DSCI-519, Assignment-3
Rishit Saiya (rsaiya@usc.edu)

Q1:

[Assumption: The company datasets CD_U, CD_V, CD_X, CD_Y are assumed as CDU, CDV, CDX, CDY respectively for this problem. The generic permissions such as read and write are used as 'r' and 'w' respectively. Notation explanation - Alice: CDX - r means that Alice can only read CDX.]

Based on the above parameters we can create the following Chinese wall policies.

Alice & Bob – Both read and write accesses need to be provided together to any CD.

Alice: CDX - r/w & Bob: CDX - r/w
Alice: CDY - r/w & Bob: CDY - r/w
Alice: CDU - r/w & Bob: CDU - r/w
Alice: CDV - r/w & Bob: CDV - r/w

Alice & Bob - Only Read access

Alice: CDX - r & Bob: CDX - r
Alice: CDY - r & Bob: CDX - r
Alice: CDU - r & Bob: CDX - r
Alice: CDV - r & Bob: CDX - r
Alice: CDX, CDU - r & Bob: CDX, CDU - r
Alice: CDX, CDV - r & Bob: CDX, CDU - r
Alice: CDY, CDU - r & Bob: CDX, CDU - r
Alice: CDY, CDV - r & Bob: CDX, CDU - r

Alice & Bob – Both read/write required for CDX, and CDV, and read-only to remaining CDs

Alice: CDX - r/w & Bob: CDV - r/w [Can't read any other CDs]
Alice: CDV - r/w & Bob: CDX - r/w [Can't read any other CDs]
Alice: CDX - r/w & Bob: CDX - r/w [Both can neither read/write CDV, or read other CDs]
Alice: CDV - r/w & Bob: CDV - r/w [Both can neither read/write CDX, or read other CDs]
Alice: CDX - r/w & Bob: CDY or CDU or CDY, CDU - r
Alice: CDV - r/w & Bob: CDY or CDU or CDY, CDU - r
Alice: CDY or CDU or CDY, CDU - r & Bob: CDX - r/w
Alice: CDY or CDU or CDY, CDU - r & Bob: CDV - r/w

However this problem can be viewed in a different approach as well. The following perceive it with following assumptions and notations:

[Assumption: If any of the cells in the tables contain values in curly braces, they denote a set i.e. only one value can be picked from them at a given time. We are assuming the primal time Alice and Bob have access to Company Databases. At the start of time, there were no prohibited Company Databases. So the scenarios shown below consider that Alice/Bob have access to the Allowed CDs. The Prohibited CDs denote the Company Database don't have access to when they are accessing the CDs given in the Allowed CDs basket. Without the loss of generality it is clear that users given which are: Alice, Bob cannot access objects of different Company Databases in the same Conflict of Interest set.]

The conflicts of interest given here are: COI1 = {X, Y}; COI2 = {U, V}

CASE-1: Both Read/Write required for CDV, CDX and read-only to remaining Company Databases

In this case, it is considered that when Alice/Bob have read/write access to CDX, they have read access to CDV and CDU. But since the problem statement states that read and write access is required for CDV, therefore, it is better to assume that the read only access case for CDV is not to be considered. Alice and Bob can fall under any of the scenarios listed below (both of them can have the same or different scenarios).

Scenarios	Prohibited CDs	Allowed CDs
Scenario 1	CDU, CDY	Read Access to CDU. Read/write to CDX.
Scenario 2	CDV	Read Access to CDU, {Read/Write Access to CDX, Read Access to CDY}
Scenario 3	CDU, CDX	Read/Write Access to CDV. Read Access to CDY
Scenario 4	CDX	Read Access to CDY, {Read Access to CDU, Read/Write Access to CDV}

The additional read access after Alice and Bob's request to CDs will be to one of the CDs mentioned, the additional assignments are:

Scenarios	Prohibited CDs	Allowed CDs
Scenario 5	CDX, CDV	Read Access to CDU, Read Access to CDY
Scenario 6	CDV, CDY	Read Access to CDU, Read/Write Access to CDX
Scenario 7	CDU, CDX	Read Access to CDY, Read/Write Access to CDV
Scenario 8	CDV, CDX	Read Access to CDY, Read Access to CDU

CASE-2: Only Read Accesses need to be provided to Company Databases
Alice/Bob can fall under any scenario listed in the below 2 tables (both of them can have same or different scenarios). The first table is for when Alice/Bob requests read access to only one of the CDs. The second table is applicable when Alice/Bob requests read access to another CD.

Scenarios	Prohibited CDs	Allowed CDs (Only Read Access)
Scenario 1	CDY	CDX, {CDU, CDV}
Scenario 2	CDU	CDV, {CDX, CDY}
Scenario 3	CDX	CDY, {CDU, CDV}
Scenario 4	CDV	CDU, {CDX, CDY}

The additional read access after Alice and Bob's request to CDs will be to one of the CDs mentioned, the additional assignments are:

Scenarios	Prohibited CDs	Allowed CDs
Scenario 5	CDV, CDY	CDU, CDX
Scenario 6	CDU, CDX	CDV, CDY
Scenario 7	CDV, CDX	CDU, CDY
Scenario 8	CDU, CDY	CDV, CDX

CASE-3: Both Read, Write Accesses need to be provided together to any Company Database.

