文件版本修正履歷表

|  |  |  |
| --- | --- | --- |
| 版次 | 變更項目 | 變更日期 |
| 1.0 | 第一版 | 2015.05.22 |
| 1.1 | 第二版 | 2016.06.07 |
| 1.2 | 第三版 | 2017.05.31 |

1. 簡介(Introduction)  
   (專案目的、專案範圍、測試目標)

一個基於Fed-MR的通用型協同式P2P殭屍網路偵測系統，專案的主要目的在於聯合多個區域雲並搭配聯邦式MapReduce運算執行聯合分析，用來偵測各式殭屍網路活動，並保證各區域雲資料之隱私性。

本次測試將依據本系統下列各項子系統，進行測試：

* 過濾階段子系統(FilterPhase)
* 群聚子系統(Group)
* 建圖子系統(Graph)
* SimRank子系統(SimRank)
  1. 子系統
     1. 測試目的(Scope of Testing)

本文件主要是在網路環境中建置P2P殭屍網路偵測系統(P2P Botnet Detection)，以下簡稱本系統)的測試計畫。在確認系統整合和結合聯邦式MapReduce運算架構(Federative MapReduce)前，必須先確認所有的設計元件均可正確的輸出，在此我們著重於子系統驗證(Subsystem Validation)及整合系統測試(Integration Test)。本文件內容將依據系統需求規格書與系統設計文件，描述關於整合測試的相關計畫與內容。並希望透過此文件之描述與實踐，達到順利進行測試工作之目的。

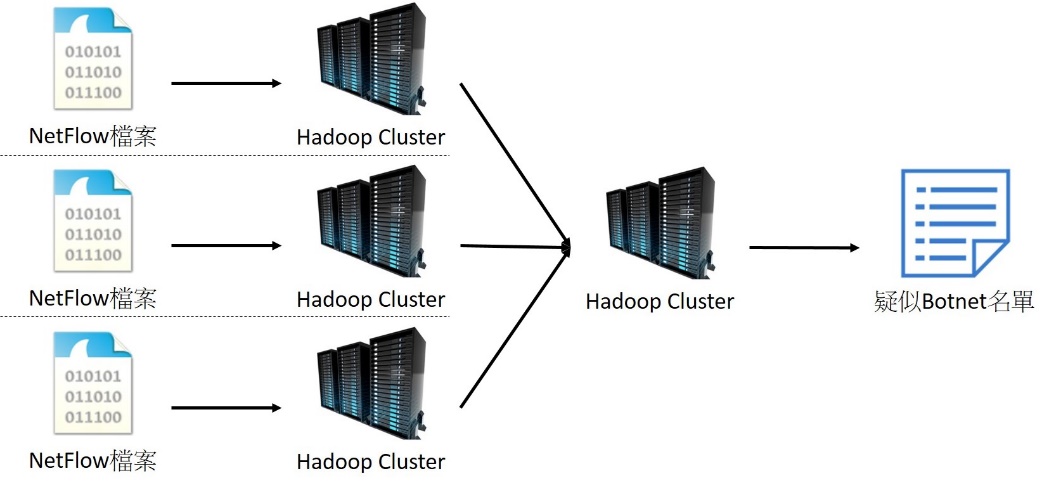
* + 1. 接受準則(Acceptance Criteria)

本測試計畫需要滿足下列的測試接受準則：

* 本系統需要對所有列為必要(Critical、Important、Desirable)之需求作完整測試。
* 測試程序需要依照本測試計畫所訂定的程序進行，所有測試結果需要能符合預期測試結果方能接受。

1. 測試環境(Testing Environment)
   1. 子系統
      1. 運行環境(Operational Environment)

對於本系統進行系統測試階段之環境說明，請參考測試環境圖所示：



* + 1. 硬體規格(Hardware Specification)

依據測試環境圖內容，關於測試環境所需的硬體規格說明，如下列所示：

* + - * 伺服器：Intel® Xeon® E3-1230 v3 @ 3.30GHz，256KiB Level 1，1MiB Level 2，8MiB Level 3快取，1600 MHz前端匯流排，記憶體為16GiB，硬碟空間1TB，網路卡Intel® I210 Gigabit Network Connection。伺服器數量6部(1群2部，共3群)，網路速度100Mbps。
    1. 軟體規格(Software Specification)

依據測試環境圖內容，關於測試環境所需的軟體規格說明，如下列所示：

* 作業系統：   
  伺服器需配置Ubuntu 14.04。  
  個人電腦需配置Microsoft Windows 10作業系統。
* JAVA版本：   
  JAVA Runtime Environment 8 (JRE 8)
* Hadoop版本：

2.7.2

* + 1. 測試資料來源(Test Data Source)

