



August, 2017

BIG-IP: 操作証跡記録機能

PRESENTED BY:

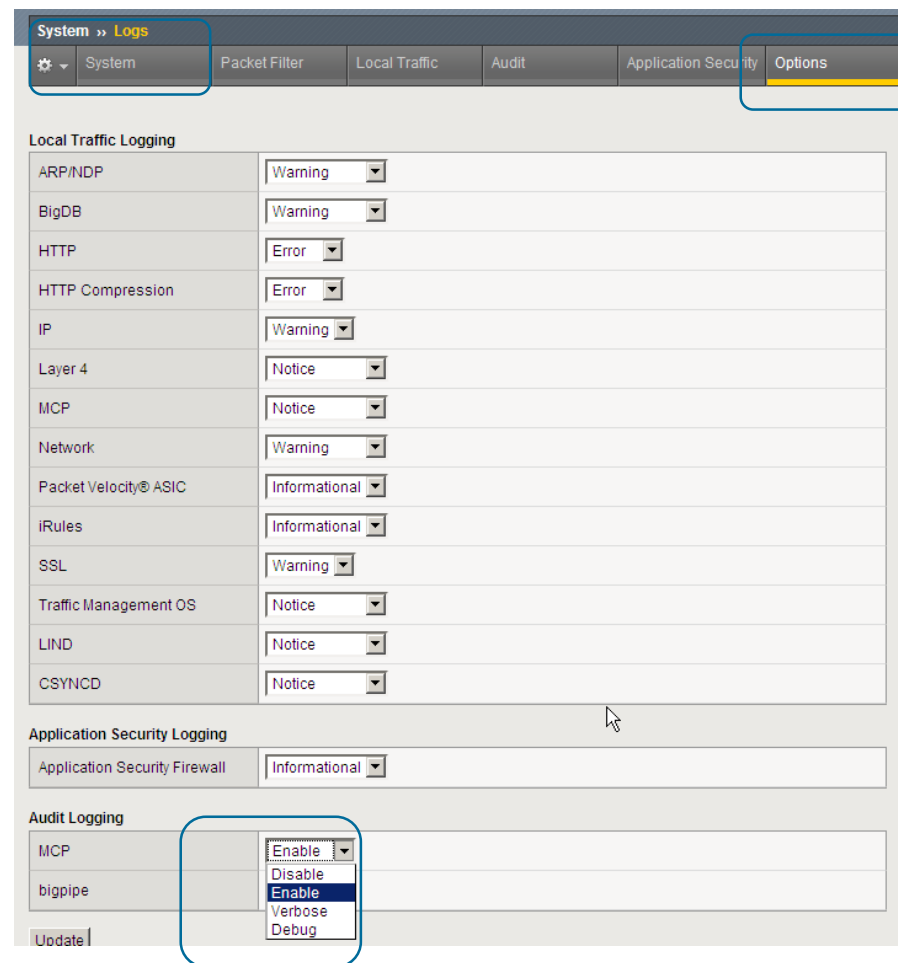
F5ネットワークスジャパン

WE MAKE APPS  **FASTER.
SMARTER.
SAFER.**

オペレーターの操作ログを残します

Auditing機能

- **記録可能な操作**
- ログイン/ログアウト
- 設定の変更
- bigpipe/tmsh
- GUI
- **ログの残し先**
- リモートsyslogサーバー
- ローカルのUnixファイル
- TACACS+サーバ(Accounting)
- RADIUSサーバ(Accounting)
- **ログの閲覧方法**
- GUI
- tmsh



操作のログ(出力例)

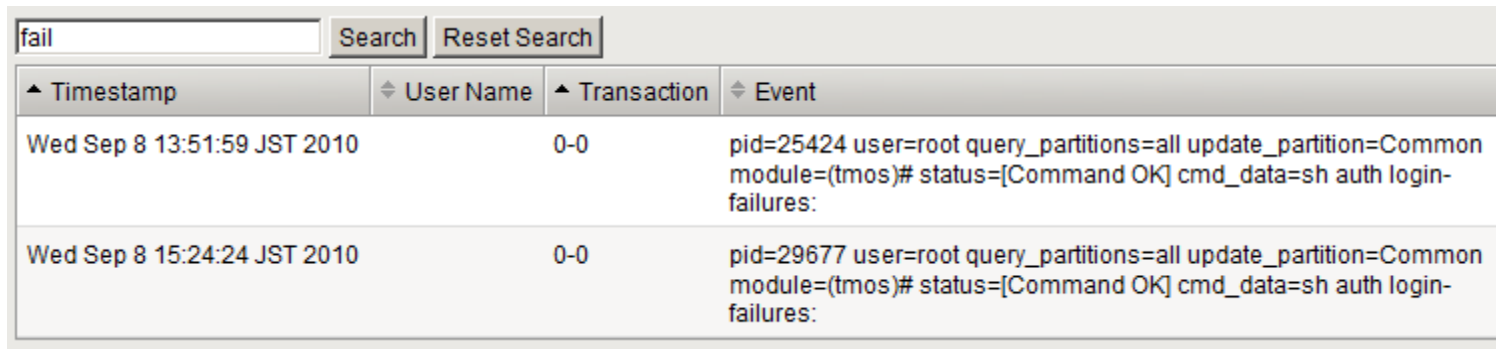
ログインのログ(syslog)

```
Jun 23 12:43:47 local/pre6-ltm6800-227 notice httpd[20717]:  
01070417:0: AUDIT - user admin - RAW: httpd(mod_auth_pam):  
user=admin(admin) partition=[All] level=Administrator tty=1  
host=10.1.2.1 attempts=1 start="Tue Jun 23 12:43:47 2009".
```

Pool MemberのDisableを行ったときのログ(syslog)

```
Jun 23 12:45:19 local/pre6-ltm6800-227 notice mcpd[5863]: 01070417:5:  
AUDIT - user admin - transaction #13837619-1 - object 0 - modify  
{ pool_member { pool_member_pool_name "ban-http-pool" pool_member_addr  
10.1.94.31 pool_member_port http pool_member_new_session_enable 0  
pool_member_update_status 1 } }
```

GUIでログの検索



Timestamp	User Name	Transaction	Event
Wed Sep 8 13:51:59 JST 2010		0-0	pid=25424 user=root query_partitions=all update_partition=Common module=(tmos)# status=[Command OK] cmd_data=sh auth login-failures:
Wed Sep 8 15:24:24 JST 2010		0-0	pid=29677 user=root query_partitions=all update_partition=Common module=(tmos)# status=[Command OK] cmd_data=sh auth login-failures:

