Microsoft Azure Lighthouse

Alan Kinane
Azure Technical Lead, MicroWarehouse

Copyright

The legal bit

Agenda

What's in store for this webinar

- Current Access Procedures
- Role Based Access Control
- Azure Governance
- Azure Lighthouse for Delegated Resource Access
- Onboarding
- Security Best Practices
- Q & A

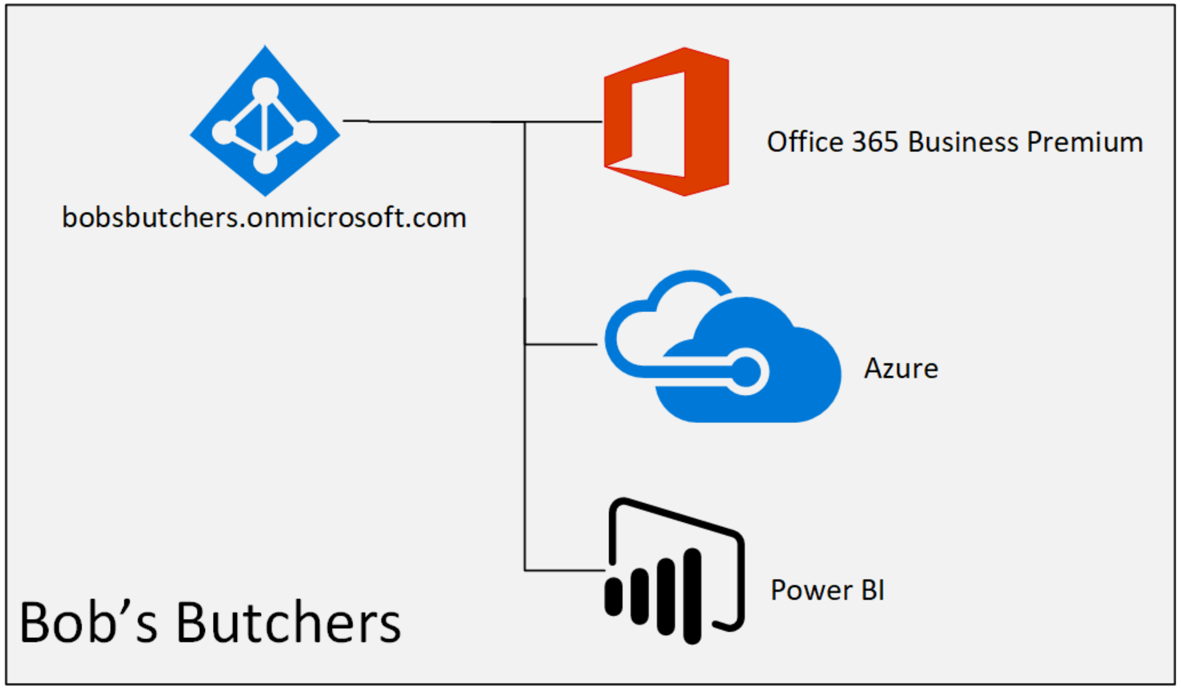
Let’s start with the basics

Terms often used but misunderstood

- Tenant
  - Always present with a MS business cloud service
  - A directory of users, groups, and password hashes
  - AKA Azure Active Directory
    - It is not “Active Directory Domain Services”
- Subscription
  - A solution you consume from Microsoft
  - Attached to a tenant
    - Azure AD provides the users, groups, and authentication/authorization
  - Many subscriptions to one tenant
  - Ideally a business (your customer) has 1 tenant only
    - Consistent usernames/passwords

