
metatron-doc-user Documentation

출시 버전 0.4.3

metatron team

2020년 01월 29일

EX-pack for Anomaly Detection

I	EX-pack for Anomaly Detection	1
1	Anomaly 확장팩 소개	3
1.1	기본 원리	3
1.2	주요 기능	4
1.3	구조	5
2	알람 룰 만들기	7
2.1	데이터 소스 선정	7
2.2	모니터링할 지표 선택하기	9
2.3	트레이닝 기간 설정하기	13
2.4	모델 선택하기	15
2.5	알람 룰 조건 설정하기	16
2.6	알람 룰 완성하기	18
3	통계	21
4	알람 룰 내역 열람·수정하기	25
4.1	알람 룰 리스트	25
4.2	알람 룰 상세	26
5	알람 내역 열람하기	29
5.1	알람 리스트	29
5.2	알람 상세	31

Part I

EX-pack for Anomaly Detection

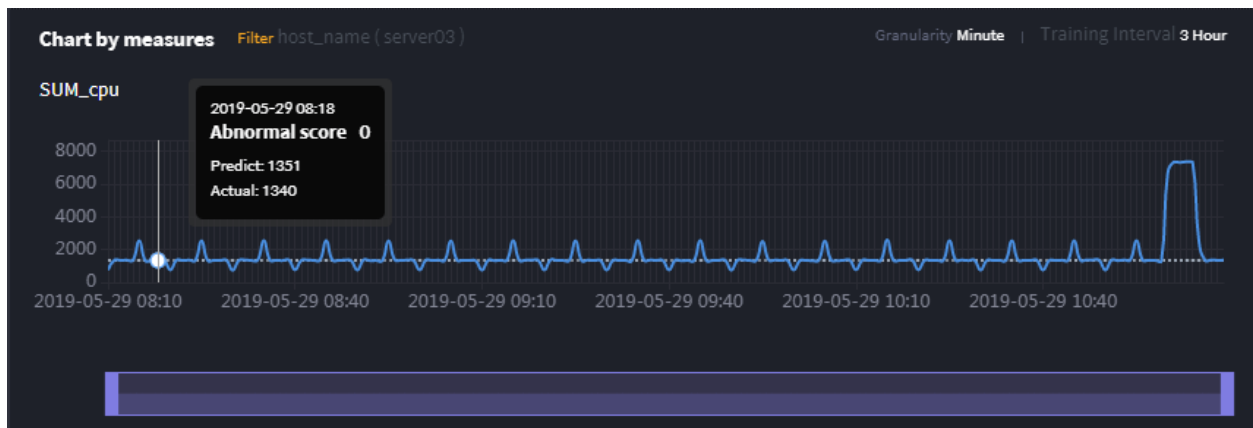
CHAPTER 1

Anomaly 확장팩 소개

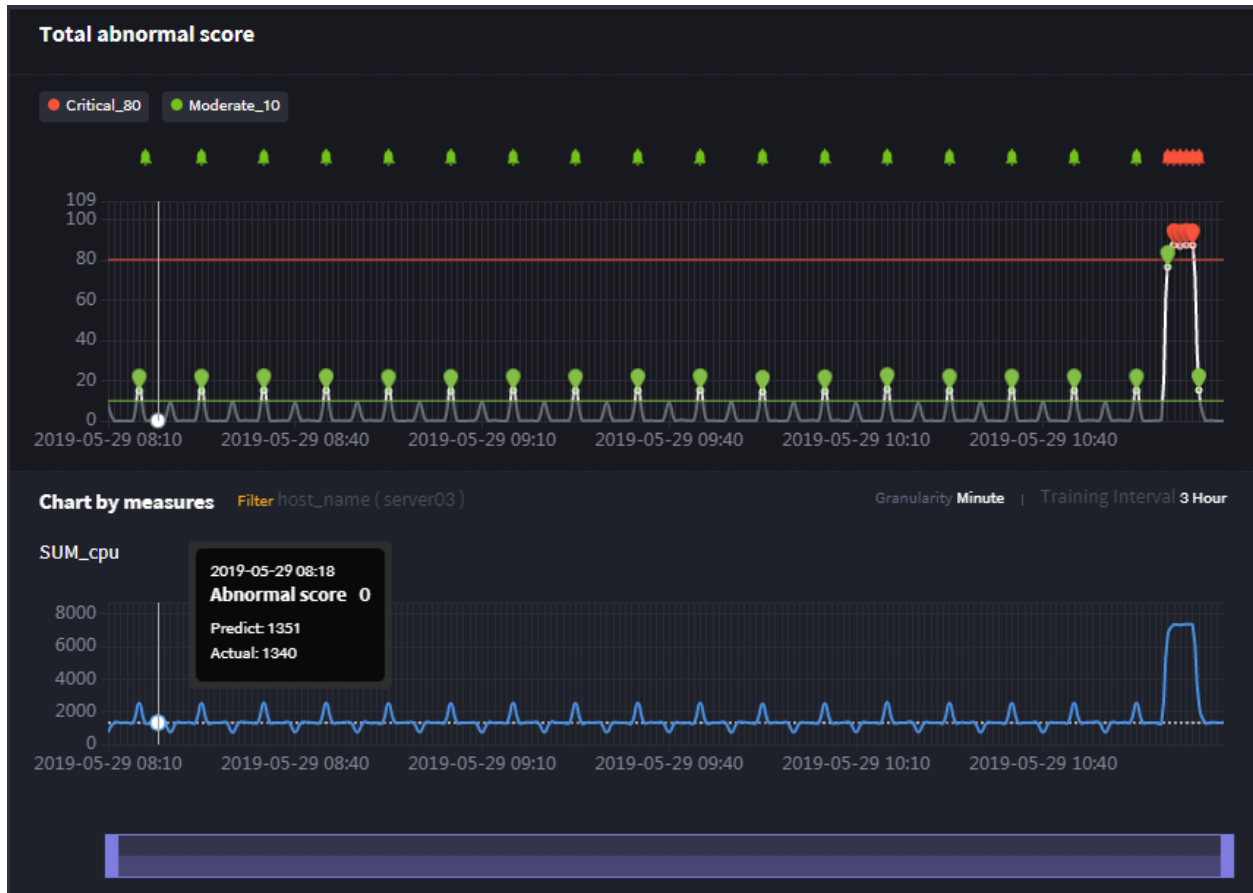
이상 탐지 확장팩 Anomaly는 Machine Learning 예측 모델을 기반으로 데이터 흐름의 비정상적인 상황을 감지하여 사용자가 즉각적으로 확인할 수 있도록 도와주는 도구입니다.

1.1 기본 원리

아래 그림과 같이 Anomaly는 대상 데이터 소스의 집계값을 실시간으로 예측하고 실제 값을 모니터링합니다.



여기서 **Predict**로 표시된 값은 머신러닝 기반으로 예측한 데이터 집계값이고, **Actual**로 표시된 값은 실제로 모니터링한 결과 값입니다. 아래 그림과 같이 두 값 간의 격차가 커질수록 **total abnormal score**가 증가하게 됩니다. 즉, 실제치가 예상치와 다르면 데이터 집계값이 그만큼 정상 범위를 벗어났다고 간주하는 것입니다.



이 예시에서는 abnormal score가 10점에 도달하면 Moderate 알람을 발생시키고, 80점에 도달하면 Critical 알람을 발생시키도록 설정되어 있습니다.

이렇게 발생하는 알람은 다양한 채널로 사용자에게 통보되어, 사용자는 데이터 이상 상황에 즉각 대처할 수 있습니다.

1.2 주요 기능

Anomaly의 주요 기능은 다음과 같습니다.

Machine Learning

머신러닝에 기반한 예측 모델이 자동으로 추천되어 사용자 편의 증대

Alarm & Report

비정상적인 상황 발생 시 즉각 알람 발동 및 보고서 생성

Analyze

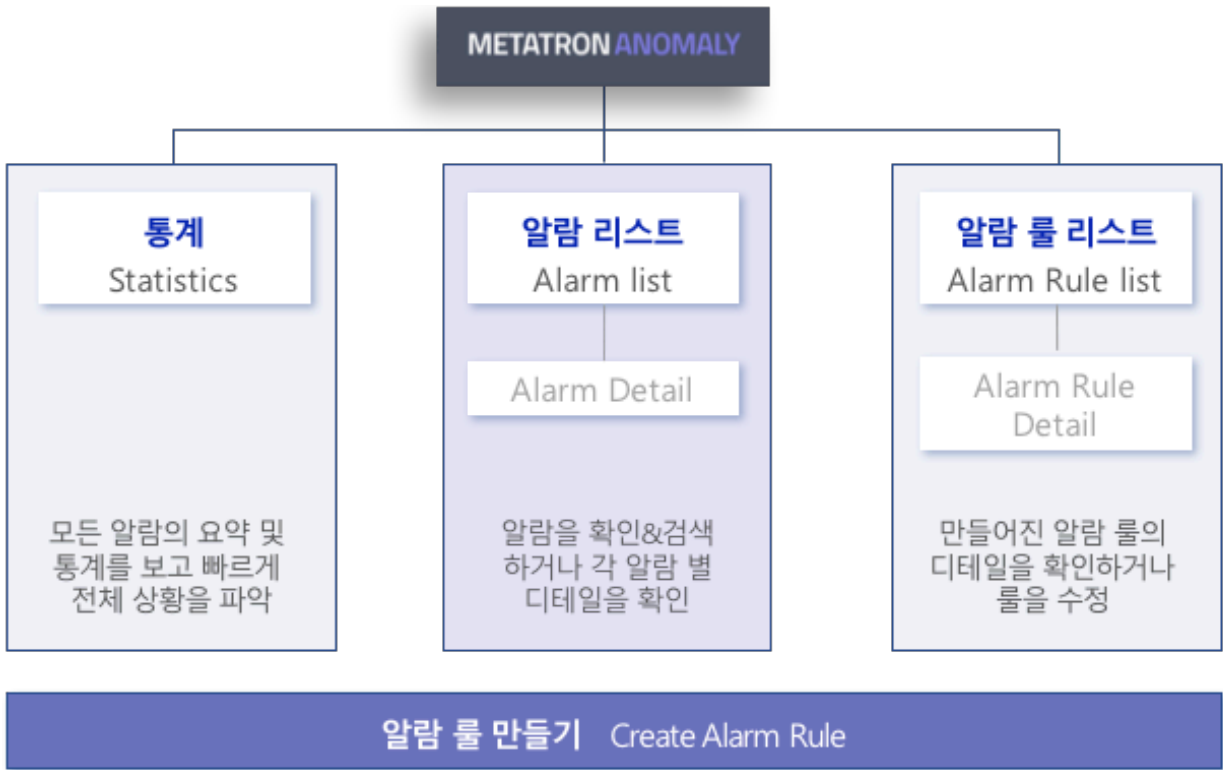
데이터로 차트 생성하고 분석하는 서비스 메타트론 디스커버리와 연계 가능

Link with Learning System

새로운 분석을 적용할 수 있도록 외부 분석 시스템과의 연계를 지원

1.3 구조

Anomaly의 메뉴 구성은 다음과 같습니다.



주요 메뉴 간 이동이 쉽고 세부 항목 간 참조 기능도 잘 구축되어 있어, 알람 룰 설정값과 발생한 알람 내역, 그리고 전반적인 알람 현황 간의 유기적인 파악이 용이합니다.

