System Design Document - TecStore

Natale Guadagno, Paolo Patrone

January 13, 2022

Contenuti

Partecipanti

Nome	Matricola
Guadagno Natale	0512106546
Patrone Paolo	0512106153

1 Introduzione

1.1 Scopo del sistema

Il sistema si propone come interfaccia unificata e semplificata per la gestione di una realtà complessa come un e-commerce.

Le interfacce sono quindi pensate per essere di immediata lettura e accessibili anche per chi ha poca dimestichezza con sistemi informatici.

1.2 Obiettivi di design

Per garantire un livello di accessibilità universale sono previsti più test di usabilità per ogni interfaccia, in modo da evidenziare criticità risolvibili.
Per facilitare l'utilizzo della piattaforma, ci si è posto anche l'obiettivo di avere un'interfaccia molto reattiva con tempi di risposta molto brevi e molti messaggi di conferma per assicurare gli utenti che le loro operazioni sono state effettuate.

1.2.1 Criteri prestazionali

Tempi di risposta	Il sistema si prepone l'obiettivo di essere il più possibile reattivo, ovvero di effettuare la maggioranza delle operazioni semplici come autenticazione, registrazione, risposta ad un ticket in meno di 1s e al più 10s per operazioni più complesse come la ricerca degli articoli.
Throughput	Il sistema si prepone l'obiettivo di gestire anche picchi improvvisi di utenza senza grossi rallentamenti. Sono previsti più webserver con *load balancer* che permettono quindi di gestire molti più utenti.
Memorizzazione di dati	Il sistema utilizzerà un database MySQL per la memorizzazione di dati testuali (informazioni degli utenti, lista degli articoli, ...) e, per evitare di rendere i file del database troppo grandi, i file immagine saranno memorizzati su disco. Tutti questi dati riceveranno dei backup periodici con strategia 3-2-1, ovvero 3 copie dei dati, su 2 dispositivi fisici diversi e almeno 1 copia in un'altra posizione geografica.

1.2.2 Criteri di affidabilità

Robustezza	L'hardware scelto per il sistema deve essere di livello aziendale e resistente a eventuali problemi hardware come la rottura di un disco fisso, attraverso l'uso di tecnologia RAID, di un alimentatore, con alimentatori ridondanti, alla mancanza di corrente attraverso batterie e sistemi UPS. In nessun caso un singolo crash hardware deve compromettere l'accessibilità al sito. In più, ci si proteggerà da problematiche software usando versioni del webserver e del sistema operativo testate e senza problemi noti.
1extbfDisponibilità	Il sistema deve garantire un *uptime* (tempo di attività) di almeno il 99.9%, ovvero un *downtime* (tempo di inattività) annualizzato di meno di 9 ore. Ciò è cruciale per far sì che l'utenza non venga scoraggiata dall'utilizzo di TecStore come negozio primario, creando perdite potenziali molto alte, soprattutto nei periodi di maggior afflusso di utenza.
Tolleranza agli errori	Il sistema deve garantire l'accessibilità anche in condizioni non ottimali, come il crash di uno dei webserver o un blackout. Ciò è garantito dai componenti ridondanti e dai backup.
Sicurezza	Il sistema deve prevedere tutte le pratiche di sicurezza fondamentali, come l'utilizzo di SSL per la trasmissione dei dati, l'utilizzo di *hashing* e *salt* per le password memorizzate nel database, tutti i dati delle carte di credito e anagrafiche devono essere cifrati prima di essere inseriti nel database utilizzando una cifratura robusta con una chiave che non deve essere esposta pubblicamente per nessun motivo. In caso di tentativo di accesso a schermate riservate da parte di un utente consumatore o viceversa, ovvero un utente del personale che cerca di accedere al catalogo, deve essere previsto un avviso e un *redirect* ad una pagina correttamente accessibile da quel tipo di utente.

1.2.3 Criteri di manutenzione

Lo sviluppo del sistema sarà condotto in modo da facilitare l'estensione utilizzando linguaggi e tecnologie standard come HTML5, CSS3, Bootstrap e Java. Il codice deve essere quindi scritto in modo che sia facile intervenire, sia per risolvere eventuali bug, sia per aggiungere nuove funzionalità.

