**KT AICC 공공지자체 고객 포털 접속 지연 장애**

kt ds Cloud사업본부 Cloud운영담당 플랫폼Tech팀 (2025.03.20)

* 장애 기본 정보

|  |  |
| --- | --- |
| 시스템명 | KT AICC 공공지자체(PG0887) |
| 서비스 개요 | 공공지자체(B2G) 대상 AICC(Artificial Intelligent Contact Center)서비스로 음성인식, 음성합성, 자연어처리, 텍스트분석 등 AI기술을 적용한 인공지능 고객센터 서비스 |
| 장애 전파 등급 | 3등급 |
| 인시던트 ID | INM25032031711 |
| 상황반장 | KT IT Ops본부 AX서비스플랫폼담당 AX플랫폼개발팀 박정진 팀장 |
| 복구반장 | kt ds Cloud사업본부 Cloud운영담당 플랫폼Tech팀 강민구 팀장 |
| 운영부서 | kt ds 플랫폼AX사업본부 AI/미디어사업담당 AI구독서비스팀 |
| 사용자 | KT AICC 공공지자체 |

* 장애 조치 개요

|  |  |
| --- | --- |
| 발생 시간 | 2025년 03월 20일 10:45 |
| 인지 시간 | 2025년 03월 20일 10:45 (인지경로: 관제(Signal)) |
| 복구 시간 | 2025년 03월 20일 15:20 (275분) |

* 장애 분석 결과
* 장애 현상/내용

- 고객 포털 로그인 후, 고객사별 포털 화면 지연 현상 발생

* 장애 파급영향

- 고객 포털 사용 불가

※ 보이스봇 서비스 영향 없음

- VOC 12 건 A'cen cloud SO센터 접수기준

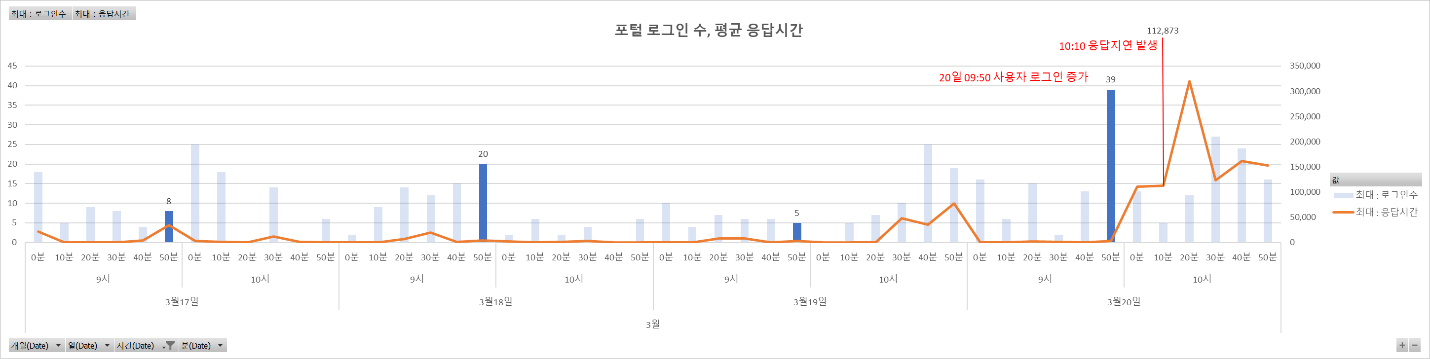
※ 전체 54개 고객사 중, 12개 고객사에서 VOC 발생

* 장애 근본 원인

- 09:50경부터 사용자 로그인이 서서히 증가 따라 10:10분경 Entropy Pool 소진되어 응답 시간 지연

※ Entropy Pool : 시스템 난수 데이터 저장소이며, 시스템의 입출력 동작에 따라 자동으로 채워지는 역할

※ java에서 Security.Random 사용시 /dev/random 참조하며, 난수가 부족할 경우 채워질 때까지 지연(응답시간 최고 300초까지 지연)