CHAPTER 2

알람 룰 만들기

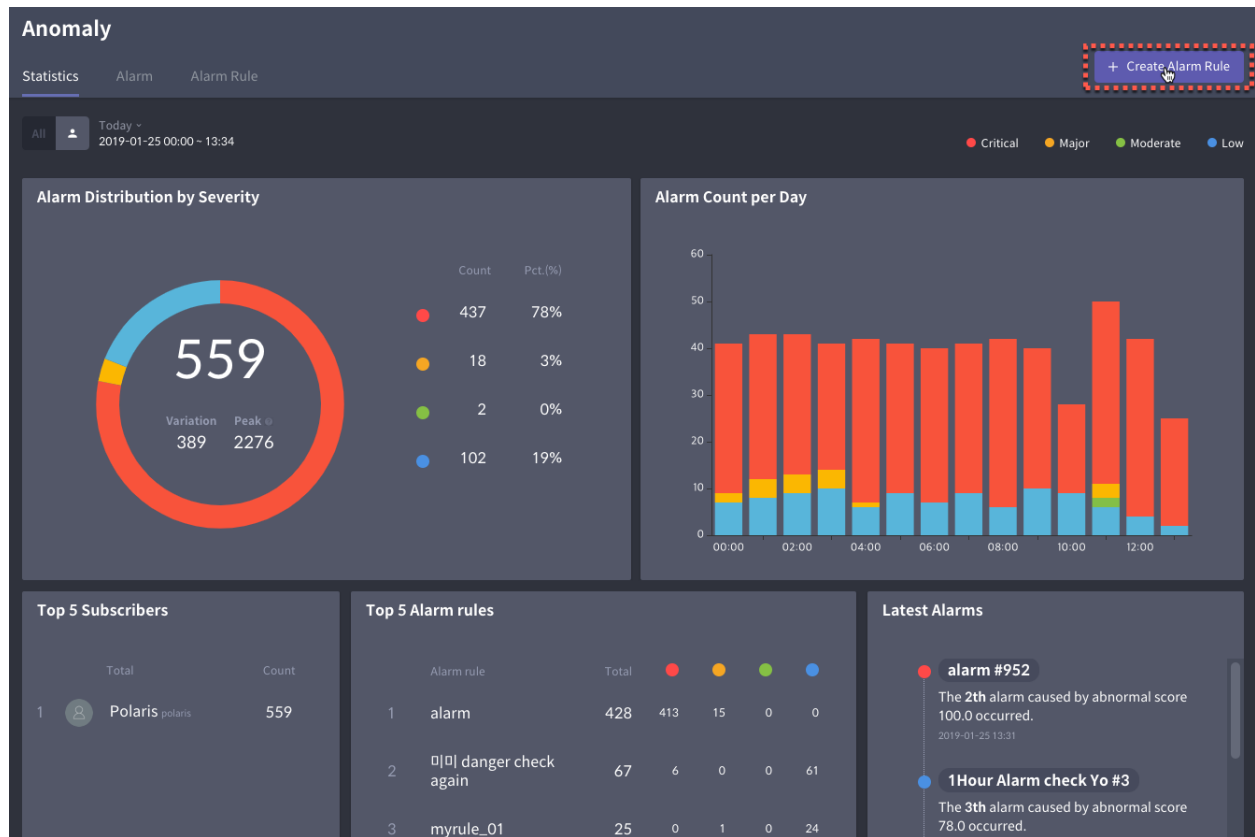
Anomaly는 다음의 절차를 순차적으로 수행하도록 안내하여 사용자가 원하는 알람 룰을 쉽게 생성할 수 있도록 지원해줍니다.

- 데이터 소스 선정
- 모니터링할 지표 선택하기
- 트레이닝 기간 설정하기
- 모델 선택하기
- 알람 룰 조건 설정하기
- 알람 룰 완성하기

2.1 데이터 소스 선정

아래와 같이 알람 룰 만들기 절차를 시작하십시오.

1. Anomaly 홈 우측 상단에 있는 **Create Alarm Rule** 버튼을 클릭합니다.



2. 모니터링하고자 하는 데이터 소스를 선택합니다.

Create an alarm rule
Please select a datasource

● ○ ○ ○ ○

Q real ☐ Show open data only Type 전체

No.	Datasource	Type	Used in	Updated
2	realtime_sample_01 Open data	수집형 데이터	All Workspaces	2018.11.28
1	realtime_server_load_01 Open data	수집형 데이터	All Workspaces	2019.01.04 ✓

더보기

realtime_server_load_01

메타데이터 이름

설명

타입 수집형 데이터

공개설정 공개

생성일 2019-01-04

사이즈 115.17 MB

Rows 18,128,223

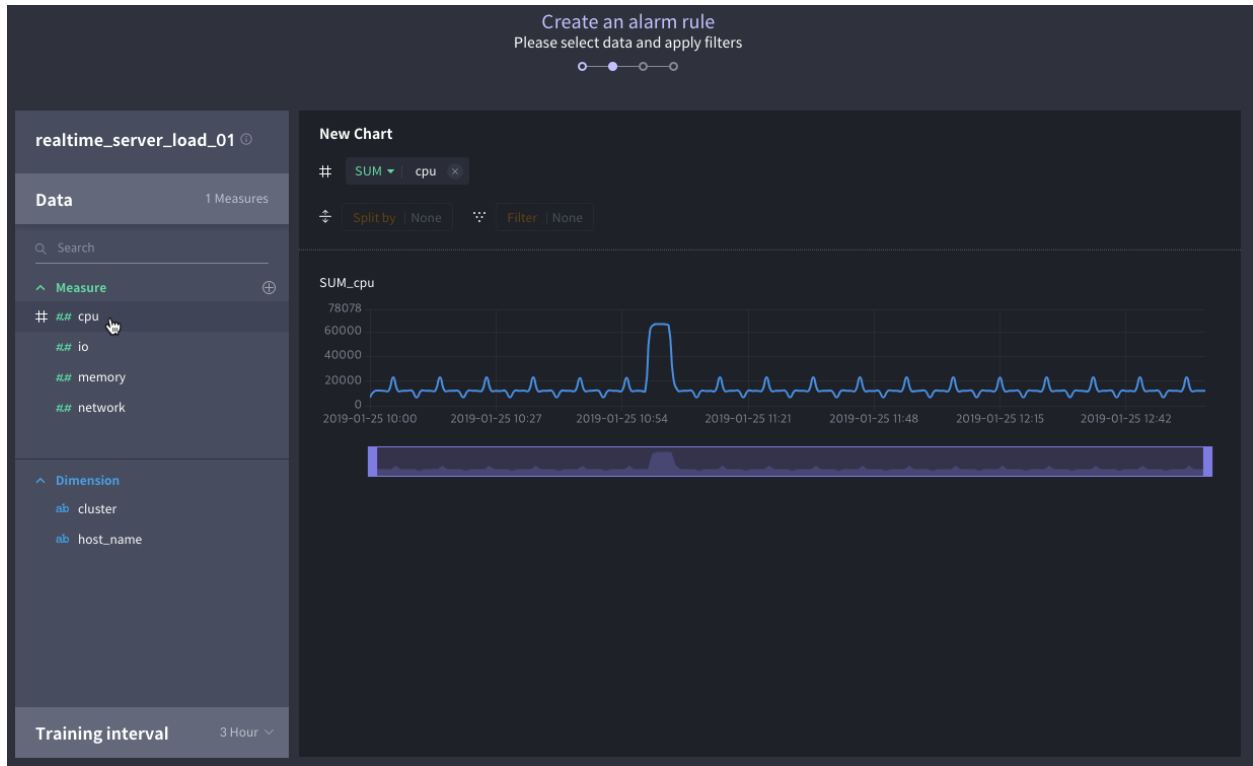
dimension	event_time
dimension	ab cluster
측정값	## cpu
dimension	ab host_name
측정값	## io
측정값	## memory
측정값	## network


Cancel Next

2.2 모니터링할 지표 선택하기

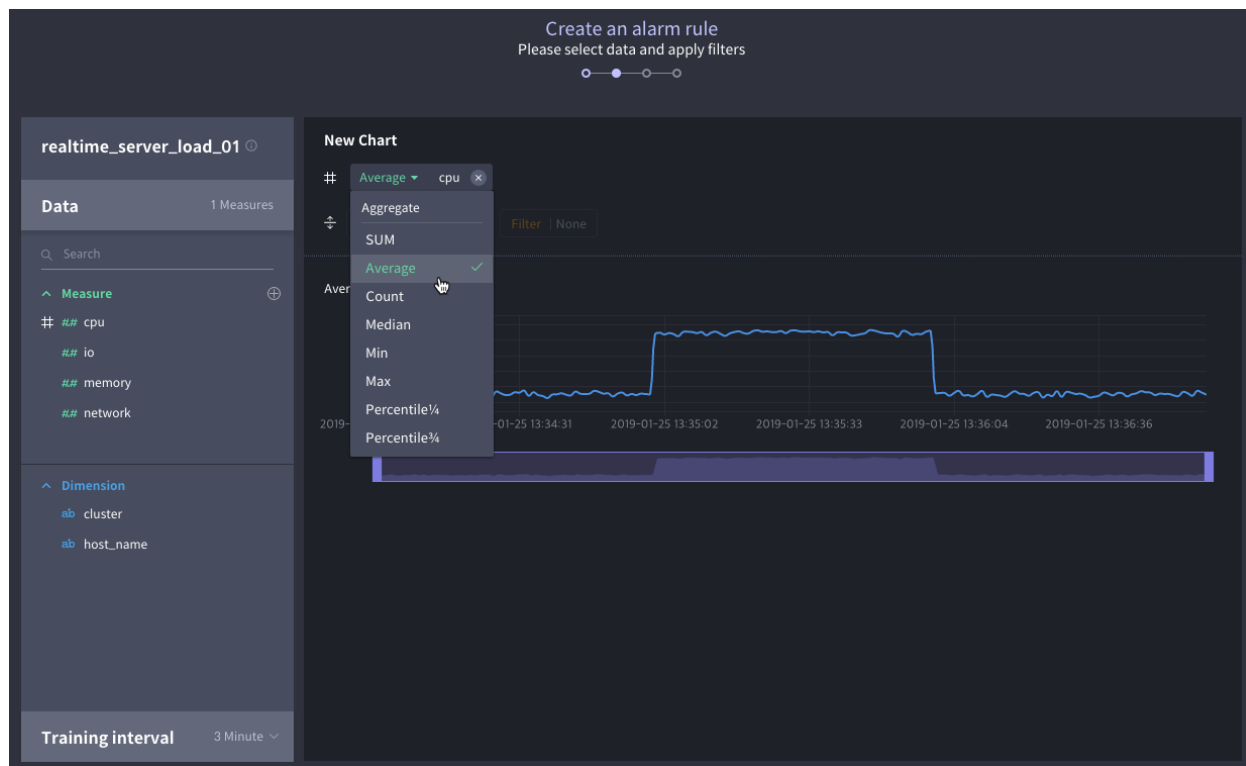
데이터 소스를 선택하면 다음 화면으로 넘어가면서 좌측에 **Data** 패널이 열립니다. 이 패널을 이용하여 아래와 같이 모니터링할 지표를 선택하십시오.


1. **Measure** 영역에서 알람을 설정하고자 하는 측정값 컬럼을 선택합니다. 클릭한 측정값 컬럼은 Aggregate 선반에 자동으로 옮겨집니다.




2. 필요할 경우 기존 컬럼에 수식을 적용하여 사용자 컬럼을 새로 만들 수도 있습니다. **Measure** 영역의 우측 상단에서  버튼을 클릭하여 대화 상자를 열고 사용자 컬럼을 설정하십시오.

