IBM Tivoli Storage Manager and Front-safe TSM Portal

For business-ready cloud infrastructures

Table of Contents

Abstract

As CEOs and CIOs increasingly consider private and public cloud computing implementations, IT service providers need to ensure that their solutions are ready for use in such environments. IBM Tivoli Storage Manager and Front-safe TSM Portal management software are an ideal combination on which to build business-ready cloud infrastructures. This paper describes how these offerings fit together to deliver an optimal cloud backup service.

Introduction

Cloud computing opens up tremendous revenue-generating opportunities for service providers. The ability to leverage shared infrastructures to deliver services to many customers can produce significant economies of scale and, thereby, enhanced profitability.

However, the breadth of service requirements from different customers can result in data centre solutions and administration becoming increasingly complex. The complexity can itself introduce inflexibility and inefficiencies which, in turn, lead to a higher total cost of ownership (TCO). However, if administration can be simplified via dynamic provisioning and self-service portals, and new technologies such as virtualisation and service automation can be applied, then the ideal cost balance can be achieved.

The elements outlined above are the foundation of cloud computing solutions. The combination of the Front-safe TSM management portal and IBM Tivoli Storage Manager as shown in figure 1, on the following page, offers the above-mentioned capabilities within a cloud backup and recovery solution.

IBM Tivoli Storage Manager provides flexible levels of data protection, and can meet a variety of Recovery Time Objectives, thereby supporting multiple levels of service from within a single service infrastructure. More importantly, Tivoli Storage Manager provides a highly scalable environment that can be configured to segregate data by client, enabling cloud providers to assure their clients that on-site and off-site backup media will not get into the hands of other users, even in a disaster recovery (DR) scenario.

The "object-based" data management techniques used by Tivoli Storage Manager also virtualise the physical attributes of the storage devices that it uses, enabling these to be shared across the whole environment.
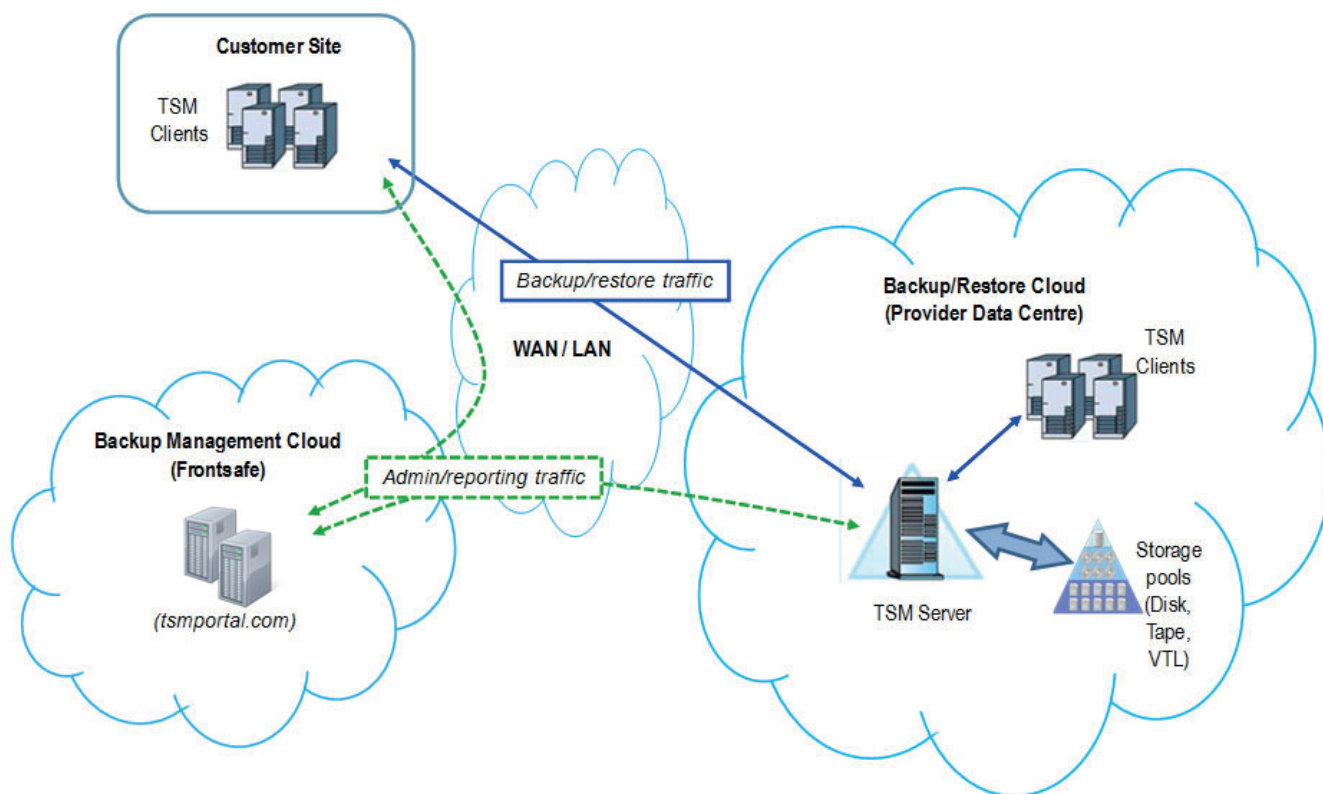
Figure 1. TSMPORTAL combines with TSM to provide a Cloud Backup and Recovery service

The Front-safe TSM portal provides a self-service front-end to the Tivoli backup solution. Administrators, or even resellers and customers, can dynamically request and acquire backup resources which are provisioned from Tivoli solutions running on a public or private cloud. Resource usage is reported by the portal, enabling integrated usage-based billing to resellers and/or end users.