Example Tenants & Subscriptions

Illustrated scenarios



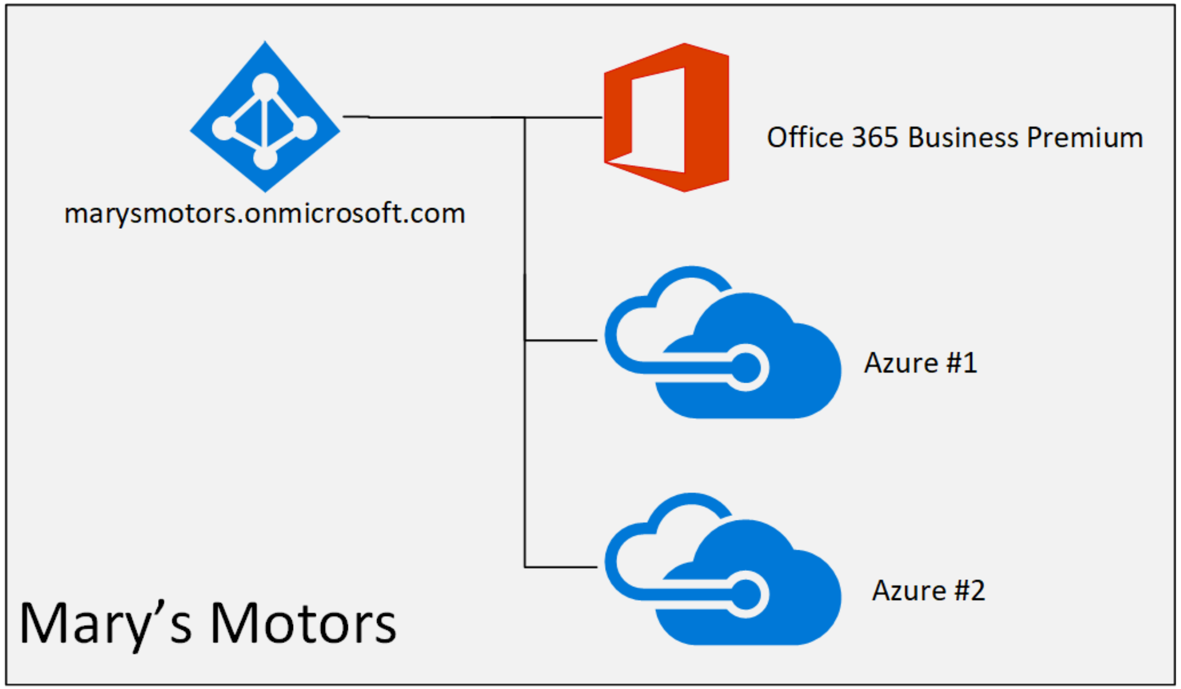
bobsbutchers.onmicrosoft.com

Office 365 Business Premium

Azure

Power BI

Bob’s Butchers



marysmotors.onmicrosoft.com

Office 365 Business Premium

Azure #1

Azure #2

Mary’s Motors

Partner Access

How you are currently managing your customers

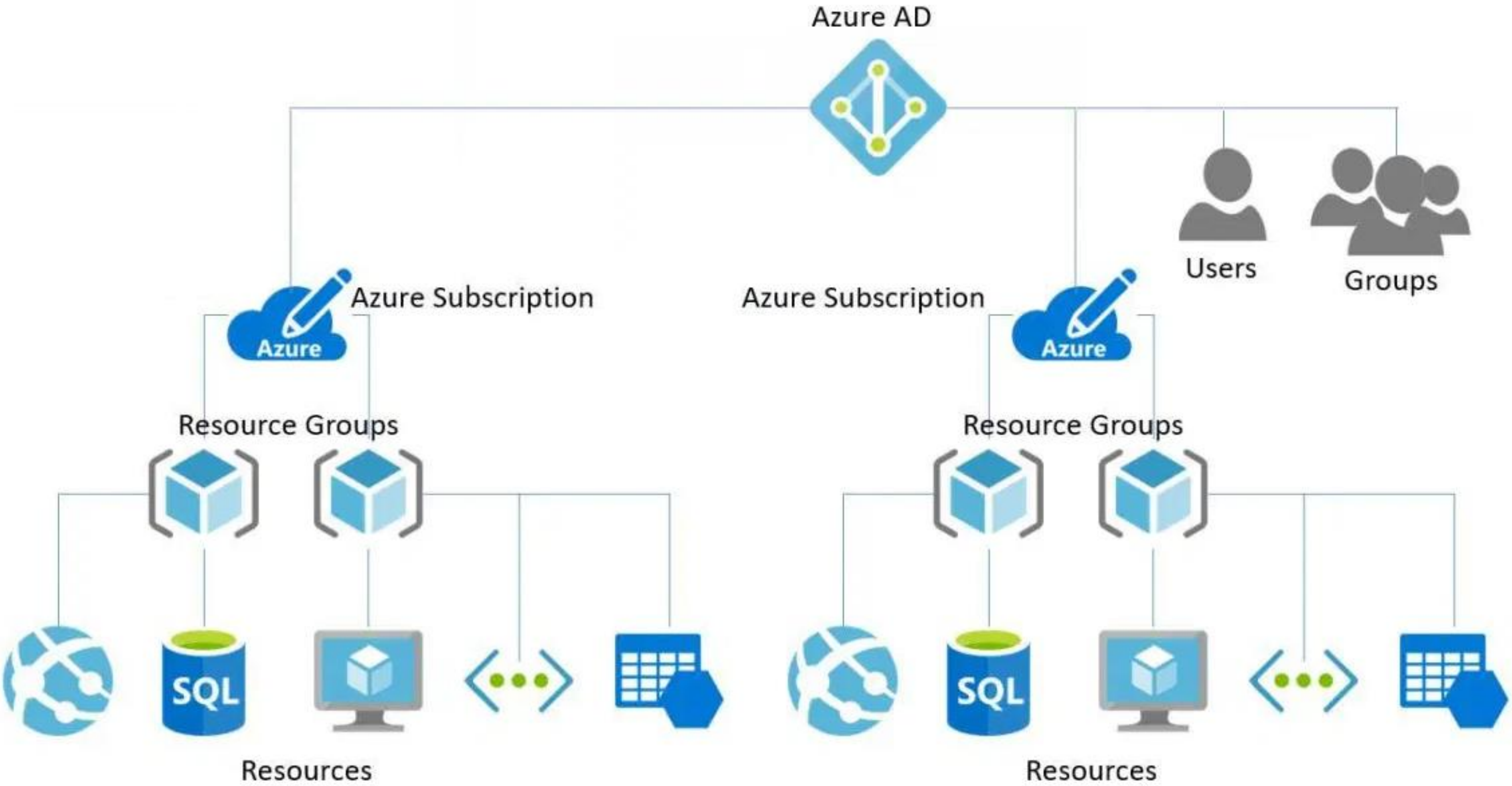
- Administer-on-Behalf-Of (AOBO)
  - As a CSP service provide you have already an established “relationship” with your customers
  - This allows you access to your customer tenants and act as an administrator
  - Most tasks can then be performed directly on the customer tenant
  - e.g. Manage users, licensing, perform general Office 365 admin tasks etc.
  - Some limitations for example you can’t access the customer’s security and compliance center
  - Access to end customer subscriptions are managed by creating role assignments from the customer Azure portal using AOBO
  - This is very difficult to manage at scale and does not support user groups outside of the tenant

Azure Resources & Resource Groups

Everything you deploy is a resource

- Resources:
  - VMs, disks, virtual networks, backups, storage, Azure SQL databases etc
  - Always deployed into a resource group
- Resource groups
  - Like a folder, somewhere to store resources in a logical group
  - Should be used for designated access control on the group level
- Delegate permissions to Resource Groups
  - Bad idea to assign permissions to individual resources – too hard to maintain
  - Grant the required access permissions to a group of users and assign to the required resource groups
  - Permissions are inherited to all of the resources in the resource group
  - IT admins sign into the Azure Portal and can only see their assigned resource groups and resources

