ZYNSTRA TECHNICAL BRIEFING NOTE

Backup

What is Backup?

Backup is a service that forms an integral part of each Cloud Managed Server. Its purpose is to regularly store an additional copy of your data and to do so in such a way that the risk of ever losing some or all of that data is minimized. Backup is designed to help you prevent data loss that may occur as a result of:

- The accidental deletion of data by a user
- The failure of one or more components on the appliance, in particular its hard disks
- The complete destruction or loss of the appliance as a result of a disaster

Backup can secure data through three distinct types of process:

- A **Local Backup**, in which a copy of your data is maintained locally on the server itself but in such a way that you are protected against individual local failures of server components
- A **Cloud Backup**, available as part of the Cloud Backup and Disaster Recovery (BUDR) option, in which a copy of the customer's data is transferred to and maintained in the Cloud so that there is protection against the complete destruction or loss of a server
- A **Device Backup**, available as part of the RDX Backup option, in which a copy of your data is transferred to and stored on an HP RDX device which uses removable media to hold the data, allowing you to take that media off-site for storage, allowing you to protect yourself against the complete destruction or loss of your server. It should be noted that, in general, Device Backup can and should only be considered if (a) your Internet connection does not have sufficient upload bandwidth to enable the transfer of your data to the Cloud sufficiently rapidly, and (b) your data volumes are low as the removable media has a relatively low physical limit to the amount of data it can store

This document provides an explanation of the Cloud Managed Server backup process. With the exception of using a HP RDX device, all backup on a Cloud Managed Server takes place automatically behind the scenes because a primary purpose of Zynstra is to lighten the workload of administrators.

A separate Technical Briefing Note contains instructions on how to integrate customer defined IaaS VM data with this automated backup process. Please see "Backing Up IaaS VMs".

Underlying Backup Principles

A Cloud Managed Server includes a fully automated process for the backup of all data on the server. Zynstra also provides an option to duplicate this information off-site either in the Cloud or for limited volumes of data on smaller appliances to an attached HP RDX device.

The primary purpose of Backup is to create a repository with a copy of data that can be used for disaster recovery. This same repository can be used to overcome data loss issues associated with any type of data-affecting failure. A tertiary purpose is to secure appliances against the accidental deletion of data. The method by which that purpose is achieved is the creation of a repository.

For practical reasons, this repository should be kept separate from original data so that in the unlikely event of fire, flood or theft, the backup data is still accessible.

Although the principles behind backup are straightforward, to discuss it in more depth a number of key terms need to be understood. These are defined in the following section.

Definition of Backup Related Terms

The definitions used here are specific to Zynstra's backup capability and replace industry terms with similar names.

Backup is a process that operates on end user and application data to take a copy of this data, store it in a separate location and create a database with a full list of all items backed up along with critical metadata attributes, for example, file name, created date, last edited date, file size plus other relevant characteristics. A metadata database makes it easier to search for files based upon a number of criteria. The Zynstra backup process always compresses data and encrypts all user data.

User and application data is the variable data, which may be files, directories or volumes generated by users and applications on the Zynstra appliance.

A ***full backup*** includes all user and application data.

An ***incremental backup*** includes all user and application data that has been added or changed since the last backup, whether full, differential or incremental, was performed.

A ***differential backup*** includes all user and application data that has been added or changed since the last full backup.

Each time a backup takes place, whether full, differential or incremental, a ***restore point*** is created. This type of restore point should not be confused with a Windows restore point. The number of restore points of each type that are kept defines the ***retention policy***. The more restore points in a retention policy, the more opportunities there are to return to a point in time and recover data. All

retention policies are a compromise: more restore points enable access to past data with more certainty and granularity of time but at a higher storage cost and greater management overhead.

Local backup is a backup that is stored on a Zynstra Cloud Managed Server.

Off-site backup is a backup that is stored on a separate device or service from a server. Examples include Microsoft Azure, Amazon AWS or a HP RDX device with removable cartridge where the cartridge is physically moved to a separate location once backup is complete.

Restore is the process of locating a file, directory or volume in a backup and copying it into the operational user and application data store. This will require decryption and decompression of the backup which will take place automatically.