- 10:18 IT관제센터를 통하여 지연 현상 공유되어 AO 담당자 서비스 점검 및 원인 분석을 위하여 지속 적인 서비스 호출로 Entropy Pool 충전 시간이 없어 지연 현상이 지속 유지됨

[발생경위 및 조치 지연사유]

- 3/15(토) AICC OS Upgrade 고도화 사업(~6/30일) 1차 B/G 고도화 진행하였고, Security.Random함수

사용시 VM 에서는 RNGD Pkg 가 필수로 필요함을 미인지

※ RNGD : Java에서 특정 Class를 사용하여 사용자 로그인 암호 호출 시, Entropy Pool에 난수 공급 별첨#2) RNGD 동작 방식

- Security.Random 사용시 시스템 커널상의 entropy 참조를 알지 못하였고, kt cloud 표준 Rocky OS

RNGD 패키지가 미 제공(현재 ITO 315대 특이사항 없음)되어, 사전 파악이 미흡

- 고도화 이후 기능테스트를 진행하였으나, entropy의 소진할 만큼의 부하가 없어 사전 발견 어려움

※ 표준 OS 고도화/대개체 시 작업절차

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **수행내역** | **수행부서** | **비고** |
| 1 | Base Image 생성 | kt Cloud | IPC/EPC Cent OS 7.6 : RNGD 기본 제공 IPC/EPC Rocky OS 8.10 : RNGD 미제공  Azure Rocky : RNGD 기본 제공 |
| 2 | kt 표준 형상으로 OS Pkg. 추가 설치 후, Golden Image 생성 | 인프라컨설팅팀  (w/kt Cloud) | ksh, 시스템 모니터링 Pkg. 등 설치 등  kt AO/IO 에 요청한 풀 SW 현행화 |
| 3 | Golden Image를 표준 OS로 등록 | 인프라컨설팅팀  (w/kt Cloud) |  |
| 4 | /etc/hosts 및 보안프로그램 설치 후, IO 담당자에게 제공 | 인프라컨설팅팀 | EPC환경 BA 수행, IPC는 IO 담당자 수행 |
| 5 | IO 담당자는 AP 업무 성격에 맞추어OS Package 및 프로그램 설치 | MW/DB/OS 구축부서 |  |

* 장애 조치 경과

|  |  |  |
| --- | --- | --- |
| **시간** | **작업내용/현상** | **비고** |
| 10:45 | 이상징후 발생 | 인지 시간(경로 : Signal) |
| 10:46 | 지연 현상 확인 및 모니터링 |  |
| 10:47 | 이상징후 발생 공지 |  |
| 10:48 | gc-prd-vbpwas01/02 IO/AO 점검 |  |
| 10:51 | KTC에 EPC 점검 요청 | EPC 이상 없음 |
| 10:52 | DB점검 특이사항 없음 |  |
| 10:55 | 고객포탈(VBPWAS01/02) 재기동 | AO(AI 구독서비스팀) 진행 |
| 10:55 | 동일 현상 발생 |  |
| 10:59 | 서비스포탈(SVCWAS01/02) 재기동 | IO(IA Core1팀) 진행 |
| 11:00 | 일시 해소 |  |
| 11:04 | 동일 현상 발생 |  |
| 11:10 | 4등급 장애전환 결정 |  |
| 11:16 | DB CPU/MEM 점검 결과 이상 없음 확인 | IO(IA Core1팀) 진행 |
| 11:18 | DBA 쿼리 점검 이상 없음 확인 |  |
| 11:20 | MW점검 결과 이상 없음 확인 | IO(IA Core1팀) 진행 |
| 11:23 | 서비스포탈(SVCWAS01/02) 2차 재기동 | IO(IA Core1팀) 진행 |
| 11:30 | SVCWAS thread dump 분석 | 플랫폼Tech팀&AI구독서비스팀 |
| 11:33 | Heap Dump 분석 | 플랫폼Tech팀&AI구독서비스팀 |
| 11:48 | 11:48 방화벽 확인(KTDS) |  |
| 12:03 | 일시 해소 |  |
| 12:04 | SVCWAS01 / 02 교차 Kill 후 분석 | IO(IA Core1팀) 진행 |
| 12:46 | KTC 방화벽 확인 |  |
| 12:52 | SafeDB 재기동 | IO(IA Core1팀) 진행 |
| 13:00 | MGRWAS 재기동 | IO(IA Core1팀) 진행 |
| 13:21 | 장애등급 상향(4등급 -> 3등급) |  |
| 14:20 | SVCWAS02번에 동일 소스 재배포 | AO(AI 구독서비스팀) 진행 |
| 14:23 | 동일 현상 발생 |  |
| 15:16 | SVCWAS02번에 JAVA.Security 옵션값 변경 적용 | 플랫폼Tech팀 작업 / 복구 시간 |
| 15:20 | 서비스 정상 확인 | AO(AI 구독서비스팀) 진행 |