Azure Resource Structure of Customer Tenant



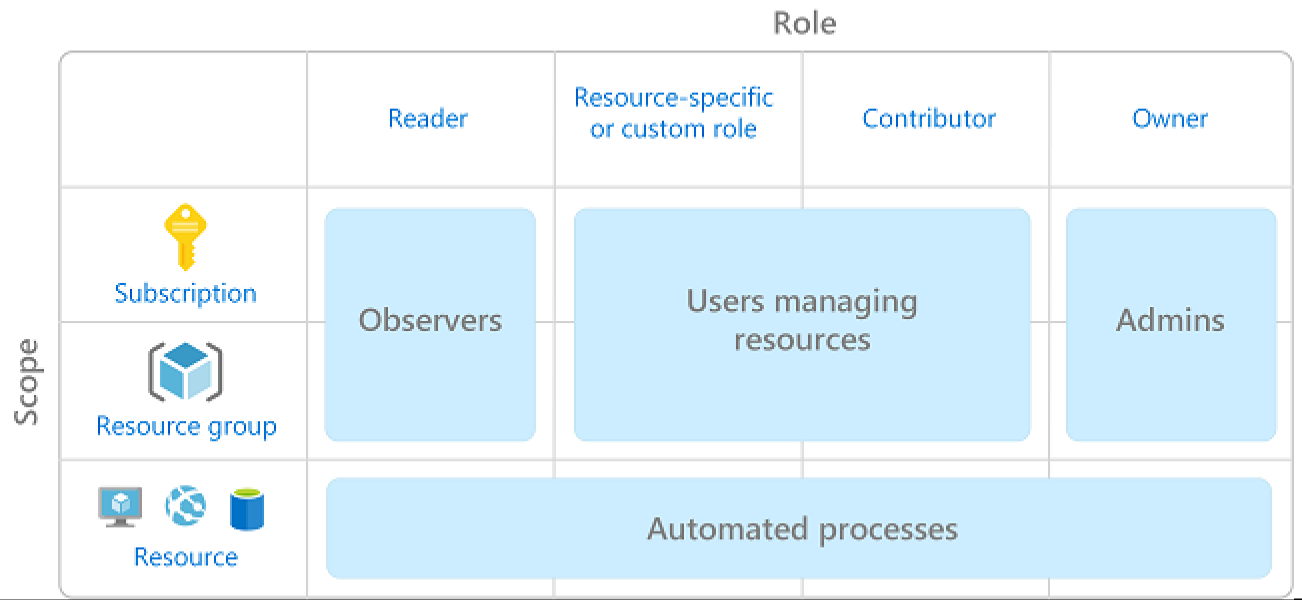
Role Based Access Control (RBAC)

A great starting point for Azure Governance

Manage who has access to which Azure resources and what they can do with them

- **Owner** - Has full access to all resources including the right to delegate access to others
- **Contributor** - Can create and manage all types of Azure resources but can’t grant access to others
- **Reader** - Can view existing Azure resources
- Management specific roles, e.g. Virtual Machine Contributor, Backup Reader, Backup Operator etc.

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles



Managing multiple customers

Some current headaches you might have

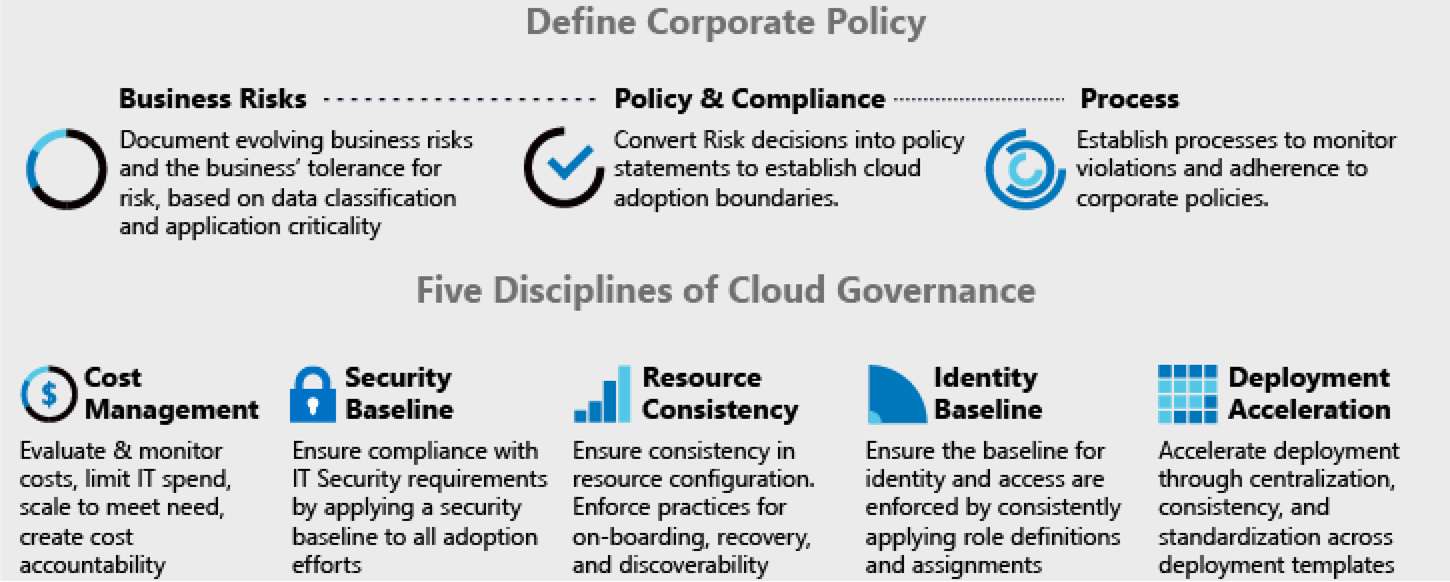
- Each tenant has to be viewed individually by “switching the directory” or by using separate logins
- No means to centrally manage your customers from a “single pane of glass” (portal)
- Difficult to monitor performance metrics and diagnostics across multiple customers visually
- Deployments are not standardised, each engineer does it their own way and has too much control
- Governance is inconsistent or non-existent

