Deploying a Mail System

When deploying an email system, there are certain things that must be considered, including domain registration & hosting, DNS records, security/encryption requirements, and more. This document will help guide you through the pre-deployment topics that must be considered before installing MDaemon.

Purchase and Register a Domain

You will need to have a domain name. There are several services from which you can purchase a domain name. One of the most popular is GoDaddy. You will also need to register your domain name with ICANN through a domain name registrar. Registration fees are typically between $10 and $40 per year. Registration gives you legal rights to the domain name for one year, and must be renewed annually. Registration allows you to be certain that you are the legal, registered owner of the domain. The world's largest domain name registrar is GoDaddy (www.godaddy.com).

SSL Certificates

SSL (Secure Sockets Layer) certificates are required for encrypted communications. You can purchase SSL certificates from GoDaddy, GlobalSign, or several other organizations. You an also generate your own self-signed SSL certificates in MDaemon via the **Security | Security Settings | SSL & TLS** configuration screen.

DNS

DNS (Domain Name System) is a system that translates domain names (such as example.com) into IP addresses that computers use to identify each other on the internet. DNS providers provide DNS servers, which are used to host DNS records that map domain names to IP addresses. DNS servers are normally managed by your Internet service provider (ISP), however, you can also host your own DNS server.

You will need the following DNS records: MX Record, A-Record, and PTR Record

MX Record - An MX record specifies the host names of mail servers that have been assigned to handle email for a domain name (example.com). A domain can have more than one MX record. MX records are prioritized by a priority number, with lower numbers designating a higher priority. Here is an example of an MX record:

```
example.com     MX preference = 5, mail exchanger = mail.server1.example.com
example.com     MX preference = 20, mail exchanger = mail.server2.example.com
example.com     MX preference = 40, mail exchanger = mail.server3.example.com
example.com     MX preference = 10, mail exchanger = mail.server4.example.com
example.com     MX preference = 30, mail exchanger = mail.server4.example.com
```

A Record - An A (address) record converts host names, such as mail.example.com, to IP addresses. Here is an example of an A record:

```
> set q=a
> mail.server1.example.com
Server: host1.example.com
Address: 10.10.10.10
Non-authoritative answer:
Name: abc-smtp-in.example.com
Address: 123.123.123.123
```

PTR Record - A PTR (pointer) record enables you to perform a reverse-DNS lookup on the IP addresses of external mail servers sending mail to your mail server. When a mail server performs a reverse lookup on an inbound connection, it queries the DNS sytem to see if you have a valid PTR record. The PTR record converts an IP address into an entry that ends in .in-addr.arpa, with the associated IP address added to the beginning of the string in reverse order. This entry then points back to its designated host name (mail.example.com). Many mail servers require a valid PTR record. Here is an example of a PTR record:

```
> set q=ptr
> 123.123.123.123
Server: host1.example.com
Address: 10.10.10.10
123.123.123.123.in-addr.arpa      name = ab-cd-efg.example.com
```

Create SPF, DKIM and DMARC Records

SPF Records - SPF (Sender Policy Framework) records are DNS records that specify IP addresses that are allowed to send mail on behalf of a domain. This helps to discourage spammers from spoofing (disguising the origin of an email message by forging the FROM header).

DKIM Records - DKIM (DomainKeys Identified Mail) is an open protocol for protecting email users against email address identity theft and email message content tampering. When an incoming message has been cryptographically signed, DKIM provides positive identification of the signer's identity along with an encrypted "hash" of the message content.

To configure and use DKIM:

- The system administrator creates a private/public key pair for the server and publishes the public key in the domain's domain name server.
- Using the private key, the sending server creates a signature for each outgoing message. The resulting signature data is stored in a "DKIM-Signature" header within the message.
- The receiving server obtains the signature from the "DKIM-Signature" header and verifies it using the signer's public key.

Instructions for configuring DKIM in MDaemon can be found in the following knowledge base article: www.altn.com/Support/KnowledgeBase/KnowledgeBaseResults/?Number=KBA-02577

DMARC Records - Domain-Based Message Authentication, Reporting and Conformance (DMARC) - DMARC is a specification designed to help reduce email message abuse, such as incoming spam and phishing messages that misrepresent their origins by forging the message's From: header. Domain owners publish DMARC records to the DNS system to inform receiving servers of their DMARC policy, which explains how they want those servers to handle messages that purport to be sent from their domain but cannot be authenticated as having actually come from it. Instructions for setting up your DMARC record can be found at www.dmarc.org.

