TECHNICAL FEATURE BRIEF:
SYMANTEC BACKUP EXEC™ 2012
MULTITENANT, PARTNER-HOSTED CLOUD BACKUPS

Multitenant, Partner-hosted Cloud Backups

Symantec Backup Exec™ 2012 Technical Feature Brief

Who should read this paper

Backup Exec Technical Feature Briefs are designed to introduce Symantec partners to key technologies and technical concepts that are associated with the Backup Exec product family. The information within a Technical Feature Brief is intended to assist partners as they design and implement data protection solutions based on Backup Exec in customer environments.

Technical Feature Briefs are authored and maintained by the Backup Exec Technical Field Enablement team.

Confidence in a connected world. Symantec.

Contents

Introduction

For Managed Services Providers, backup and recovery services continue to represent the top priority. Even a single instance of a Managed Services Provider failing to recover a client's data assets successfully or failing to ensure a client's ability to maintain business continuity in the event of a disaster could result in the following:

- Loss of that customer and associated revenues
- Damage to the Managed Services Provider's reputation

In addition to the critical nature of backup and recovery services, compounding factors such as the explosive rate of data growth, the increase in complexity of business-critical applications, and the move towards cloud computing are compelling Managed Services Providers to modernize the backup and recovery solutions they offer to their clients to ensure they remain competitive in the IT services industry.

Managed Services Providers and Cloud Solutions

Market changes in recent years have made cloud-based backup and recovery technologies attractive to both small businesses as well as Managed Services Providers. Both are looking for better solutions to store backups of critical business data at offsite locations to protect against disaster. For years, removable media solutions, such as tape, have been used to solve this problem, and both small businesses and Managed Services Providers are looking to replace these legacy processes with automated, less complex solutions.

Responding to this market trend, Managed Services Providers are looking to leverage advances in Internet bandwidth and cloud storage technologies to offer cloud backup storage as a service. Many Managed Services Providers are looking to leverage their own existing data center resources as a cloud solution and store secondary copies of customer backup data.

Backup Exec 2012

Symantec Backup Exec 2012 delivers reliable data and application protection solutions designed with the Managed Services Provider in mind. Using Backup Exec 2012, Managed Services Providers can easily protect more customer data while reducing storage and management costs through integrated data deduplication and archiving technology. Managed Services Providers can also reduce customer business downtime through integrated bare metal recovery, dissimilar hardware recovery, and virtual conversion capabilities. This enables Managed Services Providers to ensure their client's critical information on virtual or physical systems is always protected and can be restored quickly.

Key features of Backup Exec 2012 include the following:

- Market-leading data and application protection for physical and virtual server environments
- Support for the latest virtual platforms, such as Hyper-V 2008 R2 and vSphere 5.0
- First-to-market granular recovery for virtual applications from a single-pass backup
- Block-level data deduplication technology to reduce storage costs associated with backup processes
- Integrated bare metal and dissimilar hardware recovery for painless disaster recovery
- Backup-to-virtual (B2V) and Physical-to-virtual (P2V) features leverage virtual technology for migration and virtual failover
- Backup Exec 3600 Appliance offers the reliability of Backup Exec software on optimized hardware

These powerful capabilities in Backup Exec 2012 allow Managed Services Providers to protect more customer data while reducing storage management costs, optimize network utilization across physical and virtual environments, automate primary storage optimization through efficient archiving, and enable all levels of recovery for both virtual and physical resources, using a single solution.

White papers and other resources on the powerful capabilities within Backup Exec 2012 can be accessed by partners via the Symantec PartnerNet portal: https://partnernet.symantec.com/

Backup Exec Private Cloud Services

A new capability within Backup Exec 2012 allows partners to offer multitenant, offsite backup storage services to their clients leveraging their own data center resources as a cloud storage location. Known as Backup Exec 2012 Private Cloud Services, this capability is designed for Managed Services Providers looking to offer cloud-based, offsite backup storage to their clients. Backup Exec Private Cloud Services combines powerful data deduplication with multi-tenant cloud storage capabilities. This ensures customer backup data is stored securely and enables the Managed Services Providers to leverage their own data centers as the offsite repository.

Backup Exec 2012's Private Cloud Services capability allows Managed Services Providers to:

- Offer cloud-based offsite backup storage to their customers
- Leverage their own infrastructure as a cloud data center
- Combine the speed of local site recovery with remote, cloud-based disaster recovery protection
- Use Backup Exec deduplication technology to reduce backup time and storage costs
- Leverage Transfer Drives to "seed" the cloud data center or transport recovery data to a customer
- Reduce time spent managing removable media-based backup processes at customer sites
- Protect both virtual and physical customer resources
- Ensure customer backup data is encrypted and secure while in transit and while at rest
- Use their preference of VPN solutions to secure the connection between client sites and the cloud data center

This technical feature brief offers an in-depth, technical look at how Backup Exec 2012 Private Cloud Services can be leveraged by Managed Services Providers to offer efficient, multitenant cloud-based backup storage services to their clients. This includes diagrams, best practices, prerequisites, and other key technical elements of the Backup Exec 2012 Private Cloud Services solution that Managed Services Providers will need to understand.

For detailed, step-by-step instructions on implementing and configuring the different elements of a Private Cloud Services solution, please refer to the Private Cloud Services Planning and Deployment Guide available here:

http://www.symantec.com/business/support/index?page=content&id=TECH172464

Key Terms

Term	Definition
Backup Exec Private Cloud Services	Official feature name
Enterprise Server Option	Parent option of the Central Admin Server Option (CASO)
Central Administration Server (CAS)	Backup Exec server with CASO installed
Managed Backup Exec Server (MBES)	New name for Managed Media Server (MMS)
Cloud Storage Server	Backup Exec server located in Managed Services Provider's data center hosting deduplication store May be a CAS or MBES depending on configuration
Deduplication Storage Folder	Backup Exec local disk backup device enabled for data deduplication
Backup Definition	Replacement name for "policy"
Offsite Copy	Backup data stored to local Managed Backup Exec Server, then "copied" to Cloud Storage Server

Private Cloud Services

Overview

The diagram below describes a simplified, overall view of an implementation of Backup Exec 2012 Private Cloud Services and the different components and relationships involved. Individual sections of this diagram will be described in greater detail to highlight key or important elements that require additional explanation.

Backup Exec 2012 Private Cloud Services allows Managed Services Providers to offer multitenant, cloud-based offsite storage of customer backup data for disaster recovery protection. In addition, Private Cloud Services utilizes remote Managed Backup Exec Servers at each customer site to host local copies of backup data, allowing for fast and easy local recovery capabilities. Managed Services Providers can centrally monitor and manage all backup operations across their Private Cloud Services infrastructure using the Backup Exec 2012 Central Administration Server console.

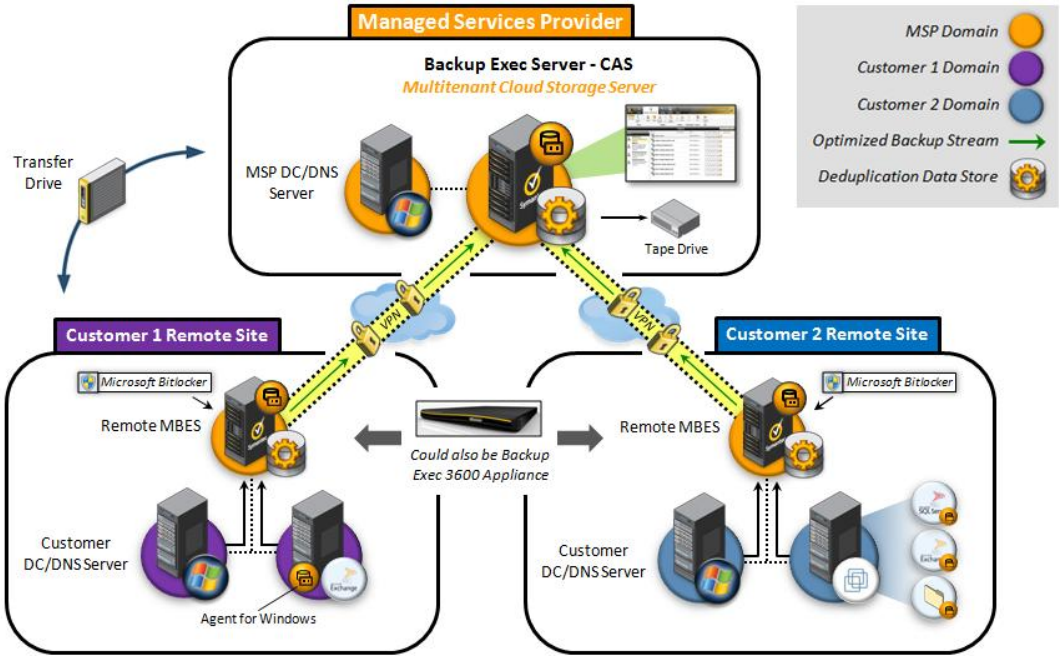

Figure 1: Multitenant Private Cloud Services Diagram

Managed Services Provider Site

Multitenant Cloud Storage Server

In a multitenant Private Cloud Services configuration, the Cloud Storage Server located at the Managed Services Provider's site will be a Backup Exec Central Administration Server with a local deduplication storage folder. The local deduplication storage folder will be shared with the remote Managed Backup Exec Servers located at each client site. Backup sets captured from client production servers will be initially stored to the Managed Backup Exec Server at the client's site, and will then be replicated to the Cloud Storage Server's deduplication storage folder. Data deduplication technology optimizes the replication process, transferring only unique blocks from local Managed Backup Exec Servers to the Cloud Storage Server.

