Student IT Research Exposition

شناص
Shinas

جامعة التقنية
والعلوم التطبيقية
University of Technology
and Applied Sciences

IMPLEMENTING EMAIL SERVICES THROUGH VIRTUAL ENVIRONMENT USING EXCHANGE SERVER

[1] Raqiya Saud Al Harth, [2] Sultan Saif Albusaidi , & [3] Ayah Saleem Al Maskari
[1]36J185@ict.edu.om, [2]36S1878@ict.edu.om, [3]36S1719@ict.edu.om,
University of Technology and Applied Sciences, Ibra, Sultanate of Oman

Abstract: Exchange Server is a platform for email, calendaring, contact management, scheduling, and collaboration. It's designed for use in business or education and runs on the Windows Server operating system. Exchange Server is designed to allow users to access the messaging platform from mobile devices, desktop computers, and web-based systems. Voice messages are supported by Exchange Server's telephony features. Users of Exchange can collaborate by exchanging calendars and documents. Organizations can use the platform's storage and security features. Exchange Server has evolved over time, and it is now a foundational component of Office 365 as a software as a service (SaaS) offering in the Microsoft cloud with Microsoft acting as the service provider. Exchange Server is noted for its high availability (HA) features, which ensure that service is maintained in the event of a failure. This covers the routes for design. Database availability groups (DAGs) were initially introduced in Exchange 2010 and rapidly became one of Exchange's most essential subsystems. When an Exchange server joins a DAG, it runs two AM roles: Primary Active Manager (PAM) and Standby Active Manager (SAM) (SAM). The PAM role will be held by the DAG member server that holds the cluster quorum resource. The PAM role will be moved to the server that acquires ownership of the quorum resource if the DAG node that has the quorum resource fails. The SAM is in charge of informing other Exchange components that execute AM clients about which database copy is active at any given time.

We'll keep the exchange server but with a different approach. In any corporation, encryption and digital certificates are critical issues. By default, Exchange Server encrypts communication between internal Exchange servers and between Exchange services on the local server using Transport Layer Security (TLS). Exchange administrators must, however, examine their encryption requirements for internal and external clients (computers and mobile devices) as well as external messaging servers. We can also utilize Clearswift Secure Exchange Gateway (SXG) to prevent vital information from being exchanged via internal email and then exiting a business. Organizations can adhere to security and compliance standards by detecting malware, suspicious scripts, and identifying sensitive data in messages and attachments based on readily created policy-based procedures.

Keywords :Exchange Server, Database availability groups, High availability, Security,