Progetto Deployment di ambiente aziendale per "Zuzzurello Solutions"

Descrizione aziendale e progettazione.

Zuzzurello Solutions, si presenta come un'azienda in fase di crescita, con necessità di una sua prima infrastruttura cloud. Il progetto mirerà a creare un'ambiente basato sui principi di una infrastruttura in cloud, ovvero virtualizzazione, sicurezza e scalabilità. Esso verrà strutturato sulla piattaforma di Microsoft Azure, e sarà in grado di ospitare un'applicazione web interna in ambiente di produzione, insieme ad un ambiente di test riservato esclusivamente al team IT dell'azienda stessa.
Il progetto verrà suddiviso su più paragrafi con varie fasi logiche, descritte nei paragrafi a seguire.

Gestione di identità e accessi (Microsoft Entra ID)

Come priorità iniziale per il progetto, andremo ad affrontare la questione "Sicurezza" e per garantire una gestione centralizzata delle varie identità, andremo ad utilizzare il servizio principale offerto da Microsoft Azure, ovvero Microsoft Entra ID (nuova nomina dell'ex "Azure Activity Directory"). Microsoft Entra ID è un servizio di gestione delle identità e degli accessi basato sul cloud che consente alle organizzazioni di proteggere e gestire le identità sia in ambienti locali che cloud. Azure ID supporta diversi metodi di autenticazione, tra cui il Single Sign-On (SSO) e il più famoso e ormai attuale MFA (Multi-Factor Authentication).

I gruppi saranno gestiti in base alla loro funzione:

- IT-Team: gruppo che include gli amministratori di sistema, sviluppatori e tutte le figure tecniche presenti in azienda.
- HR-Employees: gruppo riservato al personale dell'ufficio.

A ciascun gruppo verranno specificati i ruoli definiti "RBAC" (Role-Based Access Control), che possiamo definire come un sistema di controllo degli accessi che consente di gestire chi può accedere alle risorse e quali operazioni possono essere eseguite su esse. In pratica possiamo definire ruoli con specifici privilegi di accesso, assegnare ruoli a questi utenti, controllare tutti gli accessi alle risorse di Azure, come sottoscrizioni, gruppi di risorse o singole risorse. Assegneremo, quindi, agli utenti del gruppo IT-Team un pieno controllo come "Owner" sull'ambiente di test, e un ruolo di "Contributor" sull'ambiente di produzione.

Struttura delle Subscription e delle risorse

Per avere accesso a tutti i servizi cloud offerti dal provider di Microsoft, ovviamente, avremo bisogno di una licenza Azure. Questa licenza è essenziale per accedere e utilizzare le risorse, usare servizi di calcolo, storage e rete e consente di gestire l'accesso e il costo delle risorse. L'infrastruttura, la andremo a strutturare quindi, su singola Subscription Azure, chiamata "Zuzzurello-Primary". Dopo l'acquisto della licenza possiamo finalmente passare all'atto pratico, mantenendo la logicità descritta nel paragrafo anticipatamente. Dovremo, quindi, creare due gruppi, chiamati gruppi di risorse o Resource Group, su cui si baserà la nostra suddivisione tra gli ambienti, semplificando la gestione dei permessi, dei costi, e del ciclo di vita delle risorse. I due gruppi saranno presentati dalla nomenclatura:

- RG-Prod: dedicato all'ambiente di produzione
- RG-Test: dedicato all'ambiente di testing, accessibile solo all'IT-Team

Sicurezza e governance con Azure Policy

Come da richiesta del cliente, per garantire che vengano utilizzate solo risorse appropriate in base al budget, implementeremo nel progetto una, così definita, "Azure Policy". La Azure policy, definita in italiano come "Criteri di Azure", è un servizio che consente alle aziende di far rispettare regole e standard interni su tutte le risorse cloud in modo automatico e su larga scala e fornisce una dashboard (Pannello di Controllo) che mostra in chiaro e in modo sintetico se l'ambiente è conforme a queste regole, ergo, questo aiuta a mantenere l'ambiente cloud sicuro, conforme alle normative e coerente con le politiche aziendali. La policy verrà denominata "DenyHighPerformanceVMs" con effetto di "Deny" e un parametro (quindi le macchine da evitare nell'implementazione del progetto) "Esv5".

Il json di implementazione nel progetto risulterà così:

```
{
  "mode": "All",
  "policyRule": {
    "if": {
      "allOf": [
        {
          "field": "type",
          "equals": "Microsoft.Compute/virtualMachines"
        },
        {
          "field": "Microsoft.Compute/virtualMachines/sku.name",
          "like": "Esv5*"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  },
  "parameters": {},
  "displayName": "Blocca creazione VM serie Esv5",
  "description": "Impedisce la creazione di macchine virtuali della serie Esv5
(fascia elevata)."
}
```

Gestione delle aree sensibili

Grazie al portale di Governance con Azure Policy, possiamo gestire in modo sicuro e organizzato dei ruoli specifici nell'infrastruttura. I ruoli specifici verranno assegnati a persone o team in base alla loro responsabilità. Come da richiesta andremo a fornire dei ruoli di:

- Billing (Fatturazione), in cui gli amministratori riceveranno ruoli come Billing Reader (può solamente visualizzare informazioni di fatturazione) o Billing Administrator (Può gestire gli aspetti di fatturazione, come pagamenti e abbonamenti)
- Sicurezza, in cui il reparto IT responsabile della sicurezza utilizzerà ruoli come Security Reader (colui che può solo accedere ai dati) oppure Security Admin (colui che può gestire e configurare tutte le impostazioni)
- Auditing (Verifica e Controllo) per il team che si occuperà di controllare la conformità e le attività, che avranno un ruolo di Log Analytics Contributor (che conferisce il permesso di entrare nel log e accedere ai dati di monitoraggio).

