Backing Up Data in the Private Cloud

Meeting the Challenges of Remote Data Protection: Requirements and Best Practices

A Whitepaper
by Stefan Utzinger, NovaStor CEO (March 2011)

Table of Contents

EXECUTIVE SUMMARY

Remote offices as well as mobile and single corporate workstations are often under protected despite the fact that they contain business critical data. According to Gartner, 38% of all corporate data is located on workstations and nowhere else. However, only 35% of companies surveyed said they had implemented a comprehensive workstation data protection solution.[1]

The following paper will describe some of the common challenges associated with protecting data on laptops, home and remote offices. We will portray proven solutions to the challenges of protecting distributed business data by establishing a private cloud / enterprise cloud. Exemplary IT scenarios serve to highlight everyday challenges and depict what strategies have proven to offer successful solutions.

In this whitepaper, readers will learn which best practices can ensure business continuity throughout an organization with a distributed IT infrastructure, without requiring extensive engagement of IT staff.

[1] Gartner 2010

INTRODUCTION: THE CHALLENGE OF PROTECTING DISTRIBUTED DATA

Today's companies commonly have remote offices, employees who work from home, and/or employees who travel often to visit customers. The data that these employees create is unique and of great value to the company. However, protecting the data from loss requires unique data protection strategies that differ from the standard data protection measures employed in the headquarters.

Most companies have a reliable solution in place when it comes to their server infrastructure, but fail to realize that over a third of all critical data is not transferred from workstations to servers and therefore remains unprotected.

When distributed data needs to be gathered with a central solution and protected at a central location, problems range from software deployment to implementing and controlling corporate data protection policies.

Challenges of remote data protection:

- If left alone, remote workers and offices will implement individual backup solutions that endanger data availability and will most likely not comply with corporate policies and security standards or they will not implement a solution at all.
- Data must be transferred from remote locations to the headquarters to prevent data loss in the event of a local disaster
- Data that is transferred via the internet must be protected from unauthorized access
- Remote workers must not rely on assistance of the central IT department for data restore
- Large data loads such as complete applications cannot be recovered via an internet connection
- Bandwidth restrictions can slow data transfer

As the above collection of challenges shows, remote data protection is unlike any other data protection scenario. It requires enabling remote workers to handle all data availability issues by themselves, while at the same time enabling central IT administrators to manage the backup cloud, interfering by remote access on single installations if necessary.

This particular set of requirements can hardly be handled by strategies and solutions developed for single workstation or local network protection. Protecting distributed data requires a specific approach. Based on experience with remote data protection projects, IT specialists have developed a set of strategies that have proven successful in real life and are therefore recommended as best practices.

BEST PRACTICES FOR REMOTE AND MOBILE OFFICE BACKUP

Data protection measures for mobile workplaces and remote offices aim to ensure productivity by keeping data and applications available and protecting business data in the corporate data center.

The major challenge of remote data protection is realizing a solution that requires little administrative effort from the IT department. Additionally, a solution needs to enable the corporate headquarters as well as the staff at remote locations to backup and restore data quickly at an easy-to-use interface.

To meet the challenges of remote office backup, the following best practices have been developed.

Combine local imaging and offsite file backup to ensure data availability
Combining local and offsite backup lowers risk, and improves overall **business continuity**. The reasons for the strategy may sound obvious, but the benefits of this strategy are manifold.

- Protecting remote data offsite in the central data center protects important business data from loss due to local disaster and enables main office to restore and access the data anytime.
- Offsite backup via an online connection is preferred to shipping storage media, which has more risks, takes more time and causes higher costs than online data transfer.
- One of the greatest threats to the business continuity of an organization is data loss from a complete system crash or major physical disaster. While files need to be backed up in the central data center, huge data loads such as systems images or applications can be stored locally. Local disaster recovery images of the complete system dramatically reduce the amount of time it takes to get a remote system up after a total failure.
- Mobile and remote workplaces hold private as well as business data. The private data, often large film and photo files, requires a lot of storage space. Optimally, it should automatically be excluded from corporate protection measures. Providing users with the option to protect the private data themselves on a local storage device instead of the corporate data center decreases the corporate need for storage space.

Local installation, but central administration reduces risks and costs
While each remote or mobile workplace needs to be equipped with the backup software, the backup **management** and **monitoring** should be conducted by IT administrators at the main office.

Implementing a backup solution that allows all local and offsite backup policies to be centrally managed from a central location prevents IT staff from having to travel onsite to remote offices to solve problems and allows remote employees to focus on their primary jobs.

