# OS基本監視項目(詳細)

## 1.死活監視(Linux,Windows共通)

### 1.1 監視対象

Linux,WindowsそれぞれのOSがインストールされているインスタンスを対象とします。

### 1.2 監視設定内容

mackerel-agentからのメトリックの投稿を定期的に監視します。
一定期間この投稿がない場合、Mackerelはそのホストに異常が発生したと判断してアラートを発生させます。

## 2. リソース監視(Linux,Windows共通)

### 2.1 監視対象

mackerel-agent インストール時に指定しているロールを監視対象とします。
ロール名は以下となります。

ロール名: KCPSCloudAutomation:kcps

### 2.2 監視項目

- CPU
- メモリ
- ディスク容量

### 2.3 監視設定内容

監視項目はいずれも Mackerel ではホストメトリック監視と呼ばれる監視方法を使用することになるため、その設定内容に準じます。

#### 2.3.1 CPU

| 設定項目 | 必須/任意 | 設定値 | 備考 |
|---|---|---|---|
| type | 必須 | host | 固定値 |
| name | 必須 | CPU% (KCPS) | 監視一覧などで参照できる任意の名称。<br>重複した値でも登録可能。 |
| duration | 必須 | 5 | 指定された間隔(分)の平均値を監視します。有効範囲：1~10分。 |
| metric | 必須 | cpu% | 監視対象のホストメトリック名。<br>特定の定数文字列を指定することで、割合監視が可能。 |
| operator | 必須 | > | 指定した数値より大きいか小さいかというアラート条件を指定。<br>">" または "<"。左辺が観測値で右辺が設定できます。 |
| warning | 必須 | 70 | warningのAlert発生の閾値。 |
| critical | 必須 | 70 | criticalのAlert発生の閾値。 |
| notificationInterval | 任意 | - | 通知の再送設定をするときの再送間隔 (分)。<br>このフィールドを省略すると通知は再送されません。 |

| | | | |
|---|---|---|---|
| scopes | 任意 | KCPSManagedOption:kcps | 監視対象のサービス名またはロール詳細名。 |
| excludeScopes | 任意 | - | 監視除外対象のサービス名またはロール詳細名。 |
| isMute | 任意 | - | 監視がミュート状態か否か設定します。 |

### 2.3.2 メモリ

| 設定項目 | 必須/任意 | 設定値 | 備考 |
|---|---|---|---|
| type | 必須 | host | 固定値 |
| name | 必須 | Memory% (KCPS) | 監視一覧などで参照できる任意の名称。<br>重複した値でも登録可能。 |
| duration | 必須 | 5 | 指定された間隔(分)の平均値を監視します。有効範囲：1~10分。 |
| metric | 必須 | memory% | 監視対象のホストメトリック名。<br>特定の定数文字列を指定することで、割合監視が可能。 |
| operator | 必須 | > | 指定した数値より大きいか小さいかというアラート条件を指定。<br>">" または "<"。左辺が観測値で右辺が設定できます。 |
| warning | 必須 | 70 | warningのAlert発生の閾値。 |
| critical | 必須 | 70 | criticalのAlert発生の閾値。 |
| notificationInterval | 任意 | - | 通知の再送設定をするときの再送間隔 (分)。<br>このフィールドを省略すると通知は再送されません。 |
| scopes | 任意 | KCPSManagedOption:kcps | 監視対象のサービス名またはロール詳細名。 |
| excludeScopes | 任意 | - | 監視除外対象のサービス名またはロール詳細名。 |
| isMute | 任意 | - | 監視がミュート状態か否かを設定します。 |