The combination of IBM Tivoli Storage Manager and the Front-safe TSM portal enables IT service providers to offer a security-rich, cost-effective, cloud-based data protection service to their customers with the required flexibility and ease of deployment to quickly grow their portfolio of offerings.

Overview of IBM Tivoli Storage Manager

IBM Tivoli Storage Manager protects your data from hardware failures, errors, and unforeseen disasters by storing backup copies on offline and off-site storage. It can also create archives of files from the same "client computers", enabling its infrastructure to be shared for both purposes.

A single Tivoli environment can scale to protect thousands of computers running more than a dozen operating systems, ranging from mobile computers to mainframes that are connected via the Internet, WANs, LANs, or SANs. It offers centralized, Web-based administration, intelligent data management techniques, and comprehensive policy-based automation that all work together to minimize administration costs and the impact of backup on both computers and networks. Each of these capabilities is key to delivering an effective, 'light touch' cloud offering.

The Tivoli software family includes optional modules to allow business-critical applications that must run 24x365 to perform on-line backups that exploit the centralized data protection in Tivoli Storage Manager with no interruption to their service. Other optional software extensions allow SAN-connected computers to use the SAN for data movement, and provide hierarchical storage management to automatically move unused data files from online disk storage to offline tape storage. Tivoli Storage Manager also offers an integrated disaster planning capability to protect its own infrastructure against failure and data loss.
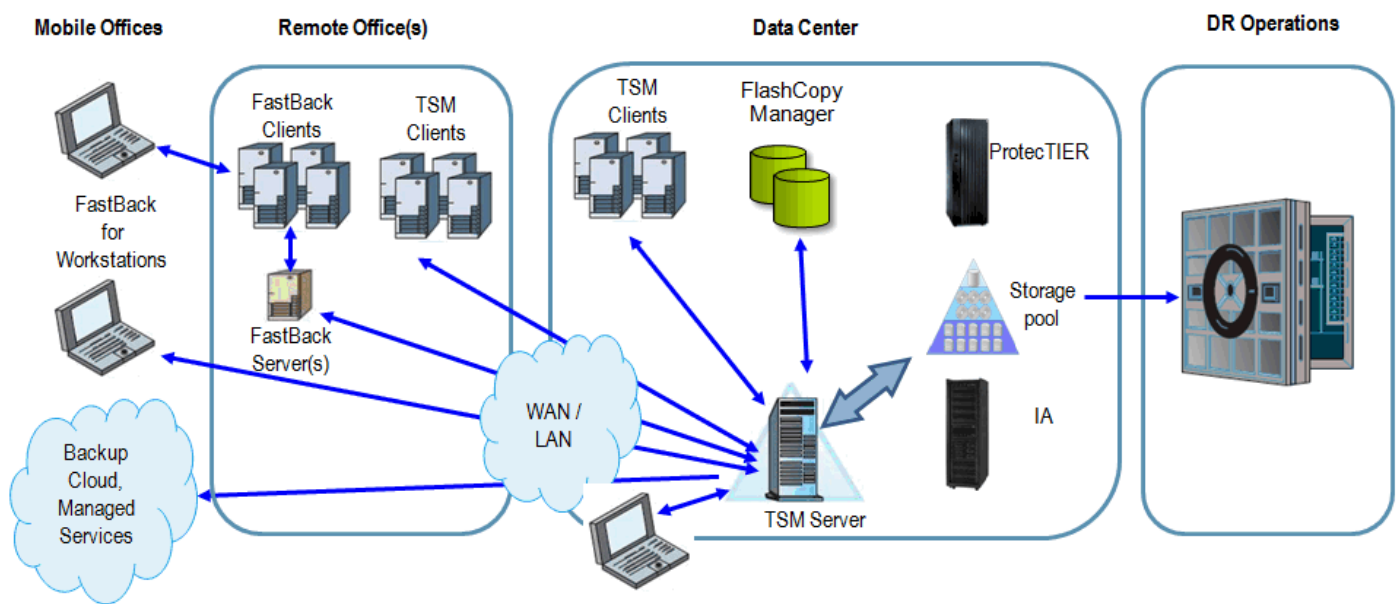
Figure 2. IBM Tivoli Storage Manager is the core component of an enterprise-wide data protection and unified recovery management system

Leverage next-generation data storage and recovery management capabilities

Tivoli Storage Manager is a family of integrated modules that work together to help businesses deliver a customized solution to manage and control their own specific data protection and retention needs from a single point of control. This advanced, highly scalable solution helps increase the efficiency of your IT operations and helps cut your storage management costs. It provides policy-based automation and monitoring of the following capabilities:

- Backup and recovery
- Online database and application protection
- Protection of virtual server environments
- Disaster recovery
- Data reduction
- Bare-metal recovery
- Space management
- Archiving and retrieval.

Tivoli Storage Manager scans the data that it is about to back up (source side) or has already backed up (target side) to identify common chunks within the data files. Only one instance is stored for each common chunk. The Tivoli software uses data deduplication to help conserve network bandwidth by not moving duplicate files or portions of a file over the network during backup operations, meaning that backups can be performed faster and the amount of space required to store backups may grow at a slower rate.

This is beneficial to both the cloud service provider (as it reduces storage hardware needs) and the end-customer (as it reduces bandwidth needs). With these diverse features, and the associated benefits that can be derived from having a shared hardware infrastructure with the ability to segregate data from different sources or with different retention criteria, Tivoli Storage Manager is the ideal basis of a cloud data protection service.

Tivoli Storage Manager also has a number of specific capabilities that optimise the use of network and storage resources. These features help minimise the setup cost for any cloud service provider while also making the service more viable for the end customer; for instance, by minimizing the network bandwidth required to send their data to the service. With Tivoli Storage Manager, you can:

- Reduce the amount of data that needs to be sent to the service by using the software's progressive incremental backup, data deduplication or compression features.
- Efficiently manage multi-location backups by exploiting the software's in-built policy-based data retention techniques.
- Define policies to automatically migrate data between different types of backup and archive storage as it ages or as the SLAs governing its retrieval change.
- Generate daily-updated disaster recovery plans to protect against failures within the service infrastructure.
- Implement data retention policy changes retroactively in the event that your end-customers' requirements change.
- Automatically distribute upgrades to client agents on the most popular platforms, making your service offering easier to support.