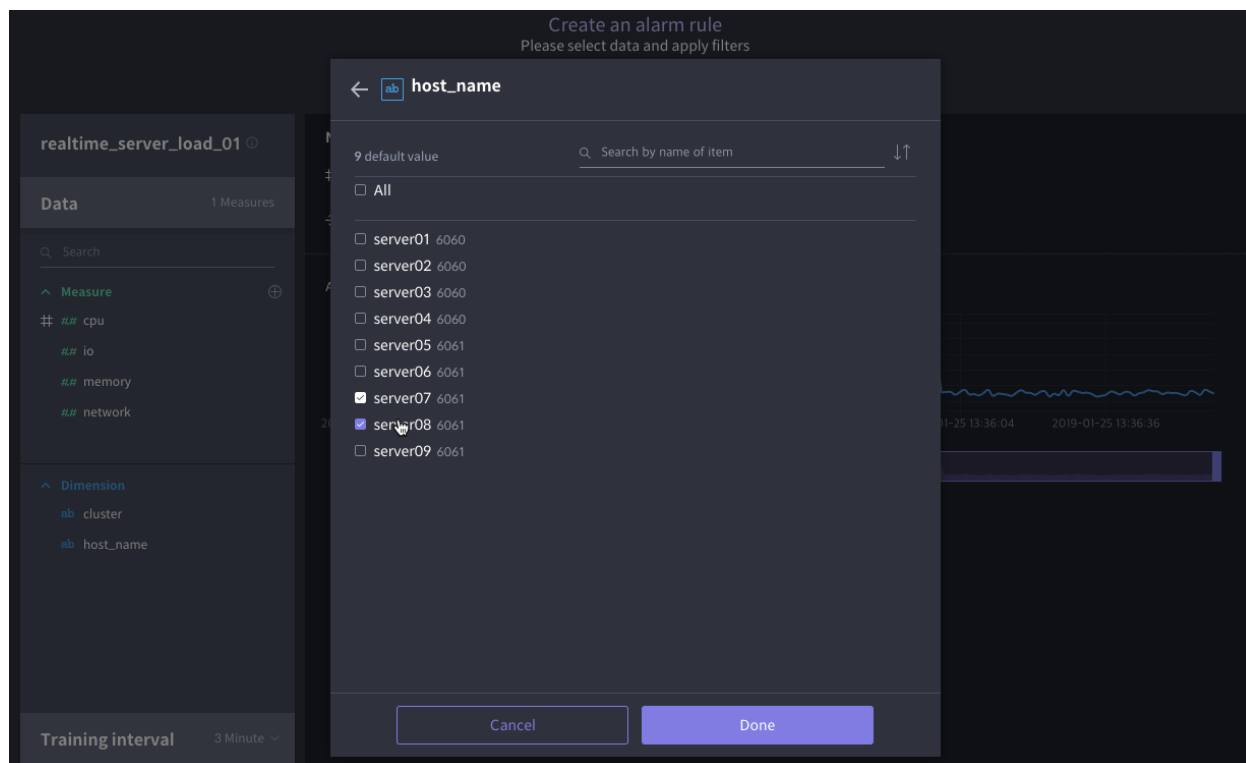
3. Aggregate 선반에 올려진 각 컬럼의 aggregate 타입 항목을 클릭하여 원하는 타입을 선택합니다.



4. 필요할 경우 차원값 컬럼을 기준으로 aggregate 데이터를 분할할 수 있습니다. **Dimension** 영역에서 분할의 기준으로 삼을 측정값 컬럼에 마우스 커서를 오버한 후  버튼을 클릭하십시오.



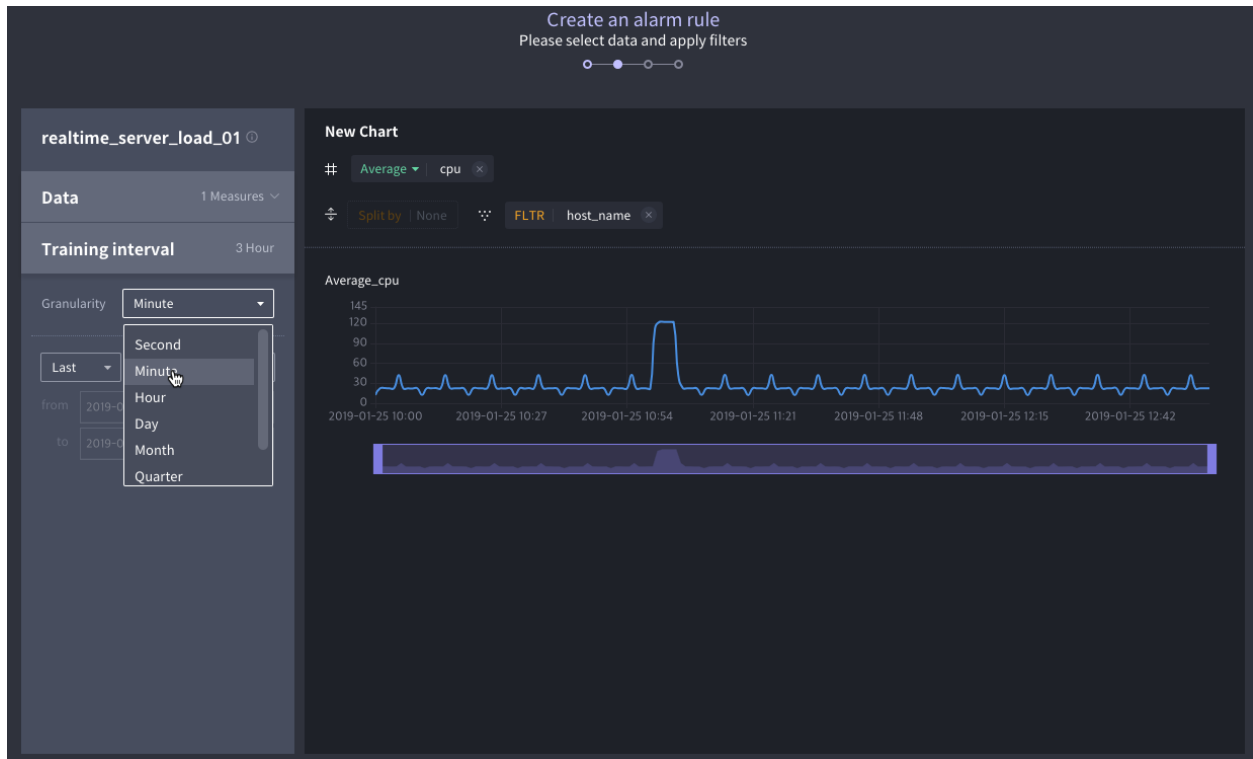
- 필요할 경우 차원값 컬럼을 기준으로 aggregate 데이터를 필터링할 수 있습니다. **Dimension** 영역에서 필터를 설정할 측정값 컬럼에 마우스 커서를 오버한 후  버튼을 클릭하십시오. 그런 다음, 모니터링하고자 하는 특정 범주들을 선택하십시오.



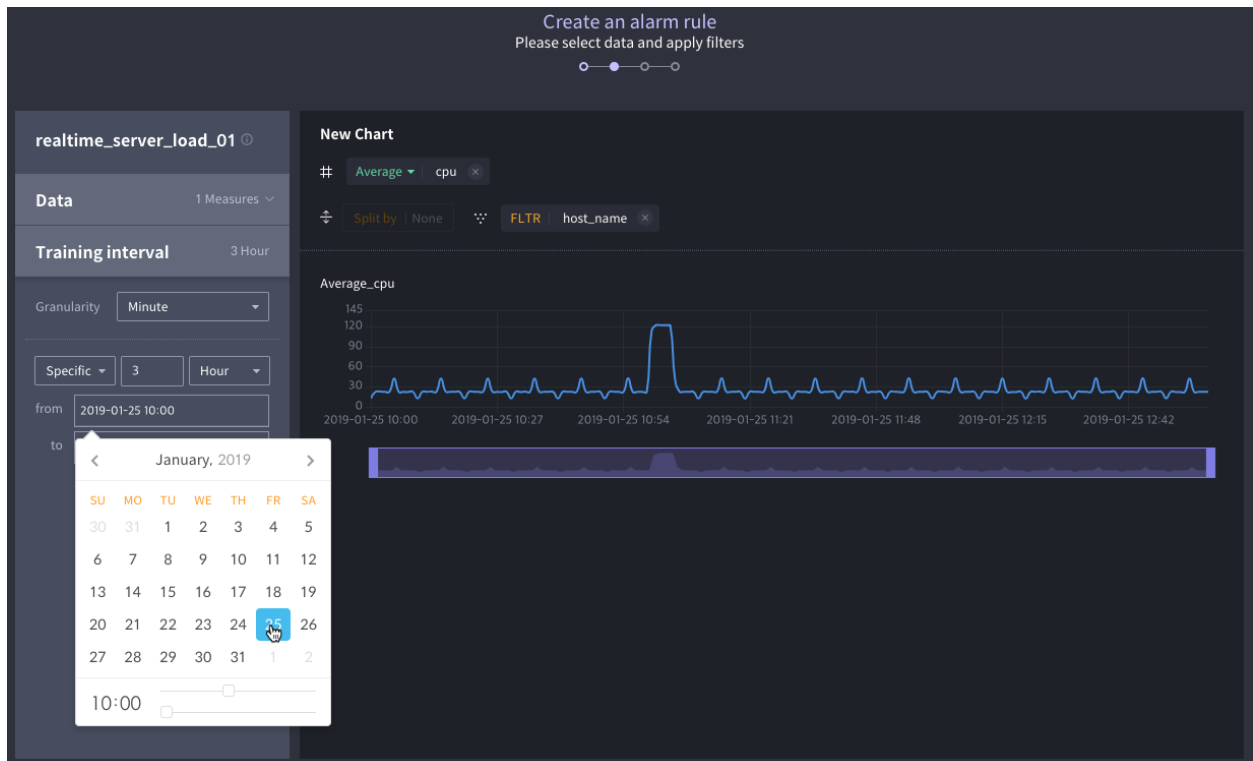
2.3 트레이닝 기간 설정하기

모니터링할 지표 선택을 마쳤으면, **Training interval** 패널에서 예측 모델 트레이닝에 사용할 데이터 범위를 선택할 수 있습니다.

1. 모델을 트레이닝시키는 데 사용할 데이터 세트의 주기를 **Granularity** 선택란에서 선택합니다.



2. 모델을 트레이닝시키는 데 사용할 데이터 세트의 기간 범위를 설정합니다.