* 장애 조치 내역
* JAVA.Security 옵션값 변경 적용

- /dev/random/에서 /dev/urandom으로 변경 후, MW 재기동

|  |  |  |
| --- | --- | --- |
| **특성** | **/dev/random** | **/dev/urandom** |
| 난수 생성 방식 | 블록킹 방식  (필요한 엔트로피가 부족할 경우 대기) | 논블록킹 방식  (즉시 데이터 제공) |
| 사용되는 엔트로피 | 안전한 난수를 위해 엔트로피가 필요함 | 엔트로피를 사용하지만 부족해도 계속 제공 |
| 용도 | 보안이 중요한 경우  (예: 암호 키 생성) | 일반적인 용도  (예: 퍼포먼스가 중요한 경우) |
| 생성 속도 | 느림  (엔트로피 부족 시 대기) | 빠름  (즉시 사용 가능한 난수 제공) |
| 보안 수준 | 더 높은 보안 수준  (엔트로피에 의존) | 통상적인 보안 수준  (사용에 따라 다름) |

* Lessons-Learned 및 시사점
* 예방 측면

- EPC Rocky OS 8.x 표준 OS Image에 RNGD Package 필수 설치 요청

- Entropy Avail 관제 정책 추가

- Open 전 성능 테스트 수행 필요

* 장애 대응 측면

- kt Rocky OS 8.10 사용 시스템에서 최초 발생한 사례로 원인 분석 장시간 소요

- 장애처리 메뉴얼 Entropy 소진 케이스 추가 및 관리

* 관제/탐지 측면

- 주요 기능 API 지연에 대한 관제 모니터링 강화 필요

* 절차/프로세스 측면

- Staging 설치 후, 약 한달간의 업무 테스트 이후 서비스 전환하였으나 미검출

- 향후 대개체 사업 추진 시 특이 모듈에 대한 부하테스트 과업 추가하여 성능 가능여부 확인

- OS플랫폼 변경 시 특히 패키지에 대한 확인 절차 추가

* 장애 후속 과제
* Quick-win 과제(1개월 내 조치 가능 과제)

|  |  |  |
| --- | --- | --- |
| **과제1** | **WAS 서버 RNGD Package 설치, Java 보안설정 Random 방식 원복** | 플랫폼Tech팀 |
| **​CRM25032089880** | 3.20 완료 |
| * + 1. KT AICC 공공지자체 WAS서버 8대 대상 rng-tools 패키지 설치     2. 장애 시 WA 적용된 Java 보안 설정 urandom에서 random으로 원복 | |
| **과제2** | **Entropy Avail 관제 정책 추가** | 플랫폼Tech팀 |
| **PBM25032121729** | 3.21 완료 |
| * + 1. 기존 OS 점검 항목에 Entropy Pool 소진 관제 패턴 추가 적용     2. Entropy Pool 소진 시, 즉시 데이터 제공 방식으로 변경 절차 체계화 하여 장애 이장시간 최소화 | |

