2017

IAAS Plan

PREPARED BY

DALE HURWITZ

[COMPANY NAME] | [Company address]

Contents

Preface

Sync has commissioned Gsolutions to provide planning consultancy for the implementation of IAAS facility to be utilized for secure and redundant data storage dedicated exclusively to services being conducted with Discovery.

While the primary focus is on the actual cloud infrastructure and implementation thereof it is imperative to consider the entire solution as external factors may have an impact.

The intention of this cloud server implementation plan is to ensure that any spend on the relevant infrastructure is effective and to ensure compliance with Discovery prior to implementation. This will ensure no wasteful expenditure and provide any relevant implementation partner a fixed specification for functionality that can be used to ensure the implementation is successful for all stakeholders.

As per the above the measurable outcome is a plan that can be used by any IAAS provider that has pre-approval from Discovery and is effective operationally for Sync.

Stakeholders

1. Sync – Johan Smal, responsible for intenal client governance and signoff
2. Gsolutions – responsible for the strategy and compiling the IAAS plan
3. Discovery – Responsible for ensuring compliance with standards and Specification approval.
4. IAAS Provider – TBC, post completion of IAAS plan approval from discovery.

Section 1: Requirements

IAAS Requirements

The IAAS provider selected for the implementation phase must be approved by Discovery post the completion of the Cloud Provider questionnaire.

IAAS Server Implementation Requirements

a. Server Hardening
b. Secure local and offsite data backups
c. Data must be encrypted at rest
d. Data secured in transit
e. AV, AM, IPS (Intrusion Prevention System)
f. Documentation

IAAS Network Requirements

a. IDS (Intrusion detection System)

Server Management Requirements

a. Patch Management
b. Backup Management
c. AV/AM/IPS Management

Enduser Device Managed Requirements

a. Patch Management

Office Network Requirements

a. UTM Appliance implementation

Productivity Suite Requirements

a. Secure transit of email
b. Email archiving
c. Security transit of data

Section 2: Planned Solution Specifications

IAAS Specifications

The IAAS provider selected for the implementation phase must be approved by Discovery post the completion of the Cloud Provider questionnaire.

The IAAS provider must have a full HA infrastructure implementation which includes redundant connectivity.

Sync being a small business currently, but with substantial growth expectation requires the IAAS provider to be able to offer a fixed cost solution that must be easily scalable. Initial requirements are:

- 4 vCPU's
- Windows Server Essentials
- 8GB RAM
- 150GB Diskspace Allocated as follows:
  - 50GB SSD for OS
  - 50GB Data Drive
  - 50GB Backup Drive
- 1 static IP
- Daily Snapshots

IAAS Server Implementation Requirements

a. Server Hardening - There are no set global standards for server hardening. Windows server has an analyzer tool which will be used. All recommendations of the tool will be complied with wherever relevant to the server roles implemented. Examples include but are not limited to user access control, stringent password policies, disabling any unnecessary services, etc.
b. Secure local and offsite data backups
   a. Local backups will be conducted to a separate disk allocated in the IAAS platform.
   b. A fully automated offsite data backup solution which includes data encryption will be implemented. The solution must include full DR capability.
   c. The Daily Snapshots will further enhance backup protection.
c. Data must be encrypted at rest – This will be done through the implementation of a comprehensive endpoint security software application.
d. Data secured in transit – Office 365 which includes the One Drive service will be integrated with AD and GP to ensure not only will all data will be secured in transit, but also internally based on user access permissions.

e. AV, AM, IPS (Intrusion Prevention System) - This will be done through the implementation of a comprehensive endpoint security software application.
f. Documentation – All configurations made will be documented in a password protected file.

IAAS Network Requirements

a. IDS (Intrusion detection System) – It is recommended that IDS be conducted through a virtual firewall attached to an IAAS platform. Default block all rules will be applied to all traffic except for specific services implemented.

Server Managed Services

To ensure compliance with the below requirements a Fully Managed Server SLA will be implemented. The relevant service must include the secure installation of a RMM tool to reduce cost and enforce policy as well as allow for transparency via reporting.

a. Patch Management
b. Backup Management
c. AV/AM/IPS Management

End-user Device Managed Services

To ensure compliance with the below requirements a pro-active Managed Endpoint service will be implemented. The relevant service must include the secure installation of a RMM tool to reduce cost and enforce policy as well as allow for transparency via reporting.

a. Patch Management

Office Network Requirements

a. UTM Appliance implementation – While it is not required in terms of compliance It is highly recommended. A good UTM appliance should allow for the following functionality:
    a. Content Filtering
    b. IPS
    c. VPN - IPSEC
    d. Bandwidth Management
    e. Connectivity Failover
    f. Anti-Virus
    g. AD Integration
    h. Reporting

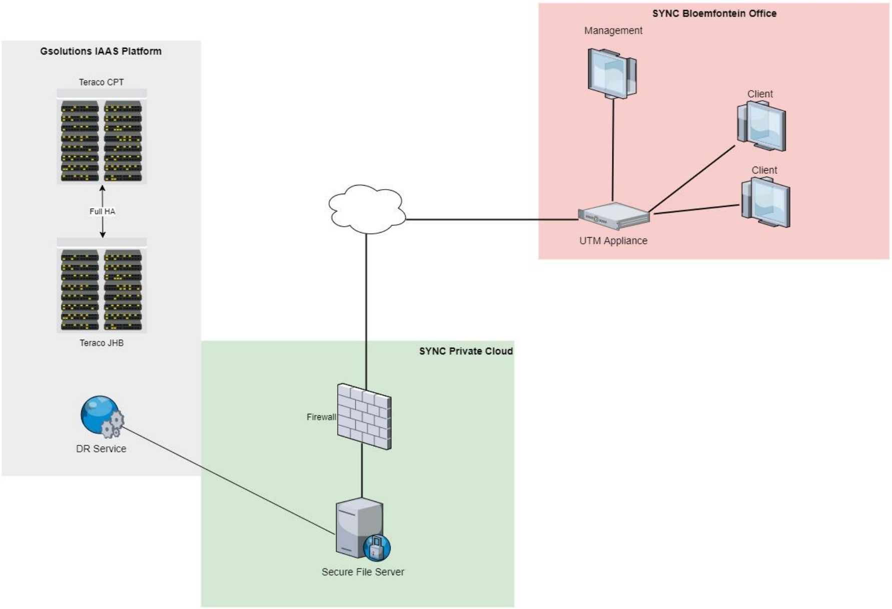
Productivity Suite Requirements

The productivity suite requirements below can all be met through the implementation of Office 365 Enterprise E1 package. It may be beneficial, but will not be essential to select the Office 365 Business Premium Package which include the Microsoft Office software suite.

a. Secure transit of email
b. Email archiving
c. Security transit of data

Section 3: Network Diagram

SYNC Network Diagram



Section 4: Summary

We thank you for reviewing the relevant. As with most IT Systems and solutions there are often many differing techniques and technologies to achieve the same result. It is always our philosophy to be collaborative and should you require / suggest any changes to the above we are open to engagement.