BUILD YOUR TAGGING STRATEGY WITH AZURE POLICY AND AUTOMATION

Presented by Doug Vanderweide

Boston Azure Meetup
November 16, 2021

HI, I'M DOUG VANDERWEIDE

- **Director of IT** at **Avanade**
  - Joint Venture of Microsoft and Accenture
  - ~50,000 employees worldwide
  - We're always hiring Microsoft talent
- 10+ years working in **Azure**
- 25+ years as a **.NET/SQL Server/open-source developer**
- Originally from Maine, 5 years in Texas

Microsoft CERTIFIED AZURE SOLUTIONS ARCHITECT EXPERT

Microsoft CERTIFIED DEVOPS ENGINEER EXPERT

Microsoft CERTIFIED AZURE ADMINISTRATOR ASSOCIATE

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

Microsoft CERTIFIED AZURE DEVELOPER ASSOCIATE

aws certified Solutions Architect Associate

A PRIMER ON GOVERNANCE

Governance is the ability to ensure your IT assets can be

identified, measured and controlled

according to your business and technical requirements

What is this?

Where is it?

What does it do?

Who owns it?

Who deployed it?

Why was it deployed?

What relies upon this?

Who controls it?

Who is paying for it?

What does it cost?

How efficient is it?

A PRIMER ON LARGE CORPORATION IT OPERATIONS

Multiple clouds (public and private)

- Azure, AWS, Rackspace, HPE, etc.

Multiple Azure subscriptions

- Dev/Test, Regional, Hub-Spoke, etc.

'Chargeback' model

- Operational costs are billed back to specific business units

IT Servicing Model

- IT department is the caretaker for assets owned / responsible to specific business units

Multiple toolsets

- SIEM, ITSM, ITIL, CMDB, IPAM, etc.

A PRIMER ON TAGGING

- Tags in Azure are key-value pairs that can be assigned to most (but not all) assets
- They store metadata that is useful for understanding the context of a resource
- Azure native, bespoke and third-party toolsets can usually retrieve tags when calling for a resource (via PowerShell, CLI, API)
- Tags exist outside, and therefore extend, the subscription / resource group hierarchy
  - Also, management groups, and departments / accounts for Enterprise Agreements

GOVERNANCE REQUIRES A SOLID TAGGING STRATEGY

- **Naming standards** can help identify asset location/purpose/use
- **Subscriptions** can group assets by purpose or business unit
- **Resource groups** can manage assets on the same lifecycle
- **Regions** can be chosen to support specific business units

But these require significant business decisions that might not scale

- **Tagging** allows us to relate services across multiple reporting dimensions, without impacting the hierarchy, region or operation of those services

A TYPICAL TAGGING STRATEGY

Tag Name	Default Value	Required?
CostCenter	US-MFG-EAST-001	Yes
Owner	US-Manufacturing-East	Yes
Version	14.0.3.5	No
BusinessCriticality	High	Yes
Contact	us-mfg-east@acme.com	Yes
TerminationDate	2021-12-31	No
WorkloadName	ERP DB Server	Yes
DataClassification	Highly Confidential	Yes

THE NEXT LARGE COMPANY THAT HAS 100 PERCENT TAGGING COVERAGE WILL BE THE FIRST

A PRIMER ON AZURE POLICY

Allows you to enforce and audit deployment compliance on Azure assets

Can be assigned at multiple scopes

- Management groups
- Subscriptions
- Resource Groups

Can be grouped together for a common outcome (‘Initiatives’)

Multiple means of enforcement

- Reject deployment
- Amend deployment
- Audit deployment (and trigger event)

TYPICAL AZURE POLICIES

- Deploy only to certain regions
- Don’t deploy expensive SKUs
- Require encryption at rest
- Allow HTTPS only on public endpoints

- Ensure VMs are set for backups
- Require NSGs on all new subnets
- Provide certain default settings
- Check for certain tags

Azure has a long list of built-in, best-practice policies: https://docs.microsoft.com/en-us/azure/governance/policy/samples/built-in-policies

PARTS OF AZURE POLICY

Definition	Describes the condition to be met and what to do
Definition Objects	Allowed values for a given configuration; e.g., allowed tag values
Assignment	Applies a Policy Definition to a specified scope (management group, subscription, resource group
Initiative	A grouping of Policy definitions for Assignment purposes; e.g., all tagging Policy might be in a tagging Initiative
Exclusions	Any assets that are exempt from the Policy definition at the Assignment scope
Remediation	What steps you would like to perform on existing assets that do not comply with a Policy

DEMO: DEPLOY AZURE POLICY FROM POWERSHELL AND TEMPLATE

POLICY CAN-DO AND CANNOT-DO

CAN

- Require the presence of a configuration value
- Restrict configuration inputs to a list of specific values
- Place a default configuration value where a value is not provided
- Override a provided configuration value with a default value

CANNOT (NATIVELY)

- Produce an "option list" of allowed values at runtime
- Complex "if-then" statements; e.g, "if deploying to East US and a DSv3 series VM, then apply a given tag value"
- Restrict configuration inputs to a range; e.g., a non-specific number between 1 and 100

TYPICAL SOLUTIONS FOR POLICY RUNTIME LIMITATIONS

- Azure DevOps
  - Collecting runtime arguments, typically from a configuration file
  - Pulling information from CMDB/ITSM/other APIs
- PowerShell scripts / Azure Automation
  - User will be prompted to enter correct values at runtime
- Azure Functions or Logic Apps
  - Complex "if-then" interpretation that doesn't require human input
  - Pulling information from external databases
  - 'Helping' DevOps / Azure Automation routines

RECAP

- Large organizations face significant challenges when trying to govern their resources
- In public cloud, tagging tends to be the most effective control plane for identifying and understanding assets
- Few organizations have sufficient tagging coverage to achieve effective governance
- Azure Policy can ensure tagging is present and complies with guidelines
- Deployment automation is typically required for effective Azure Policy implementation