MC2MC

Azure Monitor Baseline Alerting

Robert Prüst

- MVP
- MCT
- Developer @ Wortell

Azure Monitor Baseline Alerts

https://azure.github.io/azure-monitor-baseline-alerts

Azure Resources

- AmlFilesystems
  - amlFilesystems
- AnalysisServices
  - servers
- ApiManagement
  - service
- App
  - containerApps
- Automation
  - automationAccounts
- AVS
  - privateClouds
- Batch
  - batchAccounts
- Cache
  - Redis
- Cdn
  - profiles
- CognitiveServices
  - accounts
- Compute
  - virtualMachines
  - virtualMachineScaleSets
- ContainerInstance
  - containerGroups

- Storage
  - storageSyncServices
- StreamAnalytics
  - streamingjobs
- Synapse
  - workspaces
- Web
  - serverFarms
  - sites
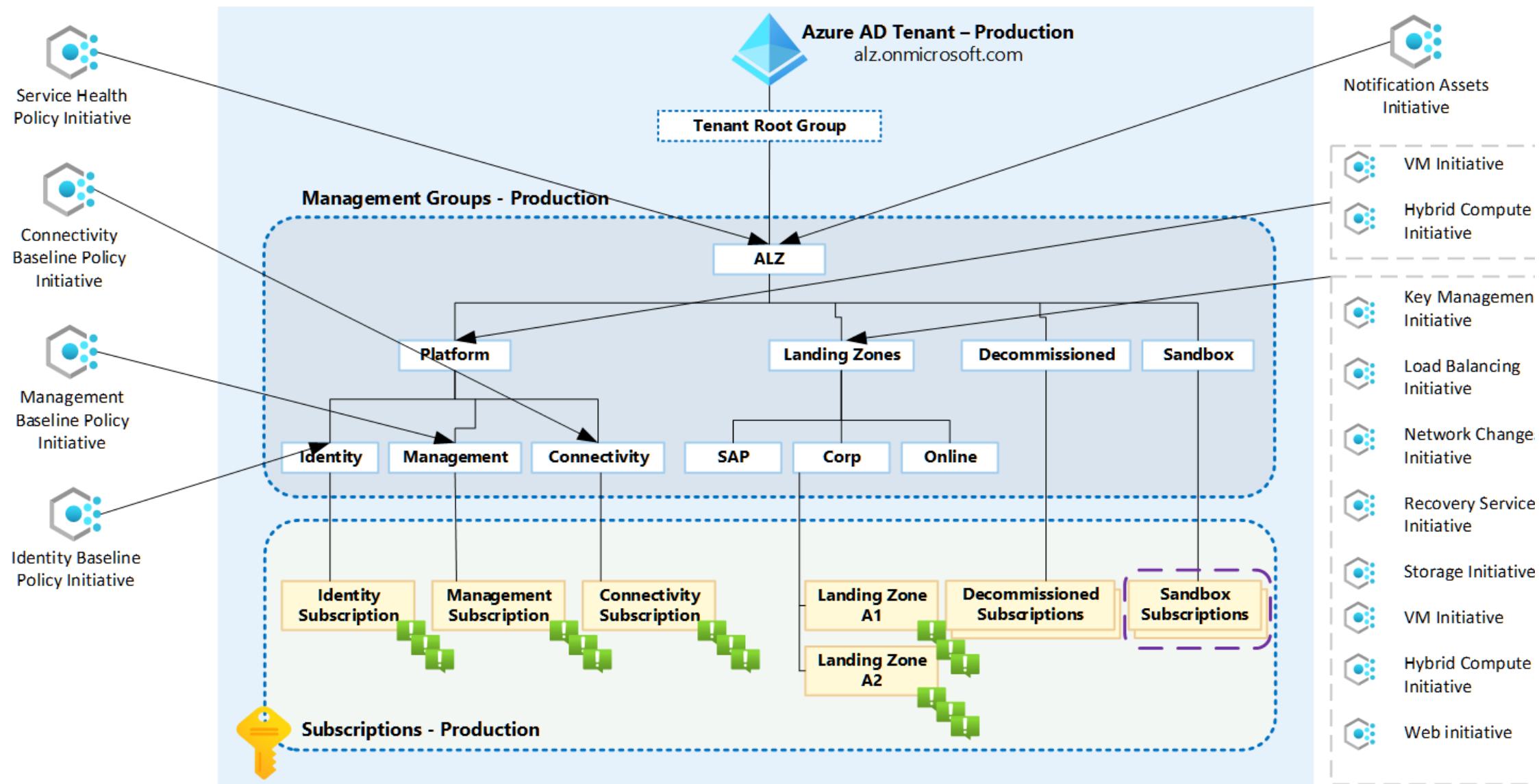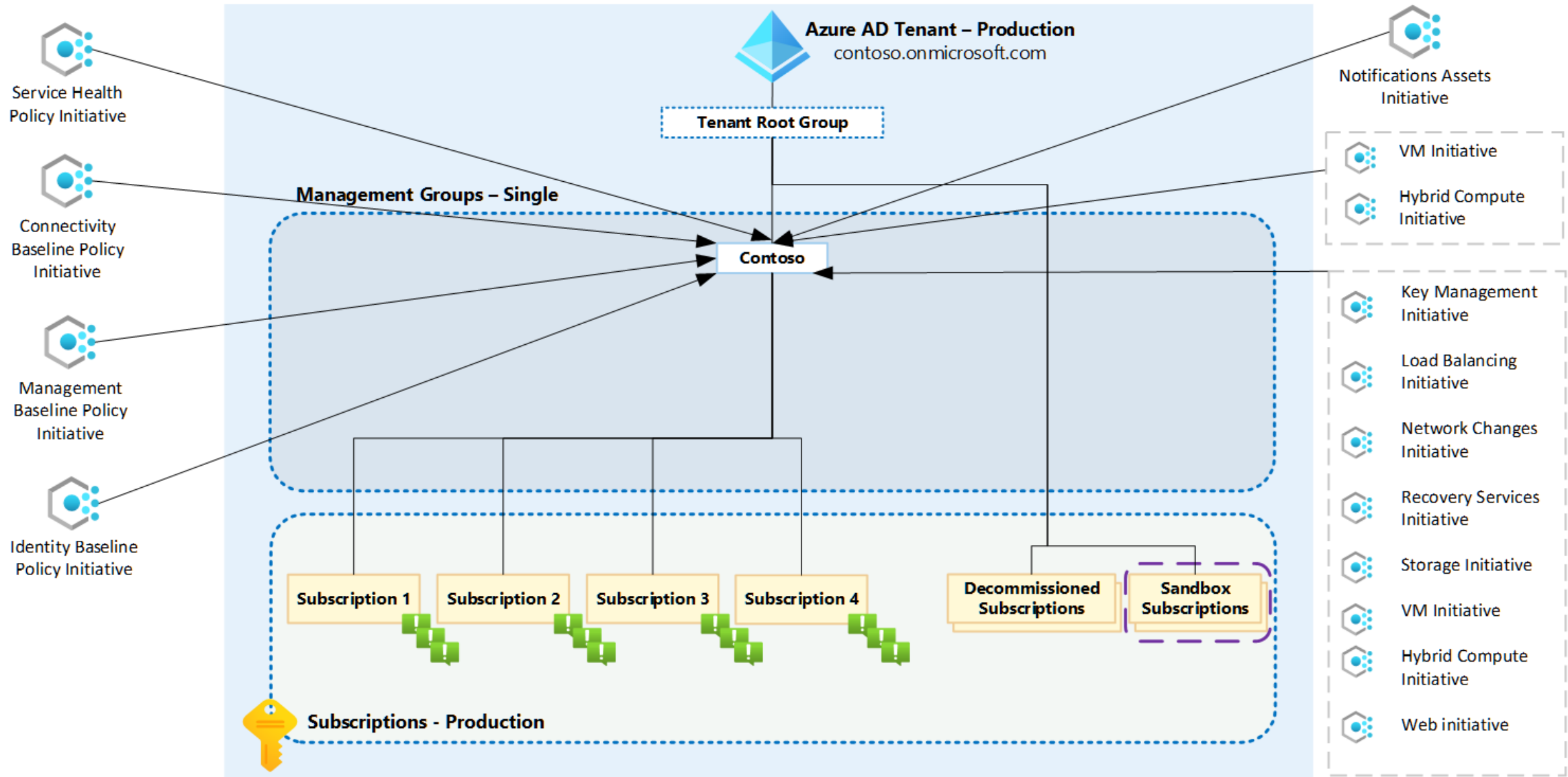
Policy | Definitions ...

