AlertNow 가이드 – Alert > Incident



Copyright ⓒ 2018 BESPIN GLOBAL All Rights Reserved.

사전 승인 없이 본 내용의 전부 또는 일부에 대한 복사, 전재, 배포, 사용을 금합니다.

1.문서 이력

|  |  |  |  |
| --- | --- | --- | --- |
| **작성일** | **작성자** | **버전** | **개정 내역** |
| 2017.11.27 | 배영수 | v0.1 | 최초 작성 |
| 2018.02.01 | 장지은 | v0.2 | opsNow->AlertNow 명칭변경 및 배포 1.0 version |
|  |  |  |  |

목차

[AlertNow 가이드 – Alert > Incident 1](#_Toc499545763)

[1 개요 4](#_Toc499545764)

[1.1 Alert 4](#_Toc499545765)

[1.2 Incident 4](#_Toc499545766)

## 개요

Incidents 메뉴를 통해 각 서비스에서 발생한 Alert들과 incident 들의 목록을 확인할 수 있습니다. 사용자는 Incidents 메뉴를 통해 처리해야 할 문제를 확인하고, 각 문제들의 처리 상태를 기록할 수 있습니다.

|  |
| --- |
|  |

Figure . Alert, Incident 의 흐름도

### Alert

CloudWatch, Azure Alert, UIM 등의 Monitoring Tool이나 기타 서비스에서 발생한 알람을 Integration 설정으로 Alarm Event를 수신 받은 경우, 이를 Alert으로 생성합니다.

* Alert 은 Raw Data 이며, 사용자가 임의로 Data를 변경하거나 생성된 Alert 을 삭제할 수 없습니다.
* Alert 을 기준으로 Incident를 생성합니다. 하지만 모든 Alert을 Incident로 생성하지 않으며, Incident Generation Rule 에 부합하는 Alert을 Incident로 생성합니다.
* Alert 은 사용자에게 Notification을 전달하지 않으며, 해당 Alert 을 통해 Incident 가 생성되어야 사용자에게 Notification 을 전달합니다.

사용자는 필요에 따라 서비스 별로 Alert 이 발생하지 않도록 Maintenance를 설정할 수 있습니다.

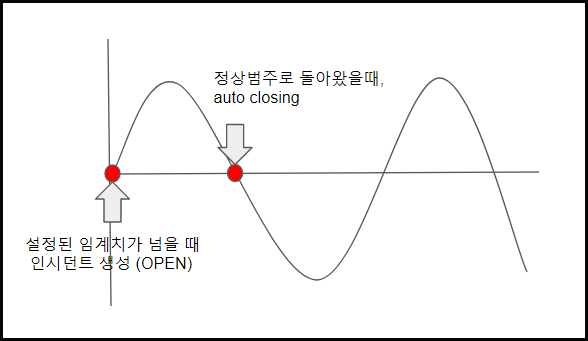
* 릴리즈, DB 작업, 인프라 작업, 보안 작업 등의 일정을 등록하여 해당 기간에 Incident의 발생을 억제할 수 있습니다.
* Maintenance 상태에서 발생한 Alert 은 Suppressed(by maintenance) 상태로 저장되며, Maintenance 일정으로 인해 해당 Alert 의 Incident가 생성되지 않았음을 확인할 수 있습니다.

### Incident

Alert이 수집되면 사전에 설정한 Incident Generation Rule을 통해 Incident가 생성됩니다. Incident 생성 이후, 사용자는 Incident에 대한 처리 상황을 기록하거나 Escalation을 통해 공지를 받을 수 있습니다.

이 외에 중복되는 incident 생성을 방지 하기 위해 Auto closing, unclosed Incident suppress 기능을 제공하고 있습니다.

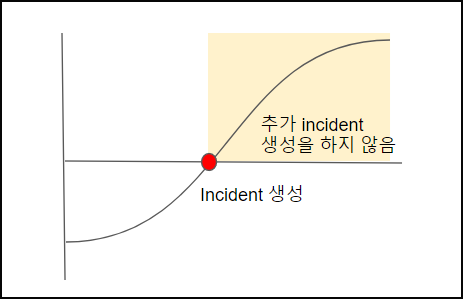
* Auto closing 기능



임계치 설정에 따라 Incident가 생성되어 있고, 만약 인스턴스 상태가 정상적으로 돌아오면, 기존에 생성된 Incident를 자동으로 closing 합니다.

