Quebra de Hashs

FELIPE TEIXEIRA

GUILHERME COUSIN

MURILO SCHMALFUSS

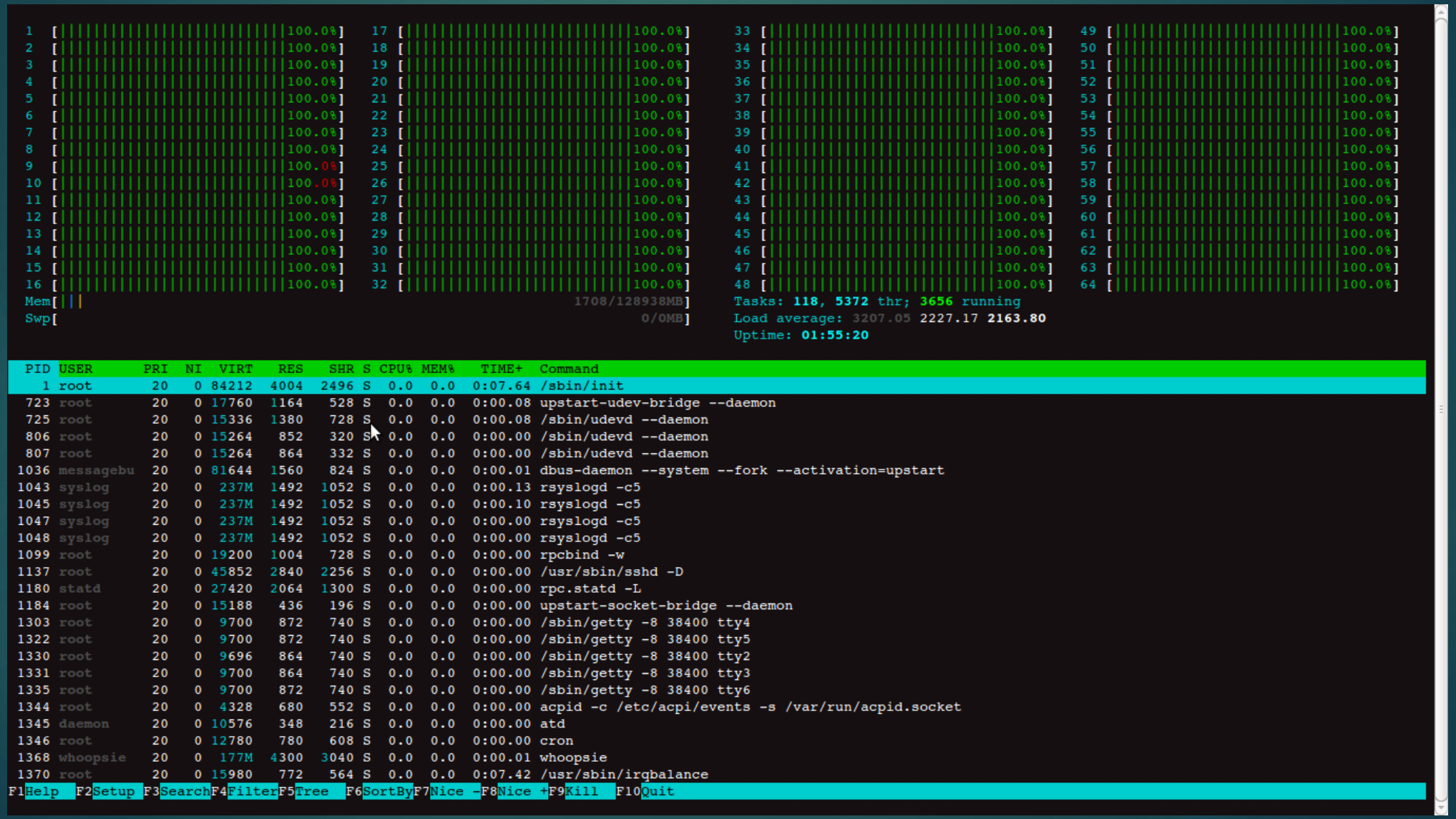
Metodologia

- Utilização do OpenMP para a paralelização dos laços de iterações
- Para a criação das hashs utilizamos a função md5 da biblioteca md5.h da openssl libcrypto

Hardware utilizado

- H2106-G7 Node: 2U cahssi, AMD quad socket SAS/Raid 0,1 on board
- 4 x Opteron 6376 16-core 2.3 GHz/16M
- 128GB Memory (32 x 4GB DDR3 DIMM 1600MHz)

Hardware utilizado



Código

- #pragma omp parallel for shared(tam, hashs_comp) private(md, stringMD, digest, i, j, k, l, m, n, o)

```
for(i = 0; i < tam; i++){
    for(j = 0; j < tam; j++){
        for(k = 0; k < tam; k++){
            for(l = 0; l < tam; l++){
                stringMD[0] = caracteres[i];
                stringMD[1] = caracteres[j];
                stringMD[2] = caracteres[k];
                stringMD[3] = caracteres[l];
                stringMD[4] = '\0';
```

Código(geração da Md5 para palavra gerada)

- MD5((unsigned char*)stringMD, strlen(stringMD), (unsigned char*) &digest);

```
for(o = 0; o < 16; o++){
    sprintf(&md[o*2], "%02x", (unsigned int) digest[o]);
```

Código(comparação)


```
// Comparação com as hashs
    for(o = 0; o < NUM_HASH; o++){
        if(memcmp(md, hashs_comp[o], sizeof(char)*33) == 0){
            #pragma omp critical
            {
                printf("%s %s\n", md, stringMD);
            }
        }
    }
```

Tempo da Aplicação

- Tempo de quebra das 240 hashs foi de aproximadamente 19 horas
- O numero de possibilidades de senhas com um alfabeto de 85 caracteres com uma combinação de 6 é 85^6 = 3771495155625

Quebra de Hashs

FELIPE TEIXEIRA

GUILHERME COUSIN

MURILO SCHMALFUSS