AZURE DAY

Che l'attributo sia con te!
ABAC, non solo ruoli in Azure!!

Massimo Bonanni @ Microsoft

Microsoft msc TECHNOLOGY NET CODE Azure Meetup TORINO TORINO.NET

AZURE DAY

Platinum Sponsor

Microsoft

msc TECHNOLOGY

Technical Sponsor

NET CODE

Azure Meetup TORINO

TORINO .NET

stickermule

Packt›

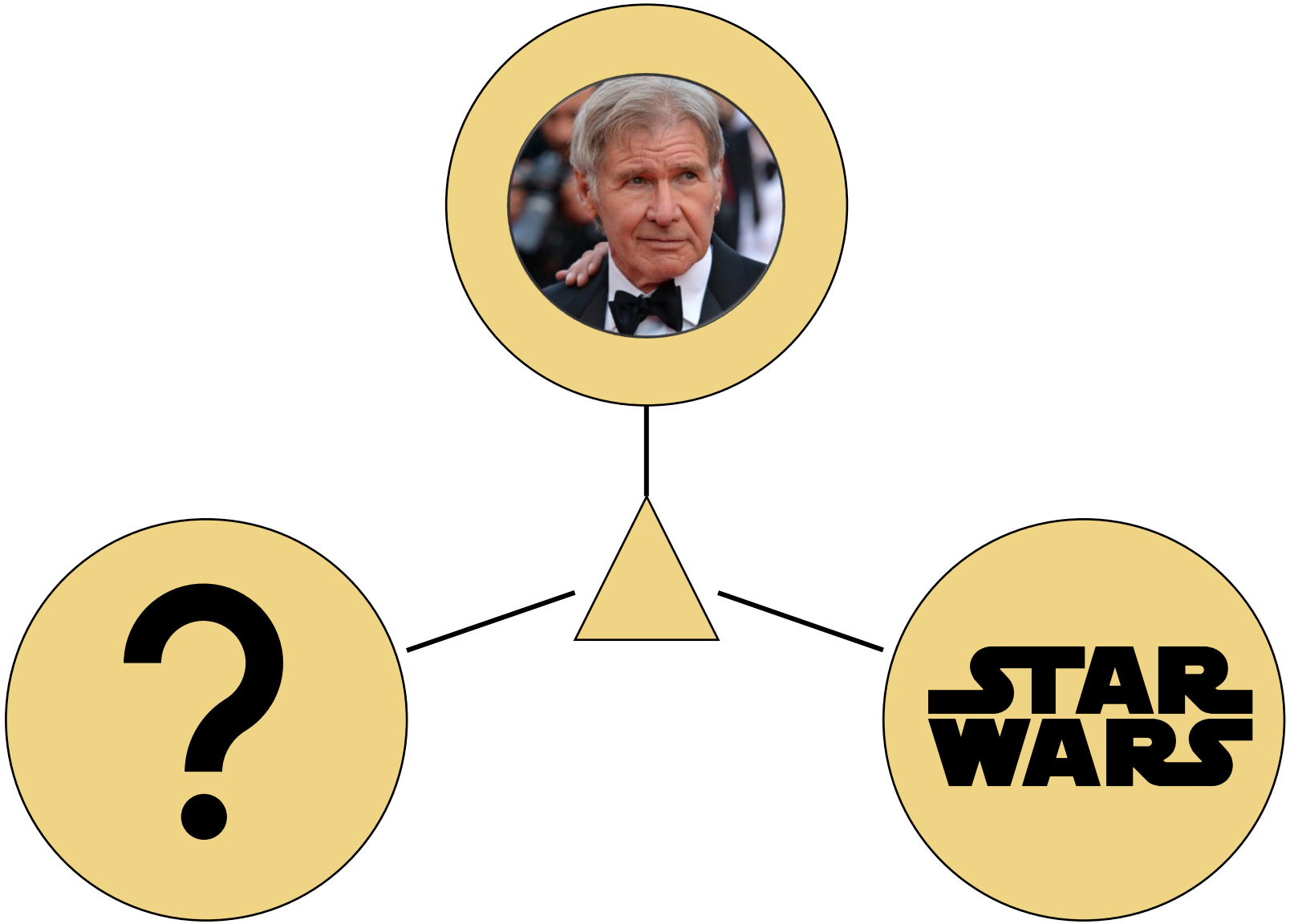
JET BRAINS

AZURE DAY

RBAC

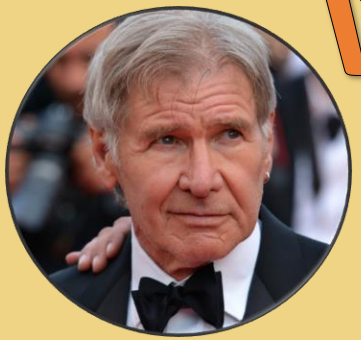
Role-Based Access Control grants or denies permissions to keep the cloud's Force balanced.

