ADT CAPS 뷰가드 신호누락 이슈 작업계획서

내용 : 뷰가드 DDNS 신호누락 현황 파악 작업 계획서

2021년 09/09(목)실행

영상보안개발팀

2021

내용

[1. 작업 개요 2](#_Toc76556066)

[1.1. 적용 사유 2](#_Toc76556067)

[1.2. 작업 요약 2](#_Toc76556068)

[1.2.1. 녹화기에서의 DDNS TCP 통신의 로킹 2](#_Toc76556069)

[1.2.2. DDNS DB 업데이트 유무 확인 2](#_Toc76556070)

[1.2.3. 분석서버로의 TCP 통신의 로킹 2](#_Toc76556071)

[1.3. 작업 일정 및 영향 범위 2](#_Toc76556073)

[1.4. 작업자 명단 2](#_Toc76556074)

[2. 작업 상세 내용 3](#_Toc76556075)

[2.1. 작업 공지 3](#_Toc76556076)

[2.2. 대상 서버 3](#_Toc76556077)

[2.3. 작업 절차 3](#_Toc76556078)

[2.3.1. 작업절차 간략 정리 2](#_Toc76556071)

[2.3.2. TCP Dump 로킹 세부사항 2](#_Toc76556071)

[2.3.3. DB 업데이트 유무 세부사항 2](#_Toc76556071)

[2.3.4. 수집되는 로그 2](#_Toc76556071)

[2.3.5. 로그 분석 2](#_Toc76556071)

[3. 사전 Test 결과 3](#_Toc76556079)

[3.1. 기능 테스트 3](#_Toc76556080)

[3.1.1. 기능 Test 결과: TCP DUMP 및 DB 업데이트 확인 유무 프로그램 4](#_Toc76556081)

[3.2. 부하 테스트 4](#_Toc76556082)

[3.3. 구 버전 호환 테스트 5](#_Toc76556083)

[4. 원상복구 계획 5](#_Toc76556084)

[4.1. 테스트 및 모니터링 결과 5](#_Toc76556085)

[4.2. 원상 복구 계획 및 소요 시간 5](#_Toc76556086)

[4.2.1. 원상 복구 시점 5](#_Toc76556087)

[4.2.2. 서비스 원상 복구 5](#_Toc76556088)

1. 작업 개요
   1. 적용 사유

* **뷰가드** **DDNS 서버의 신호누락 현상의 원인 규명과 대첵마련을 위한 로킹**
  1. 작업 요약
     1. 녹화기에서의 DDNS TCP 통신의 로킹
* 녹화기에서 보내는(Input) DDNS1번서버 TCP 통신의 로킹
* 녹화기에서 보내는(Input) DDNS2번서버 TCP 통신의 로킹
* DDNS에서 분석서버로 보내는 TCP 통신의 로킹
  + 1. DDNS DB 업데이트 유무 확인
* 녹화기에서 상태정보값을 DB 업데이트에 유무 확인
  + 1. 분석서버로의 TCP 통신의 로킹
* DDNS에서 분석서버로 보내는(Output) TCP 통신의 로킹
  1. 작업 일정 및 영향 범위
* 뷰가드 DDNS : 2021년 09 09(목) 00:00 ~ 11(토) 23:59
  + - * 1. 서버 작업 일정 및 영향범위

| **시작** | **종료** | **영향범위** | **Down Time** | **영향도** |
| --- | --- | --- | --- | --- |
| 9월 08일  17:00 | 9월 12일  12:00 | DDNS서버의 TCP, DB 로킹 | 0분 | 없음 |

* 1. 작업자 명단
     + - 1. 작업자 명단

| **소속** | **분야** | **성명** | **연락처** |
| --- | --- | --- | --- |
| ADT캡스 | 미정 | 미정 | 미정 |
| ADT캡스 | 미정 | 미정 | 미정 |
| 포커스 | Agent 설치 | 박용준 | 010-2785-5163 |
| 포커스 | 모니터링 | 김영주 | 010-2678-6506 |

1. 작업 상세 내용
   1. 작업 공지

* 미정
  1. 대상 서버
     + - 1. 작업 대상 및 작업 서버 식별

| **작업 대상** | **작업 서버 명** | **IP Address** | **내용** | **수량** |
| --- | --- | --- | --- | --- |
| DDNS 2번 | VGDD2-VML-DDN01 | 10.201.2.5 | TCP, DB 로킹 | 1 |
| DDNS 2번 | VGDD2-VML-DDN02 | 10.202.1.4 | TCP, DB 로킹 | 1 |

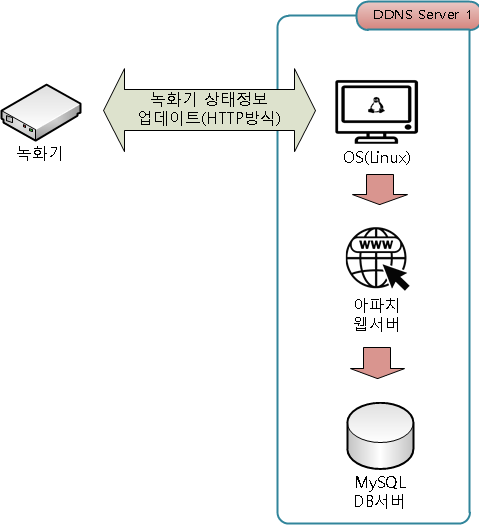
* 1. 작업 절차
     1. 작업절차 간략 정리
        + 1. DDNS 로킹 내용 정리

