1-identities.md

Certainly! Here are the main points of managing Azure identities and governance:

1. **Azure Active Directory (Azure AD)**:
   - **User and Group Management**: Create, manage, and delete users and groups.
   - **Role-Based Access Control (RBAC)**: Assign roles to users and groups to control access to resources.
   - **Self-Service Password Reset (SSPR)**: Allow users to reset their passwords without administrator intervention.
   - **Conditional Access**: Implement policies to control access based on conditions like user location or device state.

2. **Azure Subscriptions and Resource Management**:
   - **Subscription Management**: Create and manage Azure subscriptions, including cost management and billing.
   - **Resource Groups**: Organize resources into groups for easier management and access control.
   - **Azure Policy**: Define and enforce policies to ensure resources comply with organizational standards.

3. **Identity Governance**:
   - **Access Reviews**: Regularly review and certify access to resources.
   - **Privileged Identity Management (PIM)**: Manage, control, and monitor access to important resources.
   - **Entitlement Management**: Automate the assignment of access packages to users.

4. **Security and Compliance**:
   - **Multi-Factor Authentication (MFA)**: Enhance security by requiring multiple forms of verification.
   - **Identity Protection**: Detect and respond to identity-based risks.
   - **Compliance Management**: Ensure resources and identities comply with regulatory requirements.

These points cover the essential aspects of managing identities and governance in Azure[4][5]. If you need more detailed information on any specific area, feel free to ask!

Source: Conversation with Copilot, 21/08/2024 (1) AZ-104: Manage identities and governance in Azure - Training. https://learn.microsoft.com/en-us/training/paths/az-104-manage-identities-governance/. (2) Azure identity & access security best practices | Microsoft Learn. https://learn.microsoft.com/en-us/azure/security/fundamentals/identity-management-best-practices. (3) Manage Azure identities and governance. https://www.youtube.com/watch?v=toYBsLIYpgk. (4) Preparing for AZ-104 - Manage Azure identities and governance (1 of 5). https://learn.microsoft.com/en-us/shows/exam-readiness-zone/preparing-for-az-104-manage-azure-identities-and-governance-1-of-5. (5) What is Identity Governance? | Microsoft Entra ID. https://www.youtube.com/watch?v=VzEn_7Kkv38. (6) What is Identity Governance and Administration (IGA)? - SailPoint. https://www.sailpoint.com/identity-library/identity-governance/. (7) AZ 104 - Manage Identities and Governance in Azure | Udemy. https://www.udemy.com/course/az-104-manage-identities-and-governance-in-azure/.

Sure! Here are the main points of Azure Role-Based Access Control (RBAC) along with further details for each:

1. Role Assignments

- **Security Principal**: Represents a user, group, service principal, or managed identity requesting access.
- **Role Definition**: A collection of permissions, such as read, write, and delete. Examples include Owner, Contributor, and Reader.
- **Scope**: Defines the set of resources the access applies to. Scopes can be at the management group, subscription, resource group, or resource level.

2. Built-in Roles

- **Owner**: Full access to all resources, including the right to delegate access to others.
- **Contributor**: Can create and manage all types of Azure resources but cannot grant access to others.
- **Reader**: Can view existing Azure resources but cannot make any changes.

3. Custom Roles

- **Creation**: Define custom roles to meet specific needs not covered by built-in roles.
- **Permissions**: Specify exact actions allowed, such as read, write, delete, and data actions.
- **Assignment**: Assign custom roles to security principals at specific scopes.

4. Role-Based Access Control (RBAC) Best Practices

- **Least Privilege Principle**: Grant only the minimum permissions necessary for users to perform their tasks.

- **Limit Subscription Owners**: Reduce the number of subscription owners to minimize security risks.
- **Use PIM**: Implement Privileged Identity Management to manage, control, and monitor access to critical resources.