RBAC in Start Wars



RBAC in Start Wars

Who



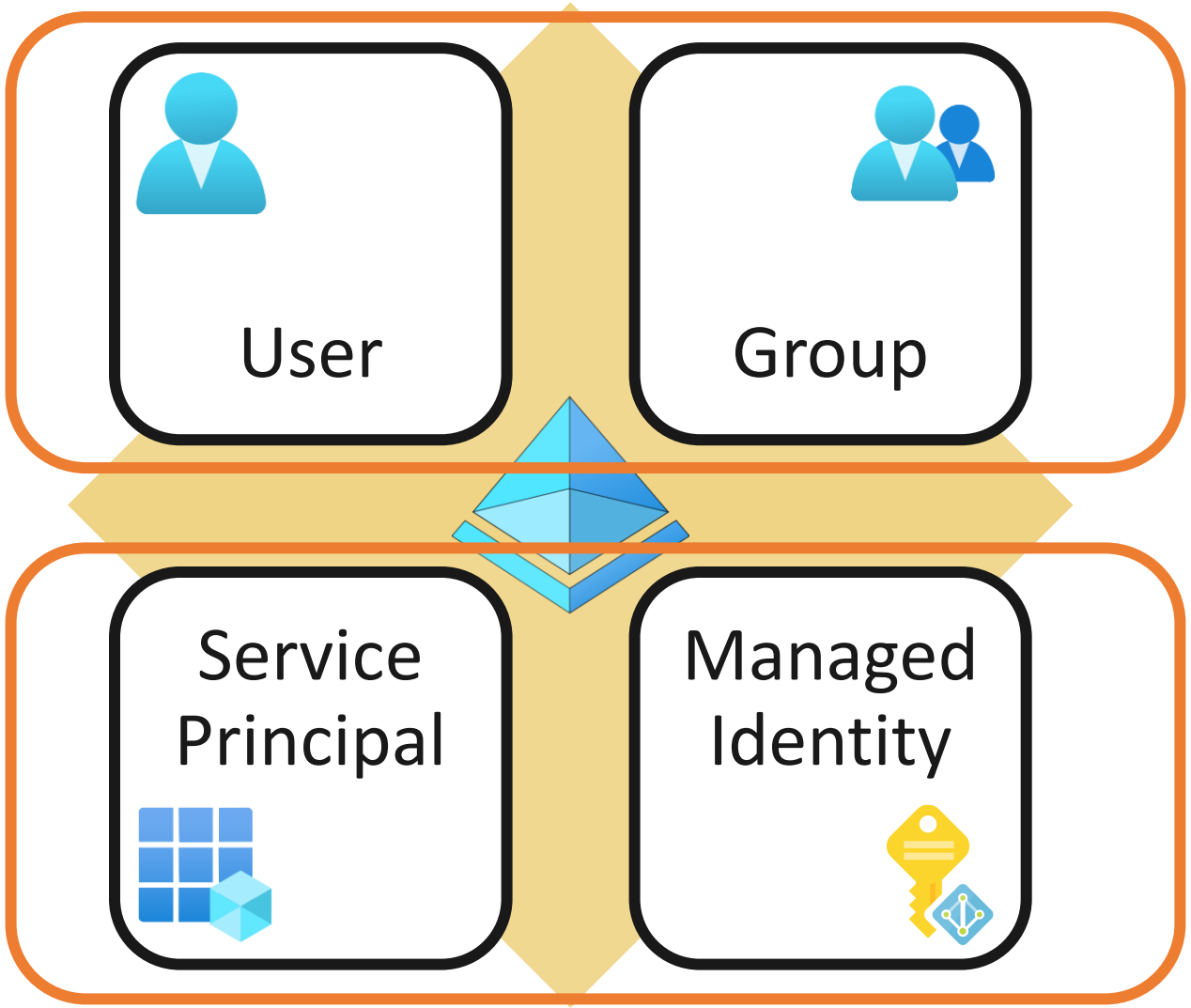
What

Where

STAR WARS

Azure **Role-Based Access Control (RBAC)** is an authorization system built on **Azure Resource Manager** that provides fine-grained access management of Azure resources.

