COLLEGE OF ENGINEERING
Since 1982

Engineering A Better Tomorrow

An Autonomous Institution

Affiliated to VTU, Belagavi
Approved by AICTE, New Delhi
Recognised by UGC with 2(f) & 12(B)
Accredited by NBA & NAAC

SEMINAR :-

Azure Active Directory

Under the Guidance of PROF.GAYATHRI T

Presented By :-

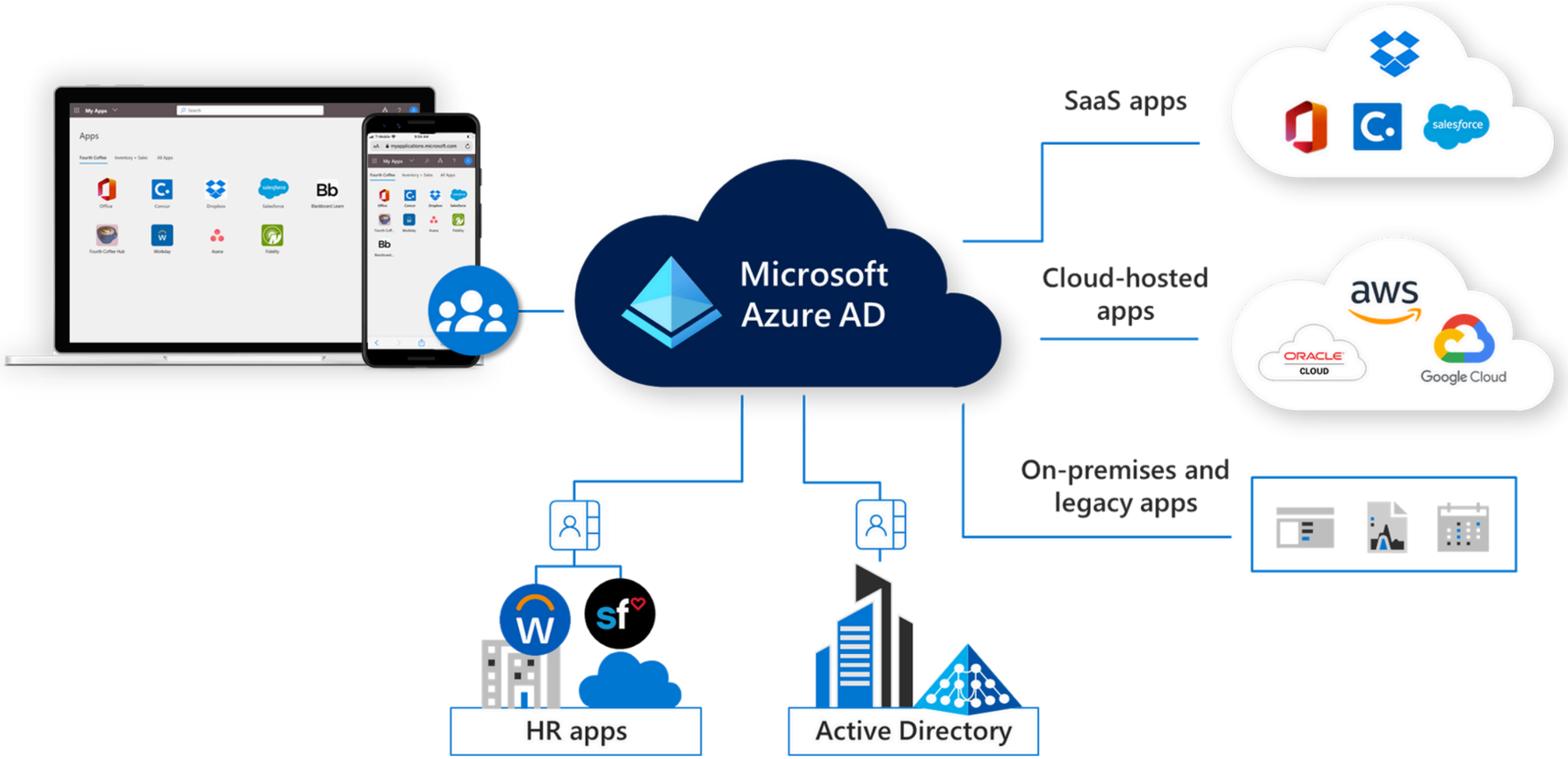
Rohan AR 1MJ20IS078

Abstract

Azure Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service. It serves as the foundation for secure and seamless access to applications, resources, and data in the cloud. Azure AD provides centralized user authentication, authorization, and identity management, enabling organizations to manage identities, enforce security policies, and facilitate single sign-on across a wide range of cloud and on-premises applications. With features like multi-factor authentication, conditional access, and identity protection, Azure AD empowers businesses to enhance security, streamline access, and drive productivity in today's digital landscape.

Introduction

- Microsoft Windows Azure Active Directory (Windows Azure AD or Azure AD) is a cloud service that provides administrators with the ability to manage end-user identities and access privileges. Its services include core directory, access management and identity protection. As the name implies, Azure AD is part of the Microsoft Azure public cloud computing platform.