Search

- Overview
- Compliance
- Remediation
- Events
- Authoring
  - **Definitions**
  - Assignments
  - Machine Configuration
  - Exemptions

+ Policy definition   + Initiative definition   ↻ Refresh

Search

| amba | Scope : **3 selected**   Definition type : **Initiative**   Policy type : **All policy types**   Category : **All categories**

▦ Edit columns   ⟼ Export to CSV

Name ↕	Latest version (pre... ↕	Definition location ↕	Policies ↕	Type ↕	Definition type ↕	Category ↕
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Connectivity	1.0.0	PSP-Subscriptions	52	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Hybrid Virtual Machines	1.0.0	PSP-Subscriptions	12	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Identity	1.0.0	PSP-Subscriptions	8	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Key Management	1.0.0	PSP-Subscriptions	8	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Load Balancing	1.0.0	PSP-Subscriptions	24	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Management	1.0.0	PSP-Subscriptions	8	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Changes in Network Routing and Security	1.0.0	PSP-Subscriptions	4	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Recovery Services	1.0.0	PSP-Subscriptions	2	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Service Health	1.0.0	PSP-Subscriptions	6	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Storage	1.0.0	PSP-Subscriptions	2	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Azure Virtual Machines	1.0.0	PSP-Subscriptions	11	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) for Web	1.0.0	PSP-Subscriptions	9	Custom	Initiative	Monitoring
Deploy Azure Monitor Baseline Alerts (AMBA-ALZ) - Notification Assets	1.0.0	PSP-Subscriptions	2	Custom	Initiative	Monitoring

	Name ↑		Type	Location
☐	Activity Log Storage Account Delete	···	Activity log alert rule	Global
☐	ActivityNSGDelete	···	Activity log alert rule	Global
☐	id-amba-prod-001	···	Managed Identity	West Europe
☐	VSE Subscription MCT - MPN-VMHeartBeatAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMHighCPUAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMHighDataDiskReadLatencyAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMHighDataDiskWriteLatencyAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMHighNetworkInAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMHighNetworkOutAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMHighOSDiskReadLatencyAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMHighOSDiskWriteLatencyAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMLowDataDiskSpaceAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMLowMemoryAlert	···	Log search alert rule	West Europe
☐	VSE Subscription MCT - MPN-VMLowOSDiskSpaceAlert	···	Log search alert rule	West Europe

M C 2

	Name ↑		Type	Location
☐	🖥️ contoso-demo-linux-vm	⋯	Virtual machine	West Europe
☐	🖧 contoso-demo-linux-vm-nic	⋯	Network Interface	West Europe
☐	🗄️ contoso-demo-linux-vm_OsDisk_1_8165c21a14b448be8b82850660dfε		Disk	West Europe
☐	🛡️ contoso-demo-nsg	⋯	Network security group	West Europe
☐	<⋅⋅> contoso-demo-vnet	⋯	Virtual network	West Europe
☐	⚠️ contoso-demo-vnet-DDOSAttackAlert	⋯	Metric alert rule	Global
☐	🖥️ contoso-demo-win-vm	⋯	Virtual machine	West Europe
☐	🖧 contoso-demo-win-vm-nic	⋯	Network Interface	West Europe
☐	🗄️ contoso-demo-win-vm_OsDisk_1_0d60f42deb3944c29b2431250f1e0a		Disk	West Europe

M C 2

Alert rules

...