5. Managing Role Assignments

- **Azure Portal**: Use the Azure portal to assign roles to users, groups, and service principals.
- **Azure CLI**: Utilize Azure Command-Line Interface (CLI) for scripting and automation of role assignments.
- **Azure PowerShell**: Employ Azure PowerShell for advanced management and automation tasks.

6. Monitoring and Auditing

- **Activity Logs**: Track changes and access to resources through Azure Activity Logs.
- **Access Reviews**: Regularly review and certify access to ensure compliance and security.
- **Alerts**: Set up alerts for critical changes or access patterns to detect and respond to potential security issues.

These points cover the essential aspects of Azure RBAC. If you need more detailed information on any specific area, feel free to ask!

Source: Conversation with Copilot, 21/08/2024 (1) Best practices for Azure RBAC | Microsoft Learn. https://learn.microsoft.com/en-us/azure/role-based-access-control/best-practices. (2) What is Azure role-based access control (Azure RBAC)?. https://learn.microsoft.com/en-us/azure/role-based-access-control/overview. (3) Azure roles, Microsoft Entra roles, and classic subscription .... https://learn.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles. (4) Understanding and Implementing Azure RBAC | NinjaOne. https://www.ninjaone.com/blog/understanding-and-implementing-azure-rbac/.

Certainly! Here are the main points of Microsoft Entra ID Conditional Access:

1. Policy Creation

- **Define Conditions**: Set conditions based on user identity, device compliance, location, and application.
- **Assign Controls**: Specify access controls like requiring multi-factor authentication (MFA) or blocking access.

2. Signals and Conditions

- **User and Group Membership**: Apply policies to specific users or groups.
- **Device State**: Enforce policies based on whether a device is compliant or domain-joined.
- **Location**: Restrict access based on geographic location or IP address ranges.
- **Application**: Target specific applications for conditional access policies.

3. Access Controls

- **Grant Controls**: Require MFA, device compliance, or terms of use acceptance.
- **Session Controls**: Control user sessions with policies like app-enforced restrictions or sign-in frequency.

4. Policy Enforcement

- **Real-Time Evaluation**: Policies are evaluated in real-time during sign-in attempts.
- **Zero Trust Security**: Implement Zero Trust principles by verifying explicitly, using least privilege access, and assuming breach.

5. Monitoring and Reporting

- **Sign-In Logs**: Monitor sign-in activities and policy evaluations.
- **Conditional Access Insights**: Gain insights into policy impact and effectiveness.
- **Alerts and Notifications**: Set up alerts for unusual sign-in activities or policy violations.

6. Best Practices

- **Start with Report-Only Mode**: Test policies in report-only mode before enforcing them.
- **Use Templates**: Utilize built-in templates for common scenarios.
- **Regular Reviews**: Periodically review and update policies to adapt to changing security needs.

These points cover the essential aspects of Conditional Access in Microsoft Entra ID[4,5]. If you need more detailed information on any specific area, feel free to ask!

Source: Conversation with Copilot, 21/08/2024 (1) Plan a Microsoft Entra Conditional Access deployment - Microsoft Entra ID. https://learn.microsoft.com/en-us/entra/identity/conditional-access/plan-conditional-access. (2) What is Conditional Access in Microsoft Entra ID? - Microsoft Entra ID .... https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview. (3)

Indirect speech - Wikipedia. https://en.wikipedia.org/wiki/Indirect_speech. (4) Los Angeles County, California - Wikipedia. https://en.wikipedia.org/wiki/Los_Angeles_County,_California. (5) Microsoft Entra ID: The Complete Guide to Conditional Access Policies .... https://securityboulevard.com/2024/03/microsoft-entra-id-the-complete-guide-to-conditional-access-policies-2/. (6) entra-docs/docs/identity/conditional-access/plan-conditional ... - GitHub. https://github.com/MicrosoftDocs/entra-docs/blob/main/docs/identity/conditional-access/plan-conditional-access.md.