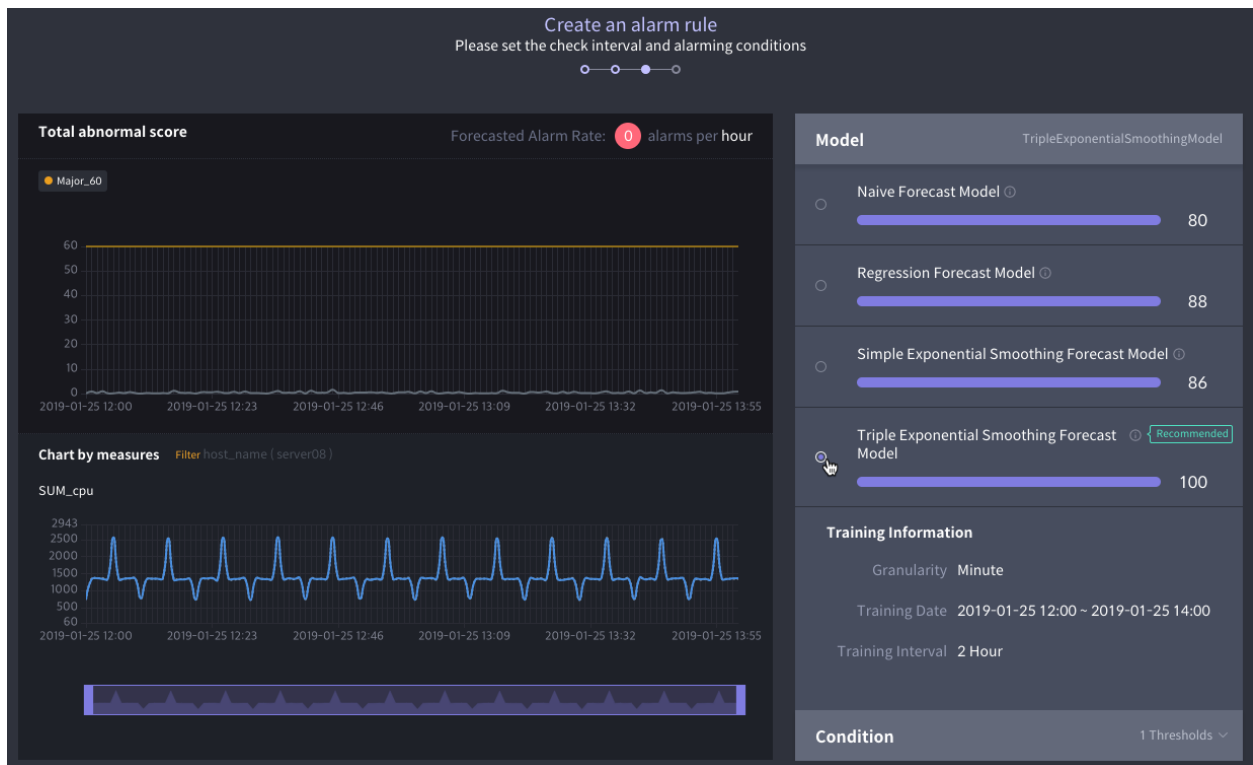


- 3. 모든 설정을 마쳤으면 **Next**를 클릭합니다.

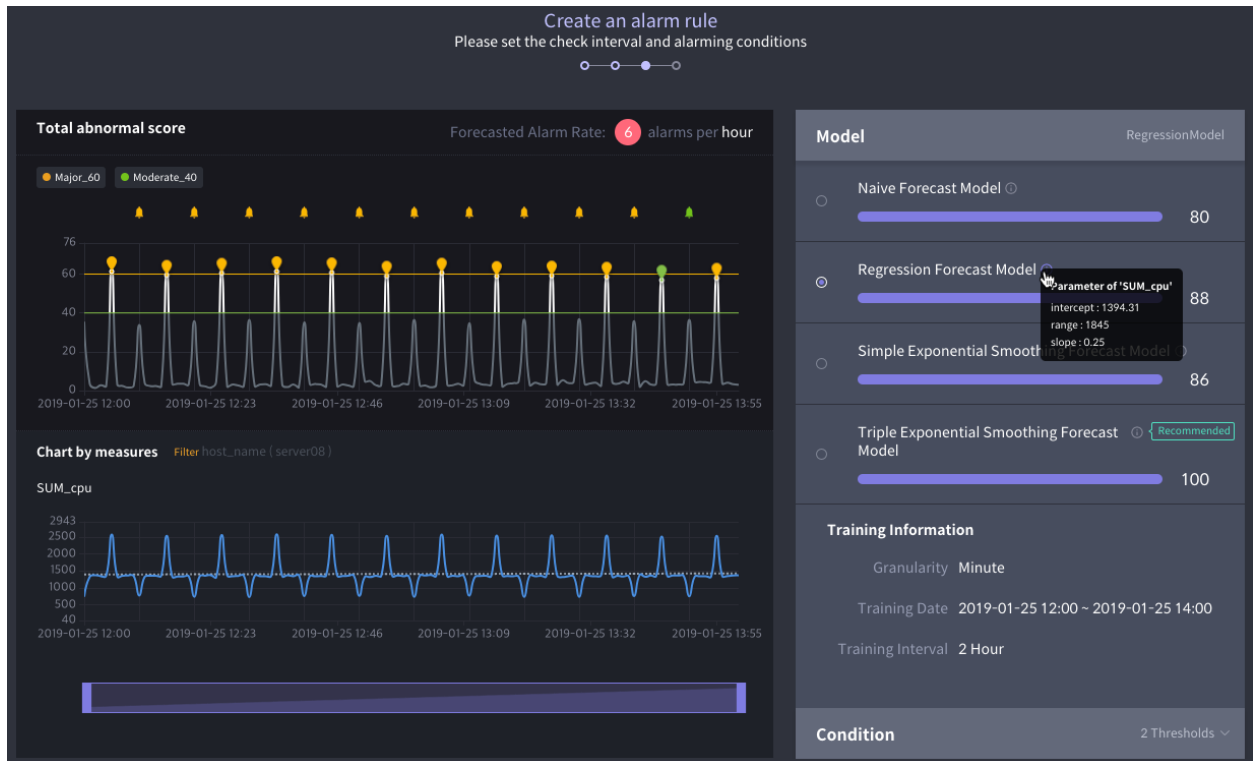
2.4 모델 선택하기

이제 **Model** 패널로 넘어가서 어떠한 예측 모델을 사용할지 선택합니다. Anomaly는 주어진 트레이닝 데이터 세트를 이용하여 각각의 모델을 트레이닝시킨 후 그 결과를 산출해줍니다. 아래 두 방법 중 하나를 통해 적합한 예측 모델을 선택하십시오.

- 기본적으로 우측에 표시되는 정확도 점수 (100점 만점)가 가장 높은 모델이 **Recommend** 표시와 함께 자동 선택 됩니다.




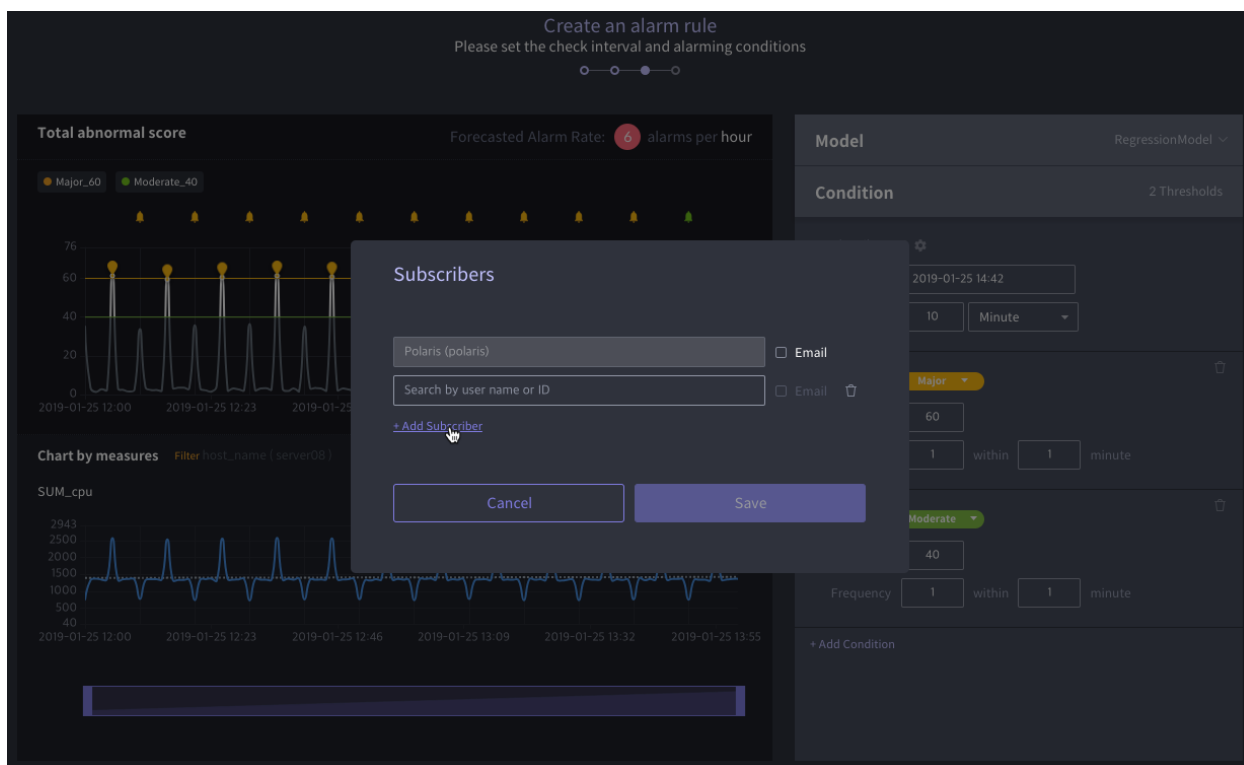
- 각 모델 항목 위에 마우스 커서를 오버하면 나타나는 상세 정보를 확인하여 가장 적합한 예측 모델을 직접 선택할 수 있습니다.



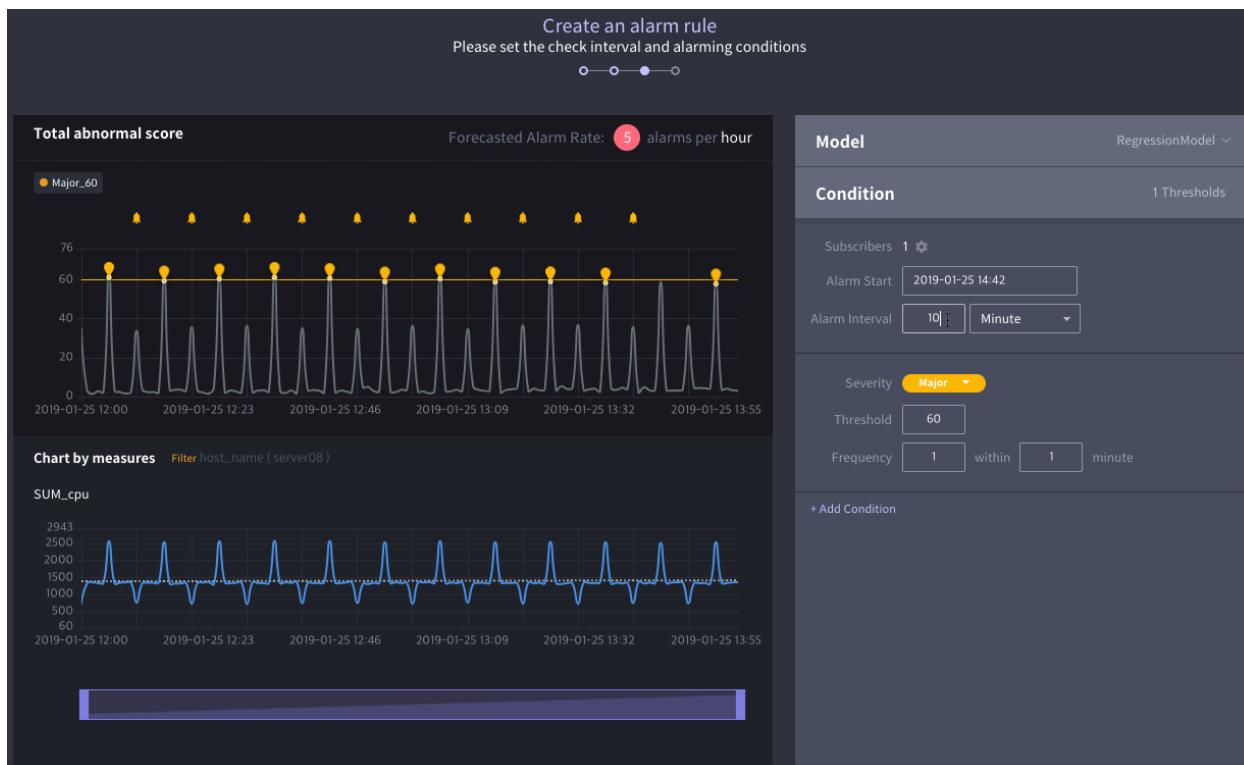
2.5 알람 룰 조건 설정하기

사용할 예측 모델을 선택하였으면, **Condition** 패널에서 알람이 발생하는 조건을 설정할 수 있습니다.

