UNIXサーバー構築 II

第7章　ログの運用と管理

ログ

■ログ

ログとはネットワークやサーバ、コンピュータなどのデバイスの動作状況を記録したもの。

■ログの分類

ログにはアプリケーション ログ、イベント ログ、サービス ログ、システム ログなどある。

UNIXのログ

UNIXのログ

UNIXには次のようなログがある。テキスト形式のログ、バイナリー形式のログがある。バイナリー形式のログは特別なコマンドを使用する。

ログインユーザーおよび利用時間、システムのリブート情報

ログイン失敗どの不正ログインの履歴情報

ユーザーの最終ログイン情報、ログインの履歴情報

セキュリティに関する情報、システムログ、起動のログ

起動時のカーネルログ、カーネルログ、aptのログなど。

syslogとは

Syslogとは

ログメッセージを転送するための規格、**クライアント/サーバ型**のプロトコルのこと。出力先や優先度に応じて、指定された出力先に送ることができる。

Ubuntuでのログ管理

Ubuntuでは**Journaldとrsyslogがインストール**されており、デフォルトで**Journaldがが動作してシステムログを収集**する。ログは一般的に

/var/log/の直下に保存されることが多い。

Journald（systemd-Journald）

Journald（systemd-Journald）

Ubuntuの標準のログ収集・保管サービス（デーモン）。

ログの確認コマンド

次のコマンドを使用して、ログを確認することができる。また、
journalctlには多くのオプションがある。

sudo journalctl　オプション

```
ecc@ecc:~$ sudo journalctl
 8月 08 13:25:37 ecc kernel: Linux version 6.2.0-26-generic
(buildd@bos03-amd64-042) (x86_64->
 8月 08 13:25:37 ecc kernel: Command line:
BOOT_IMAGE=/boot/vmlinuz-6.2.0-26-generic root=UUI>
```

JouranlctlのオプションJouranlctlのオプション

次のようなものがある

-u ・・・ ユニット単位での表示　-k ・・・ カーネルのログの表示

-S ・・・ 時間帯表示(開始時間)　-U ・・・ 時間帯表示(終了時刻)

-p ・・・ プライオリティ

プライオリティは0～7まである。0(重要度が高い)、7(重要度が低い)

0:emerg、1:alert、2:crit、3:err、4:warning、5:notice、6:info、7:debug

-f ・・・ リアルタイム

-b -1 ・・・ 前回のブートのみなオプションがある。

Journaldの設定

設定(/etc/systemd/journald.conf)

Journaldの設定はデフォルトですべてコメントアウトされている。

Storage

ログの保存先を指定 する。

①vlolatile・・・メモリ上(/run/log/journal)で保管、再起動時には消去。

②persistent・・・ディスク上で保管する。

③ **auto**・・・デフォルト、/var/log/journalディレクトリに保存。

ディレクトリがなければvoltaileディレクトリがあればpersistent。

その他の設定

SystemMaxUse、SystemKeepFree、SystemMaxFileSize、SystemMaxFiles、RuntimeMaxUse、RuntimeKeepFree、RuntimeMaxFileSize、RuntimeMaxFilesなど

System～・・・ディスク上に書き込まれる

KeepFree・・・これだけは空けておく制限

MaxFiles・・・ファイルの最大数、

MaxFileSize・・・1ファイルの最大サイズ

■ログの保管条件

以下の条件の場合、ログが保存される。

ログのファイルサイズがファイルシステムの容量の10%、または4GBよりも小さい。システムファイルの空き容量が15%、または4GBよりも小さい。

ログが収集された場所の確認

_TRANSPORT=フィールドで確認できる。次のコマンドでj確認する。

sudo journalctl -o verbose

```
ecc@ecc:~$ sudo journalctl -o verbose
Tue 2023-08-08 13:25:37.068327 JST
[s=e6cbcea7c3a147a6b3b6179f396ca785;i=1;b=ac>
    _SOURCE_MONOTONIC_TIMESTAMP=0
    _TRANSPORT=kernel
    PRIORITY=5
    SYSLOG_FACILITY=0
    SYSLOG_IDENTIFIER=kernel
    MESSAGE=Linux version 6.2.0-26-generic (buildd@bos03-amd64-042) (x86_64-lin>
    _BOOT_ID=acf627399095424bbc11f3aecb5f22df
    _MACHINE_ID=4e1eff01d76a40d390c3a5e487affef3
```

_TRANSPORT=stdout

標準出力・標準エラー出力からログを収集 。

フィールド

①ユーザージャーナルフィールド

MESSAGE=メッセージ本文、**PRIORITY=**プライオリティなどがある。

②トラステッドジャーナルフィールド

信頼できるフィールド。先頭に_がつく。_BOOT_ID,ID_PIDなど

journalctl --list-boots ・・・ ブートごとのidを確認する。

rsyslog

rsyslog

ログ収集・格納サービス。**Journald**でログを取得し、必要に応じてログを**rsyslog**へ転送する。

＊Ubuntuではjournaldとrsyslogとのどちらもが動いてるが、**journald**がまずこれらのログを読み取る。その後、**journald**が入手したすべてのログが**rsyslog**へ転送される。