Tivoli Storage Manager is the core component of an enterprise-wide data protection and recovery management solution set. It integrates seamlessly with Tivoli Storage Manager FastBack, which provides enhanced data protection and recovery of critical Microsoft Windows and Linux® servers in remote offices and in the data center. Automatic and continuous protection for desktop and laptop systems is provided by Tivoli Storage Manager FastBack for Workstations, and Tivoli Storage FlashCopy® Manager enables hardware-assisted, application-aware snapshots. These optional products offer the potential to increase the level of service in a number of key situations. For instance, where a customer may need very fast recovery of a large Windows server but has limited bandwidth network connectivity to the backup cloud, a Tivoli Storage Manager FastBack server could be deployed to enable fast local recovery and also manage data transfers to the backup cloud for off-site protection.

Why you should base your cloud offering on IBM Tivoli Storage Manager

Reduce volume of data with leading-edge data reduction features
Tivoli Storage Manager provides a number of leading-edge capabilities that reduce the amount of data that needs to be retained within the backup cloud, including:

- Progressive incremental backups with an incremental-forever backup method that eliminates redundant periodic full backups. Using this method, Tivoli Storage Manager performs a single full backup of your files and then backs up only those files which were created or changed since the previous full or incremental backup point. When doing this it retains the ability to perform a full recovery to any of your backup points and will need to restore only those files that were on your system at that time (without needing to restore a full backup, then incremental 1, incremental 2, and so on). This significantly reduces data storage and network needs.
- Built-in data deduplication that eliminates redundant files and subfile "chunks". Source-side data deduplication reduces the amount of data sent from client systems to the Tivoli Storage Manager Server. Target-side data deduplication eliminates redundant data "chunks" that have been stored multiple times. In combination, these advanced features reduce both bandwidth and storage requirements.
- Seamless integration with popular virtual tape library systems, such as the IBM ProtecTIER Deduplication Solutions, that employ in-line data deduplication for long-term retention of large data sets.

Data deduplication is defined as the elimination of redundant files and subfiles, which may also be referred to as chunks, blocks, or extents. Tivoli Storage Manager scans the data that it is about to back up (source side) or has already backed up (target side) to identify common chunks within the data files. Only one instance is stored for each common chunk.

The Tivoli software uses data deduplication to help conserve network bandwidth by not moving duplicate files or portions of a file over the network during backup operations, meaning that backups can be performed faster and the amount of space required to store backups may grow at a slower rate. This is beneficial to both the cloud service provider (as it reduces storage hardware needs) and the end-customer (as it reduces bandwidth needs).

Increase cost efficiency with hierarchical storage
In most backup and archive environments, managed data is trapped on the media to which it was originally backed up. Tivoli Storage Manager uses an object-based data storage technique to virtualise its data storage, and can thereby exploit a hierarchy of storage hardware. It can use automated policies to migrate data to its most appropriate media type, based on data value and on requirements around access and retention.

Tivoli Storage Manager automatically manages the movement of the data onto any new storage technology that is introduced into the hierarchy, simplifying the removal of old technology from the data centre.

In addition to this storage hierarchy, the open application programming interface (API) of Tivoli Storage Manager provides the ability to seamlessly manage many types of data. As soon as data is in the hierarchy, it can easily be moved from one storage device to another. Consequently, Tivoli Storage Manager can be used for:

• Backup — back up and maintain numerous file versions to enable point-in-time recovery in the event of production storage device failure, data errors or accidental file deletions.
• Archive — archive files to the hierarchy of storage for a specified amount of time, after which they automatically expire, based on policies set for each data type.
• Space management — TSM for Space Management identifies and moves less-frequently accessed and inactive files to a lower level in the hierarchy of storage. Tivoli Storage Manager HSM for Windows can automatically move lesser-used Windows files without disrupting your end users.
• Data retention enforcement — IBM System Storage Archive Manager (a "compliance mode" of TSM) prevents stored data from being changed or deleted prior to expiration dates or while a "hold" is placed on the content, helping organisations address legal and regulatory requirements.

The above features mean that service providers can increase profitability, because their offering has the agility to exploit newer, more cost-effective storage hardware as it emerges.

Enhance data security
Storage administrators must ensure that data is backed up and secure, regardless of location, and that purposely-erased data is irrecoverable. To help meet compliance requirements while maintaining IT staff productivity, Tivoli Storage Manager can generate, encrypt, store and manage encryption keys for its client machines. Furthermore, Tivoli Storage Manager can compress and encrypt data that is being moved into its hierarchy of storage. Enhanced security features within the software include:

• Automated data security encryption key management to help relieve the burden of manually tracking encryption keys and passwords.
• In-flight 256-bit AES data encryption between client and server using Secure Socket Layer (SSL).
• Ability to leverage tape-drive encryption, to offload encryption from the system to the tape drive for faster backups and restores.
• Shredding of data on disk, or the overwriting of deleted data, helping to prevent future discovery.

These features help the cloud service provider to assure customers that their data can be protected from unauthorised access by third parties.

Increase visibility of the data protection environment
Tivoli Storage Manager provides a standard feature for near-time operational monitoring and historical trend reporting of one or many Tivoli servers. The offering comes with a number of standard reports that can be used as provided or customised for your own specific circumstances/requirements, as well a scheduling feature that enables reports to be created in multiple formats such as HTML, PDF and comma-separated values (CSV). This capability means that the backup service provider can ensure that its Tivoli Storage Manager service is running optimally and delivering the expected levels of service.

