BLUESHIFT
DATA PROTECTION

Agentless Backup - How Does It Work

The Asigra backup and recovery solution does not require any agents to be installed but instead reaches out over the network to backup operating systems, file systems and applications, using industry standard programming interfaces, which inherently makes it easier to install and support than other backup and recovery solutions.

To understand how Asigra backs up data over a network without the use of agents, consider how a local hard drive on a typical PC can be accessed remotely. A system administrator only needs the right permissions to access that local hard drive over the network. A disk-to-disk backup is performed by simply copying the contents of the hard drive to another hard drive on the network.

Asigra software uses a sophisticated extension of this idea, unlike other software that requires agents on every machine. The Asigra solution is simple and elegant in concept, on a broad variety of operating systems and data types. As the industry’s only agentless, multi-site backup and recovery software solution, Asigra technology completely eliminates the negative impact of agents.

Actual backup method is different for each type of backup set. These are constantly changing and evolving as backup options are added, or versions change. Current common methods include:

Windows:
Uses standard Windows APIs, and utilizes RDP, WMI and RPC functionality.

Linux/Unix:
Uses SSH

SQL databases:
Either direct socket connection to the database, or interfaces with
database utility (rman for Oracle, pg_dump for Postgres, etc.)

VMware:
Uses VMware data protection API (VADP) over TCP connection.

The Asigra architecture consists of two software components: the DS-Client and the DS-System. DS-Client software, installed on one server (Windows, Macintosh, or Linux) at each local and remote site, captures data from its target backup machines. The DS-Client then processes the data to reduce its size (compression and deduplication), encrypts it for security, and then transmits the data via IP WAN to the DS-System at the storage location.

The DS-Client does not require installation of any backup agents on its target machines. The DS-Client fully integrates with NT domains, Trusts and Novell NDS trees and otherwise adopts the remote site’s existing LAN security settings. Using standard APIs, the DS-Client can remotely log into target backup systems, capture requested data and securely manage transmissions to the central site. Utilizing common data reduction technologies, the DS-Client minimizes the amount of data transmitted and stored at the on-site or off site vault.

The DS-System manages the storage repository for backup data transmitted from one or multiple DS-Clients. The DS-System (configured as direct-attached disk, NAS or SAN) can be installed on Linux and Windows platforms. Asigra software integrates a comprehensive feature set designed to maximize and accelerate data recoverability. An Autonomic Healing module, for example, runs seamlessly in the background to identify and isolate corrupt or otherwise problematic files. If a corrupt file is found to be irreparable, it is tagged to be re-transmitted on the next scheduled backup. Another feature, the Local Restore tool, allows remote-office storage of backup data. This ensures that local users can restore critical data immediately and at LAN speed. Additional Asigra tools include an Online File Summary, Long Term Storage policy-making, a Discovery Tool to automatically ascertain characteristics of primary data, Email Message Level Restore, Bare Metal Restore capability, Client and System Monitoring and SNMP Integration.

Why It Works

The Asigra software eliminates the requirement for locally installed agents because it leverages the protocols, APIs, methods and functionalities that platform, operating system, database and other application vendors utilize for remotely managing their own systems. Other backup and restore solutions require a unique backup agent (installed on every target machine) for each type of system and application. Asigra, however, supports all major platforms and applications with a software system composed of just two major components: the DS-Client (one installed at each site) and the DS-System (installed at the vaulting location).

Another advantage of the Asigra software is that it enables multilevel access controls. At installation, the DS-Client is assigned privileges to establish access rights that meet the requirements of the site or organization. For example, the DS-Client might be assigned multiple credentials for the same network to allow the domain administrator to backup all systems, including servers and workstations, while enabling users to control the backups of individual workstations. The Asigra software has also been highly optimized to conserve both LAN and target-system CPU resources. Implementing an Asigra backup and recovery solution produces immediate and dramatic benefits