Since Read, Write Access is to be provided at the same time, it is safe to assume that read-only access will not be shown which is allowed by the Chinese wall when Alice/Bob has Read/Write Access to a given CD. Alice and Bob can fall under any of the scenarios listed below (both of them can have the same or different scenarios).

Scenarios	Prohibited CDs	Allowed CDs
Scenario 1	CDU, CDV, CDY	Read and Write Access to CDX
Scenario 2	CDU, CDX, CDY	Read and Write Access to CDY

Scenario 3	CDV, CDX, CDY	Read and Write Access to CDU
Scenario 4	CDU, CDX, CDY	Read and Write Access to CDV

Q2:

TASK-1:

[Assumption: As per discussion in the class, 3 objects and subjects are defined for MAC policies. The notation for General Hospital Information, Patient Information and Internal Hospital Information is GHI, PI, IHI respectively. They are assumed as objects and categories too. The Hospital staff subject includes the day-to-day operations such as Administration, Cash Flow, Supply Inventory and so on. The point to be noted here is that Hospital Staff is not being included in any medical technical tasks/operations. The clearances are used of general convention such as TS, S, U which are Top Secret, Secret and Unclassified respectively. The general hierarchy of clearances are TS, S, U in that descending order itself.]

The objects with their corresponding classification are defined as follows:

Objects	Classification
General Hospital Information	U
Internal Hospital Information	S
Patient Information	TS

The subjects along with their max and current clearances are defined as follows:

Subjects	Max Clearance	Current Clearance
Doctors	TS	TS
Hospital Staff	S	U
Nurses	TS	TS

The MAC policy are defined as follows:

1. The Hospital staff has Read/Write Access over the GHI, and Read/Write Access over the IHI based upon the requirement of clearance upgrades.
2. The Doctors have Read/Write Access over the PI. Additionally they have Read Access over the IHI, GHI.
3. The Nurses have Read/Write Access over the PI. Additionally, they have Read Access over the GHI, IHI.

The Categories included here are: GHI, IHI, PI

The label assignment to subjects and objects is as follows:

Doctors: (TS, {GHI, IHI, PI})
Nurses: (TS, {GHI, IHI, PI})
Hospital Staff: (U, {GHI}) | Hospital Staff's upgraded access label: (S, {GHI, IHI, PI})
GHI: (U, {GHI})
IHI: (S, {IHI})
PI: (TS, {PI})

The MAC Access labels assignment is as follows:
1. (TS, {GHI, IHI, PI})
2. (TS, {PI})

3. (S, {GHI, IHI})
4. (S, {IHI})
5. (U, {GHI})

The Dominance Relationships in accordance to the above mentioned MAC Labels (numbering) is as follows:
1 dom 2 | 1 dom 3 | 1 dom 4 | 1 dom 5
3 dom 4 | 3 dom 5

TASK-2 (a):

The protected objects are as follows:

Object Name	Description
Trusted Device	A trusted device that segregates logs into normal and abnormal logs
Trusted Data Storage	Storage facility of all logs
Normal Logs	The log files of patient's vital signs wherein all parameters are within normal range
Abnormal Logs	The log files of patient's vital signs wherein all parameters aren't within normal range
Emergency Logs	The combined logs of normal and abnormal logs that showcase an emergent situation which emergency responders need to address immediately

The operations on protected objects are as follows: (Administrative: A, Non-Administrative: NA)

Operation Name	A/NA	Description
Read	NA	Read all three log types for authorized healthcare professionals (physicians, doctors, nurses) and emergency log red access for emergency responders
Write	NA	All Authorized healthcare professionals can create and write emergency logs
Read	A	The trusted device reads logs files sent by sensors and classify them
Write	A	The trusted device creates normal and abnormal logs files (base on the logs sent by sensors) and stores them in trusted storage
Modify Permissions	A	The sysadmins can modify object permissions, especially to revoke emergency responders' access to emergency logs after the emergency is resolved

The permissions assignment here is as follows:
Normal Logs -
- Operation: Read - Read Normal Logs
- Operation: Write - Write/Create Normal logs

Abnormal Logs -
- Operation: Read - Read Abnormal Logs
- Operation: Write - Write/Create Abnormal logs

Emergency Logs -
- Operation: Read - Read Emergency Logs
- Operation: Write - Write/Create Emergency logs
- Operation: Modify Permissions - Delegate access permissions of emergency logs

Trusted Data Storage -
- Operation: Read - Read Logs stored in trusted data storage
- Operation: Write - Write/Store logs in trusted data storage

The Roles taken here are: Emergency Responder, Physician, Nurse, Trusted Device, Sysadmin

The role to permission assignments is as follows:

Role: Emergency Responder
Object Name - Emergency Log | Operation: r

Role: Nurse
Object Name - Normal Log | Operation: r
Object Name - Abnormal Log | Operation: r
Object Name - Emergency Log | Operation: r, w
Object Name - Trusted Data Storage | Operation: r, w

