SC-300 Study Notes

≡ Beskrivelse	SC-300 notes
☰ Kategorier	Sertifisering
◷ Laget	@August 8, 2023 1:15 PM
◷ Last edited time	@August 8, 2023 2:54 PM
🔗 url	https://learn.microsoft.com/en-us/certifications/exams/sc-300/

> ⚠️ Azure AD is changing name to Entra ID

> ⚠️ Be aware of changes! - The Microsoft Documentation changes constantly - check the documentation for the latest updates.

Implement identities in Azure AD (20–25%)

Configure and manage an Azure AD tenant

Task	Business Case	Product/Service/Method	Pros	Cons	Security Risks	License Needed
Configure and manage Azure AD roles	Role-based access control	Azure AD role-based access control (RBAC)	Fine-grained access control	Complexity in managing roles	Inappropriate role assignment	Free, P1, P2
Configure delegation by using administrative units	Delegating admin tasks within organizational units	Azure AD Administrative Units	Delegation of control	Limited to certain tasks and roles	Delegation to untrusted entities	P1, P2
Analyze Azure AD role permissions	Ensuring proper permissions alignment	Azure AD roles and permissions analysis	Insight into permissions	Requires specialized tools	Overly permissive roles	
Configure and manage custom domains	Aligning Azure AD with organizational domain names	Azure AD custom domain configuration	Brand alignment	DNS management complexity	Domain-related vulnerabilities	Free, P1, P2
Configure tenant-wide settings	Global configuration for tenant behavior	Azure AD tenant-wide settings configuration	Centralized control	Limited flexibility	Misconfiguration affects entire tenant	

Create, configure, and manage Azure AD identities

Task	Business Case	Product/Service/Method	Pros	Cons	Security Risks	License Needed
Create, configure, and manage users	Managing user identities	Azure AD user management	Centralized identity management	Complexity in managing users	Unauthorized access, identity theft	Free, P1, P2
Create, configure, and manage groups	Managing group access	Azure AD group management	Group-based access control	Complexity in managing groups	Unauthorized group access	Free, P1, P2

Configure and manage device join and registration	Device management	Azure AD device management	Device control, Conditional Access	Complexity in device management	Unauthorized device access	P1, P2
Assign, modify, and report on licenses	License management	Azure AD license management	Efficient license allocation	Complexity in license management	License misuse	P1, P2

Implement and manage external identities

Task	Business Case	Product/Service/Method	Pros	Cons	Security Risks	License Needed
Manage external collaboration settings in Azure AD	External collaboration	Azure AD B2B collaboration	Collaboration enablement	Complexity in management	External collaboration risks	Free, P1, P2
Invite external users, individually or in bulk	Inviting external users	Azure AD invitations	Bulk invitations	Managing external users	Security risks with external users	Free, P1, P2
Manage external user accounts in Azure AD	Managing external user accounts	Azure AD external user management	Control over external users	Complexity in managing	Unauthorized external access	Free, P1, P2
Configure identity providers, including SAML or WS-fed	Identity federation	Azure AD identity providers	Identity federation	Complexity in configuration	Federation vulnerabilities	P1, P2

Implement and manage hybrid identity

Task	Business Case	Product/Service/Method	Pros	Cons	Security Risks	License Needed
Implement and manage Azure AD Connect	Hybrid identity	Azure AD Connect	Integration with on-premises	Complexity in setup	Synchronization errors	Free, P1, P2
Implement and manage Azure AD Connect cloud sync	Cloud synchronization	Azure AD Connect cloud sync	Cloud-based synchronization	Complexity in setup	Synchronization errors	Free, P1, P2
Implement and manage Password Hash Synchronization (PHS)	Password synchronization:	Azure AD PHS	On-premises password synchronization + High availabillity	Additional infrastructure that needs the same level of protection as DC	Password-related vulnerabilities	Free, P1, P2
Implement and manage Pass-Through Authentication (PTA)	Authentication management	Azure AD PTA	On-premises authentication	Complexity in management	Authentication-related vulnerabilities Denial of Service.	Free, P1, P2
Implement and manage seamless Single Sign-On (SSO)	Single sign-on	Azure AD SSO	Seamless authentication	Complexity in setup	SSO-related vulnerabilities	Free, P1, P2
Implement and manage Federation	Federation management	Azure AD Federation	Federation with other identity providers + with	Complexity in setup	Federation-related vulnerabilities	P1, P2

			custom attributes				
Implement and manage Azure AD Connect Health	Health monitoring	Azure AD Connect Health	Monitoring and insights	Complexity in setup	Misconfiguration risks	P1, P2	
Troubleshoot synchronization errors	Error troubleshooting	Azure AD troubleshooting tools	Tools for diagnosing synchronization errors	Complexity in troubleshooting	Misconfiguration risks		

