| Id | Nazwa polityki | Opis | Referencja | Efekt działania polityki |
|---|---|---|---|---|
| 0 | Custom subscription owner roles should not exist | Polityka nie pozwala na utworzenie roli własne, która jest właścicielem subskrypcji. | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/CustomSubscription_OwnerRole_Audit.json | Audit |
| 1 | Allowed locations | Polityka wymuszająca tworzenie zasobów w określonym regionie | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/AllowedLocations_Deny.json | Deny |
| 2 | Allowed locations for resource groups | Polityka wymusza tworzenie grup zasobów w określonych lokalizacjach | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/ResourceGroupAllowedLocations_Deny.json | Deny |
| 3 | Audit resource location matches resource group location | Sprawdzaj czy zasoby w grupie zasobów są w tej samej lokalizacji co grupa zasobów | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/ResourcesInResourceGroupLocation_Audit.json | Audit |
| 4 | Require a tag and its value on resources | Polityka wymuszająca utworzenie tagu wraz z wartością ze zdefiniowanej listy na zasobach | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Tags/RequireTagAndValue_Deny.json | Deny |
| 5 | Allowed resources types | Polityka ogranicza typy zasobów, które mogą być używane przez organizację | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/AllowedResourceTypes_Deny.json | Deny |
| 6 | Not allowed resource types | Lista usług, które nie są dopuszczone przez organizację | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/General/InvalidResourceTypes_Deny.json | Deny |
| 7 | Inherit a tag from the resource group | Polityka wymusza dziedziczenie na zasobie wskazanego tagu z grupy zasobów | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Tags/InheritTag_AddOrReplace_Modify.json | Modify |
| 8 | Require a tag on resource groups | Wymagaj określonych tagów na grupie zasobów | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Tags/ResourceGroupRequireTag_Deny.json | Deny |
| 9 | SSH access from the Internet should be blocked | Dostęp SSH do maszyn powinien być zablokowany (z sieci Internet) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/NetworkSecurityGroup_SSHAccess_Audit.json | Deny |
| 10 | RDP access from the Internet should be blocked | Dostęp RDP do maszyny powinien być zablokowany (z sieci Internet) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/NetworkSecurityGroup_RDPAccess_Audit.json | Deny |
| 11 | Disk encryption should be applied on virtual machines | Dyski maszyny wirtualnej powinny być zaszyfrowane | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_UnencryptedVMDisks_Audit.json | Audit |
| 12 | Storage account public access should be disallowed | Dostęp publiczny do konta składowania danych powinien zostać zablokowany | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Storage/ASC_Storage_DisallowPublicBlobAccess_Audit.jsonhttps://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Storage/ASC_Storage_DisallowPublicBlobAccess_Audit.json | Disabled |
| 13 | Azure Cache for Redis should reside within a virtual network | Usługa Azure Redis Cache powinna pracować w dedykowanej sieci wirtualnej | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Cache/RedisCache_CacheInVnet_Audit.json | Disabled |
| 14 | Only secure connections to your Azure Cache for Redis should be enabled | Połączenia do usługi Redis Cache mogą być wykonywane tylko z użyciem SSL | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Cache/RedisCache_AuditSSLPort_Audit.json | Disabled |

| | | | | |
|---|---|---|---|---|
| 14 | Container registries should use private links | Usługa Container Registry powinna używać tylko Private Endpointów | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Container%20Registry/ACR_PrivateEndpointEnabled_Audit.json | Disabled |
| 15 | Private endpoint should be configured for Key Vault | Usługa KeyVault powinna używać Private Endpoints | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Key%20Vault/AzureKeyVaultPrivateEndpointEnabled_Audit.json | Disabled |
| 16 | Network interfaces should not have public IPs | Interfejsy sieciowe nie powinny używać publicznych adresów IP | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/NetworkPublicIPNic_Deny.json | Disabled |
| 17 | Network Watcher should be enabled | Network Watcher powinien być włączony w ramach subskrypcji | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/NetworkWatcher_Enabled_Audit.json | auditIfNotExist |