關於測試期間所需的測試資料來源及數量 ，說明如下：(文字或表格)

1. 國家高速網路中心提供中正網路流量Log – 105/06/01~105/07/31
2. 國家高速網路中心提供成大網路流量Log – 105/06/01~105/07/31
3. 測試時程、程序和責任(Testing Schedule, Procedure, and Responsibility)
   1. 子系統
      1. 測試時程(Testing Schedule)

* 時程
  + 各子系統之內部元件整合測試 (Module Test) (105/9/14~106/4/8)
  + P2P Botnet Detection系統整合測試 (Integration Test) (106/4/13~106/4/29)
  + P2P Botnet Detection系統接受度測試 (Acceptance Test) (106/5/4~106/5/13)
* 查核點
  + 各子系統之內部元件整合測試(106/4/11)
  + P2P Botnet Detection系統整合測試(106/5/2)
  + P2P Botnet Detection系統接受度測試(106/5/16)
    1. 測試程序(Testing Procedure)
       1. 子系統驗證(Subsystem Validation)

針對P2P殭屍網路偵測演算法各階段驗證，以期達到有效殭屍網路偵測模組

* + - 1. 整合測試(Integration Testing) (Incremental Testing)

(整合測試圖)

本系統的測試流程利用腳本化進行測試，透過自動化的程序，僅需更改少許的腳本參數，便可重複且有效率的執行。

系統整合測試之次序為：IT1→IT2→IT3→IT4→IT5→IT6

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IT1 | IT2 | IT3 | IT4 | IT5 | IT6 |
| FilterPhase | Group1  FilterPhase | Group2  Group1  FilterPhase | Group3  Group2  Group1  FilterPhase | Group3  Graph  Group2  Group1  FilterPhase | Graph  Graph  SimRank  Group3  3Graph  Group2  Group1  FilterPhase |

圖二 整合系統測試

* + - 1. 接受測試(Acceptance Testing)(Alpha Testing)

本系統須達到需求規格書所列之所有功能，如下表所示：

|  |  |  |
| --- | --- | --- |
| 需求編號 | 優先順序 | 需求描述 |
| TAF-DIC-001 | 1 | 通用型P2P殭屍網路偵測演算法，各階段程式採用MapReduce運算框架為基礎，採用Java 為開發語言。 |
| TAF-DIC-002 | 1 | 雲端聯合運算架構Fed-MR：修改Hadoop原始碼Java程式 |

針對本系統之需求，本系統設計時期之使用案例(Use Case)如下圖所示，本系統須達成使用案例所列之所有功能。

Botnet Detection



FilterPhase

Group1

系統操作員

Group2

Group3

Graph

SimRank

Result

圖三 Botnet Detection系統使用案例圖

圖四 系統接受度測試

* + 1. 人員職責分配(Personnel and Responsibility)

本系統之測試人員姓名及職責如下列所示。

表一 人員職責分配表

|  |  |
| --- | --- |
| Testing Activities | Personnel |
| IT1 | 卓峰民 |
| IT2 | 卓峰民 |
| IT3 | 歐奇隴 |
| IT4 | 歐奇隴 |
| IT5 | 滕韋呈 |
| IT6 | 滕韋呈 |
| AT1 | 卓峰民 |
| AT2 | 卓峰民 |
| AT3 | 歐奇隴 |
| AT4 | 歐奇隴 |
| AT5 | 滕韋呈 |
| AT6 | 滕韋呈 |

1. 測試案例(Test Case)
   1. 子系統
      1. 整合測試案例(Integration Testing Cases)(Incremental testing)
         1. IT1 Test Case -將混合後的Log做第一階段白名單過濾、DNS過濾以及濾出P2P行為流量。

|  |  |
| --- | --- |
| 輸入 | NetFlow 格式的網路流量log |
| 輸出 | 含有P2P行為流量之Log |
| 步驟 | 將網路流量Log當做FilterPhase指令的輸入，會將非P2P行為的流量濾掉，輸出具有P2P行為流量的Log |
| 預期結果 | 輸出中僅含有P2P行為的Log |

* + - 1. IT2 Test Case -將具有相似行為之Session群聚在一起。

|  |  |
| --- | --- |
| 輸入 | IT1 Test Case之輸出Log |
| 輸出 | 已分成很多群的流量行為之Log |
| 步驟 | 將IT1 Test Case的輸出Log當做Level 1 Group指令的輸入，依照相同來源IP，目的地IP以及通訊協定找出Session，並利用特徵將相似行為之Session群聚，最後算出其特徵向量平均並輸出 |
| 預期結果 | 輸出Level 1分群(Group)後的Log |

