



Frequently Asked Questions



July 30, 2009

General

What is ANS DataSafe service?

ANS DataSafe service provides on-line off-site data backup and recovery and is an alternative to traditional in-house tape-based backup solutions. It can also be described as a backup outsourcing service or as a backup utility (pay-per-use). Data is collected from the customer via DS client software and “shipped” electronically to the data center.

How does ANS DataSafe work?

ANS DataSafe installs DS client software on hardware at the customer site to serve as a backup engine. The software can backup any server on the network, per instructions from the backup administrator. Data is transmitted to a data vault at the data center.

Can ANS DataSafe back up entire enterprise, including laptops / desktops and remote offices?

ANS DataSafe can backup your enterprise systems and applications, regardless of where they are located, as well as laptops / desktops, for a complete backup solution.

How can we be comfortable with our data being off-site?

Your data is off-site as soon as your tapes are picked up by a tape storage company like Iron Mountain, in which case it is not in a secure form and can be, and often is, lost or mishandled. In case of a restore from remotely stored tape, tremendous amount of time, effort, and expense is required.

How will ANS DataSafe service help me reduce costs and improve service levels, including reducing the restore times?

The TCO savings for ANS DataSafe service normally exceed 35%. For some companies, especially with multiple offices maintaining small amounts of critical data, the TCO savings can be much higher, around 80%.

The savings come from the following budget items that can be eliminated or reduced: backup software license costs, backup software maintenance, backup server(s), libraries, tapes, hardware maintenance, labor for deployment and configuration, labor for system maintenance, maintenance costs associated with updates of backup software as well as updates of backup agents on each server, server build times (no agent is required), asset management costs, PO issuance costs (for new licenses and maintenance renewals), asset leakage (up to 20% for a large organization), cost of Iron Mountain or similar service, DR test costs (Iron Mountain charges per test), reduction in number of IT suppliers.

Additional savings are accrued from increased productivity of IT personnel and the users they support. ANS can supply a backup appliance so that the latest version of ALL data (files, folders, EM, SQL, etc.) is kept on site. Hence, the recovery times are minimal.

If a company has a utility computing initiative, i.e., working to align operational processes with IT processes and costs, ANS DataSafe will be a natural fit.

How will ANS DataSafe service help me improve service levels, including reducing the restore times?

An individual file can be restored almost instantaneously depending on the bandwidth. Restoring large files, residing on the data vault, will require more time depending on your Internet connection. However, this takes much less time than restoring from tape, especially if your tapes are located off-site.

Only incremental backups are performed, thus, reducing the overall times and network burdens.

What are the charges for ANS DataSafe service?

Customers are charged only for the encrypted data which resides on ANS DataSafe systems, either compressed data rates or uncompressed data rates. If a customer chooses to be billed for compressed data, the total amount of “chargeable” data, on average, is half of the original customer data, assuming a 2:1 compression ration. Increasing the number of backup versions and extending the retention horizon will result in increased amount of data and higher charges. Charges are per GB per month.

At the time of install, a one-time install fee is charged.

Is there a service agreement?

Customers are asked to sign a 36-month service agreement. Service agreement defines the service and SLA levels.

Installation

Who installs the ANS DataSafe service?

ANS will install the DS client software at a customer site and provide the necessary training. The initial set up charge includes between 1 and 3 days set up support, depending on the complexity of the installation.

How is the first backup done, if we have a lot of data?

For large data volumes, the initial backup may be done to a portable unit which is shipped to the data vault or backed up online. Future backups, which are incremental, will be transmitted via your connection to the Internet.

Is software installed on any other machines?

The ANS DataSafe DS Client software is an agentless design, requiring no additional software to be installed on any machines to enable backup. The only exception is if you are doing Message Level backup / restore with Microsoft Exchange. The agent installation on Exchange server does not require a reboot.

How do we control and monitor our backups?

The DS Client software acts as your interface with ANS DataSafe and enables the configuration of all backups and restores.

Setup of Initial Backup Sets and Schedules

Who does this?

As part of the installation training, ANS will ensure that all your main servers are configured to ensure their optimum backup and will provide training to nominated customer personnel. Additional training classes are available.

