

Sistemi Operativi

Appunti delle Lezioni di Sistemi Operativi

Anno Accademico: 2024/25

Giacomo Sturm

*Dipartimento di Ingegneria Civile, Informatica e delle Tecnologie Aeronautiche
Università degli Studi "Roma Tre"*

Sorgente del file LaTeX disponibile al seguente link:

<https://github.com/00Darxk/Sistemi-Operativi>

Indice

1	Introduzione e Docker	1
1.1	Comandi di Docker	2
2	Introduzione alla Linea di Comando	3
3	Sistemi Operativi	6
3.1	Sistema Operativo come Gestore di Risorse	6
3.2	Processi	10
3.3	Scheduling	16

1 Introduzione e Docker

Questo corso anche se copre alcuni dei compiti di un amministratore di sistema, non rappresenta un corso di formazione per quest'ultimi. Si tratterà degli aspetti tipici di un kernel di un moderno sistema operativo, trattando nello specifico un sistema Linux, ma saranno applicabili ad ogni sistema operativo moderno. Sarà quindi necessaria una qualsiasi distribuzione Linux. Si utilizza Linux perché è un sistema gratuito e open-source. Si tratta di uno dei sistemi operativi più usati al mondo, usato nella maggior parte dei supercomputer e tra i web server rappresenta il 96% del primo milione in termini di traffico. Installato sul 85% di tutti gli smartphone e conta 1.6 miliardi di utenti. Una distribuzione Linux, o "distro", consiste in un sistema operativo basato sul kernel di Linux, insieme a configurazioni predefinite distribuite da organizzazioni. Esistono centinaia, se non migliaia, di distribuzioni di Linux, ognuna con un suo diverso obiettivo e caratteristiche.

Per utilizzare una distribuzione di Linux si usa il programma Docker Desktop, un software di virtualizzazione leggera. In generale sono possibili due modi di simulare un'applicazione nativa ad un altro sistema operativo. Si può utilizzare una macchina virtuale, che riproduce il sistema operativo da virtualizzare, con tutte le sue librerie, su cui viene eseguita l'applicazione. Tutto questo a sua volta si poggia su un hypervisor per gestire questi sistemi operativi, poggiato a sua volta sul sistema operativo originario della macchina. Questa è una struttura molto profonda e presenta un elevato overhead, causa quindi una perdita di prestazioni.

Negli anni '10 del 2000 si introdusse un meccanismo per alleggerire questo tipo di virtualizzazione, introducendo il concetto di container. Questi contenitori hanno al loro interno solamente l'applicazione nativa al sistema operativo e le sue librerie, senza simulare l'intero sistema operativo. Questi contenitori poggiano direttamente sul sistema operativo base, accompagnati dal software di docker. Questo processo di virtualizzazione leggera è possibile solo in alcuni casi, su Windows e Mac è possibile infatti una gestione semplificata di applicazioni per Linux in questo modo.

Docker rappresenta il software più utilizzato a livello globale per realizzare una virtualizzazione leggera. Tramite docker è possibile interagire direttamente con l'applicazione, anche se è comunque possibile caricare un sistema operativo diverso, in container Linux.

Docker presenta un'architettura a tre livelli, un client permette l'interfaccia con la macchina host, il docker host dove sono contenute le immagini ed i container. Inoltre è presente un registro online di immagini scaricabili. Un'immagine rappresenta un eseguibile con tutte le librerie al completo come container. Un'immagine rappresenta un'applicazione statica, indipendente da file esterni, ed è possibile realizzare un container basato solamente su quell'immagine. Si utilizzano immagini poiché molte applicazioni richiedono versioni diverse delle stesse librerie e file binari, per cui naturalmente solleveranno conflitti, che si vuole evitare.

Un container contiene un'applicazione eseguita in un ambiente isolato, da un'immagine base e le sue librerie e binari, da cui è possibile creare più di un container diversi. Ogni container può avere un volume, uno spazio su disco dove memorizzare dati e configurazioni indipendenti, in uno spazio isolato dall'immagine, per cui è possibile ricaricare l'immagine senza perdere i dati salvati sul volume. Si usa un volume poiché è buona norma che i container non abbiano uno stato, questo viene associato ad uno o più container specificando un mountpoint, accessibile in lettura o scrittura.

Le immagini sono dei template di sola lettura contenenti il root del filesystem che si vuole istanziare, i meta-dati, le variabili d'ambiente, e le varie configurazioni dell'applicazione che si vuole

eseguire. Queste immagini vengono costruite a strati, ognuno di questi può aggiungere, modificare o rimuovere file. Si comincia a creare un'immagine partendo da un contenitore vuoto ed aggiungendo progressivamente nuovi strati l'uno sull'altro. Tutti questi strati sono in sola lettura, solamente l'ultimo strato di default è anche in scrittura, per aggiungere configurazioni o file finali, anche se si preferisce inserirli in un volume con un ciclo di vita isolato.

Utilizzando container, immagini e volume è possibile disaccoppiare tutte le componenti del sistema operativo, le applicazioni ed i dati, rispettivamente.

1.1 Comandi di Docker

La sintassi di Docker venne ripulita ed aggiornata nel 2017, per cui risulta molto semplice ed intuitiva. Il comando principale è il prefisso **docker**, si possono scegliere operazioni sulla gestione di container, immagini o volumi specificando la parola chiave **container**, **image** o **volume**. Dopo di questi si possono inserire tipici comandi come **ls** per visualizzare gli elementi contenuti, rimuoverli con **rm**, etc. Si utilizza anche la parola chiave **network** per gestire la rete di container.

Il comando **help** fornisce una lista di comandi disponibili.

In questo corso si utilizzerà l'immagine, presente nel docker hub, **chmod84/os2425**.