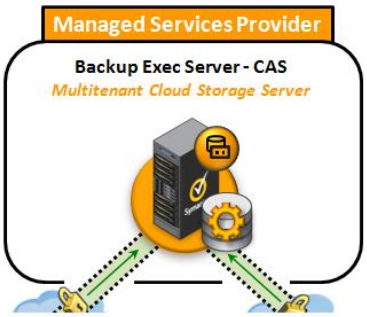

Figure 2: Multitenant Cloud Storage Server

When installing and configuring a Cloud Storage Server, the "Private cloud server" option should be selected in the 'Storage' tab of the Backup Exec Central Administration Server user interface. This setting helps ensure that jobs are dispatched to the correct Managed Backup Exec Server and target the correct storage device in a Private Cloud Services configuration.

It's important to note that when using a multitenant Private Cloud Services configuration, a Cloud Storage Server's deduplication storage folder can contain a maximum of 64 Terabytes of deduplicated data. Scalability of the 64 Terabyte capacity of a deduplication storage folder will vary depending upon a number of factors, such as deduplication ratios, the amount of front-end backup data being protected, and data retention policies. Adjusting data retention policies or migrating backup sets from the Cloud Storage Server to tape media can help solve problems where the deduplication storage folder of a Cloud Storage Server is filling up too rapidly.

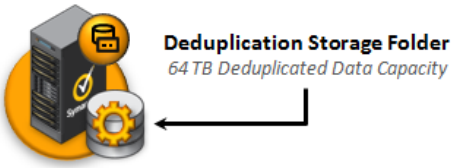

Figure 3: Deduplication Storage Folder

For Managed Services Providers with backup data hosting requirements that exceed the capacity of a single Cloud Storage Server, additional Cloud Storage Servers can be added to the environment to enable additional capacity.

Data Deduplication

The data deduplication technology within Backup Exec 2012 is an integral part of a Private Cloud Services implementation. Data deduplication processes break down streams of backup data into "blocks" of around 128k in size. Each data block is identified as either unique or non-unique, and a tracking database is used to ensure that only a single copy of a data block is saved to the deduplication storage folder of the target Backup Exec server.

For subsequent backups, the tracking database knows what data blocks have already been captured and stored to the deduplication storage folder, and only unique blocks in subsequent backup streams are stored. For example, if five different client systems are sending backup data to a Backup Exec server and a data block is found in backup streams from all five of those client systems, only a single copy of the data block will be transported over the network and stored to the deduplication storage folder by the Backup Exec server.

This process of reducing redundant data blocks saved to backup storage leads to a significant reduction in storage space needed for backups.

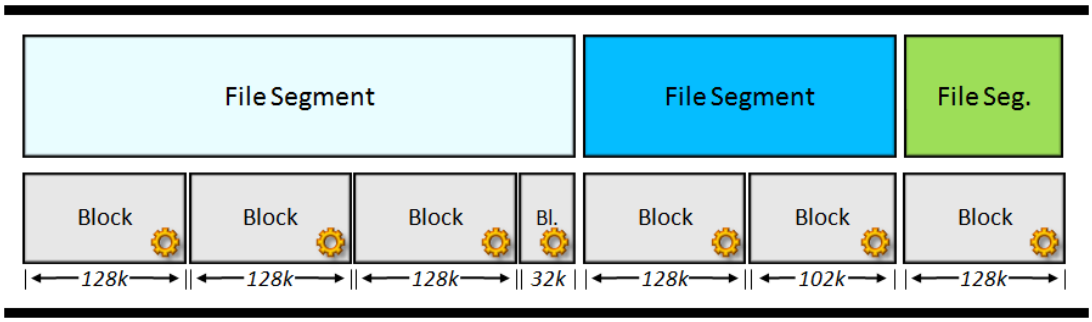

Figure 4: Data Deduplication Process

The deduplication technology within Backup Exec is applied globally across all backup streams that are stored to the deduplication storage folder of a Backup Exec server. Backup Exec 2012 includes stream handler technology designed specifically for VMware and Hyper-V backups, ensuring a high level of data deduplication efficiency when storing backups containing VMDK or VHD files.

In a multitenant Private Cloud Services configuration, both the Cloud Storage Server at the Managed Services Provider's data center as well as the Managed Backup Exec Servers at remote client sites are deduplication-enabled Backup Exec servers. In this configuration, data blocks associated with client backups will be stored in two places: the local Managed Backup Exec Server at the client site, and the Cloud Storage Server at the Managed Services Provider data center. This allows the client to benefit from rapid restore processes leveraging the local Managed Backup Exec Server's backup repository, as well as benefit from offsite disaster recovery protection if a site-level disaster occurs or the local Managed Backup Exec Server experiences a disaster event.