1.3 Definizioni, acronimi e abbreviazioni

- TecStore: nome della piattaforma
- Cliente: utente che può acquistare, vendere, richiedere assistenza
- Centralinista: utente che controlla le vendite e fornisce assistenza ai clienti
- Magazziniere: utente che controlla la spedizione degli ordini
- Amministratore catalogo: utente che gestisce le vendite da parte della piattaforma
- Amministratore personale: utente che gestisce gli account degli altri utenti, fatta eccezione per i clienti
- DBMS: Database Management System, sistema di gestione di una base di dati

1.4 Panoramica

In questo documento sono descritti in dettaglio:

- Decomposizione in sottosistemi: in cui viene esposto come il sistema è suddiviso in sottosistemi e come ogni sottosistema interagisce con gli altri.
- Mapping hardware/software: in cui vengono descritti i requisiti hardware e software su cui il sistema dovrà girare.
- Gestione dei dati persistenti: in cui viene descritto come i dati verranno memorizzati dal sistema.
- Controllo degli accessi: in cui vengono descritte le funzionalità messe a disposizione per ogni utente.
- Condizioni di boundary: in cui verranno descritte le condizioni limite del sistema come avvio, spegnimento, manutenzione e gestione dei fallimenti.

2 Sistema proposto

2.1 Panoramica

L'architettura del sistema è di tipo client/server. Il server resta in attesa di richiesta da parte degli utenti e risponde nel minor tempo possibile. I motivi per la scelta di un'architettura client/server sono principalmente:

- Performance: il sistema deve offrire buone prestazioni CPU e ottime prestazioni I/O per garantire una buona reattività.
- Scalabilità: il sistema è pensato per essere facilmente scalabile orizzontalmente.
- Affidabilità: il sistema prevede più ridondanze e backup per garantire l'accessibilità da parte degli utenti.
- Riusabilità: il sistema è facilmente riadattabile ad altre realtà di e-commerce.
- Tolleranza agli errori: il sistema prevede ridondanze sufficienti per restare operativo anche in caso di criticità di uno o più componenti.
- Riutilizzo di componenti: il sistema riutilizza più componenti in più punti per semplificare lo sviluppo.
- Basso costo: il sistema punta a ridurre i costi di sviluppo, manutenzione e gestione utilizzando metodologie di sviluppo e hardware minimale, pur rispettando i requisiti di tolleranza agli errori e affidabilità.

2.2 Controllo degli accessi

	Account	Assistenza	Carrello	Ordine	Vendita
Utente non autenticato	✓ Solo per registrazione, autenticazione e recupero password	×	×	×	✓ Solo per ricerca e visualizzazione dettagli
Cliente	✓ Solo per modifica	✓	✓	✓	✓ Fatta eccezione per autorizzazione e rifiuto di una vendita
Centralinista	×	✓ Solo per risposta e chiusura di ticket esistenti	×	×	✓ Solo per cambiamenti di stato per una vendita "In attesa"
Magazziniere	×	×	×	✓ Solo per cambiamenti di stato per ordini e rimborsi "In attesa"	×
Amministratore Catalogo	×	×	×	×	✓ Fatta eccezione per autorizzazione e rifiuto di una vendita
Amministratore Personale	✓ Solo per creazione e modifica di account di dipendenti	×	×	×	×

3 Decomposizione in sottosistemi

Per realizzare il sistema è prevista un'architettura Three-Tier, con divisione in tre sottosistemi principali:

- Presentation Layer, composto da tutte le interfacce riservate agli utenti finali.
- Application Layer, composto da tutti gli oggetti che si occupano di gestire e manipolare le operazioni e i dati che provengono dal Presentation Layer.
- Storage Layer, composto dai sistemi di memorizzazione dei dati persistenti e dalle procedure di memorizzazione e recupero di dati.

3.1 Presentation Layer

Il Presentation Layer si suddivide a sua volta in:

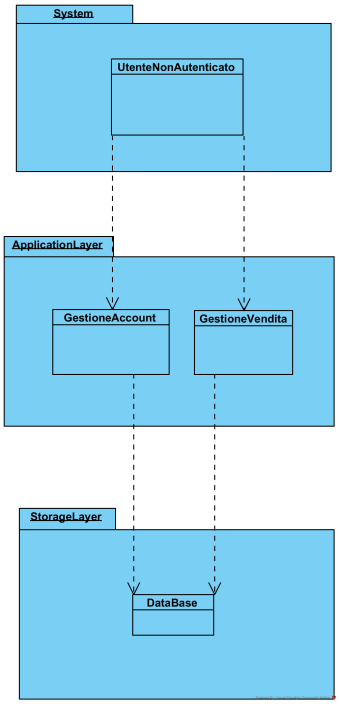
- Sottosistema cliente, che include quasi tutte le funzionalità del sito, come registrazione, autenticazione, ricerca, aggiunta al carrello, acquisto, creazione e risposta a *ticket*, vendita di articoli.
- Sottosistema centralinista, che si occupa dei *ticket* e di autorizzare le vendite dei clienti.
- Sottosistema magazziniere, che si occupa di confermare la spedizione degli ordini e confermare la ricezione degli articoli per i quali i clienti richiedono un rimborso.
- Sottosistema amministratore personale, che si occupa di gestire l'inserimento e la modifica degli account riservati ai dipendenti della piattaforma.
- Sottosistema amministratore catalogo, che si occupa di gestire l'inserimento e la modifica degli articoli venduti dalla piattaforma.

3.2 Application Layer

L'Application Layer si suddivide a sua volta in:

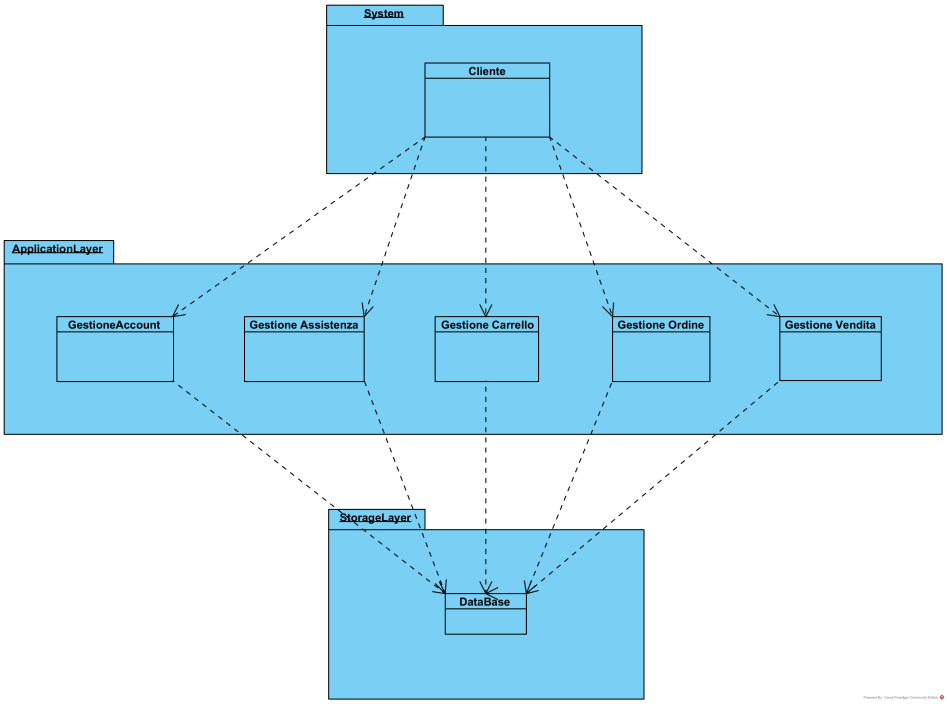
- GestioneAccount, che contiene tutte le operazioni riguardanti gli account degli utenti come registrazione, modifica e autenticazione.
- GestioneAssistenza, che contiene tutte le operazioni riguardanti i *ticket* come creazione, risposta e chiusura.
- GestioneCarrello, che contiene tutte le operazioni riguardanti il carrello come aggiunta e rimozione.
- GestioneOrdine, che contiene tutte le operazioni riguardanti gli ordini come creazione, annullamento, rimborso.
- GestioneVendita, che contiene tutte le operazioni riguardanti le vendite, sia dei clienti che della piattaforma, come creazione, rimozione, visualizzazione e modifica.