What frequency of backup can be set?

The backups can be configured as often as every hour or as infrequently as once a year.

What level of granularity is possible in setting up the backup, i.e. file level/individual database?

A backup set can include a whole server, share/volume, directory or even a single file. The backup set could even include just a registry.

How scalable is the ANS DataSafe backup solution?

ANS DataSafe backup solution can backup as little or as much data as you need.

Can the software be configured to stop backing up after a certain time has elapsed?

Yes, the software is designed to fit specific backup windows.

Compression, Encryption and Security

How and to what standard is the data encrypted?

ANS DataSafe's encryption standard is AES 256-bit. This level of encryption is approved by US Federal Government. Client data always leaves the client site, in an encrypted format. ANS does not have access to the encryption key which is stored by the client. The encryption key is required to enable a restore.

What is the typical compression ratio?

ANS DataSafe assumes a 2:1 compression ratio. ANS DataSafe employs a very powerful compression mechanism that can result in actual compression ratios up to 10:1, depending on the type of data. The compression ratios for already compressed files, e.g., zip files, can be lower than average.

What is delta blocking? How does it work?

Delta blocking divides all files into 4K blocks. When a file change is detected at backup, the Checksum of each 4K block is compared against the last known Checksum for the same block of the same file (stored in the database on the gateway). Only blocks that are different are pulled out to be re-transmitted off-site.

Transmission Off-site

How quickly will the data be transmitted?

10GB of post-compression, post-delta blocked data can be transmitted nightly over T1. A customer with 500GB of native data is estimated to generate 10GB of delta-blocked data.

Is the connection secure?

Data leaves the client site only after it has been encrypted. This is infinitely more secure than many current backup policies for unprotected and unencrypted data, e.g. 3rd party couriers taking the tapes offsite, onsite storage where tapes are left in cupboards overnight or backup data being sent offsite via the public Internet.

Do we need to install a firewall?

No, ANS DataSafe DS Client software encrypts data before sending to the vault. Although ANS strongly recommends every customer have a firewall to protect from security threats to their network.

Do we have to open my Firewall ports?

No, ANS DataSafe only needs outgoing port 3000 to be open.

Does all of our data get transferred every day?

Only newly created or changed data will get backed up. Duplicate or unchanged files will not be transmitted. In case of a restore, the file is rebuilt and the full file is delivered to the end user.

Offsite Storage

How many levels of protection does ANS DataSafe provide?

ANS DataSafe solution can provide up to 3 levels of data protection: a local backup on an appliance, a primary data center backup, and a secondary data center backup.

The primary data center is located in Simi Valley, CA. The secondary DS3 data center is located in Las Vegas, NV.

Is it secure and separate from other customers' data?

All customers are logically separated from one another at the data centers. Data encryption prevents any other party but the data owner to use the data.

Restoring Data

When can data be restored?

Data can be restored any time utilizing the tools within the DS Client software. For large restores, when restoring over the wire is not be feasible, ANS DataSafe customer service will arrange for a mobile vault to be shipped to the customer site. Customer must have an encryption key in order to enable the restore.

Can an individual file or registry be restored?

Yes, you can restore an individual file or registry and also specify which version you want to restore.

Can ANS DataSafe perform bare-metal restores?

After installing the operating system, a bare-metal restore can be performed. There is no need to apply service packs, configure domain security or install additional software to the new machine, as all this information will be included in the restore. The target hardware needs to be similar but not identical.

Can you restore a whole backup set to a point in time, e.g. last Monday?

Yes, ANS DataSafe will display all the files that were backed up on any given day and that can be restored. An administrator can just select the file from the list and enable the restore of files / directories / servers, subject to restore priorities.

How quickly will data be restored over the wire?

This is determined mainly by the customer's bandwidth. Given that the data is stored on disk, the time and effort needed to locate and access the data is negligible.

Can data be restored to a different location, e.g., to a DR site?

Yes, the restore data can be redirected as desired.

Can we perform a test re-build of the gateway and data restore?

Yes, this can be included in your service offering.