* Unclosed Incident Suppression

Cloudwatch로 수신되는 알람 중, Cloudwatch Alarm Name이 동일한 Alert에 대해 Close 되지 않은 Incident가 존재하는 경우, Incident 의 추가 생성을 제한하는 기능을 제공합니다



또한 사용자는 사용자의 판단에 따라 Alert 이 생성되지 않은 상태에서도 수동으로 Incident 를 생성해 장애 대응을 진행할 수 있습니다. (추후예정)

* 사용자는 Alert Rule 에 의해 Incident 가 생성되지 않은 Alert 을 선택해 Incident 로 생성할 수 있습니다.(추후예정)
* 사용자는 Alert 이 생성되지 않은 상태에서도 수동으로 Incident 를 생성할 수 있습니다.(추후예정)
* 사용자는 이미 Incident 가 생성된 Alert 을 선택해 다른 Incident 에 연결할 수 있습니다.(추후예정)

### Alert, Incident 관계

위 내용을 종합했을 때, Alert 과 Incident 는 아래의 관계를 가질 수 있습니다.

1. Alert 기준
   1. Incident 생성 - Alert : Generated Incident [ 1 : 1 ]
   2. 참조 Alert - Alert : Referred Alert [ 1 : N ] (추후예정)
   3. 참조 Incident - Alert : Referred Incident [ 1 : N ] (추후예정)
2. Incident 기준
   1. 생성기준 Alert - Incident : Triggered Alert [ 1 : 1 ]
   2. 인시던트 병합 - Incident : Merged Incident [ 1 : N ] (추후예정)
   3. 참조 Incident - Incident : Referred Incident [ 1 : N ] (추후예정)
   4. 참조 Alert - Incident : Referred Alert [ 1 : N ] (추후예정)

Alert는 다음과 같은 Incident 생성 결과를 가질 수 있습니다.

1. 인시던트 생성 Incident Creation
2. 생성억제(생성제한 규칙) Suppressed (by suppression rule)
3. 생성억제(유지보수) Suppressed (by maintenance)
4. 생성억제(미종료 인시던트) Suppressed (by unclosed)

## Incident

접속 경로: Incidents > Incidents

Incidents 메뉴를 통해 생성된 Incident 들을 목록으로 확인할 수 있으며, Incident 별 상세 내용을 확인하고 처리 상태를 기록할 수 있습니다. 또한 기간, 키워드를 설정해 특정 Incident를 검색할 수 있습니다.

### 화면 구성

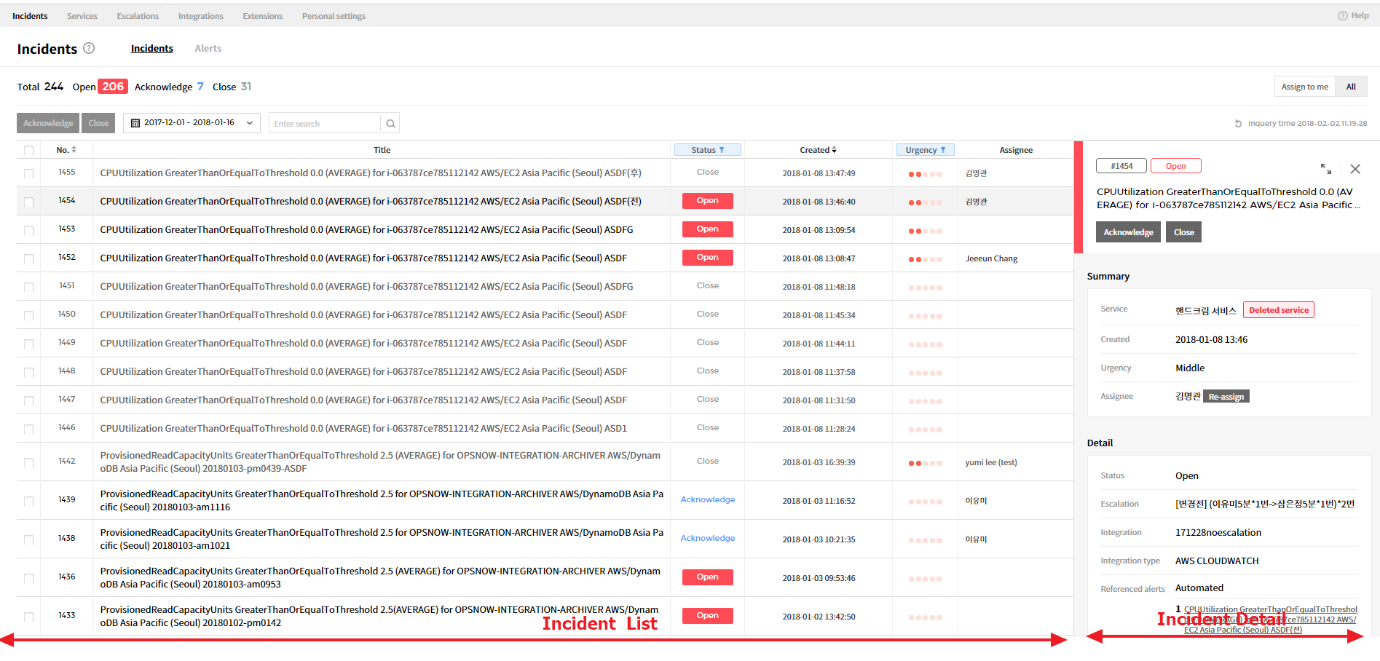
Incident 메뉴는 아래와 이미지와 같이 크게 두 영역으로 구분됩니다.