Rete Virtuale e configurazione della sicurezza

Per garantire un isolamento e la sicurezza della rete configureremo una Virtual Net (Vnet) denominandola "Vnet-zuzzurello". Una Virtual Net è una rete privata che isola e collega le risorse cloud tra di loro. Questa rete privata andremo a suddividerla in due subnet dedicate alle risorse separatamente, quindi troveremo una subnet dedicata alla produzione denominata "subnet-prod" e una subnet dedicata all' IT-Team denominata "subnet-test".

Ad ogni subnet, a sua volta, andremo ad associare un Network Security Group (NSG), che comporrà un insieme di regole che controllano quali tipi di traffico di rete saranno permessi e non, creato delle Regole NSG in cui alla subnet-test andremo ad autorizzare solo traffico in ingresso da IP aziendali e in cui andremo ad aprire solo porte strettamente necessarie come (es. porta 443 per HTTPS o 22 per SSH, se previsto).

Per rafforzare la sicurezza ulteriormente, è possibile in futuro prevedere l'utilizzo di un Azure Firewall, che servirà a filtrare in modo centralizzato il traffico in entrata e uscita.

Assegnazione Macchina Virtuale

L'ambiente di test, come da richiesta, ospiterà una sola macchina virtuale che nomineremo "vm-test-it" configurata con una dimensione economica (Standard B2s), e collegata come precedentemente descritto alla subnet "subnet-test". Grazie alle Regole NSG impostate, l'accesso a questa Vm è limitato esclusivamente ad indirizzi IP aziendali, garantendo un perimetro sicuro per i test interni. La macchina verrà utilizzata per eseguire prove, simulazioni e attività di validazione prima del rilascio del prodotto.

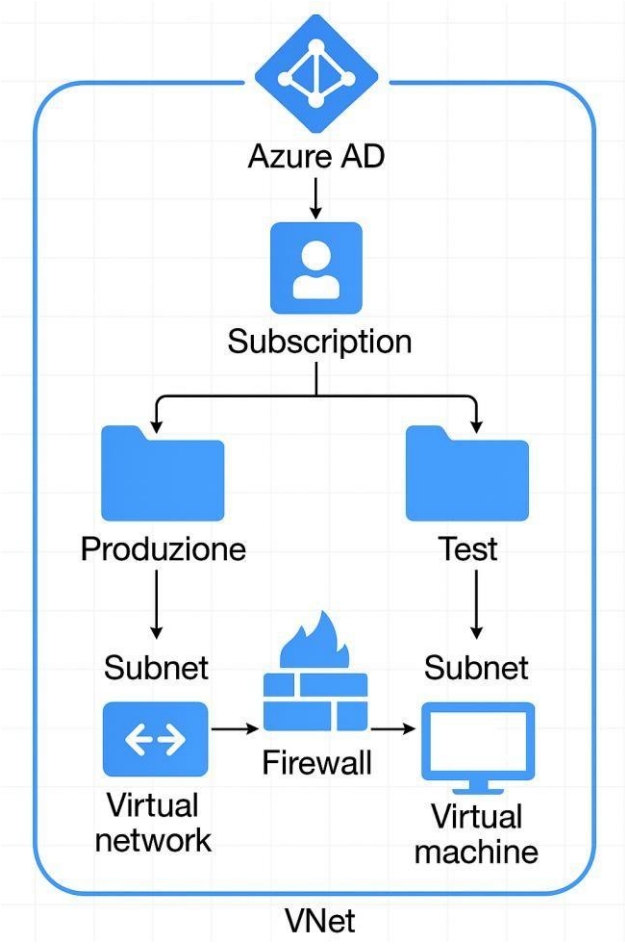
Gestione e accesso alle risorse

Per garantire una gestione efficace, flessibile e senza incoerenza dell'infrastruttura, andremo ad implementare determinati servizi per agevolare l'infrastruttura Azure.

I principali servizi che andremo ad implementare saranno:

- Azure Portal: un'interfaccia Web accessibile da browser, facile da usare per chi non conosce la riga di comando che permette anche di configurare e monitorare le risorse con pochi "clic", utilizzabile per gestioni quotidiane e configurazioni veloci senza script.
- Azure Cloud Shell: Un ambiente shell basato su Linux o PowerShell, accessibile dal browser. Include strumenti preinstallati come Azure CLI, PowerShell, Terraform, Git, editor di testo e linguaggi di programmazione (Python, Node.js, .NET) e infine Salva i file su uno storage Azure per mantenere i dati tra sessioni.
- Azure Command Line Interface (Azure CLI): uno strumento utilizzato da riga di comando per creare, configurare e gestire risorse Azure. Consente di automatizzare attività ripetitive tramite script e offre controllo granulare e flessibilità rispetto all'interfaccia grafica.

Diagramma Progetto e conclusioni



Questa Infrastruttura, rappresenta un grande inizio di partenza sicuro e organizzato per Zuzzurello Solutions, garantendo al cliente grande sicurezza grazie alla segmentazione e ai controlli degli accessi, grande governance con utilizzo di policy mirate e RBAC, flessibilità nella gestione tramite strumenti Azure.

Il progetto ovviamente può essere solo un grande inizio, sperando e consigliando anche altre implementazioni di backup, monitoraggio e altri strumenti, affinché l'esperienza possa migliorare man mano che le esigenze aziendali cresceranno.

Fonti Utilizzate: https://learn.microsoft.com/it-it/azure/?product=popular
Dichiaro di aver utilizzato, per lo sviluppo di immagini e spiegazioni più dettagliate, fonti AI.