

Problem # 02

1. ถ้านักศึกษาเป็นผู้ดูแลระบบขององค์กรที่นักศึกษาทำงานอยู่ นักศึกษาต้องตั้ง Mail Server ให้กับองค์กร นักศึกษามีวิธีในการพิจารณา Mail Server Software ที่มีการใช้งานทั่วไปในปัจจุบัน ที่เหมาะสมที่จะนำมาใช้ในการติดตั้ง Mail Server อย่างไรให้เหมาะสมที่สุดสำหรับองค์กร ตั้งแต่การเลือก Platform ที่ใช้ ตลอดจนเกณฑ์ต่างๆ ที่นักศึกษานำมาเป็นเกณฑ์ในการพิจารณา (มา 2 ตัวอย่าง)

ในการเลือก Mail Server Software นั้นมีหลักเกณฑ์หลากหลายอย่างที่จำเป็นต้องทำการพิจารณา แต่หลักเกณฑ์ที่สำคัญเป็นลำดับต้นๆที่จะนำมายกตัวอย่างนี้แบ่งได้เป็นสองหลักใหญ่ๆ

1.Capacity Planning/Scalability

ในการเลือกเซิร์ฟเวอร์อีเมลสำหรับการใช้งานนั้นขึ้นอยู่กับขนาดของจำนวนผู้ใช้เป็นสำคัญ ความสามารถในการด้าน Capacity และ Scalability จึงเป็นปัจจัยหลักในการเลือกใช้ Mail Server หากผู้ใช้มีเพียงไม่กี่ 100 Users Requirement ย่อมแตกต่างกับระบบที่มี 1000 Users ดังนั้น เพื่อประสิทธิภาพในการใช้งานและเข้าถึงของ Users ภายในองค์กร การเลือก Product ที่ตรงกับขนาดที่องค์กรต้องการและความเป็นไปได้ในการขยาย ข้อมจำกัดนี้ได้ในอนาคต ถือเป็นเรื่องสำคัญยิ่ง

2.Security/Hotfixes

ความปลอดภัยถือเป็นเรื่องสำคัญอย่างมากในการเลือกใช้ Mail Server ระบบจำเป็นต้องปลอดภัยจากช่องโหว่ ที่ผู้ไม่หวังดีอาจใช้เพื่อโจมตี ก่อให้เกิดความเสียหายต่อองค์กร เช่น Spammer และ Mail Server ที่ใช้ต้องมีการตอบสนองที่ไวต่อผู้ใช้ ในกรณีมีปัญหาด้านความปลอดภัยเกิดขึ้น ผู้ให้บริการจำเป็นต้องแจ้งถึงปัญหาและวิธีแก้ ต่อผู้ใช้ให้ได้ภายในเวลาอันรวดเร็ว

การเลือก Platform

เลือกให้เหมาะสมกับขนาดผู้ใช้ที่มี และความสามารถที่จะขยายและปรับปรุงให้เพียงพอต่อความต้องการในอนาคตได้

เลือกให้เหมาะสมกับความไวที่ต้องการขององค์กรในการใช้งาน

เลือกโดยคำนึงถึงค่าใช้จ่ายทั้งด้าน Hardware และ Software ที่ต้องใช้

เลือกโดยคำนึงถึงชนิดและจำนวนข้อมูลที่ต้องการใช้

ผมเลือก Mail Server มาสองตัวซึ่งประกอบด้วย

1.Exim

- ได้รับความนิยมสูง
- Support ทั้ง Linux/Unix, Windows, และ MacOS
- มีความสามารถในการ Customization และ Configuration สูง
- มี Log Mechanisms ถึง 3 ในการป้องกัน Email Spamming ได้แก่
- Main log, Panic log และ Reject log
- มี Pre-Build Support สำหรับระบบ Database ที่หลากหลาย เช่น MySQL,
- PostgreSQL, SQLite, Oracle DB และ Redis
- Cross-Platform Support

2.Postfix

- ใช้แพร่หลาย
- Open-Source
- มี Defense Mechanisms ที่ต่อสู้กับ Spambots and Malware ที่ดี
- Virtual Domain Support
- ประสิทธิภาพสูง Instance เดียวส่งเมลได้มากถึง 300 เมล
- Supports หลาย Databases เช่น MySQL, Memcache, SQLite, PostgreSQL, LDAP, CDB, and Berkely Database

