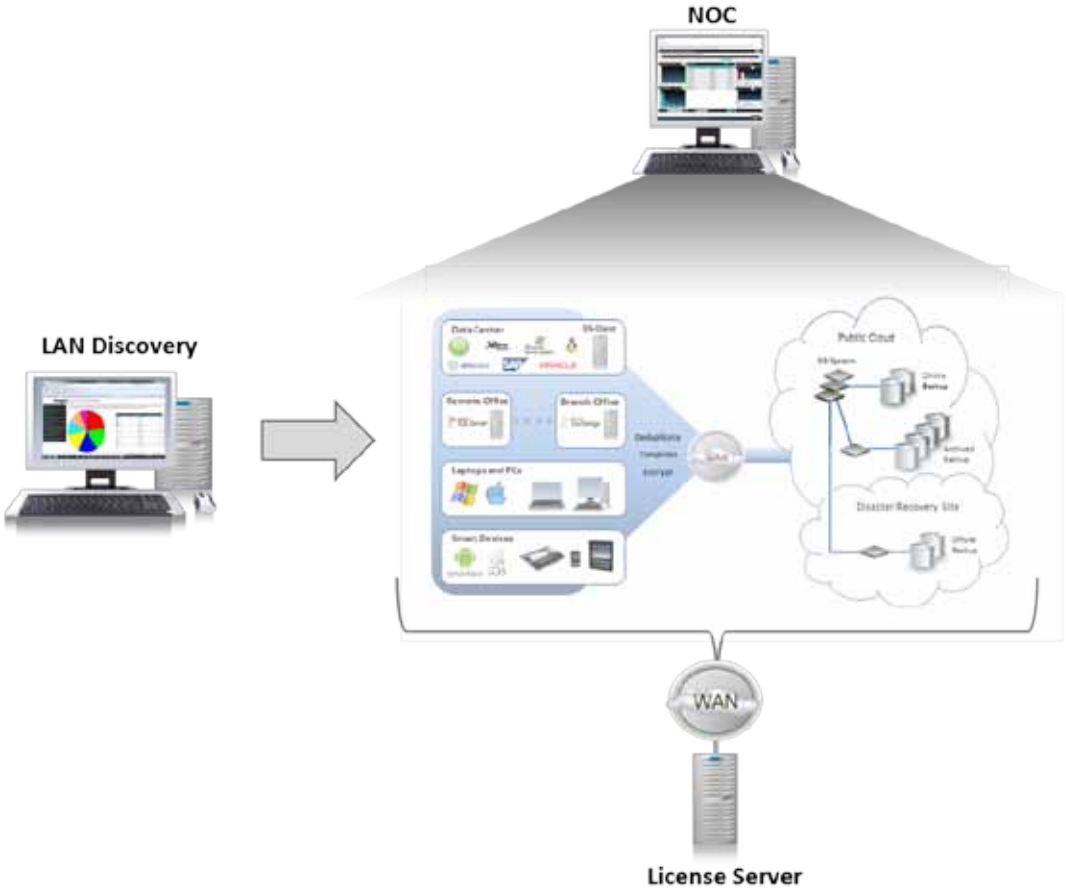
ESG Lab used NetApp network attached storage during the validation. New disk capacity was provisioned with the NetApp management console and added to the cluster. Adding disk capacity to the cluster was performed from an administrator command line interface on each node in the cluster as a new mount point was created on each node.

Next, ESG examined the powerful centralized management capabilities of Asigra Cloud Backup version 11 with a focus on the power of the LAN Discovery tool, the management DS-NOC, and the License Server.

The LAN discovery tool was used to scan the Asigra lab network. Servers, PCs, and laptops were discovered and analyzed by the tool. The tool can not only be used to plan and size an Asigra deployment, it also provides powerful reporting utilities which provide insight into the types of data that needs to be protected (e.g., file types), the size of data to be protected (e.g., the files consuming the most disk capacity), and the frequency of access (e.g., files that haven't been accessed in over a month).