Per creare un container sulla base di questa immagine, bisogna scaricarla con i seguenti comandi:

```
docker image pull chmod84/os2425
```

Questo comando di default prende l'ultima versione dell'immagine disponibile, in caso si voglia utilizzare una versione specifica si indica con : seguito dal numero di versione oppure **latest**, per l'ultima versione disponibile. Questo tag viene associato dal produttore della versione arbitrariamente, quindi potrebbe non corrispondere all'ultima versione esistente dell'immagine. In seguito per creare ed avviare il container si usa il seguente comando:

```
docker container --name os2425  
--hostname sistemi-operativi -v dati:/corso -it chmod84/os2425
```

Questo comando crea un volume chiamato "corso" nella root del filesystem.

Per avviare o terminare un container si usano i comandi:

```
docker container start os2425  
docker container stop os2425
```

Per aggiornare l'immagine bisogna prima rimuovere il vecchio container:

```
docker container rm os2425
```

In seguito si effettua una pull della nuova immagine e si crea il container come descritto precedentemente. Per avviare la shell di un container precedentemente avviato si utilizza il seguente comando:

```
docker container exec -it os2425 /bin/bash
```

2 Introduzione alla Linea di Comando

All'apertura del container docker ci si trova davanti ad una riga di comando del tipo:

```
corso@sistemi-operativi:~$
```

Il termina prima della chiocciola indica l'utente con cui si è effettuato l'accesso. La maggior parte dei sistemi operativi moderni infatti sono sviluppati su di una base multiutente. Per cui lo stesso sistema può essere utilizzato da utenti diversi, anche contemporaneamente con una separazione di privilegi, isolando i file appartenenti ai vari profili degli utenti. Si utilizza quindi l'utente **corso**. Mentre il nome dell'host è **sistemi-operativi**, specificato dopo la chiocciola. Un'ulteriore separatore **:** lo separa dai caratteri **~\$**. Il primo rappresenta un percorso, descritto successivamente, indica la directory corrente, in questo caso **~** indica la cartella di base dell'utente utilizzato per sfruttare il sistema. Il carattere **\$** indica dove viene inserito il comando o l'applicativo sulla riga di comando. Al posto di questo carattere può essere presente un cancelletto **#**, nel caso di livello di privilegio di amministratore.

Quando viene effettuato un comando, viene restituito un output a schermo, ed alla riga successiva, viene riproposto il prompt dei comandi. Non necessariamente tutti i comandi producono un output visivo a schermo.

Il comando **pwd** "Print Working Directory" stampa a schermo la directory corrente dove si sta lavorando.

```
corso@sistemi-operativi:~$ pwd
/home/corso
corso@sistemi-operativi:~$
```

Questo concetto è fondamentale, poiché mostra in quale posizione del filesystem vengono eseguiti i comandi proposti, all'interno del quale vengono effettuate le operazioni, che possono essere di creazione, modifica, rimozione, di file o di altre directory. L'indirizzo fornito si legge da sinistra verso destra, e specifica la root del filesystem **/**, dove si trova la cartella **home**, dove si trova la cartella **corso**, dove ci troviamo attualmente. Il filesystem è un oggetto di estrema complessità, che permette di astrarre in maniera semplice la virtualizzazione dei dati. Questo permette all'utente di interfacciarsi direttamente con l'hardware del calcolatore. Questo sistema organizza i file in cartelle, contenenti altre cartelle, identificate da un percorso o directory, per individuarli in modo univoco. Rappresenta il percorso dalla radice dell'albero al nodo specifico individuato nel filesystem. Le cartelle possono essere espresse equivalentemente sia come **cartella/** che **cartella**, si utilizza **/** dopo il nome della directory per specificare si tratti di una cartella e non di file. Se un nodo ha dei figli, allora si tratta di una cartella, mentre tutti i file sono foglie, ma non tutte le foglie sono file, e non possono essere espressi con uno **/** finale.

Per spostarsi all'interno del filesystem, è disponibile il comando **cd** "Change Directory", seguito dal percorso:

```
corso@sistemi-operativi:~$ cd /home
corso@sistemi-operativi:/home$
```

Per ritornare alla directory iniziale è sufficiente effettuare nuovamente un **cd**:

```
corso@sistemi-operativi:/home$ cd corso
corso@sistemi-operativi:~$
```

Se viene eseguito correttamente, non produce alcuna output, mentre se riscontra un errore viene mostrato a schermo.

Esistono essenzialmente due tipi di percorsi, relativi ed assoluti. Si distinguono semplicemente per la presenza di uno / iniziale. I percorsi assoluti specificano l'intero percorso nella sua interezza, partendo dalla radice del filesystem, come `/home/corso`. I percorsi che non iniziano con / sono percorsi relativi, come `corso`, all'interno di `/home`.

Se si utilizza un percorso assoluto, l'interprete dei comandi ci porta esattamente all'interno di quel percorso, altrimenti l'interprete dei comandi concatena la working directory con il comando relativo inserito, generando il percorso da seguire. Non c'è alcuna differenza nel funzionamento di questi due comandi, poiché viene gestito trasparentemente dal sistema operativo.

Ogni directory contiene sempre due directory speciali: `.` e `..`, dove `.` indica la directory corrente. Per cui `/home/corso/.` è uguale a `/home/corso`. Sarà molto utile in comandi successivi. La directory `..` rappresenta la directory esattamente superiore nel filesystem. Per cui `/home/corso/..` è uguale a `/home`. Quest'ultima directory ci permette di risalire l'albero del filesystem gradualmente. Viene utilizzata per semplificare il movimento all'interno del filesystem, senza necessariamente conoscere tutti i percorsi possibili alle directory superiori. Anche la radice contiene queste due cartelle, quindi sembrerebbe possibile salire al livello superiore della radice, ma il comando `cd ..` riporta alla radice.

La home directory è dove vengono archiviati tutti i file di un determinato utente, in generale in un sistema Linux, ogni utente ha una sua directory all'interno della directory `/home`, chiamata con il proprio nome utente. Utilizzare nomi differenti è possibile, ma non avviene di default. In ogni posizione del filesystem è possibile utilizzare il comando `cd ~` per spostarsi direttamente nella home directory, ma questo simbolo non è presente nelle tastiere italiane, bisognerebbe utilizzare infatti la combinazione ASCII "Alt+126". Tuttavia è possibile effettuare la stessa operazione con `cd` senza argomenti.