2. ให้นักศึกษา Access เข้าเว็บไซต์หรือ Server ใดก็ได้ที่นักศึกษาสงใจ หลังจากนั้นให้ใช้ Wireshark ดักจับ Packet และทำการ Filter เฉพาะ DNS Protocol และทำการอธิบายหรือวิเคราะห์รายละเอียดต่างๆ ของ DNS ให้ครบถ้วน

The screenshot displays the Wireshark network protocol analyzer. The main pane shows a list of captured packets, with the DNS protocol selected. The packet list includes various DNS queries and responses from 192.168.1.1 to 192.168.1.1. The packet details pane on the right shows the structure of a DNS Standard query response for 'www.reddit.com'.

No.	Source	Destination	Protocol	Length	Info
51	192.168.1.3	192.168.1.1	DNS	74	Standard query 0xbd6b A www.reddit.com
53	192.168.1.3	192.168.1.1	DNS	74	Standard query 0x909a AAAA www.reddit.com
54	192.168.1.3	192.168.1.1	DNS	74	Standard query 0x909a AAAA www.reddit.com
56	192.168.1.1	192.168.1.3	DNS	125	Standard query response 0xbd6b A www.reddit.com CNAME reddit.map.fastly.net A 151.101.9.140
57	192.168.1.1	192.168.1.3	DNS	167	Standard query response 0x909a AAAA www.reddit.com CNAME reddit.map.fastly.net SOA ns1.fastly.net
59	192.168.1.1	192.168.1.3	DNS	167	Standard query response 0x909a AAAA www.reddit.com CNAME reddit.map.fastly.net SOA ns1.fastly.net
60	192.168.1.1	192.168.1.3	DNS	125	Standard query response 0xbd6b A www.reddit.com CNAME reddit.map.fastly.net A 151.101.9.140
66	192.168.1.3	192.168.1.1	DNS	80	Standard query 0x4f46 A substrate.office.com
67	192.168.1.3	192.168.1.1	DNS	80	Standard query 0x3a86 AAAA substrate.office.com
69	192.168.1.1	192.168.1.3	DNS	288	Standard query response 0x4f46 A substrate.office.com CNAME substrate.ms-acdc.office.com CNAME outlook.ha.office365.com A ...
70	192.168.1.1	192.168.1.3	DNS	371	Standard query response 0x3a86 AAAA substrate.office.com CNAME substrate.ms-acdc.office.com CNAME outlook.ha.office365.com ...
95	192.168.1.3	192.168.1.1	DNS	79	Standard query 0xe8a6 A teams.microsoft.com
96	192.168.1.3	192.168.1.1	DNS	79	Standard query 0x178a AAAA teams.microsoft.com
97	192.168.1.1	192.168.1.3	DNS	208	Standard query response 0xe8a6 A teams.microsoft.com CNAME teams.office.com CNAME teams-office-com.s-0005.s-msedge.net CNA...
98	192.168.1.1	192.168.1.3	DNS	220	Standard query response 0x178a AAAA teams.microsoft.com CNAME teams.office.com CNAME teams-office-com.s-0005.s-msedge.net ...
146	192.168.1.3	192.168.1.1	DNS	91	Standard query 0x07bc A teams.events.data.microsoft.com
147	192.168.1.3	192.168.1.1	DNS	91	Standard query 0x999f AAAA teams.events.data.microsoft.com
148	192.168.1.1	192.168.1.3	DNS	204	Standard query response 0x07bc A teams.events.data.microsoft.com CNAME teams-events-data.trafficmanager.net CNAME skype-dat...
149	192.168.1.1	192.168.1.3	DNS	248	Standard query response 0x999f AAAA teams.events.data.microsoft.com CNAME teams-events-data.trafficmanager.net CNAME skype...
151	192.168.1.3	192.168.1.1	DNS	86	Standard query 0x7f3f A config.teams.microsoft.com
152	192.168.1.3	192.168.1.1	DNS	86	Standard query 0xf75f AAAA config.teams.microsoft.com
153	192.168.1.1	192.168.1.3	DNS	269	Standard query response 0x7f3f A config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-teams.conf...
154	192.168.1.1	192.168.1.3	DNS	281	Standard query response 0xf75f AAAA config.teams.microsoft.com CNAME config.teams.trafficmanager.net CNAME s-0005-teams.co...
765	192.168.1.3	192.168.1.1	DNS	79	Standard query 0xcd1 A aefd.nelreports.net
766	192.168.1.3	192.168.1.1	DNS	79	Standard query 0x0f43 AAAA aefd.nelreports.net
795	192.168.1.1	192.168.1.3	DNS	194	Standard query response 0xcd1 A aefd.nelreports.net CNAME aefd.nelreports.net.akamaiized.net CNAME a1851.dscg2.akamai.net ...
803	192.168.1.3	192.168.1.1	DNS	79	Standard query 0x0f43 AAAA aefd.nelreports.net
917	192.168.1.1	192.168.1.3	DNS	212	Standard query response 0x0f43 AAAA aefd.nelreports.net CNAME aefd.nelreports.net.akamaiized.net CNAME a1851.dscg2.akamai.n...
918	192.168.1.1	192.168.1.3	DNS	212	Standard query response 0x0f43 AAAA aefd.nelreports.net CNAME aefd.nelreports.net.akamaiized.net CNAME a1851.dscg2.akamai.n...
2708	192.168.1.3	192.168.1.1	DNS	79	Standard query 0xf10d A www.redditmedia.com
2709	192.168.1.3	192.168.1.1	DNS	79	Standard query 0x6192 AAAA www.redditmedia.com
2738	192.168.1.1	192.168.1.3	DNS	130	Standard query response 0xf10d A www.redditmedia.com CNAME reddit.map.fastly.net A 151.101.9.140
2739	192.168.1.3	192.168.1.1	DNS	79	Standard query 0x6192 AAAA www.redditmedia.com
2753	192.168.1.1	192.168.1.3	DNS	172	Standard query response 0x6192 AAAA www.redditmedia.com CNAME reddit.map.fastly.net SOA ns1.fastly.net
2754	192.168.1.1	192.168.1.3	DNS	172	Standard query response 0x6192 AAAA www.redditmedia.com CNAME reddit.map.fastly.net SOA ns1.fastly.net
2765	192.168.1.3	192.168.1.1	DNS	74	Standard query 0x19f0 AAAA www.reddit.com
2803	192.168.1.1	192.168.1.3	DNS	167	Standard query response 0x19f0 AAAA www.reddit.com CNAME reddit.map.fastly.net SOA ns1.fastly.net
4427	192.168.1.3	192.168.1.1	DNS	78	Standard query 0xfaae A outlook.office.com
4428	192.168.1.3	192.168.1.1	DNS	78	Standard query 0x2c84 AAAA outlook.office.com
4429	192.168.1.1	192.168.1.3	DNS	320	Standard query response 0xfaae A outlook.office.com CNAME substrate.office.com CNAME substrate.ms-acdc.office.com CNAME ou...