+ Create   ⊞ Columns   ↻ Refresh   ↓ Export to CSV   ⟳ Open query   🗑 Delete   ▷ Enable   ☐ Disable

🔍 Search | Subscription : **3 selected** | Target scope : **all** | Target resource type : **all** | Signal type : **all** | Severity : **all** | Status : **Enabled** | 🏷 _deployed_by_amba equals **True** ✕ | 🏷 Add tag filter | No group

Name ↑↓	Condition	Severity ↑↓	Target scope	Target resource type	Signal type ↑↓	Status ↑↓
☐ Activity Log Storage Account Delete	Category=Administrative, Operation name=Microsoft.Storage/storageAccounts/delete	4 - Verbose	VSE Subscription MCT - MPN	Subscription	Activity log	✅ Enabled
☐ ActivityNSGDelete	Category=Administrative, Operation name=Microsoft.Network/networkSecurityGroups/delete	4 - Verbose	VSE Subscription MCT - MPN	SubscriptioN	Activity log	✅ Enabled
☐ Activity Log Storage Account Delete	Category=Administrative, Operation name=Microsoft.Storage/storageAccounts/delete	4 - Verbose	VSE Subscription Wortell - MPN	Subscription	Activity log	✅ Enabled
☐ Activity Log Storage Account Delete	Category=Administrative, Operation name=Microsoft.Storage/storageAccounts/delete	4 - Verbose	DemoSubcription	Subscription	Activity log	✅ Enabled
☐ ActivityKeyVaultDelete	Category=Administrative, Operation name=Microsoft.KeyVault/vaults/delete	4 - Verbose	DemoSubcription	SubscriptioN	Activity log	✅ Enabled
☐ ActivityLAWorkspaceDelete	Category=Administrative, Operation name=Microsoft.OperationalInsights/workspaces/delete	4 - Verbose	DemoSubcription	Subscription	Activity log	✅ Enabled
☐ ActivityLAWorkspaceRegenKey	Category=Administrative, Operation name=Microsoft.OperationalInsights/workspaces/regeneratesharedkey/action	4 - Verbose	DemoSubcription	Subscription	Activity log	✅ Enabled
☐ ActivityNSGDelete	Category=Administrative, Operation name=Microsoft.Network/networkSecurityGroups/delete	4 - Verbose	DemoSubcription	SubscriptioN	Activity log	✅ Enabled
☐ ResourceHealthUnhealthyAlert	Previous resource status=All, Current resource status=Degraded and 1 more	4 - Verbose	All resources in 'DemoSubcription'	All	Resource health	✅ Enabled
☐ ServiceHealthAdvisoryEvent	Service names=All, Event types=All	4 - Verbose	DemoSubcription	Subscription	Service health	✅ Enabled
☐ ServiceHealthIncident	Service names=All, Event types=All	4 - Verbose	DemoSubcription	Subscription	Service health	✅ Enabled
☐ ServiceHealthPlannedMaintenance	Service names=All, Event types=All	4 - Verbose	DemoSubcription	Subscription	Service health	✅ Enabled
☐ ServiceHealthSecurityIncident	Service names=All, Event types=All	4 - Verbose	DemoSubcription	Subscription	Service health	✅ Enabled
☐ policytest80aa-AvailabilityAlert	Availability < 90	1 - Error	policytest80aa	Storage account	Metrics	✅ Enabled
☐ policytest80bb-AvailabilityAlert	Availability < 90	1 - Error	policytest80bb	Storage account	Metrics	✅ Enabled
☐ demo93fb-AvailabilityAlert	Availability < 90	1 - Error	demo93fb	Storage account	Metrics	✅ Enabled