| **시작** | **종료** | **작업 내용** | **비고** |
| --- | --- | --- | --- |
| 9월 07일 | 9월 08일 | Focus에서 특정녹화기 한대를 준비 후  와이어샤크로 DDNS 업데이트 TCP 기록을 한다. |  |
| 9월 08일  17:00 | 18:00 | DDNS 1~2 서버의 TCP 로킹 준비작업 및 시작 |  |
| 9월 08일  18:00 | 19:00 | DDNS 1 서버의 DB 업데이트 로킹 준비작업 및 시작 |  |
| 9월 08일  20:00 | 9월 12일  12:00 | DDBS TCP, DB 로그 수집 진행 |  |
| 9월 12일  12:00 | 9월 12일  12:10 | DDNS 1~2 서버의 TCP 로킹 중지 |  |
| 9월 12일  12:10 | 9월 12일  12:20 | DDNS 1 서버의 DB 업데이트 로킹 중지 |  |
| 9월 13일 | 9월 15일 | 수집된 로그정보 분석 |  |
| 9월 16일 | 9월 16일 | 분석된 로그정보로 원인 규명 |  |

* 작업 간략 설명

1. 신호누락 로그 수집을 위해 Foucs에서 특정 녹화기 1대를 와이어사크로 TCP 로그수집을 한다.
2. DDNS서버에서는 Focus에 설치된 특정 녹화기의 맥만 TCP Dump를 수집한다.
3. DB 업데이트 확인을 위해 특정 녹화기의 맥만 DB업데이트 여부를 수집한다.
4. 이후 수집된 로그를 바탕으로 분석한다.
5. 분석된 로그로 원인 파악을 한다.
   * 1. TCP Dump 로킹 세부사항

* Loging 범위



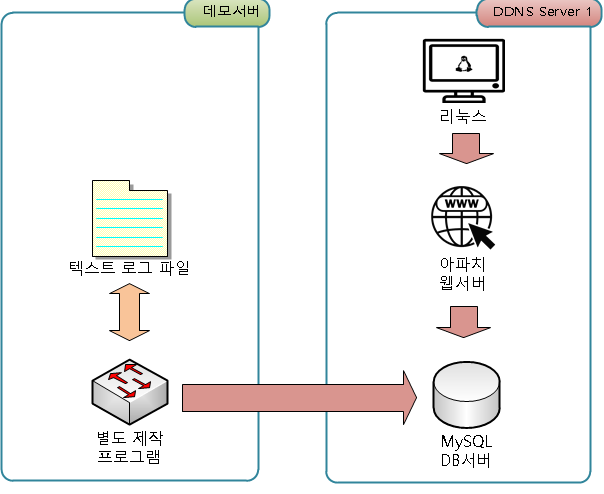
TPC 패킷 덤프

* OS 사용 명령어

tcpdump host 123.212.225.125 and tcp port 10000 > 001C84364E47.log

Linuix상에서의 tcpdump 명령어 (서비스의 영향없음)

* OS 사용 명령어
  + 1. DB 업데이트 유무 세부사항
* 작동구성



DB 업데이트 확인용 프로그램 재작.

1분마다 한번씩 DB에 접속하여 녹화기의 업데이트 내용을 확인하고 Text파일로 로그를 기록한다.

* 작동 방법

1. ADT 뷰가드 데모서버의 별도의 제작된 프로그램을 설치한다.
2. 데모서버의 설치된 프로그램은 1분에 한번씩 DB에 접속하여 특정 녹화기의 업데이트 내용만 쿼리하여 업데이트 결과를 텍스트 파일로 저장한다.

* 데모서버를 이용하는 이유

운영서버의 DB설정(트리거 및 프로시져 생성) 및 소스 변경(DDNS 소스의 수정) 없이 즉.

운영서버의 변경이 전혀 없이 DB의 업데이트를 확인하기 위해 데모서버에서 접속하는 방식으로 작동합니다.

* + 1. 수집되는 로그
* 녹화기 펌웨어의 업데이트 성공, 실패 여부 로그
* 녹화기의 통신 TCP 와이어사크 로그
* DDNS 1번 서버의 TCP Dump 로그
* DDNS 2번 서버의 TCP Dump 로그
* DB의 업데이트 유무 로그
  + 1. 로그 분석
* 작동별 로그

업데이트된 DB로그

패킷수신로그

패킷출발로그



* 녹화기에서 출발한 패킷이 정상적으로 서버의 도착하고 DB에 업데이트가 되었는지 여부를 확인

1. 사전 Test 결과
   1. 기능 테스트
      1. 기능 Test 결과: TCP Dump 및 DB 업데이트 확인 유무 프로그램

| **주요 기능** | **결과** |
| --- | --- |
| Linux상 tcpdump 작동상테 여부 | PASS |
| DB 접속하여 업데이트 유무 프로그램 작동상태 여부 | PASS |

* 1. 부하 테스트
* 해당없음
  1. 구 버전 호환 테스트
* 해당사항없음

1. 원상복구 계획
   1. 테스트 및 모니터링 결과

해당사항없음

* 1. 원상 복구 계획 및 소요 시간
     1. 원상 복구 시점
* DDNS 서버의 이상발생 시점
  + 1. 서비스 원상 복구
* 신규 소스 삭제, 기존 운용 소스 원복

| **작업 내용** | DDNS TCP DUMP 작업 종료 |
| --- | --- |
| DB 업데이트 수집 작업 종료 |
| **예상소요시간** | 5분 |