Who – Security Principal



Interactive Identities

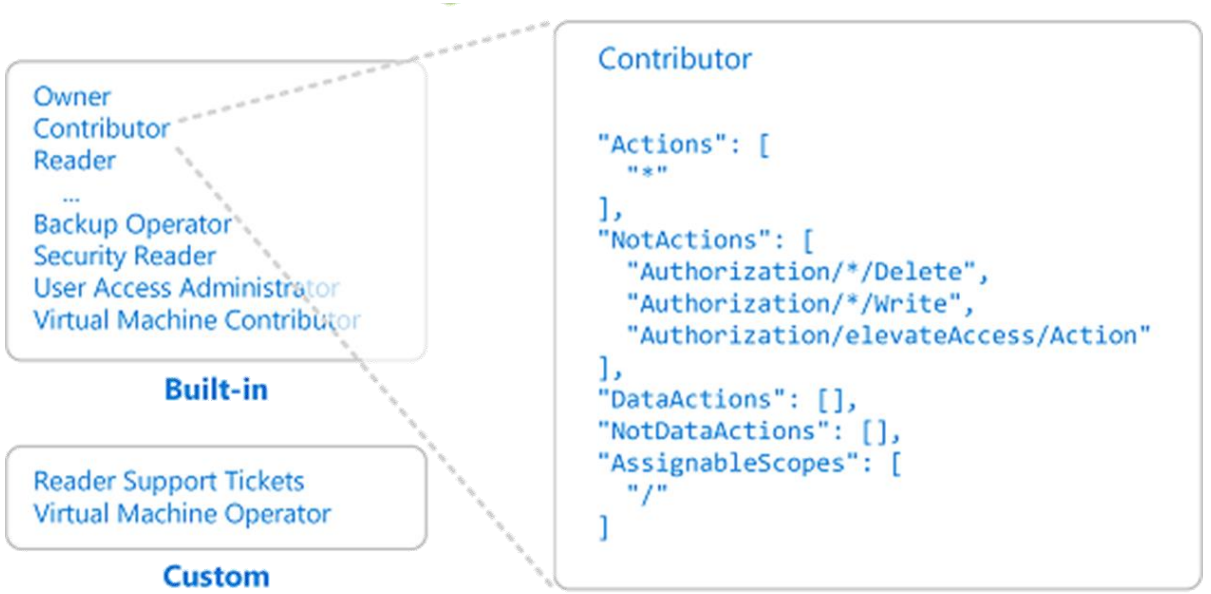
Applicative Identities

What – Role Definition

A role definition is a collection of permissions, a lists the **operations** that can be performed.

Roles can be high-level, like **owner**, or specific, like **virtual machine reader**.

Azure includes several **built-in roles** that you can use but you can create your **custom role**.