- The service gives administrators the freedom to choose which information will stay in the cloud, who can manage or use the information, which services or applications can access the information, and which end users can have access. Azure AD can help to provide single sign-on (SSO), so end users don't have to enter passwords multiple times to access cloud applications
- One of the key strengths of Azure AD lies in its versatility and scalability. It caters to organizations of all sizes, from small businesses to large enterprises, and offers flexible deployment options to meet diverse business needs. Whether it's enabling collaboration among internal teams, extending access to external partners, or securely managing customer identities, Azure AD provides the foundation for efficient and secure identity management in the cloud.


Apps
Microsoft Azure AD
SaaS apps
Cloud-hosted apps
On-premises and legacy apps
HR apps
Active Directory
salesforce
aws
ORACLE CLOUD
Google Cloud

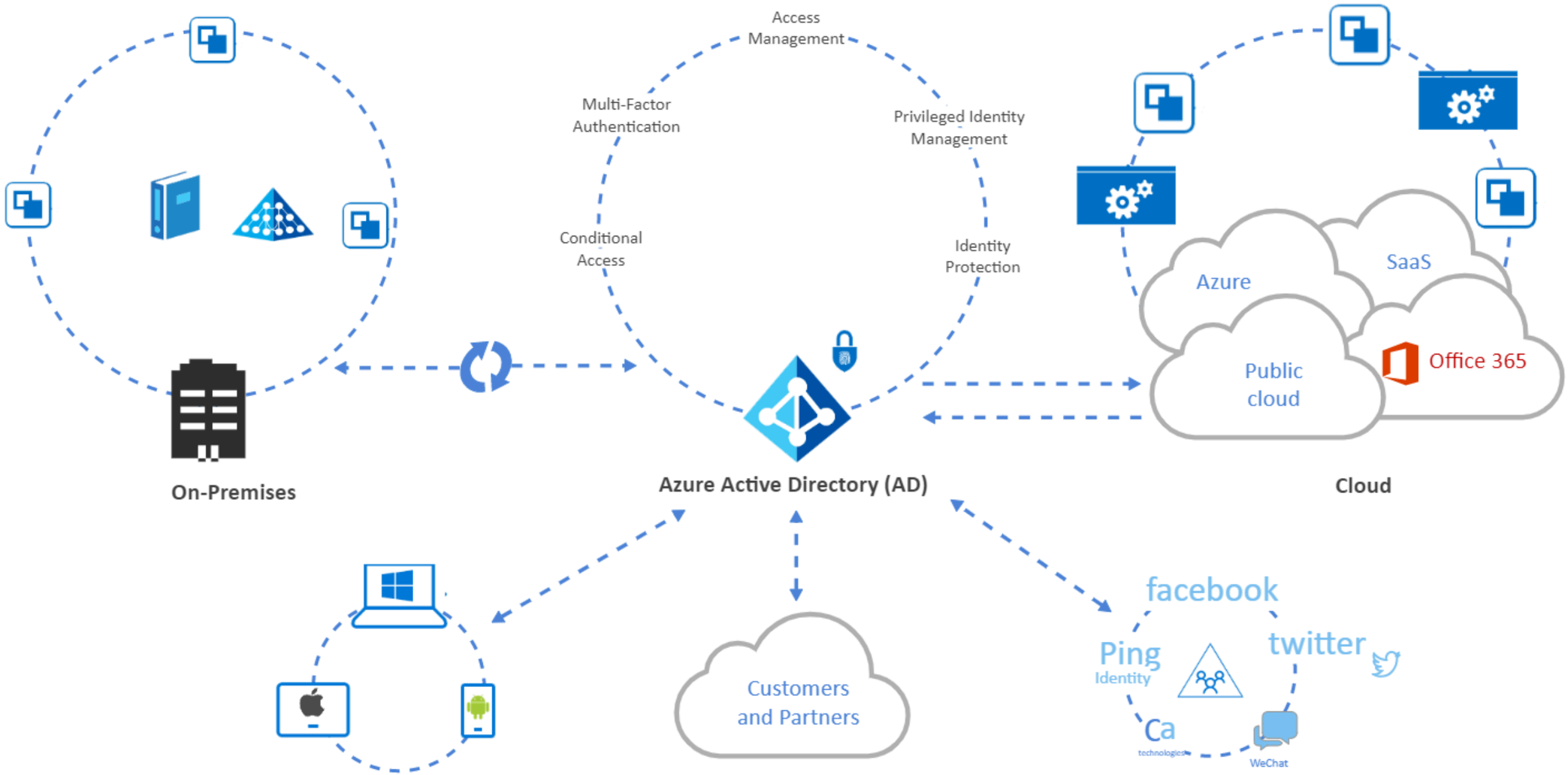
How does Windows Azure Active Directory work?