＊デフォルトの設定が**ForwardToSyslog=yes**で**MaxLevelSyslog=debug**のためサービスユニットの標準出力および標準エラー出力もジャーナルに記録している。

rsyslogの設定

- **rsyslog.conf(/etc/rsyslog.conf)**

rsyslogの設定ファイル、実際には設定を記載したファイルを読み込んでいる。実際に設定しているファイルは**/etc/rsyslog.d/**の直下に保存されている。

```
ecc@ecc:/etc/rsyslog.d$ cat 50-default.conf
#  Default rules for rsyslog.
#
#     For more information see rsyslog.conf(5) and /etc/rsyslog.conf
#
# First some standard log files.  Log by facility.
#
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
#cron.*                         /var/log/cron.log
```

ログの監視

ログの保存場所

通常ログは**/var/log/**ディレクトリの直下に保存される。ただし、各デーモンの設定により保存や保存形式を変更することができる。

```
ecc@ecc:~$ ls /var/log/
alternatives.log       btmp           lastlog
alternatives.log.1     btmp.1         mail.log
alternatives.log.2.gz  cups           mail.log.1
apache2                dist-upgrade   mail.log.2.gz
apport.log             dmesg          mail.log.3.gz
apport.log.1           dmesg.0        mysql
apport.log.2.gz        dmesg.1.gz     nginx
apport.log.3.gz        dmesg.2.gz     openvpn
apport.log.4.gz        dmesg.3.gz     private
```

主なログ

主なログ(テキスト)

主なログは以下の通り。**テキスト**形式のため**catコマンド**で確認できる。

syslog ・・・ システムログ

boot.log ・・・ 起動のログ

dmesg ・・・ 起動時のカーネルログ

kern.log ・・・ カーネルログ

apt/history.log ・・・ aptのログ

mail.log ・・・ メールサーバのログ

apache2/access.log ・・・ Apacheのアクセスログ

主なログ(バイナリ形式)

バイナリ形式のログは、コマンドを使用して表示する。

＊catコマンドでは確認しない

wtmp ・・・ ログインユーザーおよび利用時間、システムのリブート情報、コマンド：**last**

btmp ・・・ ログイン失敗、不正ログインの履歴情報、コマンド：**lastb**

lastlog ・・・ ユーザーの最終ログイン情報、コマンド：**lastlog**

ログローテーション

■ログローテーション

ログファイルの肥大化を防ぐために定期的にログファイルをいくつかのファイルに保存してローテーションします。ログの世代はファイル名の後の**数字**が該当します。 <例>boot.log.**1**

ログのローテーションlogrotate(デフォルトインストール済み)で行う。

■バージョンの確認

logrotate --version

ローテーションの設定(/etc/**logrotate.conf**)

デフォルトの設定内容は以下の通り。

weekly ・・・ ログのローテーションの周期(毎週)

rotate 4 ・・・ ログファイルの世代(4世代)

Create ・・・ 空のログファイルを作成する

#dateext ・・・ アーカイブファイル名に日付をつける

#compress ・・・ ファイルを圧縮する

■動作確認

sudo logrotate --debug /etc/logrotate.conf

logwatch

logwatchとは

ログの分析や確認するためのツール。

logwatchのインストール

sudo apt install –y logwatch

sudo mkdir /var/cache/logwatch　　・・・一時ディレクトリの作成

logwatchの起動

sudo logwatch

logwatchの設定

Logwatchの設定ファイル (/etc/logwatch/conf/logwatch.conf)

設定ファイルをコピーして、編集をする。

cd /etc/logwatch/conf/

sudo /usr/share/logwatch/default.conf/logwatch.conf .

編集

sudo vi logwatch.conf

logwatch.confの設定

今回は、ログ情報をメールで指定した宛先へ送信する。

以下の内容を変更する。

Output = mail ・・・ メールに送る

Mailto = メールの送信先 (例ecc@ecccomp.ac.jp)

Range = Today ・・・ 本日

宛先へメールを送信

sudo logwatch --output mail

Apacheのログ

デフォルトのログ

Apacheのデフォルトログは、**access.log**、**error.log**。

保存先は**000-default.conf**で指定される。

ログの設定例

ErrorLog ${APACHE_LOG_DIR}/error.log

CustomLog ${APACHE_LOG_DIR}/access.log combined

＊ APACHE_LOG_DIRは**/var/log/apache2/**

ログローテーション

Apacheのログをローションする場合、次のファイルで設定する。

/etc/logrote.d/apache2

Mailに関するログ

Mailに関するログ

Mailに関するログは**/var/log/mail.log**に保存される。

cat /etc/rsyslog.d/50-default.confで確認できる。

Mailのログを確認する例

sudo cat /var/log/mail.log | grep “from=<メールアドレス>”

status=でメールの確認ができる。

send ・・・ 送信成功、**bounced** ・・・ メールが拒否された

deferred ・・・ 送信できず、延期された

bind(DNS)のログ

bindのログ

bindのログを取得することで、DNSの調査などすることができる。出力先などの指定をすることができる。

設定は、**named.conf.options**で指定する。また、ログを保存する先のディレクトリは作成する。

①ログの保存先の作成(/var/log/named)

sudo mkdir /var/log/named

sudo chown bind:bind /var/log/named

②namedの起動オプションを修正(/etc/default/named)

-L /var/log/named/named.logを追加する

<例>

OPTIONS=“-u bind -4 –L /var/log/named/named.log”

③named.conf.optionsファイルの修正

```
logging {
   channel bind-queries-log {
      file "/var/log/named/bind.queries.log" versions 10 size 10m;
```

```
        severity info;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
    category queries{
        ”bind-queries-log";
    };
};
```

④bindの再起動

sudo systemctl restart bind9