ZYNSTRA TECHNICAL BRIEFING NOTE

Service Continuity Assurance

Introduction

Cloud Managed Servers and the services that are delivered in conjunction with them are designed to ensure that Customers enjoy a degree of service continuity and access to up-to-date data which is appropriate to the criticality of IT to their organisation. Options are available that minimise service and data loss in the event of a failure, in particular

- the **High Availability Option (HA)**, in which two server computers are deployed in a configuration known as a cluster and in which the service continues to operate even if one of those server computers experiences a failure,
- the **Cloud Backup and Disaster Recovery Option**, in which the customer's data on the server is backed up regularly to the Cloud in an encrypted form so that it can be recovered even if disaster strikes that results in (a) the destruction of the server, (b) irreparable damage to the server (for example, a flood) or (c) loss of the server (for example, theft).

This document sets out the types of failure and disaster that can occur and explains how the service and data will be restored following that type of failure or disaster. In doing so, the functioning of the High Availability option and the Cloud Backup and Disaster Recovery option are explained at a high level as both are important if an organisation wishes to enjoy a high degree of service continuity and minimal data loss in the event of a failure or disaster.

Service and Data Loss Scenarios and the Restoration Process

The most common service and data loss scenarios and the method by which service and data is restored for the Customer after the event are as follows:

What happens if a disk fails?

If a disk fails on a Cloud Managed Server without the HA option, the service will continue to operate as normal without interruption and the Customer will still have access to all its data. The data stored on an individual disk is fully mirrored in real-time onto a separate disk so that there is always an up-to-date copy of all data available. For servers with the HA option (that is, two servers operating as a cluster), data is continually replicated between the two nodes in the cluster. If a disk fails on one node, then the Virtual Machines (VMs) that were running on that node will start-up on the other, functioning node. No data is lost, but there will be a brief service interruption affecting some of the workloads on the VMs that are moving across – this typically takes 5-10 minutes. We immediately know about any disk failure through our Cloud Management Platform and we then initiate the replacement on the Customer's premises of the failed disk. This speed of replacement virtually eliminates any risk of a second disk failing before the first failed disk has been replaced and resilience re-established.

What happens if any other hardware component fails?

Servers with the HA option

If a hardware component failure occurs on one server, the other server will restart automatically and all of the functions of the server will be performed by the restarted server. The customer may notice a very short period of service loss in such a situation, typically no more than a few minutes. Zynstra detects such occurrences immediately and initiates replacement of the failed component. This speed of replacement virtually eliminates any risk of any further component failure on the server that is still functioning given that any such failure would cause a service loss until the failed component is replaced. When the failed component is replaced by HP, there will be a further short service loss as the two servers start to work together again as a cluster. This cluster restart process leads to approximately 15 minutes of service loss but can be scheduled to take place outside normal business hours, and should therefore have no impact on user productivity.

Servers without the HA option

This single server is not resilient to hardware component failures other than single disk failures which have been discussed already. If a hardware component fails, the server ceases to function entirely until the failed component has been replaced. Zynstra detects such occurrences immediately and initiates the replacement of the failed component. Once the failed component has been replaced, the server can be restarted immediately.

What happens if data becomes corrupt?

The corruption of data on a Cloud Managed Server is a rare event but may occur in extreme circumstances as a result of a defect in software running on the server. In such circumstances, the data can be restored to its state at the time of its most recent local backup. The mirrored copy of the corrupt data is of no benefit as the mirrored copy will itself contain the corruption. As a result, the only option is to revert to the most recent backup of the data which means that changes made to the data in question since that most recent backup will be lost.

The backup copy of the data from which the restoration ideally occurs is the most recent local backup of the data in question. In some circumstances however, the corruption may have found its way into that local backup of the data, in which case it is necessary to restore a backup of the data that is held in the Cloud (assuming of course the Customer has purchased the Cloud Backup and Recovery option). If the local backup of the data has become corrupt and the Customer has not purchased the Cloud Backup and Recovery option, it may not be possible to restore the data to any previous state and the Customer would need to create the data again from scratch or restore it from another external copy of the data that they may have created and retained.

We endeavour to restore data to its state prior to the corruption by the end of the next working day provided that the restoration can be performed using the local backup of the data. Should it be necessary to revert to a Cloud backup of the data to find a non-corrupt copy, this timescale may increase depending on the extent of the investigation that is required to find a non-corrupt copy of the data.

What happens if a disaster occurs on the customer's premises?

A disaster is defined as an event (such as theft, flood or fire) which renders a Cloud Managed Server unusable and/or inaccessible for an indeterminate period. Disaster recovery (DR) is the process of reinstating the server to its operational state prior to the occurrence of the disaster. The activities that happen when a disaster occurs depend on whether the customer has purchased the Cloud Backup and Disaster Recovery option. Nearly all Customers purchase this option because it enables the restoration the Customer's data and applications onto a new server following the disaster.

Servers without the Cloud Backup and Disaster Recovery option

If this option has not been purchased, we will only backup our standard software images to the Cloud; that is, none of the Customer's software images associated with any IaaS VMs will be backed up to the Cloud nor will any of the Customer's data. Following a disaster, we will replace the destroyed, lost or inaccessible server on the Customer's premises (or chosen alternative premises) with a new server of the same or a superior specification that has been pre-loaded with our standard software images (but none of the Customer's IaaS software images and none of their data). Responsibility for bearing the purchase cost of the replacement server hardware is described in our End User Licence Agreement.

Servers with the Cloud Backup and Disaster Recovery option

If this option has been purchased, the customer's data and all the software images on the server (the standard Zynstra software images as well as the images associated with any IaaS VMs) will be backed up regularly from the server to the Cloud. Following a disaster, we will replace the destroyed, lost or inaccessible server on the Customer's premises (or chosen alternative premises) with a new server of the same or a superior specification that has been pre-loaded with all of the standard software images, the software images associated with any IaaS VMs and all of the customer's data in the state it was in at the time of the commencement of the most recent backup of the data prior to the occurrence of the disaster. Responsibility for bearing the purchase cost of the replacement server hardware is described in our End User Licence Agreement.

With the Cloud Backup and Disaster Recovery option, we will also, immediately after the disaster and for an interim period whilst the server is replaced on the Customer's chosen premises, provide access in the Cloud for the Customer's users to their files that were previously stored on the server, to any Zynstra Managed Applications and their data that were included in the subscription and to any IaaS VMs. We will restore the IaaS VM software images in the Cloud and the Service Provider will be responsible for recreating the data store for any IaaS VMs from the backups that were taken of this data and retained in the Cloud. This access to what is effectively a 'Cloud instance' of the server will remain in place until the server has been restored on the Customer's chosen premises.

Backup Encryption Key Management

The Customer data that is backed up to the Cloud with the Cloud Backup and Disaster Recovery option is transferred to the Cloud and stored there in an encrypted form using RSA 2048 bit keys.

The keys themselves are held and maintained securely by us (both on the server and in the Cloud Management Platform) and can also be held and maintained by the Customer and the Service Provider if desired.

In general, we do not recommend the proliferation of the keys amongst multiple parties and/or individuals because of the risks of leakage that this can create. We also strongly recommend that we hold the keys as reliance on the Customer alone for access to the keys can create risk as the disaster which may require the use of those keys may destroy the Customer's premises.