**Lez4 19/06/2024**

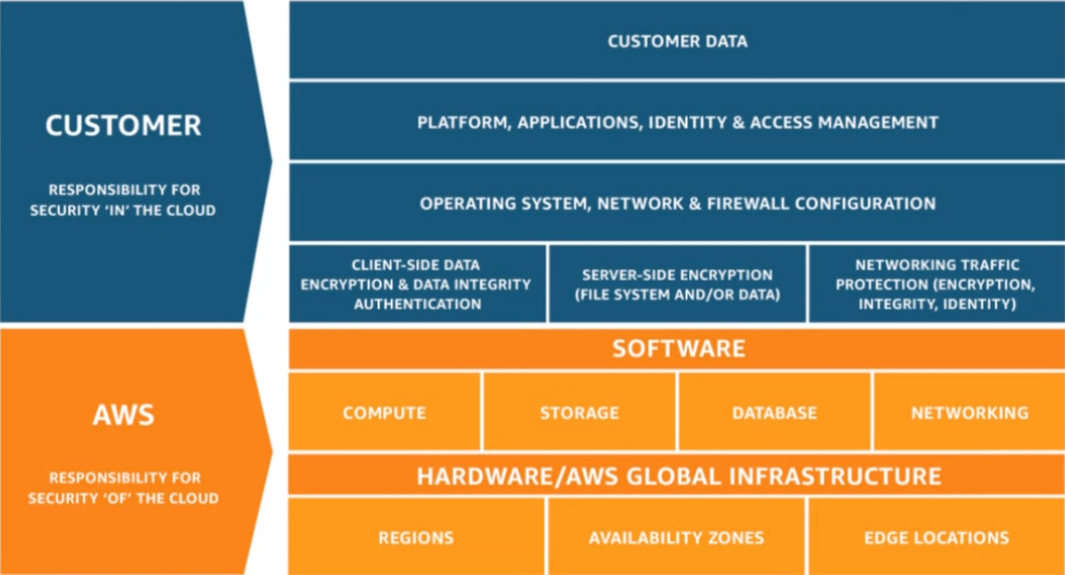
**cloud service and container**

**AWS Global Cloud Security**

**Modelli di responsabilità condivisa**

utente responsabile sicurezza nel cloud

aws responsabile sicurezza del cloud



**Responsabilità AWS**

sicurezza fisica datacenter

gestione HW e SW

infrastruttura rete

infrastruttura virtualizzazione

**Responsabilità Cliente:**

operating system

IAIAIAIIAIAIAIAIIA

<https://426918116256.signin.aws.amazon.com/console>

**IAM: Identity Access management**

Consente di controllare l'accesso a servizi di calcolo, archiviazione, database e applicazioni in AWS Cloud.iam può essere utilizzato per gestire l'autenticazione e per specificare e applicare i criteri di autorizzazione in modo da poter specificare a quali utenti possono accedere a quali servizi.

**Componenti**

**IAM user**

è una persona o un'applicazione definita in un account AWS e che deve effettuare chiamate API ai prodotti AWS. Ogni utente deve avere un nome univoco (senza spazi nel nome) all'interno dell'account AWS e una serie di credenziali di sicurezza che non sono condivise con altri utenti. Queste credenziali sono diverse dalle credenziali di sicurezza dell'utente del root dell'account AWS. Ogni utente è definito in un solo account AWS

**IAM group**

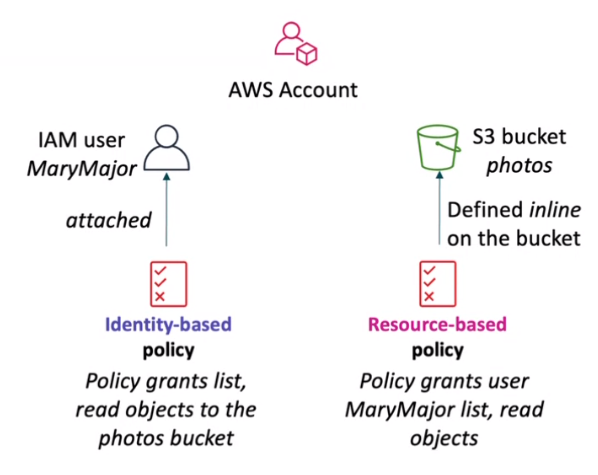
è una raccolta di utenti IAM. È possibile utilizzare i gruppi IAM per semplificare la specifica e la gestione delle autorizzazioni per più utenti