Data deduplication technology is also leveraged to optimize the process of replicating backups from the Managed Backup Exec Server at remote client sites to the Cloud Storage Server at the Managed Services Provider's location.

White papers, assessment tools, and other resources for the data deduplication technology within Backup Exec 2012 can be accessed by partners via the Symantec PartnerNet portal: https://partnernet.symantec.com/

Client Site Monitoring and Management

Another benefit of the multitenant Private Cloud Services configuration is the ability of the Managed Services Provider to monitor and manage global backup operations across all customer sites from the Central Administration Server console on the Cloud Storage Server. From this single console, the Managed Services Provider can see a centralized view of the backup status of all client servers, create and dispatch backup and recovery jobs, run reports, and perform other tasks associated with managing their Private Cloud Services environment.

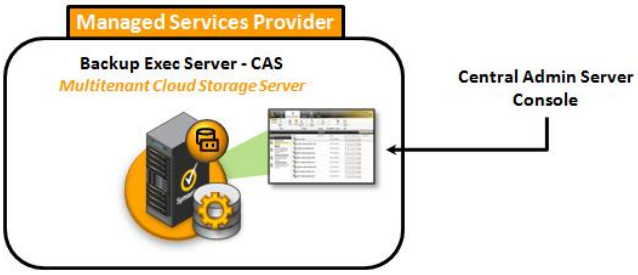

Figure 5: Central Administration Server Console

The new grouping features of the Backup Exec 2012 console make the management and monitoring of multiple customer sites even easier. From the Central Administration Server console on the Cloud Storage Server, the Managed Services Provider can easily create logical groups for each client, allowing them quick access to client-specific views.

Figure 6: Logical Server Grouping

Exporting Backups to Removable Media

After centralizing client backups to a Cloud Storage Server, Managed Services Providers retain the ability to copy or export backup sets to removable media, such as tape. This capability allows the Managed Services Provider to add additional layers of protection to customer business data by storing copies of backup sets to removable media and shipping them to an alternate location, or to periodically provide their clients with copies of their backup data.

The backup stages that store backup data to the Managed Backup Exec Server at the client side, copy backup data to the Cloud Storage Server at the Managed Services Provider's site, and copy backup data to tape (D2D2T) can be easily configured by the Managed Services Provider within a single backup definition.

Recovery Testing Services

By centralizing customer data to a Cloud Storage Server at the Managed Services Provider's location, a Private Cloud Services implementation also allows the Managed Services Provider to periodically run validation jobs against customer backup data or even perform test recovery operations. This allows peace of mind and ensures recoverability should an actual disaster occur, and can even be offered by the Managed Services Provider as an additional service to clients.

Disaster Recovery in the Cloud

Other enhancements introduced in Backup Exec 2012 give Managed Services Providers additional recovery services that can be offered to their customers, such as the ability to automatically convert client backups to fully functioning virtual machines. Should the Managed Services Provider decide to leverage this capability, a potential service could be an actual "cloud server recovery" service whereby the Managed Services Provider launches a virtual replica of a client's server on their own infrastructure, allowing client business operations to resume and continue while the original production server is repaired or restored.

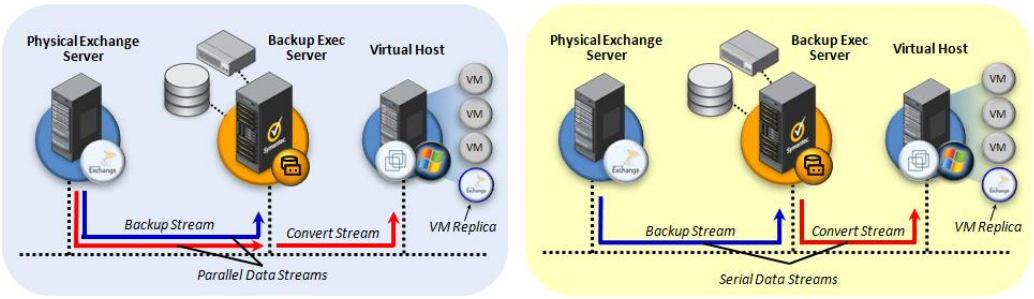

Figure 7: Virtual Conversions

The virtual conversion capabilities of Backup Exec 2012 support both the VMware vSphere and the Microsoft Hyper-V platforms.

Cloud Storage Server Security Recommendations

In order to ensure the security of critical customer backup data, Symantec recommends the following for the Cloud Storage Server at the Managed Services Provider's site:

- **Enable Encryption on the Deduplication Storage Folder** – The deduplication storage folder on the Cloud Storage Server should be encrypted, ensuring client backup data remains secure while "at rest" at the Managed Services Provider's site.
- **Do Not Enable Client-side Deduplication** – Client-side deduplication should not be enabled on the Cloud Storage Server's deduplication storage folder. This does not prevent optimized replication of backup data from client sites to the Managed Services Provider's Cloud Storage Server.
- **Member of Managed Services Provider's Domain** – The Cloud Storage Server at the Managed Services Provider's site and the Managed Backup Exec Servers at remote client sites should be members of the Managed Services Provider's domain.
- **No Client Logon Access to Managed Backup Exec Servers** – Clients should not be given logon access to the Managed Backup Exec Servers at their sites. This is a key element of maintaining multitenant protection of data across customers in a Private Cloud Services configuration.