Overview of the Front-safe TSM Portal cloud management solution

Preface

Introduction

The Front-safe TSM Portal enables the cloud delivery model for Tivoli Storage Manager. The TSM Portal includes and adds everything needed to distribute a Tivoli Storage Manager environment to remote end customers – either directly or through a network of partners and resellers.

Who this chapter addresses

This chapter addresses both technical and business people who need an understanding of how to bring Tivoli Storage Manager to market as a cloud offering. It aims to give the reader an understanding of the features and benefits of Front-safe TSM Portal.

Basic understanding of TSM Portal benefits and functions

The TSM Portal is a web business portal developed to distribute Tivoli Storage Manager as a cloud service. Data centres can use the TSM Portal to turn their Tivoli Storage Manager infrastructure 180 degrees: from simply protecting internal servers to protecting remote end customer data and bringing to market a whole new business model for backup.

The TSM Portal allows data centres to deliver Tivoli Storage Manager as a cloud offering directly to end customers or even through a network of OEM-branded dealers and partners. The solution includes everything needed for the data centre to deploy this new backup-as-a-service offering to the market, including setting up a channel of dealers and partners, user-friendly reporting, daily support functionality and billing functionality.

The structure behind the portal is as follows:
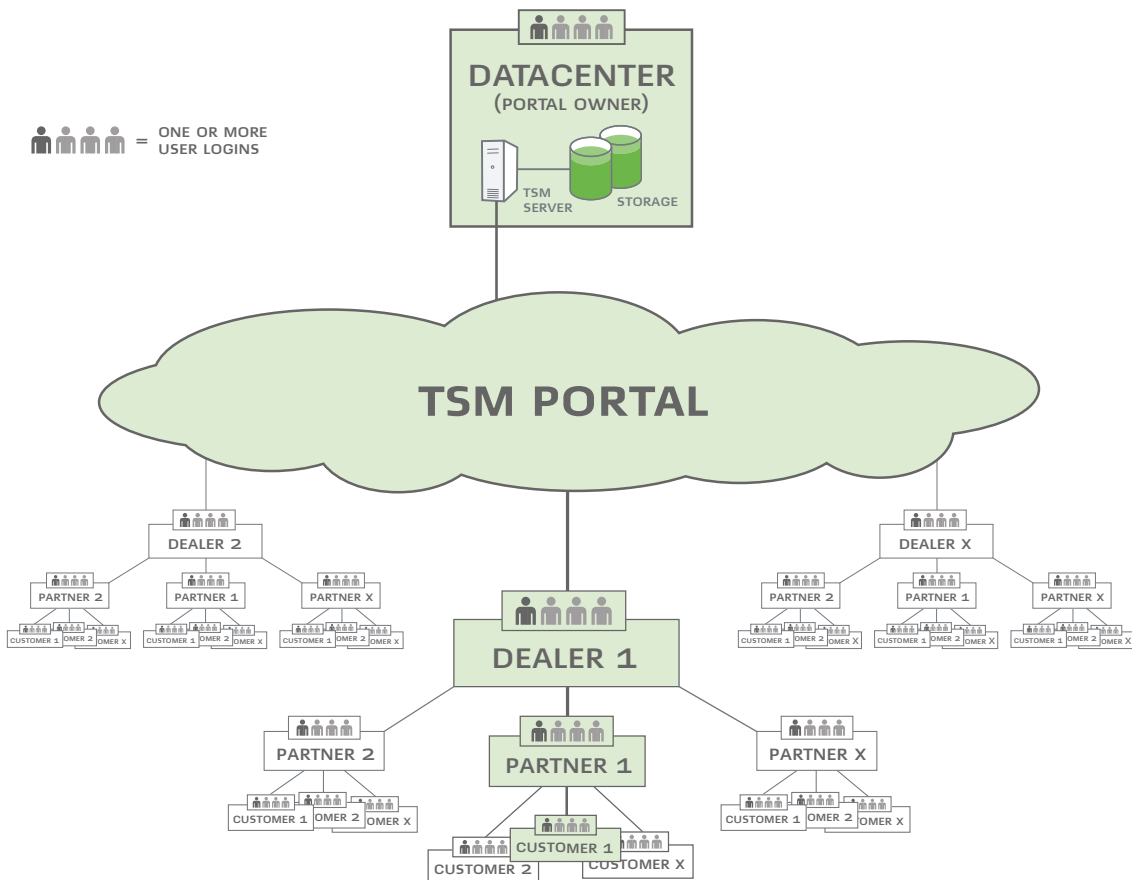
The data centre (Portal Owner) can add one or more Dealers to the portal. Dealers can add one or more Partners, and Partners can add one or more End Customers. At all levels, it is possible to add one or more users with separate logins and different rights depending on their function within an organization. The Portal Owner invoices all the Dealers on a usage basis for everything they add in the solution. Dealers invoice their Partners, and Partners invoice their End Customers. If a Portal Owner only delivers the service to end customers directly, there will be only one Dealer (this will be the Portal Owner itself). Equally, this Dealer will have only one Partner (again, the Portal Owner itself) and all End Customers will be added through this Partner.

This approach enables extreme speed in bringing a cloud-based Tivoli Storage Manager solution to market. It also eliminates complexity from Tivoli Storage Manager on the customer side, making this enterprise-class solution a viable option for small and midsize end customers. Distribution can happen directly or through the end customers preferred IT partners. Dealers, partners and even end customers can handle the activation and installation of new servers and the daily routines around the solution themselves, without involvement from the portal owner.

Access to the TSM portal

Website

Nothing needs to be installed: the TSM Portal is a web portal cloud service that can be accessed by any Tivoli Storage Manager Server worldwide. After signing an agreement on the TSM Portal, the portal owner will receive an administrative user login to the TSM Portal and will be able to log in at **https://tsmportal.com**.