3.2.1 Utente non autenticato



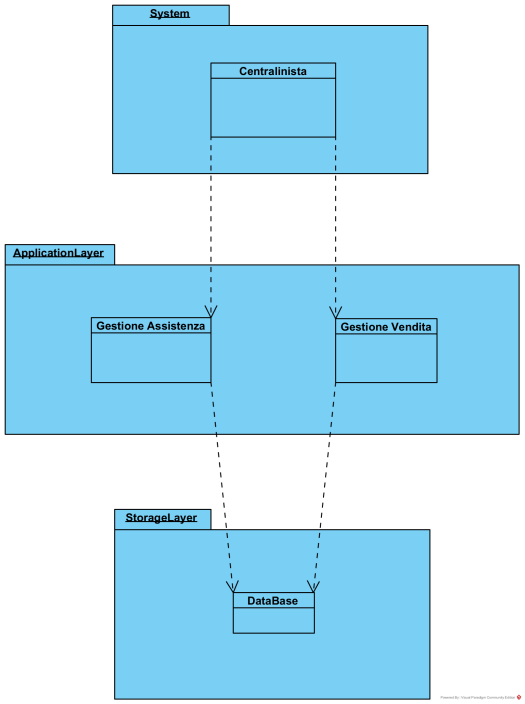
- un utente non autenticato può accedere al sottosistema Account soltanto per autenticarsi, recuperare la password e per registrarsi.
- un utente non autenticato può accedere al sottosistema Vendita soltanto per ricercare un articolo e per visualizzare i dettagli di un articolo.

3.2.2 Cliente



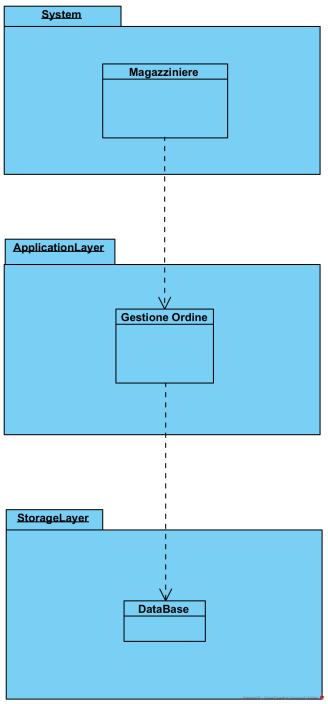
- un cliente autenticato può accedere al sottosistema Account soltanto per la modifica delle proprie informazioni come indirizzo, dati della carta di credito o password.
- un cliente autenticato può accedere al sistema assistenza per effettuare tutte le operazioni previste per il sottosistema Assistenza, quindi creazione, risposta e chiusura di un ticket.
- un cliente autenticato può accedere al sistema assistenza per effettuare tutte le operazioni previste per il sottosistema Carrello, quindi inserimento e rimozione di articoli.
- un cliente autenticato può accedere al sistema assistenza per effettuare tutte le operazioni previste per il sottosistema Ordine, quindi creazione, annullamento e rimborso.
- un cliente autenticato può accedere al sistema assistenza per effettuare tutte le operazioni previste per il sottosistema Vendita, quindi creazione, modifica e annullamento, fatta eccezione per le operazioni riservate come autorizzazione e rifiuto vendita, che sono di competenza dei centralinisti.

3.2.3 Centralinista



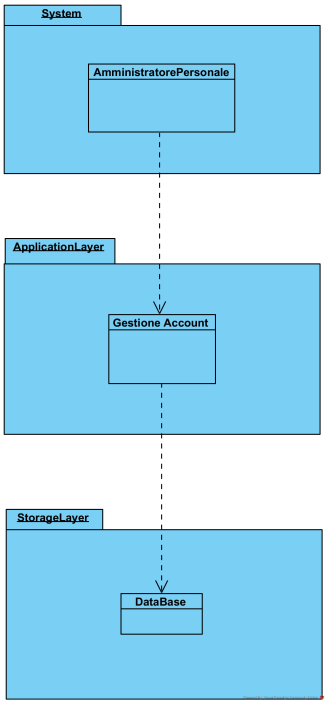
- Un centralinista ha accesso al sottosistema Assistenza per le operazioni di risposta e chiusura di un ticket, ma non può crearne uno nuovo.
- un centralinista ha accesso al sottosistema Vendita solo per l'autorizzazione o il rifiuto di una vendita immessa da un cliente.