Customer Site

Managed Backup Exec Server

In a multitenant Private Cloud Services configuration, the Backup Exec server located at the client's site will be a Managed Backup Exec Server with a local deduplication storage folder. The local deduplication storage folder will be used to host local copies of backups captured from production servers in the client's environment. Backup sets captured from client production servers will be initially stored to the Managed Backup Exec Server at the client's site, and will then be replicated to the Cloud Storage Server's deduplication storage folder.

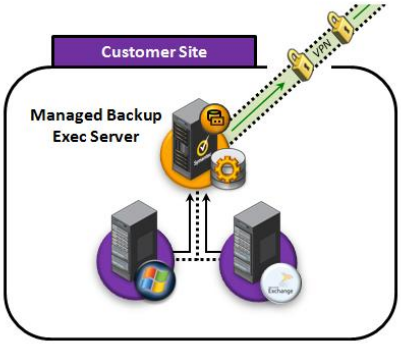

Figure 8: Managed Backup Exec Server at Client Site

Backup Exec 3600 Appliance

Depending upon the needs of a particular client, Managed Services Providers have the option of using the Backup Exec 3600 Appliance as the Managed Backup Exec Server at a client site as an alternative to building and implementing a Backup Exec server on custom hardware. Using a Backup Exec 3600 Appliance as the Managed Backup Exec Server at a customer site greatly reduces the time required to implement the client-side component of Private Cloud Services.

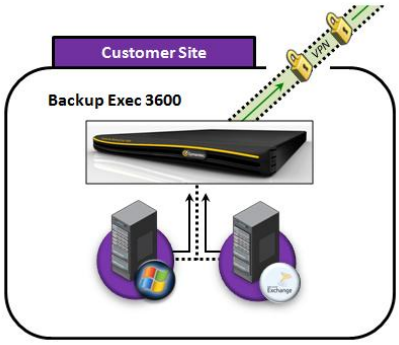

Figure 9: Backup Exec 3600 at Client Site

The Backup Exec 3600 Appliance is a pre-built, tested, and optimized Backup Exec server on a known hardware configuration, and supports all required features for a Private Cloud Services implementation, such as virtual and physical server backup support, application backup support, data deduplication, and much more.

White papers and other resources on the Backup Exec 3600 can be accessed by partners via the Symantec PartnerNet portal: https://partnernet.symantec.com/

Local Recovery Capabilities

One of the most important benefits of using Backup Exec 2012's Private Cloud Services feature is the powerful backup and recovery capabilities of Backup Exec that a Managed Services Provider can employ on behalf of a client at their local site. These capabilities include:

Physical Server Recovery Capabilities
• Bare metal and dissimilar hardware recovery
• Virtual conversion to VMware or Hyper-V
• Application recovery
• Granular application recovery
• Granular file and folder recovery

Virtual Server Recovery Capabilities
• Full virtual machine recovery
• Application recovery
• Granular application recovery
• Granular file and folder recovery
• Redirected recovery to alternate virtual host

These powerful recovery capabilities allow partners to respond to any recovery need at a remote client site, and most can be managed centrally from the Cloud Storage Server's user interface.

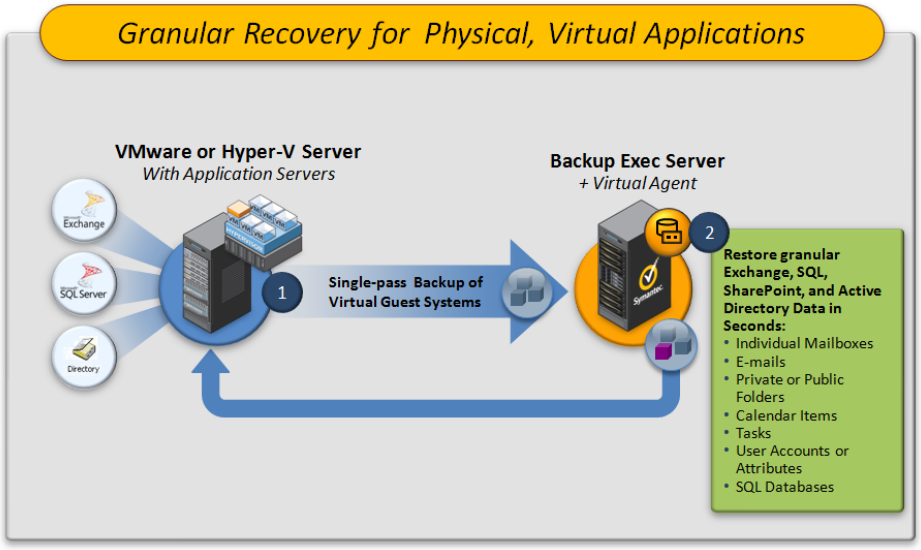

Figure 10: Powerful Recovery Capabilities

White papers and other resources on the powerful backup and recovery capabilities within Backup Exec 2012 can be accessed by partners via the Symantec PartnerNet portal: https://partnernet.symantec.com/