After login, the first task is to connect one or more Tivoli Storage Manager Servers. Each Tivoli Storage Manager Server will communicate metadata with the TSM Portal solution in order to perform the daily reporting, monthly invoicing and other tasks, as illustrated in Figure 1 in the introduction to this paper.

Tivoli Storage Manager Servers

In order for Tivoli Storage Manager Servers to communicate with the TSM Portal, they must be visible from the Internet, either through a public address or through a firewall via NAT to an internal address.

After login, the first task is to connect one or more Tivoli Storage Manager Servers. Each Tivoli Storage Manager Server will communicate metadata with the TSM Portal solution in order to perform the daily reporting, monthly invoicing and other tasks, as illustrated in Figure 1 in the introduction to this paper.

Front-safe TSM Portal administration

The TSM Portal offers a functional, easy–to–understand interface for navigation and task management. The interface is divided into three different areas, with a menu area to the left with quick access to key features of the TSM Portal. In the upper right corner are selectable options for the user who is logged on, and in the middle is a large area with details about the currently selected item.
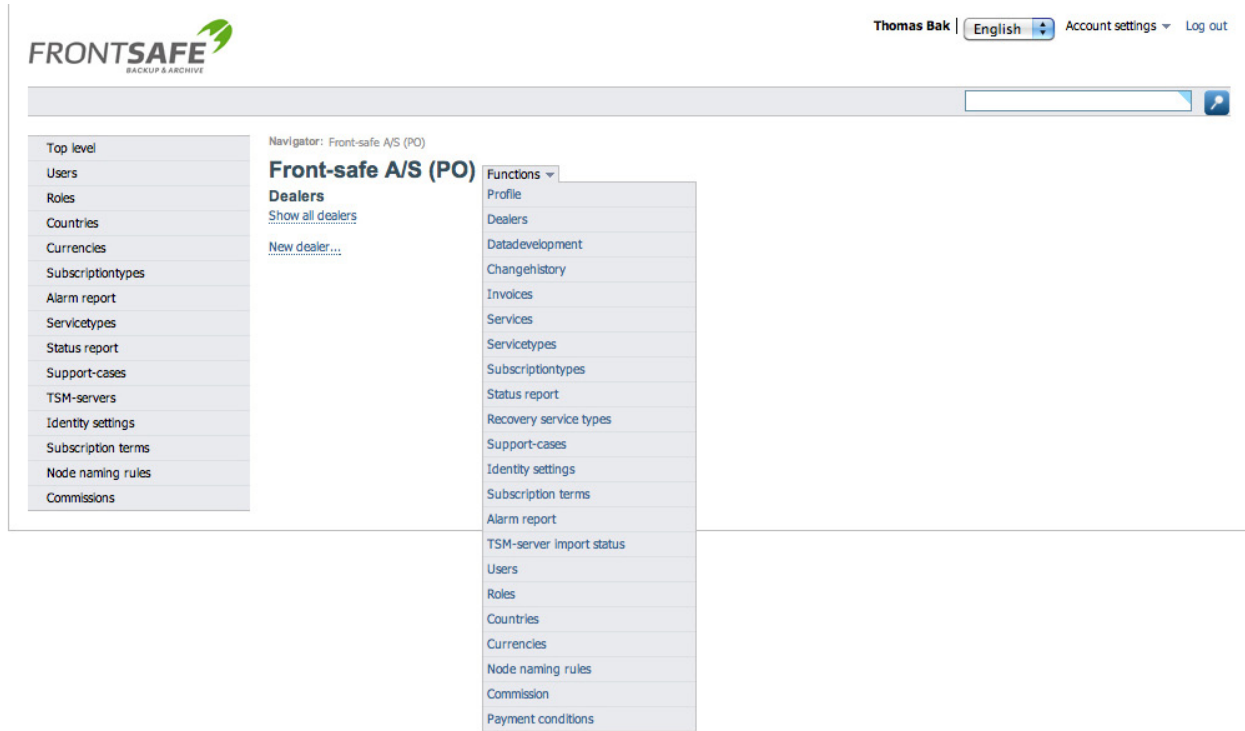
The portal owner, dealers, partners and customers are managed here, along with subscriptions and underlying servers.

The currently selected item is written with enlarged letters in the large detail view, and all available functions are selectable from a dropdown functions menu just to the right of the topic. The functions menu is customized depending on the item selected in the TSM Portal.

To maintain an overview when maneuvering around the TSM portal, the current location is always shown in a navigation line (crumb trail) at the top of the screen, where the different levels are selectable for quick navigation. The 'search' field can be used for rapid navigation to specific information in the portal.

Each user login has the option to select a preferred language. English, German and Danish are currently available.

The TSM portal contains a currency option that enables a portal owner to individually apply the desired currency for each entity, enabling the invoicing of dealers, partners or customers in other countries.

Creating entities

When creating new entities such as a portal owner, dealer, partner and customer, at least one new user login account is added to each entity. This provides the new entity with the ability to access its own structure from this entity and down to all lower levels. For example, a portal owner adds a dealer, who gets a dealer login, and from here the dealer creates and manages underlying partners. Each partner gets a user login to create and manage underlying customers.

By default, the first user to be created for an entity gets administrative rights. This means the first user can decide if other user logins should be added and what roles should be applied to these users.

Users

The TSM Portal comes with a user administration interface. Here, the administrator can add one or more users with separate user logins. This means that the Portal Owner can add more employees with their own login details and with the appropriate rights to the different parts of the TSM Portal. The same user administration interface is accessible for end customers, partners and dealers.

User rights are managed through roles defined by administrative users on each level.

Roles

One or more roles can be defined in the Roles module of the TSM Portal. When the administrator adds more users to the portal, he can associate each user with an appropriate role that will provide access to the appropriate functions. For example, the administrator can create a read-only role, then associate this role with users who should be able to login and view information, but who are not allowed to add, delete or alter anything.