3.2.4 Magazziniere



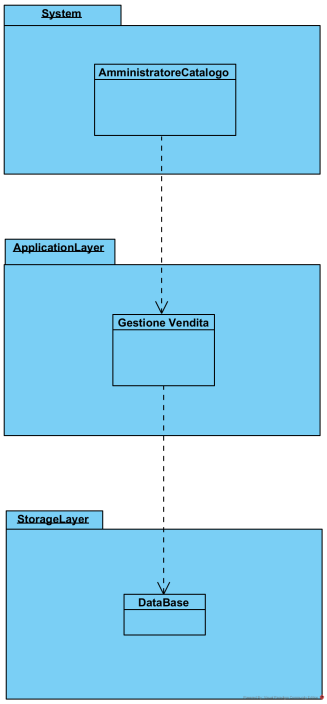
- Un magazziniere ha accesso al sottosistema Ordine solo per il cambio di stato di un ordine in seguito ad una spedizione o al cambio di stato di un rimborso in seguito al ricevimento dell'articolo.

3.2.5 Amministratore Personale



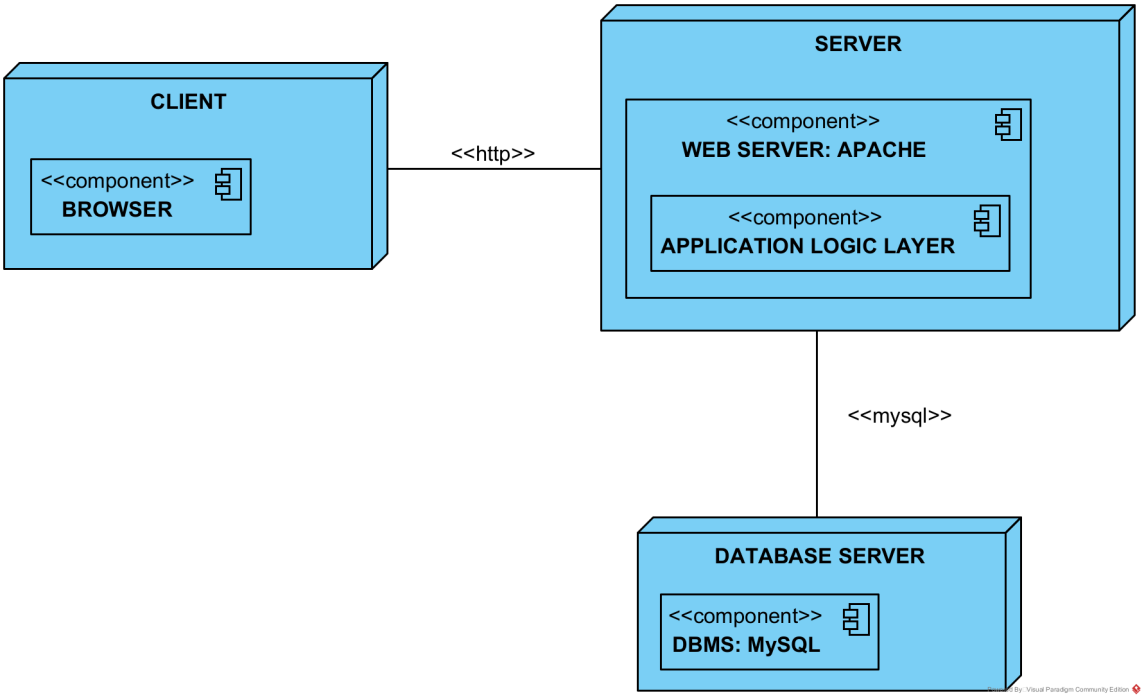
- Un amministratore del personale ha accesso al sottosistema Account solo per l'inserimento e la modifica degli account dei dipendenti.