Implement authentication and access management (25–30%)

Plan, implement, and manage Azure Multifactor Authentication (MFA) and self-service password reset

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks	License Needed	A Ir
Plan Azure MFA deployment, excluding MFA Server	Enhancing security with 2-factor authentication	Conditional Access/ Windows Hello/ Windows Hello for Business/	Increased security	Complexity in setup	MFA bypass risks	Free, P1, P2	
Configure and deploy self-service password reset	Allowing users to reset passwords themselves	Azure AD self-service password reset (SSPR)	User convenience	Potential abuse	Account compromise if not properly secured	Free, P1, P2	
Implement and manage Azure MFA settings	Customizing MFA for organizational needs	Azure MFA settings	Flexibility in MFA configuration	Complexity in management	Misconfiguration risks	P1, P2	
Manage MFA settings for users	Individual user MFA settings	Azure MFA user settings	User-specific MFA settings	Complexity in managing users	Inconsistent user settings	P1, P2	S L a a p n
Extend Azure AD MFA to third party and on-premises devices	Extending MFA to other systems	Azure MFA extensions	MFA across various platforms	Integration challenges	Security risks with third-party integrations	P1, P2	
Monitor Azure AD MFA activity	Monitoring MFA usage and activity	Azure AD MFA monitoring	Insights into MFA usage	Complexity in monitoring	Lack of monitoring may lead to unnoticed issues	P1, P2	

Plan, implement, and manage Azure AD conditional access

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks	License Needed	A Ir
Plan conditional access policies	Planning access controls	Azure AD conditional access planning	Strategic alignment with access needs	Complexity in planning	Inadequate planning leads to access issues	P1, P2	R tu D
Implement conditional access policy assignments	Assigning access policies	Azure AD conditional access assignments	Fine-grained access control	Complexity in assignments	Misassignment risks	P1, P2	
Implement	Controlling	Azure AD conditional	Dynamic access	Complexity in	Misconfiguration	P1, P2	

conditional access policy controls	access based on policies	access controls	control	controls	risks		
Test and troubleshoot conditional access policies	Testing access policies	Azure AD conditional access testing	Ensuring policy effectiveness	Complexity in testing	Ineffective policies if not tested	P1, P2	
Implement session management	Managing user sessions	Azure AD session management	Control over user sessions	Complexity in management	Session hijacking risks	P1, P2	
Implement device-enforced restrictions	Device-based access restrictions	Azure AD device restrictions	Device-level access control	Complexity in restrictions	Device-related access risks	P1, P2	
Implement continuous access evaluation	Continuous access checks	Azure AD continuous access evaluation	Real-time access evaluation	Complexity in implementation	Lack of continuous evaluation leads to risks	P1, P2	
Create a conditional access policy from a template	Using templates for access policies	Azure AD conditional access templates	Simplified policy creation	Limited customization	Template-related risks	P1, P2	

Manage Azure AD Identity Protection

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks	License Needed	A Ir
Implement and manage a user risk policy	Managing risks associated with users	Azure AD user risk policy	Proactive risk management	Complexity in management	Unmanaged user risks	P2	
Implement and manage sign-in risk policy	Managing sign-in risks	Azure AD sign-in risk policy	Protection against suspicious sign-ins	Complexity in management	Unmanaged sign-in risks	P2	
Implement and manage MFA registration policy	Enforcing MFA registration	Azure AD MFA registration policy	Enhanced security with MFA	Complexity in policy enforcement	Lack of MFA registration risks	P2	
Monitor, investigate and remediate risky users	Monitoring and managing risky users	Azure AD risky user monitoring	Identification and remediation of risky users	Complexity in monitoring	Unnoticed risky users	P2	
Implement security for workload identities	Securing workloads	Azure AD workload identity security	Security alignment with workloads	Complexity in implementation	Workload-related security risks	P2	

Implement access management for Azure resources

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks	License Needed	A Ir
Assign Azure roles	Role-based access to Azure resources	Azure RBAC	Fine-grained access control	Complexity in role assignments	Misassignment risks	Free, P1, P2	
Configure custom Azure roles	Customizing roles for specific needs	Azure custom RBAC roles	Tailored access control	Complexity in custom roles	Custom role-related risks	Free, P1, P2	
Create and configure	Managing identities for services	Azure managed identities	Simplified identity	Complexity in configuration	Misconfiguration risks	Free, P1, P2	

managed identities			management for services			
Use managed identities to access Azure resources	Using managed identities for access	Azure managed identity access	Secure and simplified access	Complexity in usage	Misuse of managed identities	Free, P1, P2
Analyze Azure role permissions	Analyzing role-based permissions	Azure role permission analysis	Insight into role permissions	Complexity in analysis	Inadequate analysis leads to permission issues	Free, P1, P2
Configure Azure Key Vault RBAC and policies	Managing access to Azure Key Vault	Azure Key Vault RBAC and policies	Secure control over secrets and keys	Complexity in configuration	Key Vault access risks	Free, P1, P2