Figure . Incident 메뉴 구성

#### Incident List

기 발생한 Incident 들을 목록으로 확인할 수 있으며, 발생한 Incident 들을 검색할 수 있습니다. Incident List 에서 Incident 선택 시, 선택한 Incident 의 정보가 Incident Detail 영역에 표시됩니다. Incident List 에서는 아래의 정보를 확인할 수 있습니다.

|  |  |  |
| --- | --- | --- |
| **항목** | **설명** | **비고** |
| No | Incident 의 Serial Number 를 표시합니다. |  |
| Title | Incident 의 제목을 표시합니다. |  |
| Status | Incident 의 상태를 표시합니다.  Incident 는 아래의 상태 값을 가집니다.   * Opened * Acknowledge * Close |  |
| Created | Incident 의 생성 날짜 및 시간을 표시합니다. |  |
| Updated | Incident 의 최종 업데이트 날짜 및 시간을 표시합니다. |  |
| Urgency | Incident 의 시급도를 표시합니다. |  |
| Service | Incident 가 발생한 서비스 이름을 표시합니다. |  |
| Assignee | Incident 의 담당자로 지정된 사용자 이름을 표시합니다. |  |

#### Incident Detail

Incident List 에서 선택한 Incident 의 상세 정보를 확인할 수 있습니다. 해당 영역은 사용자의 필요에 따라 확장해 큰 화면으로 확인할 수도 있습니다. Incident Detail에서는 아래의 정보를 확인할 수 있습니다.

|  |  |  |  |
| --- | --- | --- | --- |
| **항목** | | **설명** | **비고** |
| Summary | Service | Incident 가 발생한 서비스 이름을 표시합니다. |  |
| Created | Incident 의 생성 날짜 및 시간을 표시합니다. |  |
| Urgency | Incident 의 시급도를 표시합니다. |  |
| Assignee | Incident 의 담당자를 표시합니다. |  |
| Detail | Status | Incident 의 상태를 표시합니다.  Incident 는 아래의 상태 값을 가집니다.   * Opened * Acknowledge * Close |  |
| Escalation | Incident 에 설정된 Escalation Rule 을 표시합니다. |  |
| Integration | Incident 를 발생시킨 Integration 명을 표시합니다. |  |
| Integration Type | Incident 를 발생시킨 Integration Type을 표시합니다. |  |
| Referenced alerts | Incident 를 발생시킨 alert를 표시합니다. |  |
| Message | Alert 발생 시 첨부된 메시지를 표시합니다. |  |
| Description | Incident 의 설명을 표시합니다. 설명을 직접 입력할 수 있습니다. |  |

### Incident 상태

Incident 는 아래의 세가지 상태 값을 가지며, 상태에 따라 Title 영역을 다른 색상으로 표시합니다.

#### Opened

새롭게 Incident 로 생성되어 아직 처리 전인 상태를 의미합니다.

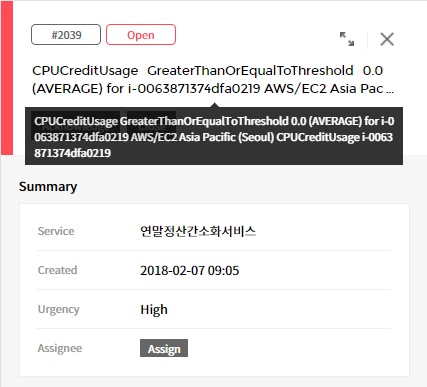


Figure . Opened Incident 의 표시

#### Acknowledge

장애 사실을 인지하고 담당자가 처리 중인 상태를 의미합니다.

