

Whitepaper – Laptop Backup for Remote Workforce

Whitepaper

The whitepaper explains the use case, existing solution and Druvaa's approach for on-the-move laptop backup for travelling employees.

Druvaa Software

docs@druvaa.com

WP/100 / 008

11/1/2008

Table of Contents

Introduction.....	2
Remote Laptop Backups	3
Bandwidth.....	3
Network Access.....	3
Security.....	3
Limitations of Existing Solutions.....	4
Server Triggered Backup.....	4
Dependence on Low Latency, High Bandwidth Network.....	4
Druvaa inSync and Data De-duplication	5
Architecture – Client Triggered Secure Backups	5
Data de-duplication	5
Druvaa SendUnique –Data De-duplication at Source	6
How SendUnique Works	6
Druvaa inSync – Ideal for Remote Backups.....	7
About Druvaa.....	7

Introduction

About 200 million employees work remotely, i.e. they are not at their desk while accessing emails, sending work updates or editing financial sheets and about 70% of this working force never plans a backup before starting or during the travel.

With over 600,000 notebooks lost on US airports, this whitepaper discusses the key concerns in remote-backup (like bandwidth and network access) and the shortcomings in existing solutions which make employees not do their backups.

Towards the end, the whitepaper discusses in details how Druvaa inSync with its client triggered backup architecture and unique data de-duplication approach, makes backup almost invisible while in office or on the move.

Remote Laptop Backups

Some of the key requirements for remote or remote laptop backup are –

1. Availability of sufficient bandwidth
2. Network access to backup server
3. Security

Bandwidth

Statistics show that on an average a business PC has about 8GB of important corporate data. Almost 80% of this data is usually in form of archived emails. The rate of addition/change of data is about 1% but the actual differential change almost doubles to about 2% because of the email archival formats used by most of the email clients like Microsoft Outlook which make a whole bunch of post-processing and index changes on archived data.

Transferring this differential data (160 MB) over a WAN connection can be a problem especially when the user wants to spend that limited time accessing and answering the new emails.

Network Access

While traveling, the users often cannot access enterprise LAN or VPN, which restricts their access to organization's secure resources. While working over the WAN the user's PC does not even have a static (publically visible) IP address. This makes it impossible for the backup server to contact the user's PC and fire a backup.

Security

Working on the WAN, un-encrypted data backup/restore can expose the corporate information making it vulnerable to eavesdropping or stealing.

Limitations of Existing Solutions

There are two major design limitations in most of the existing solutions inherited from the tape-backup legacy

1. Server triggered backup
2. Dependence of low-latency, high bandwidth network

Server Triggered Backup

Earlier when mobility was not an option, network backups used to be driven by a central backup server. The legacy still continues and even today most network based PC backup systems are still server triggered i.e. the backup server initiates the backup and restore requests. The architecture imposes three limitations –

1. **Security** – When the user is traveling, the server initiates and sends network requests out-side the corporate network. Unlike the web or email server, this is a special case and needs more attention.
2. **Access to the user's PC** – The PC must be visible to the server on a published IP address. This becomes a problem when the user is traveling and connected through WAN/Internet.
3. **Solution scalability** – The majority work is performed by the client and as the enterprise size grows the server scalability becomes a bottleneck.

Dependence on Low Latency, High Bandwidth Network

Thanks to the tape-backup legacy, most network backup systems today use same old R-Sync style checksum algorithms for incremental backups. And because of large no. of network interactions required in these algorithms, the backup systems works better on low-latency networks or less network turn-around time and faster execution.

Druvaa inSync and Data De-duplication

Druvaa inSync is an automated enterprise laptop backup solution which protects corporate data while in office or on-the-move. It features simple backup, point-in-time restore, and patent-pending de-duplication technology to make backups much faster.

Architecture – Client Triggered Secure Backups

Druvaa inSync architecture has two components –

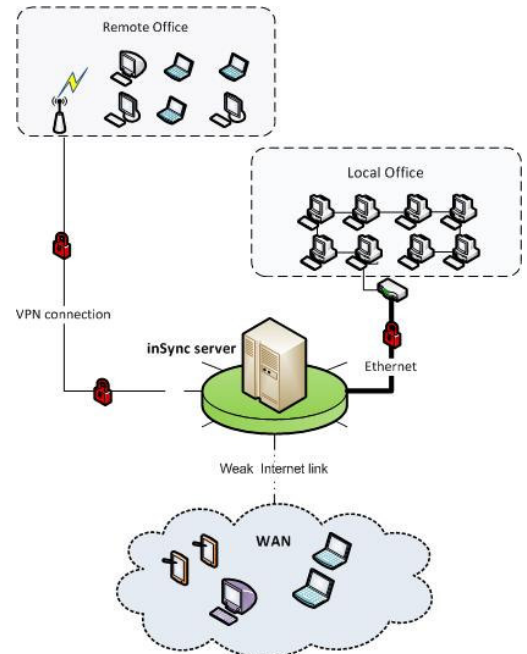
1. inSync client and
2. inSync enterprise server.