- Azure AD as a secure online ID card store. It stores individual user profiles and groups of user profiles, each with a username and password. These profiles help manage access to cloud-based apps and servers that use modern authentication methods like SAML 2.0, OpenID Connect, OAuth 2.0, and WS-Federation.

- Users can be grouped together, and each group can be given different levels of access to different apps. This way, administrators can control who gets to use what, based on their roles and responsibilities.

- Azure AD also works with single sign-on (SSO), which is like having a master key for all your cloud apps. Once a user logs in, they can access all the apps they're allowed to use without having to enter their password every time.

- When a user logs in, Azure AD creates something called an access token, which acts like a digital pass. This token is stored on the user's device and lets them access the apps they need. And for extra security, Azure AD can require users to go through additional steps, like entering a code sent to their phone, before they can access important stuff.


Access
Management
Multi-Factor
Authentication
Privileged Identity
Management
Conditional
Access
Identity
Protection
Azure
SaaS
Public
cloud
Office 365
On-Premises
Azure Active Directory (AD)
Cloud
Customers
and Partners
facebook
Ping
Identity
twitter
Ca
technologies
WeChat

Deployment Options

Azure Active Directory (Azure AD) offers flexibility in deployment, allowing organizations to choose the deployment model that best fits their requirements

1. **Cloud-Only Deployment:**

- In a cloud-only deployment, Azure AD serves as the primary identity and access management solution without reliance on on-premises infrastructure.
- Organizations manage user identities, access policies, and security settings entirely within the Azure AD portal.
- This deployment model is suitable for organizations with a cloud-first strategy, startups, or those without an existing on-premises Active Directory infrastructure.