3.2.6 Amministratore Catalogo



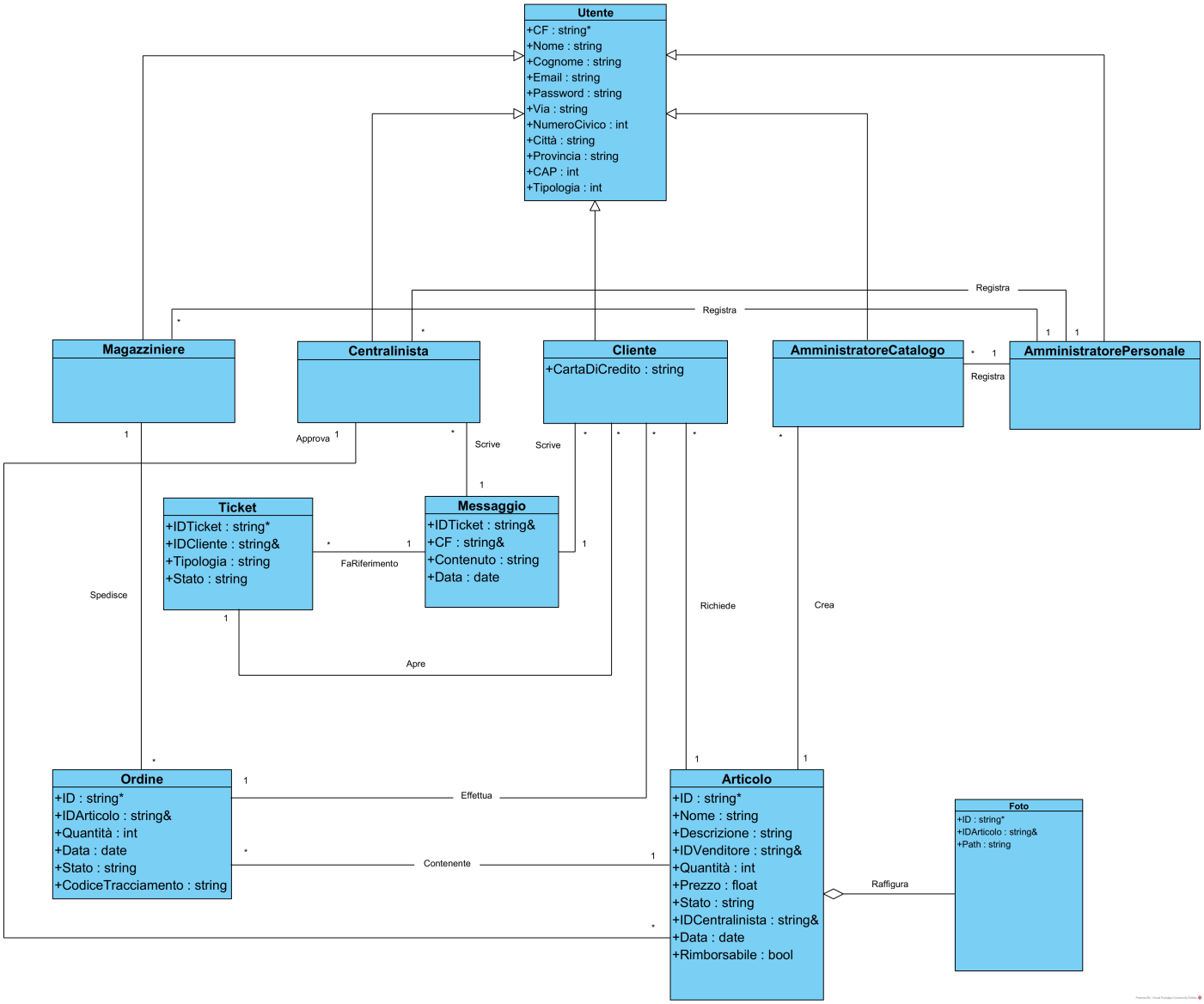
- Un amministratore del catalogo ha accesso al sottosistema Vendita solo per l'inserimento e la modifica di articoli.

3.3 Mapping Hardware/Software



- **Webserver**: Il webserver utilizzato è Apache Tomcat
- **Interface Layer**: Gli utenti si interfacciano con il sistema mediante un comune browser HTTP.
- **Application Layer**: Tutte le funzionalità del sistema sono implementate in linguaggio Java utilizzando il componente Java Servlet.
- **Storage Layer**: Il sistema utilizza il DMBS MariaDB per la memorizzazione dei dati testuali (informazioni degli account, storico ordini, lista vendite, ...) e il filesystem ext4 per memorizzare le foto degli articoli.

3.3.1 Class Diagram



4 Boundary Condition

4.1 Avvio del sistema

Per l'avvio del sistema è necessario che almeno un'istanza del webserver e del database siano attive. All'avvio del sistema operativo i due servizi devono essere quindi avviati automaticamente senza intervento manuale.

4.2 Spegnimento del sistema

Nell'eventualità in cui sia richiesto che uno dei server vada offline per qualsiasi motivo, deve essere previsto che almeno un'altra istanza del DBMS e del webserver siano attive. Se non lo sono, l'intero sistema può andare offline per un tempo indefinito.