Per creare delle directory esiste il comando `mkdir` "Make Directory", seguito dal percorso che si vuole realizzare, indicato con un percorso relativo o assoluto. Tutte le cartelle precedenti all'ultima devono esistere, per permettere di creare la cartella.

```
corso@sistemi-operativi:~$ mkdir test
```

Equivalente a

```
corso@sistemi-operativi:~$ mkdir /home/corso/test
```

Si possono creare più cartelle contemporaneamente aggiungendo un altro percorso separato da spazi:

```
corso@sistemi-operativi:~$ mkdir dir1 dir2 dir3
```

Esiste un'opzione che si può passare a `mkdir` per creare un intero percorso in una volta sola tramite `-p`:

```
corso@sistemi-operativi:~$ mkdir -p dir4/dir5/dir6
```

Se questo comando viene chiamato senza argomento, stampa un errore a schermo, poiché richiede un argomento, una cartella da creare. Non si vuole memorizzare il contenuto di tutte le cartelle del filesystem, si utilizza quindi il comando `ls` "List". Questo comando stampa a schermo la lista di tutti i file o cartelle contenute nella working directory:

```
corso@sistemi-operativi:~$ ls
test dir1 dir2 dir3 dir4
```

3 Sistemi Operativi

Quando un programma viene eseguito segue sempre una serie di passaggi, comuni per ogni programma in esecuzione su un processore, chiamato ciclo di fetch-decode-execute, analizzato dettagliatamente nel corso di calcolatori elettronici:

- Fetch: il processore preleva l'istruzione da eseguire dal programma;
- Decode: l'istruzione viene trasformata in una o più istruzioni macchina (in base al tipo di architettura del processore);
- Execute: l'istruzione macchina viene effettuata dal processore;
- Il processore aumenta il PC e passa alla prossima istruzione.

Questo sistema si basa sul modello di Von Neumann, ma le prestazioni e le aspettative per calcolatori moderni sono molto maggiori di questo, una sostanziale differenza per le macchine moderne è la capacità di eseguire più di un programma in simultanea.

Il sistema operativo è ciò che permette ai calcolatori moderni di poter effettuare queste esecuzioni simultanee, quindi si trova responsabile della gestione di tutti i programmi in esecuzione su una macchina. Ha il compito di rendere semplice l'esecuzione di un programma, permettendogli di condividere memoria con tutti gli altri processi in esecuzione, e permettergli di interagire con periferiche o dispositivi di I/O. Il compito del sistema operativo consiste nell'effettuare queste operazioni efficientemente e velocemente.

3.1 Sistema Operativo come Gestore di Risorse

Il sistema operativo effettua un'operazione di virtualizzazione, trasformando le componenti fisiche del calcolatore in una forma virtuale, indipendentemente, in modo che questi programmi siano in grado di interagirci. Ha la funzione di connettere questi programmi e l'hardware dove vengono eseguiti. Le risorse fisiche sono il processore, la memoria condivisa, il disco, le periferiche, ed altri dispositivi connessi. Questa forma virtuale è quindi più accessibile ai programmi e di più facile uso e generale. A volte quindi ci si può riferire al sistema operativo come una macchina virtuale, capace di creare versioni virtuali dei componenti del calcolatore.

Queste funzionalità introdotte dal sistema operativo possono venire invocate da parte di un qualsiasi programma, ma non è detto che a questo venga permesso di effettuare tutte le operazioni offerte. Tratteremo questo concetto nella sezione sui processi. Ai programmi sono disponibili delle chiamate di sistema, invocazioni di funzioni specifiche offerte dal sistema operativo sulle componenti virtuali, in modo che questo possa interfacciarsi direttamente con l'hardware, agendo come un intermediario per i programmi. In generale il sistema operativo offre delle librerie standard o API per potersi interfacciare con le chiamate di sistema. Queste chiamate di sistema consistono nell'eseguire programmi, accedere alla memoria e dispositivi di I/O, tra le più comuni ed utilizzate, ma in generale fornisce sulle centinaia di chiamate di sistema.

Il sistema operativo si comporta come un gestore di risorse, come il processore, la memoria ed il disco. Si definisce gestore poiché sceglie come condividere il processore a tutti i processi in esecuzione, contemporaneamente in accesso alla stessa memoria, ed allo stesso disco e periferiche.

Un calcolatore moderno dispone di un certo numero di processori fisici, o virtuali. Contengono una decina di core fisici, ma una macchina server potrebbe disporre di decine di core sparsi su più processori. Generalmente il numero di programmi in esecuzione è molto maggiore del numero di core o processori disponibili dalla macchina. Il sistema operativo è quindi in grado di fornire l'illusione di avere un numero molto elevato di core, per ciascuno dei processi in esecuzione, grazie alla virtualizzazione delle risorse.

Si considera un semplice esempio fornito dal docente nel file `cpu.c`:

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/time.h>
#include <assert.h>
#include "common.h"

int
main(int argc, char *argv[]){
    if (argc != 2) {
        fprintf(stderr, "usage: cpu <string>\n");
        exit(1);
    }
    char *str = argv[1];
    while (1) {
        Spin(1); // Repeatedly checks the time and
        returns once it has run for a second
        printf("%s\n", str);
    }
    return 0;
}
```

Questo programma prende come argomento una stringa di caratteri e ripete costantemente dopo ogni secondo il primo carattere della stringa. Si può terminare con la combinazione di tasti "Control + C". Dopo aver compilato in un file binario il codice, per eseguirlo si indica il suo indirizzo relativo, ed il sistema operativo automaticamente lo interpreta come un programma da eseguire, quindi non rappresenta un comando per eseguire direttamente il programma:

```
corso@sistemi-operativi:~$ gcc -o cpu cpu.c
corso@sistemi-operativi:~$ ./cpu "A"
```

Inoltre si possono eseguire più di un programma contemporaneamente combinando i comandi con un `&`:

```
corso@sistemi-operativi:~$ ./cpu "A" & ./cpu "B" & ./cpu "C" & ./cpu "D"
```

Tutti questi processi sembrano essere eseguiti allo stesso tempo, si definisce processo un programma in esecuzione, ma l'ordine in cui vengono effettuate le istruzioni di ogni programma non è costante.

La memoria fisica è composta da un array di byte, ed un programma mantiene tutte le sue informazioni su strutture di dati in memoria. Divise in memoria in scrittura (store), specifica i dati da scrivere al dato indirizzo, e lettura (load), specificando l'indirizzo per accedere ai dati.

Si utilizza un altro programma offerto dal docente per poter analizzare il comportamento della memoria virtuale, chiamato `mem.c`:

```
#include <unistd.h>
#include <stdio.h>
#include <stdlib.h>
#include "common.h"

int main(int argc, char *argv[]) {
    int *p = malloc(sizeof(int)); // a1: allocate some memory
    assert(p != NULL);
    printf("(d) address of p: %08x\n",
        getpid(), (unsigned) p); // a2: print out the address of the memory
    *p = 0; // a3: put zero into the first slot of the memory
    while (1) {
        Spin(1);
        *p = *p + 1;
        printf("(d) p: %d\n", getpid(), *p); // a4
    }
    return 0;
}
```

Ogni istanza del programma alloca memoria allo stesso indirizzo, e sembra aggiornare i valori allo stesso indirizzo, indipendentemente.

Eseguendo più istanze di questo programma si rivela come ogni istanza del programma abbia una sua memoria virtuale dedicata, in realtà è il sistema operativo che mappa tra questi spazi di indirizzi virtuali e la memoria fisica. In questo modo si evitano interferenze tra processi, proteggendo la stabilità e sicurezza tra i vari processi.

Questi programmi vengono eseguiti essenzialmente in contemporanea, per cui il sistema operativo deve gestire il processore per fornire l'illusione che tutti questi programmi vengono eseguiti allo stesso tempo. Questo si chiama problema della concorrenza. Programmi moderni esacerbano questo necessitando di più thread, necessitando di più core virtuali.

Si considera il seguente codice `thread.c`:

```
#include <stdio.h>
#include <stdlib.h>
#include "common.h"

int counter = 0;
int loops;
```

```
void *worker(void *arg) {
    int i;
    for (i = 0; i < loops; i++)
        counter++;
    return NULL;
}

int main(int argc, char *argv[]) {
    if (argc != 2) {
        fprintf(stderr, "usage: threads<value>\n");
        exit(1);
    }
    loops = atoi(argv[1]);
    pthread_t p1, p2;
    printf("Initial value : %d\n", counter);

    Pthread_create(&p1, NULL, worker, NULL);
    Pthread_create(&p2, NULL, worker, NULL);
    Pthread_join(p1, NULL);
    Pthread_join(p2, NULL);
    printf("Final value : %d\n", counter);
    return 0;
}
```

Questo programma utilizza due threads per modificare una variabile condivisa, incrementandone il valore da zero ad ogni ciclo. Per un numero di cicli relativamente piccolo, il valore restituito da questo programma rappresenta esattamente il doppio del valore inserito come argomento. Ma per numeri più elevati di cicli di loop, il valore tende a cambiare rispetto al valore atteso. Il problema dipende dal modo in cui viene incrementato il contatore condiviso. L'incremento del contatore non corrisponde ad un'istruzione atomica, ma è composta da tre operazioni distinte, la lettura ed il carico del valore attuale su un registro, l'incremento, ed il trasferimento in memoria. Queste tre operazioni non vengono eseguite atomicamente, da cui sorge il problema della concorrenza. Se due thread eseguono quest'operazione simultaneamente allora, è possibile che uno di questi legga il valore che l'altro ancora non ha avuto tempo di trasferire in memoria prima dell'incremento. Questo fenomeno è noto come condizione di gara, dove il risultato dipende dall'ordine in cui i thread accedono alle risorse condivise. Per risolvere questi problemi possono introdurre meccanismi di lock o di blocco, per sincronizzare i due thread, in modo che solo unthread alla volta sia in grado di accedere alla risorsa condivisa.

Quando si utilizzano questi meccanismi evitare di utilizzarli in modo improprio, altrimenti è possibile che sorgano altri problemi di deadlock, dove i thread aspettano all'infinito lo sblocco di una risorsa condivisa.

Dispositivi di memoria condivisa come DRAM memorizzano i dati in modo volatile, per l'esecuzione dei programmi. Ovvero perdono i valori memorizzati quando il sistema viene spento. Quindi si ha la necessità di memorizzare i dati in maniera persistente grazie a sistemi hardware e software. I sistemi utilizzano sistemi I/O come dischi a stato solido (SSD) o dischi rigidi (HDD),

non volatile. Dal punto di vista del software invece, per la persistenza il filesystem gestisce il disco ed è responsabile per memorizzare tutti i file che verranno creati dall'utente. Questo gestore alloca lo spazio necessario sul disco per il file, organizza i suoi dati in modo da essere disponibile in futuro, e corregge e gestisce eventuali errori che potrebbero verificarsi nel processo di scrittura.

Si considera il seguente codice per la creazione di un file con scritto "Hello World" alla directory /tmp/file del container Linux:

```
#include <stdio.h>
#include <unistd.h>
#include <assert.h>
#include <fcntl.h>
#include <sys/types.h>

int      main(int argc, char *argv[]) {
    int fd = open("/tmp/file", O_WRONLY | O_CREAT | O_TRUNC, S_IRWXU);
    assert(fd > -1);
    int rc = write(fd, "hello world\n", 13);
    assert(rc == 13);
    close(fd);
    return 0;
}
```

Le funzioni `open()`, `write()` e `close()` vengono indirizzate alla parte del sistema operativo chiamato filesystem che gestisce questo tipo di richieste.

Questa parte del sistema operativo si occupa di strati aggiuntivi di astrazione come dischi RAID, gestori di volumi logici, etc. Trova una posizione sul disco dove i nuovi dati risiederanno. Infine invia richieste di I/O ai dispositivi di memoria specifici. Il filesystem si occupa degli errori in scrittura che possono sorgere durante la scrittura su disco o guasti ai dispositivi. Utilizza due diversi meccanismi il "journaling" o "copy-on-write", e gestendo ed ordinando file in maniera efficiente sul disco. La tecnica di journaling consiste nel mantenere un registro di tutte le operazioni di scrittura, così da essere in modo di completarle o ripristinare lo stato in caso di guasti al sistema. La tecnica di copy-on-write invece consiste nella creazione di una copia, invece di sovrascriverli alla modifica dei dati. In questo modo si evitano corruzioni dei dati durante la scrittura, nella nuova posizione.

3.2 Processi

Un processo viene definito come un qualsiasi programma in esecuzione, dove un programma è un agglomerato di istruzioni isolati su una zona di memoria secondaria. Il sistema operativo ha il compito di caricare questo programma ed eseguirlo.

Per dare l'illusione di un'esecuzione simultanea di molti processi, il sistema operativo assegna ad ogni processo un quanto di tempo per cui quel processo può essere eseguito dal processore. Questi processi in esecuzione vengono poi interrotti tramite dei segnali di interrupt, ed il sistema operativo assegna il prossimo processo in coda ad essere eseguito. Il sistema operativo quindi genera una coda di processi da essere eseguiti in base in base a politiche diverse, trattate successivamente

nella sezione dedicata allo scheduling. Questo processo di condivisione del tempo si chiama “time sharing”.

L’operazione di terminare preventivamente l’esecuzione di un processo per poi passare ad eseguire un altro si chiama “context switching”. Questo fornisce l’illusione di avere molti processori virtuali dedicati ad ogni processo. Ma avere molti processi in esecuzione comporta quanti di tempo di lunghezza minore, assegnati a ciascun processo. Con un numero infinito di processi infatti, i quanti di tempo sarebbero di tempo infinitesimo, ed il sistema operativo sarebbe costantemente occupato ad effettuare l’operazione di context switching.

Quest’operazione viene effettuata dal sistema operativo indipendentemente dall’utente, la politica di gestione è salvata in un file sorgente specifico, non accessibile all’utente.

In generale un processo può essere caratterizzato dal suo stato di esecuzione, tutto ciò che questo può leggere o scrivere in esecuzione. È caratterizzato dal suo spazio di memoria assegnatoli in memoria centrale, contenente le sue istruzioni ed i suoi dati, e nei registri della CPU durante la sua esecuzione. Questi rappresentano essenzialmente un’estensione della RAM disponibile al processore. Memorizzano l’indirizzo della prossima istruzione da eseguire, il “Program Counter” (PC), e l’indirizzo dello stack, lo “Stack Pointer” (SP), associato a questa esecuzione del programma, i più importanti.

Il sistema operativo controlla il ciclo di vita dei processi, gestendo una serie di funzioni, disponibili attraverso l’API, “Application Programming Interface” dei processi:

- Create: crea un nuovo programma, caricandolo dal disco ed allocando le risorse necessarie;
- Destroy: interrompe l’esecuzione di un processo, attraverso una GUI, oppure con un comando “kill” o “kill all”. Questo processo non danneggia l’applicazione;
- Wait: mette in pausa l’esecuzione di un processo fino a quando non avviene un evento specifico;
- Miscellaneous Control: offre metodi vari per la sospendere l’esecuzione di un processo per poi riprenderla in seguito. È compreso nei meccanismi di time-sharing per permettere l’esecuzione degli altri processi in coda;
- Status: permette di ottenere informazioni riguardo il processo attuale.

Per effettuare un’operazione di creazione il sistema operativo effettua una serie di operazioni. Durante l’operazione di “Load” alloca lo spazio in memoria centrale per accomodare il programma. In seguito il programma, memorizzato sulla memoria secondaria in formato eseguibile, e viene trasferito in maniera “lazy”, pigra. Non viene trasferita la sua integrità, ma solo le istruzioni strettamente necessarie all’esecuzione del programma, e vengono trasferite ulteriori istruzioni quando vengono richieste da altre istruzioni nel processo in esecuzione. Nell’operazione di “Stack Allocation” alloca lo stack di esecuzione del programma, utilizzato per memorizzare le variabili locali, parametri di funzioni e indirizzi di ritorno. Inizializzato con gli argomenti passati alla funzione `main` nel programma, come `argc`, numero degli argomenti passati, e l’array degli stessi `argv`.

Nell’operazione di “Heap Creation” viene realizzato lo spazio di heap dove vengono contenuti i dati salvati durante l’esecuzione del programma, tramite operazioni di `malloc()`, richiedendo esplicitamente lo spazio. Questo viene poi liberato esplicitamente dal programma con un’operazione di `free()`, altrimenti viene liberato al termine della sua esecuzione.

“Initialize”: vengono inizializzati i tre descrittori di default per il programma, lo stdin, standard input; lo stdout, standard output; e lo stderr, standard errore. Canali attraverso cui il processo è in grado di comunicare con l’ambiente esterno tramite meccanismi di I/O, oppure notificare il sistema operativo di eventuali errori.

Alla fine di questo meccanismo di creazione, il sistema operativo trasferisce il controllo della CPU al processo, iniziando dalla prima istruzione dopo la funzione `main()`, punto di ingresso in molti linguaggi di programmazione.

Un processo può esser in tre stadi distinti durante la sua esecuzione. Il sistema operativo gestisce la transizione tra questi stati e garantisce che i processi vengano eseguiti correttamente, in modo efficiente.

- Running: il processo è in esecuzione, ovvero ha il controllo del processore ed esegue le sue istruzioni;
- Ready: il processo è pronto per essere eseguito , ma il sistema operativo non l’ha scelto e quindi aspetta il suo turno nella coda;
- Blocked: il processo è bloccato, perché ha richiesto delle operazioni ad alcuni dispositivi connessi al calcolatore. Impedisce che il processore rimanga occupato da un processo che non può effettivamente eseguire istruzioni.

In realtà sono presenti molti più stadi per lo stato di un processo, ma questa rappresenta una buona approssimazione.

Un processo pronto può essere schedato per essere eseguito, oppure è possibile de-schedato un processo in esecuzione per renderlo pronto. Un processo in esecuzione quando richiede accesso a memoria o a dispositivi di I/O viene bloccato, e poi sbloccato quando finisce questa operazione, diventando pronto per riprendere la sua esecuzione.

Con questi stati quindi i thread di esecuzione dei vari processi vengono intrecciati tra di loro ed il processore è sempre in esecuzione di un processo in ogni quanto di tempo. Per organizzare i dati necessari a gestire questi processi il sistema operativo utilizza strutture dati apposite, per memorizzare lo stack di esecuzione dei processi.

Si considera una di queste strutture dati:

```
// the registers x86 will save and restore
// to stop and subsequently restart a process
struct context {
    int eip; // Instruction pointer register
    int esp; // Stack pointer register
    int ebx; // Called the base register
    int ecx; // Called the counter register
    int edx; // Called the data register
    int esi; // Source index register
    int edi; // Destination index register
    int ebp; // Stack base pointer register
};
```

```
// the different states a process can be in
enum proc_state { UNUSED, EMBRYO, SLEEPING,
RUNNABLE, RUNNING, ZOMBIE };

// the information xv6 tracks about each process
// including its register context and state
struct proc {
    char *mem; // Start of process memory
    uint sz; // Size of process memory
    char *kstack; // Bottom of kernel stack
                // for this process
    enum proc_state state; // Process state
    int pid; // Process ID
    struct proc *parent; // Parent process
    void *chan; // If non-zero, sleeping on chan
    int killed; // If non-zero, has been killed
    struct file *ofile[NOFILE]; // Open files
    struct inode *cwd; // Current directory
    struct context context; // Switch here to run process
    struct trapframe *tf; // Trap frame for the
                // current interrupt
};
```

Questo codice mostra come il sistema xv6 traccia e gestisce i vari processi ed i registri per l'esecuzione dei vari processi. L'informazione relativa ai vari processi viene salvata nella struttura di tipo `proc`. Queste informazioni permettono di eseguire, terminare o riprendere l'esecuzione di un processo. Fornisce informazioni sulla memoria utilizzata dal processo, i registri utilizzati, il suo stato, i file aperti e la directory corrente, il puntatore al processore genitore.

Il sistema operativo deve effettuare queste operazioni di time sharing efficientemente. Quindi bisogna minimizzare il tempo tra la fine di un processo e l'inizio del successivo. In questo modo si minimizza l'overhead. Oltre a risolvere questo problema di overhead, il sistema operativo deve riprendere il controllo dopo che il quanto di tempo assegnato a quel processo esaurisce, altrimenti potrebbe essere eseguito ininterrottamente, senza liberare le sue risorse. Inoltre se non mantiene il controllo del processore, un processo maligno potrebbe effettuare operazioni non autorizzate e mettere a rischio il calcolatore. Il sistema operativo deve essere in grado di poter effettuare controlli di sicurezza per verificare se un dato processo sia autorizzato a compiere una certa azione.

Per risolvere il problema delle prestazioni, il processo non viene eseguito attraverso il sistema operativo, come fosse un tramite, ma viene eseguito direttamente sul processore. Questa tecnica si chiama esecuzione diretta, senza passare un livello intermedio di emulazione o interpretazione. In questo modo si riduce al minimo l'intervento del sistema operativo durante l'esecuzione. Se il sistema operativo non mantenesse il controllo sarebbe ridotto ad una semplice libreria, per svolgere funzioni importanti dei vari processi, senza poter gestire le varie risorse. Ma se il processo viene eseguito direttamente sul processore, allora il sistema operativo non può essere eseguito per mantenere il

controllo, e se il processo richiede un'operazione non consentita, il sistema operativo non ha modo di impedirglielo.

La soluzione per risolvere l'esecuzione di operazioni proibite consiste nell'avere due modalità di esecuzioni diverse, una per l'utente e l'altra per il sistema operativo. Nello spazio o modalità utente, i processi non hanno accesso a tutte le risorse hardware del calcolatore, mentre nella modalità kernel, il sistema operativo può utilizzare tutte le risorse della macchina. Le chiamate di sistema permettono ai processi di interfacciarsi con lo spazio kernel del sistema.

Nello spazio utente i processi vengono eseguiti con accesso limitato alle risorse dell'hardware, mentre le operazioni critiche come accessi in memoria, o a dispositivi di I/O non sono permesse direttamente. Nella modalità kernel ha pieno accesso a tutte le risorse del calcolatore, inclusi hardware e memoria. In questa modalità il sistema operativo esegue le operazioni richieste dai processi nello spazio utente, in questo modo gli permette di effettuare controlli di sicurezza su queste operazioni.

In generale per distinguere tra queste due modalità, è presente un flag in un registro del processore per segnalare in quale modalità ci si trova. In questo modo il processore può rifiutare le istruzioni ristrette in base al valore di questo flag. In pratica abilita il set completo delle istruzioni del kernel.

Si utilizzano le chiamate di sistema, interfaccia sicura e standardizzata per permettere ai processi di accedere a risorse di sistema o servizi critici. Permettono di eseguire operazioni come accedere al filesystem, creare o distruggere processi, comunicare con altri processi o allocare memoria. Per eseguire una chiamata di sistema il processo invoca una speciale istruzione di "trap", che effettua insieme un salto nel kernel, ed un aumento del livello di privilegio alla modalità kernel. Viene realizzata al livello del processore, come un'operazione di salto alla prima istruzione della chiamata di sistema nel kernel. Il controllo allora passa al sistema operativo, all'interno del kernel, e viene modificato il PC.

Dopo aver eseguito l'operazione richiesta dall'utente, per restituire il controllo al processo, viene invocata una chiamata "return-from-trap", ritorna all'istruzione subito seguente dalla chiamata di sistema nel programma e diminuisce il livello di privilegio allo spazio utente.