### 2.3.3 ディスク容量

| 設定項目 | 必須/任意 | 設定値 | 備考 |
|---|---|---|---|
| type | 必須 | host | 固定値 |
| name | 必須 | DISK% (KCPS) | 監視一覧などで参照できる任意の名称。<br>重複した値でも登録可能。 |
| duration | 必須 | 3 | 指定された間隔(分)の平均値を監視します。有効範囲：1~10分。 |
| metric | 必須 | disk% | 監視対象のホストメトリック名。<br>特定の定数文字列を指定することで、割合監視が可能です。 |
| operator | 必須 | > | 指定した数値より大きいか小さいかというアラート条件を指定。<br>">" または "<"。左辺が観測値で右辺が設定できます。 |
| warning | 必須 | 90 | warningのAlert発生の閾値。 |
| critical | 必須 | 90 | criticalのAlert発生の閾値。 |
| notificationInterval | 任意 | - | 通知の再送設定をするときの再送間隔 (分)。<br>このフィールドを省略すると通知は再送されません。 |
| scopes | 任意 | KCPSManagedOption:kcps | 監視対象のサービス名またはロール詳細名。 |
| excludeScopes | 任意 | - | 監視除外対象のサービス名またはロール詳細名。 |
| isMute | 任意 | - | 監視がミュート状態か否かを設定します。 |

## 3. イベントログ監視(Windowsのみ)

新たに提供される予定の check プラグインを使用します。

## 3.1 監視対象

Windows系OSがインストールされているインスタンス

## 3.2 監視設定内容

### 3.2.1 プラグイン定義

mackerel-agent.conf にプラグイン定義を記載します。

| 設定項目 | 必須/任意 | 設定値 | 備考 |
|---|---|---|---|
| 項目名 | 必須 | plugin.checks.kcps_eventlog | 設定ファイル用のキーで、"plugin.checks." で始まっている必要があり、<br>含まれるドットの数はちょうど2である必要があります。<br>2つめのドット以降は監視設定の名前として利用されます。 |
| command | 必須 | 項番3.3参照 | エージェントが定期的に実行し、<br>その終了ステータス/標準出力を監視結果として使用するコマンドです。 |
| motification_interval | 任意 | - | アラートの再送間隔を「分」で指定します。<br>省略した場合、アラートは再送通知されません。<br>10分未満は指定できません。<br>10分未満を指定した場合は、10分間隔で通知を再送します。 |
| max_check_attempts | 任意 | - | 指定した回数連続でOK以外の結果になった場合、アラートを発報します。<br>たとえば3が設定されている場合、<br>監視結果が直近3回すべてOKでなかった場合にアラートとなります。 |
| check_interval | 任意 | - | チェック監視の実行間隔を「分」で指定します。デフォルト値は1分です。<br>設定可能な範囲は1分から60分で、1分未満の場合は1分、<br>60分以上を指定した場合は60分間隔で監視が実行されます |

### 3.2.2 check-windows-eventlog プラグインオプション設定

check-windows-eventlog プラグインに指定するオプションの設定値を記載します。

| 設定項目 | 必須/任意 | 設定値 | 備考 |
|---|---|---|---|
| --log | 任意 | - | 検知対象のログタイプを指定します。指定可能なタイプは<br>・Application<br>・Security<br>・System<br>です。<br><br>指定しない場合はApplicationログが検知対象となます<br><br>※複数指定する場合はカンマ区切り |
| --type | 任意 | Error | 検知対象のイベントタイプを指定します。指定可能なタイプは<br>・Success<br>・Error<br>・Audit Failure<br>・Audit Success<br>・Information<br>・Warning<br>です。<br><br>指定しない場合はイベントタイプでの絞り込みは行いません<br><br>※複数指定する場合はカンマ区切り |
| --source-pattern | 任意 | - | イベントログの “ソース” に対しての絞り込みを行います。正規表現の指定が可能です。 |
| --message-pattern | 任意 | - | イベントログのメッセージに対しての絞り込みを行います。正規表現の指定が可能です。 |
| --warning-over | 任意 | - | 指定した値以上のwarningが検知された場合、アラートを通知します。 |
| --critical-over | 任意 | - | 指定した値以上のcriticalが検知された場合、アラートを通知します。 |
| --return | 任意 | 設定 | 検知した行をmackerelへ送信して、検知した行の内容をMackerel管理画面から確認できます。<br>指定しない場合はfalseです。 |

| | | | |
|---|---|---|---|
| --fail-fast | 任意 | - | checkの初回実行時に、過去に出力されたすべてのレコードを検知対象とします。<br>falseの場合はcheckの初回実行以降に出力されたログのみを対象とします。<br>指定しない場合はfalseです。 |