Role: Physician
Object Name - Normal Log | Operation: r
Object Name - Abnormal Log | Operation: r
Object Name - Emergency Log | Operation: r, w
Object Name - Trusted Data Storage | Operation: r, w

Role: Sysadmin
Object Name - Emergency Logs | Operation: modify permissions

Role: Trusted Device
Object Name - Trusted Data Storage | Operation: w

The constraints are as follows:

Role: Emergency Responder
Constraint - The role is allowed to access emergency logs only during critical situations

Role: Physician
Constraint - The role can read logs only of their respective patients. Additionally they are allowed to access normal, abnormal and emergency logs anytime.

Role: Nurse
Constraints: The role can read logs only of their respective patients. Additionally they are allowed to access normal, abnormal and emergency logs only during working hours.

TASK-2 (b):

Subject Attributes: Physicians, Nurses, Emergency Responders would be part of the Authorized Healthcare Professional Department whereas Sysadmin, Trusted Device would be part of the IT Department. Subjects can be associated with such department labels to differentiate.
Resource Attributes: Logs are of Normal, Abnormal and Emergency types.
Action Attributes: The access of resources might be on different levels such as read and write access rights.
Environment Attributes: The environment dependencies here as the access rights on time slots which further implies that during and after hours times are important to consider as there might be different permissions of access rights.

The ABAC policies in regards with Authorized Healthcare Professional Department is as follows:

Physicians: Trusted Storage - r, w
Physicians: Normal Logs Access of only their patients' record (during, after working hours) - r
Physicians: Abnormal Logs Access of only their patients' record (during, after working hours) - r
Physicians: Emergency Logs Access of only their patients' record (during, after working hours) - r, w

Nurses: Trusted Storage - r, w
Nurses: Normal Logs Access of only their patients' record (during working hours) - r
Nurses: Abnormal Logs Access of only their patients' record (during working hours) - r
Nurses: Emergency Logs Access of only their patients' record (during working hours) - r, w
Nurses: Normal Logs Access of only their patients' record (after working hours) - No r, w
Nurses: Abnormal Logs Access of only their patients' record (after working hours) - No r, w
Nurses: Emergency Logs Access of only their patients' record (after working hours) - No r, w

Emergency Responders: Emergency Logs Access of all patients' records (duration of patient's emergency) - r, w

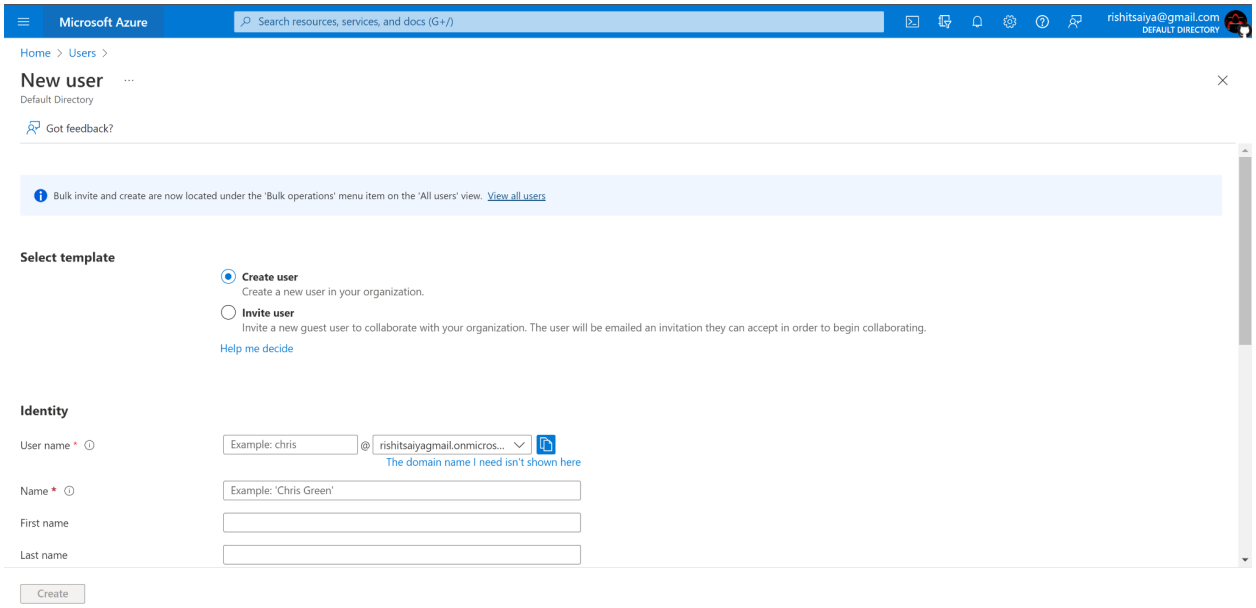
The ABAC policies in regards with IT Department is as follows:

Sysadmin: Trusted Storage - No r, w
Sysadmin: Normal Logs - No r, w
Sysadmin: Abnormal Logs - No r, w
Sysadmin: Emergency Logs - No r, w

Trusted Device: Trusted Storage - w
Trusted Device: Normal Logs - w
Trusted Device: Abnormal Logs - w

TASK-3:

The relevant screenshots are as follows:



Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home >

Users

Search

All users (preview)
Audit logs
Sign-in logs
Diagnose and solve problems

Manage

Deleted users (preview)
Password reset
User settings
Bulk operation results

Troubleshooting + Support

New support request

New user | Download users | Bulk operations | Refresh | Manage view | Delete | Per-user MFA | Preview features | Got feedback?