Ma bisogna impedire di effettuare salti arbitrari dentro al kernel, questo permetterebbe l'esecuzione di codice arbitrario all'interno del kernel, il quale potrebbe essere molto dannoso in caso sia presente un processo maligno o contenente errori o bug. Per questo al tempo di avvio del calcolatore viene generata una tabella chiamata "trap table" contenente l'indirizzo della prima istruzione di ogni chiamata di sistema, numerandole. In questo modo si può eseguire il codice del kernel in modo sicuro e solamente in punti predefiniti, riducendo il rischio di un'esecuzione dannosa di istruzioni nel kernel. Queste chiamate di sistema rappresentano l'unica un'interfaccia o API tra il processo nello spazio utente e le istruzioni del nello spazio del kernel. Tramite la trap table. A livello di hardware viene impostato su un registro l'indirizzo del gestore delle chiamate di sistema.

All'avvio di un programma viene creata un'entità processo da parte del sistema operativo, per allocare la memoria, ad una struttura dati del processo di tipo `proc`. Il codice del programma viene poi trasferito in memoria centrale, dal disco, in maniera lazy, ovvero trasferendo solamente il codice strettamente necessario, e successivamente si trasferisce solo il codice che viene utilizzato. Inoltre si realizza lo stack e l'heap dell'applicazione, e si realizza il doppio puntatore a caratteri `argv`, per gestire gli input per il processo. Si inserisce nello stack del kernel il registro ed il PC per tenere

conto del processo in esecuzione, e tiene conto delle chiamate di sistema e dei loro argomenti per effettuare system call.

Alla fine di queste operazioni bisogna passare il controllo al programma appena avviato, utilizzando una chiamata "return from trap", e bisogna specificare la prima istruzione da eseguire. L'hardware conosce l'indirizzo di memoria base dello stack che contiene il valore dei registri da inizializzare per avviare il processo. Dopo aver popolato i registri ed il PC, cambia la modalità di funzionamento allo spazio utente e salta alla prima istruzione nel metodo main.

Ora il programma in esecuzione segue le istruzioni sequenzialmente, ed eventualmente deve eseguire delle chiamate di sistema, quindi invoca una funzione di trap per saltare al livello spazio kernel, ma bisogna salvare i valori del processo nello spazio riservato nel kernel. Questo salvataggio viene effettuato in modo completamente autonomo da parte dell'hardware prima di cedere il controllo al kernel. Dopo averli salvati si eleva il livello di privilegi e si salta alla prima istruzione del gestore della trap, eseguito dal punto di vista del kernel, si eseguono le istruzioni della chiamata di sistema, e si effettua una istruzione return from trap. Il processore rimuove i valori salvati nello stack del kernel e si sposta allo spazio utente. Inoltre salta all'istruzione indicata dal PC dopo la chiamata trap.

Alla terminazione del processo non bisogna salvare i suoi valori poiché non avrà modo di effettuare altre chiamate di sistema, quindi l'hardware non svolge nessuna operazione. Il kernel quindi svuota l'area di memoria assegnata al processo e lo rimuove dalla struttura dati utilizzata per contenere la lista dei processi.

Il sistema operativo ha come obiettivo la ricerca di prestazioni più alte possibili, bisogna quindi evitare di inserire livelli in più tra il processo al processore, per impedire rallentamenti nell'esecuzione del processo. Ma allo stesso tempo si vuole mantenere il controllo del processore da parte del sistema operativo. Data la modalità descritta precedentemente il processo restituisce il controllo al sistema operativo dopo una chiamata di sistema, quindi il processore mentre l'esecuzione del processo non sta eseguendo il sistema operativo. Questo rappresenta quindi un problema, poiché un processo malevolo potrebbe non effettuare mai chiamate di sistema, quindi non restituisce mai il controllo al sistema operativo e viene bloccata l'esecuzione del sistema operativo. Questo può essere realizzato facilmente tramite un ciclo infinito. Non necessariamente però dipende da una programmazione malevola, potrebbe essere causata ad un errore o bug nel programma.

Quindi è necessario cambiare l'approccio per riguadagnare il controllo del processore dal sistema operativo. Si definiscono quindi due approcci, uno cooperativo, l'altro non cooperativo. Il primo approccio consiste nella modalità precedente, dove il sistema operativo aspetta una chiamata di sistema per riprendere il controllo del processore, oppure se viene sollevata una qualche tipo di eccezione. Esiste una chiamata di sistema `yield()` che permette di cedere il controllo del processore al sistema operativo. Ma non è garantito che ogni processo contenga una chiamata di sistema, e che vengano chiamate periodicamente.

Si vorrebbe utilizzare un sistema dove il controllo viene ceduto al sistema operativo periodicamente, questo tuttavia non può essere realizzato interamente tramite software. Bisogna quindi ricorrere al supporto dell'hardware, generando un timer all'avvio di ogni processo. Quando questo timer arriva al termine viene invocato un interrupt che passa il controllo al sistema operativo, da parte di un gestore di interrupt. Questo rappresenta uno scheduling non cooperativo. I processi che vengono eseguiti non gestiscono il controllo del processore. In questo modo è possibile al

sistema operativo riprendere il controllo nonostante la presenza di applicazioni malevoli. Questo timer lavora nell'ordine dei millisecondi, ed è indipendente dalla frequenza di aggiornamento del processore.

Un processo potrebbe non terminare tra due di questi timer interrupt, quindi il controllo passa al sistema operativo alla terminazione del programma, ed in alcuni casi viene disattivato il gestore degli interrupt e si scartano alcuni interrupt. Se dei processi hanno una priorità diversa, invece di terminare la loro esecuzione al primo interrupt, il controllo viene lasciato al processo invece del sistema operativo, fino ad un certo numero di interrupt.

Viene chiamata la funzione scheduling ad ogni interrupt per scegliere se si continua ad eseguire il processo che era in esecuzione oppure eseguire un nuovo processo. Quando viene scelto di cambiare il processo da eseguire, si effettua un context switch, un cambio di contesto, poiché tutti i valori associati al processore e dei registri vengono salvati per usarne di nuovi.