1. **Subscribers** 항목의 우측에 있는  버튼을 클릭하여 대화 상자를 연 후, 알람 발생 시 통보를 받는 대상과 방법을 설정합니다.

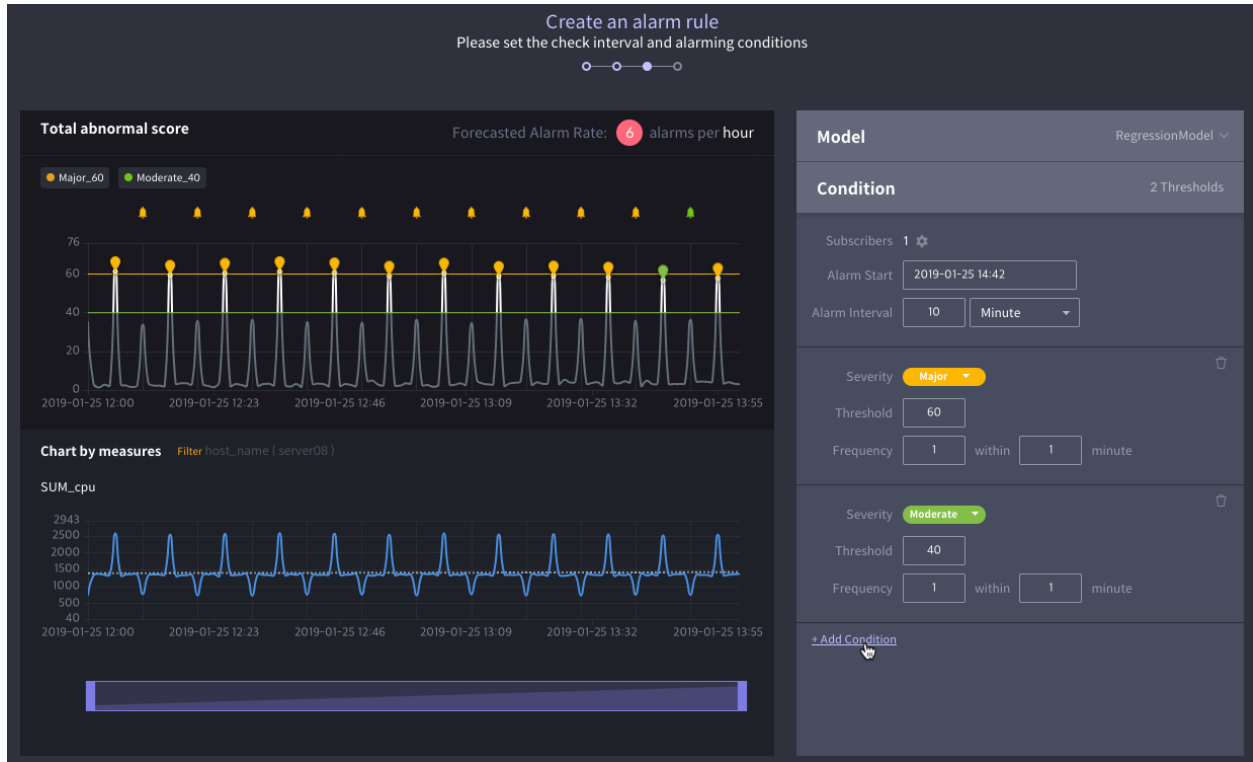


2. 아래 각 항목의 설명을 참고하여 알람이 발동되는 시기를 설정합니다.



- **Alarm Start:** 알람을 개시할 때를 설정합니다. 이 설정값에 해당하는 시간 이후부터 알람이 개시됩니다.
- **Alarm Interval:** 알람의 조건이 충족되었을 때 알람을 발생시키는 주기를 설정합니다.

3. 아래 각 항목의 설명을 참고하여 모니터링 대상 데이터의 abnormal score에 따른 알람 발동 조건을 설정합니다. 기본적으로 하나의 조건이 주어지며, + Add Condition 버튼을 클릭하면 조건을 추가할 수 있습니다.



- **Severity:** 주어진 조건에 해당하는 알람의 심각도를 설정합니다.
- **Threshold:** abnormal score가 이 설정값을 초과하면 데이터 이상 상태로 간주됩니다.
- **Frequency:** abnormal score가 한계값을 초과하는 빈도가 어떠한 때 알람을 발생시킬지 결정합니다. 예를 들어, 《3 within 5 minute》로 설정한 경우에는 abnormal score가 5분 안에 3회 이상 한계값을 초과하면 알람이 발생합니다.

4. 모든 설정을 마쳤으면 **Next**를 클릭합니다.

2.6 알람 룰 완성하기

알람 룰 설정이 끝났으면 아래와 같이 알람 룰 만들기 절차를 마무리합니다.

1. 알람 룰의 이름과 설명을 기입한 후 **Done** 버튼을 클릭합니다.

Create an alarm rule

Please set the check interval and alarming conditions

Datasource	realtime_server_load_01
Measure	cpu
Conditions	2
Forecasted rate	6 alarms per hour
Notification	1

Name

my_sample_rule_01

Description

Please enter a description

2. 생성된 알람 룰은 알람 룰 리스트의 최상단에 노출되고, 첫 알람 수행이 있기 전까지 **Prepare** 상태로 표시됩니다.

Anomaly

Statistics Alarm Alarm Rule [+ Create Alarm Rule](#)

All Current Status All

There are 13 items

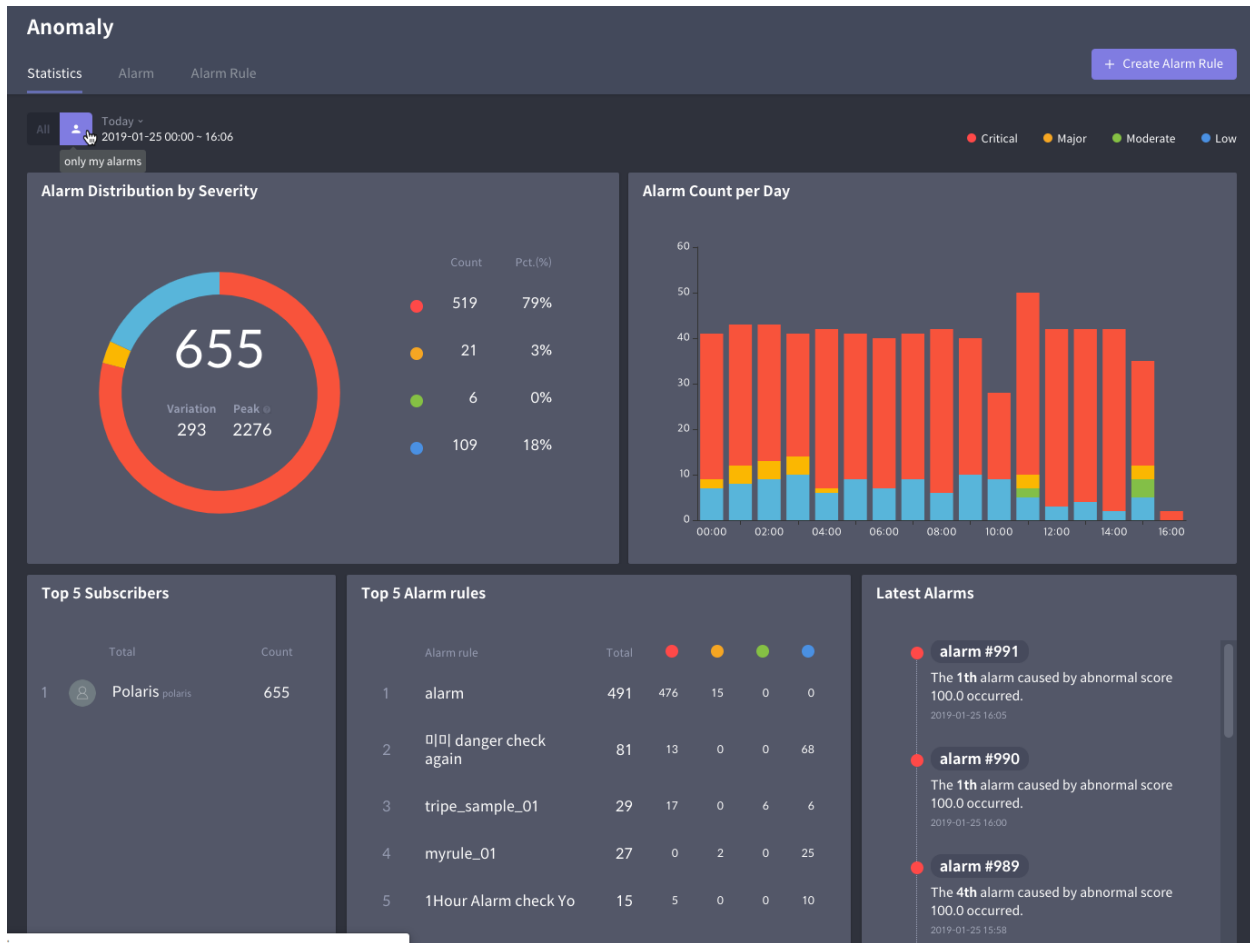
Current Status	Alarm Rule Name	DataSource	Measure	Alarm Interval	Condition	Alarm	Updated
Prepared	my_sample_rule_01	realtime_server_load_01	cpu	10 Minute	2	0	2019-01-25 14:48 by polaris
Normal	미미 danger check again	realtime_server_load_01	cpu	1 Minute	4	865	2019-01-25 14:46 by system
Normal	myrule_01	realtime_server_load_01	cpu	10 Minute	3	95	2019-01-25 14:21 by system
Normal	tripe_sample_01	realtime_server_load_01	cpu	1 Minute	4	127	2019-01-25 11:29 by system
Normal	sample_012	realtime_server_load_01	io, cpu	5 Minute	1	29	2019-01-25 11:15 by system
Abnormal	alarm	realtime_server_load_01	cpu	1 Minute	2	979	2019-01-25 02:39 by system
Abnormal	1Hour Alarm check Yo	realtime_server_load_01	cpu	1 Hour	2	3	2019-01-23 18:30 by system
Normal	server07_anomaly_real	realtime_server_load_01	cpu	2 Minute	2	221	2019-01-23 13:12 by system
Normal	server07_anomaly	realtime_server_load_01	cpu	2 Minute	2	129	2019-01-23 13:12 by system