Governance

The scaffolding for Azure solutions

“A collection of concepts and services that are designed to enable management of your various Azure resources at scale”

1. Identify the risks
2. Define and Implement Policy
3. Establish processes for compliance management



Define Corporate Policy

Business Risks - - - - - - - - - - **Policy & Compliance** ········· **Process**

Business Risks
Document evolving business risks and the business’ tolerance for risk, based on data classification and application criticality

Policy & Compliance
Convert Risk decisions into policy statements to establish cloud adoption boundaries.

Process
Establish processes to monitor violations and adherence to corporate policies.

Five Disciplines of Cloud Governance

Cost Management
Evaluate & monitor costs, limit IT spend, scale to meet need, create cost accountability

Security Baseline
Ensure compliance with IT Security requirements by applying a security baseline to all adoption efforts

Resource Consistency
Ensure consistency in resource configuration. Enforce practices for on-boarding, recovery, and discoverability

Identity Baseline
Ensure the baseline for identity and access are enforced by consistently applying role definitions and assignments

Deployment Acceleration
Accelerate deployment through centralization, consistency, and standardization across deployment templates

Governance

Tell me more about governance

Some Examples:

- Resource organisation – using resource groups the correct way and delegating access to user or management groups
- **Role Based Access Control** – who has access to do what
- **Azure Policy** – what specifically can they do, where and how much
- **Azure Blueprints** – bringing it all together in a repeatable format - a packaged solution!

Azure Lighthouse

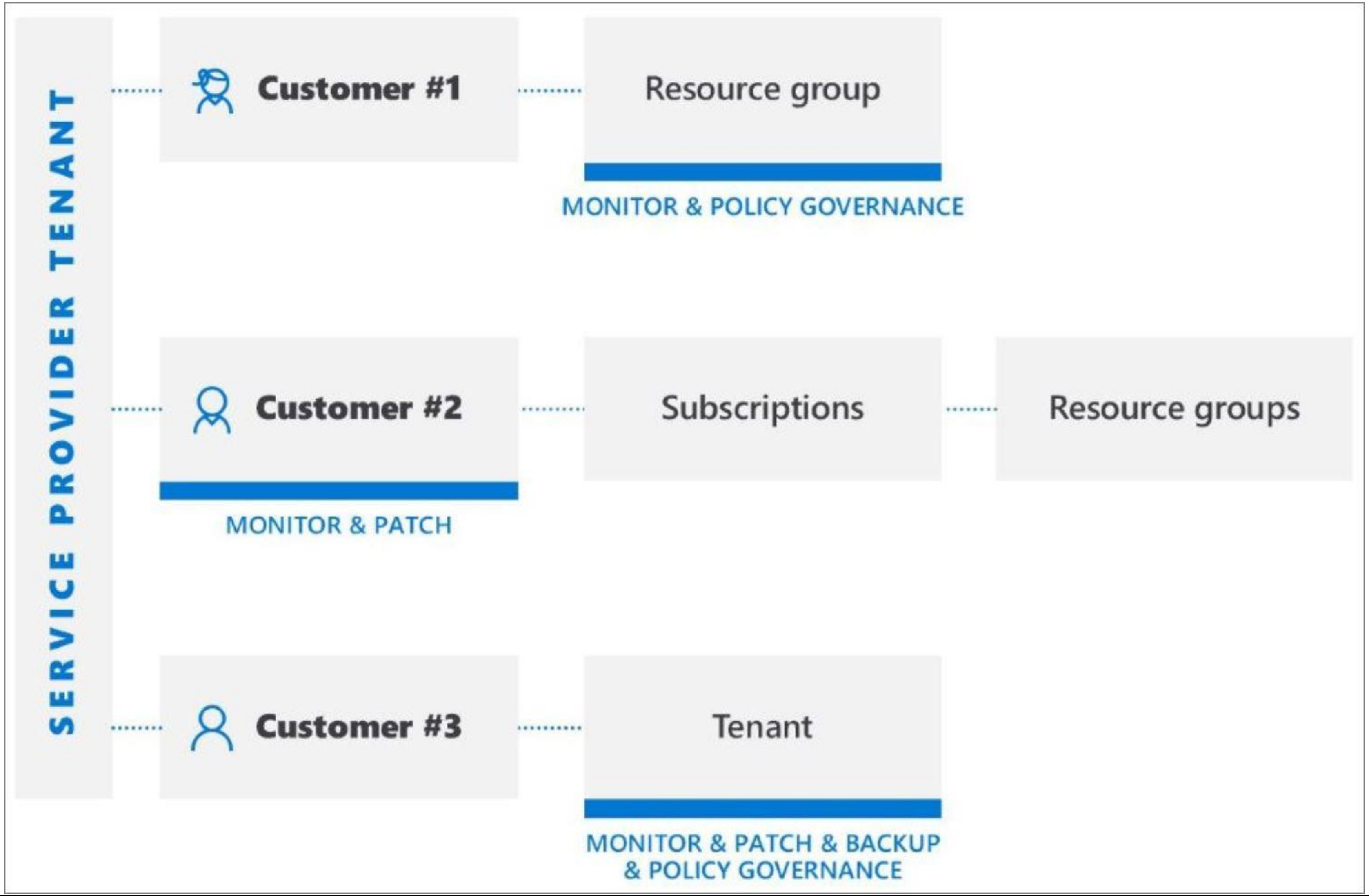
What is it?