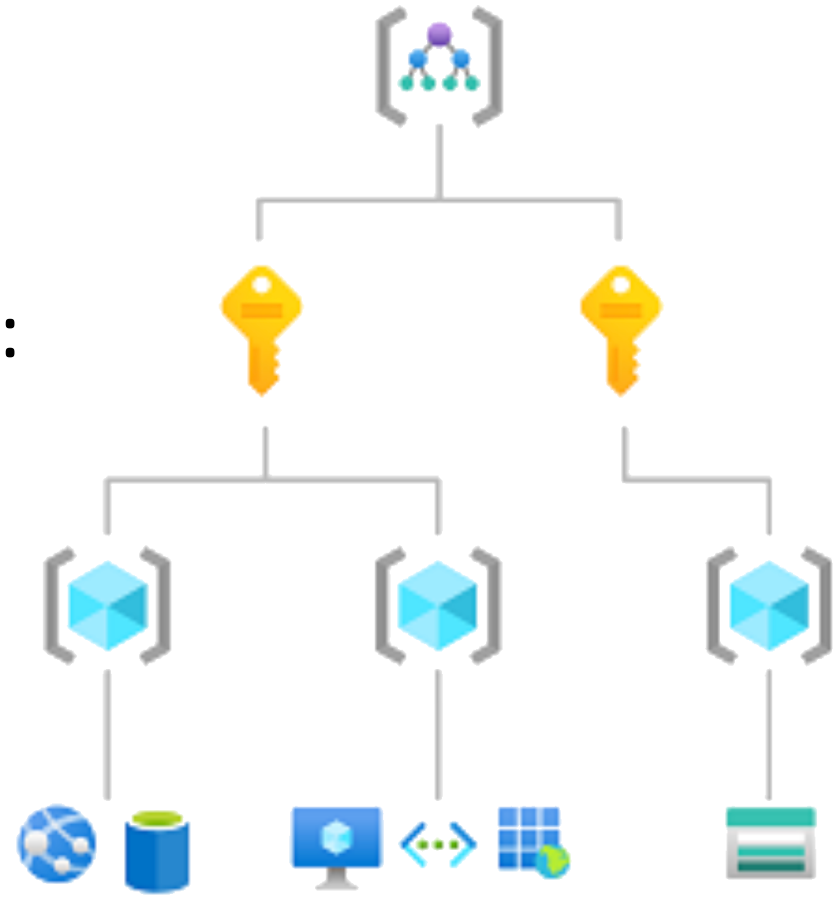


Where – Scope

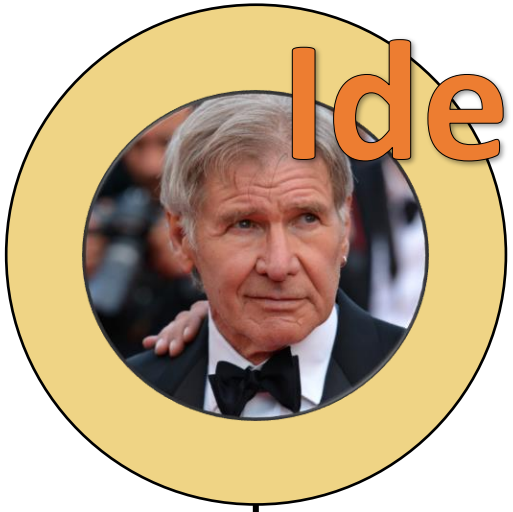
Scope is the set of resources that the access applies to.

You can specify a scope at multiple levels:

- ✓ Management group
- ✓ Subscription
- ✓ Resource Group
- ✓ Resource (sub-resource)



RBAC in Start Wars



Identity

Role

Scope

STAR WARS

AZURE DAY

- ✓ **John** has been hired to manage the administration of the company, but she can read only the invoices.
- ✓ **Invoices** are stored in a **Storage Account**.
- ✓ Within the same storage, in the same container, there are also **reports** and **receipts**.
- ✓ John will manage documents using **custom software** or through the **Storage Explorer**

