Virtual LC

5. ログ管理

5. ログ管理

1. ログ閲覧

ログの管理はサーバー管理者の最も重要な仕事の一つです。「ログ管理」では、各種サービスのログを確認したり、監視したりすることができます。

各サービスが記録したログファイルを閲覧します。

■ ログ閲覧

「ログ閲覧」のメニューをクリックすると、ログ閲覧画面が表示されます。

ここでは、ログファイルの内容を表示します。またクライアント側にダウンロードしてログを保存することができます。

プルダウンメニューより閲覧したいログファイルを選択します。

次に、プルダウンメニューより「先頭」もしくは「末尾」からのログファイルの行数を指定します。

「ダウンロード」または「表示」を選択し、ログを閲覧します。

2. ログ監視

Linux でサーバーを立てている場合バックグラウンドで実行された結果はすべてログファイルに記録されます。何か障害が起きた場合の原因究明や日々のサーバーの利用状況の調査、悪意のあるクラッカーからのアクセスの解明などログファイルの監視は様々用途に応用でき、サーバーの運用管理には欠かせない機能となっています。

ログ監視設定では logsurfer を用いたログ監視の設定を行うことができます。logsurfer は常にログの監視を行い特定のキーワードを検出するとその結果をリアルタイムでメールによるレポートを行います。

- **メールアドレスの設定**

「メールアドレス」にメールアドレスを指定します。ここで登録されたメールアドレスに対してレポート結果がリアルタイムで送信されます。

- **ログファイルの追加**

監視する対象のログファイルの追加を行います。既にいくつかの典型的なログファイルが選択肢にありますのでこの中から選ぶか、あるいはログファイル名を直接してしてログファイルを追加してください。ログファイルを追加するとルールの編集画面になります。

- **ルールの設定**

監視するログファイルに対するルールの追加・編集を行います。ここで指定したルールが上から順に評価され、ルールにマッチするとアクションが実行されます。一度ルールが評価されるとそれ以降のルールは評価されません。ここで指定されたルールはログファイルの 1 行毎に評価されます。

5. ログ管理

■ ログ監視のルール

ルールには「マッチする正規表現」「マッチしない正規表現」「アクション」の 3 つの要素があります。それぞれの要素は以下のようになります。

マッチする正規表現 - マッチするための正規表現を指定します。ここで指定した正規表現にマッチした行が見つかるとアクションが実行されます。

マッチしない正規表現 - マッチさせたくない正規表現を指定します。「マッチする正規表現」でマッチしてもここで指定した正規表現がマッチした場合はアクションは実行されません。 "-"または空文字(何も入力しない)にすると何も指定しません。

アクション

アクションには「無視」「メール送信」の 2 種類あります。

無視

何もしません。以降のルールを適用させたくない場合に使用します。

メール送信

メールを送信します。マッチした行の内容が送信されます。