A service to provide cross-customer management at scale from a single portal via delegated resource management

- Delegated Resource Management
  - You create security groups in your own partner tenant based on role and assign users
  - Assign the required amount of “Azure” permissions to these security groups using RBAC roles
  - Delegate access for these groups to your customer’s Azure at subscription or resource group level
  - This can be managed more easily at scale across your entire customer base
  - No need to switch directories anymore, all customer Azure resources are in the same context

Azure Lighthouse

Cross-customer Management



SERVICE PROVIDER TENANT

Customer #1

Resource group

MONITOR & POLICY GOVERNANCE

Customer #2

Subscriptions

Resource groups

MONITOR & PATCH

Customer #3

Tenant

MONITOR & PATCH & BACKUP & POLICY GOVERNANCE

Azure Lighthouse

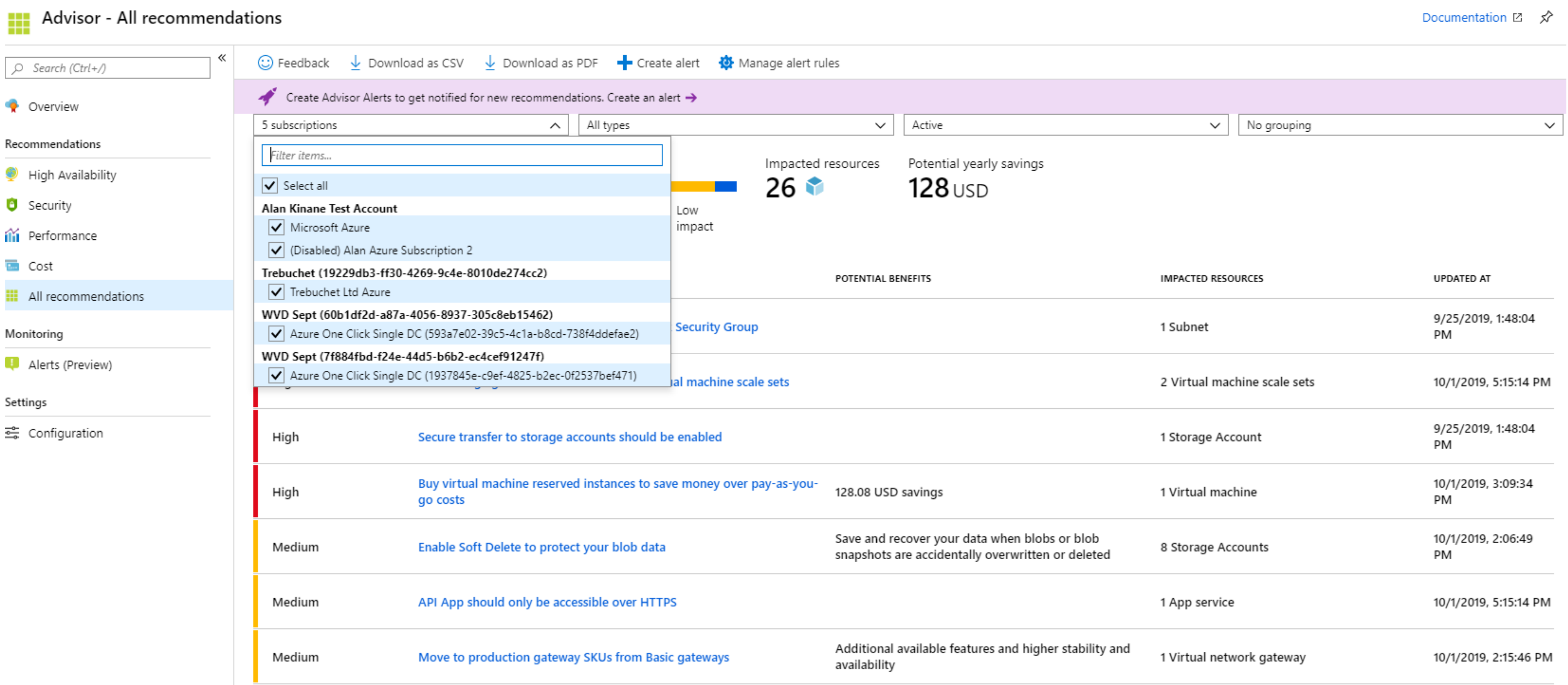
How can it help my business?

- Common use cases:
  - Manage all customer resources from your own partner environment
  - Utilise Azure advisory services across your customer base such as Service Health, Azure Advisor, Azure Monitor, Security Centre, Cost Management (coming soon to CSP) and many more
  - Apply consistent governance across all of your tenants
  - Create multi-customer dashboards and monitors
  - Centrally manage Azure security across entire customer base
  - Allows for more unified automation and reporting through scripting and APIs
  - And more to come…..

Azure Lighthouse

Give me an example

- Simple Example: Using Azure Advisor to get a list of best practice recommendations across all customers from page



Advisor - All recommendations

Create Advisor Alerts to get notified for new recommendations. Create an alert →

5 subscriptions | All types | Active | No grouping

Filter items...

