ZYNSTRA TECHNICAL BRIEFING NOTE

Microsoft Exchange

Introduction

Cloud Managed Servers can optionally include a fully managed implementation Microsoft's Exchange Server which is based on Exchange 2010 on running on Windows 2008 R2. This note explains some of the key considerations when using Microsoft Exchange as a Managed Application.

DNS Configuration

DNS CNAME and MX records should be configured to point to the new Microsoft Exchange server.

Consequently, access to the DNS record management interface of the domain hosting organization is required as part of the installation process. This is typically obtained through the administrative logon to a web portal of an existing domain hosting business. The domain hosting company must allow flexible end user management of DNS records, particularly CNAME and MX records.

Failure to provide this capability will prevent automatic mail client setup and in the worst case could prevent deployment of a local Microsoft Exchange server.

In addition to CNAME and MX records, it is necessary to configure the Reverse DNS Record, PTR, for on-site Microsoft Exchange implementations. This is required because if PTR is not set to the domain of the email system, many email providers will believe that the email server has been compromised to send spam and many email providers will reject a connection.

Microsoft Exchange SSL Certificates

Where a Cloud Managed Server is to host a local copy of Microsoft Exchange, the default self-signed Exchange SSL certificate is included. This is sufficient for core Microsoft Exchange functionality and allows communication to Microsoft Exchange services such as Outlook Web mail to be encrypted.

However, most client browsers and devices will display a warning when the initial connection is made since the SSL certificate cannot be independently verified. This warning can be safely ignored. However, if users are uncomfortable with this behaviour or if it is contrary to a customer's business policy, a trusted Certificate Authority (CA) signed SSL certificate can be purchased and installed on a Microsoft Exchange server. If a trusted third-party SSL certificate is installed, client browsers and devices will recognise and trust it as valid using a protocol build into a browser.

Advanced Features

In order to access advanced Exchange Server (MAPI) functionality, a Microsoft Outlook client is required on each edge device. Outlook Web Access (OWA) and Outlook Anywhere are supported. Outlook Anywhere is an optional Exchange feature that allows remote access to connect using RPC over HTTP that eliminates the need for a client VPN. A public CA issued SSL certificate is strongly recommended for OWA and mandatory for Outlook Anywhere.

OWA and Outlook Anywhere require an inbound port forward on port 443. In addition Outlook Anywhere requires that autodiscover CNAME DNS records needs to be configured.

Clients and Browsers

All common browsers (Internet Explorer, Safari, Firefox, Chrome) are supported. However, should a technical issue arise, the Customer Success Team will be guided by the recommendations of the browser manufacturer and/or Microsoft as to the remedial action that is required to cure the issue. This may require upgrade or downgrade of the existing browser or in some cases a recommendation to switch to a different, more compatible browser.

Microsoft supported versions of Microsoft Office on Microsoft supported Operating Systems are supported. Integration with compatible client software as defined by the manufacturer of the client software and Microsoft is supported.