Managed Backup Exec Server Security Recommendations

In order to ensure the security of critical customer backup data, Symantec recommends the following for Managed Backup Exec Servers at remote client sites:

- **Standalone Physical Hardware** – The Managed Backup Exec Server should always be hosted on standalone physical hardware, and should not be implemented as a virtual machine.
- **Disk Encryption** – A local disk encryption solution should be used to secure the system volume of Managed Backup Exec Servers, such as PGP Whole Disk Encryption or Microsoft BitLocker.

  If the Backup Exec 3600 Appliance is being used as the Managed Backup Exec Server at a client site, it is already secured with Symantec Critical System Protection technology.
- **Member of Managed Services Provider Domain** – The Cloud Storage Server at the Managed Services Provider's site and the Managed Backup Exec Servers at remote client sites should be members of the Managed Services Provider's domain. Clients should not be given log-on access to Managed Backup Exec Servers.

Replicating Client Backups to Cloud Storage Server

Optimized Duplication

The technology used to replicate customer backup data from Managed Backup Exec Servers at remote client sites to the Cloud Storage Server at the Managed Services Provider's location is referred to as Optimized Duplication. Using data deduplication technology, Managed Backup Exec Servers only transmit unique data blocks to the Cloud Storage Server, greatly optimizing the transfer process. By only transmitting unique data blocks, time and bandwidth requirements to complete replication jobs are greatly reduced.

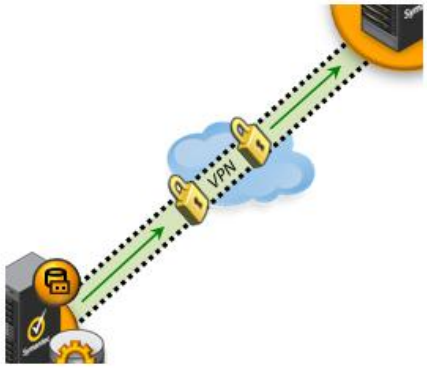

Figure 11: Optimized Duplication

White papers and other resources on Optimized Duplication can be accessed by partners via the Symantec PartnerNet portal: https://partnernet.symantec.com/

Built-in Backup Exec Security Features

To help prevent unauthorized access to critical backup data captured by Backup Exec while it is being transmitted or "in flight," all communications between Backup Exec 2012 components are encrypted using TSL/SSL encryption technology, and require a trust relationship to be established. This includes communication between the Cloud Storage Server and Managed Backup Exec Servers, communication between the Cloud Storage Server and protected servers, as well as communication between Managed Backup Exec Servers and protected servers.

To ensure critical backup data is encrypted and protected while "at rest" on the Cloud Storage Server at the Managed Services Provider's site, it is also recommended that encyrption be enabled on the deduplication storage folder of the Cloud Storage Server.

For client sites using VMware technology, it is recommended that SSL be enabled on all VMware hosts with virtual machines being protected by Backup Exec 2012.

Encrypted communications in a Private Cloud Services environment ensure that backup data and related information remain secure and protected from unauthorized access.