Frame 50: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B2238ED6-8438-475C-8B40-ASA21CB06B27}, id 0
 Ethernet II, Src: Microsof_60:ee:63 (28:16:a8:60:ee:63), Dst: HuaweiTe_8e:0a:29 (c8:0c:c8:8e:0a:29)
 Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.1
 User Datagram Protocol, Src Port: 51820, Dst Port: 53

Domain Name System: Protocol

Packets: 4503 · Displayed: 44 (1.0%) · Dropped: 0 (0.0%)

Profile: Lab05

2:57 PM 2/10/2021

เลือก : <https://www.reddit.com/>

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns

No.	Time	Source	Destination	Protocol	Length	Info
50	5.036937	192.168.1.3	192.168.1.1	DNS	74	Standard query 0xbd6b A www.reddit.com
51	5.037248	192.168.1.3	192.168.1.1	DNS	74	Standard query 0x909a AAAA www.reddit.com
53	5.068177	192.168.1.3	192.168.1.1	DNS	74	Standard query 0x909a AAAA www.reddit.com
54	5.068202	192.168.1.3	192.168.1.1	DNS	74	Standard query 0xbd6b A www.reddit.com
56	5.081296	192.168.1.1	192.168.1.3	DNS	125	Standard query response 0xbd6b A www.reddit.com
57	5.081296	192.168.1.1	192.168.1.3	DNS	167	Standard query response 0x909a AAAA www.reddit.c
59	5.085869	192.168.1.1	192.168.1.3	DNS	167	Standard query response 0x909a AAAA www.reddit.c
60	5.104967	192.168.1.1	192.168.1.3	DNS	125	Standard query response 0xbd6b A www.reddit.com
66	5.367850	192.168.1.3	192.168.1.1	DNS	80	Standard query 0x4f46 A substrate.office.com