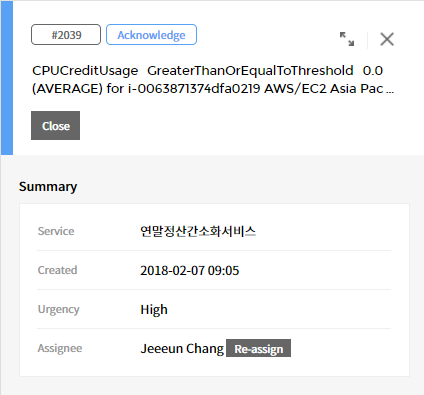


Figure . Acknowledge Incident 의 표시

#### Closed

장애 처리가 완료되어 종결된 상태를 의미합니다.

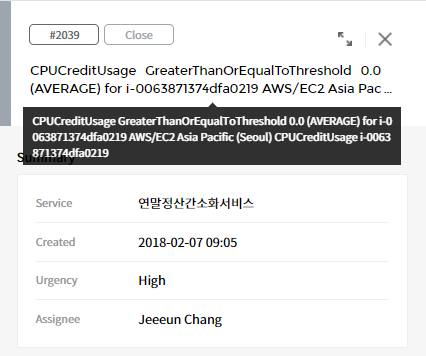


Figure . Closed Incident 의 표시

### Incident 검색

사용자는 Incident 목록에서 Incident를 기간/키워드 조건을 설정해 incident를 검색할 수 있습니다. 검색 결과는 incident 목록에 바로 표시됩니다.

#### 기간 검색

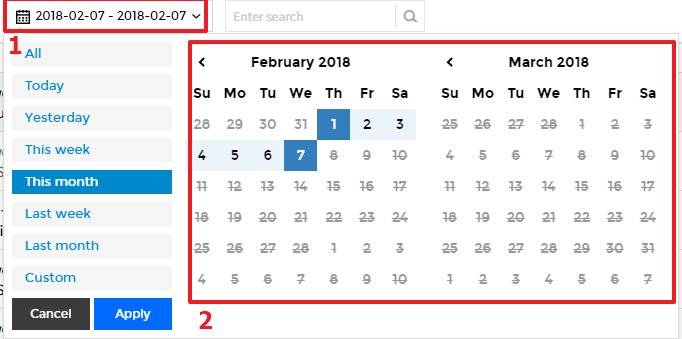


Figure 검색 조건

1. 기간 선택 Preset

사용자가 선택 가능한 기간을 Preset 형태로 제공합니다. 사용자는 아래의 기간 Preset 을 선택할 수 있으며, 선택 시 기간 선택 영역에 선택된 기간이 표시됩니다.

|  |  |
| --- | --- |
| **Preset** | **기간** |
| Today | 현재 날짜를 선택한다. |
| Yesterday | 어제의 날짜를 선택한다. |
| This week | 현재 시간을 기준으로 이번 주를 선택한다. |
| This month | 현재 시간을 기준으로 해당 월을 선택한다. |
| Last Week | 현재 시간을 기준으로 지난 주를 선택한다 |
| Last Month | 현재 시간을 기준으로 지난 달을 선택한다. |

1. Custom(기간 선택)

사용자는 검색 시작/종료일 및 시간을 선택할 수 있습니다. 기간 선택 시 선택한 기간 내의 Incident 가 Incident 목록에 표시됩니다. 또한 사용자는 좌/우 화살표를 선택해 현재 설정된 날짜를 기준으로 이전/이후 주기를 설정할 수 있습니다.

#### 키워드 검색

사용자는 키워드를 입력해 입력한 키워드와 일치하는 Incident를 검색할 수 있습니다. 선택한 기간의 Incident 중 입력한 키워드와 일치하는 Incident를 검색 결과로 표시합니다.

#### 상태 필터



Figure . 상태 필터(우측상단)

목록 내 Incident 중, Assignee가 현재 로그인한 사용자인 Incident 만 필터링해 확인할 수 있습니다.

1. Assign to me

Incident 목록에서 Assignee가 현재 로그인한 사용자인 Incident 만 표시합니다..

1. All

전체 Incident를 표시합니다.

### Incident 조작

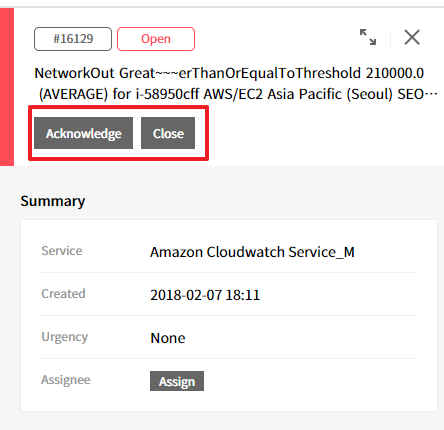
목록 내 Incident 에 대해 아래의 작업들을 수행할 수 있습니다.