☑ Select all

Alan Kinane Test Account

☑ Microsoft Azure

☑ (Disabled) Alan Azure Subscription 2

Trebuchet (19229db3-ff30-4269-9c4e-8010de274cc2)

☑ Trebuchet Ltd Azure

WVD Sept (60b1df2d-a87a-4056-8937-305c8eb15462)

☑ Azure One Click Single DC (593a7e02-39c5-4c1a-b8cd-738f4ddefae2)

WVD Sept (7f884fbd-f24e-44d5-b6b2-ec4cef91247f)

☑ Azure One Click Single DC (1937845e-c9ef-4825-b2ec-0f2537bef471)

Low impact

Impacted resources 26

Potential yearly savings 128 USD

		POTENTIAL BENEFITS	IMPACTED RESOURCES	UPDATED AT
	Security Group		1 Subnet	9/25/2019, 1:48:04 PM
	al machine scale sets		2 Virtual machine scale sets	10/1/2019, 5:15:14 PM
High	Secure transfer to storage accounts should be enabled		1 Storage Account	9/25/2019, 1:48:04 PM
High	Buy virtual machine reserved instances to save money over pay-as-you-go costs	128.08 USD savings	1 Virtual machine	10/1/2019, 3:09:34 PM
Medium	Enable Soft Delete to protect your blob data	Save and recover your data when blobs or blob snapshots are accidentally overwritten or deleted	8 Storage Accounts	10/1/2019, 2:06:49 PM
Medium	API App should only be accessible over HTTPS		1 App service	10/1/2019, 5:15:14 PM
Medium	Move to production gateway SKUs from Basic gateways	Additional available features and higher stability and availability	1 Virtual network gateway	10/1/2019, 2:15:46 PM

Azure Lighthouse

How much is it and how do I implement this?

- This is a free service – you are just accessing existing deployments with delegated permissions

- Onboarding can be delivered through a combination of two ARM templates and PowerShell – Don’t worry we can assist you with this

- Can be published as a service offering via the Azure Marketplace – some pre-requisites required for this

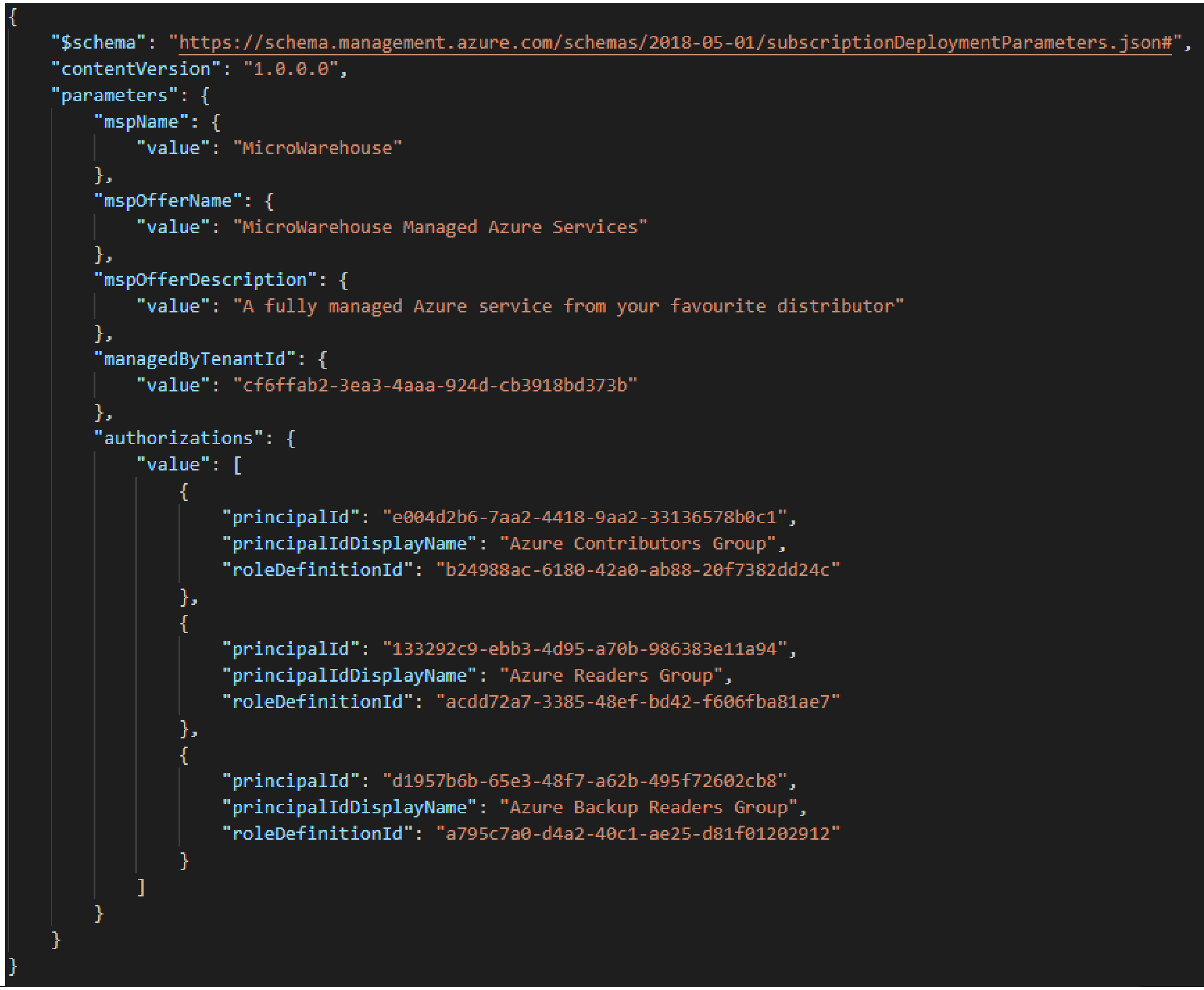
Customer Access Management

Design your delegation profiles

- Example
  - Set up a ‘Reader’ access group for IT staff who audit and assess existing deployments
  - Set up a ‘Contributor’ access group for IT staff who have full access to Azure deployments
  - Set up a ‘Backup Reader’ group for IT staff who have monitoring level access to Azure backups only

- Set these groups up on your own partner tenant and define a JSON parameters file based on this

- Deploy ARM template into customer Azure subscription(s)