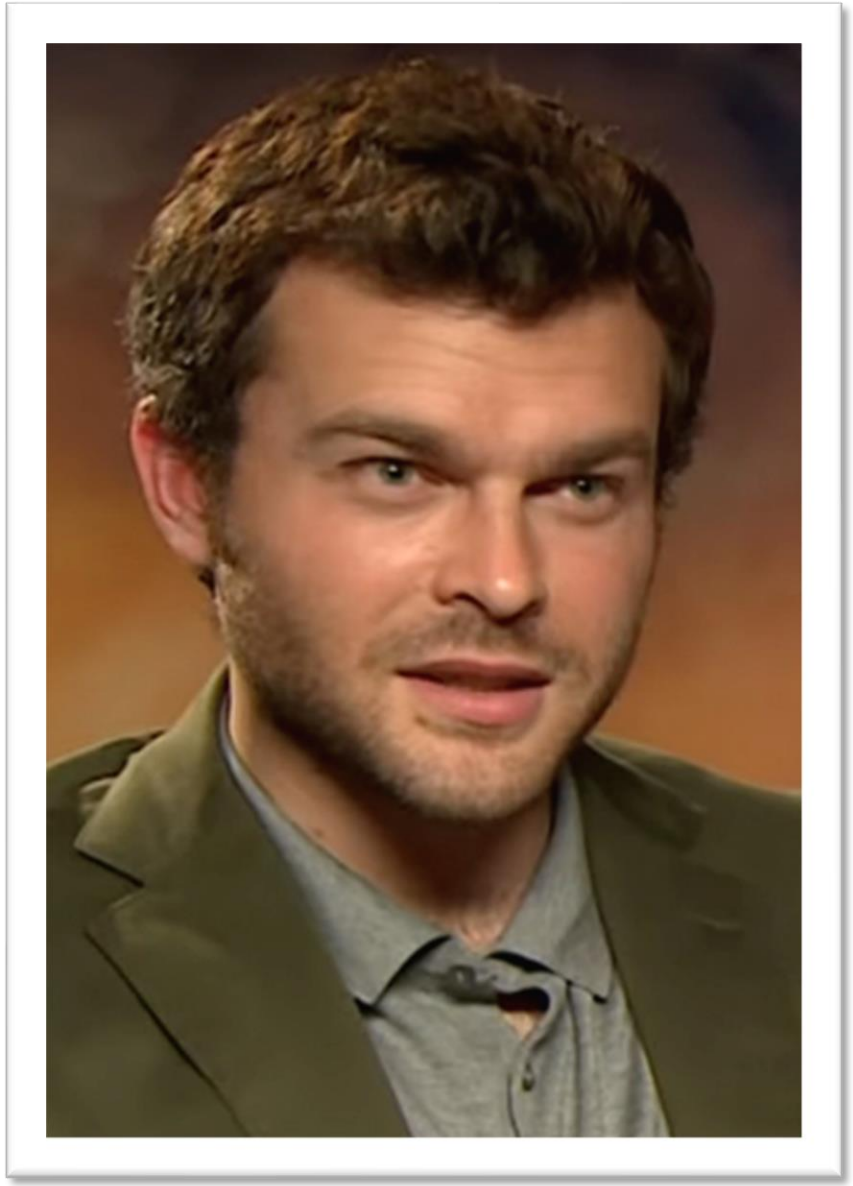
AZURE DAY

ABAC

Attribute-Based Access Control in Azure is like the Force-sensitive Jedi, unlocking data and resources based on unique attributes, not just rank or title.

AZURE DAY

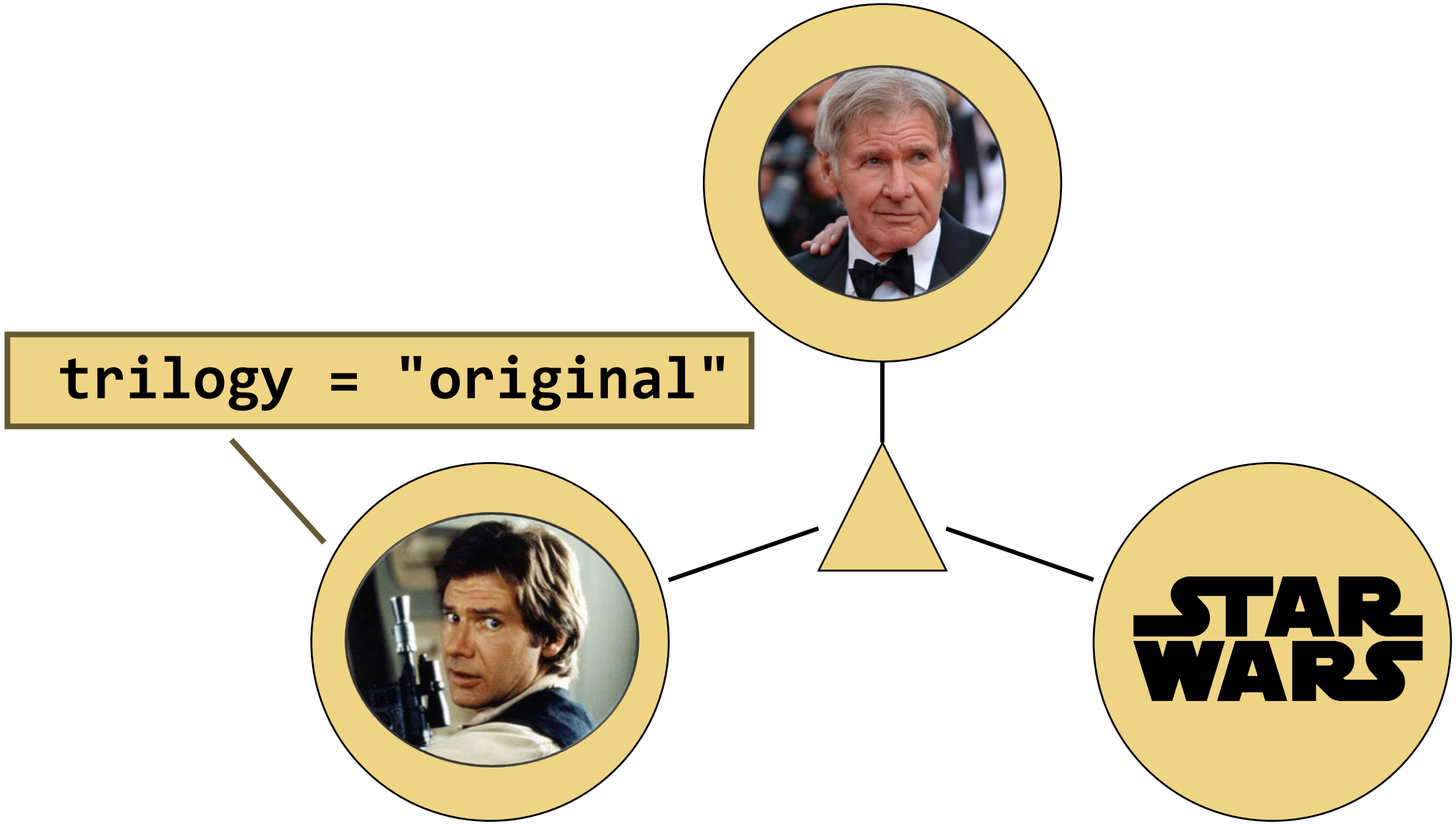
Who is he?