Certainly! Here are the fundamentals of Azure resources and subscriptions:

`1. Azure Resources`

- **Definition**: An entity managed by Azure, such as virtual machines, storage accounts, databases, and web apps.
- **Resource Groups**: Logical containers that hold related resources for easier management and organization. Each resource can only belong to one resource group.
- **Resource Management**: Resources can be managed through the Azure portal, Azure CLI, Azure PowerShell, and REST APIs.

`2. Azure Subscriptions`

- **Definition**: A logical container used to provision and manage Azure resources. Each resource is associated with one subscription.
- **Billing and Costs**: Subscriptions are used to manage billing and costs. Each subscription generates a monthly invoice based on resource usage.
- **Subscription Types**: Various types of subscriptions are available, including Pay-As-You-Go, Enterprise Agreements, and Free Trial subscriptions.

`3. Management Groups`

- **Hierarchy**: Management groups allow you to organize multiple subscriptions into a hierarchy for unified management.
- **Policy and Access Management**: Apply policies and access controls at the management group level, which are inherited by all subscriptions and resources within the group.

`4. Azure Accounts`

- **Account Administrator**: The person responsible for managing the subscription and billing. This role is assigned to the email address used to create the subscription.
- **Azure AD Tenant**: A dedicated instance of Azure Active Directory associated with the subscription, used for identity and access management.

`5. Resource Tags`

- **Purpose**: Tags are key-value pairs used to organize and categorize resources for easier management, billing, and automation.
- **Usage**: Apply tags to resources, resource groups, and subscriptions to track and manage costs, and to implement governance policies.

`6. Resource Management Tools`

- **Azure Portal**: A web-based interface for managing Azure resources.
- **Azure CLI**: A command-line tool for managing Azure resources.
- **Azure PowerShell**: A set of cmdlets for managing Azure resources through PowerShell.
- **REST APIs**: Programmatic access to Azure services for automation and integration.

These points cover the essential aspects of Azure resources and subscriptions[1][2]. If you need more detailed information on any specific area, feel free to ask!

Source: Conversation with Copilot, 21/08/2024 (1) Azure fundamental concepts - Cloud Adoption Framework. https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/considerations/fundamental-concepts. (2) Organize your Azure resources effectively - Cloud Adoption Framework .... https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/organize-resources. (3) Azure Architecture Fundamentals: Overview of Azure subscriptions .... https://dev.to/theyasirr/azure-architecture-fundamentals-overview-of-azure-subscriptions-management-groups-and-resources-1ko. (4) Azure Resources and Fundamentals | Nerdio. https://getnerdio.com/resources/microsoft-azure-fundamentals/.

In Microsoft Entra ID, there are several types of groups that you can use to manage access and collaboration. Here are the main types:

1. Security Groups

- **Purpose**: Used to manage user and computer access to shared resources.
- **Members**: Can include users, devices, service principals, and other groups (nested groups).
- **Usage**: Assign permissions to resources like SharePoint sites, Azure resources, and applications.

2. Microsoft 365 Groups

- **Purpose**: Provides collaboration opportunities by giving group members access to a shared mailbox, calendar, files, SharePoint sites, and more.
- **Members**: Can include only users.
- **Usage**: Ideal for team collaboration, project management, and communication.

3. Distribution Groups

- **Purpose**: Used for sending email notifications to a group of people.
- **Members**: Can include only users.
- **Usage**: Commonly used for email distribution lists.

4. Mail-Enabled Security Groups

- **Purpose**: Combines the features of security groups and distribution groups.
- **Members**: Can include users, devices, service principals, and other groups.
- **Usage**: Used for both managing access to resources and sending email notifications.

5. Dynamic Groups

- **Purpose**: Automatically add and remove members based on defined rules and attributes.
- **Members**: Membership is determined by rules based on user attributes (e.g., department, location).
- **Usage**: Useful for scenarios where group membership needs to be automatically updated based on user properties.

These groups help streamline the management of access and collaboration within an organization[1][2][3]. If you need more detailed information on any specific type, feel free to ask!