2. **Hybrid Identity with On-Premises Active Directory:**
   - Many organizations have an existing on-premises Active Directory infrastructure managing user identities and access to resources.
   - Azure AD offers seamless integration with on-premises Active Directory through Azure AD Connect, a tool that synchronizes on-premises directory objects with Azure AD.
   - With hybrid identity, organizations can leverage their existing investments in on-premises identity infrastructure while extending identity management to cloud services.
   - Users can enjoy a unified login experience across both cloud and on-premises resources, enhancing productivity and security.
3. **Integration with Microsoft 365 and Other Microsoft Cloud Services:**
   - Azure AD is tightly integrated with Microsoft 365 (formerly Office 365) and other Microsoft cloud services.
   - Organizations subscribing to Microsoft 365 automatically gain access to Azure AD services for user authentication, access control, and security.
   - Azure AD provides seamless access to Microsoft cloud applications such as Exchange Online, SharePoint Online, Teams, and more, simplifying user management and access control.

security features

1. **Multi-Factor Authentication (MFA):**
   - MFA adds an extra layer of security by requiring users to provide two or more forms of authentication before accessing their accounts.
   - For example, in addition to entering a password, users might also need to enter a code sent to their phone.
2. **Single Sign-On (SSO) for Cloud Applications:**
   - SSO allows users to sign in once with their Azure AD credentials and access multiple cloud-based applications without needing to enter their credentials again.
   - This makes it easier for users to access their apps securely and without having to remember multiple passwords.
3. **Context-Based Adaptive Policies:**
   - Azure AD can apply adaptive policies based on the context of the sign-in attempt, such as the user's location, device, or behavior patterns.
   - For example, if a user is attempting to sign in from a new device or location, Azure AD might require additional verification steps.
4. **Identity Governance:**
   - Identity governance features help organizations manage access to resources and ensure compliance with security policies.
   - This includes features like access reviews, privileged identity management, and lifecycle management for user accounts.

Applications

- **User Authentication and Access Management:**Azure AD serves as a centralized identity management platform, allowing organizations to authenticate and authorize users to access applications and resources.
- **Cloud Application Integration:**Azure AD enables seamless integration with a wide range of cloud-based applications, including Microsoft 365 (formerly Office 365), Salesforce, Dropbox, and more.
- **Identity Protection and Security:**Azure AD offers advanced security features to protect against identity-related threats, such as phishing attacks, account compromise, and insider threats.
- **Business-to-Business (B2B) Collaboration:**Azure AD B2B enables secure collaboration with external partners, suppliers, and customers by providing them with access to shared resources and applications.
- **Business-to-Customer (B2C) Identity Management:**Azure AD B2C allows organizations to manage customer identities and enable secure authentication for customer-facing applications and services.
- **Compliance and Reporting:**Azure AD offers reporting and auditing capabilities to help organizations monitor user activities, access patterns, and security events.

Case Studies

Case studies categorized by sector

- **Financial Services Sector:**A leading financial institution in the banking sector implemented Azure Active Directory to enhance security and compliance measures for their online banking platform, ensuring secure access to customer accounts and sensitive financial data.

- **Healthcare Sector:**A healthcare provider leveraged Azure Active Directory to centralize identity management and streamline access to electronic health records (EHR) and patient information across multiple healthcare facilities, improving operational efficiency and ensuring HIPAA compliance.

- **Education Sector:**A large university deployed Azure Active Directory to manage user identities and access controls for students, faculty, and staff across campus-wide IT systems and online learning platforms, enhancing collaboration and educational experiences while maintaining data security and privacy.

- **Retail Sector:**A global retail chain implemented Azure Active Directory to enable secure access to point-of-sale (POS) systems, inventory management applications, and employee portals across retail locations, improving customer service, inventory accuracy, and operational efficiency.

Conclusion

In conclusion, Azure Active Directory (Azure AD) stands as a pivotal solution in modern identity and access management, providing organizations with robust security measures and streamlined access controls for cloud-based applications and resources. Through features such as Multi-Factor Authentication (MFA), Single Sign-On (SSO), and continuous monitoring, Azure AD empowers businesses to bolster their security posture while facilitating seamless user experiences. By adopting Azure AD best practices and leveraging its comprehensive suite of tools, organizations can navigate the complexities of the digital landscape with confidence, ensuring data protection, compliance, and operational efficiency

MVJ College of Engineering
Near ITPB, Whitefield
Bangalore-560 067

Thank You