Implement access management for applications (15–20%)

Manage and monitor application access by using Microsoft Defender for Cloud Apps

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks	License Needed
Discover and manage apps by using Microsoft Defender for Cloud Apps	Discovering unauthorized cloud apps in the network	Microsoft Defender for Cloud Apps	Visibility into shadow IT	Complexity in management	Unauthorized app risks	E5
Configure connectors to apps	Connecting to various cloud apps	Microsoft Defender connectors	Integration with various apps	Complexity in configuration	Connector-related risks	E5
Implement application-enforced restrictions	Enforcing app-specific restrictions	Microsoft Defender app restrictions	Fine-grained app control	Complexity in enforcement	Misconfiguration risks	E5
Configure conditional access app control	Conditional access to apps	Azure AD conditional access app control	Dynamic access control	Complexity in configuration	Conditional access risks	E3, E5
Create access and session policies in Microsoft Defender for Cloud Apps	Managing access and sessions	Microsoft Defender access policies	Control over access and sessions	Complexity in policy creation	Policy-related risks	E5
Implement and manage policies for OAUTH apps	Managing OAUTH app policies	Microsoft Defender OAUTH policies	Control over OAUTH apps	Complexity in policy management	OAUTH-related risks	E5

Plan, implement, and monitor the integration of Enterprise applications

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks	License Needed
Configure and manage user and admin consent	Managing consent for app access	Azure AD consent management	Control over app access consent	Complexity in management	Consent-related risks	Free, P1, P2
Discover apps by using ADFS application activity reports	Discovering app usage	ADFS activity reports	Insights into app usage	Complexity in reporting	Unnoticed app activity risks	Free, P1, P2
Design and	Designing app	Azure AD app access	Strategic app	Complexity in	Access control	Free, P1, P2

implement access management for apps	access controls	management	access control	design	risks	
Design and implement app management roles	Designing roles for app management	Azure AD app management roles	Role-based app management	Complexity in role design	Role-related risks	Free, P1, P2
Monitor and audit activity in enterprise applications	Monitoring app activity	Azure AD app activity monitoring	Visibility into app activity	Complexity in monitoring	Unnoticed app activity risks	Free, P1, P2
Design and implement integration for on-premises apps by using Azure AD Application Proxy	Integrating on-premises apps	Azure AD Application Proxy	Secure integration with on-premises apps	Complexity in integration	Integration risks	P1, P2
Design and implement integration for SaaS apps	Integrating SaaS apps	Azure AD SaaS app integration	Seamless SaaS app integration	Complexity in integration	SaaS integration risks	Free, P1, P2
Provision and manage users, groups, and roles on Enterprise applications	Managing identities in Enterprise apps	Azure AD Enterprise app management	Centralized identity management	Complexity in management	Identity-related risks	Free, P1, P2
Create and manage application collections	Organizing apps into collections	Azure AD app collections	Organized app management	Complexity in collection management	Collection-related risks	Free, P1, P2

Plan and implement application registrations

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks	License Needed
Plan for application registrations	Planning app registrations	Azure AD app registration planning	Strategic alignment with app needs	Complexity in planning	Inadequate planning risks	Free, P1, P2
Implement application registrations	Registering apps	Azure AD app registrations	Control over app registrations	Complexity in implementation	Registration-related risks	Free, P1, P2
Configure application permissions	Setting app permissions	Azure AD app permissions	Fine-grained permission control	Complexity in configuration	Permission-related risks	Free, P1, P2
Implement application authorization	Authorizing apps	Azure AD app authorization	Secure app authorization	Complexity in implementation	Authorization-related risks	Free, P1, P2
Plan and configure multi-tier application permissions	Multi-tier app permissions	Azure AD multi-tier permissions	Complex permission structures	Complexity in configuration	Multi-tier permission risks	Free, P1, P2
Manage and monitor applications by using App governance	Managing and monitoring apps	Azure AD App governance	Oversight and control over apps	Complexity in governance	Governance-related risks	Free, P1, P2