🔍 Search

⚙ Manage action groups   ＋ Create action group

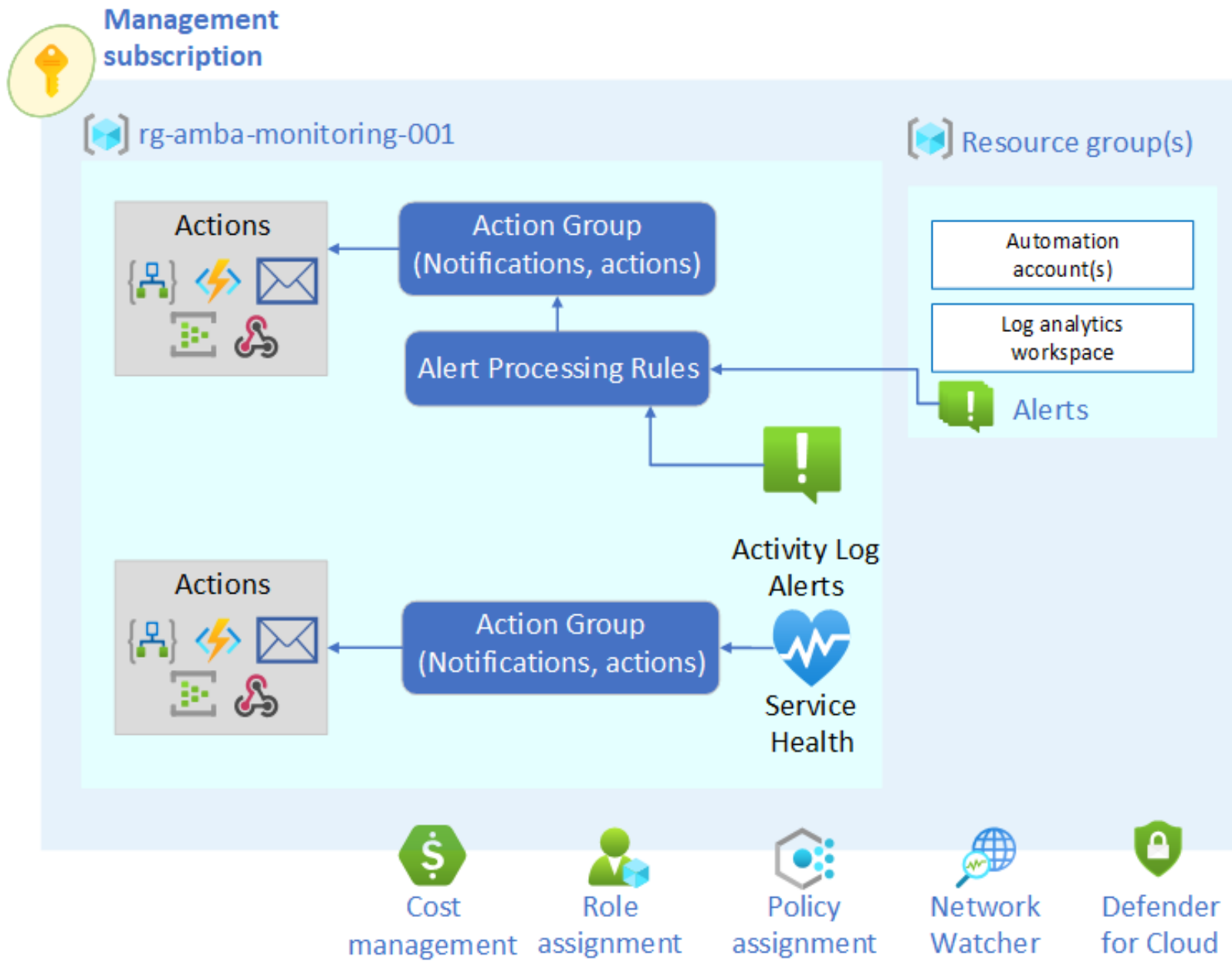| Overview |
| Activity log |
| Access control (IAM) |
| Tags |
| Diagnose and solve problems |
| History |
| Resource visualizer |

An action group invokes a defined set of notifications and actions when an alert is triggered. Learn more

ⓘ No action group selected yet

⌄ Settings
 🔒 Locks
 🔑 Identity (preview)

⌄ Alert rule configuration
 📝 **Actions**

⌄ Automation
 ▪ CLI / PS

M C C²

How can you make sure you deploy a SPECIFIC version of AMBA?

We would love to hear your feedback!

Session feedback available in home feed of the app after the session

run events

Thank You!