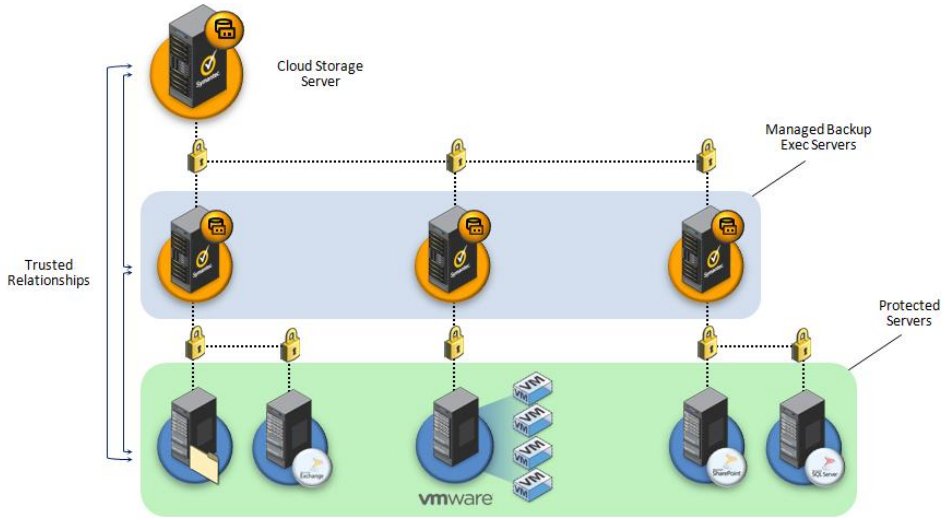

Figure 12: Backup Exec 2012 Communication Security Diagram

VPN Security Recommendations

Symantec requires that a VPN solution be used to secure the communication path between the Cloud Storage Server at the Managed Services Provider's location and Managed Backup Exec Servers at remote customer sites in a Private Cloud Services configuration. Any VPN solution preferred by the Managed Services Provider can be used.

The Private Cloud Services Planning and Deployment Guide offers additional information and details on the subject of VPN technology. The Planning and Deployment Guide is available here:

http://www.symantec.com/business/support/index?page=content&id=TECH172464

Multitenancy Support

Managed Services Provider is the Trusted Advisor

Customers that trust their data to be stored offsite at the Managed Services Provider's location in a multitenant Private Cloud Services configuration require that their backup data remain secure and protected from unauthorized access. This includes a requirement to prevent other customers from being able to access and restore their critical and private business data. A multitenant implementation of Backup Exec 2012's Private Cloud Services functionality allows Managed Services Providers to meet these customer requirements.

It's important to note that multitenant protection and security within a Backup Exec 2012 Private Cloud Services configuration does not include physical separation or partitioning of customer data at the Managed Services Provider's location; customer data will co-exist in deduplicated form on the Cloud Storage Server. This allows Managed Services Providers to gain the greatest benefit of deduplication technology and manage storage costs at their site. Multitenant protection and security is achieved by the Managed Services Provider being the full owner, operator, and trustee of backup operations across customer sites. Customers are not allowed logon access to the Managed Backup Exec Server even at their own site; they give full responsibility and ownership to the Managed Services Provider. While clients are unable to access or control backup operations of their own environment, they are also prevented from accessing other customer's data as well.

Within a multitenant Private Cloud Services configuration, the Managed Services Provider plays the role of trusted advisor for backup and recovery operations for all clients participating in their Private Cloud Services scenario.

Domain Requirements

A key element of maintaining multitenant security in a Private Cloud Services configuration lies in how the different interacting domains are configured. The Managed Backup Exec Servers at client sites are not part of client domains, but rather are a part of the Managed Services Provider's domain. Clients are not given logon access to the Managed Backup Exec Servers.

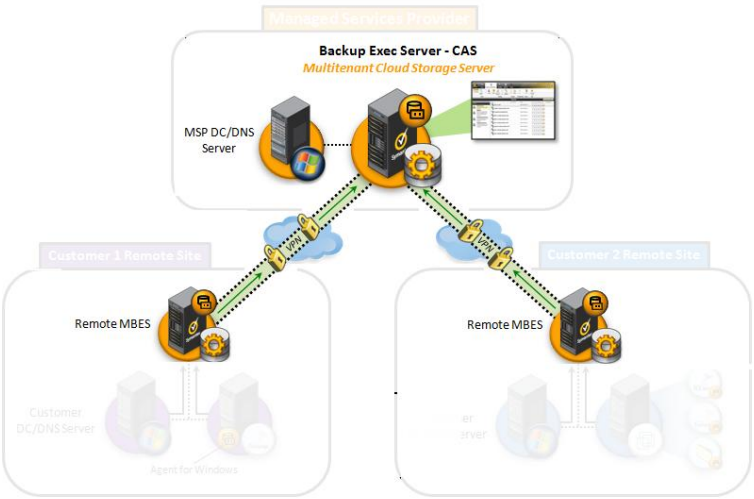

Figure 13: Managed Services Provider Domain Configuration Diagram

The Cloud Storage Server and the Managed Backup Exec Servers at each client site should be a part of the same Managed Services Provider's domain. Optionally, the Managed Services Provider has the ability to put the Managed Backup Exec Servers at client sites into a child domain of the parent domain in which the Cloud Storage Server resides. The Managed Backup Exec Servers at client sites could even be made members of different Managed Services Provider forest domains, as long as appropriate domain trusts were established between the domain in which the Cloud Storage Server resides and each Managed Backup Exec Server domain.

This configuration allows Managed Services Providers to ensure that each customer's critical business data is protected from unauthorized access – intentional or otherwise.

Transfer Drives

Seeding the Cloud Storage Server

The Managed Services Provider can leverage a transfer drive to seed the Cloud Storage Server's deduplication storage folder. This reduces the amount of data that the Managed Backup Exec server at a client site will need to replicate directly to the Cloud Storage Server at the Managed Services Providers location. This is done by storing a full backup of one or more client servers to an external storage device on the Managed Backup Exec Server, such as a USB drive. Once complete, the USB drive can be transported to the Managed Services Provider's location where the backup data will be copied to the deduplication storage folder on the Cloud Storage Server.