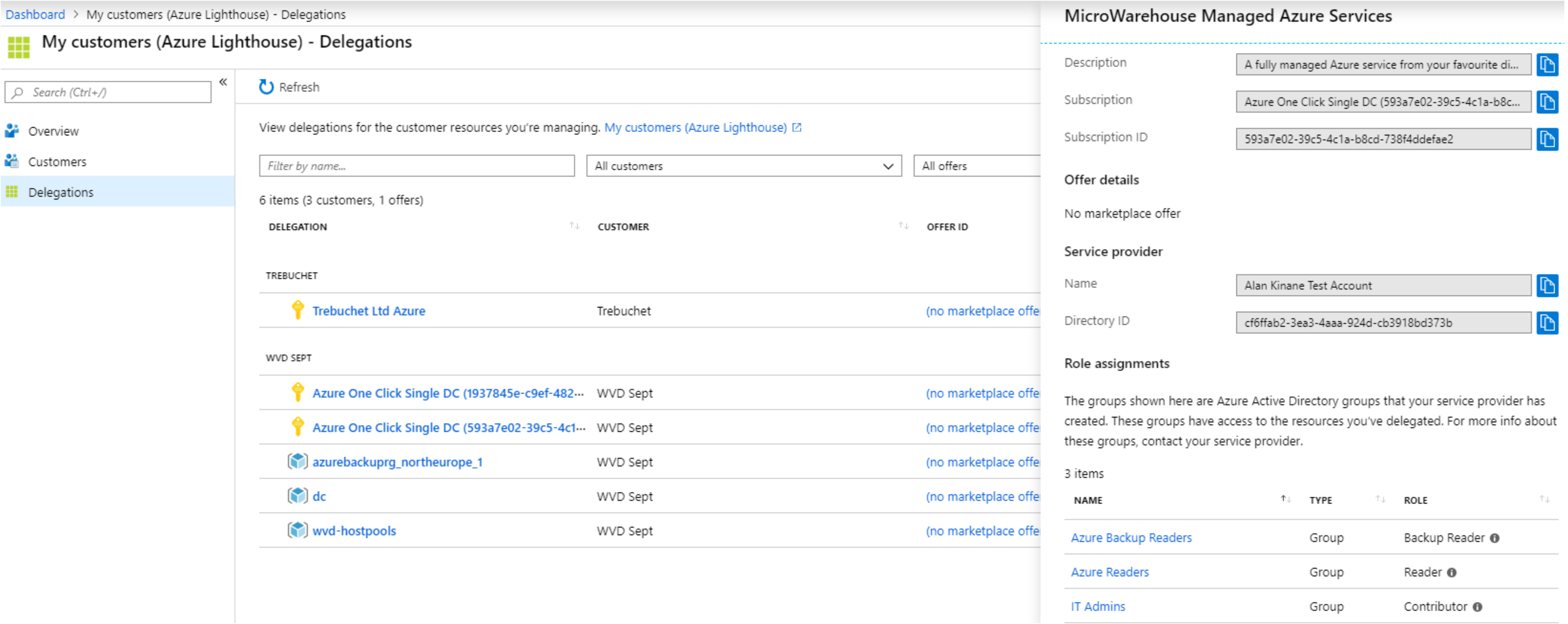


```
{
    "$schema": "https://schema.management.azure.com/schemas/2018-05-01/subscriptionDeploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "mspName": {
            "value": "MicroWarehouse"
        },
        "mspOfferName": {
            "value": "MicroWarehouse Managed Azure Services"
        },
        "mspOfferDescription": {
            "value": "A fully managed Azure service from your favourite distributor"
        },
        "managedByTenantId": {
            "value": "cf6ffab2-3ea3-4aaa-924d-cb3918bd373b"
        },
        "authorizations": {
            "value": [
                {
                    "principalId": "e004d2b6-7aa2-4418-9aa2-33136578b0c1",
                    "principalIdDisplayName": "Azure Contributors Group",
                    "roleDefinitionId": "b24988ac-6180-42a0-ab88-20f7382dd24c"
                },
                {
                    "principalId": "133292c9-ebb3-4d95-a70b-986383e11a94",
                    "principalIdDisplayName": "Azure Readers Group",
                    "roleDefinitionId": "acdd72a7-3385-48ef-bd42-f606fba81ae7"
                },
                {
                    "principalId": "d1957b6b-65e3-48f7-a62b-495f72602cb8",
                    "principalIdDisplayName": "Azure Backup Readers Group",
                    "roleDefinitionId": "a795c7a0-d4a2-40c1-ae25-d81f01202912"
                }
            ]
        }
    }
}
```

Azure Lighthouse

Managed Customers Overview

- Clear overview of your delegated access to customers subscriptions and resource groups and the assigned security roles



My customers (Azure Lighthouse) - Delegations

View delegations for the customer resources you're managing. My customers (Azure Lighthouse)

Filter by name... | All customers | All offers

6 items (3 customers, 1 offers)

DELEGATION	CUSTOMER	OFFER ID
TREBUCHET		
Trebuchet Ltd Azure	Trebuchet	(no marketplace offe
WVD SEPT		
Azure One Click Single DC (1937845e-c9ef-482...	WVD Sept	(no marketplace offe
Azure One Click Single DC (593a7e02-39c5-4c1...	WVD Sept	(no marketplace offe
azurebackuprg_northeurope_1	WVD Sept	(no marketplace offe
dc	WVD Sept	(no marketplace offe
wvd-hostpools	WVD Sept	(no marketplace offe

MicroWarehouse Managed Azure Services

Description	A fully managed Azure service from your favourite di...
Subscription	Azure One Click Single DC (593a7e02-39c5-4c1a-b8c...
Subscription ID	593a7e02-39c5-4c1a-b8cd-738f4ddefae2

Offer details

No marketplace offer

Service provider

Name	Alan Kinane Test Account
Directory ID	cf6ffab2-3ea3-4aaa-924d-cb3918bd373b

Role assignments

The groups shown here are Azure Active Directory groups that your service provider has created. These groups have access to the resources you've delegated. For more info about these groups, contact your service provider.