#### 상태 변경

Incident 의 상태를 변경할 수 있습니다. 개별 Incident 의 상태를 변경할 수 있으며, 복수의 Incident 를 선택해 상태를 일괄 변경할 수 있습니다.

1. Incident 상태 변경

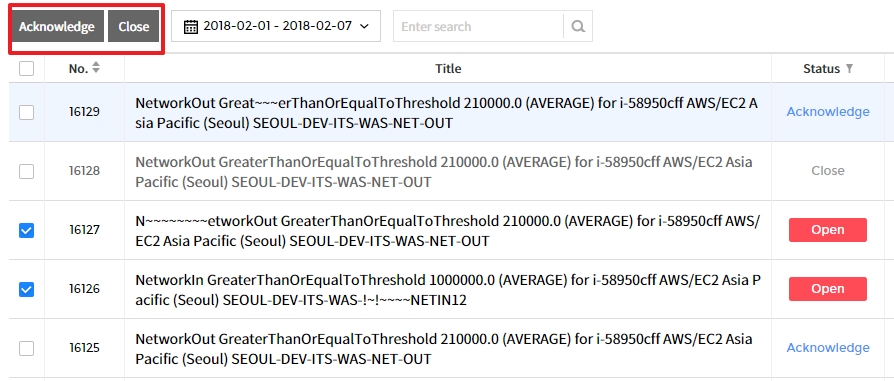
Incident Detail 화면에서 Title 하단의 버튼으로, 상태를 변경 할 수 있습니다.



* Opened 상태인 Incident 는 Acknowledge, Close 상태로 변경할 수 있습니다.
* Acknowledge 상태의 Incident 를 Close 상태로 변경할 수 있습니다.
* Close 상태의 Incident 는 상태를 변경할 수 없습니다.

1. 복수 Incident 상태 일괄 변경

Incident List 에서 상태를 변경할 Incident를 선택해 Incident 의 상태를 일괄 변경할 수 있습니다.



* 복수 Incident 선택 후, Incident List 좌측 상단의 [Acknowledge][Close] 버튼을 클릭해 상태를 변경할 수 있습니다.

#### Assignee 지정 및 변경

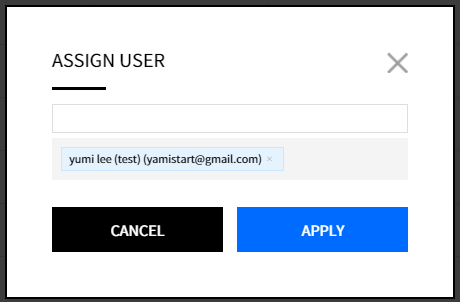
Incident별로 Assignee를 지정하거나 변경할 수 있습니다. Incident Detail 화면의 [Assign] 버튼 클릭 시 Assignee를 지정할 수 있는 팝업이 표시됩니다.

* 1. Assignee를 지정할 Incident 선택

Assignee 항목에는 현재 지정된 Assignee 의 이름이 표시되며, [Assign] 버튼 클릭 시 Assignee를 변경할 수 있는 팝업이 표시됩니다.

|  |
| --- |
|  |

* 1. Assignee 선택

Assign User 팝업을 통해 담당자를 검색 후 지정할 수 있습니다.

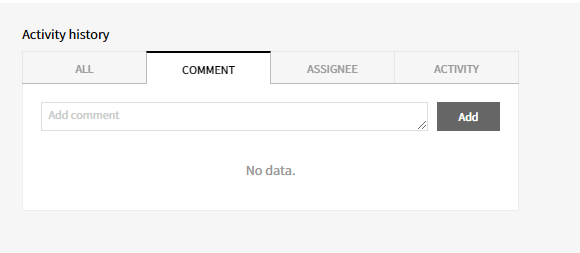
* 하나의 Incident 에 대해 복수의 Assignee를 지정할 수 없습니다.

#### 코멘트 작성

Incident에 대한 Comment를 작성할 수 있습니다.