Want to switch back to the legacy users list experience? Click here to leave the preview.

Search | Add filter

6 users found

Display name ↑	User principal name	User type	Job title	Identities	Company name	Creation ty
Abhishek	Abhishek@rishitsaiyagma...	Member	Emergency Responder	rishitsaiyagmail.onmicrosoft.com		
Harsh	Harsh@rishitsaiyagmail.o...	Member	Nurse	rishitsaiyagmail.onmicrosoft.com		
Kevin	Kevin@rishitsaiyagmail.on...	Member		rishitsaiyagmail.onmicrosoft.com		
Manjeet	Manjeet@rishitsaiyagmail...	Member	Physician	rishitsaiyagmail.onmicrosoft.com		
Rishit Saiya	rishitsaiya_gmail.com#EX...	Member		MicrosoftAccount		
Vipul	Vipul@rishitsaiyagmail.on...	Member	Sysadmin	rishitsaiyagmail.onmicrosoft.com		

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home >

Groups | All groups

Default Directory - Azure Active Directory

All groups
Deleted groups
Diagnose and solve problems

Settings

General
Expiration
Naming policy

Activity

Privileged access groups (Preview)
Access reviews
Audit logs
Bulk operation results

Troubleshooting + Support

New support request

New group | Download groups | Refresh | Manage view | Delete | Got feedback?

Search | Add filter

Search mode: Contains

5 groups found

Name ↑	Object Id	Group type	Membership type	Email
EmergencyResponder	ac719e12-0d32-43ac-b7c2-0223918885d5	Security	Assigned	
Nurse	f07770b2-c120-4b70-8754-440115265f78	Security	Assigned	
Physician	b0717849-a406-481a-8930-f250cbba38bd	Security	Assigned	
Sysadmin	9eab7bbf-f6f4-4735-ba0c-d26a2bede38d	Security	Assigned	
Trusted Device	2f2dc2fb-e366-4cd8-ae99-6c168a84a074	Security	Assigned	

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Groups | All groups > EmergencyResponder

EmergencyResponder | Members

Group

Overview
Diagnose and solve problems

Manage

Properties
Members
Owners
Roles and administrators

Add members | Remove | Refresh | Bulk operations | Columns | Got feedback?

Direct members | All members

Search by name | Add filters

Name	Type	Email	User type
Abhishek	User		Member

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Groups | All groups > Nurse

Nurse | Members

Group

Overview
Diagnose and solve problems

Manage

Properties
Members
Owners
Roles and administrators

Add members | Remove | Refresh | Bulk operations | Columns | Got feedback?

Direct members | All members

Search by name | Add filters

Name	Type	Email	User type
Harsh	User		Member

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Groups | All groups > Physician

Physician | Members

Group

Overview
Diagnose and solve problems

Manage
Properties
Members
Owners
Roles and administrators

Add members | Remove | Refresh | Bulk operations | Columns | Got feedback?

Direct members | All members

Search by name | Add filters

Name	Type	Email	User type
MA Manjeet	User		Member

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Groups | All groups > Sysadmin

Sysadmin | Members

Group

Overview
Diagnose and solve problems

Manage
Properties
Members
Owners
Roles and administrators

Add members | Remove | Refresh | Bulk operations | Columns | Got feedback?

Direct members | All members

Search by name | Add filters

Name	Type	Email	User type
VI Vipul	User		Member

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Groups | All groups > Trusted Device

Trusted Device | Members

Group

Overview
Diagnose and solve problems

Manage
Properties
Members
Owners
Roles and administrators

Add members | Remove | Refresh | Bulk operations | Columns | Got feedback?

Direct members | All members

Search by name | Add filters

Name	Type	Email	User type
KE Kevin	User		Member

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home >

Resource groups

Default Directory (rishitsaiyagmail.onmicrosoft.com)

Create | Manage view | Refresh | Export to CSV | Open query | Assign tags

Filter for any field... | Subscription equals all | Location equals all | Add filter

0 Unsecure resources | 0 Recommendations

No grouping | List view

Name	Subscription	Location
Trusted_Storage	Azure for Students	East US

< Previous | Page 1 of 1 | Next > | Showing 1 to 1 of 1 records.