CHAPTER 3

통계

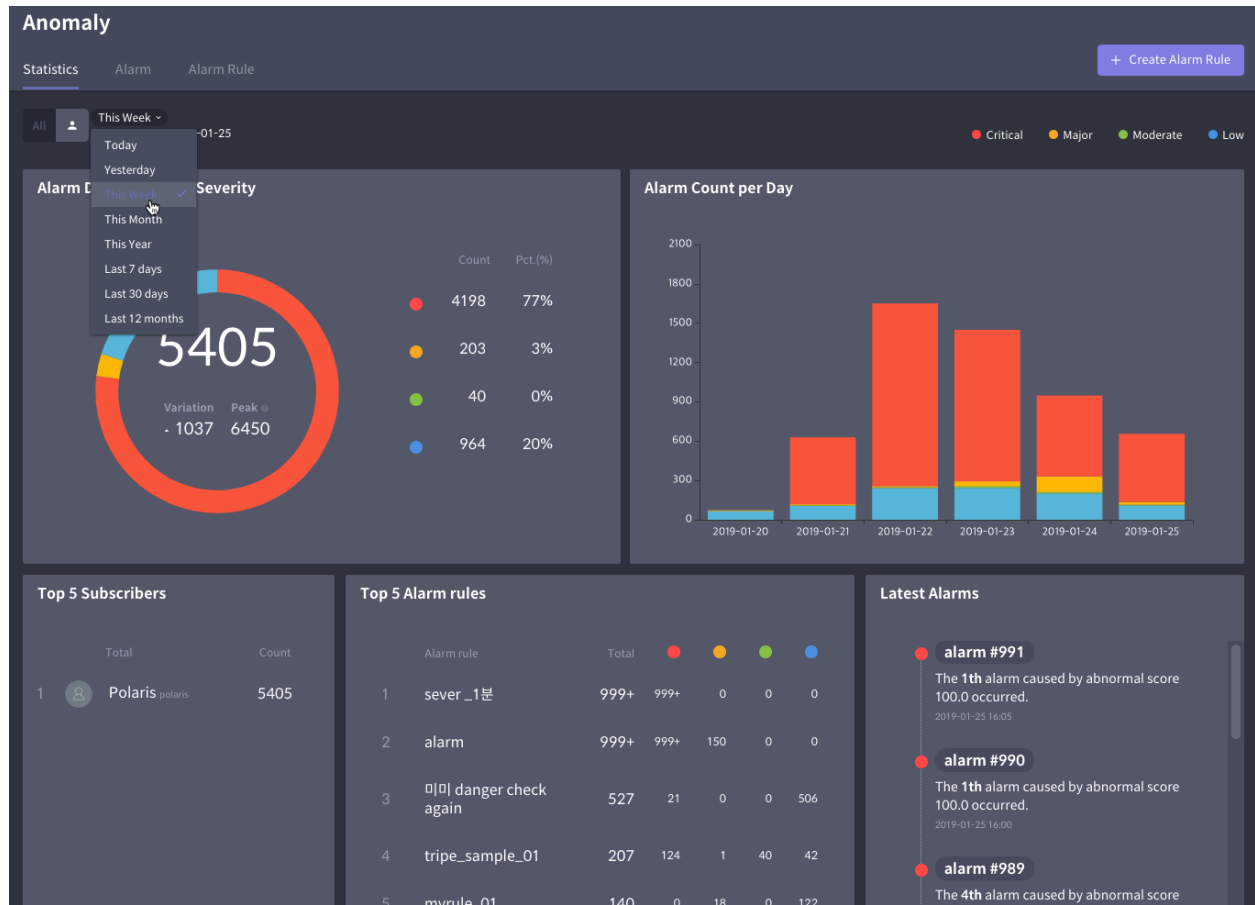
Statistics 탭 메뉴에서는 발생한 알람의 전반적인 통계를 보여줍니다. 이 페이지에서는 사용자가 지금까지 발생한 알람의 현황을 다각도로 파악할 수 있도록 중요도, 알람 발생 시기, 알람 룰 등의 다양한 기준으로 통계를 산출하여 제시합니다.

페이지 기본 구성은 다음과 같습니다.



- **Alarm Distribution by Severity:** 심각도별 알람 발생 비중을 보여줍니다.
- **Alarm Count per Time:** 시간대별 알람 빈도를 보여줍니다.
- **Top 5 Subscribers:** 가장 많은 알람을 통보받은 사용자 5명을 보여줍니다.
- **Top 5 Alarm rules:** 가장 많은 알람을 일으킨 알람 룰 5개를 보여줍니다.
- **Latest Alarms:** 가장 최근에 발생한 알람들을 보여줍니다.

페이지 상단의 기간 설정 메뉴를 이용하면 통계를 산출하는 기준 기간을 변경할 수 있습니다.



알람 룰 내역 열람 · 수정하기

Alarm Rule 탭 메뉴에서는 등록된 알람 룰을 열람 · 수정할 수 있습니다. 또한 이 메뉴에서는 선택한 예측 모델에 따라 산출되고 있는 데이터 abnormal score 현황도 쉽게 파악할 수 있습니다.

알람 룰 메뉴는 다음의 두 가지 페이지로 구성되어 있습니다.

- [알람 룰 리스트](#)
- 알람 룰 상세

4.1 알람 룰 리스트

Alarm Rule 탭으로 들어가면 현재 등록된 알람 룰들을 열거하여 보여줍니다.

Anomaly

Statistics Alarm Alarm Rule [+ Create Alarm Rule](#)

All Current Status All

There are 13 items

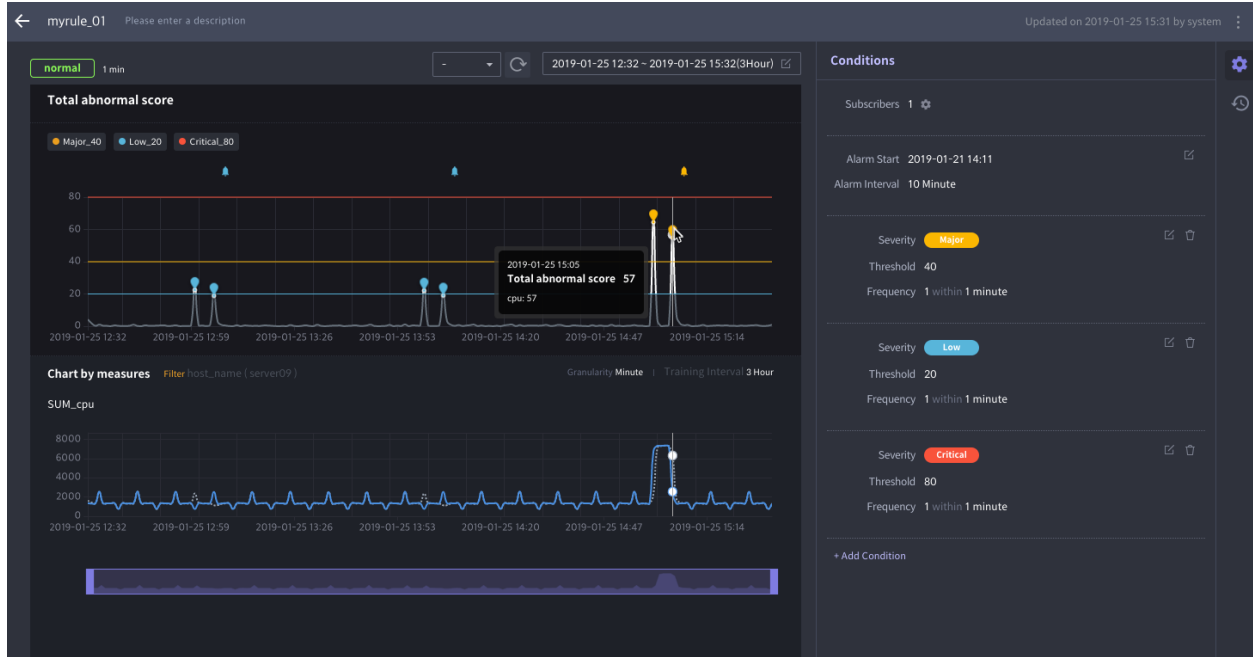
Current Status	Alarm Rule Name	DataSource	Measure	Alarm Interval	Condition	Alarm	Updated
Prepared	my_sample_rule_01	realtime_server_load_01	cpu	10 Minute	2	0	2019-01-25 14:48 by polaris
Normal	미미 danger check again	realtime_server_load_01	cpu	1 Minute	4	865	2019-01-25 14:46 by system
Normal	myrule_01	realtime_server_load_01	cpu	10 Minute	3	95	2019-01-25 14:21 by system
Normal	tripe_sample_01	realtime_server_load_01	cpu	1 Minute	4	127	2019-01-25 11:29 by system
Normal	sample_012	realtime_server_load_01	io, cpu	5 Minute	1	29	2019-01-25 11:15 by system
Abnormal	alarm	realtime_server_load_01	cpu	1 Minute	2	979	2019-01-25 02:39 by system
Abnormal	1Hour Alarm check Yo	realtime_server_load_01	cpu	1 Hour	2	3	2019-01-23 18:30 by system
Normal	server07_anomaly_real	realtime_server_load_01	cpu	2 Minute	2	221	2019-01-23 13:12 by system
Normal	server07_anomaly	realtime_server_load_01	cpu	2 Minute	2	129	2019-01-23 13:12 by system


리스트에 표시되는 정보는 아래와 같으며, 이를 기준으로 열거할 룰을 필터링하거나 검색할 수 있습니다.

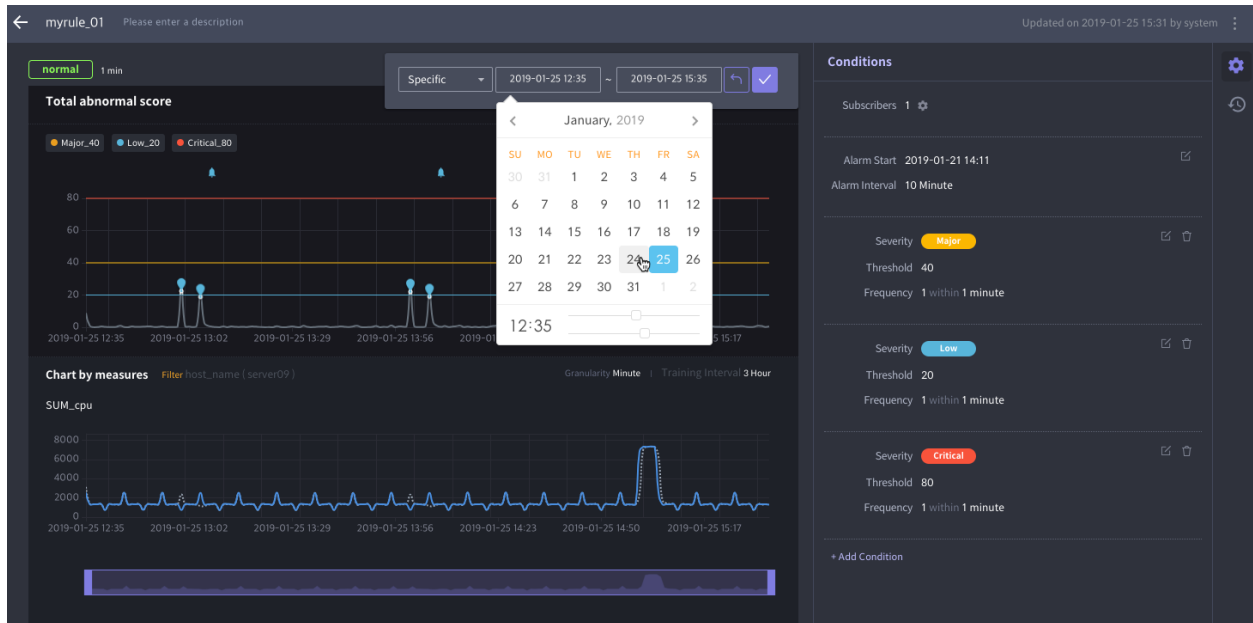
- **Current Status:** 해당 룰에 따른 모니터링 결과 상태
- **Alarm Rule Name:** 해당 룰의 이름
- **DataSource:** 모니터링 대상 데이터 소스
- **Measure:** 모니터링 대상 측정값 컬럼
- **Alarm Interval:** 알람 발생 주기
- **Condition:** 해당 룰에 적용된 알람 발생 조건의 개수
- **Alarm:** 해당 룰에 의해 발생한 알람의 수
- **Running:** 해당 룰의 모니터링 활성 여부
- **Updated:** 해당 룰을 마지막으로 업데이트한 시간과 사용자