* + - 1. IT3 Test Case -將具有相似行為的相同來源IP之流量群聚在一起。

|  |  |
| --- | --- |
| 輸入 | IT2 Test Case之輸出Log |
| 輸出 | 已分成很多群的流量行為之Log |
| 步驟 | 將IT2 Test Case的輸出Log當做Level 2 Group指令的輸入，根據相同來源IP到不同目的IP的行為進行群聚，會輸出成很多群的流量行為之Log |
| 預期結果 | 輸出Level 2分群(Group)後的Log |

* + - 1. IT4 Test Case -將具有相似行為之P2P流量群聚在一起。

|  |  |
| --- | --- |
| 輸入 | IT3 Test Case之輸出Log |
| 輸出 | 已分成很多群的流量行為之Log |
| 步驟 | 將IT3 Test Case的輸出Log當做Level 3 Group指令的輸入，依照不同來源IP的相似行為進行群聚，會輸出成很多群的流量行為之Log |
| 預期結果 | 輸出Level 3分群(Group)後的Log |

* + - 1. IT5 Test Case –進行跨叢集比較行為，若有相似行為，則在IP之間建立邊(Edge)，形成Graph。

|  |  |
| --- | --- |
| 輸入 | 所有叢集IT4 Test Case之輸出Log |
| 輸出 | 以Adjacency list來表示的graph資訊 |
| 步驟 | 將所有叢集IT4 Test Case的輸出Log當做Graph指令的輸入，會輸出以Adjacency list來表示的graph資訊 |
| 預期結果 | 輸出建圖(Graph)後的Adjacency list |

* + - 1. IT6 Test Case -利用SimRank概念"如果兩個對象和被其相似的對象所引用，那麼這兩個對象也相似"，將共同相似度的IP找出來並標記為suspicious botnet。

|  |  |
| --- | --- |
| 輸入 | IT5 Test Case之輸出Log |
| 輸出 | 可疑的Botnet list |
| 步驟 | 將IT5 Test Case的輸出Adjacency list當做SimRank指令的輸入，經過5次SimRank後，會產生一個疑似Botnet的名單 |
| 預期結果 | 輸出疑似Botnet的名單 (IP list) |

4.1.2 接受測試案例(Acceptance Testing Cases)(alpha testing)

因我們進行測試時即是在User Site使用Develop Site的環境，因此IT與AT是同時進行的測試的。因此完成測試4.1.1之內容同時也完成AT測試。

1. 測試結果與分析(Test Result and Analysis)
   1. 子系統
      1. 整合子系統測試案例(Integration Testing Cases)

表二 整合子系統測試案例

|  |  |  |
| --- | --- | --- |
| Test Case # | Results (PASS/FAIL) | Comment |
| IT1 | PASS |  |
| IT2 | PASS |  |
| IT3 | PASS |  |
| IT4 | PASS |  |
| IT5 | PASS |  |
| IT6 | PASS |  |

* + 1. 接受測試案例(Acceptance Testing Cases)

表三 接受測試案例

|  |  |  |
| --- | --- | --- |
| Test Case # | Results (PASS/FAIL) | Comment |
| AT1 | PASS |  |
| AT2 | PASS |  |
| AT3 | PASS |  |
| AT4 | PASS |  |
| AT5 | PASS |  |
| AT6 | PASS |  |

Appendix A：Traceability

1. 子計畫
   1. 子系統 vs. 測試案例(Subsystem vs. Test Cases)

表四 Subsystems vs. Test Cases Traceability Table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Subsystems  Test Cases | FilterPhase | Group1 | Group2 | Group3 | Graph | SimRank |
| IT1 | V |  |  |  |  |  |
| IT2 |  | V |  |  |  |  |
| IT3 |  |  | V |  |  |  |
| IT4 |  |  |  | V |  |  |
| IT5 |  |  |  |  | V |  |
| IT6 |  |  |  |  |  | V |

* 1. 求 vs. 測試案例(Requirements vs. Test Cases)

表五 Requirements vs. Test Cases Traceability Table

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test Cases  Requirements | IT1 | IT2 | IT3 | IT4 | IT5 | IT6 |
| TAF-DIC-001 | V | V | V | V | V | V |
| TAF-DIC-002 | V | V | V | V | V | V |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Test Cases  Requirements | AT1 | AT2 | AT3 | AT4 | AT5 | AT6 |
| TAF-DIC-001 | V | V | V | V | V | V |
| TAF-DIC-002 | V | V | V | V | V | V |

Appendix B：Glossary

(名詞) (解釋)

Fed-MR Federated MapReduce 一種軟體框架可聯合數個Hadoop叢集進行跨叢集的MapReduce程式運算，並自動彙整結果。

SimRank SimRank相似度的核心思想為：如果兩個對象和被其相似的對象所引用（即它們有相似的入鄰邊結構），那麼這兩個對象也相似。

Appendix C：Reference