# Aa

**Azure** *[b5/****p64****]*

**Azure** *[b5/****p65****]* - Azure Services

**Azure** *[b5/****p66****]* - Interacting with Online Services

**Azure** *[b5/****p67****]* - Azure in relation to Azure

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Azure AD** *[b5/****p69****]* – Microsoft Azure AD

**Azure AD** *[b5/****p70, p71, p72, p73****]* – Azure AD Authentication Flow

**Azure AD** *[b5/****p74****]* – Microsoft Authentication Systems

**Azure AD** *[b5/****p75****]* – Identity Architectures in Microsoft

**Azure AD** *[b5/****p76****]* – Synchronization and Federation

**Azure AD** *[b5/****p77****]* – Cloud Identity Models

**Azure AD** *[b5/****p77****]* – Authentication for Hybrid Indentity

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Azure Recon** *[b5/****p78****]* – Introduction to AADInternals

**Azure Recon** *[b5/****p79****]* – AADInternals Recon

**Azure Recon** *[b5/****p80****]* – Username Enumeration Endpoints

**Azure Recon** *[b5/****p81****]* – Username Enumeration: GetCredentialType Endpoint

**Azure Recon** *[b5/****p83****]* – Detecting Throttling: GetCredentialType Endpoint

**Azure Recon** *[b5/****p84, p85****]* – Username Enumeration: OAuth Token Endpoint

**Azure Recon** *[b5/****p86****]* – Legacy Authentication and Protocols

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Azure Password Attacks** *[b5/****p89****]* – Password Spraying in Azure

**Azure Password Attacks** *[b5/****p90****]* – Password Spraying Tool: TrevorSpray

**Azure Password Attacks** *[b5/****p92****]* – Password Spraying Tool: Spray365

**Azure Password Attacks** *[b5/****p94****]* – Azure Smart Lockout

**Azure Password Attacks** *[b5/****p96****]* – Bypass Strategies for Avoiding Lockout

**Azure Password Attacks** *[b5/****p97, p98****]* – Bypassing Technique: Rotating IP Addresses

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**OpenID** *[b5/****p102****]* – OpenIDConnect Flows

**OpenID** *[b5/****p103-p112****]* – Authentication Flows

**OpenID** *[b5/****p113****]* – OAuth Flow Types

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Azure Infrastructure** *[b5/****p115****]* – Infrastructure Components

**Azure Infrastructure** *[b5/****p116****]* – How Azure Organizes Items

**Azure Infrastructure** *[b5/****p117****]* – Control Plane and Data Plane

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Running Commands on Azure** *[b5/****p119****]* – Azure CLI Tools

**Running Commands on Azure** *[b5/****p120****]* – Azure CLI Basics

**Running Commands on Azure** *[b5/****p121****]* – Azure VM Operations

**Running Commands on Azure** *[b5/****p122****]* – Running Commands on Virtual Machines

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**ngrok** *[b5/****p124****]* – Introduction to ngrok

**ngrok** *[b5/****p125****]* – How Does It Work?

**ngrok** *[b5/****p126****]* – Example ngrok Flow

**ngrok** *[b5/****p127****]* – Visualization of ngrok

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**Permissions on Azure** *[b5/****p131****]* – What Is Better than Domain Admin (DA)? Global Administrator (GA)