Central IT administrators must be able to

- View and monitor the status of all distributed installations from a central console
- Control backup success, re-run failed backup jobs and contact local staff, if necessary
- Implement corporate policies such as backup schedules, selecting and excluding data from local or offsite backups, etc.
- Create users and user groups that correspond with the relevance of user data for the company, e.g. more frequent backups of data produced by management than by assistants
- Distribute software updates
- Access the local installations via a remote connection to solve potential user problems, without having to travel to the remote location

Professional Client / Server architecture for security, scalability and efficiency
Companies should choose a professional backup solution for providing data protection in a private cloud or enterprise cloud. These solutions are designed as client / server architectures. The client requirements have already been discussed above. The server side of the architecture defines the infrastructure behind the user interface from bandwidth requirement to storage server.

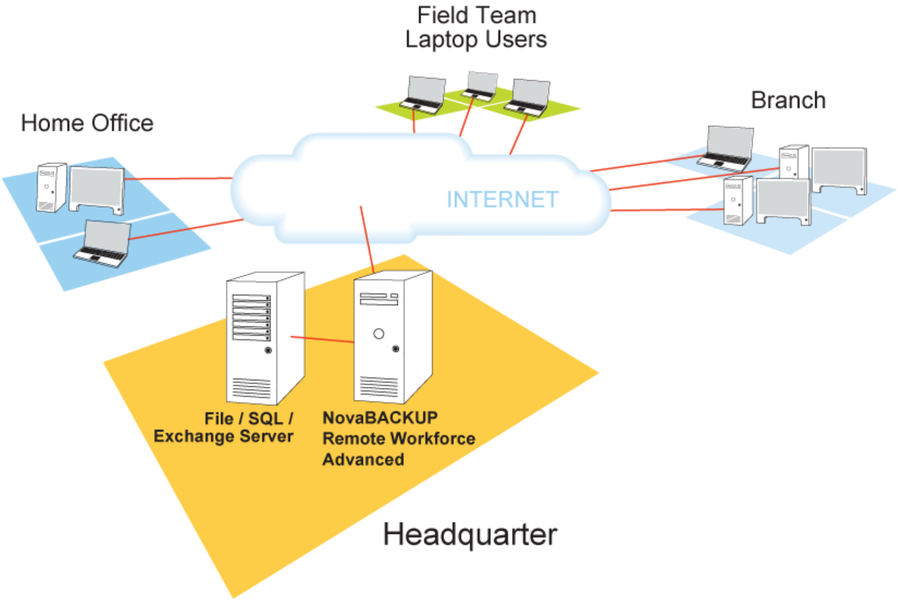
Several measures should be applied on the server side to ensure **low workload** for the administration, **high security** and an optimal **return on the investment**.

- To prevent unauthorized access, such as man-in-the-middle-attacks, data must be encrypted on the client and only be decrypted when back on the client for restore. The use of standard encryption algorithms such as Advanced Encryption Standard (AES) is highly recommended.
- Bandwidth and storage space are the main resources required for offsite backup. Administrators should be able to efficiently use and manage these resources, e.g. by bandwidth throttling, using incremental / differential backup procedures or limiting storage space per user or user group.
- As user numbers might grow, a solution should be able to scale without causing costs and huge work load for each new user.
- Initial implementation and continuous updates
- Choosing backup software that requires minimal end user interaction reduces the risk of human error and improves reliability.
- Client / server solutions provide the user interface as well as the service infrastructure. If local and online backup are covered in the user interface as well client / server solutions provide a single solution that fulfills all requirements and thus reduces the number of applications to be administered.

Choose a reputable technology partner with high quality support

Features alone do not account for a viable solution. Ease-of-use of the interfaces, but also the all over business strategy and the level of support offered, strongly contribute to the long term success of a solution.

- The market is flooded with new backup technologies. Make sure you choose a vendor that has sizeable reference accounts and provides qualified technical support, preferably from the same region.
- Check solutions for awards from independent IT experts. Ease-of-use of the user interface (client) is an important criterion, as simple handling reduces probability of user errors and requests for IT support.
- Last but not least, companies should not focus on software alone, but also on the provider. Buying a license from an anonymous online shop, will most likely cause massive problems when individual adaptions or any type of consultation is needed.


Field Team
Laptop Users
Home Office
Branch
INTERNET
File / SQL / Exchange Server
NovaBACKUP Remote Workforce Advanced
Headquarter

This diagram displays an exemplary architecture with a Private Cloud / Enterprise Cloud .

CHALLENGES & SOLUTIONS: THREE USE CASES

Three use cases from real life scenarios depict what situations lead companies to implementing a specific remote backup strategy. The solutions show the relevance of combining local and offsite backup as well as the importance of central management and remote access functionality.

Scenario 1 – Desktop workstation protection

Challenge
A large manufacturing company has 2,000 corporate workstations without a reliable backup solution. Currently, all employees are responsible for either backing up their own machines or making sure that their data is saved to a networked drive that is regularly being backed up.

The company faces the following threats to their data availability:

- Employees forget to save their data to the network drives
- Data loss incidents are becoming more common
- Successful recoveries are becoming more rare
- Recoveries require extensive time from an IT resource

Solution
By silent install, all desktop workstations to be protected are equipped with the backup client of a remote backup solution. From a central management console, the administrator creates and automates backup jobs for individual machines or custom groups.