Example of the 'create new role' functionality:
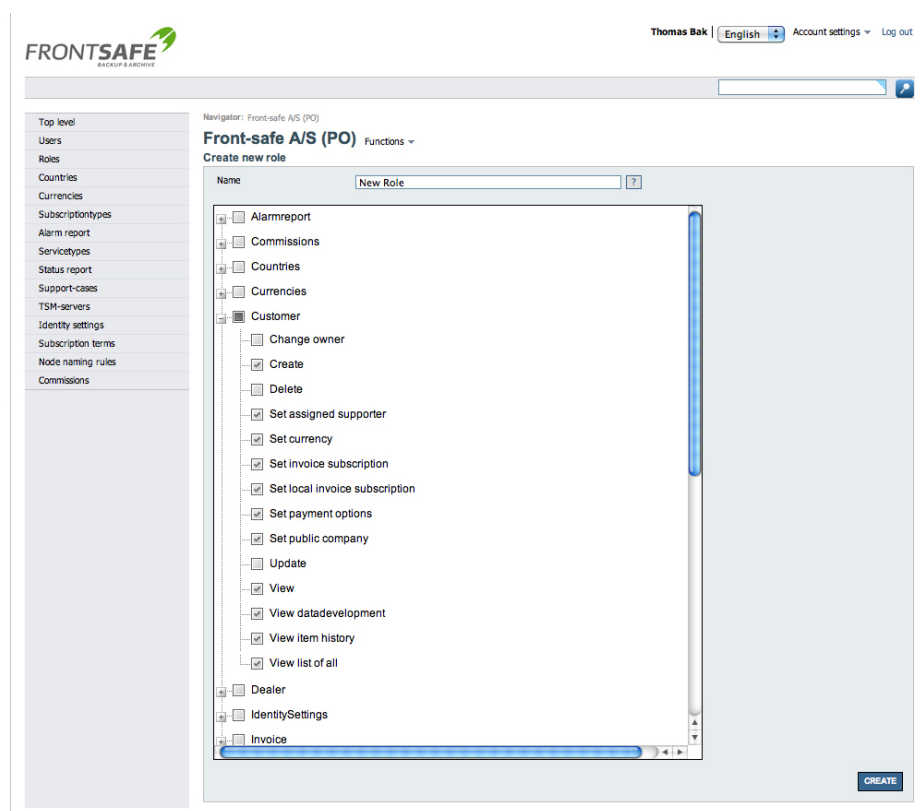
Defining a new role is an easy task in which the administrator ticks the corresponding box for each item to which the role should be granted access.

OEM branding

The TSM Portal will, by default, be branded with the portal owner's name and logo. However, when the portal owner adds a new Dealer to the portal, the portal owner can decide if this dealer will act under the portal owner name and logo, or under the dealer name and brand. This OEM branding option is accessible to the entire TSM Portal hierarchy, which means that new partners can also add their own names and logos. This makes it possible to deliver the Tivoli Storage Manager cloud-based solution to end customers together with the end customers' trusted and preferred IT partner, under this IT Partner's name and brand.

The OEM branding is activated in the 'identity settings' field in the TSM Portal. This is done by adding the dealer or partner support phone and support email, and by uploading the dealer or partner logo. It is also possible to add SMTP mail settings to ensure that all email status reports are sent from the dealer or partner mail domain instead of from the tsmportal.com domain.

Navigator: Front-safe A/S (PO)

Front-safe A/S (PO) Functions ▾
Identity settings

Support settings
Support phone
Support email

UPDATE

Logo settings
Logo   Browse
Current logo:

UPDATE

SMTP-Settings
E-mail to send from
SMTP Server
SMTP Port
SMTP use SSL ☐
SMTP user name
SMTP password

CLEAR UPDATE

Top level
Users
Roles
Countries
Currencies
Subscriptiontypes
Alarm report
Servicetypes
Status report
Support-cases
TSM-servers
Identity settings
Subscription terms
Node naming rules
Commissions

Subscriptions and billing

Portal owners, dealers and partners have access to a Products module within the TSM Portal. Here, products (defined in the TSM Portal as Subscriptiontypes) can be added. Subscriptiontypes are products that define how to invoice the Tivoli Storage Manager cloud-based service.

Multiple products can be added and it is also possible to apply different pricing models to different dealers, partners and customers. When adding a new Subscriptiontype, it is necessary to define name, monthly price, price per GB and per node, and maximum amount of data, among other variables.

Navigator: Front-safe A/S (PO)

Front-safe A/S (PO) Functions ▾
Create new subscriptiontype

Name
Fixed price
GB Included
Price per extra GB
Archive price per GB
NO of nodes - File server
Price per extra node
NO of nodes - Wrk. st.
Price per extra node
NO of nodes DB/Mail
Price per extra node
Description for partner

CREATE

Top level
Users
Roles
Countries
Currencies
Subscriptiontypes
Alarm report
Servicetypes
Status report
Support-cases
TSM-servers
Identity settings
Subscription terms
Node naming rules
Commissions

When the portal owner adds a new dealer, he will associate this dealer with a specific Subscriptiontype that will then define the cost price from portal owner to dealer. This is done by setting an 'invoice basis' on the dealer by choosing the right Subscriptiontype from a dropdown list. The dealer will then define his own products and selling prices. When the dealer adds a new partner, this partner is associated with a Subscriptiontype that defines the cost price from dealer to partner. Finally, the partner will define products with his own selling prices. These are then used to associate end customers and their Subscriptions with the right end customer prices.

An end customer can have one or more Subscriptions. A subscription is a grouping of servers. It is possible to create more than one subscription for each end customer to enable distinction between groups of servers for one end customer. If, for instance, an end customer has several geographically separate locations and the end customer wishes the servers at the various locations to be separate in terms of invoicing and reporting, that will be possible as a result of the subscription structure. Also more subscriptions for one customer allow the partner to charge different groups of servers a different price.