> Frame 56: 125 bytes on wire (1000 bits), 125 bytes captured (1000 bits) on interface \Device\NPF_{B2238ED6-8438-475C-8B40-A5A21C8D6}

> Ethernet II, Src: HuaweiTe_8e:0a:29 (c8:0c:c8:8e:0a:29), Dst: Microsof_60:ee:63 (28:16:a8:60:ee:63)

> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.3

> User Datagram Protocol, Src Port: 53, Dst Port: 51820

> Domain Name System (response)

Transaction ID: 0xbd6b **Transaction ID ไว้จับคู่ Query กับ Reply**

Flags: 0x8180 Standard query response, No error **A Flag Section**

1... .. = Response: Message is a response **บ่งบอกว่าเป็น Query (0) หรือ Response (1)**

.000 0... .. = Opcode: Standard query (0) **Opcode ระบุประเภทของ Query (0000 = Standard DNS Query)**

.... .0.. = Authoritative: Server is not an authority for domain

.... ..0. = Truncated: Message is not truncated **Truncated Response ระบุว่าข้อมูลถูกตัดทอนหรือไม่**

.... ...1 = Recursion desired: Do query recursively **Recursion Desired ,Recursion Available**

....1... .. = Recursion available: Server can do recursive queries **ระบุว่าเป็น Iterative หรือ Recursion**

....0.. = Z: reserved (0) **Z Reserved bits**

....0. = Answer authenticated: Answer/authority portion was not authenticated by the server **ระบุว่าเป็น Authenticative หรือไม่**

....0 = Non-authenticated data: Unacceptable

....0000 = Reply code: No error (0) **RCode ระบุสถานะของ Reply**

Questions: 1 **Question Count ระบุรายการข้อมูลใน Question Section ขนาด 2 Byte**

Answer RRs: 2 **Answer Record Count ระบุรายการข้อมูลใน Reply Section ขนาด 2 Byte**

Authority RRs: 0 **Authority Record Count ระบุรายการข้อมูลใน Authority Section ขนาด 2 Byte**

Additional RRs: 0 **Additional Record Count ระบุรายการข้อมูลใน Additional Section ขนาด 2 Byte**

> Queries **QName QType QClass**

> www.reddit.com: type A, class IN

> Answers **Name Type Class CName**

> www.reddit.com: type CNAME, class IN, cname reddit.map.fastly.net

> reddit.map.fastly.net: type A, class IN, addr 151.101.9.140

[Request In: 50]

[Time: 0.044359000 seconds]

Queries : QName = ระบุชื่อ Question ,QType = ระบุชนิด Question 0x0001 เป็น Host Address Records

,QClass = ระบุ Class ของ Question ที่เรียก ปกติเป็น 0x0001 คือ Internet

Answer : Name = ระบุชื่อ Answer ,Type = ระบุชนิด Answer 0x0001 เป็น Records

0x0005 เป็น CName ,Class = ระบุ Class ของ Answer ,Time to live เวลาที่ข้อมูลจะเก็บเป็น Cache หน่วยเป็นวินาที

Data length ความยาวของข้อมูล ,CName ระบุ Canonical Names

This is a response to the DNS query in this frame (dns.response_to) | Packets: 4503 · Displayed: 44 (1.0%) · Dropped: 0 (0.0%) | Profile: Lab05

จากรูปนี้จะเป็น Standard Query Response ที่มี Transaction ID เป็น 0xbd6b Opcode เป็นการค้นหาแบบปกติ ไม่มีการตัดทอนข้อมูล เป็นการค้นหาแบบ Recursion จัดเก็บใน Resource Record ประเภท A และมี CName ชื่อจริงเป็น reddit.map.fastly.net