Give feedback

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home >

Resource groups

Default Directory (rishitsaiyagmail.onmicrosoft.com)

Create | Manage view | Refresh | Export to CSV | Open query | Assign tags

Filter for any field... | Subscription equals all | Location equals all | Add filter

0 Unsecure resources | 0 Recommendations

Name	Subscription
Trusted_Storage	Azure for Students

< Previous | Page 1 of 1 | Next > | Showing 1 to 1 of 1 records.

Notifications

More events in the activity log → | Dismiss all

Resource group created

Creating resource group 'Trusted_Storage' in subscription 'Azure for Students' succeeded.

Go to resource group | Pin to dashboard

a few seconds ago

Successfully created user

Successfully created user Doctor.

5 minutes ago

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Resource groups > Trusted_Storage | Access control (IAM) >

Create a custom role

Got feedback?

Basics | Permissions | Assignable scopes | JSON | Review + create

+ Add assignable scopes

Click Add assignable scopes to select the scopes (management groups, subscriptions, or resource groups) where this role will be available for assignment.
Your role must have at least one assignable scope. Learn more

Assignable scope	Type
/subscriptions/54deb354-8dbd-4f80-b3fb-3d080e18bf6b/resourceGroups/Trusted_Storage	Resource group

Review + create | Previous | Next

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Resource groups > Trusted_Storage | Access control (IAM) >

Create a custom role

Got feedback?

Basics | Permissions | Assignable scopes | JSON | Review + create

Here is your custom role in JSON format. Learn more

Download | Edit

```
{
    "properties": {
        "roleName": "Write Only",
        "description": "",
        "assignableScopes": [
            "/subscriptions/54deb354-8dbd-4f80-b3fb-3d080e18bf6b/resourceGroups/Trusted_Storage"
        ],
        "permissions": [
            {
                "actions": [
                    "Microsoft.Storage/storageAccounts/blobServices/containers/delete"
                ],
                "notActions": [],
                "dataActions": [
                    "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action"
                ],
                "notDataActions": []
```

Using JSON

Add permissions
Specify an operation as an Action, NotAction, DataAction, or NotDataAction. Permission strings use the format {Company}.{ProviderName}/{resourceType}/{action}.

Add wildcards (*)
Add wildcards (*) to a permission string to include all permissions that match the string. For example, if you specify Microsoft.Compute/* as an Action, your role can perform all management operations in Microsoft.Compute.

Add assignable scopes
Management group scope has the format /providers/Microsoft.Management/managementGroups/{managemer
Subscription scope has the format /subscriptions/{subscriptionId}. Resource group scope has the format /subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName

Review + create | Previous | Next

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Resource groups > Trusted_Storage | Access control (IAM) >

Add role assignment

Got feedback?

Role | Members | Conditions (optional) | Review + assign

Selected role Write Only

Assign access to User, group, or service principal / Managed identity

Members + Select members

Name	Object ID	Type
Trusted Device	2f2dc2fb-e366-4cd8-ae99-6c168a84a074	Group

Description Optional

Review + assign | Previous | Next

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Resource groups > Trusted_Storage

Resource groups

Default Directory (rishitsaiyagmail.onmicrosoft.com)

+ Create | Manage view

Filter for any field...

Name

Trusted_Storage

Trusted_Storage | Access control (IAM)

Resource group

Search

Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events

Settings
Deployments
Security
Policies
Properties
Locks

+ Add | Download role assignments | Edit columns | Refresh | Remove | Got feedback?

Check access | Role assignments | Roles | Deny assignments | Classic administrators

Number of role assignments for this subscription

1 4000

Search by name or email | Type : All | Role : All | Scope : All scopes | Group by : Role

1 items (1 Groups)

Name	Type	Role	Scope	Condition
Write Only				
TD Trusted Device	Group	Write Only	This resource	Add

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Resource groups > Trusted_Storage | Access control (IAM) >

Create a custom role

Got feedback?

Basics | Permissions | Assignable scopes | JSON | Review + create

To create a custom role for Azure resources, fill out some basic information. Learn more

* Custom role name: Write Only

Description:

Baseline permissions: Clone a role | Start from scratch | Start from JSON

Role to clone: Storage Blob Data Contributor

Review + create | Previous | Next

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Resource groups > Trusted_Storage | Access control (IAM) >

Create a custom role

Got feedback?

Basics | Permissions | Assignable scopes | JSON | Review + create

+ Add permissions | + Exclude permissions

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. Learn more
To exclude specific permissions from a wildcard permission, click Exclude permissions. Learn more

Permission	Description	Permission type
Microsoft.Storage/storageAccounts/blobServices/co...	Returns the result of deleting a container	Action
Microsoft.Storage/storageAccounts/blobServices/co...	Returns the result of deleting a blob	DataAction
Microsoft.Storage/storageAccounts/blobServices/co...	Returns the result of writing a blob	DataAction
Microsoft.Storage/storageAccounts/blobServices/co...	Returns the result of adding blob content	DataAction

Definitions

Control plane
Actions specify the operations that a role is allowed to perform. NotActions specify the operations that are excluded from the allowed Actions (this is useful if a role has wildcards).

Data plane
DataActions specify the operations that a role is allowed to perform to the data within an object. NotDataActions specify the operations that are excluded from the allowed DataActions (this is useful if a role has wildcards).