* 중기 과제

|  |  |  |
| --- | --- | --- |
| **과제3** | **포탈 응답 시간 관제 추가** | AI구독서비스팀 |
| **PBM25032621744** | ~ 4.30 |
| * + 1. Entropy Pool 소진하는 API(활성유저체크/로그인/로그인 유저 정보조회/메뉴 이동)에  추가적으로 LAMP 로그 적용     2. 해당 API에서 응답지연 발생시(500~1000ms이상시) LAMP 알람 설정 | |
| **과제4** | **VM Template 내 RNGD(rng-tools 패키지) 설치** | 인프라컨설팅팀 |
| **PBM25032121731** | ~ 5.30 |
| * + 1. Linux 8.x 및 신규 버전에 대한 난수 Entropy 패키지가 포함된 Golden Image 반영 | |
| **과제5** | **IPC/EPC Base Image에 RNGD 및 VM 필수 SW 추가 검토 요청** | 인프라컨설팅팀 |
| **PBM25032821749** | ~ 9.30 |
| * + 1. Kt Cloud IPC/EPC 환경에 RNGD를 포함한 VM 필수 SW를 추가 설치 검토 필요     2. kt Cloud, kt, kt ds 3사 협의체 통해 요청 및 진행 사항 점검 | |

* 장애대응 이행도 점검 결과 : 100%수준(19개/19개)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **구분** | **#** | **점검 항목** | **점검**  **결과** | **점검 내용** |
| **장애인지** | **1** | **이상징후 발생 SMS 발송(즉시, 8분이내)** | **정상** | KT AICC 공공지자체 이벤트 발생으로 SMS 발송 (10:;48) |
| **2** | **kt ds(ISC/관제)에서 장애인지 여부**  **(외부(BA/사업부서) 문의의 경우 미흡)** | **정상** | KT AICC 공공지자체 Signal 이벤트 발생 (10:45) |
| **상황실**  **구성** | **3** | **장애 복구 반 구성(즉시)** | **정상** | 복구반 구성(10:48) |
| **4** | **장애 대응 필수 부서 참여(즉시)** | **정상** | 상황부서, 복구부서 참여(10:48) |
| **5** | **VOC 현황 파악(10분 마다)** | **정상** | VOC 0건(10:45) A'cen cloud SO센터 접수기준  ~  VOC 12건(15:47) A'cen cloud SO센터 접수기준 |
| **6** | **이상징후 종료 or 장애 전환 결정**  **(이상징후 전파 후 30분(업무) / 1시간(비업무) 이내,**  **서비스 영향도가 확인된 경우 즉시 장애로 전파/전환)** | **정상** | 장애 발생 검토(11:11)  - IT/SWW품질혁신팀, AX플랫폼개발팀,  AI구독서비스팀 |
| **7** | **종합상황실 구성(장애 판단 시, 즉시)** | **정상** | - 개설된 Teams 활용 |
| **8** | **상황반장/복구반장 확인** | **정상** | 상황반장/복구반장 지정 (11:11) 상황반장 : kt AX플랫폼개발팀 박정진 팀장 복구반장 : ktds AI구독서비스팀 조수현 팀장 |
| **장애전파**  **SMS** | **9** | **장애 등급 결정(장애 결정후, 10분 이내)** | **정상** | 장애 4등급 결정 시간(11:11)  장애 3등급 상향 결정 시간(13:21) |
| **10** | **장애 발생 SMS 문구 승인**  **(장애 결정후, 10분 이내)** | **정상** | 장애 발생 문구 승인(11:18) |
| **11** | **장애 발생 SMS 발송**  **(이상징후 전파 후 30분(업무)/1시간(비업무) 이내)** | **정상** | 장애 발생 SMS 발송(11:19) |
| **장애복구** | **12** | **장애 조치현황 OC기록(항상)** | **정상** | Teams 저장 |
| **13** | **VOC 현황 파악/보고(10분 마다)** | **정상** | VOC 0건(10:45) A'cen cloud SO센터 접수기준  ~  VOC 12건(15:47) A'cen cloud SO센터 접수기준 |
| **장애경과**  **SMS** | **14** | **장애경과 SMS 문구 최종승인(즉시)** | **정상** | [장애 경과 공지 - 1차] 문구 승인(12:17)  [장애 경과 공지 - 2차] 문구 승인(13:24)  [장애 경과 공지 - 3차] SMS 발송(14:29) |
| **15** | **장애 경과 SMS 발송**  **(장애 발생 공지후, 1시간(업무) / 2시간(비업무) 마다)** | **정상** | [장애 경과 공지 - 1차] SMS 발송(12:18)  [장애 경과 공지 - 2차] SMS 발송(13:25)  [장애 경과 공지 - 3차] SMS 발송(14:30) |
| **16** | **장애 경과 Mail 보고(ITO 위탁사 → kt IT)**  **(2시간 마다)** | **N/A** |  |
| **서비스**  **점검** | **17** | **영향 받은 서비스 점검** | **정상** | 서비스 확인(15:40)  - 운영부서 서비스 정상 확인 |
| **장애종료**  **SMS** | **18** | **장애 종료 SMS 문구 최종승인(즉시)** | **정상** | 장애 종료 문구 승인 (15:46) |
| **19** | **장애 종료 SMS 발송(서비스 점검 후 즉시)** | **정상** | 장애 종료 SMS 발송 (15:47) |
| **장애보고** | **20** | **장애 복구 Mail 보고(ITO 위탁사 → kt IT) (3시간 이내)** | **정상** | 수신 완료 |