Compression is the process of encoding information using fewer bits than the original representation. In backup, it is imperative that lossless compression is used.

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it. Encryption uses a set of ***encryption keys*** that are used to lock and unlock data. In a backup environment, it is critical that encryption keys are maintained safely because without them the original data cannot be accessed.

Zynstra ***Disaster Recovery*** or ***DR*** is the set of procedures and tools that enable the recovery of a Zynstra Cloud Managed Server following a natural or human-induced disaster.

Retention Policy is the set of rules that define the length of time that different types of backups are kept.

Recovery Point Objective (RPO) is the maximum time period during which data created or changed in that period has been lost as a result of not having been backed up to the Cloud before the disaster occurred, assuming that the customer has sufficient Internet data upload bandwidth given the rate at which their data changes (and hence needs to be backed up).

Recovery Time Objective (RTO) is the maximum time to restore appliance on the customer's premises with (if Cloud Backup purchased) the customer's user data, documents and other files as well as any Zynstra or Partner Managed Applications and their associated data.

Zynstra makes a number of service level commitments that define the minimum standard Zynstra expects to achieve if delivering the service. These commitments combine to form the **Service Level Agreement (SLA)**. Zynstra's services are defined in Zynstra Service Delivery Lifecycle & Service Levels with SLA for availability, RPO, RTO and DR are defined in Zynstra's Service Level Agreement.

Backup Schedule

On a Cloud Managed Server all backups are carried out automatically to a defined schedule. This schedule is defined and maintained by Zynstra. Backups are normally scheduled to take place at night or weekends outside of normal business hours in the local time zone of each Zynstra appliance.

Zynstra runs a full backup on an appliance once it has been commissioned.

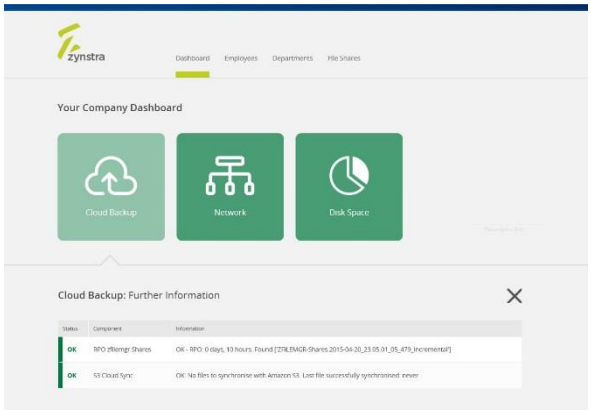
Zynstra also fully backs up the non-Zynstra software images on the appliance, including those installed Line of Business (LoB) applications in IaaS VMs (please see the separate IAAS VM Backup Technical Note to ensure pre-requisites for successful backup of these VMs are in place, without which Zynstra cannot guarantee the ability to restore LoB applications).

Once fully operational, Zynstra performs an incremental backup of file based data on four consecutive days in the week. On the fifth day, an incremental followed by a differential backup is performed. The extra incremental backup takes a short time and helps ensure that RPO is kept low even if the differential backup takes a long time. This backup cycle is repeated weekly.

Incremental backups handle incrementals of change only and therefore execute quickly and require less bandwidth to transfer them off-site. Differential backups provide a roll up of all changes since the last full backup. Using a combination of full, differential and incremental backups make it easier to reassemble a complete appliance in the event of a disaster.

Once a local backup process completes, Zynstra streams encrypted backup data to the Cloud. Streaming backup data to the Cloud is traffic managed, such that it will operate continuously, and use all available bandwidth, but on a lower priority so it will scale back if there are other types of traffic.

As the user and application data changes over time, the volume of data in a differential backup grows. At some point the length of time it takes to perform a differential backup and store it in the Cloud will become unacceptable long. Once this occurs, a full backup is performed.



It is possible for a customer to view the current status of RPO at any time through the User Control Console (see the screenshot on this page).

Zynstra's policy is that the point at which RPO becomes unacceptable is generally when it reaches 100 hours. At this point, Zynstra will automatically schedule a full backup. If the predicted length of time for a full backup exceed one week, the Zynstra Customer Success team will consult with the Service Provider that maintains the support relationship with the customer.