Plan and implement entitlement management

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks (Specific Threats)	License Needed
Plan entitlements	Planning access to resources	Azure AD Entitlement Management	Strategic alignment with access needs	Complexity in planning	Inadequate planning leading to unauthorized access	P1, P2
Create and configure catalogs	Organizing resources	Azure AD Catalogs	Structured resource management	Complexity in configuration	Misconfiguration leading to exposure of sensitive resources	P1, P2
Create and configure access packages	Packaging access for users	Azure AD Access Packages	Simplified access provisioning	Complexity in package creation	Incorrect packaging leading to excessive permissions	P1, P2
Manage access requests	Handling access requests	Azure AD Access Requests	Controlled access management	Complexity in request management	Unmanaged requests leading to unauthorized access	P1, P2
Implement and manage terms of use	Enforcing terms of use	Azure AD Terms of Use	Legal compliance	Complexity in implementation	Non-compliance with legal requirements	P1, P2
Manage the lifecycle of external users in Azure AD Identity Governance settings	External user management	Azure AD Identity Governance	Lifecycle management of external identities	Complexity in lifecycle management	Unmanaged external users leading to potential breaches	P1, P2
Configure and manage connected organizations	Managing connected organizations	Azure AD Connected Organizations	Collaboration across organizations	Complexity in connection management	Connection-related risks, such as data leakage	P1, P2
Review per-user entitlements by using Azure AD Entitlement management	Reviewing user entitlements	Azure AD Entitlement Review	Insight into user entitlements	Complexity in review process	Unreviewed entitlements leading to excessive access	P1, P2

Plan, implement, and manage access reviews

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks (Specific Threats)	License Needed
Plan for access reviews	Planning regular access reviews	Azure AD Access Reviews	Strategic alignment with compliance needs	Complexity in planning	Inadequate planning leading to compliance failures	P1, P2
Create and configure access reviews for groups and apps	Reviewing access to groups and apps	Azure AD Group/App Access Reviews	Controlled access to groups and apps	Complexity in review creation	Unreviewed access leading to unauthorized access	P1, P2
Create and configure	Structured access review process	Azure AD Access Review Programs	Organized review process	Complexity in program configuration	Misconfigured programs	P1, P2

access review programs					leading to review failures	
Monitor access review activity	Monitoring review process	Azure AD Access Review Monitoring	Visibility into review activities	Complexity in monitoring	Unmonitored activities leading to unnoticed issues	P1, P2
Respond to access review activity, including automated and manual responses	Responding to review findings	Azure AD Access Review Responses	Timely response to review outcomes	Complexity in response management	Delayed or incorrect responses leading to security risks	P1, P2

Plan and implement privileged access

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks (Specific Threats)	License Needed
Plan and manage Azure roles in Privileged Identity Management (PIM)	Role management in PIM	Azure PIM Roles	Fine-grained role control	Complexity in role management	Mismanaged roles leading to unauthorized access	P2
Plan and manage Azure resources in PIM	Resource management in PIM	Azure PIM Resources	Controlled resource access	Complexity in resource management	Mismanaged resources leading to potential breaches	P2
Plan and configure Privileged Access groups	Planning privileged access	Azure Privileged Access Groups	Strategic privileged access control	Complexity in configuration	Misconfiguration leading to excessive privileges	P2
Manage PIM requests and approval process	Managing PIM requests	Azure PIM Requests and Approvals	Controlled privileged access	Complexity in request management	Unmanaged requests leading to unauthorized privileged access	P2
Analyze PIM audit history and reports	Analyzing PIM activities	Azure PIM Audit and Reports	Insight into privileged activities	Complexity in analysis	Unanalyzed activities leading to unnoticed privileged access	P2
Create and manage break-glass accounts	Emergency access accounts	Azure Break-Glass Accounts	Emergency access when needed	Complexity in account management	Mismanaged accounts leading to unauthorized emergency access	P2

Monitor Azure AD

Task	Business Case (Example)	Product/Service/Method	Pros	Cons	Security Risks (Specific Threats)	License Needed
Design a strategy for monitoring Azure AD	Strategic Azure AD monitoring	Azure AD Monitoring Strategy	Aligned monitoring approach	Complexity in design	Inadequate monitoring leading to unnoticed issues	Free, P1, P2
Review and analyze sign-in, audit, and	Log analysis	Azure AD Log Analysis	Insight into activities	Complexity in analysis	Unanalyzed logs leading to	Free, P1, P2

provisioning logs by using the Azure Active Directory admin center					unnoticed activities	
Configure diagnostic settings, including Log Analytics, storage accounts, and Event Hub	Diagnostic settings	Azure AD Diagnostic Settings	Customized diagnostics	Complexity in configuration	Misconfigured diagnostics leading to inadequate insights	Free, P1, P2
Monitor Azure AD by using Log Analytics, including KQL queries	Advanced monitoring	Azure AD Log Analytics	Deep insights into Azure AD	Complexity in monitoring	Inadequate monitoring leading to unnoticed security risks	Free, P1 P2(for more detailed)