4.3 Fallimenti del sistema

Ci sono più scenari in cui il sistema può subire un fallimento. Partendo da quelli non critici:

1. Fallimento o spegnimento di uno dei server, che può essere causato dalla perdita di connessione ad internet, blackout o un guasto hardware. Se le ridondanze sono attive, riduce le prestazioni del sistema se ci sono più utenti, ma non è un errore critico.

2. Fallimento, spegnimento o perdita di connessione ad internet del dispositivo client, che deve essere correttamente gestito, quindi evitando, ad esempio, ordini duplicati. Il sistema deve mantenere le informazioni informazioni inserite dall'utente fino a quel momento.

Tra i fallimenti critici ci sono:

1. Fallimento di uno o più server, sia per motivi hardware che software, che può essere fatale nel caso non ci siano più ridondanze sufficienti a gestire tutta l'utenza, peggiorando le prestazioni del sito al punto in cui può fallire del tutto. È necessario un intervento manuale per ripristinare almeno un'istanza del webserver e del DBMS per ripristinare la funzionalità del sistema.

2. Fallimento dei backup, che può succedere in caso di spazio insufficiente per memorizzare i dati e che può rendere il sito inoperabile in seguito a un fallimento totale. È un errore che nella migliore delle ipotesi fa perdere qualche giorno di informazioni e, in casi catastrofici, può far perdere tutte le informazioni memorizzate nel sistema. L'ultimo caso è irrecuperabile.

4.4 Casi d'uso

4.4.1 Configurazione di un nuovo sistema

ID	UC1 NuovoServer	
Descrizione	Un sysadmin aggiunge un nuovo server.	
Partecipanti	Sysadmin	
Condizione d'ingresso	Un sysadmin ha accesso ad un nuovo server.	
Flusso di eventi	**Sysadmin**	**Sistema**
	Dà i comandi per installare Java, Tomcat e MariaDB.	
		Installa i software richiesti.
	Utilizza lo script ad-hoc per la configurazione di un nuovo server.	
		Scarica e configura i sorgenti nelle cartelle opportune e imposta i servizi per essere avviati automaticamente all'avvio del sistema operativo.
	Aggiunge l'indirizzo IP del nuovo server al load balancer.	
Condizione d'uscita	Il nuovo server è operativo e risponde alle richieste degli utenti.	

4.4.2 Avvio di un server

ID	UC2 AvvioServer	
Descrizione	Un sysadmin avvia un server.	
Partecipanti	Sysadmin	
Condizione d'ingresso	Un sysadmin accede al server.	
Flusso di eventi	**Sysadmin**	**Sistema**
	Avvia il server attraverso il tasto dedicato.	
		Avvia il sistema operativo, sincronizza il database con gli altri nodi e avvia i servizi necessari.
Condizione d'uscita	Il nuovo server è operativo e risponde alle richieste degli utenti.	

4.4.3 Avvio del sistema

ID	UC3 AvvioSistema	
Descrizione	Un sysadmin avvia il sistema.	
Partecipanti	Sysadmin	
Condizione d'ingresso	Un sysadmin accede a uno o più server.	
Flusso di eventi	**Sysadmin**	**Sistema**
	Avvia uno o più server attraverso il tasto dedicato.	
		Avvia il sistema operativo, sincronizza il database con gli altri nodi e avvia i servizi necessari.
Condizione d'uscita	Il sistema è operativo e risponde alle richieste degli utenti.	

4.4.4 Spegnimento di un server

ID	UC4 StopServer	
Descrizione	Un sysadmin spegne un server.	
Partecipanti	Sysadmin	
Condizione d'ingresso	Un sysadmin accede al server.	
Flusso di eventi	**Sysadmin** Spegne il server attraverso il tasto dedicato.	**Sistema** Salva le informazioni temporanee su disco, disattiva i servizi e il sistema operativo.
Condizione d'uscita	Il server è offline.	

4.4.5 Spegnimento del sistema

ID	UC5 StopSistema	
Descrizione	Un sysadmin spegne il sistema.	
Partecipanti	Sysadmin	
Condizione d'ingresso	Un sysadmin accede al server.	
Flusso di eventi	**Sysadmin** Spegne tutti i server attraverso il tasto dedicato.	**Sistema** Salva le informazioni temporanee su disco, disattiva i servizi e il sistema operativo.
Condizione d'uscita	Il sistema è offline.	