AZUR

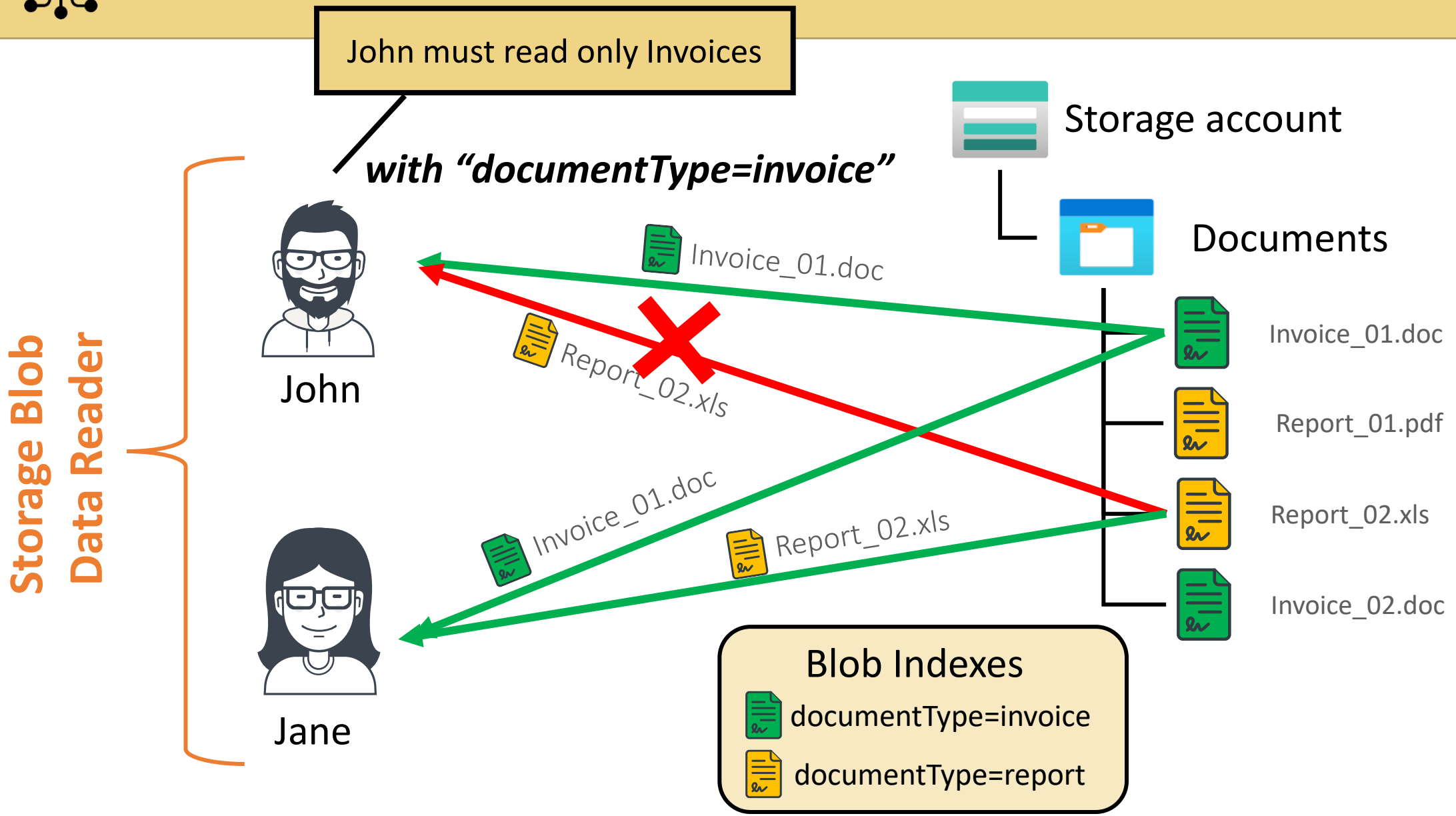
Who is he?

R(A)BAC in Start Wars



Azure **Attribute-Based Access Control (ABAC)** builds on Azure **RBAC** by adding **role assignment conditions** based on principal, resource and request attributes.