### 3.3 conf ファイル定義

実際にmackerel-agent.confの内容を記載します。

mackerel-agent.conf

```
apikey = "API"
apibase = "http://198.18.0.16/"

roles = ["KCPSManagedOption:kcps"]

[plugin.checks.kcps_eventlog]
command ='''check-windows-eventlog.exe --type=Error --return'''
```

## 4. ログ監視(Linuxのみ)

check-log プラグインを使用して監視します。

check-log プラグインの使い方については mackerel のヘルプ「ログ監視をおこなう」を参照してください。

### 4.1 監視対象

Linux(RedHat/CentOS)系OSがインストールされているインスタンス

### 4.2 監視設定内容

#### 4.2.1 プラグイン定義

mackerel-agent.conf にプラグイン定義を記載します。

| 設定項目 | 必須/任意 | 設定値 | 備考 |
|---|---|---|---|
| 項目名 | 必須 | plugin.checks.kcps_log_messages | 設定ファイル用のキーで、"plugin.checks." で始まっている必要があり、<br>含まれるドットの数はちょうど2である必要があります。<br>2つめのドット以降は監視設定の名前として利用されます。 |
| command | 必須 | 項番4.3参照 | エージェントが定期的に実行し、<br>その終了ステータス/標準出力を監視結果として使用するコマンドです。 |
| motification_interval | 任意 | - | アラートの再送間隔を「分」で指定します。<br>省略した場合、アラートは再送通知されません。<br>10分未満は指定できません。<br>10分未満を指定した場合は、10分間隔で通知を再送します。 |
| max_check_attempts | 任意 | - | 指定した回数連続でOK以外の結果になった場合、アラートを発報します。<br>たとえば3が設定されている場合、<br>監視結果が直近3回すべてOKでなかった場合にアラートとなります。 |
| check_interval | 任意 | - | チェック監視の実行間隔を「分」で指定します。デフォルト値は1分です。<br>設定可能な範囲は1分から60分で、1分未満の場合は1分、<br>60分以上を指定した場合は60分間隔で監視が実行されます |

#### 4.2.2 check-log プラグインオプション設定

check-log プラグインに指定するオプションの設定値

| 設定項目 | 必須/任意 | 設定値 | 備考 |
|---|---|---|---|
| --file | 必須 | /var/log/messages | 監視対象のファイルパス |
| --pattern | 必須 | warning<br>error<br>emerg<br>alert<br>critical | 検出したい文言のパターンを正規表現で指定します。 |
| --exclude | 任意 | - | 検出された文言から除外したいパターンを正規表現で指定します。 |
| --warning-over | 任意 | - | 設定値より多くエラー行が検出された場合にwarning |
| --critical-over | 任意 | - | 設定値より多くエラー行が検出された場合にcritical |
| --return | 任意 | 設定 | エラー行が出力され、その内容がMackerelに送信して、<br>検知した行の内容をMackerel管理画面から確認できます。<br><br>ご利用の際には秘匿情報などが意図せず送信されないようにご注意下さい。<br>また、送信内容のサイズが大きい場合、表示が切り詰められることがあります。 |

## 4.3 conf ファイル定義

実際にmackerel-agent.confの内容を記載します。

mackerel-agent.conf

```
apikey = "API"
apibase = "http://198.18.0.16/"

roles = ["KCPSManagedOption:kcps"]

[plugin.checks.kcps_log]
command = '''check-log --file /var/log/messages --pattern
'warning|error|emerg|alert|critical' --return'''
```