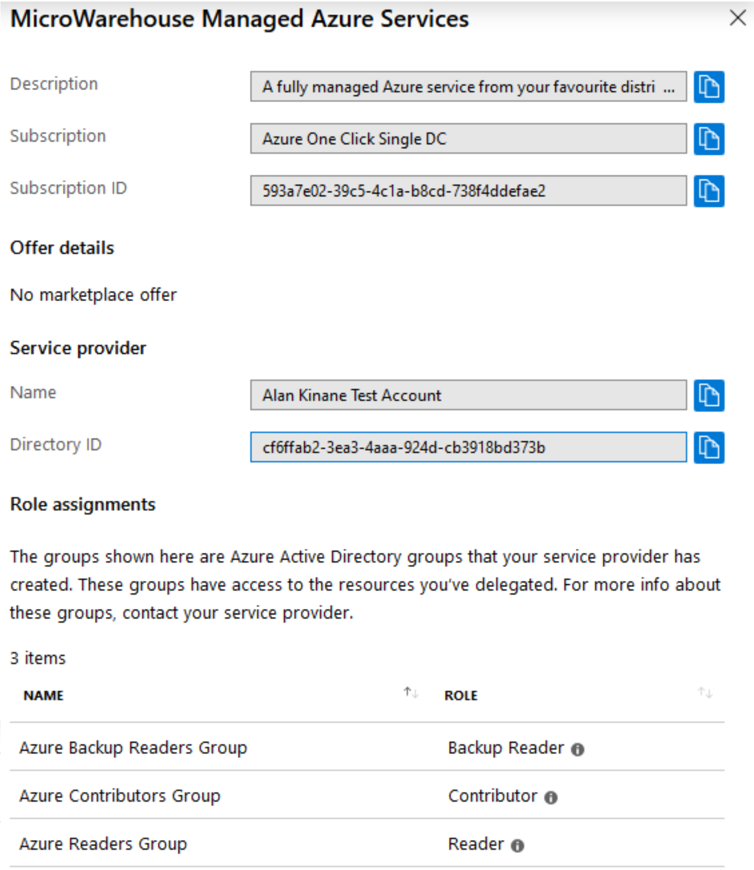
3 items

NAME	TYPE	ROLE
Azure Backup Readers	Group	Backup Reader
Azure Readers	Group	Reader
IT Admins	Group	Contributor

Azure Lighthouse

Customer's Service Provider Overview

- Clear overview of the managed service providers and assigned security roles from the customer portal
- Note: Multiple partners can be provided with delegated admin access
- Access can be revoked by the customer



MicroWarehouse Managed Azure Services

Description	A fully managed Azure service from your favourite distri ...
Subscription	Azure One Click Single DC
Subscription ID	593a7e02-39c5-4c1a-b8cd-738f4ddefae2

Offer details

No marketplace offer

Service provider

Name	Alan Kinane Test Account
Directory ID	cf6ffab2-3ea3-4aaa-924d-cb3918bd373b

Role assignments

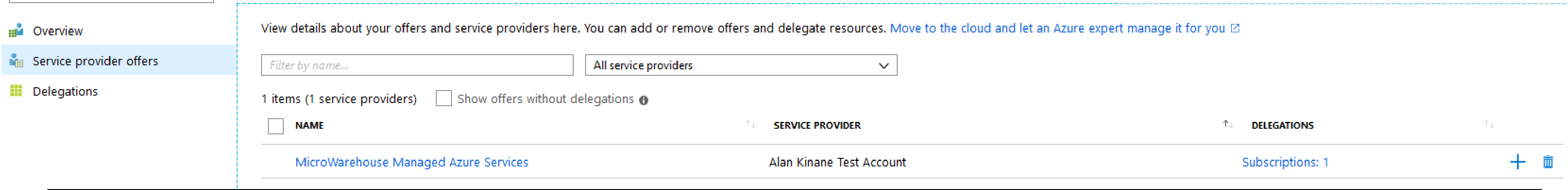
The groups shown here are Azure Active Directory groups that your service provider has created. These groups have access to the resources you've delegated. For more info about these groups, contact your service provider.

3 items

NAME	ROLE
Azure Backup Readers Group	Backup Reader
Azure Contributors Group	Contributor
Azure Readers Group	Reader

Home > Service providers (Azure Lighthouse) - Service provider offers

Service providers (Azure Lighthouse) - Service provider offers



View details about your offers and service providers here. You can add or remove offers and delegate resources. Move to the cloud and let an Azure expert manage it for you

Filter by name...

All service providers

1 items (1 service providers) □ Show offers without delegations

□	NAME	SERVICE PROVIDER	DELEGATIONS
	MicroWarehouse Managed Azure Services	Alan Kinane Test Account	Subscriptions: 1

Security Best Practices with Lighthouse

With great power comes great responsibility

- Make sure Multi-Factor Authentication is required for access
  - This is now a contractual requirement for Microsoft CSP resellers
  - Use the free conditional access baseline policy on customer tenant if needed
- Assign permissions using the least privilege principle
  - Do your staff all require full access? Does the end customer or any third parties need access?
  - Use the built-in RBAC roles (custom roles are not supported by Lighthouse)
  - Always use groups – even if there's just one user it will be easier to add and remove members later
- Don't assign access to an entire subscription unless required
  - Assign to resource groups instead
- Consider using Privileged Identity Management (PIM)
  - Provides Just-in-Time access for limited time periods based on an approval process
  - Requires an Azure AD Premium P2 license
- Use Azure Policy to enforce standards across all of your customers
  - Set up a standard naming conventions policy
  - Set restrictions on what your engineers are allowed to deploy and where

Thank-you

Any questions?

Alan Kinane

akinane@mwh.ie