The actual RPO experienced depends upon a combination of the size of a backup and the bandwidth of the Internet connection used to stream the backup to the Cloud. It is possible to achieve a lower RPO using a higher bandwidth Internet connection.

Customers who require a lower RPO will need to purchase an Internet connection that enables a backup to take place inside their target RPO time and request through their Service Provider that Zynstra perform a full backup every time their RPO threshold is exceeded.

A customer can request (via their Service Provider) that a full backup be postponed until a holiday or other quiet period if they are concerned about the impact a full backup may have on their network. This is not usually necessary because Zynstra uses traffic management to ensure backup data is streamed at a low priority so should not impact performance of other users or applications.

Protecting Local Backup Data

The Backup process stores data locally on an appliance. Backup data is compressed and encrypted and is initially stored on local disks.

In a cluster of appliances, both backup data and source user and application data are fully and continuously replicated between cluster nodes.

Standalone (non-clustered) configurations use mirrored disks. Clustered Zynstra servers use continuous node-to-node data replication. This ensures that the failure of a single physical disk will not cause a customer-affecting outage, data loss or the need to restore from backup.

Cloud Storage

Zynstra can store backup data in the Cloud in addition to locally. Storing data in the Cloud reduces the likelihood of data loss following a disaster.

The place where the backup is stored in the Cloud depends on the channel partner through whom the Zynstra appliance was purchased. It will be one of Amazon Web Services, Microsoft Azure or HP Helion.

If Zynstra's Backup and Disaster Recovery (BUDR) option has been purchased then backup data is uploaded to the appropriate backup target in the Cloud automatically.

The speed of getting data into the Cloud is dependent upon the speed of the connection between a Zynstra appliance and the Cloud. More information on required connection speeds can be found in Zynstra Technical Briefing Note on Business Internet Connectivity.

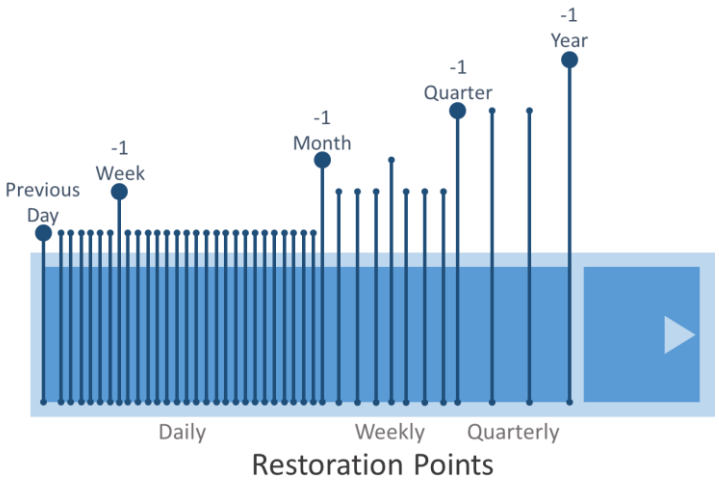
Retention Policy

Zynstra retains data locally on the appliance or cluster depending upon its age. This generally eliminates the need to access data in the Cloud when data needs to be restored following a limited local failure of one or more hardware components. The last 30 days of backup data are kept locally.

The BUDR option includes current-state or retention-policy options.

The current-state option means only backup files sufficient to restore the Zynstra Cloud Managed Server to its state at the point of the last backup are held in the Cloud.

For BUDR options with a retention period, such as one year, sufficient backup files are stored by Zynstra in the Cloud to allow restoration of files dating back to that period. The point-in-time that a data can be restored from includes backup instances for all days in the last month, all weeks in the last quarter, and all quarters in the last year.



Data that is older than the purchased retention period will be permanently deleted.

Zynstra retains a number of copies of data locally. In addition to the original user and application data, there is a mirrored copy of this data, a set of local compressed and encrypted backups and a mirrored copy of this backup. If Zynstra's BUDR option has been purchased then a full set of compressed and encrypted backups are also stored using a redundant storage option to ensure at least two further copies off site.

