

Problem

- Hotels manage employees across multiple departments with different access needs.
- Manual account and permission management is time-consuming and error-prone.
- Inconsistent access control increases security and operational risks.
- Disconnected systems make IT administration and maintenance difficult.
- Small and medium-sized hotels often operate with limited IT resources, making centralized identity management valuable for simplifying user administration and access control.

Stakeholders & Requirements

Stakeholders:

- Hotel employees (Front Desk, Housekeeping, Management, etc.)
- Hotel guests
- Hotel IT administrators

Functional Requirements:

- Centralized Active Directory authentication
- Role-based access to departmental resources
- Hotel website for reservations and guest management
- Secure shared file storage

Non-Functional Requirements:

- Secure authentication and authorization
- Scalable infrastructure for future growth
- Simple Administration through centralized management.

Our Solution

We developed a centralized hotel IT infrastructure that combines **Active Directory**, role-based access control (**RBAC**), **shared network resources**, and a **Django-based hotel management website**.

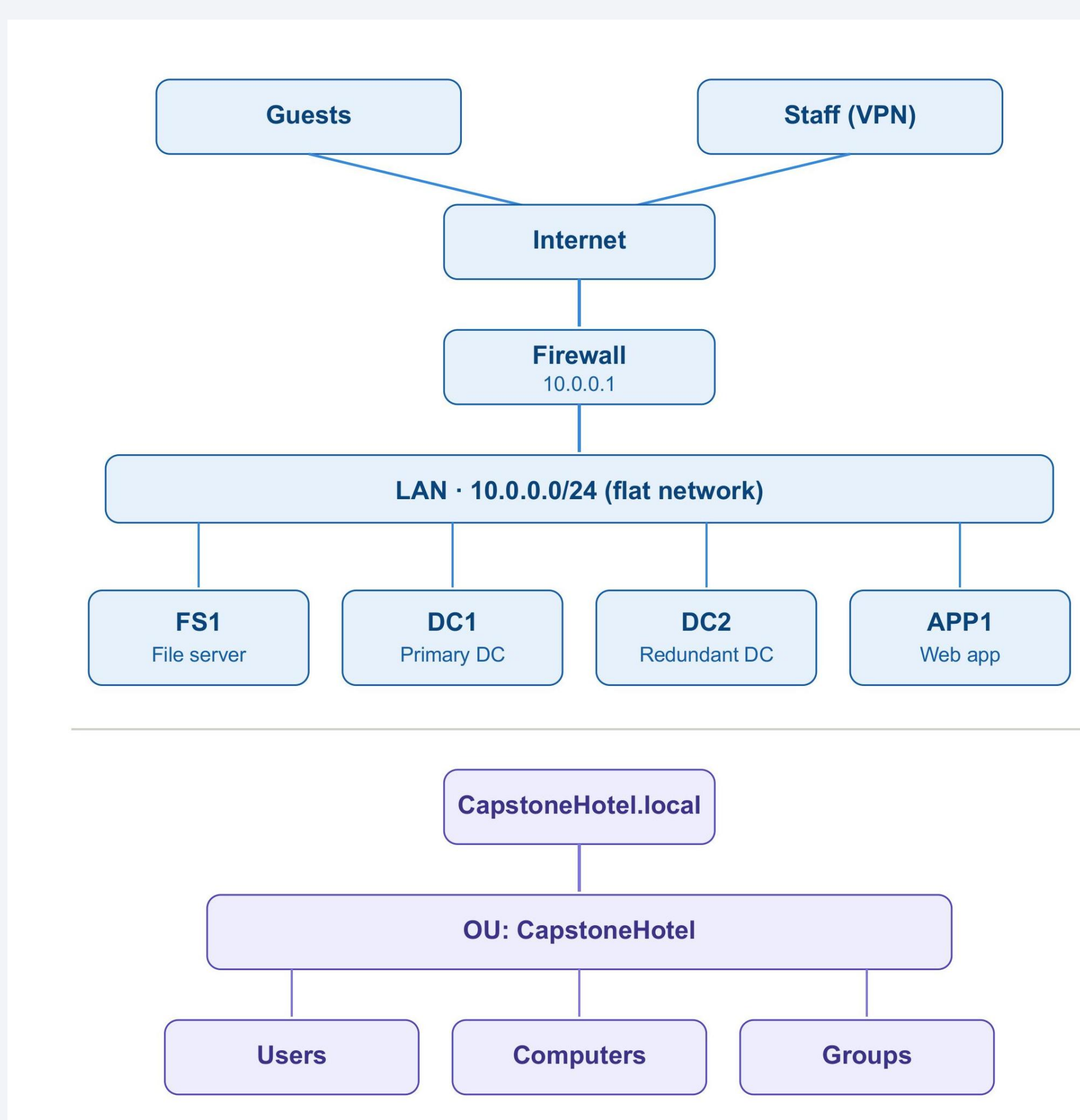
This system:

- Simplifies user administration
- Secures access to department-specific resources
- Provides a scalable foundation for hotel operations

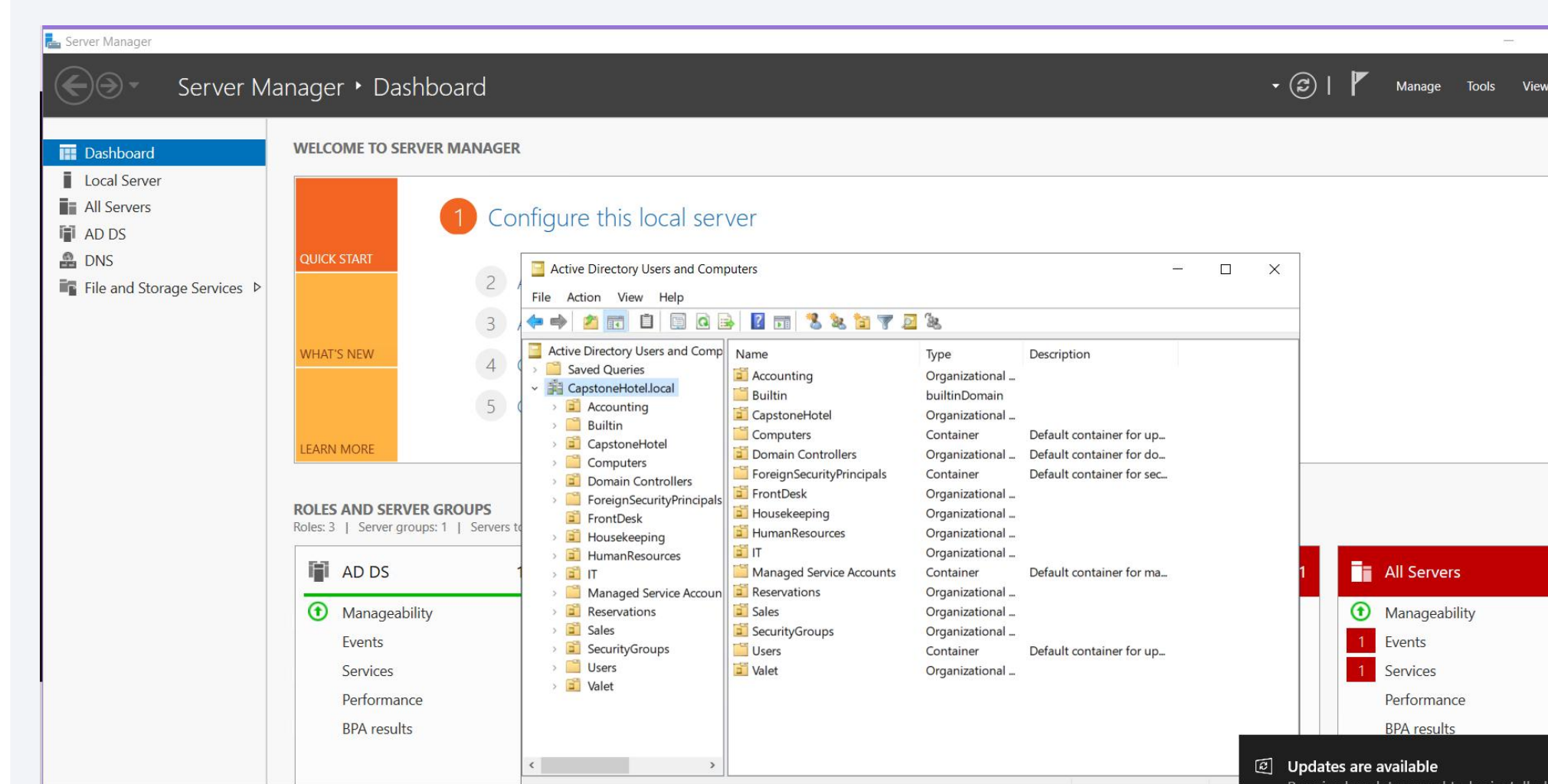
Key Design Decisions:

- Centralized Identity Management:** Active Directory provides a single source for user authentication, Group Policy, and DNS management
- RBAC:** Permissions are assigned through security groups, allowing employees to access required resources only
- Integrated Web Application:** The Django website uses LDAP to authenticate staff through AD while providing hotel reservation and management features