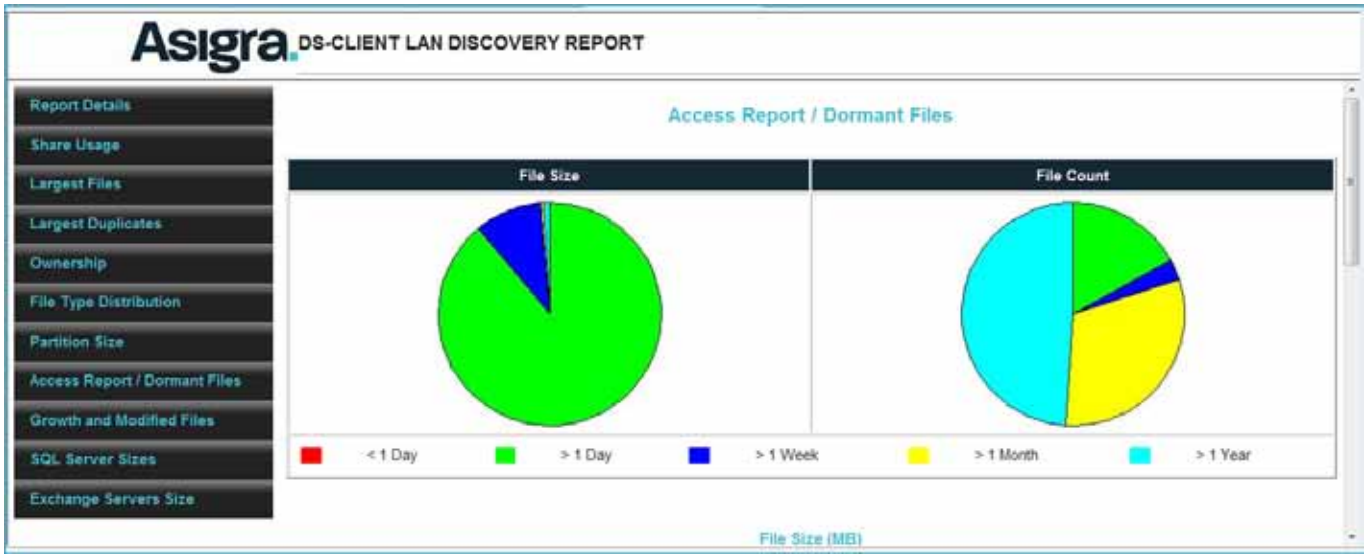
As shown in Figure 11, the centralized management capabilities of the Asigra Cloud Backup version 11 include the LAN Discovery tool for planning and optimization, the DS-NOC for centralized management of end-to-end Asigra data protection services, and the License Server for centralized monitoring and management of licensed Asigra modules (e.g., DS-System, BLM Archiver, Mobile DS-System, and Consumer DS-System).