| 18 | Public network access on Azure SQL Database should be disabled | Dostęp publiczny do usługi Azure SQL Database powinien zostać zablokowany | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/SqlServer_PublicNetworkAccess_Audit.json | Disabled |
| 19 | Public network access should be disabled for MariaDB servers | Dostęp publiczny do usługi Maria DB powinien zostać zablokowany | Public network access should be disabled for MariaDB servers | Disabled |
| 20 | Public network access should be disabled for MySQL flexible servers | Publiczny dostęp do usługi MySQL w wersji Flexible powinien zostać zablokowany | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/MySQL_FlexibleServers_DisablePublicNetworkAccess_Audit.json | Disabled |
| 21 | Public network access should be disabled for MySQL servers | Publiczny dostęp do usługi MySQL powinien zostać zablokowany | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/MySQL_DisablePublicNetworkAccess_Audit.json | Disabled |
| 22 | Public network access should be disabled for PostgreSQL flexible servers | Publiczny dostęp do usługi PostgreSQL powinien zostać zablokowany | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/SQL/PostgreSQL_FlexibleServers_DisablePublicNetworkAccess_Audit.json | Disabled |
| 23 | Storage account should use a private link connection | Konto składowania danych powinno używać połączenia połączenia Private Link | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Storage/StorageAccountPrivateEndpointEnabled_Audit.json | Disabled |
| 24 | Allowed virtual machine size SKUs | Dopuszczona lista typów wielkości maszyn dla środowiska | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Compute/VMSkusAllowed_Deny.json | Disabled |
| 25 | Role-Based Access Control (RBAC) should be used on Kubernetes Services | Klaster K8s (AKS) musi używać RBAC | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Security%20Center/ASC_EnableRBAC_KubernetesService_Audit.json | Dev&Test - Audit<br>PRD - Disabled |
| 26 | Do not allow privileged containers in Kubernetes cluster | Polityka nie pozwala na uruchamianie kontenerów w trybie uprzywilejowanym | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Kubernetes/ContainerNoPrivilege.json | Dev&Test - Audit<br>PRD - Disabled |
| 27 | Enforce internal load balancers in Kubernetes cluster | Klaster AKS musi używać tylko prywatnych Load Balancer'ów | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Kubernetes/LoadbalancerNoPublicIPs.json | Disabled |
| 28 | Ensure container CPU and memory resource limits do not exceed the specified limits in Kubernetes cluster | Kontenery uruchomione na klastrze muszą posiadać limity na użyte zasoby CPU oraz RAM | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Kubernetes/ContainerResourceLimits.json | Dev&Test - Audit<br>PRD - Disabled |
| 29 | Kubernetes clusters should not allow container privilege escalation | Polityka nie pozwala używać kontenerom esklaesklacji uprawnień | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Kubernetes/ContainerNoPrivilegeEscalation.json | Disabled |
| 30 | Network interfaces should disable IP forwarding | Interfejsy sieciowe nie mogę forwardować ruchu (użycie IP Forwarding) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/NetworkIPForwardingNic_Deny.json | Disabled |

| | | | | |
|---|---|---|---|---|
| 31 | Flow log should be configured for every network security group | Wszystkie Network Security Group mają włączone Flow Log | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/NetworkSecurityGroup_FlowLog_Audit.json | Audit |
| 32 | Activity log should be retained for at least one year | Log aktywności w ramach subskrypcji musi być utrzymywany przez minimum rok | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/ActivityLogRetention_365orGreater.json | Enabled |
| 33 | Azure subscriptions should have a log profile for Activity Log | Polityka wymusza by Activity Log miał profil eksportowania zdarzeń np. do konta składowania danych lub Log Analytics | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/Logprofile_activityLogs_Audit.json | AuditIfNotExists |
| 34 | Azure Monitor should collect activity logs from all regions | Usługa Azure Monitor ma włączone zbieranie logów w ramach wszystkich regionów | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/ActivityLog_CaptureAllRegions.json | AuditIfNotExists |
| 35 | The Log Analytics agent should be installed on Virtual Machine Scale Sets | Agent Log Analytics jest instalowany na maszynach w ramach VMSS | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/VMSS_LogAnalyticsAgent_AuditIfNotExists.json | AuditIfNotExists |