* 1. Incident detail의 full screen으로 이동

Incident Detail 화면에서 Active History 탭의 COMMENT에서 입력



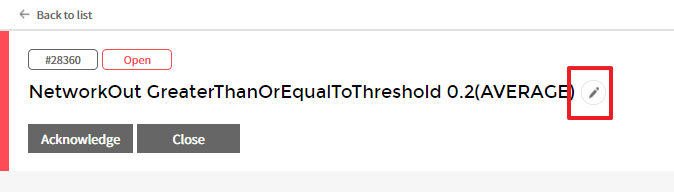
* 1. Comment 입력 후 [Add] 버튼 클릭
  2. 입력된 Comment 확인



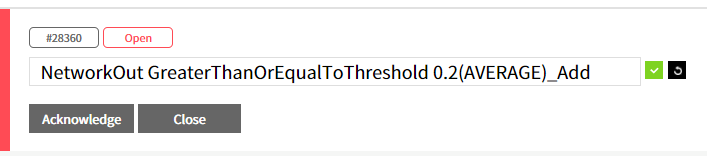
#### Title 변경

사용자의 필요에 따라 각 Incident 의 Title을 변경할 수 있습니다.

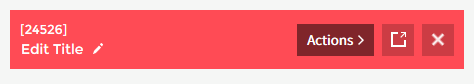
* 1. Full Screen의 Title 영역에서 [수정] 버튼 클릭



* 1. Title 수정 후, [완료] 버튼 클릭



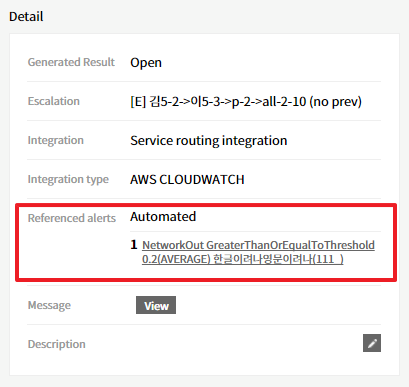
* 1. 변경된 title 확인



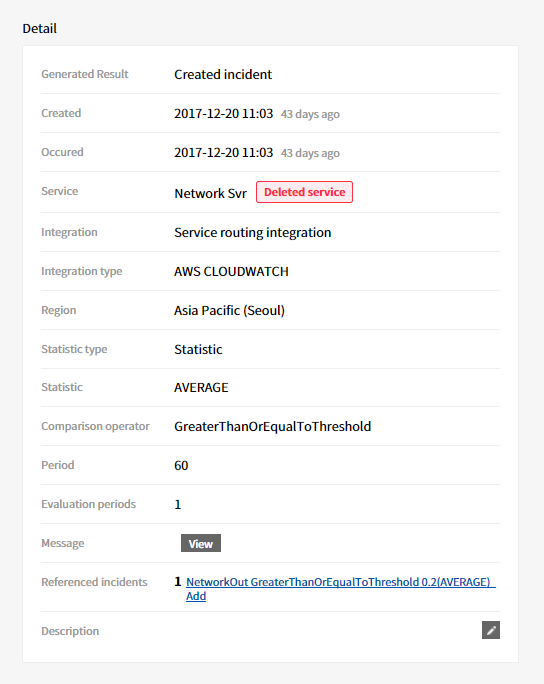
#### 연관 Alert 확인

각 Incident 의 연관 Alert 을 확인할 수 있으며, 각 Alert 의 Detail 화면으로 이동할 수 있습니다.

* 1. Incident 연관 Alert 확인



* 1. 연관 Alert 클릭해 Alert 상세 정보 확인



## Alert

접속 경로: Incidents > Alerts

Alert 메뉴를 통해 Alert 들을 목록으로 확인할 수 있으며, Alert의 상세 내용을 확인할 수 있습니다. 또한 기간, 키워드를 설정해 특정 Alert을 검색할 수 있습니다.

### 화면 구성

Alert 메뉴는 아래와 이미지와 같이 크게 두 영역으로 구분됩니다.

|  |
| --- |
|  |

Figure . Alert 구성

#### Alert list

기 발생한 Alert 들을 목록으로 확인할 수 있으며, 발생한 Alert 들을 검색할 수 있습니다. Alert List 에서 Alert 선택 시, 선택한 Alert의 정보가 Alert Detail 영역에 표시됩니다. Alert List 에서는 아래의 정보를 확인할 수 있습니다.

|  |  |  |
| --- | --- | --- |
| **항목** | **설명** | **비고** |
| No | Alert 의 Serial Number 를 표시합니다. |  |
| Title | Alert 의 제목을 표시합니다. |  |
| Status | Alert 의 상태를 표시합니다. |  |
| Created | Alert 의 생성 날짜 및 시간을 표시합니다. |  |
| Service | Alert 이 발생한 서비스 명을 표시합니다. |  |
| Integration Type | Alert이 발생한 서비스의 Integration Type을 표시합니다. |  |