Figure 11. Powered by Asigra: Simplified Planning, Management, and Licensing



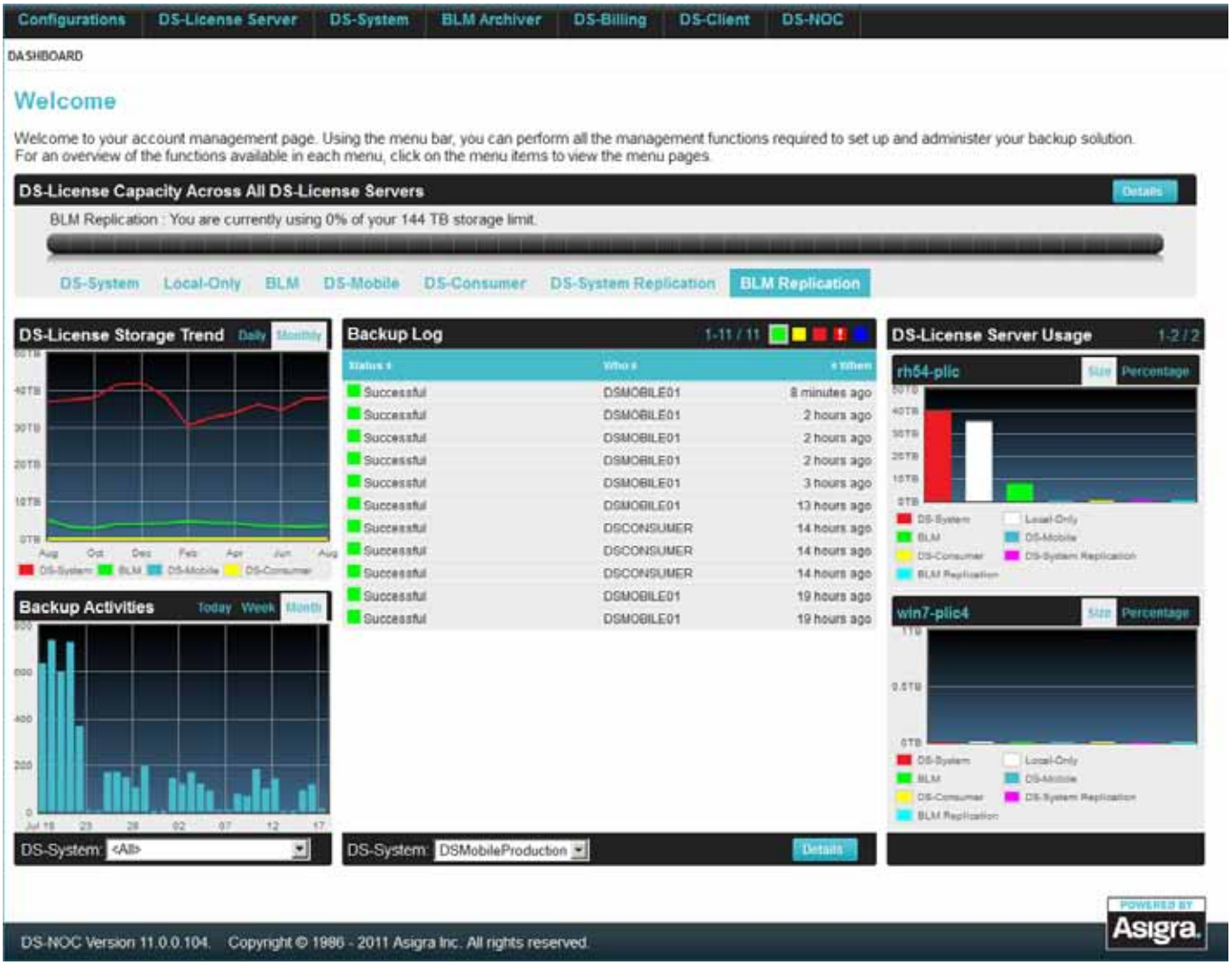
One of the many powerful LAN Discovery reports generated during ESG Lab testing is shown in Figure 12. This particular report is used to indentify dormant files that can be groomed before configuring an Asigra backup policy. Note that nearly half of the files haven't been accessed in over a year (shown in light blue in the chart on the right), yet those files represent only a small percentage of the total file size to be protected (shown in light blue in the chart on the left).

Figure 12. Powered by Asigra: LAN Discovery



The home screen for the DS-NOC, which was introduced in Asigra Cloud Backup version 11, is shown in Figure 13. ESG Lab was extremely impressed by the look and feel and power of this single pane of glass management interface. This single screen clearly shows recent backup toward the middle of the screen. Clicking on a backup job was used to drill down and diagnose backup or restore failures. The four graphs on this home page provide a clear view of all types of backup and restore activity, licensed storage capacity, and server usage.

Figure 13. Powered by Asigra: DS-NOC Dashboard



Next, ESG Lab examined the capabilities of the Asigra License Server. An Asigra License Server can be deployed anywhere in the world—all that is required is a laptop connected to the Internet. An emergency License Server can optionally be deployed as a backup. This server is used to provide automated monitoring, administration, and update of all Asigra licenses (DS-System, BLM, Mobile DS-System, Consumer DS-System). Licenses are maintained on an encrypted USB device that's plugged into the License Server. Updating a license is performed by creating and sending an encrypted copy of existing license data to Asigra. The DS-NOC screenshot shown in Figure 14 depicts the current license usage of systems in the Asigra lab during ESG Lab testing.