Wildcards (*)
A wildcard (*) extends a permission to everything that matches the string you provide. To add a wildcard permission, use the JSON tab.

Review + create | Previous | Next

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home >

Storage accounts

Default Directory (rishitsaiyagmail.onmicrosoft.com)

Create | Restore | Manage view | Refresh | Export to CSV | Open query | Assign tags | Delete

Filter for any field... | Subscription equals **all** | Resource group equals **all** | Location equals **all** | Add filter

No grouping | List view

Name	Type	Kind	Resource group	Location	Subscription
abnormallog2	Storage account	StorageV2	Trusted_Storage	East US	Azure for Students
emergencylog2	Storage account	StorageV2	Trusted_Storage	East US	Azure for Students
normallog2	Storage account	StorageV2	Trusted_Storage	East US	Azure for Students

< Previous | Page 1 of 1 | Next > | Showing 1 to 3 of 3 records.

Give feedback

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Storage accounts > emergencylog2 | Access Control

Add role assignment condition

Editor type Visual Code

To use principal (user) attributes, you must have all of the following

Condition #1

1. Add action *

Click Add action to select the actions you want to allow if the

Add action | Delete

Action Type	Action

Select actions

2. Build expression

Build one or more expressions. If the expressions evaluate to t

Add expression | Delete | Group | Ung

Save | Discard

Select an action

Select the actions you want to allow if the condition is true. If you select multiple actions, there might be fewer attributes to choose from for your condition because the attributes must be available across the selected actions.

Action	Description
Storage Blob Service Blobs	
All read operations	All Blob read operations.
List blobs	List blobs operation.
Read a blob	All blob read operations excluding list.
Write to a blob	DataAction for writing to blobs.
Sets the access tier on a blob	REST operations: Set Blob Tier.
Write to a blob with blob index tags	REST operations: Put Blob, Put Block List, Copy Blob and Copy Blob From URL.
Create a blob or snapshot, or append data	DataAction for creating blobs.
Write to a blob with blob index tags	REST operations: Put Blob, Put Block List, Copy Blob and Copy Blob From URL.
Delete a blob	DataAction for deleting blobs.
Rename a file or a directory	DataAction for renaming files or directories.

Select | Discard

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Storage accounts > emergencylog2 | Access Control (IAM) >

Add role assignment

Got feedback?

Role | Members | Conditions (optional) | Review + assign

Add an optional check to your role assignment to provide more fine-grained access control. Learn more

Selected role Storage Blob Data Contributor

Role assignment conditions Edit condition | Remove condition

```
(
 (
  !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write'})
  AND
  !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'})
 )
)
```

Review + assign | Previous | Next

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Storage accounts > emergencylog2 | Access Control (IAM) >

Add role assignment

Got feedback?

Role | Members | Conditions (optional) | Review + assign

Role Storage Blob Data Contributor

Scope /subscriptions/54deb354-8dbd-4f80-b3fb-3d080e18bf6b/resourceGroups/Trusted_Storage/providers/Microsoft.Storage/storageAccounts/emergencylog2

Members

Name	Object ID	Type
Nurse	f07770b2-c120-4b70-8754-440115265f78	Group
Physician	b0717849-a406-481a-8930-f250cbba38bd	Group

Description No description

Condition

```
(
 (
  !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write'})
  AND
  !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'})
 )
)
```

Review + assign | Previous

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Storage accounts > emergencylog2 | Access Control

Add role assignment condition

To use principal (user) attributes, you must have all of the following

Condition #1

1. Add action *

Click Add action to select the actions you want to allow if the

Add action | Delete

Action Type	Action

Select actions

2. Build expression

Build one or more expressions. If the expressions evaluate to t

Add expression | Delete | Group | Ung

Add expression

Save | Discard

Select an action

Select the actions you want to allow if the condition is true. If you select multiple actions, there might be fewer attributes to choose from for your condition because the attributes must be available across the selected actions.

Action	Description
Storage Blob Service Blobs	
All read operations	All Blob read operations.
List blobs	List blobs operation.
Read a blob	All blob read operations excluding list.

Select | Discard

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Storage accounts > normallog2 | Access Control (IAM) >

Add role assignment

Got feedback?

Role | Members | Conditions (optional) | Review + assign

Selected role Storage Blob Data Reader

Assign access to User, group, or service principal / Managed identity

Members + Select members

Name	Object ID	Type
Physician	b0717849-a406-481a-8930-f250cbba38...	Group
Nurse	f07770b2-c120-4b70-8754-440115265f78	Group

Description Optional

Review + assign | Previous | Next

Microsoft Azure | Search resources, services, and docs (G+/) | rishitsaiya@gmail.com DEFAULT DIRECTORY (RISHITSAIY...

Home > Storage accounts > abnormallog2

Storage accounts

Default Directory (rishitsaiyagmail.onmicrosoft.com)

+ Create | Restore

Filter for any field...