#### Alert Detail

Alert List 에서 선택한 Alert의 상세 정보를 확인할 수 있습니다. 해당 영역은 사용자의 필요에 따라 확장해 큰 화면으로 확인할 수도 있습니다. Alert Detail 에서는 아래의 정보를 확인할 수 있습니다.

|  |  |  |
| --- | --- | --- |
| **항목** | **설명** | **비고** |
| Incident creation | Incident generation rule에 따라 incident 생성 결과를 표시합니다. |  |
| Created | Alert 의 생성 날짜 및 시간을 표시합니다. |  |
| Occurred | Alert 의 발생 날짜 및 시간을 표시합니다. |  |
| Service | Alert 의 발생한 서비스 명을 표시합니다. |  |
| Integration | Alert 의 Integration 을 표시합니다. |  |
| Integration Type | Alert 의 발생한 서비스의 Integration Type을 표시합니다. |  |
| Region | Alert 의 발생한 지역을 표시합니다. |  |
| Statistic type | Cloud watch에 설정된 경보의 통계 타입을 표시합니다. |  |
| Statistic | Cloud watch에 설정된 경보의 통계 설정 값을 표시합니다. |  |
| Comparison operator | Cloud watch에 설정된 경보의 임계치 설정 비교 연산자를 표시합니다. |  |
| Period | Cloud watch에 설정된 경보의 기간을 표시합니다. |  |
| Evaluation periods | Cloud watch에 설정된 경보 임계치의 발생 횟수를 표시합니다. |  |
| Message | Alert 의 상세 메시지를 확인할 수 있습니다. |  |
| Description | Alert 의 상세 설명을 확인할 수 있습니다. |  |
| Related Incident | Alert 과 연결된 Incident를 표시한다. |  |

### Alert 검색

사용자는 Alert List에서 기간/키워드 조건을 설정해 Alert을 검색할 수 있습니다. 검색 결과는 Alert 목록에 바로 표시됩니다.

#### 기간 검색

|  |
| --- |
|  |

Figure 검색 조건

1. 기간 선택 Preset

사용자가 선택 가능한 기간을 Preset 형태로 제공합니다. 사용자는 아래의 기간 Preset 을 선택할 수 있으며, 선택 시 기간 선택 영역에 선택된 기간이 표시됩니다.

|  |  |
| --- | --- |
| **Preset** | **기간** |
| Today | 현재 날짜를 선택합니다. |
| Yesterday | 어제의 날짜를 선택합니다.. |
| This week | 현재 시간을 기준으로 이번 주를 선택합니다. |
| This month | 현재 시간을 기준으로 해당 월을 선택합니다. |
| Last Week | 현재 시간을 기준으로 지난 주를 선택합니다 |
| Last Month | 현재 시간을 기준으로 지난 달을 선택합니다. |

1. 기간 선택

사용자는 검색 시작/종료일 및 시간을 선택할 수 있습니다. 기간 선택 시 선택한 기간 내의 Alert이 Alert List에 표시됩니다. 또한 사용자는 좌/우 화살표를 선택해 현재 설정된 날짜를 기준으로 이전/이후 주기를 설정할 수 있습니다.

#### 키워드 검색

사용자는 키워드를 입력해 입력한 키워드와 일치하는 Alert을 검색할 수 있습니다. 선택한 기간의 Alert 중 입력한 키워드와 일치하는 Incident를 검색 결과로 표시합니다.

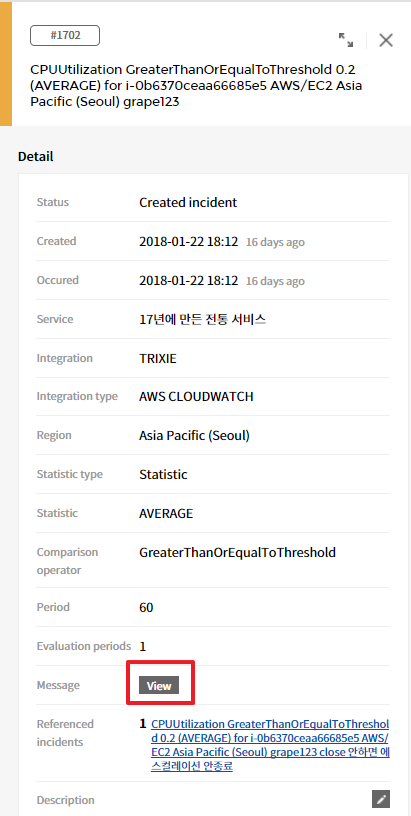
### Alert 조작

목록 내 Alert 에 대해 아래의 작업을 수행할 수 있습니다.