Figure 14. Powered by Asigra: Globally Managed License Server

Why This Matters

Cloud-based backup and recovery solutions are designed to quickly respond to the changing needs of the business without incurring downtime. Centralized monitoring of cloud-based backup infrastructure is needed to ensure the timely and correct completion of backup and restore jobs. Centralized management and licensing for all of an organization's backup and restore infrastructure reduces complexity and manpower.

ESG Lab has confirmed that Asigra's wizard-driven online upgrades, powerful DS-NOC, and automated license management reduces complexity and costs as they help IT respond quicker to the changing needs of the business.

ESG Lab Validation Highlights

- Apple iPhones, Apple iPads, and Android devices were backed up to an Asigra-enabled cloud using a simple one click user interface.
- Asigra mobile device support was used to backup and restore files residing in the "My Documents" folder on a Windows 7 laptop.
- Agent-less backups were performed for a variety of data types including Microsoft and Linux file systems, Oracle and SQL Server databases, Microsoft Exchange e-mail, and IBM iSeries folders.
- Backups and restores were performed using the native Oracle RMAN interface and SBT method.
- The security of backup and restore operations was verified via an audit of Asigra's FIPS-140 certification and an examination of encrypted backup data at rest.
- ESG Lab confirmed that Asigra Cloud Backup version 11 takes advantage of the increased bandwidth and performance of 10 Gigabit Ethernet networks.
- A centralized license manager was used to monitor and upgrade licensed capacity for a variety of Asigra modules (DS-System, BLM, and Consumer DS-System).
- The DS-NOC was used to view recent activity, health, capacity and license usage from a single pane of glass.
- Multi-tenant support and the ability to manage customer specific billing were confirmed.

Issues to Consider

- While Asigra backs up only to disk, it is designed to integrate with existing tape-based backup solutions from leading vendors. Disk-based Asigra backups can be exported as a file system and protected with existing backup software from leading vendors, ensuring compatibility with existing offsite and compliance processes. This capability also lets customers begin by using Asigra Cloud Backup to augment existing protections strategies; for example, customers may start with Asigra for virtual servers or ROBO backup, and expand as their confidence level increases.
- Depending on the volume of data, some customers may want to create their initial backup by delivering data on a storage device instead of backing up over the network. ESG did not test this feature, but Asigra supports this type of backup seeding using a variety of portable devices. A similar method is supported for large bare metal restores.
- In deploying data protection across the environment, customers should consider all parts of the cost equation. The total cost of deploying and managing individual backups directly to specified target devices, using different point solutions for each type of production data, providing bandwidth, and scaling these silos separately may be quite high, particularly as data volumes grow and compliance drives longer retention. While some are reluctant to take a risk with cloud-based backup, the TCO advantages indicate a significant potential cost advantage.
- While the License Server provides a centralized platform for simplified software license administration, automated billing for license costs and collection processes that create and return updated license files would be a welcome addition in a future version of the Asigra Cloud Backup platform. Asigra has advised ESG that this enhancement is planned for a future release.

The Bigger Truth

Since its founding in 1986, Asigra has been a truly innovative company. It offered backup to disk *25 years ago* before disk-based backup was a gleam in anyone else's eye. And Asigra did it without agents, because that was the best way for the customer—not the easy way.

Fast forward to 2011: while many improvements have been added over the years, including leveraging cloud computing to reduce costs and simplify management, the most recent version of Asigra's software is once again ahead of the field, with a breadth of offerings like no other. Many organizations protect data center servers one way, LAN-based laptops and desktops another way, and simply cross their fingers that smartphones and tablets remain intact; Asigra protects all devices with the same solution. The ability to perform enterprise-wide, cloud-based data protection across all devices, including even smart phones and tablets, from a single platform is a competitive advantage for service providers; the solution's elegance, efficiency, and management ease help keep costs down so providers can maximize profit.