Scenario


John must read only Invoices
with “documentType=invoice”
Storage account
Documents
Invoice_01.doc
Report_01.pdf
Report_02.xls
Invoice_02.doc
Storage Blob Data Reader
John
Jane
Invoice_01.doc
Report_02.xls
Invoice_01.doc
Report_02.xls
Blob Indexes
documentType=invoice
documentType=report

Conditions

You can configure conditions on role assignments for **DataActions** to achieve these goals.

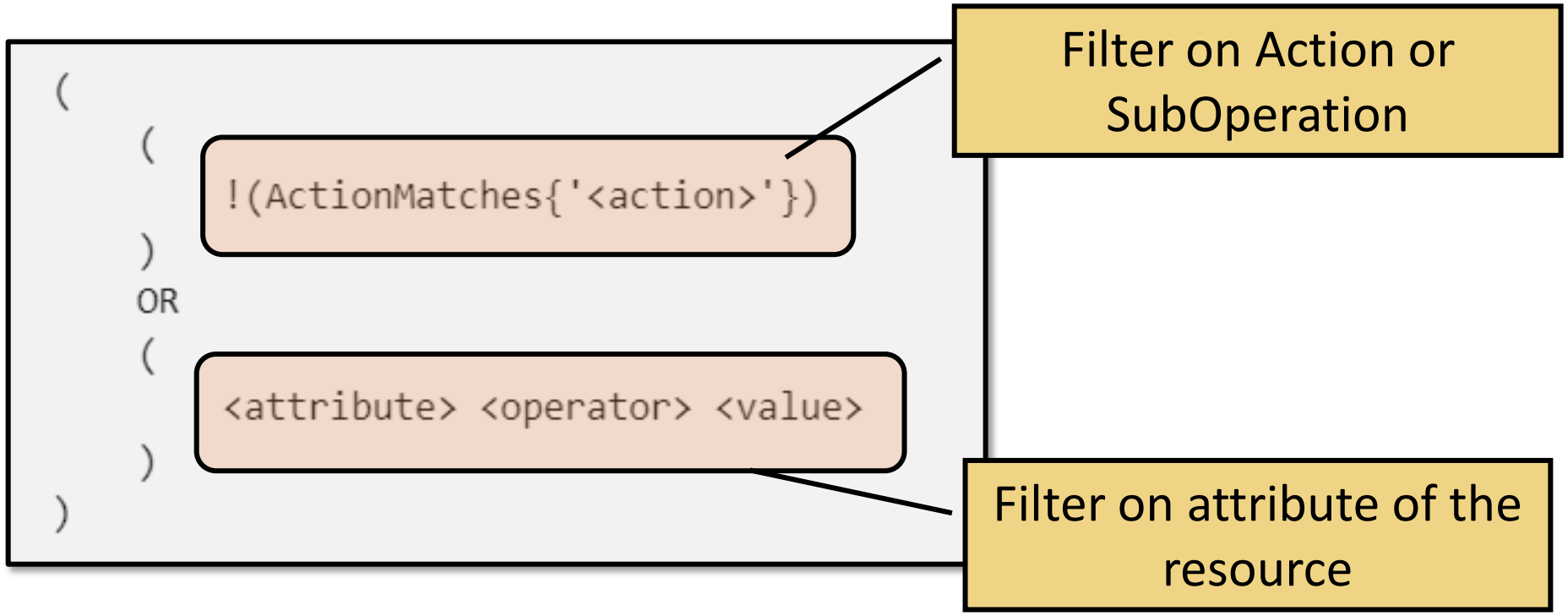
You can add conditions to **built-in** or **custom roles**.

The built-in roles on which you can use role-assignment conditions include:

- Storage Blob Data Reader
- Storage Blob Data Contributor
- Storage Blob Data Owner

Condition format and syntax

A condition is an additional check that you can optionally add to your role assignment to provide more fine-grained access control.



Condition sample

The action requested by the user is not “*reading a blob*”