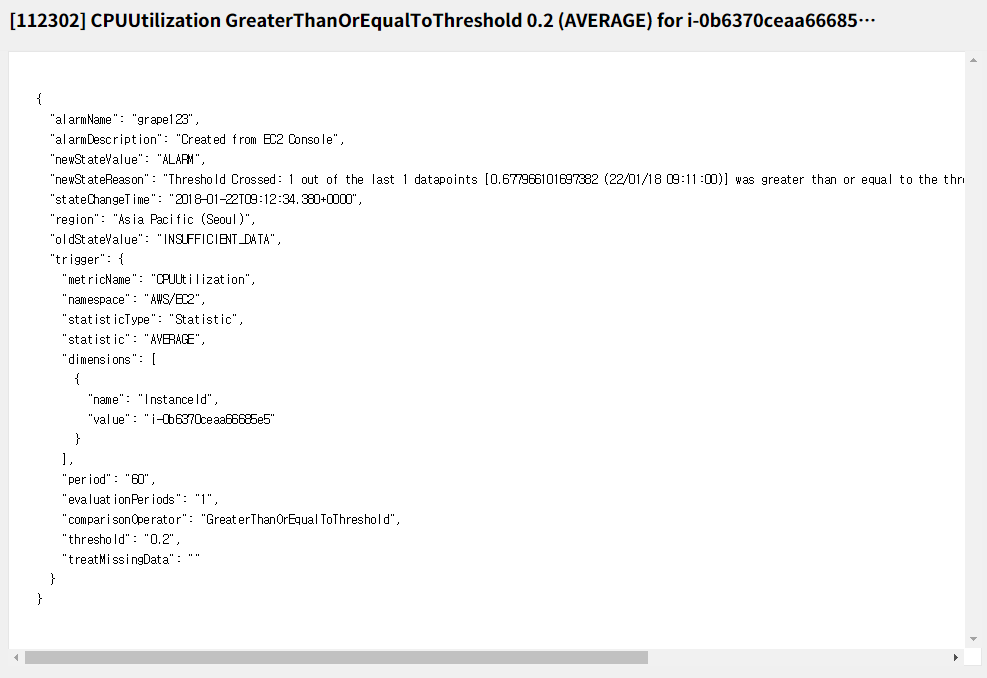
#### 메시지 확인

발생한 Alert 에 대한 상세 메시지를 확인할 수 있습니다.

* 1. Alert Detail 화면에서 [Message]>[View] 버튼을 클릭합니다.



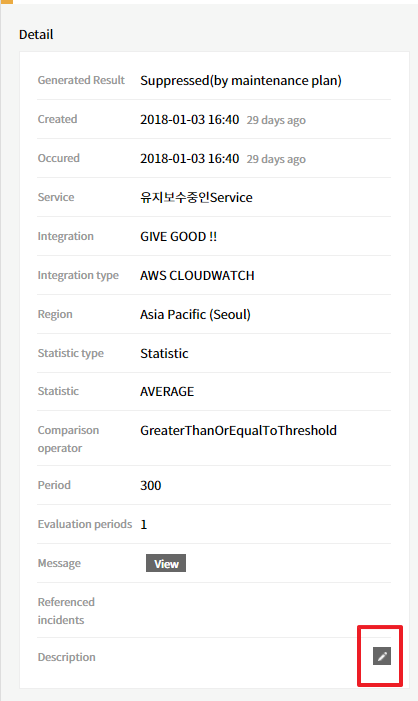
* 1. 새 탭으로 상세 Message가 표시됩니다.



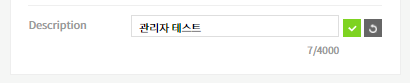
#### Description 입력

발생한 Alert 에 대해 상세 설명을 입력할 수 있습니다.

* 1. Alert Detail 화면에서 [수정] 버튼을 클릭합니다.



* 1. Description 입력 후 [저장] 버튼을 클릭합니다.

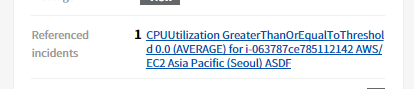


* 1. 입력된 Description 을 확인합니다.

#### 연관 Incident 보기

선택한 Alert을 통해 생성된 Incident 들을 확인할 수 있으며, 각 Incident 의 상세 화면으로 이동할 수 있습니다.

1. Alert 연관 Incident 확인



1. 연관 Incident 클릭해 Incident 상세 정보 확인