별첨 #1) AP 암호화 호출 건수 분석 결과

월~수요일 대비 9:50 접속자수 증가 Entropy Pool 사용 증가로 응답시간 지연 발생 시작

10:18 장기 지연현상 지속발생 인지 후, AO 담당자 추가 접속하면서 10:20 최대 응답시간 발생

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **시간** | **03월 17일** | | **03월 18일** | | **03월 19일** | | **03월 20일** | |
| **로그인수** | **응답시간** | **로그인수** | **응답시간** | **로그인수** | **응답시간** | **로그인수** | **응답시간** |
| 9:00 | 18 | 21,811 | 2 | 67 | 10 | 71 | 16 | 358 |
| 9:10 | 5 | 54 | 9 | 171 | 4 | 58 | 6 | 55 |
| 9:20 | 9 | 66 | 14 | 7,214 | 7 | 7,485 | 15 | 1,560 |
| 9:30 | 8 | 66 | 12 | 19,874 | 6 | 7,914 | 2 | 797 |
| 9:40 | 4 | 3,673 | 15 | 1,386 | 6 | 164 | 13 | 68 |
| 9:50 | 8 | 34,022 | 20 | 4,002 | 5 | 2,951 | 39 | 2,605 |
| 10:00 | 25 | 3,053 | 2 | 2,507 | 0 | 60 | 13 | 110,879 |
| 10:10 | 18 | 1,236 | 6 | 341 | 5 | 57 | 5 | 112,873 |
| 10:20 | 0 | 54 | 2 | 634 | 7 | 56 | 12 | 320,537 |
| 10:30 | 14 | 11,517 | 4 | 3,086 | 10 | 48,403 | 27 | 123,136 |
| 10:40 | 0 | 1,450 | 0 | 58 | 25 | 35,433 | 24 | 161,146 |
| 10:50 | 6 | 60 | 6 | 54 | 19 | 77,772 | 16 | 152,293 |

별첨 #2) RNGD 사용, 미사용에 따른 Entropy Pool 동작 방식

* RNGD 미사용 동작 방식

|  |
| --- |
| 텍스트, 도표, 스크린샷, 평행이(가) 표시된 사진  자동 생성된 설명 |

* RNGD 사용 동작 방식

|  |
| --- |
| 텍스트, 스크린샷, 도표, 평행이(가) 표시된 사진  자동 생성된 설명 |

참고) CSP OS Base Image RNGD 제공 현황

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **OS Base Image** | **국내** | | **Global** | | |
| **IPC/EPC** | **Naver Cloud** | **Azure** | **AWS** | **GCP** |
| Cent OS 7.x | 기본 제공 | OS 미제공 | OS 미제공 | OS 미제공 | OS 미제공 |
| Rocky OS 8.x | 미제공 | | 제공 | | |