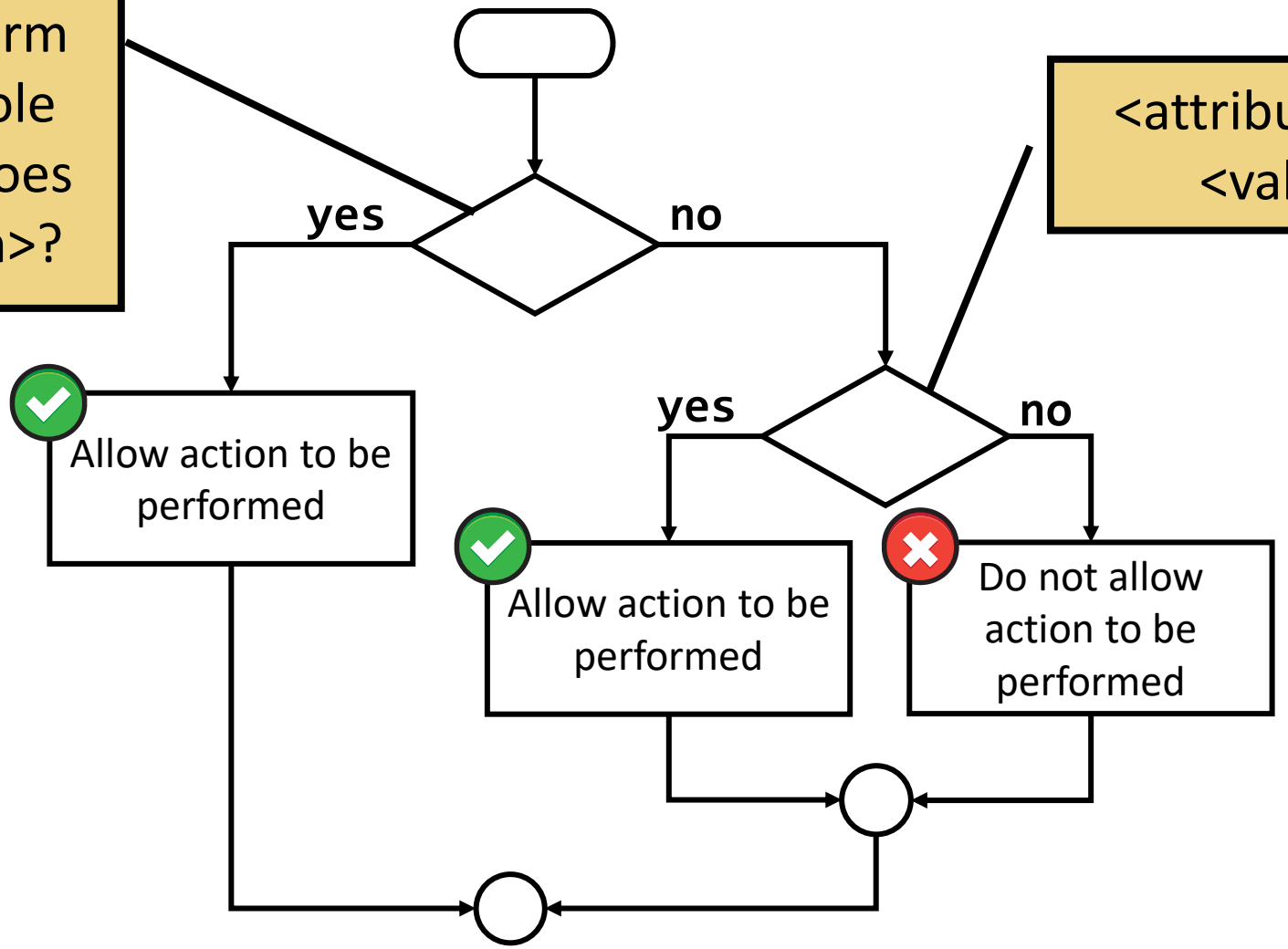
```
(
 (
  !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'})
 )
 OR
 (
  @Resource[Microsoft.Storage/storageAccounts/blobServices/containers:name] StringEquals 'documents'
 )
)
```

The name of the container the user want to access to is “*documents*”

The identity can execute all the operation except the **`read`** operation or read the blobs in the **`documents`** container.

How a condition is evaluated

User tries to perform an action in the role assignment that does not match <action>?



- ✓ **John** has been hired to manage the administration of the company, but she can read only the invoices.
- ✓ **Invoices** are stored in a **Storage Account**.
- ✓ Within the same storage, in the same container, there are also **reports** and **receipts**.
- ✓ John will manage documents using **custom software** or through the **Storage Explorer**

Conclusions

RBAC vs ABAC

RBAC and ABAC are not competing technologies for access control.

Give access with RBAC and refine it with ABAC.

ABAC pros

Flexibility

Agility

Granularity

ABAC cons

Complexity

Only Blob Storage, Data Lake Gen2 and Storage Queue

GA for Standard Storage, preview for Premium Storage

AZURE DAY

Thank you for your attention!!!

Massimo Bonanni

Technical Trainer @ Microsoft

massimo.bonanni@microsoft.com

aka.ms/maxlinkedin

AZURE DAY

Platinum Sponsor

Microsoft

msc TECHNOLOGY

Technical Sponsor

NET CODE

Azure Meetup TORINO

TORINO .NET

stickermule

Packt›

JET BRAINS