Interest in backup-as-a-service is clearly growing. Data protection research conducted by ESG in 2010 indicated that while 17% of survey respondents were currently using a third-party online backup service, an additional 38% were evaluating or considering it.[6] Maturation of cloud solutions, along with faster bandwidth speed, make private, public, and hybrid clouds a viable option for backup. The reasons are compelling: reducing backup infrastructure, usage-based pricing, consolidating backup processes.

However, the challenges that must be overcome in order to make that leap are significant. Worries over data security make organizations reluctant to take a risk on backup to the cloud, and well-publicized cloud failures have not helped the cause. Another concern is bandwidth cost; cloud-based backups will consume more network resources, so efficiency features are required to reduce the amount of data being transmitted. And then there is the challenge of managing backups for multiple device types, ensuring different RPOs and RTOs, and scaling as needed.

ESG Lab hands-on testing has validated that Asigra provides end-to-end protection for an organization's entire digital footprint. Smartphones and tablets were backed up and restored using an extremely simple single-button user interface. PCs and mobile laptops were backed up and restored with an application that's not only easy to use, but simple to install using a mass deployment model that can be used to automatically push and configure policy-based backup software to thousands of employees. Servers in data center and simulated remote and branch offices were tested as well.

ESG Lab testing confirmed that Asigra Hybrid Cloud Backup version 11 addresses the key challenges associated with providing cloud-based backup and recovery services. Trust is provided with military-grade FIPS-140 certified encryption of data in flight and at rest. Efficiency is delivered with source-side global deduplication and compression. Performance is optimized with a continuously-improving efficient architecture that maximizes use of precious LAN and WAN resources and recently added 10 Gigabit Ethernet support. Scalability is provided with an N+1 architecture that can be easily upgraded online. Last, but not least, ESG Lab was most impressed with the recently added license manager and DS-NOC with a powerful and intuitive user interface which provides centralized monitoring, management, reporting, and billing for service providers.

It's no surprise that Asigra Hybrid Cloud Backup and Recovery exceeded 400,000 protected sites in April 2011, up from 250,000 in 2010. The quality of its solutions is unmatched; Asigra goes all in, whatever the feature. For example, Asigra doesn't just provide security features, it delivers encryption up to AES 256 and obtained military-grade FIPS-140 certification. Efficiency? Asigra offers not just deduplication, but global deduplication across all sites and all devices including smartphones and tablets. Asigra's lengthy résumé in the backup space has provided the company with intimate knowledge of both customer and service provider needs, and Asigra Cloud Backup Version 11 demonstrates its expertise. So, if you are looking for cloud backup experts, look no further than Asigra.

[6] Source: ESG Research Report, *2010 Data Protection Trends*, April 2010.

Appendix

Table 2. ESG Lab Test Bed

DS-System	
Operating System	Red Hat Linux
Server	4 (3+1) x dual 2.26 GHz quad-core CPU, 24 GB (or 16) 1067 MHz RAM
Storage	NetApp DS4243 24 x 600 GB SAS 15K NetApp DS4243 24 x 300 GB SAS 15K NetApp FAS3170 NetApp DS4243 12 x 500 GB SATA 7.2K NetApp DS4243 24 x 500 GB SATA 7.2K
DS-Client	
Operating System	Windows 7
Server	1 x single 2.67 GHz quad-core CPU, 32 GB 800 MHz RAM
Storage	2 TB, 10 disks, 15K FC
Cloud Protected Data	
Backup Sources	iPhone iPad Android smartphone Windows 7 laptop File System - Windows Server 2008 R2 SP1 Microsoft Exchange 2010 Microsoft Hyper-V R2 SP1 Microsoft SQL 2008 R2 SQL VDI (pipe) SQL Buffer Oracle 11g SBT AS400/iSeries

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel:508.482.0188 Fax: 508.482.0218 | www.enterprisestrategygroup.com