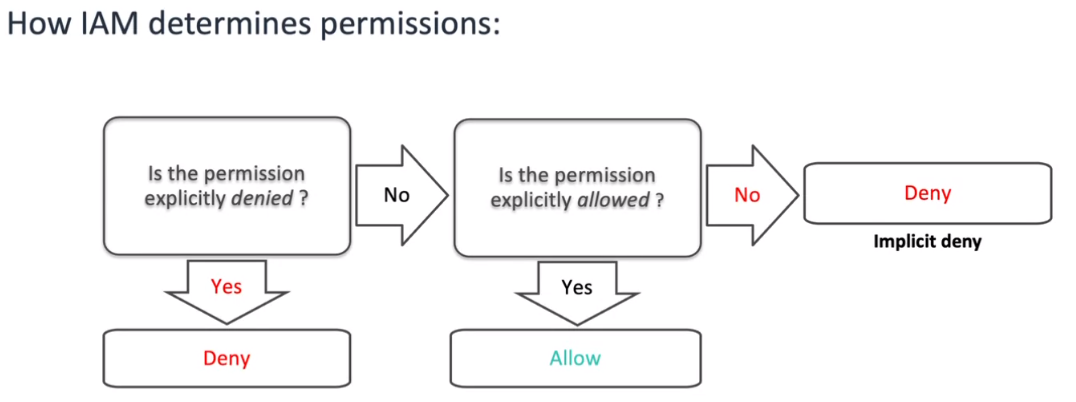
**IAM policy**

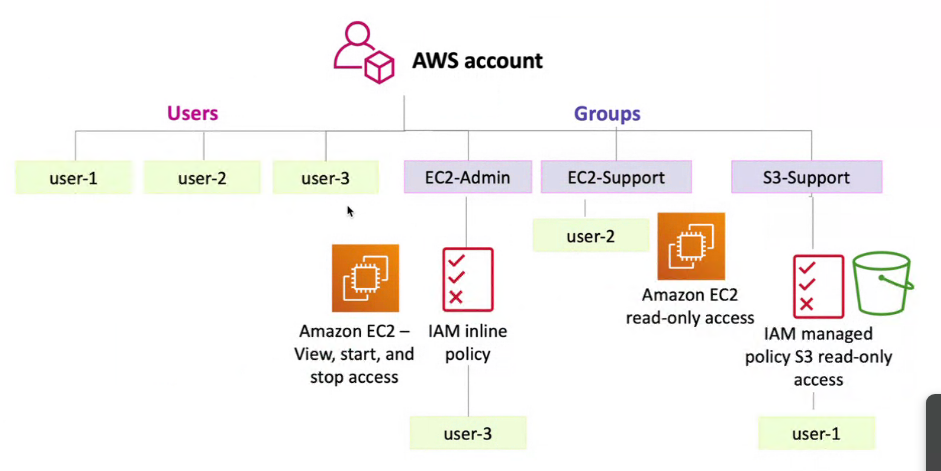
è un documento che definisce le autorizzazioni per determinare cosa possono fare gli utenti nell'account AWS. Una politica in genere concede l'accesso a risorse specifiche e specifica ciò che l'utente può fare con tali risorse. Le politiche possono anche negare esplicitamente l'accesso

**IAM role**

è uno strumento per concedere l'accesso temporaneo a risorse AWS specifiche in un account AWS.







PSW

awsITS2024!