Druvaa inSync client is a host based soft driver which gets installed on the user PCs. It is equipped with sufficient backup intelligence to *initiate and accomplish backup*. Configuring a client is a simple 5 step effort and can be completed within minutes of installation. The client triggered backup architecture enables high levels of scalability and security.

The client also has a powerful WAN optimizer to automatically prioritize network and schedule backup bandwidth as a *percentage* of available bandwidth.

Druvaa inSync Enterprise Server is a software service which runs on a dedicated sever and can scale to serve terabytes of enterprise data. The server accepts backup and restore requests on published IP addresses using a *256-byte SSL encrypted channel* and stores it locally on a *256-bit AES encrypted storage*.

The server offers intelligent user and storage capacity management which enable the administrator to create and control centralized backup policies. Advanced reporting offers various alerts, server health and user statistics. This makes the task of managing remote users much simpler.

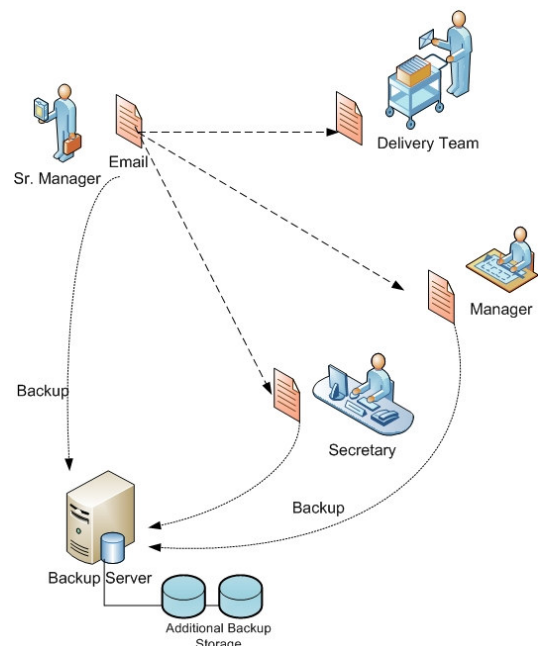


Data de-duplication

Within any enterprise, proliferation and preservation of many versions and copies of emails and documents contributes to the tremendous data growth and **more than 80%** of this PC data is common between users. For data generated by conventional office applications, where many of the file characteristics are very similar, the potential for reduction is very high.

The duplicate content increases bandwidth and storage consumption and thus becomes a bottleneck of PC backups.

The example in the figure (on the right) shows how email follow-ups within team increases the bandwidth and storage by many folds.



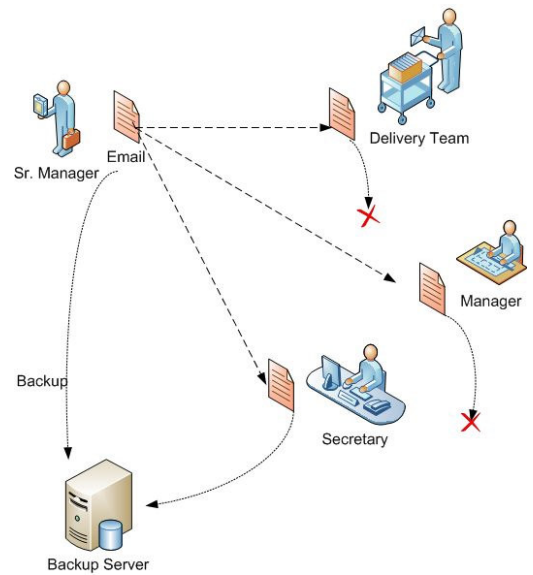
Druvaa SendUnique –Data De-duplication at Source

Druvaa inSync uses patent pending **data de-duplication** technology called **SendUnique** to remove duplicate data at the source (user’s PC) before the actual data backup is initiated. The data updates for a user are checked for duplicate content against existing data (from all the users) backed up at the server.