4.2 알람 룰 상세

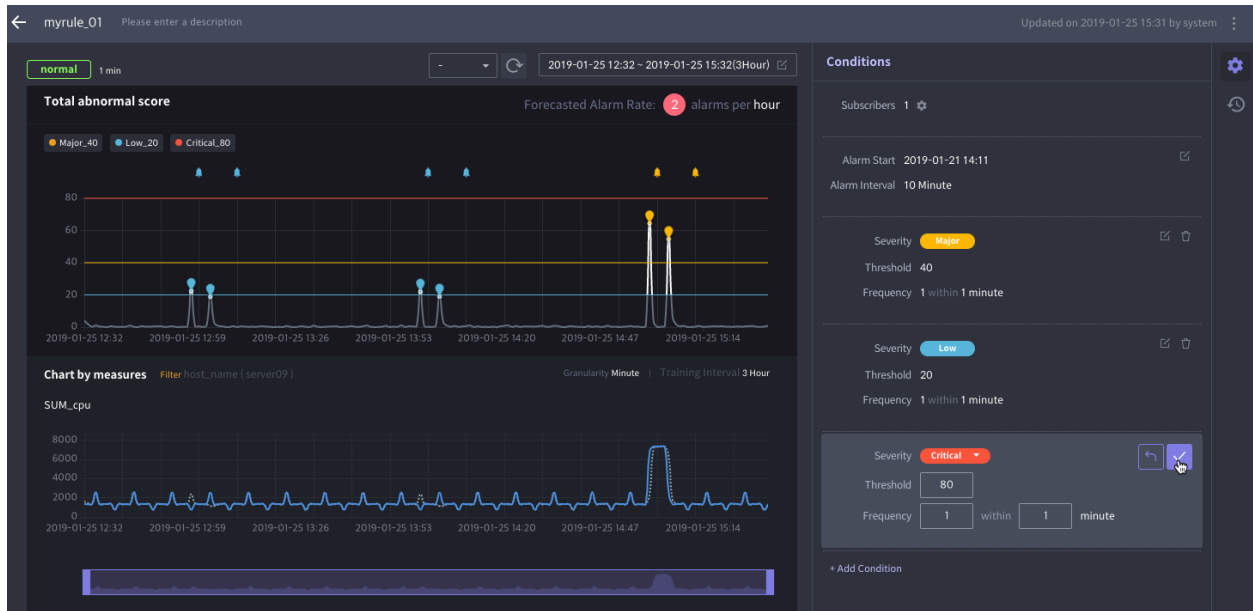
알람 룰 리스트에 열거된 항목 중 하나를 선택하면 해당 알람 룰에 대한 상세 정보를 열람하고 설정을 수정할 수 있습니다. 화면 좌측에서는 모니터링 현황을 시각화하여 보여주고, 우측에는 알람 룰 조건 설정값이 표시됩니다.





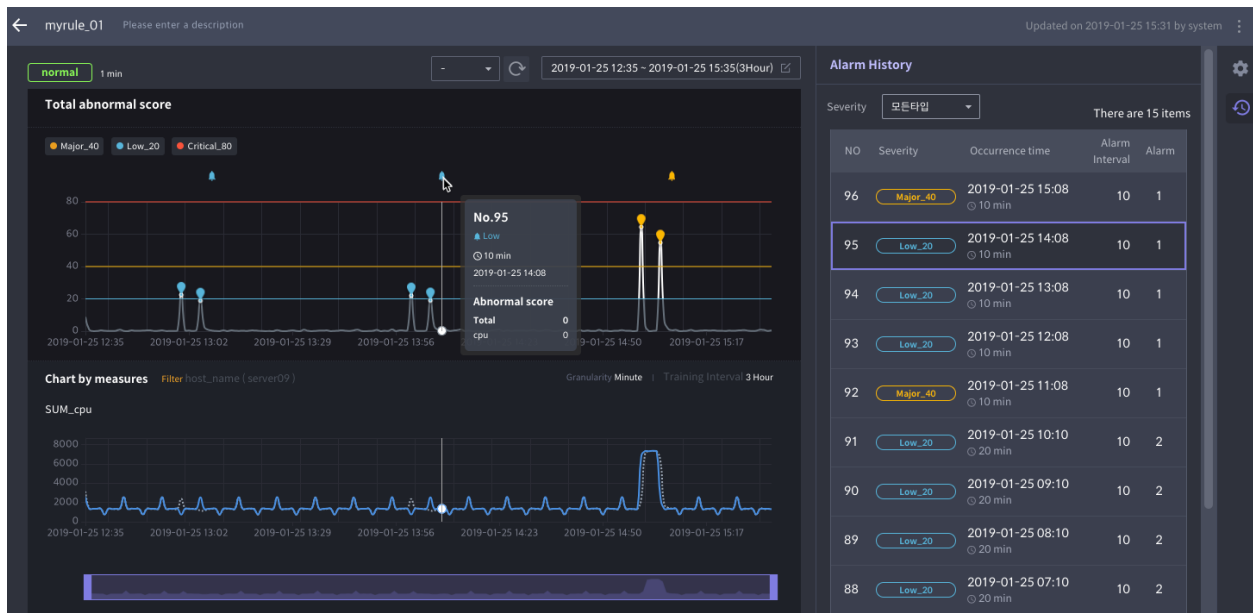
모니터링 현황 영역 상단에는 화면에 보여주는 모니터링 기간 설정값이 표시되어 있습니다.  아이콘을 클릭하면 기간 설정값을 변경할 수 있습니다.



알람 룰 조건 설정 영역에서는 기존에 설정된 알람 룰 설정값을 수정할 수 있습니다. 자세한 내용은 [알람 룰 조건 설정하기](#) 항목을 참조하십시오.



우측 끝단에서  버튼을 누르면 Conditions 패널이 Alarm History 패널로 전환되어 지금까지 발생한 알람 이력을 보여줍니다 (다시  버튼을 누르면 Conditions 패널로 되돌아옵니다).



알람 내역 열람하기

Alarm 탭 메뉴에서는 지금까지 발생한 알람 내역을 확인할 수 있습니다. 알람의 전체적인 현황을 보여주는 [통계](#) 페이지와는 다르게 이 메뉴에서는 보다 개별적인 알람들을 열람하고 탐색하는 데 최적화된 UI를 제공합니다.

이 메뉴는 다음의 두 가지 페이지로 구성되어 있습니다.

- [알람 리스트](#)
- [알람 상세](#)

5.1 알람 리스트

Alarm 탭으로 들어가면 현재까지 발생한 알람들을 열거하여 보여줍니다. 화면 상단에 있는 Alarm rule / Timeline 선택 박스를 이용하여, 알람 리스트를 알람 룰 기준으로 정렬할 수도 있고, 발생한 시간 기준으로 정렬할 수도 있습니다.

- Alarm rule (알람 룰 기준으로 정렬)

Anomaly

Statistics
Alarm
Alarm Rule

+ Create Alarm Rule

All

Alarm rule

Show Unchecked Only

Latest Alarms

Low_2

2019-01-25 15:28

▲ 1 ○ 1 min

미미 danger check again #867

realtime_server_load_01

Critical_50

2019-01-25 15:27

▲ 5 ○ 300 min

1Hour Alarm check Yo #3

realtime_server_load_01

Moderate_40

2019-01-25 15:16

▲ 4 ○ 4 min

tripe_sample_01 #132

realtime_server_load_01

Critical_80

2019-01-25 15:11

▲ 4 ○ 4 min

tripe_sample_01 #131

realtime_server_load_01

Major_40

2019-01-25 15:11

▲ 1 ○ 10 min

myrule_01 #96

realtime_server_load_01

☆ alarm 989

2019-01-25 15:58:58

▲ 4 ○ 240sec

alarm #989

realtime_server_load_01

☆ alarm 988

2019-01-25 15:51:57

▲ 1 ○ 60sec

alarm #988

realtime_server_load_01

☆ alarm 987

2019-01-25 15:31:58

▲ 1 ○ 60sec

alarm #987

realtime_server_load_01

☆ alarm #986

2019-01-25 15:01:58

▲ 2 ○ 120sec

alarm #986

realtime_server_load_01

☆ alarm #985

2019-01-25 15:01:58

▲ 1 ○ 60sec

alarm #985

realtime_server_load_01

Show all

☆ 미미 danger check again 868

2019-01-25 15:45:00

Low_2

2019-01-25 15:28:00

Low_2

2019-01-25 15:06:00

Low_2

2019-01-25 14:04:00

Low_2

2019-01-25 13:02:00

- Timeline (발생 시간 기준으로 정렬)

Anomaly

Statistics
Alarm
Alarm Rule

+ Create Alarm Rule

All

Timeline

Show Unchecked Only

Today 167

Yesterday 666

This Week 1160

Critical_80

60sec

▲ 1

alarm #364

realtime_server_load_01

2019-01-24 08:58

Critical_80

60sec

▲ 1

alarm #363

realtime_server_load_01

2019-01-24 08:57

Low_2

1 min

▲ 1

미미 danger check again #743

realtime_server_load_01

2019-01-24 08:56

Critical_80

60sec

▲ 1

alarm #362

realtime_server_load_01

2019-01-24 08:55

Critical_80

120sec

▲ 2

alarm #361

realtime_server_load_01

2019-01-24 08:53

Critical_80

120sec

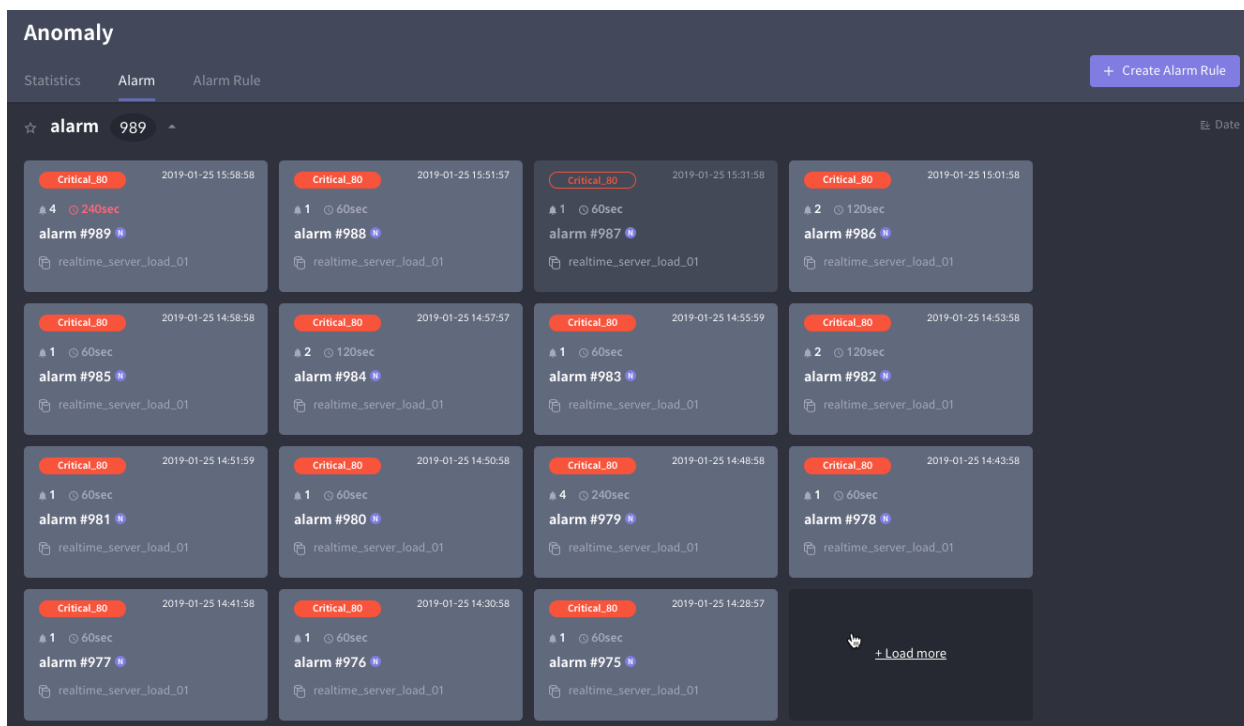
▲ 2

alarm #360

realtime_server_load_01

2019-01-24 08:51

카테고리 맨 끝에 있는 + Load more를 클릭하면 해당 카테고리 내 더 많은 알람 항목을 보여줍니다.