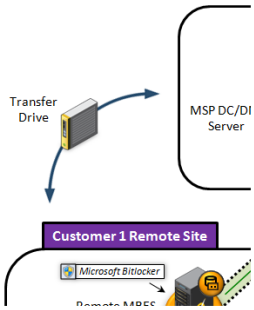

Figure 14: Transfer Drive

Additional notes, recommendations, and guidelines for seeding the Cloud Storage Server using this process can be found in the Private Cloud Services Planning and Deployment Guide available here:

http://www.symantec.com/business/support/index?page=content&id=TECH172464

Transporting Backup Data Using Transfer Drives

Transfer drives can also be leveraged to transport large amounts of backup data to a client site when a network-based recovery is not optimal or not possible. This process is essentially the reverse of the seeding process described previously. Backup data contained in the deduplication storage folder of the Cloud Storage Server can be copied to an external device, such as a USB or tape, which can then be transported to the client's site. At the client's site, the external device is inventoried and catalogued by the local Backup Exec Server, after which the data can be restored to the production servers at the client's location.

Using transfer drives in this manner can be useful for recovery operations involving large amounts of data or for disaster recovery scenarios.

Private Cloud Services Backup Calculator

Another tool provided by Symantec to help Managed Services Providers looking to leverage Private Cloud Services is the Backup Exec Private Cloud Services calculator spreadsheet. This spreadsheet tool helps Managed Services Providers determine time estimates for cloud backups using Private Cloud Services. The spreadsheet is available at no charge and can be found at the following location:

http://www.symantec.com/docs/TECH172473

Performance Considerations

Latency and Connection Guidelines

Network Recommendations

A multitenant Private Cloud Services configuration requires persistent, high-fidelity network links between the Managed Services Provider site and remote client sites. This includes the following requirements:

- Less than one percent packet loss during transmissions
- Round-trip network latency of 250 ms or less

Loss of Network Connection

Should an event occur that results in the Managed Backup Exec Server at the client site losing communication with the Cloud Storage Server, scheduled backup operations will cease. After the connection is restored, scheduled backup operations will resume as normal.

If necessary, the Managed Backup Exec Server at a client's site can be reverted to standalone mode in order to perform a local recovery operation when a connection to the Cloud Storage Server cannot be reestablished in a timely manner. Details for reverting a Managed Backup Exec Server to standalone mode are outlined in the Private Cloud Services Planning and Deployment Guide (p. 40).

ExSP Licensing Program

The Symantec Enterprise Service Provider (ExSP) Program is designed to enable Managed Services Providers to easily license Symantec products to provide outsourced and managed services to their customers. Under the ExSP program, Symantec products are licensed to the Service Provider on a monthly subscription basis, with all payments quarterly in arrears.

Through the ExSP licensing program, Symantec helps Managed Services Providers reduce upfront investment costs by providing a licensing model that aligns with the way they do business with their end-user customers.

Unlike the standard internal use or Strategic Service Provider use licenses that are sold to end-users and service Providers on a perpetual basis, ExSP licenses grant Managed Services Providers the right to use our products to provide a service to its end-users on a limited term basis.

Here are some of the key global program features of the ExSP program:

Flexible, Convenient Licensing - Licensing designed to match the way Managed Services Providers do business with their customers:

- Access to the latest software versions available under maintenance/support
- Each license provides 1 month of commercial use rights and Essential maintenance/support
- No upfront license or support fees
- Quarterly payments (in arrears) based on quarterly usage reports provided by service provider

More information on the Symantec ExSP licensing program and how partners can participate is available at the Symantec PartnerNet portal: https://partnernet.symantec.com/

For More Information

Link	Description
http://www.symantec.com/business/support/index?page=home	**Enterprise Support Portal**
www.symantec.com/business/backup-exec-for-windows-servers	**Backup Exec Family Landing Page**
www.symantec.com/business/products/whitepapers.jsp?pcid=pcat_business_cont&pvid=57_1	**White Papers, Datasheets, Solution Briefs**
http://support.veritas.com/docs/304175	**Using Backup Exec in Large Environments**
www.backupexec.com/compatibility	**Compatibility Documentation**
www.backupexec.com/skugenerator	**SKU Generator and BEST Tool**
http://www.symantec.com/docs/TECH172473	**Private Cloud Services Calculator**
http://www.symantec.com/docs/TECH172464	**Private Cloud Services Documentation**
https://partnernet.symantec.com/Partnercontent/Login.jsp	**Symantec PartnerNet Portal**

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec helps organizations secure and manage their information-driven world with data backup and recovery software.