Con questa modalità, all'avvio si inizializza la trap table, ed il gestore degli interrupt decide l'intervallo tra gli interrupt. Quando viene sollevato il timer interrupt all'esecuzione di un processo, l'hardware effettua operazioni analoghe alla chiamata di sistema. I suoi valori e registri vengono salvati nel suo stack di processo, ed il processore cambia la modalità in kernel mode e passa il controllo al sistema operativo. Il sistema operativo sceglie dal suo scheduler a quale processo restituire il controllo del processore. Scelto il processo, l'hardware riassegna i valori ed i registri e salta allo spazio utente.

Se viene sollevato un interrupt mentre il processo sta scrivendo sui dati sul disco, oppure durante l'esecuzione di una chiamata di sistema, il sistema operativo può reagire in modi diversi. Potrebbe scartare gli interrupt sollevati durante una chiamata di sistema, oppure potrebbe usare sofisticati meccanismi di lock per proteggere l'accesso a strutture dati interne. Questi meccanismi saranno analizzati dettagliatamente in una successiva sezione del corso.

3.3 Scheduling

Dopo aver trattato il meccanismo di context-switch bisogna analizzare le politiche di scheduling. Verranno utilizzate una serie di assunzioni irrealistiche. La prima di queste assunzioni è che tutti i "job", lavori che il sistema deve eseguire, abbiano lo stesso tempo di esecuzione. Si assume che tutti i lavori arrivino allo stesso momento. Si considera che ciascuno di essi venga eseguito fino al suo completamento. Ognuno di questi utilizza esclusivamente il processore, non effettuano operazioni di input/output. Si suppone infine che si conosca a priori il tempo di esecuzione di tutti questi job.

Si vuole misurare in modo quantitativo le politiche di scheduling, si introducono quindi una serie di metriche. La prima chiamata turnaround time, è il tempo di lavoro di un job, si calcola come la differenza tra il tempo di arrivo ed il tempo di completamento, data l'assunzione che tutti questi job arrivino allo stesso momento, si impone sia nullo. Quindi con queste assunzioni il tempo di turnaround corrisponde al tempo di completamento. La seconda metrica è la fairness, quanto le risorse vengono divise in modo equo rispetto a tutti i processi.

La prima politica di scheduling è la FIFO, o FCFS, "First Come, First Served", semplice e di facile implementazione. Si suppone arrivino sequenzialmente a distanza temporale minima, il primo job ad arrivare sarà il primo ad essere eseguito.

Nel momento in cui si considerano situazioni più realistiche, questa politica perde di efficienza, poiché il primo job potrebbe richiedere un tempo molto superiore ai successivi, quindi si verifica l'effetto convoglio. Il primo "vagone" è molto più grosso dei seguenti e quindi il turnaround time è molto elevato.

Nello stesso contesto si può utilizzare una gestione diversa, per migliorare il tempo di ritorno. Si considera allora una politica che esegue i lavori più corti prima, SJF "Shortest Job First", noto il tempo di esecuzione. In questo modo si minimizza il turnaround time, decisamente più basso della politica FIFO.

In uno scenario più realistico, non tutti i job arrivano nello stesso momento nel sistema, quindi è possibile che il primo lavoro che arriva sia l'unico possibile da eseguire, e sia anche il più lungo, quindi in queste condizioni si verifica nuovamente l'effetto convoglio.

Per cui si considera un sistema dove se arriva un job che richiede un tempo minore per essere completato, viene interrotta l'esecuzione del processo attuale e viene eseguito questo nuovo processo. Questa politica si chiama STCF "Shortest Time to Completion First", aggiunge un meccanismo di prevenzione a SJF, quindi viene chiamato anche PSJF, "Preemptive Shortest Job First". Ogni volta che un job entra nel sistema ne calcola il tempo di completamento e se è minore del processo attualmente in esecuzione allora si interrompe l'esecuzione del processo corrente e si esegue il nuovo processo. Quindi all'arrivo di un nuovo processo, il sistema operativo deve determinare il tempo di completamento per questi nuovi processi e per il processo attualmente in esecuzione.

Esistono altre metriche altrettanto significative come il tempo di risposta, definito come il tempo in cui il job è stato in coda, prima di essere eseguito per la prima volta. Un modo per minimizzare o controllare il tempo di risposta per un determinato job si considera la politica di scheduling "Round Robin" (RR). Questa politica effettua una suddivisione nel tempo cambiando periodicamente quale dei processi in coda viene eseguito, fino all'esaurimento dei job in coda. In questo modo viene garantito a tutti i job un quanto di tempo, essenzialmente l'intervallo di tempo tra due interrupt. Ma è possibile che questo quanto di tempo sia un multiplo del timer interrupt, in modo per sintonizzare gli interrupt e questi quanti di tempo. Secondo la definizione di fairness, questo è una politica fair poiché assegna ad ogni job la stessa quantità di CPU. Ma ottiene delle prestazioni pessime rispetto al tempo di ritorno. Infatti per minimizzare il tempo di ritorno il processore deve concentrarsi su un unico job alla volta.

La lunghezza del quanto di tempo è critico per il tempo di risposta. Diminuendo il quanto di tempo, l'overhead rappresentato dal context switch rappresenta una parte considerevole del quanto di tempo, ma diminuisce il tempo di risposta. Se aumenta il quanto di tempo, viene ammortizzato l'effetto del context switch, il tempo di risposta aumenta. Questa politica è tra le peggiori per il tempo di ritorno, ma è la più equa nella sua distribuzione delle risorse.

Si considerano ora job in grado di eseguire operazioni input/output o accessi a risorse esterne al processore, quindi possono passare dallo stato running allo stato blocked.