| 36 | Deploy Diagnostic Settings for Event Hub to Event Hub | Polityka ustawia logowanie zdarzeń z Event Hub do Event Hub (dla potrzeb potencjalnej integracji z SIEM) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/EventHub_DeployDiagnosticLog_Deploy_EventHub.json | AuditIfNotExists |
| 37 | Deploy Diagnostic Settings for Stream Analytics to Event Hub | Polityka ustawia logowanie zdarzeń z Stream Analytics do Event Hub (dla potrzeb potencjalnej integracji z SIEM) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/StreamAnalytics_DeployDiagnosticLog_Deploy_EventHub.json | AuditIfNotExists |
| 38 | The Log Analytics agent should be installed on virtual machines | Agent Log Analytics powinien być instalowany na każdej maszynie wirtualnej | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/VirtualMachines_LogAnalyticsAgent_AuditIfNotExists.json | DeployIfNotExists |
| 39 | Deploy Diagnostic Settings for Key Vault to Log Analytics workspace | Polityka ustawia logowanie zdarzeń z Key Vault do Event Hub (dla potrzeb potencjalnej integracji z SIEM) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/KeyVault_DeployDiagnosticLog_Deploy_LogAnalytics.json | DeployIfNotExists |
| 40 | Deploy Log Analytics agent for Linux virtual machine scale sets | Zainstaluj agenta Log Analytics na maszynach Linux w ramach VMSS | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/LogAnalyticsExtension_Linux_VMSS_Deploy.json | DeployIfNotExists |
| 41 | Deploy Log Analytics agent for Linux VMs | Zainstaluj agenta Log Analytics na maszynach Linux | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/LogAnalyticsExtension_Linux_VM_Deploy.json | DeployIfNotExists |
| 42 | Deploy Diagnostic Settings for Data Lake Storage Gen1 to Event Hub | Polityka ustawia logowanie zdarzeń z Data Lake do Event Hub (dla potrzeb potencjalnej integracji z SIEM) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/DataLakeStorage_DeployDiagnosticLog_Deploy_EventHub.json | DeployIfNotExists |
| 43 | Deploy Diagnostic Settings for Network Security Groups | Ustaw zbieranie zdarzeń diagnostycznych z NSG | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/DataLakeStorage_DeployDiagnosticLog_Deploy_EventHub.json | DeployIfNotExists |
| 44 | Deploy Diagnostic Settings for Data Lake Analytics to Event Hub | Ustaw zbieranie zdarzeń diagnostycznych z Data Lake do Event Hub | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/DiagnosticSettingsForNSG_Deploy.json | DeployIfNotExists |
| 45 | Deploy Diagnostic Settings for Data Lake Analytics to Log Analytics workspace | Ustaw zbieranie zdarzeń diagnostycznych z Data Lake do Log Analytics | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/DataLakeAnalytics_DeployDiagnosticLog_Deploy_EventHub.json | DeployIfNotExists |
| 46 | An activity log alert should exist for specific Administrative operations | Specjalne czynności administracyjne powinny być logowane | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/ActivityLog_AdministrativeOperations_Audit.json | AuditIfNotExists |
| 47 | Deploy Diagnostic Settings for Service Bus to Event Hub | Polityka ustawia logowanie zdarzeń z Service Bus do Event Hub (dla potrzeb potencjalnej integracji z SIEM) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/ServiceBus_DeployDiagnosticLog_Deploy_EventHub.json | DeployIfNotExists |

| | | | | |
|---|---|---|---|---|
| 48 | Deploy Diagnostic Settings for Search Services to Event Hub | Polityka ustawia logowanie zdarzeń z Search Service do Event Hub (dla potrzeb potencjalnej integracji z SIEM) | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/Search_DeployDiagnosticLog_Deploy_EventHub.json | AuditIfNotExists |
| 49 | An activity log alert should exist for specific Security operations | Specjalne czynności bezpieczeństwa powinno być logowane | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Monitoring/ActivityLog_SecurityOperations_Audit.json | AuditIfNotExists |
| 50 | Audit VMs that do not use managed disks | Audytuj maszyny wirtualne, które nie używają zarządzanych dysków | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Compute/VMRequireManagedDisk_Audit.json | Audit |
| 51 | Container Registry should use a virtual network service endpoint | Usługa do składowania obrazów maszyn powinna wykorzystywać Private Endpoint | https://github.com/Azure/azure-policy/blob/master/built-in-policies/policyDefinitions/Network/VirtualNetworkServiceEndpoint_ContainerRegistry_Audit.json | Audit |