For all entities (portal owner, dealer and partner), monthly CSV files will be available from the TSM Portal. These CSV files will show all billing lines, with all the information needed to create real invoices. Among other information, the CSV file will include both cost prices from the level above the entity and selling prices to the level below the entity. The different entities themselves decide what they want to include in the CSV output by adding and removing items from a checklist. Also, the entity can decide if the CSV file should be sent to one or more email recipients.

Client servers and end customer installation
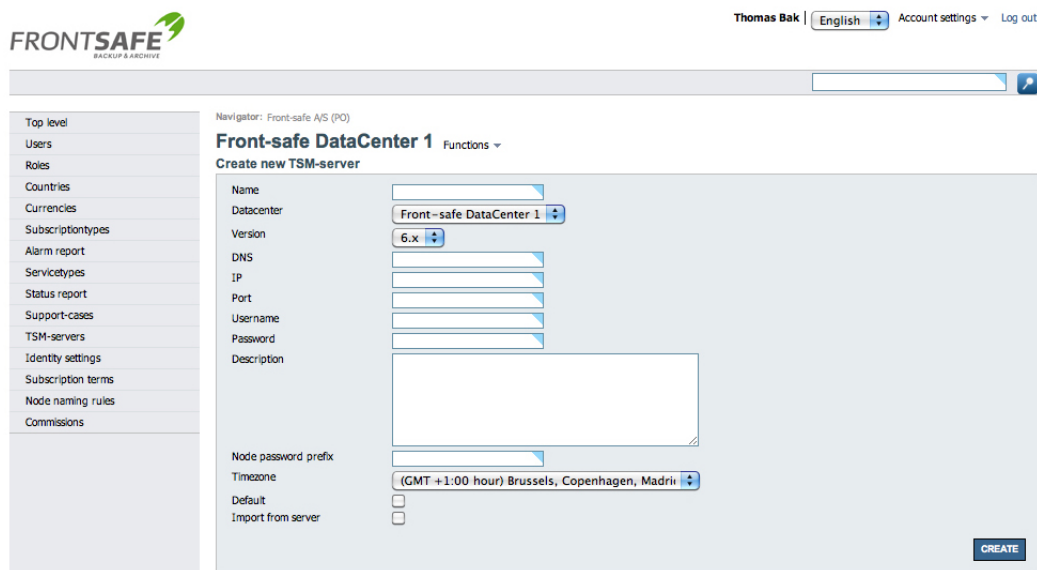
The actual implementation and installation of the Tivoli Storage Manager cloud-based solution at end customer sites includes the following steps:

- The customer details are entered in the TSM Portal, including name, address, contact information and so on.
- At least one Subscription is activated in the TSM Portal, including association with a Subscriptionstype that holds information about the pricing for this customer.
- One or more servers (Tivoli Storage Manager nodes) are activated in the TSM Portal and the TSM Portal will return a server ID (Node ID) and the name of the Tivoli Storage Manager Server where the server is activated.
- A next-next installation of the Tivoli Storage Manager Client on the customer's server is carried out.
- The Server ID and the Tivoli Storage Manager Server name are added to the Client Server option file, and a decision is made on what data should be included in backup.
- A next-next installation of a Scheduler service is performed on the Client Server.
- One or more Schedules (time of daily automatic backup) are added to the server in the TSM Portal

The installation is now complete and the server will be automatically backed up on the decided schedules. The whole installation process typically takes around 15 minutes per server.

Tivoli Storage Manager Servers

Connection between Tivoli Storage Manager servers and the TSM Portal requires a user with administrative privileges (dbuser) on every Tivoli Storage Manager Server. This user needs analyst and domain rights on Tivoli Storage Manager Servers running version 5.5 and earlier. On Tivoli Storage Manager Server version 6, policy authentication is required.

The connection of Tivoli Storage Manager Servers to the portal is now handled from the TSM server administration module of the TSM Portal:

Every Tivoli Storage Manager Server is given a name that eventually reflects the exact role of that specific server. As one Tivoli Storage Manager Server can be dedicated to a specific dealer or partner, the Tivoli Storage Manager Server name might include a reference to them..As each Portal Owner can operate more than one data centre, it is also necessary to define the data centre to which each Tivoli Storage Manager Server belongs. The Tivoli Storage Manager Server's DNS IP address can then be defined, together with the port number for communication.

In order to connect the Tivoli Storage Manager Server with the TSM Portal, the administrative user in the TSM Server is added, including user name and password.

A node password prefix can be chosen, to prefix the login password the first time an end customer's Tivoli Storage Manager client connects to the Tivoli Storage Manager Server. The password used to log in the first time will be the unique node ID with the prefix in front. This password should, of course, be changed after the first connection has been established.

The correct time zone for the Tivoli Storage Manager Server should also be set, to ensure that the daily reports are created and sent to recipients at the right time of the day. Finally, a check is made to verify whether the Tivoli Storage Manager Server is the default Tivoli Storage Manager Server for that data centre. All new clients and/or nodes activated in the TSM Portal will be activated on the default Tivoli Storage Manager Server, unless a dedicated Tivoli Storage Manager Server has been selected for the relevant partner or dealer.