Inbound Delivery Considerations

Direct SMTP Dellvery or Domain POP - You will need to determine how MDaemon will receive email. MDaemon can receive email via direct SMTP delivery using an MX record that points to the MDaemon server, or it can receive email using a catch-all address from an ISP using DomainPOP. When DomainPOP is used, the headers and body of email messages are parsed for data that would identify the message recipeint(s), such as names or embedded email addresses. MDaemon then distributes the messages to the local addresses that were parsed from the headers and message contents.

MultiPOP - Another method that MDaemon can use to receive mail is MultiPOP. MultiPOP is configured via the account editor for each account, and is used to download mail from an email address at the ISP to an individual account in MDaemon. Unlike DomainPOP, the headers are not parsed for intended recipients. Instead, all mail is downloaded directly to the acocunt that has been configured to use MultiPOP.

Outbound Delivery Considerations

In most cases, MDaemon would be configured to deliver mail directly to the receiving mail server. In some cases, however, it is necessary to deliver mail to another server (such as a mail server at your ISP). That server then delivers the message to the receiving server. In this setup, the server at the ISP is known as a smart host. You can configure a default smart host in MDaenon via the **Setup | Server Settings | Delivery** configuration screen. Per-domain smart hosts can be configured via **Setup | Domain Manager | (example.com) | Smart Host**.

Other Delivery Considerations

Many ISPs restrict access to port 25. If your ISP blocks access to port 25, then port 587, the MSA port, can be used for inbound traffic. Connections on port 587 require SMTP authentication, which can be enabled via the **Security Settings** menu in MDaemon. For outbound traffic, port 465, the SMTP SSL port, can be used.

Hardware Considerations

Hard drive selection is important for opitmal performance of your mail server. Things to consider are the total number of users whose email is being hosted on the server and the size of files stored on the server. Faster drives are recommended for better performance. On high-traffic servers, multiple hard drives can be used to improve performance.

> You can view a list of system recommendations based on the number of MDaemon users on the System Requirements page: www.altn.com/Products/MDaemon-Email-Server-Windows/System-Requirements/

Internet Connection

MDaemon works best with a dedicated internet connection and a static IP address. With a static IP address, the task of setting up your DNS records is much simpler. Your PTR and A records would only need to associate with one IP address and would not need to be changed unless your IP address changes. Many mail servers will not accept email from dynamic IP addresses.

It is possible to run MDaemon on a connection with a dynamic IP address. Three options for running MDaemon on a dynamic IP include DynDNS, ETRN/ATRN, and DomainPOP.

Dynamic DNS - A service provided by Dyn (www.dyn.com) that provides an internet domain name or URL that ponits to a dynamic (changing) IP address. This allows email messages addressed to your domain to reach your mail server at whatever IP address it has been assigned - without having to manaully update your DNS records.

The ETRN Command - An SMTP extension that signals a server storing mail for a particular domain that it is time to begin spooling the mail. ATRN is a message retrieval method that requires authentication before mail is dequeued. Using ATRN, the flow of data between MDaemon and the client domain is immediately reversed and the messages are de-spooled without having to make a new connection, unlike ETRN, which uses a separate connection after the ETRN command is sent.

DomainPOP - Can be used to download mail from a remote POP "catch-all" mailbox for redistribution to your users. Once collected, the messages are parsed for recipient data based on the message headers and contents and then placed in user mailboxes or the remote mail queue for MDaemon to deliver, just as if the messages had arrived at the server using conventional SMTP transactions.

Scanning for Spam and Viruses

We recommend enabling the spam filter in MDaemon. Navigate to the **Security | Spam Filter** menu, then make sure "Enable Spam Filter" is checked.

We also recommend installing SecurityPlus. SecurityPlus adds antivirus and Outbreak Protection to MDaemon. SecurityPlus will scan all inbound and outbound mail for spam, viruses, malware, and phishing attempts. You can learn more about SecurityPlus at: www.altn.com/Products/SecurityPlus-Antivirus-MDaemon/

Summary

The items discussed in this document will need to be considered before installing your mail server software. If you are ready to install your mail server software and you would like to use MDaemon, then you can visit our Literature page for quick-start and how-to guides to get your MDaemon mail server up and running.