Once the installation is completed, the administrator easily monitors all clients from the central management console. When necessary, the administrator can easily drill down to an individual backup job and view detailed logs to determine the cause of any failures. After providing all employees with a brief 30-minute training session, most of them find it easy to recover data on their own.

Core Benefits:

- Fast and easy implementation and deployment by silent install
- central management sharply increases the amount of successful data recoveries
- implementation of corporate protection policy decreases the data loss incidents
- Intuitive restore interface can easily be handled by non-technical users
- Reduced workload for data recovery leaves IT employees more time to focus on productive tasks

Scenario 2 – Corporate laptop protection

Challenge
A large distribution company has 1,000 drivers who distribute their products to local businesses on a daily basis. Each driver has a company laptop that they use to process orders, record inventory, and receive updates from the central office while they are in the field.

The company faces the following threats to their data availability:

- Several drivers damage their laptops in the field and lose data.
- Lack of a comprehensive backup leaves lost data unrecoverable.
- Manually reconstructing data and bringing systems up to date causes overtime costs
- Expensive data recovery methods cause further costs of several 1,000 USD

Solution
With the support of a dedicated vendor, the administrator installs and deploys the solution in under a week. An easy-to-use central management console allows the scheduling offsite backup jobs to meet corporate data availability policies put in place by management. Backups of all 1,000 laptops can be monitored, managed and, if necessary, repeated from one central interface.

In a 30-minutes-webinar, all drivers are also trained on how to use the backup client to perform local backups and restores on their own. The administrator configures local backup jobs for all of the laptops that include key inventory and order data that changes on a daily basis. This job can now be performed by the driver with one click of a mouse at the end of each shift so that he maintains daily backups on a local device in case he needs to quickly restore data even without an Internet connection.

Core Benefits:

- Critical information is protected offsite in the central storage repository
- Backup jobs are configured and carefully monitored by trained IT staff.
- End users can easily perform backups to any local device
- Restore online from central server or offline from local device for high data availability

Scenario 3 – Remote office protection

Challenge
A mid-sized bank has five regional offices and each office is currently responsible for managing its own backups. Regulations require that certain files are backed up and stored offsite. Each office is accomplishing this by charging the branch manager with performing a nightly backup to a tape and then taking the tape to a safe deposit box at another bank each morning.

Threats to data availability and securtiy

- Reconstructing lost data requires costly involvement of IT specialists
- Downtime exceeds acceptable duration
- Transfer of physical storage device (tape) entails danger of theft, loss or damage

Solution
After installing and configuring the storage server on a central storage device in a private cloud, the client backup software is installed on all workstations and servers that are going to be protected at each branch. The administrator creates and automates local and offsite backup jobs.

Now, all local and offsite backups take place without any intervention from the staff at each branch. The branch managers no longer have to worry about performing backups, which frees them up for other, more productive tasks. If a restore needs to be performed, it can either be done remotely by an administrator at the main branch or by the end users in each branch.

Core Benefits:

- Administrator schedules and monitor all backup jobs
- Administrator applies users to individual machines or custom groups
- Remote access on file level allows administrator to identify and solve problems
- Seed backups of large servers on a local device can be uploaded directly to the storage server at the main datacenter, avoiding high bandwidth usage and the long backup window required if this were to be done over the WAN.
- After initial backup only files that have changed will be backed up, reducing backup windows
- Ease-of-use allows a single administrator to manage data protection at all locations
- Once local storage is attached, data protection requires no interaction of office staff at remote locations

CONCLUSION

The business impact of data loss on remote machines can be devastating. Many companies struggle to protect data on their distributed infrastructures using traditional backup strategies, which are dangerously inadequate and inefficient. As more business critical data is generated away from company headquarters, businesses with remote branches and mobile employees are increasingly in need of a way to ensure that their entire infrastructure is protected from threats to data availability.

While there are many challenges associated with accomplishing this goal, companies interested in a comprehensive, reliable remote office backup solution can benefit by following the best practices outlined in this document.

Identifying an appropriate solution tailored to the specific challenges of remote office data protection, such as NovaBACKUP Remote Workforce, is the central key to a successful strategy. Combining local and offsite backup with a solid client-server architecture lets companies exploit the flexibility of professional solutions to map individual needs.

ABOUT NOVASTOR

NovaStor is a leading international provider of software solutions for data protection and availability. NovaStor provides software, SaaS solutions and services for local and online backup, restore and retention of business-critical data.
Clients include home, mobile, and SMB users, service providers as well as international corporations. NovaStor's cost-effective solutions are platform- and hardware-independent and ensure that optimal technological and economical use is gained from the customer's existing and future IT environment. NovaStor is headquartered in Switzerland (Zug), has offices in Germany (Hamburg) and the USA (CA, Agoura Hills), and is represented in numerous other countries through partnerships.