Source: Conversation with Copilot, 21/08/2024 (1) Learn about groups and group membership - Microsoft Entra. https://learn.microsoft.com/en-us/entra/fundamentals/concept-learn-about-groups. (2) Users, groups, licensing, and roles in Microsoft Entra ID - Microsoft .... https://learn.microsoft.com/en-us/entra/identity/users/directory-overview-user-model. (3) Understanding users and groups in Microsoft Entra ID (formerly Azure .... https://help.uis.cam.ac.uk/service/accounts-passwords/it-staff/university-central-directory/understanding-users-and-groups. (4) Account - Group Management. https://documentation.sailpoint.com/connectors/microsoft/entra_id/help/integrating_entra_id/account_group_management.html. (5) Synchronize nested AD groups in Entra ID - FirstWare DynamicGroup. https://www.dynamicgroup.net/en/news/synchronize-nested-ad-groups-in-entra-id/.

Managing built-in Azure roles involves understanding the predefined roles provided by Azure and how to assign them to users, groups, or service principals. Here are the main points:

1. Understanding Built-in Roles

- **Owner**: Full access to all resources, including the ability to delegate access to others.
- **Contributor**: Can create and manage all types of Azure resources but cannot grant access to others.
- **Reader**: Can view existing Azure resources but cannot make any changes.
- **User Access Administrator**: Can manage user access to Azure resources.

2. Assigning Roles

- **Azure Portal**:
  - Navigate to the resource, resource group, or subscription.
  - Go to **Access control (IAM)**.
  - Click **Add role assignment**.
  - Select the role and assign it to a user, group, or service principal.
- **Azure CLI**:

  ```
  az role assignment create --assignee <userPrincipalName> --role <roleName> --scope <scope>
  ```

- **Azure PowerShell**:

  ```
  New-AzRoleAssignment -ObjectId <userObjectId> -RoleDefinitionName <roleName> -Scope <scope>
  ```

3. Managing Role Assignments

- **View Role Assignments**:
  - In the Azure portal, navigate to **Access control (IAM)** and select the **Role assignments** tab.
  - Use `Get-AzRoleAssignment` in PowerShell or `az role assignment list` in Azure CLI.
- **Remove Role Assignments**:
  - In the Azure portal, navigate to **Access control (IAM)**, find the role assignment, and click **Remove**.
  - Use `Remove-AzRoleAssignment` in PowerShell or `az role assignment delete` in Azure CLI.

4. Best Practices

- **Least Privilege Principle**: Assign the minimum permissions necessary for users to perform their tasks.
- **Regular Reviews**: Periodically review role assignments to ensure they are still appropriate.
- **Use Custom Roles**: If built-in roles do not meet your needs, create custom roles with specific permissions.

These steps should help you effectively manage built-in Azure roles[4,5]. If you need more detailed information on any specific area, feel free to ask!

Source: Conversation with Copilot, 21/08/2024 (1) Azure built-in roles for General - Azure RBAC | Microsoft Learn. https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles/general. (2) Assign Azure roles using the Azure portal - Azure RBAC. https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal. (3) Azure Role-based Access Control (RBAC). https://www.youtube.com/watch?v=aJJjtKo-7hg. (4) 14 Azure AD Roles and Permissions. https://www.youtube.com/watch?v=qllLsvPPcbI. (5) Azure RBAC - Built in roles and Custom Roles. https://www.youtube.com/watch?v=z5nfltkZfrY. (6) azure-docs/articles/role-based-access-control/built-in-roles ... - GitHub. https://github.com/MicrosoftDocs/azure-docs/blob/main/articles/role-based-access-control/built-in-roles.md?toc=%2Fazure%2Fvirtual-network%2Ftoc.json. (7) Delegate Azure role assignment management using conditions. https://techcommunity.microsoft.com/t5/microsoft-entra-blog/delegate-azure-role-assignment-management-using-conditions/ba-p/3954216.