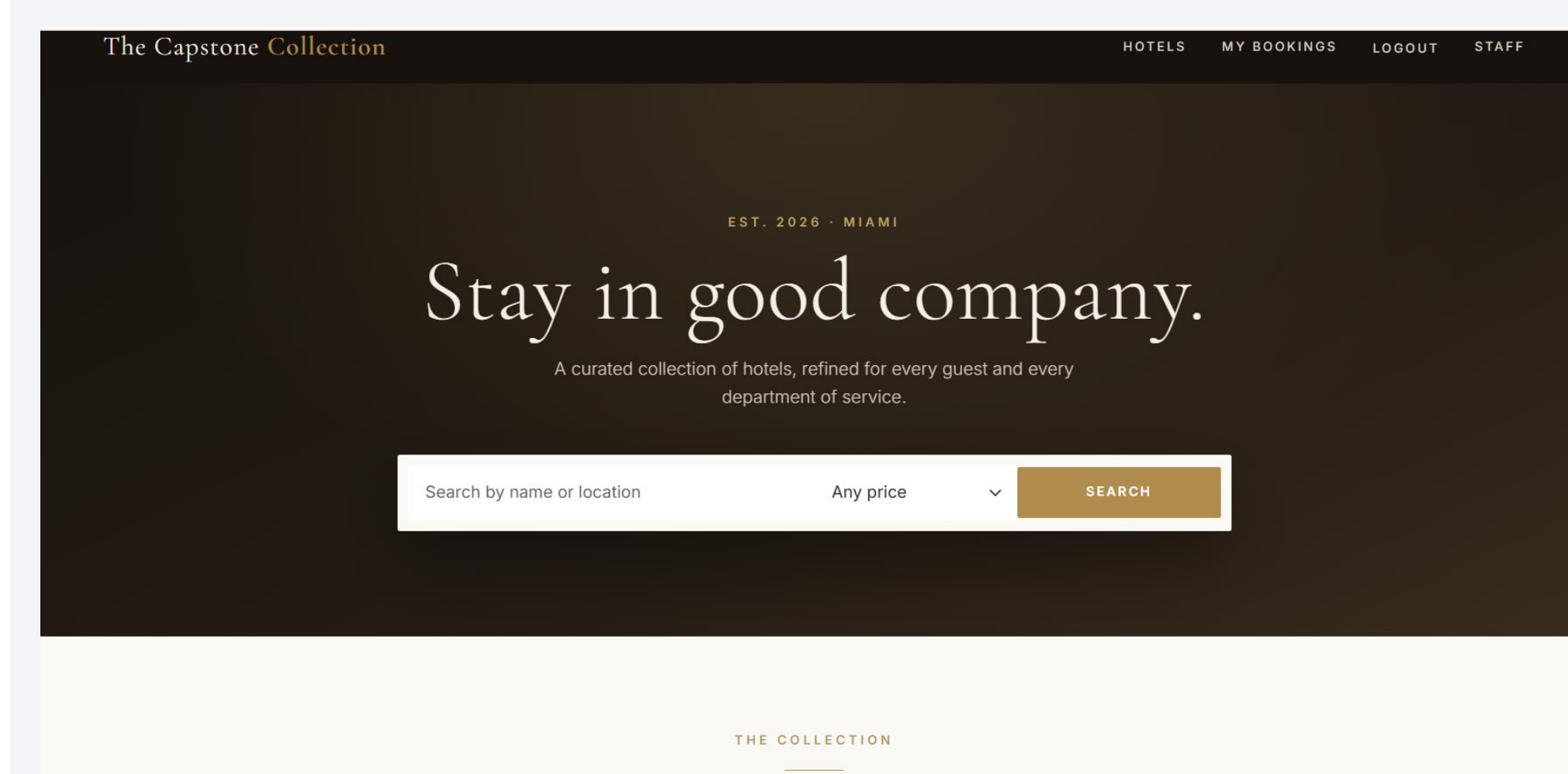
Architecture



Demo & Screenshots



Active Directory domain with centralized user, group, and organizational unit (OU) management.



Hotel management dashboard with reservation and administrative functionality.

Results & Evaluation

Validation Testing:

- Active Directory user authentication
- RBAC permissions
- Shared folder access
- Django website integration with Active Directory
- Group Policy enforcement

Validation Results:

- ✓ Successfully authenticated users through Active Directory
- ✓ Verified role-based access for hotel departments
- ✓ Confirmed secure access to departmental shared resources
- ✓ Validated website authentication and core hotel management functions

Systems & Operations (SO6)

Deployment:

- APP1 hosts the Django hotel management application
- DC1/DC2 provide Active Directory, DNS, and LDAP authentication
- FS1 stores departmental shared files and resources

Database and Infrastructure:

- SQLite stores hotel, booking, and review data
- Active Directory manages employee identities and authentication

Administration:

- User account and permissions are managed through Active Directory
- RBAC and Group Policy enforce secure access across departments
- Departmental file shares are managed using AGDLP and NTFS permissions

What's Next

- Production-ready web deployment
- PostgreSQL database migration
- LDAPS & Microsoft Entra ID (MFA)
- Automated backups and security hardening
- Additional hotel management features

Acknowledgments

We would like to thank the KFSCIS Capstone Program and Prof. Masoud Sadjadi