The server then requests backup for only newly created *unique* content and maintains a reference for common content.

For example (as shown in the figure), If there is a email follow up with a team which created 10 copies of same attachment. Any incremental backup software would pickup those 10 copies from each user’s mail box.

But, with de-duplication technology after the first copy is picked up from a user, all the other copies (from other users) are dropped as duplicates. **This saves up to 10 times backup time, bandwidth and storage.**

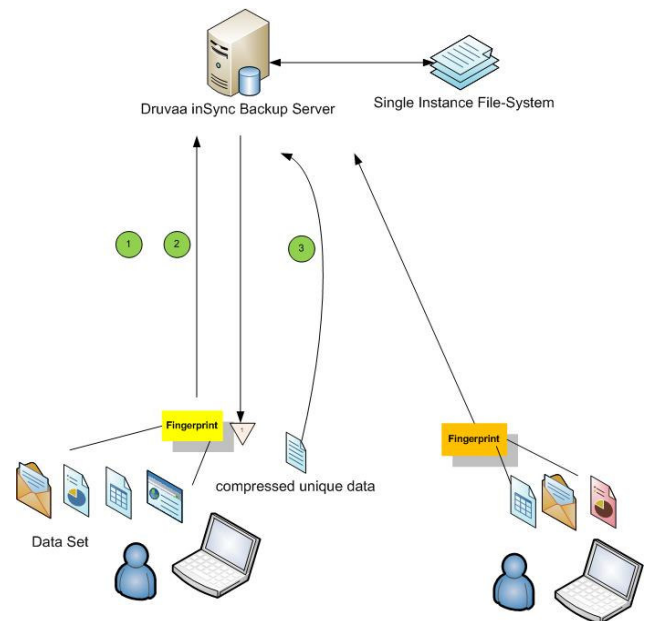


How SendUnique Works

The inSync client continuously monitors file updates on configured folders. Before sending the new data updates to the backup server it prepares a small file fingerprint and sends it to the server.

The inSync server maintains the data backed up so far (from all the clients) in its proprietary Single Instance File System (SIFS). It checks the received fingerprint against the existing backed up data to **check for duplicates at sub-file levels.**

The server checks the received fingerprint against the data backed up so far and responds back with a reference to the part of user’s data which is unique i.e. not backed up by any other user.



All the data and fingerprint changes are recorded in SIFS chronologically. This enables **time-line based from-the-past restore**. In case of loss of data the user can start a web-based restore to choose a calendar date and recover relevant data.

Druvaa inSync – Ideal for Remote Backups

Druvaa inSync is designed keeping “mobility” in mind. To summarize, some of the key product highlights which make inSync ideal for on-the-move or remote backups -

1. **10X Performance** - Druvaa inSync uses the patent pending at-source data de-duplication technology to cut down duplicate data and deliver up to 10X faster backup speeds at 90% reduction in bandwidth and storage.
2. **Client triggered Backups** - Client triggered backups ensure that backup/restore requests are initiated by the client and no requests goes out from the server. This has the following benefits –
 - a. Users can easily do a backup over WAN
 - b. Backup server is secure
 - c. Improved scalability
3. **Secure** - Druvaa inSync uses 256-byte SSL encryption for network communication and 256-bit AES encryption for storage.
4. **WAN Optimization** - The inSync client automatically senses changes to the network and makes changes to backup bandwidth and packet size. On-wire compression further ensures optimal utilization of bandwidth.
5. **Browser Based Restores** - When not on one’s PC, the user can use browser to access the backed up data over HTTPS.
6. **Advanced Reporting** - The administrator can remotely monitor user activity and help him troubleshoot. The inSync server also offers six different reports for extensive reporting.

Some of the other important features –

1. **Usability**
 - a. **Easy**, automated installation and transparent non-intrusive backups.
 - b. **Opportunistic Scheduling** starts sync on availability of bandwidth.
 - c. **Intuitive graphical interface** to manage and monitor backup.
 - d. **Locked/Open File Support** for files like Outlook working files (PST files).
2. **Administration**
 3. **User Profiles** facilitates the administrator to view/guide/control users configuration
 4. **Manage storage capacity** and user quota
 5. **Live server health** and user backup statistics.
 6. **Configurable trigger based reporting** enables queries for relevant information
 7. **Email notifications** for detailed reports

About Druvaa

Druvaa provides enterprise class consultancy and solutions for data availability and business continuity. Information about Druvaa can be obtained from www.druvaa.com