Name

- abnormallog2
- emergencylog2
- normallog2

Page 1 of 1

abnormallog2 | Access Control (IAM)

Storage account

Search

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser

Data storage

- Containers
- File shares
- Queues
- Tables

Security + networking

- Networking
- Azure CDN

+ Add | Download role assignments | Edit columns | Refresh | Remove | Got feedback?

Check access | Role assignments | Roles | Deny assignments | Classic administrators

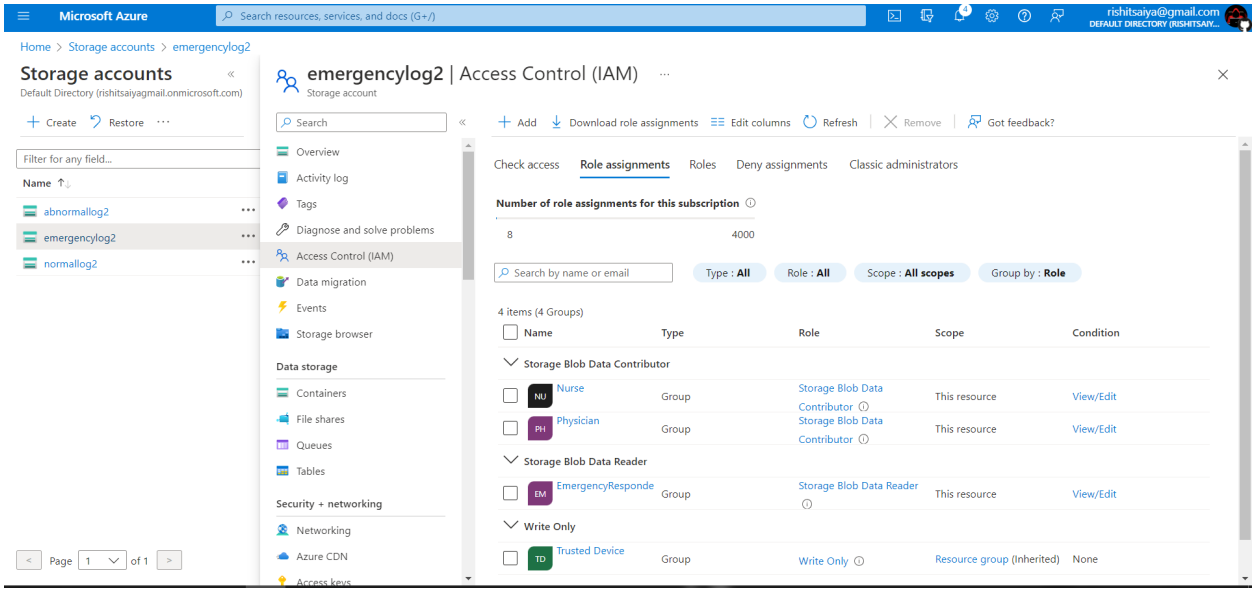
Number of role assignments for this subscription

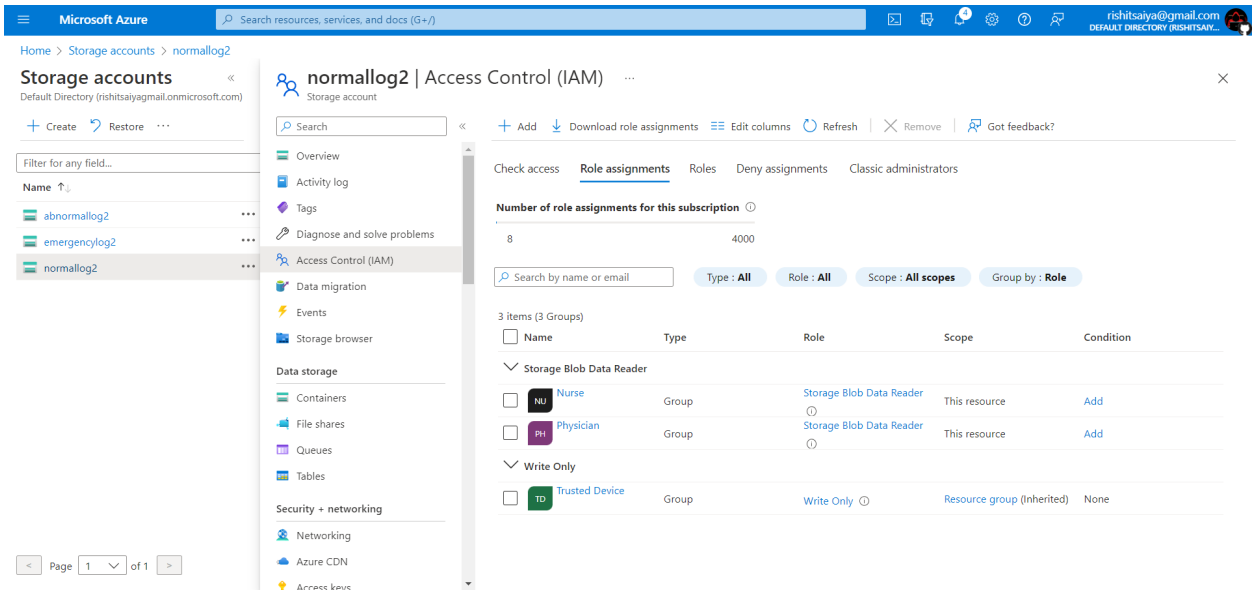
8 / 4000

Search by name or email | Type : All | Role : All | Scope : All scopes | Group by : Role