Schedules

- TSM client schedules are defined within the portal management interface. For the schedules to be displayed correctly in the portal, the following naming structure for schedules must be followed:
- BA clients' schedules must start with FILE- ie. FILE-2200-ANYDAY
- TDP for Domino schedules must start with DOMINO- ie. DOMINO-FULL-SATURDAY-2200
- TDP for Exchange schedules must start with EXCHANGE- ie. EXCHANGE-DIFF-WEEKDAY-2300
- TDP for SQL schedules must start with SQL- ie. SQL-LOG-HOURLY
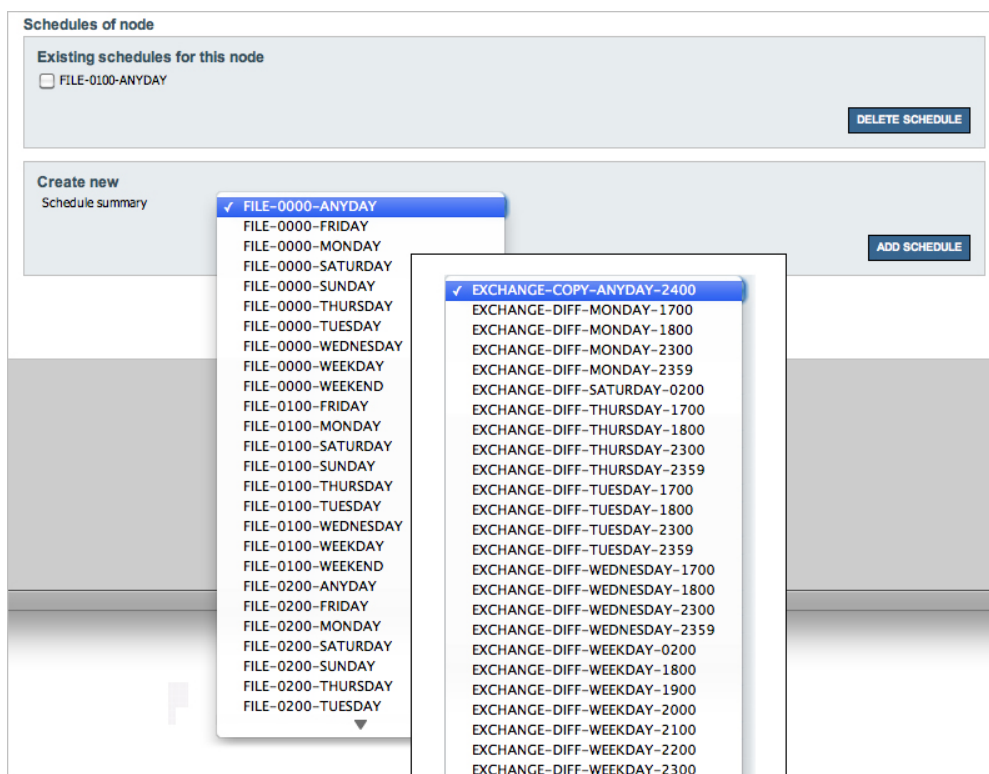
Above are two examples of the naming structure from the Backup-Archive file schedules and the Tivoli Data Protection for Exchange schedules. Schedules starting with the syntax as shown must reside on the Tivoli Storage Manager Server to be imported in the portal. All schedules residing on the Tivoli Storage Manager Servers are of course valid for association with Tivoli Storage Manager clients Those with a different schedule name than mentioned above are not visible from the TSM Portal, but can be used by the portal owner when needed.

Reporting

The TSM Portal provides the portal owner and all other entities with daily, user-friendly reports that hold information about all the backup jobs. Color schemes make it easy to find potential errors in the backup jobs. All reports are generated automatically and can be found and read in the TSM Portal, as well as being sent to one or more email recipients. It is possible to define recipients on all levels in the TSM Portal. This means that a single server report can be sent to the person responsible for only one server, the customer report can be sent to the person responsible for the customer, the partner report including all end customers for that partner can be sent to the partner's support team, the dealer report to the dealer, and so on.

For all entities (nodes, subscriptions, customers, partners, dealers and portal owners) it is also possible to retrieve a report describing the data growth for that specific entity. When retrieving the report, a start and an end date are defined and the report will show a graph of the data amount from beginning to end date.

The following shows part of a daily status mail report on Subscription level (with Front-safe name and logo):

A built-in Alarm system makes the daily support routines effective for people supporting customers, partners and dealers. The Alarm system will show only those nodes that need attention. For each node on the list, it is possible to make notes about what has been done to correct an error. These notes will then make error-handling more effective in the future.

In the Alarm system, it is possible to set differentiated alarm settings depending on the customer and even on the specific user. Among other things, it is possible to define how many times in a row a node may be 'Completed' with 0 MB transferred. This setting allows administrators to effectively discover if critical data on a server has been moved to a share, which is not included in the backup.

Support system
The TSM Portal includes a support system that allows end customers, partners and dealers to add support issues and questions in the Portal. The added issues will then be flagged to the entity above, which can then respond to the added issue or question.

Automatic Restore Control: Add-on option
The Automatic Restore Control option (ARC) allows the portal owner to automate the process of validating the backup data of critical servers in the portfolio. The solution can be distributed to end customers as an add-on solution to backup.

The ARC solution requires a VMware environment next to the Tivoli Storage Manager infrastructure in the data centre. The ARC solution can now be activated as a next-next installation on any server (node) in the TSM Portal. ARC will then initiate an automated restore of the server on a frequent basis (i.e. every month) from TSM backup data onto the VMware environment, including operating system, applications and data.

On top of the restore, it is possible to include queries into file, mail or database data to ensure the integrity of the backup data. The result, including recovery results and recovery time, will then be displayed in a user-friendly report that is automatically sent to one or more email recipients.

The following shows part of an ARC report: The ARC solution can be used as documentation for auditors of company security that random testing and validation of critical backup data has actually taken place, including test results.

The ARC solution can be used as documentation for auditors of company security that random testing and validation of critical backup data has actually taken place, including test results.

For more information

For more information on IBM Tivoli Storage Manager and Front Safe TSM Portal, visit:
http://www.ibm.com/software/ismlibrary?NavCode=1TW10SM45

IBM

Ready for

IBM | Tivoli

software

TIW14121-GBEN-00