**Permissions on Azure** *[b5/****p132****]* – Azure Permissions

**Permissions on Azure** *[b5/****p133****]* – Permissions IAM Document

**Permissions on Azure** *[b5/****p134****]* – Where Do Azure Permissions Get Applied?

**Permissions on Azure** *[b5/****p135****]* – Instance Metadata Services in Azure

**Permissions on Azure** *[b5/****p136****]* – Managed Identities in Azure

# 

**365Spray** *[b5/****p98****]*

**AADSTS** *[b5/****p85****]*

**AADInternals** *[b5/****p78, p79****]*

**AADIntPTASpy** *[b5/****p78****]*

**AADSTS 50053 (IdsLocked error code)** *[b5/****p94****]*

**Access Token *[****b5****/p107, p108, p109, p111, p112, p113, p136]***

**Account Lockout** *[b5/****p94****]*

**Actions *[****b5****/p133]***

**AD FS Federation** *[b5/****p76, p95****]*

**AD FS Extranet Lockout** *[b5/****p95****]*

**Assignable Scopes *[****b5****/p133]***

**Authentication Flow** *[b5/****p70, p71, p72****]*

**authentication profiles** *[b5/****p136****]*

**autodiscover** *[b5/****p86****]*

**AWS API Gateway** *[b5/****p96, p98****]*

**AWS Terms of Service (ToS)** *[b5/****p98****]*

**az** *[b5/****p119****]*

**az** **vm** *[b5/****p120, p121, p122****]*

**Az Key Vault *[****b5****/p136]***

**Az PowerShell 7** *[b5/****p119****]*

**Azure Active Directory (Azure AD)** *[b5/****p65, p74, p75, p102, p104, p131****]*

**Azure Active Directory Domain Services (Azure AD DS)***[b5/* ***p74, p75****]*

**Azure AD Connect Agent** *[b5/****p76****]*

**Azure AD Connect Synchronization** *[b5/****p131****]*

**Azure AD Tenant** *[b5/****p70****]*

**Azure API Management** *[b5/****p115****]*

**Azure authentication library *[****b5****/p120]***

**Azure Automation *[b5/p121]***

**Azure Backup** *[b5/****p115****]*

**Azure Blobs** *[b5/****p115****]*

**Azure CLI** *[b5/****p66, p119, p120, P135****]*

**Azure Cloud Shell** *[b5/****p66, p119****]*

**Azure Compute** *[b5/****p115****]*

**Azure CosmosDB** *[b5/****p115****]*

**Azure DevOps** *[b5/****p115****]*

**Azure FrontDoor** *[b5/****p115****]*

**Azure Platform managed identity (System Assigned Managed Identity)** *[b5/****p136****]*

**Azure PowerShell Module(s)** *[b5/****p66****]*

**Azure Portal** *[b5/****p66, p70, p103,****]*

**Azure Smart Lockout** *[b5/****p84, p89, p90, p92, p94, p95, p96, p97, p98****] [****Old Book b5/p149****]*

**B2B (Business to Business)** **Federation** *[b5/****p74****]*

**B2C (Business to Customer) Federation** *[b5/****p74****]*

**base64** *[b5/****p80****]*

**Basic Auth** *[b5/****p86, p96****]*

**Bearer Token *[****b5****/p107]***

**BuiltIn Roles *[****b5****/p132, p133]***

**BurpSuite** *[b5/****p92, p97, p98****]*

**BurpSuite IP Rotate** *[b5/****p96, p98****]*

**Central Authentication Server** *[b5/****p102****]*

**Client Credentials Flow** *[b5/****p113****]*

**Cloud Hosted Azure Active Directory Domain Services** *[b5/****p75****]*

**Cloud Identity** *[b5/****p77****]*

**Cloud Identity Models** *[b5/****p77****] [****Old b5/p70****]*

**Cloud-only Identity** *[b5/****p77****] [****Old b5/p70****]*

**Code Flow** *[b5/****p102, p104, p105, p113, p120****]*

**Conditional Access Policy** *[b5/****p72****,* ***p92****,* ***p105, p109, p112****]*