3 items (3 Groups)

Name	Type	Role	Scope	Condition
Storage Blob Data Reader				
NU Nurse	Group	Storage Blob Data Reader	This resource	Add
PH Physician	Group	Storage Blob Data Reader	This resource	Add
Write Only				
TD Trusted Device	Group	Write Only	Resource group (Inherited)	None





Q3-A:

The TCB subset is the notion that primarily concentrates on a single computer. It is one method used to address the composition issue using the Divide and Conquer strategy. According to this method, a policy subset is assigned to each TCB subset, and then it is verified that each TCB subset upholds the corresponding policy subset. Here, the system TCB is broken down into simpler components, each of which is independently checked. Following the enforcement of a single system policy by composed subsets, validated components are then correctly assembled. It makes use of the hierarchical domain structure for protection, where domains are arranged according to privilege. Each subset of the partial TCB is in its own execution domain. It enables a series of incremental evaluations that are simpler to follow. Finally, it is able to confirm that the composite TCB is accurate.

Q3-B:

TCB partition is a concept that primarily concentrates on a loosely linked network of computers. It has several parts, such as computers and networking hardware. Here, it's crucial to consider the network as a single integrated system. Different NTCB (Network Trust Computing Base) policies apply to various components. Every TCB partition carries out the assigned policy. Having secure communication connections is crucial. Information is shared through modalities like point-to-point communication due to topics on components. Subjects and objects for each TCB partition that implements a policy must be distinct from those of other TCBs in order to do so independently of other TCB partitions. The Subject is limited to just one network element in this configuration. The same network component's objects are accessed by subjects. Subjects or objects cannot be transferred from one component to another.

Q3-C:

The similarities between the two concepts of Divide and Conquer strategy are:
1. Each TCB subset complies with reference monitor specifications. In a similar vein, each element in the TCB partition satisfies the RM characteristics..
2. In order to solve a composition problem, both the concepts use the Divide and Conquer strategy.

The differences between the two concepts of Divide and Conquer strategy are:
1. The TCB partition has a different Formal Security Policy Model (FSPM) and the TCB subset has only a single FSPM.
2. The TCB partition does not follow the hierarchy but the TCB subset follows the hierarchy.
3. While TCB partition focuses on a loosely linked network of computers, TCB idea primarily focuses on a single computer.

Q4-A:

Hierarchical domains are used in TCB subsets in the order of privilege. To begin with, TCB subsets must be divided into smaller sections. A complex policy that also needs to be enforced is broken down into smaller policy components. Thereafter A TCB subset is assigned to each policy subset. Assume that TCB is partitioned into TCB subsets, each of which is in its own execution domain. Each TCB subset positioned in the hierarchically structured execution domain will be assigned to a policy subset (p1, p2, p3).
This configuration will now function with protective ring lines. These domains will be segregated, much like protective rings, and privileges will be distributed uniquely and specifically. The MAC policy p1 can be assigned to the lowest domain (such as Ring 0), p2 to the next domain (such as Ring 1), and p3 to the highest domain (such as Ring 2) (DAC). It makes it simple to maintain isolation or separation. Additional privileges can also be readily assigned and distributed. This is how these domains and protection rings are connected and how they are crucial to how the TCB subset works.

Q4-B:

A system made up of TCB subsets can be evaluated incrementally with the help of ordered domains very effectively. Assume that there are three distinct domains (d1, d2, d3). These domains are arranged hierarchically and in order of privilege. An individual execution domain will be assigned to each incomplete TCB subset. Depending on the kind of policy, every TCB subset will be considered before each access.
Only d2 (second TCB subset) will be contacted and consulted for access once a TCB subset has been consulted on d1. Only after it is finished will d3 be contacted for consulting. This approach will not permit any loopholes. If domains are not organized, incremental evaluation will face significant practical difficulties, and we will fall short of our goal because some checks may be disregarded or skipped. Ordered domains are making it possible for a series of incrementally easier evaluations.

Q4-C:

The TCB subset's incremental evaluation process will guarantee the non-bypassable property. Each TCB subset will be assessed according to the kind of policy that is assigned to it in a domain. If incremental evaluation hadn't been implemented, several checks could have been skipped. However, in this situation, incremental evaluation will prevent any checks or controls from being ignored because the next TCB subset can only be approached after the evaluation of one TCB subset has been completed. When a TCB subset is fully configured, isolation is also enforced by the execution domain (an ordered set of protection rings), which also enforces isolation and separation. These many rings/domains will be independent and distinct from one another. Verifiability is achievable at all levels in this full arrangement since this approach takes into account all TCB components and performs a step-by-step evaluation of TCB subset.