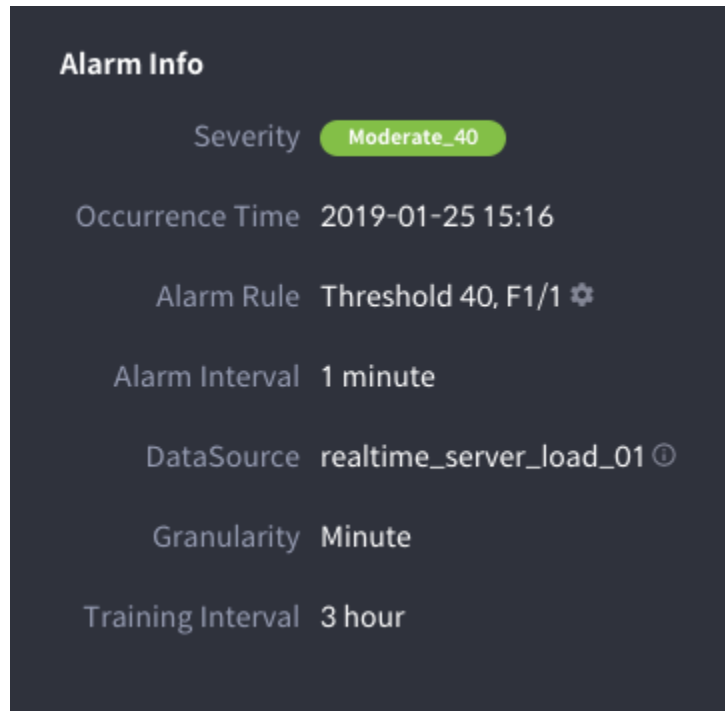


5.2 알람 상세

알람 리스트에 열거된 항목 중 하나를 선택하면 해당 알람에 대한 상세 정보를 열람할 수 있습니다. 아래는 알람 상세 페이지의 각 영역별 설명입니다.

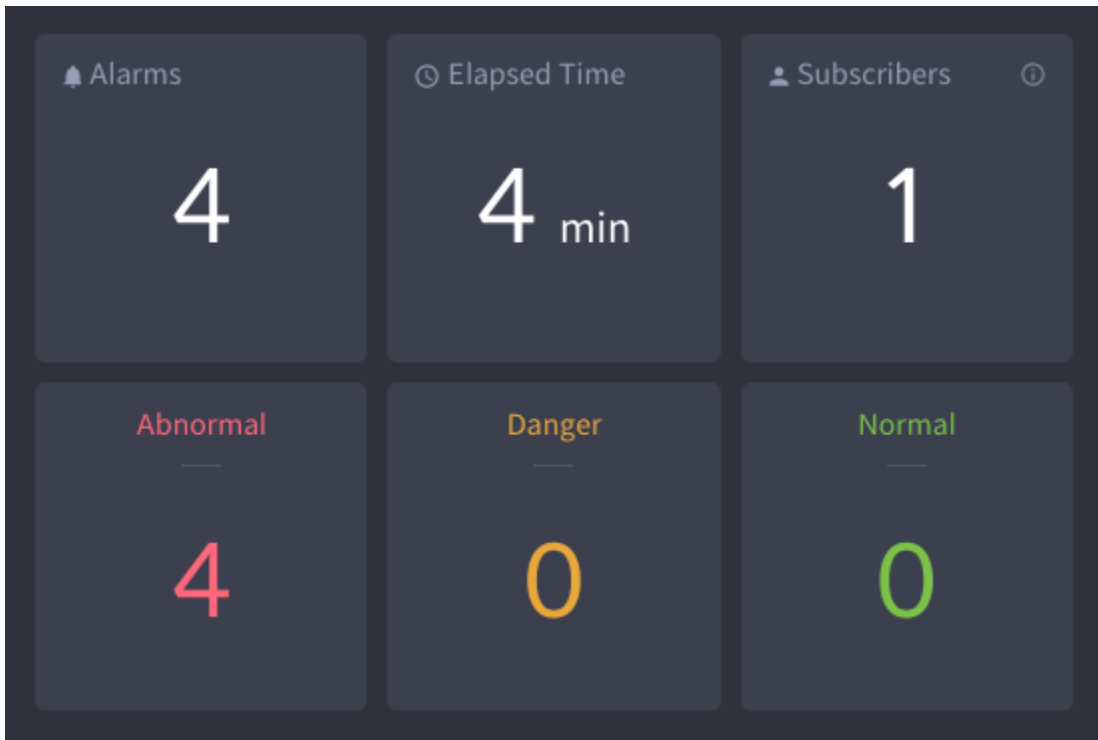
5.2.1 Alarm Info 영역

이 영역에서는 해당 알람의 심각도와 발생 시각, 그리고 이 알람을 발생시킨 룰의 설정값을 보여줍니다.



5.2.2 알람 현황 일람 상자

이 영역에서는 해당 알람의 발생 현황을 보여줍니다. 정해진 주기에 따라 알람이 연속적으로 발생하면 1개의 알람 항목으로 계속 유지됩니다. 아래 그림 예시에서는 알람이 4번의 주기 동안 연속적으로 발생하였고 (Alarms), 주기가 1분이었기 때문에 4건의 알람이 총 4분 동안 지속된 것입니다 (Elapsed Time).



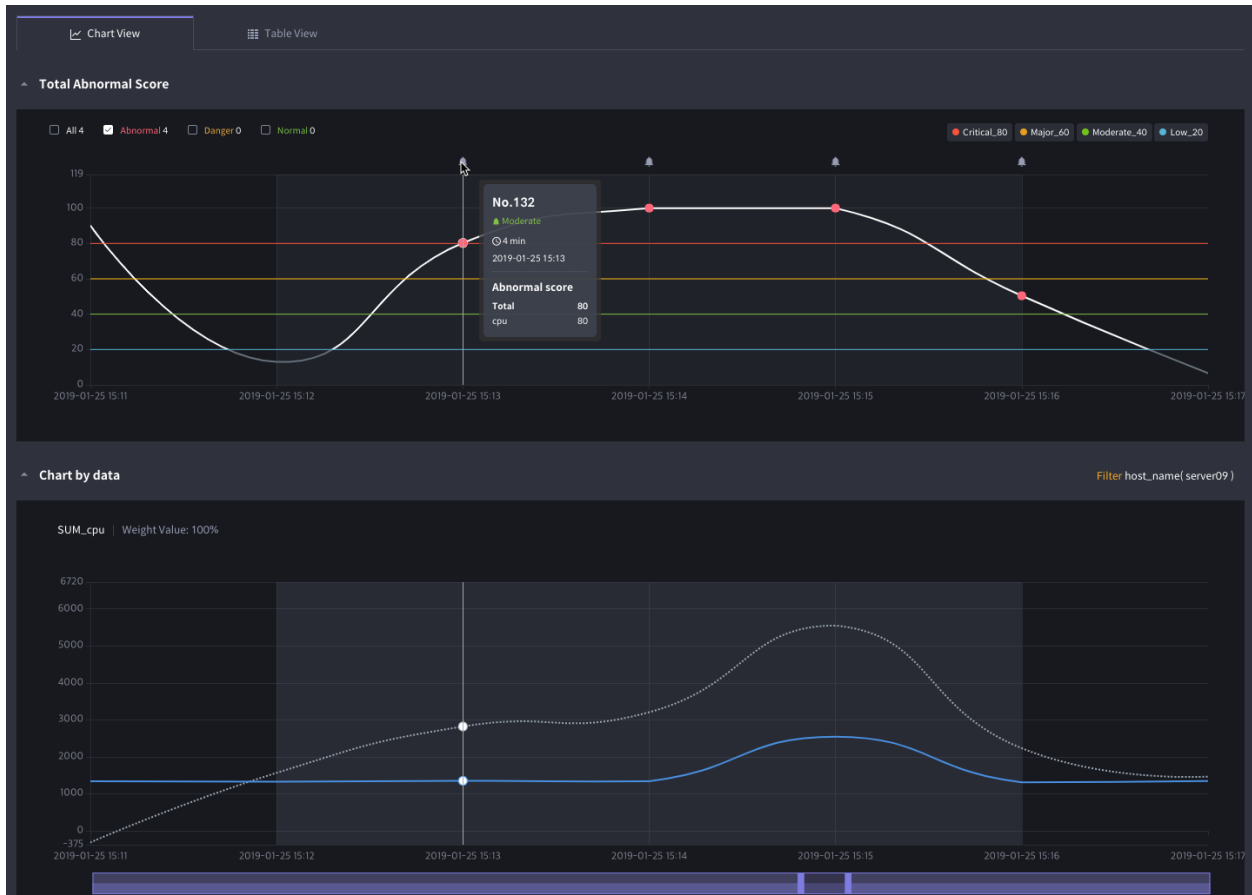
5.2.3 Alarm History 영역

이 영역에서는 해당 알람에 적용된 알람 룰에 의해 발생한 알람의 이력을 보여줍니다.

Alarm History				
NO	Severity	Occurrence time	Alarm Interval	Alarm
132	Moderate_40	2019-01-25 15:16 ⌚ 4 min	1 minute	4
131	Critical_80	2019-01-25 15:11 ⌚ 4 min	1 minute	4
130	Critical_80	2019-01-25 15:06 ⌚ 2 min	1 minute	2
129	Critical_80	2019-01-25 15:03 ⌚ 1 min	1 minute	1
		2019-01-25 15:01		

5.2.4 Chart View 탭

이 탭 영역에서는 해당 알람 구간 내에서 모니터링한 aggregate 데이터의 abnormal score 추이를 차트로 보여줍니다. 여기서는 각 조건별 점수 한계값에 도달하여 상응하는 알람 (Critical, Major, Moderate, Low) 을 일으킨 발생 건도 보고해줍니다. 차트 산출 방식에 관해서는 [기본 원리](#) 항목을 참조하십시오.



- **Total abnormal score:** 알람 룰에 포함된 모든 측정값 컬럼에 대한 abnormal score를 보여줍니다.
- **Chart by measures:** 알람 룰에 포함된 각 개별 측정값 컬럼 데이터의 예측치와 실제치의 추이를 보여줍니다.

5.2.5 Table View 탭

이 탭 영역에서는 각 알람 발생 건별로 데이터 실제치와 예측치, 그리고 abnormal score를 보여줍니다.

		Abnormal Score Detail		SUM_cpu (Weight Value: 100%)		
		Occurrence time	Total Abnormal Score	Actual	Predict	Abnormal Score
1	●	2019-01-25 15:13	80	1352	2820	80
2	●	2019-01-25 15:14	100	1341	3207	100
3	●	2019-01-25 15:15	100	2545	5548	100
4	●	2019-01-25 15:16	50	1311	2233	50

