ZYNSTRA TECHNICAL BRIEFING NOTE

Operational Responsibilities

Introduction

This document is intended for Service Providers and Customers and its purpose is to clarify both our responsibilities and those of the Service Provider once a Cloud Managed Server has been installed. In some cases, Service Providers may mutually agree with the Customer to delegate some of all of their server administration responsibilities to that Customer depending on both the Customer's technical expertise and on their desire to manage their own Cloud Managed Server.

More detailed information about the scope of the activities listed below can be found in the Technical Briefing Notes that are available on the Support Portal.

Support

- All Cloud Managed Servers are automatically monitored on a 24 x 7 basis from the Cloud Management Platform.
- Issues that are detected through automated monitoring within the standard services that are executed on every Cloud Managed Server can generally be automatically addressed/rectified and the relevant services restarted so that the impact on the availability of those services from the Customer's perspective is minimised.
- Our Support Team is responsible for supporting (addressing issues with, handling queries relating to and in some limited cases making configuration changes to) all the standard services (excluding industry standard tools such as those from Microsoft) being executed on the server.
- Our Support Team provides 3rd and 4th line support services to Service Providers during the hours published in the Support Portal. Service Providers interact directly with Customers from a support perspective and provide 1st and 2nd line support services. Our Support Team may in certain circumstances interact directly with Customers (and therefore provide all support services from 1st to 4th line) but this must be agreed in writing in advance on a case-by-case basis.
- Our Support Team does not support the physical infrastructure that may interact with each Cloud Managed Server including but not limited to the Customer's LAN and WAN connections and any other hardware or software that connects to the server (such as client PCs, mobile devices or the software running on those devices).
- The Service Provider is responsible for initially assessing any perceived technical issues that arise that may suggest that the Cloud Managed Server is not operating as documented and expected.
- After an initial technical assessment of a perceived issue by the Service Provider, and with evidence available to suggest that the issue may lie within the server and is our responsibility

based on the content of this document, the Service Provider should contact the Support Team through one of the documented support methods/channels.

Cloud Management Platform Access

- Our Support Team provides individual user accounts and OpenVPN certificates for the Cloud Management Platform to each Service Provider when they deploy their first Customer. This enables the Service Provider to connect to, monitor and configure all the Cloud Managed Servers being used by their Customers.

Networking and Security

- The Gateway Control Console provides a user interface that enables Service Providers to make the most common networking changes that are required such as configuring DHCP reservations, port forwards and creating additional OpenVPN client profiles. It also provides access to detailed reporting and network event information that Service Providers generally find valuable.
- A small set of network configuration changes can only be made by our Support Team, such as changing the LAN IP address or WAN IP address, as this information is controlled centrally by our Support Team because of the complexity of change or potential side-effects of change. Changes to these data items should therefore be requested of us by the Service Provider.

User Administration

- The User Control Console provides a user interface that enables Service Providers to inspect the health of the server at a very high level and to create and disable users and groups, reset passwords, etc.
- For most types of network deployments, Service Providers can alternatively carry out these tasks using the native Active Directory tools.
- Our Support Team does not provide any user or group administration tasks of the kinds mentioned above nor configuration any of the Microsoft based components installed within the Virtual Machines on the Cloud Managed Server.

Standard Infrastructure Services

- Direct access for Service Providers to the standard infrastructure services being executed on a Cloud Managed Server is not provided. This includes services such as monitoring, networking, security, logging and backup. These services are entirely 'locked down' and can only be accessed by our Support Team (other than where a user interface is specifically provided to enable the configuration of a particular service by the Service Provider or Customer).

Managed Services and Applications

- Each Cloud Managed Server includes certain services (such as the Domain Controller and File Server) and optionally additional applications (such as Exchange and Remote Desktop Services) that we fully manage (monitor, configure, patch, upgrade, back up).
- We are entirely responsible for the reliable and correct operation of these Managed Services and Applications, including the underlying Virtual Machines on which they reside, but the Service Provider or their Customer is responsible for the configuration of the Managed Services and Applications and for understanding and applying best practise in their configuration and use.

Infrastructure as a Service (IaaS) Virtual Machines

- Each Cloud Managed Server may contain one or more Virtual Machines with a pre-installed Operating System (OS) but with no pre-installed Applications or Services. These IaaS VMs can be requested by the Service Provider and are for the Service Provider or their Customer to install and execute the Customer's line-of-business applications.
- The Service Provider or Customer (as agreed between them) is responsible for the licensing, installation and maintenance of any software being executed in the Virtual Machine, including the troubleshooting and remedy of any issues that arise with any software (other than the OS) installed in the VM. This responsibility extends to any components not already enabled including but not limited to ADFS, web proxy, WSUS, WDS, and IPSEC VPN.
- We will not apply any OS patches or attempt to upgrade these VMs since it cannot assess the impact of such patches or upgrades on the third party software installed therein. Such patches and upgrades are therefore the responsibility of the Service Provider or their Customer.
- The Cloud Management Platform provides basic monitoring of these IaaS VMs and also provides mechanisms that will enable the backing up, locally and off-site, of the software images and data stored in these VMs. These mechanisms are documented in the Technical Briefing Notes.
- The Service Provider or their Customer is responsible for correctly using the documented mechanisms provided for local and cloud backup or for implementing alternative scripts to export backup copies of the software images and/or data.

Hardware Break-Fix

- We are responsible for arranging any on-site hardware repair or maintenance required to a Cloud Managed Server provided that the hardware has been provided as an integral part of the Service. Neither the Service Provider nor the Customer should carry out any hardware maintenance or power cycle the hardware without our prior approval to do so.