**Consent Screen** *[b5/****p106****]*

**Contributer** *[b5/****p132, p133, p134****]*

**Control Plane** *[b5/****p117****]*

**CSRF Code Flow** *[b5/****p113****]*

**curl** *[b5/****p80, p81, p83, p84, p135, p136****]*

**Custom Roles *[****b5****/p132]***

**dataActions *[****b5****/p133]***

**Data Plane** *[b5/****p117, p133****]*

**Device Code Flow** *[b5/****p113, p120****]*

**Device Code Flow** **Phishing** *[b5/****p113, p120****]*

**Domain Admin (DA)** *[b5/****p131****]*

**End user-managed identity (User Assigned Managed Identity)** *[b5/****p136****]*

**Enterprise Administrators** *[b5/****p131****]*

**error code response** *[b5/****p84, p85****]*

**error code response 50034** *[b5/****p85****]*

**error code response 50126** *[b5/****p85****]*

**Ews-Crack** *[b5/****p86****]*

**Exchange ActiveSync (EAS)** *[b5/****p86****]*

**exchange online powershell** *[b5/****p86****]*

**execution plan** *[b5/****p92****]*

**Extensions *[****b5****/p133]***

**Extranet Smart Lockout** *[b5/****p95****]*

**fat clients** *[b5/****p70****]*

**Federated Identity** *[b5/****p77****] [****Old b5/p70****]*

**Federated Authentication** *[b5/****p77****]*

**FIDO2** *[b5/****p102, p105****]*

**FireProx** *[b5/****p96, p98****]*

**flat structure** *[b5/****p74****]*

**GetCredentialType** *[b5/****p80, p81, p83****]*

**getuserrealm.srf** *[b5/****p81****]*

**Global Administrator (GA)** *[b5/****p131, p132****]*

**GUID *[****b5****/p132]***

**high rate** *[b5/****p83, p84****]*

**Hosted Azure AD DS** *[b5/****p76****]*

**Hybrid Identity** *[b5/****p77****]*

**IAM (Identity Management System)** *[b5/****p66, p74, p75, p133, p134****]*

**Identity Models** *[b5/****p77****]*

**Identities** *[b5/****p136****]*

**IdP *(Identity Provider)*** *[b5/****p72, p76, p81, p82, p108, p110, p113****]*

**IfExistsResult***[b5/****p81, p83****]*

**Instance Metadata Service (IMDS)** *[b5/****p135, p136****]*

**imap** *[b5/****p86****]*

**Invoke-AADIntUserEnumerationAsOutsider** *[b5/****p79****]*

**jitter *[****b5****/p90, p91, p97]***

**jq***[b5/****p81, p82, p83****]*

**JSON***[b5/****p92, p122, p133****]*

**JSON Web Token (JWT)***[b5/****p73, p107,p108****]*

**Kerberos *[****b5****/p74, p102]***

**LDAP *[b5/p74, p75, p76, p102]***

**IdsLocked (AADSTS 50053) *[****b5****/p94]***

**legacy authentication *[****b5****/p86]***

**legacy protocols *[****b5****/p86, p96, p102]***

**Load Balancing *[****b5****/p96, p97]***

**Log Analytics Contributor *[****b5****/p132]***

**Management Groups *[****b5****/p116, p134]***

**map4** *[b5/****p86****]*

**MailSniper** *[b5/****p86****]*

**Managed Authentication** *[b5/****p77****]*

**Metadata** *[b5/****p135, p136****]*

**Metasploit Framework** *[b5/****p86****]*

**MFA** *[b5/****p86, p90, p102, p105, p108, p112****]*

**Microsoft Active Directory Domain Services (Microsoft AD DS)** *[b5/****p75****]*

**Microsoft Azure** *[b5/****p65****]*

**Microsoft Exchange Online** *[b5/****p86****]*

**MicrosoftOnline Login portal (MSOL)** *[b5/****p71, p104, p120****]*

**Microsoft Authentication Library (MSAL) *[****b5****/p120]***

**MSOLSpray *[****b5****/p89]***

**Modern authentication *[****b5****/p86, p102]***

**NameSpaceType *[****b5****/p81]***

**ngrok *[****b5****/p124]***

**NT Hash** *[b5/****p76****]*

**NTLMv2** *[b5/****p74****]*

**Oauth2** *[b5/****p65, p74, p86, p87, p102, p104, p113, p120, p136****]*

**Oauth Token** *[b5/****p80, p84, p84, p89****]*

**Office 365 Portal** *[b5/****p66****]*

**Okta** *[b5/****p72,******p74, p102****]*

**On Prem AD DS** *[b5/****p74****]*

**On Premise** *[b5/****p75****]*

**On Premise Active Directory** *[b5/****p76, p131****]*

**On-Premise Identity Provider** *[b5/****p77****]*

**OpenIDConnect Identity Provider (OIDC IdP)***[b5/****p65, p74, p75, p102, p104, p107, p120, p131****]*

**Owner** *[b5/****p132****]*

**Pass-through Authentication (PTA)** *[b5/****p76, p77****]*

**Pass-Thru-Authentication agent** *[b5/****p78, p95****]*

**Password Guessing *[****b5****/p80, p84]***

**Password Hash Synchronization (PHS)** *[b5/****p76, p77, p95****]*

**Password Protection** *[****Old Book b5/p150****]*

**Password Spraying** *[b5/****p89****]*

**PBKDF2 Hash** *[b5/****p76****]*

**Permissions *[****b5****/p132, p133, p134]***

**Ping Federate** *[b5/****p72,******p76****]*

**PKCE** *[b5/****p113****]*

**pop3** *[b5/****p86****]*

**Powershell modules***[b5/****p78, p119****]*

**Primary Refresh Token (PRT) *[****b5****/p107, p110, p111, p113]***

**Prohibited Activities** *[b5/****p98****]*

**rate limit***[b5/****p80****]*

**Reader** *[b5/****p132, p133****]*

**Refresh Token *[****b5****/p107, p110, p111, p113]***

**Refresh Token Flow *[****b5****/p113]***

**Resource Groups *[****b5****/p116, p134]***

**Resources *[****b5****/p116, p134]***

**Role Based Access Control (RBAC)** *[b5/****p66, p132****]*

**Role Name *[****b5****/p133]***

**Roles** *[b5/****p132****]*

**Round-Robin *[****b5****/p96, p97]***

**rst2.srf *[****b5****/p80]***

**Runbooks *[****b5****/p121]***

**S3-equivalent block storage *[****b5****/p115]***

**SAML** *[b5/****p65, p74, p102****]*

**SCCM** *[b5/****p121****]*

**Secure Token Server (STS)** *[b5/****p108****]*

**SKU *[****b5****/p104]***

**Smart Lockout** *[b5/****p84, p89, p90, p92, p94, p95, p96, p97, p98****] [****Old Book b5/p149****]*

**smtp** *[b5/****p86****]*

**smtp auth** *[b5/****p87****]*

**Spray365 *[****b5****/p89, p92, p94, p98]***

**ssh *[****b5****/p97]***

**SSO** *[b5/****p69****]*

**staging mode** *[b5/****p76****]*

**Subscriptions *[****b5****/p116, p134]***

**Synchronized Identity** *[b5/****p77****] [****Old b5/p70****]*

**System Assigned Managed Identity (Azure Platform managed identity) *[****b5****/p136]***

**Tenant** *[b5/****p72, p97****]*

**Terraform** *[b5/****p113****]*

**throttle *[****b5****/p83]***

**ThrottleStatus *[****b5****/p83]***

**Token Expiration *[****b5****/p110]***

**TrevorProxy *[****b5****/p90, p97]***

**TrevorSpray *[****b5****/p86, p89, p90, p94, p97]***

**User Access Administrator Built-in role *[****b5****/p131]***

**User Assigned Managed Identity (End user-managed identity) *[****b5****/p136]***

**Username Enumeration *[****b5****/p80]***

**User(name) Principal Name (UPN)** *[b5/****p70, p72, p73, p108****]*

**WS** **Federation** *[b5/****p74, p102****]*

**X.509** *[b5/****p75****]*