Since a backup system contains at least one copy of all data that needs to be saved, the data storage requirements can be significantly higher than the capacity of an appliance. Organizing this storage space and managing the backup process can be a complicated undertaking. Zynstra manages all of this capacity management invisibly.

Local Snapshots, Windows Previous Versions and File Recovery

In the past it may have been necessary to resort to backup tapes to recover an accidentally deleted file. Zynstra takes snapshots of user and group file shares every hour. Zynstra uses this information to enable file history in Windows. This enables a user to right mouse click on a file or directory, select the "Previous Versions" tab and see a history of changes. A user can self-serve the restoration of older or deleted files using the "Copy…" or "Restore…" functions.

The depth of history is only limited by the storage capacity of the Cloud Managed Server. Typically three months history is available. The actual depth is dependent upon disk space allocated and the rate of change of data.

The snapshot feature is not supported from Apple MacOS or Linux clients.

Should a file be accidentally deleted and it is not be available within a snapshot, Zynstra will endeavor to recover the file from local backup or backups in the Cloud although there is no guarantee that the file will have existed at the time of a Zynstra backup (for example, it may have been created and then deleted in the interval between two backup restoration points). To request the recovery or an individual file or set of files, customers should request this from their Zynstra Service Provider who will in turn engage with Zynstra to recover the file or files.

Zynstra Infrastructure Backup

In addition to backing up user and application data, a Zynstra backup also stores Zynstra configuration, like the Microsoft Active Directory (AD) configuration. Zynstra Infrastructure backup stores data offsite regardless of whether Zynstra BUDR is purchased or not. Zynstra only requires a upload connection speed of 200kbits/s for the infrastructure backup to operate satisfactorily.

Zynstra manages and maintains the master images (sometimes called 'golden images') of all Zynstra software and infrastructure. The consequence of maintaining this software centrally is that it is not necessary to back it up in the same way as user or application data. This reduces the complexity and cost of backing up Cloud Managed Servers.

Encryption & Security

All backup data is encrypted using the industry standard AES-128 encryption algorithm. The AES-128 encryption algorithm uses a 128-bit key.

To secure the AES key, Zynstra uses a second encryption RSA algorithm with much longer 2048-bit keys.

Zynstra uses the RSA algorithm to encrypt the 128-bit keys used in the AES algorithm. Zynstra uses encrypts the AES key twice with two different RSA certificates so that there are always two different

master keys to decrypt the data, a normal decryption key and a backup in case the first key is misplaced.

One of these RSA encrypted AES keys is kept on the appliance for encryption and decryption of user data while the second key is kept securely by Zynstra.

Removable Local Backup using HP RDX

If a customer is unable to use BUDR because of low broadband connection speed or because they are uncomfortable with the use of the Cloud, it is possible to use a HP RDX device to backup a maximum 2TB total of system configuration, VMs and data. Please see the Technical Briefing Note about HP RDX for more information.

Backing Up IaaS VMs

The backup of applications and data in a Zynstra IaaS VM is the subject of a separate Technical Briefing Note as there are important considerations for customer and partner in terms of the placement of this data to ensure that it is backed up appropriately.

Disaster Recovery (DR)

Should a Cloud Managed Server be rendered unusable and inaccessible indefinitely or for a period of at least one week then Zynstra will initiate the Disaster Recovery process. The terms under which this is triggered and operated are described in a Zynstra Technical Note and covered by the Zynstra SLA.

Zynstra will initially recover any data backed up to the Cloud to create a virtual Zynstra appliance in the Cloud, a virtual appliance which will not include any customer or partner-managed IaaS VMs. Zynstra will operate this virtual appliance for a period of two weeks by which time a replacement appliance will have been deployed on a site of the customer's choice.

Although Zynstra will replace its Cloud Managed Server in the event of a disaster, it cannot resurrect a customer's data if it has not contracted for Zynstra's BUDR service.

In a DR scenario, restoration of IaaS VMs is the responsibility of a customer or its Service Provider. Please refer to the separate Technical Briefing Note on Backing Up IaaS VMs.